数据库安全服务(DBSS)

用户指南

文档版本01发布日期2024-11-28





版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可,任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部,并不得以任何形式传播。

商标声明

NUAWE和其他华为商标均为华为技术有限公司的商标。 本文档提及的其他所有商标或注册商标,由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束,本文档中描述的全部或部 分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定,华为云计算技术有限公司对本文 档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因,本文档内容会不定期进行更新。除非另有约定,本文档仅作为使用指导,本文 档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址: 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编: 550029

网址: <u>https://www.huaweicloud.com/</u>

目	录
---	---

1 总览	1
2 开通并使用数据库安全审计(安装 Agent)	4
	4
2.2 购买数据库安全服务	8
2.3 步骤一:添加数据库	13
2.4 步骤二:添加 Agent	19
2.5 步骤三:下载并安装 Agent	28
2.5.1 下载 Agent	28
2.5.2 安装 Agent (Linux 操作系统)	
2.5.3 安装 Agent (Windows 操作系统)	33
2.6 步骤四:添加安全组规则	
2.7 步骤五:开启数据库安全审计	
3 开通并使用数据库安全审计(免安装 Agent)	44
3.1 流程指引	
3.2 购买数据库安全服务	46
3.3 步骤一:添加数据库	51
3.4 步骤二:开启数据库安全审计	57
4 开通并使用数据库安全加密	59
4.1 步骤一: 购买数据库安全加密	59
4.2 步骤二:登录实例 Web 控制台	65
4.3 步骤三:系统功能配置及使用场景举例	67
4.3.1 场景一:加密操作流程及加密功能典型配置	67
4.3.2 场景二: 解密操作流程及解密功能典型配置	76
4.3.3 场景三: 业务测试典型配置举例	
4.3.4 场景四: 动态脱敏典型配置举例	84
5 开通并使用数据库安全运维	91
5.1 步骤一: 购买数据库安全运维实例	
5.2 步骤二:登录实例 web 控制台	
5.3 步骤三:系统功能配置及使用场景举例	98
5.3.1 快速使用指南	
5.3.1.1 运维人员操作管理体系流程	98
5.3.1.2 策略应用流程	100

5.3.2 反向代理部署配置举例	
5.3.3 自定义策略阻断举例	
5.3.4 客户端语句过滤白名单配置举例	
5.3.5 虚拟补丁防护配置举例	
5.3.6 业务字典配置举例	
5.3.7 Web 安全客户端配置举例	
5.3.8 工单审批配置举例	
6 升级数据库审计实例版本	
7 配置审计规则	131
7.1 添加审计范围	
7.2 添加 SQL 注入规则	
7.3 管理 SQL 注入规则	
7.4 添加风险操作	
7.5 配置隐私数据保护规则	
7.6 SQL 白名单	
7.6.1 添加 SQL 白名单	
7.6.2 管理 SQL 白名单	
8 查看审计结果	148
8.1 查看 SQL 语句详细信息	
8.2 查看会话分布	
8.3 查看审计总览信息	
8.4 查看审计报表	
8.5 查看趋势分析	
9 通知设置管理	
9.1 设置邮件通知	
9.2 设置告警通知	
10 查看监控信息	
10.1 查看系统监控信息	
10.2 查看告警信息	
11 备份和恢复数据库审计日志	
12 其他操作	
12.1 管理数据库安全审计实例	
12.2 查看实例概览信息	
12.3 管理添加的数据库和 Agent	
12.5 管理审计范围	
12.6 查看 SQL 注入检测信息	
12.7 管理风险操作	
12.8 管理隐私数据保护规则	
12.9 管理审计报表	

12.10 管理备份的审计日志	
12.11 查看操作日志	
13 云审计服务支持的关键操作	197
131 如何查考元审计日志	197
13.7 如何宣省公中行口心	
14 收均	100
Ⅰ♀ <u></u> 1/1 DRSS 收掠指行道明	
14.1 DB35 血红雨你呒呀 14.2 没罟些坎生螫抑则	
14.3 查看监控指标	207
	204
16 数据库安全加密管理	
16.1 数据库安全加密实例官理	
16.2 系统官理页操作指导	
16.2.1 平台官埕	
16.2.1.1 网络 <u>能且</u>	
16.2.1.2	213 217
16.2.1.3 面份与恢复能量信念	
16.2.1.5 查看高可用信息	219
16.2.2 修改安全口令	
16.2.3 初始化密钥	
16.2.4 添加数据资产	
16.2.5 业务测试和分析	
16.2.6 敏感数据发现	233
16.2.6.1 扫描资产的敏感数据	
16.2.6.2 查看扫描任务执行结果	235
16.2.6.3 在结果中创建加密队列	237
16.2.6.4 在结果中创建脱敏规则	239
16.2.6.5 新增自定义数据类型	
16.2.6.6 新增行业模板	
16.2.7 数据加密和解密	
16.2.7.1 设置加密参数	
16.2.7.2 查看加密算法	
16.2.7.3 仿真加密测试	
16.2.7.4 配置加密队列	
16.2.7.5 官埋授权	
10.2.7.0 加具群省测试	
10.2.7./	
10.2.7.0 加密农目理	255 רשר
10.2.7.3 凹/夜夜归 ¹⁹ ····································	/ 25 ۲۵۰
10.2.7.10 又衣 Dypass 油汁	

16.2.7.11 查询应用访问记录	
16.2.8 动态脱敏	
16.2.8.1 新增自定义脱敏算法	
16.2.8.2 创建脱敏规则	
16.2.8.3 配置脱敏白名单	
16.2.9 密钥管理	
16.2.9.2 配置 KMS 对接	
16.2.9.3 查看密钥信息	
16.2.10 系统管理	
16.2.10.1 手动创建账号	
16.2.10.2 组织架构管理	270
16.2.10.2.1 创建组织部门	
16.2.10.2.2 手动创建成员	
16.2.10.3 系统运维	
16.2.10.3.1 查看系统监控	
16.2.10.3.2 系统诊断	273
16.2.10.3.3 日志采集	274
16.2.10.3.4 设置自动清理	
16.2.10.4 查看消息通知	275
16.2.10.5 系统设置	
16.2.10.5.1 通用设置	276
16.2.10.5.2 时间设置	276
16.2.10.5.3 告警设置	277
16.3 安全管理员操作指导	277
16.3.1 系统管理	
16.3.1.1 查看角色	277
16.3.1.2 审核账号	278
16.3.1.3 配置安全设置	
16.4 审计管理员操作指导	
16.4.1 查看系统操作日志	281
16.4.2 查看系统设备日志	281
17 数据库安全运维管理	
17.1 数据库运维实例管理	
17.2 系统管理员操作指南	
17.2.1 首页信息	
17.2.2 资产管理	
17.2.2.1 添加数据资产	
17.2.2.2 手动添加账号	
17.2.2.3 误删恢复	292
17.2.3 策略防护	
17.2.3.1 概述	

17 2 3 2	293
17232 采唱及直	
1723221 曾理墨平的直	294
17.2.3.3 自定义策略	295
17.2.3.3.1 添加 SOL 策略	
17.2.3.3.2 添加包过滤策略	
17.2.3.3.3 启用或禁用策略	
17.2.3.3.4 添加客户端语句过滤白名单	
17.2.3.4 设置虚拟补丁	
17.2.4 审计日志	
17.2.4.1 查看审计日志信息	
17.2.4.2 回放审计日志语句	
17.2.4.3 添加业务字典	
17.2.4.4 启用业务字典功能	
17.2.5 风险管控	
17.2.5.1 执行风险扫描	
17.2.5.2 进行风险管理	
17.2.6 报表分析	
17.2.6.1 添加并生成报表	
17.2.6.2 下载并查看报表	
17.2.7 运维管理	
17.2.7.1 审批运维工单	
17.2.7.2 管理运维人员	
17.2.8 设备管理	
17.2.8.1 Bypass 设置	
17.2.9 日志设置	
17.2.9.1 配置日志保存方式	
17.2.9.2 备份还原日志	
17.2.9.2.1 自动备份	
17.2.9.2.2 手动备份	
17.2.9.2.3 还原日志	
17.2.10 系统管理	
17.2.10.1 查看平台信息	
17.2.10.2 手动创建账号	
17.2.10.3 诊断系统实时情况	
17.2.10.4 升级系统版本	
17.2.10.5 时间配置	
17.2.10.6 查看设备状态	
17.2.10.7 网络配置	
17.2.10.7.1 配置网卡信息	
17.2.10.7.2 配置路由信息	
17.2.10.8 查看和配置消息中心	

17.3 安全管理员操作指南	
17.3.1 设置审批架构	
17.3.2 系统管理	
17.3.2.1 审核账号	336
17.3.2.2 角色管理	
17.3.2.3 启用安全配置	
17.3.2.3.1 设置用户登录安全	
17.3.2.3.2 设置账号密码安全	
17.3.2.3.3 启用网络访问安全配置	
17.4 审计管理员操作指南	
17.4.1 查看操作审计日志	
17.5 数据库操作员操作指南	
17.5.1 发起运维工单申请	
17.5.2 通过 Web 安全客户端访问资产	
18 权限管理	
18.1 创建用户并授权使用 DBSS	344
18.2 DBSS 自定义策略	
18.3 DBSS 权限及授权项	
18.4 FullAccess 敏感权限配置	348

目录

1 总览

在总览页可开启数据库审计的定时刷新,查看每个实例的审计信息,查看全量实例的 语句、风险、会话的审计情况。

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安全服务",进入数据库安全审计"总览"界面。

图 1-1 进入总览

- (1) (1)				@ #9 #70 < # #555 □	在地站和 NFK版体女全般的
总宽 风险总量					
最新数据更新时间: 2024/11/11 21:21:53 G	MT+08.00			工会保	
我的审计信息					
所有实例					
3月28天7小时	339,845,482	3,765	6,332	1,187	858
审计码长	近なな最	风险登量 >	今日語句	¢⊟RIQ	\$B\$\$
单个实例信息					への絵
					88 =
清榆入宾创名称					d C
^ DBSS-		^ DBSS			
^ DBSS-		^ DBSS			
∧ DBSS-		∧ DBSS-			
△ DBSS-		^ DBSS			
A		0. DBSS			

步骤3 单击右上角"汇总信息定时刷新"开关,可开启审计信息定时刷新。

🗀 说明

开启后,系统按照预设规则每间隔1小时对全量审计信息进行刷新。

----结束

我的审计信息

展示对所有实例扫描检测的统计展示。

表 1-1 参数说明

参数名称	参数说明
审计时长	历史累计审计所有实例所用的时间。
语句总量	历史累计审计所有实例用到的查询语句。
风险总量	历史累计审计所有实例发现的风险总数。
今日语句	当日审计所有实例用到的查询语句。
今日风险	当日审计所有实例发现的所有风险。
今日会话	当日审计所有实例建立的会话数。

单个实例信息

按照单个实例的维度统计展示实例审计情况,默认展示10条,超过数量分页显示。

数据分析图展示

按照语句总量、风险总量、今日语句、今日风险、今日会话的维度分别统计展示全量 实例的审计情况。

单击右上角可切换统计图展示样式。

TOP5 语句总量

展示历史审计中使用语句最多排列前5的实例。

图 1-2 TOP5 语句总量

0

风险级别总体分析

统计所有实例中高、中、低风险等级命中次数,并且在右侧从高至低排列风险等级命 中次数最高的三个实例。

🛄 说明

支持自定义时间段查看总体风险,单击右上角的 🗐 图标选择时间区间。

风险规则总体分析

统计所有风险规则命中的次数,并且在右侧从高至低排列风险规则命中次数最高的五 个规则。

文档版本 01 (2024-11-28)

其他风险角度分析

可以从以下三个方向查看分析报告:

- 风险级别: 高、中、低风险
- 风险规则: 根据选择具体的风险规则查看
- 数据库统计:选择具体的数据库查看风险触发次数

2 开通并使用数据库安全审计(安装 Agent)

2.1 流程指引

本节内容指引您快速启用数据库安全审计服务DBSS。

背景信息

数据库安全审计支持对华为云上的ECS/BMS自建数据库和RDS关系型数据库进行审计。

须知

- 数据库安全审计不支持跨区域(Region)使用。待审计的数据库必须和购买申请的数据库安全审计实例在同一区域。
- 数据库开启SSL时,将不能使用数据库安全审计功能。如果您需要使用数据库安全 审计功能,请关闭数据库的SSL。关闭数据库SSL的详细操作,请参见如何关闭数据 库SSL?。
- 有关审计数据的保存说明,请参见数据库安全审计的审计数据可以保存多久?。

首先,您需要创建一个数据库安全审计实例,然后连接数据库与新创建的数据库安全 审计实例,连接成功后,即可开启数据库安全审计。

通过 Agent 方式审计数据库

表2-1中的数据库类型及版本,需采用安装Agent方式开启DBSS服务。

数据库类型	版本	
MySQL	 5.0、5.1、5.5、5.6、5.7 8.0(8.0.11及以前的子版本) 8.0.30 8.0.35 8.1.0 8.2.0 	
Oracle (因Oracle为闭源协议,适配版本复杂, 如您需审计Oracle数据库,请先联系客 服人员)	 11g 11.1.0.6.0 (11.2.0.1.0 (11.2.0.2.0) 11.2.0.3.0 (11.2.0.4.0) 12c 12.1.0.2.0 (12.2.0.1.0) 19c 	
PostgreSQL	 7.4 8.0、8.1、8.2、8.3、8.4 9.0、9.1、9.2、9.3、9.4、9.5、9.6 10.0、10.1、10.2、10.3、10.4、10.5 11 12 13 14 	
SQL Server	 2008 2012 2014 2016 2017 	
GaussDB(for MySQL)	8.0	
DWS	1.58.1	
DAMENG	DM8	
KINGBASE	V8	
SHENTONG	V7.0	
GBase 8a	V8.5	
GBase 8s	V8.8	
Gbase XDM Cluster	V8.0	

表 2-1 数据库安全审计支持的数据库类型和版本

数据库类型	版本
Greenplum	V6.0
HighGo	V6.0
GaussDB	 1.3企业版 1.4企业版 2.8企业版 3.223企业版
MongoDB	V5.0
DDS	4.0
Hbase (华为云审计实例: 23.02.27.182148及 其之后的版本支持) Hive (华为云审计实例: 23.02.27.182148及 其之后的版本支持)	 1.3.1 2.2.3 1.2.2 2.3.9
	3.1.23.1.3
MariaDB	10.6
TDSQL	10.3.17.3.0
Vastbase	G100 V2.2
TiDB	 V4 V5 V6 V7 V8

图 2-1 快速使用数据库安全审计流程图



表 2-2	快速使用数据库安全审计操作步驶	驟
-------	-----------------	---

步骤	配置操作	说明
1	添加数据库	购买数据库安全审计后,您需要将待审计的数据 库添加到数据库安全审计实例。
2	添加Agent	添加数据库后,您需要为添加的数据库选择 Agent的添加方式。 数据库安全审计支持对华为云上的ECS/BMS自建 数据库和RDS关系型数据库进行审计,请根据您 在华为云上实际部署的数据库选择Agent添加方
		式。
3	添加安全组规则	Agent添加完成后,您还需要为数据库安全审计 实例所在的安全组添加入方向规则TCP协议 (8000端口)和UDP协议(7000-7100端口), 使Agent与审计实例之间的网络连通,数据库安 全审计才能对添加的数据库进行审计。
4	安装 Agent(Linux操 作系统)	安全组规则添加完成后,您还需要下载Agent, 并根据Agent的添加方式在数据库端或应用端安 装Agent。
5	开启数据库安全审计	Agent安装成功后,您还需要开启数据库安全审 计功能,将添加的数据库连接到数据库安全审计 实例,才能使用数据库安全审计功能。

步骤	配置操作	说明
6	查看审计结果	数据库安全审计默认提供一条"全审计规则"的 审计范围,可以对连接数据库安全审计实例的所 有数据库进行审计。开启数据库安全审计后,您 可以在数据库安全审计界面查看被添加的数据库 的审计结果。
		须知 您可以根据业务需求设置数据库审计规则。有关配置 审计规则的详细操作,请参见 <mark>配置审计规则</mark> 。

容器化部署方式

所有数据库类型及版本均支持使用容器化部署方式,开启DBSS服务。

具体请参见: 容器化部署数据库安全审计Agent。

相关操作

- 如何选择Agent添加方式以及安装Agent的节点的详细介绍,请参见如何选择数据 库安全审计的Agent安装节点?。
- 如果审计功能无法正常使用,请参照<mark>无法使用数据库安全审计</mark>章节进行处理。

效果验证

当您将添加的数据库连接到数据库安全审计实例后,数据库安全审计将记录被添加的 数据库的操作行为。您可以在数据库安全审计界面查看被添加的数据库的审计结果。

2.2 购买数据库安全服务

本章节介绍如何购买数据库安全服务。数据库安全服务提供包年/包月计费方式。

约束与限制

- 数据库安全服务不支持跨区域(Region)使用。待审计的数据库必须和购买的数据库安全审计实例在同一区域。
- 购买数据库安全审计实例配置VPC参数,必须与Agent安装节点(应用端或数据库端)所在的VPC保持一致。否则,将导致Agent与审计实例之间的网络不通,无法使用数据库安全审计。创建共享VPC请参见共享VPC。
 数据库安全审计的Agent安装节点,请参见:如何选择数据库安全审计的Agent安装节点?。

系统影响

数据库安全服务为旁路模式审计,不影响用户业务,与本地审计工具不冲突。

前提条件

请参见DBSS权限管理确认实例账号具有相关权限。

文档版本 01 (2024-11-28)

须知

请确认购买实例的账号具有"DBSS System Administrator"、"VPC Administrator"、"ECS Administrator"和"DBSS Administrator"角色。

- VPC Administrator:对虚拟私有云的所有执行权限。项目级角色,在同项目中勾选。
- DBSS Administrator: 对账号中心、费用中心、资源中心中的所有菜单项执行任意操作。项目级角色,在同项目中勾选。
- ECS Administrator:对弹性云服务器的所有执行权限。项目级角色,在同项目中勾选。

操作步骤

- 步骤1 登录管理控制台。
- 步骤2 进入数据库安全审计购买页面。
- **步骤3** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤4 在界面右上角,单击"购买数据库安全服务"。
- 步骤5选择"区域"、"可用区类型"、"可用区"和"性能规格"。

图 2-2 选择可用区和版本规格

医喉			
• ~			
请他还还择靠正把业务的区域,可减少网络时程,摆弯访问图度。			
可用区类型			
MHORIS .			
বলহ			
Nation 可用区1 可用区2 可用区4 可用区5			
P6 # 1848			
alt-room			
		🗘	()
入门版	其动物	专业运	高级版
最多支持1个数据库实例	最多支持3个数据库实例	★ ★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★	最多支持30个数据库实例
吞吐量蜂值	春吐量維值	吞吐量蜂蕉	吞吐量蜂值
1000集/秒	3000条/秒	6000条/紗	30000条/紗
入库速率	入库速率	入库速率	入库速率
120万条/小时	360万条/小时	720万条/小时	1080万条/小时
在线SQL语句存储	在线SQL语句符储	在线SQL语句存储	在线SQL语句存储
1亿余	4亿条	6亿余	15亿条
¥1,000.00 //	¥3,000.00 //	¥6,000.00 //E	¥24,000.00 //3

各版本的性能规格说明如<mark>表2-3</mark>所示。

表 2-3 数据库安全服务版本规格说明

版本	支持的数据库实例	性能参数
入门版	最多支持1个数据库实 例	 吞吐量峰值: 1,000条/秒 入库速率: 120万条/小时 在线SQL语句存储: 1亿条

版本	支持的数据库实例	性能参数
基础版	最多支持3个数据库实 例	 吞吐量峰值: 3,000条/秒 入库速率: 360万条/小时 在线SQL语句存储: 4亿条
专业版	最多支持6个数据库实 例	 吞吐量峰值: 6,000条/秒 入库速率: 720万条/小时 在线SQL语句存储: 6亿条
高级版	最多支持30个数据库 实例	 吞吐量峰值: 30,000条/秒 入库速率: 1,080万条/小时 在线SQL语句存储: 15亿条

🛄 说明

● 支持的数据库实例通过**数据库IP+数据库端口**计量。

如果同一数据库IP具有多个数据库端口,数据库实例数为数据库端口数。1个数据库IP只有1 个数据库端口,即为一个数据库实例;1个数据库IP具有N个数据库端口,即为N个数据库实例。

例如:用户有2个数据库资产分别为IP₁和IP₂,IP₁有一个数据库端口,则为1个数据库实例; IP₂有3个数据库端口,则为3个数据库实例。IP₁和IP₂合计为4个数据库实例,选择服务版本 规格时需要大于或等于4个数据库实例,即选用专业版(最多支持审计6个数据库实例)。

- 不支持修改规格。若要修改,请退订后重购。
- 本表中在线SQL语句的条数,是按照每条SQL语句的容量为1KB来计算的。

步骤6 设置数据库安全审计参数,如图2-3和图2-4所示,相关参数说明如表2-4所示。

图 2-3 网络配置

网络配置

虚拟私有云

vpc-f76c	\sim)[(Э)	新建虚拟私有云(2
----------	--------	-----	----	----------	---

建议VPC选择时,尽量与Agent安装节点所在VPC相同。

子网

subnet-f785 V Q	新建子网 🖸
-----------------	--------

子网是虚拟私有云内的IP地址块,虚拟私有云中的所有云资源都必须部署在子网内。

安全组

Sys-default v Q 新建安全组 🖸

安全组用来实现安全组内和组间数据库安全服务的访问控制,加强数据库安全服务的安全保护。

图 2-4 高级配置

∧ 高级配置			
实例名称			
DBSS-dd37			
实例类型			
主备			
备注(可选)			
请输入备注信息			
企业项目			
default ~	◎ 新建企业项目 🖸		
标签			
如果您需要使用同一标签标识多种云资源	1, 即所有服务均可在标签输入框下拉选择同一标签,	建议在TMS中创建预定义标签 🖸	Q
十 添加新标签			
您还可以添加50个标签。			

表 2-4 数据库安全审计实例参数说明

参数名称	说明
虚拟私有云	您可以选择使用区域中已有的虚拟私有云(Virtual Private Cloud,VPC)网络,或者单击"查看虚拟私有云",跳转到 VPC管理控制台创建新的虚拟私有云。
	说明
	 请选择Agent安装节点(应用端或数据库端)所在的VPC。数据库 安全审计的Agent安装节点,请参见:如何选择数据库安全审计的 Agent安装节点?
	● 不支持修改VPC。若要修改,请退订后重购。
	更多有关虚拟私有云的信息,请参见《虚拟私有云用户指 南 》。
安全组	您可以选择区域中已有的安全组,或者在VPC管理控制台创建 新的安全组。选择实例的安全组后,该实例将受到该安全组访 问规则的保护。
	更多有关安全组的信息,请参见《虚拟私有云用户指南》。
子网	您可以选择VPC中已配置的子网,或者在VPC管理控制台为 VPC创建新的子网。
实例名称	您可以自定义实例的名称。
备注	您可以添加实例备注信息。
企业项目	该参数针对企业用户使用。
	企业项目是一种云资源管理方式,企业项目管理服务提供统一 的云资源按项目管理,以及项目内的资源管理、成员管理,默 认项目为default。
	请在下拉框中选择所在的企业项目。更多关于企业项目的信 息,请参见 《企业管理用户指南》 。

参数名称	说明
标签	可选配置,对数据库安全审计实例的标识。使用标签可以方便 识别和管理用户拥有的数据库安全服务资源。每个实例最多支 持50个标签配额。
	如用户的组织已经设定数据库安全服务的相关标签策略,则需 按照标签策略规则为数据库安全审计实例添加标签。标签如果 不符合标签策略的规则,则可能会导致数据库安全审计实例创 建失败,请联系组织管理员了解标签策略详情。

步骤7选择"购买时长",如<mark>图2-5</mark>所示。

图 2-5 选择实例购买时长

购买时长											
1个月	2个月	3个月	4个月	5个月	6个月	7个月	8个月	9个月	1年	2年	<mark>20</mark> 3年
🛃 自动续费 🏹	7解 扣费规则 和 续费	时长									

勾选"自动续费"后,当购买的数据库安全审计实例到期时,如果账号余额充足, DBSS将自动为该实例续费,您可以继续使用该实例。自动续费的周期说明如<mark>表2-5</mark>所 示。

表 2-5 自动续费周期说明

购买时长	自动续费周期
1/2/3/4/5/6/7/8/9个月	1个月
1/2/3年	1年

步骤8 确认当前配置无误后,单击"立即购买"。

如果您对价格有疑问,可以单击"了解计费详情",了解产品价格。

- **步骤9** 在"详情"页面,阅读《数据库安服务声明》后,勾选"我已阅读并同意《数据库安全服务声明》",单击"提交"。
- 步骤10 在购买页面,请选择付款方式进行付款。
 - 余额支付
 您可以通过账户的余额进行支付,余额不足时,单击"充值"进行充值。
 - a. 选择"余额支付"。
 - b. 单击"确认付款",完成购买操作。
 - 申请线上合同请款后支付
 - a. 选择"申请线上合同请款后支付",单击"生成合同"。
 - b. 在页面中填写合同信息后,单击"创建正式合同",完成购买操作。
- **步骤11** 成功付款后,在数据库安全审计实例列表界面,可以查看数据库安全审计实例的创建 情况。

----结束

文档版本 01 (2024-11-28)

后续处理

- 当实例的"状态"为"运行中"时,说明实例购买成功。
- 当实例的"状态"为"创建失败"时,系统已自动退款。您可单击"操作"列的 "更多 > 查看详情",在弹出的"创建失败实例"对话框中查看失败原因和删除 失败实例。

2.3 步骤一:添加数据库

数据库安全服务支持对华为云上的RDS关系型数据库、ECS/BMS自建数据库进行审 计。购买数据库安全审计实例后,您需要将待审计的数据库添加至数据库安全审计实 例中。

数据库安全服务支持审计的数据库类型及版本,请参见支持的数据库类型及版本。

前提条件

数据库安全审计实例的状态为"运行中"。

添加数据库

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"数据库列表",进入数据库列表界面。
- 步骤4 在"选择实例"下拉列表框中,选择需要添加数据库的实例。
- 步骤5 在数据库列表框左上方,单击"添加数据库"。

图 2-6 添加数据库

数据库列表	选择实例	DBSS-ba89	~
添加数据	库) (添加安全组规则	

步骤6 在弹出的对话框中,配置数据库的信息。

表 2-6 数据库参数说明

参数名称	说明	取值样例
数据库类别	选择添加的数据库类别,"RDS数据库"或"自建数据库"。 说明 当您选择"RDS数据库"类型时,可以直接选择您需要 添加至数据库安全服务防护的数据库。	自建数据库
数据库名称	您可以自定义添加的数据库的名称。	test1
IP地址	添加的数据库的IP地址。 IP必须为内网IP地址,支持IPv4和IPv6格式。	IPv4: 192.168.1.1 IPv6: fe80:0000:00 00:0000:000 0:0000:0000: 0000

参数名称	说明	取值样例
数据库类型	支持的数据库类型,您可以选择以下类型:	MYSQL
	MYSQL	
	ORACLE	
	PostgreSQL	
	SQLService	
	• DWS	
	GaussDB(for MYSQL)	
	GaussDB	
	• DAMENG	
	KINGBASE	
	MongoDB	
	Hbase	
	SHENTONG	
	• GBase 8a	
	GBase XDM Cluster	
	• Greenplum	
	• HighGo	
	• MariaDB	
	• Hive	
	• DDS	
	• GBase 8s	
	• TDSQL	
	Vastbase	
	• TIDB	
	● ヨ剱 描库 尖空 远择 UKACLE 的, 待申 计 的 应 用 程 序 需 重 启 , 重 新 登 录 数 据 库 。	
	 若需要使用Hive数据库审计MRS集群,需要在服务 端关闭SSL加密功能(具体参考客户端SSL加密功能 使用说明),并且在集群购买页关闭Kerberos认证。 	
端口	添加的数据库的端口。	3306

参数名称	说明	取值样例
数据库版本	支持的数据库版本。	5.0
	 当"数据库类型"选择"MySQL"时,您可以 选择以下版本: 	
	- 5.0、5.1、5.5、5.6、5.7	
	- 8.0(8.0.11及以前的子版本)	
	- 8.0.30	
	- 8.0.35	
	- 8.1.0	
	- 8.2.0	
	- 当"数据库类别"为"RDS数据库"时,自 动关联获取数据库列表,按需选择实例, Agent免安装。	
	● 当"数据库类型"选择"ORACLE"时,您可 以选择以下版本:	
	– 11g	
	– 12c	
	– 19c	
	● 当"数据库类型"选择"PostgreSQL"时,您可以选择以下版本:	
	- 7.4	
	- 8.0、8.1、8.2、8.3、8.4	
	- 9.0、9.1、9.2、9.3、9.4、9.5、9.6	
	- 10.0、10.1、10.2、10.3、10.4、10.5	
	- 11.0	
	- 12.0	
	- 13.0	
	- 14.0	
	● 当"数据库类型"选择"SQLServer"时,您可以选择以下版本:	
	- 2008	
	- 2012	
	- 2014	
	- 2016	
	- 2017	
	 当"数据库类型"选择"DWS"时,您可以选择以下版本: 	
	- 1.5	
	- 8.1	
	 当"数据库类型"选择"GaussDB(for MySQL)"时,您可以选择以下版本: 	

参数名称	说明	取值样例
	- 当"数据库类别"为"自建数据库"时,可 选择"Mysql 8.0"	
	- 当"数据库类别"为"RDS数据库"时,自 动关联获取数据库列表,按需选择实例, Agent免安装。	
	● 当"数据库类型"选择"GaussDB"时,您可 以选择以下版本:	
	- 1.4企业版	
	- 1.3企业版	
	- 2.8企业版	
	- 3.223企业版	
	● 当"数据库类型"选择"DAMENG"时,您可以选择以下版本:	
	– DM8	
	 当"数据库类型"选择"KINGBASE"时,您 可以选择以下版本: 	
	- V8	
	● 当"数据库类型"选择"HBase"时,您可以 选择以下版本:	
	- 1.3.1	
	- 2.2.3	
	 当"数据库类型"选择"SHENTONG"时,您可以选择以下版本: 	
	– v7.0	
	 当"数据库类型"选择"GBase 8a"时,您可 以选择以下版本: 	
	– v8.5	
	● 当"数据库类型"选择"GBase XDM Cluster"时,您可以选择以下版本:	
	– v8.0	
	● 当"数据库类型"选择"GBase 8s"时,您可 以选择以下版本:	
	– v8.8	
	● 当"数据库类型"选择"Greenplum"时,您可以选择以下版本:	
	– v6.0	
	• 当 "数据库类型"选择 "HighGo"时,您可以 选择以下版本:	
	– v6.0	
	• 当"数据库类型"选择"MongoDB"时,您可以选择以下版本:	

参数名称	说明	取值样例
	 − v5.0 ● 当"数据库类型"选择"MariaDB"时,您可以选择以下版本: − 10.6 	
	 当"数据库类型"选择"Hive"时,您可以选择以下版本: 1.2.2 	
	- 2.3.9 - 3.1.2 - 3.1.3	
	 当"数据库类型"选择"TDSQL"时,您可以选择以下版本: 10.3.17.3.0 	
	 当"数据库类型"选择"Vastbase"时,您可以选择以下版本: – G100 V2.2 	
	 当"数据库类型"选择"TiDB"时,您可以选择以下版本: 	
	- V4 - V5 - V6	
	- V7 - V8	
实例名	 您可以指定需要审计的数据库的实例名称。 说明 如果实例名为空,数据库安全审计将审计数据库中所有的实例。 如果填写实例名,数据库安全审计将审计填写的实例,最多可填写5个实例名,目实例名以":"分隔。 	-
选择字符集	 支持的数据库字符集的编码格式,您可以选择以下编码格式: ● UTF-8 ● GBK 	UTF-8
 操作系统	 添加的数据库运行的操作系统,您可以选择以下 操作系统: LINUX64 WINDOWS64 	LINUX64

步骤7 单击"确定",数据库列表中将新增一条"审计状态"为"已关闭"的数据库。

图 2-7 数据库添加完成



🛄 说明

 数据库添加完成后,请您确认添加的数据库信息正确。如果数据库信息不正确,请您在数据 库所在行单击"删除",删除数据库后,再重新添加数据库;

----结束

2.4 步骤二:添加 Agent

将待审计数据库添加至数据库安全审计实例后,您需要根据您在云上实际部署的数据 库选择添加Agent的方式以及在应用端或数据库端安装Agent。Agent程序会获取访问 数据库流量、将流量数据上传到审计系统、接收审计系统配置命令和上报数据库状态 监控数据,帮助您实现对数据库的安全审计。

🛄 说明

目前仅如下几种类型数据库支持免Agent安装。在添加数据库成功后免Agent安装,您可以直接 进行**步骤四:添加安全组规则**。

- GaussDB for MySQL
- RDS for SQLServer
- RDS for MySQL:
 - 5.6 (5.6.51.1及以上版本)
 - 5.7(5.7.29.2及以上版本)
 - 8.0(8.0.20.3及以上版本)
- GaussDB(DWS): 8.2.0.100及以上版本
- PostgreSQL
 - 14(14.4及以上版本)
 - 13(13.6及以上版本)
 - 12(12.10及上版本)
 - 11(11.15及以上版本)
 - 9.6(9.6.24及以上版本)
 - 9.5(9.5.25及以上版本)
- RDS for MariaDB

前提条件

数据库安全审计实例的状态为"运行中"。

常见场景

请您根据数据库类型以及数据库部署场景,为待审计的数据库添加Agent。数据库常见的部署场景说明如下:

• ECS/BMS自建数据库的常见部署场景如图2-8和图2-9所示。



图 2-8 一个应用端连接多个 ECS/BMS 自建数据库

图 2-9 多个应用端连接同一个 ECS/BMS 自建数据库



• RDS关系型数据库的常见部署场景如图2-10和图2-11所示。

图 2-10 一个应用端连接多个 RDS



图 2-11 多个应用端连接同一个 RDS



添加Agent方式的详细说明如<mark>表2-7</mark>所示。

须知

- 当您的应用端和数据库(ECS/BMS自建数据库)都部署在同一个节点上时,Agent 需在数据库端添加。
- 数据库安全审计还支持批量部署流量采集Agent,针对大规模业务场景(容器化部署应用、数据库(RDS关系型数据库)数量大),能够显著提升产品配置的效率,降低配置的复杂度,减少运维人员的日常维护压力。详细操作步骤,请参见容器化部署数据库安全审计Agent。

使用场景	Agent安 装节点	审计功能说明	注意事项
ECS/BMS自 建数据库	数据库端 或应用端	可以审计所有访问该数 据库的应用端的所有访 问记录。	 在数据库端添加Agent。 当某个应用端连接多个 ECS/BMS自建数据库时,所 有连接该应用端的数据库都 需要添加Agent。
RDS关系型 数据库	应用端 (应用端 部署 上)	可以审计该应用端与其 连接的所有数据库的访 问记录。	 在应用端添加Agent。 当某个应用端连接多个RDS 关系型数据库时,所有连接 该应用端的RDS关系型数据 库都需要添加Agent。当其 中一个RDS关系型数据库选 择"创建Agent"后,其余 RDS关系型数据库添加 Agent时,只能选择"选择 已有Agent"添加方式。详 细操作请参见•"添加方 式"选择"选择已有 Agent"。 当多个应用端连接同一个 RDS关系型数据库时,所有 连接该RDS关系型数据库的 应用端都需要添加Agent。
	代理端 (应用端 部署在云 下)	只能审计代理端与后端 数据库之间的访问记 录,无法审计应用端与 后端数据库的访问记 录。	 在应用端添加Agent。 "安装节点IP"需要配置为 代理端的IP地址。

表 2-7 添加 Agent 方式说明

添加 Agent(ECS/BMS 自建数据库)

- **步骤1** 请参见<mark>步骤一</mark>添加数据库。
- 步骤2 登录管理控制台。
- **步骤3** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤4 在左侧导航树中,选择"数据库列表",进入数据库列表界面。
- 步骤5 在"选择实例"下拉列表框中,选择需要添加Agent的数据库所属的实例。
- 步骤6 在添加的数据库所在行的"Agent"列,单击"添加Agent"。

图 2-12 添加 Agent

 Q. 泡得層性活法, 成成入关键字段素 								
	数据库信息 🖯	选择字符集 🖯	PBM2(MES)/MEI ⊖	xns 0	操作系统 ⊖	Bittes 0	Agent	操作
	名称:) 周围: MySOL 版本:5.0	UTF8	3306		LINUX64	0 已共同	董書Agent 汤加Agent	开启教师

步骤7 在弹出的"添加Agent"对话框中,选择添加方式,如<mark>图2-13</mark>所示,相关参数说明如 表2-8所示。

图 2-13 在数据库端添加 Agent

添加Agent

添加方式	○ 选择已有Agent ● 创建Agent
安装节点类型	● 数据库端 ○ 应用端
操作系统	LINUX64_X86 V
CPU阈值(%)	80
内存阈值(%)	80

_				
(取当	-)	确定	
	-90/1HB	2	WEAL	~

表 2-8 添加 Agent 参数说明(ECS/BMS 自建数据库)

参数名称	说明	取值样例
添加方式	您可以选择Agent的添加方式。	创建Agent
	 选择已有Agent 当某个应用端连接了多个数据库时,如果该应 用端的一个数据库已经添加了Agent。其他数 据库在添加Agent时,只需要选择"选择已有 Agent"添加方式。 	
	 创建Agent 如果待添加Agent的数据库需要创建Agent,请 创建新的Agent。 	
数据库名称	可选参数。当"添加方式"选择"选择已有 Agent"时,可以选择实例下已添加Agent的数据 库。	test1
Agent ID	Agent ID 当 "添加方式"选择"选择已有Agent"时,需配 置该参数。	
	您可以选择实例下已添加的Agent ID,Agent ID 由系统自动生成。	
安装节点类型	5点类型 当"添加方式"选择"创建Agent"时,需配置该 参数。	
	审计ECS/BMS自建数据库,可以选择"数据库 端"或"应用端"。	

参数名称	说明	取值样例
安装节点IP	"安装节点类型"选择"应用端"时,需配置该参数。指待审计的应用端节点的IP地址,只能填写一个。	192.168.1.1
	IP地址必须为应用端节点的内网IP地址,支持IPv4 和IPv6格式。	
操作系统	当"添加方式"选择"创建Agent"时,需配置该 参数 。	LINUX64_X8 6
	指待审计的数据库的操作系统,可以选择 "LINUX64_X86""、LINUX64_ARM"或 "WINDOWS64"。	
	说明 根据服务器架构的不同,请根据自身的服务器架构选择 对应的操作系统版本。	
CPU阈值(%)	可选参数。指待审计的应用端节点的CPU阈值,缺 省值为"80"。	80
内存阈值(%)	可选参数。指待审计的应用端节点的内存阈值,缺 省值为"80"。	80

步骤8 单击"确定",Agent添加成功。

步骤9 在成功添加Agent的数据库所在行的"Agent"列,单击"查看Agent"。在下方的 **"Agent列表"**中,查看添加的Agent信息。

图 2-14 Agent 添加完成

								0	
BSERGE O	选择宁约集 🖯	IPHAL(ISR)(REI 0	\$188 O	提作系统 O	WHEE 0	Agent	提作		
名称: sqlservr ● 開墾: SQLServer 航年: 2017	UTF8	10.0.207.105 1433	-	LINUX64	0 已开启	度置Agent 活动Agen	n 958 1009		
単築数: 1								10 V <	1 >
그분명: sqiservr									
그문원: sqiserv gent왕동									
B週時: sqbenr 									
3ලා5: sqtemr •gen955 ○ යමමාතයා, කික∂.⊁මාරක AgenD ⊕ ඉතාතයක ⊕ ඉතා	top ⊖ Nature ⊖	#11時FZ錄 Ө	CPUIRME(%) 0	Pifriddl(%) 0	3000 O	1867 1 12 0	SHA25HQIDII @	服作	0

🛄 说明

Agent添加完成后,请您确认添加的Agent信息正确。如果Agent添加不正确,请您在Agent所在 行单击"删除",删除Agent后,再重新添加Agent。

----结束

添加 Agent (RDS 关系型数据库)

当某个应用端连接了多个RDS系型数据库时, 请按以下方式添加Agent:

- 连接该应用端所有的RDS系型数据库都需要添加Agent。
- 如果连接该应用端的某个数据库已在应用端添加了Agent。其他数据库在添加 Agent时,只能选择"选择已有Agent"添加方式。

- **步骤1** 请参见<mark>步骤一</mark>添加数据库。
- 步骤2 登录管理控制台。
- **步骤3** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤4 在左侧导航树中,选择"数据库列表",进入数据库列表界面。
- 步骤5 在"选择实例"下拉列表框中,选择需要添加Agent的数据库所属的实例。
- 步骤6 在添加的数据库所在行的"Agent"列,单击"添加Agent"。

图 2-15 添加 Agent



- **步骤7** 在弹出的"添加Agent"对话框中,选择添加方式,如<mark>图2-16和图2-17</mark>所示,相关参数说明如<mark>表2-9</mark>所示。
 - "添加方式"选择"选择已有Agent" 在什么场景下需要选择"选择已有Agent"添加方式的详细介绍,请参见<mark>在什么场</mark> 景下需要选择"选择已有Agent"添加方式?。

🛄 说明

选择"选择已有Agent"添加方式,如果您已在应用端安装了Agent,该数据库添加Agent 后,数据库安全审计即可对该数据库进行审计。

图 2-16 选择已有 Agent

添加Agent

添加方式	● 选择已有Agent ○ 创建Agent		
数据库名称	gauss-6966-dbss-2	•	
★ Agent ID	~	•	
CPU阈值(%)			
内存阈值(%)			
			取消 确定

"添加方式"选择"创建Agent"

如果待添加Agent的数据库需要创建Agent,请创建新的Agent。

"安装节点类型"选择"应用端","安装节点IP"输入应用端内网IP地址。

图 2-17 在应用端添加 Agent

添加Agent

添加方式	◯ 选择已有Agent 💿 创建Age	ent		
安装节点类型	◯ 数据库端 (●) 应用端			
★ 安装节点IP		审计网卡名称		
CPU阈值(%)	80	内存阈值(%)	80	
操作系统	LINUX64_X86 V			
				取消 确

表 2-9 添加 Agent 参数说明 (RDS 关系型数据库)

参数名称	说明	取值样例
添加方式	您可以选择Agent的添加方式。	创建Agent
	 选择已有Agent 当某个应用端连接了多个数据库时,如果该应 用端的一个数据库已经在应用端添加了 Agent。其他数据库在添加Agent时,只能选择 "选择已有Agent"添加方式。 	
	 创建Agent 如果待添加Agent的数据库需要创建Agent,请 创建新的Agent。 	
数据库名称	可选参数。当"添加方式"选择"选择已有 Agent"时,可以选择实例下已添加Agent的数据 库。	tesT
Agent ID	当"添加方式"选择"选择已有Agent"时,需配 置该参数。	-
	您可以选择实例下已添加的Agent ID,Agent ID 由系统自动生成。	
安装节点类型	当"添加方式"选择"创建Agent"时,需配置该 参数。	应用端
	审计RDS关系型数据库,只能选择"应用端"。	
安装节点IP	当"安装节点类型"选择"应用端"时,需配置该 参数。指待审计的应用端节点的IP地址,只能填写 一个。	192.168.1.1
	IP地址必须为应用端节点的内网IP地址,支持IPv4 和IPv6格式。	
	须知 当审计RDS关系型数据库且应用端在云下时,代理端将 作为应用端,此时,"安装节点IP"需要配置为代理端 的IP地址。	

参数名称	说明	取值样例
审计网卡名称	可选参数。"安装节点类型"选择"应用端"时, 可以配置该参数。	-
	指侍甲订的应用端节点的网卡名称。 	
CPU阈值(%)	可选参数。"安装节点类型"选择"应用端"时, 可以配置该参数。	80
	指待审计的应用端节点的CPU阈值,缺省值为 "80"。	
	须知 当服务器的CPU超过设置的阈值,为了保证您业务的正 常运行,Agent将自动关闭,停止运行。	
内存阈值(%)	可选参数。 "安装节点类型" 选择 "应用端"时, 可以配置该参数。	80
	指待审计的应用端节点的内存阈值,缺省值为 "80"。	
	须知 当服务器上的内存超过设置的阈值,为了保证您业务的 正常运行,Agent将自动关闭,停止运行。	
操作系统	可选参数。 "安装节点类型" 选择 "应用端" 时, 可以配置该参数。	" LINUX64_ X86 "
	指待审计的应用端节点的操作系统,可以选择 "LINUX64_X86"、"LINUX64_ARM" "WINDOWS64"。	

- **步骤8** 单击"确定",Agent添加成功。
- **步骤9** 在成功添加Agent的数据库所在行的"Agent"列,单击"查看Agent"。在下方的 **"Agent列表"**中,查看添加的Agent信息。

图 2-18 Agent 添加完成

Q 选择履性筛选, 板榆入关键字接索								08
Barrenne O	选择学初集 0	IPHALOSISIAN 0	RNS 0	操作系统 0	WHERE 0	Agent	指作	
名行: sqiservr ● 開墾: SQLServer 航本: 2017	UTF8	10.0.207.105 1433	-	LINUX64	o Effe	度要Agent 活动Agenr	950 BBR	
急祭政: 1							10 V	< 1 >
DIERS: solvery								~
Logie sport								
Afterioste								
〇、这样履行知识、成成入关键字指索								Q
AgentID 0 安装节点開 0 安装节点目 0	操作系统 ⊖	审计同卡名称 0	CPU8818(%) 0	P4528820(%) 0	調用 ⊖	isitika o	SHA2568的語 0 開作	
xHEBpMB5_rlg78 应用3A 10.0.170.10	LINUX64_X86	-	80	80	8	🕒 (#201)	c64679581e0ed9a TR	agent 353 BBR

🛄 说明

Agent添加完成后,请您确认添加的Agent信息正确。如果Agent添加不正确,请您在Agent所在 行单击"删除",删除Agent后,再重新添加Agent。

----结束

后续处理

Agent添加完成后,您还需要为数据库安全审计实例所在的安全组添加入方向规则TCP 协议(8000端口)和UDP协议(7000-7100端口),使Agent与审计实例之间的网络 连通,数据库安全审计才能对添加的数据库进行审计。有关添加安全组规则的详细操 作,请参见添加安全组规则。

2.5 步骤三:下载并安装 Agent

2.5.1 下载 Agent

Agent添加完成后,您还需要下载Agent,并根据Agent的添加方式在数据库端或应用 端安装Agent。

🛄 说明

每个Agent都有唯一的Agent ID,是Agent连接数据库安全审计实例的重要密钥。若您将添加的 Agent删除,在重新添加Agent后,请重新下载Agent。

前提条件

数据库安全审计实例的状态为"运行中"。

操作步骤

- 步骤1 请参见步骤二添加Agent。
- 步骤2 登录管理控制台。
- **步骤3** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤4 在左侧导航树中,选择"数据库列表",进入数据库列表界面。
- 步骤5 在"选择实例"下拉列表框中,选择需要下载Agent的数据库所属的实例。
- **步骤6** 在数据库所在行的"Agent"列,单击"查看Agent"。在下方的**"Agent列表"**中 Agent所在行的"操作"列,单击"下载agent",将Agent安装包下载到本地。

图 2-19 下载 Agent

Internation

AUDACHARA AUDICALANDICI							
〇、送採服性採送、或能入关键字规束							Q
BRACK O	选择字符集 ⊖	Pibli(B83)SBD 0	案例名 ⊖	iiifraafa O	witten 0	Agent	操作
名称: ● 與型: MySQL 版本: 5.0	UTF8	3306	-	LINL0084	0 已失闭	查看Agent 活动Agent	开展 動除
名称:	UTF8	3306	rds-1ae5	LINUX84	o BHB	无测荡加agent	关闭 動除
名称: 	UTF8	3306	-	LINU0064	• B#R	查查Agent 添加Agent	*X1 800
9552 3							10 🗸 <
已选择: qct-test-mysql			-				
Agent3128							
〇、运得届性消活、或能入关键字搜索							
AgentiD 🖯 安装节点笑型 🖯	SETTOP 0 STATE	审计局卡名称 ⊖	CPUMB(5) 0	内标题图(%) Θ	#用 ⊖ 161	SHA25HQBME 0	操作
aR27ipl8gEsPOeb 数据库纳	LINUX64_X05	-	80	80	8 😣	休眠中 db01513dd12a3561.	下就agent 开启 删除

请根据安装Agent节点的操作系统类型,选择下载相应的Agent安装包。
- Linux操作系统
 在"操作系统"为"LINUX64"的数据库中下载Agent安装包
- Windows操作系统
 在"操作系统"为"WINDOWS64"的数据库中下载Agent安装包

----结束

2.5.2 安装 Agent (Linux 操作系统)

安装Agent后,您才能开启数据库安全审计。通过本节介绍,您将了解如何在Linux操 作系统的节点上安装Agent。Windows操作系统的Agent安装请参见<mark>安装Agent</mark> (Windows操作系统)。

前提条件

 安装Agent节点的运行系统满足Linux系统版本要求。有关Linux系统版本的要求, 请参见Agent可以安装在哪些Linux操作系统上?

常见安装场景

请您根据数据库的类型以及部署场景,在数据库端或应用端安装Agent。数据库常见的 部署场景说明如下:

ECS/BMS自建数据库的常见部署场景如图2-20和图2-21所示。



图 2-20 一个应用端连接多个 ECS/BMS 自建数据库



图 2-21 多个应用端连接同一个 ECS/BMS 自建数据库

- RDS关系型数据库的常见部署场景如图2-22和图2-23所示。
 - 图 2-22 一个应用端连接多个 RDS



图 2-23 多个应用端连接同一个 RDS



安装Agent节点的详细说明如表2-10所示。

须知

当您的应用和数据库(ECS/BMS自建数据库)都部署在同一个节点上时,Agent需在 数据库端安装。

表 2-10 安装 Agent 场景说明

使用场景	Agent安 装节点	审计功能说明	注意事项
ECS/BMS自 建数据库	数据库端	可以审计所有访问该数 据库的应用端的所有访 问记录。	 在数据库端安装Agent。 当某个应用端连接多个 ECS/BMS自建数据库时, 需要在所有连接该应用端的 数据库端安装Agent。
RDS关系型 数据库	应用端 (应用端 部署在云 上)	可以审计该应用端与其 连接的所有数据库的访 问记录。	 在应用端安装Agent。 当多个应用端连接同一个 RDS时,所有连接该RDS的 应用端都需要安装Agent。
RDS关系型 数据库	代理端 (应用端 部署在云 下)	只能审计代理端与后端 数据库之间的访问记 录,无法审计应用端与 后端数据库的访问记 录。	在代理端安装Agent。

安装 Agent

🛄 说明

在您安装新版Agent的时候,需要您为当前安装的Agent自定义一个密码。

请您根据数据库类型以及数据库的部署环境,在相应节点上安装Agent。

- 步骤1 请参见步骤二添加Agent。
- 步骤2 请参见下载Agent获取Linux操作系统Agent安装包。
- **步骤3** 将下载的Agent安装包"xxx.tar.gz"上传到待安装Agent的节点(例如使用WinSCP工具)。
- 步骤4 使用跨平台远程访问工具(例如PuTTY)以root用户通过SSH方式,登录该节点。
- 步骤5 执行以下命令,进入Agent安装包"xxx.tar.gz"所在目录。

cd Agent安装包所在目录



步骤6 执行以下命令, 解压缩 "xxx.tar.gz" 安装包。

tar -xvf xxx.tar.gz

[root@ecs-test agent]# [root@ecs-test agent]# tar -xvf ____9syBZIsBbeAhEFqE_hhD.tar.gz

步骤7 执行以下命令,进入解压后的目录。

cd 解压后的目录

[root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]# chmod +x install.sh
[root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test 192.168.0.107 ⁻ 9syBZIsBbeAhEFqE ⁻ hhD]# ll
total 36
drwxr-xr-x 2 root root 4096 Oct 25 09:50 bin
drwxr-xr-x 2 root root 4096 Oct 25 09:50 boot
drwxr-xr-x 2 root root 4096 Oct 25 09:50 cert
drwxr-xr-x 2 root root 4096 Oct 25 09:50 conf
drwxr-xr-x 2 root root 4096 Oct 25 09:50 crond
-rwxr-xr-x 1 root root 527 Oct 25 09:45 install.sh
drwxr-xr-x 2 root root 4096 Oct 25 09:50 lib
-rw-rr 1 root root 308 Oct 25 09:45 uninstall.sh
drwxr-xr-x 2 root root 4096 Oct 25 09:50 utils
[root@ecs-test9syBZIsBbeAhEFqE_hhD]#

步骤8 执行以下命令,查看是否有安装脚本"install.sh"的执行权限。

แ

- 如果有安装脚本的执行权限,请执行步骤9。
- 如果没有安装脚本的执行权限,请执行以下操作:
 - a. 执行以下命令,添加安装脚本执行权限。 chmod +x install.sh
 - b. 确认有安装脚本执行权限后,请执行<mark>步骤9</mark>。

步骤9 执行以下命令,安装Agent。

sh install.sh

文档版本 01 (2024-11-28)

[root@ecs-test [root@ecs-test	_9syBZIsBbeAhEFqE_hhD]# _9syBZIsBbeAhEFqE_hhD]# sh install.sh
check system bit.	
check system bit success!	
exist system-release file	
Linux version is CentOS 7	
dbss user not exists, create	dbss user now. Please set user password!
Enter password :	

门 说明

- 用户系统是Ubantu时,执行以下命令安装Agent: **bash install.sh**
- Agent程序是以DBSS普通用户运行的,在首次安装Agent时,需要创建Agent用户,执行sh install.sh命令后,需要您自行设置DBSS用户的密码。

界面回显以下信息,说明安装成功。否则,说明Agent安装失败。 start agent starting audit agent audit agent started start success install dbss audit agent done!

须知

如果Agent安装失败,请您确认安装节点的运行系统是否满足Linux操作系统要求,并 重新安装Agent。

步骤10 执行以下命令,查看Agent程序的运行状态。

service audit_agent status

如果界面回显以下信息,说明Agent程序运行正常。

[root@ecs-test		9syBZIsBbeAhEFqE_hhD]#			
audit agent is	runnina.	_95 YBZISBDEANEFQE_NND]#	service	audit_agent	status
[root@ecs-test		9syBZIsBbeAhEFgE hhD]#			

audit agent is running.

----结束

相关操作

- 数据库开启SSL时,将不能使用数据库安全审计功能。如果您需要使用数据库安全 审计功能,请关闭数据库的SSL。关闭数据库SSL的详细操作,请参见如何关闭数 据库SSL?。
- 有关添加Agent的详细操作,请参见<mark>步骤二:添加Agent</mark>。
- 有关卸载Agent的详细操作,请参见<mark>卸载Agent</mark>。

2.5.3 安装 Agent (Windows 操作系统)

安装Agent后,您才能开启数据库安全审计。通过本节介绍,您将了解如何在 Windows操作系统的节点上安装Agent。Linux操作系统的Agent安装请参见<mark>安装</mark> Agent(Linux操作系统)。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 安装Agent节点的运行系统满足Windows系统版本要求。有关Windows系统版本 的要求,请参见Agent可以安装在哪些Windows操作系统上?。

常见安装场景

请您根据数据库的类型以及部署场景,在数据库端或应用端安装Agent。数据库常见的 部署场景说明如下:

• ECS/BMS自建数据库的常见部署场景如图2-24和图2-25所示。



图 2-24 一个应用端连接多个 ECS/BMS 自建数据库

图 2-25 多个应用端连接同一个 ECS/BMS 自建数据库



RDS关系型数据库的常见部署场景如图2-26和图2-27所示。

图 2-26 一个应用端连接多个 RDS



图 2-27 多个应用端连接同一个 RDS



安装Agent节点的详细说明如表2-11所示。

须知

当您的应用端和数据库(ECS/BMS自建数据库)都部署在同一个节点上时,Agent需 在数据库端安装。

表 2-11 安装 Agent 场景说明

使用场景	Agent安 装节点	审计功能说明	注意事项
ECS/BMS自 建数据库	数据库端	可以审计所有访问该数 据库的应用端的所有访 问记录。	 在数据库端安装Agent。 当某个应用端连接多个 ECS/BMS自建数据库时, 需要在所有连接该应用端的 数据库端安装Agent。
RDS关系型 数据库	应用端 (应用端 部署在云 上)	可以审计该应用端与其 连接的所有数据库的访 问记录。	 在应用端安装Agent。 当多个应用端连接同一个 RDS时,所有连接该RDS的 应用端都需要安装Agent。
RDS关系型 数据库	代理端 (应用端 部署在云 下)	只能审计代理端与后端 数据库之间的访问记 录,无法审计应用端与 后端数据库的访问记 录。	在代理端安装Agent。

安装 Agent

步骤1 请参见步骤二添加Agent。

步骤2 在Windows主机安装 "Npcap" 软件。

- 如果该Windows主机已安装"Npcap",请执行步骤4。
- 如果该Windows主机未安装"Npcap",请执行以下步骤:
 - a. 请前往https://nmap.org/npcap/下载Npcap最新软件安装包。

图 2-28 下载 npcap

Downloading and Installing Npcap Free Edition

The free version of Npcap may be used (but not externally redistributed) on up to 5 systems (free license details). It may also be used on uplimited systems where it is only used with Nmap and/or Wireshark. Simply run the executable installer. Th 单击版本进行下载 ch release is available, and developers can build their apps against the SDK. The improvements for each release are documented in the Npcap Changelog.

