【商密文档，限制公开】

玖玖盾数据库审计系统 V3.0

用户使用手册

常州玖玖盾数据科技有限公司

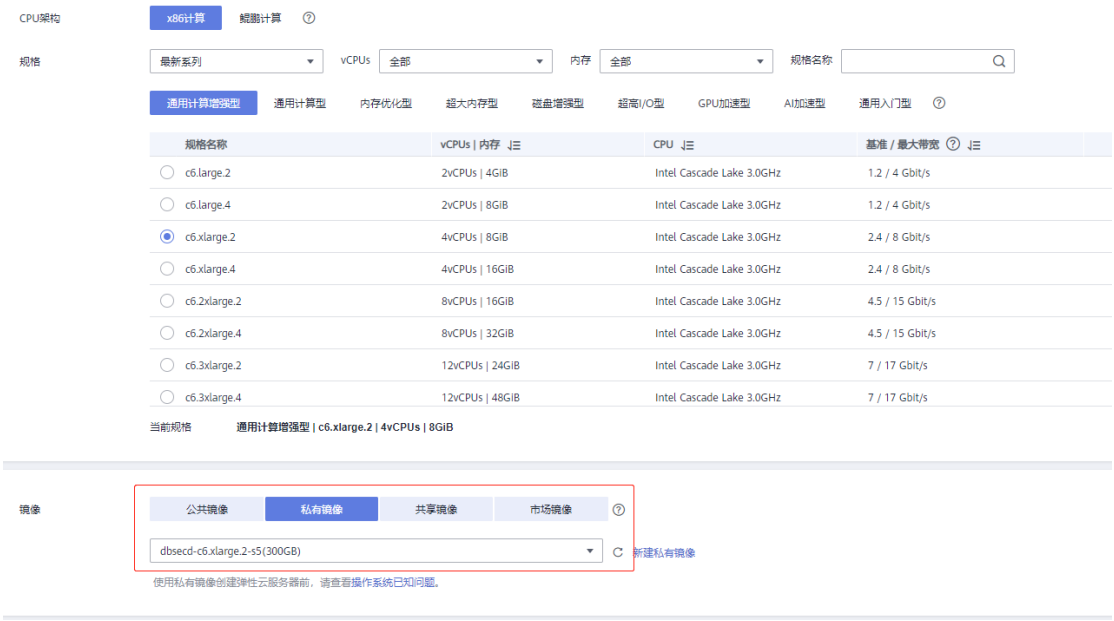
二〇二一年十一月

目录

1 华为云操作指南

1.1 操作步骤

1.购买数据库审计镜像或云服务器



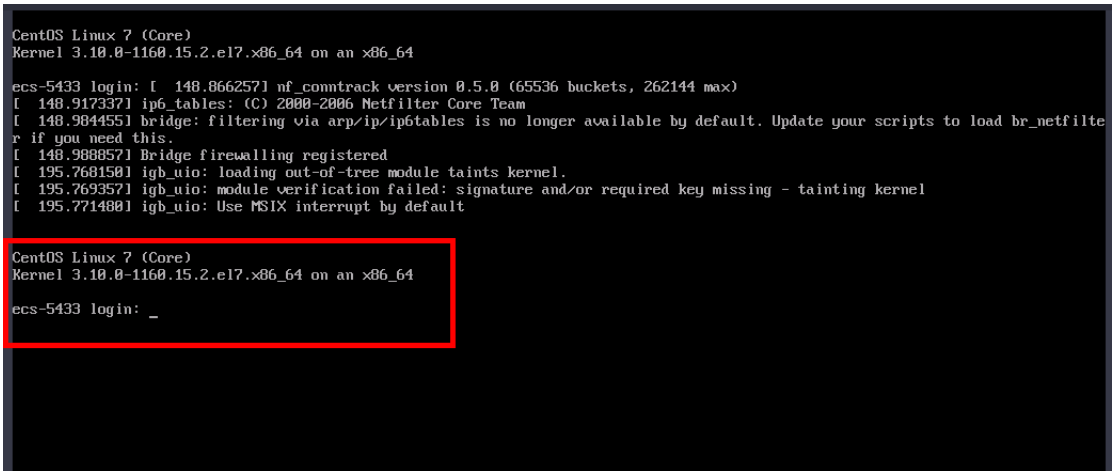
2.安全组注意端口放行

3.设置云服务器的账号密码

4.购买完成后，在控制台处选择远程登录-VNC 登录

点击【立即登录】

按照提示输入账号及密码



5.新建用户（可跳过）

因镜像禁止使用 root 用户通过 ssh 访问，如有远程登录需要，可通过一般用户登录后，再切换 root 用户。

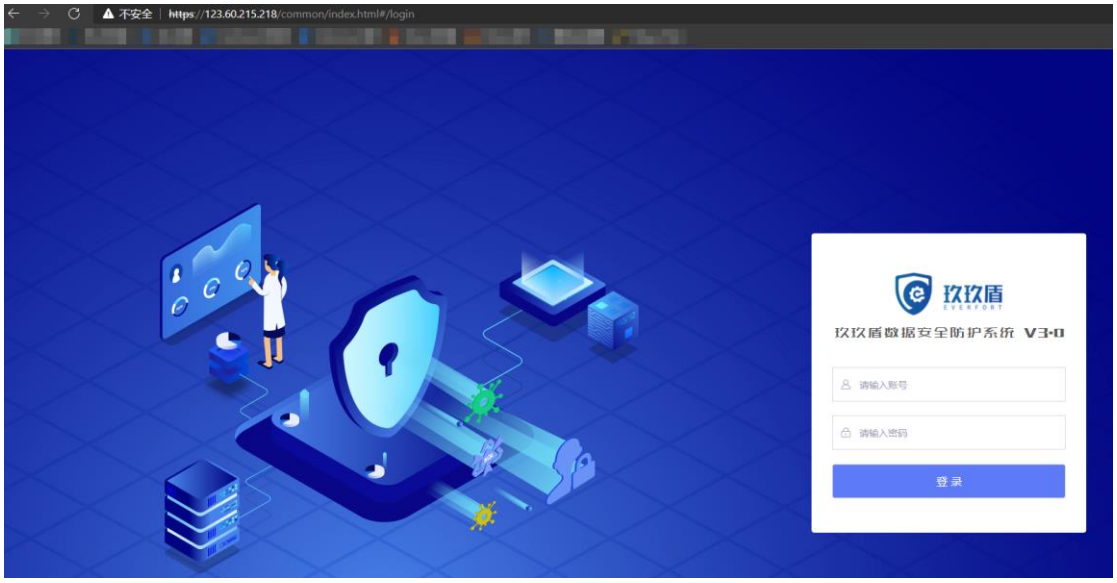
相关命令如下：

```
Adduser sirius              //添加一个新用户，名字叫Sirius
passwd sirius               //设置用户密码
su root                 //切换root 用户
```

6.重启 NetworkManager 服务

```
systemctl restart NetworkManager
```

7.通过 https://ip:8441 访问系统



1.2 软件未启动

（1）检查 Java、dbsecd 是否启动成功

具体操作：在审计服务器上，依次执行以下命令，查看对应服务是否启动成功。

ps -ef | grep java，检查 Java 是否启动成功。正常启动如图 1-1：

图 1-1 java 正常启动

systemctl status dbsecd，检查 dbsecd 是否启动成功。正常启动如图 1-2：

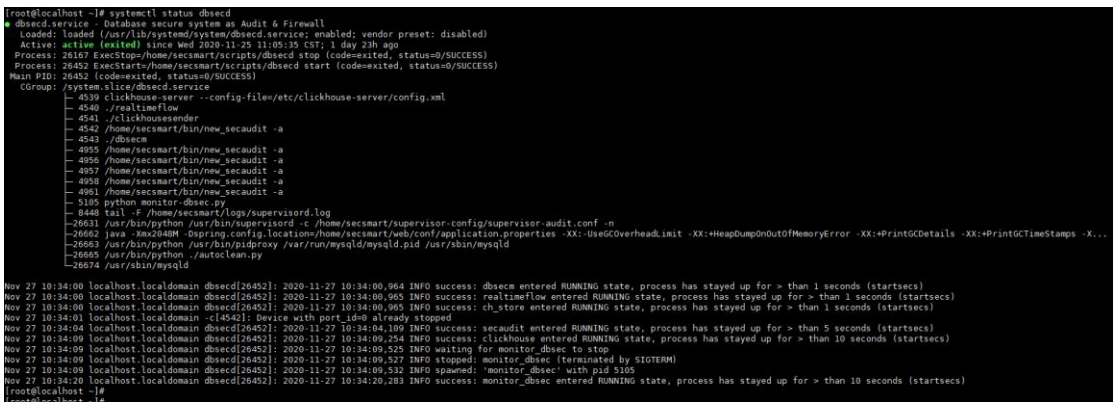


图 1-2 dbsecd 正常启动

重新启动方法：运行 systemctl restart dbsecd 重新启动

（2）检查审计服务器硬盘空间是否足够，df -h 查看磁盘使用情况。如图 1-3：

```
[root@localhost ~]# df -h
Filesystem               Size  Used Avail Use% Mounted on
devtmpfs                 6.7G     0  6.7G   0% /dev
tmpfs                    7.8G     0  7.8G   0% /dev/shm
tmpfs                    7.8G  106M  7.6G   2% /run
tmpfs                    7.8G     0  7.8G   0% /sys/fs/cgroup
/dev/mapper/centos-root   50G  7.1G   43G  15% /
/dev/sda1               1014M  150M  865M  15% /boot
/dev/mapper/centos-home  1.8T   16G  1.8T   1% /home
tmpfs                    2.0G  4.0K  2.0G   1% /opt/cache
tmpfs                    1.6G     0  1.6G   0% /run/user/0
[root@localhost ~]#
```

图 1-3 审计服务器硬盘空间

（3）检查审计服务器剩余内存是否足够、CPU 使用情况

free -m 查看审计服务器内存使用情况。如图 1-4：

```
[root@localhost ~]# free -m
              total        used        free      shared  buff/cache   available
Mem:          15772        4643         574          97       10554       10705
Swap:          7999         128        7871
[root@localhost ~]#
```

图 1-4 审计服务器内存使用情况

top 命令查看审计服务器 cpu 使用情况。如图 1-5：

```
[root@localhost ~]# top
top - 10:56:06 up 2 days, 17:47,  4 users,  load average: 0.09, 0.18, 0.22
Tasks: 182 total,   1 running, 181 sleeping,   0 stopped,   0 zombie
%Cpu(s):  1.0 us,  2.4 sy,  0.0 ni, 96.7 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem : 16150780 total,   462756 free,  4840380 used, 10847644 buff/cache
KiB Swap:  8191996 total,  8060020 free,   131976 used. 10876772 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
12356 root      20   0   32.3g  21096   1600 S   7.3  0.1   0:08.01 new_secaudit
12357 root      20   0   32.6g 181700  82096 S   7.0  1.1   0:08.31 new_secaudit
12358 root      20   0   32.7g 178372  80100 S   7.0  1.1   0:08.20 new_secaudit
12361 root      20   0   32.8g 178436  80152 S   7.0  1.1   0:08.19 new_secaudit
11936 clickho+  20   0 2835412 246900  56184 S   1.0  1.5   0:03.48 clickhouse-serv
    9 root      20   0       0      0      0 S   0.3  0.0   5:51.72 rcu_sched
11573 root      20   0       0      0      0 S   0.3  0.0   0:00.01 kworker/2:0
```

