

BEYOND
TECHNOLOGY

东软 NetEye 数据库审计系统 用户手册

东软 NDBA7000 是综合型的数据库安全平台

目 录

一、 系统概述	4
1.1 产品简介.....	4
1.2 系统登录.....	5
1.3 退出系统.....	5
1.4 修改密码.....	6
1.5 页面布局.....	6
1.6 缺省账号.....	7
二、 系统管理员	8
2.1 监控.....	8
2.1.1 系统资源使用率.....	8
2.1.2 接口信息.....	9
2.1.3 系统告警.....	9
2.2 系统配置.....	10
2.2.1 LICENSE 授权.....	10
2.2.2 服务与时间配置.....	10
2.2.3 系统升级.....	14
2.2.4 告警通知配置.....	14
2.2.5 可靠性设置.....	19
2.2.6 关联设置.....	21
2.2.7 SNMP 配置.....	21
2.2.8 翻译字典.....	21
2.2.9 硬件和诊断.....	22
2.2.10 数据与备份.....	26
三、 安全管理员	28
3.1 主页.....	29
3.2 数据库配置.....	30
3.2.1 添加数据库.....	30
3.2.2 修改和删除数据库.....	31

3.3 数据库功能设置.....	33
3.3.1 应用模式-审计.....	34
3.3.2 应用模式-防火墙.....	43
3.4 数据库日志.....	46
3.4.1 日志显示内容.....	46
3.4.2 查询日志.....	49
3.4.3 导出日志.....	50
3.4.4 统计分析.....	50
3.4.5 报表预览.....	58
3.5 策略应用.....	65
3.5.1 策略应用.....	66
3.5.2 添加策略.....	66
3.5.3 修改和删除策略.....	67
3.5.4 规则配置.....	67
3.6 策略管理.....	67
3.6.1 概述.....	67
3.6.2 默认策略.....	68
3.6.3 策略配置.....	68
3.6.4 规则配置.....	70
3.6.5 策略应用.....	74
3.7 访问控制.....	75
3.8 报表管理.....	75
3.8.1 报表设置.....	76
3.8.2 下载和删除报告.....	76
3.9 风险扫描.....	77
3.10 状态监控.....	78
3.11 监控扫描.....	78
3.11.1 漏洞扫描.....	78
3.11.2 设备扫描.....	80
3.11.3 数据库敏感扫描.....	81
3.12 安全设置.....	82
3.12.1 设置安全参数.....	83
四、 审计管理员.....	83
4.1 监控.....	84
4.2 操作日志.....	84

4.3 用户管理.....	84
五、 用户管理.....	84
5.1 新建用户.....	85
5.2 角色管理.....	86
5.3 修改用户密码	86
5.4 删除用户.....	87
5.5 授权用户.....	88
六、 操作日志.....	88
6.1 安全管理员操作日志.....	88
6.2 审计管理员操作日志.....	89
七、 附录 1：AGENT 配置手册	90
八、 附录 2：ORACLE 集群配置说明	100
九、 附录 3：多接口镜像配置	102

一、 系统概述

1.1 产品简介

东软 NetEye 数据库审计系统是一个功能全面的数据安全平台，在其上可以提供数据库审计、数据库防火墙、数据库加密等多种功能模块，可主动、实时监控数据库安全，是集 SQL 审计、访问控制、加密脱敏等于一体的专业数据安全解决方案。

在数据库审计方面，系统采用有效的数据库审计方式，针对数据库漏洞攻击、风险操作、SQL 注入等数据库风险操作行为通过不同的审计规则发生记录和告警。面向企业级用户，集应用压力分析与 SQL 监控审计为一体的产品。它以旁路的方式部署在网络中，不影响网络的性能。具有实时的网络数据采集能力、强大的审计分析功能以及智能的信息处理能力。

在数据库防护方面，系统以在线的方式部署在网络中，采用细粒度的规则阻断，同时支持会话阻断和基于 sql 语句的阻断两种方式；包含数据库风险扫描、漏洞扫描、数据敏感信息扫描、状态监控等功能；全方位立体化的对数据库进行安全加固。

通过使用本系统，可以实现如下目标：

- ✧ 审计记录 Oracle、MySQL、SQL Server、Oracle、DB2、Sybase 等多种数据库
- ✧ 监控数据库系统状态
- ✧ 实现网络行为后期取证
- ✧ 细粒度的访问控制
- ✧ 高效率的存储检索
- ✧ 内置丰富的报表模板以及行业报表模板

东软 NetEye 数据库审计系统适用于对信息保密、非法信息传播/控制比较重视的单位，或需要实施网络行为监控的单位和部门，如政府、军队机关的网络管理部门，公安、保密、

司法等国家授权的网络安全监察部门，金融、电信、电力、保险、海关、商检、学校、军工等各行业网络管理中心，以及大中型企业网络管理中心等。

1.2 系统登录

打开浏览器，在地址栏输入 https://__系统 IP 地址__，访问产品登录界面，如下。



系统默认管理员用户包括：

- SysAdmin：系统管理员
- SecAdmin：安全管理员
- Auditor：审计管理员

其它默认的登录信息包括：

- 默认密码：admin12345
- 设备默认 IP 地址：<https://192.168.1.254>

注意：用户登录到系统界面后，可创建新的用户和修改管理接口的 IP 地址。

1.3 退出系统

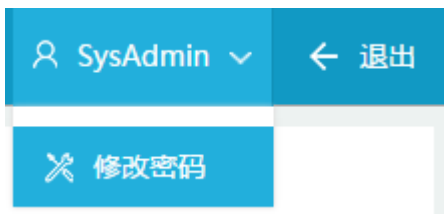
点击界面右上角<退出>按钮，即可退出系统。

退出系统时，系统不会自动保存当前配置。建议用户在退出系统前先设置保存当前配置。



1.4 修改密码

在界面右上角展开用户名下拉框，点击<修改密码>按钮，即可弹出修改密码输入框。



1.5 页面布局

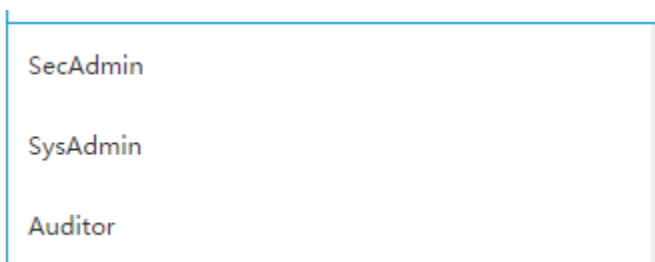
系统页面共分为：导航栏、配置区、辅助区三部分。

- 导航栏：以导航树的形式组织设备的功能菜单。用户可以在导航栏中可以方便的选择模块菜单，选择结果显示在辅助区、配置区中。
- 配置区：用户进行配置和查看的区域。
- 辅助区：显示当前配置区的页面在导航栏中的路径。



1.6 缺省账号

系统默认三个用户 SysAdmin、SecAdmin、Auditor,基于三权分立原则实现系统管理员、安全管理员、审计管理员相互监督。通过多种数据获取机制保障对所有用户的全程监控。



系统管理包括系统监控、系统配置、用户管理三部分。其中系统配置包括 LICENSE 授权、服务与时间配置、系统升级、告警通知配置、关联设置、硬件和诊断、数据与备份等。主要操作用户为 SysAdmin。

安全配置主要包括主页、系统信息、全局配置、监控扫描四部分。主页主要配置数据库信息。进入数据库配置并查看审计和防火墙、统计分析、报告预览等信息。主要操作用户为 SecAdmin。

审计管理主要包括系统管理员、安全管理员操作日志等。主要操作用户 Auditor。

二、 系统管理员

系统管理员是审计系统三大管理员之一，基于系统级别对本系统做统一的监控和管理。可以监控系统性能、操作网络配置、管理系统升级和操作系统用户。

该用户用户名：SysAdmin、缺省密码：admin12345

系统管理员登录页功能模块包括以下三部分内容：

监控模块：基于产品系统，监控产品性能

系统配置：产品系统配置

用户管理：系统用户管理

2.1 监控

系统管理员具备对整体系统的监控能力，监控内容包括系统资源使用率、接口信息、系统告警三部分信息。

2.1.1 系统资源使用率



系统资源使用率包括 CPU、内存和硬盘的使用率，判断性能压力。

2.1.2 接口信息

	接口	最大传输单元	是否回环	状态	MAC地址	IP地址	接收速率(kb/s)	接收包速率(pkts/s)	发送速率(kb/s)	发送包速率(pkts/s)
1	E0/1	9212	否	连接	00:0c:29:f9:01:48		0.41	6.00	0.00	0.00
2	E0/2	9212	否	连接	00:0c:29:f9:01:52		0.41	6.00	0.00	0.00
3	E0/3	9212	否	连接	00:0c:29:f9:01:5c		28.36	166.00	0.00	0.00
4	E0/4	9212	否	连接	00:0c:29:f9:01:66		0.41	6.00	0.00	0.00
5	HA	9212	否	连接	00:0c:29:f9:01:70		0.41	6.00	0.00	0.00
6	MGT	9212	否	连接	00:0c:29:f9:01:7a	192.168.1.254/24	0.59	9.00	0.00	0.00

接口信息包括接口、最大传输单元、是否回环、状态、MAC 地址、IP 地址、接收速率、接收包速率、发送速率和发送包速率，判断网络压力。

2.1.3 系统告警

系统告警列表 (总记录 1)

发生时间	日志类型	事件类别	事件内容
2018-02-28 08:00:00	CPU	致命	致命：CPU使用量已经超过98%

15条/页

系统告警包括告警发生时间、日志类型、事件级别和事件内容，查看资源运行情况。

2.2 系统配置

2.2.1 LICENSE 授权




系统管理员登录系统后，选择“系统配置”项，默认选中 LICENSE 授权页面，进行授权 License 的校验。

用户购买使用产品后，在本页面上传有效证书，校验通过后可正常使用。

2.2.2 服务与时间配置

服务与时间配置包括时间设置和服务配置两部分。

时间设置



15:16:46
2018-01-02

时间服务器1 自动同步

IP 端口

时间服务器2 自动同步

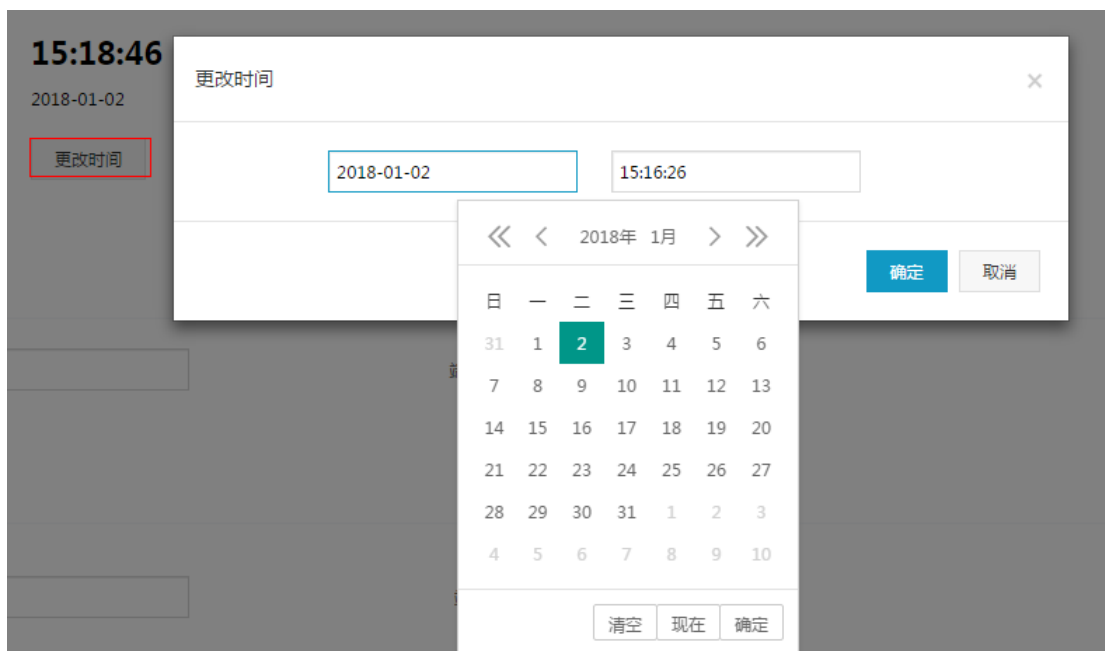
IP 端口

服务配置

时间配置：系统时间、时间服务器

服务配置：DNS 配置、WEB 配置、SSH 配置 2.2.2.1 时间配置

2.2.2.1 系统时间



在时间设置中，修改系统日期时，请单击<更改时间>按钮，将弹出日历对话框。您可以点击配置当前系统的时间，然后点击<确定>按钮，实现自定义时间设置。

2.2.2.2 时间服务器



在时间服务器中，设置 NTP 服务器的 IP 地址及服务端口（默认端口 123），点击<同步>按钮则会从相应的 NTP 服务器立即进行时间同步，勾选<自动同步>实现定时自动从相应 NTP 服务器进行时间同步，且支持 NTP 主备服务配置。

2.2.2.3 服务配置

服务配置包括三部分：

服务配置



DNS 配置

WEB 配置

SSH 配置

在 DNS 配置中，可指定三个 DNS 服务器地址，输入服务器 IP 地址后，点击<保存并生效>按钮，保存设置。

A form for DNS configuration with three input fields. The first field is labeled "DNS服务器1", the second "DNS服务器2", and the third "DNS服务器3". Each field is empty.

在 WEB 配置中，可设置对本系统的 WEB 页面访问控制。选项包括“完全访问”、“IP 白名单访问”两个选项。

访问权限 完全访问 IP白名单访问

端口

在 SSH 配置中，可设置对本系统的 SSH 远程控制。选项包括“完全访问”、“IP 白名单访问”、“禁止远程访问”三个选项。

访问权限 完全访问 IP白名单访问 禁止远程访问 (所有远程SSH均不可接入服务器,需WEB或主机操作解除。请谨慎选择!)

端口

2.2.3 系统升级

手动导入系统升级文件, 点击<升级>按钮升级系统。升级列表查看系统升级时间、概要、详细描述信息。

升级 手动导入升级文件 升级

时间	概要	详细描述
----	----	------

2.2.4 告警通知配置

告警通知方式包括五部分内容 SYSLOG 通知、邮件通知、短信通知、FTP 通知、SNMP 通知。

通知方式

SYSLOG通知	邮件通知	短信通知	FTP通知	SNMP通知
----------	------	------	-------	--------

2.2.4.1 SYSLOG 通知

SYSLOG 通知默认为“禁用”状态, 开启 SYSLOG 通知并设置 SYSLOG 通知定义, 点击<保存>。先执行“测试”, 在 SYSLOG 服务器上, 查看通知测试消息, 能正确收到消息, 对应防护数据库通知等级的日志将发送到 SYSLOG 服务器上。

SYSLOG通知

通知等级

IP

端口

数据库

2.2.4.2 邮件通知

邮件通知默认为“禁用”状态，开启邮件通知并设置邮件服务，测试通过，单击保存即可使用邮件通知功能。

邮件通知

SMTP是否验证

通知等级 低风险以上 ▼

邮件主机

收件人

发件人

密码

单封邮件统计时间周期 10 分钟 (1-500)

数据库 全部 ▼

2.2.4.3 FTP 通知

FTP 通知默认为“禁用”状态，开启 FTP 通知并设置 FTP 服务，测试通过，单击保存即可使用 FTP 通知功能。

FTP通知

通知等级

IP地址

端口 (1 - 65535)

上传目录

单次包含 条 (1 - 500)

用户名

密码

数据库

2.2.4.4 SNMP 通知

SNMP 通知默认为“禁用”状态，开启 SNMP 通知并设置 SNMP 服务，测试通过，单击保存即可使用 SNMP 通知功能。

SNMP通知

发送类型 发送统计信息 发送单条

通知等级

服务器IP地址

端口 (1 - 65535)

MIB 样例: 1.1.1.1.1.1.1.1.1

OID

数据库

2.2.4.5 短信通知

短信通知默认为“禁用”状态，开启短信通知并设置短信服务，测试通过，单击保存即可使用短信通知功能。

短信通知

通知等级

服务器IP地址

端口 (1 - 65535)

单次包含 条 (1 - 500)

收件人号码

数据库

2.2.5 可靠性设置

可靠性设置配置并显示主(备)机状态。

2.2.5.1 双机热备

设置本地和备机 HA 接口 IP 地址并保存。当防火墙(主机)故障，HA 系统检测主机故障，通知防火墙(备机)，启动备机服务，保证数据库访问业务正常运行。

双机状态

当前设备： --
服务状态： --
位置： --
主机状态： --
备机状态： --

双机设置

当前设备： 单机状态 双机状态
HA接口： HA
本地HA接口IP地址 192.168.100.100
备机HA接口IP地址

2.2.5.2 Bypass 检测

开启 Bypass 检测，检测系统 CPU、内存、服务等是否异常，确保系统的稳定性。

bypass检测

CPU超限 上限值 %
内存超限 上限值 %
系统异常
服务异常
bypass组 MGT,HA
 E0/1,E0/2

2.2.6 关联设置

配置数据库关联信息。

数据库用户信息				导入	添加
工号	姓名	部门	IP关联	操作	
46	张	财务部	172.16.0.130	编辑	删除

注意：

关联设置结合安全管理员下数据库关联配置使用。

2.2.7 SNMP 配置

SNMP 默认关闭状态，配置 SNMP 信息，点击<保存>按钮，即可查看节点信息。

SNMP配置		查看节点	保存
状态	<input type="checkbox"/>		
设备名称	<input type="text" value="xxxxxx"/>		
物理位置	<input type="text" value="xxxxxx"/>		
联系方式	<input type="text" value="xxxxxx"/>		
*community	<input type="text" value="default"/>	(V1&V2状态时必需, V3状态时除了此项其他项必需)	
支持版本	<input type="checkbox"/> V1&V2 <input type="checkbox"/> V3		