- Npcap 0.9994 installer for Windows 7/2008R2, 8/2012, 8.1/2012R2, 10/2016, 2019 (x86 and x64).
- Npcap SDK 1.05 (ZIP).
- Npcap 0.9994 debug symbols (ZIP).
 Npcap 0.9994 source code (ZIP).

The latest development source is in our Github source repository. Windows XP and earlier are not supported; you can use WinPcap for these versions.

- b. 将下载好的npcap-xxxx.exe软件安装包上传至需要安装agent的虚拟机。
- c. 双击npcap软件安装包。
- d. 在弹出的对话框中,单击"I Agree",如图2-29所示。

图 2-29 同意安装 "Npcap"

6	Npcap 0.99 <mark>84</mark> Setup	L		x
NMAP. ORG	License Agreement Please review the license terms be	efore installing N	lpcap 0.998	34.
Press Page Down to see th	e rest of the agreement.			
 NPCAP COPYRIGHT / END	USER LICENSE AGREEMENT			^
Npcap is a Windows packe (c) 2013-2019 by Insecure reserved.	t sniffing driver and library and is cop e.Com LLC ("The Nmap Project"). All I	oyright rights		
Even though Npcap source not open source software permission from the Nmap limited to installation on fiv	e code is publicly available for review, and may not be redistributed withou Project. The standard version is also re systems. We fund the Npcap proje	, it is t special o ect by		~
If you accept the terms of agreement to install Npcap	the agreement, click I Agree to conti 0.9984.	nue. You must a	accept the	
Nullsoft Install System v2.51 -				
	[I <u>A</u> gree	Cano	el

e. 在弹出的对话框中,单击"Install",不勾选安装选项,如<mark>图</mark>2-30所示。

6	Npcap 0.99 <mark>84</mark> Setup	_ □
NMAP. ORG	Installation Options Please review the following options before ir 0.9984	nstalling Npcap
Legacy loopback sup	oport for Nmap 7.80 and older. Not needed for	Wireshark.
Restrict Npcap drive	r's access to Administrators only	
Support raw 802.11	traffic (and monitor mode) for wireless adapter	rs
🗌 Install Npcap in Winl	Pcap API-compatible Mode	

图 2-30 安装 "Npcap"

在弹出的对话框中,单击"Next"。 f.

Nullsoft Install System v2.51 —

< Back

Install

Cancel

X

0	Npcap 0.99 <mark>84</mark> Setup	_ 🗆 X
NMAP. ORG	Installation Complete Setup was completed successfully.	
Completed		
Show details		
Nullsoft Install System v2,51 -		
	< Back I	Vext > Cancel

g. 单击"Finish",完成安装。

6	Npcap 0.9984 Setup 📃 🗖 🗙
NMAP.ORG	Finished Thank you for installing Npcap
Npcap has been installe	ed on your computer.
Click Finish to close this	; wizard.
Nullsoft Install System v2.51	< Back Finish Cancel

步骤3 请参见下载Agent获取Windows操作系统Agent安装包。

步骤4 以"Administrator"用户登录到Windows主机,将下载的Agent安装包"xxx.zip"复制到该主机任意一个目录下。

图 2-31 Agent 安装包

F:\agent					
	^	名称	^	修改日期	类型
	I.	4	_wK2kQJIBgZ2XJBFwbi-O.zip		WinRAR ZIP arch

步骤5 进入Agent安装包所在目录,并解压缩安装包。

步骤6 进入解压后的文件夹,双击"install.bat"执行文件。

图 2-32 双击 install.bat

📙 bin	文件夹
📙 conf	文件夹
📙 log	文件夹
script	文件夹
💿 install.bat	Windows 批处理 4 KB
🚳 uninstall.bat	Windows 批处理 2 KB

步骤7 安装成功,界面如图2-33所示,按任意键结束安装。

图 2-33 Agent 安装成功

DBSS Servcie Audit Agent Install

install DBSS audit agent start
check npcap existed success
check main process file success
check child process file success
check dll file success
check dll file success
check startup file success
已复制
已复制 1 个文件。
已复制 1 个文件。
check dbss agent config file success
check log folder success
install DBSS audit agent success
start DBSS audit agent success 吉按任音键继续

步骤8 安装完成后,在Windows任务管理器中查看"dbss_audit_agent"进程,如下图<mark>8</mark> 2-34所示。

图 2-34 查看 dbss_audit_agent 进程

R	👰 任务管理器								-		×	
文件	ŧ(E) 选	项(<u>O)</u> 查看(<u>V</u>)										
进税	2 性能	应用历史记录	启动	用户	详细信息	服务						
		^						25%	76%	2%	0	%
名利	R				状态			CPU	内存	磁盘	Þ	络
	🔳 dae	monProcess.ex	xe (32	(立)				0%	0.4 MB	0 MB/秒	0 Mb	ps '
	🔳 dbs	s_audit_agent.	exe (32	2位)				0%	1.7 MB	0.1 MB/秒	0 Mb	ps

如果进程不存在,说明Agent安装失败,请尝试重新安装Agent。

----结束

相关操作

- 有关添加Agent的详细操作,请参见<mark>步骤二:添加Agent</mark>。
- ▶ 有关卸载Agent的详细操作,请参见<mark>卸载Agent</mark>。
- 数据库开启SSL时,将不能使用数据库安全审计功能。如果您需要使用数据库安全 审计功能,请关闭数据库的SSL。关闭数据库SSL的详细操作,请参见如何关闭数 据库SSL?。

2.6 步骤四:添加安全组规则

Agent添加完成后,您需要为数据库安全审计实例所在的安全组添加入方向规则TCP协议(8000端口)和UDP协议(7000-7100端口),使Agent与审计实例之间的网络连通,数据库安全审计实例才能对添加的数据库进行审计。

本章节介绍如何为数据库安全审计实例所在的安全组添加TCP协议(8000端口)和 UDP协议(7000-7100端口)。

🗀 说明

安全组规则也可以在安装Agent前进行添加。

前提条件

数据库安全审计实例的状态为"运行中"。

添加安全组规则

- 步骤1 请参见步骤二添加Agent。
- 步骤2 登录管理控制台。
- **步骤3** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤4 在左侧导航树中,选择"数据库列表",进入"数据库列表"界面。
- 步骤5 在"选择实例"下拉列表框中,选择需要添加安全组规则的数据库所属的实例。
- 步骤6 记录Agent安装节点IP信息。

在数据库所在行的"Agent"列,单击"查看Agent"。在下方的**"Agent列表"**中,记录**"安装节点IP"**。

取消)

前往处理

图 2-35 安装节点 IP

液10起爆车 液10安全组织则							
〇、送择履性筛选、或输入关键字搜索							
Reade 0	选择字符集 ⊖	PB4L(MS)/ACL ↔	ana 0	INTER O	审计状态 ⊖	Agent	操作
名称: ● 規型: MySQL 版本: 5.0	UTF8	3306	-	LINU064	0 日前初	查看Apent 汤加Agent	开展 動物
名称: 一 規型: MySQL 版本: 8.0	UTF8	3306	rds-1ae5	LINU064	• B##	无能准tBagent	光灯 動除
8行 尚哉: MySQL 成本: 8.0	UTF8	3306		LINUX64	0 己开宫	意题Agent 活动Agent	关闭 動除
USR: 3							10 🗸
譯: qct-test-mysql							
n例表							
这得是性简洁、或输入关键字搜索							
 ● 量素性性接定 ● Gitneg 	安装节/80P ⊖ 操作系统 ⊖	#H日卡名称 0	CPUMMI(%) 0	内部间面(%) 0	調用 ⊖ 日間	if58826 0 SHA25688888 0	提作

步骤7 在数据库列表的上方,单击"添加安全组规则"。

步骤8 在弹出的弹框中,记录数据库安全审计实例的"安全组名称"(例如default),如图 2-36所示。

图 2-36 添加安全组规则

添加安全组规则

请在审计实例所在的安全组中开启必要规则,确保网络通信正常。

安全组名称	default
操作详情	1) 点击前往处理 2) 搜索当前安全组名称,打开 3) 点击入方向规则,并点击添加规则 4) 协议端口选择TCP协议8000端口和UDP协议7000-7100端口 5) 两种端口分别在源地址添加Agent节点IP,提交 详细教程

- 步骤9 单击"前往处理",进入"安全组"列表界面。
- **步骤10** 在列表上方的搜索框中选择属性筛选,或输入关键字搜索,搜索指定的安全组。单击 安全组名称。

图 2-37 安全组

全組 ①						2 使用编辑
						x)(
(1) 名称10 0	安全/15元11 0	关脱索例	雑雄 ⊖	CERTIFIC O	金織項目 0	操作
dws-teet33-0000 007e5cf5-1bc7-4b03-bdbe-77ed96ca46c0	34	143	4c035747-177b-4c66-b23b-cb3a2b9	2023/06/26 16:19:23 GMT+08:00	default	配置规则 管理实例 更多 ~

步骤11 选择"入方向规则",检查安全组的入方向规则。

请检查该安全组的入方向规则是否已为安装节点IP配置了TCP协议(端口为8000)和UDP协议(端口为7000-7100)规则。

- 如果该安全组已配置安装节点的入方向规则,请执行开启数据库安全审计。
- 如果该安全组未配置安装节点的入方向规则,请执行20。

步骤12 为安装节点添加入方向安全规则。

1. 在入方向规则页面,单击"添加规则"。

图 2-38 添加规则

基本伯	言息	入方向规则	出方向规则	关联实例	标签			
	0 安	全组规则对不同规格;	云服务器的生效情况不	5同,为了避免您的	的安全组规则不生效,	请您添加规则	前,单击此处了解详情。	
	添加	2011 (快速液			な通常用端口) /	、方向规则: 14	查看安全组配置示例(3

 在"添加入方向规则"对话框中,添加TCP协议(端口为8000)和UDP协议(端 口为7000-7100)规则。

🛄 说明

源地址可以是单个IP地址、IP地址段或安全组:

- 单个IP地址:例如192.168.10.10/32。
- IP地址段:例如192.168.52.0/24。
- 所有IP地址: 0.0.0.0/0。
- 安全组:例如sg-abc。

图 2-39 "添加入方向规则"对话框

添加入力问规	火」 教我设置					
 安全组规则双 当源地址选择 	付不同规格云服务器 ₽IP地址时,您可以≀	的生效情况不同,为了 在一个框内同时输入或	避免您的安全组规则不生效,请您添 着粘贴多个IP地址,不同IP地址以","	加规则前,单击 <mark>此处了</mark> 解详情。 隔开。一个IP地址生成一条安全组规则,		
安全组						
如您要添加多条规则 优先级 ⑦	,建议単击 与入规 策略 ⑦	则 以进行批量导入。 类型	协议端口 ⑦	源地址 ⑦	描述	操作
1-100	 	IPv4 v	基本协议/自定义TCP ∨ 8000	IP地址 > 192. ×		复制 劃除
1-100	(分)	IPv4 v	基本协议 / 自定义UDP v 7000-7100	IP地社 > 192. ×		复制 删除
			⊕ 増加1条規	171	(取消 補定

3. 单击"确定",完成添加入方向规则。

----结束

2.7 步骤五:开启数据库安全审计

数据库安全审计默认提供一条"全审计规则"的审计范围,可以对成功连接数据库安 全审计实例的所有数据库进行安全审计。开启数据库安全审计后,您可以查看被添加 的数据库的审计结果。详细操作,请参见<mark>查看审计结果</mark>。

前提条件

安装Agent的状态为"正在运行"。

开启审计

步骤1 请参见步骤三安装Agent。

步骤2 请参见<mark>步骤四</mark>添加安全组规则。

文档版本 01 (2024-11-28)

步骤3 登录管理控制台。

- **步骤4** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤5 在左侧导航栏中,选择"数据库列表",进入"数据库列表"界面。
- 步骤6 在选择实例下拉框中,选择需要开启审计的数据库安全审计实例。
- 步骤7 在待开启审计所在行的"操作"列,单击"开启",开启审计功能。

审计功能开启后,该数据库的"审计状态"为"已开启",不需要重启数据库。

图 2-40 开启数据库审计功能

100012015 THEOREM							
〇、送择届性等选,或输入关键字搜索							
MERGE O	选择字符集 ⊖	IP地址(经名)38日 0	SHE 0	操作派统 ⊖	审计状态 ⊖	Agent	提作
 (本物: ● 過型: MySQL 版本: 5.0 	UTF8	3306		LINUX54	0 已关闭	查看Apent 添加Apent	开启教师

----结束

验证审计效果

- 步骤1 开启审计后,在数据库上执行一条SQL语句(例如"show databases")。
- 步骤2 登录管理控制台。
- **步骤3** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- **步骤4** 在左侧导航栏选择"数据报表",进入"数据报表"页面。
- 步骤5 在"选择实例"下拉列表框中,选择需要验证的数据库所属的实例。
- 步骤6选择"语句"页签。
- **步骤7** 在列表上方选择时间"**全部时间"、"近30分钟"、"近1小时"、"今日"、"近7 天"、"近30天"**或自定义时间段,SQL语句列表将显示**步骤1**中输入的SQL语句。

图 2-41 查看 SQL 语句



 如果SQL语句列表中未显示输入的SQL语句,说明Agent与数据库安全审计实例之 间网络通信异常,请参照如何处理Agent与数据库安全审计实例之间通信异常? 处理。

----结束

3 开通并使用数据库安全审计(免安装 Agent)

3.1 流程指引

背景信息

数据库安全审计支持对华为云上的ECS/BMS自建数据库和RDS关系型数据库进行审计。

须知

- 数据库安全审计不支持跨区域(Region)使用。待审计的数据库必须和购买申请的数据库安全审计实例在同一区域。
- 有关审计数据的保存说明,请参见数据库安全审计的审计数据可以保存多久?。

免 Agent 方式审计数据库

部分数据库类型及版本支持免安装Agent方式,如<mark>表3-1</mark>所示。

表 3-1	支持免 Agent 安装的关系	系型数据库
-------	-----------------	-------

数据库类型	支持的版本
GaussDB for MySQL	默认都支持
RDS for SQLServer (华为云审计实例:23.02.27.182148 及其之后 的版本支持)	默认都支持

数据库类型	支持的版本
RDS for MySQL	• 5.6 (5.6.51.1及以上版本)
	• 5.7(5.7.29.2及以上版本)
	• 8.0(8.0.20.3及以上版本)
GaussDB(DWS)	• 8.2.0.100及以上版本
PostgreSQL	• 14(14.4及以上版本)
(华为云审计实例: 23.04.17.123301 及其之后	• 13(13.6及以上版本)
的版本支持)	• 12(12.10及上版本)
ジルオ 当SQL语句大小超过4KB审计时会被截断,会导致审	• 11(11.15及以上版本)
计到的SQL语句不完整。	• 9.6(9.6.24及以上版本)
	• 9.5(9.5.25及以上版本)
RDS for MariaDB	默认都支持

🛄 说明

- 免安装Agent模式配置简单、易操作,但较之安装了Agent的DBSS实例,支持的功能上存在如下差异:
 - 统计会话数量时,无法统计成功登录、与失败登录的会话个数。
 - 无法获取数据库访问时客户端的端口号。
- 由于GaussDB(DWS)服务具有日志审计开关的权限控制策略,只有华为云账号或拥有 Security Administrator权限的用户才能开启或者关闭DWS数据库审计开关。
- GaussDB默认不开启ddl,用户需要参照GaussDB用户手册操作开启如下配置:
 - audit_system_object = 130023423, 操作请参考: GaussDB开发指南。
 - datastyle=ISO,YMD,保证日期格式为yyyy-MM-dd HH:mm:ss+Z。

图 3-1 免 Agent 安装流程



表 3-2 快速使用数据库安全审计操作步骤

步骤	配置操作	说明
1	添加数据库	购买数据库安全服务后,您需要将待审计的数据 库添加到数据库安全审计实例。
2	开启数据库安全审计	您需要开启数据库安全审计功能,将添加的数据 库连接到数据库安全审计实例,才能使用数据库 安全审计功能。
3	查看审计结果	数据库安全审计默认提供一条"全审计规则"的 审计范围,可以对连接数据库安全审计实例的所 有数据库进行审计。开启数据库安全审计后,您 可以在数据库安全审计界面查看被添加的数据库 的审计结果。
		须知 您可以根据业务需求设置数据库审计规则。有关配置 审计规则的详细操作,请参见 <mark>配置审计规则</mark> 。

3.2 购买数据库安全服务

本章节介绍如何购买数据库安全服务。数据库安全服务提供包年/包月计费方式。

约束与限制

- 数据库安全服务不支持跨区域(Region)使用。待审计的数据库必须和购买的数 据库安全审计实例在同一区域。
- 购买数据库安全审计实例配置VPC参数,必须与Agent安装节点(应用端或数据库端)所在的VPC保持一致。否则,将导致Agent与审计实例之间的网络不通,无法使用数据库安全审计。
 数据库安全审计的Agent安装节点,请参见:如何选择数据库安全审计的Agent安装节点?。

系统影响

数据库安全服务为旁路模式审计,不影响用户业务,与本地审计工具不冲突。

前提条件

请参见DBSS权限管理确认实例账号具有相关权限。

须知

请确认购买实例的账号具有"DBSS System Administrator"、"VPC Administrator"、"ECS Administrator"和"DBSS Administrator"角色。

- VPC Administrator:对虚拟私有云的所有执行权限。项目级角色,在同项目中勾选。
- DBSS Administrator: 对账号中心、费用中心、资源中心中的所有菜单项执行任意 操作。项目级角色,在同项目中勾选。
- ECS Administrator:对弹性云服务器的所有执行权限。项目级角色,在同项目中勾选。

操作步骤

- 步骤1 登录管理控制台。
- 步骤2 进入数据库安全审计购买页面。
- **步骤3** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤4 在界面右上角,单击"购买数据库安全服务"。
- 步骤5选择"区域"、"可用区类型"、"可用区"和"性能规格"。

图 3-2 选择可用区和版本规格

E% ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・								
सम्बद्ध सन्दर्भ रस्रिहा संसहर सम्रह								
版本現樁								
		•	e					
入门版 最多支持1个数据库实例	基础版 最多支持3个数据库实例	专业版 最多支持6个数据库实例	高级版 最多支持30个数据库实例					
若吐量除值 1000第/秒	各社里編集 3000条/秒	新社議論後 6000第/秒	香吐量蜂值 30000条/秒					
入库遗率 120万余/小时 在球SQL语句符翰	入库速率 360万条/小时 在该SQL语句存储	入库遗率 720万条/小树 在线SQL酒句符储	入库速率 1080万条/小时 在线SQL语句存储					
1亿象 ¥1,000.00 /月	4亿余 ¥3,000.00 /河	6亿余 ¥6,000.00 _{/同}	15亿象 ¥24,000.00 _{/月}					

各版本的性能规格说明如<mark>表3-3</mark>所示。

版本	支持的数据库实例	性能参数
入门版	最多支持1个数据库实 例	 吞吐量峰值: 1,000条/秒 入库速率: 120万条/小时 在线SQL语句存储: 1亿条
基础版	最多支持3个数据库实 例	 吞吐量峰值: 3,000条/秒 入库速率: 360万条/小时 在线SQL语句存储: 4亿条
专业版	最多支持6个数据库实 例	 吞吐量峰值: 6,000条/秒 入库速率: 720万条/小时 在线SQL语句存储: 6亿条
高级版	最多支持30个数据库 实例	 吞吐量峰值: 30,000条/秒 入库速率: 1,080万条/小时 在线SQL语句存储: 15亿条

表 3-3 数据库安全服务版本规格说明

🗀 说明

• 支持的数据库实例通过数据库IP+数据库端口计量。

如果同一数据库IP具有多个数据库端口,数据库实例数为数据库端口数。1个数据库IP只有1 个数据库端口,即为一个数据库实例;1个数据库IP具有N个数据库端口,即为N个数据库实例。

例如:用户有2个数据库资产分别为IP₁和IP₂,IP₁有一个数据库端口,则为1个数据库实例; IP₂有3个数据库端口,则为3个数据库实例。IP₁和IP₂合计为4个数据库实例,选择服务版本 规格时需要大于或等于4个数据库实例,即选用专业版(最多支持审计6个数据库实例)。

- 不支持修改规格。若要修改,请退订后重购。
- 本表中在线SQL语句的条数,是按照每条SQL语句的容量为1KB来计算的。

步骤6 设置数据库安全审计参数,如图3-3和图3-4所示,相关参数说明如表3-4所示。

图 3-3 网络配置

网络配置

虚拟私有云

vpc-f76c	-f76c	~)	[Q]	新建虚拟私有云 [
----------	-------	-----	-----	-----------

建议VPC选择时,尽量与Agent安装节点所在VPC相同。

子网

subnet-f785 v		Q	新建子网	Ø
---------------	--	---	------	---

子网是虚拟私有云内的IP地址块,虚拟私有云中的所有云资源都必须部署在子网内。

安全组

组ピ

安全组用来实现安全组内和组间数据库安全服务的访问控制,加强数据库安全服务的安全保护。

图 3-4 高级配置

∧ 高级配置
实例名称
DBSS-dd37
实例类型
主备
备注(可选)
请输入备注信息
企业项目 default V Q 新建企业项目 C
标签
如果您需要使用同一标签标识多种云资源,即所有服务均可在标签输入框下拉选择同一标签,建议在TMS中创建预定义标签 🕐 📿
+ 添加新标签
您还可以添加50个标签。

表 3-4 数据库安全审计实例参数说明

说明				
您可以选择使用区域中已有的虚拟私有云(Virtual Private Cloud,VPC)网络,或者单击"查看虚拟私有云",跳转到 /PC管理控制台创建新的虚拟私有云。 说明				
 请选择Agent安装节点(应用端或数据库端)所在的VPC。数据库安全审计的Agent安装节点,请参见:如何选择数据库安全审计的Agent安装节点? 不支持修改VPC。若要修改,请退订后重购。 更多有关虚拟私有云的信息,请参见《虚拟私有云用户指 				

参数名称	说明
安全组	您可以选择区域中已有的安全组,或者在VPC管理控制台创建 新的安全组。选择实例的安全组后,该实例将受到该安全组访 问规则的保护。 更多有关安全组的信息,请参见《虚拟私有云用户指南》。
子网	您可以选择VPC中已配置的子网,或者在VPC管理控制台为 VPC创建新的子网。
实例名称	您可以自定义实例的名称。
备注	您可以添加实例备注信息。
企业项目	该参数针对企业用户使用。
	企业项目是一种云资源管理方式,企业项目管理服务提供统一 的云资源按项目管理,以及项目内的资源管理、成员管理,默 认项目为default。
	请在下拉框中选择所在的企业项目。更多关于企业项目的信 息,请参见 <mark>《企业管理用户指南》</mark> 。
标签	可选配置,对数据库安全审计实例的标识。使用标签可以方便 识别和管理用户拥有的数据库安全服务资源。每个实例最多支 持50个标签配额。
	如用户的组织已经设定数据库安全服务的相关标签策略,则需 按照标签策略规则为数据库安全审计实例添加标签。标签如果 不符合标签策略的规则,则可能会导致数据库安全审计实例创 建失败,请联系组织管理员了解标签策略详情。

步骤7选择"购买时长",如图3-5所示。

图 3-5 选择实例购买时长

ļ	购买时长											
	1个月	2个月	3个月	4个月	5个月	6个月	7个月	8个月	9个月	1年	2年	3#
1	✔ 自动续费 了	?解 扣盡规则 和 续费	时长									

勾选"自动续费"后,当购买的数据库安全审计实例到期时,如果账号余额充足, DBSS将自动为该实例续费,您可以继续使用该实例。自动续费的周期说明如表3-5所示。

表 3-5 自动续费周期说明

购买时长	自动续费周期
1/2/3/4/5/6/7/8/9个月	1个月
1/2/3年	1年

步骤8 确认当前配置无误后,单击"立即购买"。

如果您对价格有疑问,可以单击"了解计费详情",了解产品价格。

- **步骤9** 在"详情"页面,阅读《数据库安服务声明》后,勾选"我已阅读并同意《数据库安全服务声明》",单击"提交"。
- **步骤10** 在购买页面,请选择付款方式进行付款。
 - 余额支付
 您可以通过账户的余额进行支付,余额不足时,单击"充值"进行充值。
 - a. 选择"余额支付"。
 - b. 单击"确认付款",完成购买操作。
 - 申请线上合同请款后支付
 - a. 选择"申请线上合同请款后支付",单击"生成合同"。
 - b. 在页面中填写合同信息后,单击"创建正式合同",完成购买操作。
- 步骤11 成功付款后,在数据库安全审计实例列表界面,可以查看数据库安全审计实例的创建 情况。

----结束

后续处理

- 当实例的"状态"为"运行中"时,说明实例购买成功。
- 当实例的"状态"为"创建失败"时,系统已自动退款。您可单击"操作"列的 "更多 > 查看详情",在弹出的"创建失败实例"对话框中查看失败原因和删除 失败实例。

3.3 步骤一:添加数据库

数据库安全服务支持对华为云上的RDS关系型数据库、ECS/BMS自建数据库进行审 计。购买数据库安全审计实例后,您需要将待审计的数据库添加至数据库安全审计实 例中。

数据库安全服务支持审计的数据库类型及版本,请参见支持的数据库类型及版本。

前提条件

数据库安全审计实例的状态为"运行中"。

添加数据库

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"数据库列表",进入数据库列表界面。
- 步骤4 在"选择实例"下拉列表框中,选择需要添加数据库的实例。
- 步骤5 在数据库列表框左上方,单击"添加数据库"。

图 3-6 添加数据库

数据库列表	选择实例	DBSS-ba89	~
添加数		添加安全组规则	

步骤6 在弹出的对话框中,配置数据库的信息。

表 3-6 数据库参数说明

参数名称	说明	取值样例
数据库类别	选择添加的数据库类别,"RDS数据库"或"自建数据库"。 说明 当您选择"RDS数据库"类型时,可以直接选择您需要 添加至数据库安全服务防护的数据库。	自建数据库
数据库名称	您可以自定义添加的数据库的名称。	test1
IP地址	添加的数据库的IP地址。 IP必须为内网IP地址,支持IPv4和IPv6格式。	IPv4: 192.168.1.1 IPv6: fe80:0000:00 00:0000:000 0:0000:0000: 0000

参数名称	说明	取值样例
数据库类型	支持的数据库类型,您可以选择以下类型:	MYSQL
	MYSQL	
	ORACLE	
	PostgreSQL	
	SQLService	
	• DWS	
	GaussDB(for MYSQL)	
	GaussDB	
	DAMENG	
	KINGBASE	
	MongoDB	
	Hbase	
	SHENTONG	
	• GBase 8a	
	GBase XDM Cluster	
	Greenplum	
	• HighGo	
	MariaDB	
	Hive	
	• DDS	
	• GBase 8s	
	• TDSQL	
	Vastbase	
	• TIDB	
	● 自敛据库奀型选择ORACLE时,待审计的应用程序需 重启,重新登录数据库。	
	 若需要使用Hive数据库审计MRS集群,需要在服务 端关闭SSL加密功能(具体参考客户端SSL加密功能 使用说明),并且在集群购买页关闭Kerberos认证。 	
端口	添加的数据库的端口。	3306

参数名称	说明	取值样例
数据库版本	支持的数据库版本。	5.0
	 当"数据库类型"选择"MySQL"时,您可以 选择以下版本: 	
	- 5.0、5.1、5.5、5.6、5.7	
	- 8.0(8.0.11及以前的子版本)	
	- 8.0.30	
	- 8.0.35	
	- 8.1.0	
	- 8.2.0	
	- 当"数据库类别"为"RDS数据库"时,自 动关联获取数据库列表,按需选择实例, Agent免安装。	
	● 当"数据库类型"选择"ORACLE"时,您可 以选择以下版本:	
	– 11g	
	– 12c	
	– 19c	
	 当"数据库类型"选择"PostgreSQL"时,您 可以选择以下版本: 	
	- 7.4	
	- 8.0、8.1、8.2、8.3、8.4	
	- 9.0、9.1、9.2、9.3、9.4、9.5、9.6	
	- 10.0、10.1、10.2、10.3、10.4、10.5	
	- 11.0	
	- 12.0	
	- 13.0	
	- 14.0	
	● 当"数据库类型"选择"SQLServer"时,您可以选择以下版本:	
	- 2008	
	- 2012	
	- 2014	
	- 2016	
	- 2017	
	 当"数据库类型"选择"DWS"时,您可以选择以下版本: 	
	- 1.5	
	- 8.1	
	 当"数据库类型"选择"GaussDB(for MySQL)"时,您可以选择以下版本: 	

参数名称	说明	取值样例
	- 当"数据库类别"为"自建数据库"时,可 选择"Mysql 8.0"	
	- 当"数据库类别"为"RDS数据库"时,自 动关联获取数据库列表,按需选择实例, Agent免安装。	
	● 当"数据库类型"选择"GaussDB"时,您可 以选择以下版本:	
	- 1.4企业版	
	- 1.3企业版	
	- 2.8企业版	
	- 3.223企业版	
	● 当"数据库类型"选择"DAMENG"时,您可 以选择以下版本:	
	– DM8	
	● 当"数据库类型"选择"KINGBASE"时,您可以选择以下版本:	
	- V8	
	● 当"数据库类型"选择"HBase"时,您可以 选择以下版本:	
	- 1.3.1	
	- 2.2.3	
	 当"数据库类型"选择"SHENTONG"时,您 可以选择以下版本: 	
	- v7.0	
	 当"数据库类型"选择"GBase 8a"时,您可 以选择以下版本: 	
	– v8.5	
	● 当"数据库类型"选择"GBase XDM Cluster"时,您可以选择以下版本:	
	- v8.0	
	 当"数据库类型"选择"GBase 8s"时,您可 以选择以下版本: 	
	- v8.8	
	● 当"数据库类型"选择"Greenplum"时,您可以选择以下版本:	
	– v6.0	
	● 当"数据库类型"选择"HighGo"时,您可以 选择以下版本:	
	– v6.0	
	● 当"数据库类型"选择"MongoDB"时,您可 以选择以下版本:	

参数名称	说明	取值样例
	 v5.0 当"数据库类型"选择"MariaDB"时,您可以选择以下版本: 10.6 	
	 当"数据库类型"选择"Hive"时,您可以选择以下版本: 	
	- 1.2.2	
	- 2.3.9	
	- 3.1.2	
	 - 3.1.3 ● 当"数据库类型"选择"TDSQL"时,您可以 选择以下版本: 	
	- 10.3.17.3.0	
	● 当"数据库类型"选择"Vastbase"时,您可以选择以下版本:	
	– G100 V2.2	
	● 当"数据库类型"选择"TiDB"时,您可以选 择以下版本:	
	– V4	
	– V5	
	– V6	
	- V7	
	- V8	
实例名	您可以指定需要审计的数据库的实例名称。 说明	-
	 如果实例名为空,数据库安全审计将审计数据库中 所有的实例。 	
	 如果填写实例名,数据库安全审计将审计填写的实例,最多可填写5个实例名,且实例名以";"分隔。 	
选择字符集	支持的数据库字符集的编码格式,您可以选择以 下编码格式:	UTF-8
	• UTF-8	
	• GBK	
操作系统	添加的数据库运行的操作系统,您可以选择以下 操作系统:	LINUX64
	• LINUX64	
	WINDOWS64	

步骤7 单击"确定",数据库列表中将新增一条"审计状态"为"已关闭"的数据库。





🗀 说明

 数据库添加完成后,请您确认添加的数据库信息正确。如果数据库信息不正确,请您在数据 库所在行单击"删除",删除数据库后,再重新添加数据库;

----结束

3.4 步骤二:开启数据库安全审计

数据库安全审计默认提供一条"全审计规则"的审计范围,可以对成功连接数据库安 全审计实例的所有数据库进行安全审计。开启数据库安全审计后,您可以查看被添加 的数据库的审计结果。详细操作,请参见<mark>查看审计结果</mark>。

开启审计

- 步骤1 请参见步骤三安装Agent。
- 步骤2 请参见<mark>步骤四</mark>添加安全组规则。
- 步骤3 登录管理控制台。
- **步骤4** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤5 在左侧导航栏中,选择"数据库列表",进入"数据库列表"界面。
- 步骤6 在选择实例下拉框中,选择需要开启审计的数据库安全审计实例。
- **步骤7** 在待开启审计所在行的"操作"列,单击"开启",开启审计功能。 审计功能开启后,该数据库的"审计状态"为"已开启",不需要重启数据库。

图 3-8 开启数据库审计功能

181182494 (B10824948)							
Q 选择履性筛选,或输入关键字搜索							
数据库信息 ⊖	选择字符集 ⊖	IP地址(核省)/第□ Θ	实例名 🖯	操作系统 ⊖	审计状态 0	Agent	操作
名称:) 尚型: MySQL 版本: 5.0	UTF8	3306	-	LINUX84	0 已关闭	意看Apent 添加Apent	开出翻除

----结束

验证审计效果

步骤1 开启审计后,在数据库上执行一条SQL语句(例如"show databases")。

步骤2 登录管理控制台。

- 步骤4 在左侧导航栏选择"数据报表",进入"数据报表"页面。
- 步骤5 在"选择实例"下拉列表框中,选择需要验证的数据库所属的实例。
- 步骤6选择"语句"页签。
- **步骤7** 在列表上方选择时间"**全部时间**"、"近30分钟"、"近1小时"、"今日"、"近7 天"、"近30天"或自定义时间段,SQL语句列表将显示步骤1中输入的SQL语句。

图 3-9 查看 SQL 语句

 序号
 SQL器句
 客户稿户
 数据库用户
 风险等级
 规则
 操作类型
 生成时间
 操作

 1
 show databases
 192.168.0.140
 192.168.0.225
 root
 - 全面计规则
 SHOW
 2020/07/06 17:01:05 GMT+08:00
 详信

----结束

4 开通并使用数据库安全加密

4.1 步骤一: 购买数据库安全加密

本章节介绍如何购买数据库安全加密实例,数据库安全加密提供包年/包月计费方式。

须知

数据库安全加密功能现处于公测阶段,如需使用请<mark>提交工单</mark>申请开通数据库安全加密 功能。

约束与限制

数据库安全加密与访问不支持跨区域(Region)使用。加密与访问的数据库必须和购买的实例在同一区域。

操作步骤

- 步骤1 登录管理控制台。
- 步骤3 在界面右上角,单击"购买数据库安全服务"。
- 步骤4选填购买相关信息。

图 4-1 基础配置

基础配置							
服务类型							
数据库安全审计	数据库	安全加密	数据库安全运维				
计费模式							
包年/包月							
区域							
•			~				
请就近选择靠近您业	务的区域, 可减	沙网络时延, 提	高访问速度。				
可用区类型							
通用可用区							
可用区							
随机分配	可用区1	可用区2	可用区3	可用区4	可用区5	可用区6	可用区7
备可用区							
随机分配	可用区1	可用区2	可用区3	可用区4	可用区5	可用区6	可用区7
版本规格							
1资产量 1并发数		3资产量 3并发数		6资产量 6并发数		10资产量 10并发数	1

表 4-1 基础配置参数说明

参数名称	参数说明	取值样例
服务类型	选择购买的实例类型。	数据库安全加密
计费模式	选择购买实例的计费模式。	包年/包月
区域	选择实例的区域。不同区域的资 源之间内网不互通,请选择邻近 的区域,可以降低网络时延、提 高访问速度。	-
项目	选择实例需要归属的项目,方便 管理。	-
可用区类型	根据实际情况选择可用区类型。	-
可用区	可用区指在同一区域下,电力、 网络隔离的物理区域,可用区之 间内网互通,不同可用区之间物 理隔离。 支持部署在一个可用区。	-
备可用区	支持部署在一个可用区。	-

图 4-2 版本规格

版本规格

1资产量 1并发数	3资产量 3并发数	6资产量 6并发数	10资产量 10并发数

表 4-2 数据库安全加密版本性能规格说明

版本	支持的数据库实例	系统资源要求	性能参数
1资产量	只支持1个数据库	● CPU: 8U ● 内存: 16GB	 加解密性能: 20000QPS 最大并发连接数: 1500
3资产量	最多支持3个数据 库	● CPU: 8U ● 内存: 16GB	 加解密性能: 20000QPS 最大并发连接数: 1500
6资产量	最多支持6个数据 库	● CPU: 16U ● 内存: 32GB	 加解密性能: 40000QPS 最大并发连接数: 3000
10资产 量	最多支持10个数据 库	● CPU: 16U ● 内存: 32GB	 加解密性能: 40000QPS 最大并发连接数: 3000

图 4-3 网络配置

网络配置

虚拟私有云

vpc-default vpc-d

建议VPC选择时,尽量与Agent安装节点所在VPC相同。

子网

subnet-default	~	a	新建子网「
		· · · ·	

子网是虚拟私有云内的IP地址块,虚拟私有云中的所有云资源都必须部署在子网内。

安全组



安全组用来实现安全组内和组间数据库安全服务的访问控制,加强数据库安全服务的安全保护。

分配Ipv4地址

自动分配IP地址 V

弹性IP(可选)

-请选择	~	Q
12.		-

表 4-3 网络配置参数说明

参数名称	参数说明	取值样例
虚拟私有云	选择需要绑定的虚拟私有云。	-
	虚拟私有云可以方便的管理、配 置内部网络,进行安全、快捷的 网络变更,尽量与Agent安装节点 所在VPC相同。	
安全组	安全组用来实现安全组内和组间 数据库安全服务的访问控制,加 强数据库安全服务的安全保护。	-
子网	子网是虚拟私有云内的IP地址块, 虚拟私有云中的所有云资源都必 须部署在子网内。	-
	说明 子网具有物理地域属性:通用可用区 不能使用边缘可用区的子网,边缘可 用区不能使用通用可用区的子网	
分配lpv4地址	选择lpv4地址。	自动分配IP地址
弹性IP(可选)	选择绑定实例的弹性IP。	-

图 4-4 高级配置和登录信息

∧ 高级配置

实例名称

DBSS-f264

实例类型

主备

备注(可选)

请输入备注信息

登录信息

用户名

sysadmin

登录密码

	8
确认密码	

Ì

表 4-4 高级配置和登录信息参数说明

参数名称	参数说明	取值样例
实例名称	自动生成,也可自定义名称。	-
实例类型	当前仅支持主备类型。	主备
备注(可选)	当前实例的备注信息。	-
用户名	默认生成的用户名。	sysadmin

参数名称	参数说明	取值样例
登录密码	设置登录实例的密码。	-
	说明 设置的登录密码需要满足以下几个条 件:	
	● 8~26个字符。	
	 至少包含以下字符中的2种:大写字母、小写字母、小写字母、数字和特殊字符~!@#\$%^&*()_+`=-[] {};':,".<>?/\。 	
	不能与用户名或倒序的用户名相 同。	
确认密码	输入确认密码,需要登录密码一 致。	-

图 4-5 购买时长

购买时长											
1个月	2个月	3个月	4个月	5个月	6个月	7个月	8个月	9个月	<mark>位</mark> 1年	2年	244 344
✔ 自动续费 了	W 扣费规则 和 续费	时长									

勾选"自动续费"后,当购买的数据库安全加密到期时,如果账号余额充足,DBSS将 自动为该实例续费,您可以继续使用该实例。自动续费的周期说明如<mark>表4-5</mark>所示。

表 4-5 自动续费周期说明

购买时长	自动续费周期			
1/2/3/4/5/6/7/8/9个月	1个月			
1/2/3年	1年			

步骤5 确认当前配置无误后,单击"立即购买"。

如果您对价格有疑问,可以单击"了解计费详情",了解产品价格。

- **步骤6** 在"详情"页面,阅读《数据库安全服务声明》后,勾选"我已阅读并同意《数据库 安全服务声明》",单击"提交"。
- 步骤7 在购买页面,请选择付款方式进行付款。
 - 余额/在线支付
 您可以通过账户的余额进行支付,余额不足时,单击"充值"进行充值。
 - a. 选择"余额支付"。
 - b. 单击"确认付款",完成购买操作。
 - 申请线上合同请款后支付
 - a. 选择"申请线上合同请款后支付",单击"生成合同"。
b. 在页面中填写合同信息后,单击"创建正式合同",完成购买操作。

步骤8 成功付款后,在数据库安全加密实例列表界面,可以查看数据库安全加密实例的创建 情况。

----结束

4.2 步骤二:登录实例 Web 控制台

系统管理员使用web浏览器登录数据库加密与访问控制控制台,可以管理和维护数据 库加密与访问控制。

出厂默认用户名如<mark>表1 系统默认账号信息</mark>所示,具体实际用户名密码请从技术支持工 程师处获取。

表 4-6 系统默认账号信息

出厂默认角 色	出厂默认 账号	说明
系统管理员	sysadmin	主要负责系统配置和系统日常运行维护。 具体操作请参见 <mark>系统管理员操作指导</mark> 。
安全管理员	secadmin	主要负责系统用户管理和系统安全管理。 具体操作请参见 <mark>安全管理员操作指导</mark> 。
审计管理员	audadmin	主要负责对系统管理员和安全管理员的操作行为进行审 计跟踪、分析和监督检查。 具体操作请参见 <mark>审计管理员操作指导</mark> 。

前提条件

- 您已经从技术支持工程师处获取登录用户名和密码。
- 支持浏览器:
 - Chrome 77版本及以上。
 - 密信浏览器1.0.0.7。

操作步骤

步骤1登录实例。

- 方式一:登录服务管理控制台,进入数据库加密与访问控制页面,在目标实例 "操作"列单击"远程登录"或"本地登录"。
- 方式二:通过方式一进入的数据库加密与访问控制页面获取"弹性IP",在浏览器地址栏中输入访问地址,按回车键,进入登录界面。
 访问地址:https://服务器弹性IP地址:端口,例如https://100.xx.xx.54:9595。

步骤2 (可选)在安全告警页面,单击"高级"。

图 4-6 安全告警

▲ 不安全	https://192.1 9595	☆	⊜	无痕模
	A			
	您的连接不是私密连接			
	攻击者可能会试图从 19. 54 窃取您的信息(例如:密码、通讯内容或信用卡(息)。 <u>了解详情</u>	言		
	NET::ERR_CERT_AUTHORITY_INVALID			
	高级	车接		

步骤3 (可选)在详情说明中,单击继续前往xx.xx.xx.(不安全)。

图 4-7 继续前往

隐藏详情	返回安全连接
此服务器无法证明它是1 的原因可能是配置有误或您的证	;您计算机的操作系统不信任其安全证书。出现此问题 主接被拦截了。
继续前往1 39 (不安全)	

步骤4 输入用户名、密码和验证码,单击"登录"。

步骤5 首次登录后,需要修改默认密码,详细操作请参见修改登录密码。 在后续使用过程中,建议您定期修改密码,确保登录安全。 ----**结束**

修改登录密码

步骤1 在Web控制台,鼠标移动到右上角的用户名。

图 4-8 修改密码

sysadmin
合 修改密码
G 退出

- 步骤2 在下拉框中,单击"修改密码"。
- **步骤3** 在修改密码对话框中,输入原始密码和新密码,单击"确定",新密码规则如<mark>表4-7</mark>所示。

修改完成后,您需要退出Web控制台,使用新密码重新登录。

表 4-/ 1 修改 密码	表 4-7	修改密码
----------------------	-------	------

参数	说明
原密码	输入原来的登录密码。
新密码	 输入修改后的新密码。 为了登录安全,建议您将密码设置成复杂密码,例如包含以下多种字符组合: 大写字母(从A到Z) 小写字母(从a到z) 数字(0~9) 特殊符号(例如:!@#\$)
确认密码	重新输入修改后的新密码。

----结束

4.3 步骤三:系统功能配置及使用场景举例

4.3.1 场景一:加密操作流程及加密功能典型配置

加密操作流程

数据库加密与访问控制的加密操作流程图和流程介绍如下<mark>图4-9</mark>所示。



图 4-9 加密操作流程

1. (首次)初始化密钥。

首次使用系统时,根据密钥来源初始化密钥。具体操作,请参见<mark>初始化密钥</mark>。

- 添加数据源。
 在使用数据脱敏功能前,您需要将数据资产添加到系统中。具体操作,请参见添加数据资产。
- 3. (可选)配置行业模板和敏感数据类型。

系统已经内置满足大部分需求的敏感数据类型和通用行业模板。如果您有特殊需求,也可以自定义敏感数据类型和行业模板。具体操作,请参见<mark>新增行业模板</mark>和 新增自定义数据类型。

- (可选)执行敏感数据发现。
 通过敏感数据发现任务,自动扫描和识别出数据资产中的敏感数据。具体操作, 请参见扫描资产的敏感数据。
- (可选)查看任务执行结果。
 通过查看任务执行结果,检查结果是否符合敏感数据要求。具体操作,请参见查 看扫描任务执行结果。
- (可选)仿真加密测试。
 通过仿真加密测试,检查目标是否支持加密。具体操作,请参见仿真加密测试。

7. 创建加密队列。

您可以在敏感数据发现任务的结果中,根据敏感数据信息创建加密队列。具体操 作,请参见<mark>在结果中创建加密队列</mark>。

同时,也支持在数据加密模块直接创建加密队列。具体操作,请参见<mark>配置加密队</mark> <mark>列</mark>。

8. 授权管理。

配置加密后,默认情况下访问数据库时,您只能看到加密后的数据。应用系统正 常运行需要获取加密前的数据,此时您需要为应用系统进行授权操作。具体操 作,请参见<mark>管理授权</mark>。

- 9. 配置完成后,您可以通过以下方式验证配置结果。
 - 使用已授权的客户端地址和用户,通过代理方式访问数据库,此时可以查看 到加密前的明文数据。
 - 使用未授权的客户端地址或用户,通过代理方式访问数据库,此时只能查看 到加密后的数据。

加密功能典型配置

数据库加密与访问控制支持为数据库的敏感数据进行加密,保障数据的安全性。本举 例展示如何对数据库进行加密。

组网说明

数据库加密与访问控制采用反向代理方式,典型组网如下<mark>图4-10</mark>所示。

图 4-10 典型组网



前提条件

- 设备和应用系统路由可达。
- 设备和数据库路由可达。

步骤一:添加数据源

在使用前,需要在资产管理中添加目标数据库。

1. 使用sysadmin用户登录实例Web控制台。

- 2. 在左侧导航栏,选择"资产管理 > 数据源管理"。
- 3. 单击右上角的"添加数据源"。
- 在"添加数据源"对话框中,设置资产信息。
 主机信息和日志信息为可选操作,数据库服务器需要开启SSH服务。

图 4-11 添加数据源

• 数据源名称:	demo		0				
• 数据源类型:	MySQL			• 数据源版本:	5.7		
读写分离/RAC:	开启						
• 数据源地址:	172. 139		٥	• 数据源端口:	3310		
• 代理地址:	eth1:172.		v	* 代理婰曰:	14099	自动分配	
管理 V		· WAY-WIT HAD BEE	-		70		
doc_demo	51D/809545/68114	 socialities root 	1 <u>5</u>	0 ·····	19	0	

- 5. 配置完成后,单击"测试数据库连接",检查是否能够连上数据库。
- 6. 单击"测试账号权限",检查数据库账号权限是否满足加密要求。
- 7. 单击"保存",保存数据资产的配置信息。

步骤二:执行敏感数据发现任务

- 1. 使用sysadmin用户登录实例Web控制台。
- 2. 在左侧导航栏,选择"敏感数据发现 > 敏感数据扫描"。
- 3. 找到目标数据资产,单击"任务配置"。
- 4. 在"任务配置"对话框中,设置敏感数据发现任务。

抽样数量: 100	00		
最大线程数 ①: 〇 1			
□ 42項	可选择的模式	[] 1項	已选中的模式
朝榆入肥即内容	٩	開始入設成内容	Q,
 ddmtest2 demo emp_nthl_uact_b 	•	doc_demo	
0项	可选择的表	1項	已选中的表
請給入證案內容	٩	请输入推动内容	٩,
	表名		表名
			ys_user
電天	200 H	×	1 / 1 >

图 4-12 配置敏感数据发现任务

- 5. 单击"保存",完成敏感数据任务配置。
- 6. 找到目标数据资产,单击 》按钮执行敏感数据发现任务。

执行开始后,系统自动扫描识别敏感数据。扫描时间和需要扫描的数据量有关,数据 量越多,需要扫描的时间越长,您可以在页面查看扫描进度。

步骤三:进行仿真加密测试

在为数据库表进行加密前,先进行仿真加密测试,检查数据库是否满足加密要求。

- 1. 使用sysadmin用户登录实例Web控制台。
- 1. 在左侧导航栏中,选择"业务测试 > 仿真测试"。
- 2. 单击"新增加密测试"。
- 3. 在"新增加密测试"对话框中,配置测试目标。

保存

图 4-13	新增加密测试
--------	--------

数据	原名称:	demo			V demo
					~ ~
• 1	夏式名:	doc_demo			✓ 数据源类型: MySQL
	-				数据源版本: 5.7
	农台:	sys_user			数据源地址: 1
加密算	1法①:	SM4_128			◇ 数据源端口: 」
					主机P:
校验算	陆():	SM3_HMAC_16			≥
加密	列表				CPU:
择	列名		数据类型	备注信息	0%
	dept	t_id	bigint(20)	Department ID	内存:
	user	_name	varchar(720)	User account	网络:
	nick	_name	varchar(720)	User's nickname	ю:
	user	_type	varchar(272)	user type(00syste	操作系统:
	ema	a	varchar(2928)	email	
	pho	nenumber	varchar(2928)	phone number	
	sex		varchar(272)	gender	

4. 单击"保存"。

测试完成后,用户可以在列表中查看测试结果,单击"详情"查看加密流程中各 个节点的完成情况。

测试完成后,单击"删除",删除此仿真加密测试。

🗀 说明

- 如果仿真测试存在问题,请根据页面提示排查问题。
- 如果测试后需要配置加密队列,需要先删除此仿真加密测试。

步骤四: 在发现结果中创建加密队列

- 1. 使用sysadmin用户登录实例Web控制台。
- 2. 在左侧导航栏,选择"敏感数据发现 > 敏感数据扫描"。
- 3. 在扫描任务列表页面,找到目标数据资产,单击"查看"。
- 4. 在扫描结果列表页面,找到目标数据库表,单击"添加加密队列"。
- 5. 在"新增加密队列"对话框中,设置加密信息。

冬	4-1	4	新增加	密队	列
---	-----	---	-----	----	---

所增加密队列				×
• 数据源名称:	demo			V demo
• 模式名:	doc_demo			∨ 数据源类型: MySQL
* 表名:	sys_user			数据源版本: 5.7 数据源地址: 17
•加密算法 ①:	SM4_128			∨ 数据源端口:
▪校验算法 ①:	SM3_HMAC_16			主初UP: ✓ 主初3時口:
* 每批条数:	8191	* 鎖	程数: 4	CPU: 0%
启动队列:				内存: 0%
•加密列表				网络:
选择 列名	5	数据类型	备注信息	IO:
dep	ot_id	bigint(20)	Department ID	撮作系统:
use	r_name	varchar(720)	User account	
nick	c_name	varchar(720)	User's nickname	
use	r_type	varchar(272)	user type(00syste	
em	ail	varchar(2928)	email	
pho	onenumber	varchar(2928)	phone number	

初始化表 完成

- 6. 在加密算法中选择加密的算法。
- 7. 单击"加密列表"页签,勾选需要加密的列名称。
- 8. 单击"初始化表",开始对数据表进行初始化。
- 9. 单击"完成",创建加密队列。

加密队列执行结束后,访问数据库时查询到的都是加密后的数据。此时需要为应用系统(或客户端)进行访问授权,保证应用系统(或客户端)能正常使用。

步骤五:设置访问授权

授权管理模块中支持客户端授权和用户授权,两者授权取交集。

- 1. 使用sysadmin用户登录实例Web控制台。
- 2. 在左侧导航栏中,选择"数据加密 > 授权管理"。
- 3. 在数据源列表中,单击目标数据源。
- 4. 找到目标加密数据库表,单击"客户端授权"。
- 5. 在"客户端授权"对话框中,设置客户端IP地址范围、时间范围和星期范围,单 击"保存"。

图 4-1	5 客府	白端授权
-------	------	------

IP范围 ①:	196.168.0.100-196.168.0.120					
	196.168.1.100-1	196.168.1.12	0		٥	00
时间点范围:	00	©] - [23	©	
星期范围:	星期一	V] - [星期天	~	

IP地址范围支持设置起始IP和结束IP,单击^①按钮可以添加多个IP地址范围,最多 设置5个IP地址范围。

6. 找到目标加密数据库表,单击"用户授权"。

图 4-16 田户授权

7. 在"用户授权"对话框中,对数据库用户设置相应的权限,单击"保存"。

请输入用户名	Q			
用户	权限			
root	查询	🔲 添加	[]] 编辑	□ 删除
mysql.infoschema	查询	🔲 添加	[]] 编辑	□ 删除
mysql.session	查询	🔲 添加	- 编辑	□ 删除
mysql.sys	查询	🔲 添加	□ 编辑	□ 删除
			取消	清空保

<u>∕</u>∧ 注意

此处以DBeaver工具为例,在实际使用过程中,您需要修改应用系统对接到数据库的 连接信息。 本文以DBeaver工具为例,通过代理连接到数据库。

图 4-17 通过代理连接数据库

🚱 DBeaver 5.0.2	12 创建新连接	× 🧟 创建新连接 ×
文件(F) 編編(E) 导航(N) 捜索(A) 株 1 ☆ 」 「 「 」 「 ※ ◆ 「 项目 33 □ □	s 选择新连接类型 MySQL standard driver	送 選 MySQL连接 MySQL连接设置 MulSQL
●項目 22 □ ● d ^{ad} ○ → □ General	MySAL standard driver Type part of database/driver name to filter Name Cache ClickHouse CURID S DB2 Defuy M Exasol Firebird 3.x Flat files (CSV) Correption 122 Contemport 232 Contemport 242 Con	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
Project 22	> ● HSQLD8 ● Informix ● Ingres 项目 General ④ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	日達接 (84 ms) 通定 6 5 影成链接 2 4

- 1. 单击 4 图标。
- 2. 在选择新连接类型对话框中,选中MySQL。
- 3. 单击下一步。
- 4. 在"设置MySQL连接"对话框中,设置连接信息。
 - 连接信息说明:
 - 服务器地址:使用数据库加密与访问控制的访问IP地址。例如192.xx.xx.54。
 - 端口:使用代理端口,即创建资产时设置的代理端口(14099)。
- 5. 单击"测试链接",测试是否能够连接到数据库。
- 6. 测试通过后,单击"下一步",按照界面提示完成操作。

步骤七: 验证加密结果

参考步骤六(通过代理连接数据库)操作连接数据库,验证授权是否配置成功:

1. 用户的IP地址为192.168.0.105(授权地址),通过代理方式,使用授权用户(例 如root)访问数据库,可以查看到明文数据。

图 4-18 明文数据

	128 user_id 71?	123 dept_id \[]?	ADC user_name T1?	ADC nick_name \T ?	ADC user_type \T ?	®© email ₹ ?	^{ADC} phonenumber ▼ ‡?	ADC sex T1?	ADC avatar 71?
1	1	103	admin	兼備	00	@163.com	158888888	1	
2		105	ry	*8	00	₩@qq.com	156666666	1	