图 1-5 cpu 使用情况

2 登录与修改密码

2.1 登录

在浏览器中输入“https://管理 IP”登录数据库审计与防护系统，输入用户名和密码。

图2-1 系统登录

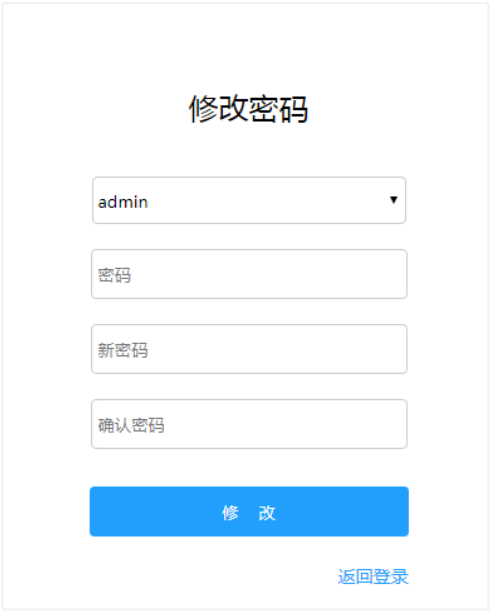
说明

- IP 地址根据实际情况修改，实际用户名密码请咨询厂家实施人员。
- 设备默认出厂 IP：192.168.0.254，出厂用户名/密码：admin/111111

2.2 修改密码

1. 单击<修改密码>，进入修改密码界面。

图2-2 密码修改



2. 输入密码、新密码、确认密码，单击<修改>。
3. 可以等待跳转登录界面，也可以单击<返回登录>回到登录界面。

3 首页

在[首页]中可以查看整体或单个数据库的使用情况。

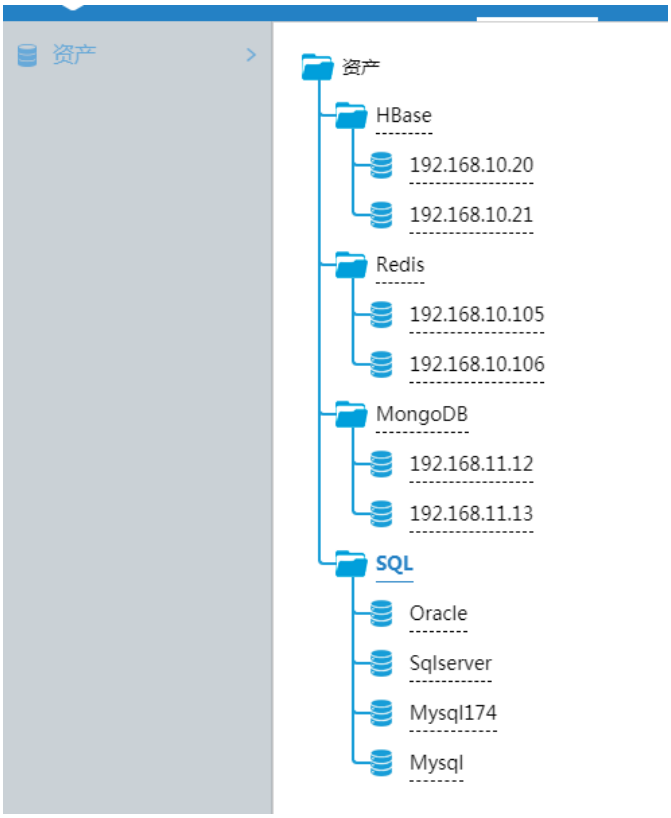
3.1 查看流量

1. 进入首页之后，单击左上角<资产>。

图3-1 首页

2. 单击需要查看的资产。

图3-2 资产实例



3. 查看流量

可以查看最近 5 分钟、最近 1 小时、最近 24 小时、最近 7 天的流量情况。

说明

A 开头的数据库是系统自动发现的。

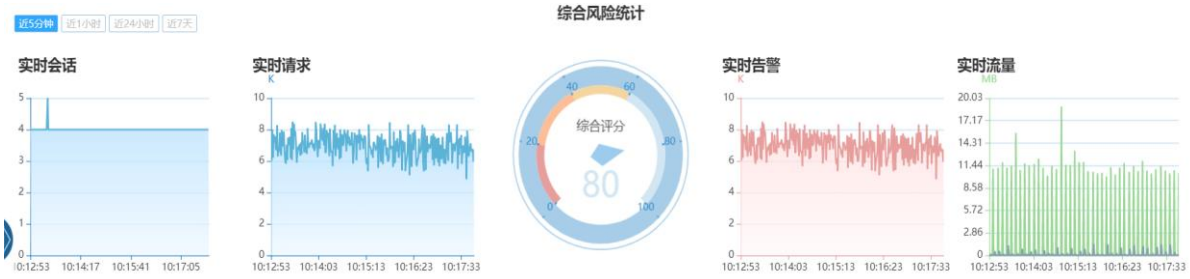
如果有 SQL 数据量产生，则表示网络数据捕获正常；反之，则网络或系统存在异常。

首页下方图表分为组视角和单个资产视角，组视角 top5：会话 top5，请求数 top5，风险数 top5，执行时长；

单个视角 top5：客户端 top5，操作命令 top5，表名访问量 top5，风险类型 top5。

3.2 查看综合风险统计

在[首页]中可以看到实时会话、实时请求、综合风险统计、实时告警、实时流量。



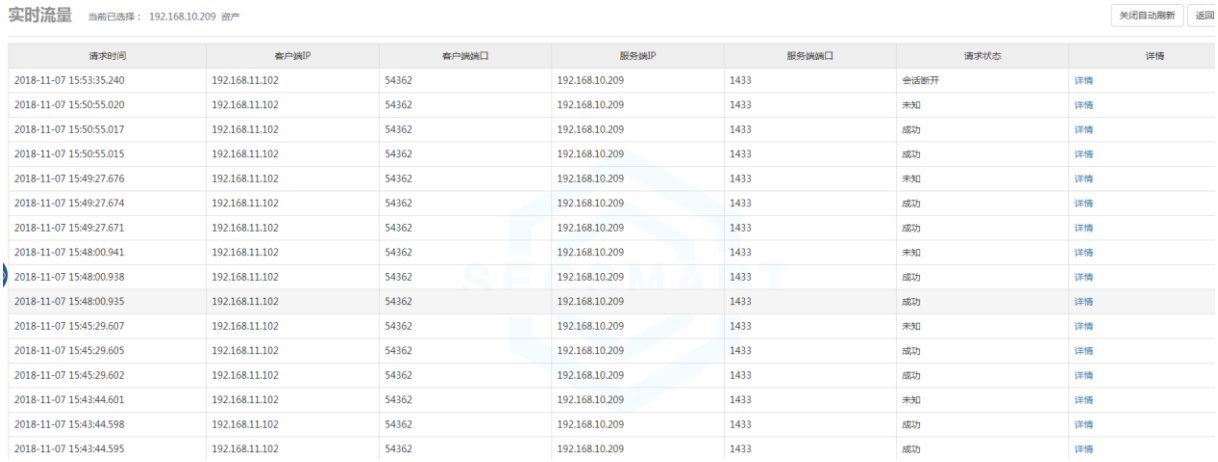
3.3 查看最新告警

1. 在[首页]中可以查看最新告警。

图3-3 最新告警

2. 单击实时请求栏右侧<更多>可以查看当前流量的详情。

图3-4 实时流量



请求时间	客户端IP	客户端端口	服务端IP	服务端端口	请求状态	详情
2018-11-07 15:53:35.240	192.168.11.102	54362	192.168.10.209	1433	会话断开	详情
2018-11-07 15:50:55.020	192.168.11.102	54362	192.168.10.209	1433	未知	详情
2018-11-07 15:50:55.017	192.168.11.102	54362	192.168.10.209	1433	成功	详情
2018-11-07 15:50:55.015	192.168.11.102	54362	192.168.10.209	1433	成功	详情
2018-11-07 15:49:27.676	192.168.11.102	54362	192.168.10.209	1433	未知	详情
2018-11-07 15:49:27.674	192.168.11.102	54362	192.168.10.209	1433	成功	详情
2018-11-07 15:49:27.671	192.168.11.102	54362	192.168.10.209	1433	成功	详情
2018-11-07 15:48:00.941	192.168.11.102	54362	192.168.10.209	1433	未知	详情
2018-11-07 15:48:00.938	192.168.11.102	54362	192.168.10.209	1433	成功	详情
2018-11-07 15:48:00.935	192.168.11.102	54362	192.168.10.209	1433	成功	详情
2018-11-07 15:45:29.607	192.168.11.102	54362	192.168.10.209	1433	未知	详情
2018-11-07 15:45:29.605	192.168.11.102	54362	192.168.10.209	1433	成功	详情
2018-11-07 15:45:29.602	192.168.11.102	54362	192.168.10.209	1433	成功	详情
2018-11-07 15:43:44.601	192.168.11.102	54362	192.168.10.209	1433	未知	详情
2018-11-07 15:43:44.598	192.168.11.102	54362	192.168.10.209	1433	成功	详情
2018-11-07 15:43:44.595	192.168.11.102	54362	192.168.10.209	1433	成功	详情

