天翼云 •安全专区•云数据库审计

用户使用指南

中国电信股份有限公司云计算分公司

目录

1 如何开始

1.1 产品概述

1.1.1 特点

数据库审计系统可通过设计其相关业务策略，实现审计符合业务策略的网络行为、跟踪访问重要数据源的网络行为、阻断不符合业务策略的不法网络行为。

数据库审计系统支持按照企业的业务进行策略设计，通过对网络中繁杂的数据操作进行智能识别和解析，能够对数据库的新增、查询、修改、删除以及相关主机协议、部分应用服务的操作进行保全，并还原操作者的操作轨迹，为管理者提供数据异常、泄露以及篡改提供详细依据，为管理者提供追究责任、进行安全改进提供数据支持，并提供长期趋势分析报表，作为企业安全政策以及网络规划的参考。

1.1.2 主要功能

本产品涵盖以下几大功能：

- 审计

➢ 通过对网络行为进行的记录，可用来分析网络状况和确定网络使用者的相关责任的活动。

- 策略：根据业务需求，而制定的网络行为分析引擎。

➢ 产品的核心功能，对网络行为进行采集的分析引擎进行配置，将通过引擎的数据包过滤后，提供给审计功能使用。

➢ 具有丰富的管理配置功能。

- 告警：包含告警规则设置和告警事件的查看功能。

➢ 告警规则：系统对审计事件之间的关系进行形式化描述。针对符合策略的事件进行关联分析。抽取出对于安全管理人员真正有用的安全信息，提供实时告警，从而协助安全管理人员快速识别安全事故。

➢ 告警事件：查看由告警规则产生的事件。

- 报表：包含系统内置报表和自定义报表，能够将业务分析情况以报表的形式提交给指定的部门。

➢ 内置报表：常见通用报表，例如：基本的合规报表。

- 自定义报表：提供编辑报表模板的功能，利于创建基于公司业务要求的报表。
- 系统：对系统内部进行相关的设置，并进行统一的管理。
- 系统配置：配置系统运行参数，包含：服务器配置、备份归档设置以及系统维护等功能。
- 系统维护：对系统的自身的维护信息，包含管理地址、许可导入、时间同步等。

1.1.3 产品价值

对于业务系统的管理审计人员和高层管理者而言，数据库审计系统能够帮助用户达到以下目标：

- 数据操作实监控：对所有外部或是内部用户访问数据库和主机的各种操作行为实时监控；
- 安全预警：对入侵和违规行为进行预警和告警，并能够指导管理员进行应急响应处理；
- 事后调查取证：对于所有行为能够进行事后查询、取证、调查分析，出具各种审计报表报告。

1.1.4 产品描述

本产品是一款硬件设备。

本产品采用旁路方式部署到网络中，不影响网络性能。

本产品随着型号的不同，产品形态会有所区别，但至少具有两个网口：一个管理口，一个网络监听口。

1.2 兼容性

1.2.1 浏览器兼容

本系统采用 B/S 架构，支持 IE8 及以上浏览器、Chrome 浏览器、Firefox 火狐浏览器。为了保证良好的浏览效果，推荐使用 Chrome 浏览器。

1.2.2 屏幕分辨率兼容

本系统仅保证屏幕水平方向像素范围为 1366 到 1920 时的显示效果，推荐使用屏幕分辨率 1920 x 1080（即 1080p）以获得最佳显示体验。

2 系统登录

在需要操作数据库审计系统的机器（称为客户机）上打开 chrome 浏览器，如选择其他浏

览器则需要将访问地址添加进受信任的站点。登录方式请参考“天翼云安全专区安全管理中心使用手册”。

系统采用三权分立的模式，各平台的功能与职责不同，权限不同，相互监督。

角色	基本权限
系统管理员	监控墙、部署方式、数据维护、系统管理、许可证等
安全管理员	监控墙、策略配置、风险检索、报表查看、对象管理等
审计管理员	监控墙、操作日志

3 用户管理

3.1. 添加用户

创建新用户时，只能分配给新用户自己平台的权限，比如系统管理员只能创建具有部署方式、数据维系统管理等权限的用户，可按需分配权限。在导航栏点击用户图标-用户管理-添加，依次输入新用户信息

用户名：testone（不可修改）

真实姓名：Jessica

邮箱：Jessica@163.com

手机号码：17622223333

QQ：963369963

备注：目前居住在深圳市罗湖区 xxx，备用手机号为 17633332222（最长 128 个字符）

权限模块：分配监控墙和许可证模块

点击保存后会提示给该用户分配的初始密码，如图：

新打开浏览器，使用 testone 用户及初始密码进行初登录（建议第一次登录修改密码完善个人信息）。

3.2 编辑用户

点击导航栏用户图标-用户管理菜单，可以看到该平台中所有添加的用户，包括他们的基本信息，在线状态。打开指定用户的锁定状态，该用户被锁定不能登陆。可对用户进行编辑、重置密码、删除、查看详情操作。