2. 用户的IP地址为192.168.0.105(授权地址),通过代理方式,使用非授权用户 (例如user01)访问数据库,只能查看到加密数据。

图 4-19 加密数据

123 user_id \1 2	123 dept_id 🏹	? ABC user_name	Tt? ABC nick	_name \1 ?	ABC user_type 71?	ABC email 🏹	? ABC P	phonenumber	¥1?	ABC Sex	T1 ?
1	10	3 admin	803		00	[NULL]	[NU	JLL]		1	
2	10	5 ry	800		00	[NULL]	[NU	JLL]		1	

根据添加资产时配置的无权限缺省显示参数,显示对应加密结果。

3. 用户的IP地址为192.168.3.105(非授权地址),通过代理方式,使用授权用户 (例如root)访问数据库,只能查看到加密数据。

图 4-20 加密数据

123 user_id \[?	123 dept_id \[1 23	ABC user_name \\$?	♣∎⊂ nick_name 🏹	? ABC user_type ▼\$?	email ₹ ?	RBC phonenumber $\forall \uparrow$?	ADC sex \T ?
1	103	admin	300	00	[NULL]	[NULL]	1
2	105	ry	30.0	00	[NULL]	[NULL]	1

4. 此时,通过原数据库地址连接访问,查看到密文数据。

图 4-21 加密数据

RBC user_name 11? RBC nick_name 11? RBC user_type 11	RBC email T1? RBC phonenumber T1?	RBC sex T1?
admin 00	00002F50F6A9ED206D6746551FCF(00006C1C8EA0E32B7B3C110	0 1
y 00	00002F50F6E9AA3D206B44B0040C 00006C1C80AEED2575321F0	E 1

4.3.2 场景二: 解密操作流程及解密功能典型配置

解密操作流程

数据库加密与访问控制的解密操作流程图和流程介绍如下<mark>图4-22</mark>所示。

图 4-22 解密操作流程



- (可选)仿真解密测试。
 通过仿真解密测试,检查目标是否支持解密。具体操作,请参见仿真解密测试。
- 创建解密队列
 创建解密队列,解密数据。具体操作,请参见配置解密队列。

解密功能典型配置

为数据库资产进行加密后,如果业务变更等影响,不再需要对数据库资产进行加密。 此时,您需要通过解密功能和回滚表结构功能恢复数据库表。本举例为用户展示为数 据库表进行解密功能。

前提条件

已经为数据库表进行加密,具体操作,请参见<mark>场景一:加密操作流程及加密功能典型</mark> <mark>配置</mark>。

步骤一:进行仿真解密测试

在为数据库表进行解密前,先进行仿真解密测试,检查数据库是否满足解密要求。

- 1. 使用sysadmin用户登录实例Web控制台。
- 2. 在左侧导航栏中,选择"业务测试 > 仿真测试"。
- 3. 单击"新增解密测试"。
- 4. 在"新增解密测试"对话框中,配置测试目标。

图 4-23 新增解密测试

数据》	原名称:	demo			~	demo	
٠٤	夏式名:	doc_demo			×	数据源类型: MySQL	
5	表名:	sys_user				数据源版本: 5.7	
						SXBARABAL: 1	
加密算	阹①:	SM4_128				数据源端口:	
枯硷管	B≠ ⊕.	SM3 HMAC 16				主机IP:	
1.8.222.94	MA OI	5115_111716_10				主机端口:	
加密	列表					CPU:	
择	列名	i i	数据类型	备注信息			0%
	dept	t_id	bigint(20)	Department ID		PSH#:	0%
	user	_name	varchar(720)	User account		网络:	
	nick	_name	varchar(720)	User's nickname		10:	
	user	_type	varchar(272)	user type(00syste		操作系统:	
ł.	ema	il	varchar(2928)	email			
ł	pho	nenumber	varchar(2928)	phone number			
	sex		varchar(272)	gender			

5. 单击"保存"。

测试完成后,用户可以在列表中查看测试结果,单击"详情"查看解密流程中各 个节点的完成情况。

如果仿真测试存在问题,请根据页面提示排查问题。

测试完成后,单击"删除",删除此仿真解密测试。
 如果测试后需要配置解密队列,需要先删除此仿真解密测试。

步骤二: 创建解密队列

- 1. 使用sysadmin用户登录实例Web控制台。
- 2. 在左侧导航栏中,选择"数据加密 > 解密队列管理"。
- 3. 单击右上角的"新增解密队列"。
- 在"新增解密队列"对话框中,设置和加密对应的数据信息,包括资产名称、模式名和表名。

图 4-24 新增解密队列

	99			
 数据源名科 	称: demo			demo
• 模式	음: doc_demo			∨ 数据源类型: MySQL
• 表	움: sys_user			数据源版本: 5.7 数据源地址: 1
•加密算法(: SM4_128			→ 数据源端口:
 校验算法(: SM3_HMAC_16			主机IP:
•每批条	数: 6553	• #	乾程数: 4	王어 Gami
启动队	列: 🔽			0% 内存:
				0%
• 加索列表	i i			网络:
•加密列表 选择	列名	数据类型	备注信息	网络: IO:
•加索列表 选择	ž 列名 dept_id	数据类型 bigint(20)	酱注信息 Department ID	网络: 10: 摄作系统:
•加索列表 选择	i 옛名 dept_id user_name	数据类型 bigint(20) varchar(720)	裔注倫題 Department ID User account	网络: IO: 摄作系统:
•加密列表 选择 :	初名 dept_id user_name nick_name	数据类型 bigint(20) varchar(720) varchar(720)	裔注信题 Department ID User account User's nickname	网络: 10: 操作系统:
•加索列表 选择 :	社 列名 dept_id user_name nick_name user_type	数据类型 bigint(20) varchar(720) varchar(720) varchar(272)	衛注倫題 Department ID User account User's nickname user type(00syste	网络: IO: 摄作系统:
•加索列表 选择 :	利名 dept_id user_name nick_name user_type email	数据类型 bigint(20) varchar(720) varchar(720) varchar(272) varchar(2928)	裔注信題 Department ID User account User's nickname user type(00syste email	网络: 10: 撮作系统:

5. 勾选"启动队列",创建完成后自动启动解密队列。

6. 单击"完成",创建解密队列。

步骤三:验证配置效果

解密后,通过原数据库地址或者通过代理地址,查询数据库表内容,示例如下<mark>图4-25</mark> 所示,表示数据库表已经恢复。

图 4-25 通过代理查询结果

	¹² ∂ user_id \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	123 dept_id \[?	ADC user_name	Tt? ADC nick_name	T1?	ABC user_type	T 1?	🕫 email 🏹	ADC phonenumber 🏹	ADC sex	T1?	ABC avatar	T1 ?
1	1	103	admin	兼調		00		@163.com	158888888888888888888888888888888888888	1			
2	2	105	ry	##		00		=@qq.com	156 66666	1			

4.3.3 场景三: 业务测试典型配置举例

数据库加密与访问控制支持通过业务分析功能对数据库资产进行前期分析,排除加密 后可能影响的业务错误,业务测试流程如<mark>图</mark>4-26所示。

图 4-26 业务测试流程



组网说明

数据库加密与访问控制采用反向代理方式,典型组网如下<mark>图4-27</mark>所示。

图 4-27 典型组网



前提条件

- 设备和应用系统路由可达。
- 设备和数据库路由可达。

步骤一:添加数据源

在使用前,需要在资产管理中添加目标数据库。

- 1. 使用sysadmin用户登录实例Web控制台。
- 2. 在左侧导航栏,选择"资产管理 > 数据源管理"。
- 3. 单击右上角的"添加数据源"。

4. 在"添加数据源"对话框中,设置资产信息。

• 数据源名称:	demo	0				
• 数据源类型:	MySQL		• 数据源版本:	5.7		
读写分离/RAC:	开启					
• 数据源地址:	172. 139	0	▶ 数据源端口:	3310		
• 代理地址:	eth1:172.		* 代理端口:	14099	自动分配	
张号管理 > * 数据库/实例名/	SID/服务名/模式	• 数据库账号	* 数据库语	码		
doc_demo	C	root	0		0	

主机信息和日志信息为可选操作,数据库服务器需要开启SSH服务。

- 5. 配置完成后,单击"测试数据库连接",检查是否能够连上数据库。
- 6. 单击"测试账号权限",检查数据库账号权限是否满足加密要求。
- 7. 单击"保存",保存数据资产的配置信息。

步骤二: 创建业务分析任务

在加密之前,创建业务分析任务,测试业务SQL是否支持。

- 1. 使用sysadmin用户登录实例Web控制台。
- 2. 在左侧导航栏,选择"业务测试>业务分析"。
- 3. 在页面左侧数据源处,单击目标数据源。

图 4-29 添加业务分析任务

		demo	10.000 10.000	III: MySQL 1: root	16.4 10.92	: 5.7 #1010: 172.16.36.251		素例后	doc_demo			
oraclewwwwwwwww oracle19cwwwwwww	(ISC: 27	v][3	#8(Q,		11.838/1 ×	分析报表	解析研究员	16 11 39	ri 21	С	© 1
 MySQL 	@ (8)(S	82	6	5316570	100	异常记录			分析	1971		
 demo demo myralq SQLServer 人大会合 満訴-A PostgreSQL TDSQL TDSQL 					No.							

4. 单击"新增分析表",配置需要分析的数据表,单击"确定"。

图 4-30 配置分析的数据表

• 模式名:	doc_d	lemo		v	demo
					N 4
* 表名:	sys_us	ser		Ŷ	数据源类型: MySQL
	-		12		数据源版本: 5.7
	0 228	分析 (●) 指定列分	र्थत		数据源地址:
	选择	列名	数据类型	备注信息	数据源端口:
		dept_id	bigint(20)	Department ID	主机IP:
		user_name	varchar(720)	User account	主机端口:
		nick_name	varchar(720)	User's nickname	CPU:
		user_type	varchar(272)	user type(00system user)	0%
		email	varchar(2928)	email	0%
		phonenumber	varchar(2928)	phone number	网络:
		sex	varchar(272)	gender	10:
					操作系统:

找到目标表格,单击启动按钮》。

步骤三:通过代理执行业务SQL语句

通过代理地址访问数据库,并执行业务SQL语句,检验数据库表和字段加密后是否影响业务。

- 1. 使用sysadmin用户登录实例Web控制台。
- 在左侧导航栏选择"资产管理 > 数据源管理",找到目标数据库并单击编辑查看 数据库代理IP和端口号。

图 4-31 查看代理 IP 和端口号

• 数据源名称:	demo						
• 数据源关型:	MySQL		v	• 数据源版本:	5.7		
读写分离/RAC:	开启						
• 数据源地址:	172. 158		0	• 数据源编口:	-		
•代理地址:	eth1:172	1		• 代理演曰:	14099 2 自动	分配	
•代理地址: 2理 ~	eth1:172	1	(v)	• 代理编口:	14099 2 Eb	分配	
 代理地址: 2理 > 数据库/实例名/ doc_demo 	eth1:172	 数据库标: root 	<	 代理M口: 数据応じ ● ● ● 	14099 2	98 0	

3. 在数据库连接工具上,使用代理IP和端口访问数据库。

图 4-32 访问数据库

▼MySQL - 新建连接	×
常规 高级 数据库 SSL SSH HTTP	
<u> </u>	
连接名: 加密测试	
主机: 172.14 1.158	
端口: 14099	
用户名: root	
密码:	
☑ 保存密码	
测试连接 确定	取消

IP和端口使用上一步骤中获取的代理IP和端口;用户名和密码使用数据库原来的用户名和密码。

4. 执行业务使用的SQL语句。

以上SQL语句仅为示例,在实际使用时,您需要执行业务上使用的SQL语句,便于 系统进行业务分析。

表 4-8 SQL 语句示例

SQL类型	示例
正常语句	SELECT * FROM `sys_user`;
异常语句	SELECT * FROMM `sys_user`;
阻断语句	RENAME TABLE sys_user to abc;

步骤四: 查看业务分析结果

执行业务SQL语句后,系统会记录异常和阻断的SQL语句,并分析阻断原因。

- 1. 使用sysadmin用户登录实例Web控制台。
- 2. 在左侧导航栏,选择"业务测试 > 业务分析"。
- 3. 在页面左侧数据源处,单击目标数据源。
- 4. 单击"解析异常SQL",查看执行的异常SQL语句。

图 4-33 异常 SQL 语句

解析异常SQL			>
			寺田
发现异常	发现时间	关联列	异常详情
SQL无法解析	2024-08-27 13:24:43	-	select * fform table
SQL无法解析	2024-08-27 13:25:34	-	select * formm table
SQL无法解析	2024-08-26 13:34:44	5	/* ApplicationName=DBeaver
			总共 3 条 〈 1 〉 15 条/页 >

5. 查看阻断的SQL语句和系统建议。

图 4-34 阻断 SQL 语句

· (2):(2):(2):(2):(2):(2):(2):(2):(2):(2):	23 N	٩	総量操作 ~	分析报表	解析异常SQL	新潮分	后表	C	۲	I
模式名	表名	分析列	NS.	异常记录	3	分析	腺作			
doc_demo	sys_user	email.phonenumber	分析中	1		ø	查看日	38	2	

- 6. 在异常记录列,查看阻断的SQL语句数量。
- 7. 单击"查看日志",查看阻断的具体SQL语句和错误提示。

图 4-35 阻断 SQL 语句日志

查看分析日志			Х
模式名: doc_demo	表名: sys_user		导出
发现异常	发现时间	关联列	异常详情
illegal operation	2024-08-27 13:51:45	/	RENAME TABLE sys_user to abc
			总共1条 < 1 > 15条/页 >

8. 单击"分析报表",可用查看系统对此表格的加密建议。

图 4-36 分析建议

分析报表)
						导出
策略建议	建议原因	模式	表名	列名	异常详情	操作
表不可加密	illegal operation	doc_demo	sys_user	/	RENAME TABLE sys_user to abc	删除
					总共1条 < 1 > 15	条/页 ∨

业务测试结果表明此数据库表如果加密的话将影响业务的SQL语句运行,所以不 建议对此数据库表进行加密操作。

4.3.4 场景四: 动态脱敏典型配置举例

动态脱敏操作流程

数据库加密与访问控制支持配置动态脱敏策略,对数据库资产中的明文数据进行脱敏展示,动态脱敏流程如<mark>图4-37</mark>所示。



图 4-37 动态脱敏流程

1. 添加数据源。

在使用数据脱敏功能前,您需要将数据资产添加到系统中。具体操作,请参见<mark>添</mark>加数据资产。

2. (可选)配置行业模板和敏感数据类型。

系统已经内置满足大部分需求的敏感数据类型和通用行业模板。如果您有特殊需求,也可以自定义敏感数据类型和行业模板。具体操作,请参见<mark>新增行业模板</mark>和 新增自定义数据类型。

- 执行敏感数据发现。
 通过敏感数据发现任务,自动扫描和识别出数据资产中的敏感数据。具体操作, 请参见扫描资产的敏感数据。
- (可选)查看任务执行结果。
 通过查看任务执行结果,查看命中的敏感数据。具体操作,请参见查看扫描任务执行结果。
- 5. 创建脱敏规则。

您可以在敏感数据发现任务的结果中,根据敏感数据信息创建加密队列。具体操 作,请参见<mark>在结果中创建脱敏规则</mark>。

同时,也支持在动态脱敏模块直接创建脱敏规则。具体操作,请参见创建脱敏规则。

6. (可选)配置脱敏白名单。

配置脱敏规则并启用后,默认情况下访问数据库的明文数据时,您只能看到脱敏 后的数据。配置脱敏白名单后,白名单中的用户访问数据库可查看到明文数据。 具体操作,请参见1.4.8.3 配置脱敏白名单。

7. 配置完成后,您可以代理访问验证脱敏规则配置效果。

动态脱敏典型配置

数据库加密与访问控制支持对数据库中的明文敏感数据进行动态脱敏。本举例展示如 何对数据库明文数据进行动态脱敏。

步骤一:添加数据源

在使用前,需要在资产管理中添加目标数据库。

- 1. 使用sysadmin用户登录实例Web控制台。
- 2. 在左侧导航栏,选择"资产管理 > 数据源管理"。
- 3. 单击右上角的"添加数据源"。

图 4-38 添加数据源

在"添加数据源"对话框中,设置资产信息。
 主机信息和日志信息为可选操作,数据库服务器需要开启SSH服务。

• 数据源名称:	demo		0					
• 数据源类型:	MySQL			• 数据源版本:	5.7			
读写分离/RAC:	开启							
• 数据源地址:	172. 139		0	• 数据源端口:	3310			
* 代理地址:	eth1:172.			*代理端口:	14099	自动分配		
建建 >	cin /Rds-dz Jate=*	• WHERE		 No 102 etc. 30 	ana a			
\$0(\$RJ#r/34;17912)/	SIU/883543/9820	root		0	19-3 1-1-1		0	
doc_demo								

- 5. 配置完成后,单击"测试数据库连接",检查是否能够连上数据库。
- 6. 单击"测试账号权限",检查数据库账号权限是否满足加密要求。
- 7. 单击"保存",保存数据资产的配置信息。

步骤二:执行敏感数据发现任务

1. 使用sysadmin用户登录实例Web控制台。

- 2. 在左侧导航栏,选择"敏感数据发现 > 敏感数据扫描"。
- 3. 找到目标数据资产,单击"任务配置"。
- 4. 在"任务配置"对话框中,设置敏感数据发现任务。

图 4-39	配置敏感数据发现任务
--------	------------

5篇	
抽样数量: 1000	
最大线程数 ①: 〇 1	
☐ 42 項 可选择的模式	□ 1项 已选中的模式
消益入资 素内容 Q	→ 請給入證案內容 9、
ddmtest2 demo emp_nthl_uact_b	doc_demo
0项 可选择的表	1项 已选中的表
調給入設定内容	请输入推荐内容 Q
表名	麦名
	sys_user
重无政策	< <u>1</u> / 1 >

5. 单击"保存",完成敏感数据任务配置。

6. 找到目标数据资产,单击》按钮执行敏感数据发现任务。

执行开始后,系统自动扫描识别敏感数据。扫描时间和需要扫描的数据量有关,数据 量越多,需要扫描的时间越长,您可以在页面查看扫描进度。

步骤三: 在发现结果中创建脱敏规则

- 1. 使用sysadmin用户登录实例Web控制台。
- 2. 在左侧导航栏,选择"敏感数据发现>敏感数据扫描"。
- 3. 在扫描任务列表页面,找到目标数据资产,单击"查看"。
- 4. 在扫描结果列表页面,找到目标数据库表,单击"添加脱敏规则"。
- 5. 在"添加脱敏规则"对话框中,设置脱敏信息。

图 4-40 添加脱敏规则

▶ 规则名称:	脱敏demo				
* 模式名:	doc_demo				V
*表名:	sys_user				
* 脱敏列表					
名		数据类型	命中率	脱敏算法 ①	
hone		手机号码	100%	部分遮蔽	\vee
ł		固定电话号码	100%	部分遮蔽	V

- 6. 配置规则名称,并在脱敏列表中选择数据类型对应的脱敏算法。
- 7. 单击"保存"。

脱敏规则保存后自动启用,访问数据库时查询到的明文数据均为脱敏后的数据。此时 可配置脱敏白名单,命中白名单则放行不脱敏。

步骤四: 配置脱敏白名单

- 1. 使用sysadmin用户登录实例Web控制台。
- 2. 在左侧导航栏中,选择"动态脱敏 > 脱敏规则"。
- 3. 在左侧数据源列表中,单击目标数据源。
- 4. 找到目标数据源的脱敏规则列表中,单击"脱敏白名单"。
- 5. 在白名单列表页面,单击"添加白名单"。
- 6. 在"添加白名单"对话框中,设置白名单范围,完成后单击"保存"。

数据源:	demo			
数据库用户名:	请输入			
IP范围 ①:	172.16.215.107		0	•
授权开始时间:	请选择日期	白		
授权结束时间:	请选择日期	Ë		
放行规则:	 全部规则 	指定规则		

支持配置的白名单参数包括数据库用户名、IP地址范围、开始时间、结束时间, 各参数为"且"的关系,若配置多参数个需同时命中,白名单方可生效。

步骤五:通过代理连接数据库

图 4-41 添加白名单

▲ 注意

此处以DBeaver工具为例,在实际使用过程中,您需要修改应用系统对接到数据库的 连接信息。

本文以DBeaver工具为例,通过代理连接到数据库。

Clinese 52.2	C SEPAR		××:	() silenas 0	×
	选择新连接类型 MySQL standard driver			Ramysourite Mysouramen Mysoura	n.
☐ E.e. *	Pyper part of distance/binds rame to the: New Q Schw Q ChickSchware C CORID E CDRID E > 5 DRIV > ✓ Defry	2	-	■ 取2 取220回 ■ 200 日本 100 日	
Project 11 Project 12	Or Lead Finebid 2 Trabid 2 Trabid 2 Trabid (CD) Orenegian 3 4 4 4 4 4 4 4 4 4 4 4 4 4			Lovel Clem 2 1872 Seven: MyCOL 57.33 log Diver: MyCOL 57.34 log Diver: MyC	×
Sol EX Diagrams g ^A Solpts 4	() (1-910 T-910 3451	Ra Incon	62)	() +1−010 T−010+ R04 R04)

图 4-42 通过代理连接数据库

- 1. 单击中图标。
- 2. 在选择新连接类型对话框中,选中MySQL。
- 3. 单击下一步。
- 在"设置MySQL连接"对话框中,设置连接信息。
 连接信息说明:
 - 服务器地址:使用数据库加密与访问控制系统的访问IP地址。例如 192.xx.xx.54。
 - 端口:使用代理端口,即创建资产时设置的代理端口(14099)。
- 5. 单击"测试链接",测试是否能够连接到数据库。
- 6. 测试通过后,单击"下一步",按照界面提示完成操作。

步骤六:验证脱敏结果

参考步骤五(通过代理连接数据库)操作连接数据库,验证脱敏规则及脱敏白名单是 否配置成功:

1. 用户的IP地址为172.16.215.108(非脱敏白名单中的地址),通过代理方式访问数 据库,只能查看到脱敏数据。

图 4-43 脱敏数据

	^{ABC} phone ∜ ‡	ABC tel 🛛 🟹 🕻	ABC email	۲:
1	158****8628	0571****500	and an index of the local sector	
2	183****8185	0571*****500	here and the second second	
3	170****7826	0571****500		

 用户的IP地址为172.16.215.107(脱敏白名单中的地址),通过代理方式访问数据 库,能查看到明文数据。

图 4-44 明文数据

	ABC phone 🏾 🕄 🕻	ABC tel 🛛 🟹 🕻	ABC email
1	1585 88628	0571-88 2500	and and a part of the second second
2	1833 88185	0571-88 2500	the second second second
3	1701 07826	0571-88 2500	and the second se

5 开通并使用数据库安全运维

5.1 步骤一: 购买数据库安全运维实例

本章节介绍如何购买数据库安全运维实例,数据库安全运维提供包年/包月计费方式。

须知

数据库安全运维功能现处于公测阶段,如需使用请<mark>提交工单</mark>申请开通数据库安全运维 功能。

约束与限制

数据库安全运维不支持跨区域(Region)使用。加密与访问的数据库必须和购买的实例在同一区域。

操作步骤

- 步骤1 登录管理控制台。
- 步骤3 在界面右上角,单击"购买数据库安全服务"。
- 步骤4选填购买相关信息。

图 5-1 基础配置

数据库安全加密 数据库安全运维
×
1, 可减少网络时延, 提高访问速度。
可用区2 可用区3 可用区4 可用区5 可用区6 可用区7
▶ ▶, 可减少网络时延, 提高访问速度, ▶ ▶ ▶ ▶ ■ <

表 5-1 基础配置参数说明

参数名称	参数说明			
服务类型	选择购买的实例类型。			
计费模式				
区域	选择实例的区域。不同区域的资源之间内网不互通,请 选择邻近的区域,可以降低网络时延、提高访问速度。			
项目	选择实例需要归属的项目,方便管理。			
可用区类型	根据实际情况选择可用区类型。			
可用区	可用区指在同一区域下,电力、网络隔离的物理区域, 可用区之间内网互通,不同可用区之间物理隔离。 支持部署在一个可用区。			

图 5-2 版本规格

版本规格

1资产量	3资产量	6资产量	10资产量
1并发数	3并发数	6并发数	10并发数

表 5-2 数据库安全运维版本性能规格说明

版本	支持的数据库实例	系统资源要求	性能参数
1资产量	只支持1个数据库	• CPU: 4U • 内存: 8GB	性能: 25000QPS最大并发连接数: 3000
3资产量	最多支持3个数据 库	• CPU: 4U • 内存: 8GB	性能: 25000QPS最大并发连接数: 3000

版本	支持的数据库实例	系统资源要求	性能参数
6资产量	最多支持6个数据 库	• CPU: 8U • 内存: 16GB	性能: 35000QPS最大并发连接数: 5000
10资产量	最多支持10个数据 库	• CPU: 8U • 内存: 16GB	性能: 35000QPS最大并发连接数: 5000

图 5-3 网络配置

网络配置

虚拟私有云

vpc-default 🗸		Q	新建虚拟私有云 🖸
---------------	--	---	-----------

建议VPC选择时,尽量与Agent安装节点所在VPC相同。

子网

subnet-default 🗸 🖓 新建子网 🖸

子网是虚拟私有云内的IP地址块,虚拟私有云中的所有云资源都必须部署在子网内。

~] Q

安全组

Sys-FullAccess	~	Q	新建安全组 🖸
----------------	---	---	---------

安全组用来实现安全组内和组间数据库安全服务的访问控制,加强数据库安全服务的安全保护。

分配lpv4地址

自动分配IP地址 V

弹性IP(可选)

--请选择--

表 5-3 网络配置参数说明

参数名称	参数说明
虚拟私有云	选择需要绑定的虚拟私有云。 虚拟私有云可以方便的管理、配置内部网络,进行安 全、快捷的网络变更,尽量与Agent安装节点所在VPC 相同。
安全组	安全组用来实现安全组内和组间数据库安全服务的访问 控制,加强数据库安全服务的安全保护。
子网	子网是虚拟私有云内的IP地址块,虚拟私有云中的所有 云资源都必须部署在子网内。 说明 子网具有物理地域属性:通用可用区不能使用边缘可用区的子 网,边缘可用区不能使用通用可用区的子网

参数名称	参数说明	
分配lpv4地址	选择Ipv4地址。	
弹性IP(可选)	选择绑定实例的弹性IP。	

图 5-4 高级配置和登录信息

へ 高级配置

实例名称

DBSS-f264

实例类型

主备

备注(可选)

请输入备注信息

登录信息

用户名

sysadmin

登录密码

Č	Ş
---	---

确认密码

Ø

表 5-4 高级配置和登录信息参数说明

参数名称	参数说明	取值样例
实例名称	自动生成,也可自定义名称。	-
实例类型	当前仅支持主备类型。	主备
备注(可选)	当前实例的备注信息。	-
用户名	默认生成的用户名。	sysadmin

参数名称	参数说明	取值样例
登录密码	设置登录实例的密码。	-
	说明 设置的登录密码需要满足以下几个条 件:	
	● 8~26个字符。	
	 至少包含以下字符中的2种:大写字母、小写字母、小写字母、数字和特殊字符~!@#\$%^&*()_+`=-[] {};':,".<>?/\。 	
	不能与用户名或倒序的用户名相 同。	
确认密码	输入确认密码,需要登录密码一 致。	-

图 5-5 购买时长

购买时长											
1个月	2个月	3个月	4个月	5个月	6个月	7个月	8个月	9个月	<mark>位</mark> 1年	2年	244 344
✔ 自动续费 了	W 扣费规则 和 续费	时长									

勾选"自动续费"后,当购买的数据库安全加密到期时,如果账号余额充足,DBSS将 自动为该实例续费,您可以继续使用该实例。自动续费的周期说明如<mark>表5-5</mark>所示。

表 5-5 自动续费周期说明

购买时长	自动续费周期
1/2/3/4/5/6/7/8/9个月	1个月
1/2/3年	1年

步骤5 确认当前配置无误后,单击"立即购买"。

如果您对价格有疑问,可以单击"了解计费详情",了解产品价格。

- **步骤6** 在"详情"页面,阅读《数据库安全服务声明》后,勾选"我已阅读并同意《数据库 安全服务声明》",单击"提交"。
- 步骤7 在购买页面,请选择付款方式进行付款。
 - 余额/在线支付
 您可以通过账户的余额进行支付,余额不足时,单击"充值"进行充值。
 - a. 选择"余额支付"。
 - b. 单击"确认付款",完成购买操作。
 - 申请线上合同请款后支付
 - a. 选择"申请线上合同请款后支付",单击"生成合同"。

b. 在页面中填写合同信息后,单击"创建正式合同",完成购买操作。

步骤8 成功付款后,在数据库安全运维实例列表界面,可以查看数据库安全运维实例的创建 情况。

----结束

5.2 步骤二:登录实例 web 控制台

管理员登录Web控制台后,可以管理和维护数据库运维安全管理系统。

前提条件

您已经从技术支持工程师处获取登录用户名和密码。

背景信息

出厂默认用户名和密码如下,具体实际用户名密码请从技术支持工程师处获取。

用户名	角色	说明
sysadmin	系统管理员	日常维护数据库运维安全管理系统,例如配置数据资 产、配置防护策略、查看审计日志等。
		默认密码为购买实例时设置的密码,首次登录进行重 置密码。
		具体操作,请参见 <mark>系统管理员操作指南</mark> 。
secadmi n	安全管理员	系统管理数据库运维安全管理系统,例如人员管理、 系统配置等。
		默认密码为购买实例时设置的sysadmin用户密码相 同,首次登录进行重置密码。
		具体操作,请参见 <mark>安全管理员操作指南</mark> 。
audadmi	审计管理员	对数据库运维安全管理系统进行审计,保障合规性。
		默认密码为购买实例时设置的sysadmin用户密码相 同,首次登录进行重置密码。
		具体操作,请参见 <mark>审计管理员操作指南</mark> 。
datadmi n	数据库操作员	数据库运维人员,通过安全客户端进行日常运维;通 过运维工单申请高风险操作。
		默认密码为购买实例时设置的sysadmin用户密码相 同,首次登录进行重置密码。
		具体操作,请参见 <mark>数据库操作员操作指南</mark> 。

表 5-6 权限说明

操作步骤

步骤1登录实例。

文档版本 01 (2024-11-28)

- 方式一:登录服务管理控制台,进入数据库运维页面,在目标实例"操作"列单击"远程登录"或"本地登录"。
- 方式二:通过方式一进入的数据库运维页面获取"弹性IP",在浏览器地址栏中 输入访问地址,按回车键,进入登录界面。
 访问地址:https://服务器弹性IP地址:端口,例如https://100.xx.xx.54:18443。
- 步骤2 (可选)在安全告警页面,单击"高级"。

图 5-6 安全告警

▲ 不安全 https://1	00
	您的连接不是私密连接
	攻击者可能会试图从 1 9 窃取您的信息(例如:密码、通讯内容或信用卡信息)。了解详情
	NET::ERR_CERT_AUTHORITY_INVALID
	Q 如果您想获得 Chrome 最高级别的安全保护,请 <u>开启增强型保护</u>
	高级

步骤3 (可选)在详情说明区域单击"继续前往xx.xx.xx.(不安全)"。

图 5-7 进入登录页面

隐藏详情	返回安全连接
此服务器无法证明它是1); 您计算机的操作系统不信任其安全证的原因可能是配置有误或您的连接被拦截了。	E书。出现此问题
继续前往1 9 (不安全)	

- 步骤4 进入登录页面后,输入"用户名"、"密码",单击"登录"。
- 步骤5 登录成功后,您可以进入Web控制台,查看和配置数据库运维安全管理系统。

🗀 说明

初次登录系统,您需要修改默认密码。具体操作请参见<mark>修改登录密码</mark>。

----结束

修改登录密码

步骤1 在Web控制台,单击右上角的用户名,在下拉框中单击"修改密码"。

图 5-8 修改密码

Sysadmin
☆ 修改密码
G 退出

步骤2 在修改密码对话框中,修改密码并单击"确定"。

参数	说明
原密码	输入原来的登录密码。
新密码	输入修改后的新密码。
	说明 为了登录安全,建议您将密码设置成复杂密码,例如包含以 下多种字符组合:
	● 大写字母(从A到Z)
	● 小写字母(从a到z)
	● 数字(0~9)
	 ● 特殊符号(例如:!@ # \$)
确认密码	重新输入修改后的新密码。

表 5-7 参数说明

步骤3 修改完成后,您需要退出Web控制台,使用新密码重新登录。

----结束

5.3 步骤三:系统功能配置及使用场景举例

5.3.1 快速使用指南

5.3.1.1 运维人员操作管理体系流程

数据库运维安全管理系统设置了完善的运维人员操作管理体系,流程如<mark>图</mark>5-9所示。



图 5-9 运维人员操作管理流程

- 安全管理员需先添加审批人(系统管理员)与申请人(数据库操作员)账号。具体说明请参见手动创建账号。
- 2. 新增的账号需先经安全管理员审核通过。具体说明请参见审核账号。
- 安全管理员设置审批架构,设置审批人与申请人。具体说明请参见设置审批架构。
- 系统管理员需给目标资产开启Web认证,以便后续能给数据库操作员进行资产认证授权。具体说明请参见添加数据资产。
- 系统管理员添加数据资产账号信息,用于给数据库操作员资产认证授权。具体说 明请参见**手动添加账号**。
- 系统管理员找到目标数据库操作员,并进行资产授权操作。具体说明请参见管理 运维人员。
- 7. 随后数据库操作员对目标资产发起运维工单申请。具体说明请参见发起运维工单 申请。
- 8. 对应系统管理员(审批人)审批工单申请。具体说明请参见<mark>审批运维工单</mark>。
- 审批通过,数据库操作员需先登录系统,随后可以通过安全客户端或本机其他数据库客户端进行操作。具体说明请参见通过Web安全客户端访问资产。

5.3.1.2 策略应用流程

数据库运维安全管理系统支持多种策略的设置与应用,以实现各种数据级的访问控制,策略应用流程如<mark>图5-10</mark>所示。

图 5-10 策略应用流程



- 1. 系统管理员添加数据资产,并进行相应设置。具体说明请参见<mark>添加数据资产</mark>。
- 进行防护策略设置,包括策略基本配置、集合配置、自定义策略(SQL策略、包 过滤策略、客户端语句过滤白名单)、设置虚拟补丁。具体说明请参见策略设 置。
- 3. 勾选要启用的策略并应用使之生效。具体说明请参见管理基本配置。
- 在后续操作中,您可在审计日志中查看到命中策略的记录。具体说明请参见查看 审计日志信息。

5.3.2 反向代理部署配置举例

反向代理模式,数据库运维安全管理系统通过代理资产进行安全防护。本示例组网情况如<mark>图1反向代理组网</mark>所示。
图 5-11 反向代理组网



表 5-8 组网说明

设备	说明
客户端	IP地址: 192.168.1.10
数据库运维安全管理系统	IP地址: 192.168.12.59
MySQL数据库	• IP地址: 192.168.11.78
	● 数据库版本:MySQL 5.7

设置反向代理模式

- 步骤1 使用安全管理员secadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,单击"设备管理 > 模式设置",在"模式选择"处选择反向代理,单击"保存"。

----结束

添加数据资产

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"资产管理>资产配置",在页面右上角单击"添加"。
- 步骤3 在"添加资产"对话框中,配置资产信息。

图 5-12 添加数据资产

添加资产						×
*资产名称:	demo	*资产类型:	MySQL			
* 资产IP:	192.168.11.78	*资产端口:	3306			
*数据库/实例名:	employees	* 数据库账号:	employees	* 数据库密码:	•••••	
web认证:		误删恢复配置	: 💽			
部署模式:	反向代理	* 端口 ②:	9587			
L						
					测试连接 保存	取消

□□ 说明

记录反向代理使用的端口号(9587),后续需要通过设备地址+代理端口访问数据资产。 步骤4 单击"保存",完成数据资产的配置信息。

----结束

通过代理连接数据库

本文以"DBeaver工具"为例,通过数据库运维管理系统代理连接到数据库。

- 步骤1 单击"DBeaver工具"的 ₩ 图标,在选择"新连接类型"对话框中,选中 "MySQL",单击"下一步"。
- **步骤2** 在设置MySQL连接对话框中,设置连接信息。配置信息如<mark>图4 通过代理连接数据库</mark>所示,其中:
 - 服务器地址:使用代理服务器IP,即数据库运维安全管理系统的访问IP地址。例如 192.168.12.59。
 - 端口:使用代理端口,例如9587。

图 5-13 通过代理连接数据库



步骤3 单击"测试链接",测试是否能够连接到数据库。

步骤4 测试通过后,单击"下一步",按照界面提示完成操作。

----结束

验证配置效果

使用系统管理员账号登录数据库运维管理系统,您可以查看到审计日志信息。

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"审计日志 > 日志检索"。
- 步骤3 单击"SQL日志"页签,单击"最新日志",查看最新的审计日志信息。如图5 查看审 计日志所示,数据库运维安全管理系统已经可以审计到业务日志。

图 5-14 查看审计日志

数据库用户	资产客户端IP	策略	风险级别	操作	数据库IP	捕获时间
root	192.168.1.10	全部审计	无风险	LOGOUT	192.168.11.78	2021-11-15 16:51:03
root	192.168.1.10	全部审计	无风险	LOGIN	192.168.11.78	2021-11-15 16:51:03
- management	THE R. LEWIS	1000	in stars	10.04	10.0001-001	100 Cold 100 Cold 10
	manual second	-	1000	10.000	100.00010.000	and included as
	1000 MR	and the second	1000	10.000	100.000.0000	and the second second

----结束

5.3.3 自定义策略阻断举例

此示例展示在反向代理的系统部署模式下,配置自定义策略。如果访问行为匹配策略,则根据策略执行操作。

本示例组网情况如下图1反向代理组网所示。

图 5-15 反向代理组网



表 5-9 组网说明

设备	说明
客户端	IP地址: 192.168.1.10
数据库运维安全管理系统	IP地址: 192.168.12.59
MySQL数据库	● IP地址: 192.168.11.78 ● 数据库版本: MySQL 5.7

添加数据资产

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"资产管理 > 资产配置"。
- 步骤3 单击页面右上角"添加",在添加资产对话框中,设置资产信息。

图 5-16 添加数据资产

添加资产							×
* 资产名称:	demo	*资产类型:	MySQL				
* 资产IP:	192.168.11.78	* 资产端口:	3306				
* 数据库/实例名:	employees	* 数据库账号:	employees	* 数据库密码:	•••••		
web认证:		误删恢复配置					
部署模式:	反向代理	∗ 端口 ⑦:	9587				
					测试连接	保存	取消

🛄 说明

请记录反向代理使用的端口号(9587),后续需要通过设备地址+代理端口访问数据资产。 步骤4 单击"保存",保存数据资产的配置信息。

----结束

添加自定义策略

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"策略防护>策略定义"。
- 步骤3 单击 "SQL策略" 页签新增一个策略组,在策略组列表区域,添加策略组。
- 步骤4 单击"添加策略组",在弹出对话框配置策略组名称、基于策略组,单击"确定"。

图 5-17 新建策略组

添加策略组			×
* 名称:	demo		
* 基于:	新建	~	
		取消	确定

步骤5 创建完成后,可单击策略组名称修改策略信息,修改完成后单击右上角"保存"。 **步骤6** 单击目标策略组,单击 + 图标,设置策略名称和类型,单击"确定"。

图 5-18 添加策略

添加策略			×
* 名称:	test		
* 类型:	默认	~	
		取消 确?	Ē

步骤7 单击策略名称,在策略详情页面修改策略信息,如图5-19所示,表示禁止root用户访问user表。

图 5-19 配置策略内容

基本信息					
策略名称: test		* 风险等级: 高风险 v	* 响应动作: 阻断		v
记录日志: 🔵		锁定访问:			
资产信息(源)					
资产客户端IP:	包含任意 🗸 🗸	请输入	主机名:	包含任意 🗸 🗸	诗输入
操作系统用户:	包含任意 🗸 🗸	请输入	数据库用户:	包含任意 🗸 🗸	root ×
数据库用户组:	包含任意 🗸 🗸	请选择	资产客户端:	包含任意 🗸 🗸	请输入
资产客户端MAC:	请输入		应用客户端IP:	包含任意 🗸 🗸	请输入
应用用户组:	包含任意 >>	请输入	时间组:	包含任意 🗸 🗸	请输入
应用用户:	包含任意 >>	请输入			
目标信息					
目标表:	包含任意 🗸 🗸	user ×	数据库:	包含任意 🗸 🗸	请输入
影响行数:	等于 ~ ~	请输入	字段:	包含所有 🗸 🗸	请输入
表组:	包含所有 >	请洗择			

门 说明

在策略详情中可以从多个维度设置策略信息,包括策略基本信息、资产信息、目标信息、访问信 息和时间等。 步骤8 单击页面右上角"保存",完成保存策略信息。

----结束

使用自定义策略生效

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"策略防护>策略设置"。
- **步骤3** 单击"基本配置"页签。进入页面后,在当前已选择资产下拉栏中,选择目标资产后,勾选"SQL策略"。
- 步骤4 单击 [4]编辑图标, 勾选"策略组名称", 单击"确定"。
- 步骤5 单击页面右上角"策略应用",使配置生效。

门 说明

每次修改策略组,都需要在策略设置中单击策略应用,使策略修改生效。

```
----结束
```

通过代理连接数据库

本示例以"DBeaver工具"为例,通过数据库运维安全管理系统代理连接到数据库。

图 5-20 通过代理连按数据库	图 5-20	通过代理连接数据库
------------------	--------	-----------

DBeaver 5.0.2	· ② 创建新连接	– 🗆 X	- ◎ 创建新连接 - □ ×
文件(F) 編報(E) 导航(N) 捜索(A) S	<mark>选择新连接类型</mark> MySQL standard driver		は 選 MySQL 法接役置 MySQL 法接役置 MySQL 法接役置 MySQL 法接役目
General Ceneral	Type part of database/driver name to filter Name Support ChickHouse ChickHous	# ^ 2	常规 驱动器性 代理服务器IP和端口 服务器地址 192.168.12.59
	> ✓ Cordy Wh Exacol Wh Exacol With Findbird With State Blass (CSM) (C) Greenplum > [] H2		tocal Client: v で は数据库寄会 したは Client: マ で は数 ない ない ない
Project 23 DataSc Project 23 Project 24 Project 24	● Indomax ● Ingres 項目 General ⑦ 《上一步(8) 下步(N)> 死道(7) 取消	▼ ✓ 測試链接	

步骤1 单击"DBeaver工具"的 [4]图标,在选择新连接类型对话框中,选中"MySQL"。

步骤2 单击"下一步"。

步骤3 在设置MySQL连接对话框中,设置连接信息,如图5-20所示。

- 服务器地址:使用代理服务器IP,即数据库运维安全管理系统的访问IP地址。例如 192.168.12.59。
- 端口:使用代理端口,例如9587。

步骤4 单击"测试链接",测试是否能够连接到数据库。

文档版本 01 (2024-11-28)

步骤5 测试通过后,单击"下一步",按照界面提示完成操作。

----结束

验证配置效果

步骤1 在DBeaver工具上,通过以下命令查询数据库mysql的user表信息。

select user, host from mysql.`user`;

步骤2 如<mark>图5-21</mark>所示,查询操作被阻断。

图 5-21 查询 user 表及结果

 株●●②※□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□) → [Ag MySQL - test
 ▼ îm 获振库 > ② information_schema > ③ employees > ③ mysql > ③ performance_schema 	🛱 Error executing query 👩 — 🗆 X
> ② test > ③ test > ③ wordpress > 配用户 > 配语现员 > 配系统信息	② Query execution failed 原因: SQL 错误 [1064] [42000]: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'select user,host from mysqL'user` LIMIT 0, 200' at line 1
	後定 洋畑信息(D) >> のT select user, nost from mysql: user 「 MICA ー 7 - SUG 24(2)スレデビビス(Mica # C (2) で C (1) + Space)

- 步骤3 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤4 在左侧导航栏,选择"审计日志 > 日志检索"。
- 步骤5 单击 "SQL日志" 页签, 单击 "最新日志", 查看最新的审计日志信息。
- 步骤6 如图5-22所示,数据库运维安全管理系统已经可以审计到命中自定义策略的行为的日志。

图 5-22 查看审计日志

数据库用户	资产客户端IP	策略	风险级别	操作	数据库IP	捕获时间
root	192.168.1.10	全部审计	无风险	SHOW	192.168.11.78	2021-11-16 10:40:49
root	192.168.1.10	demo	高风险	SELECT	192.168.11.78	2021-11-16 10:40:49
100	10.000	1000	100	1000	100.00	2010/07/07 00:000
100	The second second	Terr		10.00	ALC: NO. OF STREET, ST	April 11 March 1

⁻⁻⁻⁻结束

5.3.4 客户端语句过滤白名单配置举例

此示例中通过配置客户端语句过滤白名单,如果流量匹配策略,则过滤目标审计日 志。

本示例组网情况如<mark>图1 反向代理组网</mark>所示。

图 5-23 反向代理组网



表 5-10 组网说明

设备	说明
客户端	IP地址: 192.168.1.10
数据库运维安全管理系统	IP地址: 192.168.12.59
MySQL数据库	IP地址: 192.168.11.78数据库版本: MySQL 5.7

添加数据资产

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,选择"资产管理 > 资产配置",在页面右上角单击"添加"。
- 步骤3 在添加资产对话框中,配置资产信息。

图 5-24 添加数据资产

添加资产								×
*资产名称:	demo	* 资产类型:	MySQL					
* 资产IP:	192.168.11.78	*资产端口:	3306					
*数据库/实例名:	employees	* 数据库账号:	employees		* 数据库密码:	•••••		
web认证:		误删恢复配置:						
部署模式:	反向代理	* 端口 ②: 〔	9587]				
						测试连接	保存	取消

🗀 说明

记录反向代理使用的端口号(9587),后续需要通过设备地址+代理端口访问数据资产。

步骤4 单击"保存",完成数据资产的配置信息。

----结束

通过代理连接数据库

本文以"DBeaver工具"为例,通过数据库运维安全管理系统代理连接到数据库。

- **步骤1** 单击"DBeaver工具"的<mark>计</mark>图标,在选择新连接类型对话框中,选中MySQL,单击下 一步。
- **步骤2** 在设置MySQL连接对话框中,设置连接信息。配置信息如<mark>图4 通过代理连接数据库</mark>所示,其中:
 - 服务器地址:使用代理服务器IP,即数据库运维安全管理系统的访问IP地址。例如 192.168.12.59。
 - 端口:使用代理端口,例如9587。

图 5-25 通过代理连接数据库



步骤3 单击测试链接,测试是否能够连接到数据库。

步骤4 测试通过后,单击下一步,按照界面提示完成操作。

----结束

生成客户端语句

- 步骤1 在DBeaver工具上连接数据资产。
- 步骤2 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤3 在左侧导航栏,选择"审计日志 > 日志检索"。
- **步骤4** 单击"SQL日志"页签,单击最新日志,查看最新的审计日志信息,连接数据库时审计12条日志。

文档版本 01 (2024-11-28)

图 5-26 查看日志

数据库用户	资产客户端IP	策略	风险级别	操作	数据库IP	捕获时间
root	192.168.1.10	全部审计	无风险	SELECT	192.168.11.78	2021-11-16 14:23:53
root	192.168.1.10	全部审计	无风险	SELECT	192.168.11.78	2021-11-16 14:23:53
root	192.168.1.10	全部审计	无风险	SHOW	192.168.11.78	2021-11-16 14:23:53
root	192.168.1.10	全部审计	无风险	SHOW	192.168.11.78	2021-11-16 14:23:53
root	192.168.1.10	全部审计	无风险	SHOW	192.168.11.78	2021-11-16 14:23:53
root	192.168.1.10	全部审计	无风险	SET	192.168.11.78	2021-11-16 14:23:53
root	192.168.1.10	全部审计	无风险	SET	192.168.11.78	2021-11-16 14:23:53
root	192.168.1.10	全部审计	无风险	SET	192.168.11.78	2021-11-16 14:23:53
root	192.168.1.10	全部审计	无风险	SET	192.168.11.78	2021-11-16 14:23:53
root	192.168.1.10	全部审计	无风险	SHOW	192.168.11.78	2021-11-16 14:23:53
root	192.168.1.10	全部审计	无风险	SELECT	192.168.11.78	2021-11-16 14:23:53
root	192.168.1.10	全部审计	无风险	LOGIN	192.168.11.78	2021-11-16 14:23:53

步骤5 单击"详情",查看第一个SET操作日志信息,SQL内容如<mark>图5-27</mark>所示,记录SQL模式 描述: "SET NAMES utf8mb4"。

图 5-27 SET 的 SQL 内容

匹配的策略:	全部记录:无风险;
SQL内容:	SET NAMES utf8mb4
SQL结果内容:	
SQL模式:	SET NAMES utf8mb4

----结束

添加客户端过滤白名单

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"策略防护>策略定义"。
- 步骤3 单击"客户端语句过滤白名单"页签,进入页面后,单击"添加"。
- 步骤4 在添加客户端语句过滤白名单对话框中,添加过滤信息。

图 5-28 添加过滤信息

添加客户端语句过》	包名单	×
* SQL:	SET NAMES utf8mb4	
		11
* 工具:	dbeaver	
		10
数据库:	MySql	\vee
状态:	启用	\sim
		取消 确定

步骤5 单击"确定",完成过滤信息添加操作。

----结束

配置策略生效

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"策略防护 > 策略设置"。
- 步骤3 单击"基本配置"页签。在当前已选择资产中,选择目标资产并勾选"SQL策略"。
- **步骤4**单击¹²编辑图标,勾选客户端语句过滤白名单。
- **步骤5**单击"确定",单击右上角"策略应用",使配置生效。 ----结束

验证配置效果

- 步骤1 在DBeaver工具上重新连接数据资产。
- **步骤2** 在日志检索页面查看审计日志,如所示,登录审计信息为11条,有一条SET操作已经被 过滤。

图 5-29 查看过滤效果

数据库用户	资产客户端IP	策略	风险级别	操作	数据库IP	捕获时间
root	192.168.1.10	全部审计	无风险	SELECT	192.168.11.78	2021-11-16 14:55:22
root	192.168.1.10	全部审计	无风险	SELECT	192.168.11.78	2021-11-16 14:55:22
root	192.168.1.10	全部审计	无风险	SHOW	192.168.11.78	2021-11-16 14:55:22
root	192.168.1.10	全部审计	无风险	SHOW	192.168.11.78	2021-11-16 14:55:22
root	192.168.1.10	全部审计	无风险	SHOW	192.168.11.78	2021-11-16 14:55:22
root	192.168.1.10	全部审计	无风险	SET	192.168.11.78	2021-11-16 14:55:22
root	192.168.1.10	全部审计	无风险	SET	192.168.11.78	2021-11-16 14:55:22
root	192.168.1.10	全部审计	无风险	SET	192.168.11.78	2021-11-16 14:55:22
root	192.168.1.10	全部审计	无风险	SHOW	192.168.11.78	2021-11-16 14:55:22
root	192.168.1.10	全部审计	无风险	SELECT	192.168.11.78	2021-11-16 14:55:22
root	192.168.1.10	全部审计	无风险	LOGIN	192.168.11.78	2021-11-16 14:55:22

----结束

5.3.5 虚拟补丁防护配置举例

虚拟补丁规则功能是通过内置数据库特征漏洞库信息,并将其转化为防护特征攻击的 特征策略,对命中策略的攻击进行虚拟补丁拦截防护。

组网需求





表 5-11 组网参数说明

设备	说明
客户端	IP地址: 172.16.196.33
数据库运维安全管理系统	IP地址: 172.16.47.58
Oracle数据库	• IP地址: 172.16.32.41
	● 数据库版本: Oracle 11

添加数据资产

步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。

步骤2 在左侧导航栏,选择"资产管理 > 资产配置"。

步骤3 单击右上角的"添加"。

步骤4 在添加资产对话框中,设置资产信息。

图 5-31 添加数据资产

添加资产							×
*资产名称:	demo	* 资产类型:	Oracle \lor				
* 资产IP:	172.16.47.58	*资产端口:	1521				
数据库/实例名:	dbsrv2	数据库账号:	sys as sysdba	数据库密码:	•••••		
web认证:		误删恢复配置: 🔵					
部暋模式:	反向代理	* 端口 ⑦:	9001				
RAC:							
					测试连接	保存	取消

🛄 说明

请记录反向代理使用的端口号(9001),后续需要通过设备地址+代理端口访问数据资产。

步骤5 单击"保存",保存数据资产的配置信息。

----结束

应用虚拟补丁策略

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,选择"策略防护 > 策略设置"。
- 步骤3 单击"基本配置"页签。
- 步骤4 在当前已选择资产中,选择目标资产。
- 步骤5 勾选启用虚拟补丁。
- **步骤6**单击^[2]编辑图标。
- 步骤7选择风险等级。
- **步骤8**单击"确定"。
- 步骤9 单击右上角的"策略应用",使配置生效。

----结束

文档版本 01 (2024-11-28)

验证配置效果

步骤1 通过代理方式连接数据库。具体操作,请参见通过代理连接数据库。

步骤2 执行以下命令,注入SQL语句。

select SYS.KUPP\$PROC.CREATE_MASTER_PROCESS.CHANGE_USER from dual;

步骤3 使用系统管理员sysadmin账号登录数据库运维管理系统。

步骤4 在"审计日志 > 日志检索"页面,查看审计日志。

图 5-32 查看审计日志

SYS	172.16.196.33	默认策略	无风险	BEGIN	通过	172.16.47.58	2022-04-22 17:49:08
SYS	172.16.196.33	虚拟补丁	高风险	SELECT	通过	172.16.47.58	2022-04-22 17:49:08

图 5-33 查看日志详情

查看详情					Х
资产名称:	数据库:		数据库用户:	10.0	
数据库IP:	资产客户端:	2010.000	资产客户端IP:	0.004.0	
资产客户端端口:	操作:	0.00	执行时长 (窒秒)) :	
动作:	记录方式:	总是记录	风险等级:	高风险	
影响/返回行数: -	捕获时间:	2024-03-06 10:33:03	主机名:	-	
操作系统用户: -	会话ID:	1.000000	操作对象:	-	
匹配的策略: 入侵[SQL注入]->SYS.KUPP\$PROC包	回中存在权限提升漏洞:	高风险;			
SQL内容:					
SQL结果内容:					
SQL模式:					

----结束

5.3.6 业务字典配置举例

该模块可配置业务字段,配置的业务名称可以用来翻译日志中的信息。可添加业务字 典的项有IP、账号、操作、操作对象。添加的业务字典都可进行编辑和修改。

组网需求



表 5-12 组网说明

设备	说明
客户端	IP地址: 192.168.1.10
数据库运维安全管理系统	IP地址: 192.168.12.59
MySQL数据库	• IP地址: 192.168.11.78
	● 数据库版本: MySQL 5.7

添加数据资产

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"资产管理 > 资产配置"。
- 步骤3 单击右上角的"添加"。
- 步骤4 在添加资产对话框中,设置资产信息。

图 5-35 添加数据资产

添加资产								Х
*资产名称:	demo	*资产类型:	MySQL					
* 资产IP:	192.168.11.78	* 资产端口:	3306					
* 数据库/实例名:	employees	* 数据库账号:	employees		* 数据库密码:	•••••		
web认证:		误删恢复配置	: 💽					
部署模式:	反向代理	* 端口 ②:	9587					
				1				
						测试连接	保存	取消

🛄 说明

请记录反向代理使用的端口号(9587),后续需要通过设备地址+代理端口访问数据资产。 步骤5 单击"保存",保存数据资产的配置信息。

----结束

产生审计日志

- 步骤1 通过代理方式连接数据库。具体操作,请参见通过代理连接数据库。
- **步骤2**执行以下命令。 SELECT * FROM wp_users;
- 步骤3 使用系统管理员账号 (例如sysadmin)登录数据库运维安全管理系统。
- 步骤4 在"审计日志 > 日志检索"页面,查看审计日志。

图 5-36 查看日志

数据库用户	资产客户端IP	策略	风险级别	操作	数据库IP	捕获时间
root	192.168.1.10	全部审计	无风险	SHOW	192.168.11.78	2021-11-16 15:35:36
root	192.168.1.10	全部审计	无风险	SELECT	192.168.11.78	2021-11-16 15:35:36
100		1000			10000	10000
100	1000	1000		10.00	100000	101010-0012-000

----结束

添加业务字典翻译

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,选择"审计日志 > 业务字典"。
- 步骤3 配置客户端和服务端IP的业务字典。
 - 1. 单击IP页签。
 - 2. 单击"添加",配置服务器IP的业务字典,单击"确定"。

图 5-37 服务器 IP 业务字典

添加IP翻译		×
* IP地址:	192.168.11.78	
* IP类型:	服务端IP	
* 业务名称:	网站数据库	
状态:		
	取消	确定

3. 单击"添加",配置客户端IP的业务字典,单击"确定"。

图 5-38 客户端 IP 业务字典

添加IP翻译		×
* IP地北:	192.168.1.10	
* IP类型:	客户端IP	
* 业务名称:	测试部门	
状态:		
	取消	〕定

步骤4 配置操作的业务字典。

- 1. 单击操作页签。
- 2. 单击"添加",配置操作的业务字典,单击"确定"。

图 5-39 服务器 IP 业务字典

添加操作翻译		×
* 数据库类型:	SQL V	
* 操作:	SELECT V	
* 业务名称:	查询	
	取消	确定

步骤5 在左侧导航栏,选择"审计日志 > 业务字典"设置。

步骤6 开启业务IP和业务操作开关。

图 5-40 开启开关

业务字典开关	
业务IP	
业务账号	
业务操作	
业务操作对象	

----结束

验证配置效果

步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。

步骤2 在"审计日志 > 日志检索"页面,查看到业务字典翻译后的审计日志。

图 5-41 查看日志

数据库用户	资产客户端IP	策略	风险级别	操作	数据库IP	捕获时间
root	测试部门())	全部审计	无风险	SHOW	网站数据库()	2021-11-16 16:22:52
root	测试部门()	全部审计	无风险	查询(SELECT)	网站数据库()	2021-11-16 16:22:52

步骤3 单击目标审计日志栏的详情,查看到业务字典翻译后的日志详情。

图 5-42 查看日志详情

查看详情						×
资产名称:	demo	数据库:	dur-2	数据库用户:	212	
数据库IP:	网站数据库()	资产客户端:	DBeaver 6.1	资产客户端IP:	测试部门(
资产客户端端口:	42744	数据库MAC:	00-00-00-00-00	资产客户端MAC:	00-00-00-00-00	
操作:	查询(SELECT)	执行时长 (窒秒)	:1	动作:	通过	

----结束

5.3.7 Web 安全客户端配置举例

数据库运维安全管理系统为用户提供Web认证功能,资产开启Web认证后,未经过认 证的数据库客户端不可访问该资产。数据库操作员可以先登录数据库运维安全管理系 统,随后通过Web安全客户端或本机上的数据库客户端访问该资产。

组网需求



表 5-13 组网说明

设备	说明	
客户端	IP地址: 192.168.1.10	
数据库运维安全管理系统	IP地址: 192.168.12.59	
MySQL数据库	• IP地址: 192.168.11.78	
	● 数据库版本: MySQL 5.7	

添加数据资产

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"资产管理 > 资产配置"。
- 步骤3 单击右上角的"添加"。
- 步骤4 在添加资产对话框中,设置资产信息和反向代理部署模式并开启web认证。

图 5-44 添加数据资产

添加资产						×
*资产名称:	demo	*资产类型:	MySQL V			
* 资产IP:	192.168.11.78	*资产端口:	3306			
* 数据库/实例名:	employees	* 数据库账号:	employees	* 数据库密码:	•••••	
web认证:		误删恢复配置	:			
部署模式:	反向代理	* 端□ ②:	9587			
					测试连接 保存	取消

步骤5 单击"保存",保存数据资产的配置信息。

----结束

添加账号信息

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"资产管理 > 账号管理"。
- 步骤3 单击右上角的添加账号。
- 步骤4 在新增账号对话框中,选择资产和对应的账号信息。
- 步骤5 配置完成后,单击测试链接,检查数据库是否能够连接。
- 步骤6 测试通过后,单击"保存",保存账号信息。

----结束

关联数据库操作员和资产账号

🛄 说明

此处以默认数据库操作员账号(datadmin)为例,实际场景中您需要为每个数据库操作员单独 创建账号。

- 步骤1 在左侧导航栏,选择"运维管理 > 人员管理"。
- 步骤2 找到目标数据库操作员,单击"配置中心"。
- 步骤3 在账号设置对话框中,开启授权状态、密码代填并选择账号。

----结束

验证配置效果

步骤1 数据库操作员未登录数据库运维安全管理系统,使用本机上的DBeaver通过代理服务器访问数据资产,此时被阻断。操作详情请参见通过代理连接数据库。

图 5-45 客户端访问结果

连接设置

MySQL 8+ 连接设置

ſ	NysqL.