3. 单击<返回首页>，返回首页。

4 审计

4.1 告警

告警功能是用来记录所有资产的告警信息，可在告警进行查询、筛选操作。

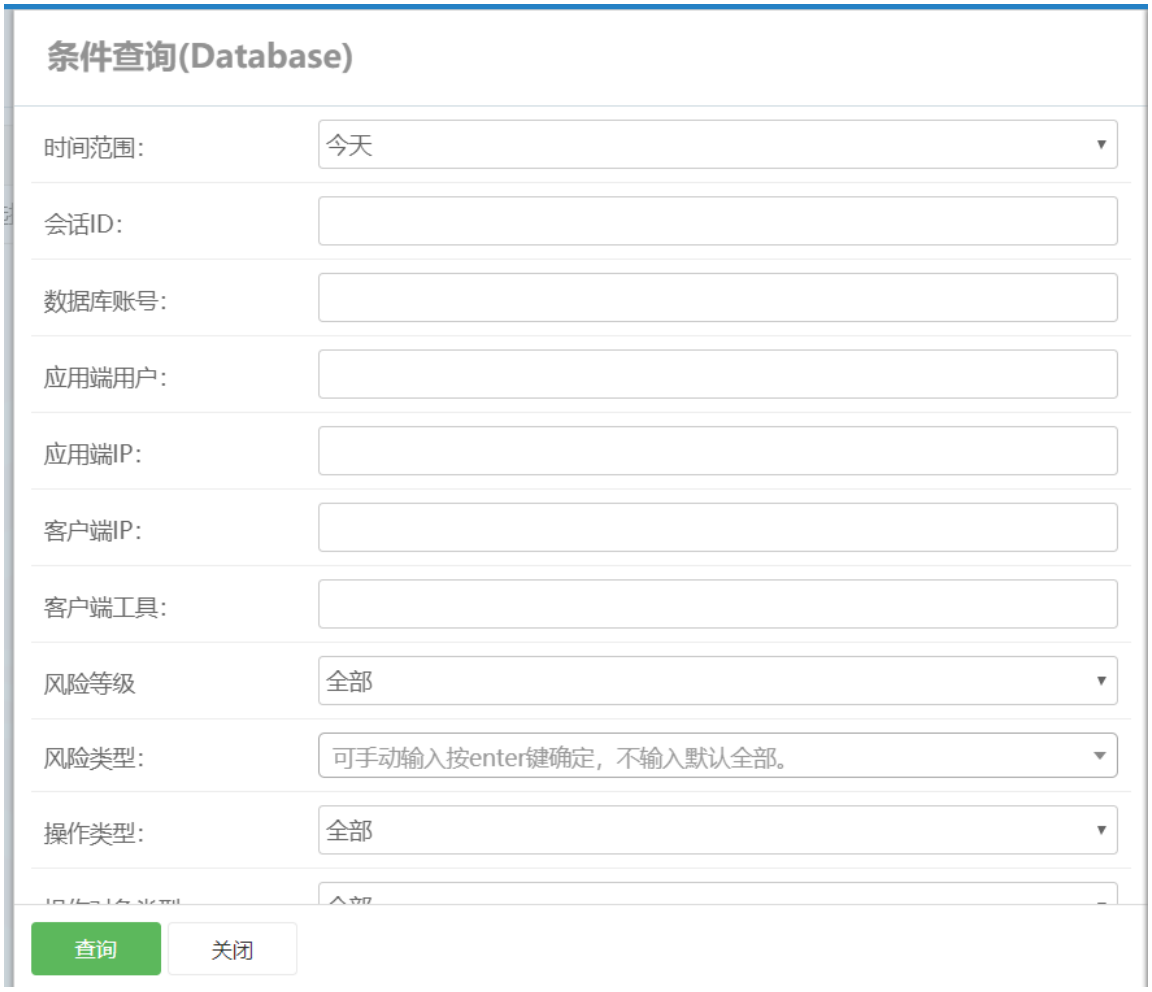
4.1.1 告警列表

1. 进入[审计]页面，单击<资产>选择需要查看的数据库。
2. 选中之后，点击空白处，然后单击<告警>，可查看告警列表和进行告警处理，默认进入告警列表。

图4-1 告警列表

3. 单击<条件查询>进行告警日志条件过滤。

图4-2 条件查询



4.1.2 告警处理

图4-3 告警处理

1. 单击<条件查询>进行告警日志条件过滤。

图4-4 告警条件查询

2. 单击<未处理>可以查看未处理的告警信息。
3. 单击<已处理>可以查看已处理的告警信息。

图4-5 已处理告警详情

4.2 检索

检索功能是用来记录资产的所有日志信息，包括登陆日志、访问日志、和告警日志，都可以在检索进行查询。

1. 进入[审计/检索]页面。

图4-6 检索详情

说明

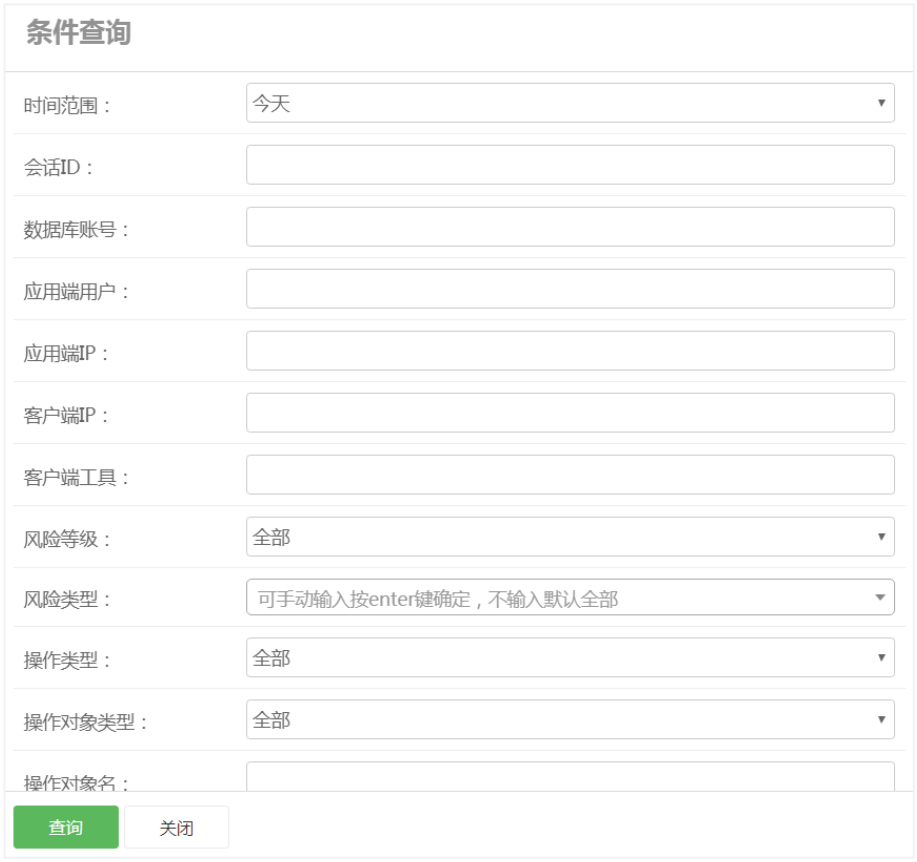
检索时间：

告警、检索、会话的检索时间默认为 5 分钟，可用过设置检索时间，缩短要检索的内容；

检索时间改变后，告警、检索、会话的检索时间都会相应的改变。

2. 单击<条件查询>。

图4-7 检索条件



3. 选择需要检索的条件，然后单击<查询>。
4. 单击最后一栏的<详情>，可以查看更详细的信息。

图4-8 单条信息详情

5. 单击<添加规则>，会出现白名单、黑名单、自定义。
6. 单击<白名单>，可以进行白名单的设置。

图4-9 添加白名单

注意

取反的意思是，除了填写的不能通过之外其他的都可以。

每天的几点是时间段，如果需要选择一个小时的时间段，只需要选那个时间点就行。

表4-1 白名单配置表

字段	内容
名称	给添加的白名单附加名字，便于区分
数据库账号	确认访问的数据库账号是否产生告警
时间	选择时间范围，确认访问的时间段是否产生告警
客户端IP	确认访问的客户端IP是否产生告警，可以是默认的，也可以进行二次添加
客户端工具	确认访问的客户端工具是否产生告警

操作命令	确认访问的操作命令是否产生告警，可以是默认的，也可以进行二次添加
操作对象类型	确认访问的操作对象类型是否产生告警，可以是默认的，也可以进行二次添加
操作对象名	确认访问的操作对象是否产生告警，可以是默认的，也可以进行二次添加
SQL语句	确认访问的SQL语句是否产生告警，可以进行二次添加

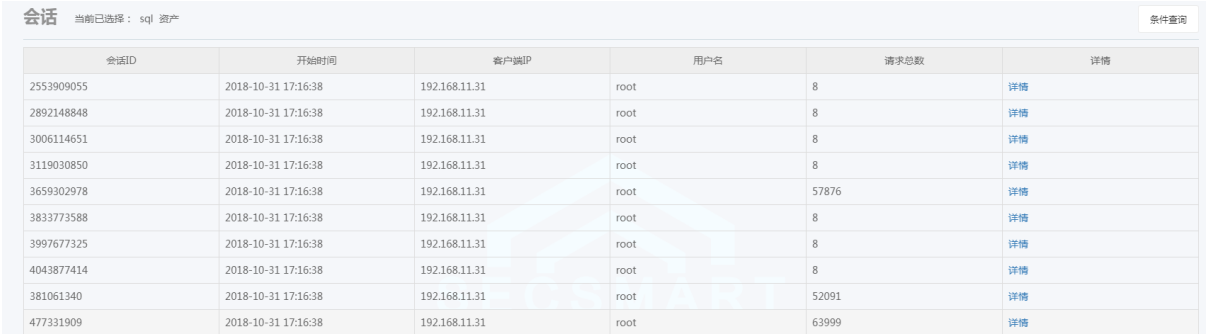
7. 单击<提交>，完成白名单的配置。
   白名单规则可以在<策略>里面的<白名单>查看。
8. 单击<添加规则>，选择<黑名单>，进行黑名单的配置。
9. 填好信息之后，单击<提交>。
   黑名单规则可以在<策略>里面的<黑名单>查看，还可以进行规则的自定义。
10. 单击<自定义>。
11. 单击<提交>，产生自定义规则。
    自定义规则可以在<策略>里面的<自定义>查看。

4.3 会话

会话功能是记录当前的实时会话，会显示当前正在访问数据库的所有会话，可以查看每个会话的所有请求、每个请求的详细信息。

1. 返回审计列表。
2. 单击<会话>，可以查看当前连接数据库的用户数。

图4-10 会话



注意

点击<详情>可以查看执行的 SQL 语句。

4.4 会话回放

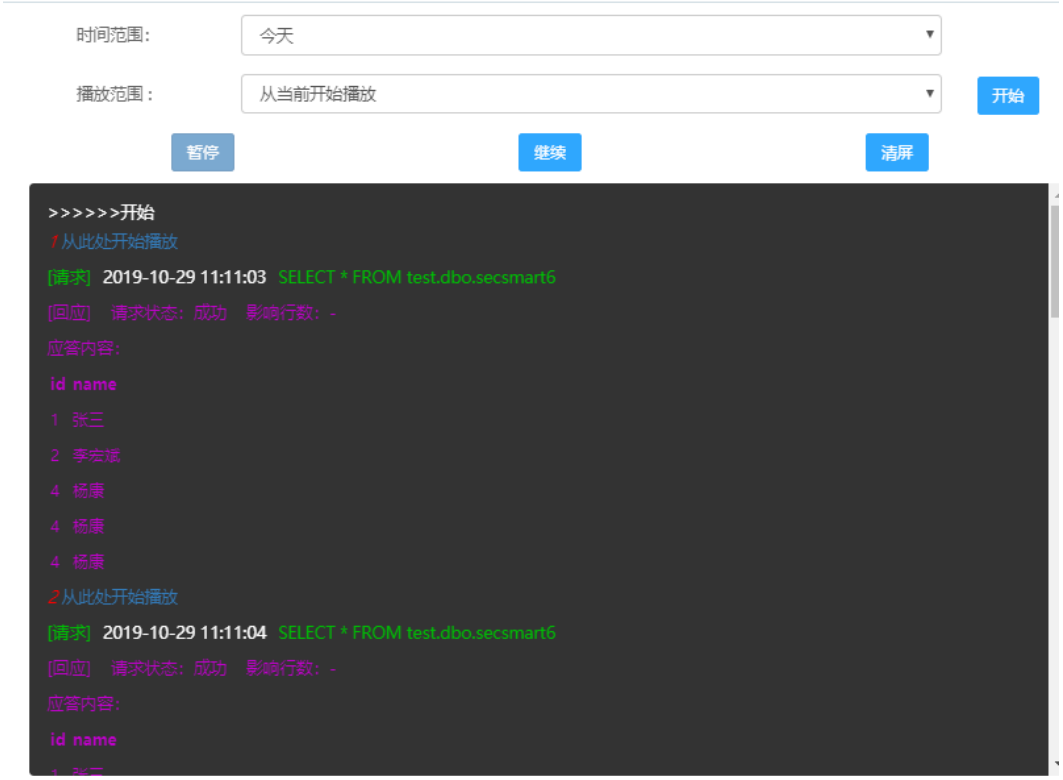
1. 单击<条件查询>，可以按照时间范围、会话 ID、源 IP、操作命令、操作对象、SQl 关键字，进行查询，

