

ICS 35.240

A 90

GF

公安部计算机信息系统安全产品质量监督检验中心检验规范

MSTL_JGF_04-018 0101—2006

信息安全技术 日志分析产品检验规范

2006-01-01 发布

2006-02-01 实施

公安部计算机信息系统安全产品质量监督检验中心 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 产品安全功能要求	1
4.1 日志收集	1
4.2 日志分析管理	2
4.3 安全功能	2
4.4 审计功能	2
5 产品安全保证要求	3

前 言

为了规范全国日志分析产品的开发与应用，保障公共信息网络安全，根据公安部公共信息网络安全监察局的要求，本规范对日志分析产品提出了安全功能要求和保证要求，作为对其进行检测的依据。

本规范由中华人民共和国公安部公共信息网络安全监察局批准。

本规范起草单位：公安部计算机信息系统安全产品质量监督检验中心。

公安部计算机信息系统安全产品质量监督检验中心负责对本规范的解释、提升和更改。

信息安全技术 日志分析产品检验规范

1 范围

本规范规定了日志分析产品的安全功能要求和安全保证要求。
本规范适用于日志分析产品的开发及检测。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求（idt ISO/IEC 15408-3:1999）

3 术语和定义

3.1 日志分析产品

通过代理方式或标准端口集中接收日志信息，并对所收集的日志信息进行统计分析的产品。

3.2 审计日志

指日志分析产品自身审计产生的信息。

3.3 日志信息

指各种设备（安全设备、网络设备、操作系统、应用系统、备份系统等）所产生的日志。

3.4 审计信息

指所有的审计日志和日志信息。

3.5 日志数据源

用以产生日志信息的软件系统或硬件设备。

3.6 审计中心

用于完成日志信息的分析处理功能的功能模块。

3.7 日志代理

为获取特定设备上的日志信息而运行在该设备上的功能模块

4 产品安全功能要求

4.1 日志收集

4.1.1 数据源控制

提供对日志数据源的授权控制机制，只有授权的日志数据源所发送的日志信息才能被审计中心接收。

4.1.2 基于标准的日志获取

支持标准 Syslog 格式日志或 SNMP Trap 格式日志的接收。

4.1.3 基于代理的日志获取

提供代理机制获取其日志信息，如操作系统日志，安全设备报警信息等。

4.1.4 数据源范围

数据源可包括：安全设备（防火墙，IDS 等），网络设备（路由器，交换机等），操作系统的系统日

志 (Windows, Linux 等); 应用系统 (如 FTP、WEB 服务器等)。

4.1.5 日志格式的统一

能对多种日志进行集中分析和处理, 能够将各种不同格式的日志格式化为统一的日志数据格式。且格式化时不能造成字段丢失。

4.1.6 日志数据的预处理

提供基于一定策略对原始日志数据进行筛选等预处理功能, 预处理工作应该在将原始日志存入数据库前完成。

4.1.7 防止数据丢失

当与审计中心连接出现故障时, 要有一定的措施防止日志信息丢失。确保该时段内的各项日志信息在连接恢复正常之后续传到审计中心。

4.2 日志分析管理

4.2.1 日志实时监视

能够对部分或者全部数据源所产生的日志信息进行实时监视。

4.2.2 审计代理状态监视

能够监视日志代理的状态, 查看其运行是否正常等。

4.2.3 报警

可对指点的事件提供报警功能, 报警方式可以为email、短信等。

4.2.4 条件查询

提供基于时间、源地址、目的地址、协议类型、危险级别等字段的组合查询。

4.2.5 统计报表

能够手动或自动生成统计报表。至少能按各数据源生成报表。

4.2.6 报表格式

报表应至少支持一种常用的文件格式 (如HTML、XLS等), 如使用专有报表格式, 必须提供报表浏览工具。

4.2.7 数据库支持

日志信息存储应支持一个常用的数据库 (如MySQL, Oracle等)

4.2.8 日志数据管理

应能够对日志数据进行备份/删除, 应提供数据的导入/导出功能。

4.3 安全功能

4.3.1 管理员身份鉴别

应保证只有授权管理员和可信主机才有权使用产品的管理功能, 具备对授权管理员和可信主机进行身份鉴别的功能。

4.3.2 管理员权限

- a) 管理员属性修改 (更改密码等);
- b) 启动、关闭全部或部分监测功能;
- c) 修改日志分析产品其它安全策略。

4.4 审计功能

4.4.1 审计数据生成

应至少能对下列事件进行审计:

- a) 日志分析产品的启动和关闭;
- b) 鉴别成功和失败;
- c) 其它重要操作行为, 如增加、删除管理员, 存档、删除、清空日志等。

应在每一个日志记录中记录事件发生的日期和时间、事件描述。

4.4.2 审计管理

应提供下列审计日志管理功能：

- a) 只允许授权管理员访问审计日志；
- b) 提供对审计日志的查询功能；
- c) 授权管理员能存档、删除和清空审计日志。

5 产品安全保证要求

保证要求按 GB/T 18336.3—2001 第二级执行。
