

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

-,	系	统概述…		4
	1.1	产品简:	介	4
	1.2	系统登录	录	5
	1.3	退出系统	充	5
	1.4	修改密码	冯	6
	1.5	页面布	冒	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	置1	0
		2.2.1	LICENSE 授权1	0
		2.2.2	服务与时间配置1	0
		2.2.3	系统升级1	4
		2.2.4	告警通知配置1	4
		2.2.5	可靠性设置1	9
		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2	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	哩	. 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	制	. 75
	3.8	报表管	哩	. 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	借	. 77
	3.10) 状态监	空	. 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	2 安全设	置	. 82
		3.12.1	设置安全参数	. 83
m	<u>њ</u>			00
飞 、	申.	「官埋页		. 83
	4.1	监控		. 84
	4.2	操作日期	志	. 84



	4.3	用户管理	84
五、	用」	户管理	
	5.1	新建用户	85
	5.2	角色管理	
	5.3	修改用户密码	
	5.4	删除用户	
	5.5	授权用户	
六、	操	作日志	88
	6.1	安全管理员操作日志	
	6.2	审计管理员操作日志	
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	



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、

4



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。

	账号登录 最信赖的、最专业的数据安全专家
东软NetEye数据库审计系统	SecAdmin ~
最信赖的、最专业的数据女主专家	登录

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。

오 SysAdmin ~	← 退出
🎗 修改密码	

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。





Neusoft क	欲NetEye数据库审计系统 ロ主页 © 系統配置 & 用户管理	오 SysAdmin ~	← 退出
 系統配置 LICENSE提及 服务与时间配置 系统升级 ឥ等透灯配置 	LICENSE接权 机器的SN码 010100201162277269 激活文件	援权信息	
可靠性设置 关联设置 SNMP配置 翻译字典 ジー硬件和诊断) 置数描与暂份)	■銅原袋状态 系统状态: 已勤活 系统版本: 东政NetEye設議業审计系统V2.0 (build:5.5.1.16532) 近紀到期: 无残制 进纪提块: 服务扫描,数据库防火墙 (测试版),数感数跟扫描,风险扫描,数据库审计,状态磁控,演测扫描		

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。

SecAdmin
SysAdmin
Auditor

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(pck/s)	发送速率(kb/s)	发送包速率(pck/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	香	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	香	连接	00:0c:29:f9:01:66		0.41	6.00	0.00	0.00
5	НА	9212	쥼	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	СРИ	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

Neusoft	东软	letEye数据库审计系统	☆ 主页	③系統配置	& 用户管理		오 SysAdmin 🗸	← 退出
2、系統配置	~	LICENSE授权						
LICENSE接收 服务与时间配置 系统升级 告答通知配置		机器的SN码 01 激活文件	010100201162277269				授权信息 授权激活	
可靠性设置 关联设置		当前系统状态						
SNMP配置 翻译字典 양·硬件和诊断 副 数据与备份	>	系统状态: 巴謝 系统版本: 东敏 授权服期: 无罪 授权模块: 服务	活 NetEye数据库审计系统V2.0 制 扫描,数据库防火墙(测试器	(build:5.5.1.16532 反),敏感数据扫描,	2) ,风险扫描,数据库审计,状态监控	,漏洞扫描		

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 更改37间		
时间服务器1		自动同步 同步 保存
Ib	調□ 123	
┃ 时间服务器2		□ 自动同步 同步 保存
Ip)靖□ 123	
服务配置		保存并生效
DNS配置 WEB配置 SSH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

												_
15:18:46	更改时间											×
2018-01-02												
更改时间		2018-01-02				15:1	16:26					- 1
			~	<	20	18年	1月	>	\gg		Tim ¹	
			B	_	=	Ξ	四	五	六	佣疋	収済	3
			31	1	2	3	4	5	6			
		ÿ	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			
						清空	现初	Æ	确定			

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

时间服务器1		自动同步 同步 保存
IP	30日 123	
时间服务器2		■ 自动同步 同步 保存
Ip	靖口 123	

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
-------	-------	-------

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。

DNS服务器1	
DNS服务器2	
DNS服务器3	

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	443	

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	22					

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	0
通知等级	低风险以上
IP	
端口	514
数据库	全部 🔻
	保存测试

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	\bigcirc	
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 🔻	
	保存 测试	

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	低风险以上	
IP地址		
端口	21	(1-65535)
上传目录		
单次包含	10	条(1 - 500)
用户名		
密码		
数据库	全部 🔻	
	保存测试	

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。 东软 NDBA 数据库安全



SNMP通知	0		
发送类型	◎ 发送统计信息	◉ 发送单条	
通知等级	低风险以上	Ŧ	
服务器IP地址			
端口	162		(1-65535)
MIB			样例: 1.1.1.1.1.1.1.1.1.1
OID			
数据库	全部	*	
	保存测	试	

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。 东软 NDBA 数据库安全



短信通知	
通知等级	低风险以上
服务器IP地址	
端口	18259 (1-65535)
单次包含	10 条 (1-500)
收件人号码	
数据库	全部
	保存 测试

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:	 ● 単机状态 ◎ 双机状态
HA接囗:	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	\bigcirc	上限值	95	%
内存超限	\bigcirc	上限值	95	%
系统异常	\bigcirc			
服务异常	\bigcirc			
bypass组	\bigcirc	MGT,HA		
	\bigcirc	E0/1,E0/2		

东软 NDBA 数据库安全



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			
Ię	+	姓名	٠	部门	+	IP关联	+		操作		
46		张		财务部		172.16.0.130)	ß	编辑 面 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 代存
the state of the s	5 ()		
设备名称	anonox		
物理位言	I XXXXXXXX		
联系方式	xxxxxxx J		
*community	y default (V1&V2快恋时必要	≜, V3快您时持了此项其他项业辅)	
支持板本	⊧ 🗹 V1&V2 🔲 V3		
常用节点信息			
OID		名称	描述
.1.3.6.1.4.1.2021.4		memorry	系统內存信息
13.6.1.2.1.25.2.3		hrStorage	彩纹动曲性带
			Set of Colonian Sector
1.3.6.1.4.1.2021.10.1.3		laLoad	系统CPU负载
1.3.6.1.4.1.2021.10.1.3 1.3.6.1.4.1.2021.11		laLoad systemStatus	系統CFU洗剤 系統CFU洗剤
13.8.1.4.12021.10.13 13.8.1.4.12021.11 13.8.1.2.1.2		laLoad systemStatus Interfaces	系統CFU造業 系統CFU連章 系統F4-定意

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		下数度版 导入 新建数据库名
名称	翻译内容	操作
🔻 🗎 oracle	甲骨文	+ 添加子项 🖸 編輯 🔟 删除
🔻 📔 user	用户	+ 添加子项 🖸 編編 👜 删除
ame	用户名	2 編編 面 删除
SQL关键字字典设置		下载模板 导入 新建
SQL关键字	翻译内容	操作
1 select	查询	☑ 编辑 · 面 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。

同卡重炸						
名称	Ib	MAC	Mask	状态	功論	操作
1 E0/1		4c:cc:6a:20:a1:46		WF开		12 編集
2 E0/2		4c:cc:6a:20:a1:47		WFFF		12 清清
3 E0/3		4c:cc:6a:20:a1:48		连接		12 编辑
4 E0/4		4c:cc:6a:20:a1:49		断开		12 编辑
5 HA	192.168.100.100	4c:cc:6a:20:a1:4a		断开	ha	12 编辑
6 MGT	172.16.1.129	4c:cc:6a:20:a1:4b	255.255.255.0	连接	mgt	12 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 様式 接口 Bypass 中価時 前回 E0/1.E0/2 中価時 点回 E0/3.E0/4 名称 网桥IP地址 MASK Vlan透传 Bypass 网桥 联动 操作 PUT 和:3 ___* 東开启 1 br0 匕 编辑 2 br2 未联动 未开启 巳 編辑



2.2.9.3 接口功能

在系统配置中,点击"硬件和诊断一>接口设置一>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)。

			保持手
	名称	开启边能	
1	E0/1		
2	E0/2		
3	E0/3	×Web節计 ×Pp節计 ×勞施問紙 ×對旗集審计	
4	E0/4	× Web第十 × Fp审计 × 劳动提新 × 改编集审计	