注意：可以删除和锁定在线用户。删除会立即提示需要重新登陆，锁定会在下一次登录

4 基本功能审计

4.1. 添加保护对象

登录安全管理平台-点击保护对象-添加一个保护对象，如下所示：

对象名：oracle_object

状态：默认开启

告警：默认关闭（按需开启）

数据库类型：Oracle

版本号：Oracle 11g（选择安装的对应版本号）

Ip 地址：172.23.1.62（可输入 IP 段形式，用 ‘-’ 隔开）

端口号：1521（可输入多端口，用 ‘|’ 隔开）

数据字符集：GB2312

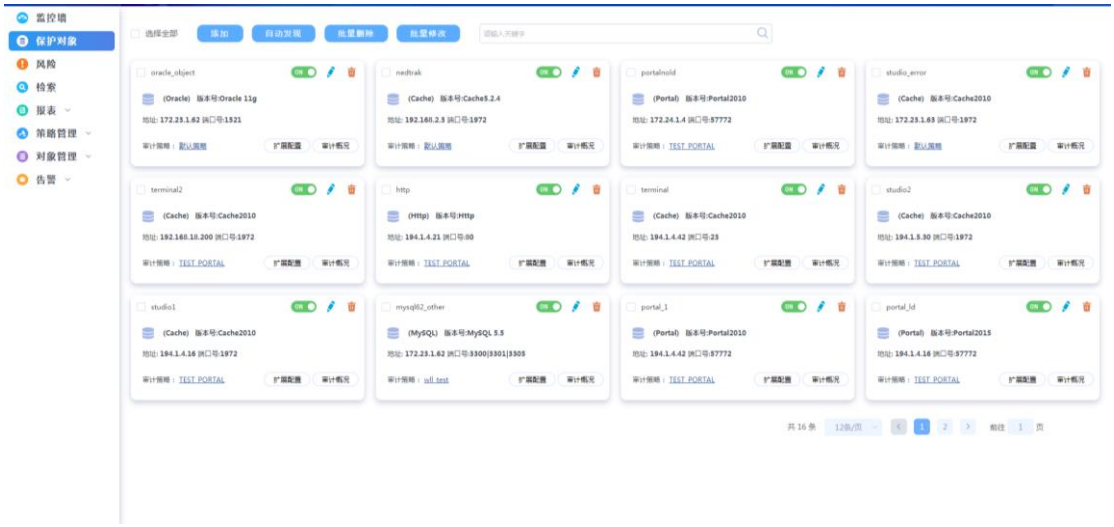
His 产商：空（按需配置）

审计策略：默认策略（按需配置）

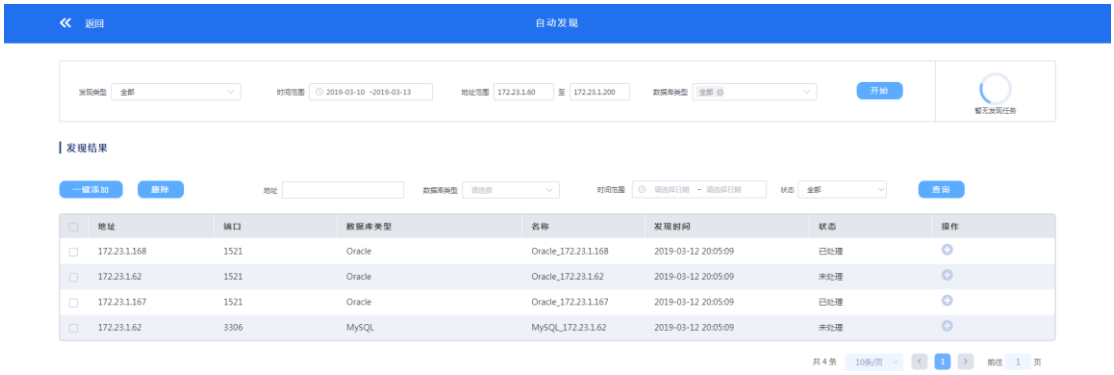
告警策略：空（按需配置）

注意：根据自己数据库安装时的配置选择编码，编码选择错误可能会导致乱码问题。

保存成功后，可对原有配置进行单个编辑，配置扩展配置以及批量修改（状态、策略）。



还有另外一种添加保护对象的方式-自动发现。在保护对象界面点击自动发现按钮，配置扫描范围，根据自动发现扫描出来的对象选择性添加到保护对象中。