常用节点信息		
OID	名称	描述
.1.3.6.1.4.1.2021.4	memory	系统内存信息
.1.3.6.1.2.1.25.2.3	hrStorage	系统磁盘信息
.1.3.6.1.4.1.2021.10.1.3	laLoad	系统CPU负载
.1.3.6.1.4.1.2021.11	systemStatus	系统CPU信息
.1.3.6.1.2.1.2	Interfaces	系统网卡信息

2.2.8 翻译字典

翻译字典包括业务字典设置和 SQL 关键字字典设置，默认关闭状态。配置业务字典和 SQL 关键字字典，点击<保存>按钮即可。

业务字典设置 <input checked="" type="checkbox"/>			下载模板	导入	新建数据库名
名称	翻译内容	操作			
oracle	甲骨文	+ 添加子项 编辑 删除			
user	用户	+ 添加子项 编辑 删除			
name	用户名	编辑 删除			

SQL关键字字典设置 <input checked="" type="checkbox"/>			下载模板	导入	新建
SQL关键字	翻译内容	操作			
1 select	查询	编辑 删除			

2.2.9 硬件和诊断

硬件和诊断主要包括接口设置、接口功能和诊断分析三部分。

2.2.9.1 接口设置

显示界面名称、IP、MAC、MASK、状态、功能。支持编辑接口功能。另外支持网卡重排功能，良好兼容支持多扩展槽位的硬件型号设备接口面板顺序对应关系。

网卡重排						
名称	IP	MAC	Mask	状态	功能	操作
1 E0/1		4ccc6a20a146		断开		编辑
2 E0/2		4ccc6a20a147		断开		编辑
3 E0/3		4ccc6a20a148		连接		编辑
4 E0/4		4ccc6a20a149		断开		编辑
5 HA	192.168.100.100	4ccc6a20a14a		断开	ha	编辑
6 MGT	172.16.1.129	4ccc6a20a14b	255.255.255.0	连接	mgt	编辑

2.2.9.2 接口组

数据库防火墙功能部署时，配置设备接口功能，支持代理和透明部署模式。

添加									
名称	模式	接口	Bypass	网桥IP地址	MASK	网桥	联动	Vlan选择	操作
1 br0	半透明 透明	E0/1,E0/2	<input type="checkbox"/>			<input type="checkbox"/>	非联动	未开启	编辑
2 br2	半透明 透明	E0/3,E0/4	<input type="checkbox"/>			<input type="checkbox"/>	非联动	未开启	编辑

2.2.9.3 接口功能

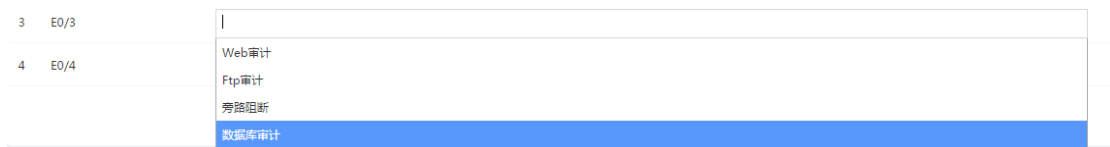
在系统配置中，点击“硬件和诊断—>接口设置—>接口功能>”页面，支持配置开启业务接口的审计业务功能。（注：Agent 审计也需开启接口功能）。



1 开启接口功能

示例：开启 E0/3 接口的数据库审计功能。

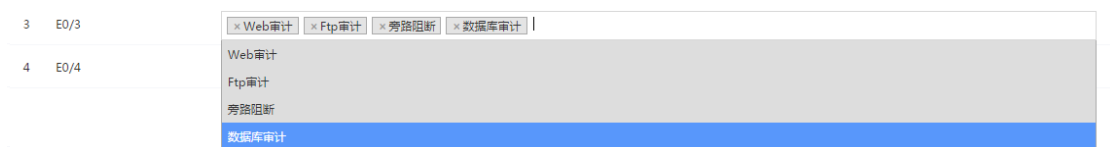
首先单击 E0/3 接口右侧的选框，会出现矩形的下拉框，然后单击下拉框中的数据库审计，选框中将会出现数据库审计。最后单击<保存>按钮即可生效。



2 取消接口功能

示例：取消 E0/3 接口的数据库审计功能。

首先单击 E0/3 接口右侧的选框，会出现矩形的下拉框，然后单击下拉框中已添加的数据库审计，选框中的数据库审计将消失。最后单击<保存>按钮即可。



2.2.9.4 接入即审计

接口设置
接口组
接口功能
接入即审计

状态

接口

停止时间

接入即审计支持配置开启后，实现自动防护审计引擎的添加，审计效果的展示。

选取已接入的审计接口，配置分析的停止时间。

注意：

1. 业务接口开启的审计功能，才能在该功能下的<接口>显示，
2. 该功能仅限于数据库旁路镜像审计使用。

2.2.9.5 路由设置

路由设置包括系统路由表和静态路由表。支持添加静态路由功能。

系统路由表				
目的IP地址	子网掩码	网关	优先级	接口
192.168.1.0	255.255.255.0	0.0.0.0	0	MGT

静态路由表				
目的IP地址	子网掩码	网关	优先级	操作
				<input type="button" value="添加"/>

2.2.9.6 诊断分析

1 抓包诊断分析

编辑抓包信息，诊断分析并实时查看抓包结果。支持下载抓包文件。

接口选择 数据库选择 抓包时间(秒) 诊断并写入文件 开始分析

2 网络、路由诊断

实时查看路由是否可达、跟踪路由状态。

Ping Tracert 开始分析

3 端口探测

分析并展示端口状态

IP 端口号 开始分析

2.2.10 数据与备份

2.2.10.1 FTP 设置

FTP 设置默认为关闭状态。设置 FTP 服务，点击<保存>按钮，系统在指定时间上传备份文件。备份文件列表查看备份信息。

FTP设置

测试 保存

状态

FTP服务器端口

每日上传时间 点

登录FTP的用户名

自动上传 天 (0-365) 以前的备份文件

登录FTP密码

失败重传

上传文件存放FTP上的目录

FTP服务器IP

备份文件列表

文件来源	名称	生成时间	备份文件大小(MB)	备份内容	状态	操作
------	----	------	------------	------	----	----

2.2.10.2 备份还原

备份还原包括日志备份和系统配置备份两部分。

1 日志备份

备份数据库审计日志并生成压缩文件

日志备份

自动备份
手动备份

自动备份

备份频率 日

开始时间 请选择月份 00:00:00

日志范围 全部备份

2 系统配置备份

备份系统配置并生成压缩文件。

系统配置备份
备份

2.2.10.3 数据清理

数据清理包括日志清理和恢复出厂设置

数据清理配置
保存

自动检测

检测频率 每半个小时

数据存储上限 80%

超时审计处理策略 审计停止写入

超时数据清理策略

- 备份系统并上传所有备份文件
- 清理系统业务数据
- 清理系统配置数据
- 删除 3 个月以前的审计日志

恢复出厂设置
恢复出厂设置

1 数据清理配置

当日志文件占用文件系统到指定上限时，配置审计处理策略。

数据清理配置

自动检测

检测频率 每半个小时

数据存储上限 80%

超限时审计处理策略 审计停止写入

超限时数据清理策略

- 备份系统并上传所有备份文件?
- 清理系统业务数据?
- 清理系统配置数据?
- 删除 3 个月以前的审计日志

2 恢复出厂设置

执行恢复出厂设置后，除系统授权状态和接口功能部分，其它配置均恢复为初始状态。

恢复出厂设置

三、 安全管理员

安全管理员是系统默认存在的用户，是监控、管理、配置安全策略的用户。

该用户用户名：SecAdmin、缺省密码：admin12345。

安全管理员包括主页、系统信息、全局配置、监控扫描四部分。



3.1 主页

主页包括数据概况和最新流量两部分。

数据库概况包括添加、编辑和删除数据库，进入数据库可以配置并开启数据库审计功能，查看数据库审计日志信息、统计分析、报告预览、状态监控、风险扫描。



最新流量：展示最新的日志信息

时间	数据库(实例)	数据库用户	数据库IP	客户端IP	客户端应用程序	风险等级	规则	动作	操作类型	SQL语句	操作
2018-03-01 19:03:43	master	sa	172.16.1.224	172.16.1.130	Microsoft JDBC Drive...	无风险	全量计划策略控制策略->...	放行	SELECT	select sys.schemas.na...	详情 会话详情
2018-03-01 19:03:43	master	sa	172.16.1.224	172.16.1.130	Microsoft JDBC Drive...	无风险	全量计划策略控制策略->...	放行	NONE	select castnull as cha...	详情 会话详情
2018-03-01 19:03:43	master	sa	172.16.1.224	172.16.1.130	Microsoft JDBC Drive...	无风险	全量计划策略控制策略->...	放行	SELECT	select sys.schemas.na...	详情 会话详情
2018-03-01 19:03:42	master	sa	172.16.1.224	172.16.1.130	Microsoft JDBC Drive...	无风险	全量计划策略控制策略->...	放行	NONE	sp_dbattype_info_300...	详情 会话详情
2018-03-01 19:03:42	master	sa	172.16.1.224	172.16.1.130	Microsoft JDBC Drive...	无风险	全量计划策略控制策略->...	放行	SELECT	select sys.schemas.na...	详情 会话详情
2018-03-01 19:03:42	master	sa	172.16.1.224	172.16.1.130	Microsoft JDBC Drive...	无风险	全量计划策略控制策略->...	放行	NONE	select castnull as cha...	详情 会话详情
2018-03-01 19:03:42	master	sa	172.16.1.224	172.16.1.130	Microsoft JDBC Drive...	无风险	全量计划策略控制策略->...	放行	NONE	sp_configure 'user co...	详情 会话详情
2018-03-01 19:03:42	master	sa	172.16.1.224	172.16.1.130	Microsoft JDBC Drive...	无风险	全量计划策略控制策略->...	放行	NONE	select ositem user	详情 会话详情

3.2 数据库配置

进入安全管理主页，数据库管理包括数据库的添加、编辑和删除。



3.2.1 添加数据库

在安全管理主页，点击<添加>按钮，选择不使用配置向导，弹出“添加数据库”配置界面，界面默认选择 Oracle 数据库、版本号 9i、端口号 1521。输入名称、选择数据库类型、选择模式、接口、输入数据库(实例)、IP、备注、确认端口、版本，点击<确定>按钮即可。

添加数据库×

*名称	<input type="text"/>	类型	<input type="text" value="Oracle"/>
模式	<input type="text" value="审计"/>	接口	<input type="text" value="E0/3"/>
版本	<input type="text" value="9.1.0.1"/>	*数据库(实例)	<input type="text"/>
*端口	<input type="text" value="1521"/>	*IP	<input type="text"/>
备注	<input type="text"/>		

3.2.2 修改和删除数据库

点击<编辑>按钮，弹出编辑数据库界面，回显创建数据库时添加的内容，修改数据库名称、数据库实例、备注，点击<确定>按钮，保存修改数据库信息。

编辑数据库 ×

*名称	<input type="text" value="172.18.200.20"/>	类型	<input type="text" value="Oracle"/>
模式	<input type="text" value="审计"/>	接口	<input type="text" value="E0/3"/>
版本	<input type="text" value="9.1.0.1"/>	*数据库(实例)	<input type="text" value="oracle"/>
*端口	<input type="text" value="1521"/>	*IP	<input type="text" value="172.18.200.20"/>
备注	<input type="text"/>		

点击<删除>按钮，弹出删除提示框，提示用户：确定删除此数据库！，点击<确定>按钮，删除数据库。

注意：

1. 可以修改名称、数据库(实例)、备注。其它项均支持修改。
2. 删除数据库时，需先关闭审计或防护墙模式开关。
3. 删除数据库后，数据库下的统计分析、报表预览、状态监控、风险扫描信息均被删除，但该库的审计日志仍被保留。

3.3 数据库功能设置

安全管理员登入，进入数据库，选中“设置->功能设置”项，进入数据库设置页面，界面左下角显示当前数据库基本信息，用户可以在配置区设置数据库审计及防火墙、Agent 配置信息。

100pts
设置

- 日志 >
- 设置 >
 - 功能设置
 - 策略应用
 - 访问控制
 - 自学习防护
- 扫描 >
- 状态监控 >
- 数据脱敏 >

数据库IP
172.18.200.20
数据库类型
Oracle
版本
9.1.0.1
数据库(实例)
oracle

审计与防火墙

应用模式 审计 防火墙

数据来源

编码

关联配置

旁路阻断

数据脱敏

无连接会话识别

监控数据库应管

影响行辅助

邮件告警通知

模糊化日志

会话超时 天 时 分

Agent

CPU

内存

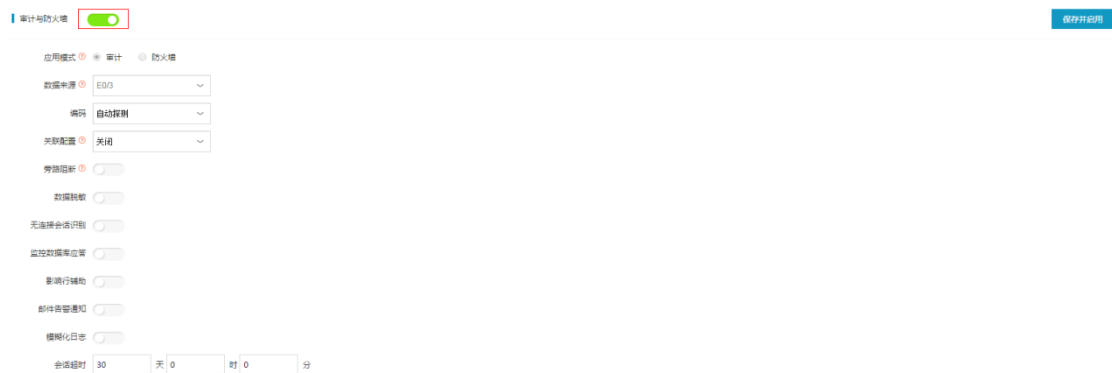
接收端口 (7000 ~ 8000)

CPU阈值

3.3.1 应用模式-审计

3.3.1.1 审计

审计数据来源(接口)显示网卡名称,引擎只有停止状态下,可以编辑数据来源(接口),点击“保存并启用”按钮,接口信息保存成功。



注意:

1. 选择的数据库来源(接口)需要开启审计功能,若未开启审计功能,则要在系统管理员下“系统配置->硬件和诊断->接口设置->接口功能”中选择对应接口和功能,点击<保存>按钮,接口功能开启成功,否则审计无日志。
2. 手动添加数据库,进入设置页面,数据库审计默认显示启用状态。
3. 配置向导添加数据库,进入设置界面,数据库审计默认显示启用状态。

3.3.1.2 数据来源(接口)

系统管理员下开启接口审计功能。数据来源接口必须是“up”的状态。



3.3.1.3 编码方式

某些数据库编码方式特殊，审计结果为乱码，需要指定编码方式。（如：人大金仓为 GBK）



编码包括 GBK、UTF-8、UNICODE、GB2312、UTF-16、UTF-32、自动探测七种，默认选中自动探测。

注意：引擎启用状态下也可以编辑编码方式，点击<保存并启用>按钮，保存成功。该功能也支持防火墙模式。

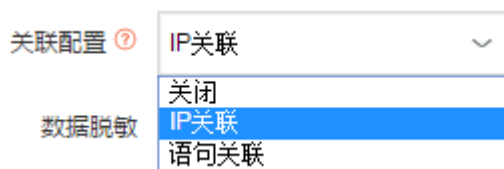
3.3.1.4 关联配置

1 概述

关联配置包括 IP 关联、语句关联两部分。

IP 关联：通过 IP 地址关联工号、姓名和部门信息，来实现 IP 地址的别名管理。

语句关联：通过指定的 SQL 语句关联工号、姓名和部门信息



2 配置步骤

关联设置：登入系统管理员，“系统配置->关联设置”，进行添加或导入用户的工号、姓名、部门、IP 地址信息。

数据库用户信息					导入	添加
工号	姓名	部门	IP关联	操作		

关联配置：IP 关联、语句关联

IP 关联开启即可

关联配置 ?

数据脱敏

IP关联

关闭

IP关联

语句关联

语句关联：指定的 SQL 语句（例如：`select * from user where ID =:id`）

关联配置 ?

