Log File Retention Policy

Institute for Advanced Study

March 8, 2012 (revision 230)

Contents

1 Executive Summary

The Institute for Advanced Study (IAS) creates log files[1] during the course of doing business. Log files are stored for the exclusive use of IAS staff for specific business reasons[2] or to satisfy legal requirements. Log files are destroyed after their business use is completed.

The IAS Computing Department maintains a document titled *Log File Retention Guidelines*, which contains procedures for retaining and destroying log files.

[1] We define log file as *historical digital records concerning the use and operation of a computer system or networked device.*

[2] Examples of business reasons include, but are not limited to: troubleshooting, forensic investigation, statistics, billing, and documentation.

2 Purpose and Scope

The purpose of this this Policy is to identify the retention and destruction rules for log files on computer systems and networked devices that are owned and managed by the IAS. This Policy does not indicate rules for authorized access to log files.

3 Recording and Retention of Log Files

Each computing group must establish, maintain, and make available to the IAS Network and Security Officer a systematic process for the recording, retention, and destruction of log files in accordance with this policy. The destruction of logs must be postponed whenever a subpoena, discovery motion, or other legal notice is received. Such destruction should also be postponed if the material might be needed for an imminent legal action.

3.1 Computing Staff Retention of Log Files for Future Reference

If a log file contains relevant information that is useful for future reference, or for a pending transaction, or could be used as evidence of a management decision, it should be retained.

Staff members are responsible for retaining important logs. If a log is needed for documentation purposes, it is the responsibility of the computing staff to move these specific logs to another IAS-owned system (e.g. a trouble ticketing system) prior to the destruction of the log after it has reached its maximum retention time.

3.2 Log File Rotation

Effort should be made to rotate log files daily if possible. If daily rotation is not possible, then log files should be rotated on the shortest possible time frame.

3.3 Log File Retention Times

Log file retention times are specified in *Log File Retention Guidelines.*

3.4 Centralized Logging Server

In the case of an incident, System Administrators are required to provide adequate logs for investigation.

In order to facilitate this, a centralized logging server has been setup for the IAS community.

Systems that allow inbound connections from the Internet must log to this centralized logging server.

It is encouraged, but not required, for non-Internet facing systems to send their logs to the IAS centralized logging server as well. This will expedite the process of gathering logs in the case of an incident, and will also give insight into unknown issues via log correlation.

4 Destruction of Log Files

Log files must be destroyed when their retention time passes.

When specified for destruction, all original, backups and copies of logs should be destroyed. *For this reason, log files should not be backed up to removable media and should stay on the centralized log server or the local filesystem of the machine on which they are generated. In addition, care should be taken to exclude log files from computer disk images.*

This policy recommends deleting log files as opposed to log entries.

Retention is intended to work on a best-effort approach based on a given log file's rotation schedule. Log files that rotate daily are ideal. In some cases, daily rotation is not possible, so it may be necessary to keep a log file longer than indicated in section 3.3.

Logs should be destroyed in the most destructive and economical way available. The actual deletion methods are specified in *Log File Retention Guidelines*.

5 Enforcement of This Policy

The IAS Network and Security Officer is responsible for enforcing this policy.

6 Changes to The Guidelines

The Strategic Planning Committee (SPC) is responsible for maintaining the *Log File Retention Guidelines*. The SPC must notify computing staff of changes to the *Log File Retention Guidelines*. The SPC may make changes to *Log File Retention Guidelines* whenever necessary, but shall review the *Log File Retention Guidelines* annually.

7 Related Documents

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

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