

东软 NetEye 数据库审计系统 用户手册



东软公司



目 录

-,	系	统桌面…		4
二、	系	统管理…		4
	2.1	系统配	置模块	5
		2.1.1		5
		2.1.2	硬件和诊断	. 15
		2.1.3	可靠性设置	. 26
		2.1.4	告警通知	. 31
	2.2	备份还	原模块	. 37
		2.2.1	备份还原	. 37
		2.2.2	数据清理	. 41
_	ф.,	人可里		
二、	女	王能直…		. 44
	3.1	数据库	引擎管理	. 44
		3.1.1	添加	. 44
		3.1.2	删除	. 45
		3.1.3	编辑	. 46
		3.1.4	自动发现	. 47
		3.1.5	审计防火墙	. 48
		3.1.6	状态监控	. 52
		3.1.7	风险扫描	. 53
		3.1.8	操作	. 55
	3.2	数据库'	审计与防火墙	. 57
		3.2.1	审计防火墙	. 57
		3.2.2	策略中心	. 74
		3.2.3	最新流量	. 94
	3.3	设备和	敏感数据扫描	. 95
		3.3.1	模块构成	. 96
		3.3.2	服务扫描	. 96
		3.3.3	数据扫描	106



		3.3.4	服务发现	113
		3.3.5	数据发现	119
	3.4	风险扫	描	126
		3.4.1	添加风险扫描	126
		3.4.2	引擎列表	127
		3.4.3	数据库风险扫描	127
	3.5	数据库	状态监控	135
		3.5.1	添加数据库状态监控	135
		3.5.2	引擎列表	136
		3.5.3	概况	137
		3.5.4	配置	147
		3.5.5	<u> </u>	148
		3.5.6	记录	151
	3.6	运维审	计	152
		3.6.1	FTP 引擎列表	152
		3.6.2	规则列表	154
四、	检	索和报表	₹	155
	4.1	审计检	索(检索)	155
	4.1	审计检 4.1.1	索(检索) 数据库审计检索	155 156
	4.1	审计检 4.1.1 4.1.2	索(检索) 数据库审计检索 FTP 检索	155 156 187
	4.1 4.2	审计检 4.1.1 4.1.2 报表…	索(检索) 数据库审计检索 FTP 检索	155 156 187 189
	4.1 4.2	审计检 4.1.1 4.1.2 报表… 4.2.1	索(检索) 数据库审计检索 FTP 检索 报告	155 156 187 189 189
	4.1 4.2	审计检 4.1.1 4.1.2 报表… 4.2.1 4.2.2	索(检索) 数据库审计检索 FTP 检索 报告 报告结果	155 156 187 189 189 203
五、	4.1 4.2 其	审计检 4.1.1 4.1.2 报表 4.2.1 4.2.2 他模块和	索(检索)数据库审计检索	155 156 187 189 189 203 203
五、	4.1 4.2 其 5.1	审计检 4.1.1 4.1.2 报表 4.2.1 4.2.2 他模块和 监控	索(检索)数据库审计检索	155 156 187 189 203 203 203
五、	4.1 4.2 其 5.1	审计检 4.1.1 4.1.2 报表 4.2.1 4.2.2 他模块 和 5.1.1	索(检索)	155 156 187 189 203 203 203 203
五、	4.1 4.2 其 5.1	审计检 4.1.1 4.1.2 报表 4.2.1 4.2.2 他模块和 5.1.1 5.1.2	索(检索)数据库审计检索	155 156 187 189 203 203 203 203 203 204
五、	4.1 4.2 其 5.1	审计检 4.1.1 4.1.2 报表 4.2.1 4.2.2 他模块 5.1.1 5.1.2 5.1.3	索(检索)	155 156 187 189 203 203 203 203 204 205
五、	4.1 4.2 其 5.1	审计检 4.1.1 4.1.2 报表 4.2.1 4.2.2 他模 控 5.1.1 5.1.2 5.1.3 5.1.4	索(检索)	155 156 187 189 203 203 203 203 203 204 205 206
五、	4.1 4.2 其 5.1	审计检 4.1.1 4.1.2 报表 4.2.1 4.2.2 他模 控 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5	索(检索)	155 156 187 189 203 203 203 203 204 205 206 207
五、	4.1 4.2 其 5.1	审计检 4.1.1 4.1.2 报表 4.2.1 4.2.2 他 监1.1 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5 面	索(检索)	155 156 187 189 203 203 203 203 203 204 205 206 207 207
五、	 4.1 4.2 其 5.1 5.2 	审计检 4.1.1 4.1.2 报表 4.2.1 4.2.2 他模 控 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5 面 5.2.1	索(检索) 数据库审计检索	155 156 187 189 203 203 203 203 204 205 206 207 207 208



	5.2.3	SecAdmin 用户管理	213
5.3	告警		214
	5.3.1	数据库告警	214
	5.3.2	FTP 告警	218
5.4	系统审	计	219
	5.4.1	审计防火墙操作日志管理	219
	5.4.2	日志	220



一、 系统桌面

本系统登录后的桌面布局大致如下图,具体功能模块可能随授权许可的具体情况而有增减变化。

Neusoft



二、 系统管理

系统管理包括 license 授权、时间配置、服务配置、系统监控、系统告警、用户安全设置、数据库授权、升级、接口配置、路由配置、接口功能、关机和重启、BYPASS 设置、双机热备、告警通知、备份还原等。主要操作用户为 SysAdmin。



2.1 系统配置模块

2.1.1 系统配置

在系统配置的首页显示当前的系统版本信息,如下图所示:

备份还原	系统配置	
系统配置		系统配置
LICENSE授权		点击左面的导航菜单进行相应的操作。
时间配置		1012011020
服务配置		ACONTROO
系统监控		本版本发布更新时间: 2016-05-14 12:49
系统告警		
用户安全设置		
数据库授权		
升级		

2.1.1.1 LICENSE 授权

在 LICENSE 授权页面,可进行授权操作。

用户能够从"当前系统状态"栏中查看到系统是否已经授权,以及具体的授权模块等信

息。



系统配置	LICENSE授权						
LICENSE授权	机器的SN码	03010100101163160024	↓ 获取机器信息				
时间配置	激活文件	选择文件 +	✔ 授权激活				
服务配置							
系统监控	当前系统优态						
系统告警	系统状态:	已授权!					
用户安全设置	系统到期时间:	2016-08-13 14:57:43					
勬据库授 权	授权模块:	状态监控,风险扫描,运维审计,设备数据发现,审计防火墙,					
升级							

2.1.1.2 时间配置

在时间配置模块,用户可以设置系统时间和 NTP 服务器时间的自动同步。

备份还原系统配	置			
系統配置	时间配置			
LICENSE授权	日期和时间			
时间配置	系统时间	2016-05-17 18:12:15		
服务配置	📚 更新系统时间	🔮 注意:修改或同步时间可能导致浏览器当前的页面会话失效,设置后需要重新登录系统。		
系统监控	时间服务器1			
系统告警	IP			
用户安全设置	靖口	123		
数据库授权	自动同步			
升级				
硬件和诊断	□ 保仔 □ 同步 □ 江息:设置"目动同步"后,系统会每大和时间服务器问步一次.			
接口设置	时间服务器2			
路由设置	IP			
接口功能	靖口	123		
关机和重启	自动同步			
可靠性设置	● 保存 △ 同步 💡 注意:设置	望"自动同步"后,系统会每天和时间服务器同步一次。		
BYPASS设置				

当您需要修改系统日期时,请单击时间框的右侧"日历"按钮。此时,将弹出一个微型 日历。您可以点击选择年、月、日或点击"今天"按钮选择当前操作系统的时间。然后点击 "更新系统时间"按钮,即可实现时间的自定义设置。



时间配置								
日期和时间								
系统时间	201	6 -0 5	-17 1	8:12	:15	17,		_
📚 更新系统时间	₩	•	五二	月 20 三	016 四	五	+ + 六	
时间服务器1	24 1	25 2	26 3	27 4	28 5	29 6	30	
IP	8	9	10	11	12	13	14	
端口	15 22	16 23	17 24	18 25	19 26	20 27	21 28	
自动同步	29	30	31	1	2	3	4	
🗎 保存	18: 今月	12:18 E	5 🔇	确定	-		关闭	<mark>涛器同步一次.</mark>

在时间服务器中,用户可设置 NTP 服务器的 IP 地址及服务端口(默认端口 123)。设置 后要点击"保存"按钮进行保存。点击"同步"按钮则会从相应的 NTP 服务器进行时间同步。 勾选"自动同步"后,设备将每天定时自动从相应 NTP 服务器进行时间同步。且支持 NTP 主备服务配置。



时间服务器1	
IP	
山	123
自动同步	
■ 保存 ● 同步 ● 同步 ● 注意:	:设置"自动同步"后,系统会每天和时间服务器同步一次.
时间服务器2	
IP	
端口	123
自动同步	
🖹 保存 🔷 同步 💡 注意:	:设置"自动同步"后,系统会每天和时间服务器同步一次.

2.1.1.3 服务配置

服务配置包括 DNS 配置,WEB 配置、SSH 配置三个部分。



备份还原 系	統配置	
系统配置	服务配置	
LICENSE授权	DNS 配置	
时间配置	DNS服务器 1	
服务配置	DNS服务器 2	
系统监控	DNS服务器 3	
系统告警	WEB 配置	
用户安全设置		 完全访问
数据库授权	访问权限	◎ 禁止远程访问 💡 所有远程WEB均不可接入服务器,需SSH或主机操作解除。请谨慎选择!
升级		◎ IP白名单访问
硬件和诊断	服务端口	443 * (1~65535)
接口设置	SSH 配置	
路由设置		
接口功能	1/JIPI/XPR	 ● 禁止还怪切问 ① IP白名单访问 ● IP白名单访问
关机和重启	服务端口	22 * (1~65535)
可靠性设置	■ 保存并生効	
BYPASS设置	E MUTTA	

在 DNS 配置中,可指定三个 DNS 服务器地址,填写后用"保存并生效"按钮保存设置。

DNS 配置	
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 访问控制。选项包括"完全访问"、"禁止远程访问"、"IP 白名单访问" 三个选项。其中"IP 白名单访问"选项需自定义 IP 地址集。如果本系统的 WEB 服务端口被更改,需在服务端口栏将端口修改为被设定的端口值,如下图所示:



WEB 配置	
访问权限	 完全访问 禁止远程访问 新有远程WEB均不可接入服务器,需SSH或主机操作解除。请谨慎选择! IP白名单访问
服务端口	443 * (1~65535)
IP地址集	注:IP之间请使用英文逗号 *,* 分隔。

修改配置后需点击"保存并生效"按钮保存配置。

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"、"禁止远程 访问"、"IP 白名单访问"三个选项。其中"IP 白名单访问"选项需自定义 IP 地址集。如 果本系统的 SSH 服务端口被更改,需在服务端口栏将端口修改为被设定的端口,如下图所示:

SSH 配置	
访问权限	 ● 完全访问 ● 禁止远程访问 ● 新有远程SSH均不可接入服务器,需WEB或主机操作解除。请谨慎选择! ● IP白名单访问
服务端口	22 * (1~65535)
IP地址集	注:IP之间请使用英文逗号 "," 分隔。
🗎 保存并生效	

2.1.1.4 系统监控

系统监控页面分为系统资源和网卡运行信息两个部分,包括设备的 CPU、内存、交换分 区、磁盘监控曲线图,以及接口信息(MAC 地址、IP 地址、接收和发送数据信息等)。如下 图所示:





2.1.1.5 系统告警

系统告警页面可以查看设备运行状态的告警详细信息,包括"发生时间"、"日志类型"、 "状态"、"时间级别"、"事件内容"、"处理备注"等。在系统告警页面还可以进行处理告警, 和删除告警操作。

系	系统告答							
*	✔ 处理 💼 告警删除							
		发生时间	日志类型	状态	事件级别	事件内容		
1		2016-05-16 10:43:37	应用	未处理	警告	数据库审计防火墙停止完成。。。		
2		2016-05-16 10:44:38	应用	未处理	警告	数据库审计防火墙启动完成。。。		
з		2016-05-16 22:00:00	CPV	未处理	严重	严重: CPV使用量在95%到98%之间		
4		2016-05-17 17:46:19	应用	未处理	警告	数据库审计防火墙停止完成。。。		
5		2016-05-17 17:47:54	应用	未处理	警告	数据库审计防火墙启动完成。。。		
6		2016-05-20 21:00:00	CPU	未处理	警告	警告: CPV使用量在90%到95%之间		



2.1.1.6 用户安全设置

通过用户安全设置页面,用户可进行"登录安全参数"、"密码长度参数"、"密码过期参数"、"下载文件密码"的设置。设置后需点击"保存"按钮进行保存。

备份还原	系统配置	
系统配置	用户安全设置	
LICENSE授权	登录安全参数	60 🗸 秒之内,用户尝试登录的失败次数超过 3 🗸 次,锁定该用户 1 🗸 分钟
时间配置		
服务配置	密码长度参数	密码最短长度 8 🗸 密码最长长度 30 🗸
系统监控		
系统告警	系统告警 家码过期参数	状态 ◎ 启用 ⑧ 禁用
用户安全设置		密码过期时间 30 天(时间只能为正整数,且不超过365天)
数据库授权		
升级	下载文件密码	打开导出或下载的文件时,所需密码:长度6~20字符或不填写;
硬件和诊断	■ 保存	
接口设置		
路由设置		

登录安全参数设置在规定时间内用户输入错误密码的次数,如果超出规定次数,则将该用户锁定一段时间。默认为 1min 内,用户连续 3 次密码输入错误则将该用户锁定 1 分钟。

用户安全设置				
登录安全参数	60 🗸 秒之内,用户尝试登录的失败次数超过 3 🗸 次,锁定该用户 1 🗸 分钟			
通过密码长度	逐参数可设定密码的长度范围。			
密码长度参数	密码最短长度 1 🗸 密码最长长度 21 🗸			

密码过期参数的设置可控制密码的有效期。



密码过期参数	状态 ◎ 启用 ● 禁用 密码过期时间 30 天 (时间只能为正整数,且不超过365天)		
设置下载文件密码后,下载报告等文件后解压相应压缩包时需输入密码。			
下载文件密码	•••••• 题 7开 导出或下载的文件时,所需密码;长度6~20字符或不填写;		

2.1.1.7 数据库授权

系统以具备一定权限的远端用户账号访问数据库,读取数据库相应信息,来支持状态监控和风险扫描功能。数据库授权页面提供 ORACLE、SQLSERVER 等数据库的授权脚本下载,供数据库 DBA 创建一定权限的数据库用户,开放给数据库审计产品,用于数据库状态监控和风险扫描。

备份还原	系统配置			
系统配置	请下载所需数据库类型授权			
LICENSE授权	数据库类型	描述		
时间配置	ORACLE	状态监控支持。		
肥冬两罢	SQLSERVER	状态监控支持。		
版方自由	MYSQL	状态监控支持,风险扫描不支持。		
系统监控	SYBASE	状态监控支持,风险扫描不支持。		
系统告警	INFORMIX	状态监控支持,风险扫描不支持。		
用户安全设置	DAMENG7	状态监控支持,风险扫描不支持。		
数据库授权				
升级	下载的SQU脚本,由	下载的SQL脚本,由数据库DBA管理员执行,并创建有权限用户,本系统相应模块使用该用户;		
硬件和诊断	请详看脚本说明。			

Neusoft

如下图所示:

-- please replace all the username and password to yours. create user c##username identified by password; grant connect to c##username; -- dbmon grant select on v_\$instance to d#Ausername; grant select on v_\$database to d#Ausername; grant select on v_\$eession to d#Ausername; grant select on v_\$eession to d#Ausername; grant select on v_\$galarea to cd#Ausername; grant select on v_\$filestat to d#Ausername; grant select on v_\$filestat to d#Ausername; grant select on v_\$filestat to d#Ausername; grant select on vy\$filestat to d#Ausername; grant select on vy\$filestat to d#Ausername; grant select on vy\$filestat to d#Ausername; grant select on vy\$gastat to d#Ausername; grant select on v_\$ggast to d#Ausername; grant select on v_\$ggast to d#Ausername; grant select on v_\$ggast to d#Ausername; grant select on v_\$gastat to d#Ausername; grant select on v_\$gastat to d#Ausername; grant select on v_\$ibiraryvache to d#Ausername; grant select on sys.dba_temp_files to d#Aus -- dbmon grant select on sys.dba_free_space to c##username; grant select on v_\$log to c##username; grant select on v_\$log file to c##username; grant select on v_\$session, wait to c##username; grant select on vy.\$session, wait to c##username; grant select on sys.dba_rollback_segs to cc##username; grant select on dba_blockers to c##username; grant select on dba_vaiters to c##username; grant select on dba_vaiters to c##username; grant select on u_\$ratters to c##username: grant select on u_\$rattaname to c##username; grant select on u_\$rilestat to c##username; grant select on v_\$rilestat to c##username; grant select on v_\$rollstat to c##username; grant select on v_\$rollstat to c##username; grant select on v_\$rollstat to c##username; -- scan -- scan grant select on sys.user\$ to c##username; grant select on t_bus_pswconf_code_user to c##username; grant select on sys.link\$ to c##username; grant select on v\$ession to c##username; grant select on dba_role_privs to c##username; grant select on dba_profiles to c##username; grant select on dba_audit_session to c##username; grant select on dba_users to c##username; grant select on v\$parameter to c##username; grant select on dba_roles to c##username; grant select on dba_tab_privs to c##username;

- grant select on dba tables to c##username
- grant select on v\$license to c##username; grant select on dba_indexes to c##username

2.1.1.8 升级

通过升级页面,用户可升级系统补丁包。

点击"手动导入升级文件"弹出导入升级文件的窗口,点击"+"按钮,选择升级文件路 径,点击"上传"。点击"升级"。弹出确认窗口,点击"确定",系统进入升级状态。

在升级页面,用户可以查看到升级记录,包括:时间、概要和详细描述。



数据库与应用安全加固系统					
备份还原系	统配置				
系统配置	升级				
LICENSE授权	◆ 手动导入升级文件 ③ 升级				
时间配置	升级记录				
服务配置	时间				
系统监控	导入升级文件 🛛				
系统告警	C:\fekeneth\VDSR01_VDSR01_030_+··· + ★ 上传				
用户安全设置					
数据库授权					
升级					
硬件和诊断					
接口设置					



2.1.2 硬件和诊断

2.1.2.1 接口设置

通过接口设置页面能够查看到接口状态,包括接口名、接口地址、启用状态等信息,如 下图所示:



设	设备接口扰态						
2	2 刷新						
	接口名	接口地址	启用状态				
1	enpO	44:8a:5b:f4:5f:63	连接				
2	enp1	d8:cb:8a:ab:d0:0a	连接				
3	enp2	d8:cb:8a:ab:d0:0b	断开				
4	enp3	d8:cb:8a:ab:d0:0c	连接				
5	enp4	d8:cb:8a:ab:d0:0d	连接				
6	enp5	44:8a:5b:3e:cd:46	断开				
7	enp6	44:8a:5b:3e:cd:47	断开				
8	enp7	44:8a:5b:3e:cd:48	断开				

旁路审计设置

在旁路审计设置中能够添加、删除和编辑旁路审计接口。如下图所示:

旁路审计设置						
🕂 添加 💼 删除 🥒 编辑						
接口名	IP地址	掩码	网关			
1 enp1						

添加审计接口

点"添加"按钮,弹出旁路审计端口设置窗口,选择相应的接口,依次填写 IP 地址,掩 码, 网关。点击"确定"按钮进行保存。

旁路审计端口设	置
接口名	《 该输入项为必输 《
IP地址	enp2 enp3
掩码	enp4 enp5
网关	enp6 enp7
♀ 多个IP地 写,如2个	enp8 时 : 192.168.1.200/192.168.1.201
	✓ 确定 業 取消



提示:

1、IP 地址、掩码、网关为可选填写。

2、在完成上述步骤后需要点击右侧"保存"按钮,否则所做配置不生效。

删除审计接口

选中相应的审计接口,点击"删除"按钮,弹出确认窗口,单击"确定"即可成功删除 相应审计接口。

确认		X	
④ 确定要删除该条记录信息吗?			
	✔ 确定 業 取消		

提示:在完成上述步骤后需要点击右侧"保存"按钮,否则删除不生效。

编辑审计接口

通过编辑审计接口页面,可以通过接口名更改审计接口;并且可以更改 IP 地址、掩码、 网关。选中相应的审计接口,点击"编辑"按钮,弹出旁路审计端口设置窗口,编辑相应信 息,单击"确定"。



旁路审计端口设置							
接口名	enp2 🗸						
IP地址	192.168.60.6						
掩码	255.255.255.0						
网关	192.168.60.2						
 							

提示:在完成上述步骤后需要点击右侧"保存"按钮,否则编辑的配置不生效。

网桥接口设置

防火墙串联部署时需设置网桥接口,通过网桥接口设置页面,能够查看到已添加的网桥 信息,可以进行添加删除等操作。如下图所示:

旁路审计设置 网桥接口设置 其他设置							
网桥接口列表							
★ 添加网桥 面 删除网桥 ➡ 添加接口 面 删除接口							
网桥组编号 网桥IP地址 子网摘码 接口 VLAN 透传状态							

添加网桥

点击"添加网桥"按钮,弹出添加窗口,输入编号、IP地址、子网掩码,点击"确定" 按钮。



网桥组添加	×
网桥组编号	1 (1~255)
网桥IP地址	192.168.50.5
子网掩码	255.255.255.0
	✔ 确定

添加接口和 Vlan 透传

选中相应网桥,点击"添加接口"按钮,弹出网桥组接口设置窗口。点击接口栏的下拉三角按钮,选中相应接口;

网桥组接口设置		×
网桥组编号	br1	
接口	enp3,enp4 🗸	•
VIANID送传	enp2	
VEANIDIAN	enp3	
	enp4	✔ 确定
	enp5	
	enp6	
	enp7	
	enp8	

勾选 VLAN ID 透传的"开启"选项,输入 VLAN 编号,点击"确定"按钮。



网桥组接口设置	
网桥组编号	br1
接口	enp4,enp3 🗸
	 ● 开启 50
VLAN ID透传	接口与VLAN ID透传为完全匹配: 如:接口为A, B, VLAN ID透传为 100,则最终设置为A.100, B.100。
	✔ 确定

提示: 在完成上述步骤后需要点击右侧"保存"按钮, 否则编辑的配置不生效。 删除接口

选中相应网桥,点击"删除接口"按钮,弹出提示窗口。点击"确定"

提示		×
?	确定要删除该网桥的接口信息吗?	
	✔ 确定 🗮 取消	

删除网桥

选中相应网桥,点击"删除网桥"按钮,弹出提示窗口。点击"确定"

提示		
?	确定要删除该网桥信息吗?	
	✔ 确定 業 取消	



提示:

1、在完成上述步骤后需要点击右侧"保存"按钮,否则删除不生效。

2、删除网桥前需先删除接口,否则无法删除网桥。

其他设置

通过其他设置页面,可以设置管理接口和 HA 接口。

旁路审计设置	网桥接口设置 其他设置		6	🔒 保存	
管理口配置					
接口	enp0	✔ 黛 端口不可更改			
IP地址	172.16.1.128	子网掩码	255.255.255.0		
HA口配置 🗌 启					
接口		~			
IP地址		子网掩码			

管理口配置

通过管理口配置项目,可配置管理口的 IP 地址。

管理口配置			
接口	enp0 🗸	💡 端口不可更改	
IP地址	172.16.1.128	子网掩码	255.255.255.0

提示:在完成上述步骤后需要点击右侧"保存"按钮,否则编辑的配置不生效。

HA 口配置

为确保设备的高可用性,系统提供双机热备的功能,正常情况下主机服务运行,备机通 过心跳线监视主机的状态,主机出现问题时,切换到备机上运行,保证审计和防火墙模式能 够正常运行。双机热备需要在主机和从机上都配置 HA 口。



设置 HA 接口:(主机地址和备机地址需是同一网段(如: 主机 192.168.100.100, 备 机 192.168.100.101)

旁路审计设置 网格	桥接口设置 其他设置		□ 保存
管理口配置			
接口	enp0 🗸 🧕	满口不可更改 <u></u>	
IP地址	172.16.1.77	子网掩码	255.255.255.0
HA口配置 🗹 启用			
接口	enp1 🗸	Г	
IP地址	192.168.100.100	子网掩码	255.255.255.0

提示: 个别机型平台 HA 口(如 H61 机型没有单独的 HA 口)可以通过去使用,释放作为业务接口使用。

2.1.2.2 路由设置

系统路由表

通过系统路由表页面,能够查看到路由信息。如下图所示:

ž	系统路由表 静态路由表				
3	刷新				
	目的IP地址	子网掩码	网关	优先级	接口
1	link-local	255. 255. 0. 0	0. 0. 0. 0	1002	enp5
2	link-local	255. 255. 0. 0	0. 0. 0. 0	1003	enp6
3	link-local	255. 255. 0. 0	0. 0. 0. 0	1004	enp7
4	link-local	255, 255, 0, 0	0. 0. 0. 0	1005	enp8
5	link-local	255. 255. 0. 0	0.0.0.0	1006	enp0
6	link-local	255. 255. 0. 0	0.0.0.0	1007	enp1
7	link-local	255, 255, 0, 0	0.0.0	1008	enp2
8	link-local	255. 255. 0. 0	0.0.0.0	1009	enp3
9	link-local	255. 255. 0. 0	0. 0. 0. 0	1010	enp4
10	172.16.1.0	255, 255, 255, 0	0.0.0.0	0	enp0

静态路由表

在静态路由表页面,可以添加、删除和查看静态路由。



+	★ 添加				
	目的IP地址	子网掩码	网关	优先级	
1	172. 17. 200. 0	255. 255. 255. 0	192. 168. 50. 1	60	

添加

点击"添加"按钮,弹出路由添加窗口,输入目的 IP 地址、子网掩码、网关、优先级后 点击"确定"即可成功添加路由。

路由添加		×
目的IP地址	172.17.200.0	
子网掩码	255.255.255.0	
网关	192.168.50.1	
优先级	60	(1~255)
		✔ 确定

删除

选中已添加的路由条目,点击"删除"按钮,弹出提示窗口,点击"确定"即可成功删 除路由。



2.1.2.3 接口功能

通过接口功能页面,可以设置接口模块审计功能。



接口功	複口功能			
┣ 保7	圖 保存并生效			
接	口名	开启的功能(双击此列的单元格可编辑)		
1 eng	pl	Web审计, Ftp审计, Telnet审计, Ync审计, Ssh审计, Smtp审计, Pop3审计, Imap审计, 务路阻断, 数据库审计		
2 eng	p2	Web审计, Ftp审计, Telnet审计, Vnc审计, Snh审计, Sntp审计, Pop3审计, Imap审计, 务路阻断, 数据库审计		
3 eng	p5			
4 eng	26			
5 eng	p7			
6 eng	p8			

示例:开启 enp5 接口的数据库审计功能。

双击 enp5 接口右侧的选框,点击下拉三角,选中添加模块审计项。点击"保存并生效" 按钮。

接	口功能		
E	保存并生效		
	接口名	开启的功能 (双击此列的单元格可编辑)	
1	enpi	数据库审计, 旁路阻断, Inap审计, Pop3审计, Sntp审计, Ssh审计, Ync审计, Telnet审计, Ftp审计, Web审计	
2	enp2	数据库审计, 旁路阻断, Inap审计, Pop3审计, Satp审计, Sah审计, Ync审计, Telnet审计, Ftp审计, Web审计	
3	enp5	数据库审计	~
4	enp6	数据库审计	
5	enp7	旁路阻断	
6	enp8		
		ropom pr Sntp审计	
		Ssh审计	
		Vnc审计	
		Telnet审计	
		Ptp审计	
		Webm)+	

示例: 取消 enp5 接口的数据库审计功能。

双击 enp5 接口右侧的选框,点击下拉三角,将已选中数据库审计选项点掉。点击"保存并生效"按钮。



接	口功能		
B	保存并生效		
	接口名	开启的功能 (双击此列的单元格可编辑)	
1	enpi	Web审计, Ftp审计, Telnet审计, Vnc审计, Ssh审计, Sntp审计, Pop3审计, Imap审计, 旁路阻断, 数据库审计	
2	enp2	Web审计, Ftp审计, Telnet审计, Vnc审计, Ssh审计, Sntp审计, Pop3审计, Inap审计, 旁路阻断, 数据库审计	
3	enp5	· · · · · · · · · · · · · · · · · · ·	2
4	enpő	数据库审计	
5	enp7	旁路阻断	
6	enp8	Imap用计 Pon3面计	
		Smtp审计	
		Ssh审计	
		Vnc审计	
		Telnet#it	
		Ftp#it	
1		Yeb审计	

2.1.2.4 关机和重启

通过关机和重启页面,可对设备进行关机和重启操作。



点击"重启"按钮,弹出确认窗口,点击"确定"

确认	×
3 确定要重启吗?	
✔ 确定	🗙 取消

点击"关机"按钮,弹出确认窗口,点击"确定"





2.1.3 可靠性设置

2.1.3.1 **BYPASS**

BYPASS 保障当设备意外宕机等情形下,作为防火墙串口部署方式不会影响客户端与数据库的连通性,保障业务能够正常进行。通过 BYPASS 设置页面可手动控制 BYPASS 的启用 与停用。

BYPASS设置		
	enp1 点击 <mark>启用</mark> BYPASS enp2	enp3 点击 <mark>启用</mark> BYPASS enp4
	enp5 点击 <mark>启用</mark> BYPASS enp6	enp7 点击 <mark>启用</mark> BYFASS enp8
♀ 1. 拥有管 2. 点击, i 3. 若接口	<mark>理口(C)或14接口(H)的网卡组,不可设置BYPASS状态;</mark> 可进行启用或取消BYPASS状态; 已用于旁路或网桥,设置为BYPASS状态可能产生影响。	Л

示例: 启用 BYPASS

点击"启用"按钮,弹出提示窗口,点击"确定"。相应接口进入 BYPASS 状态,此时 设备不再对相应接口的数据进行审计也不能够实现阻断等功能。





示例:停止 BYPASS

点击"停止"按钮,弹出提示窗口,点击"确定"。相应接口退出 BYPASS 状态,此时 设备恢复对相应接口的数据进行审计,能够实现阻断等功能。

提示		
?	确定要对该组网口 <mark>停止</mark> BYPASS 吗 ?	
	✔ 确定 業 取消	

2.1.3.2 双机热备

为确保设备的高可用性,系统提供双机热备的功能,正常情况下主机上服务运行,备机 通过心跳线监视主机的状态,主机出现问题时,切换到备机上运行,确保数据库防火墙功能 正常运行,同时保障了用户生产环境下的高可用性。

示例: 防火墙模式开启双机热备

 1) 设置 HA 接口:(主机地址和备机地址需同一网段(如:主机 192.168.100.100, 备机 192.168.100.101)



旁路审计设置 网	桥接口设置	其他设置				■ 保存
管理口配置						
接口	enp0		✔ 💡 端口7	下可更改		
IP地址	172.16.1.	.77		子网掩码	255.255.255.0	
HA□配置 ☑ 启用						
接口	enp1		~			
IP地址	192.168.1	100.100		子网掩码	255.255.255.0	

2) 添加网桥(主机和备机都要操作,备机不能自动学习)

旁路审计设置	阿桥接口设置 其他设置			□ 保存
网桥接口列表				
➡ 添加网桥	💼 删除网桥 🛛 🕈 添加接口 🛛 💼	刪除接口		
网桥组编号	网桥IP地址	子网掩码	接口	VLAN 透传状态
1 br1	192. 168. 50. 5	255. 255. 255. 0	enp2, enp3	未开启
				h
3)	添加路由(只在主	机上配置即可)		



数据库与应用安全	加固系统		系统管理员: Syskdmin 🔒 🕅	改密码 🔤 📩 安全退出
备份还原	系统配置			
系统配置	▲ <u>系统路由</u> 表 静态路由表			
LICENSE授权	▶ 添加 💼 刪除			
时间配置	目的IP地址	子网掩码	网关	优先级
服务配置	2 172.16.0.0	255. 255. 255. 0	192. 168. 50. 10	60
系统监控		1		
系统告警				
用户安全设置				
 				
升级				
硬件和诊断				
接口设置				
路由设置				
接口功能				
关机和重启				
可靠性设置				
BYPASS设置				
双机热备				
告警通知				
置酒				

4) 添加并开启数据库引擎(只在主机上配置即可)

数据	库与应用的	全加固系统				安全管理	员: SecAdmin 💼	修改密码 🔤 古 安全	退出
	数据库引	擎 用户管理							
数据库引	擎列表								
+ 添加	∕ 编辑	Q、自动发现							
名称		类型	IP	端口	缺省数据库	审计防火墙	状态监控	风险扫描	操作
172. 17. 20	0.194:3306/	MYSQL	172.17.200.194	3306	mysql	▋ <u>详情</u> 📅 删除	+ 添加	-	× BHES
									-

5) 开启双机热备(只在主机上操作即可,需要勾选网桥端口)



数据库与应用安全加固系	筑			系统管理员:Systemin 🔒 修改密码 📥 安全退出
备份还原系统面	置			
系統配置	双机状态			
LICENSE授权	当前设备	主机	服务状态	O 运行 位置: 主机
时间配置	主机状态	O 运行	备机状态	0 停止
服务配置	双机设置			
系统监控	双机模式	○ 不启用 ◎ 启用双相	ก	
系统告警	HA接口	enp1		
用户安全设置	主机HA接口IP地址	192.168.100.100	💡 不能为空	2,请在"接口设置"页面设置。
数据库授权	备机HA接口IP地址	192.168.100.101	💡 双机状态	下,不可更改。
升级	联动接口选择	enp0 enp	1 🗹 enp2 🖉	enp3 enp4 enp5 enp6 enp7
硬件和诊断				
接口设置	□ 保存			
路由设置				
接口功能				
关机和重启				
可靠性设置				
BYPASS设置				
双机热备				
告警通知				
配置				
SYSLOG				
<				

备注:

 备机能够自动学习数据库引擎等设置(开启双机热备后就学习,并非在主机掉线后 学习);

 备机不能自动学习网桥,需要在主机和备机上都做设置,如果备机没有设置网桥, 会影响到备机对加固点的学习;

3) 主机重新上线后,服务会自动切回主机上运行。



2.1.4 告警通知

2.1.4.1 配置

在告警配置页面可查看已添加的告警条目,并对告警条目进行添加、删除和重新加载等 操作。

告警配置				
🕇 添加 💼 删除 🍣 重新加载				
告警级别	通知类型	类型详细	引擎	
1 中风险	EMAIL	admin_user10datafort.cn(启用)	172.17.200.190:60000/test1	

添加

点击"添加"按钮,弹出新增告警的窗口。通过点击下拉三角符号,选择告警级别、通 知类型、类型详情、引擎等选项,点击"确定"按钮,实现添加告警。

新增告警	
告警级别	中风险
通知类型	EMAIL
类型详情	admin_user1@datafort.cn(启用 🗸
引擎	172.17.200.190:60000/test1 V
	✔ 确定 😫 取消

删除

选中相应告警条目。点击"删除"按钮,弹出确认窗口,点击"确定",即可删除相应告 警条目。





重新加载

点击"重新加载"按钮,对告警条目重新加载。

提示	×
加载成功!	