注意：配置扩展配置有利于查看审计结果。自动发现暂时只支持扫描默认端口的对象，比如 MySQL 的 3306 端口。

4.2 配置别名

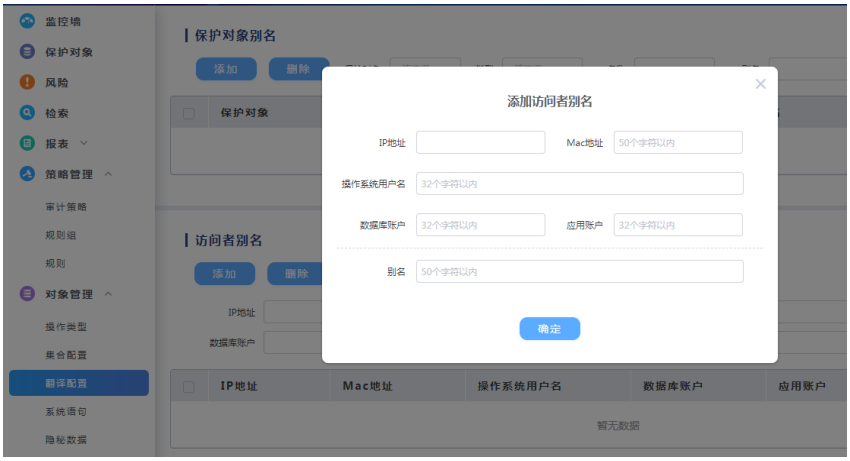
4.2.1 保护对象别名

登录安全平台，点击对象管理-翻译配置-保护对象别名-添加。添加信息如下所示：

设置的别名会在检索中相应的表名、字段名、关键字、客户端进程、翻译字段进行标注翻译，方便识别和查看。

4.2.2 访问者别名

登录安全管理平台，点击对象管理-翻译配置-保护对象别名-添加。翻译成别名，方便在审计结果中直观的看到是谁操作了数据库。

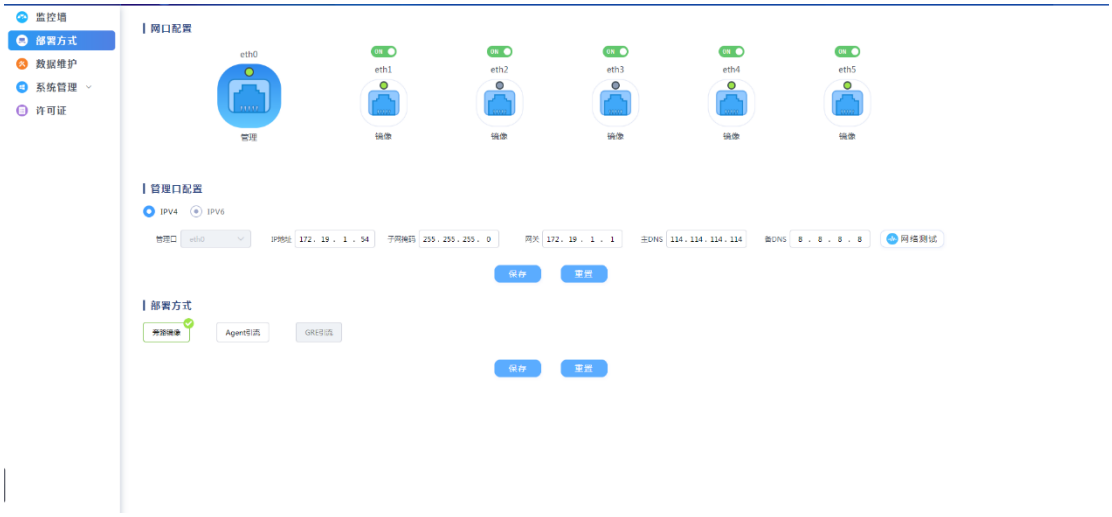


注意：1、对于设置了多个附加条件的，需要同时满足这些条件才会显示别名。2、对于指向同一个访问者的配置，优先显示条件个数多的，条件个数相同的优先显示最后配置的别名。

4.3 审计环境部署

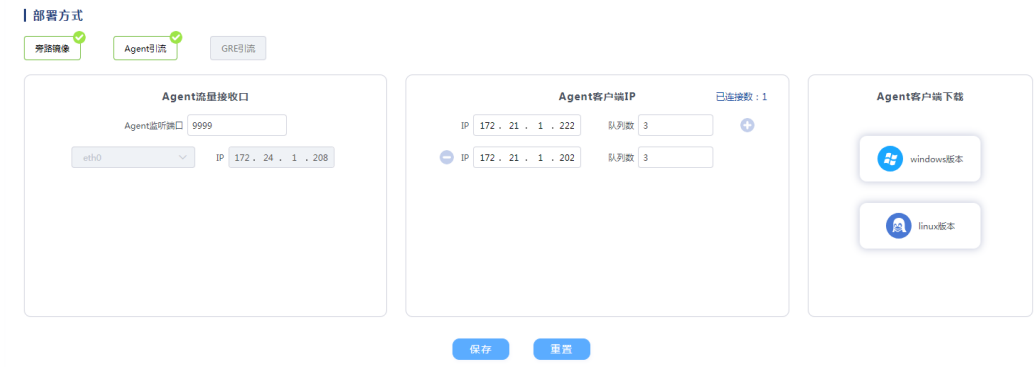
登录系统平台-部署方式。可控制网口运行状态，更改管理口（eth0）配置，配置审计部