2. 查询完成，生成会话列表，点击列表回放字段，进行回放

3. 回放页面，可以选择时间范围和播放范围；

播放范围，可以选择从当前开始（指这个会话从这条语句开始播放）、播放全部（播放整个会话）。

4. 单击<开始>，会话开始回放，



5. 单击<暂停>，会话播放停止，

6. 暂停或者播放完后，序号后面出现“从此处开始播放”，点击可从当前语句开始播放。

5 分析

5.1 查看统计分析图

分析功能是用来做数据分析，可进行多维分析，并且可以生成报表。

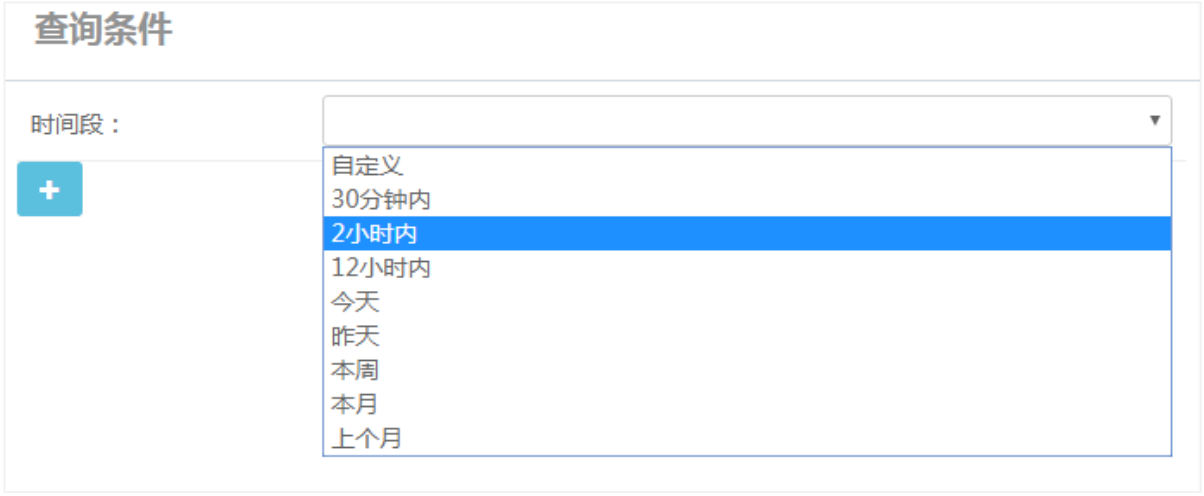
1. 单击<分析>，进入分析界面。

2. 单击<资产>，选择需要查看的数据库。

5.2 查询条件

1. 选择时间段。

图5-1 时间段

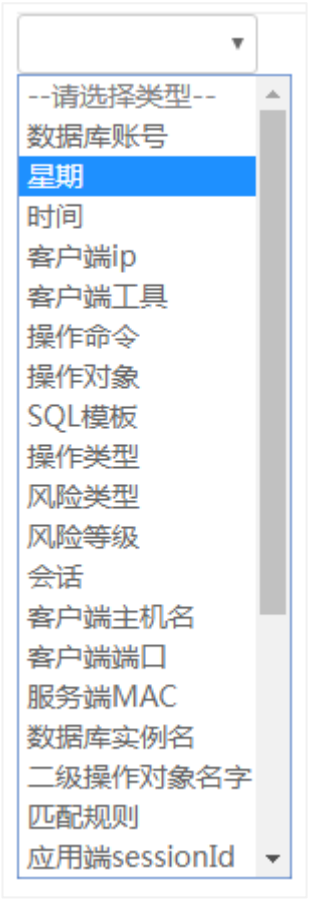


说明

- 也可以自定义时间段。

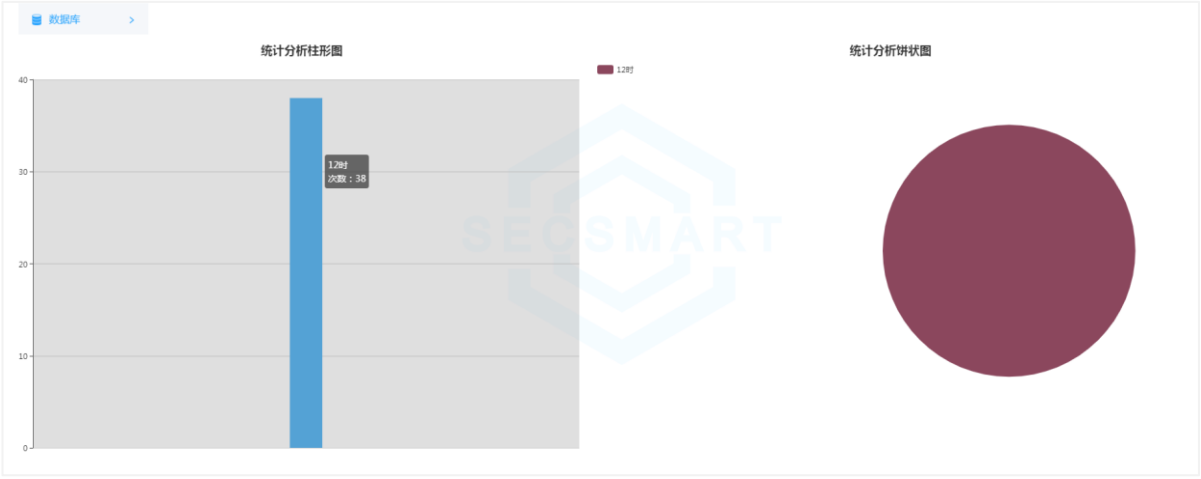
2. 单击<+>，选择分析类型。
3. 单击<选择类型>，有 28 种类型可供选择。

图5-2 具体类型



4. 选择需要查看的类型，以选择“时间”为例进行统计。

图5-3 统计分析，单击空白处，显示饼状图。



5. 选择<时间>生成统计图之后，可以继续添加类型。

图5-4 继续添加条件

6. 单击<12 时>之后，会出现<+>。

7. 单击<+>，可以添加除时间外的类型。

条件可以依次添加

图5-5 综合条件

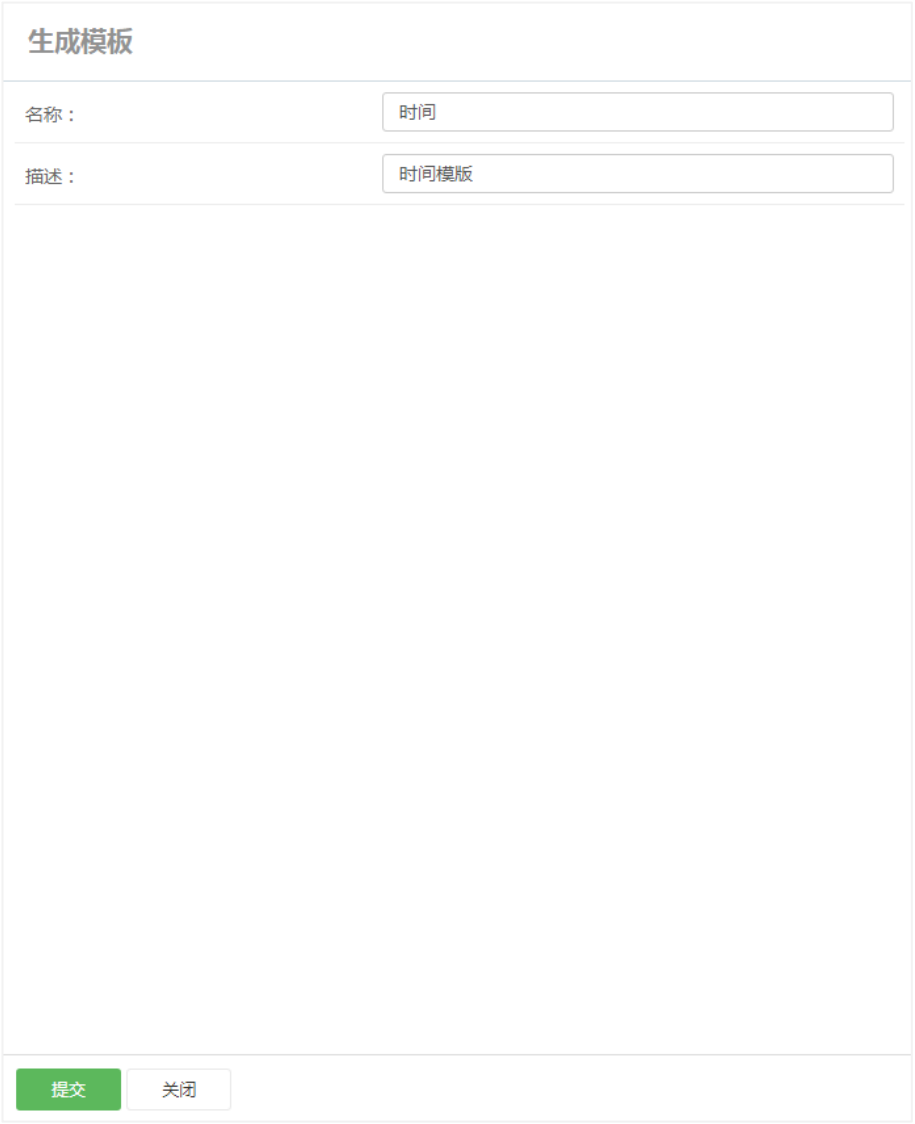
注意

只能添加能查询到的条件。

5.3 生成模板

1. 单击<生成模版>。

图5-6 模板



说明

- 此模板为自定义模板，根据查询条件而生成的模板。

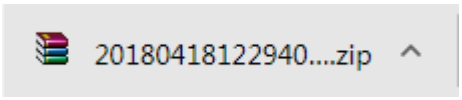
5.4 下载报表

1. 单击<下载报表>。

图5-7 报表类型

2. 选择 PDF 之后会自动下载，下载的为压缩包。

图5-8



说明

- pdf、csv、html 下载的都为压缩包，依次的 PDF、表格、图片。

6 策略

6.1 选择数据库

进入[策略]页面，单击<资产>选择需要添加策略的数据库。

图6-1 策略总览

6.2 白名单

1. 单击<白名单>，会显示已经配置的白名单策略。如在审计栏添加的测试白名单。
2. 选中需要更改的白名单，可以进行现有白名单的更改，如详情、编辑、删除。
3. 单击<添加>可添加新的白名单策略。