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, 然后点击下拉框中的数据库审

计,选框中将会出现数据库审计。最后点击<保存>按钮即可生效。

3	E0/3	1	
4	E0/4	Web审计	
4	20/4	Ftp审计	
		旁路阻断	
		数据库审计	

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,然后点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。最后点击<保存>按钮即可。

3 E0/3	×Web审计 ×Ftp审计 ×劳路阻断 ×数据库审计
4 60/4	Web审计
4 10/4	Ftp审计
	旁路阻断
	数据库审计



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。	t 🛑		
接口	= E0/2		
停止时间	司 2018-03	3-03 00:00:00	
	保存		

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				С
目的叩地址	子闷地码	同关	优先级	接口
192.168.1.0	255.255.255.0	0.0.0.0	0	MGT
静态路由表				atāji
目的IP地址	子闷淹弱	同关	优先级	操作



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 E0/1 · 数据库证	选择 全部数据库 🔻	抓包时间(秒) 5	¥	诊断并写入文件	开始分析
2	网络、路由诊断	:				
孠	民时查看路由是否	可达、跟踪路	各由状态。			
Pi	ng	Tracert				开始分析

3 端口探测

分析并展示端口状态

IP	拷口号		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	21		
每日上传时间	18	Я	졒	送录FTP的用户名 💿	123456		
自动上传	30	天(0~365)以前的备份文	(+	登录FTP密码 123456			
失败重传	2	Ŧ	上传文作	件存放FTP上的目录	130		
FTP服务器IP	172.16.0.130						
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 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 ▼	自动备份	手动备份			
备份频率 □ ▼ 开始时间 请选择月份 00:00:00 日志范围 全部备份 ▼		自动备份	0		
开始时间 请选择月份 00:00:00 日志范围 全部备份 ▼		备份频率	Ħ	Ŧ	
日志范围 全部备份 ▼		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。

系統設置备份	i li
--------	-----------------

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 数据存储上限	5 每半小/dJ 80%	
超限时审计处理策略 超限时数据清理策略	 ■ 計停止写入 ■ 备份系统并上特称有备份文件³ ■ 清理系统业与数据³ ■ 清理系统配置数据³ ■ 清理系统配置数据³ ■ 動勢 3 个月以前的审计日志 	
┃ 恢复出厂设置	依其	[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。

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⑦	
	□ 清理系统业务数据③	
	□ 清理系统配置数据⑦	
	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。



☆ 主页 ◎ 系统信息 □ 全局配置 ◎ 监控扫描

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 (忠记录 31,4	493条)										日前の新聞
100 ·	数据库(实例) +	設現库用户 +	2018/#3P +	客户IIIP +	客户端应用程序 +	NI2550 +	规则 +	an .	操作类型	 SQL酒句 + 	理作
2018-03-01 19:03:43	master	10	172.16.1.224	172.16.1.130	Microsoft JDBC Drive	无限增	全审计策略复制策略->	1077	SELECT	select sys.schemas.na	四 译版 22 会法评估
2018-03-01 19:03:43	master	50	172.16.1.224	172.16.1.130	Microsoft JDBC Drive	HRM	全审计策略批制策略->	MATE	NONE	select cast(null as cha	四 弹性 医会活淬使
2018-03-01 19:03:43	master	18	172.16.1.224	172.16.1.130	Microsoft JDBC Drive	无 RU 和	全寨计策略荒利策略->	1805	SELECT	select sys.schemas.na	(7) 课情 三会运序情
2018-03-01 19:03:42	master	10	172.16.1.224	172.16.1.130	Microsoft JDBC Drive	无限增	全审计策略规制策略->	旅行	NONE	sp_datatype_info_100	(P) 评估 二 会运洋情
2018-03-01 19:03:42	master	54	172.16.1.224	172.16.1.130	Microsoft JDBC Drive	无风险	全审计策略展制策略->	政行	SELECT	select sys.schemas.na	(1) 详備 21 会选注稿
2018-03-01 19:03:42	master	54	172.16.1.224	172.16.1.130	Microsoft JDBC Drive	无风险	全軍计策略展刺策略->	政府	NONE	select cast(null as cha	图 体例 盐金运体场
2018-03-01 19:03:42	master	sa	172.16.1.224	172.16.1.130	Microsoft JDBC Drive	无风险	全审计策略复制策略->	旅行	NONE	sp_configure 'user co	(F) 洋橋 21 会活洋橋
2018-03-01 19:03:42	master	-	172.16.1.224	172.16.1.130	Microsoft JDBC Drive	于规始	全面计管路留制领路->	\$\$\F	NONE	select system user	四 读描 起 会话读描



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			类型	Oracle		<i>,</i>
模式	审计	•	接口	E0/3	•	r
版本	9.1.0.1	*	*数据库(实例)			
* 端□	1521		*Ib			
备注						
					保存	取消

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	172.18.200.20		类型	Oracle		
模式	审计	Ŧ	接口	E0/3	-	
版本	9.1.0.1	Ŧ	*数据库(实例)	oracle		
*端口	1521		*IÞ	172.18.200.20		
备注						
					_	
					保存	取消

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。

 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。

\frown	审计与防火墙	
100 _{pts}	应用模式 📀	 ● 审计 ● 防火増
	数据来源 📀	E0/3 ~
设要	编码	自动探测 ~
×4	关联配置 🕐	关闭 ~
同日志、	旁路阻断 ᅁ	
② 设置>	数据脱敏	
功能设置	无连接会话识别	
策略应用	监控数据库应答	0
访问控制	影响行辅助	0
自学习防护	邮件告警通知	0
今 扫描 >	模糊化日志	0
→ 状态监控 >	会话超时	30 天 0 时 0 分
③ 数据脱敏 >		
	Agent	
数据库IP	CPU	0%
172.18.200.20 数据库类型	内存	0%
Oracle 版本 9.1.0.1	接收端口	7000 (7000 ~ 8000)
数据库(实例) oracle	CPU阀值	85

东软 NDBA 数据库安全



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。

审计与防火增						保存并启用
应用模式 🖲	◎ 审计 ○ 防火塘					
数据来源 🖲	E0/3	~				
编码	自动探测	~				
关联配置 🕐	关闭	~				
旁路唱新 🕐						
数据税数						
无连接会话识别						
监控数据库应答						
影响行辅助						
部件告答通知						
模糊化日志						
会活超时	30 天 0	et 0	分			

注意:

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。

数据来源 🔞	E0/3	~
--------	------	---



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	自动探测 ~
关联配置 💿	UTF-8 GBK UNICODE
旁路阻断 🕐	UTF-16 UTF-32
数据脱敏	自动探测

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

关联配置 🕐	IP关联 ~
数据脱敏	关闭 IP 关联 语句关联

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	÷	1	姓名	+	部门	+	IP关联	÷		操作
关联酝	已置: IP	・关联	、语句	关联						
IP 关耳	关开启艮	可								
关联	配置 🔊	IP关 关闭	·联		~					
ž	牧据脱敏	·天间 IP关 语句	」 ·联]关联							
语句关	、联:指	定的	SQL 语	句(例如	: sele	ct * from	user v	where II) =:id)	
关联	配置 🤊	语句关	(联		\sim					
		SQL	吾句							
3 编辑	員和删除									
点击<	编辑>打	安钮,	弹出编	辑框,修	改姓名	、工号、音	『「」、 I	9, 点击<	<确定>按領	即可。
点击<	删除>打	安钮,	提示'	"确认删除	",点च	告<确认>,	删除瓦	戈功。		
数据库用户	信息								导入 液	bn
195	+ 3	性名 ⊮-+	÷	部门 +	IP	€ ₩ ↓			操作	
1007	5	王王		対反部	192	.168.100.123			い 編辑 Ш 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;

4 E0/4	×Web审计 ×Ftp审计 ×劳路阻断 × 数据库审计
	Web审计
	Ftp审计
	旁路阻断
	数据库审计

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 🕐	E0/3	~	
	编码	自动探测	~	
	关联配置 곗	关闭	\sim	
	旁路阻断 ᅁ			
		⊠ ≑ E0/4		~

