

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_04-021 0101—2006

信息安全技术 数据库安全审计产品检验规范

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 审计功能要求	1
4.2 自身安全功能要求	2
5 产品安全保证要求	3
6 数据库安全审计产品安全技术要求的等级划分	3

前 言

为了规范全国数据库安全审计产品的开发与应用，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，本规范对数据库安全审计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 数据库安全审计产品检验规范

1 范围

本规范规定了数据库安全审计产品的安全功能要求和安全保证要求。
本规范适用于数据库安全审计产品的开发及检测。

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

下列术语和定义适用于本规范：

3.1 数据库安全审计

数据库安全审计产品是对网络中指定数据库的使用状态进行跟踪并记录的产品。

3.2 审计日志

审计日志是指数据库安全审计产品自身审计产生的信息。

3.3 审计记录

审计记录是指跟踪指定数据库的使用状态产生的信息。

3.4 审计信息

审计信息是指所有的审计日志和审计记录的总称。

4 产品安全功能要求

4.1 审计功能要求

4.1.1 审计记录

4.1.1.1 数据库访问信息采集

应对下列数据库访问内容进行审计

- a) 访问对象和被访问对象：应记录访问的用户名和被访问对象的名称（包括数据库服务器名称，数据库名称和表名等等）对于网络数据库安全审计产品，还必须对网络数据库通讯的源地址和目标地址（地址包括 IP 地址、MAC 地址）进行记录；
- b) 访问时间：应记录用户访问数据库的时间；
- c) 访问类型：应记录用户对数据库服务器的各种操作（包括读、写、查询、添加、修改以及删除等操作）；
- d) 访问内容：应记录用户访问的具体数据。

4.1.1.2 审计记录回放

应对部分数据库操作命令进行回放。

4.1.2 审计日志

4.1.2.1 审计日志内容

应记录安全审计产品自身的审计，记录内容至少应包括：

- a) 管理员登陆事件。

- b) 事件日期与时间、主体身份和事件结果（成功或失败）

4.1.2.2 其他审计日志

应记录安全审计产品自身的审计，记录内容至少应包括：

- a) 符合表 1 中的所有可审计事件；
- b) 表 1 细节一栏中指定的附加信息。

表1 可审计事件

事件	细节
所有对审计记录或审计日志的删除或清空	记录时间
从审计记录或审计日志中读取信息	
在信息采集功能运行时所有对审计配置的修改	
所有鉴别机制的使用	位置
对角色中用户组的修改	修改后的用户身份
安全审计系统组件的启动与关闭	

4.1.3 审计查阅

应提供查询审计记录或审计日志的功能。

4.1.4 可理解的格式

应使审计结果为人所理解。

4.1.5 防止审计数据丢失

- a) 产品应将生成的审计记录和审计日志储存于一个永久性的介质中。
- b) 当审计存储耗尽/失败/受攻击情况发生时，产品应确保审计记录和审计日志不被破坏。
- c) 产品应能够制定某种策略，具体处理当审计存储接近最大存储空间时的情况。（例如：安全审计产品可“忽略可审计事件”或“覆盖所存储的最早的审计记录”或“阻止产生所有可审计事件（除有特权的授权用户外）”，并发送一个告警信息。）

4.1.6 可选择查阅

- a) 应提供基于 4.1.1.1 所列各项条件，对审计记录进行查询和排序的工具；
- b) 应提供基于日期和时间、主体身份、事件类型、相关事件成功或失败等条件，对审计日志进行查询和排序的工具。

4.1.7 分析结果处理

4.1.7.1 审计跟踪管理

授权管理员应能对审计记录进行创建、删除和清空。

4.1.7.2 报表功能

产品应根据审计记录进行统计和分析，并且能根据预先定义的模板生成报表。

4.2 自身安全功能要求

4.2.1 自主访问控制

4.2.1.1 属性定义

产品应为每个管理角色规定与之相关的安全属性，例如管理角色标识、鉴别信息、隶属组、权限等。

4.2.1.2 属性初始化

产品应提供使用默认值对创建的每个管理角色的属性进行初始化的能力。

4.2.2 身份鉴别

4.2.2.1 基本鉴别

产品应在执行任何与授权管理员或用户相关功能之前鉴别授权管理员或用户的身份。

4.2.2.2 鉴别失败处理

产品应能在鉴别尝试达到最大失败次数后，终止用户建立会话的过程。

4.2.3 可信数据

4.2.3.1 远程保密传输

与远程可信组件的传送过程中,产品应提供保护所有的信息数据不被泄漏的功能。

4.2.3.2 审计信息完整性

产品应提供在各种使用情况下,保证所有审计信息完整性的功能:

- a) 应提供防止非授权用户对审计记录或审计日志内容修改或手工添加的功能;
- b) 应提供防止未授权的删除本地存储的审计记录或审计日志的功能。

5 产品安全保证要求

保证要求按 GB/T 18336.3—2001 第二级执行。

6 数据库安全审计产品安全技术要求的等级划分

根据数据库安全审计产品的开发、生产及实际应用情况,数据库安全审计产品的安全功能要求划分成二个等级。

数据库安全审计产品安全技术要求等级划分如表 2 所示。

表2 数据库安全审计产品安全功能等级划分表

功能类	基本要求	增强要求
4.1.1.1 数据库信息采集	√	√
4.1.1.2 审计记录回放		√
4.1.2.1 审计日志内容	√	√
4.2.2.2 其他审计日志		√
4.1.3 审计查阅	√	√
4.1.4 可理解的格式	√	√
4.1.5 防止审计数据丢失		√
4.1.6 可选择查阅		√
4.1.7 分析结果处理		√
4.2.1 自主访问控制	√	√
4.2.2.1 基本鉴别	√	√
4.2.2.2 鉴别失败处理		√
4.2.3 可信数据	√	√
基本要求: 为数据库安全审计产品的最低安全级别。 增强要求: 为进一步提升产品安全功能的附加要求。		