0

常规 驭	动属性	
服务器地址	: 192.168.12.59	
端口	9587	
<i>ြ</i> 连接	古误	– 🗆 🗙
8	Can not read response from server. Exper read 0 bytes before connection was unexp	cted to read 4 bytes, pectedly lost.
Advanced	settings:	网络设置(SSH、SSL、Proxy)
		连接详情(名称、类型)
驱动名称:	MySQL 8+	编辑驱动设置

步骤2 使用数据库操作员账号 (例如datadmin) 登录数据库运维管理系统。

步骤3 随后使用安全客户端或本机上的数据库客户端成功连接访问数据库。

• 使用安全客户端

在左侧导航栏,单击选择"运维管理 > 安全客户端",在安全客户端页面,可以 访问查看资产中信息。

图 5-46 查看资产信息

 № wordpress@192.168.11.78-mysql ◆ 団 数据库 	📰 wp_users 🏾 📰 wp_c	omments		
 information_schema wordpress 	Properties 🎛 Data			
✓ 由表	Enter a SQL expression to filte	r results		
wp_commentmeta	# 123 comment_ID It	123 comment_post_ID 41	RBC comment_author It	RBC comment_author_email
m wp_links	1 1	1	一位WordPress评论者	wa*uu@wordpress.example
● wp_postmeta ● wp_posts ● wp_term_relationships ● wp_term_relationships ● wp_terms ● wp_uterms ● wp_uterms ● wp_usermeta ● wp_users ● so 视题 > so 视题 > ● 存在过程 > ● 经过路 > ● Events				
> 🛐 用户 > 🛅 系统信息				

 使用本机上的客户端工具 成功连接数据库。

图 5-47 客户端连接成功

连接设置 MySQL 8+ 道	接设置			M	JSQL.
常规 驱动	属性				
服务器地址:	192.168.12.59				
端口:	9587]			
/2 成功					
U Driv 6d4 已道	ver: MySQL Conn leaa273bc181b4d 註接 (193 ms)	ector/J mysql-connecto f1c8ad0821a2227f116f	r-java-8.0. edf)	11 (Revisi	ion: 确定
Advanced se	ettings:		网络设置(连接	SSH、SSL 新情(名称	.、Proxy) 、
驱动名称: My	ySQL 8+			编	輯驱动设置

----结束

5.3.8 工单审批配置举例

对于超出一般访问控制权限以外的运维操作,运维人员如确需执行的,数据库运维安 全管理系统还提供了工单审批机制。运维人员可以预先将需要操作的语句、脚本、对 象以及所需要的权限填入工单进行申请,由系统指定的审批人员批准之后,方可在指 定的时间窗口内进行。

操作完成后权限自动收回,完美兼顾安全和业务。

说明:此项功能配置需要datadmin,sysadmin,secadmin三个角色的管理员配合操 作。

- datadmin:数据库运维人员,通过安全客户端进行日常运维;通过运维工单申请 高风险操作。需要工单申请菜单权限。
- sysadmin:系统管理员,日常维护数据库运维安全管理系统,例如配置数据资 产、配置防护策略、审批运维工单、查看审计日志等。需要资产管理、策略防 护、工单审批、审计日志等菜单权限。
- secadmin:安全管理员,系统管理数据库运维安全管理系统,例如人员管理、系统配置等。需要审批架构的菜单权限。

组网需求

图 5-48 反向代理组网



表 5-14 组网说明

设备	说明
客户端	IP地址: 172.16.197.57
数据库运维安全管理系统	IP地址: 172.16.35.212
MySQL数据库	• IP地址: 172.16.47.63
	● 数据库版本: MySQL 5.7

添加数据资产

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"资产管理 > 资产配置"。
- 步骤3 单击右上角的"添加"。
- 步骤4 在添加资产对话框中,设置资产信息和反向代理部署模式并开启web认证。

图 5-49 添加数据资产

添加资产							×
* 资产名称:	mysql_172.16.47.63	*资产类型:	MySQL v				
* 资产IP:	172.16.47.63	*资产端口:	6003				
数据库/实例名:		数据库账号:		数据库密码:			
web认证:		误删恢复配置:					
部署模式:	反向代理	* 端口 ②:	9018				
					测试连接	保存	取消

步骤5 单击"保存",保存数据资产的配置信息。

----结束

添加账号信息

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"资产管理 > 账号管理"。
- 步骤3 单击右上角的添加账号。
- 步骤4 在新增账号对话框中,选择资产和对应的账号信息。
- 步骤5 配置完成后,单击测试连接,检查数据库是否能够连接。
- 步骤6 测试通过后,单击"保存",保存账号信息。

----结束

关联数据库操作员和资产账号

🛄 说明

此处以默认数据库操作员账号(datadmin)为例,实际场景中您需要为每个数据库操作员单独 创建账号。

- 步骤1 在左侧导航栏,选择"运维管理 > 人员管理"。
- 步骤2 找到目标数据库操作员,单击"配置中心"。
- 步骤3 在账号设置对话框中,开启授权状态、密码代填并选择账号。

----结束

添加自定义策略

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"策略防护 > 策略定义"。
- 步骤3 单击SQL策略页签。
- 步骤4 新增一个策略组,在策略组列表区域,添加策略组。

文档版本 01 (2024-11-28)

- 1. 单击"添加策略组"。
- 2. 设置策略组的名称和基于哪个策略组,单击"确定"。

图 5-50 新建策略组

添加策略组				×
* 名称:	demo			
* 基于:	新建	~		
		取	消	确定

3. 创建完成后,单击策略组名称,修改策略信息,单击右上角的"保存"。

步骤5 在策略组中添加新策略。

- 1. 鼠标移动到目标策略组,单击十添加图标。
- 2. 设置策略名称和类型,单击"确定"。

图 5-51 添加策略

添加策略					×
* 名称:	test				
* 类型:	默认		~		
			取	消	确定

步骤6 配置策略内容。

- 1. 单击策略组前面的 展开图标。
- 2. 单击策略名称,在策略详情页面修改策略信息。

在策略详情中可以从多个维度设置策略信息,包括策略基本信息、资产信息、目 标信息、访问信息和时间等。

图 5-52 配置策略内容

策略汇总						保存清空
基本信息						
策略名称: test			* 风险等级: 高风脸 🗸	* 响应动作: 阻断		
记录日志: 🔵		1	此定访问:			
资产信息(源)						
资产客户端IP:	包含任意		请输入	主机名:	包合任意 >	请输入
操作系统用户:	包含任意		请输入	数据库用户:	包含任意 🗸 🗸	请输入
数据库用户组:	包含任意		请选择	资产客户端:	包含任意 >	请输入
资产客户端MAC:	请输入			应用客户端IP:	包含任意 🗸 🗸	请输入
应用用户组:	包含任意		请输入	时间组:	包含任意 🗸 🗸	请输入
应用用户:	包含任意		请输入			
目标信息						
目标表:	包含任意	~	test ×	数据库:	包含任意 >	请输入
影响行数:	等于	v	请输入	字段:	包含所有 >>	请输入
表组:	包含所有		请选择			

3. 单击右上角的"保存",保存策略信息。

----结束

使自定义策略生效

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,选择"策略防护>策略配置"。
- 步骤3 单击基本配置页签。
- 步骤4 在当前已选择资产下拉栏中,选择目标资产。
- 步骤5 勾选SQL策略。
- **步骤6**单击^[2]编辑图标。
- 步骤7 勾选策略组名称。
- **步骤8**单击"确定"。
- 步骤9 单击右上角的策略应用,使配置生效。

🛄 说明

每次修改策略组,都需要在策略设置中单击策略应用,使策略修改生效。

----结束

安全管理员添加审批架构

- 步骤1 使用安全管理员secadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,选择"用户管理 > 审批架构"。
- 步骤3 单击右侧"添加"按钮。
- 步骤4 在添加成员信息弹框填写信息。
- 步骤5 单击右上角的"添加"。

🗀 说明

请先添加系统管理员审批人账号,随后添加数据库操作员申请人账号。

图 5-53	添加成员信息
--------	--------

◎○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○	查 数据库运维安全管理系统						û 🔹 secadmin∨
-	用户管理 / 审批编约						
	✓ 審批契約	成员列表					漢加 制除
	□ 审批人-sysadmin	R 9	使用人	相织角色	±8/]	10140	設作
日志设置 ~		datadmin	datadmin	(申请人)			4048 BSP:
⑦ 用户管理 *						忠共1:	♣ < 1 > 15 条/页 ∨
审批集构							
AD线管理							
LDAP管理							
2 系统运输 ~							

----结束

数据库操作员发起运维工单申请

- 步骤1 使用数据库操作员datadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"运维管理 > 工单申请"。
- 步骤3 单击"工单申请",在发起审批对话框中,设置工单信息。
- 步骤4 配置工单信息。

图 5-54 发起审批

* 申请名称:	申请工单					
*资产名称:	mysql_172.16.47.63 ×		数据库实	例名: 请输入		
客户端工具:	请输入		客户	端IP: 172.16.197.5	7	
是否开启授权码: (X		* 申请操作	时间: 2024-02-21	15:35:03 ~ 2024-	02-22 15:35:03
申请事由:	请输入		li.	备注: 请输入		
						添加
操作方式	操作语句	操作命令	操作对象-表	操作对象-列	SQL脚本	操作
常规操作		ALL	test			编辑 删除

步骤5 配置完成后,单击"提交"按钮,在确认提示框中单击"确定"。

----结束

系统管理员审批运维工单

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"运维管理 > 工单审批"。
- 步骤3 找到目标工单申请,进行审批。
- 步骤4 在编辑审批对话框中,设置审批意见,并单击"同意"(或驳回)。

🛄 说明

如果审批同意,运维操作员可以进行后续运维操作。如果被驳回,运维操作员无法进行后续运维 操作。

图 5-55 登录 Web 控制台

编辑审批					×
* 申请名称:	申请工单				
* 资产名称:	mysql_172.16.47.63		数据库实例名:		
客户端工具:			客户端IP:	172.16.197.57	
是否开启授权码:			*申请操作时间:	2024-02-21 15:35:03 ~ 2024-	02-22 15:35:03 📋
申请事由:			备注:		li.
* 审批意见:					lo
操作方式	操作语句	操作命令	操作对象-表	操作对象-列	SQL脚本
常规操作		ALL	test		
				同意	驳回 取消

----结束

验证配置效果

- 步骤1 使用数据库操作员datadmin账号登录数据库运维管理系统。
- **步骤2** 使用本机上的DBeaver通过代理服务器访问数据资产中test表,如果审批通过此时可正常访问。

操作详情请参见通过代理连接数据库。

图 5-56 客户端访问结果

	test ×						-					
■	🚍 属性 🔜 数据 🚠 ER 图											
	田test は ふ ふ 一个 SQL 表达式来过滤结果 (使用 Ctrl+Space) 日本 マ → マ											
架		12🛃 id 🛛 💌	ABC prefecture	RBC Home_return_permit 🔹 💌	ABC Sex 🔍 💌	🕫 National 🛛 💌	ADC county					
×.	1	1	和静县	M92386054	男	京族	资阳					
▦	2	2	甘德县	M48107235	女	德昂族	龙岩					
4	3	3	昌江黎族自治县	M57036298	男	朝鮮族	黑河					
₽Ř	4	4	酉阳土家族苗族自治县	M29716830	女	藏族	海西					
÷	5	5	永登县	M37461925	女	普米族	阿坝					
	6	6	务川仡佬族苗族自治县	H94576028	男	布朗族	楚雄					
	7	7	会宁县	H97340586	男	纳西族	西宁					
	8	8	两当县	H51340867	女	基诺族	常德					
	9	9	莫力达瓦达斡尔族自治旗	M17054863	男	鄂伦春族	威海					
	10	10	金平苗族瑶族傣族自治县	H98631720	女	满族	常徳					
	11	11	乌拉特后旗	H56947318	女	仫佬族	吐魯番					
	12	12	秦安县	M34091528	男	俄罗斯族	南充					

步骤3 使用本机上的DBeaver通过代理服务器访问数据资产中test表,如果审批被驳回或同意后被撤销,此时会被阻断。

操作详情请参见通过代理连接数据库。

图 5-57 客户端访问结果

∃ 属性	■ 数据 品 ER 图	🖙 mysql 1 1 1
test	■ 【MAN MACH SQL 表达式来过滤结果 (使用 Ctrl+Space)	
\wedge	SQL 错误 [08S01]: Communications link failure	
	The last packet successfully received from the	Details >> 💧

文档版本 01 (2024-11-28)

6 升级数据库审计实例版本

本章节指导您如何升级您的数据库实例版本。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 数据库实例版本低于当前最新版本。

操作步骤

- 步骤1 登录管理控制台。
- 步骤3 在左侧导航树中,选择"实例列表",进入"实例列表"界面。
- 步骤4 在"版本"列单击"升级"。

图 6-1 升级实例版本



步骤5 在弹出的对话框中单击"是",开始实例版本升级。

-----结束

7 配置审计规则

7.1 添加审计范围

数据库安全审计默认提供一条"全审计规则"的审计范围,可以对成功连接数据库安 全审计的所有数据库进行安全审计。您也可以通过添加审计范围,设置需要审计的数 据库范围。

须知

全审计规则优先级高于自定义添加的审计范围规则,若您需要重新添加审计范围规则,请禁用"全审计规则"。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 请参考**开启数据库安全审计**成功开启数据库安全审计功能。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"审计规则"。
- 步骤4 在"选择实例"下拉列表框中,选择需要添加审计范围的实例。
- 步骤5 在审计范围列表框左上方,单击"添加审计范围"。

🛄 说明

- 数据库安全审计默认提供一条"全审计规则"的审计范围,可以审计所有连接数据库安全审 计实例的数据库。该审计规则默认开启,您只能禁用或启用该审计规则。
- 全审计规则优先级高于自定义添加的审计范围规则,若您需要重新添加审计范围规则,请禁用"全审计规则"。

步骤6 在弹出的对话框中,设置审计范围,如<mark>图7-1</mark>所示,相关参数说明如<mark>表7-</mark>1所示。

图 7-1 "	添加审计范围"对话框 围
* 名称	audit00
* 数据库名称	t × v
操作类型	□ 登录 □ 操作
数据库账户	
例/hP	请输入IP/IP段,多个请以换行符相隔,不可重复(默认全审计): 请输入IP/IP段
濵P	请输入IP/IP段,多个请以换行符相隔,不可重复(默认全审计): 请输入IP/IP段
源端口	请输入端口,多个请以换行符相隔,不可重复(默认全审计): 済输入IP端口
	(

表 7-1 审计范围参数说明

参数名称	说明	取值样例
名称	自定义审计范围的名称。	audit00
数据库名称	选择 "全部数据库" 或选择待添加审计范围的数据 库。	db03
数据库账户	可选参数。输入数据库的用户名。 可增加多个账户,多个账户间用逗号隔开。	-

取消)

确定

参数名称	说明	取值样例
操作类型	审计范围的操作类型,包括"登录"和"操作"。 当选择"操作"时,可以选择"全部操作",或选 择"数据定义"、"数据操作"或"数据控制"的 操作。	登录
数据库账户	可选参数。输入数据库的账户名。 可增加多个账户,多个账户间用逗号隔开。	-
例外IP	可选参数。输入不需要对数据库操作行为进行审计的IP地址。 说明 例外IP规则优先级高于源IP规则,当例外IP和源IP中填写的IP地址有重叠时,将不对重叠IP的数据库操作行为进	-
	行审计。	
源IP	可选参数。输入访问待审计数据库的IP地址或IP地 址段。 IP必须为内网IP地址,支持IPv4和IPv6格式。	-
源端口	可选参数。输入访问待审计数据库的端口。	-

步骤7 单击"确定"。

添加成功,审计范围列表新增一条状态为"已启用"的审计范围。

----结束

相关操作

除了添加数据库安全审计的审计范围,您还可以通过启用或禁用SQL注入检测,以及 添加风险操作,设置数据库安全审计的审计规则。

7.2 添加 SQL 注入规则

数据库安全审计提供"添加SQL注入规则",您可根据需要自定义添加对应的SQL规则,添加后可以对成功连接数据库安全审计的所有数据进行安全审计。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 请参考开启数据库安全审计成功开启数据库安全审计功能。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。

步骤3 在左侧导航树中,选择"审计规则"。

步骤4 在"选择实例"下拉列表框中,选择需要添加审计范围的实例。

步骤5 选择"SQL注入"页签。

🛄 说明

仅自定义创建的规则可以使用编辑和删除功能,默认的规则仅可使用启用和禁用功能。 步骤6 单击"添加SQL注入规则",在弹窗中填写相关信息。

图 7-2 添加 SQL 注入规则

添加SQL注入规则

★ 规则名称				
<mark>★</mark> 风险等级	ā	中	低	无风险
* 状态				
★ 正则表达式				
测试正则表达式				
原始数据			Mit	
结果				4

取消 确定

表 7-2 SQL 注入规则参数说明

参数名称	参数说明	取值样例
规则名称	目标SQL规则的名称,可自定义输入。	邮编SQL注入规则
风险等级	目标SQL规则的风险级别,可以选择以下 级别: • 高 • 中 • 低 • 无风险	中
状态	开启或关闭当前SQL注入规则。 • : 开启 • - : 关闭	

参数名称	参数说明	取值样例
正则表达 式	目标SQL规则采用正则表达式检测的公 式,需要您根据需要检测的内容来输入确 定。	^\d{6}\$
原始数据	正则表达式能检测的正确数据。	628307
	输入正则表达式能检测的正确数据,单击 "测试"对正则表达式进行检测。	
结果	显示测试的结果:	命中
	● 命中	
	● 未命中	
	说明	
	– 测试结果为"命中":表示正则表达式 无误;	
	– 测试结果为"未命中": 表示正则表达 式有误。	

步骤7填写完成,确认信息无误,单击"确定",添加完成,新增的SQL注入规则默认为SQL 注入列表第一条。

----结束

7.3 管理 SQL 注入规则

数据库安全审计的SQL注入规则默认开启,您可以对SQL注入规则执行禁用、启用、编 辑和设置优先级操作。

须知

一条审计数据只能命中SQL注入中的一个规则。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 启用SQL注入规则前,请确认SQL注入规则的状态为"已禁用"。
- 禁用SQL注入规则前,请确认SQL注入规则的状态为"已启用"。

禁用 SQL 注入规则

SQL注入规则默认开启,您可以根据使用需要禁用SQL注入规则。禁用SQL注入规则 后,该审计规则在审计中将不生效。

步骤1 登录管理控制台。

步骤2 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。

- 步骤3 在左侧导航树中,选择"审计规则"。
- 步骤4 在"选择实例"下拉列表框中,选择需要禁用SQL注入规则的实例。
- 步骤5 选择"SQL注入"页签。
- 步骤6 在SQL注入规则所在行的"操作"列,单击"禁用"。

图 7-3 禁用 SQL 注入规则

审计范围 SC	2L注入 风险操作 18	制設据保护			
「液加SQLI主人	ARRI				
○ 选择属性等	选,或输入关键字搜索				0
序号 令	各称 ⊖	SQL命令特征 ⇔	风险等级 ↔	状态 🖯	操作
1	MYSQL报错型SQL注入	正则表达式	• 商	0 已启用	设置优先级 禁用 编辑 删除
2	HAVING报镭SQL注入	正则表达式	• 中	0 已度用	设置优先级 禁用 编辑 删除
3	UNION联合宣询SQL注入	正则表达式	• #	 已 已 市 	设置优先级 禁用 編編 删除
4	时间型SQLI主入	正则表达式	• #	0 已度用	设置优先级 禁用 編輯 删除

禁用SQL注入规则成功,该SQL注入规则的状态为"已禁用"。

----结束

启用 SQL 注入规则

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"审计规则"。
- 步骤4 在"选择实例"下拉列表框中,选择需要启用SQL注入规则的实例。
- 步骤5选择"SQL注入"页签。
- 步骤6 在SQL注入规则所在行的"操作"列,单击"启用",启用该规则。

图 7-4 启用 SQL 注入规则

(KtolSQLEA-4901)					
○ 选择属性	筛选,或输入关键字搜索				Q @
序号 ⊖	名称 ⊖	SQL命令特征 ⊖	风险等级 ⊖	状态 ⊖	操作
1	test240403	正则表达式	• 低	 已禁用 	设置优先级 启用 編編 删除
2	MYSQL报错型SQL注入	正则表达式	 高 	 已 日 前 	设置优先级 蒙用 编辑 删除

步骤7 启用SQL注入规则成功,该SQL注入规则的状态为"已启用"。

----结束

SQL 注入规则设置优先级

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"审计规则"。
- 步骤4 在"选择实例"下拉列表框中,选择需要SQL注入规则设置优先级的实例。
- 步骤5选择"SQL注入"页签。
- **步骤6**在SQL注入规则所在行的"操作"列,单击"设置优先级",在弹出的窗口中单击 "优先级"的选框选择想要设置的优先等级,数字越小优先级越高,选择完成,单击 "确定"完成设置。

图 7-5 设置优先级

设置优先级

优先级	1	^	
	1		
	2		
正则表	3	• 高	
	4		
正则表)	5	• 中	
正则表)	6	• 中	
	7		
正则表	8	- +	

----结束

编辑 SQL 注入规则

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"审计规则"。
- 步骤4 在"选择实例"下拉列表框中,选择需要编辑SQL注入规则的实例。
- 步骤5 选择"SQL注入"页签。

🛄 说明

仅自定义创建的SQL注入规则可以使用编辑功能,默认的规则仅可使用启用和禁用功能。

步骤6 单击"操作"列的"编辑",可对目标规则的参数进行编辑,参数说明如表7-3所示。

图 7-6 编辑 SQL 注入规则

编辑SQL注入规则

★ 规则名称	(test240403)	_IDSQL		
<mark>*</mark> 风险等级	盲	中	低	无风险
* 状态				
★ 正则表达式	^[1-9]\d{5}(1	19 20)\d{2}(0	[1	
测试正则表达式				
原始数据				
结果				4

取消 确定

表 7-3 SQL 注入规则参数说明

参数名称	参数说明	取值样例
规则名称	目标SQL规则的名称,可自定义输入。	邮编SQL注入规则
风险等级	目标SQL规则的风险级别,可以选择以下 级别:	中
	● 	
	• 中	
	● 低	
	● 无风险	
状态	开启或关闭当前SQL注入规则。	
	• 🔍 : 开启	
	• • · · · · · · · · · · · · · · · · · ·	
正则表达 式	目标SQL规则采用正则表达式检测的公 式,需要您根据需要检测的内容来输入确 定。	^\d{6}\$
原始数据	正则表达式能检测的正确数据。	628307
	输入正则表达式能检测的正确数据,单击 "测试"对正则表达式进行检测。	

参数名称	参数说明	取值样例
结果	显示测试的结果:	命中
	● 命中	
	• 未命中	
	说明	
	– 测试结果为"命中":表示正则表达式 无误;	
	– 测试结果为"未命中": 表示正则表达 式有误 。	

步骤7 编辑完成,确认信息无误,单击"确定",完成修改。

----结束

删除 SQL 注入规则

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"审计规则"。
- 步骤4 在"选择实例"下拉列表框中,选择需要删除SQL注入规则的实例。
- 步骤5 选择"SQL注入"页签。

🗋 说明

仅自定义创建的SQL注入规则可以使用删除功能,默认的规则仅可使用启用和禁用功能。 步骤6 单击"操作"列的"删除",对目标规则进行删除。

图 7-7 删除 SQL 注入

序号 ⊖	21 7 0	SQL命令特征 ⊖	风险等级 ⊖	₩ 8 θ	授作
1	A	正则表达式	• 16	○ 已練用	设置优先级 启用 编辑 勤除
2	MYSQL接触型SQL/主入	正则表达式	• 商	 E局用 	说是优先说 發用 编辑 删除

----结束

7.4 添加风险操作

数据库安全审计内置了"数据库拖库检测"和"数据库慢SQL检测"两条检测规则, 帮助您及时发现数据库安全风险。同时,您也可以通过添加风险操作,自定义数据库 需要审计的风险操作规则。

须知

一条审计数据只能命中风险操作中的一个规则。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 请参考**开启数据库安全审计**成功开启数据库安全审计功能。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"审计规则"。
- 步骤4 在"选择实例"下拉列表框中,选择需要添加风险操作的实例。
- 步骤5选择"风险操作"页签。
- 步骤6 在风险操作列表左上方,单击"添加风险操作"。
- **步骤7**在"添加风险操作"界面,设置基本信息和客户端IP地址,相关参数说明如表7-4所示。

图 7-8 设置基本信息和客户端 IP 地址

基本信息 * 风险操作名称 * 风险等级 高 中 低 无风险 * 状态 * 应用到数据库 test

客户端IP/IP段

请输入IP/IP段,多个以换行符相隔(不可重复)

请输入数据		
		1

表 7-4 风险操作参数说明

参数名称	说明	取值样例
风险操作名称	您可以自定义风险操作的名称。	test

参数名称	说明	取值样例
风险级别	选择风险操作的级别,可以选择以下级别:	高
	● 高	
	• 中	
	● 低	
	● 无风险	
状态	开启或关闭风险操作。	
	• 〇: _{开启}	
	• ① : _{关闭}	
应用到数据库	选择应用该风险操作的数据库。	-
	您可以勾选"全部数据库"或选择某数据库使用该风险操作规则。	
客户端IP/IP段	输入客户端的IP地址或IP地址段。	192.168.0.0
	IP地址支持IPv4(例如,192.168.1.1)和IPv6(例	
	xu, fe80:0000:0000:0000:0000:0000:0000:0000)格 式。	

步骤8 设置操作类型、操作对象、执行结果,相关参数说明如表7-5所示。

图 7-9 设置操作类型、操作对象和执行结果

操作类型					
✔ 登录 ✔ 操作					
全部操作					
数据定义 (DDL) CREATE TABLE	CREATE TABLESPACE	DROP TABLE	DROP TABLESPACE		
数据操作 (DML) UPDATE	INSERT	DELETE	SELECT	SELECT FOR UPDATE	
数据控制 (DCL) CREATE USER	DROP USER	GRANT	REVOKE	ROLLBACK	
操作对象					
添加操作对象 忽略大小写					
序号 目标数据库	目标表		字段		操作
1 asd					确定 取消
执行结果					
* 影响行数 大于等于	~ 0	行			
* 执行时长 大于等于	~ O	電秒			
确定 取消					

表 7-5 参数说明

参数名称	说明	取值样例
操作类型	风险操作的类型,包括"登录"和"操作"。 当选择"操作"时,可以选择"全部操作",或选 择"数据定义(DDL)"、"数据操作 (DML)"或"数据控制(DCL)"的操作。	操作
操作对象	单击"添加操作对象"后,输入"目标数据库"、 "目标表"和"字段"信息。单击"确定",添加 操作对象。	-
执行结果	设置"影响行数"和"执行时长"的执行条件后, 输入行数和时长值,执行条件包括: • 大于 • 小于 • 等于 • 大于等于 • 小于等于	-

步骤9 单击"保存"。

----结束

相关操作

- 如何对所有数据库设置数据库安全审计规则?
- 如何设置数据库安全审计的INSERT审计策略?

7.5 配置隐私数据保护规则

当需要对输入的SQL语句的敏感信息进行脱敏时,您可以通过开启隐私数据脱敏功 能,以及配置隐私数据脱敏规则,防止数据库用户敏感信息泄露。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 请参考**开启数据库安全审计**成功开启数据库安全审计功能。

操作步骤

步骤1 登录管理控制台。

- 步骤3 在左侧导航树中,选择"审计规则"。

步骤4 在"选择实例"下拉列表框中,选择需要配置隐私数据保护规则的实例。

步骤5选择"隐私数据保护"页签。

🛄 说明

仅自定义创建的规则可以使用编辑和删除功能,默认的规则仅可使用启用和禁用功能。 步骤6开启或关闭"存储结果集"和"隐私数据脱敏"。

存储结果集

建议关闭 ① 》。关闭后,数据库安全审计分析平台将不会存储用户SQL语句的结果集。

如果用于PCI DSS/PCI 3DS CSS认证,禁止开启。

注:结果集存储只支持agent方式审计数据库。

隐私数据脱敏

建议开启 。开启后,您可以通过配置隐私数据脱敏规则,防止数据库敏感 信息泄露。

步骤7单击"添加自定义规则",在弹出"添加自定义规则"对话框中设置数据脱敏规则, 如<mark>图7-10</mark>所示,相关参数说明如**表7-6**所示。

图 7-10 添加自定义规则

添加自定义规则

★ 规则名称	
★ 正则表达式	
★ 替换值	***
原始审订 示例 当设置I 脱敏后的	十日志:alter user dba with password 'mypassword'; E则表达式为:password ['"].*['"]替换值为:password ***时 9日志为:alter user dba with password ***

表 7-6 自定义规则参数说明

参数名称	说明	取值样例
规则名称	自定义规则的名称。	test
正则表达式	输入需要配置的正则表达式。	-
替换值	输入正则表达式脱敏后的替换值。	###

取消)

确定

步骤8 单击"确定"。

规则列表中新增一条状态为"已启用"的脱敏规则。

----结束

效果验证

以脱敏"护照号"信息,且审计的数据库为MySQL为例说明,请参考以下操作步骤验 证隐私数据脱敏功能是否生效:

步骤1 开启"隐私数据脱敏",并确保"护照号"规则已启用,如图7-11所示。

图 7-11 规则已启用

《物理定》	XMR)								
(法择属)	○ 选择属性境密、或输入关键字接索								
序号 ⇔	規則名称 ⇔	規則类型 🗇	正則表达式 🕀	替换值 ⇔	状态 ⇔	操作			
1	护服号	默认		***	 已启用 	蒙用 编辑 删除			

- 步骤2 使用MySQL数据库自带的客户端,以root用户登录数据库。
- 步骤3 在数据库客户端,输入一条SQL请求语句。

```
select * from db where HOST="护照号";
```

- 步骤4 在左侧导航栏选择"数据报表",进入"数据报表"页面。
- 步骤5 根据筛选条件,查询输入的SQL语句。
- **步骤6** 单击该SQL语句,在"语句详情"页面查看SQL请求语句信息,隐私数据脱敏功能正常,"SQL请求语句"显示脱敏后的信息。

图 7-12 隐私数据脱敏



----结束

其它操作

添加自定义脱敏规则后,您可以根据使用需求,对自定义规则执行以下操作:

禁用

在需要禁用的规则所在行的"操作"列,单击"禁用",可以禁用该规则。禁用 该规则后,系统将不能使用该数据脱敏规则。 图 7-13 禁用自定义脱敏规则

						1
序号 ⊖	規則名称 ⊖	規則类型 😌	正则表达式 🖯	1999AL 0	165 O	操作
1	的现在	飲い		***	 已出用 	禁用 编辑 勤務
2	军官征号	Str.U.			 已度用 	新用 明日 数钟
3	民族	BKU.			○ 已雇用	新用 编辑 動脉
4	银行卡号	BKU.			0 已雇用	新用 印后 動物
5	身份证券	BRU.			 C 品用 	100 100 100
6	GPS信息	BGJ.			 已用用 	10 10 10 10 10 10 10 10 10 10 10 10 10 1
7	test	自定义	password	***	o Bar	2017 - 2019: 2019:

● 编辑

在需要修改信息的规则所在行的"操作"列,单击"编辑",在弹出的对话框中,修改规则信息。

图 7-14 编辑自定义脱敏规则

0 88	規則名称 ⊖	規則実型 0	正则表达式 0	e mana	秋志 0	操作
1	2058 - 9	数以			0 已抱用	新用 编辑 勤務
2	军官任号	REA.			o eem	MR 998 899
3	R#	RGA.			 C目目用 	新用 编辑 數時
4	银行卡号	BRSA.			 E展用 	80 88 89
5	身份证号	Brij,			 已與用 	展用 编辑 動物
6	GPS信息	飲み			0 已应用	第用 编辑 數錄
7	test	日生义	password		0 已治用	就用 编辑 影除

● 删除

在需要删除的规则所在行的"操作"列,单击"删除",在弹出的提示框中,单击"确定",删除该规则。

图 7-15 删除自定义脱敏规则

啓谷 ⊖	規則名称 ⊖	規則業型 ⊖	正则表达式 0	● ● ●	秋志 0	操作
1	护领导	動い、			 已扁用 	新用 印后 数 种
2	军直迁号	Btu.		***	 已展用 	新用 印运 動物
3	RM	BNU.		***	 E展用 	55.7 (G)() 559
4	银行卡号	BKU.		***	 已呈用 	50.70 (A)() 2019
5	最份证券	BKJ.			o Eem	MR 668 899
6	GPS编题	REA.			o eem	55.90 (R40) 2599
7	test	自定义	password		o Ber	禁用 编辑 影致

7.6 SQL 白名单

7.6.1 添加 SQL 白名单

可将发现的有风险SQL语句添加为白名单,添加后审计SQL语句时白名单SQL语句将被 忽略。

约束限制

数据报表支持已扫描且存在风险的SQL语句加入白名单。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航栏选择"数据报表",进入"数据报表"页面。

步骤4 在"选择实例"下拉列表框中,选择需要查看会话信息的实例。

步骤5 选择"语句"页签,查看有风险的SQL语句。

步骤6 添加SQL语句至白名单。

- 添加单条SQL语句
 - a. 在需要添加至白名单SQL语句的"操作"列单击"添加到白名单"。

图 7-16 添加到白名单

- c. 确认无误,单击"确定",完成添加。
- 批量添加SQL语句
 - a. 勾选需要添加白名单的SQL语句,单击上方的"一键加白"。

冬	7-1	8	一键加白
---	-----	---	------

语句	会话	趋势分析
<u> </u>	-键加白)

b. 在弹窗中选择目标SQL语句添加白名单的数据库和描述说明。

图 7-19 添加 SQL 白名单

添加SOL自名单 SQL语句 应用到数据库 描述 SELECT target_data FROM sys.dm_xe_session_targets xet … 应用到数据库 ✓ 描述

c. 确认无误,单击"确定",完成添加。

----结束

7.6.2 管理 SQL 白名单

可对已添加的SQL语句白名单进行编辑、禁用、删除等操作。

前提条件

需要关联的SQL语句已经添加至白名单。

文档版本 01 (2024-11-28)

操作步骤

步骤1 登录管理控制台。

- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航栏选择"审计规则",进入"审计规则"页面。
- 步骤4 在"选择实例"下拉列表框中,选择需要查看会话信息的实例。
- 步骤5 选择 "SQL白名单" 页签, 查看所有SQL语句白名单。
- 步骤6 对白名单进行管理。
 - 单击目标SQL语句"操作"列的"编辑",可对描述和应用的数据库进行修改。
 - 单击目标SQL语句"操作"列的"禁用",禁用后当前SQL语句在审计时不执行该规则。

🛄 说明

禁用后会有大约1分钟的延迟。

 单击目标SQL语句"操作"列的"删除",删除后SQL语句不可恢复白名单,只能 重新添加,同时SQL也将被重新进行扫描检测。
 如果需要删除多条白名单SQL语句,勾选需要删除的SQL语句,单击上方的"一键 删除",确认删除即可。

门 说明

SQL白名单在变动后,对已审计的数据不会生效,保持原有审计结果。

-----结束

8 查看审计结果

8.1 查看 SQL 语句详细信息

添加的数据库连接到数据库安全审计实例后,您可以查看该数据库详细的SQL语句信 息。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 请参考**开启数据库安全审计**成功开启数据库安全审计功能。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航栏选择"数据报表",进入"数据报表"页面。
- 步骤4 在"选择实例"下拉列表框中,选择需要查看SQL语句信息的实例。
- 步骤5选择"语句"页签。
- 步骤6 查询SQL语句信息。

图 8-1 查询 SQL 语句

SQL语句	客户编P	数据库印城名	数据库用户	数据库名	风险等级	规则	操作类型	电应结果	生成的间 0	操作
SET DEADLOCK_PRIORITY -10			-	master	无风险	全审计规划	SET	SUCCESS		annes(
SELECT target_data FROM sys.d			-	mester	无风险	全审计规则	SELECT	SUCCESS		派加到白索
SET DEADLOCK_PRIORITY -10			-	master	无风险	全审计规则	SET	SUCCESS		iāte n iejas (
ALTER EVENT SESSION (tolomot				master	无风险	全审计规划	ALTER	SUCCESS		8.0995-87

您可以按照以下方法,查询指定的SQL语句。

选择"时间范围"("全部时间"、"近30分钟"、"近1小时"、"今日"、
 "近7天"、"近30天"),单击Q,列表显示该时间段的SQL语句。

文档版本 01 (2024-11-28)

选择"风险等级"("(全选)"、"高"、"中"、"低"或"无风险"),
 单击Q,列表显示该级别的SQL语句。

🗀 说明

一次查询最多可查询10,000条记录。

步骤7 单击需要查看语句详情信息的SQL语句。

步骤8 在"语句详情"提示框中,查看SQL语句的详细信息,相关参数说明如表8-1所示。

须知

审计语句和结果集的长度限制为10,240字节。超出部分,系统将不记录在审计日志中。

图 8-2"语句"提示框

语句详情 会话ID acd5fb23-5122-477e-942c-11d9bdaabb89 数据库实例 mysql 数据库类型 MySQL 5.7.18 数据库用户 root 客户端MAC地址 数据库MAC地址 客户端IP 数据库IP/域名 客户端端口 39106 数据库端口 3306

客户端名称 ---操作类型

SET

操作对象类型 ---

响应结果

SUCCESS 影响行数

开始时间 10:49:35 GMT+08:00

响应结束时间 10:49:35 GMT+08:00

SQL请求语句

SET character_set_results = NULL

请求结果 ---

确定

表 8-1 SQL 语句详情参数说明

参数名称	说明
会话ID	SQL语句的ID,由系统自动生成。
数据库实例	SQL语句所在的数据库实例。
数据库类型	执行SQL语句所在的数据库的类型。
数据库用户	执行SQL语句的数据库用户。
客户端MAC地址	执行SQL语句所在客户端MAC地址。
数据库MAC地址	执行SQL语句所在数据库MAC地址。
客户端IP	执行SQL语句所在客户端的IP地址。
数据库IP/域名	执行SQL语句所在的数据库的IP地址/域名。
客户端端口	执行SQL语句所在的客户端的端口。
数据库端口	执行SQL语句所在的数据库的端口。
客户端名称	执行SQL语句所在客户端名称。
操作类型	SQL语句的操作类型。
操作对象类型	SQL语句的操作对象的类型。
响应结果	执行SQL语句的响应结果。
影响行数	执行SQL语句的影响行数。
开始时间	SQL语句开始执行的时间。
响应结束时间	SQL语句结束的时间。
SQL请求语句	SQL语句的名称。
请求结果	SQL语句请求执行的结果。

----结束

相关操作

- 如果SQL语句列表中未显示输入的SQL语句,说明Agent与数据库安全审计实例之 间网络通信异常,请参照如何处理Agent与数据库安全审计实例之间通信异常? 处理。
- 数据库开启SSL时,将不能使用数据库安全审计功能。如果您需要使用数据库安全 审计功能,请关闭数据库的SSL。关闭数据库SSL的详细操作,请参见如何关闭数 据库SSL?。

8.2 查看会话分布

添加的数据库连接到数据库安全审计实例后,您可以查看该数据库的会话分布情况。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 请参考开启数据库安全审计成功开启数据库安全审计功能。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航栏选择"数据报表",进入"数据报表"页面。
- 步骤4 在"选择实例"下拉列表框中,选择需要查看会话信息的实例。
- **步骤5**选择"会话"页签。
- 步骤6 查看会话分布表。
 - 在"选择数据库"下拉列表框中,选择"全部数据库"或指定的数据库,可以查 看实例中所有的数据库或指定的某个数据库的会话信息。
 - 选择审计的时间("近30分钟"、"近1小时"、"今日"、"近7天"或"近30
 天");或者单击^(三),选择开始时间和结束时间,查看指定的时间段的会话信息。

图 8-3 会话分布表

日均 会话 趋势分析	
3時約6年 金田和島市 >)	800000 161001 48 1678 1500 FMBH-16500 E
客户结会试分布表 TOP10	数据库用户会试介布图 TOP10
查户20月P	散週审用户

----结束

相关操作

- 数据库开启SSL时,将不能使用数据库安全审计功能。如果您需要使用数据库安全 审计功能,请关闭数据库的SSL。关闭数据库SSL的详细操作,请参见如何关闭数 据库SSL?。
- 如果审计功能无法正常使用,请参照无法使用数据库安全审计章节进行处理。
- 您可以配置数据库的审计规则,详细操作请参见<mark>配置审计规则</mark>。

8.3 查看审计总览信息

添加的数据库连接到数据库安全审计实例后,您可以查看数据库的审计总览信息,包 括数据库的审计信息、实例信息、数据分析情况。

前提条件

添加的数据库实例版本须在23.05.23.193055及以上版本。

- 数据库安全审计实例的状态为"运行中"。
- 请参考开启数据库安全审计成功开启数据库安全审计功能。

操作步骤

步骤1 登录管理控制台。

- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- **步骤3** 查看审计信息、单个实例信息和数据分析图展示。
 - 审计信息

汇总显示所有数据库安全审计实例的审计时长、语句总量、风险总量、今日语 句、今日风险和今日会话。

图 8-4 查看我的审计信息

	8888994992 2004/11/25 11%224 GMT-08:00 🔐 988894925 ISRN 9750100 1								
表的审计信息									
	附有实例								
	19天18小时	346,053,327	345,591,3	33	42,097,412	42,039,487		568	
	#计时长	頃の必要	RESE	>	今日長切	今日风险		今日会話	

单击右上角" 💭 ",开启信息汇总定时刷新。定时刷新开启后,系统刷新频 率为1次/小时。单击右上角"立即刷新",即可立即刷新审计信息。

单个实例信息

单击"~",查看每个数据库安全审计实例的审计时长、语句总量、风险总量、 今日语句、今日风险和今日会话。

图 8-5 查看单个实例信息

单个实例信息

謝輸入实例名称 ✓ DBSS-			^ DBSS-
审计时长 19天18小时	语句总量 4,821	风险总量 85	↑ DBSS-
今日语句 4	今日风险 0	今日会话 4	^ DBSS-
^ DBSS			
^ DBSS			

数据分析图展示

教记分析图展示

单击 "[^(C)" 或 "[^(L)]",通过饼图或柱形图,展示所有数据安全审计实例的语句总量分析、风险总量分析、今日语句分析、今日风险分析和今日回话分析,另外还统计展示对应数据的TOP5。

图 8-6 查看数据分析图展示

· · · · · · · · · · · · · · · · · · ·	今日风险分析 今日会运分析				
	語句結論		() ()	TOP5 语物总量	
	 DBSS 通知思想 	346,034,840%		0855-	346,034,840
	 DBSS- 语句思量 	13,66035		DBSS-	13,990
346 053 327	 DBSS- 通知効量 	4,821余		DBSS-	4,821
	 DBSS- 景切想量 	6魚		Date	
	 DBSS- 语句总量 	0条			
	▲ 1/2 ▼			DESS	0

- **步骤4** 单击上方"风险总量",进入"风险总量"界面。单击"🗎",选择时间范围,查看 指定时间段的所有数据库安全审计实例的风险分析。
 - 风险级别总体分析图

单击 " (, 或 ") " , 通过饼图或柱形图,展示所有数据库的高风险等级命中次数、中分险等级命中次数和低分险等级命中次数,另外还展示数据库风险次数命中排行TOP3。

图 8-7 风险级别总体分析

2.		
AMPROSEERING 2004/10/06 17:00:18 GMT-08:00		
总体分析		2024/09/09 17:02:05 - 2024/10/09 17:02:05
风热感到总体分析图		
	c B	TOP3 数据库局地分数由中国行
S2725/Bite+KS2t	1次/5次	0855 2
+5250826+1/32	4次/5次	0855- 2
世辺が衰退かび波	0次/5次	1

风险规则总体分析
 展示所有数据库的风险规则命中次数,另外还展示风险规则命中排行TOP5。

图 8-8 风险规则总体分析

本分 析		
	风险规则由中次数	TOP5 风险规则命中排行
5	UNON&642850(12).0=028 38 Editements/0=028 18 EP#E(2).0=028 18	UNICN都会世际54注入 数据单数地址前 数等指定入3

- 其他风险角度分析
 - 风险级别:展示每个数据库的高风险命中次数分析、中风险命中次数分析和 低风险命中次数分析。

图 8-9 风险级别分析



- 风险规则:展示某风险规则被数据库命中次数的分析情况。

图 8-10 风险规则分析



- 数据库统计:展示每个数据库命中分险规则的分析情况。

图 8-11 数据库统计分析

其他风险角度分析		(取現地的計 →) DDS5- → →
	数据库风险规则分析	
2	1.UNNONWA前面SQLE入曲中の数 12次 三部6月 2.855年16月9日の数 12次 三部6月 1.011010110110110110110111011110111	

- 步骤5 在左侧导航栏选择"数据报表",进入"数据报表"页面。
- 步骤6 选择"趋势分析"页签,进入"趋势分析"页面。

步骤7 在"选择实例"下拉列表框中,选择需要查看审计总览信息的实例。

- 步骤8 查看数据库的总体审计情况,以及数据库的风险分布、会话统计和SQL分布信息。
 - 在"选择数据库"下拉列表框中,选择"全部数据库"或指定的数据库,可以查 看实例中所有的数据库或指定的某个数据库的总览信息。
 - 选择审计的时间("近30分钟"、"近1小时"、"今日"、"近7天"或"近30
 天");或者单击¹¹,选择开始时间和结束时间,查看指定的时间段的总览信息。

图 8-12 SQL 分布

SQL分布					UPDATE 📕 I	NSERT 📕 DELET	e 📕 SELECT	其他操作
1								
0.8								
0.6								
0.4								
0.2								
0 2020/03/27 09:38:00 09:41:00	2020/03/27 2020/03/27 09:44:00 09:47:00	2020/03/27	2020/03/27	2020/03/27	2020/03/27	2020/03/27	2020/03/27	

----结束

相关操作

- 数据库开启SSL时,将不能使用数据库安全审计功能。如果您需要使用数据库安全 审计功能,请关闭数据库的SSL。关闭数据库SSL的详细操作,请参见如何关闭数 据库SSL?。
- 如果审计功能无法正常使用,请参照无法使用数据库安全审计章节进行处理。
- 您可以配置数据库的审计规则,详细操作请参见<mark>配置审计规则</mark>。

8.4 查看审计报表

数据库安全审计默认提供一条"全审计规则"的审计范围,可以对成功连接数据库安 全审计的所有数据库进行审计。添加的数据库连接到数据库安全审计实例后,可以立 即生成审计报表或者按计划生成审计报表,并在线预览、下载审计报表。

前提条件

• 数据库安全审计实例的状态为"运行中"。

文档版本 01 (2024-11-28)

• 请参考**开启数据库安全审计**成功开启数据库安全审计功能。

报表类型

数据库安全审计为用户提供了8种报表模板,各报表名称如**表8-2**所示。用户可根据实际业务情况**生成报表、设置报表的执行任务**。

表 8-2 报表说明

报表模板名称	报表类型	说明
数据库安全综合报表	综合报表	提供数据库整体审计状况,主要从 风险分布、会话分布和登录状况等 几个维度进行审计分析,为数据库 管理提供整体审计状况依据。
数据库安全合规报表	合规报表	根据《中国国家信息安全保护检验 标准》和国家等级保护的检测要求 对数据库进行数据统计。帮助数据 库管理人员、审计人员及时发现各 种异常行为和违规操作,并为快速 定位分析、整体信息管理提供决策 依据。
SOX-萨班斯报表	合规报表	参考《萨班斯法案》针对用户全面 把控数据库内部活动的要求,对数 据库进行数据统计。帮助数据库管 理人员、审计人员及时发现各种异 常行为和违规操作,并为快速定位 分析、整体信息管理提供决策依 据。
数据库服务器分析报 表	数据库专项报表	分别为数据库活动用户统计、访问 数据库来源IP数量统计、数据库登录 及请求统计分析和使用数据库操作 时间判断数据库服务器性能。
客户端IP分析报表	客户端专项报表	统计源IP中客户端应用程序、数据库 用户数量和SQL语句数量。
DML命令报表	数据库操作专项报表	通过DML命令分析用户与特权操 作。
DDL命令报表	数据库操作专项报表	通过DDL命令分析用户与特权操 作。
DCL命令报表	数据库操作专项报表	通过DCL命令分析用户与特权操作。

步骤一: 生成报表

DBSS支持"立即生成报表"和"按计划生成报表"两种方式。其中,按计划生成报表 支持自定义报表的生成时间、频率、格式等信息。请根据实际需求选择报表的生成方 式。

文档版本 01 (2024-11-28)

• 方式一: 立即生成报表

步骤1 登录管理控制台。

- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"报表"。
- 步骤4 在"选择实例"下拉列表框中,选择需要生成审计报表的实例。
- 步骤5选择"报表管理"页签。
- 步骤6 在需要生成报表的模板所在行的"操作"列,单击"立即生成报表"。

表模板列表
表模板列表

National State of the state of					
〇、选择属性弱选、或输入关键字搜索					Q 0
服表模板名称 ⊖	关股数据库 ↔	英型 令	mis ⊖	HDHER46Z O	操作
数据库安全综合报表	全部数据库	综合报表	数据库安全综合报表	○ 已开启(華天)	设置任务 立即生成服装
数据库安全合规服表	全部数据库	合规服表	数据库安全合规报表	 已关闭(每周) 	设置任务立即生成报表
SOX-萨班斯提表	全部數据库	合规报表	SOX-萨驼斯根表	 已关闭(編問) 	设置任务 立即生成服装
数据库服务输分析报频	全部数据库	数据库专项报制	数据库服务器分析报表	○ 已共紀(華間)	设置任务立即生成服装
客户请旧分析报表	全部数据库	客户颁专项报表	客户确IP分析报表	 已关闭(每周) 	设置任务立即生成服务
DDL命令报票	全部数据库	数据库操作专项报表	DDL命令报表	 已关闭(每周) 	设置任务立即生成服务
DCL命令报表	全部数据库	數据库操作专项报表	DCL命令报表	 已关闭(毎周) 	设置任务 立即生成报表
DML命令报表	全部設現库	数据库操作专项报表	DML命令授表	 已关闭 (每周) 	设置任务 立即生成服表

步骤7 在弹出的对话框中,单击^{IIII},设置报表的开始时间和结束时间,选择生成报表的数据 库。

Х

图 8-14 "立即生成报表"对话框

立即生成报表

★ 时间范围	2024/11/08 00:00:00 - 2024	/11/08 10:06:09	
★ 数据库	全部数据库	~	
		〔 取消	确定

步骤8 单击"确定"。

----结束

- 方式二:设置定期发布报表
- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"报表"。
- 步骤4 在"选择实例"下拉列表框中,选择需要设置执行任务的报表的实例。

步骤5选择"报表管理"页签。

步骤6在需要立即生成报表的模板所在行的"操作"列,单击"设置任务",如图8-15所示。

图 8-15 设置任务

报表结果 报表管理					
 运探属性筛选,或输入关键字搜索 					
报表模板名称 ⊖	关联数据库 ⊖	業型 ⊖	描述 ⊖	计别任务状态 🖯	操作
数据库安全综合报表	全部数据库	综合报表	数据库安全综合报表	 已关闭(每天) 	设置任务立即生成报表
SOX-萨旺斯报表	全部数据库	合规程表	SOX-萨旺斯提表	 已关闭(每周) 	设置任务 立即生成报表
数据库安全合规报费	全部数据库	合规报表	歡選幸安全合规报表	 已共闭(每周) 	设置任务 立即生成报表
数据库服务器分析报表	全部数描库	数据库专项报表	数据库服务器分析报表	 已关闭(每周) 	设置任务 立即生成报表
客户确IP分析报表	全部数据库	客户端专项报表	客户端IP分析报表	 已关闭(每周) 	设置任务 立即生成报表
DML命令探索	全部数据库	数据库操作专项报表	DML命令探赛	 已关闭(每周) 	设置任务 立即生成报表
DCL命令振费	全部数据库	数据库操作专项报表	DCL命令报费	 已关闭(每周) 	设置任务 立即生成报表
、 DDL命令振奏	全部数据库	数据库操作专项报表	DDL命令报表	 E关闭(每周) 	设置任务 立即生成报表

总条数:8 10 ∨ 〈 1 →

步骤7 在弹出的对话框中,设置计划任务参数,如<mark>图8-16</mark>所示,相关参数说明如表8-3所示。

х

图 8-16 "计划任务"对话框

计划任务

1 告警基础功能免费, 触发产生的告警消息由消息通知服务发送, 可能产生少量费用, 具体费用由消息通知服务结算。						
★ 启动任务						
★ 消息通知						
★ 消息通知主题	test-syx 下拉框只展示订阅状态为" <mark>已确</mark> " 消息通知按需计费,不同区域及	✓ Q 查看消息通知主题 从"的消息通知主题。 3. 3. 3. 3. 3. 3. 3. 3. 3. 3. 3. 3. 3.				
* 报表类型	日报	~				
★执行方式	执行一次	~				
时区	GMT+08:00					
★执行时间	16点	~				
★ 数据库	全部数据库	v				
		取消 确定				

表 8-3 计划任务参数说明

参数名称	说明	取值样例
启动任务	开启或关闭计划任务。	
	• 〇: _{开启}	
	• ① : _{关闭}	
消息通知	开启或关闭消息通知。 消息通知触发的消息由消息通知服务发送,消息通 知服务为收费服务,按需计费,不同区域及计费项 产生费用不同,价格详情请参见 <mark>SMN价格详情</mark> 。	
	• C: 开启	
	• ① : _{关闭}	
消息通知主题	 通过下拉框选择已有的主题,或者单击"查看 消息通知主题"创建新的主题,具体操作请参 见创建主题。 	-
	 每个消息通知主题可添加多个订阅,并可选择 多种订阅终端(例如短信、邮件等),详细订 阅说明请参见添加订阅。 	
	更多关于主题和订阅的信息,请参见《 消息通知服 务用户指南 》。	
报表类型	选择生成的报表类型,可以选择:	周报
	• 日报	
	● 周报	
	● 月报	
执行方式	选择报表执行的方式,可以选择:	周期执行
	● 执行一次	
	● 周期执行	
执行时间	选择报表执行的时间点。	10点
数据库	选择执行报表任务的数据库。	-

步骤8单击"确定"。

----结束

步骤二:预览、下载审计报表

预览或下载审计报表前,请确认报表的"状态"为"100%"。

须知

如果您需要在线预览报表,请使用Google Chrome或Mozilla FireFox浏览器。

步骤1 登录管理控制台。

- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"报表"。
- 步骤4 在"选择实例"下拉列表框中,选择需要预览或下载审计报表的实例。
- **步骤5** 在需要预览或下载的报表所在行的"操作"列,单击"预览"或"下载",如<mark>图8-17</mark> 所示,在线预览报表结果,或下载并查看报表。

图 8-17 预览或下载报表

报	製結果 报表管理								
	〇、选择属性筛选,或输入关键	腔撞索							0
	报表名称 ⇔	关联数据库 ⇔	报表类型 ⇔	生成时间 ↔	橋式 ⇔	秋恋 ⊖		操作	
	数]]]库安全合规报表	全部数据库	实时报表	2024/03/25 10:53:35 GMT+08:00	pdf		100%	预选下载 删	6
	数据库安全综合报表	全部数据库	实时报表	2024/03/25 10:51:59 GMT+08:00	pdf		100%	预选下载制	B
	DML命令报表	全部設選率	实时报表	2024/03/25 09:15:14 GMT+08:00	pdf		100%	预改下载删	8
	数温库安全综合报表	全部数据库	实时报表	2024/02/27 20:34:26 GMT+08:00	pdf		100%	预选下载删	9
	≙先数:4 10 ∨ <	1 >							

----结束

相关操作

为什么不能在线预览数据库安全审计报表?