2.1.4.2 **SYSLOG**

通过 SYSLOG 页面可以查看到已添加的 SYSLOG 条目,实现 SYSLOG 条目的添加、编辑、和删除操作。

SIZTO ()				
★ 添加 / 編組 面前除糸				
IP	端口	发送者标识	状态	
1 172. 17. 200. 103	514	test	启用	

添加与编辑

点击"添加"按钮,弹出新增窗口。输入 IP 、端口、发送标识等参数,选择启用或禁用, 点击"确定"按钮,实现添加。"测试"按钮,能够测试是否成功。



新增 🗵	
IP	172.16.1.127 *
端口	514 * (1~65535)
发送标识	test *
是否启用	● 启用 ○ 禁用
💡 SYSLOG特性,同一网段内均可发送成功。请准确配	
🍸 测试 🖌 确定 🗮 取消	

点击"编辑"按钮,能够对上述添加中设置的参数进行修改。

编辑	
IP	172.16.1.127 *
端口	514 * (1~65535)
发送标识	test *
是否启用	● 启用 ◎ 禁用
♀ SYSL0G特性,同一网段内均可发送成功。请准确配置	
7 测试 🖌 确定 🗮 取消	

删除

点选已添加的条目,点击"删除"按钮,弹出确认窗口,点击"确定"实现删除。





2.1.4.3 邮件

通过邮件页面。可配置邮件服务器地址,发件人等信息。在收件人条目中输入接收告警 信息的管理员的邮件地址;邮件主机条目中输入邮件服务器的 IP 地址;发件人和密码条目中 输入发送邮件账户的相关信息;SMTP 是否验证选择启用或禁用;发送设置中可设置单封邮 件中包含的条数。配置参数后,点击"保存"按钮,保存相关配置。可通过"测试"按钮测 试是否成功。

邮件服务器配置 ⑦				
邮件服务器配置				
收件人	admin_user1@datafort.cn *			
邮件主机	172.17.200.103 *			
发件人	root *			
密码	*			
SMTP是否验证	● 启用 ◎ 禁用			
发送设置				
单封邮件包含	10 条*(1~500)			
□ 保存 ? 测试				



2.1.4.4 **FTP**

通过 FTP 页面,可配置 FTP 服务器地址,上传用户等信息。在状态条目中选择启用或禁用;在 IP 地址条目中输入接收告警信息的 FTP 服务器的 IP 地址,并配置相应的端口信息;用 户名和密码条目中输入上传用户的相关信息;上传目录条目中设置上传到 FTP 服务器的目录; 发送设置中可设置单次包含的条数。配置参数后,点击"保存"按钮,保存相关配置。可通 过"测试"按钮测试是否成功。

FTP服务器配置 ⑦	
FTP服务器配置	
状态	● 启用 ○ 禁用
IP地址	172.17.200.194 * 端口21 * (1~65535)
用户名	user1 *
密码	*****
上传目录	/pub *
发送设置	
单次包含	10 条* (1~500)
□ 保存	

2.1.4.5 **SNMP**

通过 SNMP 页面,设置 SNMP 服务器地址等信息。在状态条目中选择启用或禁用;在 IP 地址条目中输入 SNMP 服务器的 IP 地址,并配置相应的端口信息;OID 和 MIB 中输入相


关信息(默认 OID 条目为 public);发送设置中可设置发送类型为"发送统计信息"或"发送单条"。配置参数后,点击"保存"按钮,保存相关配置。可通过"测试"按钮测试是否成功。

SIMP服务器配置 ⑦					
SNMP服务器配置					
状态	● 启用 ○ 禁用				
服务器IP地址	* 端口162 * (1~65535)				
OID	public *				
MIB	.1.1.1.1.1.1.1.1.1 *样例: .1.1.1.1.1.1.1.1.1 (1可替换数字)				
发送设置					
发送类型	◎ 发送统计信息 ⑧ 发送单条				
 ♀ SNMP特性,同一网络内均可发送成功。请准确配置! ■ 保存 ⑦ 测试 					

2.1.4.6 短信

通过短信页面,配置短信服务器地址等信息。在状态条目中选择启用或禁用;在 IP 地址 条目中输入服务器的 IP 地址,并配置相应的端口信息;发送设置中可设置单次包含的条数及发 送格式。配置参数后,点击"保存"按钮,保存相关配置。可通过"测试"按钮测试是否成 功。



短信接口配置 🕜	
短信接口配置	
状态	● 启用 ○ 禁用
服务器IP地址	* 端口18259 *(1~65535)
发送设置	
单次包含	10 条*(1~500)
发送格式	13811112222# ✓ 格式:目标手机号#信息内容;支持单一手机发送!
🗎 保存 🍸 测试	t

2.2 备份还原模块

2.2.1 备份还原

备份还原 系统	配置				
备份还原	自动备份				
自动备份	是否开启自动备份	◎ 是 ● 否			
手动备份	在每天的	1	(0~23)点进行备份 ,存放位置: backu	lb.	
FTP备份	■ 保存				
备份还原	备份文件列表				
数据清理	备份文件名	备份时间	备份耗时(s]数据结束时间	备份文件大小 备份方式 文件状态 最后一次恢	夏
备份文件清理					
自动清理					
恢复出厂设置					



2.2.1.1 自动备份

通过自动备份页面可设置是否开启自动备份功能,以及自动备份的时间和存放位置。在 备份文件列表中可以查看到自动备份所生成的备份文件。

自动备份			
是否开启自动备份	◎是 ◎否		
在每天的	1	(0~23)点进行备份,存放位置: backup)
备份文件列表			
备份文件名	备份时间	备份耗时(s. 数据结束时间	备份文件大小 备份方式 文件状态 最后一次恢复

2.2.1.2 手动备份

通过手动备份页面可进行手动备份,在备份文件列表中可以查看到所生成的备份文件。 包括备份文件名、备份时间、备份耗时、数据结束时间、备份文件大小、备份方式、最后一 次恢复等信息

手动备份							
■ 备份							
备份文件列表							
备份文件名	备份时间	备份耗时(s	数据结束时间	备份文件大小	备份方式	文件状态	最后一次恢复
manuBackup_20160517135011_9650.t	<pre>« 2016-05-17 13:50:11</pre>	1054.818	2016-05-17 13:50:11	5286. 571718	手动备份	未上传	

2.2.1.3 FTP 备份

在 FTP 备份页面中,可设置是否开启 FTP 备份,设置备份文件上传时间等,如下图:



m酒器								*
状态	◎ 启用 ⑧ 禁用							
自动上传	在每天的 1		(0~23) 点 , 自动上	传 2		(1~365)天以前的	备份文件。	
FTP服务器IP								
FTP服务器端口	21							
登录FTP的用户名		♀需要	具有创建和删除文	4和文件夹的权限的	的用户			
登录FTP的密码								
上传文件存放在FTP上的目 录		(为空即)	TP服务器跟路径)					
■保存 7 測试								
备份文件列表								
备份文件名	备份时间	备份耗时(数	据结束时间	备份文件大/备份)	方式 文件状态	最后一次恢复	操作 🝞	
manuBackup_20160517135011_96	2016-05-17 13:50:11	1054.818 20	16-05-17 13:50:11	5286.571718 手动者	备伤 未上传		↑ <u>上传</u>	

状态:选择启用和禁用。

自动上传:设置每天上传的时间,及上传的内容。

FTP 服务器 IP:设置备份文件所上传存放的 FTP 服务器的 IP 地址。

FTP 服务器端口: FTP 服务器所开启的 FTP 服务的端口, 默认为 21。

登录 FTP 的用户名: 登录 FTP 服务器所用的用户名,该用户需要具有创建和删除文件及 文件夹的权限。

登录 FTP 的密码:登录 FTP 服务器的用户所对应的密码。

上传文件存在在 FTP 上的目录: 文件在 FTP 服务器上的存放位置。

"保存"和"测试"按钮

通过"保存"按钮保存以上配置。通过"测试"按钮测试是否能够成功登录 FTP 服务器。 成功则在右下角弹出成功提示窗口



提示	×
操作成功!	

失败则在屏幕中央提示错误。

错误
操作过程出错,此次操作无效!
登录ftp服务器失败!
✔ 确定

备份文件列表

在备份文件列表中可以查看到所生成的备份文件。包括备份文件名、备份时间、备份耗时、数据结束时间、备份文件大小、备份方式、最后一次恢复等信息。并且通过操作栏的"上传"按钮可将相应的备份文件上传至相应的 FTP 服务器。

备份文件列表						
备份文件名	备份时间	备份耗时(数据结束时间	备份文件大/备份方式文件状态 最后一次恢复	操作 🝞	
manuBackup_20160517135011_96	2016-05-17 13:50:11	1054.818	2016-05-17 13:50:11	5286.571718 手动备伤 未上传	◆ <u>上传</u>	

2.2.1.4 备份还原

通过备份还原页面,可进备份查询,可以"备份方式"、"备份日期"、"备份文件存放的 目录"三个条件进行筛选查询,筛选后符合条件的备份文件将会显示在备份文件列表中。通 过备份文件所对应的"还原"按钮进行还原。



备份查询								
备份方式	◎ 自动备份 ⑧ 手动會	酚						
备份日期		17:	17					
备份文件存放的目录	backup							
Q 查询 正 重置								
								_
备份文件列表								
备份文件名	备份时间	备份耗时(数据结束时间	备份文件大	备份方式 文件状态	最后一次恢复	操作 🕐	
manuBackup_20160517135011_96	2016-05-17 13:50:11	1054.818	2016-05-17 13:50:11	5286. 571718	手动备伤 未上传		🌑 <u>还原</u>	

2.2.2数据清理

2.2.2.1 备份文件清理

通过备份文件清理页面,可进备份查询,可以"备份方式"、"备份日期"、"备份文件存 放的目录"三个条件进行筛选查询,筛选后符合条件的备份文件将会显示在备份文件列表中。 可通过备份文件所对应的"删除"按钮行删除。

备份方式	◎ 自动备份 ◎ 手动會	昏份					
备份的日期		2 📆		12-			
备份文件存放的目录	backup						
Q. 查询							
备份文件列表							
备份文件复	备份时间	备份耗时	(数据结束时间	备份文件大	备份方式文件状态	最后一次恢复	操作 🝞
BUXUTE							



2.2.2.2 自动清理

通过自动清理页面,可对文件系统默认配置和每日自动清理配置进行设置。

文件系统默认配置	
配置	当文件系统达到 80 %时,存储系统将执行 审计停止写入 🗸 操作。
每日自动清理配置	
每日自动清理	◎ 启用 ● 禁用 💡 启用后,系统在每天的0点开始清理
在线数据可占有文件系统的最大比例是	80 %
	☑ 备份系统并上传所有备份文件
如果大干此没定值系统将自动产生告警并	🗹 清理系统业务数据 🗌 🖓 扫描、检索、报表中的数据,配置信息不处理,如引擎、策略等
	☑ 清理系统配置数据 ♀ 系统监控、系统报警、告警配置的信息
	删除3个月以前的审计日志
冒 保存	

文件系统默认配置

通过文件系统默认配置,可设置当文件系统达到一定百分数时,存储系统执行"审计停止写入"或是"覆盖最早的记录"操作。

文件系统默认配置						
配置	当文件系统达到 80	%时,	存储系统将执行	审计停止写入	~	操作。
				审计停止写入		
母日日动育理院直				覆盖最早记录		

每日自动清理配置

通过每日自动清理配置,可设置是否开启此功能,以及在线数据可占有文件系统的最大 比例;如果大于此设定值系统将自动产生告警并执行那些操作。



每日自动清理配置	
每日自动清理	◎ 启用 ⑧ 禁用 🔮 启用后,系统在每天的0点开始清理
在线数据可占有文件系统的最大比例是	80 %
如果大于此设定值系统将自动产生告警并	 ✓ 备份系统并上传所有备份文件 ⑦ 开启此功能需要确保远程(FTP)页面中的ftp配置可用 ✓ 清理系统业务数据 ⑦ 扫描、检索、报表中的数据,配置信息不处理,如引擎、策略等 ✓ 清理系统配置数据 ⑦ 系统监控、系统报答、告答配置的信息 ✓ 删除3个月以前的审计日志 ⑦ 删除3个月以前的审计日志
周 保存	

每日自动清理:设置是否启用。

在线数据可占有文件系统的最大比例是: 设置相应的百分值。 如果大于此设定值系统将自动产生告警并: 选取所需要执行的操作。

提示:所做的配置需要点击"保存"按钮进行保存,否则不能生效。

2.2.2.3 恢复出厂设置

通过恢复出厂设置页面可以进行清理系统配置数据、清理系统业务数据、恢复出厂设置 操作。

恢复出厂设置	
清理系统配置数据	♣ 清理系统管理数据 ♥ 系统配置数据主要包括:系统监控、系统报答、告答配置的信息
清理系统业务数据	★ 清理系统业务数据
恢复出厂设置	⑦ 恢复到出厂时的设置 ⑦ 恢复出厂设置:此操作将删除系统所有数据,恢复到出厂时的状态,请谨慎操作!

系统配置数据主要包括:系统监控、系统报警、告警配置的信息。 系统业务数据主要包括:扫描、报表中的数据,配置信息不处理,如引擎、策略等。



恢复出厂设置:此操作将删除系统所有数据,恢复到出厂时的状态,请谨慎操作! 警告:以上操作将会更改已做的系统配置等,请谨慎点击。

三、 安全配置

安全配置主要包括添加数据库引擎、配置并开启审计或防火墙功能等。主要操作用户为 SecAdmin,主要模块包括"通用配置"、"数据库审计与防火墙"、"设备和敏感数据扫描"、 "风险扫描"、"数据库状态监控"等。

3.1 数据库引擎管理

所要审计保护的数据库被称为引擎。在使用数据库审计、防火墙以及数据库状态监控、 风险扫描等功能前首先需要添加数据库引擎信息。包括数据库 IP、端口、类型、缺省数据库 等。添加数据库引擎,需 SecAdmin 用户在"通用配置"模块进行操作

3.1.1 添加

进入"通用配置"模块的"数据库引擎"页面,点击"添加"按钮,弹出添加引擎窗口, 如下图所示:



 名称 172.17.200.191:5236/DAME IP 172.17.200.191 端口 5236 类型 达梦7 ✓ 缺省数据库 DAMENG 缺据库的默认端口: [Oracle 1521] [SQL S erver 1433] [DB2 50000] [MySql 3306] [S ybase 5000] [达梦 5236] 	添加引擎	E
IP 172.17.200.191 端口 5236 类型 达梦7 ✓ 缺省数据库 DAMENG	名称	172.17.200.191:5236/DAME
端口 5236 类型 达梦7 ✓ 缺省数据库 DAMENG	IP	172.17.200.191
类型 达梦7 ✓ 缺省数据库 DAMENG 愛 数据库的默认端□: [Oracle 1521] [SQL S erver 1433] [DB2 50000] [MySql 3306] [S ybase 5000] [达梦 5236]	端口	5236
缺省数据库 DAMENG	类型	达梦7 🗸
爱据库的默认端□: [Oracle 1521] [SQL S erver 1433] [DB2 50000] [MySql 3306] [S ybase 5000] [达梦 5236]	缺省数据库	DAMENG
2. 福宁		

名称: 名称可以根据填写的引擎信息自动生成,建议根据本引擎数据库功能用途手动改 写名称以便区分。

IP: 所要审计保护的数据库 IP 地址。

端口:系统显示为各数据库默认端口号,在实际配置中请按照环境情况填写。

类型:系统所支持的所有数据库类型,根据情况选择所审计保护的数据库类型。

缺省数据库:即数据库实例名,系统显示为各数据库默认实例名;根据实际情况填写数 据库实际实例名。

3.1.2 删除

点击需要删除的引擎的 "删除引擎"按钮,弹出 "提示"窗口,点击确定即可删除





提示:当数据库引擎正在被"审计防火墙"、"状态监控"、"风险扫描"之中的任一模块 所使用,则不能删除,需要先停止使用方可删除。

3.1.3 编辑

点选需要编辑的引擎,点击"编辑"按钮,弹出编辑引擎窗口,编辑需要修改的信息, 点击"确定"



数据库引擎 用户管理						
数据库引擎列表						
🕇 添加 📝 编辑 🔍 自动发现	R					
名称	类型		IP		端口	缺省数据库
172.17.200.190:60000/test1	DB2		172.17	7. 200. 190	60000	test1
172.17.200.194:3306/testdb	MYSQL		172.17	7. 200. 194	3306	testdb
192.168.0.98:3306/mysql	MYSQL		192.16	88.0.98	3306	mysql
172.17.200.193:1521/oracle	ORACLE		172.17	7. 200. 193	1521	oracle
172.17.200.20:1521/orcl	ORACLE		172.17	7. 200. 20	1521	orcl
172.17.200.191:5236/DAMENG	达梦7		172.17	7. 200. 191	5236	DAMENG
	编辑引擎		X			
	名称	172.17.200.191:5236/DA	MEN			
	IP	172.17.200.191				
	端口	5236				
	缺省数据 库	test1				
		*	确定			

提示:当数据库引擎正在被"审计防火墙"、"状态监控"、"风险扫描"之中的任一模块 所使用,则不能进行编辑,需要先停止使用方可编辑。

3.1.4 自动发现

点击 "自动发现"按钮,弹出自动发现窗口,输入起始和结束 IP 及端口,点击 "扫描" 按钮,扫描结束后,扫描到的引擎会被自动加入到数据库引擎列表中。



自动发现						×
起始IP	172.17.200.193			起始端口	3306]
结束IP	172.17.200.194]	结束端口	3309	
扫描完成! [172.17.200. [172.17.200. [172.17.200. [172.17.200. [172.17.200. [172.17.200. [172.17.200. [172.17.200. [172.17.200. 开始扫描	194] : [3309] 194] : [3308] 194] : [3307] 194] : [3306] 193] : [3309] 193] : [3308] 193] : [3307] 193] : [3306]	: 无法法 : 无无法 : 无无法 : 无无法 : 无无法 : . 无法	接接接功接接接接 已添	加到引擎中!		
						Q 扫描

3.1.5 审计防火墙

在使用数据库审计或防火墙功能时首先需要添加数据库引擎,添加数据库引擎后添加审 与防火墙功能。若设备为旁路部署则使用审计功能,同时需要选择镜像数据库的来源接口; 若设备串联在网络中则使用防火墙功能。详细配置需结合"数据库审计与防火墙模块"

点击数据库引擎所对应的"审计或防火墙"的"添加"按钮,弹出添加审计或防火墙窗 口,如下图所示:



甲叶的入垣	状态监控	风险扫描	操作
■ <u>〕 详情</u> 📅 删除	+ 添加	📑 逆情 🛛 📅 删除	🗙 删除引擎 🌱 测试连接
▋ <u>〕 谨情</u>	III <u>详情</u> 📅 删除	-	🗶 删除引擎 🌱 测试连接
▋ <u>〕 〕</u> 〕 〕 〕 〕 〕 〕 □ □ □ □ □ □ □ □ □ □ □ □	+ 添加	-	🗙 删除引擎 🌱 测试连接
▋ <u>〕 〕</u> 〕 〕 〕 〕 〕 〕 □ □ □ □ □ □ □ □ □ □ □ □	+ 添加	II <u>详情</u> 📅 🖿 🖻 🖿 💼	🗙 删除引擎 🌱 测试连接
+ 添加	+ 添加	+ 添加	🗶 删除引擎 77测试连接
+ 添加	+ 添加	+ 添加	🗙 删除引擎 🌱 测试连接
<u>+ 添加</u>	🕂 添加	-	🗶 删除引擎 🌱 测试连接
忝加审计或防火 墙			
名称 172.17.200.20:1	521/orcl		
名称 172.17.200.20:1 应用模式 ◎ 审计 ◎ 防火	521/orcl 墙		

名称:所添加审计防火墙的名称,默认为添加的数据库引擎的名称。

应用模式:根据需求以及设备在网络环境中的连接情况,选择是审计模式还是防火墙模式。

网口名称: 审计数据的来源口,根据镜像所连接设备的网口进行选择。

3.1.5.1 示例 1: 添加审计

添加 IP 为 172.17.200.20 的数据库引擎的旁路审计功能。

点击数据库引擎所对应的审计或防火墙的 "添加"按钮,弹出 "添加审计或防火墙" 窗口,如下图所示:



	1-46221-1-104	17FTF
+ 添加	II <u>详情</u> 📅 III <u>除</u>	🗶 删除引擎 🌱 测试连接
III <u>详情</u> 📅 删除	-	🗶 删除引擎 🌱 测试连接
+ 添加	-	🗶 删除引擎 🌱 测试连接
+ 添加	▋ 注信 📅 删除	🗶 删除引擎 🌱 测试连接
+ <u>添加</u>	+ 添加	🗶 删除引擎 🌱 测试连接
+ 添加	+ 添加	🗶 删除引擎 🌱 测试连接
+ 添加	-	🗶 删除引擎 🌱 测试连接
521/orcl		
墙		
~		
	 ★ 添加 + 添加 + 添加 + 添加 + 添加 + 添加 * 添加 * 添加 	* 法加 ** 译面 ** 译面 ** 述面 * 添加 - ** 添加 * 添加 ** 添加 ** 添加 * 添加 ** 添加 ** 添加 * 添加 ** 添加 * * 添加 * * * 添加 * *

根据实际情况镜像口连接设备的 enp1 口 (需要 SysAdmin 用户或是有系统管理模块权限的用户,在 "系统管理"模块> "系统配置" > "接口设置"中将 enp1 设置为审计口,并在"接口功能"中开启 enp1 口的审计功能),故网口选择 enp1。点击 "确定"。

3.1.5.2 示例 2: 添加防火墙

添加 IP 为 172.17.200.191 的数据库引擎的防火墙功能。设备通过设备的 enp3,enp4 串联接入网络环境 (需要 SysAdmin 用户或是有系统管理模块权限的用户,在系统管理模块> "系统配置" > "接口设置"中将 enp3,enp4 设置为网桥,网桥名为 br1),网口名称选择 br1。



审计防火墙		状态监控	风险扫描	操作
🔢 逆情 🛛 📾 📾 🕅	ž	+ 添加	■ <u>详情</u> 前 删除	🗶 🖮 🕅 🖄 🎦 🎫 🗱 🗱 🎽
🔢 详情 🏛 删除	Ì	☷ <u>详情</u> 	-	🗶 🖮 🕅 🖄 🎦 🖄 🗶
🔢 道情 📅 删除	ž	+ 添加	-	🗮 🖮 🕅 🖄 🎦 🐘 🗮
🔢 <u>详情</u> 📅 删除	ž	+ 添加	■ <u>详情</u> 前 删除	🗶 🖮 🕅 🖄 🎦 🎫 🗮
🔢 注情 ี 📾 📾 📾	ž	+ 添加	+ 添加	🗶 🖮 🕅 🖄 🎦 🎫 🗮
+ 添加		+ 添加	+ 添加	🗶 删除引擎 \Upsilon <u>测试连接</u>
+ 添加		+ 添加	-	🗮 删除引擎 🌱 测试连接
	添加审计或防火	墙 🛛 🛛		
	名称 1	72.17.200.191:5236/DAME		
	应用模式	◎ 审计 ⑧ 防火墙		
	网口名称	r1 🗸		
		✔ 确定		

3.1.5.3 示例 3: 删除审计或防火墙

点击已添加的审计或防火墙对应的 "删除"按钮,弹出确认窗口点击 "确定"即可删 除。

审计防火墙	状态监控	风险扫描	操作
III <u>详情</u> 💼 IIII 🟦	+ 添加	III <u>详情</u> 📅 删除	🗙 删除引擎 77 测试连接
III <u>详情</u> 💼 删除	II <u>详情</u> 📅 III 🟦	-	🗙 删除引擎 77 测试连接
III <u>详情</u> 📅 删除	+ 添加	-	🗙 删除引擎 77 测试连接
II <u>详情</u> 💼 删除	+ 添加	III <u>详情</u> 📅 删除	🗙 刪除引擎 77 测试连接
■】 <u>详情</u> 1 <mark>日 删除</mark>	+ 添加	+ 添加	× 删除引擎 7° 测试连接
III <u>详情</u> 前 删除	+ 添加	+ 添加	★ 刪除引擎 了? 测试连接
确认	8	3	
(2) 确认删	★ 确定 ★ 取消		



提示:添加了数据库引擎的审计防火墙功能后,点击"详情"按钮,能够跳转到 "数据 库审计与防火墙"模块,在此模块可以控制该引擎的审计和防火墙功能是否开启,并为其进 行"策略"设置。

3.1.6 状态监控

数据库状态监控,实时监控数据库运状态,如服务器的运行时间、内存及存储的使用情况等。在异常时进行预警,防止业务瘫痪,保障业务系统的可用性(详细信息参考 5.5 章节)。

示例 1: 添加数据库监控

添加 IP 为 172.17.200.194 的数据库引擎的状态监控功能。

点击数据库引擎所对应的"状态监控"的"添加"按钮,弹出添加数据库监控窗口,如 下图所示:

审计防火墙	状态监控	ž		风险扫描		操作	
▋〕 逆情 前 删除	+ 添加			🚦 逆情 📅 删除		🗶 🖩 🕅 🎦 🗮	<u> ?? 测试连接</u>
■ <u>详情</u> 前 删除	+ 添加			-		🗶 🔤除引擎	<u> 7 测试连接</u>
▋] 逆情 龠 删除	🕂 添加			-		🗶 🖮除引擎	<u> ?? 测试连接</u>
▋】 道情 前 删除	+ 添加	添加数据库出	监控			🗶 🖮除引擎	<u> ?? 测试连接</u>
▋】 逆情 龠 删除	┿ 添加		472 47 200 40	4-000 (h+-)		🗶 🖹除引擎	17测试连接
■ 详情 前 删除	+ 添加	名称	172.17.200.19	14:3306/testar		🗶 🖮除引擎	<u> ??" 测试连接</u>
		用户名	root				
		密码					
		缺省SID	testdb				
				🛩 确	淀		

名称:数据库状态监控的名称,默认为数据库引擎的名称。

用户名: 所要监控数据库的用户名。此用户名需要具有一定的数据库系统权限。 密码:填写用户名对应的密码。



缺省 SID: 所监控数据库的实例名,系统默认显示的为各数据库所默认的实例名。

输入相应信息后点击 "确定"即可。

示例 2: 删除数据库监控

点击已添加的数据库监控对应的 "删除"按钮,弹出 "确认"窗口点击 "确定"即可删除。

审计防	5火墙	状态监控	风险扫描	操作
11 逆	情 💼 删除	★ 添加	II <u>详情</u> 📅 删除	💥 删除引擎 🌱 测试连接
■道	值 💼 删除	副 道情 💼 删除	-	★ 删除引擎 了 测试连接
11 逆		◆ 添加	-	💥 删除引擎 🌱 测试连接
∎単	_佳 确认	X	II <u>详情</u> 📅 III 🟦	💥 删除引擎 🌱 测试连接
∎単	值 🕐 确认删除吗?		+ 添加	💥 删除引擎 🌱 测试连接
∎逍	Li V		+ 添加	¥ 删除引擎 7°测试连接
	✔ 确定	* 取消		

提示:添加了数据库引擎的状态监控功能后,点击"详情"按钮,能够跳转到"数据库 状态监控"模块。

3.1.7风险扫描

数据库系统是一个复杂的系统资料,数据库存在许多风险,其中不少是致命的缺陷和漏洞。一旦遭到攻击,攻击者可能以 DBA 的身份进入数据库系统,也可能进入操作系统,下载整个数据库文件。为此本系统提供风险扫描模块,使用户能更早的发现风险与漏洞。

示例 1: 添加数据库风险扫描

添加 IP 为 172.17.200.193 的数据库引擎的风险扫描功能。





点击数据库引擎所对应的"风险扫描"的 "添加"按钮,弹出添加风险扫描窗口,如下 图所示:

审计防火墙	状态监控		风险扫描	风险扫描		
■ <u>〕 详情</u> 前 删除	💠 添加		■ <u>详情</u>	前 删除	🗶 删除引擎	17测试连接
■ <u> 详情</u> 前 删除	■ <u>详情</u>	📅 🎟 🟦	-		🗶 🖮除引擎	<u> 7° 测试连接</u>
II <u>详情</u> 📅 删除	+ 添加		-	_	🗶 🖿 🕅	7" 测试连接
■ 道情 💼 删除	+ 添加		+ 添加		🗶 删除引擎	了测试连接
II <u>详情</u> 📅 删除	+ 添加	沃加粘促医白紫			🗶 🖮除引擎	7 ° <u>测试连接</u>
〓 <u>详情</u> 📅 删除	🕈 添加	スペルIII (2016) 1711日 名称 172.17.200.193:1521/oracle			🗶 删除引擎	<u> 7°测试连接</u>
				oracle		
		用户名	system			
		密码				
		缺省数据库	oracle			
				✔ 确定		

名称:数据库状态监控的名称,默认为数据库引擎的名称。

用户名: 所要监控数据库的用户名。此用户名需要具有一定的数据库系统权限。

密码:填写用户名对应的密码。

缺省数据库:所监控数据库的实例名,系统默认显示的为各数据库所默认的实例名。

输入相应信息后点击 "确定"即可。

示例 2: 删除风险扫描

点击已添加的风险扫描的数据库引擎对应的 "删除"按钮,弹出确认窗口点击 "确定" 即可删除。



IP	端口	缺省数据库	审计防火墙	状态监控	风险扫描	操作
172, 17, 200, 190	60000	test1	■ 逆陸 💼 ■除	+ 添加	■ 道情 音 删除	× mikel 弊 了" 测试
192. 168. 0. 98	3306	mysql	副 道情 💼 删除	+ 添加	-	🗙 🖮 🏦 🕄 🎢 🕅 🕅 🕅
172. 17. 200. 194	3306	test1	副 逆情 📅 删除	+ 添加	-	🗙 🖮 🟦 राष्ट्री 🏝 🌱 ग्रीसि
192. 168. 0. 99	60000	test1	副 逆陸 🛛 🏛 📾 🕅	+ 添加	+ 添加	X mikel X 7 Ditti
	确认					
(2) iii						
	IP 172. 17. 200. 190 192. 168. 0. 98 172. 17. 200. 194 192. 168. 0. 99	IP 講日 172.17.200.190 60000 192.168.0.98 3306 172.17.200.194 3306 192.168.0.99 60000 第次 (学) 确认	IF 端口 鉄省数据库 172.17.200.190 60000 testi 192.168.0.98 3306 mysql 172.17.200.194 3306 testi 192.168.0.99 60000 testi Second Second	III 講口 缺省数据库 审计防火措 172.17.200.190 60000 test1 11 建造 值 雷融急 192.168.0.98 3306 sysql 11 建造 值 雷融急 172.17.200.194 3306 test1 11 建造 值 雷融急 192.168.0.99 60000 test1 11 建造 值 雷融急 192.168.0.99 60000 test1 11 建造 值 雷融急	III 端口 終金数据库 审计防火造 状态监控 172.17.200.190 60000 test1 第 译适 金融金 + 适加 192.168.0.98 3306 eysql 第 译适 金融金 + 适加 172.17.200.194 3306 test1 第 译适 金融金 + 适加 192.168.0.99 60000 test1 第 译适 金融金 + 适加	III 端口 缺省数据库 审计防火墙 状态监控 风险扫描 172.17.200.190 60000 testi 11 逆流 11 回 <

提示:添加了数据库引擎的风险扫描功能后,点击"详情"按钮,能够跳转到 "风险扫描"模块。

3.1.8 操作

操作对应 "删除引擎"和 "测试连接"两个按钮。

3.1.8.1 删除引擎

点击需要删除的引擎的 "删除引擎"按钮,弹出提示窗口,点击"确定"即可删除。





提示:当数据库引擎正在被"审计防火墙"、"状态监控"、"风险扫描"之中的任一模块 所使用,则不能删除,需要先停止使用方可删除。

3.1.8.2 测试连接

点击需要测试的引擎的 "测试连接"按钮,如何网络可达则在屏幕右下角提示如下:

提示	×
连接成功,路由可达 !	