语句关联

SQL语句

3 编辑和删除

点击<编辑>按钮，弹出编辑框，修改姓名、工号、部门、IP，点击<确定>按钮即可。

点击<删除>按钮，提示“确认删除”，点击<确认>，删除成功。

数据库用户信息					导入	添加
工号	姓名	部门	IP关联	操作		
1007	张三丰	研发部	192.168.100.123	编辑 删除		

注意：该功能也支持防火墙模式。

3.3.1.5 旁路阻断

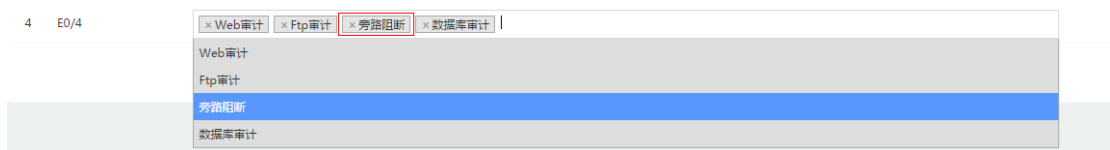
1 概述

数据库审计匹配阻断策略规则时，审计系统瞬间构造大量 RST 报文，模拟从数据库端发送给远端用户，远端用户收到大量 RST 报文，将关闭与数据库建立的已有连接，从而达到了旁路阻断的效果。



2 配置步骤

接口功能配置：开启数据库审计和旁路阻断功能，若未开启，在系统管理员下“系统配置->硬件诊断->接口设置->接口功能”选择对应接口数据库审计和旁路阻断功能，点击<保存>按钮；



旁路审计设置：配置审计和阻断接口(网卡)；

审计与防火墙

应用模式 [?] 审计 防火墙

数据来源 [?]

编码

关联配置 [?]

旁路阻断 [?]

网卡

数据引擎：配置绑定审计接口(数据来源(接口))和阻断接口(网口)，同时关联上阻断策略规则；



审计接口：在日志中查看匹配产生的阻断审计日志；

注意：

1. 引擎只有停止状态下可以编辑。
2. 需要到用户端路由可达。
3. 注意指定的旁路阻断发包接口，一般情况，审计接口与发包接口不同，有些交换机会屏蔽瞬间产生的 RST 报文。

3.3.1.6 无连接会话识别

1 概述

无连接会话识别应用场景：客户端已连接数据库，业务正常运行中，此时双方流量中已不再交互连接信息，故审计到的日志记录没有数据库的连接信息。开启无连接会话识别后，应用端实时建立了与数据库的新连接，审计系统匹配后，日志记录中会关联连接信息，如数据库用户名，操作系统用户，主机名，客户端应用程序。

注意：该功能存在误关联的现象，仅支持数据库审计模式。

2 配置步骤

无连接会话识别

(1) 开启无连接会话识别

(2) 客户端新建一次连接

3.3.1.7 监控数据库应答

监控数据库应答默认为“未启用”状态，若启用监控数据库应答功能，响应状态为执行成功、执行失败、登录、注销等。否则为未知。可以在日志详情中查看 SQL 语句的响应状态，

监控数据库应答

注意：该功能也支持防火墙模式。

3.3.1.8 邮件告警通知

1 概述

通过邮件发送数据库的告警信息

2 配置步骤

(1) 告警通知配置：系统管理员登入->系统配置->告警通知配置->邮件通知；

邮件通知

SMTP是否验证

通知等级

邮件主机

收件人

发件人

密码

单封邮件统计时间周期 分钟 (1-500)

数据库

(2) 安全管理员登入，在主页上进入数据库，点击<设置>，开启邮件告警通知状态，输入收件人邮箱地址

邮件告警通知

收件人

注意：该功能也支持防火墙模式。

3.3.1.9 模糊化日志

1 概述

防止请求语句中敏感信息泄露(如：身份证号、手机号等)，将审计日志中敏感信息模糊化处理后存储。审计日志中用户只看到替换模糊后的参数值。

模糊化日志

注意：引擎“启用”状态下也可以编辑模糊化日志。

2 添加

点击<添加>按钮，弹出提示框，输入名称、正则式、替换值，点击<确定>按钮。

名称	正则	替换值	操作
help	help	###	编辑 删除
+ 添加			

3 编辑和删除

点击<编辑>按钮，弹出编辑框，修改名称、正则式、替换值，点击<确定>按钮即可。

点击<删除>按钮，提示“确认删除”，点击<确认>，删除成功。

名称	正则	替换值	操作
help	help	###	编辑 删除
+ 添加			

注意：该功能也支持防火墙模式。

3.3.1.10 数据库辅助登录

配置数据库辅助登录，点击<保存并启用>按钮即可。

数据库辅助登录

IP地址 端口 用户名

密码

注意：

1. 该功能仅适用于 SQL Server2005/2008/2014 数据库。
2. 必须支持到数据库路由可达，否则测试连接失败。
3. 该功能也支持防火墙模式。

3.3.1.11 会话超时

会话超时默认 30 天。设置会话超时，点击<保存并启用>按钮即可。

会话超时 天 时 分

注意：该功能支持数据库审计模式下，应用端长连接情况的应用需求。

3.3.1.12 Agent

当工作环境中无法部署端口镜像时，可以部署 agent 方式进行数据库审计。

Agent

CPU

内存

接收端口 (7000 ~ 8000)

CPU阈值

审计端口

审计接口

Agent插件下载 [windows\(Vista及更高\)插件下载](#) [windows\(Server2003/XP\)插件下载](#) [linux插件下载](#)

IP	掩码	操作
127.0.0.1	255.255.255.255	删除
+ 添加		

3.3.1.13 云审计

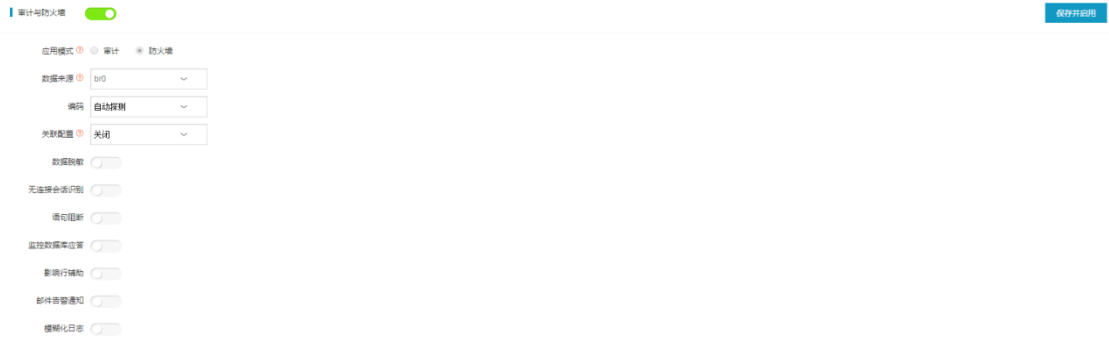
支持 MySQL 数据库虚拟化的审计。

当工作环境不支持镜像，不支持数据库代理配置，同时要求实现数据库审计功能，可以配置该功能实现数据库审计。

3.3.2 应用模式-防火墙

3.3.2.1 防火墙模式

数据来源(接口)显示接口名称，引擎只有停止状态下，可以编辑数据来源(接口)，点击“保存并启用”按钮，接口信息保存成功。



3.3.2.2 数据来源(接口)

系统管理员下开启接口组模式，所组成的接口必须是“up”状态。



3.3.2.3 数据脱敏

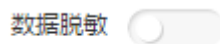
1 概述

数据脱敏是基于数据库防火墙代理部署模式下的功能，通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。

注意：该功能仅支持数据库防火墙代理模式。

2 配置步骤

- (1) 设备与脱敏数据库网络可达。
- (2) 数据脱敏配置包括三部分：表脱敏、SQL 脱敏、授权。



3.3.2.4 监控数据库应答

监控数据库应答默认为“关闭”状态，若启用监控数据库应答功能，响应状态为执行成功、执行失败、登录、注销等。否则为未知。可以在日志详情中查看 SQL 语句的响应状态，

监控数据库应答

3.3.2.5 影响行辅助

1 概述

影响行辅助默认为“关闭”状态，若开启影响行辅助并配置“影响行数”规则后，用户对数据库进行增删改查操作后，审计日志详情显示用户操作数据库后影响的数据条数并匹配到相应的影响行数规则。

2 配置步骤

(1) 设备和数据库保持网络可达。

(2) 配置“影响行数”：“安全管理员登入->全局配置->策略管理->编辑全审计策略->结果->影响行数”（开启状态，设定影响行数）

结果



响应时间	影响行数	发生次数	认证结果
	状态 <input checked="" type="checkbox"/>		
	影响行数 等于		影响行数

(3) 配置“影响行辅助”：安全管理员登入，进入数据库，点击<设置>，开启影响行辅助，输入数据库 DBA 用户名和密码。

影响行辅助

用户名 密码

是否有管理员权限 是 否

3.4 数据库日志

数据库日志包括审计日志、检索日志、会话日志。用户可以查看日志，可以根据不同的条件查询日志，导出日志，可以根据不同的条件统计分析日志，导出报告。

3.4.1 日志显示内容

日志显示分四部分全局日志、检索日志、会话日志。

日志按时间倒序展示，默认显示 15 条。

日志列表 (总记录 557条)

时间	数据库用户	数据库IP	客户端IP	风险等级	规则	动作	操作类型	SQL语句	操作
2018-01-02 16:32:28	sys	172.17.200.25	172.16.2.126	高风险	22->22:全审计报精察制...	放行	LOGOUT	logout	详情 会话详情
2018-01-02 16:32:25	sys	172.17.200.25	172.16.2.126	高风险	22->22:全审计报精察制...	放行	SELECT	select dbms_transaction...	详情 会话详情
2018-01-02 16:32:25	sys	172.17.200.25	172.16.2.126	高风险	22->22:全审计报精察制...	放行	SELECT	select 1 from dual	详情 会话详情
2018-01-02 16:32:25	sys	172.17.200.25	172.16.2.126	高风险	22->22:全审计报精察制...	放行	SELECT	select 1 from dba_fm_s...	详情 会话详情
2018-01-02 16:32:25	sys	172.17.200.25	172.16.2.126	高风险	22->22:全审计报精察制...	放行	SELECT	select 1 from dba_views...	详情 会话详情
2018-01-02 16:32:25	sys	172.17.200.25	172.16.2.126	高风险	22->22:全审计报精察制...	放行	SELECT	select 1 from dba_objec...	详情 会话详情
2018-01-02 16:32:25	sys	172.17.200.25	172.16.2.126	高风险	22->22:全审计报精察制...	放行	SELECT	select 1 from dba_trigg...	详情 会话详情
2018-01-02 16:32:25	sys	172.17.200.25	172.16.2.126	高风险	22->22:全审计报精察制...	放行	SELECT	select 1 from dba_objec...	详情 会话详情
2018-01-02 16:32:25	sys	172.17.200.25	172.16.2.126	高风险	22->22:全审计报精察制...	放行	SELECT	select 1 from dba_edtio...	详情 会话详情
2018-01-02 16:32:25	sys	172.17.200.25	172.16.2.126	高风险	22->22:全审计报精察制...	放行	SELECT	select 1 from dba_jobs ...	详情 会话详情
2018-01-02 16:32:25	sys	172.17.200.25	172.16.2.126	高风险	22->22:全审计报精察制...	放行	SELECT	select 1 from dba_objec...	详情 会话详情
2018-01-02 16:32:25	sys	172.17.200.25	172.16.2.126	高风险	22->22:全审计报精察制...	放行	SELECT	select 1 from dba_qua...	详情 会话详情
2018-01-02 16:32:25	sys	172.17.200.25	172.16.2.126	高风险	22->22:全审计报精察制...	放行	SELECT	select 1 from dba_qua...	详情 会话详情
2018-01-02 16:32:25	sys	172.17.200.25	172.16.2.126	高风险	22->22:全审计报精察制...	放行	SELECT	select 1 from apex_rele...	详情 会话详情
2018-01-02 16:32:25	sys	172.17.200.25	172.16.2.126	高风险	22->22:全审计报精察制...	放行	SELECT	select 1 from sys.dba_re...	详情 会话详情

15条/页 1 2 3 4 5 6 ... > 跳转到 1 GO

点击日志列表右侧操作列的<详情>按钮，查看日志详细信息，点击日志详情右下角<上一页>或<下一页>，查看单条日志详情。

日志详情



时间	2018-02-28 09:12:10	风险等级	无风险
动作	放行	策略规则	全审计策略复制策略->全审计策略
数据库名称	192.168.0.4	数据库类型	ORACLE
数据库(实例)	sxqy	数据库IP	192.168.0.4
数据库用户	scott	数据库端口	1521
数据库MAC	00-04-96-97-79-E4	客户端IP	207.168.0.12
客户端MAC	00-E0-4C-68-1A-48	客户端应用程序	E:\阳光门诊诊间\mzzj.exe
客户端端口	64181	客户端操作系统主机	MYFCM6N0AS7NOUV
客户端操作系统用户	Administrator	日志级别	总是记录
响应时长	0毫秒	响应状态	注销
操作对象		操作对象类型	None
操作类型	LOGOUT	其他	
返回长度	0Byte		
SOL语句	logout		

上一条
下一条
取消

1 最新流量

安全管理员身份登录系统，审计配置完成后，操作数据库，主页最新告警中能够查看所有数据库的日志信息列表，主页显示日志信息包括时间、数据库(实例)、数据库用户、数据库IP、客户端IP、客户端应用程序、风险等级、规则、动作、操作类型、SQL 语句十一项内容，若查看其它日志信息，点击<详情>按钮可以查看日志详情。

时间	数据库(实例)	数据库用户	数据库IP	客户端IP	客户端应用程序	风险等级	规则	动作	操作类型	SQL语句	操作
2018-02-28 18:12:54	ord	STARNG	172.16.1.108	172.16.1.144	JDBC Thin Client	无风险	全审计策略复制策略->...	放行	SELECT	select round(sumpin...	详情

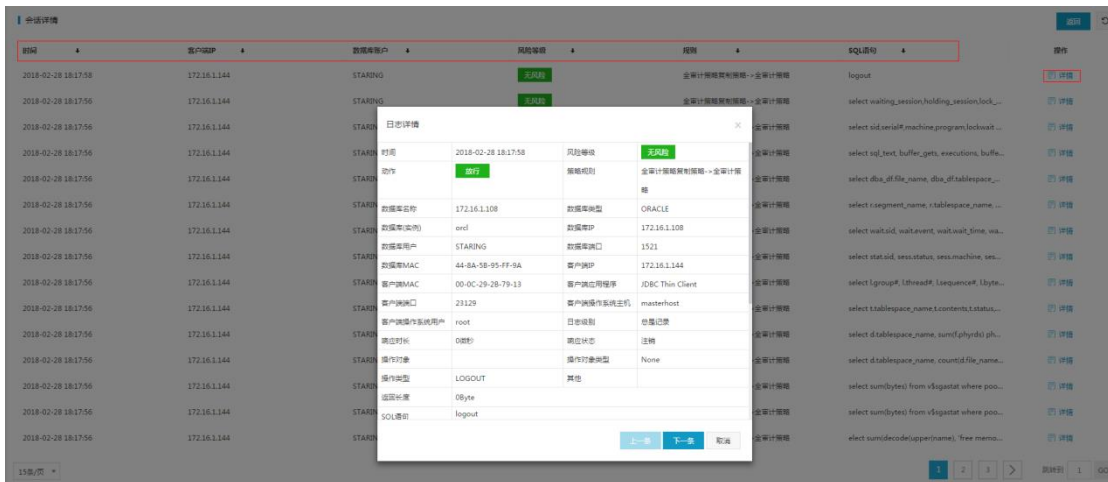
2 检索

首页进入数据库，在数据库菜单日志子选项中点击“检索”项，进入检索模块，查看单个数据库的日志列表。检索界面显示日志信息包括时间、数据库用户、数据库 IP、客户端 IP、风险等级、规则、动作、操作类型、SQL 语句九项内容，若查看其它日志信息，点击<详情>按钮可以查看日志详情。



3 会话

在主页界面操作列，点击<会话详情>按钮，进入会话详情界面，展示会话日志信息，会话详情界面显示日志信息包括时间、客户端 IP、数据库账户、风险等级、规则、SQL 语句六项内容，若查看其它会话信息，点击<详情>按钮可以查看会话详情。

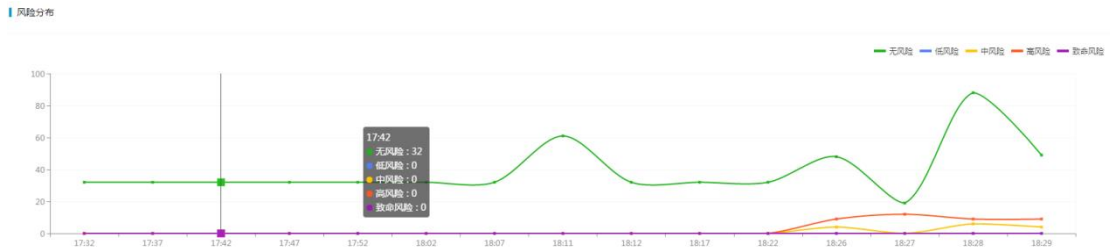


4 概况

进入数据库，选择日志子项概况，可以查看数据库概况信息。

概况包括三部分：

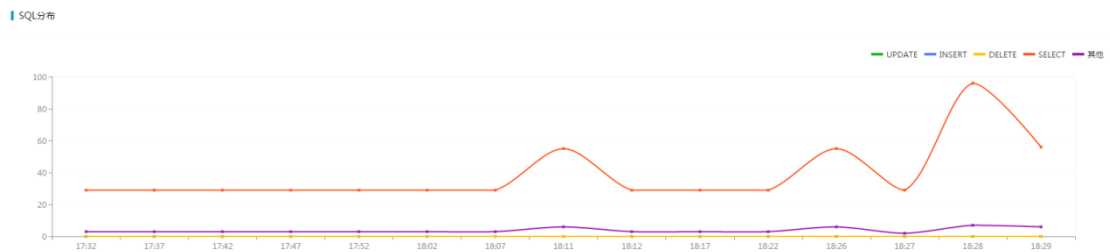
风险分布



会话统计



SQL 分布



3.4.2 查询日志

检索有查询功能，点击<筛选>按钮，展开查询条件，设置查询条件，点击<查询>按钮可以查看指定的审计日志。

客户端IP	<input type="text" value="客户端IP"/>	数据库用户	<input type="text" value="数据库用户"/>	关键字	<input type="text" value="关键字"/>	操作类型	<input type="text" value="操作类型"/>
策略	<input type="text" value="策略"/>	风险等级	<input type="text" value="风险等级"/>	动作	<input type="text" value="动作"/>	数据库(实例)	<input type="text" value="数据库(实例)"/>
<input type="button" value="查询"/> <input type="button" value="取消"/>							