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;

阻断策略规则	高风险	~	阳峭	~	27378	🗐 详情	[] 编辑	官 删除

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	\bigcirc	
SMTP是否验证	\bigcirc	
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	172.18.200.20	
	保存 测试	

(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	邮箱地址

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	替换値	操作
help	help	\$##\$	「「編辑」 面 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	\$##\$	□ 編辑 □ 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	3.2.6.3	通	1433	用户名	
密码					
	测试连接				

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 30 天 0 ♦ 时 0 5	会话超时	30	天	0	\$	时	0	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	0				
	CPU		-		
	内存		-		
	接收端口	0	(7000 ~ 8000)		
	CPU阀值	85			
	审计端口	0			
	审计接口	~			
Agent	插件下载	windows(Vista及更高)插件下载 (》 windows(Server2003/XP)插	<u>件下载</u> ⑦	<u>linux插件下载</u> ⑦
		IP	掩码	操作	
	审计IP	127.0.0.1	255.255.255.255	面 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。



■ 审计与防火增			
应用模式 🕖	() 审计	⑧ 防火機	:
数据来源 🖲	br0		\sim
编码	自动探测	I	~
关联配置 💿	关闭		~
数据税缴			
无连接会话识别			
语句阻断			
监控数据库应答			
影响行辅助			
部件告替通知			
模糊化日志			

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。

数据来源 🕐	br0	~	

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。

数据脱敏



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 **SOL** 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		
	k	Ka 💽			
	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	sys		密码	
	是否有管理	理员权限 💿 是 🛛 🖓	КП П		
		测试连接			

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。

┃日志列表 (急记录 557₫	ę)								素部活合の
时间 +	数据库用户 4	数据库IP +	客户编IP +	风险等级 ◆	规则 + 动作	+ 12	昨美型 ◆	SQL语句 +	探作
2018-01-02 16:32:28	SYS	172.17.200.25	172.16.2.126	海风殿	22->22:全审计策略规制策 放行	LC	DGOUT	logout	E) 详情 22 会话详情
2018-01-02 16:32:25	SYS	172.17.200.25	172.16.2.126	海风殿	22->22:全审计策略复制策 放行	SE	ELECT	select dbms_transaction	四 详情 22 会话详情
2018-01-02 16:32:25	SYS	172.17.200.25	172.16.2.126	海风险	22->22:全审计策略复制策 故行	SE	ELECT	select 1 from dual	四 洋情 詰 会话洋情
2018-01-02 16:32:25	SYS	172.17.200.25	172.16.2.126	2617132	22->22:全审计策略复制策 放行	SE	ELECT	select 1 from dba_xml_s	四 洋情 註 会话洋情
2018-01-02 16:32:25	SYS	172.17.200.25	172.16.2.126	NO CONTRACTOR OF	22->22:全审计策略规制策 放行	SE	ELECT	select 1 from dba_views	四 详情 註 会运洋债
2018-01-02 16:32:25	SYS	172.17.200.25	172.16.2.126	満足にな	22->22:全审计策略复制策 放行	SE	ELECT	select 1 from dba_objec	[7] 详情 篇 会话详情
2018-01-02 16:32:25	SYS	172.17.200.25	172.16.2.126	海风险	22->22:全审计策略复制策 放行	SE	ELECT	select 1 from dba_trigg	[1] 详情 篇 会活洋情
2018-01-02 16:32:25	SYS	172.17.200.25	172.16.2.126	海风险	22->22:全审计策略复制策 故行	SE	ELECT	select 1 from dba_objec	四 洋情 詰 会活洋情
2018-01-02 16:32:25	SYS	172.17.200.25	172.16.2.126	ALFUR:	22->22:全审计策略复制策 放行	SE SE	ELECT	select 1 from dba_editio	四 详情 註 会活洋情
2018-01-02 16:32:25	SYS	172.17.200.25	172.16.2.126	通同論	22->22全审计策略规制策 放行	SE	ELECT	select 1 from dba_jobs	四 详情 22 会运洋债
2018-01-02 16:32:25	SYS	172.17.200.25	172.16.2.126	満足線	22->22:全审计策略复制策 放行	SE	ELECT	select 1 from dba_objec	[7] 详情 22 会活洋情
2018-01-02 16:32:25	SYS	172.17.200.25	172.16.2.126	高风险	22->22;全审计策略复制策 故行	SE	ELECT	select 1 from dba_queu	門 详情 器会活洋情
2018-01-02 16:32:25	SYS	172.17.200.25	172.16.2.126	海风险	22->22;全审计策略复制策 故行	SE	ELECT	select 1 from dba_queu	E) 详情 EI 会活洋情
2018-01-02 16:32:25	SYS	172.17.200.25	172.16.2.126	ALFUR:	22->22:全审计策略复制策 放行	SE SE	ELECT	select 1 from apex_relea	四 详情 註 会活洋情
2018-01-02 16:32:25	SYS	172.17.200.25	172.16.2.126	当同論	22->22:全审计策略规制策 放行	SE	ELECT	select 1 from sys.dba_re	四 详情 22 会活洋情
15条/页 *							1 2 3 4	4 5 6 _ >	期转到 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。



 \times

日志详情

时间 2018-02-28 09:12:10 风险等级 无风险 动作 放行 条略规则 全审计策略复制策略->全审计策 数据车名称 192.168.0.4 数据库类型 ORACLE 数据库(梁例) sqy 数据库第四 192.168.0.4 数据库第四 数据库(梁例) squ 数据库第四 192.168.0.4 308.0.4 数据库(梁例) scott 数据库第回 192.168.0.4 309.0.4 数据库(梁例) scott 数据库第回 192.168.0.4 309.0.4 数据库(梁例) scott 数据库第回 192.168.0.4 309.0.4 数据库(梁例) scott 数据库第回 192.168.0.12 309.0.12 数据库(梁) 0-60-42-68-1A-48 客户端风田程序 E\(\U0.12\U1.10\U1.				
放行 策略規则 全审计策略复制策略->全审计策 数据库名称 192.168.0.4 数据库类型 ORACLE 数据库(染例) \$xqy 数据库第四 192.168.0.4 3 数据库(本例) \$cott 数据库第回 192.168.0.4 3 数据库(本例) \$cott 数据库第日 192.168.0.4 3 数据库和AC 0-04-96-97-79-E4 餐户端应用程序 207.168.0.12 3 客户端MAC 0-E0-4C-68-1A-48 客户端应用程序 EV用光门诊诊间\mzzj.exe 3 客户端操作系统用户 64181 客户端反用程序 EV目光10000 3 窗口时长 0 日志级别 日気の見 3 婚妹対象 10 日立教 14 3 小面前すれない 周向状表 日志级别 14 3 操作対象 10 10 10 10 旅行教 10 現作 10 10 別ない 10 10 10 10 別ない 10 10 10 10 別ない 10 10 10 10 <td>时间</td> <td>2018-02-28 09:12:10</td> <td>风险等级</td> <td>无风险</td>	时间	2018-02-28 09:12:10	风险等级	无风险
NumberNumberNumberNumber数据库名称192.168.0.4数据库关型ORACLE数据库(空例)xqy数据库IP192.168.0.4数据库用户scott数据库端口1521数据库MAC0-04-96-97-79-E4客户端印207.168.0.12客户端MAC0-E0-4C-68-1A-48客户端应用程序EV旧光门诊诊向\mzzj.exe客户端端口64181客户端虚作系统主机MVFCM6NOAS7NOUV客户端操作系统用Administrator日志级别位是记录响应时长0微秒順应状态注销操作对象LOGOUT其他NoneSOL语行Egout	动作	放行	策略规则	全审计策略复制策略->全审计策
数据库名称192.168.0.4数据库类型ORACLE数据库(实例)skqy数据库IP192.168.0.4数据库用户scott数据库端口1521数据库MAC0-04-96-97-79-E4客户端IP207.168.0.12客户端MAC00-E0-4C-68-1A-48客户端应用程序E:\IP:\IP:\IP:\IP:\IP:\IP:\IP:\IP:\IP:\IP				略
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 0-04-96-97-79-E4 客户端IP 207.168.0.12 客户端MAC 0-E0-4C-68-1A-48 客户端应用程序 E:\IPLYTipWin(mzzj.exe) 客户端操作系统用户 64181 客户端操作系统主机 MYFCM6N0AS7NOUV 窗向时长 0微秒 日志级別 总是记录 順应时长 0微秒 順位状态 注销 操作对象 IOGOUT 其他 IOGOUT 近回长度 08yte Ingout Ingout	数据库名称	192.168.0.4	数据库类型	ORACLE
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\IRHC10300[\mmzj.exe 客户端端口 64181 客户端虚作系统主机 MYFCM6N0AS7NOUV 客户端操作系统用户 Administrator 日志级别 总是记录 响应时长 0微秒 响应状态 注销 操作对象 「 Jone 返回长度 08yte 其他 SOL语句 Iogout Jone	数据库(实例)	sxqy	数据库IP	192.168.0.4
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 客户端操作系统主印 MYFCM6N0AS7NOUV 客户端操作系统用户 Administrator 日志级别 总是记录 响应时长 0微秒 响应状态 注销 操作对象 - 操作对象类型 None 返回长度 0gout 其他 -	数据库用户	scott	数据库端口	1521
客户端MAC00-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MVFCM6N0AS7NOUV客户端操作系统用户Administrator日志级别总是记录响应时长0微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ByteSOL语句logout	数据库MAC	00-04-96-97-79-E4	客户端IP	207.168.0.12
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微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08yteSOL语句logout	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
客户端操作系统用户 Administrator 日志级别 总是记录 响应时长 0微秒 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 - -	客户端端口	64181	客户端操作系统主机	MYFCM6N0AS7NOUV
响应时长 0微秒 响应状态 注销 操作对象 ////////////////////////////////////	客户端操作系统用户	Administrator	日志级别	总是记录
操作対象 Mone 操作対象美型 None 操作类型 LOGOUT 其他 返回长度 OByte SOL语句 logout	响应时长	0微秒	响应状态	注销
操作类型 LOGOUT 其他 返回长度 OByte SOL语句 logout	操作对象		操作对象类型	None
返回长度 OByte SOL语句 logout	操作类型	LOGOUT	其他	
SOL语句 logout	返回长度	OByte		
	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。