8.5 查看趋势分析

添加的数据库连接到数据库安全审计实例后,您可以查看数据库的趋势分析,包括数 据库的语句趋势分析:语句数量趋势、会话统计和SQL分布,还包括风险趋势分析: 风险分布、SQL注入趋势和风险操作趋势。

前提条件

- 添加的数据库实例版本在23.05.23.193055及以上版本支持该功能。
- 数据库安全审计实例的状态为"运行中"。
- 请参考开启数据库安全审计成功开启数据库安全审计功能。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择"区域"后,单击页面左上方的 —— ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。

步骤3 在左侧导航栏选择"数据报表",进入"数据报表"页面。

- 步骤4 选择"趋势分析"页签,进入"趋势分析"页面。
- 步骤5 在"选择实例"下拉列表框中,选择需要查看审计总览信息的实例。
- 步骤6 查看数据库的总体趋势情况。
 - 单击控制台右侧的"重新生成趋势分析"。

图 8-18 重新生成趋势分析

面句 会话 趋势分析	生成趋势分析数据	X
语句趋势分析 风险趋势分析 数据库:全部	法経動通常 全部数描定 イ	曲新設備生成时间: 2024/10/11 11.24-13 GMT+08-00 (重新生成趋势分析)
风险分布	建器分析时间提 近30分钟 近1小时 今日 近7天 近30天	
	开始日期-结束日期	📕 商风給 📕 仲风給 📕 低风焓
600		
500		
400		
300		

- 在"选择数据库"下拉列表框中,选择"全部数据库"或指定的数据库,可以查 看实例中所有的数据库或指定的某个数据库的语句趋势分析和风险趋势分析。
- 选择审计的时间("近30分钟"、"近1小时"、"今日"、"近7天"或"近30
 天");或者单击⁽¹⁾,选择开始时间和结束时间,查看指定的时间段的语句趋势分析和风险趋势分析。

图 8-19 语句数量趋势



图 8-20 会话统计



图 8-21 SQL 分布



图 8-22 风险分布



图 8-23 SQL 注入趋势



图 8-24 风险操作趋势



. สหน้าต่ำ สนในต่ำ สนในต่ สนในต่ำ สนในต่ำ

----结束

9 通知设置管理

9.1 设置邮件通知

开启邮件通知后,当数据库设置的告警事件发生或生成报表时,您可以收到告警或报 表生成的通知邮件。

前提条件

数据库安全审计实例的状态为"运行中"。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"设置"。
- 步骤4 在"选择实例"下拉列表框中,选择需要设置邮件通知的实例。
- 步骤5 设置邮件通知,相关参数说明如表9-1所示。

邮件通知	
* 收件人	请输入收件人,多个请以换行符相隔(不可重复):
	请输入收件人
抄送人	请输入抄送人,多个请以换行符相隔 (不可重复):
	请输入抄送人

图 9-1 设置邮件通知

表 9-1 邮件通知参数说明

应用

参数名称	说明	取值样例
邮件通知	开启或关闭邮件通知。数据库安全审计默认开启邮 件通知,当数据库发生设置的告警事件或生成报表 时,数据库安全审计将发送通知邮件。	0
	• C: 开启	
	• ① : _{关闭}	
收件人	输入收件人的邮箱地址。	-
抄送人	可选参数。输入抄送人的邮箱地址。	-

步骤6单击"应用"。

----结束

9.2 设置告警通知

通过设置告警通知,当数据库发生设置的告警事件时,您可以收到DBSS发送的告警通 知,及时了解数据库的安全风险。否则,无论是否有危险,您都只能登录管理控制台 自行查看,无法收到告警信息。

- 告警通知信息可能会被误拦截,若您未收到相关告警信息,请在信息拦截中查看。
- 系统每5分钟进行一次告警统计,并触发告警通知。

 数据库安全审计告警基础功能免费,触发产生的告警消息由消息通知服务发送, 消息通知服务为付费服务,价格详情请参见SMN价格详情。

前提条件

数据库安全审计实例的状态为"运行中"。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"设置"。
- 步骤4 在"选择实例"下拉列表框中,选择需要设置告警通知的实例。
- 步骤5选择"告警通知"页签。
- 步骤6 设置告警通知,相关参数说明如表9-2所示。

图 9-2 设置告警通知

告警	通知	备份与恢复	风险导出	
	0	告警基础功能免费,	触发产生的告警消息由消息通知服务发送,可能产生少量费用,具体费用由消息通知服务结算。	
	全月	局设置		
	消息	見通知		
	* 消息	見通知主题	test- ~ Q 查看消息通知主题	
			下拉框只展示订阅状态为"已确认"的消息通知主题。 消息通知按需计费,不同区域及计费项产生费用不同。 了解计费详情	
	每月	天发送告警总条数	65535	
	X.	验日志告警设置		
	쑴혈	管风险等级	✔ 高 中 (低	
	系	统资源告警设置		
	CP	U告警阈值(%)	80	
	内存	字告警阈值(%)	80	
	磁盘	盘告警阈值(%)	80	
			应用	

表 9-2 告警通知参数说明

参数名称	说明	取值样例
消息通知	开启或关闭消息通知。数据库安全审计的告警基础 功能免费,触发产生的告警消息由消息通知发送, 可能会产生少量费用,具体的收费详情,请参见 SMN价格详情。	
	• ① : _{关闭}	
	• 一 : 开启	
消息通知主题	 通过下拉框选择已有的主题,或者单击"查看 消息通知主题"创建新的主题,具体操作请参 见创建主题。 	-
	 每个消息通知主题可添加多个订阅,并可选择 多种订阅终端(例如短信、邮件等),详细订 阅说明请参见添加订阅。 	
	说明 在选择主题前,请确保您主题中订阅状态为"已确 认",即当前订阅终端可用,否则可能不能收到告警通 知。	
	更多关于主题和订阅的信息,请参见《 消息通知服 务用户指南 》。	
每天发送告警 总条数	每天允许发送的告警总条数。 须知	30
	 如果每天的告警数超出该参数值,超出部分的告警信 息将不会发送通知。 	
	 告警通知无固定时间,系统每5分钟统计一次,并发送告警通知。 	
告警风险等级	选择产生告警通知的风险日志告警风险等级,可以 选择:	一日日
	● 高	
	 ● 中 	
	● 低	
CPU告警阈值 (%)	设置审计实例系统资源CPU告警的阈值。当超过该 阈值时,产生告警通知。	80
内存告警阈值 (%)	设置审计实例系统资源内存告警的阈值。当超过该 阈值时,产生告警通知。	80
磁盘告警阈值 (%)	设置审计实例系统资源磁盘告警的阈值。当超过该 阈值时,产生告警通知。	80

步骤7 单击"应用",完成设置。

----结束

10 查看监控信息

10.1 查看系统监控信息

通过查看数据库安全审计的系统监控信息,您可以了解系统资源和流量使用情况等信 息。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 请参考**开启数据库安全审计**成功开启数据库安全审计功能。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"实例列表",进入"实例列表"界面。
- 步骤4 单击需要查看系统监控信息的实例名称,进入实例概览页面。
- 步骤5 选择"系统监控"页签,进入系统监控页面。
- 步骤6 查看系统监控信息。

选择审计的时间("近30分钟"、"近1小时"、"今日"、"近7天"或"近30 天");或者单击^曲,选择开始时间和结束时间,查看指定的时间段的系统监控信 息。

图 10-1 查看系统监控信息

版版 系统监控 音響监控 操作日志 标签	
原紙盒腔 最低重整的词 2024/100 11 44 17 OMT-00 00	1250000 21504 40 1275 12575 (RedSH-GredsH)
系统 ■ 697 ■ CPU	流量 (MB/s) ■ 原来 ■ 第22 0.02
50%	0.0915
30% 20% 10%	0.009
05. 202411.08 202411.08 202411.08 202411.08 202411.08 202411.08 0100 0157 03.54 05.52 07.49 0546	2014/1/08 2024/1/08 2024/1/08 2024/1/08 2024/1/08 2024/1/08 2020 20157 20154 20154 20154 20169 20164
数期中心分区 ● 465-0681月、8月491.8808 5%	(@) 发统()区 233308时用。BH2R4508

----结束

10.2 查看告警信息

本章节介绍如何查看数据库安全审计的告警信息,以及当处理告警后如何确认告警。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 请参考**开启数据库安全审计**成功开启数据库安全审计功能。
- 请参考<mark>设置告警通知</mark>成功设置告警通知。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"实例列表",进入"实例列表"界面。
- 步骤4 单击需要查看告警信息的实例名称,选择"告警监控",进入告警监控页面。
- 步骤5 查看告警信息,如图10-2所示,相关参数说明如表10-1所示。

图 10-2 查看告警信息

8 835	系统监控	告警监控	操作日志	标签						
2	1 智列表									
	⇔⊟			✓ 0.38¥I	8 性研造,成输入关	建字把来				
	жена а			5822 A		法管闭的新成 合	WARNE O	曲认我表 台	1014 A	10.00
	2024/11/08 1	1:47:27 GMT+0	5:00	风险规则告誓		() 美国社		末确认	Risk SQL Risk Level: HIGH Risk	anu, 1909
	2024/11/08 1/	1:31:04 GMT+0	5:00	风险规则告誓		() 潮风論		未确认	Risk SQL Risk Level: HIGH Risk	ani), 809
	2024/11/08 1	1/29/59 (SMT+0	100	0.0000.000		0 #80		#28U	Risk SOL Risk Level HIGH Risk	201 809
	0 3034/11/08 1	19 53 OMT+0	1.00	(100-10-10-10-10-10-10-10-10-10-10-10-10-		0 2010			Birk SOL Birk Land HIGH Bir	2011 2010
		10.55 GMT-0	2.00	TRANSPORT		0 2010		4260	Plate SQL Plate Lawel HIGH Plate	

表 10-1 告警信息参数说明

参数名称	说明
发生时间	告警发生的时间。
告警类型	告警的类型,包括: 审计流量超限 CPU异常 内存异常 磁盘异常 审计容量不足 日志备份OBS失败 Agent异常 风险规则告警
告警风险等 级	告警的风险等级,包括: 高风险 中风险 低风险
恢复时间	恢复告警的时间。
确认状态	告警的确认状态。
描述	告警的相关描述信息。
操作	告警支持的操作,包括: • 确认 • 删除

您可以按照以下方法,查询指定的告警信息。

- 选择"发生时间范围"("近30分钟"、"近1小时"、"今日"、"近7天"、
 "近30天"或自定义时间),单击^Q,列表显示该时间段的告警信息。
- 选择"告警风险等级"("全选"、"高"、"中"或"低"),列表显示该级别的告警信息。
- 选择"告警类型",列表显示该类型的告警信息。
- 选择"确认状态"("未确认"或"已确认"),列表显示该状态的告警信息。

----结束

后续处理

 如果某条告警信息已经处理完成,您可以在该告警所在行的"操作"类,单击 "确认",标识该告警已确认并处理。告警确认后,告警状态为"已确认"。

图 10-3 确认告警信息

🗌 strie 0	告醫类型 ⊖	告罄风险等级 ⊖	States of the st	militis 🕈	mix O	展作
2024/11/08 14:53:13 GMT+08:00	风险规则告警	🙆 赛风险		未确认	Risk SQL, Risk Level: HIGH, Risk	确认 删除
2024/11/08 14:49:56 GMT+08:00	风险规则告警	() 英风险		未确认	Risk SQL, Risk Level: HIGH, Risk	确认一般种
2024/11/08 14:47:45 GMT+08:00	风险规则告警	() 英风险		未确认	Risk SQL, Risk Level: HIGH, Risk	确认一般种
2024/11/08 14:46:40 GMT+08:00	风险规则告警	() 英风险		未确认	Risk SQL, Risk Level: HIGH, Risk	确认一般种
2024/11/08 14:45:34 GMT+08:00	风险规则告誓	🙆 赛风险		未确认	Risk SQL, Risk Level: HIGH, Risk	确认一般种
2024/11/08 14:40:07 GMT+08:00	风险规则告誓	🕐 東风脸	-	未确认	Risk SQL, Risk Level: HIGH, Risk	1000、1000
2024/11/08 14:40:07 GMT+08:00	风险规则告誓	⑦ 東风脸		未确认	Risk SQL, Risk Level: HIGH, Risk	850. BIN
2024/11/08 10:47:27 GMT+08:00	风险规则告誓	O 東风脸		未造认	Risk SQL, Risk Level: HIGH, Risk	850, 509
2024/11/08 10:31:04 GMT+08:00	风险规则告誓	O 東风脸		未造认	Risk SQL, Risk Level: HIGH, Risk	45U, 509
2024/11/08 10:29:59 GMT+08:00	风险规则告誓	O 東风脸		未确认	Risk SQL, Risk Level: HIGH, Risk	400, <u>80</u> 9
2024/11/08 10:28:53 GMT+08:00	风险规则告誓	🕐 東风壯		未确认	Risk SQL, Risk Level: HIGH, Risk	御い, 田田
2024/11/08 10:28:53 GMT+08:00	风险规则告誓	🙆 赛风险	-	已编认	Risk SQL, Risk Level: HIGH, Risk	160. 20

您可以选中待确认的多条告警,单击"批量确认",同时确认多条告警信息。

图 10-4 批量确认告警信息

告誓列表

社園時以						
48	 〇、送祭開性同 	1造,或输入关键字提紧				
 ※生时间 ⁽¹⁾ 	白田美型 ⊖	告款风险等级 🖯	ikanstii) ⊖	Rilitz 🕈	ния Ө	10/11
2024/11/08 14:53:13 GMT+08:00	风险规则皆警	🕐 高风险	-	未确认	Risk SQL, Risk Level: HIGH, Ris	a
2024/11/08 14:49:56 GMT+08:00	风险规则告誓	() 周风脸	-	未确认	Risk SQL, Risk Level: HIGH, Ris	k
2024/11/08 14:47:45 GMT+08:00	风险规则告誓	() 海风险		来确认	Risk SQL, Risk Level: HIGH, Ris	a
2024/11/08 14:46:40 GMT+08:00	风险规则皆警	() 高风脸	-	未确认	Risk SQL, Risk Level: HIGH, Ris	a

 如果某条告警信息已经处理完成,您可以在该告警所在行的"操作"类,单击 "删除"。在弹出的确认框中,单击"确认",完成该条告警删除。

图 10-5 删除告警信息

告誓列表			删除告警信息			×		
正是收认			删除该告誓信息后将无法 創将删除以下告誓信息	位置.		- 1		
		- 或相入失量子统系	发生时间	告察类型	估發风險等级			
※生时间 ⁽¹⁾	四部类型 🖯	告答风险制	2024/11/08 10:28:	风险规则装蓄	() 高风脸		ана Ө	操作
2024/11/08 14:53:13 GMT+08:00	风险规则告誓	🙆 東风船					Risk SQL Risk Level: HIGH Risk	建议 重制
2024/11/08 14:49:56 GMT+08:00	风险规则监警	🙆 潮风地					Risk SQL, Risk Level: HIGH, Risk	碑以 删除
2024/11/08 14:47:45 GMT+08:00	风险规则告誓	🙆 東风絵		-	未續认	-	Risk SQL, Risk Level: HIGH, Risk	890. 1979
2024/11/08 14:45:40 GMT+08:00	风险规则装置	🚺 萬风脸			来确认		Risk SQL, Risk Level: HIGH, Risk	确认 删除
2024/11/08 14:45:34 GMT+08:00	风险规则告誓	🙆 東风脸			未确认		Risk SQL, Risk Level: HIGH, Risk	49 10、1919
2024/11/08 14:40:07 GMT+08:00	风险规则告誓	🙆 東风脸			未确认		Risk SQL, Risk Level: HIGH, Risk	49 10、1919
2024/11/08 14:40:07 GMT+08:00	风险规则监警	🙆 憲风脸			未确认		Risk SQL, Risk Level: HIGH, Risk	确认 删除
2024/11/08 10:47:27 GMT+08:00	风险规则告誓	🙆 東风脸			未确认		Risk SQL, Risk Level: HIGH, Risk	49 10、1919
2024/11/08 10:31:04 GMT+08:00	风险规则监警	🙆 憲风脸			未确认		Risk SQL, Risk Level: HIGH, Risk	确认 删除
2024/11/08 10:29:59 GMT+08:00	风险规则告誓	🙆 東风脸			未确认		Risk SQL, Risk Level: HIGH, Risk	493、1939
2024/11/08 10:28:53 GMT+08:00	风险规则监警	🙆 萬风脸			来确认		Risk SQL, Risk Level: HIGH, Risk	碑以 删除
2024/11/08 10:28:53 GMT+08:00	风险规则告誓	🕐 東风絵			日織以		Risk SQL, Risk Level: HIGH, Risk	886A 8870

11 备份和恢复数据库审计日志

数据库安全审计支持将数据库的审计日志备份到OBS桶,实现高可用容灾。您可以根 据需要备份或恢复数据库审计日志。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 请参考**开启数据库安全审计**成功开启数据库安全审计功能。

注意事项

- 执行备份后,审计日志将备份到对象存储服务上,系统自动为您创建桶,桶将按用量收费。有关对象存储服务的计费详情,请参见价格详情。
- 有关审计日志的保存说明,请参见数据库安全审计的审计数据可以保存多久?。

OBS 细粒度授权

DBSS备份和恢复需要OBS授权,没有IAM授权相关权限的用户,需要由有Security Administrator权限的用户手动进行授权。

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ——,选择"管理与监管 > 统一身份 认证服务 IAM"。
- 步骤3 选择左侧导航树的"权限管理 > 权限",单击右上角的"创建自定义策略"。
- **步骤4** 填写策略参数。策略名称为"DBSS OBS Agency Access",策略配置方式选择 "JSON视图"。填写策略内容如下:

```
"Version": "1.1",

"Statement": [

{

"Effect": "Allow",

"Action": [

"obs:object:PutObjectVersionAcl",

"obs:object:GetObjectVersion",

"obs:object:GetObject",

"obs:object:GetObject",

"obs:object:GetObjectVersionAcl",

"obs:bucket:HeadBucket",
```

			"obs:object:GetObjectAcl", "obs:bucket:CreateBucket", "obs:bucket:ListBucket",
			"obs:object:PutObject"
			1,
			"Resource": [
			"OBS:*:*:object:*".
			"OBS:*:*:bucket: <i>OBS桶1的名称</i> ".
			"OBS:*:*:bucket: OBS桶2的名称" //可添加多个桶。
]
		l	1
	1	J	
ι	1		
ſ			



图 11-1 创建自定义策略

权限	创建自定义策略	
0	自定义策略是对系	统策略的扩展和补充,您可以创建自定义策略以实现定制的权限管理。 🕜
7	★策略名称	DBSS OBS Agency Access
	策略配置方式	可视化视图 JSON视图
۲.	r 策總內容	<pre>1 * { 2</pre>
		① 从已有策略复制
	策略描述	请输入策略描述 (可选)
		0/256 4
	作用范围	**
		· 确定 · 取消 · · · · · · · · · · · · · · · · ·

步骤5选择左侧导航树上的"委托",单击右上角"创建委托"。

步骤6 填写委托参数。委托名称为"dbss_depend_obs_trust",委托类型选择"云服务", 云服务选择"DBSS"。如<mark>图11-2</mark>所示。
图 11-2 创建委托

委托 / 创建委托	
* 委托名称	dbss_depend_obs_trust
* 委托类型	 普通账号 将账号内资源的操作权限委托给其他华为云账号。 云服务
	将账号内资源的操作权限委托给华为云服务。
* 云服务	DBSS
★ 持续时间	永久 >
描述	请输入委托信息。
	0/255 4
	完成 取消

步骤7 单击"立即授权",勾选**步骤4**中创建的自定义策略,将权限(DBSS OBS Agency Access)添加到委托(dbss_depend_obs_trust) 中,如<mark>图11-3</mark>所示。单击右下角的 "下一步"。

图 11-3 选择策略

< 授权		
1 3	38 (2) REG-MECH (3) Ref	
委托"dt	is_depend_obs_trust1存拥有所遗策略	
	223(1) 从其他区域项目要制权限	28#21 ~
•	名称	类型
	DBSS OBS Agency Access	自定义策略
	AAD FullAccess DDoS電影图题条有切类	系统策略
	AAD ReadonlyAccess DDoSR版的后述可能代码,拥有如此代码的用户代源监查着DDoSR版的	系统旗略

步骤8 授权范围选择"所有资源",单击右下角的"确定",显示授权成功如<mark>图11-4</mark>所示, 单击"完成"后等待15分钟授权生效。

图 11-4 完成授权

授权			
② 选择策略 ———— (>) 设置最小援	双范围 ———— 3 完成		
		ビー ビー ジ ガロのの ガロの ジョン ジェン ガロの ガロの ジェン ガロの ジェン ガロの ガロの ジェン ガロの ジェン ジェン	R管理·授权管理] 列表宣著
名称 🖯	作用范围	类型 ↔	描述 ⊖
DBSS OBS Agency Access	所有资源	自定义策略	
		大規	

----结束

自动备份数据库审计日志

步骤1 登录管理控制台。

- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"设置"。
- **步骤4** 在"选择实例"下拉列表框中,选择需要设置备份的实例,选择"备份与恢复"页签。
- **步骤5** 单击"修改自动备份设置",在弹出的对话框中,设置自动备份参数,相关参数说明 如表11-1所示。

图 11-5 "设置自动备份"对话框

设置自动备份

 1. 审计日志将备份到对象存储服务的OBS幅中,OBS幅按照存储用量收费,由对象存储服务结算。 2. 开启自动备份,请先选择OBS幅作为审计日志备份桶。DBSS服务将获取该桶的读写权限。 					
自动备份					
备份周期	每天	~			
开始时间	2024/04/02 19:38:58				
桶名称	请选择桶 可选择已有OBS桶或默认桶,默认桶不存在时将被 OBS服务默认使用按需计费模式,不同区域及计费	○ 別時到該桶 △ 創建新认桶 2月动创建 時项产生费用不同。 了解计费详情			
文件导出目录	请输入文件夹名称				
自动备份授权	同意DBSS服务获取该OBS幅读写权限,用于 注:授权成功后预计15分钟,自动备份才会生效	审计日志备份导出 (取消) 确定			

表 11-1 自动备份参数说明

参数名称	说明	取值样例
自动备份	开启或关闭自动备份。	
	• 🕶 : _{开启}	
	• 一 :关闭	
备份周期	选择自动备份的周期,可以选择:	
	● 每天	
	● 每小时	
开始时间	单击 ^国 ,选择开始备份的时间。	2020/01/14 20:27:08

参数名称	说明	取值样例
桶名称	设置备份使用的OBS桶名称,可以选择: 创建默认桶 选择已有桶 说明 单击"创建默认桶",将进行OBS授权,用于审计日志备份导出。 审计日志只能导出到DBSS服务创建的桶。 	20f18-7a5a-4 042
文件导出目录	在OBS桶中创建备份文件的目录。	test
自动备份授权	 投置自动备份任务时,请先进行自动备份授权。勾线自动备份授权后,将同意DBSS服务获取该OBS桶读写权限,用于审计日志备份导出。 注意 授权成功后预计15分钟,自动备份才会生效。 	

步骤6 单击"确定",设置完成。

🛄 说明

自动备份设置完成后,当数据库新产生数据时,新产生的数据备份会在1小时后完成备份,届时 可查看备份情况。

----结束

恢复数据库审计日志

数据库审计日志备份成功后,您可以根据需要恢复数据库的审计日志。

须知

日志数据恢复风险较大,在恢复日志数据前,请您确认备份的日志数据的准确性或完整性。

步骤1 登录管理控制台。

- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"设置"。
- **步骤4** 在"选择实例"下拉列表框中,选择需要恢复日志的实例,选择"备份与恢复"页签。
- 步骤5 在需要恢复数据库审计的备份日志所在的"操作"列,单击"恢复日志"。

图 11-6 恢复日志

日志名称 🖯	育份时间 🖯	文件大小 🖯	备份方式 🕀	育份范围 ⇔	sha256 🖯	任务状态 令	操作
auto_backup_20241107	2024/11/0	20 Byte	自动备份	2024/11/07 00:00:00 GMT+08:00-2024/11/07 23:59:59 GM	59869db34853933b239f1e2219cf7d431d	😔 自动	恢复日志 翻除
auto_backup_20241106	2024/11/0	20 Byte	自动备份	2024/11/06 00:00:00 GMT+08:00-2024/11/06 23:59:59 GM	59869db34853933b239f1e2219cf7d431d	😔 自动	依复日志 删除

步骤6 在弹出的提示框中,单击"确定"。

图 11-7 确认恢复审计日志

确定要恢复审计日志auto_backup_20241107-00_00~23_59[×] 吗?

数据恢复风险较大,请您先确认备份准确性或完整性,谨慎操作!



----结束

风险导出

开启风险导出可以帮助您导出风险等级高的操作日志到对象存储服务上,并自动为您 创建桶,桶按照存储用量收费。

🛄 说明

开启风险导出前,需进行OBS细粒度授权。

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"设置"。
- 步骤4 在"选择实例"下拉列表框中,选择需要导出风险的实例,选择"风险导出"页签。
- **步骤5** 在需要导出风险日志的数据库右侧操作栏单击 💭 ,开启风险导出 。

图 11-8 开启风险导出

风险导出设置	风险导出设置					
() 选择属性的	病选,或输入关键字搜索					
序号 ⊖	数据库名称 ⊖	IP地址端口 令	风险导出 令			
1	test-mysql	3306	关闭			
2	rds	3306	关闭			
3	test	3306	美 闭			

步骤6 开启风险导出后DBSS服务将自动创建OBS桶,作为风险日志导出桶。

- 桶名称:可选择"创建默认桶"和"使用已有桶"。
- 文件导出目录:在OBS桶中创建风险导出文件的目录。
- 风险导出授权:设置风险导出桶时,请先进行风险导出授权。勾线风险导出授权
 后,将同意DBSS服务获取该OBS桶读写权限,用于风险日志导出。

⚠ 注意

授权成功后预计15分钟,风险导出才会生效。

图 11-9 自动创建 OBS 桶

设置风险导出桶

1. 风险日 2. 开启版	日志將导出到对象存储服务的OBS桶中,OBS桶按照存储用最收费,由对象存储服务结算。 J险导出,请先选择OBS桶作为风险日志导出桶。DBSS服务将获取该桶的读写权限。
桶名称	请选择桶 ~ C 跳转到该桶 创建默认桶
	可选择已有OBS桶或默认桶,默认桶不存在时将被自动创建 OBS服务默认使用按需计费模式,不同区域及计费项产生费用不同。 了解计费详情
文件导出目录	请输入文件夹名称
风险导出授权	 同意DBSS服务获取该OBS桶读写权限,用于风险日志导出 注:授权成功后预计15分钟,风险导出才会生效
	取消 确定

----结束

12 _{其他操作}

12.1 管理数据库安全审计实例

成功购买数据库安全审计实例后,您可以查看实例信息,开启、重启或关闭实例。

前提条件

- 重启实例和关闭实例前,请确认实例的状态为"运行中"。
- 开启实例前,请确认实例的状态为"已关闭"。

查看实例信息

- 步骤1 登录管理控制台。
- 步骤3 在左侧导航树中,选择"实例列表",进入"实例列表"界面。
- 步骤4 查看数据库安全审计实例信息,相关参数说明如表12-1所示。

图 12-1 查看数据库安全审计实例信息

例名称/変源10 ⊖	秋恋 0	实制现储 🖯	计费模式 ⊖	版本 Θ	已关联数据库-数据库总数 ⊖	企业项目 ⊖	操作
855-	0 运行中	入门版	包年/包月 29天后到期	24.09.03.141647	0/1	default	配置审计规则 续唐 更多 >
899.							

🗀 说明

- 单击实例名称,可以查看该实例的概览信息。
- 可以在列表上方的筛选框中根据实例名称、状态、实例规格、资源ID、计费模式、版本或企业项目,搜索指定的实例。

表 12-1 实例信息参数说明

参数名称	说明
实例名称/资源ID	实例的名称和资源ID。资源ID由系统自动生成。
实例规格	实例的规格。
计费模式	实例的计费模式(包年/包月)和到期时间。
版本	数据库安全审计的实例版本。
状态	实例当前的运行状态,包括: 运行中 创建中 故障 已关闭 已冻结 公安冻结 违规冻结 未实名认证冻结 合作伙伴冻结 创建失败
已关联数据库/数 据库总数	实例的已关联的数据库和实例可以支持关联的数据库总数。
企业项目	该实例的企业项目名称。
操作	对该实例进行相关操作: 配置审计规则 续费 开启 关闭 重启 查看详情 查看监控指标 开启自动续费 退订 释放 删除

🛄 说明

根据需要,您还可以对实例执行以下操作:

重启

在需要重启的实例所在行的"操作"列,选择"更多 > 重启",在弹出的对话框中,单击 "确定",可以重启该实例。

开启

在需要开启的实例所在行的"操作"列,选择"更多 > 开启",在弹出的对话框中,单击 "确定",可以开启该实例。

关闭

在需要关闭的实例所在行的"操作"列,选择"更多 > 关闭",在弹出的对话框中,单击 "确定",关闭该实例。关闭实例后,系统将停止对该实例上的数据库进行安全审计。

删除

在需要删除创建实例失败所在行的"操作"列,选择"更多 > 删除",在弹出的对话框中, 单击删除,删除创建失败的实例。实例删除后,实例列表不再显示该条实例。

查看详情
 在创建实例失败所在行的"操作"列,选择"更多>查看详情",在弹出的对话框中,可查
 看实例创建失败详情。

----结束

12.2 查看实例概览信息

通过查看数据库安全审计实例的概览信息,您可以查看实例的基本信息、网络配置信息和关联数据库信息。

前提条件

数据库安全审计实例的状态为"运行中"。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"实例列表",进入"实例列表"界面。
- 步骤4 单击需要查看信息的实例名称,进入实例概览页面。
- **步骤5** 查看实例的"基本信息"、"网络配置信息"和"关联数据库",相关参数说明如表 12-2所示。

图 12-2 查看实例概览信息

概范	系统监控 告誓监控 操作日志 标签	
基本信	8	
2928	BBS Z	住認短期 基础现于支持3个实例
实例D	ď	可用区
保注	a	fuelso Billion
15年	24.09.03.141647	(EUD)1/FI 2024/10/31 15:01.49 GMT+08:00
计表现	C 包括10日	30801FI 2024/11/00 23:59:59 GMT+00:00
240	C52410311447EV28X	MGA732 19
20030	1 新聞是人意問題 0	
网络配	置信息	
唐 9383	TE VPC-IPV-	子网 subnet-lpv4
중순법	l.	内局护
关联数	R#	「「「「「」」の「「」」の「「」」の「「」」の「「」」の「「」」の「「」」の
SQLS	ERVER tosa	

表 12-2 实例概览信息参数说明

类别	参数名称	说明
基本信息	实例名称	实例的名称。单击名称后的之,可以修改实例名称。
	实例ID	实例的ID,由系统自动生成。
	可用区	实例所在的可用区。
	版本	您创建DBSS实例时对应的DBSS实例版本,您不同时 间创建的DBSS实例的版本可能会有差别。 DBSS实例版本影响的范围: • 支持的数据库类别 • 支持的数据库版本
	备注	实例的备注信息。单击备注后的 <mark>之</mark> ,可以修改备注信 息。
	性能规格	实例的性能规格。
	创建时间	实例创建的时间。
	到期时间	实例到期的时间。
	企业项目	该实例的企业项目名称。
	计费模式	实例的计费模式(包年/包月)。
	订单号	购买该实例的订单号。单击订单号,可以查看购买该 实例的详情订单信息。
	到期策略	实例到期后的策略,包括: • 自动续费 • 到期进入宽限期
	剩余天数	实例到期剩余天数。
网络配置	虚拟私有云	实例所在的虚拟私有云。
信息	安全组	实例所在的安全组。

类别	参数名称	说明
	子网	实例所在的子网。
	内网IP	实例的IP地址。
关联数据 库	-	实例已关联的数据库信息。 单击"管理数据库",跳转到数据库列表页面。有关 添加数据库的详细操作,请参见 <mark>步骤一:添加数据</mark> <mark>库</mark> 。

-----结束

12.3 管理添加的数据库和 Agent

成功添加数据库后,您可以查看数据库信息,关闭、删除数据库。如果数据库添加了 Agent,您还可以查看Agent信息、关闭或删除Agent。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 请参见添加数据库成功添加数据库。
- 关闭数据库前,请确认数据库的"审计状态"为"已开启"。

查看数据库信息

步骤1 登录管理控制台。

- 步骤3 在左侧导航树中,选择"数据库列表",进入"数据库列表"界面。
- 步骤4 在"选择实例"下拉列表框中,选择查看的数据库所属的实例。
- 步骤5 查看数据库信息,相关参数说明如表12-3所示。

可以在列表上方的搜索框中选择属性筛选,或输入关键字搜索,搜索指定的数据库。

	表 12-	-3 数	据库信	息参数	说明
--	-------	------	-----	-----	----

参数名称	说明
数据库信息	数据库的名称、类型以及版本信息。
选择字符集	数据库的编码字符集。
IP地址/端口	数据库的IP地址和端口。
实例名	数据库的实例名称。
操作系统	数据库运行的操作系统。

参数名称	说明
审计状态	数据库的审计状态,包括:● 已开启● 已关闭
Agent	单击"添加Agent",可以为数据库添加Agent。

🛄 说明

您可以根据使用需求,对添加的数据库执行以下操作:

- 关闭
 - 在需要关闭的数据库所在行的"操作"列,单击"关闭"后,在弹出的提示框中,单击 "是",数据库的"审计状态"为"已关闭"。
 - 关闭数据库后,数据库安全审计将停止对该数据库进行安全审计。
- 删除
 - 在需要删除的数据库所在行的"操作"列,单击"删除"后,在弹出的提示框中,单击 "确定",删除该数据库。
 - 删除数据库后,如果需要对该数据库进行安全审计,请重新添加该数据库。

----结束

查看 Agent 信息

步骤1 登录管理控制台。

- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"数据库列表",进入"数据库列表"界面。
- 步骤4 在"选择实例"下拉列表框中,选择查看的Agent所属的实例。
- 步骤5 单击数据库左侧的 V 展开Agent的详细信息,相关参数如表 Agent参数说明所示。

表 12-4 Agent 参数说明

参数名称	说明
Agent ID	Agent的ID,由系统自动生成。
安装节点类型	安装节点的类型,包括"数据库端"或"应用端"。
安装节点IP	安装Agent的节点的IP地址。
操作系统	安装Agent运行的操作系统。
审计网卡名称	安装节点的网卡名称。

参数名称	说明
CPU阈值(%)	安装节点的CPU阈值,缺省值为"80"。
	说明 当安装节点的CPU超过设定的阈值时,Agent将停止工作。您可以直 接升级服务器的CPU。
内存阈值(%)	安装节点的内存阈值,缺省值为"80"。
	说明 当安装节点的内存超过设定的阈值时,Agent将停止工作。您可以直 接升级服务器的内存。
通用	Agent是否为通用Agent。
SHA256校验值	Agent安装包的校验值。
运行状态	安装节点的运行状态。

🗀 说明

您可以根据使用需求,对添加的Agent执行以下操作:

- 关闭
 - 在需要关闭的Agent所在行的"操作"列,单击"关闭"后,在弹出的提示框中,单击 "是",Agent状态为"关闭"。
 - 关闭Agent后,数据库安全审计将停止对连接该Agent的数据库进行安全审计。
- 删除
 - 在需要删除的Agent所在行的"操作"列,单击"删除"后,在弹出的提示框中,单击 "确定",删除该Agent。
 - 删除Agent后,如果需要对连接该Agent的数据库进行安全审计,请重新添加Agent。

----结束

12.4 卸载 Agent

在数据库端或应用端的节点安装Agent后,当不需要审计数据库时,您可以在安装 Agent的节点卸载Agent。

前提条件

已在安装节点安装了Agent程序。

在 Linux 操作系统上卸载 Agent

- **步骤1** 使用跨平台远程访问工具(例如PuTTY)以**root**用户通过SSH方式,登录已安装Agent的节点。
- **步骤2**执行以下命令,进入Agent安装包"xxx.tar.gz"解压后所在目录。 cd Agent安装包解压后所在目录
- 步骤3 执行以下命令,查看是否有卸载脚本"uninstall.sh"的执行权限。 ॥

- 如果有卸载脚本的执行权限,请执行步骤4。
- 如果没有卸载脚本的执行权限,请执行以下操作:
 - a. 执行以下命令,添加卸载脚本执行权限。 chmod +x uninstall.sh
 - b. 确认有安装脚本执行权限后,请执行<mark>步骤4</mark>。

步骤4 执行以下命令,卸载Agent。

sh uninstall.sh

如果界面回显以下信息,说明卸载成功。

uninstall audit agent... exist os-release file stopping audit agent audit agent stopped stop audit_agent success service audit_agent does not support chkconfig uninstall audit agent completed!

----结束

在 Windows 操作系统上卸载 Agent

- 步骤1 进入Agent安装文件的目录。
- 步骤2 双击"uninstall.bat"执行文件,卸载Agent。
- 步骤3 验证Agent已卸载成功。
 - 1. 打开任务管理器,查看"dbss_audit_agent"进程已停止。
 - 2. 查看Agent安装目录,安装目录内容已经全部删除。

-----结束

12.5 管理审计范围

添加审计范围后,您可以查看审计范围信息,也可以启用、编辑、禁用或删除审计范 围。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 请参见添加审计范围成功添加审计范围。
- 启用、编辑和删除审计范围前,请确认审计范围的状态为"已禁用"。
- 禁用审计范围前,请确认审计范围的状态为"已启用"。

注意事项

数据库安全审计默认提供一条"全审计规则"的审计范围,可以审计所有连接数据库 安全审计实例的数据库。该审计规则默认开启,您只能禁用或启用该审计规则。

查看审计范围信息

步骤1 登录管理控制台。

- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"审计规则"。
- 步骤4 在"选择实例"下拉列表框中,选择需要查看审计范围的实例。
- 步骤5 查看审计范围信息,相关参数说明如表12-5所示。

可以在列表上方的搜索框中选择属性筛选,或输入关键字搜索,搜索指定的审计范 围。

图 12-3 查看审计范围信息

(添加爾计范围	D .							
○ 法評議性等	选,或输入关键字搜索							
座号 ⊖	名称 Θ	SIGNP 0	源IP 🖯	aswe⊡ ⊖	数据库名称 ⊖	数据库账户 ⊖	秋志 0	操作
1	update	any	any	any	全部数据库	any	○ 已禁用	扁用 網續 删除
2	全审计规则	any	any	any		any	 已自用 	禁用 编辑 删除

表12-5 审计范围信息参数说明

参数名称	说明
名称	审计范围的名称。
例外IP	该审计范围内的白名单IP。
源IP	访问数据库的IP地址或IP地址段。
源端口	审计的IP地址端口。
数据库名称	审计范围的数据库。
数据库账户	数据库的用户名。
状态	审计范围的状态,包括:
	● 已启用
	● 已禁用

🛄 说明

根据需要,您还可以对审计范围执行以下操作:

● 启用

在需要启用的审计范围所在行的"操作"列,单击"启用",数据库安全审计将对该审计范围的数据库进行审计。

- 编辑(仅自定义创建审计范围的支持)
 在需要编辑的审计范围所在行的"操作"列,单击"编辑",在弹出的对话框中,您可以修改审计范围。
- 禁用

在需要禁用的审计范围所在行的"操作"列,单击"禁用",在弹出的对话框中,单击 "是",可以禁用该审计范围。禁用审计范围后,该审计范围规则将不在审计中执行。

• 删除(仅自定义创建审计范围的支持)

在需要删除的审计范围所在行的"操作"列,单击"删除",在弹出的对话框中,单击"确 定",可以删除该审计范围。删除审计范围后,如果需要对该审计范围进行审计,请重新添 加该审计范围。

----结束

12.6 查看 SQL 注入检测信息

本章节介绍如何查看数据库安全审计的SQL注入检测信息。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 请参考开启数据库安全审计成功开启数据库安全审计功能。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"审计规则"。
- 步骤4 在"选择实例"下拉列表框中,选择需要查看SQL注入检测信息的实例。选择"SQL注入"页签。
- 步骤5 查看SQL注入检测信息,相关参数如表12-6所示。

可以在列表上方的搜索框中选择属性筛选,或输入关键字搜索,搜索指定的SQL注入 规则。

在"操作"列单击"设置优先级",可以修改SQL注入规则的优先级。

图 12-4 查看 SQL 注入检测信息

() 法経歴性等	Q. 这场银行杂选、或最大关键字程序							
降号 ⊖	名称 ⊖	SQL命令特征 ⊖	风险等级 ⊖	RE O	操作			
1	test240403	正则顺达式	• 65	○ 己酰用	设置优先级 启用 编辑 勤除			
2	MYSQL报槽型SQL注入	正则表达式	• %	○ 已度用	设置优先级 禁用 编唱 勤除			
3	HAVING授權SQL注入	正则表达式	• #	 已雇用 	设置优先级 祭用 编辑 數除			
4	UNION就会置限SQL注入	ERIMANT	• #	o Ber	2200.542 MH 941 200			
5	时间型SQL注入	正则表达式	• 中	 已应用 	设置优先级 禁用 编辑 數除			
6	個編式SQL注入1	正则表达式	• 商	 已展用 	设置优先级 祭用 编辑 數除			
7	個聯式SQLI主入2	正则表达式	• 至	o Ber	设置优先级 然用 编唱 勤助			
8	布尔型SQL注入	正则表达式	• ā	 已应用 	设置优先级 禁用 编辑 數除			
9	时间型SOL注入2	正则表达式	• 商	 已后用 	设置优先级 祭用 偏振 動脉			
10	带外注入	正则表达式	• %	o Ber	设置优先级 禁用 编辑 勤除			

表 12-6 SQL 注入检测信息参数说明

参数名称	说明
名称	SQL注入检测的名称。
SQL命令特征	SQL注入检测的命令特征。
风险等级	SQL注入检测的风险等级,包括: • 高 • 中 • 低 • 无风险
状态	SQL注入检测的状态,包括: • 已启用 • 已禁用
操作	SQL注入规则的操作,包括: 设置优先级 禁用 编辑 删除

----结束

12.7 管理风险操作

成功添加风险操作后,您可以查看风险操作信息,也可以启用、编辑、禁用、删除风 险操作,或设置风险操作优先级。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 请参见添加风险操作成功添加风险操作。
- 启用风险操作前,请确认风险操作的状态为"已禁用"。

• 禁用风险操作前,请确认风险操作的状态为"已启用"。

设置优先级

步骤1 登录管理控制台。

- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"审计规则"。
- **步骤4**在"选择实例"下拉列表框中,选择需要设置风险操作优先级的实例。选择"风险操作"页签。
- 步骤5 在需要设置优先级的风险操作所在行的"操作"列,单击"设置优先级"。

图 12-5 设置风险操作的优先级

(18-2010-04-12-Bet	n=					
 Q. 选择属性部 	等选,或输入关键字搜索					Q
☆号 令	名称 0	分类 😌	特征 🖯	风险等级 ⊖	秋志 令	操作
1	數据库拖库检测	OPERATE	客户牌(Any)操作[SELECT]对象[• 商	○ 已启用	设置优先级 禁用 更多 ~
2	数据库偿SQL检测	OPERATE	春户ı拥[Any]操作[REVOKE,DRO		0 已启用	设置优先级 葉用 更多 ~
3	谢他DROP操作	OPERATE	客户號[Any]膜作[DROP]对象[Any	y] • 商	○ 已扁用	设置优先级 禁用 更多 >

步骤6 在弹出的对话框中,选择"优先级"后,单击"确定",完成设置。

图 12-6 设置优先级

设置优	先级		
优先级	1	~	
			取消 确定

----结束

查看风险操作信息

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"审计规则"。
- 步骤4 在"选择实例"下拉列表框中,选择需要查看风险操作的实例。
- 步骤5选择"风险操作"页签。
- 步骤6 查看风险操作信息,相关参数说明如表12-7所示。

可以在列表上方的搜索框中选择属性筛选,或输入关键字搜索,搜索指定的风险操 作。

图 12-7 查看风险操作信息

	D					
Q 选择属性第	选,或输入关键字搜索					Q
座号 ⊖	名称 🖯	分类 🖯	特征 0	风险等级 ↔	NOS O	操作
1	散還库拖库检测	OPERATE	審户譜[Any]操作[SELECT]对像[• 	0 已启用	设置优先级 禁用 更多 ~
2	数据库信SQL检测	OPERATE	春户]][Any]摄作[REVOKE,DRO	• 低	0 已启用	设置优先级 葉用 更多 ~
3	离危DROP操作	OPERATE	套户讀[Any]摄作[DROP]对象[Any]	• <u>ä</u>	 已扁用 	设置优先级 禁用 更多 >

表 12-7 风险操作信息参数说明

参数名称	说明
名称	风险操作的名称。
分类	风险操作的类别。
特征	风险操作的特征。
风险等级	风险操作的风险级别,包括: • 高 • 中 • 低 • 无风险
状态	风险操作的状态,包括: • 已启用 • 已禁用

🛄 说明

根据需要,您还可以对风险操作执行以下操作:

在需要启用的风险操作所在行的"操作"列,单击"启用",数据库安全审计将对该风险操 作进行审计。

● 编辑

在需要编辑的风险操作所在行的"操作"列,选择"更多 > 编辑",在风险操作界面,您可 以修改风险操作。

禁用

在需要禁用的风险操作所在行的"操作"列,单击"禁用",在弹出的对话框中,单击 "是",可以禁用该风险操作。禁用风险操作后,该风险操作规则将不在审计中执行。

删除

在需要删除的风险操作所在行的"操作 > 更多"列,选择"更多 > 删除",在弹出的对话框 中,单击"确定",可以删除该风险操作。删除风险操作后,如果需要对该风险操作的规则 进行安全审计,请重新添加该风险操作。

```
----结束
```

12.8 管理隐私数据保护规则

您可以查看隐私数据保护规则,启用、编辑、禁用或删除脱敏规则。

文档版本 01 (2024-11-28)

前提条件

数据库安全审计实例的状态为"运行中"。

查看隐私数据保护规则信息

步骤1 登录管理控制台。

- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"审计规则"。
- 步骤4 在"选择实例"下拉列表框中,选择查看隐私数据保护规则的实例。
- 步骤5选择"隐私数据保护"页签。

🛄 说明

仅自定义创建的规则可以使用编辑和删除功能,默认的规则仅可使用启用和禁用功能。

步骤6 查看规则信息,相关参数说明如表12-8所示。

🛄 说明

• 存储结果集

建议关闭 。 关闭后,数据库安全审计分析平台将不会存储用户SQL语句的结果集。 如果用于PCI DSS/PCI 3DS CSS认证,禁止开启。 注:结果集存储只支持agent方式审计数据库。

• 隐私数据脱敏

建议开启 。开启后,您可以通过配置隐私数据脱敏规则,防止数据库敏感信息泄 露。

图 12-8 查看脱敏规则信息

存储结果集 审计分析平台将 开启状态	存续用户SQL谱句的结果集,可能包含数数	野数据,建议关闭。(如用于 PCI	DSS / PCI BDS CSS认证,此继须禁止开曲)			
隐私数据脱敏						
通过编写脱敏规	则,防止敏感数描泄露,建议开启。					
开启状态 🧲	D					
(添加自定义)	规则					
Q 选择属性的	筛选,或输入关键字搜索					
座号 令	規则名称 ⇔	規則类型 令	正则表达式 令	曹操値 令	状态 令	操作
1	论服号	RtiJ.			○ 已启用	禁用 编辑 删除
2	军官证号	BGA.			 已與用 	禁用 编辑 删除
3	民族	Rtij.			○ 已启用	禁用 编辑 删除
4	银行卡号	RGA			 已启用 	葉用 编辑 删除
5	身份证券	默认	-		 已启用 	禁用 编辑 删除
6	GPS信息	数は人			 已息用 	禁用 编辑 删除

表 12-8 脱敏规则信息参数说明

参数名称	说明
规则名称	该规则的名称。

参数名称	说明		
规则类型			
	● 默认		
	• 自定义		
正则表达式	该规则的正则表达式。		
替换值	正则表达式脱敏后对应的替换值。		
状态	该规则的启用状态,包括:		
	 ● 已启用 		
	● 已禁用		

🛄 说明

根据需要,您还可以对规则执行以下操作:

禁用

在需要禁用的规则所在行的"操作"列,单击"禁用",可以禁用该规则。禁用该规则后, 系统将不能使用该数据脱敏规则。

● 编辑

在需要修改信息的规则所在行的"操作"列,单击"编辑",在弹出的对话框中,修改规则 信息。

删除

在需要删除的规则所在行的"操作"列,单击"删除",在弹出的提示框中,单击"确 定",删除该规则。

----结束

12.9 管理审计报表

数据库安全审计默认提供一条"全审计规则"的审计范围,可以对成功连接数据库安 全审计的所有数据库进行审计。添加的数据库连接到数据库安全审计实例后,您可以 查看报表模板信息和报表结果。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 请参考开启数据库安全审计成功开启数据库安全审计功能。
- 请参见步骤一:生成报表成功生成审计报表。

查看报表信息

步骤1 登录管理控制台。

文档版本 01 (2024-11-28)

- 步骤3 在左侧导航树中,选择"报表"。
- 步骤4 在"选择实例"下拉列表框中,选择查看报表信息的实例。
- 步骤5 查看报表信息。

图 12-9 查看报表信息

表结果 报表管理							
Q 选择属性筛选,或输入关	建宁注发						
提表名称 ⇔	关联数据库 ↔	报表类型 ⊖	生成时间 令	橋式 ⊖	#65 ⊕		操作
数据库安全综合报表	全部数据库	实时报表	2024/11/08 09:51:27 GMT+08:00	pdf		100%	预范 下數 删除
数据库安全综合报表	全部数据库	日报	2024/10/10 16:05:26 GMT+08:00	pdf		100%	预泡 下號 删除
数据库安全综合报表	全部数据库	日报	2024/09/06 16:13:37 GMT+08:00	pdf		100%	预泡下就删除
客户講IP分析报表	全部数据库	实时报表	2024/07/30 16:12:34 GMT+08:00	pdf		100%	预泡 下航 删除
数据库服务器分析报表	全部数据库	实时报表	2024/07/30 16:11:47 GMT+08:00	pdf		100%	预选下载 删除
客户通IP分析报表	全部数据库	实时报表	2024/07/30 16:10:43 GMT+08:00	pdf		100%	预泡 下载 删除

🛄 说明

- 可以在列表上方的搜索框中选择属性筛选,或输入关键字搜索,搜索指定的报表。
- 报表类型"实时报表"为系统自动生成,报表格式统一为PDF格式。
- 在需要删除的报表所在行的"操作"列,单击"删除",在弹出的对话框中,单击"确定",您可以删除该报表。删除报表后,如果查看该报表结果,需要重新手动生成报表。

----结束

查看报表模板信息

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"报表"。
- 步骤4 在"选择实例"下拉列表框中,选择需要查看报表模板的实例。
- 步骤5选择"报表管理"页签。
- 步骤6 查看报表模板信息。

图 12-10 查看报表模板列表

泉田平 数表管理					
〇、造券属性等选、或输入关键字提案					0
报表模板名称 ⊖	关联数据库 🖯	実理 0	描述 ⊖	计划任务状态 🖯	操作
数据库安全综合报表	全部数据库	综合探察	数据库安全综合报表	○ 已开启(每天)	设置任务 立即生成很表
数据库安全合规报表	全部数据库	合规报表	数据库安全合规报表	 已关闭(每周) 	设置任务 立即生成报表
SOX-萨班斯报表	全部数据库	合现报表	SOX-萨班斯报题	 已共闭(每周) 	设置任务 立即生成报表
数選库服务醫分析报表	全部数据库	数据库专项报表	数据库服务器分析报表	 已关闭(每周) 	设置任务 立即生成报表
客户通IP分析报表	全部数据库	客户请专项报表	客户跳IP分析报表	 已关闭(每周) 	设置任务 立即生成报表
DDL命令报表	全部数据库	数据库操作等项报表	DDL命令报题	 已关闭(每周) 	设置任务 立即主成报票
DCL命令撥裹	全部数据库	数据库操作专项报表	DCL命令报表	 已关闭(每周) 	设置任务 立即生成报表
DML命令授表	全部数据库	数据库操作专项报表	DML命令报表	 已关闭(每周) 	设置任务立即主成报表

门 说明

- 报表类型为系统自动生成,包括"合规报表"、"综合报表"、"数据库专项报表、"客户端专项报表"和"数据库操作专项报表"。
- 计划任务状态可手动设置开启或关闭,可设置为"每日"、"每周"或"每月"。
- 在需要变更模板的报表所在行的"操作"列,单击"设置任务",可以修改报表的计划任务。单击"确定"生效后,单击"立即生成报表",可在报表结果界面中查看报表结果。

----结束

12.10 管理备份的审计日志

备份审计日志后,您可以查看备份的审计日志信息,或删除备份的审计日志。

前提条件

- 数据库安全审计实例的状态为"运行中"。
- 请参考**开启数据库安全审计**成功开启数据库安全审计功能。
- 请参见**备份和恢复数据库审计日志**成功备份审计日志。

查看备份的日志信息

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"设置"。
- 步骤4 在"选择实例"下拉列表框中,选择需要查看日志的实例。
- 步骤5选择"备份与恢复"页签。
- 步骤6 查看备份的审计日志信息,相关参数说明如表12-9所示。

可以在列表上方选择时间"全部时间"、"近1小时"、"近24小时"、"近7天"或 "近30天"或自定义时间段,查看选择时间范围内的备份日志信息。或在列表上方的 搜索框中选择属性筛选,或输入关键字搜索,搜索指定的备份日志。

图 12-11 查看备份审计日志信息

备份日志列表							
全部时间		✓ Q 88	属性筛选,或输入	关键字搜索			
日志名称 🖯	备份时间 🖯	文件大小 ⊖	备份方式 🖯	番份范围 ⊖	sha256 ⊖	任务状态 🖯	操作
auto_backup_20241111	2024/11/1	20 Byte	自动备份	2024/11/11 00:00:00 GMT+08:00-2024/11/11 23:59:59 GM	59869db34853933b239f1e2219cf7d	😔 自动备份完成	你复日志 翻除
auto_backup_20241110	2024/11/1	20 Byte	自动备份	2024/11/10 00:00:00 GMT+08:00-2024/11/10 23:59:59 GM	59869db34853933b239f1e2219cf7d	📀 自动备份完成	依复日志 翻除
auto_backup_20241109	2024/11/1	20 Byte	自动备份	2024/11/09 00:00:00 GMT+08:00-2024/11/09 23:59:59 GM	59869db34853933b239f1e2219cf7d	📀 自动备份完成	依護日志 翻除
auto_backup_20241108	2024/11/0	20 Byte	自动备份	2024/11/08 00:00:00 GMT+08:00-2024/11/08 23:59:59 GM	59869db34853933b239f1e2219cf7d	📀 自动备份完成	依复日志 副除
auto_backup_20241107	2024/11/0	20 Byte	自动备份	2024/11/07 00:00:00 GMT+08:00-2024/11/07 23:59:59 GM	59869db34853933b239f1e2219cf7d	😒 自动备份完成	依実日志 副除
auto_backup_20241106	2024/11/0	20 Byte	自动备份	2024/11/06 00:00:00 GMT+08:00-2024/11/06 23:59:59 GM	59869db34853933b239f1e2219cf7d	📀 自动备份完成	依据日志 删除
auto_backup_20241105	2024/11/0	20 Byte	自动备份	2024/11/05 00:00:00 GMT+08:00-2024/11/05 23:59:59 GM	59869db34853933b239f1e2219cf7d	📀 自动备份完成	你复日志 删除
auto_backup_20241104	2024/11/0	20 Byte	自动备份	2024/11/04 00:00:00 GMT+08:00-2024/11/04 23:59:59 GM	59869db34853933b239f1e2219cf7d	📀 自动备份完成	依复日志 翻除
auto_backup_20241103	2024/11/0	20 Byte	自动备份	2024/11/03 00:00:00 GMT+08:00-2024/11/03 23:59:59 GM	59869db34853933b239f1e2219cf7d	😒 自动备份完成	依実日志 副除
auto_backup_20241102	2024/11/0	20 Byte	自动备份	2024/11/02 00:00:00 GMT+08:00-2024/11/02 23:59:59 GM	59869db34853933b239f1e2219cf7d	😒 自动备份完成	依据日志 删除

表 12-9 审计日志参数说明

参数名称	说明
日志名称	日志的名称,由系统自动生成。
备份时间	执行日志备份操作的时间。
文件大小	日志的文件大小。
备份方式	日志的备份方式。
sha256	备份日志的校验值。
备份范围	日志的备份时间段。
任务状态	日志的备份状态。

🛄 说明

在需要删除的日志所在行的"操作"列,单击"删除",在弹出的对话框中,单击"确定",您 可以删除该备份日志。

----结束

12.11 查看操作日志

本章节介绍如何查看数据库安全审计的操作日志信息。

前提条件

数据库安全审计实例的状态为"运行中"。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航树中,选择"实例列表"。
- 步骤4 单击需要查看操作日志的实例名称,进入实例概览页面。
- 步骤5 选择"操作日志"页签,进入操作日志列表页面。
- 步骤6 查看操作日志,相关参数说明如表12-10所示。

可以在列表上方选择时间**"全部时间"**、"近30分钟"、"近1小时"、**"今日"**、 "近7天"或"近30天"或自定义时间段,查看选择时间范围内的操作日志信息。或在 列表上方的搜索框中选择属性筛选,或输入关键字搜索,搜索指定的操作日志。

图 12-12 查看操作日志

作日志列表						
9B	✓ ○ 送採属性描述,或输入关键字液素					
用P名 🔤	股生时间 令	功能 令	ibiti 🖯	最作利象 令	描述 令	sa≅ ⊖
security_dbss_d00485254	2024/11/12 15:11:34 GMT+08:00	数据意列表	下動預売	F3g2H5MBR8YZnITjbKy	下數审计赛户调	😒 🛤
security_dbss_d00485254	2024/11/12 15:11:33 GMT+08:00	数据库列表	191 0	F3g2H5MBR8YZnITjbKy	添加新的审计Agent	😒 থেয়া
security_dbss_d00485254	2024/11/12 15:11:27 GMT+08:00	数据库列表	面新	mysql	开启审计案户调	গ্রহা
security_dbss_d00485254	2024/11/12 15:11:24 GMT+08:00	数据库列表	::::::::::::::::::::::::::::::::::::::	mysql	创建新的数据库	😒 1525

表 12-10 操作日志参数说明

参数名称	说明
用户名	执行操作的用户。
发生时间	执行操作的时间。
功能	执行的功能操作。
动作	执行功能操作的动作。
操作对象	执行操作的对象。
描述	执行操作的描述信息。
结果	执行操作的结果。

----结束

相关操作

- 数据库安全审计的操作日志默认保存多久?
- 数据库安全审计的操作日志是否可以迁移?

