

NIST 特别出版物 800-92

---

# 计算机安全日志管理指南

## ——国家标准和技术研究所的建议

---

**Karen Kent**

**Muruugiah Souppaya**

美国商务部国家标准和技术研究所

---

NIST 特别出版物 800-92

**NIST**

**National Institute of  
Standards and Technology**  
Technology Administration  
U.S. Department of Commerce

计算机安全日志

管理指南

——国家标准和技术

研究所的建议

---

计算机安全

---

国家标准和技术研究所  
信息技术实验室  
计算机安全处

Gaithersburg, MD 20899-8930

2006 年 9 月



美国商务部  
部长: Carlos M. Gutierrez

技术管理局  
商务部技术副部长: Robert C. Cresanti

国家标准和技术研究所  
所长: William Jeffrey

---

# 目录

## 执行摘要

### 1 概述

- 1.1 权限
- 1.2 目的和范围
- 1.3 适用对象
- 1.4 篇章结构

### 2 计算机安全日志管理概述

- 2.1 计算机安全日志的基础知识
  - 2.1.1 安全软件
  - 2.1.2 操作系统
  - 2.1.3 应用
  - 2.1.4 日志的用处
- 2.2 日志管理的需要
- 2.3 日志管理的挑战
  - 2.3.1 日志生成和存储
  - 2.3.2 日志保护
  - 2.3.3 日志分析
- 2.4 应对挑战
- 2.5 总结

### 3 日志管理基础设施

- 3.1 架构
- 3.2 功能
- 3.3 基于 Syslog 的集中式日志软件
  - 3.3.1 Syslog 格式
  - 3.3.1 Syslog 安全
- 3.4 安全信息和事件管理软件
- 3.5 其他类型日志管理软件
- 3.6 总结

### 4 日志管理规划

- 4.1 定义角色和责任
- 4.2 建立日志策略
- 4.3 确保策略可行
- 4.4 设计日志管理基础设施
- 4.5 总结

### 5 日志管理操作流程

- 5.1 配置日志源
  - 5.1.1 日志的生成
  - 5.1.2 日志的存储和销毁
  - 5.1.3 日志的安全
- 5.2 分析日志数据
  - 5.2.1 获得对日志的理解

- 
- 5.2.2 排列日志条目的优先级
  - 5.2.3 系统基础设施两个层面的分析比较
  - 5.3 响应被识别的事件
  - 5.4 管理长期日志数据存储
  - 5.5 提供其他操作支持
  - 5.6 进行测试和检验
  - 5.7 总结
- 附录 A 术语表**
- 附录 B 缩略语**
- 附录 C 工具和参考文献**