注意：

风险等级包括无风险、低风险、中风险、高风险、致命风险五种类型

动作包括放行、报警、阻断三种

策略包括策略管理中自定义策略和系统内置策略

3.4.3 导出日志

检索日志均支持导出报表功能。导出报表支持 WORD、PDF、EXCEL 三种格式，可以自定义导出日志行数，最多支持两万行。还可以根据查询条件导出报表，日志按照时间倒叙展示。

点击<导出报表>按钮，弹出导出选项框，设置导出报表日志行数、选择报表格式，点击<确定>按钮即可导出报表。

报表导出

行数 全部 (最多两万行) 指定 _____ 行数

导出格式

- Pdf
- Pdf
- Excel
- Word

确定 取消

3.4.4 统计分析

首页进入数据库，在日志子选项中点击“统计分析”项，进入统计分析界面。默认展示历史日志、今日日志统计饼状图和日志月统计柱状图。



选择统计分析类型包括客户端 IP、客户端操作系统用户、客户端工具、客户端操作系统主机名、服务端 IP、服务端 MAC、数据库用户、操作对象、操作类型、动作和风险等级。

- 客户端 IP
- 客户端操作系统用户
- 客户端工具
- 客户端操作系统主机名
- 服务端 IP
- 服务端 mac
- 数据库用户
- 操作对象
- 操作类型
- 动作
- 风险等级

统计分析时间可选择本日、本周、本月、最近 1 小时、最近 2 小时、最近 3 小时、最近 7 天、最近 30 天以及自定义时间范围

选择统计分析类型、时间即可生成统计分析结果。

今日
本周
本月
最近1小时
最近2小时
最近3小时
最近7天
最近30天

<< < 2018年 1月 2018年 2月 > >>

日	一	二	三	四	五	六	日	一	二	三	四	五	六
31	1	2	3	4	5	6	28	29	30	31	1	2	3
7	8	9	10	11	12	13	4	5	6	7	8	9	10
14	15	16	17	18	19	20	11	12	13	14	15	16	17
21	22	23	24	25	26	27	18	19	20	21	22	23	24
28	29	30	31	1	2	3	25	26	27	28	1	2	3
4	5	6	7	8	9	10	4	5	6	7	8	9	10

选择时间

点击统计分析结果中<生成报告>按钮，即可生成报表。报告支持 WORD、PDF、EXCEL 三种格式。

报表导出 ×

格式

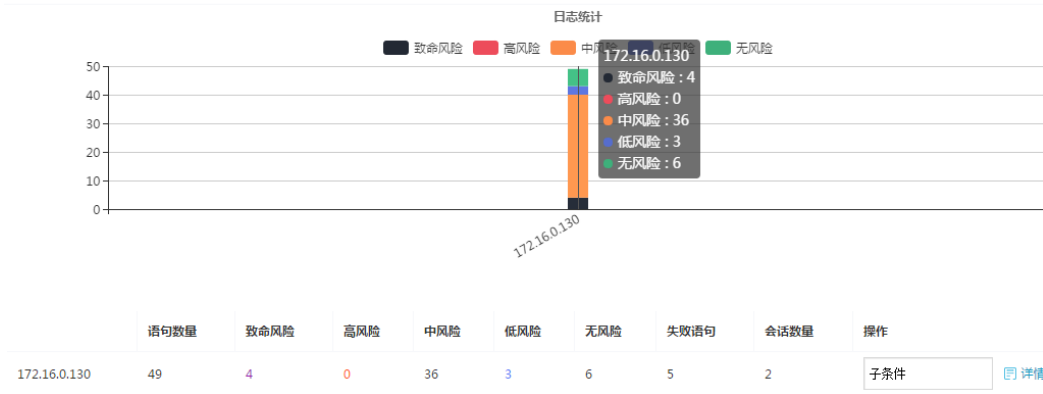
- Pdf
- Pdf**
- Excel
- Word

可以通过“管理配置->报告列表”中查看生成报告，生成报告包括报告名称、范围、报告生成时间、内容、状态及操作。

统计分析支持类型如下：

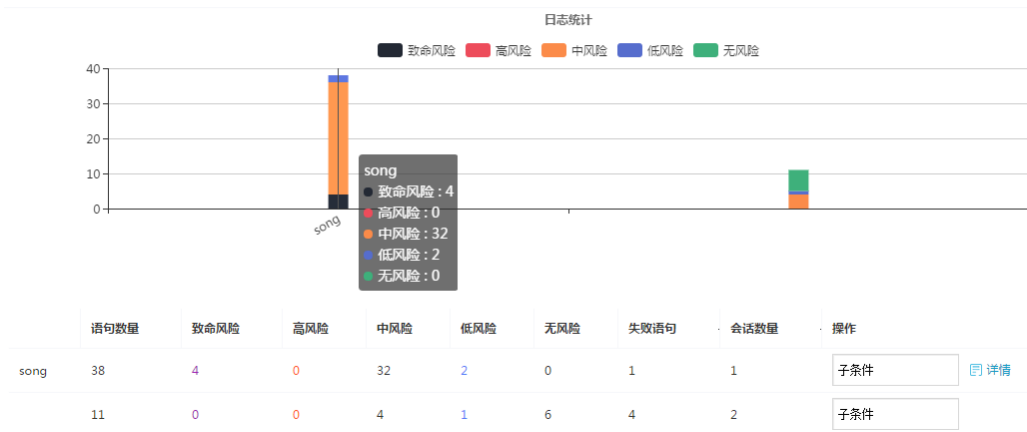
客户端 IP

日志统计



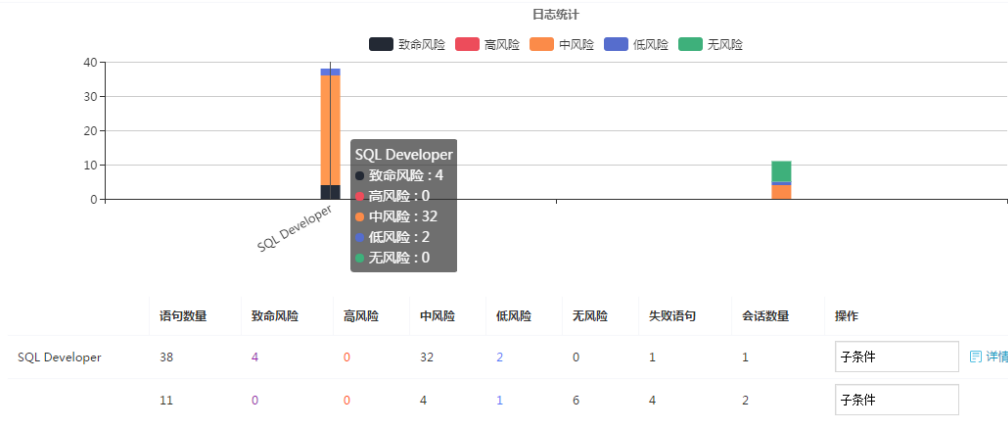
客户端操作系统用户

日志统计



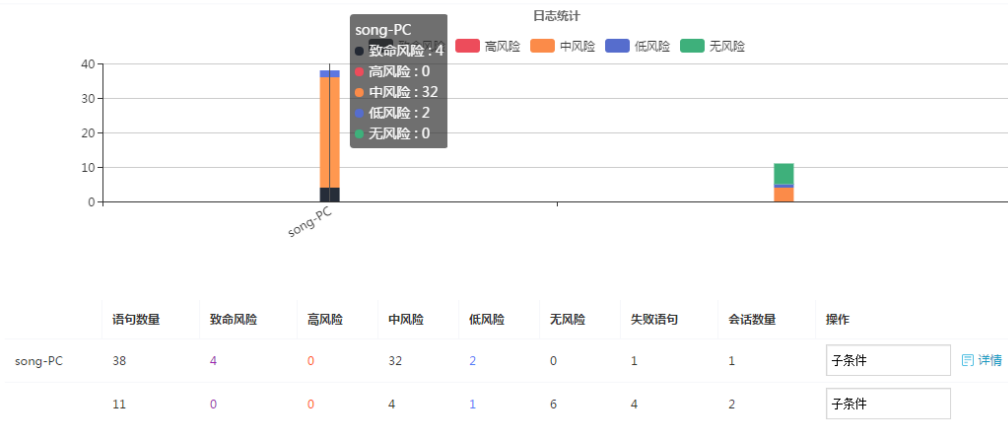
客户端工具

日志统计



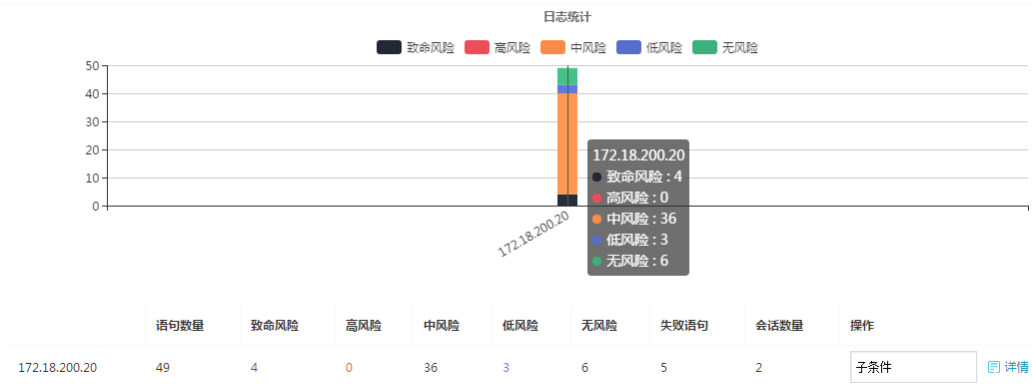
客户端操作系统主机名

日志统计



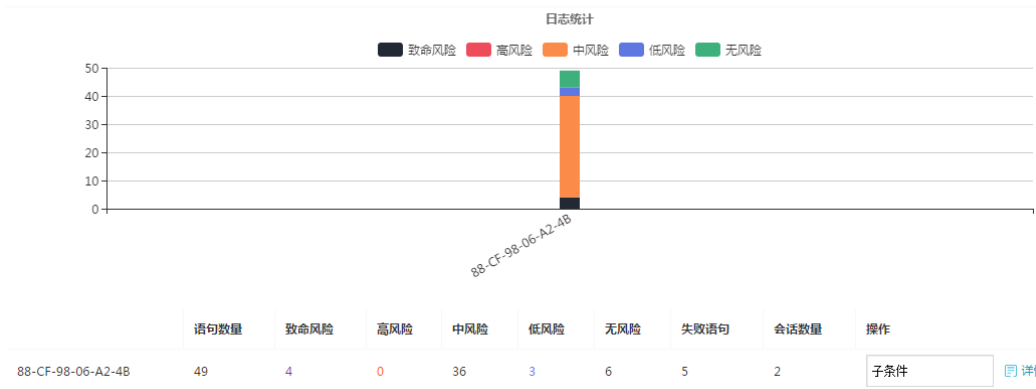
服务端 IP

日志统计



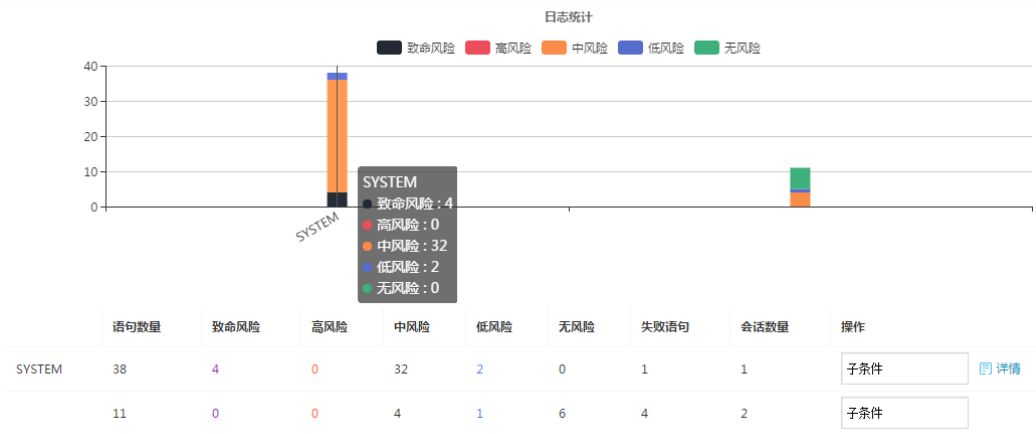
服务端 MAC

日志统计



数据库用户

日志统计



操作对象

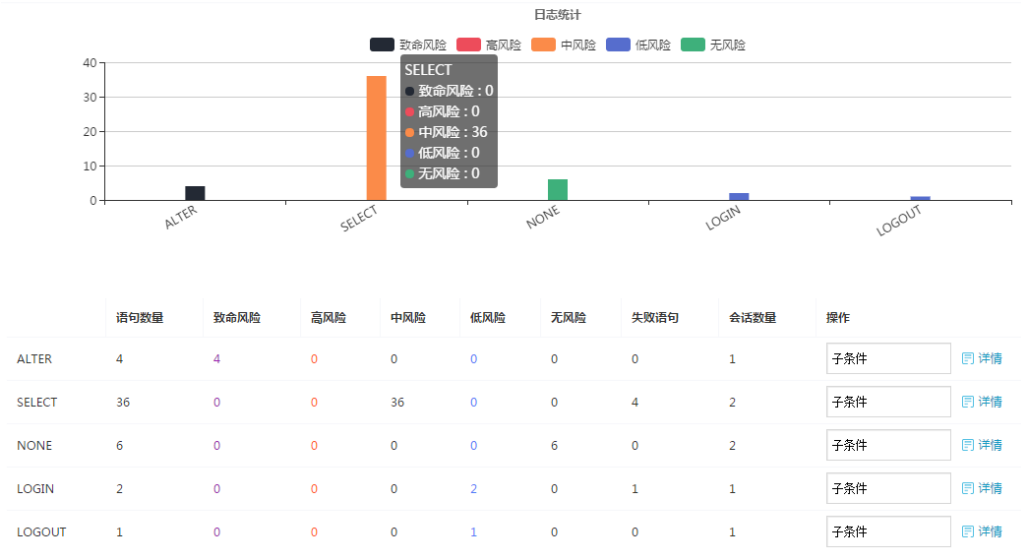
日志统计

[生成报告](#)



操作类型

日志统计



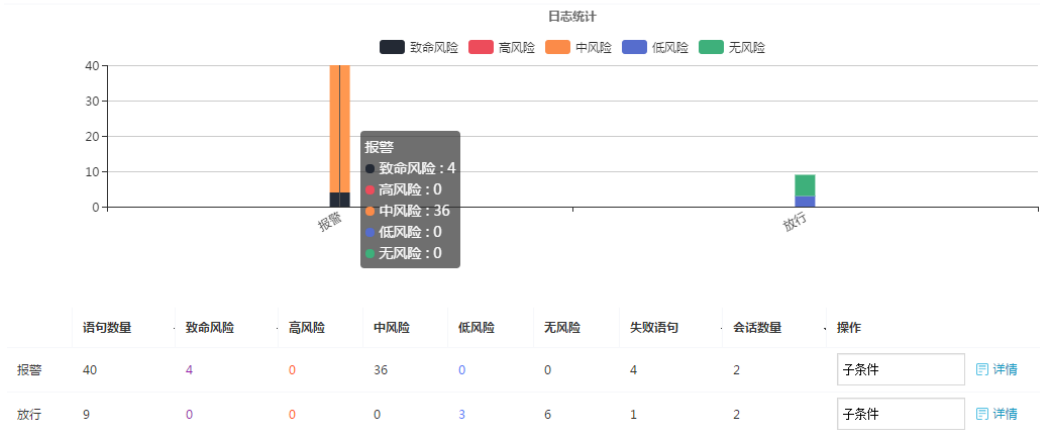
动作

日志统计



类型

日志统计

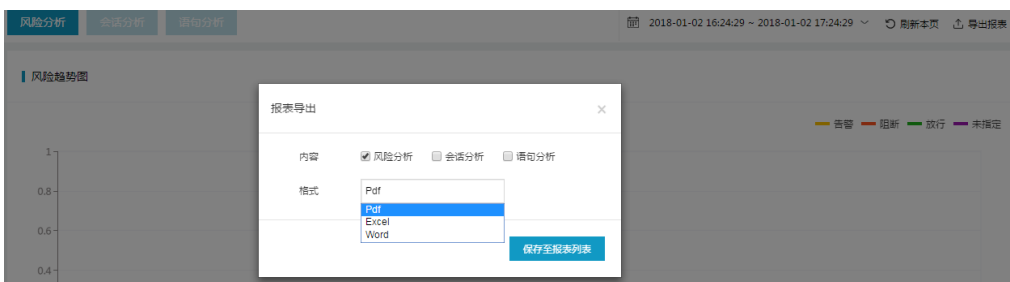


3.4.5 报表预览

报表预览包括：风险分析、会话分析、语句分析三部分。



点击<导出报表>按钮，弹出报表导出提示框，选择报表内容、格式，点击<保存至报表列表>即可生成报表。报表支持 PDF、WORD、EXCEL 格式三种格式。



可以通过“全局配置->报表管理”中查看生成报表

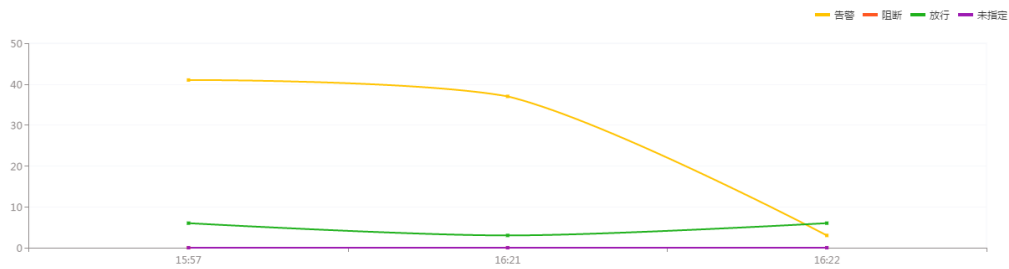
名称	范围	生成时间	内容	格式	状态	操作
172.16.1.108会话分析-语句分析180301093942	172.16.1.108	2018-03-01 09:39:42	会话分析-语句分析	Pdf	100% 已完成	下载 删除
172.16.1.108风险分析180301093932	172.16.1.108	2018-03-01 09:39:32	风险分析	Pdf	100% 已完成	下载 删除