如果网络不可达则提示如下:

儲						
这 连接失败,路由不可达!						
路由不可达						
✓ 确定						



3.2 数据库审计与防火墙

所属用户: SecAdmin。

审计,即数据库审计模块,旁路部署在数据库和客户端之间,提供数据库操作的事后查 询分析和实时的告警,同时带有旁路阻断等功能。

防火墙即数据库防火墙,串联部署在数据库和客户端之间,能主动防御或阻断对数据库 的攻击或自定义的危险行为,能有效地对数据库提供防护。

3.2.1 审计防火墙

3.2.1.1 审计和防火墙列表

审计和防火墙列表显示已经添加的数据库审计或防火墙引擎信息,可对引擎进行编辑、 删除、启动和停止操作。

	审计防火墙		策略中心	い 最新	流量			
审计防火墙列表								
🥒 编辑	🥒 编辑 💼 删除 🕨 启动 🔳 停止							
名称		审计类型	状态	类型	IP			
172.17.200	.190:6	审计	运行中	DB2	172			
172.17.200	. 194:3	审计	已停止	MYSQL	172			
192, 168, 0,	98:330	审计	已停止	MYSQL	192			
192.168.0.	99:600	审计	运行中	DB2	192			

编辑



选择要编辑的引擎,点击审计防火墙列表下的 "编辑"此模式下只可以修改以下四项信

息。

- a) 名称:可以修改引擎的名称,便于查看和分析。
- b) 所属采集器: 修改所属采集器, 以应用其它采集器。
- c) 应用模式: 切换审计或防火墙模式。
- d) 网口名称: 在切换镜像口后需要修改为切换后对应的网口名称才能继续接收数据。

添加审计或防火墙							
名称	172.17.200.20:1521/or V						
IP	172.17.200.20						
端口	1521						
类型	ORACLE 🗸						
缺省SID	orcl						
所属采集器	localhost 🗸						
应用模式	◎ 审计 ◉ 防火墙						
网口名称	br1 🗸						
	✔ 确定						

提示: 审计或防火墙功能运行中的引擎要先停止再进行编辑。

删除

删除数据库引擎的审计或防火墙功能。点选相应引擎,点击"删除"按钮,弹出确认窗口,点击"确认"。



ւչ			
2	确定删除该审计或	防火墙吗?	
\checkmark			
		A The SALE	
	✓ 娴定	🧸 取消	
	પ ?	认 ④ 确定删除该审计或 ✓ 确定	 ↓ ④ 确定删除该审计或防火墙吗? ✓ 确定 ★ 取消

提示: 审计或防火墙功能运行中的引擎要先停止才能删除。

启动

数据库引擎添加审计和防火墙功能后,默认是停止状态,需要启动才能开始记录信息。 点击要启动的引擎,选择"审计防火墙列表"下的"启动"。需要启动的引擎的状态栏显示 为运行中后,引擎启动成功,可以继续进行其它配置。

审计网	审计防火墙		心最新	新流量				
审计防火墙列表								
🥒 编辑 💼 删除 🕨 启动 🔳 停止								
名称	审计类型	状态	类型	IP				
172.17.200.190:6	防火墙	运行中	DB2	172				
172.17.200.191:5	防火墙	运行中	达梦7	172				
172, 17, 200, 193;1	审计	运行中	ORACLE	172				
172.17.200.194:3	审计	运行中	MYSQL	172				
172.17.200.20:15	防火墙	已停止	ORACLE	172				
192.168.0.98:330	审计	运行中	MYSQL	192				

停止

有些情况需要停止引擎的审计或防火墙功能,如排查故障、编辑引擎信息、删除引擎。 选择要停止的引擎,选择"审计防火墙列表"下的"停止",此引擎对应的数据库审计或防火 墙功能暂时停止。此引擎的"状态"栏显示为"已停止"后,引擎停止成功



审计图	防火墙	策略中	心最新	「流量				
审计防火墙列表								
✓ 编辑								
名称	审计类型	状态	类型	IP				
172.17.200.190:6	防火墙	运行中	DB2	172				
172.17.200.191:5	防火墙	运行中	达梦7	172				
172, 17, 200, 193;1	审计	运行中	ORACLE	172				
172.17.200.194:3	审计	运行中	MYSQL	172				
172.17.200.20:15	防火墙	已停止	ORACLE	172				
192.168.0.98:330	审计	运行中	MYSQL	192				

3.2.1.2 设置

点击相应的数据库引擎,右侧会出现对应的设置页面。



审计防火墙 策略中心 最新流量		
审计防火墙列表	设置 特征模型	型 模型策略
✓ 编辑 面 删除 ▶ 启动 ■ 停止	应用模式	● 审计 ◎ 防火墙 💡 引擎停止的状态下才可编辑
名称 审计类型 状态 类型 IP		
172.17.200.190:6 审计 运行中 DB2 172	数据来源(接口)	enp1 • 引擎停止的状态下才可编辑
172.17.200.194:3 审计 已停止 MYSQL 172		- 开启数据库应答收检
192.168.0.98:330 审计 已停止 MYSQL 192	监控数据库应管	
192.168.0.99:600 审计 运行中 DB2 192	数据库登录辅助	□ 开启数据库辅助获取连接信息 [适用于SQL SERVER2005、2008] ⑦
	远程监控	□ 启动远程监控
	本地监控	□ 启动本地监控
	威胁监控	□ 启动威胁监控
	模糊化日志	□ 启动模糊化日志
	旁路阻断	□ 启用旁路阻断
	🗎 保存并生效	
	自动学习状态	──段时间后关闭&生成规则 ▼ 停止时间: 2016-05-30 1 保存

应用模式

根据实际的需求选择应用模式:审计或防火墙。

	应用模式	◉ 审计	◎ 防火墙	引擎停止的状态下才可编辑					
抈	提示:注意部署方式是否对应。								
米女	女据来源								

配置数据库的通讯包的来源的网络接口,要与此数据库的数据实际连接的镜像口对应。

数据来源(接口)	enp1 •	💡 引擎停止的状态下才可编辑

监控数据库应答



处理数据库的响应分析和结果分析的设置。

开启数据库应答监控:开启时分析数据库的回应信息。

开启返回结果解析:开启时分析数据库的回应信息的结果内容,如分析出返回行数等。

	✔ 开启数据库应答监控
监控数据库应答	☑ 开启返回结果解析

数据库登录辅助

由于有些特殊的数据库对通讯进行了加密处理,造成了直接解析数据库的协议无法得到 所需要的审计信息,如用户名等。这种情况下直接添加引擎无法实现审计和防火墙的功能, 此时就需要使用数据库登录辅助功能,对数据库进行再次通讯以获取必要的信息。目前适用 于 SQL SERVER 2005、2008 及以上版本,设置界面如下图所示。

☑ 开启数据库辅助获取连接信息 [适用于SQL SERVER2005、2008] ⑦ 设置						
IP地址		端口				
用户名		密码				
数据库名						

IP 地址:数据库引的 IP。但如果条件允许,建议最好给数据库新增1个专门用于该 类通信的 IP 以便区分。

端口:对应的端口号。

用户名:可以是 tools\ddi 建立的受限用户。

密码:用户名对应的密码。

数据库名:默认 master, 若为其它请手动修改。

点击"测试连接",显示成功后保存配置,若测试失败请检查数据库是否正常连接以 及配置是否正确。



此处的用户名可以是数据库超级管理员。有些情况为了安全起见,不能提供很大的管理 员权限,此时可以使用我们提供的 SQL 脚本,建立受限权限的用户,只保留数据库审计和防 火墙所需的数据库权限。

远程监控

远程监控适用于软件镜像部署的模式。首先需要在数据库上安装镜像软件,然后在页面 上进行配置,即可进行远程监控。

修改脚本

linux:

./linux/csremote.sh

将其中 DB_PORT=3306 中 3306 改为 数据库端口

将其中 DB_IP=192.168.1.55 中 192.168.1.55 改为 数据库 ip

将其中 INTERFACE=eth3 中 eth3 改为 数据库使用网卡

将其中 RA_TARGET_IP=192.168.1.157 中 192.168.1.157 改为 审计

接口对应 ip。

windows:

./windows/csremote.bat

将其中 DB_PORT=1433 中 1433 改为 数据库端口

将其中 DB_IP=192.168.1.61 中 192.168.1.61 改为 数据库 ip

将其中 INTERFACE=1 中 1 改为 数据库使用网卡

将其中 GATEWAY=192.168.1.254 中 192.168.1.254 改为 数据库所在

网关

将其中 RA_TARGET_IP=192.168.1.189 中 192.168.1.189 改为 审计 接口对应 ip.



在被监控的数据库所在主机上执行如下脚本

linux: ./linux/csremote.sh

windows: ./linux/csremote.bat

检查审计系统 nc 是否启动, 若没有启动执行 sudo nc - I 7000

系统配置, IP 地址设置为当前引擎对应数据库的 IP, 端口号默认为 7000。

本地监控

一些小型的 B/S 应用,WEB 服务器和数据库服务器在一台机器上,此时数据库和客户 端不需要通过网络接口,需要需要审计和防火墙,应进行本地监控的配置。本地监控需要运 行被监控的数据库和我们的WEB 应用,并对其进行一定配置,系统中配置页面如下图所示。 下面我们举例说明本地监控的使用方法。

✓ 启动本地监控			
设置			
IP地址		端口	
用户名		密码	
数据库名	? 测试连接		

数据库相关配置

向数据库安装 install-script 中的脚本,按照 localmon\Oracle 和

localmon\SQLServer下 readme.txt 中的说明执行安装,并记下其中的密码。

WEB 应用所需配置

WEB 应用中的配置为建立引擎以及配置本地监控,具体操作步骤如下:

a) 在引擎项目下,选择"添加",填入相应的数据库信息。

b) 对已添加的引擎,选择"审计与防火墙"列下的"添加","应用模式"选择"审计",填入自 定义的名称,并选择网口名称,选择完成。



c) 查看已添加"审计与防火墙"的详情,选择"设置"分页,选择"本地监控",在本地监控的 详细设置中填入相关信息:被监控的数据库 Ip,用户名和密码,用户名为:

CSBIT_CONSOLE_ACCESS_QRY, 密码为安装过程中输入的后一个密码。数据库端口、名称。

点击"测试连接",如果提示连接成功则表示以上数据可用,否则,请检查以上输入是 否正确.

在左侧的"引擎列表"中选择启动以上设置的引擎。

本地监控测试

启动 tapcenter 测试版,tapcenter 会将本地监控收到的 SQL 信息在控制台中输出, 其启动命令行如下:

#./tapcenter --logtostderr=true --minloglevel=0

tapcenter 将会收到被对被监控数据库进行的操作并显示在控制台中,包括以下内容操作类型:login, logout 和 Others(执行 SQL 语句)

一般操作相关信息:seesionid,操作发生的时间,执行 sql 所花费的时间,对于 login 操作,还包括以下信息:

数据库用户名, 连接数据库的应用程序名称, 系统名称, 系统用户名, 主机名,数据库名, 客户端 IP, 客户端, 客户端端口, 数据库 MAC。

对于 Other 类型的操作,包括 sql_text(被执行的 SQL 语句),reply(执行结果),replyLen(执行结果长度)

注意:

a) 目前仅支持 Oracle 和 SQLServer。

b) 测试过程中可以手工输入一些 SQL 语句,查看 tapcenter 是否监控到。

c) 如果用户 login,执行 sql,马上 logout,将较难监控到其操作。



威胁监控

有一些特殊的状态,虽然行为合规,但可能会对数据库造成威胁,对此时需要进行数据 库威胁监控,如下图所示:

1		
×.	后列威肋监控	

- 设 <u>晋</u>		
风险等级: 无 ▼		
□ SQL注入监控		
🗌 缓冲区溢出监控		

主要的可选设置项有:

风险等级:可以主动设置威胁行为的风险等级,高风险和致命风险会显示在告警页 面上,以便管理员及时发现威胁行为。

SQL 注入监控: SQI 注入就是通过把 SQL 命令插入到 Web 表单提交或输入域名或 页面请求的查询字符串,最终能够欺骗服务器执行恶意的 SQL 命令。开启 SQL 注入监控后 系统会识别恶意的 SQL 命令并及时告警或阻拦。

缓冲区溢出监控。缓冲区溢出攻击可以导致程序运行失败、系统宕机、重新启动等 后果。更为严重的是,可以利用它执行非授权指令,甚至可以取得系统特权,进而进行各种 非法操作。开启缓冲区溢出监控后,系统在面对缓冲区溢出风险的时候会进行告警或阻拦。

模糊化日志

为了保护敏感的信息,如电话号码、身份证号等,可以将这些信息进行模糊处理以增加 保密性,设置界面如下图所示。



✓ 启动模糊化日志

设置			
🕇 添加 🧪 编辑	量 💼 删除		
名称	正则式	替换值	

每个项有如下的内容:

名称: 该条模糊化信息的标识。

正则式: 替换的正则式内容。点击"添加",出现如下图所示界面。

添加		×
名称		
正则式		0
替换值	###	(默认'###')
		✔ 确定

点击图中的"?",会出现如下图所示的正则表达式帮助文档。



正则表达式帮助文档						
什么是正则表达式?						
正则表达式(regular expression)描述了一种字符串匹雪的模式。本系统用来检查一个数据库请求中是否含有某种子串。是由普通字符(例如 字符 a到2)以及特殊字符(称为元字符)组成的文字模式。正则表达式作为一个模板,将某个字符模式与所搜索的字符串进行匹配。本系统采用 使用最广泛的perl兼容正则表达式系统。						
主要的正则表达式符号表						
字符	描述					
١	将下一个字符标记为一个特殊字符、或一个原义字符、或一个向后引用、或一个八进制转义符。例如,'n' 匹配字符 "n"。'\n' 匹配一个换行符。序列 '\\' 匹配 "\" 而 "\(" 则匹配 "("。					
٨	匹配榆入字符串的开始位置。如果设置了RegExp对象的Multiline 属性,^ 也匹配 '\n' 或 '\r' 之后的位 置。					
\$	匹配榆入字符串的结束位置。如果设置了RegExp 对象的Multiline 属性,\$ 也匹配 '\n' 或 '\r' 之前的位置。					
*	匹配前面的子表达式零次或多次。例如,zo* 能匹配 "z" 以及"zoo"。* 等价于{0,}。					
+	匹配前面的子表达式一次或多次。例如,'zo+' 能匹配 "zo" 以及"zoo",但不能匹配 "z"。+ 等价于 {1,}。					
?	匹配前面的子表达式零次或一次。例如,"do(es)?" 可以匹配 "do"或 "does" 中的"do" 。? 等价于 {0,1}。					
{n}	n是一个非负整数。匹配确定的n次。例如,'o{2}' 不能匹配"Bob" 中的 'o',但是能匹配 "food" 中的两个 o。					
{n,}	n 是一个非负整数。至少匹配n次。例如,'o{2,}' 不能匹配 "Bob"中的 'o',但能匹配 "foooood" 中的所有 o。'o{1,}' 等价于'o+'。'o{0,}' 则等价于 'o*'。					
{n,m}	m和n均为非负整数,其中n <= m。最少匹配 n 次且最多匹配m次。例如,"o(1,3)" 将匹配 "fooooood" 中的前三个o。'o(0,1)'等价于 'o?'。请注意在逗号和两个数之间不能有空格。					

替换值:敏感信息替换成的文字,默认'###',可以修改为任意值,则凡是出现匹配 到上面的正则表达式的信息,即自动替换为此值。

旁路阻断

在引擎未启动的情况下,可以选择启用旁路阻断功能,此时在旁路部署的数据库审计模 式下依然可以对数据库操作进行阻断。旁路阻断与数据库防火墙的阻断区别: 旁路阻断通过 旁路发 RST 包进行阻断。如下图所示,启用旁路阻断,选择阻断包发送的网卡,成功开启旁 路阻断功能。

旁路阻断	☑ 启用旁路阻断 网卡: enp1 ▼	♀引擎停止的状态下才可编辑
3 保存并生效		



自动学习状态

通过自动学习状态可以控制学习开始和结束及生成策略。如下图所示:

自动学习状态	一段时间后关闭&生成规则	停止时间:	2016-05-16	📆 🗎 保存
	开启 关闭&生成规则 一段时间后关闭&生成规则 关闭&不生成规则			

3.2.1.3 特征模型

在"特征模型"模块中可对"学习"进行设置,自动学习访问数据库的行为,并对行为进行分析学习,将学习到的模型,生成相应的策略,只要点击停止学习后,模型就会应用到相应的策略上。

・ 添加 ● 部93 ● 293 <th>设置</th> <th>特征</th> <th>模型 模型</th> <th>範略</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	设置	特征	模型 模型	範略								
前月名 資明銀蟹 項田銀蟹 項正数量 应用程序数量 日本	+ 添加	💼 删除	🖴 刷新			学习	查询组	时间限制	特权操作	高级设置		
system 0 0 0 0 sys 0 0 0 0 0 0 sys 0 0 0 0 0 0 0 sys 0 0 0 0 0 0 0 0 sys 0	用户名	查询数量	查询组数量	源IP数量	应用程序数量	目标						
ays 0 0 0 0 掛規席 Sohema 数量 表格与操作 ● 報告 ●	system	0	0	0	0	+ 添加 💼	刪除 🗎 保	存 🗖 副新	1 锁定	❣ 任意值		
表格与操作 □ 報告報告報告報告報告報告報告報告報告報告報告報告報告報告報告報告報告報告報告	sys	0	0	0	0	数据库		Schema		数量		
表格与操作 副新 小 微读 文 任意值 ★ 添加 壶 刪除 邑 保存 □ 副新 小 微读 文 任意值 表 这择 更新 抗入 剛除												
表格与提作 □ ● <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>												
表協与援作 副 保存 副新 日 保存 副新 小・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・												
表临与操作 副新 日 保存 副新 ① 截定 ***********************************												
表格与操作 副 保存 □ 朝新 ① 裁定 Y 任意值 ★ 送择 更新 插入 翻除												
表名与操作 副新 Q 供意值 ★ 边择 更新 抵入 剛除												
◆ 添加 □ Wift □ 保存 □ 副新 ① 微定 ▼ 任意值 表 这择 更新 払入 明除						表格与操作						
表 选择 更新 插入 删除						+ 添加 💼	🖩 🗎 🗎 保	存 🗖 刷新	∩∎ 锁定	❣ 任意值		
						表	选择	Ţ	巨新	插入	刪除	

学习



"学习"的内容包括目标,表格与操作,源 IP,源应用程序,操作系统主机名,操作系统用户。

学习	查询组 日	村间限制 特权操作	高级设置	
目标				
+ 添加 💼	🖥 刪除 🛛 🗎 保存	🖴 刷新 🧧 锁定	❣ 任意值	
数据库		Schema	数里	
表格与操作				
+ 添加 📑	🖥 删除 🛛 🗎 保存	😂 刷新 🧧 锁定	❣ 任意值	
表	选择	更新	插入	刪除

查询组

"查询组"提供特征模型学习到的 sql 语句,可进行策略配置。



学习	查询组	时间限制	特权操作	高级设置				
查询组								
╋ 添加SQL	💼 删除 🛛 🗎	保存 🗖 🚍 刷	新 🔓 锁定	🍸 任意值	[
查询组					查询	建议模式	强制模式	
4 🕤					1	细颗粒度	細颗粒度 ▼	
📄 selec	t						中颗粒度 细颗粒度	

时间限制

用户可以根据自己的实际环境,设置具体的时间,年月日均可选择。

学习	查询组	时间限制	特权操作	高级设置
天时间段			\$ -	\$
周时间段			• -	\$
月时间段			\$ -	\$
🗎 保存				

特权操作


系统提供默认的特权操作类型,用户可以根据需要选择相应的特权操作,选择完成后点 击"保存"即可。

学习	查询组	时间限制	特权操作	高级设置	
			<pre>>> truncate c dbcc chec grant syst drop appl create role create age create ser alter syno drop data</pre>	luster cktable em privilege ication role e gregate rver audit specif nym base audit spec	ication
■ 保存					•

高级设置

"高级设置"中主要包括了"特征模型与保护策略"、"学习普通(DML)查询组的单个 查询"、"查询组列表设置","表格与操作列表设置"等。



学习	查询组	时间限制	特权操作	高级设置	
- 特征模型与 ● 不保护 ● 访问敏 ● 任何操	5保护策略 (DBA) 感表时保护 作都保护			-	
-学习普通 ● 将所有 ● 将所有 ● 切换为	(DML) 查询组的 查询组切换为" 查询组切换为" "中颗粒度"所	单个查询 细颗粒度" 中颗粒度" 需的查询数:			
正在处理不 查询组列表 ● 关闭: ● 敏感相 ● 开放模作 ● 大幅感模作 ● 敏感模 ● 开放模	K属于特征模型, 设置 任何不属于特征 关试、不属于特征 可不属于特征 可不属于特征 式:不属于特征 式:不属于特征 式:不属于特征	并且与任何查 模型的查询组都 含敏感表格时, 模型的查询组将 特征模型的表格 转征模型的表格 模型的表格与操	间组都不匹酉的 会引发违规 不属于特征模型 不会引发违规 与操作都将引发 时,不属于特征 作将不会引发追	查询 型的查询组才会 这违规 E模型的表格与 E规	引发违规 操作才会引发违规
计入规	则的最小重复次数	讫:	10)	
₿ 保存					

3.2.1.4 模型策略

系统默认的模型策略,用户可根据实际情况对这些默认的策略进行风险等级以及操作类型设置,点击"保存"后生效。



设置 特征模型 模型策略				
称	已启用	告警级别	操作	
🗀 尝试执行特权操作		高风险 ▼	通过 ▼	
📄 无法跟踪的数据库用户		高风险 ▼	通过 ▼	
📄 时间违规		高风险 🔻	通过 🔻	
📄 未授权的主机		高风险 ▼	通过 ▼	
📄 未授权的操作系统用户		高风险 ▼	通过 ▼	
📄 未授权的敏感表格		高风险 ▼	通过 ▼	
📄 未授权的数据库和Schema		高风险 ▼	通过 ▼	
📄 未授权的数据库用户		高风险 ▼	通过 ▼	
📄 未授权的查询组		高风险 ▼	通过 ▼	
📄 未授权的源IP地址		高风险 ▼	通过 ▼	
📄 未授权的源应用程序	2	高风险 ▼	通过 🔻	
📄 未授权的表操作访问	v	高风险 ▼	通过 ▼	

3.2.2策略中心

3.2.2.1 全局参数

在策略和规则下都可以进行"全局参数"的配置,配置好全局参数,可以在配置每一条 具体的规则时直接使用已配置好的参数。

IP 集

"IP 集"即访问数据库服务的 IP 地址段。点击如下图的 IP 集,点击 "添加内容"。在 弹出框中输入起始和结束 IP,点击 "确定",成功设置 IP 集。

· 📴 IP集	添加内容 清空
---------	---------

如下图所示,如果有不再需要的 IP 集,点击"删除"可以删除该 IP 集,或点击"清空" 清空所有 IP 集。

▲ 19 IP集	添加内容 清空
■ 10. 0. 0. 120~10. 0. 0. 122	<u>删除</u>
■ 10. 0. 0. 122~10. 0. 0. 123	<u>删除</u>

也可以通过 "清空"按钮将所有 IP 集删除



源应用程序集

源应用程序,即访问数据库服务的机器上的执行程序标题。点击如下图所示的源应用程序集,点击"添加内容",在弹出框中输入客户端程序,点击"确定",成功设置源应用程序集。删除、清空同上。

◢ 1 ◎ 源应用程序集	添加内容 清空
📄 db2bp. exe	删除

操作系统用户集

操作系统用户,即访问数据库服务的机器的登陆系统的用户,如下图所示。点击"操作 系统用户集",点击"添加内容",在弹出框中输入操作系统用户名,点击"确定",成功设 置操作系统用户集。

🔺 📴 操作系统用户集	添加内容 清空
🖹 tom	⊞₺₤

操作系统主机集

操作系统主机,即访问数据库服务的机器的主机,如下图所示。点击"操作系统主机集", 点击"添加内容",在弹出框中输入操作系统主机名,点击"确定",成功设置操作系统主 机集。删除、清空同上。

🔺 📴 操作系统主机集	· · · · · · · · · · · · · · · · · · ·
📄 TANG-DATAFORT	刪除

数据库用户集

数据库用户,即访问数据库的用户。点击 "数据库用户集",点击 "添加内容",在弹出框中输入数据库用户名,点击 "确定",成功设置数据库用户集。



🔺 📴 数据库用户集	添加内容 清空
📑 dbm	<u>刪除</u>
🗎 db2inst1	删除
🗎 tom	删除

数据库表

数据库表,即数据库中存放数据的具体的表。点击 "数据库表",点击 "添加集",在 弹出框中输入数据库表组名,点击 "确定",成功设置数据库表组。

选中添加的表组,点击"添加内容",输入表名,点击"确定",成功在数据库表组下添加数据库表名。

▲ 193 数据库表	添加集
▲ 📴 自动学习	添加内容 删除
🖹 xixi	
📄 emp	
SYSCAT. TABLES	
🗎 user_test1	
🖹 'user_test2'	
DINFORMATION_SCHEMA. PROFILING	删除
🖹 'user_test1'	
🗐 user_test2	
🗎 user_info	
🗎 user_test	删除
🗐 newone	
🖹 newon	
≠ 📴 इ1	添加内容 删除
🗎 use_info	删除

存储过程集

存储过程是在大型数据库系统中,一组为了完成特定功能的 SQL 语句集,存储在数据库 中经过第一次编译后再次调用不需要再次编译,用户通过指定存储过程的名字并给出参数(如



果该存储过程带有参数)来执行它。如图,点击 "添加内容"后,输入存储过程集名,成功 添加存储过程集。

存储过程集	添加内容 清空
📄 execute	删除

数据库列集

数据库列,即数据库中存放数据的具体的表中的列。点击 "数据库列集",点击 "添加 集",在弹出框中输入数据列名,点击 "确定",成功设置数据库列集。

4 📴 数据库列集	添加内容 清空
*	
🖹 xixi.*	删除
🖹 name	
SYSCAT. TABLES. TABNAME	
📄 @@character_set_database	
🖹 STATE	
📑 feom	
📄 QUERY_ID	
user_info.*	删除

数据库 Schema 集

数据库中的 Schema,为数据库对象的集合,一个用户一般对应一个 schema。为了区 分各个集合,数据库 Schma 需要一个名字,在数据库 Schema 集的设置中需要添加的就是 集合的名字。点击 "数据库 Schema 集"后的 "添加内容",填写数据库名与模式名,点 击 "确定"后成功添加数据库 Schema 集。



▷ 🚺 操作系统:	添加	×	私加内容	<u>清空</u>
▷ 📴 数据库用户			私加内容	<u>清空</u>
▷ 📴 数据库表			る加集	
4 💽 存储过程1	模式名	*	<u>私加内容</u>	<u>清空</u>
📄 execut			趙金	
▷ 🖸 数据库列集		♥ 明定 ● 収/月	<u>私加内容</u>	<u>清空</u>
🔺 📴 数据库Seh	ema集		添加内容	<u>清空</u>
*oracl	e. *Schema		删除	

SQL 异常字符串组

点击 "SQL 异常字符串组",点击 "添加集",在弹出框中输入数据库表组名,点击 "确 定",成功设置 SQL 异常字符串组。

选中添加的组,点击"添加内容",输入异常字符串,点击"确定",成功添加异常字 符串。

▲ 10 SQL异常字符串组	<u>添加集</u>
4 📴 gl	添加内容 删除
📄 where	删除
📄 select	删除

查询组

点击查询组,点击 "添加集",在弹出框中输入组名,点击 "确定",成功设置组。 选中添加的组,点击 "添加内容",输入查询语句,点击 "确定",成功添加查询语句。

2 19 查询组	添加集
4 📴 (select, xixi)	添加内容 清空
📄 select * from xixi	<u>刪除</u>



3.2.2.2 策略

策略可以应用于引擎中,所有对引擎对应的数据库的操作,都要经过引擎中配置的策略 的分析,当一个引擎存在多个策略时,要分别被每个策略所分析,并根据每个策略的结果进 行记录、告警或其它操作。

添加删除策略

在"策略中心"下,点击"添加策略"。弹出添加策略的弹窗

	审计防火墙	策略中心	
+ + 添加策 略	➡ 添加规 则	★上 +下 移 移	
添加策略			×
名称:			
基于:	新建		~
			✓ 确定

首先填写策略名称作为标识。基于选项条目选择"新建"或已存在的策略,点击"确定", 成功建立一条新的策略;若选择基于已存在的策略,如基于默认策略,则建立的策略中包含 默认策略中的所有配置。

删除策略,点击策略后面的 "删除",弹出确认窗口,点击 "确定",成功删除策略。

🛚 📴 默认策略	添加	删除
Þ 📴 AS	添加	删除



确认		×
2	若有子节点则子节点一起删除,	
4	确定要删除吗?	
	✔ 确定 🗮 取消	

策略配置

概要

如下图所示,概要处显示该策略的名称和最后的修改时间。

概要	名称	AS
	修改时间	2015-02-27 01:00:51

大小写敏感设置

如下图所示,可以设置数据库用户、操作系统用户、客户端程序是否区分大小写,默认 不区分。

	数据库用户	◎ 区分大小写 ⑧ 不区分大小写
大小写敏感设置	操作系统用户	◎ 区分大小写 ⑧ 不区分大小写
	客户端程序	◎ 区分大小写 💿 不区分大小写

应用到引擎

如下图所示,选择策略应用到的引擎,可以同时选择多条,则该策略的配置以及该策略下的规则的配置全部应用到选择的引擎。



应用到	I					
🗎 保祥	<u>.</u> 7					
	名称	IP	端口	网口	数据库类型	审计类型
1 🗸	10.0.0.121:1521/orcl	10.0.0.121	1521	fire1	ORACLE	防火墙

