文件编号	HDSAS-BZB-000001
版　　本	V2019Q1_B2019031901
文档密级	公开
受控状态	受控

黑盾数据库安全审计系统

——标准版

福建省海峡信息技术有限公司

版权声明

1. 权利归属

本文档中的 HD-SAS 的所有权和运作权等版权法及有关法律规定的权利和一切商业权益均归福建省海峡信息技术有限公司（下称海峡信息），海峡信息提供的服务将完全按照其发布的本声明以及相关的操作规则严格执行。因 HD-SAS 所产生的一切知识产权归福建省海峡信息技术有限公司，并受版权、商标、标签和其他财产所有权法律的保护。

2. 其它产品说明

本文档中所提及的所有其他名称是各自所有者的品牌、产品、商标或注册商标。

3. 授权声明

任何组织和个人对海峡信息产品的拥有、使用以及复制、修改等涉及版权法等有关法律所规定的权利都必须经过海峡信息书面同意和有效授权。

4. 管理

用户对信息和服务的使用是根据所有适用于海峡信息的国家法律、地方法律和国际公约或协定。

5. 特别提示

- 使用本产品之风险由使用者自行承担。海峡信息对使用本产品不提供任何明示或默示的担保或保证，包括但不限于商业适售性、特定目的之适用性及未侵害他人权利等担保或保证；
- 海峡信息在任何情况下均不就因使用或不能使用本软件而发生的损失（包括但不限于营业利润损失、业务中断、业务信息、文档、数据丢失或其他经济损失）承担赔偿责任，即使已通知本公司有可能发生该损失的亦是如此。本产品并不是对现有的和将来的所有种类的病毒或漏洞均有效，本公司不保证本产品会对目前或将来的任何种类病毒或漏洞皆有效；
- 从本公司获得的任何信息或建议，无论是书面或口头形式，除非另有约定或协议，将不构成本声明之外的任何担保或保证。

6. 有限责任

海峡信息仅就产品说明书中说明的范围承担责任，海峡信息对引起使用或传播的任何损害（包括直

接的、间接的、偶然的、特殊的或继起的损害）不负任何责任（即使已经建议海峡信息这些损害的可能性）。

7. 法律适用

使用海峡信息产品适用海峡信息所在国家的法律法规、国际公约或协定。

8. 目的

本声明仅为文档信息的使用，非为广告或产品背书目的。

9. 争议处理

- 本声明受中华人民共和国法律管辖并按其解释；
- 用户与海峡信息之间因使用本产品所引起的争议由双方当事人协商解决或由有关部门调解；协商或调解不成的，依照中华人民共和国法律相关规定予以解决。

目 录

1 概述

1.1 系统背景

企业机构的信息化程度越高，企业对信息系统的依赖就越强烈，而后台的数据库是信息化系统的心脏，数据库中存放着大量企业的重要信息，例如：财务信息、客户信息、合同等。数据库是企业的核心资产，是最有价值的部分，因此也引起了不少黑客的觊觎。