13云审计服务支持的关键操作

13.1 如何查看云审计日志

开启了云审计服务后,系统开始记录DBSS资源的操作。云审计服务管理控制台保存最近7天的操作记录。

查看 DBSS 的云审计日志

- 步骤1 登录管理控制台。
- 步骤3 单击左侧导航树的"事件列表",进入事件列表信息页面。
- **步骤4** 可以在列表上方选择时间**"最近1小时"**、"最近1天"、"最近1周"或自定义时间段,查看选择时间范围内的事件信息。或在列表上方的搜索框中选择属性筛选,或输入关键字搜索,搜索指定的事件。

图 13-1 事件列表

最近1周	~	Q 云服务: DBSS × 添加标选条件					×🕘 🔾
學件名称	末服务	资源类型	演選名称	洗燈印	操作用户	非体现别	操作时间
cloudServiceInstanceCreate	DBSS	dbss	DESS	e8a47caa2600a4816f		o normal	2024/11/06 11:38:37 GMT+08:00

步骤5 单击需要查看的事件名称,查看该事件的信息。

图 13-2 查看事件信息

事件列表 ①				1	事件概范				
(##.~)					基本供用				760141510
最近1周	✓] Q Ξ₩	第Ⅰ DBSS × 通加端透振性			₩i‡ID	90563829-90/0-11ef-0910-215629910b91	28 3	DBSS	
事件名称	云腦與	安连实型	<u>表面名称</u>	沙甜 瓜	事件发生时间	2024/11/06 11:38:37 GMT+06:00	2792	diss	
cloudServiceInstanceCreate	DBSS	doss	D659	e8a47					
⊕\$\$\$\$(1 10 ¥ < 1				1	arx州中 事件返回码	200	2017-01/-	DBSS	
					1 2 3 4 5 6 7 8 9 10 11 12 13 4 15 16 17 10 19 20 12 23 4 25 72 28 29 29	Trace (d1, 1000202-040-116-046) Trace (m2, 1000000000000000000000000000000000000	15629910 atte", cfd3c082 8c24ac20 bcb857f4 20", 3fccfd3c 20", 3fccfd3c do5", dd5", dd5",	691", ", ", 092", MCcfd3c082:user:lasbadd	I shuai",

----结束

13.2 云审计服务支持的 DBSS 操作列表

数据库安全服务通过云审计服务(Cloud Trace Service,CTS)为用户提供云服务资源的操作记录,记录内容包括用户从管理控制台或者开放API发起的云服务资源操作请求以及每次请求的结果,供用户查询、审计和回溯使用。

云审计服务支持的DBSS操作列表如表13-1所示。

表 13-1 云审计服务支持的数据库安全服务操作列表

操作名称	资源类型	事件名称
创建实例	dbss	createInstance
删除实例	dbss	deleteInstance
开启实例	dbss	startInstance
关闭实例	dbss	stopInstance
重启实例	dbss	rebootInstance
实例状态变化	dbss	cloudServiceInstanceStatus
创建包周期实例	dbss	cloudServiceInstanceCreate
实例元数据变化	dbss	updateMetaData

14 监控

14.1 DBSS 监控指标说明

功能说明

本节定义了数据库安全服务上报云监控服务的监控指标的命名空间,监控指标列表和 维度定义,用户可以通过云监控服务提供管理控制台或API接口来检索数据库安全服务 的监控指标和告警信息。

命名空间

SYS.DBSS

🗀 说明

命名空间是对一组资源和对象的抽象整合。在同一个集群内可创建不同的命名空间,不同命名空间中的数据彼此隔离。使得它们既可以共享同一个集群的服务,也能够互不干扰。

监控指标

表14-1 数据库安全服务支持的监控指标

指标 ID	指标名 称	指标含义	取值范围	测量对象	监控周期 (原始指 标)
cpu_u til	CPU使 用率	该指标用于统计测量 对象的CPU利用率。 单位:百分比 采集方式:100%减去 空闲CPU占比	0~100 % 值类型: Float	数据库审计实例	1分钟

指标 ID	指标名 称	指标含义	取值范围	测量对象	监控周期 (原始指 标)
mem_ util	内存使 用率	该指标用于统计测量 对象的内存利用率。 单位:百分比 采集方式:100%减去 空闲内存占比	0~100 % 值类型: Float	数据库审计实例	1分钟
disk_u til	磁盘使 用率	该指标用于统计测量 对象的磁盘利用率。 单位:百分比 采集方式:100%减去 空闲磁盘占比	0~100 % 值类型: Float	数据库审计实例	1分钟
hx_pr ocess _statu s	防护实 例进程 状态	该指标用于展示防护 实例的进程状态。 说明 该防护实例已不再维 护。	0/1	数据库审计实例	1分钟
hx_po rt_sta ts	防护实 例端口 状态	该指标用于展示防护 实例的端口状态。 说明 该防护实例已不再维 护。	0/1 • 0: 端 口 · · · · · · · · · · · · · · · · · · ·	数据库审计实例	1分钟
hx_pr oxy_n um	防护实 例代理 数量	该指标用于展示防护 实例的代理数量。 说明 该防护实例已不再维 护。	≥0	数据库审计实例	1分钟
hx_pr oxy_st atus	防护实 例代理 状态	该指标用于展示防护 实例的代理状态。 说明 该防护实例已不再维 护。	0/1 0:代 理态常 1:状 素 1:状 志常 	数据库审计实例	1分钟

指标 ID	指标名 称	指标含义	取值范围	测量对象	监控周期 (原始指 标)
hx_qp s	防护实 例每秒 查询数	该指标用于展示防护 实例的每秒查询数。 说明 该防护实例已不再维 护。	≥0	数据库审计实例	1分钟
hx_rp s	防护实 例每秒 请求数	该指标用于展示防护 实例的每秒请求数。 说明 该防护实例已不再维 护。	≥0	数据库审计实例	1分钟
hx_ac tive_c onnec tions_ num	防护实 例活跃 连接数	该指标用于展示防护 实例的活跃连接数。 说明 该防护实例已不再维 护。	≥0	数据库审计实例	1分钟

14.2 设置监控告警规则

通过设置DBSS告警规则,用户可自定义监控目标与通知策略,设置告警规则名称、监 控对象、监控指标、告警阈值、监控周期和是否发送通知等参数,帮助您及时了解数 据库安全状况,从而起到预警作用。

前提条件

请参见购买数据库安全服务成功购买数据库安全审计。

操作步骤

- 步骤1 登录管理控制台。
- 步骤3 在左侧导航树栏,选择"告警>告警规则",进入"告警规则"页面。
- 步骤4 在页面右上方,单击"创建告警规则",进入"创建告警规则"界面。
- 步骤5 设置告警规则名称。

图 14-1 设置告警规则名称

* 名称	alarm-igxc	
1444 July 1		
油还		
		0/256 🥢

步骤6 告警类型选择"指标",在"云产品"下拉列表框中选择"数据库安全服务",选择 "资源层级"、"监控范围",设置触发规则、模板、是否发送通知,选择**"通知方** 式"和**"通知策略"**,如<mark>图14-2</mark>所示。

图 14-2 设置	DBSS	监控告警规则
-----------	------	--------

* 告警类型	指标 事件
* 云产品	◎ 数据库安全服务 - 数据库安全服务 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
* 资源层级 ⑦	云产品 🗅 子继度
★ 监控范围	全部资源 指定资源 当选择全部资源时: 1、该维度下新购的资源将自动绑定到告警规则; 2、该维度下任何实例满足告警策略都会触发告警。 选择排款资源
★ 触发规则	关联楼板 自定义创建 选择关联楼板后,所关联楼板内容等改后,读告警规则中所包含策略也会跟随修改。
★ 模板	请选择
发送通知	
* 通知方式	
★ 通知策略	-请选择
高级配置 ~	归履企业项目 标签

步骤7 单击"立即创建",在弹出的提示框中,单击"确定",告警规则创建成功。

----结束

14.3 查看监控指标

您可以通过管理控制台,查看DBSS的相关指标,及时了解数据库安全状况,并通过指标设置防护策略。

前提条件

DBSS已对接云监控,即已在云监控页面设置监控告警规则。有关设置监控告警规则的 详细操作,请参见<mark>设置监控告警规则</mark>。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 单击页面左上方的 ──,选择"管理与监管 > 云监控服务 CES"。
- 步骤3 在左侧导航树栏,选择"云服务监控",进入"云服务监控"页面。
- 步骤4 单击目标看板名称"数据库安全服务 DBSS"。

图 14-3 云服务监控

転服务監控 ⊙			
027202			
〇、送採期性採送、採輸入外継字規束			
看板名称 ⊖	● ● ● ●	物面个数 ③ ④	6.8
数据库安全服务 DBSS	1	● 紧急 0 ● 重要 0 ● 次要 0 ● 痛示 0	☆
洲登进口报 员 SMN	1	 ・ 採執 0 ● 課題 0 ● 沈題 0 ● 描示 0 	
最新設:2 10 V (1)>			

步骤5 在目标DBSS实例所在行的"操作"列中,单击"查看监控指标",查看对象的指标详 情。

图 14-4 查看监控指标

< 云服务监控详情				
21676285 V 21676285	~			
资源评情 云服务概范				
实例列表				
ROTALE				
O. RANNER				
☐ 258: 0	10 0	ate o	ち用へ取	25
-	d1707ab0-b312-45e5-abr1-01205081#1	-	● 武物 ○ ● 重要 ○ ● 次要 ○ ● 指示 ○	意看这拉端乐 · 西多 ~

-----结束

15_{共享 VPC}

操作场景

购买数据库安全审计实例配置VPC参数,必须与Agent安装节点(应用端或数据库端) 所在的VPC保持一致。否则,将导致Agent与审计实例之间的网络不通,无法使用数据 库安全审计。

创建 VPC

- 步骤1 登录管理控制台。
- **步骤2** 单击页面左上角的 ── ,选择"管理与监管 > 资源访问管理 RAM",进入"资源访问管理"页面。
- 步骤3 单击页面左侧 "我的共享 > 共享管理",进入"共享管理"页面。
- 步骤4 单击页面右上角的"创建共享",进入"创建共享"页面。
- **步骤5** 选择资源类型为"vpc: subnet",选择对应区域,勾选需进行共享的VPC。单击"下一步:权限配置"。

图 15-1 指定共享资源

基本信息						
88	resource-share-skc0					
-						
982						
	0256 /					
65	如果如果要使用用一份医防治异种工作器。因为有服品均可在155 在下方物情绪人相信人内容的导击"我们,我可能够至加入此处	MANTAINA-SE BUEINSTABRINSE BURGASE ()				
	2840 3 420148 2840 3 42010					
	entrativisticos estas					
制定共享表展 254522	現在記述は中学的に思いない。 第4年間の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の	关系				
0257	vpc.subnet	▼ ♥ ₩6λ58888 Q	0597		25.93	MNERAL V
01458 😒		RIR	8/8/10	18.M	突进关型	80
subnet-f7 14c5682a	185 x x x x x x x x x x x x x x x x x x x	124	subret-1785 14c56x2a 69e8-404 a0x7-ab8955711430		vpc subnet	×

步骤6进入"权限配置"页面,选择指定资源类型支持的共享权限,配置完成后,单击页面 右下角的"下一步:指定使用者"。

图 15-2 权限配置

日始共享党团接受 xpc subnet 活动反馈 default ypc subnet statement		
11860W	A19880	
default upc subnet statement	vpc subnets get	
	vpc privatelps create	
	vpc ports create	
	vpc.subheteronimerfaces:create	
	vpc subnets intTags	

步骤7 进入"指定使用者"页面,指定共享资源的使用者,配置完成后,单击页面右下角的 "下一步:配置确认"。

图 15-3 指定使用者

୍ତି ଖାଇଅଭିନୟ —— 🕑 ଗୋଇଥିଲା —— 👔 ଖାଇଅଭିନକ —— 🕧 ନିଆଳାନ			
 第二次時代書 ○ ChineEalのわれ事 ○ ChineEalのわれ事 			
使用機能型 「協力支持等ローーマー			
诸威人S为云所导D	位用200	使用者名称	19h
如何重要保持安排号(07	59x758x44b1b4418x18843fcc833c883	-	×
			E-9 T-9: NEWA

表15-1参数说明

参数名称	参数说明
使用者类型	 组织 关于组织创建相关操作可参见创建组织。 说明 如果您未打开"启用与组织共享资源"开关,使用者类型将无法选择"组织"。具体操作可参见启用与组织共享资源。 华为云账号ID

步骤8 进入"配置确认"页面,确认配置无误后,单击页面右下角的"确认",完成资源共 享实例的创建。

图 15-4 配置确认

	- (v) nezha	- Carrier					
基本信息							
45/9 resource-share-skc0							
4E.6 -							
68							
共审批团							
発展の			28		安准灵型		
Hc56a2a-69a8-4far-a007-a09955711430					vpc subnet		
共享资源权限							
和思想				资源类型			
default vpc subret statement				vpcsubret			
资源任用者							
使用20 0				使的含名称			
59e750e44b1b4410a10543/cctt3c003				-			
							2-9 84

----结束

使用 VPC

步骤1 登录管理控制台。

- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在界面右上角,单击"购买数据库安全服务"。

图 15-5 选择可用区和性能规格

步骤4选择"区域"、"可用区类型"、"可用区"和"性能规格"。

计器模式 包示/00月			
可用区类型			
可用区 1885-542 町用区2 町用区3			
版本规格			
		†	•
入门版 最多支持1个数据库实例	基础版 最多支持3个数据库实例	专业版 最多支持6个数据库实例	高级版 最多支持30个数据库实例
百吐量峰值 1000条/秒	吞吐量蜂值 3000条/秒	百吐量峰值 6000条/秒	吞吐量峰值 30000 条/秒
入库速率 120万条/小时	入库速率 360万条/小时	入库速率 720万条/小时	入库速率 1080万条/小时
在线SQL语句存储 1亿条	在词SQL语句存储 4亿条	在线SQL语句存储 6亿条	在线SQL语句存储 15亿条
¥1,000.00 //B	¥3,000.00 /用	¥6,000.00 //B	¥24,000.00 //j

项目:选择企业项目管理中需要购买数据库安全服务的项目。计费以及权限管理,将 依据企业项目进行管理。

各版本的性能规格说明如<mark>表15-2</mark>所示。

表 15-2 数据库安全服务	予版本规格说明
-----------------------	---------

版本	支持的数据库实例	性能参数
入门版	最多支持1个数据库实 例	 吞吐量峰值: 1,000条/秒 入库速率: 120万条/小时 在线SQL语句存储: 1亿条
基础版	最多支持3个数据库实 例	 吞吐量峰值: 3,000条/秒 入库速率: 360万条/小时 在线SQL语句存储: 4亿条
专业版	最多支持6个数据库实 例	 吞吐量峰值: 6,000条/秒 入库速率: 720万条/小时 在线SQL语句存储: 6亿条
高级版	最多支持30个数据库 实例	 吞吐量峰值: 30,000条/秒 入库速率: 1,080万条/小时 在线SQL语句存储: 15亿条

🛄 说明

• 数据库实例通过数据库IP+数据库端口计量。

如果同一数据库IP具有多个数据库端口,数据库实例数为数据库端口数。1个数据库IP只有1 个数据库端口,即为一个数据库实例;1个数据库IP具有N个数据库端口,即为N个数据库实例。

例如:用户有2个数据库资产分别为IP₁和IP₂,IP₁有一个数据库端口,则为1个数据库实例; IP₂有3个数据库端口,则为3个数据库实例。IP₁和IP₂合计为4个数据库实例,选择服务版本 规格时需要大于或等于4个数据库实例,即选用专业版(最多支持审计6个数据库实例)。

- 不支持修改规格。若要修改,请退订后重购。
- 云原生版仅支持在RDS控制台购买。
- 本表中的系统资源要求,是指购买数据库安全审计实例时会消耗的系统资源。购买时,用户的系统需要满足审计版本对应的配置。
- 本表中在线SQL语句的条数,是按照每条SQL语句的容量为1KB来计算的。

步骤5 选择数据库安全审计的虚拟私有云及子网,相关参数说明如表15-3所示。

图 15-6 设	设置数据库安全审计参数
* 虚拟私有云	C 宣看虚拟私有云
	虚拟私有云可以方便的管理、配置内部网络,进行安全、快捷的网络变更。
	建议VPC选择时,尽量与Agent安装节点所在VPC相同。
* 安全组	
	安全组用来实现安全组内和组间数据库安全服务的访问控制,加强数据库安全服务的安全保护。
* 子网	
	子网是虚拟私有云内的IP地址块,虚拟私有云中的所有云资源都必须部署在子网内。
* 企业项目	✓ C 新建企业项目
	企业项目是一种云资源管理方式,企业项目管理服务提供统一的云资源按项目管理,以及项目内的资源管理、成员管理。
★ 实例名称	DBSS-be0c
备注	请输入备注信息

表 15-3 数据库安全审计实例参数说明

参数名称	说明	
虚拟私有云	您可以选择使用区域中已有的虚拟私有云(Virtual Private Cloud,VPC)网络,或者单击"查看虚拟私有云",跳转到 VPC管理控制台创建新的虚拟私有云。	
	说明	
	 请选择Agent安装节点(应用端或数据库端)所在的VPC。数据库 安全审计的Agent安装节点,请参见:如何选择数据库安全审计的 Agent安装节点? 	
	● 不支持修改VPC。若要修改,请退订后重购。	
	更多有关虚拟私有云的信息,请参见《虚拟私有云用户指 南 》。	
安全组	您可以选择区域中已有的安全组,或者在VPC管理控制台创建 新的安全组。选择实例的安全组后,该实例将受到该安全组访 问规则的保护。	
	更多有关安全组的信息,请参见《虚拟私有云用户指南》。	
子网	您可以选择VPC中已配置的子网,或者在VPC管理控制台为 VPC创建新的子网。	
实例名称	您可以自定义实例的名称。	

-----结束
16 数据库安全加密管理

16.1 数据库安全加密实例管理

通过管理控制台可登录实例侧,同时可对实例进行重启、关闭、解绑EIP等操作。

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航栏选择"数据库安全加密",查看数据库安全加密实例。

图 16-1 数据库安全加密实例

数据库安全加密					◎ 満意変子() < 最新設	
Q 25FE1925. 5563.7481	Faltar					Q 0
THER O	¥tz ⊖	CHIZE O	此和P能社 ⊖	WIEIP O	计模模式 ⊖	19/5
D855 10e018	0 遗行中	王智			包年/包月 19天后到期	远程登录 续奏 更多 >
D898- 97094	• 道行中	主筆			包平/包月 22月成别期	法控制录 体展 更多 ~

⁻⁻⁻⁻⁻结束

远程登录

步骤1 在目标实例"操作"列单击"远程登录"。

图 16-2 远程登录数据库安全加密实例

数据的	安全加密					◎ 満意変汗的 < 最新动き	1 使用烟霜	购买数据库安全服务
	DIFETRE DELATE	1177 A		annound A	Inter A	umbe A	19.0	Q 0
	A3960 0	606 C	ARKE	ELPHPTRIE O	MIT o	and an P	DETE	
	f0e01	0 2017	主聲			19天盘影响	這種整束 续数	N 19.5 -
	DE555 97094	 透行中 	主教			包带/包月 22天照别朋	5997 W	8 E8 -

步骤2 跳转至登录页面,输入实例的账号密码,单击"登录"进入数据库加密控制台。

-----结束

重启实例

步骤1 在目标实例"操作"列选择"更多 > 重启"。

图 16-3 重启数据库安全加密实例

数据库安全加密					S RESTO	
	建字投资					00
RHRB 0	₩8 0	実例类型 ↔	盘翔炉地址 ↔	3#性IP Ө	计数据式 ↔	授作
085 10e01	0 道行中	主新			包用/包月 19天開到期	2月日日 (京都) 开启
DBS 9709	0 遗行中	主智			包年/包月 23天照到明	(592) (592) (593)
DBSE 21cer	□ 我跟中	19	-			特別史全祖 注記: 解却 EIP
HARD 3						重要で66 开通日本は4時 < 1 > 進行 1955
						89

步骤2 在弹窗中确认重启,单击"确认",实例开始自动执行重启。

----结束

前にはたみられた

关闭实例

步骤1 在目标实例"操作"列选择"更多 > 关闭"。

图 16-4 关闭数据库安全加密实例

AND TALANCE						
	18					
SN2B 0	秋 四 日	实例类型 ↔	distupate 0	SWEEP O	计要模式 Θ	10 ft
D855- 154018	◎ 這行中	主教			包带/包月 19天祭到朝	酒程登录 読載 更多 ∧ 开始
DBSS 97094	• 遠行中	主發			银年/松月 22天然到期	☆根 美術
DBSS- 21oect	○ 80000中	主教			包年/包月	御武安全祖 15日 「新聞」
母議歌: 3						重量報码 开通目动振動 く 1 > 通び 部位 翻除

- 田田市道的 - 小長新坊市 - 11 伊田道家 - 日本

◎ 満意意序() 《 最新物志 □ 伊田城園 ● 170

步骤2 在弹窗中确认关闭,单击"确认",实例开始自动执行关闭。

----结束

兼招店安全捕农

修改安全组

步骤1 在目标实例"操作"列选择"更多 > 修改安全组"。

图 16-5 数据库安全加密实例修改安全组

运择履性保迈,或输入5	代建学搜索) [Q]
M28 0	865 0	采制类型 Ө	distribute 0	SWEED O	计要模式 8	操作
898 e018	○ 道行中	主要			包平/包月 19天起制期	辺程投票 体表 更多 ヘ 开启
855 7024	0 适行中	主要			包甲/包月 22天常到期	2012 王府 光灯
BSS LCRO	□ 838 P	主教	-		包平/包月	「市営業主法」 活売 輸送 EIP
tt: 3						正式(1) 开通白切検器 < 1
						透订

步骤2 在弹窗中选择安全组,单击"确认",实例所属安全组修改完成。

🗀 说明

只能选择已有的安全组。

----结束

解绑 EIP

步骤1 在目标实例"操作"列选择"更多 > 解绑EIP"。

图 16-6 数据库安全加密实例解绑 EIP

数据库安全加密					◎ 満意変示的 ~ <	最新动态 □ 使用推荐 购买数据库安全服务
Q. 选择履性转进、规能入3	·健宇推救					
安制名称 0	秋志 0	实制类型 0	此期10%地址 ⊖	₩性P 0	计模模式 Θ	操作
0855 10e015	0 运行中	主新			包甲/包月 19天開到期	这种独豪 续奏 更多 ~ 开启
0855 97094	0 遠行中	主新			包用/包月 22天開到期	这程 光灯
0855 21080	D 创建中	主教		-	包年/包月	修改安全组 这部型 解除 日P
世祭数: 3						展創出94 开選由均映表 < (1) >
						退订
						1722
						858

步骤2 在弹窗中确认解绑,单击"确认",实例将解绑EIP。

----结束

重置密码

步骤1 在目标实例"操作"列选择"更多 > 重置密码"。

图 16-7 数据库安全加密实例重置密码

3、运程履性保运、或输入3	关键字观索					Q
enza 0	1625 O	1200 R 20 0	ERUPANI O	WILLP O	HERE O	開作
DESS IDe011	0 @行中	29			包年/包月 19天后到明	远程建築 续重 更多 へ 开启
D655 97094	0 遗行中	王智			包年/包月 22天后到明	建田 法规 关闭
DESS 210ec	0 台灣中	王肇		-	包带/包月	特改支金組 注印 輸出 EP
ABC: 3						■重009 开通口动块商 <

步骤2 在弹窗中输入需要修改的密码,单击"确定",修改密码完成。

----结束

退订

步骤1 在目标实例"操作"列选择"更多 > 退订"。

图 16-8 退订数据库安全加密实例

数据库安全加密					@ #\$\$ 70	最新动态 口 使用喧嚣 购买政策库安全服务
Q. 这种最佳转达,或能入	关键字错击					Q 0
2012/0	秋志 ⊖	实现实现 0	±RiPitti ↔	₩EP Θ	计数据式 0	操作
DBSS 10e011	0 遗行中	王智			包年/包月 19天后到昭	远程登录 续奏 更多 ~ 开启
DBSS 97094	• 18ff=	29			包平/他月 22天然到期	ing Xi
0855 21060	□ 金融中	主新	-		包年/包月	伊政安全祖 ^{12月22} 解釈 EIP
·思乐歌: 3						2015年1月1日 第115年1月1日 第115日 第11

步骤2 在弹窗中确认退订信息,单击"是",完成退订。

----结束

删除

步骤1 在目标实例"操作"列选择"更多 > 删除"。

图 16-9 删除数据库安全加密实例

数	据库安全加密					Q R\$2;00 < 8805	こ 使用損料	REALFACTER
	〇、运得服性保运、或输入关键学表来							00
	THER 0	NS 0	实例类型 0	diriphite 0	WHIP 0	计模模式 ↔	1911	
	D655 f0e011	o 遗行中	±9			包平/包月 19天后王期	580.2	: 朱熹 王多 ヘ 开府
	D688 97094	0 适行中	29			包平/包月 22天后王期	318	堂 日
	DBSS 21080	C 10110389	主誓	-		6年/6月	STE	学校安全地 戦後 EIP
	(988) 3							単語を20 开通目的時間 〈 1 〉 出げ 和政 和政

步骤2 在弹窗中确认删除信息,单击"确定",完成删除。

----结束

16.2 系统管理员操作指导

16.2.1 平台管理

在初次使用数据库加密与访问控制时,您需要先完成本章节中的基础配置操作,才能 正常使用。

16.2.1.1 网络配置

系统的网络设置功能,支持配置网卡信息、DNS服务器和路由策略信息等。

- 网卡信息:包括网络IP地址、网关地址等信息,一般在初次安装部署或者网络环境变更时,需要配置。
- DNS服务器:设置DNS服务器地址,如果资产为域名时,必须要配置DNS服务器。
- 路由策略信息:如果设备存在多网卡,需要根据网络规划方案配置路由策略信息。

▲ 注意

- 请根据网络环境规划配置设备的网络信息,如果网络配置错误,您可能无法通过网络Web访问设备。此时,您需要直连设备后,重新配置网络信息。
- 修改路由信息前,请确保您了解路由对网络的影响,谨慎操作,避免断网。
- 若要修改网卡IP,必须通过该页面配置,不能直接在后台通过修改网卡配置文件的 方式修改,否则会导致ssh服务(22端口)的IP绑定错误。

前提条件

已经获取设备需要配置的IP地址等网络信息。

配置网卡信息

步骤1 使用系统管理员sysadmin账号登录实例Web控制台。

图 16-10 编辑网口

- 步骤2 在左侧导航栏,选择"系统管理 > 网络管理"进入"网卡列表"界面。
- 步骤3 在目标网卡"操作"列单击"编辑",进入"编辑网口"对话框,如<mark>图16-10</mark>所示。

编辑网口		>
网口名称	: eth0	
* 网口类型	: 业务口	\vee
网口描述	请输入	
* 地址类型	: IPv4	\vee
IPv4配置		
* IP地址及于	四掩码: 172.1 : 2	\vee
	+ 添加(1/10)	
	网关: 172	
	DNS:	
		1.

步骤4 参考表16-1,配置网卡信息。

表 16-1 配置网卡信息

参数	说明
网口名称	默认网口名称,无法更改。

取 消

确认

参数	说明
网口类型	选择网口类型。网口类型包括: 管理口 业务口
网口描述	设置您需要的描述。
地址类型	选择地址类型。地址类型包括: • 不配置地址 • IPv4 • IPv6 • IPv4 & IPv6
IP地址及子 网掩码	IP地址:您的设备IP地址。根据您的网络规划决定,需要和数据库等数据资产互通。 子网掩码:设置您的子网掩码。根据您的网络规划决定。
网关地址	您的网关地址。
DNS	设置您需使用的域名服务器。

步骤5单击"确定",完成配置。

----结束

配置路由信息

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"系统管理 > 网络管理"进入"路由列表"界面。
- 步骤3 单击"添加路由",进入"添加路由"对话框中。

图 16-11 添加路由

0 修改路由信	息前,请确保您了解路由对网络的影响,谨慎操作,避免断网。	
*地址类型:	IPv4 IPv6	
* 目标地址:	19 0	
* 子网掩码:	24 0	~
下一跳地址:	19 1	
* 选择接口:	eth0	

步骤4 参考表16-2,设置路由信息。

表 16-2 设置路由信息

参数	说明	
地址类型	选择地址类型包括:	
	• IPv4	
	• IPv6	
目标地址	即目标网络IP地址。	
了 网掩码 (IPv4)	配置目标地址的子网掩码。	
前缀长度 (IPv6)	配置目标地址的前缀长度。	
下一跳地址	配置下一跳地址,一般是网关地址。	
选择接口	手动选择流量外发的网卡。	

步骤5 单击"确定",完成配置。

-----结束

16.2.1.2 升级系统版本

如果需要使用新版本,可以通过系统升级功能进行版本升级。

X

常见的升级使用场景包括:

- 旧版本存在功能、安全等问题,需要升级新版本修复问题。
- 用户需要使用某些新功能,需要升级到新的版本。

门 说明

双机高可用场景下升级时,需先进入"平台管理 > 高可用管理"页面关闭数据同步按钮,然后 停止备机B的高可用(若为双主模式则关闭一台主机的高可用),先对设备B进行升级,升级成 功后,开启设备B的高可用,停止设备A的高可用,对设备A进行升级,升级完成后,开启设备A 的高可用,再开启数据同步,此步骤可保障双机 HA 升级时业务影响最低。

前提条件

如果新版本更新了加密算法或者密钥,直接升级可能导致数据解密问题。建议在升级 前解密所有表。

▲ 注意

建议在升级之前,手动备份系统的配置信息。具体操作,请参见<mark>备份与恢复配置信</mark> <mark>息</mark>。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"系统管理 > 系统运维"。
- 步骤3 单击"系统升级"进入"系统升级"界面。
- 步骤4 单击"上传升级脚本"。
- **步骤5** 在"版本变更"话框中,单击"点击或将文件拖拽到这里上传",上传系统升级包, 升级包请联系技术支持获取。

图 16-12 上传升级包

版本变更



步骤6 升级成功后,在版本变更历史中,查看系统的升级记录。

----结束

16.2.1.3 备份与恢复配置信息

数据库加密与访问控制支持通过手动和自动备份系统配置文件,方便故障情况下恢复 数据。

备份配置信息

备份配置信息将备份所有配置信息,包括系统配置、资产管理、敏感数据发现和密钥 管理等信息。为了系统的灾备能力,建议定期备份系统配置信息。

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"系统管理>备份恢复"进入"备份恢复"界面。

步骤3 单击"备份"页签,选择手动备份或者周期性自动备份两种方式。

- 手动备份:将备份信息直接保存在服务器。
 - a. 在立即备份区域,单击立即备份。
 - b. 在选择备份方式对话框的下拉栏中,选择备份保存位置。

图 16-13 选择备份方式

	* 手动备份类型:	本地备份	N	1
			取消	确认
c. 单击	"确定"。			
周期性自調	动备份:			
a. 在周	期备份区域,单击设置	置。		
图 16	5-14 配置自动备份			
	周期备份:开启			會设置
]2				

b. 在设置周期备份对话框中,配置周期备份信息,配置信息如<mark>表16-3</mark>所示。

表 16-3 备份说明

参数	说明	
备份方式	可选择本地备份。	
更换周期	设置密钥更新的周期,支持以下选项:	
	■ 无:不进行周期性更新。	
	■ 每天:每天更新一次。	
	■ 每周:每周更新一次。	
	■ 每月:每月更新一次。	
更换时间	根据更换周期,配置密钥更新的时间点。	

- c. 单击"保存"。
- d. 在备份文件列表中,可以查看备份信息,单击 图标,将备份文件下载到本地。
 下载的备份文件可以用于恢复系统配置信息。具体操作,请参见恢复配置信息。

----结束

恢复配置信息

通过导入配置文件,可以将配置信息恢复到某一个备份时间点。一般用于故障恢复或 者设备迁移。

前提条件

- 待恢复的数据库加密与访问控制服务器需要为重新安装后的初始化状态,即无任何数据资产配置。
- 已生成并下载配置备份文件,具体操作,请参见备份配置信息。
- 步骤1 登录数据库加密与访问控制。
- 步骤2 在左侧导航栏,选择"系统管理>备份恢复"进入"备份恢复"界面。
- 步骤3 单击"恢复"页签。
- 步骤4 单击右上角的"立即恢复"。
- 步骤5 在"数据恢复"对话框中,输入安全口令并上传备份文件。
- 步骤6 单击"确认"。

----结束

16.2.1.4 查看平台信息

初次使用产品时,请联系技术支持工程师进行系统授权,授权后方可使用产品的各项 功能。

文档版本 01 (2024-11-28)

授权后,您可以在"系统管理 > 平台信息"区域查看授权到期的剩余时间以及授权期限时间,授权到期后请联系技术支持工程师进行重新授权。

表 16-4	平台信息
--------	------

区域	参数	说明
基本信息	产品名称	显示本产品的名称。
	系统版本	显示产品的版本。
	引擎版本	显示引擎版本。
	系统时间	显示系统时间。
	开机时间	显示服务器开机时间。
公司信息	公司名称	显示公司的名称。
	公司电话	显示公司的电话。
	公司网站	显示公司的网址。
	公司地址	显示公司的地址。
授权信息	机器型号	显示机器的型号。
	资产数量	显示可添加资产的总数量。
	已用列数/最大加密列 数	显示最大加密列数以及当前已用的加密列 数。
	已用列数/建议最大脱 敏列数	显示最大脱敏列数以及当前已用的脱敏列 数。
	bypass数	显示可用的bypass总服务量。
授权信息	SM2国密证书	显示SM2国密证书支持情况。

16.2.1.5 查看高可用信息

若系统采用高可用部署,您可以在"系统管理 > 高可用管理"页面查看高可用信息, 包括主备机IP与VIP、主备机的运行时间以及各项指标的状态。

若采用高可用模式,对于已有数据资产的单机组HA的场景,请注意以下事项:

- 若增加VIP地址,需要将所有已有数据源的代理地址手动修改为VIP地址;
- 若HA配置时VIP地址填写原单机物理IP地址,则无需修改每个数据源的代理地址。

🛄 说明

双机高可用场景下升级时,需先进入"平台管理 > 高可用管理"页面关闭数据同步按钮,然后 停止备机B的高可用(若为双主模式则关闭一台主机的高可用),先对设备B进行升级,升级成 功后,开启设备B的高可用,停止设备A的高可用,对设备A进行升级,升级完成后,开启设备A 的高可用,再开启数据同步,此步骤可保障双机 HA 升级时业务影响最低。

16.2.2 修改安全口令

为了保障密钥本身的安全性,在进行创建、编辑和修改密钥等管理操作时,需要先验 证安全口令。为了系统的安全性,建议您妥善保管安全口令信息,此章节介绍如何修 改安全口令。

在初始化密钥等操作时会显示默认的安全口令提示信息,建议您在正式使用设备前修 改默认的安全口令。同时,建议您定期更新安全口令。

获取默认口令请提交工单。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- **步骤2** 在左侧导航栏,选择"系统管理 > 系统设置"进入"通用设置"界面,单击"安全口 令设置"进入"安全口令"界面。
- 步骤3选择"安全口令"。
- 步骤4 在输入框中,设置新的安全口令,单击"保存"。

密钥口令不可遗忘,修改后请将口令保存在安全介质内。

图 16-15 修改安全口令

安全口令

 密钥口令不可遗忘, 修改后请将口令保存在安全介质内 				
*安全口令:	请输入			
* 确认安全口令:	清输入			
	保存重置			

步骤5 在"口令校验"框中,输入旧的安全口令,单击"确定"。

----结束

16.2.3 初始化密钥

在初次使用加密功能前,用户需要初始化密钥。

数据库加密与访问控制的密钥包括根密钥(RK)、数据源密钥(DSK)和数据加密密 钥(DEK),具体说明如<mark>初始化密钥</mark>所示 。

Х

取消

初始化

表 16-5 密钥种类说明

密钥种类	说明
根密钥(RK)	初始化密钥后生成,不对外暴露。
数据源密钥 (DSK)	在添加数据源时生成,由根密钥(RK)加密保存。
数据加密密钥 (DEK)	在添加加密队列任务时初始化生成,由数据源密钥(DSK)加密 保存。

操作步骤

- 步骤1 登录数据库加密与访问控制。
- 步骤2 在左侧导航栏,选择"密钥管理 > 密钥配置"。
- 步骤3 单击"初始化密钥"。
- **步骤4**在口令校验对话框中,输入安全口令,单击"确定"。 安全口令如何设置,请参见修改安全口令。
- 步骤5 在初始化密钥对话框中,设置密钥来源,参数如<mark>表16-6</mark>所示。

图 16-16 初始化密钥

初始化密钥

* RK密钥来源:	系统内置	
* DSK密钥来源:	系统内置	
* DEK密钥来源:	系统内置	

文档版本 01 (2024-11-28)

表 16-6 初始化密钥

参数	说明
RK密钥来源	配置RK(根密钥)来源,支持以下来源:
	● 系统内直:系统内直的固定密钥,仅限于测试使用。
	● 密钥平台:系统对接的密钥平台。 如何配置密钥平台,请参见 <mark>配置KMS对接</mark> 。
	配置后,在密钥平台中选择平台厂商。
	说明 KMS需要的权限:KMS CMKFullAccess。
DSK密钥术源	
	● 系统内置:系统内置的固定密钥,仅限于测试使用。
	 密钥平台:系统对接的密钥平台。 如何配置密钥平台,请参见配置KMS对接。
	配置后,在密钥平台中选择平台厂商。
	KMS需要的权限:KMS CMKFullAccess。
DEK密钥来源	配置DEK密钥来源,支持以下来源:
	 系统内置:系统内置的固定密钥,仅限于测试使用。
	● 密钥平台:系统对接的密钥平台。 如何配置密钥平台,请参见配置KMS对接。
	和"你们的"是"的"你们",你们不知道。
	KMS需要的权限:KMS CMKFullAccess。

步骤6 单击"初始化"完成密钥初始化。

----结束

16.2.4 添加数据资产

在系统中添加数据资产(即数据库)后,您可以对数据库进行敏感数据识别,对敏感 信息进行加解密、脱敏等操作。

本文通过添加MySQL数据库为例,您需要根据实际情况添加相应的数据资产。

使用约束

表 16-7 数据库加密支持纳管的数据源及版本

数据库	版本号
MySQL	5.5 、5.6、5.7、8.0、8.0.13+
Oracle	11.1、11.2、12c、19c
SQLServer	2012、2016

数据库	版本号
PostgreSQL	9.4、11.5
DM	6、7.6、8.1
Kingbase	V8 R3、V8 R6
MariaDB	10.2
GaussDB	A
TDSQL	5.7
TBASE	V2.15.17.3
RDS_MYSQL	5.6、5.7、8.0
RDS_PostgreSQL	11

表 16-8 数据库加密的数据库账号权限

数据库	需要select权限的系统表名	数据库账号权限
MySQL	mysql.user	select
	performance_schema.*	insert
		create
		update
		delete
		drop
		alter
		index
RDS_MY	mysql.user	select
SQL	performance_schema.*	insert
		create
		update
		delete
		drop
		alter
		index

数据库	需要select权限的系统表名	数据库账号权限
TDSQL	mysql.user performance_schema.*	select insert create update delete drop alter index
MariaDB	mysql.user performance_schema.*	select insert create update delete drop alter index
DM	SYS.ALL_SUBPART_KEY_COLUMNS SYS.ALL_USERS SYS.ALL_CONS_COLUMNS SYS.ALL_CONSTRAINTS SYS.ALL_TABLES SYS.ALL_TABLE_COLUMNS SYS.ALL_COL_COMMENTS SYS.ALL_OL_COMMENTS SYS.ALL_IND_COLUMNS SYS.ALL_IND_COLUMNS SYS.ALL_INDEXS V\$VERSION V\$LOCK SYS.DBMS_LOB SYS.DBMS_METADATA	用户角色必须是dba
postgreS QL	pg_catalog.pg_class pg_catalog.pg_index pg_catalog.pg_user pg_catalog.pg_indexes information_schema.columns information_schema.sequences information_schema.tables pg_catalog.pg_sequence	用户必须是表的owner或 者是dba

数据库	需要select权限的系统表名	数据库账号权限	
RDS_Pos tgreSQL	pg_catalog.pg_class pg_catalog.pg_index pg_catalog.pg_user pg_catalog.pg_indexes information_schema.columns information_schema.sequences information_schema.tables pg_catalog.pg_sequence	用户必须是表的owner或 者是dba	
TBASE	pg_catalog.pg_class pg_catalog.pg_index pg_catalog.pg_user pg_catalog.pg_indexes information_schema.columns information_schema.sequences information_schema.tables pg_catalog.pg_sequence	用户必须是表的owner或 者是dba	
GAUSSD B	pg_catalog.pg_class pg_catalog.pg_index pg_catalog.pg_user pg_catalog.pg_indexes information_schema.columns information_schema.sequences information_schema.tables pg_catalog.pg_sequence	用户必须是表的owner或 者是dba	
KINGBAS E 8.6 (pg模 式)	pg_catalog.pg_class pg_catalog.pg_index pg_catalog.pg_user pg_catalog.pg_indexes information_schema.columns information_schema.sequences information_schema.tables pg_catalog.pg_sequence pg_catalog.pg_matviews	用户必须是表的owner或 者是dba	

数据库	需要select权限的系统表名	数据库账号权限
KINGBAS	sys_catalog.sys_class	用户必须是表的owner或
E 8.3	sys_catalog.sys_index	者是dba
	sys_catalog.sys_user	
	sys_catalog.sys_indexes	
	information_schema.columns	
	information_schema.sequences	
	information_schema.tables	
	sys_catalog.sys_sequence	
	sys_catalog.sys_matviews	
Oracle	SYS.ALL_SUBPART_KEY_COLUMNS	用户角色必须是dba
	SYS.DUAL	
	SYS.ALL_USERS	
	SYS.ALL_CONS_COLUMNS	
	SYS.ALL_CONSTRAINTS	
	SYS.ALL_TABLES	
	SYS.ALL_TABLE_COLUMNS	
	SYS.ALL_COL_COMMENTS	
	SYS.ALL_PART_KEY_COLUMNS	
	SYS.ALL_IND_COLUMNS	
	SYS.ALL_INDEXS	
	SYS.V_\$INSTANCE	
	SYS.DBMS_LOB	
	SYS.DBMS_METADATA	
	DBA_TABLES	
	DBA_TAB_COLS	

数据库	需要select权限的系统表名	数据库账号权限
SQLserve	sys.tables	schemaSelect
r	sys.indexes	schemalnsert
	sys.index_columns	schmeaUpdate
	sys.default_constraints	schemaAlter
	sys.systypes	createTable
	sys.extended_properties	VIEW SERVER STATE
	sys.foreign_key_columns	加密表的select
	sys.check_constraints	加密表的insert
	sys.foreign_keys	加密表的alter
	sys.columns	
	sys.objects	
	sys.all_columns	
	sys.types	
	sys.syslogins	
	sys.all_objects	
	sys.schemas	
	sys.key_constraints	
	sys.computed_columns	
	sys.triggers	
	sys.partition_schemes	
	sys.dm_sql_referencing_entities	

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"资产管理 > 数据源管理"。
- 步骤3 单击右上角的"添加数据源"。
- 步骤4 在添加数据源对话框中,设置资产信息,详细信息如表16-9所示。

表 16-9 添加数据源参数配置

参数	说明
数据库信息	
数据源名称	自定义设置数据资产名称。
数据源类型	在下拉栏中选择数据库类型。支持的数据库类型及版本请参见 <mark>使</mark> 用约束。
数据源版本	在下拉栏中,选择数据库的具体版本号。

参数	说明
读写分离/RAC	如果数据库是读写分离部署,需要勾选此选项,并设置从数据库 节点信息。
数据源地址	设置数据库的IP地址。
数据源端口	设置数据库的连接端口。
代理地址	从下拉框中选择代理地址,即数据库访问与控制的IP地址。
代理端口	设置代理端口。运维人员通过代理IP + 代理端口访问数据库。
	● 取值范围: 1025-65535。
	 您可以在范围内设置一个任意的空闲端口。不能使用其他数据 资产已经使用的端口。例如,数据资产A使用了14000端口, 那么数据资产B则不能使用14000端口。
	可单击"自动分配",由系统自动分配空闲的代理端口。
数据库/实例 名/SID/服务名/ 模式	设置数据库/实例名/SID/服务名/模式。
数据库账号	设置数据库登录用户。
数据库密码	设置数据库登录密码。
加密参数	
加密方式	• 设置资产加密方式,可选项如下:
	– 一资产一密:资产下DEK相同,支持连接查询,支持跨库 查询 。
	– 一列一密:资产下DEK不同,不支持连接查询,不支持跨 库查询。
无权限缺省显示	• 设置用户没有权限访问数据库时看到结果。可选项如下:
	- 密文: 查看到密文信息,编码格式为BASE64或者十六进 制,具体请参见 <mark>设置加密参数</mark> 。
	 - 缺省数据:查看到缺省数据,同时需要设置字符串类型的 缺省数据。
	– NULL:查看到的内容为空。
主机信息(可选)	
配置监控阈值后, 密,资源使用率超 置。	系统只会在数据库服务器监控阈值范围内对数据进行分批次的加 时间值后停止加密,降低对业务的影响。如果条件允许,建议配
主机IP	设置主机IP地址。
主机端口	设置主机SSH服务端口,默认SSH服务端口为22。
用户名	设置主机登录用户名。
密码	设置主机登录密码。

参数	说明	
字符集	主机使用的字符集,测试主机连接后自动获取。	
主机操作系统	主机的操作系统信息,测试主机连接后自动获取。	
内核	主机的内核信息,测试主机连接后自动获取。	
指标监控阈值	设置主机监控指标(CPU、内存、IO、网络)的阈值。系统仅在 阈值范围内对数据库数据进行加密,降低对业务的影响。	
日志信息		
数据库日志文件 名	设置数据库日志文件路径+文件名。例如:/usr/local/mysql/ binlogs/mysql-bin.000060。	

- 步骤5 (可选)配置完成后,单击"测试数据库连接",检查数据库是否能连接。
- **步骤6**(可选)单击"测试账号权限",检查数据库账号权限是否满足加密要求。 如果数据库账号权限不满足加密要求,请参考<mark>表</mark>16-8,配置数据库账号权限。
- **步骤7** (可选)如果配置主机信息,单击"测试主机连接",检查是否能连上主机,并自动获取字符集和主机操作系统。
- 步骤8 单击"保存",保存数据资产的配置信息。

资产添加完成后,您可以在数据源列表中查看新添加的数据资产信息,如<mark>图16-17</mark>所 示。

图 16-17 数据源列表



步骤9 在列表中,单击启用按钮 💭 ,启用数据库代理。

启用后,可通过代理IP+代理端口访问数据库。

----结束

相关操作

- 在数据源列表"策略配置"列单击^合,跳转到加密队列配置页面。建议在配置加密队列前进行敏感数据识别,具体操作,请参见扫描资产的敏感数据。
- 在数据源列表"策略配置"列单击^争,跳转到脱敏规则配置页面。建议在配置脱 敏规则前进行敏感数据识别,具体操作,请参见扫描资产的敏感数据。
- 在数据源列表"操作"列单击"编辑",修改数据资产信息。
- 在数据源列表"操作"列单击"删除",删除不再需要的数据资产。

🛄 说明

如果提示当前数据库未回滚表结构,请根据实际情况,回滚表结构或者配置解密队列。

16.2.5 业务测试和分析

在正式使用加密前,建议先对数据库进行测试,检验业务中使用的SQL语句是否能够 在加密环境中使用,排除加密后可能影响的业务错误,降低业务测试成本。进行数据 加密后,数据的特征发生变化,由原来的中文、英文、数字变成了十六进制字串符。 从而导致部分原来可以正常执行的SQL在数据加密后无法执行。

例如:字符串模糊查询、数值的运算、范围查找等。

在加密前通过业务分析功能将用户使用的SQL语句进行分析,从而判断数据表是否可加密。

- 解析异常SQL语句:无法解析的SQL语句,例如错误的SQL语句、太复杂而无法解析的SQL语句等。
- 阻断SQL语句:数据库加密与访问控制不支持的SQL语句。

操作步骤

步骤1 使用系统管理员sysadmin账号登录实例Web控制台。

步骤2 创建业务分析任务:

- 1. 在左侧导航栏,选择"业务测试>业务分析"。
- 2. 在页面左侧数据源处,单击目标数据源。

图 16-18 选择数据源

数据源

请输入 Q

- Oracle
- MySQL



- mysgl4648
- 3. 单击"新增分析表",配置需要分析的数据表,单击"确定"。

图 16-19 新增分析表

· #8500-42 -	dos demo	In demo
* 1983:0451 :	doc_demo	(}
* 表名:	sys_user	✓ 数据源类型: MySQL
		数据源版本: 5.7
	· 至表分析 / 指定列分析	数据源地址: 17.
		数据源端曰:
		主机IP:
		主机编口:
		CPU:
		0%
		内存: 0%
		网络:
		10:
		操作系统:
		取7 9出

图 16-20 启动

4.