1 风险分析

风险分析包括四部分：

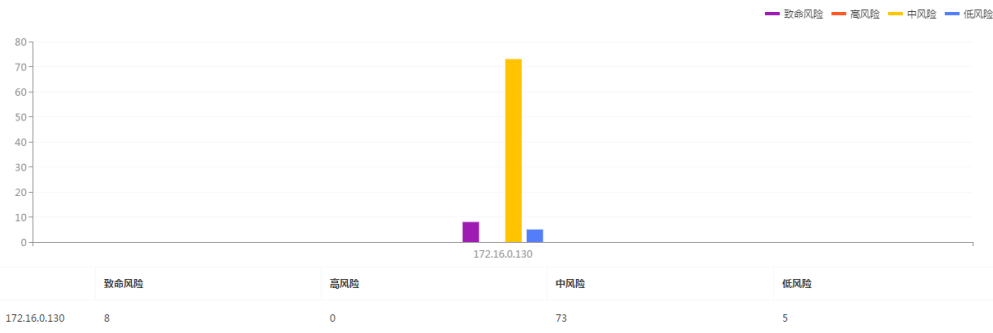
数据库风险趋势

风险趋势图



客户端 IP 分布 Top10

客户端IP分布Top10



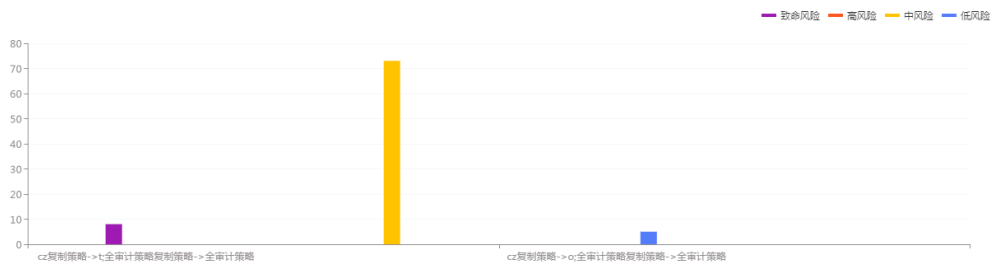
数据库账号分布 Top10

数据库账号分布Top10



规则命中分布 Top10

规则命中分布Top10



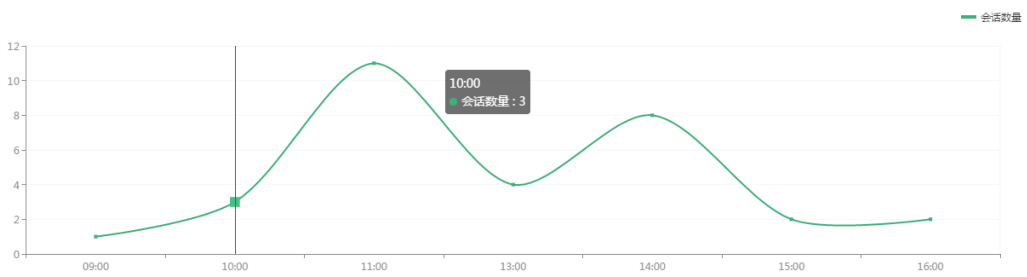
	致命风险	高风险	中风险	低风险
cz复制策略->t全...	8	0	0	0
cz复制策略->r全...	0	0	73	0
cz复制策略->o...	0	0	0	5
全审计策略复制策...	0	0	0	0

2 会话分析

会话分析包括六部分：

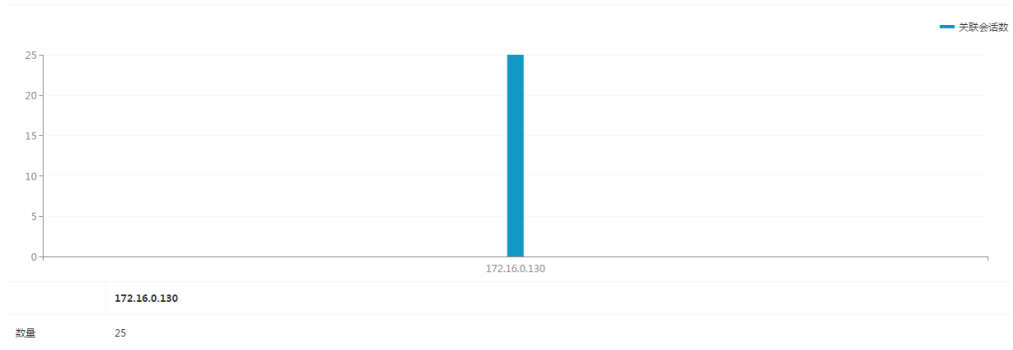
会话统计

会话统计



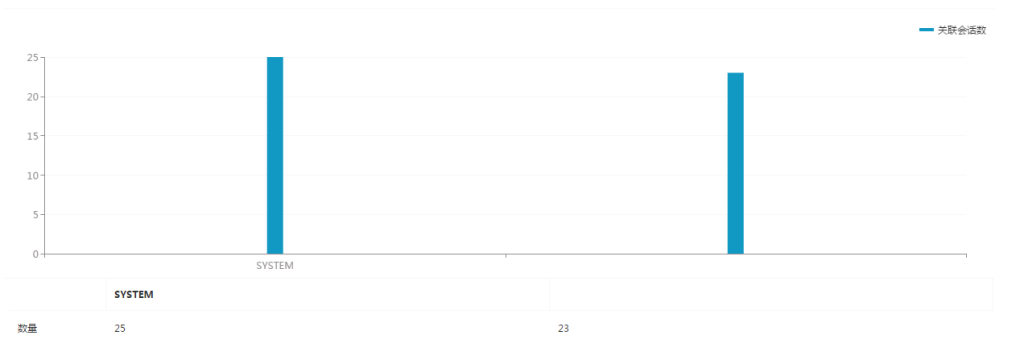
客户端 IP 分布 Top10

客户端IP分布Top10



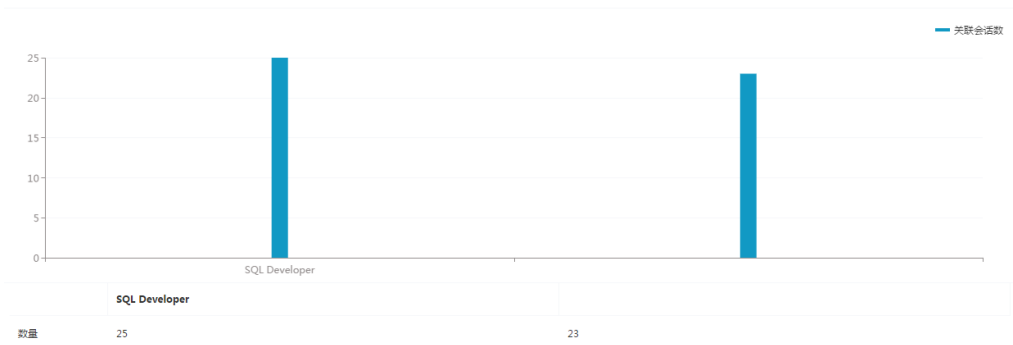
数据库账号分布 Top10

数据库账号分布Top10



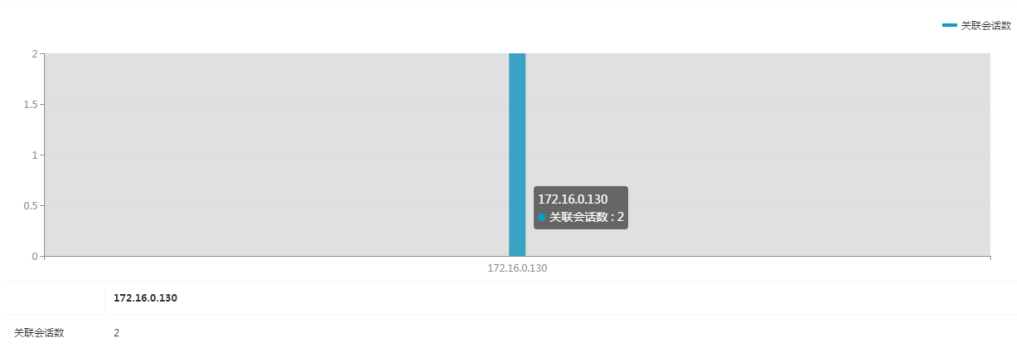
客户端工具分布 Top10

客户端工具分布Top10



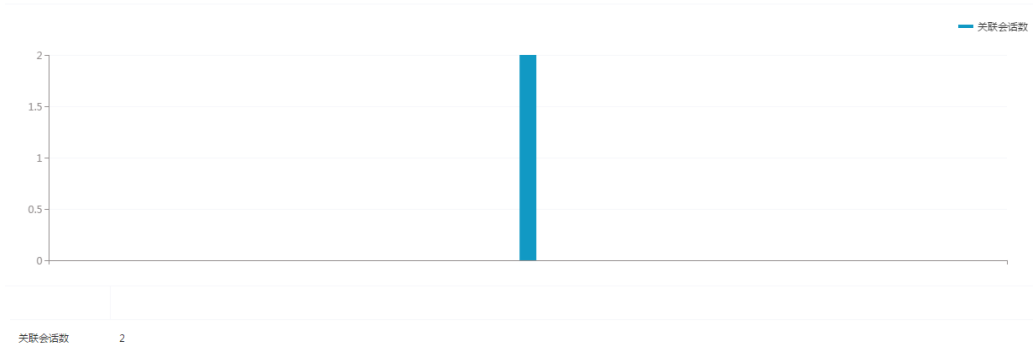
失败客户端 IP 分布 Top10

失败会话客户端IP分布Top10



失败会话数据库账号分布 Top10

失败会话数据库账号分布Top10

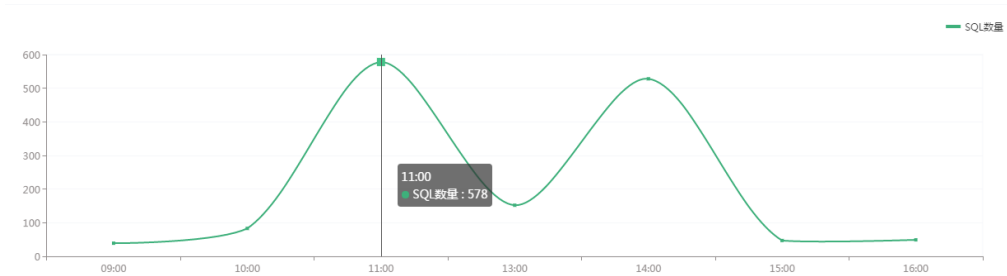


3 语句分析

语句分析包括七部分：

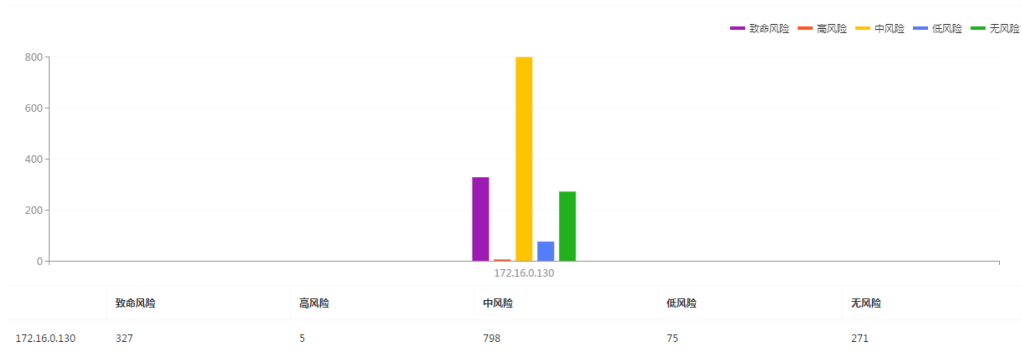
SQL 压力

SQL压力



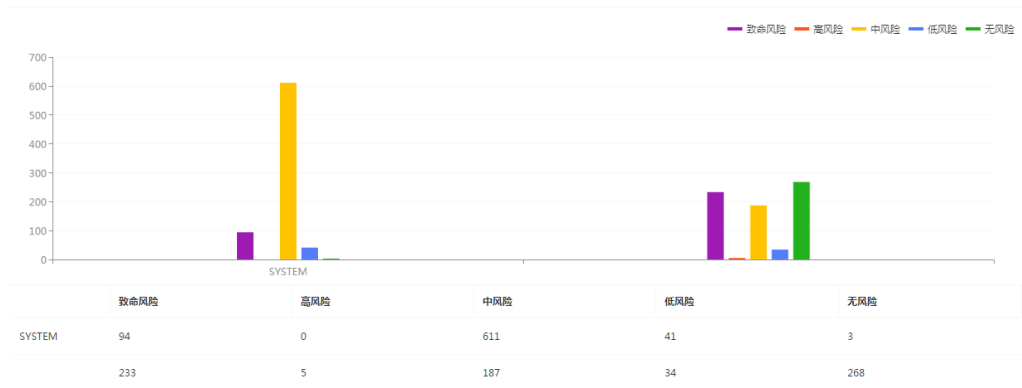
客户端 IP 分布 Top10

客户端IP分布Top10



数据库账号分布 Top10

数据库账号分布Top10



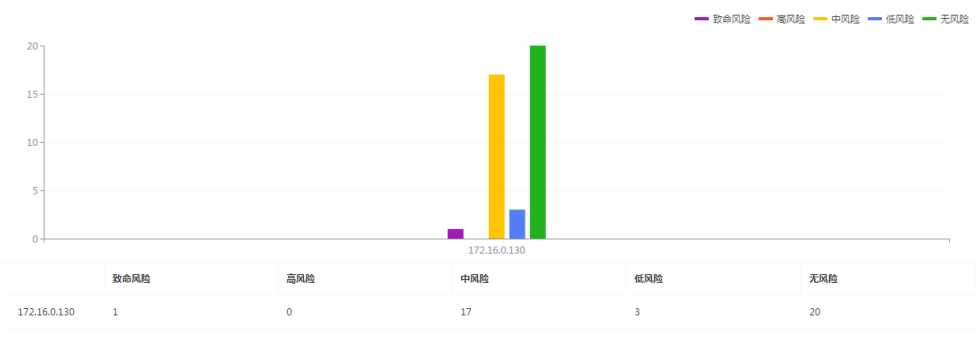
SQL 类别分布 Top10

SQL类别分布Top10



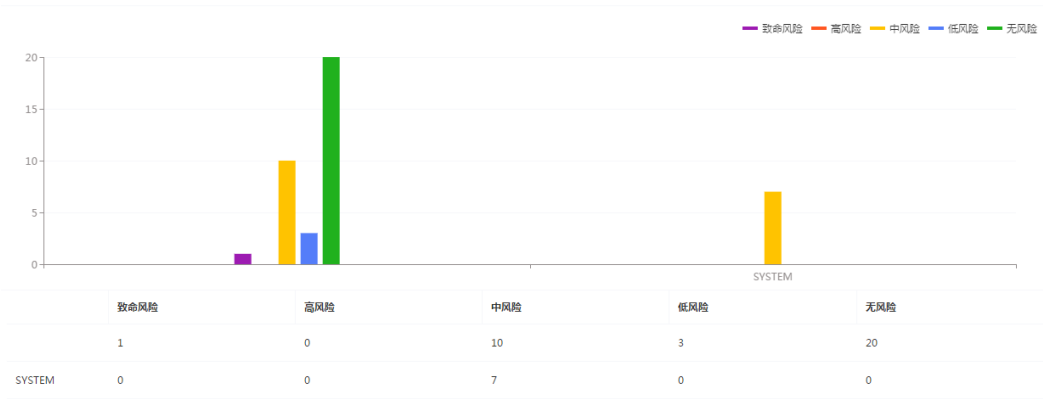
失败语句客户端 IP 分布 Top10

失败语句客户端IP分布Top10



失败语句客户端账户分布 Top10

失败语句数据库账户分布Top10



SQL 语句数量最多 Top10

SQL语句数量最多Top10

SQL语句	捕获-累计
session close	104
select parameter,value from nls_session_parameters union all select 'db_timezone' name, dbtimezone value from dual union all select 'session_timezone' name, sessi...	75
login	67
select 1 from dba_mviews where 1=2	25
select 1 from dba_queues where 1=2	25
alter session set plsql_optimize_level=0	25
select user from dual	25
select sys_context('userenv','sid') from dual	25
select 1 from apex_release where 1=2	25
select 1 from sys.obj\$ where 1=0	25