最新普	曾 > 172.16	i.1.108 (总记录 3,290条)																		日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日
Bili	٠	数据库(实例) 4	数据库用户	+	設落库1P	٠	客户端IP	+	客户端应用程序 ∔	风险等级	+	规则	+	动作	+	提作类型	٠	SQL语句	+	80
2018-0	2-28 18:12:54	ord	STARING		172.16.1.108		172.16.1.144		JDBC Thin Client	无风险		全面计策略	军创话路	放行		SELECT		select roun	d(sum(pin	E 洋橋 21 会活洋橋



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。

日志列表	(总记录 413条)																り、日本の方法
时间	+	数据库用户	+	数据库1P	٠	宫户编IP	+	风险等级	+	规则	+	动作	•	操作类型	+	SQL语句	+	接作
2018-02-28	18:17:56	STARING		172.16.1.108		172.16.1.144		无风险		全审计策略贯	《刺策略->全	放行		SELECT		select round	sum(pinhit	⑦ 洋債 に 会话洋債

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。

昭间 +	Scrittip 4	設備年後户 +	网络琴眼	*	規則 +		squille) +	操作
018-02-28 18:17:58	172.16.1.144	STARING	光AUS		全审计预结其利用结	>全审计策略	logout	(1) (# 10
018-02-28 18:17:56	172.16.1.144	STARING	END		全审计策超聚制策略	全审计策略	select waiting_session_holding_session_lock	② 讲版
018-02-28 18:17:56	172.36.1.144	STARIN 日志详情			×	全带计预制	select sid serial#machine.program.lockwait	罰 译情
018-02-28 18:17:56	172.16.1.144	STARIN 时间	2018-02-28 18:17:58	风险等级	无风险	全部计编辑	select sql_text, buffer_gets, executions, buffe	四 評議
018-02-28 18:17:56	172.16.1.144	STARD 32/F	拔行	頒略规则	全审计策略复制策略->全审计策略	全审计策略	select dba_df.file_name, dba_df.tablespace	टा जन्म
018-02-28 18:17:56	172.16.1.144	STARIN DIESEN	172-16-1-108	数据库关型	ORACLE	金寨计兼暗	select r.segment_name, r.tablespace_name,	的。這個
018-02-28 18:17:56	172.16.1.144	STARIN 款还有(实例)	orcl	数据库IP	172.16.1.108	全审计策略	select waitsid, waitevent, waitwait_time, wa	回神情
18-02-28 18:17:56	172.16.1.144	STARIN	STARING 44-84-58-95-FF-94	数展準済日	1521	全审计编辑	select stat.sid, sess.status, sess.machine, ses	23 inte
018-02-28 18:17:56	172.16.1.144	STARIN SEMMAC	00-0C-29-28-79-13	客户选应用程序	JDBC Thin Client	全审计策略	select Lgroup#, Lthread#; Lseguence#, Lbyte	門評価
18-02-28 18:17:56	172.16.1.144	STARIN A ARK	23129	臺內满發作系统主机	masterhost	全审计规程	select t.tablespace_name_t.contents_t.status	创计情
18-02-28 18:17:56	172.16.1.144	客户读得作系统用户 实达时长	root OBES	日志吸制 第四状态	想是记录	全事计策略	select ditablespace_name, sum(f.phyrds) ph	27 MB
18-02-28 18:17:56	172.16.1.144	STARIN 操作对象		操作的象类型	None	全审计策略	select ditablespace_name, countid file_name	⑦ 详博
18-02-28 18:17:56	172.16.1.144	STARIN	LOGOUT	其他		全审计策略	select sum(bytes) from v\$sgastat where poo	四,評價
18-02-28 1817:56	172.16.1.144	适回长度 STARIN SOLER	08yte logout			全审计策略	select sum(bytes) from v\$sgastat where poo	四 洋橋
018-02-28 18:17:56	172.16.2.144	STARIN				全审计策略	elect sum(decode(upper(name), 'free memo	(T) (#14
				_	50N			10147

4 概况

进入数据库,选择日志子选项概况,可以查看数据库概况信息。 概况包括三部分:

风险分布









18:11

18:02

18:12

18:17

18:22

18:26

18:27

18:28

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。



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。



东软 NDBA 数据库安全

今日	~	<	20	18年	1月					201	18年	2月	>	\gg
本周					-/ -							-/ -	<i>r</i>	~~
本月	日	_	Ξ	Ξ	四	五	六	日	_	Ξ	Ξ	四	五	六
最近1小时	31	1	2	3	4	5	6	28	29	30	31	1	2	3
最近2小时	7	8	9	10	11	12	13	4	5	6	7	8	9	10
最近3小时	14	15	16	17	18	19	20	11	12	13	14	15	16	17
最近7天	21	22	23	24	25	26	27	18	19	20	21	22	23	24
最近30天	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	鲥间										清	ź i	确定

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。



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



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





日志统计



	语句数量	致命风险	高风险	中风险	低风险	无风险	失败语句	会话数量	操作	
ALTER	4	4	0	0	0	0	0	1	子条件	🗄 详情
SELECT	36	0	0	36	0	0	4	2	子条件	🗄 详情
NONE	6	0	0	0	0	6	0	2	子条件	曰 详情
LOGIN	2	0	0	0	2	0	1	1	子条件	🗊 详情
LOGOUT	1	0	0	0	1	0	0	1	子条件	🗐 详情

动作

日志统计



类型





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。

风险分析 会话分析 语句分析

前 2018-01-02 16:24:29 ~ 2018-01-02 17:24:29 ∨ ○ 刷新本页 ① 导出报表

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。

风险分机	БТ					前 2018-01-02 16:24:29 ~ 2018-01-02 17:24:29 ~ ♡ 刷新本页 ① 导出投	表
风险走	趋势图					_	
			报表导出		×	- 音響 - 唱新 - 放行 - 未指定	
			内容	🕑 风险分析 🛛 会话分析	🔲 语句分析		
0.8 -			格式	Pdf Pdf			
				Excel Word	保存至报表列表		
0.4 -			_				