规则

添加删除规则

如下图,首先选中一条策略,点击"添加规则"或策略后的"添加",都会弹出添加规则

框。

+	╋ 添加规 则	!	◆下 移
规则名称		类型	操作
▶ 📴 默认策略	ł		添加 删除
🔺 🚺 AS			添加 删除

规则的逻辑关系

如下图,规则中包含"默认"、"优先级"、"白名单"、"黑名单"四种。四种类型之间的 优先级为:黑名单、白名单、优先级、默认。

添加规则	×
名称:	
类型:	● 默认 □ 优先级 □ 白名单 □ 黑名单
	✓ 确定 ¥ 取消

一条操作的匹配过程如下:

黑名单规则



匹配到黑名单的规则,匹配到一条则不再继续往下匹配,处理方式为"阻断→总是记录 →高风险";若未匹配成功,进入白名单规则。

白名单规则

匹配到白名单的规则,匹配到一条则不再继续往下匹配,处理方式为"通过→不记录→ 无风险";若未匹配成功,进入优先级规则。

优先级规则

优先级规则从上往下匹配,匹配到一条则不再继续往下匹配;若未匹配成功,进入默认 规则。

默认规则

需要将默认规则下的规则依次进行匹配,对所有匹配到的结果进行处理。

规则的上移下移

规则的位置会影响匹配的优先级,所以规则,需要上移下移,点击要移动的规则,点击"上 移"或"下移",改变规则顺序。

++ 添加策 + 添加號 略 则	见	◆下 移
规则名称	类型	操作
🔺 🌆 默认策略		添加 删除
111 黒名单	黑名单	删除
1100 白名单	白名单	
111 优先级	优先级	
💷 默认规则	无优先级	删除

规则的保存

一条规则设置完成后,一定要保存,未保存的配置在离开页面后会全部消失,操作人员 在配置的过程中一定要养成随时保存的良好习惯,如下图,点击"保存规则",弹出提示框 "保存成功",成功保存规则。

82



▶ 展开全部配置项▶ 折叠全部配置项● 保存规则			
🗎 保存规则	💊 展开全部配置项	ヘ 折叠	全部配置项
			🗎 保存规则

规则的展开

要配置某个条件的具体内容,需要先把规则条目展开。如下图所示,点击规则条目前面 的 "展开",展开此条目的配置栏,按实际需要配置好相应条目后,点击 "保存规则"。

🔨 折叠	🕈 选取	时间
天时间段		□ 0
周时间段		
月时间段		1 31
🌭 展开	🕈 选取	源 IP 地址
🌭 展开	🕈 选取	源应用程序
🌭 展开	🕈 选取	目标表
🍆 展开	🕈 选取	存储过程
🌭 展开	🕈 选取	操作
💊 展开	🕈 选取	受影响的行

条件的选取

一条规则有很多条件可选,但多数情况下并不需要所有的条件。在需要某个条件时,需要拉取规则,如下图所示,点击一个条件前的"选取",即此规则中选取了这个条件,只有被 拉取的条件才会在规则中生效,页面上被拉取到绿线内。



k. дт	 Tracels 	
▶ 辰井	◆ 取)月	山田
🌭 展开	🔸 取消	源 IP 地址
🌭 展开	🔸 取消	源应用程序
🌭 展开	🔸 取消	目标表
🌭 展开	🔸 取消	操作
🌭 展开	🔸 取消	ন্য]
🌭 展开	🔸 取消	操作系统主机名
🌭 展开	🔸 取消	存储过程
🌭 展开	↑ 选取	受影响的行
🌭 展开	1 选取	特权操作

条件是否包括

每个条件后面都有"包括"、"不包括"的选项。如下图,条件"目标表"已经展开,填写了表"help",若默认选择"不包括",则所有操作中未影响表"help"的都会匹配到此条件。

🔨 折叠	目标表					
		* *	help	4	◎包括	● 不包括
自定义: [Ŧ		

条件间的逻辑关系

设置规则时有许多可选条件,在一般情况下的配置中,我们只选取其中的一部分条件进行配置。这些条件之间是"与"的关系,一条操作在对此规则进行匹配时,需匹配规则下配置的所有条件才能成功匹配此规则。

规则配置



处理方式

如下图所示,处理方式包括"操作"、"日志记录级别"、"风险等级"三个内容。

🔨 折叠 🛛 处理2	行式	
操作	通过	~
日志记录级别	不记录	~
风险等级	无风险	~

左上角的"折叠"处可以选择"折叠"或"展开"。

"操作"分为三种,"通过"、"报警"、"阻断"。"通过"则不做任何额外处理。"报警"则依然通过,但会提示告警信息以便管理员及时发现问题。"阻断"则匹配到此条规则的操作会被阻断。

"日志记录级别"分为三种,"不记录"、"采样"、"总是记录"。"不记录"即凡是匹配 到此条规则的操作都不做记录。"采样"即匹配到此规则的操作随机记录部分。"总是记录" 即匹配到此规则的操作全部记录。

风险等级共五种,"无风险"、"低风险"、"中风险"、"高风险"、"致命"。为不同的 规则分别选择不同的风险等级,以便区分风险操作的危险程度。

时间

可以将客户端访问操作数据库的时间作为规则,如在非工作时间的操作可视为高风险。

🔦 折叠 🛛 💺 取消	时间
天时间段	□ 0
周时间段	
月时间段	1 31 🗘



源 IP 地址

每一项客户端对数据库的操作都包含源、目的 IP。其中"目的 IP"就是所操作的数据库的 IP,源 IP 即客户端 IP。规则可以针对源 IP 进行筛选。

▲ 折叠 + 取消 源 IP 地址				
172.16.0.126~172.16.0.126 192.168.0.167~192.168.0.167	* >>	A		
	• <<		◎包括	◉ 不包括
自 起始ip: 定 终止ip: 义		*		

选中要配入规则的 IP, 点击图中"》"后将此 IP 集配入规则,点击后如下图所示:

🔦 折叠	🕈 选取	源 IP 地址					
10.0.0.1	22~10.0.0.	123	* >> • <<	10.0.0.120~10.0.0.122	*	●包括	◉ 不包括
自 起始 [;] 定 义 终止;	p:				Ŧ		

在下方的"自定义"处添加 IP 后,点击"»"同样可以添加 IP 集到规则中。添加 好 IP 集,选择是否包括,保存后"源 IP 地址"条件生效。

源应用程序

源应用程序,即数据库客户端访问数据库服务的应用程序。



🔨 折叠	🔸 取消	源应用程序						
db2bp.e	xe		*		*	●包括	◉ 不包括	
自定义:]		-			

选择已经在全局参数配置好的源应用程序或自定义的应用程序,点击"》",选择是否包括,保存后,成功配置"源应用程序"条件。

目标表

目标表,即对数据库的操作实际所影响到的表。准确的设置目标表后,凡是涉及到该目标表的操作都会匹配此条件。设置方式同上。

🔨 折叠	● 选取	目标表				
			* >> *	A	●包括	◉ 不包括
自定义: [-		

存储过程

存储过程是在大型数据库系统中,一组为了完成特定功能的 SQL 语句集,存储在数据库中经过第一次编译后再次调用不需要再次编译,用户通过指定存储过程的名字并给出参数(如 果该存储过程带有参数)来执行它。选中已在全局参数配置好的存储过程或自定义,点击"》", 选择是否包括后,保存规则,成功配置条件"存储过程"。



🔨 折叠	🕈 选取	存储过程					
		~	· · ·	execute	*	◎包括	◉ 不包括
自定义: [Ŧ		

操作

"操作"指的是数据库操作具体的操作类别。分为"查询、添加、修改、删除、特权操作、登入、登出"七种操作,可选择其中的一项或几项。保存后成,功配置条件"操作"。

🔦 折叠	1 选取	操作			
查询 添加 修改 删除 特权操作 登入 登出			· · ·	*	◎ 包括 ® 不包括

受影响的行

"受影响的行"指的是数据库操作所影响的表中的行的数量,此项只对 mysql 数据库起作用。选择好限定条件大于、小于、等于等关系后,写入影响行数,如按图中设定,则影响大于等于 5 行的一条数据库操作会匹配到此条件。

影响行数		✓ 大于等于 ✓ 5 行 (注:该条件只对 mysql 数据库起 等工	作用)
🌭 展开	🕈 选取		
՝ 展开	🕈 选取	特权小于	
🌭 展开	🕇 选取	操作 <mark>大于等于</mark>	
🌭 展开		★1 ★1 不等于	



列

"受影响的列"指的是数据库操作所影响的表中的行名。添入相应的列名,选择是否包括后保存,成功设置条件"列"。

🔦 折叠 🛛 💺 取消 🛛 列			
@@character_set_database * xixi.* name `user_test2`.*	*	◎包括	● 不包括
自定义:			

特权操作

数据库中除了基本的增、删、改、查操作外的操作都称为特权操作。系统自带了特权操 作类型,选择要配置的特权操作类型,点击"》",选择是否包括后,保存规则,成功配置条 件"特权操作"。

Alter Create	^			
Deny Drop	>>			
Grant Kill	<		◎包括	◉ 不包括
Restore	 •			
自定义:				

操作系统主机名

操作系统主机,即数据库客户端访问数据库服务器的登陆系统的主机。添加操作系统的 主机名称作为条件选择是否包括,保存,成功设置条件"操作系统主机名"。



🔨 折叠	↑ 选取	操作系统主机名			
自定义: [× ×	•	◎包括	 不包括

操作系统用户名

操作系统用户,即数据库客户端访问数据库服务器登陆系统的用户。选择已经配置好的操作系统用户名或自定义操作系统用户名,点击"》",选择"包括"或"不包括"后保存,成功配置"操作系统用户名"条件。

ุ 新叠	♦ 取消	操作系统用户名		
自定义: [◆ ×	●包括	● 不包括

表组

在全局参数下配置好数据库表组后,在此处可以对数据库表组进行配置,匹配到表组下的表,则成功匹配到"表组"条件。



◆ 折叠 🔸 取消 表组	
自动学习 test	● 包括 ● 不包括

查询响应时间

"查询响应时间"指的是数据库查询的响应速度。选择好限定条件"大于、小于、等于" 等关系后,毫秒数,如按图中设定,则查询的响应时间大于等于5毫秒的查询会匹配到此条件。

🔦 折叠	↑ 选取	查询响应时间	
响应时间		☑ 大于等于 ∨ 5	臺秒
to RT	A Martin	等于	
▶ 焼井	▼ 选职	────────────────	
💊 展开	🕈 选取	数:小于	
💊 展开	↑ 选取	数: <mark>大于等于</mark>	
↘ 展开	↑ 选取	大于 敏: 云等于	

认证结果

认证结果,即一次操作的返回结果,执行是成功还是失败(只对登入动作有效),选择"成功"、"失败"或"全部"后,相应结果的操作会匹配到此条件。

ヘ 折叠	🔸 取消	认证结果
认证结果		● 失败 ● 成功 ● 全部 (注:1.该条件只对 登入 操作有效;2.需要开启 数据库应答监控 功能)



数据库与 Schema

数据库中的 Schema,为数据库对象的集合,一个用户一般对应一个 schema。为了区 分各个集合,数据库 Schma 需要一个名字,在数据库 Schema 集的设置中需要添加的就是 集合的名字。选择已经在全局参数配置好的数据库与 Schema 集,点击"》",选择是否包括 后,保存规则。

*oracle.*Schema	*	A		
	>>		●包括	◉ 不包括
自 数据库: 定 模式名: 义		Ţ		

数据库用户名

数据库用户名,即登录数据库的用户名称,当此条件中包含的数据库用户登录数据库或 做任何操作时,都会匹配到此条件。

🔦 折叠 🛛 💺 取消	数据库用户名			
tom dbm db2inst1	*	*	●包括	◉ 不包括
自定义:		Ŧ		

敏感数据访问

如果在"敏感数据扫描"模块下扫描出了数据库的敏感数据,开启判断敏感数据后,所 有对敏感数据的操作都会匹配到此条件。选择是否开启"判断敏感数据"后,保存规则,成 功配置条件"敏感数据访问"。



🔨 折叠	🕈 选取	敏感	数据访问	
判断敏感数	涺	◎是	●否	

发生次数

发生次数限定的是 IP 或用户的操作频率,按照图中设置,若任意 IP 在 1 秒内做了 5 次操作,则匹配到此规则。

🔨 折叠	↑ 选取	发生次数	
发生次数		ip	✔ 在1 秒 发生 5 次

SQL 异常

SQL 语句有时会提示异常,例如执行超时、表不存在等情况,启用 SQL 异常检测,在 SQL 执行出现异常时会匹配到此条件。

🔦 折叠	🕈 选取	SQL异常	
是否启用		◎启用	◉ 不启用

SQL 异常字符串

设置异常字符串后,会检测使 SQL 出现异常的字符串,添入 SQL 异常字符串,或通过 正则表达式确定 SQI 异常字符串格式,选择是否包括后,保存规则,成功配置条件 "SQL 异 常字符串"。

🔨 折叠	🕈 选取	SQL异常字符串			
SQL异常字符	守串				
			●包括	◎ 不包括	🖲 正则 🝞
▲ 折叠	1 选取	敏感字典			

SQL 异常字符串组



在全局参数下配置好 SQL 异常字符串组后,在此处可以对 SQL 异常字符串组进行配置。 SQL 语句匹配到 SQL 异常字符串组中的 SQL 异常字符串,则此条件被成功匹配。

ヘ 折叠	♣ 取消 SQL异常字符串组				
g1	A	>>> <	A		● 包括 ● 不包括
	-		Ŧ	,	

查询组

在全局参数下配置好查询组后,在此处可以对查询组进行配置。SQL 语句匹配到查询组 中的条目,则此条件被成功匹配。

◆ 折叠 🔸 取消 查询组		
(select,xixi) (update,xixi) (insert,xixi) (select,'user_test2')	*	▲ ● 包括 ● 不包括 ▼

3.2.3 最新流量

通过最新流量页面能够查看到日志列表,点选列表中的日志条目,在页面下侧将显示该 条日志的详细信息。如下图所示:



审	十防火墙 策略中心 最新流量											
日志列表												
审计防火墙	告警规师	9	风险等级	捕获时间		鉄据库用户	SQL类别		sul语句			
1 172. 17. 200. 190 :0	50000/swyle 塑动用	计/默认规则:无风险	无风险	2016-05-24 12:09:57		db2inst1	Select		SELECT + FROM SYSCA	T. SCHEMATA ORDER BT SCHEMANAR	I WITH UR	<u> </u>
2 172.17.200.190:6	2 172.17.200.190:60000/swgle 爱认策略-爱认规则:无风险) 无约		无风险	2016-05-24 12:09:57		db2inst1	Select		SELECT * FROM SYSCAT. DATATIFES WHERE METATIFE = 'S' ORDER BY TIPESCHEMA, TIPESAME WITH UR			
3 172.17.200.190:6	50000/smple 默认解释	计/数认规则:无风险;	无风险	2016-05-24 12:09:58		db2inst1	Select		SELECT 'R:' TRIM(SCHEMA) '.' SPECIFICHAME FROM SYSCAT. BUTINEAUTH WHERE (GRANTEETTPE = 'C			
4 172.17.200.190:6	SU000/sample 默认详细	計)默认规则:无风险;	无风险	2016-05-24 12:09:58		db2inst1	None		SELECT ANTHORITY PR	ON TABLE (STSPROC. AUTH_LIST_A	THORITIES_FOR_	AVTHED (?, 'V')) AS T WHERE 'T' IN
5 172.17.200.190:6	SU000/sample 默认解释	->獣认规则: 无风险 ;	无风险	2016-05-24 12:09:58		db2inst1	Login		login			
6 172.17.200.190:6	SU0DO/zample 默认解释	->獣认规则: 无风险 ;	无风险	2016-05-24 12:09:55		db2inst1	Login		login			
7 172.17.200.190.6	SUODO/sample Milling	->yonghu: 高印脸 ; 數认编唱->数认规则: 无	高风险	2016+05+24 12:07:48		db2inst1	Logout		logout			
8 172.17.200.190.6	SUODO/sample Milling	}->yonghu: 高印脸 / 數认策略->数认规则: 无	高风险	2016+05+24 12:07:48		db2inst1	Login		login			
9 172.17.200.190.6	30000/sample 塑心用	テ:原発が提べー課業が増く (別AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	嘉风险	2016-05-24 12:07:47		db2inst1	Logout		logout			
10 172.17.200.190:6	30000/sample 野认用#	}->yonghu: 高印絵 默认策略->默认规则: 天	嘉风险	2016-05-24 12:07:47		db2inst1	Logout		logout			
11 172.17.200.190:6	30000/sample 野认用#	->獣认规则:无风险 ;	无风险	2016+05-24 12:04:28		db2inst1	Select SHIEC		SELECT * FROM SYSCAT. SCHEMATA ORDER BY SCHEMANAME WITH UR			
12 172.17.200.190:0	20000/sample 塑认用用	计/默认规则:无风险 :	无风险	2016-05-24 12:04:25		db2inst1	Select SELECT * FROM SY		SELECT * FROM SYSCA	SCAT. DATATIFES WHERE WETATIFE = 'S' ORDER BY TIFESCHEMA, TIFENAME WITH UR		
13 172.17.200.190:6	20000/sample 默认策则	计/数认规则:无风险 ;	无风险	2016-05-24 12:04:25 db2in		di2inst1	Select SELECT 'B:' 1		SELECT 'B:' TRIM	CRIM(COCMENNA) '.' SPECIFICHAME FROM STSCAT. ROUTIMEAUTH FORMER (GRANTERTIFE = ')		
14 172.17.200.190:6	10000/smple 数认知	计)数认规则:无风险 ;	无风险	2016-05-24 12:04:25 db2inst1 Wes		None	SELECT ANTHORITY FROM TABLE (STSPECC ANTH_LIST_ANTHORITIES_FOR_ANTHOD (0, 'V')) AS I WHERE 'Y' I			ANTHER (", 'U")) AS I WHERE 'I' IN		
15 172.17.200.190:6	50000/smple 默认單語	計)數认規則:无风险;	无风险	2016-05-24 12:04:28	db2instl Log		Login	login				
16 172.17.200.190:6	SU000/smple 默认策图	計)數认規則: 无风险 ;	无风险	2016-05-24 12:04:25		db2inst1	Login		login			
17 172.17.200.190:6	SU000/sample 默认策要	->ip: 中风脸; 默认策略->默认规则: 无风险	中风险	2016-05-24 11:56:25		db2inst1	Logent		logaut			
18 172.17.200.190.6	50000/sample 數认解析	I→ip: 中风脸; 累认策略→累认规则: 无风险	中风险	2016-05-24 11:56:25		db2inst1	Logout		logout	locout		
19 172.17.200.190.6	20000/sample 塑心和	□->ip: 中风腔 ; 聖认策略->聖认規則: 无风腔	中风险	2016-05-24 11:56:28		db2inst1	Logout logout		logout			
20 172.17.200.190.6	SUCCO/sample Milling	┣->ip:中风腔) 默认策略->默认规则:无风腔	中风险	2016-05-24 11:56:28		db2inst1	Login		login			
21 172 17 200 190 6	SUODO/sample Milling	}->ip: 中风脸 ↓	中风险	2016-05-24 11:56:26			None		Session Start			-
30 • • • •	第1 共II页 H O											显示1到30,共486记录
审计防火增名称	172.17.200.190:60000/sample	数据库实例	test1		双摆车 关于	l		DB2		数据库用户		db2inst1
操作类型	Table	操作对象	SYSCAT.SCH	EMATA 数据库IP				172.17.200.190		音户))(P)		172.16.0.88
数据库MAC	00-00-00-00-00	客户講MAC	00-00-00-0	00-00-00 主机名				Lenovo-PC		操作系统用户		
有户讲程序	程序 db2jcc_application 音户接用户名 音户接用户名		寮户決決 日	1		50185		捕获时间		2016-05-24 12:09:57		
执行时长(驚秒)	0	助作	通过		日志級則			总是记录		风险攀级		无风险
告誓规则	默认策略->默认规则:无风险;	SQL舞剧	Select		哨应状态			未知				
SQL槽句	SELECT * FROM SYSCAT.SCHEMATA OR	DER BY SCHEMANAME WITH UR										
00100												

3.3 设备和敏感数据扫描

所属用户: SecAdmin。

扫描与发现功能是用于确定网络中用户核心数据库和关键数据位置的有效方法。管理员 可以配置扫描范围并进行扫描,扫描发现执行完毕后,即可配置监测这些发现的项目并对访 问它们的行为进行监控和报告。数据库审计设备允许您根据要求和网络的情况创建自定义默 认扫描。



扫描发现 服务发	发现 数据发现
扫描引擎列表 《	引擎名称: test
+添加 童 删除	配置 凭证 扫描 高級
名称 类型 状态	扫描使果媒作 目前不知到规则
test 数据扫描 已扫描 db2 数据扫描 已扫描 orcal 数据扫描 6%	数据类型选择 Ø 姓名 Ø 申請 Ø 电描 Ø 身份证号 Ø 邮编 Ø 帐号 Ø 地址 Ø 申請 Ø 很行识别代码 Ø 药物名称 Ø 密码 Ø 很行;卡号 Ø
	扫描设置 @ 扫描视图 @ 扫描系统库
	日補助排除所造范围 ・日補助排除所造范围 対策率设置 ・设置対策等 対策等设置 ・设置対策等

3.3.1 模块构成

扫描与发现功能由2部分构成:服务扫描、数据库扫描。

服务发现:服务发现功能能够扫描网络中的开放端口以及确定这些监听端口的服务。 如主机 IP、端口、主机操作系统类型和服务的类型等。并实现自动或手动将这些服务添加到 "引擎"上的功能。

数据发现:通过对数据库服务器的扫描,实现对数据库的表名称、schema、敏感数据、敏感表等的自动发现,帮助用户快速定位核心数据资产并对其实施保护。

3.3.2 服务扫描

扫描引擎界面如下图所示



	扫描发现 服务发	规 数据发现	见								
扫描引	攀列表 《	引擎名称: te	st								
+ 添	10 🏦 删除	配置	凭证	扫描	高级						
名称	类型 状态	扫描结果操作		🔲 自动添加到期	QQU						
test db2 orcal test1	数据扫描 已扫描 数据扫描 已扫描 数据扫描 63 服务扫描 已扫描	数据类型选择 扫描设置	i	 ✓ 姓名 ✓ 药物名称 ✓ 扫描视图 	 ✓ 邮箱 ✓ 密码 扫描系统库 	 ✓ 电话 ✓ 银行卡号 	☑ 身份证号	☑ 邮编	☑ 地址	☑ 总额	
		扫描范围设置	ł	 扫描时排除用 数据库设置 数据表设置 	f违范围 ● 只 ⑦ 设置 ② 设置	扫描所选的范围 数据库 数据表					
		■ 保存									

3.3.2.1 添加服务扫描

1.在扫描功能页面中,选择"扫描发现">"添加"。出现添加扫描引擎窗口;
 2.在添加扫描引擎窗口中,选择扫描类型为:"服务扫描"
 3.输入引擎名称,点击"确定"按钮后完成添加扫描引擎。



扫描发现服务发	扫描发现 服务发现 数据发现										
扫描引擎列表 《	引擎名称: test										
+添加 童 删除	配置 凭证	扫描	高級								
名称 类型 状态	扫描结果操作	🔲 自动添加到规	2.00								
test 数据扫描 已扫描		✔ 姓名	✓ 邮箱	☑ 电话	☑ 身份证号	☑ 邮编	☑ 帐号	☞ 地址	☑ 总额	☑ 银行识别代码	
db2 数据扫描 已扫描 orcal 数据扫描 6%	数据类型选择	☑ 药物名称	☑ 密码	☑ 银行卡号							
test1 服务扫描 已扫描	扫描设置	✓ 扫描视图	□徳辺図 🗸 江道安治会官								
			(洗花園 ◉ 只括)	3描所洗的范围							
	扫描范围设置	数据库设置	The aller								
		数据表设置	添加引擎	and a last							
	The little		扫描类型	服労扫描	~						
	目 保仔		引擎名称	test2							
						✔ 确定					

3.3.2.2 删除服务扫描

1.在扫描引擎列表中,选中要删除的服务扫描引擎,选择 "删除"。出现删除扫描引擎 窗口;

2.在删除扫描引擎提示框中,点击"确定"按钮后删除选定的扫描引擎。



扫描发现服务发	发现 数据发现
扫描引擎列表 《	引擎名称: test2
+添加 童 删除	政责 扫描 高级
名称 类型 状态	扫描結果操作 目前添加到引擎
test 数据扫描 已扫描	网段设置 ⑧ 本网段内 ◎ 法舆时地址组 ◎ 设定网段
4b2 数据扫描 已扫描	 · · · · · · · · · · · · · · ·
orcal 数据扫描 b%	
test2 服务扫描 未扫描	22378ECKEREBIRGLERE Common Port group
	Image: All (金田邨: All (金田 和))))))))))))))))))))))))))))))))))))

3.3.2.3 配置

扫描引擎配置界面如下图所示:



	扫描发现服务发	定现 数据发现							
扫描引擎	3攝51學列表 《 31學名称: test2								
+ 添加	Sha 💼 M9% 💼 🕅 🕰 🕹 🖓								
名称	类型 状态	扫描结果操作	🗌 自动添加到引	寧					
test	数据扫描 已扫描	网段设置	 本网段内 (〕 洗择IP地址组 ○ 设5	全网段				
db2	数据扫描 已扫描		□设定端□范围	1					
orcal	数据扫描 6%								
test1	服务扫描 已扫描	端口设置	选择已设定的	│周田组: Common Portg	roup 🗸	B			
test2	服务扫描 未扫描								
			🗹 ALL (全部都	不选表示扫描时不限制服	务类型)				
			CACHE	DAMENG6	DAMENG7	✓ DB2	GBASE	INFORMIX	KINGBASE
		服务类型	KSTORE	MS-SQL	MYSQL	ORACLE	POSTGRESQL	SYBASE	TERADATA
			FTP	🗹 НТТР	MTTPS				
		单一IP超时设置	500	(1~9999)秒					
		■ 保存							

配置方法如下:

在扫描引擎列表中,选中已经添加的扫描引擎,出现引擎配置信息界面;

选择"配置"页面,配置如下信息:

扫描结果操作:

自动添加到引擎: 扫描完成后自动添加到引擎列表中

网段设置:

本网段内:扫描当前网段;

选择 IP 地址组: 扫描设置的 IP 地址组(在 "高级"页面中设置 IP 地址组);

设定网段:扫描设置的特定网段;

端口设置:设置扫描的端口(在"高级"页面中设置端口组)

服务类型:

ALL: 表示以下所有服务类型;



CACHE、DAMEN6、DAMEN7、DB2、GBASE、INFORMIX、KINGBASE、KSTORE、 MS-SQL、MYSQL、ORACLE、POSTGRESQL、SYBASE、TERADATA、FTP、HTTP、 HTTPS

用户可根据需要选择上述所列任意组合的服务类型进行扫描;

扫描超时设置:扫描超时返回时间,默认 500 毫秒。

配置完成后,点击"保存"按钮完成配置扫描引擎。

3.3.2.4 扫描

立即扫描

1.在扫描页面中,选择配置完成后的服务扫描引擎名称,点击"扫描"子页面进入服务 扫描功能页面;

2. 在扫描页面中,选择立即扫描,开始进行服务扫描,并实时显示扫描进度。

	扫描发现 服务物	现 数据发现	
扫描引	擎列表 《	引擎名称: test2	
+ 添加	0 💼 删除	配置 扫描 高级	
名称	类型 状态	立即扫描 Q 立即扫描 Q 停止扫描	
test	数据扫描 已扫描	启用任务	
db2	数据扫描 已扫描		
orcal	数据扫描 6%	□ 保存	
testl	服务扫描 已扫描		
test2	服労扫描 30%		

定时扫描



如果需要设置定时扫描功能,可以进行如下设置:

1. 在扫描页面中,勾选"启用定时扫描",展开定时扫描配置项;

2.设置定时扫描选项:

频率设置:设置扫描只执行一次,或者是重复执行

定时设置:设置扫描执行的时间和周期

开始日期:设置定时扫描开始日期

3.设置完成后,点击"保存"后,系统会按照用户的设置,定时调度扫描服务进行扫描。

扫描发现 服务发	扫描发现 服务发现 数据发现									
扫描引擎列表 《	引擎名称:test2									
+添加 💼 删除	配置 扫描	高級								
名称 类型 状态	立即扫描	Q. 立即扫描 Q. 停止扫描								
test 数据扫描 已扫描	启用任务									
db2 刻塘扫描 已扫描 orcal 数据扫描 6%	定时扫描设置									
test1 服务扫描 已扫描		(i) th/f—/*								
test2 服务扫描 95%										
	频率设置	愛 "执行一次": 按配置执行一次在号,在时间条件符合时执行扫描,配置不再保存; "重复执行": 按配置循环检测任务,在时间条件符合时执行扫描,配置不会清除。								
	定时设置	 ※ 每日注順 ◎ 每原扫描 ◎ 每月扫描 设置 20 <								
	开始日期	2016-05-06								
	日 供存									

3.3.2.5 高级设置

高级设置菜单中,设置 IP 组集合和端口组集合,在服务扫描配置时使用。 高级设置默认初始界面如下所示:



	扫描发现 服务发现 数据发现								
扫描引導	攝引擎列法 《 引擎名称: test2								
+ 添加	💼 स्राह्य	E	配置 扫描 高級						
名称	类型	状态	D'91#A						
test	数据扫描	已扫描							
db2	数据扫描	已扫描	名称 歐置信息						
orcal	刻港扫袖	5%							
test2	服务扫描	己扫描							
	10771414	CIAM							
			磷口组集合						
			◆ 法加 ◆ 法加子项 / 编辑 盦 ₩%						
			名称 配置信息						
			D Comon Fort group						
			D ADC Default Port						
			1						

IP 组集合

IP 组集合添加初始页面如下图所示:

引擎名称: server_scan										
配置	扫描	高级								
IP组集合			添加卫地址组							
+添加 +	添加子项	/编辑 💼	IP组名称							
名称		配置信!	初始配置	□ 增加IP组的初始设置						
					✔ 确定					

1. 在扫描引擎列表页面中,添加的扫描引擎后,进入高级设置页面;

2.选择 IP 组集合>"添加",弹出添加 IP 地址组窗口

3. 输入 IP 组名称, 点击"确定"按钮后完成添加扫描引擎。



引擎名称: server_scan									
配置	扫描	高级							
卫组集合			添加卫地址组						
♣ 添加	+ 添加子项 🖌	🛚 编辑 💼	IP组名称	ip_group1					
名称		配置信)	初始配置	□ 增加IP组的初始设置					
					✔ 确定				
		C							

4.选择成功添加的 IP 组集合名称后,点击"添加子项",弹出如下图所示页面,根据需要选择设置 IP 类型和 IP 地址后,点击"确定"按钮后完成添加 IP 组。

引擎名称: server_scan					
配置 扫描	高级				
IP组集合					
+添加 +添加子项	🥖 编辑 🛛 💼 删除				
名称	配置信息				
ip_group1					
		添加卫设置			
		类型	单一IP	~	
		IPtttt	单—IP		
			IP范围 IP网段		
			11 1342		✔ 确定
		<u></u>			

端口组集合

端口组集合初始页面如下图所示:



端口组集合									
🕂 添加 🕂 添加子项 🥒 🏼	扁辑 💼 删除								
名称	配置信息								
▷ 🦲 Common Port group									
▷ 🦲 ADC Default Port									

默认 Common Port group 和 ADC Default Port 两个集合可以包括常大多数见服务端

口;

如果用户需要自己定义端口组集合,操作步骤如下:

1. 在扫描引擎列表页面中,选择添加的扫描引擎后,进入高级设置页面;

2.选择端口组集合>"添加",弹出添加端口组窗口

3. 输入 "端口组名称", 点击 "确定" 按钮后完成添加扫描引擎。

		添加端口组		X
		端口组名称	port_group	
端口组集合		引用已有设置		
🕂 添加 🕂 添加子项 🏒	👂 编辑 🛛 🏛 刪除			
名称	配置信息	初始配置	□ 增加端口组的初始设置	
⊳ 🦲 Common Port group			🛩 ā	解 定
▷ 🧰 ADC Default Port				

4.选择成功添加的端口组集合名称后,点击"添加子项",弹出如下图所示页面,根据需要选择设置服务类型和对应的端口后,点击"确定"按钮后完成添加。



		添加端口设置	1	×
		服务	oracle	
端口狙集合		端口	 	
+ 添加 + 添加子项 🥢 🖇	扁辑 💼 删除			确定
呂称	配置信息			
🗅 🧰 Common Port group				
🗅 🧰 ADC Default Port				
port_group				

3.3.3数据扫描

数据扫描模块对网络中的数据库进行扫描,并使用自定义算法对数据库中各种类型的数据进行分类。这些扫描信息可以用来保护针对敏感数据库的活动,并对此类活动进行审计。

对数据敏感表和字段扫描需要的配置包括确定在网络中搜索数据库和数据时使用的用户 名、密码、数据库类型、service ID(MSSQL),以及确定是否要将它们自动添加至引擎进行 监测和保护。

3.3.3.1 添加数据扫描引擎

在扫描功能页面中,点击"扫描发现">"添加"。弹出添加引擎窗口;
 在添加扫描引擎窗口中,选择扫描类型"数据扫描";
 输入引擎名称,点击确定按钮后完成添加扫描引擎。



扫描发现服务发	扫描发现 服务发现 数据发现								
扫描引擎列表 《	引擎名称: sss								
+添加 💼 🕬涂	配置 扫描	高级							
名称 类型 状态	Ⅲ组集合								
sss 服务扫描 未扫描	🕇 添加 🕂 添加子项 🥒 斜	離後 💼 删除							
	名称	配置信息							
			添加引擎		×				
			扫描类型	数据扫描 🗸					
			引擎名称	服务扫描 教掘扫描					
					✓ 确定				
	端口组集合								
	🕇 添加 🕂 添加子项 🥒 绯	輪 💼 删除							
	名称	配置信息							
	D 🚞 Common Port group								
	> 🧰 ADC Default Port								

3.3.3.2 删除数据扫描引擎

1.在扫描引擎列表中,选择要删除的数据扫描引擎;点击 "删除"。出现删除数据扫描 引擎窗口;

2.在删除扫描引擎提示框中,点击"确定"按钮,删除选定的扫描引擎。

	扫描发现 服务发现 数据发现										
扫描引擎列表 《 引擎名称: cccc											
+ 添加	童 明修余	武法	凭证 扫描	高级							
名称	类型 状态	扫描结果操作	🔲 自动添加到	规则							
0000	服务扫描 未扫描 数据扫描 未扫描	数操类型选择	 姓名 	 邮箱 密码 	 □ 电活 □ 银行+号 	□ 身份证号	🔲 邮编	□ 帐号	□ 地址	🔲 总额	□ 银行识别代码
		扫描设置	□ 扫描视图 〔	扫描系统库							
		扫描范围设置	 扫描时排除 数据库设置 数据表设置 	所法范围 0 F 0 设置 0 设置	提示 ④ 确定删除吗	?					
		● 保存			V 1	社 取消					


3.3.3.3 配置

1.在扫描引擎列表中,选择添加的数据扫描引擎。出现引擎配置信息界面;

2.配置条目如下:

扫描结果操作:勾选"自动添加到规则"后,扫描完成后自动添加到规则列表中;

数据类型选择:选择要扫描的数据类型,默认支持类型:姓名、邮箱、电话、身份 证号、邮编、帐号、地址、总额、银行识别代码、药物名称、密码、银行卡号,用户可根据 需要自定义扫描类型;

扫描设置: 可根据用户数据需要, 选择"扫描视图"或者"扫描系统库";

扫描范围设置: 设置扫描的范围;

数据库设置:设置数据库,手动添加需要扫描的数据库;

数据表设置:手动设置要扫描的数据表及其列名;

3. 配置完成后,点击 "保存"按钮完成配置数据扫描引擎。

扫描发现服务》	发现 数据发现								
扫描引擎列表《	引擎名称: ecce								
🕈 添加 💼 删除	配置 凭证	扫描 高級							
名称 类型 状态	扫描结果操作	🔲 目动添加到规则							
sss 服务扫描 未扫描 cccc 数据扫描 未扫描	数据类型选择	姓名 即編 电波 특分간号 即編 ※응 地址 思訳 银行记号代码 劳物名称 包码 银行 문号							
	扫描设置	□ 扫描视图 □ 扫描系统库							
扫描范围设置		 · 扫描时排映新选范围 · 只扫描新选的范围 · 只扫描新选的范围 · 我還來说量 · 公童数编來 · 公童数编來 · 公童数编表 · 公童数编表 · 公童数编表 · 公童数编表 · · · · · · · · · · · · · · ·							
	₿ 保存								

3.3.3.4 凭证

凭证页面用来设置数据扫描时使用的数据库权限,方法如下:



1. 在扫描引擎列表中,选择已添加的数据扫描引擎。出现引擎配置信息界面;

2.单击选择"凭证"页面,配置如下信息:

扫描源:可以"根据服务扫描结果"配置扫描源,也可自定义进"配置新的来源" 进行配置,如下图所示:

扫描发现 服务》	扫描发现 服务发现 数据发现							
扫描引擎列表 《	引擎名称: ecce							
➡ 添加 童 刪除	配置 凭证 扫描 高級	Ŗ						
名称 类型 状态	⑧ 根据服务扫描结果							
555 服务扫描 未扫描	详细设置一根据服务扫描结果							
0000 颜梧扫抽 木扫袖	+ 添加 童 删除	添加扫描凭证一根据服务扫描线	結果 🛛					
	服务扫描名称 主机名	服务扫描名称	~	服务ID(SID)	服务器IP			
		服务器IP	✓ < 该输入	项为必输项				
		服务类型	~					
		主机名						
		服务ID (SID)						
		用户名						
		密码						
			D. 重置 🖌 确定 🗶 取消					
	◎ 配置新的未源							
	详细设置一配置新的来源							
	◆添加 量 删除							
	IP 3%		主机名		服务ID (SID)			

3. 配置完成后(例如: 配置新的来源), 点击 "保存"按钮完成配置凭证。

扫描 服务发现	数据发现 接入发现			
扫描引擎列表 《	引擎名称: data_scan			
🛨 添加 💼 删除	配置 凭证 扫描	高級		
名称 类型 状态	◎ 跟攜服务扫描结果			
server_s(服务扫描 已扫描	详细设置-根据服务扫描结果			
and her some solution and the	+添加 童 删除			
	服务扫描名称 主机名	服务	服务ID(SID)	服务器IP
	◎ 配置新的来源			
	详细设置-配置新的来源			
	+添加 童 删除			
	TD	補口	主机名	服泰TD (STD)
	11		all o'd mi	JR/Jab (Cab)



3.3.3.5 扫描

立即扫描

1.在"扫描发现"页面中,选择已添加的数据扫描引擎名称后,点击"扫描"配置页面, 打开数据扫描页面;

2.在数据扫描页面中,选择"立即扫描",开始进行数据扫描,并实时显示扫描进度。

	扫描发现 服务发现 数据发现							
扫描引擎	扫描引擎列表 《 引擎名称: eece							
╋ 添加	💼 刪除			西田田	凭证	扫描	高级	
名称	类型	状态		立即扫描		Q. 立即扫描		
sss	服务扫描	未扫描		白田仁久				
0000	数据扫描	未扫描					•	
				🗎 保存				

定时扫描

如果需要设置定时扫描功能,可以进行如下设置:

1. 在扫描页面中,勾选"启用定时扫描"页面展开定时扫描配置项;

2. 设置定时扫描选项:

频率设置:设置扫描只执行一次,或者是重复执行

定时设置:设置扫描执行的时间和周期

开始日期:设置定时扫描开始日期

3. 设置完成后,点击"保存"后,系统会按照用户的设置,定时调度数据扫描服务进行 扫描。



	扫描发	现服	服务发	现 数据发现	R						
扫描引擎	阿表		«	引擎名称: ccc	c						
+ 添加	💼 刪除			配置	凭证	扫描	高级				
名称	类型	状态		立即扫描		Q. 立即扫描					
555	服务扫描	未扫描		启用任务		✓ 房用完时扫描					
0000	数据扫描	未扫描		合叶扫描沉里							
	AEM'ST-HHIRE LE										
频率设置 定时设置		频率设置		 执行一次 重复执行 "执行一次" "执行一次" "重复执行" 	" : 按配置执行 " : 按配置循环	一次任务,在时间条件符 金测任务,在时间条件符	合时执行扫描,】 合时执行扫描,】	配置不再保存; 配置不会清除。			
			 ● 毎日扫描 ● 毎周扫描 ② 費 整点设置: 0 ✓ 整点 								
				开始日期		2016-04-27	17:				
1											

高级

在扫描功能页面中,选择相应的服务扫描引擎名称后,点击 "扫描发现"页面。
 点击数据扫描引擎,打开数据扫描页面;

2. 在数据扫描页面中,单击进入 "高级"设置页面,如下图所示:

数据库与应用安全加固系	数据库与应用安全加图系统 安全管理员: Seekahain 🔒 俗欢密码 🚺 安全港出 📮 返回主							
扫描发现服务发	扫描发现 服务发现 数据发现							
扫描引擎列表 《	引擎名称: cccc							
🕂 添加 💼 删除	配置 凭证	扫描 高級						
名称 类型 状态	数据类型							
sss 服务扫描 未扫描	▲ 添tm ▲ 添tma	216 帝 明修全						
cccc 数据扫描 未扫描	1745	ま ク	제소	具饰上度	** #1		由変	
	1110	4001	794	10/2 (V)52	×±		138	
	▶ □ 另历业与							
	▶ <u>□</u> 忌額							
	▷ 🗀 银行识别代码							
	▷ □ 药物名称							
	▷ □密码							
	▷ 🛄 银行卡号							

3. 在此页面中, 用户可以添加需要关注的数据类型设置, 在 "数据类型"项中单击 "添 加", 如下图所示:



扫描 服务发现 数据发现 接入发现									
扫描引擎列表 《	引擎名称: data_scan	引擎名称:data_scan							
+添加 畫 刪除	配置 凭证	國置 凭证 扫描 高級							
名称 类型 状态	数据类型	药据类型							
server_s(服务扫描 已扫描	◆ 添加 / 编辑 ◆ 添加子项 童 删除								
data_scar 颈張扫袖 木扫袖	名称	表名	列名		最短长度	类型	内容		
	▶□姓名								
	▶ 🛄 邮箱								
	▷ 🛄 电话								
	▷ 🛄 身份证号	添加数据类	型定义						
	▷ 💼 邮编	数据类型	名称	车牌号码					
	▶ 🚞 帐号				18 TR				
	▷ 🗀 地址				▼ RMAE				
	▷ 🗀 总额								
	▷ 🗀 银行识别代码								
	▷ 🛄 药物名称								
	▶ 💼 密码								
	▷ 🗀 銀行卡号								

4.选中自定义添加的数据类型,点击 "添加子项,"设置数据类型的内容后,点击 "确 定"即可。

扫描 服务发现	数据发现 接入发现							
扫描引擎列表《	引擎名称: data_scan							
+添加 💼 删除	配置 凭证	扫描	高级					
名称 类型 状态	数据类型							
server_s(服务扫描 已扫描	+ 添加 🥒 編輯 + 添加子	项 💼	田邦余					
data_scar 颈鴉扫抽 木扫油	名称	表名		列名	最短长度	类型	内容	
	▶□姓名		添加数据类型		×			
	▷ 💼 邮箱		添加数据类型模式	基于名称模式 🗸 🗸				
	▶ 🗀 电话		本々称	car				
	▷ 🛄 身份证号		2010/02	cai				
	▷ 🧰 由終編		列名称	number				
	▷ ○ 帐号		最短长度	6				
			-14-701	had				
			~=	rui				
					✔ 确定			
	2 二 57 的名称							
	2 山 依旧下ち							
	日中府与时							



3.3.4 服务发现

3.3.4.1 服务发现结果

1.单击 "服务发现" > "服务器发现结果"页面,页面显示服务发现的扫描结果,如 下图所示:

	服务发现							
务署发现结果	开始时间		9 结束时间		任务名称	~		
#	RSHIP		得多文化		0			
~ * * #	in the little		100 L		4 100 6 110 6 700	18 da 17 da	18 A. 17 (4 17 A	1.0.1.000.00
方尖堂	F38007161	服労當17 服労購口	服労省	000 D	本信思	操作系统	操作系统版本	加入加回点
作系统类型	1 2015-04-03 1	3:43:C 172.16.4.9.443	RTTPS	open T	LS 1.0	LABORN	2.6.3	
	2 2015-04-03 1	3:43:U 172.16.4.1 21	FIF	open F	ileZilla ftpd U.9.41 beta	Microsoft Windows	7 (2008	-
	3 2015-04-03 1	3:43:1172.16.4.1 1433	NS-SQL	open M	icrosoft SQL Server 2008 10.0.1600;	Microsoft Windows	7 [2008	10.1.10000
	4 2015-04-03 13	3:43:11/2.16.4.1 1521	UKACLE	open O	racie INS Listener 11.1.0.6.0 (for	Microsoft Windows	1 12008	<u> C </u>
	5 2015-04-02 20):01:0 172.16.4.1 3306	WTSQL	open M	ySQL 5.5.23	Microsoft Windows	7 [2008	★加入加固点
	6 2015-04-03 13	3:43:1 172.16.4.1 523	082	obeu I	BW DBZ Database Server 9.07.6	Linux	2.6.X	+ 加入加固点
	7 2015-04-03 13	3:47:4 172.16.4.1 443	HTTPS	2 argo	SL#3	Wicrosoft Windows	7 [2008	-
	8 2015-04-03 13	3:47:4 172.16.4.1:3306	WISQL	ogen M	pSQL 5.5.3-m3-community	Microsoft Windows	2003	+加入加固点
	9 2015-04-03 13	3:47:4 172.16.4.1 443	HTTPS	open T	LS 1.0	Linsus	2.6.X	-
	10 2015-04-03 13	3:47:4 172.16.4.1 443	HTTPS	open T	LS 1.0	Linux	2.6.1	-
	11 2015-04-03 13	3:47:4 172.16.4.2 443	HTTPS	open T	LS 1.0	Linux	2.6.1	-
	12 2015-04-03 13	3:47:4 172.16.4.2 3305	WISQL	open M	ySQL 5.1.73	Linux	2.6.X	+ 加入加固点
	13 2015-04-03 13	3:47:5 172.16.4.2 8080	HTTP	opan A	pache Toncat/Coyote JSP engine 1.1	Linux	2.6.X	-
	14 2015-04-03 13	3:47:5 172.16.4.2 443	HTTPS	open S	SLv3	Microsoft Windows	7 2008	-
	15 2015-04-03 13	3:47:5 172.16.4.2 523	DB2	opan I	BM DB2 Databaze Server 9.07.6	Microsoft Windows	7 2008	+ 加入加固点
	16 2015-04-03 13	3:47:5 172.16.4.2 8080	HTTP	open A	pache httpd 2.2.22 ((#in32))	Microsoft Windows	7 2008	-
	17 2015-04-03 13	3:47:5 172.16.4.2 50000	DB2	open I	BM DB2 Database Server (QDB2/MT64)	Microsoft Windows	7 2008	+ 加入加固点
	18 2015-04-03 13	3:49:5 172.16.4.2 443	HTTPS	open T	LS 1.0	Linun	2.6.X 3.X	-
	19 2015-04-02 16	5:48:5 172.16.0.1 80	HTTP	open u	nimov	unknow os	2.4.X 2.6.X,,,,	-
	20 2015-04-02 16	5:48:5 172.16.0.1 443	HTTPS	open O	penSSL (SSLv3)	unknow os	2.4.1 2.6.1,,,,	-
	21 2015-04-02 15	5:38:4 172.16.0.2 21	FTP	closed u	nknow	unknow os	2.6.X 3.X 2.4.X, , , 3.X,	-
	22 2015-04-02 15	5:38:4 172.16.0.2 80	HTTP	closed u	nknov	unknos os	2.6.X 3.X 2.4.X, , 3.X,	-
	23 2015-04-02 15	5:38:4 172.16.0.2 443	HTTPS	open T	LS 1.0	unknow os	2.6.X 3.X 2.4.X, , , 3.X,	-
	24 2015-04-02 15	5:38:4 172.16.0.2 1433	WS-SQL	closed u	nknov	unknow os	2.6.X 3.X 2.4.X, , , 3.X,	+加入加固点
	25 2015-04-02 15	5:38:4 172.16.0.2 1521	ORACLE	closed u	nimov	unknow os	2.6.X 3.X 2.4.X, , , 3.X,	+加入加固点
	26 2015-04-02 15	38:4 172.16.0.2 3306	WTSQL	closed u	nknov	unknow os	2.6.X 3.X 2.4.X, , 3.X,	+加入加固点
	27 2015-04-02 15	5:38:5 172.16.0.2 50000	082	closed u	nimov	unknos oz	2.6.X 3.X 2.4.X, , 3.X,	+加入加固点
	28 2015-04-02 16	5:48:5 172.16.0.3 21	FTP	open F	ileZilla ftpd 0.9.41 beta	unknow os		-

2. 用户可以按需求定制查询扫描发现的服务;

3.3.4.2 概要

1.单击"服务发现">"概要"页面,页面显示服务发现的概要信息,如下图所示:





2.用户可以按条件进行过滤筛选 点击 "概要" > "条件筛选"

数据库与应用安全加固新	系统				安全	管理员: Sed	Admin		
扫描发现服务	发现 数据发现								
服务扫描结果	概要								
服务器发现结果	Q 条件筛选	Q 条件筛选 🕞 报表导出							
概要	不同网段的服务的	数 里			操作系统	物里			
服务类型									
操作系统类型	条件过滤	不同网络的服务的数量 【】 【】 【】 【】 【】 【】 【】 【】 【】 【】 【】 【】 【】							
	扫描引擎	~							
	开始时间	12	服务器IP						
	结束时间	12	服务端口						
	端口状态	×	服务器操作系统				-		
	服务类型	×	服务版本						
				Q 查询	■ 重置	🗙 取消			

3.用户可以导出报表,点击"概要">"报表导出"



扫描发现 服务发行	现 数据发现				
服务扫描结果	概要				
服务器发现结果	Q 条件筛选 🔄 报表导出				
概要	不同网段的服务的数里				
服务类型					
操作系统类型	🛢 导出选项 🛛 🔀				
	· R表格式 PDF格式 ~				
	PDF格式				
	EXCEL格式 ● 40元 ● 取消				
	5 WORD格式				

3.3.4.3 服务类型

1.单击"服务发现">"服务类型"页面,页面显示服务发现的服务类型信息,如下图所示:



扫描 服务发现	2 数据发现 接入发现	
	服务类型	
服务器发现结果	Q.条件筛选 😨 报表导出	
板麦	服务类型占比	不同问度服务占比
服务类型	服务类型占比	不同阿提服务占比
鞍作系线 类型	MS-SQL 05 ORACLE 75 TENET: 65 TENET: 65	60 20 80.METER SENSITIONE AND DE ANDRE DI DESCRIT ON EL COMPLEX SAMA CARD STAND TO DESCRITO DE ANDRE
		修売支担除本占比 60 40 20 20 10 10 10 10 10 10 10 10 10 1
	BANNER AN BERTTALETMARRONOMENERUMANNAN OVER OTBEN CHANNAN AND FRANKLINGEN BERTANDER BERTAN BERTANDER BERTANDER BERTA	CALMERZ #65.04517811938979001806/0912040698910910010985415090-040191640199194640199194640199194640199194640199 CALLMERZ97 ALTON AUTH ALT WEATH PROMYS SQL SERVER

2.用户可以按条件进行过滤筛选 点击"服务类型">"条件筛选"

扫描发现 服务发	现 数据发现
服务扫描结果	服务类型
服务器发现结果	Q条件筛选 💂 报表导出
概要	ander sie mit 111.
服务类型	条件过滤
操作系统类型	
	开始时间 證 服务器IP
	结束时间 證 服务端口
	端口状态
	服务类型 ✓ 服务版本 — — — — — — — — — — — — — — — — — — —
	Q. 查询 📭 重置 🗮 取消

3.用户可以导出报表,点击"服务类型">"报表导出"。



扫描发现 服务发现	见 数据发现		
服务扫描结果	服务类型		
服务器发现结果	🔍 条件筛选 🔄 报表导出	出	
概要	andrask mildelle		
服务类型	🛢 导出选项		
操作系统类型	报表格式	PDF格式 V	T I
		PDF格式 EXCEL格式 · · · 确定 X 取消	л
		WORD格式	٦

3.3.4.4 操作系统类型

1.单击"服务发现">"操作系统类型"页面,页面显示服务发现的操作系统类型信息,如下图所示:





2. 用户可以按条件进行过滤筛选,点击"操作系统类型">"条件筛选"。

扫描发现服务发	数据发现	
服务扫描结果	操作系统类型	
服务器发现结果	Q条件筛选 😨 报表导出	
概要	条件过渡	3
服务类型	扫描引擎	1
操作系统类型	开始时间 🛅 服务器IP	
	结束时间	
	端口状态 服务器操作系统	
	服务类型 / 服务版本 /	
	🔍 查询 🛛 📭 重置 🗮 🗙 取消	

3.用户可以导出报表,点击"操作系统类型">"报表导出"。

	扫描发现	服务发现	数据发现				
服务	S扫描结果		操作系统类型				
ļ	贤务器发现结果		Q 条件筛选	🔄 报表导出	4		
ŧ	要		🛢 导出选项				
J	服务类型		报表格式		PDF格式	-	
ŧ	操作系统类型				PDF格式		
					EXCEL格式	● ・ ・ ・ ・ ・ ● ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	■ 製油 P
			VRP: (1	0%)	WORD格式		



3.3.5 数据发现

3.3.5.1 数据发现结果

1.单击"数据发现">"数据发现结果"页面,页面显示数据发现的扫描结果,如下图所示:

扫描 服务	g现 数据发现 接入发现	Q.								
	数据扫描结果-表数据									
数据发现结果	开始时间	11 (d)	和时间	🛗 任务名和		~				
截要	服务器IP	He s	(美型	✓ Q 查述		保存到策略				
敏感数据服务器	Bijiji	服务器IP	主机名	救援库	模式名	表	表类型	服务类型	敏感	
数据类型分布	1 2015-04-02 18:19:04	172.16.0.13		orcl	STS	USERS	TABLE	OBACLE	V	
非常吃完到公布	2 2015-04-02 18:19:04	172. 16. 0. 13		orcl	STS	1800\$	TABLE	ORACLE	V	
数据库关望力型	3 2015-04-02 18:19:04	172. 16. 0. 13		orcl	STS	STARS	TABLE	OBACLE	V	
	4 2015-04-02 18:19:05	172.16.0.13		orcl	STS	VIEWTRCOL\$	TABLE	ORACLE	V	
	5 2015-04-02 18:19:05	172. 16. 0. 13		orcl	SYS	ATTROOL\$	TABLE	OBACLE	V	
	6 2015-04-02 18:19:05	172.16.0.13		orcl	STS	COL\$	TABLE	OBACLE	V	
	7 2015-04-02 18:19:05	172.16.0.13		orcl	STS	C08\$	TABLE	ORACLE	4	
	8 2015-04-02 18:19:05	172.16.0.13		orcl	STS	TS\$	TABLE	OBACLE	V	
	9 2015-04-02 18:19:05	172.16.0.13		orcl	STS	08,7\$	TABLE	OBACLE	V	
	10 2015-04-02 18:19:05	172.16.0.13		orcl	STS	UGBOUP\$	TABLE	OBACLE	V	
	11 2015-04-02 18:19:05	172.16.0.13		orel	STS	5118\$	TABLE	OBACLE	V	
	12 2015-04-02 18:19:06	172.16.0.13		orcl	STS	PROFILANE\$	TABLE	OBACLE	V	
	13 2015-04-02 18:19:06	172.16.0.13		orcl	STS	LINUS	TABLE	OBACLE	V	
	14 2015-04-02 18:19:06	172. 16. 0. 13		orcl	STS	PROPS\$	TABLE	OBACLE	V	
	15 2015-04-02 18:19:06	172.16.0.13		orcl	STS	INCEIP	TABLE	OBACLE	W	
	20 💌 📢 📢 第	1 共14页 🕨 射 🐧							显示1到20	0,共263记录
	数据扫描结果-列数据									
	列名称	列数	國典型	长度		扫描数据类	1	扫描模式		

2.用户可以按需求定制查询扫描发现的服务。

3.3.5.2 概要

1.单击"数据发现">"概要"页面,页面显示如下图所示:





2.用户可以按条件进行过滤筛选,点击"概要">"条件筛选"。

扫描发现 服务发	现 数据发现			
数据扫描结果	概要			
数据发现结果	🔍 条件筛选 📮 报:	表导出		
概要	条件过渡			
敏感数据服务器	扫描引擎	~	数据类型	~
数据类型分布	开始时间	12	服务器IP	
数据库类型分布	结束时间	12	服务端口	
	服务类型	~	主机名	
	DB名称		Schema名称	
	表名称		表类型	
	列名称		列类型	
	列最小长度		扫描模式	
				Q 查询 🖸 重置 🗶 取消

3.用户可以导出报表,点击"概要">"报表导出"。



扫描发现 服务发现	2 数据发现			
数据扫描结果	概要			
数据发现结果	🔍 条件筛选 🔄 报表导出	L		
概要				
敏感数据服务器	■ 导出选项			1
数据类型分布	报表格式	PDF格式 V		基于网段
粉很庆贵刑公五		PDF格式 EXCEL格式	✓ 确定 ¥ 取消	
纵顶件关望 万仰	etrol	WORD格式		IJ

3.3.5.3 敏感数据服务器

1.单击 "数据发现" > "敏感数据服务器"页面,页面显示如下图所示:

副 数据发展 接入发展			
敏感數据服务器			
Q、条件筛选 🔄 报表导出			
基于服务器的敏感数据分布		基于	干服务器的服务类型分布
	基于服务器的敏感数据分布		基于服务器的服务类型分布
300			mysql: 1 % \ / ms-sql: 1 %
200 100 0 172.16.0.12	172.16.0.13 17 电线 数	2.16.0.253	oracle: 98 %
	取認規模 接入发現 接合数据为2 Q 条件研究 G 新件研究 G 新件研究 G 新件研究 G 新生活 G 新生 G 新	数据发现 後続 数据方式 全 和件研究 200 200 200 200 100 0 172.16.0.12 172.16.0.13 172.	RS# 24現 HA 24 H

2.用户可以按条件进行过滤筛选,点击"敏感数据服务器">"条件筛选"。



扫描发现 服务发行	现 数据发现				
数据扫描结果	敏感数据服务器				
数据发现结果	🔍 条件筛选 😨 报:	表导出			
概要	条件过滤				X
敏感数据服务器	扫描引擎	~	数据类型	~	
数据类型分布	开始时间	1 00 120	服务器IP]
数据库类型分布	结束时间	12:	服务端口		
	服务类型	~	主机名		
	DB名称		Schema名称		
	表名称		表类型		
	列名称		列类型		
	列最小长度		扫描模式	×]
				Q 查询 🖪 重置 🗙 职	消

3.用户可以导出报表,点击"敏感数据服务器">"报表导出"。

扫描发现 服务发现	见 数据发现			
数据扫描结果	敏感数据服务器			
数据发现结果	Q 条件筛选 🔄 报表导出			
概要	🛢 导出选项			
敏感数据服务器	报表格式	PDF格式 V		
数据类型分布		PDF格式		
数据库类型分布		EXCEL格式 WORD格式		
	20			

3.3.5.4 数据类型分布

1.单击"数据发现">"数据类型分布"页面,页面显示如下图所示:





2. 用户可以按条件进行过滤筛选,点击"数据类型分布">"条件筛选"。

扫描发现 服务发现	2 数据发现		
数据扫描结果	数据类型分布		
数据发现结果	🔍 条件筛选 🔄 报表导出		
概要	条件过滤		X
敏感数据服务器	扫描引擎	✓ 数据类型	
数据类型分布	开始时间	提 服务器IP	
数据库类型分布	结束时间	記服务端口	
	服务类型	▶ 主机名	
	DB名称	Schema名称	
	表名称	表类型	
	列名称	列类型	
	列最小长度	扫描模式	×
			Q 查询 🛛 🗣 重置 🗮 取消

3.用户可以导出报表,点击"数据类型分布">"报表导出"。



扫描发现 服务发现	2 数据发现	
数据扫描结果	数据类型分布	
数据发现结果	🔍 条件筛选 🔓 报表	导出
概要	🛢 导出选项	
敏感数据服务器	报表格式	PDF格式 V
数据类型分布		PDF格式
数据库类型分布	密码: (11 %) ―	EXCEL格式 WORD格式

3.3.5.5 数据库类型分布

1.单击"数据发现">"数据库类型分布"页面,页面显示如下图所示:

扫描 服务发现	数据发现 接入发现	
	數据库类型分布	
盘锯发现结果	Q、条件筛选 😡 报表导出	
截要	教姻库类型	基于服务类型的敏感数据分布
敏感数据服务器	數据床类型	基于服务类型的敏感数据分布
政制 (天主 2) 94 截 图 序类型分布	mysql: 1 % ms-sql: 1 %	200 200 100 0
	🔲 ms-sql 📕 oracle 🔛 mysql	🔳 1 🔳 电话 💴 姓名

用户可以按条件进行过滤筛选,点击"数据库类型分布">"条件筛选"。



扫描发现 服务发现	观 数据发现				
数据扫描结果	数据库类型分布				
数据发现结果	🔍 条件筛选 📓 报	表导出			
概要	条件过渡				
敏感数据服务器	扫描引擎		数据类型		~
数据类型分布	开始时间	17	服务器IP		
数据库类型分布	结束时间	12	服务端口		
	服务类型		主机名		
	DB名称		Schema名称		
	表名称		表类型		
	列名称		列类型		
	列最小长度		扫描模式		~
				Q 查询	重置 🗙 取消

3.用户可以导出报表,点击"数据库类型分布">"报表导出"。

扫描发现 服务发现	观 数据发现	
数据扫描结果	数据库类型分布	
数据发现结果	Q条件筛选 🔄 报表导出	
概要		
敏感数据服务器	报表格式PDF格式	
数据类型分布	PDF格式	mysql
数据库类型分布	mysql: (25 %) WORD格式	



3.4 风险扫描

所属用户: SecAdmin。

数据库系统是一个复杂的系统资料,数据库存在许多风险,其中不少是致命的缺陷和漏洞。一旦遭到攻击,攻击者可能以 DBA 的身份进入数据库系统,也可能进入操作系统,下载整个数据库文件。为此本系统提供风险扫描模块,为用户能更早的发现风险与漏洞。

3.4.1 添加风险扫描

进入 "通用配置" > "选择引擎",点击添加风险扫描按钮,如下图所示。

数据库	川擎 用户管理							
数据库引擎列表								
+添加 / 编辑 Q 自动发现								
名称	类型	IP	端口	缺省数据库	审计防火墙	状态监控	风险扫描	
172.17.200.190:6000	0 DB2	172, 17, 200, 190	60000	test1	▋ 1111111111111111111111111111111	+ 添加	+ 添加	
172.17.200.194:3306	/ MYSQL	172. 17. 200. 194	3306	testdb	🔢 <u>详情</u> 📅 删除	■ 道情 💼 删除	-	
192.168.0.98:3306/m	y MYSQL	192.168.0.98	3306	mysql	IIII <u>详情</u> 📅 删除	+ 添加	-	

点击添加按钮后,需输入如下信息:

名称: 该风险扫描的名称。

用户名: 该数据库管理员的用户名。

密码: 该数据库管理员的密码。

缺省数据库:系统默认的数据库。

以下信息输入完成后,点击"确定"后,完成风险扫描的添加。如下图所示。



添加数据库扫描	Ä	×
名称	172.17.200.190:60000/test1	
用户名	myadm	
密码		
缺省数据库	test1	
	✔ 确	定

3.4.2 引擎列表

选择该引擎可以进行"删除"操作。

3.4.3 数据库风险扫描

3.4.3.1 扫描策略

进入"风险扫描">"扫描策略"

扫描策略:扫描数据库时的策略,系统默认有"授权"、"系统"两个大的策略组,每个 大组包含了相应的策略,用户可根据自身需要选择相应的策略,策略选择完成后进行扫描, 系统将会根据所选的策略扫描出相应的风险。如下图所示:



添加策略组

点击"添加策略组"后,弹出添加策略组窗口。

策略名称: 该策略组的名称。

类型: 该数据库的类型。

勾选 "授权"、 "系统"两个大的策略组中需要添加的策略,点击保存,完成对该策略 组的添加。如下图所示:



添加策略组			×
策略组名称: test1	类型:	DB2	~
▲ 🔄 🗹 授权			
🗎 🗹 当前访问里			
▷ 🧰 🗖 系统			
			■ 1禾仔

授权

当前访问量

风险描述: 连接量过大可能导致服务运行缓慢甚至崩溃,也有可能是恶意攻击,管理员需及时查看原因。

产生原因:同一时间访问数据库量过多

系统



cat_cache 溢出

风险描述:检测 cat_cache 是否溢出。cat_cache 溢出将可能导致信息丢失并加大被 攻击的风险。

产生原因:缓冲区太小或被恶意操作。

cat_cache 堆溢出

风险描述: cat_cache 堆溢出将可能导致信息丢失并加大被攻击的风险。

产生原因:缓冲区太小或被恶意操作。

锁超时

风险描述:锁超时可能一直占用系统资源而导致无法返回结果。

产生原因:当一个进程访问数据库表或者字段的时候,另一个程序正在执行带锁的访问 (比如修改数据),那么这个进程就会等待,当等待很久锁还没有解除就会锁超时,报告一个 系统错误,拒绝执行相应 SQL 操作。

编辑策略组

编辑策略组:对已添加的策略组进行调整的操作,可以再进行策略的添加、删除操作以 及对策略组名称的修改。如下图所示:



编辑策略组			×
策略组名称: test1	类型:	DB2	~
▲ 😋 🗹 授权			
📄 🗹 当前访问里			
4 😋 🗹 系统			
📄 🗹 cat_cache 溢出			
📄 🗹 cat_cache 堆溢出			
📄 🗹 锁超时			

策略参数配置

- 参数配置:对相应的策略进行参数配置,有的策略会显示无需参数配置。
- 风险等级:系统对该风险级别等级的评定。
- 风险描述:描述该风险的具体情况以及解决的一些建议。
- 产生原因: 描述产生该风险的原因。



点击"保存"后,完成策略参数的配置。再此进行扫描,将会按照新的策略来扫描数据 库,发现相应的风险。如下图所示:

策略参数配置		
策略类型: DB2 ~		
▲ 🔁 授权		
📄 当前访问里		
4 🔄 系统	参数配置:	60000 毫秒
📄 cat_cache 溢出		
🖹 cat_cache 堆溢出	风险等级	低风险
前 () () () () () () () () () () () () ()		检测数据库运行过程中是否存在锁超时。锁超时可能一直占用系 统资源东导致主法 近回结果。
		统灾原则寻找尤本赵巴结未。
	风险描述	
		当一个进程访问数据库表或者字段的时候,另一个程序正在执行带动的访问(比如修改数据),那么这个进程就会等待,当等待
		很久锁还没有解除就会锁超时,报告一个系统错误,拒绝执行相 应sor 操作。
	产生原因:	
		□ 保存

风险扫描

这个模块是在前面策略组添加、策略组编辑以及策略组参数配置操作完成后,最终进行的最重要,也是本模块最核心的操作,即风险扫描。

用户: 数据库管理员的用户名。

风险策略:即添加编辑后的策略组名称。

点击 "扫描"弹出风险扫描窗口。如下图所示:



风险扫描				×
用户	sa	风险策略	dsf	
正在扫描【1	92.168.9.3:1433/master】存储	过程启动设置 : 无风险		•
正在扫描【1	92.168.9.3:1433/master】系统	表访问权限设置: 低风	验	
正在扫描【1	92.168.9.3:1433/master】用户	级联授权 : 无风险		
系统检测				
正在扫描【1	92.168.9.3:1433/master】存储	过程加密 : 高风险		
正在扫描【1	92.168.9.3:1433/master】触发	器加密 : 无风险		
正在扫描【1	92.168.9.3:1433/master】视图	加密 : 高风险		=
正在扫描【1	92.168.9.3:1433/master】复制	权限设置 : 无风险		
正在扫描【1	92.168.9.3:1433/master】审计	跟踪状态 : 无风险		
正在扫描【1	92.168.9.3:1433/master】C2 审	矿模式 : 无风险		
扫描完成				-
				☐ 开始扫描

弱口令检测

弱口令指的是仅包含简单数字和字母的口令,例如"123"、"abc"等,因为这样的口令 很容易被别人破解,从而使用户的计算机面临风险,因此不推荐用户使用。

点击 "开始检测,"将会显示出相应的弱口令。

3.4.3.2 历史报表

报表就是用表格、图表等格式来动态显示数据,可以用公式表示为:"报表 = 多样的格式 + 动态的数据"。历史报表记录了风险扫描的详细信息。提供给查询的人更加详细的信息,以便对当时存在的风险有一个直观形象的了解。如下图所示:

-	日描策略	历史报表								
ŵ	查看报表	看报表 💼 朝祭祝表								
	报表		IP	数据库名	数据库类型	生成时间				
	Riskscan_20	0150318010049_5191.pdf	192.168.9.3	master	SQLSERVER	2015-03-18 01:00:50				
3	Riskscan_20	0150304215648_6757.pdf	192.168.1.3	master	SQLSERVER	2015-03-04 21:56:49				
3	Riskscan_20	0150304181634_4819.pdf	192.168.1.3	master	SQLSERVER	2015-03-04 18:16:34				

查看报表



选择需要查询的报表,点击"查看报表",将会显示该报表的所有详细信息。如下图所示:

🛅 查看报表 安全评估报告: Riskscan_20150318010049_5191.pdf 评估执行时间: 2015年03月18日 01:00:50 服务器 IP 或 IP 子网: 192.168.9.3 1.0 通过的测试: 83% 溜 0.75 対 出 0.56 者 根据定义的扫描策略执行的测试,所定义数据库环境的数据访问接近 最佳实践。还应考虑将此评估作为审计任务调度,以不断评估这些环 0.2 境和跟踪改进。 1 扫描次数 (单位:次) 一通过率 风险比例图 结果摘要 正在显示4个扫描结果 高 中 低 低风险:50% 高风险:50% 认证 0 0 系统 2 0 授权 0 2 中风险:0% ●高风险:50%●中风险:0%●低风险:50% 🔄 导出报表 🗶 取消

导出报表

点击 "导出报表",可将该报表下载保存起来,以便之后的查看。如下图所示:





删除报表

选择需要删除的报表,点击"删除报表",即可删除该报表。

3.5 数据库状态监控

所属用户: SecAdmin。

数据库状态监控可以看到数据库服务器当前的运行信息,包括服务器的运行时间、内存 及存储的使用情况等。从而及时发现服务器的异常情况,更好的维护数据库服务器。

3.5.1 添加数据库状态监控

进入 "通用配置" > "选择引擎",点击状态监控的 "添加"按钮。如下图所示:



名称	类型	IP	端口	缺省数据库	所属控制器	审计与防火墙	状态监控
192.168.1.45:1521/orcl	ORACLE	192.168.1.45	1521	orcl	localhost	▋ <u>〕详情</u>	+ <u>添加</u>
192.168.1.9:1433/maste	SQLSERVER	192.168.1.9	1433	master	localhost	+ <u>添加</u>	+ <u>添加</u>

点击"添加"按钮后,需输入如下信息:

名称: 该状态监控的名称。

用户名: 该数据库管理员的用户名。

密码: 该数据库管理员的密码。

缺省数据库:系统默认的数据库。

已下信息输入完成后,点击"确定"后,完成数据库状态监控的添加。如下图所示:

添加数据库 监	Ŷ	×
名称	192.168.1.11:1433/master	
用户名		
密码		
缺省数据库	master	
	🖌 🏹	腚

3.5.2 引擎列表

点击选择相应引擎可,对该引擎进行开启、停止和删除操作如下图所示:



状态监控				
引擎列表			C	0
🕨 启动 🔳 停止 💼 删除				
状态 名称	IP	类型		
运行 172.17.200.194:3306/testdb	172, 17, 200, 194	MYSQL		

提示: 引擎只有在停止状态下才能被删除

3.5.3 概况

该页面包括监视器信息、用户权限、用户权限附表、请求数等信息,用户可以快速从该 页面了解到对应数据库的运行概况,如下图所示:

	状态监控																					_	
引擎列表	0	0	引擎名称:	172.17.200.1	194:3306/1	testab 监控 🛛	导出报表																
▶ 启动 ■	 停止 會 888 		観兄	DKE.		5¥	记录																
状态 名称		IP	出来现在																				
运行 172.1	7.200.194:3306/testd	172	Wit o																				
			主机											localhost.1	ocaldonain (1	72.17.200.194:33	06)						
			作總年版本 Source distribution (S.1.71)																				
		- 11	启版时间 2016-05-06 10.54-43																				
			SSL (10世) 115A4120																				
		- 11	SaL模式											STRICT_TRAN	S_TABLES								
			根目录											/usr/									
			用户权限表																				
			HISTRANE	USERMARE	SELECT	INSERT	UPDATE	DELETE	CREATE	DROP	RELOAD	SHUTDOWN	PROCESS	S FILE	GRANT	REFERENCES	INDEX	ALTER	SHD#DB	S1788_	CREATE	ETNPTAI LOCHTABLES	EXECUTE
			х	jack	т	т	Y	τ	T	т	т	τ.	T	т	т	Ŧ	τ	т	т	Y	т	T	т
			х	jhon	т	т	Y	T	т	т	T	r	T	т	х	T	T	т	т	Y	т	T	T
			х	nyada	т	т	Y	τ	т	т	т	r	T	т	т	r	τ	т	т	Y	τ	T	T
			x	root	т	т	Y	τ	т	т	T	r	T	T	т	r	τ	т	т	Y	τ	T	T
			х	ton	T	T	Y	T	T	T	T	r	T	Y	x	Y	T	T	T	Y	T	T	T
		- 18	x	user2	T	¥	R	8	х	я	¥	8	8	н	8	8	8	я	8	8	8	x	8
			用户的网络会																				
			HISTRAME	USEEBA	anz .	REFLICTAVE	REPLOLIENT	CREA	TEVIEY	SHOWVIEN	CHEATEROUTIST	ALTERS	INTINE	CREATEUSER	EVENT	TRIGGER	CI	EATETABLESPA	CE MAIQUESTICHS	MATUFDA	UTE	MAXCOMMECTIONS	MAIUSEBCORNECTION
			x	jeck		Y	т	T		Y	T	T		т	T	Y	8	/A	0	0		0	0
			x	jhan		Y	ч	Y		Y	Y	Y		Y	Ŧ	Y	8	/A	0	0		0	0
		- 1	x	nyada		Y	Y	Y		Y	Y	Y		Y	Y	Y	8,	/A	0	0		0	0
			x	rost		ĭ	Y	T		Y	Y	Y		Y	Y	Ť	8,	/A	0	0		0	0
			x	tos		T	T	T		T	T	T		T	T	T	8,	'A	0	0		0	0
			x	user2		8	8	3		8	x			8	8	8	8	A	0	0		0	0
		- 11	请求赦											连接统计									
		- 11					3	と思い请求	th:			◆ 抽	(字节数					ì	直接统计			-	打开的连接数
		- 11	1,500									 + 请羽 - 小田 		4									
		- 1						0				= 20		,				3				_	
		- 11	1,000											, ,									
		- 11	+											+ 2 -									



3.5.3.1 监视器信息

监视器信模块,主要包含了如下信息,该模块显示的信息以便用户更清晰的了解数据库 的详细信息。

主机: 主机名。 数据库版本: 数据库的版本。 启动时间: 该引擎启用的时间。 SSL (加密): 是否启用了 ssl 加密。 SQL 模式: 数据库所使用的 SQL 模式。 根目录: 数据库的根目录。 如下图所示:

概況	配置	告警	记录		
监视器信息					
属性				值	
主机				localhost.localdomain (172.17.200.194:3306)	
数据库版本				Source distribution (5.1.71)	
启动时间				2016-05-06 10:54:43	
SSL(加密)				DISABLED	
SQL模式				STRICT_TRANS_TABLES	
根月录				/usr/	•

3.5.3.2 用户权限表

用户权限表模块,主要包含数据用户名(USERNAME)以及对应用户可以登录数据库的 主机(HOSTNAME),用户对数据库所具有的权限(select、insert、update……)等信息。 如下图所示:



用户权限表												
HOSTNAME	USERNAME	SELECT	INSERT	UPDATE	DELETE	CREATE	DROP	RELOAD				
%	tom	Y	Y	Y	Y	Y	Y	Y				
%	user2	Y	N	N	N	N	N	N				
%	zim	Y	Y	Y	Y	Y	Y	Y				
127.0.0.1	root	Y	Y	Y	Y	Y	Y	Y				
172, 16, 0, 12	26 lisa	Y	N	N	N	N	N	N				
localhost		N	N	N	N	N	N	N				

3.5.3.3 用户权限附表

用户权限附表模块,主要包含数据用户名(USERNAME)以及对应用户可以登录数据库的主机(HOSTNAME),用户对数据库所具有的权限(replslave、replclient、createview……)等信息。如下图所示:

用户权限附表						
HOSTNAME	USERNAME	REPLSLAVE	REPLCLIENT	CREATEVIEW 📥	SHOWVIEW	CREATEROUTINE
%	tom	Y	Y	Y	Y	Y
%	user2	N	N	N	N	N
%	zim	Y	Y	Y	Y	Y
127.0.0.1	root	Y	Y	Y	Y	Y
172, 16, 0, 126	lisa	N	N	N	N	N
localhost		N	N	N	N	N

3.5.3.4 请求数

请求数模块,主要包含接收字节数、请求数、发送字节数三方面的信息如下图所示:





提示:"请求数"和"发送字节数"默认为灰色未显示折线图状态,用户点选上图中右上 角的相应名称后,相应折线图会加以显示。

3.5.3.5 连接统计

连接统计模块,主要包含打开的连接数、断开的连接数、断开的客户端数三方面的信息, 如下图所示:





提示:"断开的连接数"和"断开的客户端数"默认为灰色未显示折线图状态,用户点选 上图中右上角的相应名称后,相应折线图会加以显示。

3.5.3.6 线程明细

线程明细模块,主要包含缓存中的线程、已用线程两方面的信息,如下图所示:





提示:"已用线程"默认为灰色未显示折线图状态,用户点选上图中右上角的相应名称后, 相应折线图会加以显示。

3.5.3.7 表锁定

表锁定模块,主要包含直接锁定、锁等待两方面的信息,如下图所示:





提示:"锁等待"默认为灰色未显示折线图状态,用户点选上图中右上角的相应名称后, 相应折线图会加以显示。

3.5.3.8 主键击中率

主键击中率模块,主要包含主键击中率、已用主键缓冲区、主键缓冲区大小三方面的信 息,如下图所示:




3.5.3.9 查询缓存击中率

查询缓存击中率模块,主要包含查询缓存击中率、队列缓存大小、队列缓存限制三方面 的信息,如下图所示:





队列缓存大小	ОМВ
队列缓存限制	ОМВ
查询缓存击中率	0%

3.5.3.10 查询统计

查询统计模块,主要包含插入的查询、更新的查询、删除的查询、选择的查询四方面的 信息,如下图所示:





提示:"更新的查询"、"删除的查询"、"选择的查询"默认为灰色未显示折线图状态,用 户点选上图中右上角的相应名称后,相应折线图会加以显示。

3.5.3.11 数据明细

数据模块,主要包含数据库名称、数据库大小、数据目(个)三方面的信息,如下图所示:





3.5.4 配置

从配置页面,用户可以快速的浏览到相应数据库的配置信息如下图所示:



状态监控							
引擎列表 🔘 🔘	引擎名称: 172.17.200.194:3306/testab 监控 🖕 导出报表						
▶ 启动 ■ 停止 音 閉除	教父 四面 由等 记录						
状态 名称 12	N768						
道行 172.17.200.194:3308/testdb 172	Ret	15					
	属性 Land and and And						
	denote at Counts	0 binner					
	and here	vinay					
	angeline alles black size	8107					
	ind for some	0					
	All defining and	902					
	att	6.0 08					
	been seemed	N7					
	ante general de avieter sins	0.000 C					
	have ad	5 MPC (DI VR					
	and a second data	0.					
	an of the second second	0					
	ahir@ab_uas	0 07					
	ang valer lar mara linit	0					
	init conset						
	anat schedul er	177					
	line tone	575 ST					
	0 mere emergian light	20					
	inch furblar at the small	1					
	inch state ashed	and is a mail					
	inin haffer size	121(77)					
	The maxim set mine inform	07					
	and hofee size	131072					
	Advent size	1000					
	landle	loos (Tiblane 31					
	Los more lin	10.00000					
	and detaile the	- Asia lineare					
	al ana alifa arrare	1000					
	ft nin ward len	4					
	nar allowed packet	1048576					

3.5.5告警

在该模块,主要是配置告警的条件,在配置项中,选择相应的配置条件,然后填选阈值, 这里的阈值是一个衡量是否安全的标准,可以设置大于、小于、等于等条件,如果当前值偏 离阈值,可将其报警。如下图所示:





3.5.5.1 配置项

在该模块主要显示了一些告警规则,可根据需要选择配置项,其中主要有几大项分别是: 请求数、连接统计、线程明细、表锁定、主键击中率、查询缓存击中率、查询统计以及数据 明细。如下图所示:







3.5.5.2 编辑告警配置

该模块是针对左侧所选取的具体的配置项,进行阈值编辑的,根据需要设定阈值,点击 保存后即可生效,当偏离阈值时将会告警。如下图所示:



3.5.6 记录

该模块主要是针对告警模块,记录的是告警,在该模块可以查询到告警的表,还可以根据时间来筛选告警,可以进行查询、重置与导出三项操作,导出的格式支出 WORD、EXCELE、PDF。如下图所示:

监控告警讨	监控告答记录								
时间区间	0		到		名称	~	Q、 直询 日: 重置 日: 単置		

同时还会显示该告警记录的时间、名称、原因以及风险等级。



状态监控				
引擎列表 💿 🔘	引擎名称: 172.17.200.194:3306/testab 监控 📮 导出振表			
▶ 启动 🔳 傳止 💼 删除	概況 配置 告警 记录			
状态 名称	监控告警记录			
运行 172.17.200.194:3306/test				
	时间区间	到	名称	✓ Q 查询 D 重量 😡 导出
	时间 名称		原因	风险等级
	1 2016-05-09 17:33:29 请求数		8 > 5	低

3.6 运维审计

所属用户: SecAdmin。

通过运维审计模块可对 FTP 服务器进行审计。

3.6.1 FTP 引擎列表

在 FTP 引擎列表中可以查看到已添加的 FTP 引擎,包括其 IP 地址、端口、网口名、过 滤记录保存天数等信息;通过"添加"、"编辑"等按钮进行相应操作

ETPrait							
FTP引擎列表							
+添加 / 编辑 /							
IP	端口	网口名	过滤记录保存天数	连续登录失败n次后告警	状态	操作	
172 17 200 190	21	eppl	3	3	运行由		

3.6.1.1 添加

点击"添加",弹出新建引擎窗口,输入 IP 端口网口,选择网口名称(审计接口),设置 记录天数、连续失败多少次的风险等级,点击"确定"进行保存。



新建引擎	×
IP	
端口	21
网口名称	~
记录天数	3
连接失败	5 次 无风险 🗸
	✔ 确定

3.6.1.2 编辑

点选已添加的 FTP 引擎,点击"编辑"按钮,弹出编辑引擎窗口,除 IP 地址外其它参数 均可修改。点击"确定"保存修改。

编辑引擎	×
IP	172.17.200.190
端口	21
网口名称	enp1 🗸
记录天数	3
连接失败	3 次 中风险 🗸
	✔ 确定

提示:引擎审计在停止状态下方可编辑。



3.6.1.3 默认设置

通过默认设置可配置记录参数和连续失败多少次的风险等级。点选相应引擎,点击"默 认设置",弹出默认设置窗口,修改相应参数,点击"确定"。

默认设置	×
记录天数	3
连接失败	5 次 无风险 🗸
	✔ 确定

3.6.1.4 启动和停止

点选相应引擎,点击"启动"或"停止",开启或关闭相应引擎的审计功能。

rrr3際列表						
🕇 添加 🥒 编辑 🥒 默认设置	◆添加 / 瞬間 / 野は设置 ▶ 向均 ■ 停止					
IP	端口	网口名	过滤记录保存天数	连续登录失败x次后告警	状态	操作
172 17 200 190	21	anni	3	3	设行由	

3.6.2 规则列表

在规则列表中可以查看到已添加的规则;通过"添加"、"编辑"、"删除"等按钮进行相应操作

示例:添加



点击"添加",添加/编辑规则窗口,输入规则名称;选择风险等级;针对客户端 IP、服务器 IP、文件名、文件类型、敏感词、正则匹配、文件大小等条目进行规则配置,点击"保存"进行保存。

添加/编辑规则					×
规则名称	test 🗸	🗷 设为默认规则	风险等级	中风险 🗸	
客户端IP	172. 16. 0. 126	 ●包含 ● 不包含 	服务器IP	172. 17. 200. 190)包含 〇 不包含
文件名	1. txt	 包含 不包含 	文件类型	txt)包含 ⑧ 不包含
敏感词	1		正则匹配	*)
文件大小	大于等于 🖌 0.00	MB			
					保存

四、 检索和报表

4.1 审计检索(检索)

所属用户: SecAdmin。

审计检索模块中包含了数据库审计检索(检索)和 FTP 检索两个大的模块,通过检索模块,用户能够按条件筛选审计日志。



可以生成检索中不同时间段的报表。

在检索中实时生成不同维度的报表。所谓不同维度就对不同条件的组合查询。

服务器维度: 被监测服务器、受监测数据库、数据库服务器性能。

源分析维度: 源应用程序、数据库用户、源主机、源 IP、登录分析、源就用的性能。 数据的访问模式: 最多查询、查询类型分析、敏感数据查询、查询记录、数据修改分析。 特权操作: 特权查询概述、表删除与截断、存储过程的更改、数据库与 Schemar

的更改、DCL 命令、DDL 命令、本机审计更改、新创建的用户。

其它信息: 失败的登录、SQL 错误、未检测的加密登录。 基于时间的分析:每天、每周、每时。

4.1.1数据库审计检索

4.1.1.1 过滤器

时间

1. 默认选择从下拉菜单选择一天、三天、一周、一个月、三个月。如下图所示:



2. 第二种为自定义时,从某一时间点另一时间点。如下图所示:



二 自定义时间范	1		×
开始时间	12	该输入项为必输项	`
结束时间	17.	整点设置	~ ·
			✔ 确定 🗮 取消

过滤

过滤包括的可选条目有:引擎、策略、数据库类型、数据库 IP、数据库 MAC、数据库实例、数据库用户、操作、操作类型、操作对象、字段、客户端 IP、客户端 MAC、客户端端口、 主机名、操作系统用户、客户端程序、执行时长、动作、风险等级、影响行数、SQL 语句、 SQL 结果、响应状态、SQL 模型。



口过滤设置	ī		X
💊 展开	↑ 选取	引擎	Â
☞ 展开	★ 选取	策略	
🌭 展开	★ 选取	数据库类型	
☞ 展开	★ 选取	数据库IP	
☞ 展开	★ 选取	数据库MAC	
☞ 展开	★ 选取	数据库实例	
🌭 展开	★ 选取	数据库用户	
🌭 展开	♠ 选取	操作	
🌭 展开	★ 选取	操作类型	
🌭 展开	★ 选取	操作对象	
🦕 展开	♠ 选取	字段	
▶ 展开	★ 选取	客户端IP	
🌭 展开	♠ 选取	客户端MAC	
🌭 展开	♠ 选取	客户端端口	
🌭 展开	★ 选取	主机名	
🌭 展开	★ 选取	操作系统用户	
╘ 展开	↑ 选取	客户端程序	
╘ 展开	↑ 选取	执行时长	
💊 展开	↑ 选取	响应状态	-
		🛩 āj	淀

更新

"更新"按钮可以刷新右侧显示,当更改过滤条件时,需用"更新"刷新右侧数据。



检索 FTP检索						
过滤器 《	1	如据列表				
时间 最近三个月 🗸 🥒	:	🗙 列定义 📮 回放				
		引擎	捕获	告警规则	数据库用户	客户端
	1	. 172.17.200.194:3306/t	2016-05-13 18:28:09	默认策略-/默认规则: 无风险	tom	172.1
报告列表	2	2 172.17.200.194:3306/t	2016-05-13 16:28:10	默认策略-/默认规则: 无风险	tom	172. 1
名称	3	3 172.17.200.194:3306/t	2016-05-13 16:27:55	默认策略-/默认规则: 无风险	tom	172.1)
▲ 😋 视图		172.17.200.194:3306/t	2016-05-13 16:27:55	默认策略-/默认规则: 无风险	tom	172. 1
□	ę	5 172.17.200.194:3306/t	2016-05-13 16:27:55	默认策略-/默认规则: 无风险	tom	172. 1
	6	172.17.200.194:3306/t	2016-05-13 16:22:59	默认策略-/默认规则: 无风险	tom	172. 1
▲ 🔄 服务器分析	1	172.17.200.194:3306/t	2016-05-13 16:22:59	默认策略-/默认规则: 无风险	tom	172. 1
	8	3 172.17.200.194:3306/t	2016-05-13 16:22:59	默认策略-/默认规则: 无风险	tom	172. 1
	9	172.17.200.190:60000/	2016-05-13 16:22:44	默认策略-/默认规则: 无风险	db2inst1	172. 1
▲ 😋 来源分析	1	0 192.168.0.98:3306/mys	2016-05-13 16:12:00	默认策略-/默认规则: 无风险	dbm	192. 1
□ · · · · · · · · · · · · · · · · · · ·	1	1 192.168.0.98:3306/mys	2016-05-13 16:12:00	默认策略-/默认规则: 无风险	dbm	192. 1
□ ■ 源应用程序	1	2 192.168.0.98:3306/mys	2016-05-13 16:12:00	默认策略-/默认规则: 无风险	dbm	192. 1
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	1	3 192.168.0.98:3306/mys	2016-05-13 16:12:00	默认策略-/默认规则: 无风险	dbm	192. 1
	1	4 192.168.0.98:3306/mys	2016-05-13 16:12:00	默认策略-/默认规则: 无风险	dbm	192. 1
■ 登录分析	1	5 192.168.0.98:3306/mys	2016-05-13 16:12:00	默认策略-/默认规则: 无风险	dbm	192. 1
■ 源应用程序性能	1	6 192.168.0.98:3306/mys	2016-05-13 16:12:00	默认策略-/默认规则: 无风险	dbm	192. 1)

导出

"导出"按钮可以将筛选的数据以 PDF、WORD、EXCEL 等格式导出,便于用户查看与分析。



检索 FTP检索										
过滤器	«	麲	屠列表							
时间 最近三个月 🗸 🧪		*	列定义	🚍 回放						
			引擎		捕获		告警规则		数据库用户	客户
Q 过滤 📚 更新 🖬 导出 👗 报告		1	172.17.2	200.194:3306/t	2016-05	-13 18:28:09	默认策略/测	认规则:无风险	tom	172.1
报告列表		2	172.17.3	200.194:3306/t	2016-05	-13 16:28:10	默认策略->测	\认规则:无风险	tom	172.1
名称		З	172.17.3	200.194:3306/t	2016-05	-13 16:27:55	默认策略-/测	认规则:无风险	tom	172.1
▲ ← 视图	*	4	172.17.3	200.194:3306/t	2016-05	-13 16:27:55	默认策略-/测	认规则:无风险	tom	172.1
■ ###		5	172.17.3	200.194:3306/t	2016-05	-13 16:27:55	默认策略-/测	认规则: 无风险	tom	172.1
副教掘		6	172.17,2	200 194:3306/+	2016-05	-13 16:22:59	戰法答惑->₹	钻板叫: 无风险	tom	172.1
▲ Ө 服务器分析		7	172.17	🛢 导出选项						172.1
■ 数据库服务器分析		8	172.17	报表格式		PDF格式	~			172.1
■ 数据库服务器性能		9	172.17	行数		PDF格式			nst1	172.1
▲ 즉 来源分析		10	192.16	1900		EXCEL格式				192.1
■ 源教据库用户		11	192.16			nukuhgı, CSV格式		• 确定 🗮 取	肖	192.1
■ 酒应田程序		12	192.168	0.98:3306/mys	2016-05	HTML格式		认规则:无风险	dbm	192.1
■ 源主机		13	192.168	0.98:3306/mys	2016-05	-13 16:12:00	默认策略///////////////////////////////////	认规则:无风险	dbm	192.1
□ 硕工P		14	192.168	0.98:3306/mys	2016-05	-13 16:12:00	默认策略-/测	认规则:无风险	dbm	192.1
		15	192 168	0.98.3306/mm/s	2016-05	-13 16:12:00	興/山谷略->理	いる。	dhm	192 1

报告

点击"报告"按钮,弹出添加报告的窗口,点击"确定"会将报告列表中选中的条目导 入到报表模块中。

数据库与应用安全加固系统						安全管理员:	SecAdmin	🔒 修改密码	占 安全退出	🖵 返回主
检索 FTP检索										
过滤器	《 数据库	名及用户	Р́							
时间 最近三个月 🗸 🖊		数据库名及用户								
Q 过滤 📚 更新 📮 导出 🖬 报告	5									
报告列表	rtrui.									
名称	2 2									
4 😋 视图	≜ ⁴ E									
■ 概要	増け									
動 数据				the log of the set of the set of the						
▲ 🔄 服务器分析			报告名称	数据库服 穷器分析						
勤務库服务器分析	0			分别为数库名称及数据库	用户数柱图	及访 🔺				
劃数据库服务器性能			描述	名称为数据库登录及点击	统计报表分	别电		null		
▲ 🔄 来源分析				到地名、川田口、肥金、	合体到电、					
源数据库用户	来源耶	统计			✔ 确定	🗙 取消				
▶ 源应用程序										
📄 源主机		来源叶统计								
■ 源IP	2									
📄 登录分析										
■ 酒店田程度性能	rtrul									



报告 报告结果				
报告列表				
🕂 添加 💼 删除 📑 时间排序	▋ 分类排序			
名称	类型	修改时间	计划	来源
🛛 😋 检索-来源分析				
🗈 源数据库用户	源数据库用户	2016-05-13 18:52:14		模块导入
⊿ 🔄 检索-视图				
副数据	数据	2016-05-13 18:41:36		模块导入

4.1.1.2 报告列表

报告列表包含视图、服务器分析、来源分析、数据访问模式、特权操作、其他视图、基 于时间的分析,几个大条目。

报告列表	
名称	
▶ 🧰 视图	
▷ 🧰 服务器分析	
▷ 🧰 来源分析	
▷ 🧰 数据访问模式	
▷ 🧰 特权操作	
▷ 🧰 其他视图	
▷ 🗀 基于时间的分析	

视图



▲ → 视图
副 概要
動 数据

视图为检索策略的结果呈现,分为"概要"与"数据"视图。还可以基于"过滤"来查 看所需要的查看内容。

视图的"概要"信息主是通过用户点击情况,按天、周、小时、来进行统计,可以形成 表格及柱状图进行输出。

如下图所示:

流里纲	充计					
流量组	流计概	要				
				流重统计		
事件一	累计		登录─数里	数据库用户名─不重复数里	引擎─不重复数量	操作系统主机名一不重复数里
133532	251		2225542	1	1	1
点击装	物細分	(扱)				
	15M			点击数细分(按天)		
赖單	10M					
林集	5M			13353251		
	ΟM			2016-04-27		