署的方式



4.3.1 Agent 引流

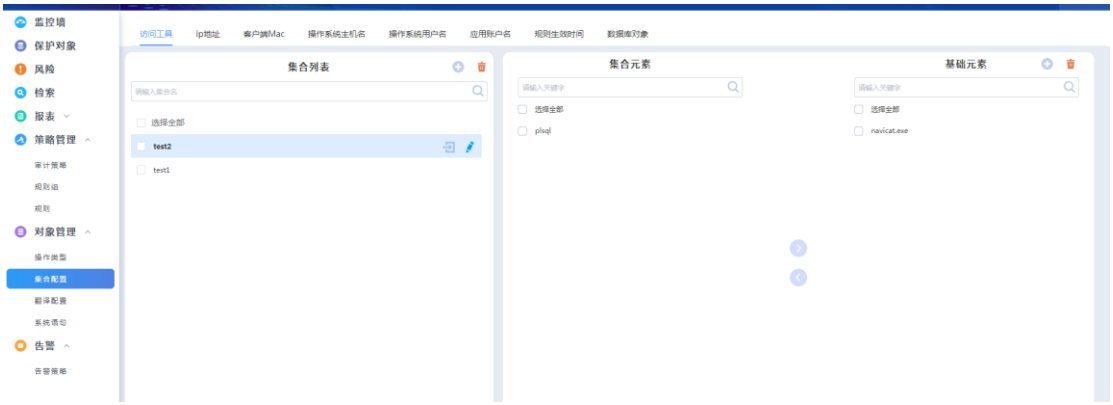
支持通过管理口 eth0 引流方式进行审计，可对多个服务器进行配置引流，下载对应 agent 版本。在 agent 客户端 IP 配置服务器所在的 IP，按需分配队列，总队列加起来不超过 32。



4.4 采集数据和审计查询

4.4.1 审计查询准备

可配置一些基础元素，方便直接在检索中查询。登录安全平台-对象管理-集合配置。在访问工具基础元素中添加客户端程序名 navicat.exe。



在操作系统用户名基础元素中添加用户名 wlli

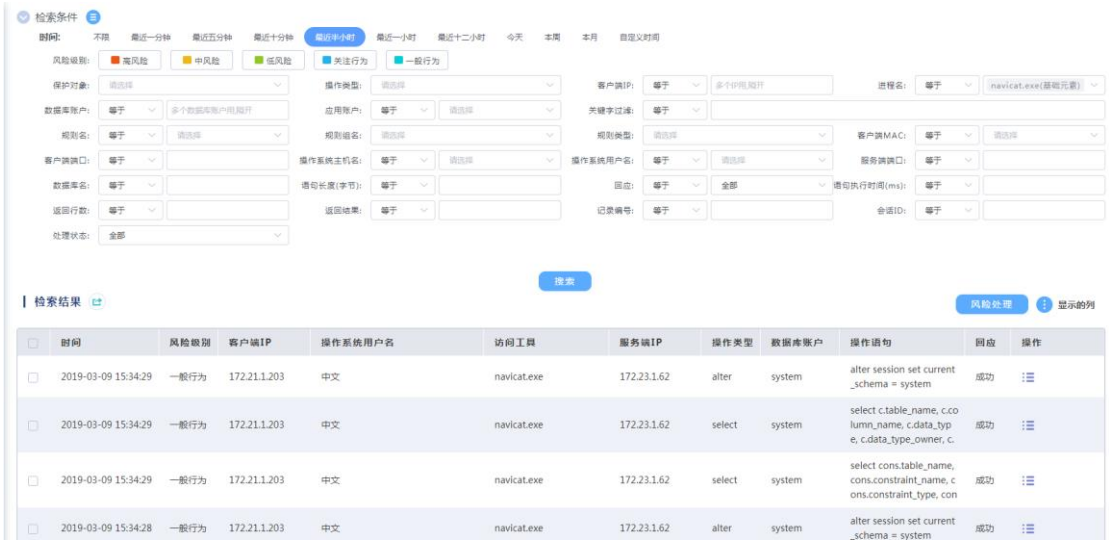
注意：集合配置中的部分基础元素会自动从审计的记录中提取元素，所以，在有审计记录的前提下，无需自己配置基础元素。