可以通过"全局配置->报表管理"中查看生成报表

报表结果 报表设置									
报表列表 (台记录2条)									
名称	范围 全部 🔻	生成时间	内容	桔式	秋志				操作
172.16.1.108会诺分析,语句分析180301093942	172.16.1.108	2018-03-01 09:39:42	会适分析,语句分析	Pdf		100% 已完	成	*	下账 窗 删除
172.16.1.108风路公标180301093932	172.16.1.108	2018-03-01 09:39:32	风险分析	Pdf		100% 日来	威	*	化下载 田田時



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



数据库账号分布 Top10

[▮] 数据库账号分布Top10





规则命中分分布 Top10



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







数据库账号分布 Top10

┃数据库账号分布Top10





客户端工具分布Top10





东软 NDBA 数据库安全







失败会话数据库账号分布 Top10

┃ 失败会话数据库账号分布Top10



关联会话数 2

3 语句分析

语句分析包括七部分:

SQL压力





东软 NDBA 数据库安全







数据库账号分布 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 10 SYSTEM 致命风险 高风险 中风险 低风险 无风险 1 0 10 3 20 SYSTEM 0 0 0 0

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。



删除

单库策略			重新下发 添加
序号	策略	状态	操作
0	全审计策略無制策略(共1条规则,启用1条)		目 详情 面 删除
0	22 (共1条规则, 雇用1条)		同 详情 前面 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	5	策略	状态		攝作
Ð)	全审计策略氦制策略 (共1条规则, 启用1条)		□ 详悔	青毛
2		22 (共1条规则, 屆用1条)		🗊 详情	青

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。

▲库策略				里新下发 添加
序号	策略	新聞前市語8	秋志	操作
Θ	全审计策略复制策略 (共1条规则, 启用1条)	30.000-000 Contractions of the second s		四 洋情 自動除
Θ	黑名单复刻策略(共7条规则,启用7条)	名称 语域写新谱策略名称		同 详情 盲 删除
0	白名单質制策略(共4条规则,应用0条)	请描述一下		四 详情 盲 謝除
0	入侵检测策略复制策略(共444条规则,屈用0条)	描述		四洋橋 直 删除
0	通用sql注入策略复制策略(共6条规则,启用6条)			[7] 详情 窗 删除
		操作系统用户: 🔍 区分大小写 💌 不区分大小号		
		客户颁程序: 🔘 区分大小写 🖲 不区分大小写		
		199.1. R2/24		

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

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 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。





+ 添加 曰 全局参数	规则列表 基本信息							居 重词 ~
 	【 黑名单 (总记录 7)					批量操作	应用到数据库	添加
王 當 全审计策略	□ 秋恋	名称	等级	动作	优先级	+ #	ene Ene	
王 圖 入侵位利策略		高危DCL语句	高风险 🗸	振響 〜	7		回洋情 区编辑	ti Bile
+ 💼 cz		高危DDL语句4	高风险 ~	授幣 ~	6		目详情 ビ 編編	直 删除
🕂 💼 plzd	•	高危DDL语句3	高风险 🗸	报警 〜	5		回洋情 区编辑	直 删除
王 🧰 阻断策略		高危DDL语句2	高风险 🗸	报警 〜	4		四洋情 已编辑	ti mie
		高危DDL语句1	高风险 🗸	报警	3		目详情 ビ 編編	1 11111
	•	高危操作2	高风险 🗸	报警 〜	2		目详情 区编辑	直 删除
	•	高危操作1	高风险 ~	振響 ~	1		門 详情 「区 編編	10 MIA
	15条页 🔻							

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。 点击<确定>按钮,新增策略。

	┃ 通用sql注入策略 (他记录	6)								北麓路市 (四月形和)	10 IS
王 章 主要计算机 王 章 入侵性的服務	8 HS	名称 MYSQL报酬型SQLIE入	新增全局策略				×	优先级 27336	•	操作 前 详持 〔2	(44) 0 mm
▲ 國際和印度人類地		HAVING開催SQLI主人	86	读话写影言信号	12.17			27335		费祥情 已	
	8 💼	UNION翻查置词SQU主人	53	请描述一下				27334		四神体 已	
		时间型SQU主人					~	27333		割 神精 (2	
	a 💼	植蝴蝶SQU主人	模板未浸	全局策略	~		~	27332		四洋橋 已	A4 8 89
	8 19条页 •	布尔雷SQU主人	欄板 数編車用户: 場作五线用户:	 空前消晒 区分大小写 区分大小写 	 不区分大小司 不区分大小司 		*	27331		17) (M 18)	96 D 20
			首户决程序:	 区份大小写 	● 不区分大小写						
						100 K	Ria				

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
	数据库用户	新增策略默认数据库用户不区分大小写
区分入	操作系统用户	操作系统用户默认不区分大小写
小与	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, 点击提示框中的<确定>按钮,即可删除策略。



+ 添加 🛯 全局参数	规则列表 基本信息					25 夏河 ~
+ ■ #S# 1<	通用sql注入策略 (色记录6)				批量操作	应用到数据库 添加
王 = 全审计策略	0 K2	80	\$P.05	动作	优先级 4	操作
 王 二人投位利用時 王 二 通用sal注入策略 	•	MYSQL报键型SQLL主入	海戸社 〜	报警 〜	27336	同洋情 区编编 由删除
		HAVING原槽SQLI主入	中风险 ~	报警 〜	27335	同洋情 乙编辑 直删除
		UNION联合置词SQU主入	中风险	振撃 く	27334	四洋橋 乙烯磷 直出除
		时间型SQL注入	中风险 ~	授整 ~	27333	同洋情 乙编编 直删除
		価等式をQU注入	高风险 ~	振撃 ~	27332	同详情 乙编辑 直删除
		布尔型SQU主入		报警 〜	27331	回洋情 区编辑 直删除
	15条页 🔻					

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
	deny	致命风险 🗸	阻断	27366	目 详情 IC 编辑 前 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)					批量攝作	应用到数据库	添加	
	状态	各称	等级	动作	优先级	+	操作	
		deny	致命风险 ~	阳峨f ~	27366		同 详情 🛛 編辑	面 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
	deny	致命风险 ~	阳唐f ~	27366	目 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
	deny	致命风险 🗸	阻断~	27366	同详情 IC编辑 面 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	名称	
描述	描述一下规则的基本信息	
状态		
等级	无风险 ~	
动作	放行 ~	
日志记录级别	不记录 ~	

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IP	客户端]	[具 客户端操作系统用户	客户满操作系统主机名	
	状态	0		
	范围	不包含	~	
	自定义	起始IP	- 终止IP	
			» «	

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
	¥	大态 🔵	
	702	范围 不包含	~
			»
			«

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	~

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	数据库用户 敏感数据访问 web		webI	Р	web用户名	
		状态						
		每日(时)	开始时间			- 40	结束时间	
		每周(周)	开始时间			- 40	结束时间	
		每月(日)	开始时间			- 40	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多或多个数据库。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



 \times

确认

取消

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。

应用到数据库(默认选中已应用的数据库)

数据库名	数据库类型	数据库IP
1725	Oracle	172.17.200.25
1820	Oracle	172.18.200.20
1790	DB2	172.17.200.90
1870	MySQL	172.18.200.70
172.16.1.180	SQLServer	172.16.1.180

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。

数据库服务访问控制 (参记录1)							源ba
目的IP	第口	客户编IP				动作	操作
172.18.200.11	22	172.16.0.1	2.16.0.180			四面	12 编辑 直 删除
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。



报末结果 服素设置						
报表列表 (总记录7条)						
各称	范围全部 🔻	生成时间	内容	枯式	状态	操作
春户跳应用程序性能	全部	2018-02-05 14:45:23	音户跳应用程序性能	Pdf	100% E#ut	★ 下就 箇 删除
登录分析	全部	2018-02-05 14:45:21	登录分析	Pdf	100% 已完成	金 下統 圓 删除
客户跳IP	全部	2018-02-05 14:45:18	客户演IP	Pdf	100% B#st	和田 服子 生
春户确操作系统主机	全郎	2018-02-05 14:45:16	畜户通過作系统主机	Pdf	100% 已地成	金 下数 圓 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% 已充成	和田 田 田子 史
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% E#st	★ 下数 御 删除
数据库审计综合状况报告	全部	2018-02-05 14:43:13	数据库审计综合状况报告	Pdf	100% 已先成	金 下数 圓 删除
15条页 ~						