麲	据列表						
*	列定义 🗧 回放						
	引擎	捕获	告警规则	数据库用户	客户端IP	风险等级	操作
1	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192. 168. 0. 168	无风险	DJ 📥
2	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略─>默认规则: 无风险	SYSTEM	192. 168. 0. 168	无风险	SI
3	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略─>默认规则: 无风险	SYSTEM	192. 168. 0. 168	无风险	ហ
4	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略─>默认规则: 无风险	SYSTEM	192. 168. 0. 168	无风险	IJ
5	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192.168.0.168	无风险	ц
6	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192.168.0.168	无风险	ц
7	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192.168.0.168	无风险	DI
8	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192.168.0.168	无风险	SI
9	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192.168.0.168	无风险	ហ
10	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192.168.0.168	无风险	IJ
11	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192.168.0.168	无风险	ц
12	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192. 168. 0. 168	无风险	ц
13	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192. 168. 0. 168	无风险	DJ
14	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192. 168. 0. 168	无风险	SI
15	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192. 168. 0. 168	无风险	ហ
16	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192. 168. 0. 168	无风险	IJ
17	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192. 168. 0. 168	无风险	ц
18	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192. 168. 0. 168	无风险	ц
19	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略─>默认规则: 无风险	SYSTEM	192. 168. 0. 168	无风险	DJ
20	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略─>默认规则: 无风险	SYSTEM	192. 168. 0. 168	无风险	SI
21	192.168.0.97:1521/orc	2016-04-27 15:05:46	默认策略→>默认规则: 无风险	SYSTEM	192.168.0.168	无风险	ហ

服务器分析

数据库服务器分析

被监测数据库由两个柱状图及一个表格够成,分别为数库名称及数据库用户数柱状图及 访问数据库来源 IP 柱状图(同源多 IP),表格名称为数据库登录及点击统计报表分别由数据 名、引擎、登录-数量、事件累计构成。





数据库服务器性能

数据库的性能指标主要是通过对数据库的操作时间为维度来判断数据的性能。通过四个 图与一个表格来体现数据库的性能。分别是请求响应时间(1秒以下、1秒以上10以下、10



秒以上)、SQL 类型时长累计(在一段时间内所有对数据库操作 SQL 用时累计)、服务的繁忙 占比(基于源 IP 的平均响应时间占比)。表操作时长累计(数据库中表的响应时长的累计)。 如下图所示:







来源分析

来源分析是通过源应用程序、数据库用户、源主机、源 IP、登录分析、源应用程序的性能等进行不同角度的分析数据的点击率、登陆及相关统计。



4 😋 来源分析	
🗈 源数据库用户	
📑 源应用程序	
📄 源主机	
📄 源IP	
📄 登录分析	
📄 源应用程序性能	

源数据库用户

源数据库用户分析,通过不同的数据库用户访问不同的数据库进行分析。主要构成为一 个柱状图与表格。柱状图是数据库用户访问不同的库与事件数构成。表格是通过用户、引擎、 数据库名称、登录-数量、事件-累计等项目进行统计的。

如下图所示:

检索 FTP检索							
过滤器 《	数据库审计检索						
时间 最近-天 ✓ ✓ ✓ Q、过速 ② 更新 ⑤ 导出 🛓 报告	15M		数据库审计检索				
报告列表	10M						
24 · · · · · · · · · · · · · · · · · · ·	ени ж ж ж б б б б б б б б б б б б б		Sister				
			orcl				
	数据库审计检索详细						
■ 源主机		數据库审计检索详细					
■ 源IP	数据库用户 名	引擎	救据库名	登录−数里	事件─累计		
■ 登录分析	SYSTEM	192.168.0.97:1521/orcl	orcl	2225542	13353251		
📄 源应用程序性能							
▲ 😋 数据访问模式							
📄 最多查询							
📄 查询类型分析							
📄 敏感度查询							

源应用程序

通过源应用程序的用户、主机、IP、引擎等角度进行统计。通过三个图一个表格方式呈现。表格方式包括源应用程序、引擎、登录-数量。





 □ 須应用程序性能 ▲ 会勤損告访问模式 □ 最多查询 □ 查询类型分析 □ 敏感度查询 □ 管询记录 	db2bp.exe 1 (33%)	db2bp.exe: (33 %)						
📄 数据修改分析	应用程序其干容 录数	应田 耜臣其于 發臺動						
▲ 🔄 特权操作								
📄 特权查询总览		应用程序基于登录数						
📄 表格删除与截断	源应用程序	引擎	登录-数里					
📄 存储过程的更改	null	172.17.200.194:3306/testdb	2					
📄 数据库与Schema的更改	db2bp. exe	172.17.200.190:60000/sample	1					
📄 DCL命令	SQL Developer	172.17.200.193:1521/oracle	1					
📄 DDL命令								
📄 本机审计								
📄 特权创建用户	-							



源主机

统计访问数据的主机相关信息,主要包括数据库客户端在主机上的数量、数据库用户在 主机上的数量、主机上登录不同数据库的数量、主机综合信息等,通过三个柱状图一个图格 来呈现。







源 IP

统计源 IP 中数据库应用程序的数量、数据库用户数量,由两个柱状图和一个表格组成。





登录分析

统计登陆数据库的用户、操作系统主机名、源应用程序、数据库用户、数据库引擎、数据库名、数据库 Schema、数据库 IP、登录-数量。以一个柱状图和一个表格显示。详见下图



检索 FTP检索								
过滤器 《	数据库用户登录	统计						
时间 最近一小时 🗸 🖊				数据库用	户登录统计			
Q 过滤 📚 更新 😱 导出 👗 报告	2							
报告列表	調整							
名称	1 Å 1							
▲ 🔄 视图								
📑 概要	發電							
📄 数据								
4 😋 服务器分析	0	41			0		36	
動調库服务器分析		41.		_	(ES)		oraci	
📄 数据库服务器性能					N/A			
▲ 🔄 来源分析								
📄 源数据库用户	数据库登录信息							
■ 源应用程序				約据6	安容录信自			
源主机	撮作 至结主机 夕	循向田程度	新 据医田 白 2	리敬	+ 立 示 信 心	約据店≤℃₩₩₩₩	* 新堀宏TP	浴录粉田
III 源IP	null	null	ton	172 17 200 194:3	sxaa+-	8x Miltionanit	172 17 200 194	立小 9X主 2
····································	TANG-DATAFORT	dh2hn exe	db2inst1	172 17 200 190 6	TESTI		172 17 200 190	1
	tang-datafort	SQL Developer	SYSTEM	172, 17, 200, 193; 1	oracle		172.17.200.193	1

源应用程序性能

分析源应用程序的性能,用户操作平均时间、过长时间、应用程序的时间占比、平均累 计时间。通过柱状图及表的形式呈现。

	检察	寮 F1	TP检索			
过滤器					«	用户操作数据库省时间累计
时间	最近	ыб—д 🗸 🗸			•	用户操作数据库的时间累计
Q ,过滤	3	更新	😼 导出	┇ 报	÷	
报告列表						
名称						
4 😑 视图						
🖹 観	要					
副数据						
▲ 😑 服务器分析						
黄目	動調					
() 東海	婚库服 \≠⊆	的寄住	86			
- (山木)(A) 日 酒	いい 秋城底	田山				
□	応用程	1979年1月7日				操作大于地的拥户
画源	主机					操作大于1秒的用户
源	IP					
111 111 1111 11111 1111111111111111111	录分析	f				
■ 源	应用程	昆序性能				
⊿ 😑 数据i	方问模:	±.				
🗎 最	多查询	1				
🗎 査	间类型	劉分析				
(御) 🗐	感度查	间				
🖹 🖆	海记录					



数据访问模式

根据数据的查询类型、数量、及数据的修改来进行分析。包括最多查询、查询类型分析、 敏感度查询、查询记录、数据修改分析。

🔺 🕞 数据访问模式	
📑 最多查询	
📄 查询类型分析	
📄 敏感度查询	
📓 查询记录	
📄 数据修改分析	

最多查询

统计数据库的时间数量、客户达端对应 IP 的请求数量,通过柱状图形式呈现。





查询类型分析

统计分析数据中的特权操作、无特权操作、敏感数据、不敏感数据。通过饼状图及表格 形式呈现。如下图所示:



敏感度查询

在数据库及表组中统计敏感信息。通过柱状图及综合表格来呈现。



检索 FTP检索					
过滤器	«	救据库表组 敏感度统计			
时间 最近一天 🗸 🗸			数据库表组敏感度统计		
Q 过滤 📚 更新 😡 导出 👗 报告					
报告列表					
名称					
▲ → 数据访问模式	*				
📄 最多查询					
📄 查询类型分析					
動感度查询					
查询记录					
🖹 数据修改分析					
▲ 🔄 特权操作					
特权查询总览		敏感信息统计表			
🖹 表格删除与截断			物成件自然让中		
📄 存储过程的更改		Webmatter Hilbert F	電燈信息或可表	18 0 - 10	100 AL 100 M 1
📄 数据库与Schema的更改		源应用程序 数据库名	数据库SCHEMA	操作对象	●仟-茶廿
■ DCL命令					
■ DDL命令					
🖹 本机审计					
📄 特权创建用户					
▲ 😋 其他視图					
► + Bééb巡寻					

查询记录

统计请求响应大小数量、应用程序请求占比、用户请求占比、响应大小累计。通过饼状 图、柱状图以及表格形式呈现。如下图所示:







数据修改分析

统计数据访问中的 insert、updata、delete 等对数据库表修改的操作。通过柱状图与 表格形式展现。如下图所示:

检索 FTP检索									
过滤器	《 数据库用户对表的	的修改							
时间 最近一天 🗸 🗸		数据库用户对表的修改							
Q、过滤 📚 更新 😡 导出 👗 报告	7.5M								
报告列表	5M								
名称	發展								
🔺 🗁 数据访问模式	* # 2.5M			_					
📄 最多查询									
📄 查询类型分析	ом								
📄 敏感度查询					1 EN				
🖹 查询记录					Star.				
🖹 数据修改分析				UPDAT	te 🔳 delete 📒 insi	ERT			
a 🔄 特权操作									
📄 特权查询总览	数据库表修改记录	R							
📄 表格删除与截断					新編座素修改记录				
存储过程的更改		救援安久	物据研SCHEWA	操作	場作未到	据-froit第	501 导觉信白	容易须急行物要hn	
📄 数据库与Schena的更改	SUBAPIT	stan+ta	syngatorinak	THEFT	TRIPPEZ	DRIF-X334	345开布目动	2004401982 96/04	
■ DCL命令	SVSTER	oral	oral SVSTRM	IPDATE	Table	test		0	
📄 DDL命令	SISTER	orei] SISTER	DELETE	Table	test		0	
🖹 本机审计	SISTER	01.01	or or. STSTEM	DELEIE	Tante	Lesc		v	
特权创建用户									
▲ 🔄 其他视图									
■ 失败的發录									



特权操作

统计特权操作相关信息包括特权查询总览、表删除与截断、存储过程的更改、数据库与 Schema 的更改、DCL 命令、DDL、本机审计、特权创建用户。通过柱状图饼状图及表格式 形展现。

特权查询总览

统计特权操作相关信息,包括特权操作类型、特权操作对象信息、基于源与操作的特权操作请求。分别通过柱状图、饼状图、表格的形式展现。如下图所示:



表格删除与截断



统计不同用户对表的删除与截断(drop、truncate)通过柱状图及表格的形式展现。如下图所示:



存储过程的更改

统计用户对表的操作,表的类型属于 Procedure、Function 并且操作属于特权操作。通过柱状图与表格方式展现。



	检索	FTF	检索												
过滤器						«	1	基于用户的特权操作							
时间	最近一	天		~							基	于用户的特权操作			
Q ,过渡	2 更	新	导出	ï	报告		L								
报告列表															
名称							1								
⊿ 😋 数据	访问模式					•									
🖹 🖥	多查询						Ŀ								
🗎 🖆	间类型分	析					Ŀ								
a	感度查询						Ŀ								
111 111 1111 1111 11111 11111111111111	间记录						Ŀ								
■ 数	相修改分	析					Ŀ								
▲ 🔄 特权	操作						Ŀ								
🖹 Ħ	財查询总	览					1	基于目标表的特权操作							
≣ ₹	格删除与	截断									基	于目标表的特权操作			
自有	储过程的	更改					a	리鐅	参据库用户名	操作系统主机名	操作		操作类型	操作对象	SOL语句-不重复教理
L	U据库与So	hen alf]	更改				Ľ	51-9-	2010-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0	AND ADDREED BY	20011		and a case	2000170220	1.1.1.2.1.1.2.1.1.2.1.1.2.1.2.1.2.1.2.1
📄 Di	1.給令														
بر 🗐	Lary.														
<u>∎</u> 4	机电计	<u> </u>													
1	HX回り運用 holl回	н													
▲ 🔄 具10	1次(23)														

数据库与 Schema 的更改

分析用户对数据库及 Schema 的特权操作,通过柱状图及表格的形式展现。

检索 FTP检索	
过滤器 《	用户对数据库与Schena的特权操作
时间 最近一天 🗸 🗸	用户对数据库与Schema的转积操作
Q、过滤 🕲 更新 😨 导出 🖬 报告	
报告列表	
名称	
 → 数据访问模式 	
📄 最多查询	
📑 查询类型分析	
📄 敏感度查询	
📄 查询记录	
📄 数据修改分析	
a 🗁 特权操作	
持权查询总览	数据库与Schena特权操作的统计
📄 表格删除与截断	
存储过程的更改	數据库与Schema持权操作自该会计
■ 数据库与Sohem 的更改	
📄 DCL命令	
DDL命令	
本机审计	
持权创建用户	
4 😋 其他视图	
■ 生胎的警费	

DCL 命令

通过 DCL 命令分析用户与特权操作,通过饼状图与表格展现。


检索 FTP检索										
过滤器	«	操作类型占比								
时间 最近一天 🗸 🗸						操作类型占	Ł			
Q、过滤 🕲 更新 🔂 导出 谋 报告										
报告列表										
名称										
▲ 😋 数据访问模式	*									
📄 最多查询										
📄 查询类型分析										
📄 敏感度查询										
📄 查询记录										
📄 数据修改分析										
4 😑 特权操作										
📄 特权查调总览		DCL命令操作详细								
📄 表格删除与截断						n m A A 48 0	er 146./00			
📄 存储过程的更改						DCL带安强1	F 1 = 300	1		
📄 数据库与Schema的更改		引擎	操作	操作类型	操作对象	数据库用户名	操作对象	数据库IP	SQL语句不重复数 事件-累计	
📄 DCL命令										
📄 DDL命令										
📄 本机审计										
🖹 特权创建用户										
🔺 😋 其他视图										

DDL 命令

通过 DDL 命令分析用户与特权操作,通过饼状图、柱状图与表格展现。

检索 FTP检索	
过滤器 《	擬作类型占比
时间 最近一天 🗸 🖍	操作类型占比
Q 过滤 C 更新 🔄 导出 👔 报告	
报告列表	
名称	
▲ 😋 数据访问模式 🔷	
📄 最多查询	
📄 查询类型分析	
■ 敏感度查询	
■ 査询记录	
数据修改分析 ① ① ① ①	
	操作类型数里
高校対理的画み	操作类型频量
■ 数据库与Schene的更改	
 ■ DCL命令	
■ IDL命令	
🖹 本机审计	
📄 特权创建用户	
4 😋 其他视图	
📄 失败的登录	

本机审计

分析操作类型为 Audit Operation、Audit 特权操作,通过饼状图与表格形式展现。



检索 FTP检索	
过滤器 《	
时间 最近天 🗸 🗸	
Q 过滤 😋 更新 🔄 导出 👗 报告	
报告列表	操作类型数量
名称	
▲ 🔄 数据访问模式 🔷	
📄 最多查询	
📄 查询类型分析	
📄 敏感度查询	
📄 查询记录	
📄 数据修改分析	
▲ 🔄 特权操作	- 37
持权查询总览	
📄 表格删除与截断	
存储过程的更改	
📄 数据库与Schema的更改	
BCL命令	操作类型详细
■ DDL命令	操作参用详细
🗈 本机审计	に「アニューマー4 フ数 秋坂年田白夕 堤北を分かれり 堤化口色 oni道つにて毎日秋田
持权创建用户	うチ 家族時代の一台 球目の形式主い人台 球目的家 344時代で生態数里
▲ 🔄 其他视图	
📄 失败的登录	

特权创建用户

统计创建用户的方法的占比,包括 INSERT USER 表的方法、CREATE USER 的方法、GRANT 的方法。通过饼状图的形式展现。



统计创建用户的相关的CREATE USER方法和GRANT的方法。

创建用户方法

新用户分布

•

新用户分布

创建用户详细			
	创建	用户详细	
引擎	数据库用户名	操作系统主机名	操作对象

其它视图

统计分析其它类别的视图包括失败的登录、SQL错误、未监测的(加密的)登录、非特权创建用户,通过饼状图、柱状图等进行分析。

失败的登录

统计登录数据库失败的次数与数据库的类型。通过柱状图和表格的方式展示。详见下图。





SQL 错误

统计每个引擎或服务器发生的 SQL 异常请求的数量,通柱状图与表格的方式展现。SQL 异常通常是请求的语句异常。例如: select I love you select*.8 phoneNum show tables use mysql show databases print "serverName…………" + sysuser exp select * from select*.*from select* select*from all tables 等。详见下图。





查间服务器的SQL错误

		查询服务器的SQL错误		
引擎	客户端IP	操作	SQL语句	事件-累计
172.17.200.194:3306/testdb	172. 16. 0. 126	SELECT	select name, host from USER	1
172.17.200.194:3306/testdb	172. 16. 0. 125	LOGIN	login	1
172.17.200.194:3306/testdb	172. 16. 0. 125	SELECT	select name, host from user	1

未监测的(加密的)登录

统计无法解析的用户名,在识别到验证流量已加密但却无法解密时,不论是出于何种原 因无法解密,通过饼状图与柱状图及表格方式展现。如下图所示:





无法解析用户详细					
		无法解析用户词	纤细		
引擎	数据库IP	客户端IP	操作系统主机名	登录−数里	
172.17.200.194:3306/testdb	172. 17. 200. 194	172. 16. 0. 126	null	1	
172.17.200.194:3306/testdb	172. 17. 200. 194	172. 16. 0. 125	null	2	

基于时间的分析

根据时间的维度来分析 SQL 请求数量,包括每天、每周中的某一天、每天的某一时刻。 通过柱状图与表格来展现。

基于天

统计每天的点击数量通过柱状图与表格的方式展现。



	检索	FTP检索									
过滤器			«	点击数细分	(接天)						
时间	最近一	ξ 🗸 🗸						点击	数细分 (按天)		
Q ,过渡	2 更	新 🔄 导出 🚺 报告		15M						_	
报告列表				10M							
名称				田 田 一 田							
1 D T	感度查询		•	新							
≝ ■ #	(明记求 +B48354)	łf		5M							
▲ 🛁 特权:	瞬作	91									
目特	权查询总	览		OM					1		
憲 患	格删除与	截断							~0 ⁴⁻² '		
🗎 存	储过程的	更改							2010		
🗎 🆄	据库与So	hens的更改		占主新加公	(12年) 洋畑						
📄 DC	L命令			MC4903473	10007 ####						
🗎 DI	L命令							点击爹	领细分(按天)详细		
🗎 本	机审计			日期		事件-累计	登录一	数量	数据库用户名─不重复数量	引擎─不重复数量	操作系统主机名-不重复数量
🗎 特	权创建用	户		2016-04-27		13353251	22255	42	1	1	1
⊿ 😋 其他	视图										
🗎 失	败的登录										
📄 SG	口错误										
■ 未	监测的(加密的) 登录									
	特权创建	用户									

基于周

统计每周中的每天点击数量,通过柱状图与表格形式展现。如下图所示:



基于小时

统计每天中的每小时点击数量,通过柱状图与表格形式展现。如下图所示:



时间 最近一天 🗸 🗸			đ	(击数细分(按小时)		
Q. 过滤 😋 更新 📮 导出 👔 报告	15	M				
报告列表						
名称	· 塑	2M				
 ■ 宣明に求 ■ 数据修改分析 ▲ → 特权操作 	51	м				
 詩权查询总览 表格刪除与截断 	0	м				
📄 存储过程的更改				15:00		
■ 数据库与Scheme的更改 ■ DCL命令	点击数细	盼 (按小时) 详细				
📄 DDL命令			点;	击数细分(按小时)详细		
🖹 本机审计	整点	事件-累计	登录一数量	数据库用户名─不重复数量	引擎─不重复数量	操作系统主机名-不重复数量
📄 特权创建用户	15:00	13353251	2225542	1	1	1
🔺 🚖 其他视图						
📑 失败的登录						
🖹 SQL错误						
📄 未监测的(加密的)登录						
📄 非特权创建用户						
▲						

4.1.1.3 点击数按天细分(小时)

统计一天中小时的点击数通过柱状图展现,同时在表格中展现点击详细信息包括小时(24 小时)、点击、登录、用户、引擎、主机。

4.1.2 FTP 检索

4.1.2.1 FTP 数据检索

查询结果

通过 FTP 数据检索页面可检索查看 FTP 客户端从服务器下载或上传文件的操作。可以时间、服务器 IP、客户端 IP、用户名、文件名、关键字为条件进行筛选查询。通过"重置"按钮,清除所设置的条件,点选相应文件,点击"批量下载"按钮可将文件下载到本地。通过 "导出"按钮可将条目以文件的形式导出到本地。"生成报表"按钮,可生成 FTP 审计报表, 并以文件形式导出下载到本地。



查询结界	ę.										
时间 区间		12-	到			12-	服 务 器 IP			客 户 端 IP	
用户 名			文件 名				关键字			 Q. 查询 ↓ 批量下载 ▲ 生成报表 	重置 ▲ 导出
	操作时间	服务器IP	客户端II	P	用户名	文件名		文件大小	上传 / 下载	链接地址	
	2016-05-23 16:27	: 172, 17, 200, 190	172, 16, 0	0. 125	ftpuser	1. txt		2.17K	下载	/1. txt	

概要

在概要中能够查看到相应文件的文件名和存放路径等信息。

概要
文件名: 1. txt
ftp路径: /1. txt
<u>查看更多内容</u>

4.1.2.2 FTP 指令检索

通过 FTP 指令检索页面可检索查看 FTP 客户端所执行的 FTP 指令。可以时间、服务器 IP、客户端 IP、指令、用户名为条件进行筛选查询。



NTRIA 0-042 Birgan Birgan Birgan Diamond Control Contrecontrol Control Control Contrecontrol Control Contre	PTrűg Ódág By-Báty D
操作詞 服券器12 用户站 指令 1 2016-05-21 53 72.2 172.17 200.190 172.16.0.125 4 053.6 f guaser 2 2016-05-23 15.37.2 172.17 200.190 172.16.0.125 4 017 3 2016-05-23 15.37.2 172.17 200.190 172.16.0.125 4 017 4 2016-05-23 15.36.4 172.17 200.190 172.16.0.125 4 0153.4 5 2016-05-23 15.36.4 172.17 200.190 172.16.0.125 f guaser 017 6 2016-05-23 15.36.4 172.17 200.190 172.16.0.125 f guaser 017 7 2016-05-23 15.36.4 172.17 200.190 172.16.0.125 f guaser 017 7 2016-05-23 15.36.1 172.17 200.190 172.16.0.125 f guaser 017 7 2016-05-23 15.36.1 172.17 200.190 172.16.0.125 f guaser 017 7 2016-05-23 15.36.5 172.17 200.190 172.16.0.125 f guaser 017 8 2016-05-23 15.36.5 172.17 200.190 172.16.0.125 <th>操作封肩 服务器IP 第/編IP 用户名 描令 1 2016-05-23 15:37.22 172:17.200.190 172:16.0.125 ftyuser 1028.ftyuser 2 2016-05-23 15:37.22 172:17.200.190 172:16.0.125 4 QUIT 3 2016-05-23 15:35.52 172:17.200.190 172:16.0.125 4 USER 4 4 2016-05-23 15:36.47 172:17.200.190 172:16.0.125 ftyuser QUIT 5 2016-05-23 15:36.52 172:17.200.190 172:16.0.125 ftyuser QUIT</th>	操作封肩 服务器IP 第/編IP 用户名 描令 1 2016-05-23 15:37.22 172:17.200.190 172:16.0.125 ftyuser 1028.ftyuser 2 2016-05-23 15:37.22 172:17.200.190 172:16.0.125 4 QUIT 3 2016-05-23 15:35.52 172:17.200.190 172:16.0.125 4 USER 4 4 2016-05-23 15:36.47 172:17.200.190 172:16.0.125 ftyuser QUIT 5 2016-05-23 15:36.52 172:17.200.190 172:16.0.125 ftyuser QUIT
1 2016-05-21 i5 37.22 172.17 200.190 172.16.0.125 fyuser UER fyuser 2 2016-05-23 i5 37.11 172.17 200.190 172.16.0.125 4 0UT 3 2016-05-23 i5 35.02 172.17 200.190 172.16.0.125 4 0ER 4 4 2016-05-23 i5 36.07 172.17 200.190 172.16.0.125 4 0UT 5 2016-05-23 i5 36.07 172.17 200.190 172.16.0.125 fyuser 0UT 5 2016-05-23 i5 36.07 172.17 200.190 172.16.0.125 fyuser 0UT 6 2016-05-23 i5 36.07 172.17 200.190 172.16.0.125 fyuser 0UT 7 2016-05-23 i5 36.01 172.17 200.190 172.16.0.125 fyuser 0UT 7 2016-05-23 i5 36.01 172.17 200.190 172.16.0.125 fyuser 0UT 8 2016-05-23 i5 36.01 172.17 200.190 172.16.0.125 fyuser 0UT 9 2016-05-23 i5 36.01 172.17 200.190 172.16.0125 fyuser 0UT	1 2016-05-23 15 37.22 172 17 200.190 172 16 0.125 fyuser UER fyuser 2 2016-05-23 15 37.11 172 17 200.190 172 16 0.125 4 UTT 3 2016-05-23 15 36.52 172 17 200.190 172 16 0.125 4 UER 4 4 2016-05-23 15 36.54 172 17 200.190 172 16 0.125 fyuser UTT 5 2016-05-23 15 36.57 172 17 200.190 172 16 0.125 fyuser UTT
2 2016-05-23 35.37.11 172.17.200.190 172.16.0.125 4 QIT 3 2016-05-23 15.35.82 172.17.200.190 172.16.0.125 4 1528.4 4 2016-05-23 15.36.84 172.17.200.190 172.16.0.125 4 1528.4 5 2016-05-23 15.36.84 172.17.200.190 172.16.0.125 4pase QIT 6 2016-05-23 15.36.04 172.17.200.190 172.16.0.125 4pase 1528.4 typese 7 2016-05-23 15.36.00 172.17.200.190 172.16.0.125 4pase QIT 7 2016-05-23 15.36.00 172.17.200.190 172.16.0.125 4pase QIT 8 2016-05-23 15.36.00 172.17.200.190 172.16.0.125 fpaser QIT 9 2016-05-23 15.36.00 172.17.200.190 172.16.0.125 fpaser QIT	2 2016-05-23 15:37:11 172: 17:200.190 172: 16.0.125 4 QIIT 3 2016-05-23 15:36:35 172: 17:200.190 172: 16.0.125 4 ISER 4 4 2016-05-23 15:36:47 172: 17:200.190 172: 16.0.125 Fyster QIIT 5 2016-05-23 15:36:47 172: 17:200.190 172: 16.0.125 Fyster QIIT
3 2016-56-23 153.65 172.17.200.190 172.16.0.125 4 UER 4 4 2016-56-23 153.64 172.17.200.190 172.16.0.125 fpuser 0TT 5 2016-56-23 153.63.07 172.17.200.190 172.16.0.125 fpuser 0TT 6 2016-56-23 153.60.07 172.17.200.190 172.16.0.125 fpuser 0TT 7 2016-56-23 153.60.00 172.17.200.190 172.16.0.125 fpuser 0TT 8 2016-56-23 153.60.00 172.17.200.190 172.16.0.125 fpuser 0TT 7 2016-56-23 153.60.00 172.17.200.190 172.16.0.125 fpuser 0TT 8 2016-56-23 153.60.00 172.17.200.190 172.16.0.125 fpuser 0TT	3 2016-05-23 153.98 172.17.200.190 172.18.0.125 4 VER8 4 4 2016-05-23 153.96.47 172.17.200.190 172.16.0.125 fpuser 9UT 5 2016-05-23 153.96.47 172.17.200.190 172.16.0.125 fpuser 9UT
4 2016-055-23 15 38.47 172.17.200.190 172.16.0.125 fuguer QIIT 5 2016-055-23 15 38.625 172.17.200.190 172.16.0.125 fuguer VESB fuguer 6 2016-055-23 15 38.053 172.17.200.190 172.16.0.125 fuguer VESB fuguer 7 2016-055-23 15 38.053 172.17.200.190 172.16.0.125 fuguer VESB fuguer 8 2016-055-23 15 38.053 172.17.200.190 172.16.0.125 fuguer VESB fuguer 9 2016-055-23 15 38.555 172.17.200.190 172.16.0.125 fuguer VESB fuguer	4 2016-05-23 15':36:47 172:17.200.190 172:16.0.125 ftyuser QUIT 5 2016-05-23 15':36:25 172:17.200.190 172:16.0.125 ftyuser MUT
5 2016-05-23 15:30.25 172.17.200.190 172.18.0.125 Fugure VEXE Fugure VEXE Fugure 6 2016-05-23 15:30.00 172.17.200.190 172.16.0.125 Fugure VIII VIII VIIII VIIII VIIIII VIIIIII VIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	5 2016-05-23 15:36:25 172.17.200.190 172.16.0.125 ftpuser VSER ftpuser
6 2016-05-23 15:36:19 172: 17:200.190 172: 16.0.125 Fysser QIIT 7 2016-05-23 15:36:00 172: 17:200.190 172: 16.0.125 Fysser USER fysser 8 2016-05-23 15:35:55 172: 17:200.190 172: 16.0.125 Fysser QIIT	
7 2016-05-23 15:36:00 172 172 103 102 16:0.125 Figure USER Figure 8 2016-05-23 15:35:55 172 172 10:0.125 Figure QUIT	6 2016-06-23 15:38:19 172.17.200.190 172.16.0.125 ftpuser QUIT
8 2016-05-23 15:35:55 172.17.200.190 172.16.0.125 fryuser QUIT	7 2016-05-23 15:38:00 172.17.200.190 172.16.0.125 ftpuser USER ftpuser
	8 2016-05-23 15:35:55 172.17.200.190 172.16.0.125 ftpuser QUIT
9 2016-05-23 15:35:21 172.17.200.190 172.16.0.125 ftpuser USER ftpuser	9 2016-05-23 15:35:21 172.17.200.190 172.15.0.125 ftpuser USER ftpuser

4.2 报表

所属用户: SecAdmin。

报表模块内置了报表模版,这些报告可以通过预定义模板来使用。也可以修改报告中预 定义的参数,来满足不同需求。

4.2.1 报告

通过报告模块,用户可以进行添加配置报告模版,设置修改模版参数,导出报告等操作。



报告列表					Wif	数据范围	计划	结果集					B 保存	10 立即注
+添加 會開除 副时间	序 副分类排序				名称	SOX	教掘库请求异常	分析						
名称	类型	修改时间	计划 升	未原		2450	(保护的)教媒座)	行的起出资源	春印范围的。					
🔺 😋 默认报告-S0X					描述									
■ 50x数据库请求异常分析	常异末高调肤线202	\$ } {2016-05-16 18:55:19	3	手动添加										
🖌 🛁 检索-视图					文件类型	PDF	楊式	~						
截要	観察	2016-05-16 18:55:09	3	手动添加										
	獻網	2016-05-13 18:41:36	1	植块导入										
▲ 😑 其他-其他														
自定义	自定义	2016-05-16 17:17:01	4	手续添加										
▲ 😑 检索-未源分析														
	源赴据库用户	2016-05-13 18:52:14	8	A 10 A 10										
				展 大守人										
				御 大守人										
				操 状等人										
				探 状羽人										
				探 状羽人										