模式名	表名	分析列	状态	异常记录	分析	操作
doc_demo	sys_user	dept_id.user_name.nick_name	未开始	0	0	查看日志 编辑 删除

步骤3 使用代理地址访问数据库,并执行SQL语句。

- 在"资产管理 > 数据源管理"页面获取代理地址。
 IP地址即数据库加密与访问控制的IP,代理端口即添加数据资产时所配置的代理端口。
- 在数据库工具上配置访问代理地址并连接。
 主机和端口请参照前面步骤,用户名和密码根据数据库实际情况配置。以下图片 仅为示例,请根据具体数据库工具配置代理访问连接。

图 16-21 配置访问代理地址

NySQL - 新建连接		×
常规 高级 数据库 SSL SSH HTTP		
<u> </u>		
连接名: 加密代理		
主机: 172. 158		
端口: 14099		
用户名: root		
密码:		
测试连接	确定	取消

3. 在数据库工具上执行异常SQL语句。 例如执行以下语句:

表 16-10 异常示例

类型	语句
异常SQL语句	select * fform table
阻断SQL语句	RENAME TABLE sys_user to abc

步骤4 在Web控制台查看异常SQL语句的日志。

- 1. 在左侧导航栏,选择"业务测试 > 业务分析"。
- 2. 在页面左侧数据源处,单击目标数据源。
- 3. 单击"解析异常SQL",查看异常SQL语句。

图 16-22 异常 SQL 语句

解析异常SQL			X
			导出
发现异常	发现时间	关联列	异常详情
SQL无法解析	2024-08-27 13:24:43	-	select * fform table
SQL无法解析	2024-08-27 13:25:34		select * formm table
SQL无法解析	2024-08-26 13:34:44	-	/* ApplicationName=DBeaver
			总共3条 < 1 > 15条/页 >

步骤5 在Web控制台查看阻断SQL语句的业务分析。

- 1. 在左侧导航栏,选择"业务测试 > 业务分析"。
- 2. 在页面左侧数据源处,单击目标数据源。
- 3. 在列表中可用查看到异常记录数量。

图 16-23 查看阻断 SQL 语句数量

□ 模式名	表名	分析列	状态	异常记录	分析	操作
doc_demo	sys_user	dept_id.user_name.nick_name	分析中	1	0	查看日志

4. 单击"查看日志"查看阻断SQL语句的异常记录。

图 16-24 查看阻断 SQL 语句记录

查看分析日志			Х
模式名: doc_demo	表名: sys_user		今日
发现异常	发现时间	关联列	异常详情
illegal operation	2024-08-27 13:51:45	/	RENAME TABLE sys_user to abc
			总共1条 < 1 > 15条/页 >

5. 单击"分析报表",可用查看系统对此表格的加密建议。

如<mark>图16-25</mark>所示,如果用户有对数据库表进行重命名的操作,则系统不建议对此表 格进行加密操作。

图 16-25 分析建议

						导出
策略建议	建议原因	模式	表名	列名	异常详情	操作
表不可加密	illegal operation	doc_demo	sys_user	/	RENAME TABLE sys_user to abc	删除



16.2.6 敏感数据发现

16.2.6.1 扫描资产的敏感数据

通过敏感数据发现任务,您可以自动获取数据资产中的敏感数据表信息。

文档版本 01 (2024-11-28)

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"敏感数据发现 > 敏感数据扫描"。
- 步骤3 找到目标数据资产,单击"任务配置"。

在任务配置对话框中,配置敏感数据发现任务。

表 16-11 敏感数据发现任务参数

参数	说明
抽样数量	设置抽样扫描的抽样数量。
	抽样扫描,指从数据集合中抽取一定数量的数据进行识别。抽样 越多,识别越精准;抽样越少,扫描速度越快。
最大线程数	设置任务使用的最大线程数。
	敏感数据发现任务可以使用多线程,线程数越多,扫描效率越 高,同时占用的设备资源也越多。
选择模式	选择需要加密的数据库模式(Schema)。
	在左侧的可选择的模式选中目标模式,单击>按钮,移动到已选中 的模式。
选择表	选择模式后,自动选择该模式下所有表。如果只选择单个模式, 您可以根据需要调整该模式下的表数量。
	如果部分表格不需要扫描,在右侧的已选中的表选中目标对象, 单击<按钮,移动到可选择的表。
敏感数据选择	在下拉栏中选择行业模板,选中后会扫描模板中设置的数据类 型。
	系统已经内置常用的行业模板,您也可以自定义配置行业模板, 具体操作请参见 <mark>新增行业模板</mark> 。
	如果选择不使用模板,则在需要发现的数据类型中手动设置需要 扫描的数据类型。
需要发现的数	手动选中需要扫描的数据类型。
据类型 	仅在敏感数据类型选择为不使用模板时,此参数可以设置。

抽样数量: 1000			
最大线程数 ①: 〇 1			
□ 42 项	可选择的模式	🗌 1 项	已选中的模式
语输入脱震内容	٩	清输入推荐内容	٩,
ddmtest2 demo emp_nthl_uact_b		doc_demo	
0 项	可选择的表	1 项	已选中的表
請输入股票内容	٩	请输入推荐内容	٩
- 表名			表名
			sys_user
 較无数弱			

图 16-26 配置敏感数据发现任务

步骤4 单击"保存",完成敏感数据任务配置。

步骤5 在目标数据资产,单击¹执行敏感数据发现任务。

执行开始后,系统自动扫描识别敏感数据。扫描时间和需要扫描的数据量有关,数据 量越多,需要扫描的时间越长,您可以在页面查看扫描进度。执行完成后,"任务状 态"显示为"扫描完成"。

----结束

16.2.6.2 查看扫描任务执行结果

敏感数据发现任务执行完成后,系统会扫描并识别数据资产中的敏感数据。您可以在 执行结果中查看具体的敏感数据信息。

操作步骤

步骤1 使用系统管理员sysadmin账号登录实例Web控制台。

步骤2 在左侧导航栏,选择"敏感数据发现 > 敏感数据扫描"。

文档版本 01 (2024-11-28)

步骤3 (可选)设置搜索项,并单击搜索图标,查询指定数据资产。

- 步骤4 找到目标数据资产,单击"查看"。
- **步骤5** 在扫描结果列表页面,查看扫描全部结果。

表 16-12 扫描结果

参数	说明
数据源名称	敏感信息所在的数据资产名称。
模式	敏感信息所在的模式。
表名	敏感信息所在的表名/视图名。
表列数	数据库表的表列数。
是否可加密	数据库表是否支持加密。
不可加密原因	如果表不可加密,提示不可加密的原因。
敏感数据发现时间	敏感数据发现时间。

图 16-27 扫描结果

步骤6 对于数据库表,单击"编辑",可以查看表字段信息。

如<mark>图16-28</mark>所示,表字段信息中显示列信息和列对应的敏感数据类型。如果扫描结果不匹配真实情况,您可以修改敏感数据类型信息。

表 子段信息							
列名	数据类型	字段长度	最高命中率	匹配结果	敏感数据类	型	
user_id	BIGINT	20	0%	未命中	无	~	
dept_id	BIGINT	20	0%	未命中	无	\leq	
user_name	VARCHAR	720	0%	未命中	无	×	
nick_name	VARCHAR	720	0%	未命中	无	v.	
user_type	VARCHAR	272	0%	未命中	无	\vee	
email	VARCHAR	2928	100%	电子邮箱地址: 100%	电子邮	\mathbf{v}°	
phonenumber	VARCHAR	2928	100%	手机号码: 100%	手机号码	×	
sex	VARCHAR	272	0%	未命中	无	\sim	
6							

图 16-28 编辑表字段信息

----结束

16.2.6.3 在结果中创建加密队列

根据敏感数据发现结果,针对性的创建加密队列,本章节介绍如何在结果中创建加密 队列。

在配置加密队列之前,建议先进行仿真加密测试,检验加密过程中是否会存在问题, 并解决相应问题。

您也可以在数据加密中创建加密队列。具体操作,请参见配置加密队列。

在加密之前,数据表信息为正常明文信息,示例如<mark>图16-29</mark>所示。

图 16-29 加密前查询结果

	12@ user_id \\\ \	123 dept_id \[?	ADC user_name T	nick_name \T ?	ADC user_type T?	nnc email ₹ ?	^{nbc} phonenumber ▼ ‡?	ADC sex T1?	ADC avatar T?
1	1	103	admin	兼領	00	=@163.com	1588888888	1	
2	2	105	ry	兼領	00	=@qq.com	156 66666	1	

前提条件

在创建加密队列之前,已经创建密钥。

创建加密队列

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"敏感数据发现 > 敏感数据扫描"。
- 步骤3 在扫描任务列表页面,找到目标数据资产,单击"查看"。
- 步骤4 在扫描结果列表页面,找到目标数据库表,单击"添加加密队列"。

步骤5 在添加加密队列对话框中,设置加密信息,配置信息如表16-13所示。

表 16-13 添加加密队列

参数	说明
数据源名称	数据资产的资产名称。
模式名	资产的模式名。
表名	资产的表名。
加密算法	在下拉栏中选择加密的算法。 可以在 <mark>查看加密算法</mark> 页面查看支持的算法类型。
校验算法	在下拉栏中选择校验的算法。 校验算法用于重要数据的完整性校验,可以在 <mark>查看加密算法</mark> 页面查看 支持的算法类型。
每批条数	设置加密队列每批处理的数据量。
线程数	设置加密队列占用的线程数量。
启动队列	勾选后,创建队列后自动启动队列。

图 16-30 添加加密队列

曾加密队	列			
• 数据源	名称: demo			emo demo
*模	式名: doc_demo			☆ 数据源类型: MySQL
•	表名: sys_user			数据源版本: 5.7 数据源地址:
加密算法	法①: SM4_128			> 数据源端口: ■
校验算法	法①: SM3_HMAC_16	i		主切IP: > → 印油口:
* 毎 批	条数: 8191	* 約	法程数: 4	CPU:
启动	队列: 🔽			0%
• 加處列	则表			网络:
选择	列名	数据类型	备注信息	IO:
	dept_id	bigint(20)	Department ID	操作系统:
	user_name	varchar(720)	User account	
	nick_name	varchar(720)	User's nickname	
	user_type	varchar(272)	user type(00syste	
	email	varchar(2928)	email	

步骤6 单击"加密列表"页签,勾选需要加密的列名称,并设置是否启用模糊查询功能。

加密后,默认情况下无法进行模糊查询。如果符合以下情况,勾选启用模糊查询后支 持模糊查询,模糊查询支持%和_两种符号。

- 密文编码方式为十六进制,不支持BASE64模式编码。如何配置,请参见设置加密参数。
- 字段为字符串类型(varcha)。其它类型不支持。

图 16-31 选择加密列

选择	列名	数据类型	启用模糊查询	备注信息	10:
	dept_id	bigint(20)		Department ID	操作系统:
	user_name	varchar(720)		User account	
	nick_name	varchar(720)		User's nickname	
	user_type	varchar(272)		user type(00syste	
~	email	varchar(255)		email	
~	phonenumber	varchar(255)		phone number	
	sex	varchar(272)		gender	

步骤7 单击"初始化表",开始对数据表进行初始化。

步骤8 单击"完成",创建加密队列。

-----结束

结果验证

- **步骤1** 加密队列创建完成后,在"数据加密 > 加密队列管理"中查看和管理新建的加密队列。
- **步骤2**加密队列完成存量数据加密后会自动移出。此时队列为已移出状态,但系统还会继续进行正常加密数据。

图 16-32 全密文模式



步骤3 再次查询数据库表,查询结果是已被加密的数据示例如图16-33所示。

图 16-33 加密后数据

		an ache on	www.user_name	REC NICK_name	noc user_type 💌	nic email 👻	All phonenumber	noc sex	*
1	.1	103	admin1	88	00	IEC9Ykn7WLo5IcdW4BVGzT1RiGX2tbcsc2YLq2YF8UIz	IEC9YU/9Xrw/UcZQ485DhmoSSMUNEH0Y1GGW5Kw=	1	_
2	2	105	admin2	88	00	IEC9Vkn7WLo5IcdW4BVGzT1RiGX2tbcsc2YLq2YF8Ulz	IEC9Z0/9Xrw/UcZQ49ggt+ihzLNuPWy1DOYzPhQ=	1	

----结束

16.2.6.4 在结果中创建脱敏规则

根据敏感数据发现结果,针对性的创建脱敏规则,本章节介绍如何在结果中创建脱敏规则。

您也可以在动态脱敏模块中创建脱敏规则。具体操作,请参见创建脱敏规则。

在脱敏之前,数据表信息为正常明文信息(数据未加密或加密后进行用户授权),示例如<mark>图16-34</mark>所示。

图 16-34 脱敏前查询结果

	ABC phone 🏾 🕄 🕻	ABC tel 🛛 🟹 🕻	ABC email
1	1585 88628	0571-88 2500	and and advantage of the second
2	1833 88185	0571-88 2500	Contraction and the second
3	1701 07826	0571-88 2500	the state of the s

创建脱敏规则

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"敏感数据发现>敏感数据扫描"。
- 步骤3 在扫描任务列表页面,找到目标数据资产,单击"查看"。
- 步骤4 在扫描结果列表页面,找到目标数据库表,单击"添加脱敏规则"。

您也可以在扫描结果列表页面单击"批量添加脱敏规则",将根据扫描敏感数据时使用的行业模板批量生成脱敏规则。如何配置行业模板,请参见<mark>新增行业模板</mark>。

步骤5 在添加脱敏规则对话框中,设置脱敏信息,配置信息如表16-14所示。

参数	说明
规则名称	填写脱敏规则的名称。
模式名	资产的模式名。
表名	资产的表名。
脱敏列表	在脱敏列表中配置脱敏算法。

图 16-35 添加脱敏规则

*规则名称: 脱敏	demo			
* 模式名: doc_	demo			V
* 表名: sys_u	ser			
* 脱敏列表				
旧名	数据类型	命中率	脱敏算法 ①	
hone	手机号码	100%	部分遮蔽	\sim
al	固定电话号码	100%	部分遮蔽	~

步骤6单击"保存"。

----结束

结果验证

- 1. 脱敏规则创建完成后,在"动态脱敏 > 脱敏策略"中查看和管理新建的脱敏规 则。
- 2. 再次使用代理查询数据库表,查询结果是已被脱敏的数据,示例如图16-36所示。

图 16-36 脱敏后数据

	^{ABC} phone ₹ ‡	ABC tel 🛛 🟹 🕻	ABC email	T:
1	158****8628	0571****500	and an interaction of the local states of the	
2	183****8185	0571*****500	Service States and states	
3	170****7826	0571****500		

16.2.6.5 新增自定义数据类型

如果默认数据类型不能满足业务需求,您可以创建自定义的数据类型。

正则表达式(RegularExpression)描述了一种字符串匹配的模式,可以用来检查一个 串是否含有某种子串、将匹配的子串做替换或者从某个串中取出符合某个条件的子串 等。

操作步骤

步骤1 使用系统管理员sysadmin账号登录实例Web控制台。

步骤2 在左侧导航栏,选择"敏感数据发现 > 数据类型管理"。

文档版本 01 (2024-11-28)

X

步骤3 在"数据类型列表"页面,单击右上角的"添加自定义类型"。

步骤4 在添加自定义类型对话框中,配置自定义数据类型。

系统支持通过匹配"列名称"或者匹配"数据内容"来创建自定义数据类型。

• 匹配列名

图 16-37 匹配列明

添加	自定	义类型	
NUNDH		ヘスエ	

居类型名称:	地址	0
* 定义方式:	● 列名 ○ 数据内容	
*列名:	address	0
* 数据类型:	地址 (中文)	\vee
备注说明:	地址信息	0
		4 (200

取消 保存

表 16-15 匹配列名

参数	说明
数据类型名 称	设置自定义的数据类型名称,方便后续管理。
定义方式	选择列名。
列名	输入关键词或者输入正则表达式。 说明: 列名中只要包含关键词或者与正则表达式匹配,则表示 命中。
数据类型	选择对应的敏感数据类型。 内置类型包括数值、字符串、地址组、身份证号、电子邮箱、 身份证号、手机号、日期等。
数据类型说 明	描述您的数据类型说明信息。

文档版本 01 (2024-11-28)

• 匹配数据内容

图 16-38	匹配数据内容
---------	--------

添加自定义类型		Х
* 数据类型名称:	手机号	0
* 定义方式:	○ 列名 (●) 数据内容	
*正则表达式:	0?(13 14 15 17 18)[0-9]{9} 1 只支持字符串正则匹配	0
备注说明:	手机号	0
		3 / 200 /

取消 保存

表 16-16 匹配数据内容

参数	说明
数据类型名称	设置自定义的数据类型名称,方便后续管理。
定义方式	定义方式选择数据内容。
正则表达式	设置匹配自定义数据的正则表达式。 例如手机号码的正则表达式如下: 0?(13 14 15 17 18)[0-9]{9}
数据类型说明	描述您的数据类型说明信息。

步骤5单击"保存"。

新增完成后,您可以在数据类型列表页面查看新增加的自定义数据类型。

图 16-39 自定义数据类型

数据类型名称	数据类型属性	备注说明	操作
地址	自定义类型	地址信息	测试 编辑 删除
手机号	自定义类型	手机号	测试 编辑 删除

步骤6 (可选)单击"测试",输入测试数据验证自定义类型是否符合预期结果。

----结束

相关操作

后续您可以根据情况,在数据类型列表页面进行以下管理操作。

- 编辑自定义的数据类型:单击"编辑",修改自定义数据类型。
- 删除自定义的数据类型:单击"删除",删除不再使用的自定义数据类型。

16.2.6.6 新增行业模板

行业模板是敏感数据类型的合集,能添加多个不同的数据类型(例如车架号、军队证件、三证合一码等)。用户可以根据行业特点,设置自定义的行业模板,在执行敏感 数据发现任务时直接引用此行业模板,避免每次都需要选择数据类型。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"敏感数据发现 > 行业模板"。
- 步骤3 在"模板列表"页面,单击右上角的"添加行业模板"。
- 步骤4 在添加行业模板对话框中,配置模板信息,配置信息如表16-17所示。

图 16-40 添加模板

* 行业模板名称:	官网模板			
备注说明:	官网涉及的敏感数据			
				9/2
安全策略:	☑ 脱敏策略			
敏感数据选择:	■ 全选			
	□ 姓名 (简体中文)	身份证号(中国大陆)		
	□ 年官证亏 ▼ 电子邮箱地址	港澳通行证号 邮政编码	☑ 地址 (中文) □ 固定电话号码	
	✔ 手机号码	1 组织机构名称	统一社会信用代码	
脱敏算法选择:	数据类型	脱敏算法 ①		
脱敏算法选择:	数据类型 * 地址(中文)	脱敏算法 ① 部分遮蔽		~
脱敏算法选择:	数据类型 *地址(中文) *电子邮箱地址	脱敏算法 ① 部分遮蔽 部分遮蔽		~
表 16-17 配置模板参数表

参数	说明
行业模板名 称	设置行业模板的名称。
备注说明	描述行业模板的信息。
安全策略	勾选脱敏策略后,行业模板中包含脱敏策略。需在下方选择脱敏算 法。
敏感数据选 择	模板包含的敏感数据类型,包括以下: 全选:选择全部数据类型,包括内置数据类型和自定义数据类型。 内置数据类型:系统自带的内置数据类型。 自定义数据类型:用户手动创建的自定义数据类型。
脱敏算法选 择	对于勾选的敏感数据,配置对应的脱敏算法。 调用行业模板扫描敏感数据并在敏感数据扫描结果中批量创建脱敏规 则时,将使用此处配置的脱敏算法。

步骤5单击"保存",新增行业模板。

----结束

相关操作

• 模板创建完成后,您可以在模板列表页面查看新增加的行业模板。

图 16-41 新增模板成功

行业模板名称	包含敏感数据关型	备注说明	策略应用	操作
官网模板	手机号码、电子邮稿地址、地	官阿涉及的敏感数据	æ	编辑 复制 删除
默认美型模板	邮政编码、护照号、电子邮箱	53	2 -	32.81
企事业单位敬愿信息模质	电子邮箱地址、固定电话号码…	2	20	30(M)
个人敏感信息模板	电子邮稿地址、港澳通行证号	8	2	规制

• 关于模板的管理操作如表16-18所示。

表 16-18 管理操作

操作	说明
单击编辑	修改自定义行业模板。
单击删除	删除不再使用的自定义行业模板。
单击复制	快速复制修改新的行业模板。

16.2.7 数据加密和解密

16.2.7.1 设置加密参数

配置加密后密文的编码方式,支持十六进制和BASE64等。如果您需要支持模糊查询功 能,则加密参数必须配置为十六进制。

使用约束

仅在系统中没有配置资产时可以修改密文编码方式。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"数据加密 > 加密参数"。
- **步骤3** 在"加密参数"页面的"密文编码方式"下拉栏中,可以选择"十六进制"、 "BASE64"等。
- 步骤4 配置后,加密表的密文显示为十六进制编码的字符串或者BASE64编码的字符串,具体示例如下图16-42所示。

图 16-42 十六进制编码的密文示例



----结束

16.2.7.2 查看加密算法

初始化密钥后,系统会根据密钥生成对应的加密算法,用户可以在算法查看页面查看 系统支持的加密算法。

前提条件

确保已初始化密钥,具体初始化密钥操作,请参见<mark>初始化密钥</mark>章节。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏中,选择"数据加密 > 算法查看"。
- 步骤3 在"算法查看"页面,查看算法具体信息。
 - ----结束

16.2.7.3 仿真加密测试

在配置加密队列前,建议先通过仿真加密测试,检查加密是否存在问题。

操作步骤

步骤1 使用系统管理员sysadmin账号登录实例Web控制台。

文档版本 01 (2024-11-28)

- 步骤2 在左侧导航栏中,选择"业务测试 > 仿真测试"。
- 步骤3 单击"新增加密测试"。
- 步骤4 在"新增加密测试"对话框中,配置测试目标,相关参数如表16-19所示。

图 16-43 新增加密测试

曾加密测	liat						2
• 数据源	夏名称:	demo			~	demo	
* 8	赋名:	doc_demo			×.	教 据源类型: MySQL	
	現名・	svs user				数据源版本: 5.7	
	ALL.					数据源地址: 1	
• 加密算	嘘⊙;	SM4_128			V (数据源端口: 」	
						主机P:	
• 校验算	底();	SM3_HMAC_16				主机满口:	
•加索3	列表					CPU:	
选择	列名		数据类型	备注信息		肉落・	0%
~	dept	_id	bigint(20)	Department ID		F317.	0%
~	user	_name	varchar(720)	User account		网络:	
~	nick	name	varchar(720)	User's nickname		10:	
	user	_type	varchar(272)	user type(00syste		操作系统:	
	ema	il	varchar(2928)	email			
	pho	nenumber	varchar(2928)	phone number			
	sex		varchar(272)	gender			

保存

表 16-19 仿真测试

参数	说明
数据源名称	资产的资产名称。
模式名	资产的模式名。
表名	资产的表名。
加密算法	在下拉栏中选择加密的算法。 可以在 <mark>查看加密算法</mark> 页面查看支持的算法类型。
校验算法	在下拉栏中选择校验的算法。 校验算法用于重要数据的完整性校验,可以在 <mark>查看加密算法</mark> 页面查 看支持的算法类型。

步骤5 单击"加密列表"页签,勾选需要加密的列名称。

步骤6单击"保存"。

测试完成后,用户可以在列表中查看测试结果,单击"详情"查看加密流程中各个节点的完成情况。

步骤7 测试完成后,单击"删除",删除此仿真加密测试。

▲ 注意

如果测试后需要配置加密队列,需要先删除此仿真加密测试。

----结束

16.2.7.4 配置加密队列

- 如果您已了解数据库表结构,可以直接在加密队列管理页面直接添加。配置加密 后,未授权用户查询对应的数据库信息时,将只查看到密文内容。
- 如果对敏感数据分布不了解,可使用敏感数据发现功能扫描您的数据库,在识别结果中创建加密队列,对数据库表进行加密,具体操作请参见在结果中创建加密队列。

前提条件

在配置加密队列之前,建议先进行仿真加密测试,检验加密过程中是否会存在问题, 并解决相应问题再进行配置,具体操作,请参见<mark>仿真加密测试</mark>。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏中,选择"数据加密 > 加密队列管理"。
- 步骤3 单击右上角的"新增加密队列"。
- 步骤4 在"新增加密队列"对话框中,设置加密信息,相关参数如表16-20所示。

表 16-20 新增加密队列

参数	说明
资产名称	资产的资产名称。
模式名	资产的模式名。
表名	资产的表名。
加密算法	在下拉栏中选择加密的算法。 可以在 <mark>查看加密算法</mark> 页面查看支持的算法类型。
校验算法	在下拉栏中选择校验的算法。 校验算法用于重要数据的完整性校验,可以在 <mark>查看加密算法</mark> 页面查 看支持的算法类型。
每批条数	设置加密队列每批处理的数据量。
线程数	设置加密队列占用的线程数量。
启动队列	勾选后,创建队列后自动启动队列。

图 16-44	新增加密队列
---------	--------

• 数据	源名称: den	no			demo
•	模式名: doc	_demo			数据源类型: MySQL
	• 表名: \$y\$	user			数据源版本: 5.7 数据源地址: 172 16 36 251
• 加密1	啊法①: SM	4_128			数据源端口: 3306
· 校验	u注①: SM	3_HMAC_16		v	主机P:
• 每	批祭数: 819	1	• 线程数:	4	EPU:
启	动队列: 🔽				0% 内存:
• bas	例表				0% 网络:
选择	列名	数据类型	启用模糊查询	备注信息	10:
	dept_id	bigint(20)		Department ID	操作系统:
	user_name	varchar(720)		User account	
	nick_name	varchar(720)		User's nickname	
	user_type	varchar(272)		user type(00syste	
	email	varchar(255)		email	
	phonenum	varchar(255)		phone number	

步骤5 单击"加密列表"页签,勾选需要加密的列名称,并设置是否启用模糊查询功能。

图 16-45 选择加密列

		RAINAL	后用侵相复词	备注信息	10,	
	dept_id	bigint(20)		Department ID	操作系统:	
	user_name	varchar(720)		User account		
	nick_name	varchar(720)		User's nickname		
	user_type	varchar(272)		user type(00syste		
2	email	varchar(255)		email		
1	phonenumber	varchar(255)		phone number		
	sex	varchar(272)		gender		

加密后,默认情况下无法进行模糊查询。如果符合以下情况,勾选"启用模糊查询" 后支持模糊查询,模糊查询支持%和_两种符号。

- 密文编码方式为十六进制,不支持BASE64模式编码。如何配置,请参见设置加密参数。
- 字段为字符串类型,如:varchar、text。其它类型不支持。

步骤6 单击"初始化表",开始对数据表进行初始化操作。

步骤7 单击"完成",创建加密队列。

步骤8 如果配置时未勾选"启动队列",单击加密队列的启动按钮 (),开始加密。

加密队列加密时如果中断,可以单击启动按钮⁽⁾,系统会在原来的进度上继续加密。

操作结果

 加密队列创建完成后,可以在列表中查看和管理新建的加密队列。加密队列完成 存量数据加密后会自动移除。此时队列为"已移除"状态,但系统还会继续进行 正常加密数据。

图 16-46 加密队列



• 加密完成后,未授权用户查询到的数据是已经加密过的数据。

图 16-47 加密数据

1	1	🖁 user_id 🛛 💌	123 dept_id	٠	ADC user_name	noc nick_name 🔹	noc user_type 💌	RSC email 👻	ABC phonenumber	not sex	-
1	E			103	admin1	88	00	IEC9Vkn7WLo5lcdW4BVGzT1RiGX2tbcsc2VLq2VF8Ulz	IEC9YU/9Xrw/UcZQ485DhmoSSMUNEH0Y1GGW5Kw=	1	_
2		2		105	admin2	88	00	IEC9Vkn7WLo5lcdW4BVGzT1RiGX2tbcsc2YLq2YF8Ulz	IEC9Z0/9Xrw/UcZQ49ggt+ihzLNuPWy1DOYzPhQ=	1	

相关操作

在任务队列的列表中,您可以管理加密队列。

- 单击"详情",可以查看"加密队列状态"、"队列名"、"被加密表名"、 "被加密列名"、"加密算法"等信息。
- 单击"编辑",可以修改"加密的数据库列"等信息。

16.2.7.5 管理授权

支持在授权管理页面为访问数据库的客户端和数据库用户授权。

授权管理模块中支持客户端和用户授权,两者授权取交集,详情请参见<mark>设置客户端授</mark> 权和设置用户授权。

管理授权示例说明如下:

表 16-21 设置示例说明

参数	示例值
客户端授权	IP地址范围:
	• 192.168.0.100~192.168.0.120
	• 192.168.1.100~192.168.1.120
用户授权	wordpress用户支持查询、添加、修改权限。

配置后结果如下:

- 如果用户的IP地址为192.168.0.105,通过代理方式,使用wordpress访问数据库, 可以查看到明文数据。
- 如果用户的IP地址为192.168.0.105,通过代理方式,使用非wordpress访问数据 库,只能查看到加密数据。
- 如果用户的IP地址为192.168.3.105,通过代理方式,使用wordpress访问数据库,只能查看到加密数据。

设置客户端授权

通过访问数据库的客户端维度进行授权。

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏中,选择"数据加密 > 授权管理"。
- 步骤3 在数据源列表中,单击目标数据源。
- 步骤4 找到目标加密数据库表,单击"客户端授权"。
- 步骤5 在"客户端授权"对话框中,设置客户端IP地址范围、时间范围和星期范围。

图 16-48 客户端授权

IP范围 ①:	196.168.0.100-	196.168.0.120		٥	Θ
	196.168.1.100-	196.168.1.120		٥	Θ
时间点范围:	00	0 -	23	0	
星期范围:	星期一	~ -	星期天	\vee	

Х

🗀 说明

- IP地址范围支持设置起始IP和结束IP,单击 ●按钮可以添加多个IP地址范围,最多设置5个IP 地址范围。
- 时间点范围的取值范围为00~23,数值表示整点范围。例如,取值10表示10:00~10:59,包含10:00和10:59;如果时间点范围设置为08~18,则表示的时间范围为08:00~18:59,包含08:00和18:59。

步骤6 单击"保存"。

----结束

设置用户授权

在用户维度进行授权来控制访问数据库的权限。

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏中,选择"数据加密 > 授权管理"。
- 步骤3 在数据源列表中,单击目标数据源。
- 步骤4 找到目标加密数据库表,单击"用户授权"。
- 步骤5 在"用户授权"对话框中,设置需要授权的数据库用户。

图 16-49 用户授权

用户授权

REAL VID H					
用户	权限				
root	查询	🔲 添加		□ 删除	
mysql.infoschema	查询	🔲 添加	🏼 编辑	🗐 删除	
mysql.session	查询	🔲 添加	🏼 编辑	🗐 删除	
mysql.sys	查询	🔲 添加	🏼 编辑	□ 删除	
			取消	清空	保存

步骤6单击"保存"。

----结束

16.2.7.6 仿真解密测试

在配置解密队列之前,建议先进行仿真解密测试,验证解密功能。

前提条件

需要解密测试的表格已经在加密队列中完成加密,即已完成<mark>配置加密队列</mark>。

文档版本 01 (2024-11-28)

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏中,选择"业务测试 > 仿真测试"。
- 步骤3 单击"新增解密测试"。
- 步骤4 在"新增解密测试"对话框中,配置测试目标。

图 16-50 新增解密测试

 数据源名称: demo 				~	A demo	
					4 Þ	
•模式名:	doc_demo			×	数据源类型: MySQL	
• 表名:	sys_user				数据源版本: 5.7	
					数据源地址: 1	
*加密算法①:	SM4_128				数据源端口:	
* 核驗質法 ①:	SM3 HMAC 16				主机IP:	
1X22412 ().	511152111110210				主机端口:	
•加赛列表					CPU:	
选择列	B	数据类型	备注信息		0%	
de	pt_id	bigint(20)	Department ID		内存:	
use	er_name	varchar(720)	User account		网络:	
nic	k_name	varchar(720)	User's nickname		10:	
use	er_type	varchar(272)	user type(00syste		操作系统:	
em em	ail	varchar(2928)	email			
9 ph	onenumber	varchar(2928)	phone number			
sex	t.	varchar(272)	gender			

步骤5 单击"保存"。

测试完成后,用户可以在列表中查看测试结果,单击"详情"查看解密流程中各个节 点的完成情况。

步骤6 测试完成后,单击"删除",删除此仿真解密测试。

如果测试后需要配置解密队列,需要先删除此仿真解密测试。

----结束

16.2.7.7 配置解密队列

如果数据库不再需要加密,可通过配置解密队列进行解密。配置解密后,对应的数据 库列中的信息将变为加密前的明文数据。

您可以在"加密队列管理"页面,找到目标加密队列,单击"添加至解密队列"创建 解密队列;也可以在"解密队列管理"页面创建解密队列。

此处以在"解密队列管理"页面为例,介绍如何创建解密队列。

文档版本 01 (2024-11-28)

前提条件

在配置解密队列前,建议先进行仿真解密测试,检验解密过程中是否存在问题,具体 操作请参见<mark>仿真解密测试</mark>。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏中,选择"数据加密 > 解密队列管理"。
- 步骤3 单击右上角的"新增解密队列"。
- 步骤4 在"新增解密队列"对话框中,设置需要解密的数据相关信息。
 - 数据信息包括资产名称、模式名和表名。您可以在下拉栏中直接选择。
 - 如果目标数据库模式中没有被加密的表格,则无法选择表名,请先对其进行加密,详细加密操作请参见配置加密队列。

图 16-51 新增解密队列

用王牌名	队列							
• 数据源	ī名称: c	lemo				demo		
• 60	武 名: 0	loc_demo			~	数据源类型: MySQL		
	表名: s	ys_user				数据源版本: 5.7 数据源地址: 1		
 加密算: 	法①: 5	M4_128			~	数据源端口:		
• 校验算	法①: 5	M3_HMAC_16				主机P: ±初始□-		
• 每批	北条数: 6	.553	• #	耀致: 4		CPU:		
启动	肋队列: 🔽					0%		
• hosta	列表					0% 网络:		
(Break)								
选择	列名		数据类型	备注信息		ю:		
选择	列名 dept_ic	<u>(</u>	数据类型 bigint(20)	备注信息 Department ID		IO: 操作系统:		
· mad() 选择	列名 dept_ic user_na	I	数据类型 bigint(20) varchar(720)	备注信息 Department ID User account		10: 摄作系统:		
选择	列名 dept_ic user_na nick_na	I ame	数据类型 bigint(20) varchar(720) varchar(720)	备注信题 Department ID User account User's nickname		10: 操作系统:		
选择	列名 dept_ic user_n: nick_na user_ty	I ame pe	数据类型 bigint(20) varchar(720) varchar(720) varchar(272)	备注信题 Department ID User account User's nickname user type(00syste		10: 攝作系統:		
me827 选择 〇 〇 〇	列名 dept_ic user_n: nick_na user_ty email	f ame ime pe	数据类型 bigint(20) varchar(720) varchar(720) varchar(272) varchar(2928)	备注信题 Department ID User account User's nickname user type(00syste email		IO: 操作系统:		

步骤5 勾选"启动队列",创建完成后自动启动解密队列。

步骤6 单击"完成",创建解密队列。

解密完成后,数据库表对应列的数据已经被解密,即数据库列中的数据恢复到明文状 态。

----结束

16.2.7.8 加密表管理

对于加密表,系统支持在Web页面编辑索引和编辑非加密列。

编辑索引

在数据量较大时(例如大于1000万行),查询加密列非常耗时,通过添加索引可以加 快查询效率。添加索引可以直接在数据库资产上操作,也可以在系统上操作。本文介 绍在系统中为加密列添加索引。

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏中,选择"数据加密 > 加密表管理"。
- 步骤3选择"数据源>资产名称"。
- 步骤4 在列表中,查看被加密表清单。用户可以通过模式和表名称搜索目标被加密表。
- 步骤5 找到目标被加密表,单击"编辑索引",进入索引列表界面。
- 步骤6 单击"添加索引"。
- **步骤7** 在"添加索引"对话框,配置索引参数。选择加密列,并配置索引名称和索引长度, 单击"预览"查看添加索引的SQL语句。

图 16-52 添加索引

	行过程中全部时间波,诸可	NUCLEUF	SALING
▶选择列:	NAME	8	ALTER TABLE 'TEST'.'ddm_rules5' ADD INDEX 'test'('NAME' (100)) USING BTREE
索引名称:	test	0	
索引长度:	100	(范围: 1~3072)	
注释:	请输入		
		07500,	
	预览		

步骤8 单击"保存"。

----结束

X

编辑非加密列

一般情况下,对数据资产中的数据库表进行加密后,用户不能直接在数据库中进行添 加新列操作。如需添加新列,需要先对此加密表进行全量解密,然后才能添加新列。 此场景需要停止现网业务,对用户业务影响比较大。

系统支持在不全量解密的情况下添加列,通过"编辑非加密列"功能,用户可以在不 全量解密的情况下添加列,仅在执行时会锁定加密表,对现网影响小。

🗋 说明

如果用户需要在加密表中大量改动列,仍然需要对加密表全量解密后进行修改。

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏中,选择"数据加密 > 加密表管理"。
- 步骤3选择"数据源>资产名称"。
- 步骤4 在列表中,查看被加密表清单,用户可以通过模式和表名称搜索目标被加密表。
- 步骤5 找到目标被加密表,单击"编辑非加密列"。
- 步骤6跳转后,单击添加列。
- **步骤7** 在添加列对话框,配置列参数,配置新增列的列名称、数据类型、是否非空、默认值和列长度,单击"预览"查看添加列的SQL语句。

□□ 说明

默认值的内容不支持包含单引号或双引号。

图 16-53 添加列

添加列

*列名:	name	٥	ALTER TABLE 'TEST'.'ddm_rules5' ADD COLUMN 'name' VARCHAR (10) DEFAULT 'name' NULL
数据类型:	VARCHAR	~	
非空:) 是 🖲 否		
认值 ①:	'name'	٥	
列长度:	10	٥	
注释:	请输入		
		0 / 50 /	
	预览		

步骤8 单击"保存"。

----结束

16.2.7.9 回滚表结构

数据库表初始化后,系统会修改表结构。如果需要恢复到原状态,需要进行回滚表结 构。

场景:在数据库表进行初始化后,开始加密前,若需回退到原始状态需执行手动回滚 表结构。

• 数据源名	称: demo			V & demo
• 模式	名: doc_demo			∨ 数据源类型:MySQL
• 表	Svs user			数据源版本: 5.7
100				数据源地址: 17
加密算法	(): SM4_128			∨ 数据源端口:
4430.002+	O. CHIZ HMAC 10			主机IP:
仪短羿法	U: SMIS_HMAC_IC	2		↓ 主机端口:
* 每批条	数: 8191	* \$	乾程数: 4	CPU:
				0%
(Cath)				
10 AJRA	列: 🔽			内存:
• 加麥列表	列: 🔽			内存: 0% 网络:
- 加坡列表 选择	列: ▼ 列名	数据类型	备注信息	内存: 0% 网络: IO:
·加宏列表 选择	列: I	数据类型 bigint(20)	备注信息 Department ID	内存: 0% 网络: IO: 操作系统:
*加密列表 选择	列: ♥ 別名 dept_id user_name	数据类型 bigint(20) varchar(720)	裔注信题 Department ID User account	内存: 0% 网络: IO: 撮作系统:
·加密列录 选择	列: 회사 외성 에서 이다. 이다. 이다. 이다. 이다. 이다. 이다. 이다.	数据类型 bigint(20) varchar(720) varchar(720)	备注侦息 Department ID User account User's nickname	内存: 0% 网络: IO: 操作系统:
·加密列录 ·加密列录	列: 회원: 列名 dept_id user_name nick_name user_type	数据类型 bigint(20) varchar(720) varchar(720) varchar(272)	裔注旗原 Department ID User account User's nickname user type(00syste	内存: 0% 网络: IO: 操作系统:
·加密列求 ·加密列求 	列: 로 列名 dept_id user_name nick_name user_type email	数据类型 bigint(20) varchar(720) varchar(272) varchar(272) varchar(2928)	新注航息 Department ID User account User's nickname user type(00syste email	内存: 0% 网络: 10: 操作系统:

图 16-54 初始化表

操作步骤

步骤1 使用系统管理员sysadmin账号登录实例Web控制台。

- 步骤2 在左侧导航栏中,选择"数据加密 > 回滚表结构"。
- 步骤3 单击"数据源",选择资产名称、模式名称,如图16-55所示。

Q

图 16-55 选择模式



请输入

- mysql
- demo

doc_demo

- 步骤4 在列表中,选择数据库表,单击"检查关联队列"。
- 步骤5 单击"还原表结构"。
- 步骤6 单击"还原列"。

数据资产中所有表回滚完成后,您可以到数据源管理页面,对数据资产进行删除等操 作。

----结束

16.2.7.10 安装 Bypass 插件

数据加密后如果出现设备单点故障,在大数据量场景下密文恢复工具解密时间较长。 该场景下可使用bypass插件,在加密设备单点故障的情况下利用插件对客户的密文数 据实时加解密,保证客户的业务进行快速恢复。

建议提前部署好Bypass插件,以应对加密设备单点故障的情况。

使用约束

- 支持的数据库类型为MySQL。
- 逃生插件的安装仅支持jre8及以上、linux_x86环境。

插件状态

插件部署在客户的应用系统上。插件状态有三种:

- online:准备状态,插件状态正常。可以通过心跳进行状态检测,加密系统会定 期推送相应的加密配置和密钥文件到插件端。等待加密系统故障后切换到激活状 态。
- bypass:激活状态,插件状态正常。插件已检测到加密系统异常,插件开始工作,修改应用连接从网关代理到直连数据库,并对jdbc请求中的数据进行加解密。

当应用配置连接的是网关加密代理地址且应用到网关加密代理地址不通时,插件 将切换到bypass状态。

操作步骤

- 步骤1 登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"数据加密 > bypass管理"。
- 步骤3 单击页面右上角的"插件下载",下载插件安装包gde-agent.tar.gz。
- 步骤4 插件下载后,根据客户应用系统的部署场景,安装插件。

----结束

操作结果

安装完成后,插件列表出现插件信息。如果加密设备出现单点故障,插件开始工作。

16.2.7.11 查询应用访问记录

应用通过代理访问数据库后,系统会自动记录到访问记录列表中。管理员可以通过访问记录列表,定期检查和审计。

前提条件

设备仅记录应用通过代理访问数据库的记录信息。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"数据加密 > 应用访问记录"进入"访问记录列表"界面。
- **步骤3** 在访问记录列表中,查看应用的访问记录信息,包含查看资产名称、数据源IP、代理 IP、应用IP等信息。

可以通过设置资产类型和资产名称,过滤对应的访问记录。

----结束

16.2.8 动态脱敏

16.2.8.1 新增自定义脱敏算法

系统内置多种针对敏感数据的脱敏算法,如果默认脱敏算法不能满足业务需求,您可以创建自定义的脱敏算法。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"动态脱敏 > 脱敏算法"。
- 步骤3 在"脱敏算法列表"页面,单击右上角的"添加自定义算法"。
- 步骤4 在添加自定义算法对话框中,配置自定义脱敏算法。

Х

图 16-56 添加自定义算法

添加自定义算法

联数据类型:	电子邮箱地址	V
算法类型:	● 字符串	
	保留前 0 字符 保留后 6	字符
* 遮蔽符号:	×	V
备注说明:	请输入	
		0 / 200

表 16-22 添加自定义算法

参数	说明
算法名称	设置自定义的算法名称,方便后续管理。
关联数据类型	选择脱敏算法关联的敏感数据类型。
算法类型	设置脱敏数据保留的前后字符数。
遮蔽符号	选择脱敏使用的遮蔽符号。
算法说明	描述您的算法类型说明信息。

步骤5 单击"保存"。

新增完成后,您可以在数据类型列表页面查看新增加的自定义脱敏算法。

图 16-57 自定义脱敏算法

 算法高性
 数据类型
 脱敏类型
 备注说明
 操作

 电子邮箱地址-电子邮箱保留后...
 自定义算法
 电子邮箱地址
 遮蔽脱敏
 编辑
 删除

----结束

相关操作

后续您可以根据情况,在脱敏算法列表页面进行以下管理操作。

- 编辑自定义的脱敏算法:单击"编辑",修改自定义脱敏算法。
- 删除自定义的脱敏算法:单击"删除",删除不再使用的自定义脱敏算法。

16.2.8.2 创建脱敏规则

通过创建脱敏规则,可对数据库中的明文数据起到脱敏效果,保障数据安全。

- 如果您已了解数据库表结构,可以在脱敏策略页面直接添加规则脱敏规则。配置 脱敏规则后,非脱敏白名单用户查询对应的数据库信息时,将只查看到脱敏数 据。
- 如果对敏感数据分布不了解,可使用1.4.6 敏感数据发现功能扫描您的数据库,在 识别结果中创建脱敏规则,具体操作请参见1.4.6.4 在结果中创建脱敏规则。

对于数据表中的数据既启用加密又启用脱敏的场景,不同配置的效果如下:

- 数据表已加密且用户已授权时,开启脱敏,则查询返回脱敏数据;
- 数据表已加密且用户未授权时,开启脱敏,则查询直接返回密文,不脱敏。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏中,选择"动态脱敏 > 脱敏策略"。
- 步骤3选择"数据类型>数据源名称"。

图 16-58 选择数据源

NySQL

_	_		_	
С	ρ	m	\sim	
u	<u> </u>		v	

- 👂 🥯 Oracle
- PostgreSQL

步骤4 在目标数据源的脱敏规则列表页面,单击"添加自定义规则"。

步骤5 在"添加脱敏规则"对话框中,配置脱敏规则参数。相关参数如表16-23所示。

Х

取消

保存

表 16-23 添加脱敏规则

参数	说明
规则名称	设置脱敏规则的名称。
模式	选择数据资产的模式。
表名	选择数据资产的表名。
列名	选择需要脱敏的列名。 可以在1.4.7.2 查看加密算法页面查看支持的算法类型。
数据类型	选择该列对应的敏感数据类型。 可添加自定义数据类型,具体操作,请参见 1.4.6.5 新增自定义数据 <mark>类型</mark> 。
算法类型	选择对该列使用的脱敏算法。 可添加自定义脱敏算法,具体操作,请参见 1.4.8.1 新增自定义脱敏 <mark>算法</mark> 。

图 16-59 添加脱敏规则

添加脱敏规则

* 规则名称:	脱敏test	
*模式:	doc_demo	
*表名:	sys_user	~
*列名:	email	V
▶数据类型:	电子邮箱地址	V
▶ 脱敏算法:	部分遮蔽	¥

步骤6单击"保存",创建脱敏规则。

----结束

操作结果

脱敏规则创建完成后,可以在列表中查看和管理新建的脱敏规则。添加的脱敏规则自动处于开启状态。

图 16-60 脱敏规则

规则名称	数据源名称	模式	表名	列名	数据类型	脱敏算法	启用/停用	操作
脱敏test	demo	doc_demo	sys_user	email	电子邮箱地址	部分達蔽	•	编辑 删除

• 脱敏完成后,非白名单用户查询数据库的明文数据,显示的是脱敏数据。

图 16-61 脱敏后数据

12 <mark>7</mark> user_id 🛛 🕄 🕻	123 dept_id 🏾 🕄 🕻	ABC user_name 1	^{ABC} nick_name	ABC user_type 1	ABC email 💦 🕄 🕻
1	100	adada -	the second se	-66	1***3@163.com
2		17 C	10 C	-	1***3@qq.com

相关操作

在脱敏规则列表中,您可以管理脱敏规则。

- 单击启用/停用栏按钮,可以启用/停用脱敏规则。
- 单击"编辑",可以修改脱敏规则相关信息。
- 单击"删除",可以删除不再使用的脱敏规则。
- 单击"批量操作",可以在下拉框中批量启用/停用、删除脱敏规则。

16.2.8.3 配置脱敏白名单

支持在白名单列表页面添加脱敏白名单,支持从数据库用户名、IP范围、开始时间及 结束时间这几个参数设置白名单,各参数之间为"且"的关系,若配置多个参数需同 时满足才可生效。满足脱敏白名单时,可查看未脱敏的明文数据。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏中,选择"动态脱敏 > 脱敏策略"。
- 步骤3选择"数据类型>数据源名称"。

图 16-62 选择数据源

NySQL

demo

- Oracle
- PostgreSQL

步骤4 在目标数据源的脱敏规则列表页面,单击"脱敏白名单"。

步骤5 在"白名单列表"页面,单击"添加白名单"。

步骤6 在"添加白名单"对话框中,设置白名单参数,相关参数如表16-24所示。 各参数之间为"且"的关系,若配置多个参数需同时满足才可生效。

表 16-24 添加白名单

参数	说明				
数据源	显示数据源名称。				
数据库用户名	设置加入白名单的数据库用户名。				
IP范围 设置加入白名单的IP范围。					
开始时间	设置白名单生效的开始时间。				
结束时间	设置白名单生效的结束时间。				
放行规则	 全部规则:该数据源的全部脱敏规则均放行。 指定规则:该数据源的指定规则放行,需选择指定放行的规则。 				

图 16-63 添加白名单

数据库用户名:	root	
IP范围 ①:	请输入	•
受权开始时间:	2024-08-27 16:31:14	
受权结束时间:	2024-08-31 16:31:22	
於行却刚小	全部抑则 / 指定抑则	

步骤7 单击"保存"。

----结束

16.2.9 密钥管理

16.2.9.1 更新数据源密钥 DSK

用户可以手动更新或者周期性更新数据源密钥DSK,保障业务安全性。

前提条件

已经初始化密钥,详细操作请参见<mark>初始化密钥</mark>。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- **步骤2** 在左侧导航栏,选择"密钥管理 > 密钥配置"。
- 步骤3 在密钥更新区域,配置手动更新或者周期性更新数据源密钥DSK。

图 16-64 密钥更新

密钥更新	
仅更新DSK	
周期更新 密明:- 编辑	立即更新密钥

- 步骤4 如果手动更新数据源密钥DSK,请按照以下步骤进行操作:
 - 1. 单击"立即更新密钥"。
 - 2. 在"口令校验"对话框中,输入安全口令,单击"确定"。
- 步骤5 如果周期性更新数据源密钥DSK,请按照以下步骤进行操作:
 - 1. 在周期更新密钥处,单击"修改"。
 - 2. 在"修改密钥更新周期"对话框中,配置更新时间,相关参数如<mark>表16-25</mark>所示。

图 16-65 修改密钥更新周期

修仪密钥史新周期

	-	~	

表 16-25 修改密钥更新周期

参数	说明
更换周期	设置密钥更新的周期,支持以下选项: - 无:不进行周期性更新。 - 每天:每天更新一次。 - 每周:每周更新一次。 - 每月:每月更新一次。
更换时间	根据更换周期,配置密钥更新的时间点。

步骤6单击"保存"。

-----结束

后续操作

更新数据源密钥DSK后,系统销毁原DSK,并生成新的DSK。您可以在<mark>查看密钥信息</mark>查 看密钥变更情况。

16.2.9.2 配置 KMS 对接

密钥管理的密钥源支持从KMS系统中获取。目前支持华为云。

KMS系统(Key Management Service)作为一种密码平台产品,可以为第三方密码应用 提供密钥管理服务。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"密钥管理 > KMS管理"。
- 步骤3 单击"华为云"页签。
- 步骤4 配置华为云KMS对接参数,相关参数如表16-26所示。

表 16-26 参数说明

参数	说明			
项目名	华为云的region名,可从KMS控制台Web页面的URL中获取,如 <mark>图</mark> 16-66所示。			
用户名	IAM的用户名。			
用户密码	IAM的用户密码。			
用户主体账号	IAM的租户名,即IAM用户所属的账号。			
密钥名称	华为云KMS的密钥别名。			

图 16-66 华为云 KMS 界面参数示意

C D M	tps://consol	shuaweicloud.com/console/?region=cn-north-48loc	ale=zh-cn#/dew/kms/keyList/customKe			A 🟠 🗿 🛡 G	i 🖆 🖷 👒 🍧
		1	🚯 把米米开局数感播作保护。	存在安全风险,请您附往 安全设置>数据操作>操作保护 开向数据图	inge. Nafia		
🛔 \$P\$为云 丨 🟠	12865 Q	208四 👻		22	Q 展用与成本 资源 企业 :	开发工具 餐宴 支持与服务 工单 曾体中3	
数据加密控制台	ŝ	密钥管理 ③					1938年6月 日本市田田
8988		() 就進出參加政策加減服務使用体验講研, 出生費的	意见和建议是我们转唤得开产品体验的原动力。	感谢您的参与!			×
来初对管理		KMS融广活动: 2019年12月12日至2022年3月31日,	STREAM S	永久免疫使用。			
凭服管理		KMS能增的服务:计算实服务—ECS, IMS, FACS, GA	CS, CSBS: 存储类服务—EVS, VBS, OBS, SI	S, SFS Turbo: 图据库实验给—MySQL, PosigreSQL, SQL Serv	w, DDS.		
专用印度	*						
弹性云服务器	P	自定义密钥 默认密钥 专属密钥库					
对象存住服务	e	一共可以追踪 20 个密钥,您还可以追踪 18 个密钥。					
云侧份	ø	品用 预用 数种 取消费	08	所有密切算法	 所有密钥状态 	 ・ ・ ・	(15≝101 × C ⊕
云硬盘	ø	31840 JE	務器	密明算法获用途	編組約488金額 1Ξ	10ft	
			(1) 就用	AES_296 ENCRYPT_DECRYPT	运销管理	品用 開除	
			19 BR	AES_256 ENCRYPT_DECRYPT	或切答理	9773 8599	

步骤5 单击"测试连接"。

步骤6 连接成功后,单击"保存"。

----结束

后续操作

配置完成后,初始化密钥时可选择通过密钥平台获取密钥。具体操作请参见<mark>初始化密</mark> <mark>钥</mark>。

16.2.9.3 查看密钥信息

系统会记录已创建的密钥ID、密钥类型等相关信息。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"密钥管理 > 密钥查看"。
- 步骤3 搜索和查看密钥相关信息。

图 16-67 查看密钥

密钥查看

密钥类型	全部	V	密钥状式	全部	\sim			C @ I
生成时间	J V	开始日期	~	结束日期	8	关联关系:全部	~	
密钥ID	密钥类型	密钥来源	密钥长度	密钥状态	密钥关联	关系	生成时间	销毁时间
607	DEK	系統内置	128位	• 销毁	资产: de	mo-表sys_user-列ph	2024-08-27 16:19:53	2024-08-27 16:21:13
604	DEK	系统内置	128位	• 销毁	资产: de	mo-表sys_user-列em	2024-08-27 16:19:53	2024-08-27 16:21:13
601	DEK	系统内置	128位	• 生效	资产: de	mo-表ddm_rules5-列	2024-08-27 16:14:38	
598	DEK	系统内置	128位	• 生效	资产: de	mo-表ddm_rules5-列…	2024-08-27 16:14:38	

----结束

16.2.10 系统管理

16.2.10.1 手动创建账号

系统默认已经创建系统管理员(sysadmin)、审计管理员(audadmin)和安全管理 员(secadmin)账号。如果有多个员工需要使用系统,建议您为每个员工单独创建账 号,便于管理。

账号的权限由角色决定,系统默认创建系统管理员、审计管理员和安全管理员角色。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,单击"系统管理 > 账号管理"。
- 步骤3 在页面右上角,单击"新建账号"。
- 步骤4 在"新建账号"对话框中,配置账号相关信息,配置信息如表16-27所示。

图 16-68 新建账号

新建账号		×
* 账号:	assetmanager	
* 密码:		
* 确认密码:		
使用人:	张三	
* 关联角色:	系统管理员 🗸 🗸	
电话:	1300000000	
邮箱:	test@example.net	
使用期限:	 永久 定义期限 	
备注说明:	资产管理员	
	5 / 200 ,	
	取消	提交审核

表 16-27 新建账号

参数	说明
账号	设置账号名称。
密码/密码 确认	设置和确认账号的密码。 建议用户初次登录后修改密码,并定期更新密码,从而降低信息泄漏 风险。
使用人	设置使用人。
角色	 在下拉栏选择角色。 安全管理员 审计管理员 系统管理员
电话	设置电话号码。
邮箱	设置邮箱地址。
使用期限	选择使用期限。
时间期限	 当您选择使用期限为定义期限时,请设置时间期限。 账号创建之后立刻生效,但超过设置的时间期间后账号失效,无法通过此账号登录管理平台系统。
备注说明	描述备注说明。

步骤5 单击"提交审核"。

步骤6 在列表中找到刚创建的账号,在启用状态列,打开启用开关。

🗀 说明

新增的账号自动处于"未审核"状态,通过审核之后可以登录系统。具体操作请参见审核账号。

----结束

相关操作

后续您可以根据情况,在账号列表页面进行以下管理操作。

表 16-28 批量管理操作

操作	说明
单击编辑	修改账号信息。
单击删除	删除不再使用的账号。
单击启用	启用账号。

操作	说明
单击停用	停用账号,停用后将不能使用此账号登录系统。
单击重置密码	系统自动为账号修改密码,重置后的密码与账号相同。

16.2.10.2 组织架构管理

通过组织管理,管理组织架构信息和部门内成员信息。

16.2.10.2.1 创建组织部门

部门可以用来管理人员,根据公司实际需求创建部门,完善组织架构。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"系统管理>组织管理"。
- 步骤3 在左侧的组织架构区域,单击"添加组织"。
- 步骤4 在"添加组织"对话框中,配置组织部门相关信息。