对信息资产的威胁主要分为两类：一类是破坏，将数据篡改、删除、损坏；另一类是数据泄漏，对机密信息的窃取。

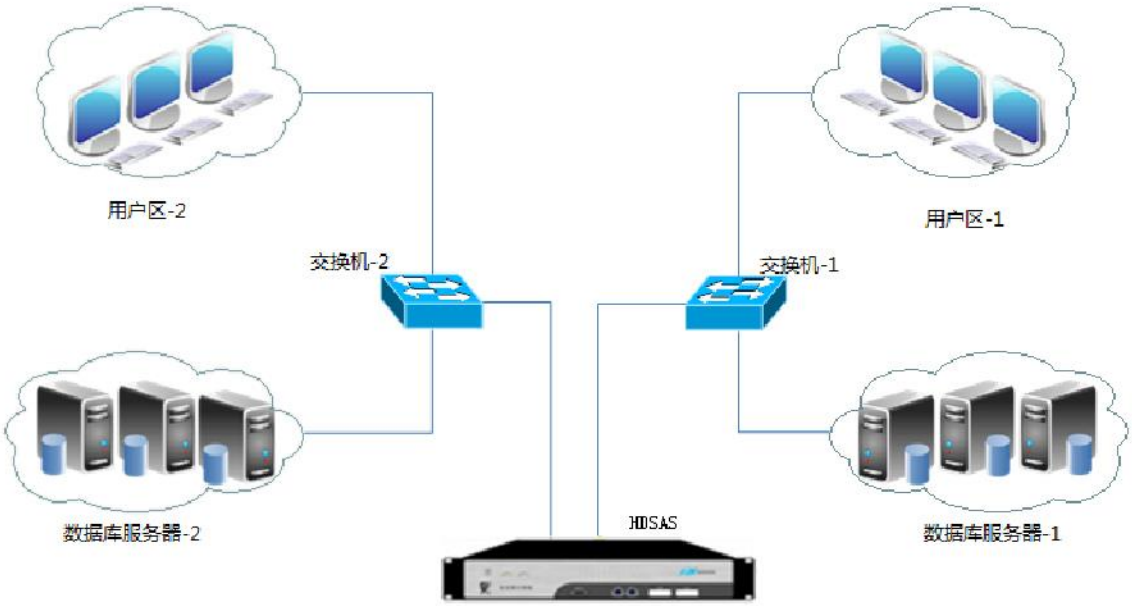
1.2 产品特点

黑盾数据库安全审计系统利用更合理的网络和信息安全技术手段，实现对数据库操作行为审计、深入分析，监测并识别风险事件，及时告警并对其取证保留现场，是多功能为一体的全方位的数据库安全审计系统。

系统支持同时审计多种不同的数据库，具有灵活性和广泛的适用性。

该系统采用网络旁路实时侦听方式，全线速采集网络上所有会话流，对网络中业务系统数据库进行全面的风险分析与安全监控审计、告警。关注核心数据和业务的完全审计，不参与被监控网络的数据传输活动，因此不对网络结构和性能产生任何影响，具有很好的透明性和安全性。

图1-1 典型部署图



1.3 系统功能

系统分为五大模块分别是：监控中心、审计中心、策略中心、报表中心及系统管理。五大模块功能各有侧重点，相互作用，使系统具备了以下功能，帮助系统管理员解决实际问题。

(1) 系统实时监控

不仅对自身性能（CPU 使用率、内存使用率和硬盘使用率）进行状态监控，还对信息系统数据库产生的安全事件进行 24 小时监控，并以统计图表的形式展示，让管理员一目了然。

(2) 事前预防

准确的定位各种风险事件行为，检测到威胁时可根据用户需求进行告警和实时阻断，将业务系统的风险事件防范工作，由被动式的事后分析，提升到主动式全面预防的水平。

(3) 有效、准确的识别规则

任何违反审计规则的操作都会被检测，做到准确、有效地识别具有风险的行为。

(4) 事中现场取证

通过实时监测并智能地分析、还原各种数据库操作，解析数据库操作，还原 SQL 操作语句；跟踪数据库访问过程中的所有细节。提供数据库操作行为、应用服务器行为、终端录像实现事后审计，为追踪、惩罚犯罪份子提供强有力的证据。

(5) 报表管理

除了根据安全经验和行业需求提供了预定义的报表模板外，管理员还可利用自定义报表功能根据需要定制报表。此外还可将生成的报表发送到指定邮箱，方便查阅。此外报表支持导出成 PDF 格式文件。

(6) 审计日志管理

保存大量数据库审计日志的同时，还支持对早期的数据进行归档。当需要时可以通过数据回档的形式调阅早期的数据。解决了海量数据的有效存取的问题，为用户提供更全、更有效的数据。

1.4 系统角色

系统将系统角色划分为四类：系统管理员、系统审计员、系统安全员、系统监察员。每类角色对系统拥有不同的访问、控制权限。具体如下：

(1) 系统管理员（sys）

系统默认用户名及密码为：sys/sys。对系统的主要操作包括：

- 个人信息管理。
- 查看系统运行状态。
- 系统运行参数配置。
- 此外无权操作其他角色功能。

(2) 系统审计员（audit）

系统默认用户名及密码为：audit/audit。对系统的主要操作包括：

- 个人信息管理。
- 查看系统运行状态。
- 系统自身运行日志信息。
- 无权操作其他角色功能。

(3) 系统安全员（sec）

系统默认用户名及密码为：sec/sec。对系统的主要操作包括：

- 个人信息管理。
- 查看系统运行状态。
- 与业务有关的操作及信息查看。
- 无权操作其他角色功能。

三类角色对系统的操作权限不同，分别被赋予了不同的权限，参见表 1-1。

表1-1 各类角色权限分配

一级菜单	二级菜单	sys	audit	sec
监控中心	运行状态	√	√	√
	安全态势	-	-	√
	流量钻取	-	-	√
	统方事件	-	-	√
	事件查看	-	-	√
	入侵事件	-	-	√
	监察视图	-	-	-
审计中心	语句查询	-	-	√
	URL审计	-	-	√
	行为审计	-	-	√
	SQL模板	-	-	√
	因子监测	-	-	√
	网络审计	-	-	√
	对比分析	-	-	√
报表中心	报表任务	-	-	√
	事件报表	-	-	√
	统方报告	-	-	√
	报表查看	-	-	√
策略中心	监听配置	√	-	√
	事件定义	√	-	√
	对象管理	√	-	√
	客户端信息	√	-	√
	敏感信息	√	-	√
	事件响应	√	-	√
	三层关联	√	-	√