4.4.2 操作客户端工具

在操作系统用户名为 wlli 的客户端上，打开 Navicat 客户端工具，连接主机为 172.23.1.62 的 Oracle 数据库，并进行一系列操作。

在安全管理平台上检索模块进行数据查询，可根据自己的需要选择相应的查询条件（每页默认显示 10 条记录）。

在进程名中选择刚才配置的基础元素 navicat.exe 或者包含 navicat.exe 的集合，就可以查询到相关的 navicat 操作的记录了。

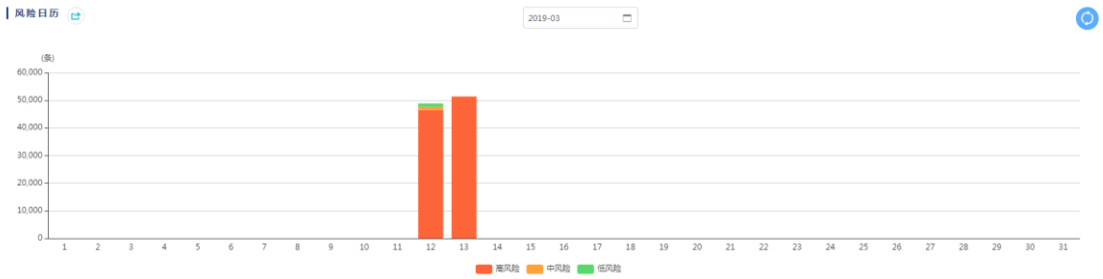


同时在选择了进程名基础上再在用户名中选择 wlli 基础元素进行查询，就只能查询到用户名为 wlli，进程名为 navicat 的记录了，像上图中用户名为中文的记录就查不到了。