3.8.1 报表设置

点击<报表设置>按钮,进入高级报表界面。

指法结果 私未设置				
高级报表				
和田	编述	10歳で周	计划任务	操作
🕶 🎦 雅明短期				
前展岸部会状况报告	展示系统内违加的所有的某些的综合状况。	Bril.	伴用	团 计划任务 副 生成接条
数据库安全分析报音	对當時數據厚進行的安全線蛋份新	Brs.4.	停用	回 计划任务 昌 生成损费
▼ 🍋 服装器分析				
款据库服务器分析	分别为数据库名称及数据库用户数柱状面及访问数据库申请P中面(同原命P),事格名称为数据库登录及考虑统计报表分别自数。	BESA.	伊用	6 数据范围 图 计划任务 副 全成资料
約44本服券器性能	通过对数据库的最佳的现为建度来利斯数编的性能。	Brist,	停用	© 數據范围 团 计现任员 醫 生成服務
🔻 🗎 麻源分析				
款据库用户分析	還过不同的救援車用戶访问不同的救援車進行分析。	IN.L.	伊用	◎ 數層活面 团 计现任号 酉 生成资素
▶ 南户满应用程序	通过算户供应用程序的数据库用户、算户链提作系统主机、客户链区、整要等进行统计分析	BEU.	停用	◎ 数据范围 团 计划任务 盟 生成服務
▶ 客户课操作系统主机	统计访问数据等的客户编辑作系统主机相关信息	Rtul	使用	© 数据论图 凹 计划任务 目 生成服素
■ 業产減少	统计理》中等户确立用程序、数据型用户数量,循环数量	BHA,	伊用	© 数据活圈 团 计划任号 四 生成报表
▶ 登录分析	统计整要数据等的用户,操作系统主机名、通信用程序、用户,接合类型、目标IP、数据等、Schema、整学数量。	BISA.	体用	© 数据范围 凹 计划任号 督 生成报表
春户满应用银序性能	分析漫应用程序的性能,对于操作时长盛过起的操作,进行统计;用户操作干均时间,过长时间,应用程序的时间去比、干均要…	Rhu,	停用	③ 數据范围 四 计划任师 四 生成服務
🔻 📙 操作典型分析				
▶ 特权操作分析	统计将权操作相关谋善,包括将权操作类型、将权操作对象谋善、基于遵与操作的将权操作者求。	BUN.	绿用	◎ 數據范围 团 计磁任务 昌 生成报表
唐·唐相對除物軟新	统计不同用户对意的删除与载新(drop/truncate)。	献以	停用	◎ 数据管理 ② 计划任务 ◎ 生成服務
▶ 种仙过程的更放	统计用户对导的操作,导的局型属于Procedure、Function并且操作属于特权操作。	野以	停用	◎ 数据范围 图 计划任务 圖 生成投票
DCL#+	通过DCL命令分析用户与研促操作。	Rest.	停用	◎ 對靈花園 図 计划任务 篇 生成接承

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 全部 🔻	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	上 下载 直 静除
1725风脸分析180102170516	1725	2018-01-02 17:05:16	风险分析	Pdf	100% 已完成	业 下戦 面 删除
1725风险分析180102170516	1725	2018-01-02 17:05:16	风险分析	Pdf	100% 已完成	业 下载 面 删除
1725风险分析,会适分析,语句分析180102105728	1725	2018-01-02 10:57:28	风险分析,会适分析,语句分析	Word	100% 已完成	业 下载 面 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。





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。



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





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。

减利于摘 历史服表 运泡车 开放								
【扫描引擎列表 (台记录1)								新建引擎
名称 IP 数据库版本	60280507	40.5 BIG	19 14		×	扫描结束	19.00	操作
L1_108oracle 172.16.1.108 ORACLE(11.2.0.	3.0) 2018-03-01 14:22:20	完成				2018-03-01 14:23:57	任风险:1 中风险:5 毫风险:1	◎扫描 自動除
15条/页 *		• 3	称	数据库	手动添加 *			
		* 17	,					
					6217 101/14			
			_	_	_			
国山収主・ オ	5毛 巳山	叫於	√収主					
加丈取衣・重	211、寸山	1、 加内	TRAX					
雇用扫描 历史报表 雇利 库 升级								
Manager Construction				1010 VII 40	1.010			
接要名称 	数据库IP	数据库美型	10)	归 须 引擎名称	生成时间			E BITA
	17112011200	on acception	,	1,100,100	1010-05-01 141305		O TENK IN ANIMA E	
15張/页 *								
漏洞库:系约	吃默认的数	据库漏	詞					
数据库漏洞种关	风	验漏洞种类			日月间			
Postgresgl展网 DM7度间 Sybase展网							-	低风脸 — 中风脸 — 高风脸
	racle.me.mp 350 300 250				50 40 -			\wedge
	200 150 SOLServer運用 100				30 - 20 -		\wedge	$// \wedge$
MySQLIBH DB	50 0	商风险震调	中风险鹰网	低风险尾同		And		
					2005年 2009年 2010年 2010年 第4季度 第2季度 第1季度 第4季度	2011年 2012年 2013年 第3季度 第2季度 第1季度	2013年 2014年 2015年 21 第4季度 第3季度 第2季度 第	016年 2016年 2017年 11季度 第4季度 第3季度
数据库关型 全部 🔻 风	29等级 全部	▼ 名称(携要)						重要 查询
【 濃洞库 (徳记录 530)								
名称	发现时间	等级	数据库类型	接要				操作
Oracle数据库服务器的Java VM组件中的脆弱性	2017-10-19 00:00:00	低风险	Oracle	Oracle数据库服务器的Jav	va VM组件中的存在多个未知的意间。			四 详情
Oracle設描單證券器的XML設描單這件層同	2017-10-19 00:00:00	(ERUS)	Oracle	Oracle数据库服务器的XM	AL数据库编件中容易受到攻击。			(1) 详情
Oracle数据库服务器的RDBMS安全组件展用	2017-10-19 00:00:00	(ERUS)	Oracle	Oracle数据库服务器的RD	8MS安全组件中容易受到攻击。			(1) 详情
Oracle数据率服务器的核心RDBMS组件中属同	2017-10-19 00:00:00	但我以後	Oracle	Oracle数据库服务器的核	URD8MS组件中容易受到攻击.			回 详情
Oracle数据库服务器 "WLM" 和 "Spatial" 组件多个未指定的								
	0篇 2017-10-18 14:48:23	常风险	Oracle	這个主机正在运行Oracle	数据库服务器并且容易出现多个未指定的安全篇词.			(7) 洋橋
Oracle数据库服务器的RDBMS安全组件存在属词	6編 2017-10-18 14:48:23 2017-08-08 11:29:03	常风险 (任风)常	Oracle Oracle	这个主机正在运行Oracle Oracle数据库服务器的RD	数编库服务器并且容易出现多个未指定的安全漏洞。 98MS安全退件中容易受到攻击。			图 译编 图 详编

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。



aren Datas are 74		
1 740		手动导入升级文件 升级
개規记录 (自然 0)	雨入升施文件 × ×	
256	并成2: 件 他这些之中 他	
	60 R.4	

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。

新建引擎

*名称 服务举型	请填写扫描引擎的名称	ξ		
	起始IP	终止IP	操作	
网段设置		+ 添加		
			保存	取消
点击操作列<扫描>即]_].			
10.100	192	2.168.10.10-192.168.10.100	未开始 ◎ 宣看结果	◎ 扫描 面 删除

X



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。

KARIAS SALANT	2000										
扫描引擎列表(乐记录1)											新建引集
20	Received	数据工业	新建引取						RA		
108數學教展扫描		电流导份证明。审视银行中导		96Z		12.00			9 2	212日編 章 役重 音 勝昧	
15葉/页 *			*88	108數感数编扫描	政黨有	172.16.1.108					
			*用户名	sys	*8056	oracle					
			*主机名	172.16.1.108							
							X.				
					_	_		_			