图6-2 白名单具体内容

4. 单击<提交>，产生新的白名单。通过<首页><实时流量>界面查看白名单是否生效。

> **注意**
>
> 查看流量前请确认是否有对数据库的操作。
>
> 白名单默认风险等级信任、黑名单默认风险等级非法。
>
> 策略优先级：网络防护 > 数据过滤>白名单 > 黑名单 > 自定义 > 智能防护 。

6.3 黑名单

1. 单击左边列表里的<黑名单>可以看到以往的黑名单列表，可以对以往的黑名单进行详情查看、编辑、删除。
2. 单击<添加>添加新的黑名单。
3. 单击<提交>生成黑名单。可在[首页]的“最新告警”中查看匹配黑名单的是否显示非法告警。

6.4 自定义

自定义是对一些白名单、黑名单等规则的一些补充。

1. 进入[策略/自定义]页面，可对已有自定义进行查找、详情查看、编辑、删除。
2. 单击<添加>，增加新的自定义。
3. 单击<提交>，产生新的自定义规则。

6.5 智能防护

智能防护功能可根据用户行为自动生成防护策略，智能防护功能默认开启，用户行为匹配规则时会产生告警。

1. 单击<智能防护>，进入智能防护界面。
2. 智能防护是每天 0 点，自动根据前 24 个小时，数据库账号对数据库的操作而产生的规则。可对已有规则进行详情查看和编辑。

6.6 网络防护

网络防护功能是用来对 ip 访问进行过滤的，设置网络防护规则后，该 IP 对应的资产访问日志，将不再记录。

1. 单击<网络防护>，进入网络防护界面。
2. 单击<新增>，进行网络防护的增加。

图6-3 新增网络防护

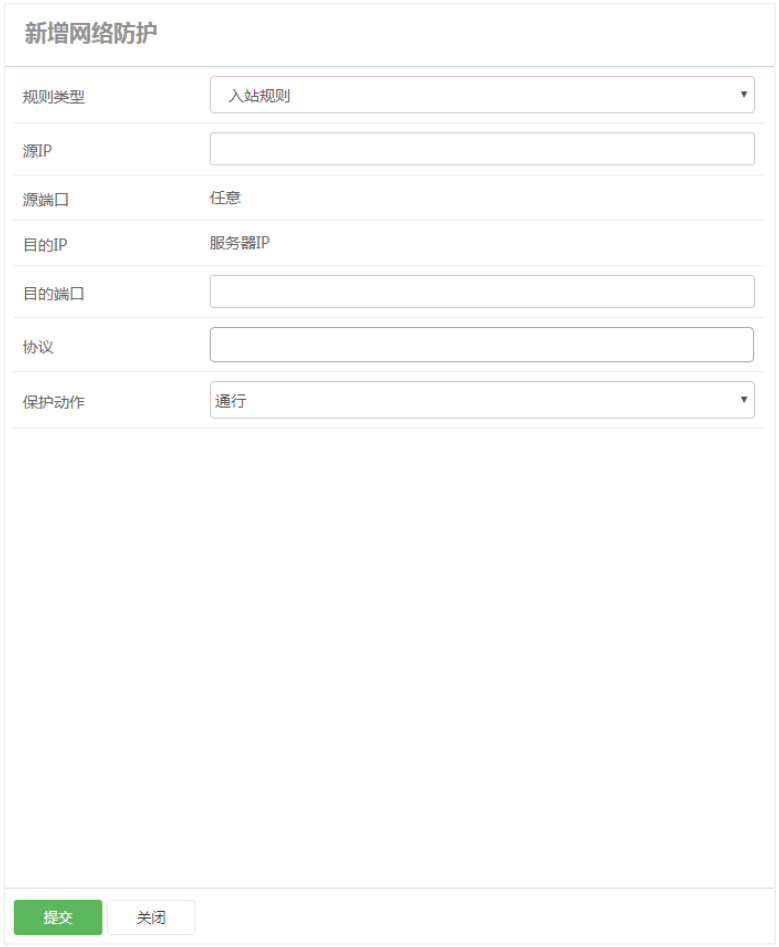


表6-1 新增网络防护配置表

字段	含义
规则类型	入站和出战规则的选择
源IP	允许通过的目的IP
源端口	运行通过的目的源端口
目的IP	服务器IP
目的端口	服务器端口
协议	选择传输协议
保护动作	通过和忽略，通过有记录，忽略就是默认合法，不记录

注意

网络防护的目的就是信任这个来源 IP。

6.7 漏洞攻击

系统内置漏洞特征库，当用户访问行为符合漏洞攻击特征时，会匹配漏洞攻击规则，产生告警风险。

1. 单击<漏洞攻击>，出现漏洞攻击列表，勾选对应的漏洞，漏洞攻击生效。

图6-4 漏洞攻击列表

2. 单击<编辑>出现编辑界面，可修改漏洞等级及保护动作。

图6-5 编辑漏洞攻击

3. 单击<提交>，完成漏洞攻击的策略修改。
4. 单击<详情>，可以查看漏洞攻击的详情。

图6-6 漏洞攻击详情

注意

漏洞攻击列表里的漏洞攻击模式是系统自带的，勾选之后生效，会产生告警。可通过查找数据库版本查看对应漏洞，进行选择。

6.8 数据过滤

数据过滤功能主要是过滤非用户操作语句的，可以用来过滤工具自带的访问语句，避免审计过多没有的信息。

1. 单击<数据过滤>，进入数据过滤界面。
2. 点击<添加> ，弹出添加规则界面。
3. 下滑规则界面，单击<添加语句>，勾选需要过滤的正则语句。
4. 单击<确认>，完成规则添加，实时流量和审计页面不会再出现已过滤的语句。

7 报表

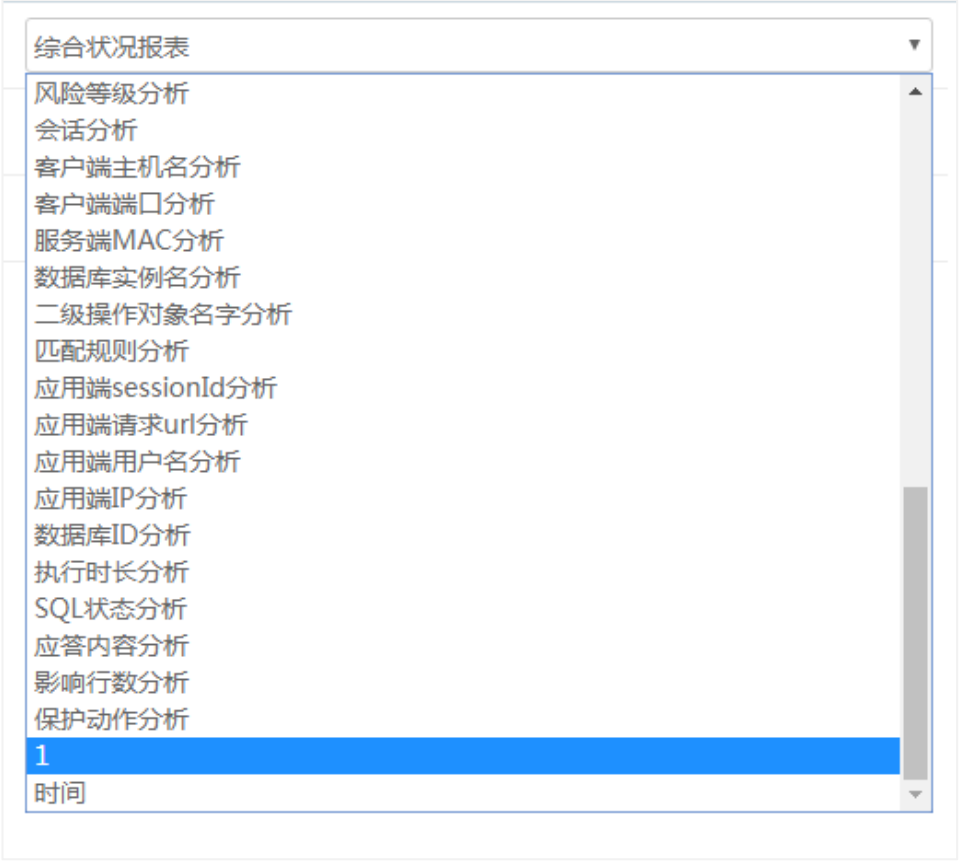
7.1 报表生成

1. 选择<资产>后，单击<报表生成>。
2. 单击右上角<报表生成>，可选择报表模板、时间段，报表格式。

图7-1 生成报表

3. 单击<综合状况报表>，会出现 44 种系统默认的报表模板，和自己添加的报表模板。

图7-2 报表模板



说明

- 在模板中可以看到之前在<分析栏>生成的报表模板,如上图已选择的“1”为分析栏生成模板。

1. 单击<1>这个报表模板，然后选择审计时间段，最后选择报表的格式：PDF、CSV、HTML。
2. 单击<提交>即可生效。

图7-3 报表生成具体信息

	压缩包名	格式	状态	报表周期	审计时间段	下载次数	下载
☐	1524210966047_20180419~20180420_A1...	PDF	生成完成	手动	2018-4-19到2018-4-20	0	下载

说明

- 只有等<状态栏>的<待生成>变为<生成完成>才可以进行报表的下载。

3. 下载后进行解压就可以看相关报表信息。

7.2 报表模板

1. 单击<报表模板>，进入自定义报表模板列表。
2. 如果需要添加新的自定义模板，请到<分析><查询条件>里添加条件，然后单击<生成模板>。
3. 可以对已有模板进行详情的查看和删除。

7.3 定时任务

1. 单击<定时任务>，进入定时任务列表。
2. 单击<新增任务>，进行任务的新增。

图7-4 新增任务

图7-5 定时任务配置表

字段	含义
报表模板	含有44种内置模板，可以进行自主的添加。
报表格式	PDF、CSV、HTML
报表周期	生成报表的周期
时间	每天的几点
分钟	每天的几点几分
收件人邮箱	报表所发送的邮箱，邮箱只要能接受邮件都可以