一级菜单	二级菜单	sys	audit	sec
	入侵检测规则	√	-	√
	交换机信息	√	-	√
系统管理	网络配置	√	-	-
	用户管理	√	√	√
	系统服务	√	-	-
	日志响应	√	-	-
	数据归档	-	-	√
	调试工具	√	-	-
	配置管理	√	-	-
	系统信息	√	-	-
	管理主机	√	-	-
	运行日志	√	-	-
	操作日志	-	√	√

说明

sys、audit、sec 是系统超级用户，四个超级户默认是不可以被删除，但可以被锁定（但要求创建一个与根用户一样的权限）。

各角色除了上表描述的权限外，还拥有对本组用户增删改查的权限。且 sys 就类似信息科人员，协助纪检科定义准确的统方规则。所以分配他们对象定义及事件定义的权限。

1.5 登录界面说明

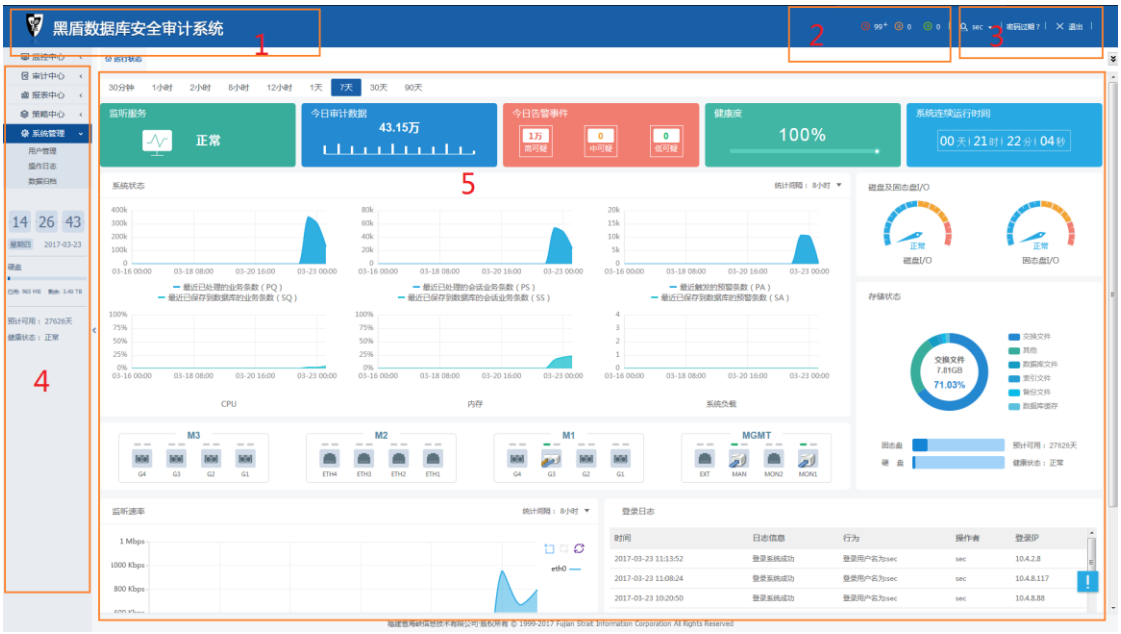
系统登录界面为各个系统角色的登录入口，同时，在登录界面右上角还提供系统配套工具的下载，包含火狐浏览器安装包、历史数据回档客户端、录屏客户端与工具以及流量探针客户端。

图1-2 登录界面

图1-3 工具下载

1.6 主界面说明

图1-4 主界面



上图是系统界面的分布图，每个区分别是：

1、产品名称；2、系统提示栏；3、账户信息；4、左栏菜单；5、功能操作区。

下面逐个介绍各个区的主要功能。

1. 产品版本信息

此处放置的是产品名称。

2. 系统提示栏

本系统中放置了三个图标，分别显示了自系统运行时管理员未查看的高可疑、中可疑、低可疑事件的统计。单击对应的图标会跳转到“事件查看”界面，相关的内容可以参考“事件查看”部分的介绍。如下图所示从左到右依次是高、中、低可疑事件的状态提示。

图1-5 系统提示栏

当统计数量超过 99 条时，系统将显示“99+”，鼠标移动到在数值上可以看到事件的等级和发生统计结果。如下图所示