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。



8087-16	统计结束 数据类型								
BIE	翻 请选择日期	→ 任务名称 全部	▼ 服労翻P		服务关型 全部	*			意識
軟感表数据	(中国) (中国) (中国) (中国) (中国) (中国) (中国) (中国)								
时间	服务器IP	主机名	数据库 者	式名 表 (夜圈)	表类型	服务类型	敏感	操作
				/					
				智无拘	8				
15条/页 *									
敏感列数据	■ (忠记录0)								
列名称		教務美型	长度		扫描类型		扫摄模式		操作
;	またまま	法 加	あまお捉						
3	奴 ////天空	/が加、 加休	蚁 念 奴 加。						

和48559% 统计结束	数据类型					
数摄类型						35.b0
名称	表名	列名	最短长度	类型	内容	操作
▶ 📔 姓名						+ 添加子项 盲 影除
▶ 🐂 邮箱						+ 添加子谈 窗 删除
▶ 📔 电波						+ 添加子项 直 删除
▶ 📔 身份证券						+ 添加子项 自 删除
▶ 🐂 £8ig						+ 添加子项 窗 删除
▶ 📔 银行识别代码						+ 添加子项 自 删除
▶ ■ 药物名称						+ 澤加子项 自 影除
▶ 📔 药物价格						+ 添加子颂 窗 删除
▶ 📔 窗码						+ 质加子液 直 删除
▶ 📔 银行卡号						+ 添加子项 自 影钟

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	60	Ŧ	秒之内,	用户尝试登录的	的失败次数超过	3	Ŧ	锁定该用户	1	Ŧ	分钟
登录会话超时	30			分钟不操作	,自动退出						
密码长度参数	密码最短长度	8			密码最长长度	30	*				
密码过期参数	\bigcirc										
密码过期时间	7			时间只能为	正整数,且不超过	17天					
下载文件密码 🕄											
确认密码											

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。

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。

保存



4.1 监控

系	统资源使用率											
CPU 100% 80% 60% 40% 20%	 				HFE(2.95G)					RE(1466)		
	接口	最大传输单元	是吉田环	秋志	MAC地址	IP地址		接收速率(kb/s)	接收包速率	(pck/s)	发送速率(kb/s)	发送包速率(pck/s)
1	E0/1	9212	#	连接	00:0c:29:F9:01:48			0.65	9.00		0.00	0.00
2	E0/2	9212	ē.	连接	00:0c:29:f9:01:52			0.65	9.00		0.00	0.00
3	E0/3	9212	ā.	進接	00:0c:29:f9:01:5c			0.83	12.00		0.00	0.00
4	E0/4	9212	a	连接	00:0c:29:f9:01:66			0.65	9.00		0.00	0.00
5	НА	9212	a	连接	00:0c:29:f9:01:70			0.65	9.00		0.00	0.00
6	MGT	9212	a	追接	00:0c:29:f9:01:7a	172.16.1.18	2/24	0.83	12.00		0.00	0.00
影	統吉警列表 (总证	己录 2)										
双生	1896A)				日志美型		事件类别		事件内容			
201	8-03-01 05:50:00				CPU		致命		飲命:CPU使用量已经能	1298%		

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	◎ 取満援权

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	款认管理员	正常	◎ 授权 直 删除 匕 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	
輸入密码	
确认密码	
	确定 取消

东软 NDBA 数据库安全



5.2 角色管理

安全管理员下,进中"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。

用户管理	角色管理		
角色管理			添加
	角色名	授权機块	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、数据库防火境、状态监控、漏阀扫描。	
2	系统操作员	数据率适明加密	
3	审计操作员		
4	role1	设备扫描	□ 編辑 直 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	test_star	
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)	
	确定取消	

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

东软 NDBA 数据库安全



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。



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					〒 重词 節 2018-01-02 00:00:00 ~ 2018-01-02 23:59:59 ∨
日志						以当前条件导出
序号	用户名 🖡	IP +	操作时间 🕴	功能点 🕴	动作 +	详插信题 🔸
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	查阅操作日志	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 13:53:03	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	古管理							名 査询	6	团 2018-03	-01 16:27	/:20 ~ 2	2018-03-	1 17:27:	:20 ~
Г	lb	用户名	3542-07			今日 本周	«	(2018年	3月				2018年	19)) »
	主府 取消					本月 最近1小时	E - 25 2	- = = 5 27 28	1	五 六 2 3	8 1	2	= = 3 4	四 王 5 (5 7
	Auditor	1/2-10-1-100	TOTO-02-01 11/2013	2.4.7%	五日大石	最近2小时	4 5	6 7	8	9 10	8	9 1	10 11	12 13	3 14
2	Auditor	172.16.1.180	2018-03-01 17:24:00	操作日志	査询操作日志	最近3小时 最近7天	11 1	2 13 14	15	16 17	15	16 1	17 18	19 20	0 21
3	Auditor	172.16.1.180	2018-03-01 17:23:51	警察系统	整入系统	最近30天	25 2	9 20 21 5 27 28	29	23 24 30 31	29	30	1 2	3 4	1 5
4	Auditor	172.16.1.180	2018-03-01 17:17:13	登录系统	登出系统			3 4					8 9		1 12
5	Auditor	172.16.1.180	2018-03-01 17:14:14	登录系统	登入系统		选择时	0						清空	确定
6	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						
7	Auditor	172.16.1.180	2018-03-01 17:08:06	登录系统	登入系统			用户Aud	itor登入	系统					
155-65	~														

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。

日本 加名 P 第 1 <th1< th=""> 1 1</th1<>	操作日志管理	理							图 重调	
内局 中 中 中 中 中 日 1 1 1 1 1 <th1< th=""> 1 <th1< th=""> <th1< th=""></th1<></th1<></th1<>	日志									以当前条件导出
Auditor 172.16.0.130 2018-0 行政 金銀(集成万万行) 活政 2 Auditor 172.16.0.130 2018-0 号出物式 Pdf 3 Auditor 172.16.0.130 2018-0 4 Auditor 172.16.0.130 2018-0	序号	用户名	÷	IP	+	报表导出操作时间			×	
2 Auditor 172.16.0.130 2018-0 Puf - 3 Auditor 172.16.0.130 2018-0 -	1	Auditor		172.16.0.130		2018-0: 行数	● 全部(最多两万行) ◎ 指定	行数		
3 Auditor 172.16.0.130 2018-0 4 Auditor 172.16.0.130 2018-0	2	Auditor		172.16.0.130		2018-0: 导出檔	Pdf v			
4 Auditor 172.16.0.130 2018-0 単記 取消	3	Auditor		172.16.0.130		2018-0:				
	4	Auditor		172.16.0.130		2018-0:			確定 取消	
5 Auditor 172.16.0.130 2018-01-02.13.53.12 操作日志 重调操作日志 重调操作日志	5	Auditor		172.16.0.130		2018-01-02 13:53:1	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	6	Auditor		172.16.0.130		2018-01-02 13:53:1	登录系统	登入系统	用户Auditor登入系统	

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									7	查询		2 17:36:44 ~ 20)18-01-02 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	+	详情信息	+		
1	SecAdmin		172.16.0.85		2018-01-02 1	8:16:31	审计日志检索		创建任务		执行审计日志制	素任务		
2	SecAdmin		172.16.0.130		2018-01-02 1	8:16:30	审计日志检索		创建任务		执行审计日志相	蒙任务		
3	SecAdmin		172.16.0.180		2018-01-02 1	8:16:22	登录系统		登出系统		用户登出系统			
4	SecAdmin		172.16.0.130		2018-01-02 1	8:16:21	审计日志检索		创建任务		执行审计日志物	蒙任务		
5	SecAdmin		172.16.0.85		2018-01-02 1	8:16:21	审计日志检索		创建任务		执行审计日志制	蒙任务		