3. 单击<提交>，定时任务配置完成。

说明

- 定时任务的报表模板无法直接删除，需要先取消任务，才能删除。
- 设置定时任务需要先配置好邮件服务器。

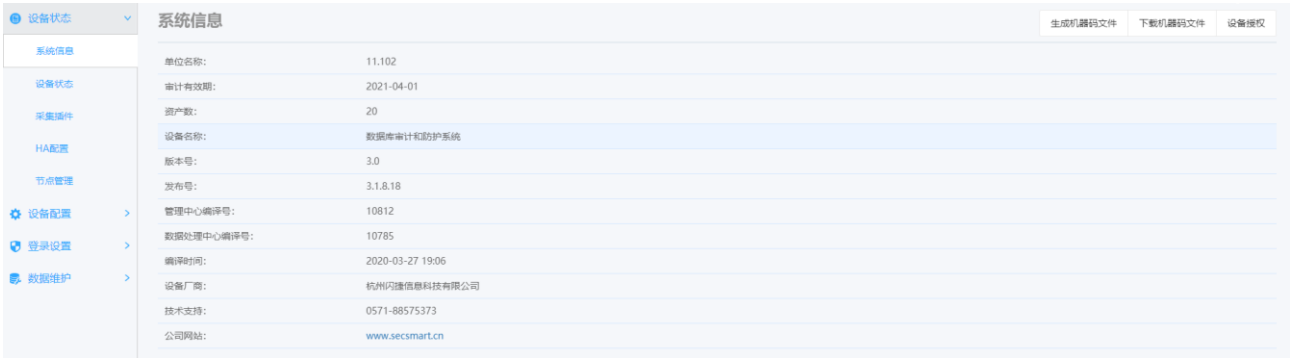
8 系统

8.1 设备状态

8.1.1 系统信息

1. 单击<设备状态>。
2. 单击<系统信息>，可以看到系统的常见信息。

图8-1 系统信息



可以看到右上角有<生成证书>、<下载证书>、<设备授权>，三个选项。

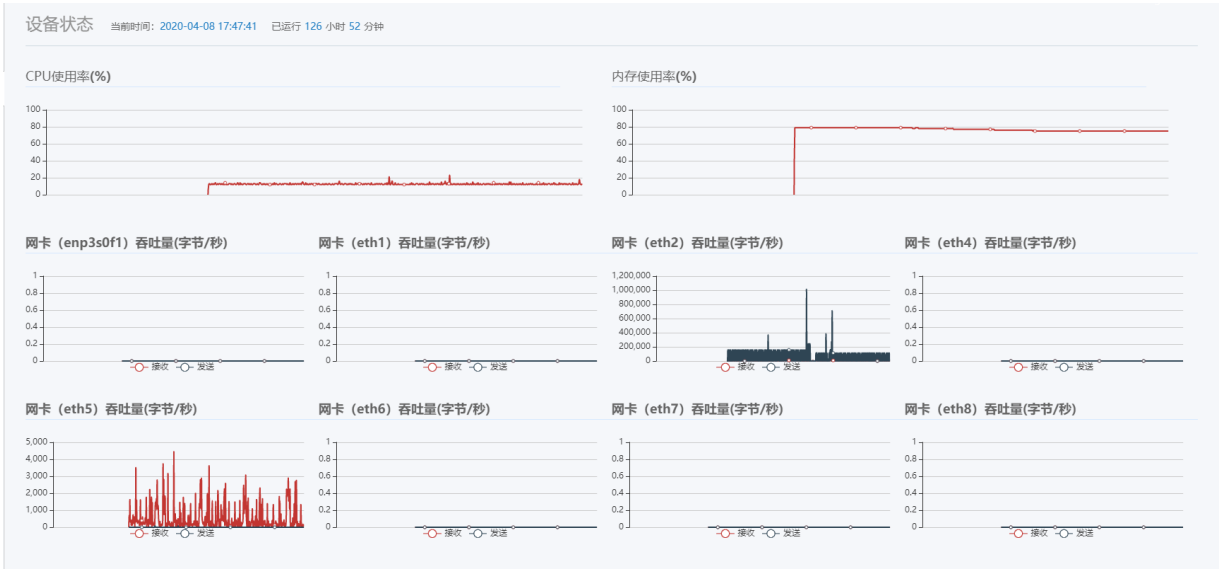
表8-1 设备授权配置表

字段	含义
生成证书	首次登录次系统，需要单击生成证书，系统自动生成一个证书，用来区分不同的设备
下载证书	下载刚刚生成的证书
设备授权	下载的证书需要发给厂商公司，由厂商公司对证书进行修改和密钥的添加，完成后发回给客户，然后客户上传至系统

8.1.2 设备状态

1. 单击<设备状态>，可以看到设备的 CPU 使用率、内存使用率、网卡吞吐量、程序占用空间情况、CPU 和内存使用占比拼图。

图8-2 设备状态



8.1.3 采集插件

1. 单击<采集插件>，可以看到云上数据库的状态。

图8-3 云上数据库状态

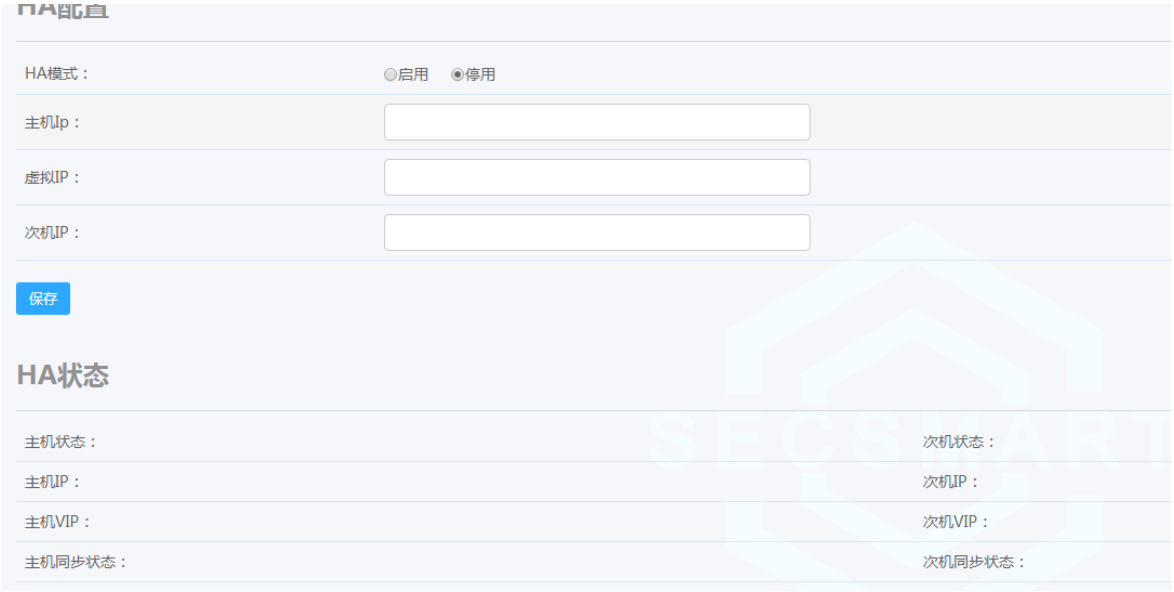
注意

采集插件里显示的数据库 CPU、内存使用率，是装了插件的数据库的状态，使用镜像配置的数据库看不了数据库的状态。

8.1.4 HA 配置

1. 单击 HA 模式〈启用〉，当前审计系统无法访问时，会自动切换到备机。
2. 填写主机 ip，虚机 ip 和次机 ip，点击〈保存〉。

图8-4 HA 配置



8.1.5 节点管理

注意

安装时要选择部署模式：单机模式、分布式中心、分布式节点。
节点没有 web 界面，节点需要手动添加

图8-5 单机模式

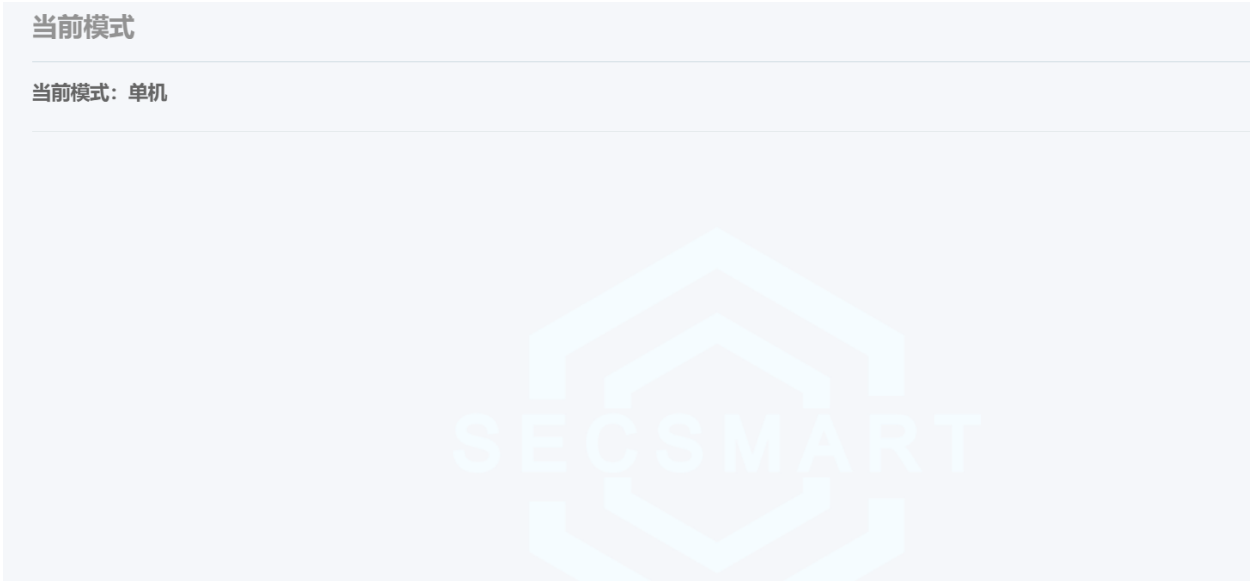
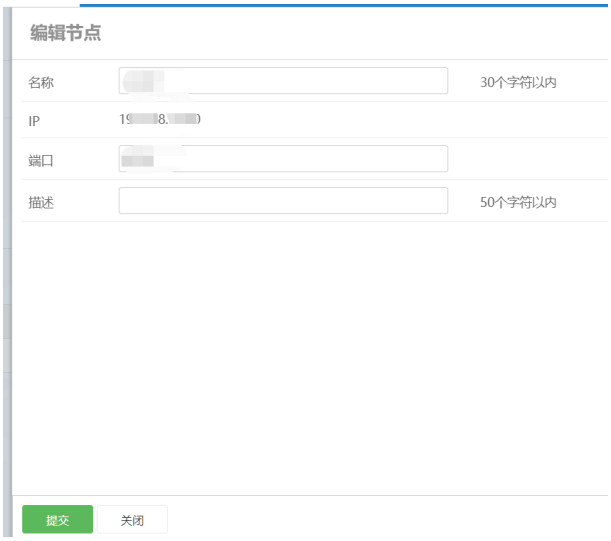