3.5 策略应用

安全管理员登录系统，进入数据库，展开数据库菜单栏“设置”项，选中“策略应用”，进入策略应用界面。添加系统内置策略。

序号	策略	状态	操作
1	全审计策略复制策略 (共1条规则, 启用1条)	<input checked="" type="checkbox"/>	详情 删除
2	22 (共1条规则, 启用1条)	<input checked="" type="checkbox"/>	详情 删除

3.5.1 策略应用

点击<启用>按钮策略应用到数据库。

点击<详情>按钮, 查看策略下的规则列表基本信息。

序号	策略	状态	操作
1	全审计策略复制策略 (共1条规则, 启用1条)	<input checked="" type="checkbox"/>	详情 删除
2	22 (共1条规则, 启用1条)	<input checked="" type="checkbox"/>	详情 删除

3.5.2 添加策略

点击<添加>按钮, 数据策略名称、描述, 选择策略模板, 是否区分大小写。点击<确定>按钮, 即可添加策略。

注意: 进入数据库后添加的策略为单库策略, 在全局策略中不可见且在全局策略中不可添加和单库策略名称相同的策略。

3.5.3 修改和删除策略

点击<详情>按钮，进入策略下的规则详情即可修改策略。

点击<禁用>按钮，禁止应用策略到当前数据库；

点击<删除>按钮，弹出“确认删除”提示框，点击<确定>按钮删除策略。

状态	名称	等级	动作	优先级	+	操作
<input checked="" type="checkbox"/>	全审计策略	无风险	放行	27330		详情 编辑 删除

3.5.4 规则配置

点击<详情>按钮，进入规则详情列表，规则的添加、修改、删除、应用详见 3.6.4 规则配置。

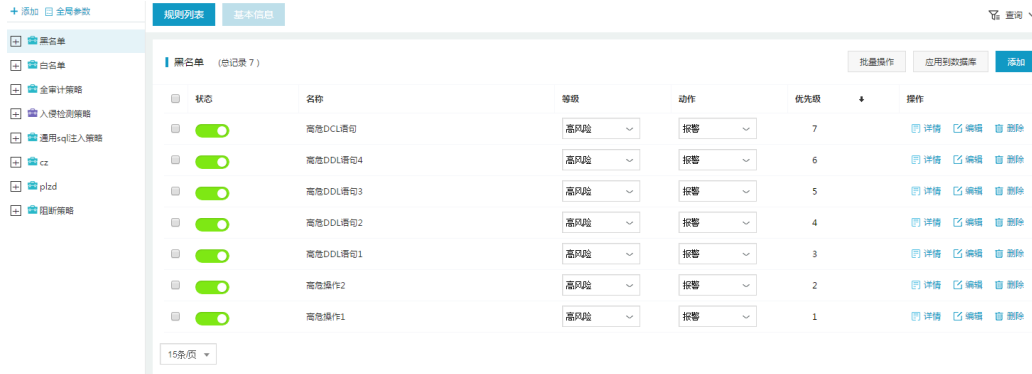
3.6 策略管理

策略中包含多条规则，应用到数据库上，所有对数据库引擎的 sql 操作，都要经过策略的匹配分析。并根据策略中规则的结果进行记录、告警或其它操作。

当一个数据库引擎应用了多个策略时，要依次被每个策略匹配分析。

3.6.1 概述

在导航栏中选择“全局配置>策略管理”进入策略模块，系统提供默认策略包括黑名单、白名单、全审计策略、入侵检测和 sql 注入。用户可以新建和删除策略，每条策略下包含多条规则，用户可以查询、新建、修改、删除规则。



3.6.2 默认策略

进入策略管理模块，默认策略包括五部分：

黑名单：主要针对高危 DCL 操作语句，预置风险等级为高风险、动作为报警

白名单：主要针对可信任操作、信任客户端用户、违规阻断、信任客户端 IP 等进行不记录动作

全审计策略：主要针对可信任操作、信任客户端用户、违规阻断、信任客户端 IP 等进行不记录动作

入侵检测策略：主要针对 Oracle、MySQL、SQL Server 数据库虚拟补丁。即数据库漏洞、SQL 注入漏洞等。可以查看漏洞 CVE 编号、漏洞名称、漏洞类型等详细信息

通用 sql 注入策略：针对 SQL 注入不同类型详细信息

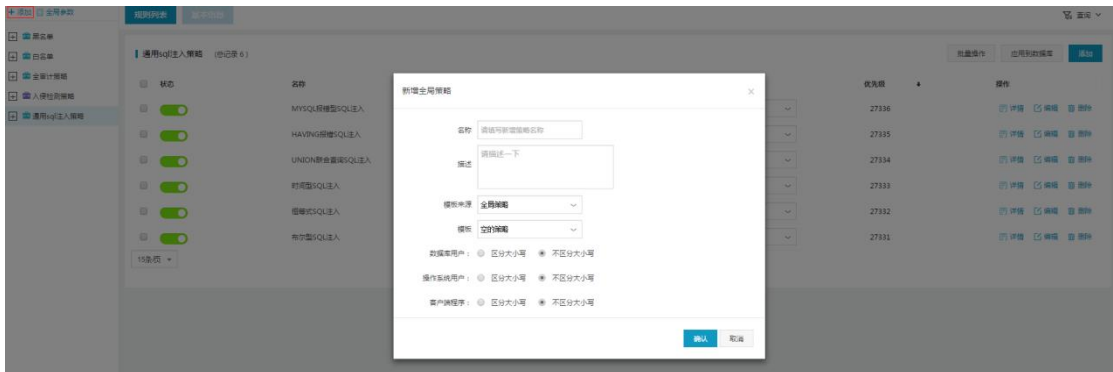
3.6.3 策略配置

策略配置包括策略的添加和删除

3.6.3.1 添加

单击<添加>按钮，弹出“新增策略”提示框，输入名称、描述、选择模板、区分大小写。

单击<确定>按钮，新增策略。



配置项说明：

配置项		说明
名称		设置策略名称
描述		设置策略描述，对名称的补充说明
模板		选择策略应用模板，即：已经新增的策略及策略下的规则复制粘贴至当前策略下。 默认：空的策略
区分大小写	数据库用户	新增策略默认数据库用户不区分大小写
	操作系统用户	操作系统用户默认不区分大小写
	客户端程序	客户端程序默认不区分大小写

3.6.3.2 删除

选择辅助栏删除的策略，单击<删除>按钮，弹出提示框，提醒用户确认删除选择策略，单击提示框中的<确定>按钮，即可删除策略。

状态	名称	等级	动作	优先级	操作
ON	MYSQL数据库SQL注入	高风险	报警	27336	详情 编辑 删除
ON	HAVING语句SQL注入	中风险	报警	27335	详情 编辑 删除
ON	UNION联合查询SQL注入	中风险	报警	27334	详情 编辑 删除
ON	时间型SQL注入	中风险	报警	27333	详情 编辑 删除
ON	嵌套式SQL注入	高风险	报警	27332	详情 编辑 删除
ON	布尔型SQL注入	高风险	报警	27331	详情 编辑 删除

3.6.4 规则配置

3.6.4.1 查询策略

选择策略，配置区显示当前策略下的所有规则，用户可以根据不同的筛选条件查看指定的规则。

1 查询

选择规则状态、风险等级、动作、输入关键字，点击<查询>按钮，查找规则

2 详情

点击配置区规则列表操作下的<详情>按钮，查看规则详情，包括过程名称、所属策略、状态、等级、动作、客户端 IP、客户端工具、操作系统用户、数据库账号。

状态	名称	等级	动作	优先级	操作
ON	deny	致命风险	阻断	27366	详情 编辑 删除

3.6.4.2 添加

点击<添加>按钮，进入规则配置页面，输入规则配置基本信息：名称、描述，选择状态、等级、动作、日志记录级别，点击规则配置条件，展开配置框，输入配置信息，点击<保存>按钮，即可添加规则。



plzd (总记录 1)	批量操作	应用到数据库	添加		
状态	名称	等级	动作	优先级	操作
<input checked="" type="checkbox"/>	deny	致命风险	阻断	27366	详情 编辑 删除

3.6.4.3 修改

点击<编辑>按钮，进入“编辑规则”页面，修改规则基本信息及条件，点击<保存>按钮，即可修改规则。



状态	名称	等级	动作	优先级	操作
<input checked="" type="checkbox"/>	deny	致命风险	阻断	27366	详情 编辑 删除

3.6.4.4 删除

点击<删除>按钮，弹出确认删除提示框，点击<确定>按钮，即可删除规则。



状态	名称	等级	动作	优先级	操作
<input checked="" type="checkbox"/>	deny	致命风险	阻断	27366	详情 编辑 删除

3.6.4.5 规则配置条件

规则信息包括六部分：

基本信息：配置规则名称、描述、状态、等级、动作、日志记录级别

基本信息

名称

描述

状态

等级

动作

日志记录级别

客户端：包含客户端 IP、客户端工具、客户端操作系统用户、客户端操作系统主机名

客户端

客户端IP	客户端工具	客户端操作系统用户	客户端操作系统主机名
-------	-------	-----------	------------

状态

范围

自定义 -

»

«

SQL：包括 SQL 语句、SQL 关键字、SQL 正则、特权操作、操作类型

SQL

SQL语句	SQL关键字	SQL正则	特权操作	操作类型
-------	--------	-------	------	------

状态

SQL语句

操作对象：包括表组、字段、数据库 Schema、目标表

操作对象

表组	字段	数据库与Schema	目标表
----	----	------------	-----

状态

范围

结果：包括响应时间、影响行数、发生次数、认证结果

| 结果

响应时间	影响行数	发生次数	认证结果
------	------	------	------

状态

执行时长 等于 数量(毫秒)

其它：包括时间、查询组、数据库用户、敏感数据访问、webIP、web 用户名

| 其它

时间	查询组	数据库用户	敏感数据访问	webIP	web用户名
----	-----	-------	--------	-------	--------

状态

每日(时) 开始时间 - 结束时间

每周(周) 开始时间 - 结束时间

每月(日) 开始时间 - 结束时间

3.6.5 策略应用

策略应用即将配置的全局策略批量应用到防护的单个数据库或多个数据库。选择策略，点击<应用到数据库>按钮，弹出应用到数据库配置框，如图所示，可以查看数据基本信息包

含数据库名、数据库类型、数据库 IP 三部分。可选择一个或多个数据库，也可以选择数据库名(全选按钮)，选择所有的数据库。点击<确定>按钮，即可应用策略到数据库。



3.7 访问控制

进入数据库，选中设置项访问控制，点击<添加>按钮，输入端口、类型和 IP 地址，点击<保存>添加完成。



点击<编辑>按钮，弹出编辑框，修改端口、类型、IP 地址，点击<保存>按钮即可。

点击<删除>按钮，提示“确认删除”，点击<确认>，删除成功。

3.8 报表管理

安全管理员身份登录系统，选择“全局配置->报表管理”，进入报表结果界面。

名称	范围	生成时间	内容	格式	状态	操作
客户端应用程序性能	全部	2018-02-05 14:45:23	客户端应用程序性能	Pdf	100% 已完成	下载 删除
登录分析	全部	2018-02-05 14:45:21	登录分析	Pdf	100% 已完成	下载 删除
客户端IP	全部	2018-02-05 14:45:18	客户端IP	Pdf	100% 已完成	下载 删除
客户端操作系统主机	全部	2018-02-05 14:45:16	客户端操作系统主机	Pdf	100% 已完成	下载 删除
数据库服务器分析	全部	2018-02-05 14:45:08	数据库服务器分析	Pdf	100% 已完成	下载 删除
数据库安全分析报告	172.18.200.11	2018-02-05 14:45:01	数据库安全分析报告	Pdf	100% 已完成	下载 删除
数据库审计平台状况报告	全部	2018-02-05 14:43:13	数据库审计平台状况报告	Pdf	100% 已完成	下载 删除

3.8.1 报表设置

点击<报表设置>按钮，进入高级报表界面。

名称	描述	数据范围	计划任务	操作
数据库连接池报告	展示系统内连接的所有数据库的连接池。	默认	停用	计划任务 生成报表
数据库安全分析报告	对目标数据库进行的安全报告分析。	默认	停用	计划任务 生成报表
数据库服务器分析	分别为数据库名称及数据库用户连接位置及连接数据库连接池 (连接池IP)。表格名称为数据库名称及连接池名称。	默认	停用	数据范围 计划任务 生成报表
数据库服务器性能	通过计划任务生成数据库服务器性能报告。	默认	停用	数据范围 计划任务 生成报表
数据库分析	通过不同的数据库用户不同的数据库进行分析。	默认	停用	数据范围 计划任务 生成报表
客户端应用程序	通过客户端应用程序的数据库用户、客户端操作系统主机、客户端IP、登录策略进行统计分析。	默认	停用	数据范围 计划任务 生成报表
客户端操作系统主机	统计计划任务生成数据库服务器性能报告。	默认	停用	数据范围 计划任务 生成报表
客户端IP	统计计划任务生成数据库服务器性能报告。	默认	停用	数据范围 计划任务 生成报表
登录分析	统计登录数据库的用户、操作系统主机、源应用程序、用户、登录策略、目标IP、数据库、Schema、登录数据。	默认	停用	数据范围 计划任务 生成报表
客户端应用程序性能	分析通过应用程序性能、对于操作时通过计划任务、进行统计；用户操作平均时间、过长的时间、应用程序的响应时间、平均值。	默认	停用	数据范围 计划任务 生成报表
操作策略分析	统计计划任务生成报告、生成报告生成策略、生成报告生成策略、基于策略生成报告生成策略。	默认	停用	数据范围 计划任务 生成报表
策略删除与更新	统计不同用户连接数据库连接池 (drop/truncate)。	默认	停用	数据范围 计划任务 生成报表
策略删除与更新	统计用户连接数据库连接池 (drop/truncate)。	默认	停用	数据范围 计划任务 生成报表
SQL审计	通过SQL审计分析平台生成报告。	默认	停用	数据范围 计划任务 生成报表

高级报表包含两部分：

系统生成报表

按计划生成报表

3.8.2 下载和删除报告

点击<下载>按钮，即可下载报表。

点击<删除>按钮，弹出“确认删除”提示，点击<确认>即可删除报表。

名称	范围	生成时间	内容	格式	状态	操作
1725风险分析180102170516	1725	2018-01-02 17:05:16	风险分析	Pdf	100% 已完成	⌵ 下载 ⌵ 删除
1725风险分析180102170516	1725	2018-01-02 17:05:16	风险分析	Pdf	100% 已完成	⌵ 下载 ⌵ 删除
1725风险分析180102170516	1725	2018-01-02 17:05:16	风险分析	Pdf	100% 已完成	⌵ 下载 ⌵ 删除
1725风险分析,会话分析,语句分析180102105728	1725	2018-01-02 10:57:28	风险分析,会话分析,语句分析	Word	100% 已完成	⌵ 下载 ⌵ 删除

3.9 风险扫描

进入数据库，选中扫描项风险扫描，输入数据库(实例)、用户名、密码，点击<开启>按钮，即可开启风险扫描。



开启风险扫描

🗄️ orcl

👤 用户名

🔒 密码

是否有管理员权限 是 否

开启

风险扫描支持三部分：

风险扫描

弱口令检测

风险扫描结果预览已经报表下载

- 风险扫描
- 弱口令检测
- 历史报表

3.10 状态监控

进入数据库，选中状态监控，输入数据库(实例)、用户名、密码，点击<开启>按钮，即可开启状态监控。查看数据库状态。



开启状态监控

是否有管理员权限 是 否

3.11 监控扫描

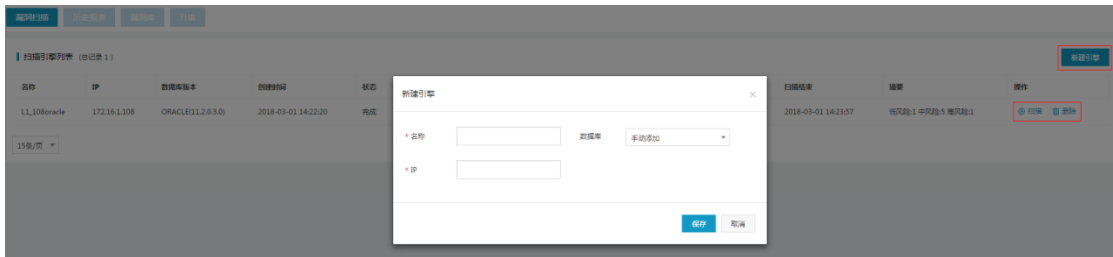
安全管理员身份登录系统，选中“监控扫描”，会出现下拉框漏洞扫描、设备扫描、数据库敏感扫描三部分。