4.2.1.1 报告列表

在报告列表中,用户可进行模版添加、删除、排序。





报告列表				
🕂 添加 💼 删除 🚦 时间排序	▋ 分类排序			
名称	类型	修改时间	计划	来源
┛ 😋 默认报告-SOX				
📄 SOX数据库请求异常分析	SOX数据库请求异常分析	2016-05-16 18:55:19		手动添加
⊿ 😋 检索−视图				
🗎 概要	概要	2016-05-16 18:55:09		手动添加
📔 数据	数据	2016-05-13 18:41:36		模块导入
⊿ 😋 其他−其他				
📄 自定义	自定义	2016-05-16 17:17:01		手动添加
⊿ 😋 检索-来源分析				
📄 源数据库用户	源数据库用户	2016-05-13 18:52:14		模块导入

添加

点击"添加"按钮,弹出添加窗口。报告类型有"检索"、"默认报告"、"其他"三项可供选择;每项可供选择的详细条目在"类型"列表中显示,点击即可选中。通过"确定"按钮,保存选择和配置。



■ 増加报告			E		
报告类型	检索	~			
类型		描述			
4 😑 视图					
📄 概要		通过用户点击情况,按天、周、小时、来进行统计。			
📄 数据		可查询显示不同过滤器的结果集合明细。			
🔺 🔂 服务器分析					
📄 数据库服务器	分析	分别为数库名称及数据库用户数柱图及访问数据库来源IP柱图(
📄 数据库服务器	性能	通过对数据库的操作时间为维度来判断数据的性能。			
🔺 😋 来源分析					
📄 源数据库用户	l	通过不同的数据库用户访问不同的数据库进行分析。			
📑 源应用程序		通过源应用程序的用户、主机、IP、加固点、服务 等角度进行线			
🗎 源主机		统计访问数据的主机相关信息。			
📄 源IP		统计源IP中SQL Client、数据库用户数量。			
📑 登录分析		统计登陆数据库的用户、操作系统主机名、源应用程序、用户、			
📑 源应用程序性	彪	分析源应用程序的性能,对于操作时长超过1秒的操作,进行统计	A.		
🔺 🔂 数据访问模式					
📄 最多查询		统计请求SQL最多的源IP地址、服务类型,并同时统计数据是否之	,		
📄 查询类型分析		统计分析数据中的特权操作、无特权操作、敏感数据、不敏感数	[
📄 敏感度查询		在数据库及表组中统计敏感信息。			
📄 查询记录		统计请求大小(尺寸)、不同用户请求数里及占比、应用程序请			
🖹 粉帽修动分析	:	给讲新课话问由的 (meant youdate, dalate 笙动物氓房主修改	•		



报告类型	默认报告	~
类型		描述
4 😑 DPA		
📄 DPA数据库管理	理活动	对DPA保护的数据库进行的DDL和DCL访问。
📄 DPA数据库请:	求异常分析	对DPA保护的数据库进行的超出策略语句。
4 😋 SOX		
📄 SOX数据库管理	理活动	对SOX保护的数据库进行的DDL和DCL访问。
📔 SOX数据库请:	求异常分析	对SOX保护的数据库进行的超出策略语句范围的。
📔 SOX活动用户		对SOX保护的数据库进行的活动状态的用户的访问情况统计。
📄 SOX活动用户	(表格)	对SOX保护的数据库进行的活动状态的用户的访问情况统计(表标
🖌 🔄 等级保护		
📄 等保数据库管	理活动	对等级保护的数据库进行的DDL和DCL访问。
📄 等保数据库诸	家异常分析	对等级保护的数据库进行的超出策略语句范围的。
📄 等保活动用户	3	对等级保护的数据库进行的活动状态的用户的访问情况统计。
📄 等保活动用户	コ(表格)	对等级保护的数据库进行的活动状态的用户的访问情况统计(表
4 😋 医疗防统方		
📑 HIS数据库管理	理活动	对HIS保护的数据库进行的DDL和DCL访问。
📄 HIS数据库请:	求异常分析	对HIS保护的数据库进行的超出策略语句范围的。
🗎 HIS活动用户		对HIS保护的数据库进行的活动状态的用户的访问情况统计。
📄 HIS活动用户	(表格)	对HIS保护的数据库进行的活动状态的用户的访问情况统计(表标

✔ 确定

🗎 増加报告		
报告类型	其他	~
类型		描述
⊿ 😋 其他		
🗎 自定义		可自定义需要检索的数据,及所有的可显示样式。



删除

点选已添加的模版,点击"删除"按钮,弹出确认窗口,点击"确定",即可成功删除。

报告列表								
➡ 添加 💼 删除 🚦 时间排序 🚦 分类排序								
名称	类型	修改时间	计划	来源				
⊿ 🔂 其他−其他								
🗈 自定义	自定义	2016-05-16 17:17:01		手动添加				
▲ 🔄 检索-来源分析								
■ 源数据库用户				模块导入				
▲ 🔄 检索-视图	?) 确定要删除吗?							
🖹 数据	Vr .			模块导入				
	✔ 确定	🗙 取消						

时间排序

点击"时间排序",系统将会把已添加的模版按照添加时间的倒序进行排序。



报告 报告结果								
报告列表								
🛨 添加 💼 删除 📑 时间排序	➡ 添加 童 删除 ■ 时间排序 ■ 分类排序							
名称	类型	修改时间	计划	来源				
⊿ 😋 其他−其他								
🗈 自定义	自定义	2016-05-16 17:17:01		手动添加				
◢ 🔄 检索-来源分析								
📄 源数据库用户	源数据库用户	2016-05-13 18:52:14		模块导入				
⊿ 🔄 检索-视图								
📓 数据	数据	2016-05-13 18:41:36		模块导入				

分类排序

点击"分类排序",系统将会把已添加的模版按类别进行排序。



🕇 添加 💼 删除 📑 时间排序	■ 分类排序			
呂称	类型	修改时间	计划	来源
⊿ 😑 检索-视图				
🗈 概要	概要	2016-05-16 18:55:09		手动添加
🖹 数据	数据	2016-05-13 18:41:36		模块导)
◢ 😋 检索-来源分析				
📄 源数据库用户	源数据库用户	2016-05-13 18:52:14		模块导)
⊿ 😋 默认报告-SOX				
📄 SOX数据库请求异常分析	SOX数据库请求异常分析	2016-05-16 18:55:19		手动添加
⊿ 😋 其他其他				
🗎 自定义	自定义	2016-05-16 17:17:01		手动添加

4.2.1.2 概述

概述包括名称、描述、和文件类型。名称指所生成报告的标题名称和文件命名,用户可进行手动修改配置。描述指生成文档中对内容的描述简介,用户同样可进行修改编辑。文件类型包括 PDF、EXCEL、WORD 等格式可供选择。



概述	数据范	胡 计划 结果集	🗎 保存	1 立即生成
名称		SOX数据库请求异常分析123		
描述		对SOX保护的数据库进行的超出策略语句近面的。		
文件类型		PDF格式 V		
		Perfect EXCEL/启式 VORME式 CSV格式 XTML指式		

提示:修改配置后,需点"保存"按钮进行保存,否则不生效。

4.2.1.3 数据范围

"数据范围" 允许您将报告中包含的数据限制为选定"数据范围" 字段中的数据。配置数据范围不是必需的,但配置数据范围有助于集中关注数据的特定子集。



ł	既述 數	相范围	计划	结果集			🗎 保存	🧰 立即生成
时间范围	۲	从: 到: 最后的:	最近一小时		~	时		ĺ
	◆ 折叠 CLOSE COMM CHEC DBCC DEALL DECL/ DELET DENY DISAB	◆取消 E IENT KPOINT LOCATE ARE IE LE	操作		ALERT CALL COMMI CREAT DROP EXECU GRANT OTHER ROLLB RPC	T E ITE S ACK	•	●包括◎不包括
:+	 展开 展开 展开 展开 展开 展开 展开 展开 展开 、展开 	 * 选取 	数据库用户 操作对象 客户端IP 主机名 操作系统用户 客户端程序 SQL语句 SQL结果	1				
減器	 ▶ 展开 ▶ 展开 ▶ 展开 ▶ 展开 ▶ 展开 	 ↑ 选取 ↑ 选取 ↑ 选取 ↑ 选取 ↑ 选取 	SQL模型 引擎 策略 数据库IP					
	 ◆ 展开 ◆ 展开 ◆ 展开 ◆ 展开 	 ↑ 选取 ↑ 选取 ↑ 选取 ↑ 选取 ↑ 选取 	数据库MAC 客户端MAC 响应状态 字段					
	▶ 展开▶ 展开	 ↑ 洗取 ↑ 洗取 	数据库类型 数据库实例					



条件名称	操 作	可选元素	自定义	备注
时间范围	点选、自定义	最近一小时、最近一天、最近 三天、最近一周、最近一个日	是	
 客户端 IP	点选、自定义	学习+IP 集	是	
客户端 MAC	点选、自定义	自定义	是	
数据库 IP	点选、自定义	通用配置中配置的引擎的 IP	是	
数据库 MAC	点选、自定义	自定义	是	
客户端程序	点选、自定义	学习+源应用程序集	是	
操作类型	点选	None 、 Aggregate 、 BrokerPriority 等	否	
操作对象	点选、自定义	学习	是	
操作	点选	增删查改、特权操作、登入、 登出。	否	
影响行数	点选+自定义值	大于、小于、等于、小于等于、 大于等于	是	
字段	点选、自定义	学习+数据库列集	是	某表的某列
响应状态	点选	默认、未知、登录成功、登录 失败、超时、等	否	
主机名	点选、自定义	学习+操作系统主机集	是	
操作系统用户	点选、自定义	学习+操作系统用户集	是	
数据库实例	点选、自定义	学习	是	
执行时长	点选+自定义值	大于、小于、等于、小于等于、 大于等于	是	毫秒
数据库类型	点选	ORACLE 、 MYSQL 、 SYBASE、CACHE 等	否	
SQL 语句	点选、自定义	自定义	是	
SQL 结果	点选、自定义	自定义	是	
数据库用户	点选、自定义	学习+数据库用户集	是	
SQL 模型	点选、自定义	自定义	是	
引擎	点选	通用配置中添加的引擎	否	
策略	点选	策略中心中的策略	否	
动作	点选	通过、报警、阻断	否	



风险等级	点选	无风险、低风险、中风险、高 风险、致命	否	
客户端端口	点选+自定义值	大于、小于、等于、小于等于、 大于等于	是	

提示:修改配置后,需点"保存"按钮进行保存,否则不生效。

4.2.1.4 计划

在"计划"中用户可以设定时间用以自动生成报告。可设置频率、时间及发送邮件的地址。

概述	数据范围	计划	结果集		🗎 保存	🏛 立即生成
启用计划		✔ 启用计划				
计划设置						
频率设置		 执行一次 重复执行 "执行一次" "重复执行" 	 : 按配置执行 : 按配置循环 	一次计划,在时间条件符合时却 检测计划,在时间条件符合时却	11行计划,配置不再 11行计划,配置不会	保存; 清除。
定时设置		 ● 毎日计划 ・设置 整点设置:0) 每周计划 (● 毎月计划 ✓ 整点 		
开始日期	[2016-05-17	17.			
发送邮件						

启用计划

勾选"启用计划"启用生成报告的计划任务。



概述	数据范围	计划	结果集	🗎 保存	100 立即生成
启用计划		☑ 启用计划			

计划设置

频率设置,可设定计划执行的频率;分为执行一次和重复执行两个选项。

広志いの単	 ● 执行一次 ● 重复执行
<u> </u>	
	"重复执行" :按配查循环检测计划,在时间条件符合时执行计划,配查不会清除。

定时设置

定时设置,可设定生成报告周期任务的执行时间、分为每日计划、每周计划、每月计划; 可设定计划执行的具体整点时间。

	● 每日计划 每周计划
定时设置	· ^皮 整点设置: 0 · · · · · · · · · · · · · · · · · ·

开始日期

开始日期,可设定计划开始执行的日期。

开始日期	2016-05-17	12.

发送邮件

设定接收报告的邮箱地址



提示:修改配置后,需点"保存"按钮进行保存,否则不生效。

4.2.1.5 结果集

通过结果集,用户能查看到对应模版已生成的报告,并能够进行重新发送、下载和删除 操作。重新发送会将报告发送到设定的邮箱中,下载会将报告下载到本地,删除则将报告从 列表中删除。

	概述	数据范围	计划	结果集				🗎 保存	🧰 立即生成
	名称				生成时间	发送状态	操作		
1	<u>SOX数据库</u>	请求异常分析─S	OX数据库请求早	常分析123 201	60517C 2016-05-17 09:22:42	立即生成	1	新发送 🔸	下载 🗶 🔤 🕅 🕅
2	<u>SOX数据库</u>	请求异常分析-S	SOX数据库请求早	<u> 常分析 201605</u>	170920 2016-05-17 09:20:48	立即生成	- 1	謝发送 🔸	下载 🗶 删除

4.2.1.6 "保存"按钮

在概述、数据范围、计划中修改配置后,需点"保存"按钮进行保存,否则不生效,且 修改的参数会丢失。

8	■ 保存	🗎 保存 💼 立即生成
伊	菥	森 💼 立即生成

4.2.1.7 "立即生成"按钮

点击立即生成按钮,会根据选中的模版,和在概述、数据范围中修改的参数生成报告。 并在结果集中显示。



4.2.2 报告结果

通过报告结果,用户可以浏览到所有生成的报告,包括报告的名称、生成时间、发送状态等。并能够按照类型进行筛选。通过每条报告后的重新发送、下载、删除按钮,可进行重 新发送、下载和删除操作。重新发送会将报告发送到设定的邮箱中,下载会将报告下载到本 地,删除则将报告从列表中删除。

	报告	报告结果							
类	業型								
报律	结果								
	名称	生成时间		发送状态	操作				
1	SOX数据库请求	<mark>:异常分析-SO</mark> 2016-05-17 09::	22:42	立即生成	▲ 重新发送 🔸 下載 🗶 删除				
2	<u>SOX数据库请求异常分析-SO</u> 2016-05-17 09:20:48			立即生成	■ 重新发送 🔸 下載 🗶 删除				

五、 其他模块和配置

5.1 监控

所属用户: SysAdmin、SecAdmin、Auditor。

监控这个模块,主要用检测设备的运行状态,主要包括运行信息、访问趋势、引擎列表、 高风险告警列表、系统告警列表这几个模块。通过"监控"模块用户能够及时发现和解决设 备存在的问题,如 CPU 占用率高,磁盘空间不足等。

5.1.1 运行信息

所属用户: SysAdmin、SecAdmin、Auditor。



运行信息模块,包括设备的 CPU、内存、交换分区、磁盘四者的监控曲线图,以及网卡的信息(如网卡名称、最大传输单元、是否回环、状态等)。通过此模块,用户能够快速的了 解设备的运行状态。如下图所示:

通行機関										
COURT			100 90 90 70 70 50 50 30 30 10 0	的神	100 80 70 90 90 90 90 90 90 90 90 90 90 90 90 90	内存交換区	100 90 80 70 90 90 90 90 90 90 90 90 90 90 90 90 90	ità		
同卡名称	最大传输单元	是否因环	状态	mAC地址	IP地址	接收字节数	接收数据包	发送字节数	发送数据包	
1 br1	1500		直接	d8.cb.8a.ab.d0.0c	192. 168. 50. 5/24	32056 13	24307	2113 13	21319	
2 enp0	1500		连接	44:8a:5b:f4:5f:63	172. 16. 1. 128/24	24801 33	276260	52684 33	0	
3 empl	1500		连接	d8:cb:8s:sb:d0:0s		5674554 XB	18381258	1201162501 13	17290000008	
4 enp3	1500		道接	d8:eb:8u:ub:d0:0e		17 10	154	28 10	362	
5 enp4	1500		连接	d3:cb:8s:sb:d0:04		32674 13	28834	2105 83	21290	

5.1.2 访问趋势

所属用户: SecAdmin。

访问趋势模块,包括被访问趋势、事件排名、攻击趋势三者的监控曲线图,通过此模块, 用户能够快速的了解设备的访问状态。如下图所示:





5.1.3 引擎列表

所属用户: SecAdmin。 引擎列表模块,包括以下几个方面的信息, 名称:该引擎的名称。 类型:数据库的类型。 IP:该数据库引擎的 IP。 端口:数据库服务使用的连接端口。 缺省数据库:默认数据库。 如下图所示:





5.1.4 高风险告警列表

所属用户:SecAdmin。 高风险告警列表模块,主要包含以下信息, 审计防火墙:引擎的类型。 告警规则:设计的规则。 捕获时间:捕获该SQL语句的具体时间。 数据库:被保护的数据库。 数据库用户:数据库的用户名。 客户端IP:访问该数据库的IP。 处理状态:处理的状态。 处理人:具体的处理人。 SQL类别:该SQL语句的类别。

SQL 语句: 该 SQL 语句的具体内容。



如下图所示:

高	高风輪告警列表									
	审计防火墙	告警规则	捕获时间	数据库	数据库用户	客户端IP	处理状态	处理人	SQL类别	SQL语句
5	192.168.0.99:6000C	test1-≻rules2: 高≸	2016-05-24 19	TEST1	db2inst1	192.168.0			Create	create table haha (name warchar(10))
6	192.168.0.99:60000	test1-≻rules2: 髙	2016-05-24 19	TEST1	db2inst1	192.168.0			Delete	delete from haha where name='jack'
7	192.168.0.99:60000	test1-≻rules2: 高≸	2016-05-24 19	TEST1	db2inst1	192.168.0			Delete	delete from haha where name='tom'
8	192.168.0.99:60000	test1-≻rules2: 髙	2016-05-24 19	TEST1	db2inst1	192.168.0			Create	create table haha (name warchar(10))
9	192.168.0.99:60000	test1-≻rules2: 髙	2016-05-24 19	TEST1	db2inst1	192.168.0			Delete	delete from haha where name='jack'
10	192.168.0.99:60000	test1-≻rules2: 髙	2016-05-24 19	TEST1	db2inst1	192.168.0			Delete	delete from haha where name='tom'
11	192.168.0.99:60000	test1-≻rules2: 髙	2016-05-24 19	TEST1	db2inst1	192.168.0			Create	create table haha (name varchar(10))
12	192 168 0 99-60000	test1->rnles2: 萬	2016-05-24 19	TEST1	dh2inst1	192 168 0			Nelete	delete from baba where name=' iack'

5.1.5 系统告警列表

所属用户: SysAdmin、SecAdmin、Auditor。

系统告警列表模块,主要有发生时间、日志类型、状态、事件级别、事件内容、处理备 注几项内容,方便用户及时发现高危的报警。及时发现可能危险、。

如下图所示:

发生时间	日志类型	状态	事件级别	事件内容	处理备注
5 2016-05-06 10:58:49	应用	已处理	警告	数据库审计防火墙停止完成。。。	12
6 2016-05-05 16:52:52	应用	未处理	警告	数据库审计防火墙启动完成。。。	
7 2016-05-05 16:51:44	应用	未处理	警告	数据库审计防火墙停止完成。。。	
8 2016-05-05 16:41:43	应用	未处理	警告	数据库审计防火墙启动完成。。。	
2016-05-05 16:41:25	应用	未处理	警告	数据库审计防火墙停止完成。。。	
0 2016-05-05 15:22:10	应用	未处理	警告	数据库审计防火墙启动完成。。。	

5.2 通用配置

所属用户:SysAdmin、SecAdmin、Auditor。 本模块主要进行数据库引擎添加和管理以及用户管理, SysAdmin 用户可用此模块尽心用户的添加和管理



SecAdmin 用户可用此模块进行用户授权管理;在使用数据库审计、数据库状态监控、 风险扫描等功能前都要首先在此模块添加配置相应的引擎及引擎。

Auditor 用户可用此模块进行用户授权管理。

5.2.1 SysAdmin 用户管理

SysAdmin 用户通过通用配置模块可以添加用户,并对用户授权

提示:未授权的用户只对监控模块有权限,授权后的用户对监控和系统管理两个模块有 权限

5.2.1.1 用户添加

1.SysAdmin 用户进入通用配置模块在用户管理页面点击 "添加"

用户管理	
用户列表	
 + 添加 ☆ 修改密码 □ 授权 	
用户名	角色名
admin	系统操作员
admin1	默认管理员

2.弹出添加用户窗口,输入用户名和密码然后点击"确定"



添加用户	×
用户名称	admin2
输入密码	
确认密码	••••••
	字母开头,并要包含数字,长度在
	✔ 确定

5.2.1.2 授权管理

3.点选添加的用户,点击 "授权"按钮即可对该用户授权

用户列表	
+ 添加	
用户名	角色名
admin	系统操作员
admin2	系统操作员
admin1	默认管理员

4.点选已授权的用户,点击 "取消授权"按钮即可取消对该用户的授权



用户管理		
用户列表		
🕇 添加 💼 删除 🥒 修改密码	ロ 取消授权	
用户名		角色名
admin2		系统操作员
admin		默认管理员

提示:已授权的用户"角色名"显示为系统管理员,未授权的用户"角色名"显示为默认管理员。

5.2.1.3 用户删除

点选需要删除的用户,点击"删除"按钮,弹出确认窗口,单击"确定"即可删除用 户,如下图所示:

用户管理	
用户列表	
+添加 亩 删除 ✓ 修改密码 Ц 授权	
用户名	
admin	
admin2 确认 😢	
admin1 确认删除吗?	
✔ 确定 ★ 取消	



5.2.1.4 修改密码

点选需要修改密码的用户,点击 "修改密码"按钮,弹出修改密码窗口,输入原始密码 及新密码单击 "确定"即可完成密码的修改,如下图所示:

-			
用户列表			
🕈 添加 💼 删除	🥒 修改密码	🖵 取消授权	
用户名			
admin	修改密码	X	
admin2			
	用户名称	admin2	
	原始密码		
	新密码		
	确认密码		
	♀ 密码需以 8和30之间.	字母开头,并要包含数字.长度在	
		✔ 确定	

5.2.2 Auditor 用户管理

Auditor 用户通过通用配置模块可以对 SysAdmin 用户添加但未进行授权的用户,进行 授权。

提示:授权后该用户对"系统审计"和"监控"两个模块具有权限

5.2.2.1 授权管理

1.点选需要授权的用户,点击 "授权"按钮即可对该用户授权



用户管理	
用户列表	
□ 授权	
用户名	角色名
admin	审计操作员
admin1	默认管理员

2.点选已授权的用户,点击 "取消授权"按钮即可取消对该用户的授权

	用户管理	
用户列表		
🖵 取消授权		
用户名		角色名
admin		审计操作员
admin1		默认管理员

提示:已授权的用户"角色名"显示为审计操作员,未授权的用户"角色名"显示为默 认管理员。



5.2.3 SecAdmin 用户管理

SecAdmin 用户通过通用配置模块可以对 SysAdmin 用户添加但未进行授权的用户,进行授权。

提示:授权后该用户继承 Secadmin 用户除"用户管理"以外的所以权限。

5.2.3.1 授权管理

1.点选需要授权的用户,点击 "授权"按钮即可对该用户授权

	数据库引擎	用户管理			
用户列表					
日授权					
用户名					角色名
admin1					默认管理员
1					

2.点选已授权的用户,点击 "取消授权"按钮即可取消对该用户的授权



	数据库引擎	用户管理			
用户列表					
🖵 取消授权					
用户名					角色名
admin1					安全操作员

提示:已授权的用户"角色名"显示为安全操作员,未授权的用户"角色名"显示为默认管理员。

5.3 告警

所属用户: SecAdmin。

该模块用于显示数据库审计、防火墙的告警信息,以及对告警信息进行处理。

5.3.1 数据库告警

5.3.1.1 高风险告警

进入告警功能模块,点击"数据库告警">"数据库高风险",显示风险级别为高和致 命的告警信息。



数据库告警 FT	TP告警										
	高	高风险列表									
高风险列表	2	更新									
SQL注入风险列表		审计防火墙	告警规则	捕获	數据库实例	数据库用户	客户端IP	处理状态	处理人		
自定义查询	1	172.17.200.194:3306/	my->test1: 高风险 ; my1->test2: ;	高风险;2016-05-16 16:02:39	9 null	root	172.16.0.125				
	当	前记录详情									
	Ĩ	计防火墙名称		数据库实例				数据库类型			
				***Petro							

告警信息按照时间倒序显示,具体功能如下:

更新

重新检索告警信息,操作方法如下:

点击"更新"按钮,则将新检索告警信息并显示。

5.3.1.2 Sql 注入风险列表

显示所有的 sql 注入风险。
NetEye 数据库审计系统



数据库与应用安全加	固系统		安全管理员: SecAdmin	🏛 修改密码	📩 安全退出	🖵 返回主页			
数据库告警	FTP告警								
	高风险列表	高現驗機							
高风险列表	📚 更新								
SQL注入风险列表	审计防火墙	告警规则	捕获数	据库实{数据库用}客户端IP	处理状态 处理人	处理备注 SQL参	别 SQL语句		
自定义查询									
	当前记录详情								
	审计防火墙名称		数据库实例		数据库类型		数据库用户		
			数据库IP		客户端IP		数据库MA	с	
	客户端MAC		主机名		操作系统用户		客户端程序	:	
	客户端用户名		客户端端口		捕获		执行时长(雷]秒)	
	司行軍		日志级别		风险等级		告警规则		
	SQL类别		响应状态						
	SQL语句								
	SQL结果								

具体功能如下:

更新

操作方法如下:

点击"更新"按钮,则将会重新检索告警信息并显示。

5.3.1.3 自定义查询

显示所有风险级别的告警信息,操作方法如下:

首先选择告警信息的过滤条件,条件包括操作时间、数据库实例、策略、SQL 类别、动

作、风险等级、关键字、客户端 IP、数据库用户、客户端用户名;

设置好条件后,点击提交查询,则显示按照条件过滤后的告警信息。

告警信息的详情缺省不显示,如要显示,则点击页面右下角的向上的箭头,或点击显示 详情按钮。

NetEye 数据库审计系统



数据库与历用交全加图系统 安全管理说:Satabain 🛑 能改变用 👘 安全混出 🖵 范回目							
数据库告警 FTP告警							
	查询结果						
高风险列表	✓ 处理 ✓ 全部处理 ② 更新 Q 导出报表 I 显示详持 Q 提交查询 □ 重置查询						
SQL注入风险列表	操作时间	9 B	数据库实例	策略 🗸			
自定义查询	SQL类别 🗸	动作	风险等级	✓ 关键字			
	客户端IP	数据库用户	记录条数上限	客户演用户名			
	■ 审计防火墙 告警规则	捕获 数据库实(数据库用)客户满IP	处理状态 处理人 处理备注 SQL类	別 SQL语句			
	20 ▼ 14 4 第 1 共1页 ▶)	Ó		显示0到0, 共0记3			

具体功能如下

处理/全部处理

对告警信息进行备注,标识已处理过此告警,操作方法如下:

- 1. 选中某一条或几条告警信息,选中"处理"或"全部处理";
- 2. 在显示的对话框中,填写处理备注;
- 3. 选则确定。系统将记录处理备注,处理人和处理时间。

更新

重新检索告警信息,操作方法如下:

点击更新按钮,则将会按照当前过滤条件,重新检索告警信息并显示。

导出报表

将当前的告警信息导出为报表文件,操作方法如下:

- 1. 点击导出报表,显示导出条件的对话框;
- 2. 填写或选中导出条件,并选择确定;
- 3. 系统将生成报表文件,并下载。



显示详情

点击则显示告警信息的详情;

提交查询

点击则按照当前过滤条件提交查询,并显示新的告警信息;

重置查询

点击则把查询条件置为缺省值。

5.3.2 FTP 告警

查询结果

通过 FTP 告警页面可检索查看 FTP 告警信息。可以时间、服务器 IP、客户端 IP、用户 名、文件名、关键字和风险等级为条件进行筛选查询。通过"重置"按钮,清楚所设置的条 件,点选相应文件,点击"批量下载"按钮可将文件下载到本地。通过"导出"按钮可将条 目以文件的形式导出到本地。



概要

在概要中能够查看到相应文件的文件名和存放路径等信息。



NetEye 数据库审计系统



5.4 系统审计

所属用户: Auditor。

系统审计模块记录了用户登录、登出系统,更改网卡接口设置、导出报告、等操作。

5.4.1 审计防火墙操作日志管理

通过管理模块,用户可对系统日志进行过滤筛选,可操作的条件包括:操作时间、IP、 用户名、功能点、动作。用户可通过"查询"按钮按照设置的条件尽行查询,通过"重置" 按钮可将查询条件恢复为缺省值(空)。

审计	防火墙操作日志							
审计防火墙操作日志管理								
操作时间[开始]	2016-05-10 17:51:52	操作时间[结束]	2016-05-17 17:51:56	IP				
用户名		功能点		动作				
操作	Q 查询 L 重置	管理	◆ 以当前条件导出					

通过"以当前条件导出"用户可将日志的详细信息以 PDF、WORD 等文件的形式导出, 以方便查阅,在弹出中可设置导出行数。

▲ 当前条件导	出文件	×			
	◎ 全部(最多20000行)				
行数	◉ 指定行数: 500	(1~20000)			
报表格式	PDF格式 🗸				
	PDF格式				
	EXCEL格式	✔ 确定 🗮 取消			
	WORD格式				
登录系统		登入系统			



5.4.2 日志

E	志模块	显示了用。	户名、IP、	操作时间、	功能点、动作	、详细信息。	方便用户查看。
日志	i						
	序号	用户名	IP	操作时间	功能点	动作	详细信息
1	94	Auditor	172. 16. 1. 126	2016-05-16 17:33:17	豐录系统	聖入系统	螢录成功!
2	93	SecAdmin	172. 16. 1. 126	2016-05-16 17:33:10	登录系统	登出系统	退出成功!
3	92	SecAdmin	172. 16. 1. 126	2016-05-16 17:17:01	报告	增加报告	增加报告成功,类型:自定义
4	91	SecAdmin	172. 16. 1. 126	2016-05-16 16:44:46	风险告答	告響处理	处理成功,内容:已处理
5	90	SecAdmin	172. 16. 1. 126	2016-05-16 15:53:03	登录系统	登入系统	登录成功 !
6	89	Auditor	172. 16. 1. 126	2016-05-16 15:52:57	登录系统	登出系统	退出成功!
7	88	Auditor	172. 16. 1. 126	2016-05-16 15:52:55	登录系统	登入系统	登录成功 !
8	87	SysAdmin	172. 16. 1. 126	2016-05-16 15:52:46	登录系统	登出系统	退出成功!
9	86	SysAdmin	172. 16. 1. 126	2016-05-16 15:52:44	登录系统	登入系统	登录成功 !
10	85	SecAdmin	172. 16. 1. 126	2016-05-16 15:52:40	登录系统	登出系统	退出成功!
11	84	SecAdmin	172. 16. 1. 126	2016-05-16 14:27:02	登录系统	登入系统	登录成功!
12	83	SecAdmin	172. 16. 1. 126	2016-05-16 14:26:55	登录系统	登出系统	退出成功!
13	82	SecAdmin	172. 16. 1. 126	2016-05-16 14:12:17	登录系统	登入系统	登录成功!
14	81	SecAdmin	172. 16. 1. 126	2016-05-16 13:14:19	登录系统	登入系统	登录成功 !
15	80	SecAdmin	172. 16. 1. 126	2016-05-16 10:15:55	审计防火墙	引擎控制	启动成功, 名称: 172.17.200.194:3306/testdb
16	79	SecAdmin	172. 16. 1. 126	2016-05-16 10:15:54	审计防火墙	引擎控制	停止成功, 名称: 172.17.200.194:3306/testdb
17	78	SecAdmin	172. 16. 1. 126	2016-05-16 10:08:02	登录系统	登入系统	登录成功!
18	77	SysAdmin	172. 16. 1. 126	2016-05-16 10:07:57	登录系统	登出系统	退出成功!
19	76	SysAdmin	172. 16. 1. 126	2016-05-16 10:07:45	登录系统	登入系统	登录成功!
20	75	SysAdmin	172.16.1.126	2016-05-16 10:06:33	登录系统	登入系统	密码错误,帐号已被锁定,1后再登录!