图8-6 分布式中心：

1. 点击<新增>，填写名称、IP、端口、描述(可不填写)，添加节点

2. 选中已添加的节点，点击<编辑>，可以编辑，名称、端口、描述。



3. 选择已添加的节点，单击<关联资产组>，勾选该节点关联的资产。

4. 选择已添加的节点，单击<数据源配置>，进入网卡列表；
5. 单击<数据源列表>，进入数据源列表；
6. 单击<新增>，添加数据源，
7. 选择已添加的节点，单击<删除>，点击确认，删除选中的节点。

8.2 设备配置

1. 编辑名称

1) 单击<设备配置>，进入设备配置界面。

2) 选中之后，单击<编辑名称>进行名称编辑。

3) 单击<提交>后生效。

2. 删除设备

如果要删除设备，勾选要删除的设备，单击<删除设备>即可。

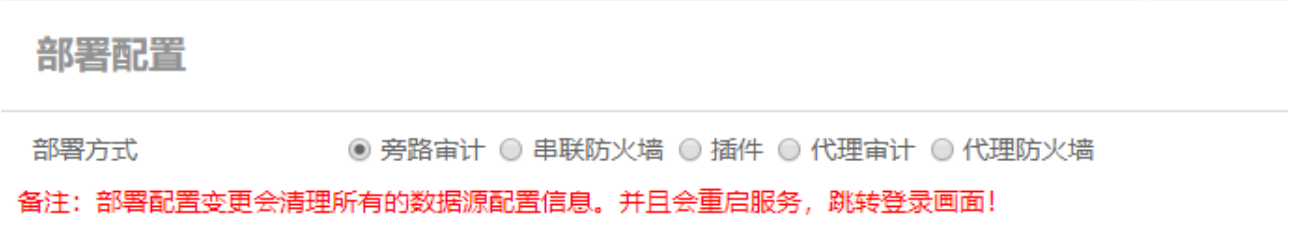
说明

- 只能删除停用的设备。

8.2.1 部署配置

1) 单击<部署配置>，可以选择部署模式。

图8-7 部署配置



8.2.2 连通性测试

1. 单击<连通性检测>，可以检查设备的连通性。

图8-8 连通性检查

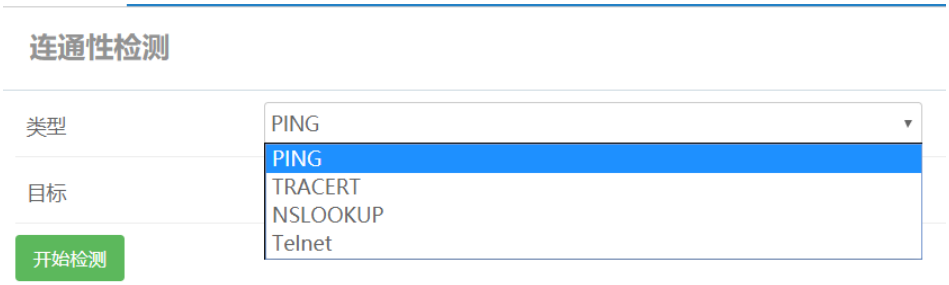


图8-9 连通性测试配置表

类型	含义
PING	Ping设备的网络是否能通。
TRACERT	查看本机到目的地址所需要经过的网关。
NSLOOKUP	可以查到DNS记录的生存时间还可以指定使用哪个DNS服务器进行解释。
Telnet	查看本机到其他设备的的端口是否能通。

注意

连通性检查在审计设备出现问题的时候会用到。

8.2.3 时间配置

1. 单击<时间配置>，进行系统时间的配置，可以选择本机所在的时间，也可以是时间服务器。

图8-10 时间配置

8.2.4 插件下载

单击<插件下载>，可以下载 Windows、和 Linux 插件。

此插件是用来安装在不能用镜像方法抓流量的数据库，比如：

1）交换机镜像端口不可用或者丢包严重；

2）需要监控发生在数据库服务器本地的数据库操作，如直接登录到数据库服务器并操作数据库；

3）需要监控以加密连接（SSL）进行的数据库访问。

8.2.5 插件配置

选中要配置的插件，单击<插件配置>，会出现抓包规则和阀值。

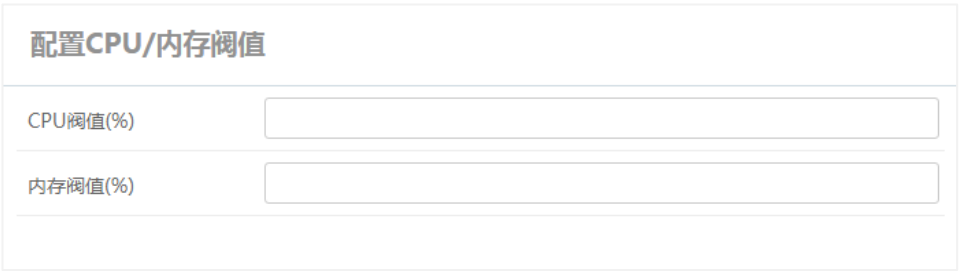
图8-11 插件配置

1. 单击<抓包规则>进入“抓包规则”界面。

图8-12 抓包规则

2. 单击<新增>添加端口号，依据数据库类型添加对应的端口号。
3. 可单击<阀值>设置目标审计设备的阈值。

图8-13 阀值



警告

- 这里设置的阀值，当插件所在的设备 cpu 或者内存使用率超过阀值后，插件不进行转发审计内容。

8.2.6 网卡配置

1. 选中系统自带的设备，单击<网卡配置>。

图8-14 网卡配置

2. 单击<数据源配置>，单击<添加>，选择合适的网卡。
3. 单击<路由配置>，路由配置是为了使两个不同网段之间可以互相通信。

图8-15 路由配置

注意

此路由配置，配置的是静态路由。

4. 单击<SNMP 配置>，启用或停用该配置。
5. 单击<Bypass 配置>，查看 Bypass 配置。

8.3 登录设置

1. 编辑

选中一个用户，单击<编辑>，可以对口令认证方式选择是否启用。

停用之后，这个用户就不能登录审计系统。

2. 修改密码

对该账号进行密码的修改。

此系统一个有三个地方可以进行密码的修改：

1、登录界面的修改密码，

2、<系统><登录设置>里的修改密码，

3、系统右上角界面的修改密码。

图8-16 修改密码

3. 登录认证设置

登录认证设置是对登录和密码规则的一些设置。

图8-17 登录认证设置

4. 访问控制

访问控制是对访问审计系统设置白名单。

警告

- 设置了白名单之后，只有白名单之内的 IP 可以访问。
- 设置白名单的时候请勾选 WEB，不然即使是正确的 IP，也访问不了。

8.4 数据维护

8.4.1 配置数据

1. 新建备份

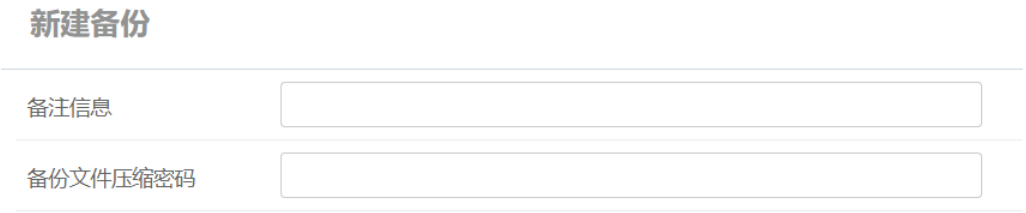
1） 单击<配置数据>，会出现配置数据详情。

图8-18 数据配置详情

2） 单击<新建备份>，添加备份消息。

图8-19 新建备份

备份文件压缩密码要谨慎保存，避免备份的配置数据无法恢复。



3） 单击提交生成备份消息。

2. 异地备份

1） 单击<异地备份配置>。

图8-20 异地备份配置

表8-2 异地备份配置表

字段	含义
备份方式	FTP
备份周期	每日、每周、每月、手动
FTP路径	FTPip地址：端口号/路径
用户名	FTP用户名
密码	FTP密码
备份文件压缩密码	压缩文件密码，压缩密码一定要谨慎保存，避免配置恢复时数据无法恢复。

3. 删除备份

对备份文件进行删除。

4. 上传备份并恢复

选择以前下载的备份文件，然后上传。

注意

此备份为系统配置的备份。

8.4.2 审计数据

1. 异地备份配置

1) 单击<审计数据>

2) 单击<异地备份配置>，进入异地备份配置列表。

图8-21 异地备份配置

表8-3 异地备份配置表

字段	含义
备份方式	FTP
备份模式	全量：对全部进行备份 增量：在上一次的基础上进行备份
备份周期	每日、每周、每月、手动
FTP路径	FTPip地址：端口号/路径
用户名	FTP用户名
密码	FTP密码
备份文件压缩密码	解压缩密码

2. 删除备份

对备份文件进行删除。

注意

此备份的为系统日志文件。

8.4.3 数据清理

1. 单击<数据清理>，进入数据清理页面，数据清理分为手动清理和自动清理，
2. 手动清理

清理早于 XX 日期的本地备份文件和运行日志，点击删除，开始清理早于配置时间的本地备份文件和运行日志。

清理早于 XX 日期的审计日志；选择日期时间，点击删除，开始清理早于配置时间的审计日志；

3. 自动清理

最大阈值和最小阈值必须选择同时配置

达到最大阈值开始清理，清理到最小阈值停止清理。

4. 勾选转储要配置转储的 ftp 路径、用户名称、密码

勾选转储失败不清理，达到最大阈值时开始转储，转储失败不做清理操作

不勾选转储失败不清理，达到最大阈值开始转储，转储失败开始清理。

勾选自动清理 XX 天前的审计数据，达到最大阈值开始清理 XX 天的审计数据。

图8-22 数据清理

8.4.4 告警发送

1. 告警发送

单击<告警发送>，可以对告警发送的方式进行编辑。

图8-23 告警发送方式

2. FTP

单击<FTP>，进入 FTP 设置。

图8-24 FTP 设置

说明

- 等级里可以选择：全部、低风险、中风险、高风险、非法。
- 风险的等级为向上兼容，即配置了低风险，可以发送低风险及以上的告警。

3. EMAIL

单击<EMAIL>，进入 EMAIL 设置。

图8-25 EMAIL 设置

4. SYSLOG

单击<SYSLOG>，进入 SYSLOG 设置。

图8-26 SYSLOG 设置

5. SNMP

单击<SNMP>，进入 SNMP 设置。

图8-27 SNMP 设置

8.4.5 升级与恢复

升级与恢复主要就是对升级信息的查看和恢复出厂设置。

1. 单击<升级>，选择升级包，填写升级内容。
2. 单击<上传>，等待升级完成即可。
3. 单击 <恢复出厂设置>。
4. 单击<确认>完成，等待恢复出厂设置完成即可。