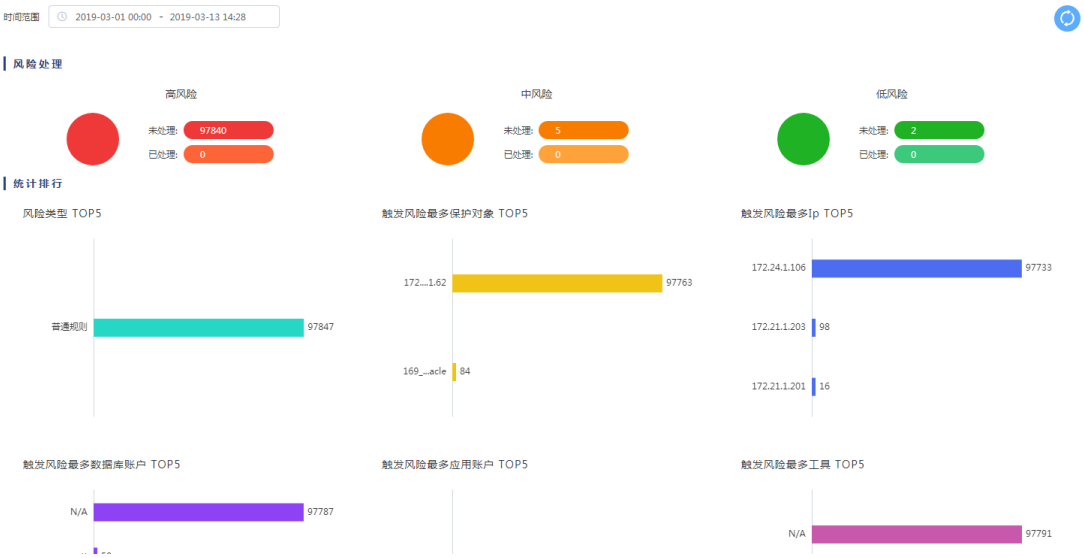
4.5 风险统计查看

登录安全管理平台，直接点击风险，该界面的条形图饼状图均可点击跳转至对应检索记录。

风险日历，展示本月风险级别分布。



可根据时间范围查询风险处理情况以及风险统计情况，如下。



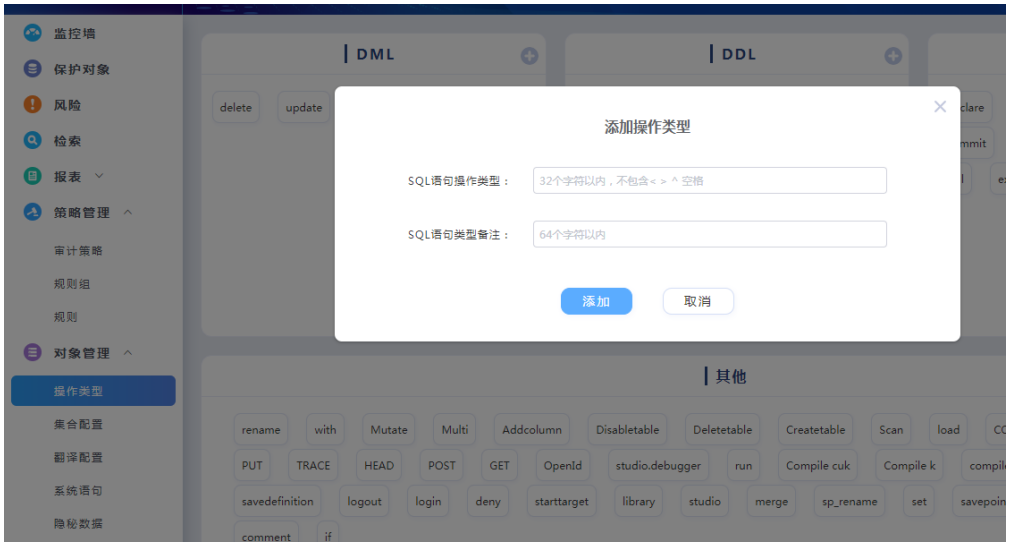
5 审计策略

5.1 规则配置

5.1.1 操作类型配置

除了系统内置的操作类型外，用户还可自行添加操作类型。

安全管理平台-对象管理-操作类型。点击展示框右上角的按钮进行添加，添加完成后还需点击下方保存按钮。



5.1.2 普通规则配置

登录安全管理平台-策略管理-规则。如下图，配置一条规则名为中风险，操作类型为select，关键字为测试的一条普通中风险规则。在高级配置中，可按需配置，这里，我们选择刚刚配置的访问工具 navicat.exe(基础元素)。

再往下，选择语句执行回应为成功，点击添加。

规则配置完毕，用 navicat.exe 登录数据库，凡是操作的 SQL 语句中带有“测试”，且查询成功的行为都会触发 ‘中风险’，用其他客户端工具操作的同样语句不会触发风险。

5.1.3 组合规则配置

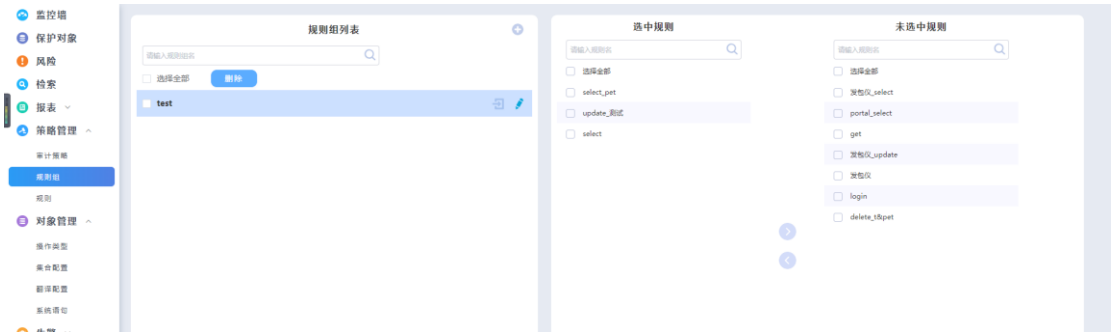
在规则界面中，点击添加规则，下拉框选择规则类型为组合规则，可看见如下界面：

触发的类型可选择组合、统计。

组合规则是根据几个规则在一定时间段内被触发是就会触发风险；统计规则是一定时间内一条规则达到触发的次数就会触发风险。比如我们选择统计规则，命名为统计规则。规则选择上面配置的 select 规则，在 10min 内如果触发了两次 select 规则就会产生一条名为统计规则的高风险。配置界面如下：

5.2 规则组配置

登录安全管理平台-策略管理-规则组。点击规则组列表的按钮，添加一条名为 test 的规则组，选择自己想要的规则添加到该规则组中，如下图：



5.3 审计策略配置

登录安全管理平台-策略管理-审计策略。点击添加按钮，出现弹框界面，添加一条策略名称为“审计策略 test”，审计方式选择全审计，添加自己要应用的规则或者规则组。

如果选了按规则审计，系统只审计那些触发了审计规则的记录。如果有些记录不触发告警也要审计出来，可以设置一些风险行为为‘不审计’的规则。

注意：审计策略应用到保护对象中才生效。同时选择规则和规则组，即使有包含关系也

5.4 系统语句

登录安全管理平台-对象管理-系统语句。将确认正常的操作的 sql 语句标注为系统语句，在以后的审计中将不做审计，比如添加数据库类型为 mysql，操作语句为 select * from pet。则只要操作 mysql 数据库都审计不到这条语句，操作其他数据库的这条语句可以审计

到。

5.5 隐秘数据

登录安全管理平台-对象管理-隐秘数据，将保护对象中的关键数据在审计的返回结果中做隐秘处理，防止二次泄密

6 报表

报表是对审计结果进行分类统计，并以图形和图表的方式展示给管理员，便于管理员查看。

6.1 服务器分析

点击报表-分析报表-服务器分析，可以看到被监测的数据库以及数据库服务性能两张图表。均可根据年份月份保护对象名进行查询，查询结果可以已 excel、word、pdf 形式导出。

6.1.1 被检测的数据库

条形图：显示账户数最多的数据库（Top5）、连接数据库服务的访问者 IP（Top5）

列表：当月操作和登录次数最多的数据库信息列表（Top100）

6.1.2 数据库服务性能

条形图:显示查询语句执行时间分布（Top5）

饼状图：显示繁忙的数据库服务器（按审计对象分，Top5）

列表：当月语句执行时间最长的查询信息列表(Top100)