3.11.1 漏洞扫描



漏洞扫描包括：查看扫描的漏洞，创建、扫描、删除漏洞扫描引擎。

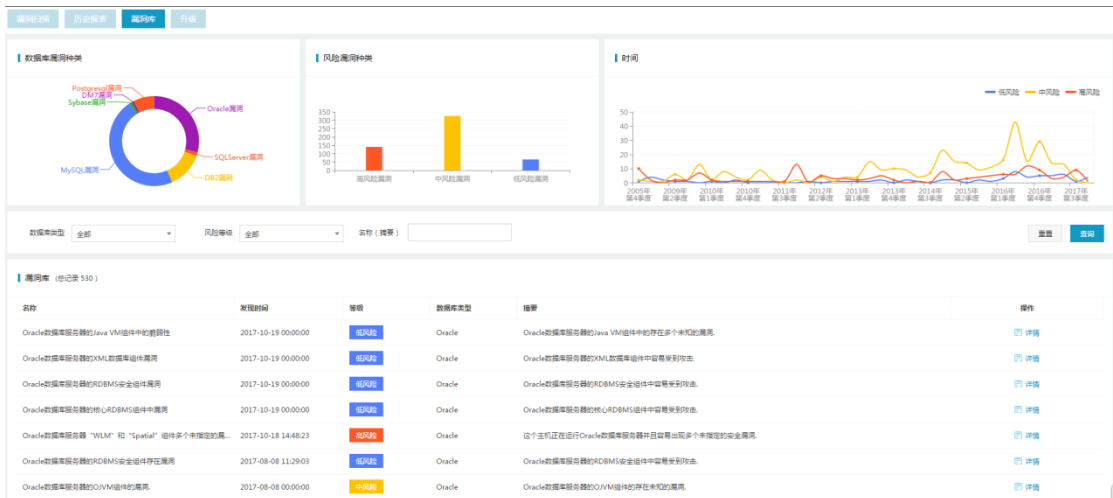
选择导航栏漏洞扫描项，点击<新建引擎>，弹出新建引擎弹出框，输入漏洞扫描引擎名称、扫描的数据库和地址，点击<保存>按钮即可。



历史报表：查看、导出、删除报表

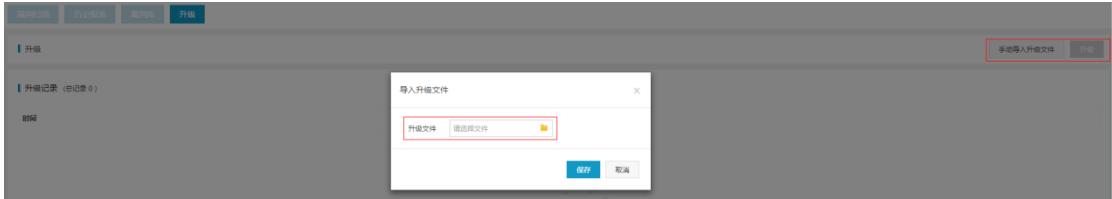


漏洞库：系统默认的数据库漏洞



升级：漏洞库同步更新，防范漏洞库危险

选择导航栏升级项，选择<手动导入升级文件>，上传漏洞包，点击<保存>按钮，然后选中<升级>按钮，进行升级即可。



3.11.2 设备扫描



设备扫描包括：查看扫描设备的结果，创建、扫描、删除设备扫描引擎。

统计结果包括：查看扫描结果，执行加入数据库列表。

选择导航栏设备扫描项，点击<新建引擎>按钮，弹出新建引擎弹出框，输入设备扫描引擎名称、服务类型、网段设置，点击<保存>按钮即可。



点击操作列<扫描>即可。

3.11.3 数据库敏感扫描



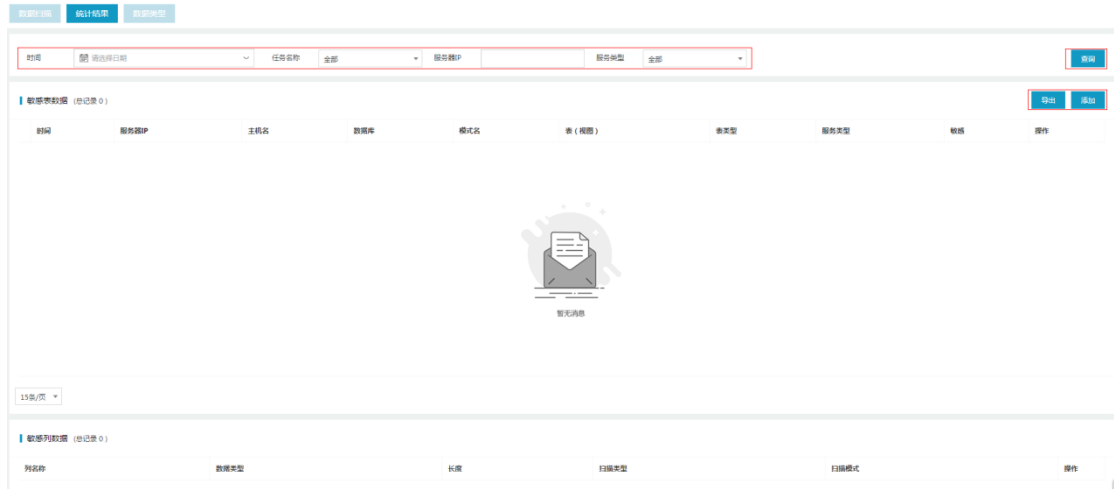
数据扫描包括：查看扫描的数据库敏感数据，创建、扫描、设置、删除数据库敏感扫描引擎。

选择导航栏数据扫描项，点击<新建引擎>按钮，弹出新建引擎弹出框

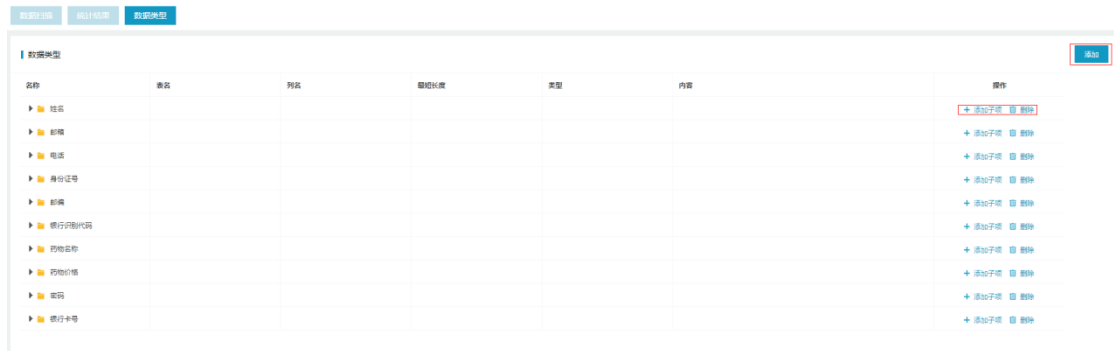
输入敏感数据扫描引擎名称、所扫描的数据库、数据库用户名、密码和数据库的 IP 地址，点击<下一步>，选择扫描操作、数据库类型、扫描设置和扫描范围，然后点击<保存>按钮即可。



统计结果：根据时间、任务名称、服务器 IP、服务器类型条件，查询敏感数据表、列和类型，导出生成报表，添加数据库敏感表。



数据类型：添加、删除敏感数据。



3.12 安全设置

安全管理员身份登录系统，选择“全局配置->安全设置”选项，进入安全设置界面。

安全设置包括：登录安全参数、登录会话超时、密码长度参数、密码过期参数、下载文件密码五部分内容。

| 安全设置

登录安全参数	<input type="text" value="60"/>	秒之内，用户尝试登录的失败次数超过	<input type="text" value="3"/>	锁定该用户	<input type="text" value="1"/>	分钟
登录会话超时	<input type="text" value="30"/>	分钟不操作，自动退出				
密码长度参数	密码最短长度	<input type="text" value="8"/>	密码最长长度	<input type="text" value="30"/>		
密码过期参数	<input type="checkbox"/>					
密码过期时间	<input type="text" value="7"/>	时间只能为正整数，且不超过7天				
下载文件密码	<input type="text"/>					
确认密码	<input type="text"/>					

3.12.1 设置安全参数

设置用户安全各项参数，点击<保存>按钮即可。

| 安全设置

保存

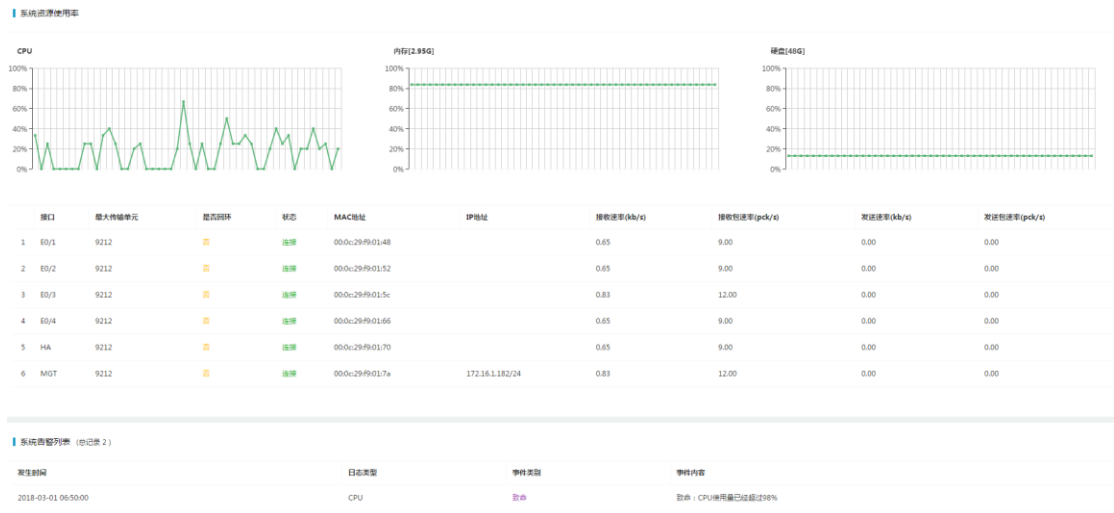
四、 审计管理员

审计管理员区别与系统管理员和安全管理员，是系统级管理人员，针对本系统进行管理操作。

该用户用户名：Auditor、缺省密码：admin12345。

审计管理员包括监控（主页）、操作日志、用户管理三部分。

4.1 监控



4.2 操作日志

审计管理员只有一个权限，查询系统管理员和安全管理员的操作日志。

4.3 用户管理

针对系统创建的默认管理员授权为审计管理员。

用户管理

用户名	角色名	状态	操作
admin12345sys	系统操作员	正常	
admin12345sec	安全操作员	正常	
admin12345aud	审计操作员	正常	取消授权

五、 用户管理

系统管理员身份登录系统，选择“用户管理”项，进入用户管理界面。

默认显示系统默认用户。

用户管理			新增用户
用户名	角色名	状态	操作
test_star	默认管理员	正常	授权 删除 修改密码

用户管理包括用户的添加、修改、删除和授权。

添加：系统管理员可以添加用户

修改：系统管理员可以修改所有用户的信息。安全管理员仅能修改安全管理员密码，

审计管理员仅能修改审计管理员密码

删除：系统管理员可以删除用户

授权：系统、安全、审计管理员仅能授自身权限内的操作

5.1 新建用户

点击<添加>按钮，弹出“添加用户”提示框，输入用户名称、输入密码、确认密码，点击<确定>按钮。

添加用户
×

用户名

输入密码

确认密码

确定
取消

5.2 角色管理

安全管理员下，选中“用户管理->角色管理”项，默认角色名安全操作员、系统操作员、审计操作员。用户可以自定义创建、修改和删除角色。



角色名	授权模块	操作
1 安全操作员	设备扫描,敏感数据扫描,风险扫描,数据库审计,数据库防火墙,状态监控,漏洞扫描,	-
2 系统操作员	数据库透明加密	-
3 审计操作员		-
4 role1	设备扫描	编辑 删除

5.3 修改用户密码

点击<修改密码>按钮，弹出“修改密码”提示框，输入原始密码、新密码、确认密码，点击<确定>按钮。

修改密码 ×

用户名

原始密码

新密码

确认密码

(密码长度为8-30位字母和数字组成)

注意：不同用户登录系统，可以通过右上角“修改密码”项，可修改当前用户密码

5.4 删除用户


点击<删除>按钮，弹出“确认删除”提示，点击<确定>按钮，即可删除用户。



注意：系统默认用户：SysAdmin、SecAdmin、Auditor 只能修改密码，不能删除

5.5 授权用户

安全管理员登录系统，选择“全局配置->用户管理”选项，即可进入用户管理界面。



用户名	角色名	状态	操作
stadmin	默认管理员	正常	授权

安全管理员只能授权安全操作员和自定义角色权限。

点击<授权>按钮，弹出“授权”提示框，选择授权用户权限，点击<确认>按钮，授权成功。

注意：安全用户可以授权角色安全操作员和自定义角色

六、 操作日志

操作日志区别于数据库日志，是针对本系统执行审计管理操作，包括两部分：

安全管理员：针对本系统审计管理员执行的管理操作

审计管理员：针对本系统系统管理员和安全管理员执行的管理操作

6.1 安全管理员操作日志

安全管理员登录系统，选择“系统信息->操作日志”选项，进入安全管理员操作日志界面。

日志内容包括审计管理员用户名、本系统 IP 地址、操作时间、功能点、动作和详细信息。

操作日志管理 查询 2018-01-02 00:00:00 - 2018-01-02 23:59:59

日志 以当前条件导出 以当前条件导出

序号	用户名	IP	操作时间	功能点	动作	详情信息
1	Auditor	172.16.0.130	2018-01-02 17:18:13	登录系统	登出系统	用户登出系统
2	Auditor	172.16.0.130	2018-01-02 16:59:47	登录系统	登入系统	用户Auditor登入系统
3	Auditor	172.16.0.130	2018-01-02 13:53:39	登录系统	登出系统	用户登出系统
4	Auditor	172.16.0.130	2018-01-02 13:53:22	操作日志	查询操作日志	查询操作日志
5	Auditor	172.16.0.130	2018-01-02 13:53:12	操作日志	查询操作日志	查询操作日志
6	Auditor	172.16.0.130	2018-01-02 13:53:10	登录系统	登入系统	用户Auditor登入系统
7	admin12345aud	172.16.0.130	2018-01-02 13:52:03	登录系统	登出系统	用户登出系统
8	admin12345aud	172.16.0.130	2018-01-02 13:52:56	操作日志	查询操作日志	查询操作日志
9	admin12345aud	172.16.0.130	2018-01-02 13:52:53	登录系统	登入系统	用户admin12345aud登入系统
10	Auditor	172.16.0.130	2018-01-02 13:52:24	登录系统	登出系统	用户登出系统

安全管理员可以查询审计管理员的操作日志，查询条件包括操作时间、IP 地址、用户名和功能点。

操作日志管理 查询 2018-03-01 16:27:20 - 2018-03-01 17:37:20

IP: 用户名: 功能点:

1	Auditor	172.16.1.180	2018-03-01 17:24:00	操作日志	查询操作日志	
2	Auditor	172.16.1.180	2018-03-01 17:23:51	登录系统	登入系统	
3	Auditor	172.16.1.180	2018-03-01 17:17:13	登录系统	登出系统	
4	Auditor	172.16.1.180	2018-03-01 17:14:14	登录系统	登入系统	
5	Auditor	172.16.1.180	2018-03-01 17:12:12	登录系统	登出系统	用户登出系统
6	Auditor	172.16.1.180	2018-03-01 17:08:06	登录系统	登入系统	用户Auditor登入系统

15条页

今日 2018年 3月 2018年 4月

本月

日	一	二	三	四	五	六
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

选择日期

点击<以当前条件导出>按钮，选择导出日志行数、报表格式，点击<确定>按钮即可导出操作日志。

操作日志管理 查询 2018-01-02 00:00:00 - 2018-01-02 23:59:59

日志 以当前条件导出 以当前条件导出

1	Auditor	172.16.0.130	2018-0			
2	Auditor	172.16.0.130	2018-0			
3	Auditor	172.16.0.130	2018-0			
4	Auditor	172.16.0.130	2018-0			
5	Auditor	172.16.0.130	2018-01-02 13:53:12	操作日志	查询操作日志	查询操作日志
6	Auditor	172.16.0.130	2018-01-02 13:53:10	登录系统	登入系统	用户Auditor登入系统

报表导出

行数 全部 (最多两百万行) 指定 _____ 行数

导出格式 Pdf

6.2 审计管理员操作日志

审计管理员的身份登录系统，即可查看操作日志。

审计管理员只有一个权限，查询系统管理员和安全管理员的操作日志。

审计管理员可以查询操作日志，查询条件包括操作时间、IP 地址、用户名和功能点。

操作日志管理 🔍 查询 2018-01-02 17:36:44 ~ 2018-01-02 18:36:44

日志 以当前条件导出

序号	用户名	IP	操作时间	功能点	动作	详细信息
1	SecAdmin	172.16.0.85	2018-01-02 18:16:31	审计日志检查	创建任务	执行审计日志检查任务
2	SecAdmin	172.16.0.130	2018-01-02 18:16:30	审计日志检查	创建任务	执行审计日志检查任务
3	SecAdmin	172.16.0.180	2018-01-02 18:16:22	登录系统	退出系统	用户退出系统
4	SecAdmin	172.16.0.130	2018-01-02 18:16:21	审计日志检查	创建任务	执行审计日志检查任务
5	SecAdmin	172.16.0.85	2018-01-02 18:16:21	审计日志检查	创建任务	执行审计日志检查任务