8.4.6 报文分析

报文分析为了能更快、更及时的解决研发与现场出现的问题，此功能适用于对已支持的协议数据进行实时抓取。开启后会影响审计系统性能

1. 报文分析，抓取所以数据库的请求浏览包
2. 单击<配置>，点击开启，即会开启。
3. 单击<查找>，可以按照关键字和会话 ID 进行检索。

8.4.7 手动抓包

该功能主要是为了方便用户随时抓包使用，用户只需要输入一些简要配置信息后，就可以抓到生产环境的数据。此功能也用于抓取网络中任何协议的数据。

1. 单击<抓包配置>，可选择数据源、选择 ip、端口、大小，进行抓包，包最大 500M；单击<提交>，开始抓包
2. 单击<停止>，停止抓包
3. 选择已经抓取的数据包，单击<删除>，进行删除。

说明

- 旁路镜像：只可以按照网卡数据源进行抓包

8.4.8 系统诊断

系统诊断功能主要是为了排查审计系统出现的问题，当不能远程的时候，可以在不进入后台的情况下，下载报错日志，快速定位并解决系统问题。

系统诊断由若干条命组成，在后台实时执行， 点击下载，系统会自动打包日志文件，下载到本地计算机。

9 日志

9.1 操作日志

操作日志：用户对系统所做操作的记录，可进行条件的查询。

图9-1 条件查询

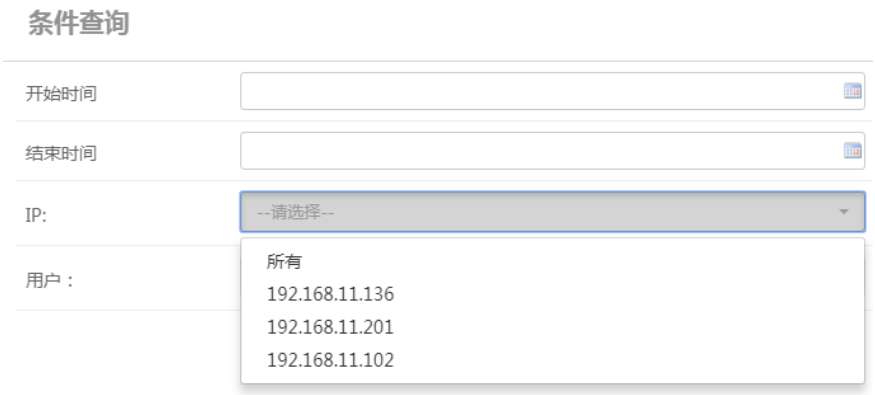


图9-2 操作日志

10 资产

10.1 资产列表

选择要查看的资产或资产组信息

1. 单击<资产列表>，可以看到刚刚选择的数据库或数据库组。

可以对数据库资产进行编辑、删除、和敏感数据扫描。

注意

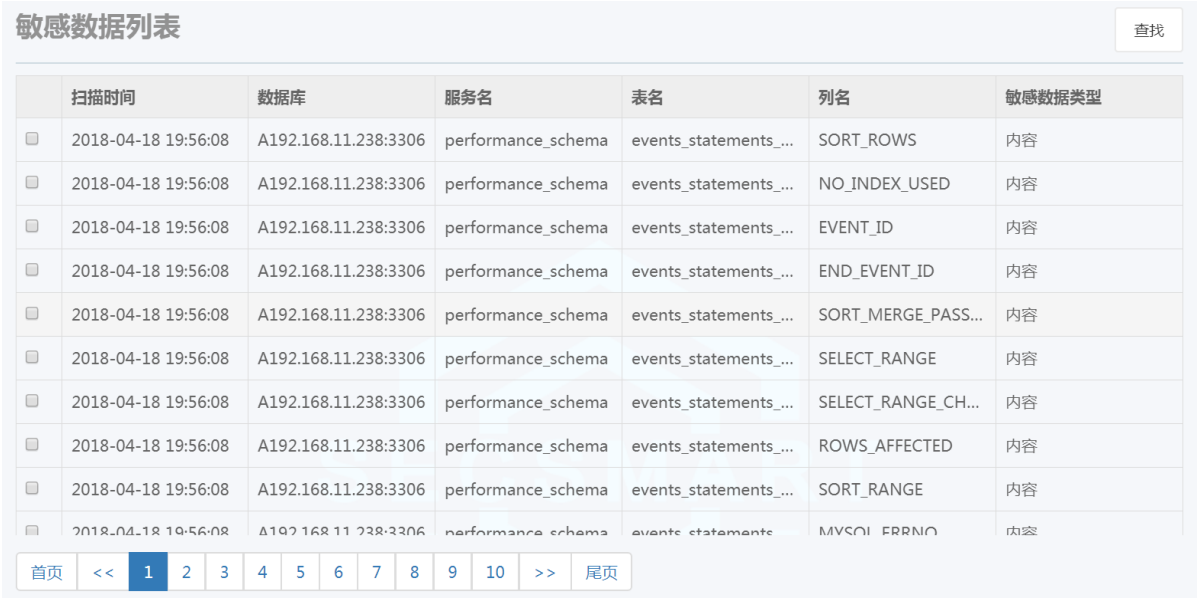
- 添加只能在数据库组下才能添加数据库。
- 进行数据库扫描的时候，数据库账号和密码必填。
- 敏感数据扫描的规则根据规则列表里添加的规则进行扫描，扫描结果在扫描结果列表显示。

10.2 敏感扫描结果列表

敏感规则主要是用来发现数据库的敏感信息。

1. 单击<敏感扫描结果列表>，进入敏感扫描结果列表。可以看到在<数据库列表>进行的敏感数据扫描的结果，并且可以进行结果的查找。

图10-1 敏感数据扫描结果列表



10.3 敏感数据规则列表

1. 单击<敏感数据规则列表>，进入规则列表，也可以对已有规则进行编辑和删除。

图10-2 敏感数据规则列表

2. 单击<添加>，进行敏感数据扫描规则的添加，选中已添加的规则，可进行规则修改。

图10-3 敏感数据扫描规则的添加

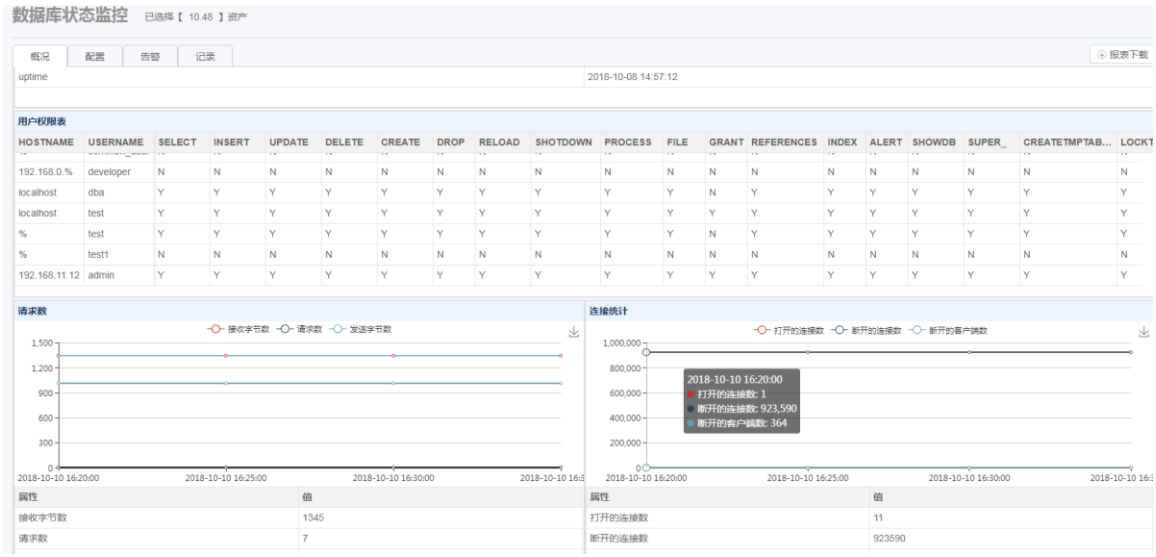
表10-1 添加敏感数据规则配置表

字段	含义
名称	给添加的规则名称命名
基于表名扫描	添加需要扫描的表
基于列名扫描	添加需要扫描的列
基于内容扫描	添加需要扫描的内容，用正则表达式表示

10.4 数据库状态监控

1. 单击<数据库状态监控>，可以查看当前所选的资产的概况、配置、告警和记录。

图10-4 数据库概况



2. 单击<配置>可以查看当前数据库配置信息。
3. 单击<告警>可以配置当前数据库告警策略。
4. 单击<记录>可以查询当前数据库告警记录。

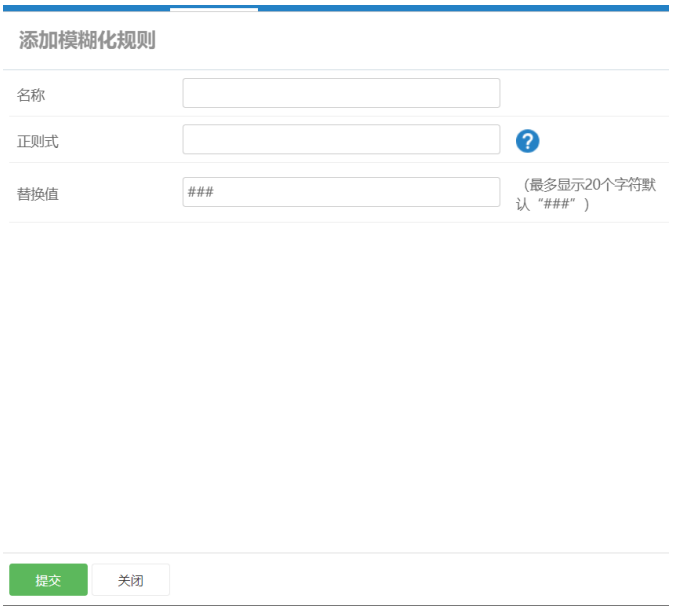
注意

- 目前支持 MySQL 和 Oracle 数据库的状态监控。
- MySQL 可以查看当前所选的资产的概况、配置、告警和记录，Oracle 可以查看当前数据库的概况、表空间、会话、回退、SGA、权限、告警、记录

10.5 模糊化规则

模糊化规则主要是用来对敏感数据进行模糊化处理的，可对敏感数据进行保护。

1. 单击<添加模糊化规则>，填写模糊化规则名称，正则式，替换值，
2. 单击 可以查看模糊化匹配规则帮助。



3. 选择已添加的规则，单击<编辑>，可编辑规则名称、正则式、替换值。
4. 选中已添加的规则，单击<删除>，可删除已添加的规则。
5. 单击<查询>，可按名称、正则式、替换值查询模糊化规则。