6.2 源分析

点击报表-分析报表-源分析，可以看到数据库账户、客户端、访问者 IP 三张图表。均可根据年份月份保护对象名或者访问者 ip 进行查询，查询结果可以已 excel、word、pdf 形式导出。

6.2.1 数据库账户

条形图：显示最活跃的数据库账户（Top5）

饼状图：显示活跃数据库账户操作类型分布（Top5）和数据库账户登录数量分布（Top5）

列表：按操作次数由高到低显示当月数据库账户登录和操作信息列表(Top100)

6.2.2 客户端

条形图：使用最少的客户端（根据账户数，Top5）

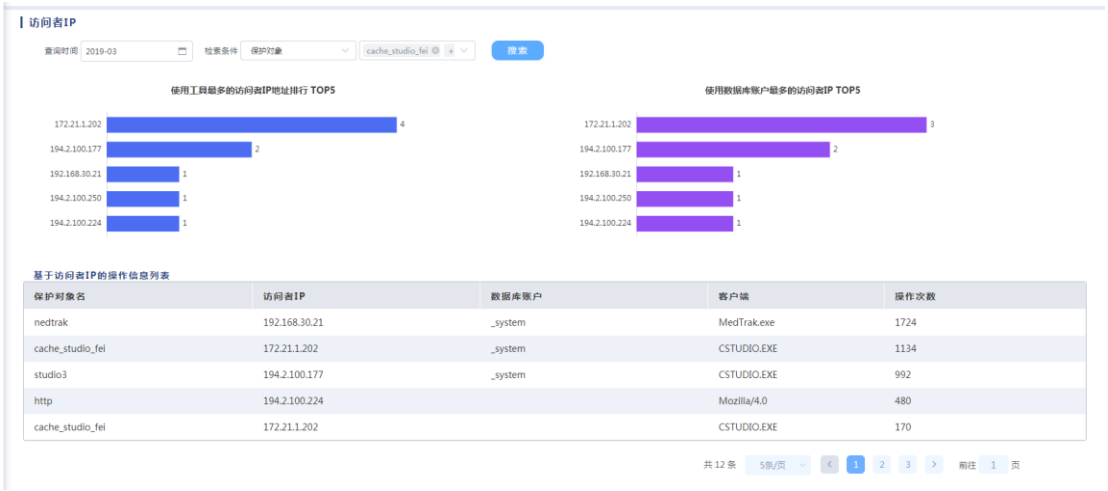
饼状图：使用最少的客户端（根据访问者 IP 数，Top5）和使用客户端登录数量分布（Top5）

列表：按访问次数由高到低显示当月客户端会话信息列表（Top100）

6.2.3 访问者 IP

柱状图：使用工具最多的访问者 IP 地址排行（Top5）、使用数据库账户最多的访问者 IP（Top5）

列表： 按访问次数由高到低显示当月访问者 IP 的操作信息列表（Top100）



6.3 等保报告

点击报表-合规报表-等保报告，显示数据库审计状态统计、客户端风险访问分析、审计

日志统计分析三部分统计信息。

6.3.1 数据库审计状态统计

统计 1 月份内，数据库审计概要内容展现，帮助用户快速了解当前数据库审计状态(Top100)。

6.3.2 客户端访问分析

统计 1 月份内，数据库是否存在可能非法的客户端访问及访问状态分析(Top100)。

6.3.3 审计日志统计分析

统计被审计数据库的审计记录数统计与 1 月份内，所有被审计数据库产生的操作次数，帮助审计人员进行趋势分析(Top100)。

7 通知

通知方式支持 SYSLOG 和 SNMP 通知。

7.1 SNMP 通知

进入互联网服务器，配置 SNMP 服务器，服务器 IP 为接收 SNMP 通知的机器的 IP。

配置好后切换到安全平台，到告警策略中配置 SNMP 告警。选择告警事件级别，添加接受者和 SNMP 的通知方式。将告警策略应用到需要通知的保护对象中，打开告警开关，一旦保护对象发生了相应级别的风险事件，就会以 SNMP 发送告警。

7.2 SYSLOG 通知

进入互联网服务器，配置 SYSLOG 服务器，服务器 IP 为接收 SNMP 通知的机器的 IP。

配置好后切换到安全平台，到告警策略中配置 SYSLOG 告警。选择告警事件级别，添加接受者和 SYSLOG 的通知方式（事件级别与 SYSLOG 的消息等级需一致）。将告警策略应用到需要通知的保护对象中，打开告警开关，一旦保护对象发生了相应级别的风险事件，就会以 SYSLOG 发送告警。