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。

操作日志管理					12 重调	🛗 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 +	报表导出 躁		×	羊情信息 +
1	SecAdmin	172.16.0.85	20: 行数 💽 全部 (最多雨	雨万行) ◎ 指定行数		执行审计日志检责任务
2	SecAdmin	172.16.0.130	20: 导出指式 Pdf	Ŧ		执行审计日志检索任务
3	SecAdmin	172.16.0.180	20:			用户登出系统
4	SecAdmin	172.16.0.130	20:		确定 取消	执行审计日志检索任务
5	SecAdmin	172.16.0.85	2018-01-02 18:16:21	审计日志检索	创建任务	执行审计日志检索任务

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:



E0/1 E0/	2 E0/3 E0/4 HA MGT		
接口设置	接口组 接口功能 接入即审计		
		6	栫
名称	开启功能		
1 E0/1			
2 E0/2	×旁路阻断 ×数据库审计		
3 E0/3	×数据库审计		
4 E0/4	×旁路阻断		

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:

提示		×
\triangle	是否使用配置向导进行数据库添加与配置!	
	使用	不使用



东软 NDBA 数据库安全

					×
	基本信息	模式选择		策略配置	
*名称	172.16.1.253	类型	Oracle	▼	
版本	11.2.0.1	▼ *数据库(实例)	ORCL		
*端口	1521	*IP	172.16.1.253		
备注					
				\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	步

基	本信息	模式选择	策略配置
模式	审计	•	
接口	E0/2	•	
×Ц	E0/2	. The	



基本信息	模式选择	策略配置
策略		状态
全审计策略复制策略		
黑名单复制策略		
白名单		\bigcirc
入侵检测策略		
通用sql注入策略		

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)

webserver.conf	- 记事本	
文件(F) 编辑(E)	格式(O) 查看(V) 帮助(H)	
https://172.16	5.2.143/base/receiveagentin	fo

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。

	A 10	At 11-73 873	10.000		
收藏夹	当称	惨战日期	英型	大小	
下载	🙀 ca-bundle.crt	2017/1/28 2:21	安全证书	256 KB	
桌面	Cache	2016/8/22 14:08	文件	1 KB	
最近访问的位置	:// curl.exe	2017/2/25 3:51	应用程序	2,022 KB	
	curl_new.exe	2009/3/3 22:36	应用程序	304 KB	
<u>د</u>	BBAAgent.exe	2018/6/21 17:13	应用程序	514 KB	
2040	DBACapture.exe	2018/8/1 11:42	应用程序	533 KB	
	🚳 install.bat	2018/6/21 15:21	Windows 批处理	1 KB	
n international and a second s	🔜 install.exe	2016/5/19 18:54	应用程序	412 KB	
	instsrv.exe	2018/9/28 17:41	应用程序	88 KB	
り首乐	libeay32.dll	2018/9/28 17:41	DLL 文件	1,132 KB	
	ibssl32.dll	2008/3/18 17:35	DLL 文件	200 KB	
计算机	🎲 npcap-0.81.exe	2018/6/21 11:52	应用程序	710 KB	
~本地磁盘 (C:)	srvany.exe	2006/6/28 4:55	应用程序	8 KB	
∍ 本地磁盘 (D:)	🚳 uninstall.bat	2018/5/3 15:15	Windows 批处理	1 KB	
a 本地磁盘 (E:)	📑 uninstall.exe	2016/5/19 18:55	应用程序	412 KB	
	e webserver.conf	2018/6/21 17:59	CONF 文件	1 KB	
	🖻 说明.doc	2018/8/1 12:06	DOC 文件	89 KB	
F71.44	📄 说明.txt	2018/5/3 15:19	文本文档	3 KB	

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:

◎ 服务								X
文件(F) 操作(A) 3	ē看(V) 帮助(H)							
) 🗟 🛛 🖬 🕨 🔳 🕪 👘							
🥋 服务(本地)	⑤ 服务(本地)							
	DBAAgent	名称	描述	状态	启动类型	登录为		^
		鵒 CNG Key Isolation	CNG		手动	本地系统		
	启动此服务	🔍 COM+ Event Sys	支持	已启动	自动	本地服务		
		🔍 COM+ System A	管理		手动	本地系统		E
		🔍 Computer Brow	维护	已启动	手动	本地系统		
	油还:	🔍 Credential Mana	为用		手动	本地系统		
	双脑/车甲订录动术订	Cryptographic S	提供	已启动	自动	网络服务	_	
		🔅 DBAAgent	数据		自动	本地系统		
		Capture DBACapture	数据		自动	本地系统		
		🔅 DCOM Server Pr	DCO	已启动	自动	本地系统		
		🔍 Desktop Windo	提供	已启动	自动	本地系统		
		🔍 dgbased	Devi		自动	本地系统		
		C DHCP Client	为此	已启动	自动	本地服务		
		Diagnostic Policy S	ervice	已启动	自动	本地服务		
		🔍 Diagnostic Servi	诊断	已启动	手动	本地服务		
		🔍 Diagnostic Syste	诊断	已启动	手动	本地系统		
		🔍 Disk Defragmen	提供		手动	本地系统		
		🔍 Distributed Link	维护	已启动	自动	本地系统		
		🔍 Distributed Tran	协调		手动	网络服务		
	ļ	🔍 DNS Client	DNS	已启动	自动	网络服务		Ψ.
	∖扩展√标准/							

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 阀值,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 (7000 ~ 8000)		
CPU阀值	85			
审计端口	1521			
审计接口				
Agent插件下载	windows(Vista及更高)插件下载 ⑦	windows(Server2003/XP)損	<u>純下載</u> ②	linux插件下载 ^⑦
	IP	掩码	操作	
审计IP	127.0.0.1	255.255.255.255	面 删除	
	172.16.1.253	255.255.255.255	面 删除	
		1.5714		

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)

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。





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 阀值,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	7000 ~ 8000)		
CPU阀值	85			
审计端口	1521			
审计接口				
Agent插件下载	windows(Vista及更高)插件下载 ⑦	windows(Server2003/XP)	<u> 插件下载</u> ⑦	<u>linux插件下载</u>
	IP	掩码	操作	
审计IP	127.0.0.1	255.255.255.255	面 删除	
	172 16 1 252	255 255 255 255		

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 阀值设置过小,需要适当调整 CPU 阀值,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

钵信息		模式选择	添加	子库	策略配置
名称	测试库		数据库类型	Oracle	v
类型	集群		版本	11.1.0.2	v
	单库			Transex	
IP	集群		*端口	1521	
服务名	racdb		库优先级		
备注					

1).添加 oracel 集群的数据库防护引擎



×

编辑中显示的 oracle 集群配置。



S称	scanIP-IPv6-rac		类型	集群	*
				•	-
莫式	防火墙	*	接口	br1	*
效据库类型	Oracle	*	版本	11.1.0.1	*
P	172.18.200.231 集群	scanip	<mark>*</mark> 端口	1521	
牧据库(实例)	racdb 集群服务名	\$	库优先级	0	
對注					

2).添加 oracle 集群单节点 IP 的配置。



×

下一步

			添加单库IP
IP1	172.18.200.211		
IP2	172.18.200.212	- +	

在"设置"中可以编辑 oracle 集群节点。

编码	自动探测	~	1				
关联配置 💿	关闭	~					
语句阻断		设置子库					×
监控数据库应答			-			oracle集群中	
影响行辅助			IP1	172.18.200.231	-	的单节点	
邮件告替通知			IP2	172.18.200.212			
模糊化日志			IP3	172.18.200.211	-	+	
Vxlan	$\overline{\mathbf{O}}$						
设置子库 🛈						保存	关闭

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。

MGT E1/1 E1/2 E1/3	E1/4	E2/3 E2/4	
		选择镜像的业 务物理接口	
接口设置 按口组 按口初能 编辑bond组	按个即审计 Doug语按口		×
名称 接口1 1 bond1	E2/1	接口2 E2/2	_
ă	2置bond接口	J	确定取消
MGT E1/1 E1/2 E1/3 E1/4	E2/1 E2/2 E2/3 E2/4		
接口设置 接口組 接口功能 接入即审计 添加	bond组接口		
名称 接口 1 bond1 E2/1,E2/2	IP地址	MASK	操作 乙 编辑 面 删除

2).数据库审计旁路模式 bond 接口调用。

东软 NDBA 数据库安全



模式	审计	*		
接口	bond1	-		