点击<以当前条件导出>按钮，选择导出日志行数、报表格式，点击<确定>按钮即可导出操作日志。



七、附录 1：Agent 配置手册

1. 使用说明

当工作环境中交换机不支持端口镜像，或虚拟化的部署时，又要达到数据库审计的功能，就需要使用 Agent 部署数据库审计。

2. 工作原理

数据库 Agent 审计是基于 C/S 架构设计，Agent 插件作为 agent_client 端，安装在数据库服务器上，审计系统作为 agent_server 端，服务端口 TCP443 端口和 UDP700* (700* 基于在审计系统配置的端口为准)。

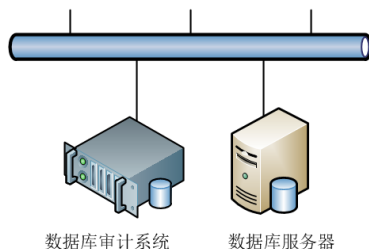
Agent 与审计系统通信分两部分：

一部分是配置参数协商、CPU 内存信息上报：通过服务端口 TCP443，agent_client 端周期性收集数据库 CPU、内存、接口信息，发送给审计系统 agent_server 端；审计系统 agent_server 返回审计系统侦听 UDP 端口、抓取流量的接口及过滤 IP 信息给 agent_client 端。Agent_client 通过审计系统 server 返回的接口及过滤 IP 生成抓取流量服务。

另一部分是数据库流量数据上传到审计系统：agent_client 抓取到数据库操作流量后，生成临时文件，并通过向审计系统 agent_server，通过服务 UDP 端口 700*发送此数据库操作数据，审计系统接收到此数据后，交由审计系统处理，分析并生成审计日志。

3. 组网说明

数据库审计系统与数据库服务器路由可达，比如数据库审计系统 IP：172.16.1.82，数据库服务器 IP 为：172.16.1.253。



4. Agent 插件安装及配置说明（windows 版）

1) 登录数据库审计系统，配置审计接口及 IP 信息等配置。

Sysadmin 登录系统→系统配置→硬件和诊断→接口功能→保存：

配置接口审计功能：



2) . 登录数据库审计及防护系统，配置数据库审计引擎等配置（以配置向导为例）。

Secadmin 登录系统→主页（数据库概览）→添加→配置向导→基本信息→模式选择（审计：S1GE1）→策略配置（全审计策略）→保存并启用：



×

基本信息 模式选择 策略配置

*名称	<input type="text" value="172.16.1.253"/>	类型	<input type="text" value="Oracle"/>
版本	<input type="text" value="11.2.0.1"/>	*数据库(实例)	<input type="text" value="ORCL"/>
*端口	<input type="text" value="1521"/>	*IP	<input type="text" value="172.16.1.253"/>
备注	<input type="text"/>		

下一步

×

基本信息 模式选择 策略配置

模式	<input type="text" value="审计"/>
接口	<input type="text" value="E0/2"/>

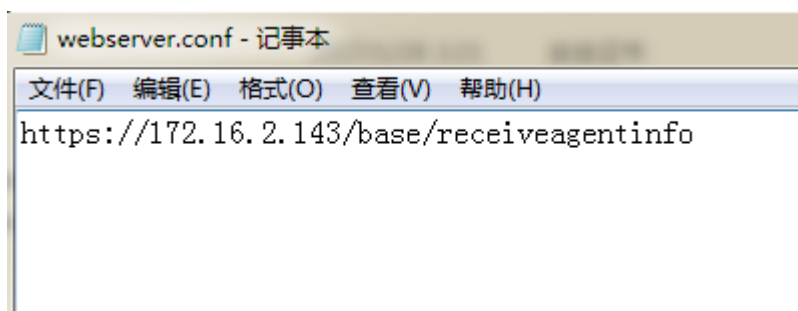
上一步 下一步



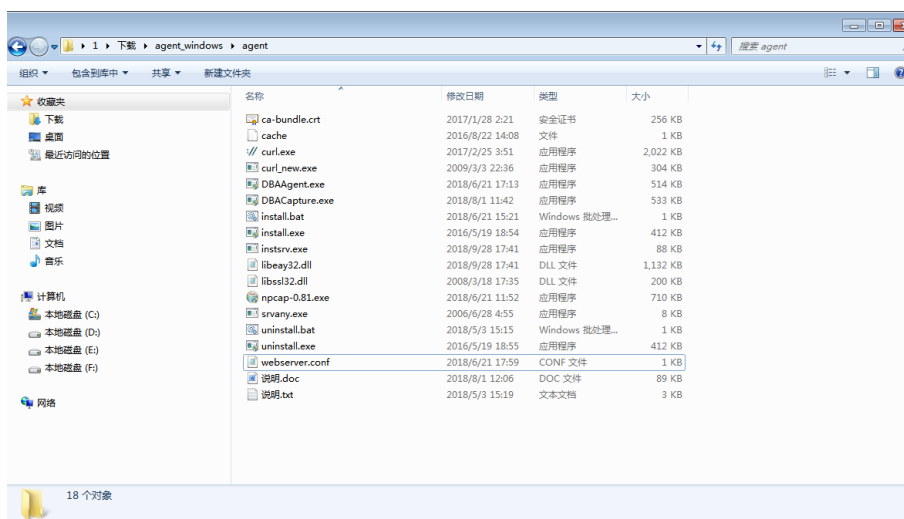
3). 进入此数据库引擎界面, 点击‘设置’进入功能设置界面, 下载 window 相应的 Agent 插件:



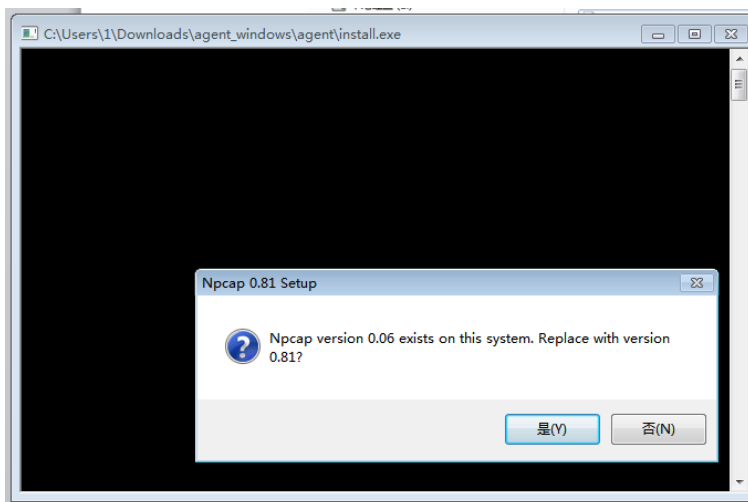
4) .把 Agent 程序拷贝到数据库服务器上，存放分区根目录下并解压（目录不要太深，名称不可随意更改），进入 Agent 目录中，修改 webserver.conf 中的配置：其中的 IP 为数据库审计系统的 IP,此 IP 可与数据库服务器互联，URL 格式：
https://172.16.1.82/base/receiveagentinfo（此 URL 只适用新 UI）



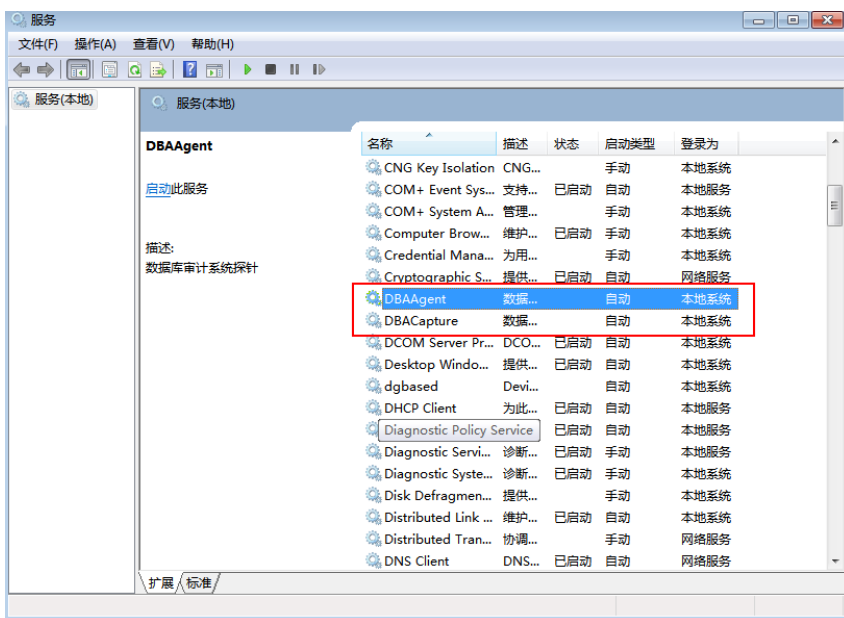
5) .根据 Agent 中‘说明’文档，安装 Agent 插件到数据库服务器上：
执行 install.exe 安装 Agent 程序到数据库服务器中。



弹出是否安装 Npcap 程序，若首次安装 Agent 插件，此 Npcap 程序需安装。



6) . 安装 Npcap 只需默认安装即可，安装完成后，Agent 也会默认安装完成，详细可查阅安装包中的说明；如果已安装过 Npcap 程序，只需选择否，Agent 程序就会默认安装完成。查看 Agent 程序是否正常启动，可查看服务，win 系统下‘运行’中输入 services.msc，找到服务名为 DBAAgent 和 DBACapture 两个服务：



7) . Agent 安装完成后，登录数据库审计系统，开启 Agent 功能：

Secadmin 登录数据库审计及防护系统，在主页中数据库概览中进入单库界面，点击‘设置’进入功能设置界面，开启 Agent，修改接收端口（Agent 服务端口，如 7000），设置 CPU 阈值，其他配置默认，配置完成后，点击保存。



Agent

CPU 0%

内存 0%

接收端口 (7000~8000)

CPU阈值

审计端口

审计接口

Agent插件下载 [windows\(Vista及更高\)插件下载](#) [windows\(Server2003/XP\)插件下载](#) [linux插件下载](#)

审计IP	掩码	操作
127.0.0.1	255.255.255.255	删除
172.16.1.253	255.255.255.255	删除

注：审计接口为 Agent 插件从数据库服务器中取出并发送到审计系统上，故需先安装 Agent 插件，再开启审计系统中的 Agent。

至此，可以看到当前服务器的 CPU 和内存使用率，Agent 审计已部署完成。

8) . 卸载 Agent 插件，执行 `uninstall.exe` 即可卸载成功。

5. 安装 Agent 插件到数据库服务器（linux 版）

1) . 安装 Agent 插件到数据库服务器，把 Agent 安装包 `agent_linux.tar.gz` 拷贝到数据库服务器上，通过命令：`tar -xvf agent_linux.tar.gz` 解压，`cd` 进入 Agent 目录下：执行 `./install` 命令，输入 `https://172.16.1.82:443` 参数按回车，Agent 安装完成。

注：172.16.1.82 为审计系统的 IP，此 IP 与数据库服务器路由可达。

```
[root@localhost ~]# cd /home/
[root@localhost home]# ls
agent_linux.tar.gz king
[root@localhost home]# tar -xvf agent_linux.tar.gz
agent/
agent/db_agent_pcap.c
agent/db_agent_pcap_32
agent/db_agent_polling.c
agent/db_agent_polling_32
agent/install.sh
agent/libpcap.so.1.2.1_32
agent/libpcap.so.1.2.1_64
agent/libpcap.so.1_32
agent/libpcap.so.1_64
agent/pcap.h
agent/ReadMe.txt
agent/uninstall.sh
agent/编译说明.txt
agent/db_agent_pcap_64
agent/libpthread.a
agent/db_agent_polling_64
[root@localhost home]# cd agent
[root@localhost agent]# ls
db_agent_pcap_32 db_agent_pcap_64 db_agent_pcap.c db_agent_polling_32 db_agent_polling_64 db_
[root@localhost agent]# ./install.sh
Input the agent web ctrlcenter info, format as http://ip:port or https://ip:port
https://192.168.30.22
db_agent_polling: 没有进程被杀死
[root@localhost agent]#
[root@localhost agent]#
[root@localhost agent]#
```

2). Agent 安装完成后，登录数据库审计系统，开启 Agent 功能：

Secadmin 登录数据库审计及防护系统，在主页中数据库概览中进入单库界面，点击‘设置’进入功能设置界面，开启 Agent，修改接收端口（Agent 服务端口，如 7000），设置 CPU 阈值，其他配置默认，配置完成后，点击保存。



注：审计接口为 Agent 插件从数据库服务器中取出并发送到审计系统上，故需先安装 Agent 插件，再开启审计系统中的 Agent。

3). 卸载 Agent 插件，Agent 目录下执行 ./uninstall。

6. 应对措施

1). 当出现 Agent 工作异常，包括审计系统获取 CPU 内存信息出现异常、审计流量传输出现异常，需要执行卸载 Agent 插件后，重新执行安装 Agent 插件，从而恢复 Agent 正常工作。

2). 安装多个 Agent 时，需要手动修改服务端口 700*，每个 Agent 对应一个服务端口。

3). Agent 审计必须确保审计系统与数据库服务器之间路由可达。

4). 出现 Agent 不工作时，如果因 CPU 阈值设置过小，需要适当调整 CPU 阈值，等待数秒后，Agent 会自动工作。

5). 选择的审计接口必须是 UP 状态，并且开启了数据库审计功能。

6). 审计接口与路由到达数据库服务器的接口可以不是同一个接口。

7).安装新版本的 Agent 时，需要查看上一版本的 Agent 服务是否存在，若存在需要卸载，安装新版本的 Agent 插件。

八、附录 2：Oracle 集群配置说明

1) .添加 oracel 集群的数据库防护引擎



The screenshot shows a configuration window for adding an Oracle database engine. The window has a close button (X) in the top right corner. The configuration is organized into four tabs: '基本信息' (Basic Information), '模式选择' (Mode Selection), '添加子库' (Add Sub-database), and '策略配置' (Strategy Configuration). The '基本信息' tab is currently selected and highlighted in blue. The configuration fields are as follows:

*名称	测试库	数据库类型	Oracle
*类型	集群	版本	11.1.0.2
*IP	集群	*端口	1521
*服务名	racdb	库优先级	
备注			

The '类型' (Type) dropdown menu is open, showing '集群' (Cluster) as the selected option, which is highlighted in blue. Other options visible are '单库' (Single Database). A '下一步' (Next Step) button is located at the bottom right of the configuration area.

编辑中显示的 oracle 集群配置。

编辑数据库 ×

添加防护数据库引擎，选择集群方式的配置

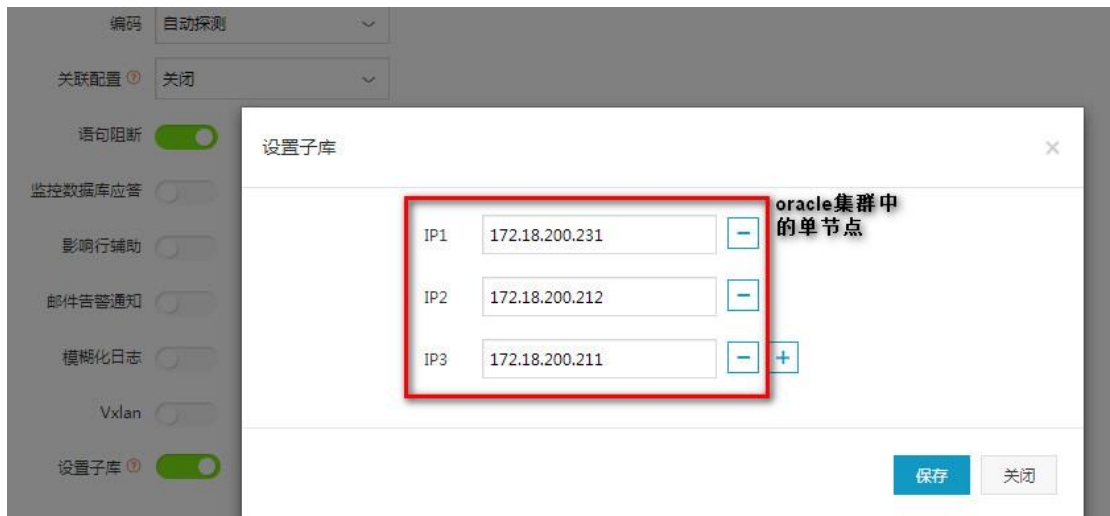
*名称	scanIP-IPv6-rac	类型	集群
模式	防火墙	接口	br1
数据库类型	Oracle	版本	11.1.0.1
*IP	172.18.200.231 集群 scanip	*端口	1521
*数据库(实例)	racdb 集群服务名	库优先级	0
备注			

保存 取消

2) .添加 oracle 集群单节点 IP 的配置。



在“设置”中可以编辑 oracle 集群节点。



在该数据库引擎中进行检索和统计的报表均是整合后的日志结果。

九、附录 3：多接口镜像配置

该场景用于交换机主备环境镜像，聚合接口镜像的数据库旁路审计模式。

1) .多审计业务接口配置 bond。



2) .数据库审计旁路模式 bond 接口调用。

×

基本信息 **模式选择** 策略配置

模式

接口