7.3 系统告警通知

对设备异常状态进行监控，发送告警通知。登录系统管理平台-系统管理-系统告警，配置告警方式，接收人，选择触发告警的条件。如图所示：

8 备份与恢复

以下才操作均在系统管理平台

8.1 配置 FTP

进入系统管理-互联网服务器中，配置 FTP 服务，可将审计记录，日志等信息备份会转存到指定的 FTP 服务器上，服务器 IP 为 FTP 服务所在的 IP。

8.2 手动备份

在数据维护模块中，添加存储方式为本地，手动备份如下信息：

存储方式可选择本地或者远程（备份到 FTP 服务器上）。备份文件会存储在本地或者是 FTP 服务器上，可以在本地文件列表或 FTP 服务器中进行下载。

8.3 自动备份

在数据维护模块中，添加自动备份，可以对备份的数据、审计记录的级别、备份的方式以及备份周期和备份时间进行设置，界面如下：

8.4 数据恢复

点击数据维护-数据恢复，点击导入文件，将备份到 FTP 服务器或本地的备份数据导入系统中，然后进行恢复。

8.5 配置信息收集

点击系统维护-配置信息收集，可以一键导出和导入设备的配置信息

9 黑白名单

登录系统管理平台-系统管理-系统安全。在该页面可以通过地址或者地址段形式配置黑白名单。如配置 172.21.1.200 为黑名单，成功后，使用该 ip 登录管理界面

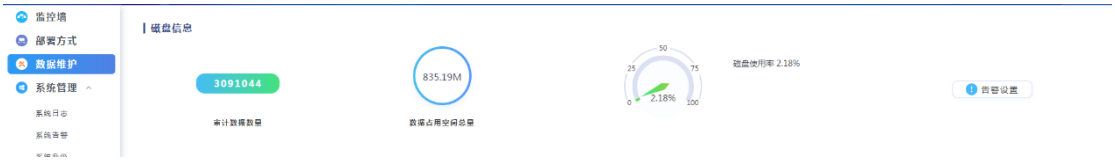
注意：以黑名单优先，比如黑名单设置 1.1.1.1-1.1.1.10，白名单设置 1.1.1.2，那么白名单设置无效，1.1.1.2ip 还是不能登录。

10 系统状态

以下操作均在系统管理平台。

10.1 磁盘信息查看

可通过监控墙界面查看磁盘信息状态，也可以去数据维护中查看磁盘信息。



10.2 安全等级配置

可选择默认安全等级（高中低），也可自定义安全条件，比如设置密码复杂度为高，则所有用户设置密码时，密码长度必须不小于 15 度，密码组成需三种以上符号，才可设置成功。

10.3 日志收集

在系统维护日志信息收集中，点击收集，出现各个类型日志预计文件大小，点击需要的

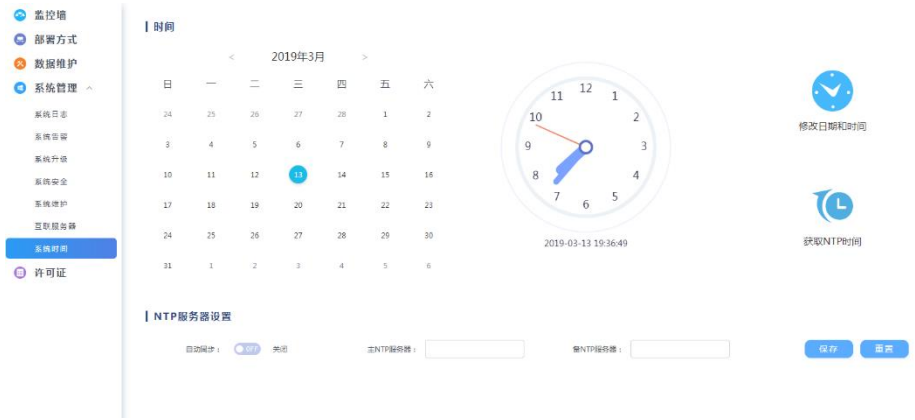
收集的日志类型点击收集。

10.4 抓包工具

在系统维护抓包工具中配置抓包条件，进行抓包，下载抓取的报文后查看详细报文。

10.5 系统时间

在系统时间中，修改设备时间，也可配置 ntp 自动同步时间。



11 日志查看

11.1 系统日志

登录系统管理平台-系统管理-系统日志。查看设备产生的所有的系统日志，可以针对指定查询条件查询系统日志。

11.2 操作日志

登录审计管理平台-操作日志。查看用户行为产生的所有操作日志，可以针对指定查询条件查询操作日志。

12 数据清理

12.1 手动清理

在数据维护模块中，点击手动清理，可对三种数据类型进行制定时间、保护对象、风险级别进行清理，如图：

12.2 自动清理

在数据维护模块中，点击添加自动清理，针对指定配置条件进行清理，如图：

13 设备管理

在系统管理平台-系统管理-系统维护-设备管理中，可以对数据库审计系统和审计引擎做重启、关闭等操作

恢复出厂后，IP 为 10.0.0.1，子网掩码为 255.255.255.0