图 16-69 添加组织

 * 组织名称: 开发部 * 组织编号: 009 * 上级组织: 无上级组织 ∨ 	添加组织		×
 * 组织编号: 009 * 上级组织: 无上级组织 ∨ 	* 组织名称:	开发部	
* 上级组织: 无上级组织 V	* 组织编号:	009	
	* 上级组织:	无上级组织 🗸 🗸 🗸	

表 16-29 添加组织

参数	说明
组织名称	设置部门名称。
组织编码	设置组织的内部编码信息。
上级部门	在下拉框中选择上级部门。 如果不选择,则默认新建部门为一级部门。

取消

确认

步骤5 单击"确认"。

----结束

16.2.10.2.2 手动创建成员

通过新增人员信息,完善组织架构。可根据公司实际人员需求创建。

前提条件

已有部门用于管理人员,关于部门的相关操作请参见创建组织部门。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"系统管理>组织管理"。
- 步骤3 单击"添加成员"。
- 步骤4 在添加成员对话框中,配置人员相关信息。

图 16-70 添加用户

添加成员		×
* 成员名:	张三	
* 成员编号:	0015	
* 所属组织:	开发部	/
绑定账号:	请选择	/
	取消	确认

表 16-30 添加用户

参数	说明
成员名称	建议设置使用人姓名。
成员编号	设置编号数,建议使用员工工号等唯一标识信息。 编号不可和已有人员编号重复。
所属组织	在下拉框中选择组织部门。
绑定账号	在下拉框中选择成员账号。

步骤5 单击"确认"。您可以在组织架构页面查看新增的成员。

----结束

相关操作

后续可以根据情况,在组织管理页面进行以下管理操作。

表 16-31 管理操作

操作	说明
单击编辑	编辑成员信息。
单击删除	删除不再需要管理的成员。

16.2.10.3 系统运维

16.2.10.3.1 查看系统监控

您可以通过设备状态页面,查看系统的资源使用情况,方便排查问题。同时支持进行 重启服务、重启/关闭设备等管理操作。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"系统管理 > 系统运维"。
- **步骤3** 查看设备的运行时间、CPU使用率、内存使用率、网卡吞吐量、磁盘使用情况等信息,详细信息如表16-32所示。

图 16-71 查看设备状态



表 16-32 设备状态

参数	说明
系统概况	展示系统实时的CPU使用率与内存使用率。
CPU使用率	展示最近15分钟系统CPU使用率的变化情况。
内存使用率	展示最近15分钟系统内存使用率的变化情况。
吞吐量	展示最近15分钟系统网卡的吞吐量变化情况。
磁盘使用情况	展示各文件系统与挂载点的使用情况。

步骤4 (可选)在页面的右上角,进行重启服务、重启/关闭设备等操作。

▲ 注意

重启服务、重启/关闭设备的操作影响资产管理业务的运行,建议在业务低谷运行时执 行本操作。

----结束

16.2.10.3.2 系统诊断

实时查看系统内核,CPU、内存、磁盘、网卡等资源情况。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"系统管理 > 系统运维",单击"系统诊断"。
- 步骤3 单击"诊断命令"的下拉框,选择您需要诊断的服务。 诊断项目包括内核版本、CPU&MEM、磁盘、网卡、磁盘IO和PING。
- **步骤4**单击"执行",进行系统诊断。

图 16-72 系统诊断

诊断命令:	内核版本 > 执行
	Linux version 5.10.0-182.0.0.95.r1941_123.hce2.aarch64 (abuild@szxrtosci10000) (gcc_old (GCC) 10.3.1, GNU ld (GNU Binutils) 2.37) #1 SM
	P Fri Jun 28 09:41:47 UTC 2024

----结束

16.2.10.3.3 日志采集

您可以通过一键采集页面,可设置系统默认日志级别及采集后台日志,方便排查问 题。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"系统管理 > 系统运维",单击"系统诊断 > 一键采集"。
- 步骤3 单击"开始采集",执行复现问题的操作。
- **步骤4**单击"完成复现",等待报告生成。
- 步骤5 在"历史记录"中的"操作"选择"下载",将下载的文件提供给相关人员。

	2	3
采集	复现问题	生成报告
点击开始采集技品,系统会 自动采集系统所有错误日志 开始采集 历史记录 (采集最近5次)	语复现问题,系统将自动采 集系约指误,超时自动完成 或者手动立即响成	自动生成报告, 生成完成后 可下载报告
生成时间	文件名	操作
2024-08-27 20:28:23	172.16.46.177_20240827202804.zip	下載 删除

图 16-73 日志采集

----结束

16.2.10.3.4 设置自动清理

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"系统管理>系统运维",单击"系统清理"。
- 步骤3 设置自动清理配置。

图 16-74 设置自动清理

白	动清理	
E	山川庄	

* 清理策略	✓ 日志留存超过	180	天⑦
* 清理时间	00:00:00	ý	
保存	重置		

步骤4 单击"保存"。

----结束

16.2.10.4 查看消息通知

在消息中心,您可以查看系统的通知告警等消息,配置推送的消息类型、消息模板和 接收角色等。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"系统运维 > 消息通知"。
- 步骤3 在全部、通知、告警、待办和其他等页签,查看最近的通知告警等信息。

图 16-75 消息中心

全部已续	3 💿	I
消息类型		
系统告誓		
	消息类型 系统哲智	消息关型 系统告望

----结束

16.2.10.5 系统设置

文档版本 01 (2024-11-28)

16.2.10.5.1 通用设置

您可以在通用设置页面,将系统默认语言进行中英文切换。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"系统管理 > 系统设置"。
- 步骤3 单击"通用设置"页签。
- 步骤4 将默认语言下拉框选择语言(可选中文或English)。

图 16-76 选择默认语言

默认语言:	中文	~
	English	
	中文	

----结束

16.2.10.5.2 时间设置

系统支持手动修改服务器时间,或者通过网络获取系统时间。

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Web控制 台。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"系统管理 > 系统设置"。
- 步骤3 单击"时间设置"页签。
- 步骤4 如需手动修改系统时间,请参考此步骤:

图 16-77 手动修改系统时间

设置时间: 🔘 通过网络获取系统时间 💿 通过手动设置系统时间

*设置日期时间:	2024-08-28 17:18:48	8
保存	恢复默认	

- 1. 单击设置时间日期的下拉栏,在提示框中选择日期和时间,单击确定。
- 单击"保存",弹出"修改系统时间后请重启服务,否则部分功能将无法生效。",单击"确定"完成系统时间修改。

步骤5 如果需要通过网络获取系统时间,请参考此步骤:

图 16-78 通过网络获取系统时间

设置时间:	 通过网络获取系统时间 	◎ 通过手动设置系统时间
* NTP服务器地址:		
保存	恢复默认	

- 1. 在NTP服务器地址输入框填入时间服务器的IP或域名。
- 单击"保存",弹出"修改系统时间后请重启服务,否则部分功能将无法生效。",单击"确定"完成系统时间修改。

```
----结束
```

16.2.10.5.3 告警设置

您可以通过告警设置,配置发送到消息通知告警的触发值、等级和频率。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"系统管理 > 系统设置"。
- 步骤3 单击"告警设置"页签。
- 步骤4 单击要修改告警的"编辑",在对话框修改告警的阈值、等级和频率。
- **步骤5**单击"确认"

----结束

16.3 安全管理员操作指导

16.3.1 系统管理

16.3.1.1 查看角色

系统已经默认创建系统管理员、审计管理员、安全管理员等角色。

文档版本 01 (2024-11-28)

操作步骤

- 步骤1 使用安全管理员secadmin账号登录实例Web控制台。
- **步骤2** 在左侧导航栏,选择"系统管理 > 角色管理"。
- 步骤3 查看内置角色相关信息,详细信息如<mark>图16-79</mark>所示。

图 16-79 查看角色列表

角色列表					C @ I
角色苔癣	6588-84	61225F9	88.09	应用标志	提作
安全管理员	*	2019-06-13 14:21:48	安全管理员	()	
审计管理员	20	2019-06-13 14:21:48	审计管理员		
系统管理员	*	2019-06-13 14:21:48	系统管理员	(C)	

----结束

16.3.1.2 审核账号

创建账号后,需要安全管理员审核通过后,才能正常使用。系统支持"手动审核"和 "自动审核"两种方式。

默认情况下需要安全管理员手动审核账号,您也可以打开自动审核开关,自动通过账 号。

图 16-80 自动审核



|--|

前提条件

已经创建新的用户账号。

操作步骤

- 步骤1 使用安全管理员secadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"系统管理 > 账号审核"。
- 步骤3 找到需要审核的账号,单击"通过"。
- 步骤4 在提示框中,单击"确定"。

-----结束

16.3.1.3 配置安全设置

安全管理员可以通过平台登录安全设置、账号密码安全设置、网络访问安全设置三方面保障系统自身的安全性。

操作步骤

- 步骤1 使用安全管理员secadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"系统管理 > 系统设置"。
- 步骤3 在平台登录安全设置区域,配置登录安全相关参数。

图 16-81 平台登录安全设置

平台登录安全设置	
安全管理方式:	 安全模式 (https) 更新证书
图片验证码:	
空闲超时登出:	30 分钟
多端登录:	 是 否 允许同一账号同时在多个客户端登录。
登录安全策略:	
	在 5 分钟内,用户连续尝试登录描误最多 5 次,对应账号和客户端IP锁定时长为 10
	分钟(解锁后者仍然尝试失败,将再次锁定)。
双因子安全认证:	● 仅密码 图码和USBKey

表 16-33 平台登录安全设置

参数	说明		
安全管理方式	支持使用HTTPS安全模式。		
动态验证码	 选择登录时是否启用动态验证码。 启用后,系统登录时,输入正确的动态验证码是必要条件之一,可以防暴力破解密码。 		
空闲超时登出	设置账号超时自动退出时间。		
多端登录	设置是否支持多端登录功能。 • 是:同账号支持在多个地方同时登录。 • 否:一个账号登录后,不能在其他地方登录。		
登录安全策略	 选择是否启用登录安全策略,防止账号被暴力破解。 例如,用户账号如果在3分钟内,登录信息连续输入错误3次,则此账号在5分钟内将被锁定,无法登录到系统。 		

参数	说明
双因子安全认	设置登录认证方式。
证	 仅密码:登录时只使用密码认证。
	 密码和USBKey:登录时需要密码且用户需将存储有证书的 USBKey插上设备,以实现身份认证。

步骤4 在账号密码安全设置区域,设置初次登录强制更改密码,并设置密码内容要求及有效 期。

图 16-82 账号密码安全设置

账号索码安全设置					
初次登录强制更改密码:		0			
• 密码长度要求:	至少	7	位		
密码复杂度要求:	包含	🖸 数字 🗹	小写字母	大写字母	特殊字符
• 密码有效期:	30	天			

步骤5 在网络访问安全设置区域,设置网络访问限制。

图 16-83 网络访问安全设置

网络访问安全设置		
登录IP限制:	 接受所有IP 限制IP 	
网络权限配置:	□ 禁止ICMP探测 □ 禁止SSH登录	
HOST代理白名单:	可配置20个,以施行符号属并	接受多个IP地址或域名以换行分隔 格式示例: 192.168.0.1 2001.cdba=1
	目动添加	& www.xxx.com

表 16-34 网络访问安全设置

参数	说明	
登录IP限制	设置是否限制访问来源:	
	 接受所有IP:不限制访问来源。 限制IP:仅支持允许登录IP地址名单中的IP访问数据库加密 与访问控制的Web控制台。 	
参数	说明	
-----------	--	
允许登录IP地址	填写允许登录的IP地址,多个地址用换行隔开。	
网络权限配置	设置是否禁止ICMP探测和SSH登录。	
	● 启用禁止ICMP探测:关闭ICMP功能,则其他设备无法ping 系统。	
	● 启用禁止SSH登录:禁止SSH访问系统。	
	说明 禁止SSH登录后,运维人员将不能通过SSH访问服务器后台。	
HOST代理白名单	填写HOST代理白名单,支持IP地址或域名。	

步骤6 单击"确定"生效。

----结束

16.4 审计管理员操作指导

16.4.1 查看系统操作日志

系统会保存所有的操作记录,审计管理员可以定期检查系统日志,保障系统自身安全 和确保符合合规要求。

操作步骤

- 步骤1 使用审计管理员audadmin账号登录实例Web控制台。
- 步骤2 在左侧导航栏,选择"日志管理 > 操作日志"。
- 步骤3 (可选)设置过滤条件,单击搜索,查询对应操作审计日志。

图 16-84 设置过滤条件

日志管理 设备日志 現作日志	^	2024-08-20 17/06/14 ~ 2024-08-27 17/06/14 問語的相信, 中, 内容等的第一 年,							
		操作时间	操作账号	握作iP	操作内容	操作结果	使用人	操作	
		2024-08-27 17:05:29	audadmin	No. 10. 10. 10.	型录	成功	audadmin	详细	
		2024-08-27 17:05:00	sysadmin	1.000	查询信任人员	成功	sysadmin	511:00	

步骤4 在列表查看系统日志信息。

----结束

16.4.2 查看系统设备日志

系统会保存所有的设备消息记录,审计管理员可以定期检查设备日志,保障系统自身安全和确保符合合规要求。

操作步骤

步骤1 使用审计管理员audadmin账号登录实例Web控制台

文档版本 01 (2024-11-28)

步骤2 在左侧导航栏,选择"日志管理 > 设备日志"。

步骤3 (可选)设置过滤条件,单击搜索,查询对应设备日志。

图 16-85 设置过滤条件

日志管理	^	级别	日志归类	20	24-08-20 17:14	:25 - 2024-08-27 17:14:25 📋	操作账号	✓ 谢输入	Q			C 🕲 I
设备日志		日志归类	日志说明	级别		时间	日志信息		模块名称	操作账号	1	最作IP
编作日志		登录日志	用户登录成功	通知		2024-08-27 17:05:29	用户登录成功 (UserType	=HTTPS	用户认证	audadmin	1	72.16.197.57
		登录日志	用户登录成功	通知		2024-08-27 16:40:48	用户登录成功 (UserType	=HTTPS	用户认证	secadmin	1	72.16.197.57

步骤4 在列表查看设备日志信息。

----结束

17 数据库安全运维管理

17.1 数据库运维实例管理

通过管理控制台可登录实例侧,同时可对实例进行重启、关闭、解绑EIP等操作。

- 步骤1 登录管理控制台。
- **步骤2** 在页面上方选择"区域"后,单击页面左上方的 ── ,选择"安全与合规 > 数据库安 全服务 DBSS",进入数据库安全审计"总览"界面。
- 步骤3 在左侧导航栏选择"数据库安全运维",查看数据库安全运维实例。

图 17-1 数据库安全运维实例

数据库安全运维					0 R\$270 < 8	新动态 口使用指弯 的复数能增长全能的
Q. 送採履性等选, 成施入3	《经子指束					00
北州名称 0	秋念 Θ	\$3M类型 0	虚积₽地址 Θ	WEEP 0	计数模式 Θ	指作
DOM_ 76545	0 遗行中	#U.			包年/包月 19天后到期	
DBSS fb3o4c	0 适行中	主新			包年/包月 30天成到期	這種動象 採購 更多 ~
DBSS a701fc	0 遗行中	主筆			包年/包月 約天開到明	這個聖景 秋春 更多 ~
DBSS ITZa58	o 遗行中	MH 57.			包年/他月 30天成别期	二日日日 二日日 二日日 二日日 二日日 二日日 二日日 二日日 二日日 二日

----结束

远程登录

步骤1 在目标实例"操作"列单击"远程登录"。

图 17-2 远程登录数据库安全运维实例

Construint Constru	18n
2024 0 요구우 해외 탄자(1) 2025	
805 O 进行中 主張 哲师/包月 304	近極動発 探察 更多 ~
	3999 ## ## ## *
855 0 道行中 王章 包式包开 7916 王章 赵石相知道	

步骤2 跳转至登录页面,输入实例的账号密码,单击"登录"进入数据库运维控制台。

----结束

重启实例

步骤1 在目标实例"操作"列选择"更多 > 重启"。

图 17-3 重启数据库安全运维实例

) ISANGTAS, 1000-1	关键字搜索					Q
RNRD 0	₩8 0	金利美型 0	diministe O	SWEEIP 🖯	计要模式 ⊖	操作
DOM_ 78545	0 遗行中	単れ			包半/包月 19天常利用	送程登录 映表 更多 ∧ 开启
DBSS B3c4c	• 遗行中	1.9			包平/包月 30天成長期	近程 共活
DESS a701k	0 進行中	主教			包甲/包月 30天描列明	律改安全组 透程 編成 印户
D688 12a58	• 道行中	A847,			包平/包月 30天成到期	重量运行 近程: 开通口动块奏

步骤2 在弹窗中确认重启,单击"确认",实例开始自动执行重启。

----结束

关闭实例

步骤1 在目标实例"操作"列选择"更多 > 关闭"。

图 17-4 关闭数据库安全运维实例

库安全运维						最新动态 口使用加高 购买数据车支全部
Q 选择履性转进,或输入3	关键字输放					0
WHERE 0	kt⊄ ⊖	XHX2 O	BRIPELL O	WEIP O	计截模式 Θ	操作
DOM_ 78545	0 遗行中	ma/			包年/包月 19天后到昭	远程登录 续载 更多 ^ 开启
DBSS fb3c4	 ● 還行中 	1.9			银年/银月 30天后到期	2日 英田
DB55 a7015	 ● 重行中 	主莽			包平/也月 30天雷到期	特許安全地 2019年 和GHI EIP
D855 12458	○ 還行中	##[包举/包月 30天偏到明	重重空码 2012 开通祭坊续勝 3017
B27: 4						1102 (1) 2000

步骤2 在弹窗中确认关闭,单击"确认",实例开始自动执行关闭。

----结束

修改安全组

步骤1 在目标实例"操作"列选择"更多 > 修改安全组"。

图 17-5 数据库安全运维实例修改安全组

數振	祚安全运维					⊕ 第88991 < 88505	
	〇、送外屋住外送、成船入大楼子披来						
	RMRR 0	80 0	文列 类型 0	透照P地址 Θ	301EIP ⊖	计曲模式 ⊖	操作
	DOM 7554	0 透行中	#6			包年/包月 19天后到朝	近程建築 续奏 更多 へ 开启
	0885 10304	o 遗行中	主報			包年/包月 30天武劉朝	10日 11日 天活
	0055 a7011	○ 运行中	主教			包带/包月 30天晨到朝	 (市政安全组) (ご理) 解説 EIP
	D855 #2x51	o 遗行中	44-5L			包年/也月 30天后到朝	重重定明 远程 开道自动续奏 退订
	9320:4						HIR (1)>

步骤2 在弹窗中选择安全组,单击"确认",实例所属安全组修改完成。

🛄 说明

只能选择已有的安全组。

----结束

解绑 EIP

步骤1 在目标实例"操作"列选择"更多 > 解绑EIP"。

图 17-6 数据库安全运维实例解绑 EIP

数据库安全运维						最新动态 🗅 使用信用 野环境总统安全服务
0. ISANGUNIS. INALA	建字段素					Q 0
THRE O	₩Ø ⊕	SHRE 0	distribute 0	3#EEP ⊖	计要数式 🖯	操作
DOM_ 71:545	 适行中 	単の			包甲/包月 19天扁到期	这样登录 续费 更多 ~ 开启
DBSS fb3ck	◎ 還行中	主筆			包年/包月 30天后到期	重度 法理 关闭
D688 a7019	o 适行中	主新			包平/包月 30天雷到期	参数安全組 通歴 解初 EP
D855 #2x58	 違行中 	##1].			包年/包月 20天昭到期	重重定码 远程 开道自动披露 退灯
后张政: 4						==== < (1) >

步骤2 在弹窗中确认解绑,单击"确认",实例将解绑EIP。

----结束

重置密码

步骤1 在目标实例"操作"列选择"更多 > 重置密码"。

图 17-7 数据库安全运维实例重置密码

据库安全运维					@ RER ifo <	Restance Contraction Restation of the Re
C SABLANS. WARAS	·#7:88					00
SHAR 0	465 O	THE O	EROPHSLE O	3₩1±IP ↔	计要模式 🖯	授作
DOM. 76545	0 道行中	激动;			包平/包月 19天然到期	辺程設定 は男 更多 ^ 开注
D855 10304	0 适行中	主發			包亭/包月 30天雪到期	27년 里泉 矢灯
D855 a7015	O 进行中	主節			包带/包月 30天祭到期	作次安全组 2019 解解 EIP
D855 17a51	0 遗行中	单约			包年/包月 於天照到期	重要运转 运程 开通各切种器 透订
598: 4						100 () → 200

步骤2 在弹窗中输入需要修改的密码,单击"确定",修改密码完成。

----结束

退订

步骤1 在目标实例"操作"列选择"更多 > 退订"。

图 17-8 退订数据库安全运维实例

数据库安全运维					Q 2002170 -	·最新结志 1 使用描词 新开政府专业全部并
O. ISABELNE. AND.A.	建学校家					
201217 0	₩8 0	SMRE 0	distribute 0	24(Etb 0	计表模式 ↔	操作
DOM. 7854	0 适行中	单约	10.0.109.21	100.93.2.211	包年/包月 19天開到期	辺接登景 体裁 更多 へ 开启
D855 15364	0 遗行中	主命	192.168.0.155	100.05.217.205	60年/60月 30天临利限	王忠 天司
DBS5 a7011	0 遗行中	主句	10.0.67.0	100.95.158.255	包年/包月 30天后到明	停改安全場 1992 和田 EIP
D885 #2a51	○ 道行中	離初	10.0.236.196	100.95.157.196	包年/包月 30天动王闻	重重实码 滤程 开通如块期 流行
952:4						HIX BDR

步骤2 在弹窗中确认退订信息,单击"是",完成退订。

----结束

删除

步骤1 在目标实例"操作"列选择"更多 > 删除"。

图 17-9 删除数据库安全运维实例

数据库安全运维					田田市(100) 田市(100) 田市(100) 田市(100)	最新动态 1 使用描词 购买数据库安全服务
	(#Filter					Q ()
XBISR O	¥02 0	ANTE O	此和P地址 0	3₩tBiP Θ	计数模式 Θ	操作
DOM 71645	0 遗行中	单约			包年/包月 19天開到期	近程数录 续载 要多 ∧ 开启
D855 103c4	0 遗行中	主動			包年/包月 30天祭到朝	10日 10日 11日
0855 a7011	0 遗行中	主筆			包年/包月 20天照到明	作改安全级 运输2 编数 EIP
0895 #2x51	o 遗行中	#15			银年/松月 20天后到明	重重运动 运程 开通色动体器 透灯
想张政: 4						Hitt 2014

步骤2 在弹窗中确认删除信息,单击"确定",完成删除。

----结束

17.2 系统管理员操作指南

17.2.1 首页信息

在首页以可视化面板的形式展示系统的统计信息。

首页页面显示的可视化面板信息,包括数据资产概览信息、网络流量、业务监控和系 统资源使用情况等信息。

操作步骤

步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。

步骤2 默认进入首页页面,在首页中查看信息。

图 17-10 首页信息看板



表17-1 首页信息看板

区域	说明
数据资产统计	统计关系型数据库资产数量、大数据资产数量和资产总 数。
网络流量	统计近3分钟所有网卡的网络流量信息。
业务监控	统计各风险级别的业务访问数量。
CPU	统计近3分钟的实时CPU使用率。
内存	统计近3分钟的实时内存使用率。
磁盘	统计近3分钟的实时磁盘使用率。

----结束

17.2.2 资产管理

17.2.2.1 添加数据资产

本章节将介绍如何在系统上添加需要保护的数据资产(数据库、大数据等),操作过程中将以添加Oracle数据库为例,请根据实际情况添加相应的数据资产。

使用约束

表 17-2 数据库运维支持纳管的数据源及版本

兼容性软件 名称	兼容版本情况	功能差异化描述				
数据库	版本	协议解 析单向	协议解 析双向	风险扫 描	密码代 填	web认 证
Oracle	11.1.0.60	√	√	√	√	√
	11.2.0.1	√	√	√	√	√
	12.2.0.1	√	×	√	√	√
	19c	√	×	√	√	√
	12.1.0.2	√	√	√	√	√
	11.2.0.4	√	√	√	√	√
MySQL	5.5 (测试版本:5.5.64- MariaDB)	\checkmark	√	×	√	√
	5.6	√	√	×	\checkmark	√
	5.7.29	√	√	×	\checkmark	√
	5.7.36	√	√	×	√	√
	5.7.32	√	√	×	√	√
	8.0.21	√	√	×	√	√
	8.0.22	√	√	×	\checkmark	√
	8.0.27	√	√	×	√	√
	8.0.28	√	√	×	√	√
SQL Server	2008	√	√	√	×	√
	2014	√	√	√	×	√
	2019	√	√	√	×	√
DB2	8	√	×	√	√	√
	10	√	×	√	√	√
DM7	7.1.2	\checkmark	×			√
DM8	8.1.2.84	√	×	×	√	√
PostgreSQ	10	√	√	×	×	√
L	12.2	√	√	×	√	×

兼容性软件 名称	兼容版本情况	功能差昇	幹化描述			
	9.6.6	\checkmark	×	×	×	√
	12.4	\checkmark	√	×	\checkmark	√
	12.3	\checkmark	√	×	\checkmark	√
Hive	1.1	\checkmark	×	×	×	×
	2.1.1	\checkmark	√	×	×	×
Kingbase	7.1.2.0480	\checkmark	×	×	×	×
GaussDB	100	\checkmark	×	×	×	×
	200	\checkmark	×	×	×	×
TDSQL	10.3.14.6.0_D014	\checkmark	√	×	×	×
TBase (TBase (PG)	V2.15.17.3.6	V	\checkmark	×	×	×
GreemPlu m	4.3.8.1	√	×	×	√	√

前提条件

已获取资产IP地址、端口号、资产类型、数据库账号、数据库密码、数据库名/实例名 等信息。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,选择"资产管理 > 资产配置",进入资产配置页面后,单击"添加"。
- 步骤3 在添加资产对话框中,设置资产信息。

图 17-11 添加资产

添加资产

添加页厂							^
* 资产名称:	oracle_zz	*资产类型:	Oracle \lor				
* 资产IP:	17 0	* 资产端口:	1521				
* 数据库/实例名:	orcl	* 数据库账号:	system	* 数据库密码:	•••••		
web认证:		误删恢复配置:					
部署模式:	反向代理	* 端口 ②:	9001				
RAC:							
					测试连接	保存	取消

表 17-3 添加资产参数说明

参数	说明
资产名称	自定义数据资产名称。
资产类型	选择数据资产类型。 支持Oracle、SQL Server、DB2、MySQL、DM7、Kingbase、 PostgreSQL、Hive、GaussDB 200、TBase、TDSQL、 GreenPlum、DM8。
资产IP	填写数据资产的IP地址。
资产端口	填写数据资产对应的端口号。 默认Oracle数据库端口为"1521"。
数据库/实例名	填写数据库名称或者实例名称。
数据库账号	填写数据库登录用户名。
数据库密码	填写数据库登录密码。
web认证	开启Web认证后,仅通过认证的数据库操作员可以通过Web安 全客户端或已认证的数据库客户端访问数据库。 后续操作,请参见 <mark>通过Web安全客户端访问资产</mark> 。
误删恢复配置	设置是否开启误删恢复配置。开启后,系统将支持对数据库误删 操作进行恢复。 误删恢复详细操作请参见 <mark>误删恢复</mark> 。
部署模式	显示部署模式,支持反向代理模式。
端口	设置代理端口,取值范围:9000~10000。
RAC	Oracle数据库是否启用RAC部署方式。 默认未启用RAC,如果启用了RAC,将还需要设置Oracle的 SCAN IP或VIP信息,并设置本机代理IP地址。

步骤4 单击"保存",保存数据资产的配置信息。

添加完成后,您可以在资产列表中查看新添加的数据资产信息。

----结束

相关操作

后续您可以根据情况,进行以下数据资产管理操作:

- 保护数据资产:找到目标资产,打开保护状态开关。
- 编辑数据资产:单击"编辑",修改数据资产信息。
- 删除数据资产:单击"删除",删除数据资产。

门 说明

删除前需要先关闭资产的保护状态。

17.2.2.2 手动添加账号

资产账号信息用于对数据库操作员的Web认证授权,以实现对人员访问的控制。

手动添加资产账号信息,用于对数据库操作员的Web认证授权,以实现对人员访问的 控制。添加的账号信息也可用于对已授权人员的密码代填,实现数据库操作员免密访 问和维护数据库,避免数据库账号密码的泄露。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,选择"资产管理 > 账号管理",进入账号管理页面后,单击"添加账 号"。
- 步骤3 在添加账号对话框中,设置资产账号信息。

图 17-12 添加账号

添加账号	×	
*选择资产:	oracle_zz v 目前去括例产类型Oracle_SOLServer_DR2_MvSOL_DM7	
	GreenPlum, TIDB, OceanBase, DM8	
* 数据库账号:	test	
* 数据库密码:		
数据库/实例名/SID:	orcl	
服务名/Tenant:		
管理员账号:		
	注: 只有蚁烟库账号没有修改密始仪账时才可以集谈选项	
管埋员密码:	注:只有数据库账号没有修改密码权限时才可以填该选项	
	测试连接 保存 取 消	

表17-4 添加账号参数说明

参数	说明
选择资产	在下拉栏中选择数据资产。
数据库账号	数据库登录用户。
数据库密码	数据库登录密码。
数据库/实例 名/SID	数据库名称、实例名称或者SID。

参数	说明
服务名/Tenant	● 对于Oracle资产, "数据库/实例名/SID " 或 "服务名/ Tenant " 两个参数中二选一,填写一个 。
	● 对于Informix和Oceabase资产, "数据库/实例名/SID" 或 "服务名/Tenant"两个参数都需要填写。
	● 其他资产无需配置"服务名/Tenant"。
管理员账号	针对改密功能,数据库账号没有修改密码权限时才可以填该选 项。
管理员密码	针对改密功能,数据库账号没有修改密码权限时才可以填该选 项。

步骤4 配置完成后,单击"测试连接",检查配置是否正确和数据库是否能够连接。

步骤5 测试通过后,单击"保存",保存数据资产的账号信息。

----结束

相关操作

后续您可以根据情况,在账号管理页面进行以下操作:

- 编辑账号:单击"编辑",编辑账号信息。
- 删除账号:单击"删除",删除账号。
- 单条账号改密:单击"改密配置",根据需求设置改密规则。
- 批量账号改密:选中账号,单击"批量改密",根据需求设置改密规则。

🛄 说明

进行改密设置前,请确认数据库账号拥有改密权限,或已添加管理员账号。

- 批量关闭周期改密:单击关闭自动改密,选中目标资产,批量关闭已设置的周期 改密功能。
- 添加账号信息后,您可以将数据库操作员和数据库账号进行关联,以实现Web认 证授权和密码代填。具体操作,请参见管理运维人员。

17.2.2.3 误删恢复

系统支持对数据库的DROP与TRUNCATE操作影响的数据进行恢复,以应对误删情况的 发生。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"资产管理>误删恢复"。
- 步骤3 在当前已选择资产栏选择目标资产,并设置操作类型或状态查询相应误删操作。
- **步骤4** 找到目标误删记录,可进行如下操作:
 - 查看误删详情:单击"详情",查看误删操作详情记录。

- 恢复误删数据:单击"恢复",将数据恢复到资产原位,恢复状态变为已恢复。
- 删除误删记录:单击"删除",删除误删记录,不再保留数据。

步骤5 根据自身需求设置数据保留时长。

----结束

17.2.3 策略防护

17.2.3.1 概述

策略防护功能包括策略设置、自定义策略、虚拟补丁策略模块。

系统支持配置多种维度策略,策略组合种类多达数百种,能够精准实现各种数据级的 访问控制。

- 主体颗粒度可细化至用户、IP、主机、程序、时间、频次等。
- 客体颗粒度可达针对表、列、行数等。
- 行为颗粒度可达基本操作、特权操作、SQL语句、异常、存储过程等。

17.2.3.2 策略设置

17.2.3.2.1 管理基本配置

本章节介绍如何对数据库防护策略进行基本的配置,并应用生效。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,选择"策略防护 > 策略设置",并在策略设置页面,单击"基本配置"页签。
- 步骤3 在当前已选择资产中,选择目标资产。
- **步骤4**勾选需要应用的策略,单击
- 步骤5 配置具体策略选项。

图 17-13 启用策略

当前已选择资产: my	ysql v	策略应用
应用的策略 (对策略内	容的更改不会立刻生效,需手动点击"策略应用")	
☑ 访问控制		
☑ SQL策略	8 🖸 🗹 启用虚拟补丁 🖸	
✔ 全部记录		
未命中策略时默认;	动作: 通过 🗸	

在策略默认动作中选择通过或者阻断。

通过(默认):如果访问操作命中开启的策略,默认通过;如果策略定义里的响应动作为阻断,则阻断。

 阻断:如果访问操作命中开启的策略,则直接阻断;如果策略类型为白名单,则 通过。白名单设置方法请参见自定义策略。

步骤6 单击右上角的"策略应用",使配置生效。

----结束

17.2.3.2.2 管理集合配置

配置集合信息(例如客户端IP、数据库用户等)后,在设置策略时可选择对应集合。 实现信息统一维护,避免多处维护。

背景信息

系统支持配置的集合类型如下图17-14所示,此处以配置资产客户端IP集为例。

图 17-14 集合信息

tt 资产客户端IP集	⊞ 资产客户端集	🖂 操作系统用户集	∃ 操作系统主机集
 · · 数据库用户集 	せ 表组集	● 字段集	● 数据库Schema集
⊕ 適組	· · · · · · · · · · · · · · · · · · ·	⊞ 应用客户端IP集	⊕ 应用用户集
⊕ 应用用户组集	⊞ 时间组集		

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,选择"策略防护 > 策略设置",并在策略设置页面,单击"集合配置"页签。
- 步骤3 将鼠标移动到资产客户端IP集,单击右侧显示的十。
- 步骤4 设置开始IP和结束IP,单击"确定"。

图 17-15 添加资产客户端 IP 集

向[资产客户端IP集]添加[资产客户端IP]	×
* 开始IP: 192. 10	
* 结束IP: 192	
取消	定

步骤5 配置完成后,您可以在配置策略时选择对应的集合。例如,在"策略防护>策略定义"页面配置自定义策略时,可选择资产客户端IP集,如<mark>图17-16</mark>所示。

图 17-16 选择资产客户端 IP 集

策略详情				
命中策略后记录	総結果集: 🔵			
基本信息				
策略名称: test			* 风险等级:	低风险
记录日志:				
资产信息(源)				
资产客户端IP:	包含任意	\sim	请输入	
操作系统用户:	包含任意	~	19210~192 .99	

----结束

17.2.3.3 自定义策略

17.2.3.3.1 添加 SQL 策略

系统已经内置策略组和策略,您可以根据需求添加自定义的SQL策略。

背景信息

自定义策略包含功能如下:

- 支持对缺省数据库策略组进行编辑和删除操作。
- 支持对自定义策略组进行添加、编辑和删除操作。
- 支持对策略组的规则进行添加、删除、编辑、上移、下移操作。
- 可根据自身业务场景对资产信息、目标信息、访问信息进行策略配置。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,选择"策略防护 > 策略定义",并在策略定义页面,单击"SQL策略"页签。
- 步骤3 (可选)如需新增策略组,请按照如下步骤操作。
 - 1. 在策略组列表区域,单击"添加策略组"。
 - 2. 设置策略组基本信息,并单击"确定"。

图 17-17 添加策略组

添加策略组			×
* 名称:	demo		
* 基于:	缺省MySQL策略	\sim	
		取消	确定

表 17-5 添加策略

参数	说明	
名称	自定义策略组名称。	
基于	可选 新建 或 基于 : - 新建:创建一个空白策略组。 - 基于:选择其他策略组(例如缺省MySQL策略)作 为模板,在其基础上进行编辑。	

3. 创建完成后,单击策略组名称,修改策略信息,单击右上角的"保存"。

图 17-18 策略信息

策略信息	
名称:	demo
修改时间:	2021-11-10 16:06:53
数据库用户:	○ 区分大小写 (●) 不区分大小写
操作系统用户:	🔵 区分大小写 💿 不区分大小写
资产客户端:	○ 区分大小写 ● 不区分大小写

步骤4 在策略组中添加新策略。

1. 鼠标移动到目标策略组,单击+添加目标。

图 17-19 添加策略按钮

▲ SQL注入策略		11
▲ demo	+ 🗊 🖸	6

2. 设置策略名称和类型,单击"确定"。

图 17-20 添加策略

添加策略			×
* 名称:	test		
* 类型:	黑名单	\vee	
		取	确定

表 17-6 添加策略

参数	说明
名称	自定义策略名称。
类型	- 可选择默认、优先级、白名单和黑名单四种类型:
	■ 黑名单 :访问阻断。
	■ 白名单 :访问通过。
	 优先级:策略匹配先于默认类型,默认访问通过,可自行修改。
	 默认:默认访问通过,可自行修改。 策略类型的优先级顺序为:黑名单 > 白名单 > 优先级 > 默认。同一个类型则按顺序执行,有阻断则阻断。

3. 单击策略组前面的 展开图标,查看策略。

图 17-21 展开策略组

▼ demo		21
test	🖂 🗊 Et El	黑
影响行数测试		优
高危操作-ALTER		默认
高危操作-DROP		默认
高危操作-TRUNCATE		默认
权限变更		默认

单击策略名称,在策略详情页面修改策略信息。
 如果设置策略详情时要使用集合组,请先进行集合配置,详情参见管理集合配置。

图 17-22 修改策略详情

基本信息								
策略名称:高危操作-/	ALTER	* 风险等级	: 高风险 v	* 响应动作:	阻断			~
记录日志:			锁定访问: 🔵					,
资产信息(源)								
资产客户端IP:	包含任意 🗸	/ 请输入		主机名:	包含任意		请输入	
操作系统用户:	包含任意	/ 请输入		数据库用户:	包含任意	~	root ×	
数据库用户组:	包含任意 🗸	/ 请选择		资产客户端:	包含任意		请输入	
资产客户端MAC	请输入			应用客户端II	P: 包含任意		请输入	
应用用户组:	包含任意 🗸	/ 请输入		时间组:	包含任意		请输入	
应用用户:	包含任意 🗸	/ 请输入						
目标信息								
目标表:	包含任意 🗸	/ 请输入		数据库:	包含任意		请输入	
影响行数:	等于 ~	/ 请输入		字段:	包含所有		请输入	
表组:	包含所有	/ 请选择						

表 17-7 策略详情

参数		说明
基本信息	风险等级	命中策略告警的级别。
	响应动作	命中策略动作设置阻断或通过。
	记录日志	命中策略是否记录日志。
	锁定访问	响应动作为阻断时,可选择是否根据IP 或用户锁定访问。
资产信息(源)	资产客户端IP	数据库客户端的IP。
	主机名	数据库客户端的主机名。
	操作系统用户	数据库客户端的操作系统用户名。
	数据库用户	数据库客户端的访问数据库资产使用 的用户名。
	数据库用户组	数据库客户端的访问数据库资产使用 的用户组。
	资产客户端	数据库客户端工具。
	资产客户端MAC	数据库客户端工具所在PC的MAC。
	应用客户端IP	三层防护,应用端的IP。
	应用用户组	三层防护,应用端的用户组。
	时间组	时间段组。

参数		说明	
	应用用户	三层防护,应用用户。	
目标信息	目标表	访问资产的表。	
	数据库	数据库信息。例如,MySQL数据库中 的test模式,可以表示为mySQL.test。	
	影响行数	访问资产影响行数。	
	关联表个数	查询表个数。	
	字段	查询资产表的字段。	
	表组	查询的表组。	
访问信息	访问次数	数据库客户端访问资产的次数。	
	执行时长	执行语句的时长。	
	请求状态	客户端请求的状态。	
	存储过程	访问的存储过程。	
	操作命令	客户端执行的命令类型。	
	特权操作	客户端特权操作。	
	查询组	查询语句组。	
	SQL字符串	客户端执行的SQL字符串。	
	操作语句	客户端执行的操作语句。	
	SQL十六进制序列	客户端执行的SQL十六进制序列。	
	执行结果关键字	结果集关键字。	
	时间选择	策略执行的时间控制。	

在策略详情中可以从多个维度设置策略信息,包括策略基本信息、资产信息、目标信息、访问信息和时间等。

例如,您可以如上图设置,表示禁止root用户访问数据资产。

- 5. 单击右上角的"保存",保存策略信息。
- **步骤5** (可选)如果需要调整策略的优先级,将鼠标放到策略上,单击➡或者➡进行上移或者 下移。

图 17-23 调整策略优先级顺序

▼ demo	22
test	黑 日 🗊 🗹
test02	罴
影响行数测试	优
高危操作-ALTER	默认
高危操作-DROP	默认

🛄 说明

策略优先级顺序为: "黑名单 > 白名单 > 优先级 > 默认",同一类型的越上面,优先级越高。 仅支持同一种类型之间进行上、下移动。

步骤6 使配置生效。

- 1. 在左侧导航栏,选择"策略防护>策略设置"。
- 2. 勾选"启用SQL策略"。
- 3. 单击 🗹 编辑图标,勾选目标策略组,单击"确定"。
- 4. 单击"策略应用"。

更多信息,请参见管理基本配置。

----结束

相关操作

除了新增操作外,系统还支持对策略组和策略进行以下管理操作:

- 策略组:
 - 编辑策略组:鼠标移动到策略组,单击^[2],修改策略组名称。
 - 删除策略组:鼠标移动到策略组,单击 💷,删除策略组。
 - 复制策略组:鼠标移动到策略组,单击,复制整个策略组。
- 策略:
 - 编辑策略信息:单击策略名称,修改策略信息。
 - 编辑策略:鼠标移动到策略,单击🗹,修改策略名称。
 - 复制策略:鼠标移动到策略,单击口,复制整个策略。
 - 删除策略:鼠标移动到策略,单击,则,删除策略。

17.2.3.3.2 添加包过滤策略

根据网络数据包的五元组(源IP、源端口、目的IP、目的端口、协议)与配置规则进行 匹配,根据匹配规则的操作,进行数据包的放行或阻断。

约束与限制

包过滤策略只支持桥接代理模式,其他模式下请勿进行相关配置。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,选择"策略防护>策略定义",并在策略定义页面,单击"包过滤策略"页签。
- **步骤3** 单击策略名称,在策略汇总区域,配置五元组信息和匹配规则操作,单击右上角的 "保存"。

图 17-24 配置策略

策略汇总						保存	清空
协议:	ТСР	V	响应动作:		◉ 放行	〇 阻断	
源ip:	192 100			源端口 ②:	请输入		
目的ip:	192200			目的端口 ②:	22 ×		

表 17-8 配置策略

参数	说明	
协议	可选择TCP、UDP、ICMP协议。	
响应动作	包括放行和阻断。	
源IP	数据包发送端IP。	
源端口	数据包发送端端口(ICMP协议下,此端口可不填)。	
目的IP	数据包接收端IP。	
目的端口	数据包接收端端口(ICMP协议下,此端口不填)。	
注意:如果选择TCP协议,则源IP、源端口、目的IP和目的端口必填一项,再单击保 存。如果不填写直接保存的话,会造成无法访问Web页面、无法连接SSH等问题。		

步骤4 在策略列表框上设置策略默认动作为放行或阻断。

- 放行:如果访问命中开启的策略,默认通过;如果策略定义里的响应动作为阻断,则阻断。
- 阻断:如果访问命中开启的策略,则直接阻断。

----结束

相关操作

除了新增操作外,系统还支持对策略进行以下管理操作:

文档版本 01 (2024-11-28)

- 编辑策略:鼠标移动到策略,单击²,修改策略名称。
- 删除策略:鼠标移动到策略,单击9,删除策略。

17.2.3.3.3 启用或禁用策略

策略在创建时默认为启用状态,您可以根据实际情况启用或者禁用。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"策略防护>策略定义"。
- 步骤3 切换到目标策略,例如,单击"SQL策略"页签。
- 步骤4 如果需要切换单个策略,请参考此步骤。
 - **图 17-25** 切换策略状态



- 1. 单击目标策略组前面的 图标,展开策略。
- 2. 找到目标策略,单击策略前面的状态图标,启用或禁用策略。
 - 上图中,①部分策略为禁用状态,单击后可以启用策略。
 - 上图中,②部分策略为启用状态,单击后可以禁用策略。

步骤5 如果需要批量切换同策略组的多个策略,请参考此步骤。

- 1. 鼠标移动到目标策略组,单击 2 图标。
- 2. 在编辑策略组对话框中,勾选需要启用的策略,未勾选的表示需要禁用的策略。

图 17-26 批量启用或禁用策略

编辑策略组		×
* 名称: 缺省Oracle策略		
全选 全不选 高危操作-ALTER	高危操作-DROP	
 ✓ 高危操作-TRUNCATE ✓ 批量数据复改 ✓ 批量数据泄露 	 ✓ 权限变更 ✓ 批量数据删除 ✓ 数据库用户密码泄露 	
 ✓ 无Where更新或者删除 ✓ SQL中包含注入常用的时间函数 ✓ 账户暴力破解 	 ✓ SQL中包含对外通讯 ✓ 工具导出操作 ✓ 撞库 	

3. 单击"确定"。

----结束

17.2.3.3.4 添加客户端语句过滤白名单

在客户端操作SQL语句时,会固定产生一些不需要记录的语句。这些语句可能会干扰 您识别正常的SQL操作语句。通过添加客户端语句过滤白名单,审计日志将不记录这 些客户端语句,避免因匹配到特定策略后产生误报。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,选择"策略防护>策略定义"。
- 步骤3 单击"客户端语句过滤白名单"页签,并单击"添加"。
- 步骤4 在添加客户端语句过滤白名单对话框中,添加数据。

图 17-27 添加白名单

添加客户端语句过》	虑白名单	×
* SQL:	SELECT * FROM dual\n	
* 工具:	PLSQL Developer	1
数据库:	Oracle	*
状态:	启用	~
	取消	确定

表 17-9 添加白名单

参数	说明
SQL	需要添加白名单的SQL语句。
工具	数据库客户端。
数据库	数据库类型。
状态	在下拉栏中选择启用或禁用,默认启用。

步骤5单击"确定"。

步骤6 使配置生效,您需要进行以下步骤:

- 1. 在左侧导航栏,选择"策略防护 > 策略设置"。
- 2. 在基本配置页的应用的策略栏勾选启用SQL策略。
- 3. 单击启用SQL策略旁的^[2]。
- 4. 在策略列表页面勾选客户端语句过滤白名单,单击"确定"。
- 5. 在基本配置页单击策略应用,配置生效。

更多信息,请参见管理基本配置。

配置完成后,数据库客户端访问资产时,如果规则命中SQL语句,那么在"审计日志 > SQL日志"页面的审计日志列表里不记录此日志。

----结束

相关操作

后续您可以根据情况,进行以下白名单管理操作:

- 编辑白名单:单击编辑,修改白名单信息。修改后请参考管理基本配置,使配置 生效。
- 删除白名单:单击删除,删除不再需要使用的白名单。
- 启用白名单:找到目标白名单,打开状态开关。

17.2.3.4 设置虚拟补丁

此模块包括虚拟补丁和虚拟补丁例外两部分,设置并开启**虚拟补丁规则**后,会依据内 置数据库漏洞特征库信息,对命中策略的攻击进行虚拟补丁拦截防护。**虚拟补丁规则** 例外能防止正常业务运行下误报情况的发生。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,选择"策略防护 > 虚拟补丁",进入虚拟补丁页面后,单击"虚拟补 丁规则"页签。
- 步骤3 单击右上角的"添加"按钮,新增虚拟补丁规则。

图 17-28 添加 SQL 攻击策略

* 攻击类型:	SQL注入		V
* 状态:	启用		~
* 响应动作:	通过		~
* 关键字:	grant&identified by 注: 仅目定义策略修改才生效!		
特征:	(\s); ^)grant(.*?)to\s?((*.+?*)]([^\s\(*,]+))\s?identified\; 注: 仅自定义策略修改才生效!	;by	
* 详细:	Exploit database CVEs		

表 17-10 添加 SQL 攻击策略

参数	说明
名称	自定义虚拟补丁规则名称。
攻击类型	选择攻击类型。可选SQL注入与缓冲区溢出。
状态	设置规则启用与否。
响应动作	设置响应动作。
关键字	填写SQL攻击的关键字。
特征	填写SQL攻击的特征。
详细	填写SQL攻击的详细介绍。

步骤4 单击"虚拟补丁规则例外"页签查看例外规则,并进行设置。

虚拟补丁规则例外在"风险管控 > 风险管理"页面进行添加,详情参见<mark>进行风险管</mark> <mark>理</mark>。

步骤5 执行以下操作使配置生效。

- 1. 在左侧导航栏,选择"策略防护>策略设置"。
- 2. 勾选启用虚拟补丁。
- 3. 单击 二编辑图标,选择风险等级,单击"确定"。
- 4. 单击"策略应用"。

更多信息,请参见<mark>管理基本配置</mark>。

----结束

17.2.4 审计日志

17.2.4.1 查看审计日志信息

审计日志包含审计日志信息和业务字典配置信息。

数据资产开启保护后,系统会对每个数据库操作进行审计,您可以通过查看审计日志 信息了解具体信息,方便数据资产管理和事后回溯。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"审计日志 > 日志检索"。
- 步骤3 根据资产类型,单击对应的日志页签(例如单击SQL日志)。
- 步骤4 单击最新日志,查看最新的审计日志信息。

图 17-29 查看审计日志

最新日志	检索列表								
总共 1,719 条	15∨								刷新
数据库用户	资产客户端IP	策略	风险级别	操作命令	响应动作	数据库IP	捕获时间	操作	
root	17 .44	默认策略	无风险	LOGOUT	通过	17 1	2023-05-31 14:04:06	详情	回放
root	17 .44	默认策略	无风险	LOGOUT	通过	17 1	2023-05-31 14:04:06	详情	回放
SYS	12	默认策略	无风险	LOGOUT	通过	17	2023-05-31 10:19:21	详情	回放
SYS	12	默认策略	无风险	LOGOUT	通过	17	2023-05-31 10:19:21	详情	回放

步骤5 单击检索列表,设置查询条件,查询目标审计日志信息。

步骤6 (可选)在审计日志列表中,单击"详情",查看此条日志的详细信息。 ----**结束**

17.2.4.2 回放审计日志语句

如果在查看审计日志时部分内容不好识别,您可以通过回放审计日志涉及的语句了解信息。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"审计日志 > 日志检索"。
- 步骤3 根据资产类型,单击对应的日志页签(例如单击SQL日志)。
- 步骤4 单击最新日志或者检索列表,查看审计日志。
- 步骤5 (可选)设置对应检索条件,单击"查询",查询对应审计日志。

步骤6 找到目标审计日志,单击"回放"。在会话回放对话框中,查看回放语句。

图 17-30 回放

会话回放

0 [请求] 2024-08-23 18:24:22

<SYS>:logout

0 [请求] 2024-08-23 18:24:22

<SYS>:SELECT 'YES' FROM USER ROLE PRIVS WHERE GRANTED ROLE='DBA'

----结束

17.2.4.3 添加业务字典

对于IP地址、SQL操作等专业信息,系统支持通过业务字典功能,将这些专业信息翻译 成用户容易理解的业务信息。

系统支持配置的业务字典类型包括IP、账号、操作和操作对象。

- 添加IP类型的业务字典
- 添加账号类型的业务字典
- 添加操作类型的业务字典
- 添加操作对象类型的业务字典

添加 IP 类型的业务字典

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"审计日志 > 业务字典"。
- 步骤3选择"操作"页签。
- 步骤4 单击"添加",配置业务字典信息,单击"确定"。

图 17-31 IP 类型业务字典

添加IP翻译		×
* IP地址:	192	
* IP类型:	服务端IP V	
* 业务名称:	网站数据库	
状态:		
	取消	确定

表 17-11 IP 类型业务字典

参数	说明
IP地址	设置IP地址。
IP类型	在下拉栏中选择IP地址类型,包括服务器端IP、客户端IP和应用端 IP。
业务名称	IP地址对应的业务名称。
状态	开启和关闭此业务字典。 开启状态:添加业务字典后直接为开启状态。 关闭状态:配置完成后不生效,需要手动开启。

步骤5 在左侧导航栏,选择"审计日志 > 业务字典设置",打开业务字典开关。

----结束

添加账号类型的业务字典

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"审计日志 > 业务字典"。
- 步骤3选择"账号"页签。
- 步骤4 单击"添加",配置业务字典信息,单击"确定"。

图 17-32 账号类型业务字典

添加账号翻译		×
* 账号:	test	
* 账 号类型 :	数据库账号 >	
* 资产:	mysql_demo01 V	
* <u>业</u> 务名称:	测试部门	
状态:		
	取消	确定

表17-12 账号类型业务字典

参数	说明	
账号	设置账号名称。	
账号类型	在下拉栏中选择账号类型,包括 "数据库账号" 和 "应用端账号" 。	
资产	在下拉栏中选择账号对应的资产。	
业务名称	账号对应的业务名称。	
状态	开启和关闭此业务字典。	
	● 开启状态: 添加业务字典后直接为开启状态。	
	• 关闭状态: 配置完成后不生效, 需要手动开启。	

步骤5 在左侧导航栏,选择"审计日志 > 业务字典设置",打开业务字典开关。

----结束

添加操作类型的业务字典

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"审计日志 > 业务字典"。
- 步骤3选择"账号"页签。
- 步骤4 单击"添加",配置业务字典信息,单击"确定"。

图 17-33 操作类型业务字典

添加操作翻译		×
* 操作:	SELECT	
* 数据库类型:	SQL V	
* 业务名称:	查询	
	取消	确定

表17-13 操作类型业务字典

参数	说明
操作	设置数据库操作命令,例如SELECT等。
数据库类型	在下拉栏中选择数据库类型。
业务名称	操作对应的业务名称。

步骤5 在左侧导航栏,选择"审计日志 > 业务字典设置",打开业务字典开关。

----结束

添加操作对象类型的业务字典

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"审计日志 > 业务字典"。
- 步骤3选择"操作对象"页签。
- 步骤4 单击"添加",配置业务字典信息,单击"确定"。

图 17-34 操作对象类型业务字典

添加操作对象翻	沿泽	×
* 操作对象:	employees	
* 业务资产:	mysql_demo01 V	
* 所属实例:	EMPLOYEES	
* 业务名称:	员工信息表	
状态:		
	取消	确定

表 17-14 操作对象类型业务字典

参数	说明
操作对象	设置数据库操作对象,例如数据库、表等。
业务资产	在下拉栏中选择资产。
所属实例	所属的数据库实例名。
业务名称	操作对象对应的业务名称。
状态	开启和关闭此业务字典。 • 开启状态:添加业务字典后直接为开启状态。 • 关闭状态:配置完成后不生效,需要手动开启。

步骤5 在左侧导航栏,选择"审计日志>业务字典设置",打开业务字典开关。

----结束

17.2.4.4 启用业务字典功能

在业务字典页面中配置业务字典信息并开启后,业务字典功能还不能直接生效。您还 需要在业务字典设置页面中打开对应业务字典类型的开关,才能正式生效。

操作步骤

步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。

步骤2 在左侧导航栏,选择"审计日志 > 业务字典"。

文档版本 01 (2024-11-28)

步骤3 在业务字典设置列表中,打开对应业务字典类型的开关,在弹出的确认提示框中单击 "确定"。

图 17-35 业务字典开关

业务字典开关	
业务IP	
业务账号	
业务操作	
业务操作对象	

----结束

17.2.5 风险管控

17.2.5.1 执行风险扫描

风险管控支持手动扫描风险信息、查看系统审计的风险问题和配置风险告警接收方式。

通过多个维度为资产进行风险扫描,识别资产的潜在风险,并支持导出风险报表。

背景信息

目前支持资产类型Oracle、SQL Server、DB2、DM7。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"风险管控 > 风险扫描"。
- 步骤3 在资产列表区域,单击"添加风险扫描"。
- 步骤4 在"添加风险扫描"对话框中,选择目标资产,单击"确定"。

图 17-36 添加资产

*选择资产:	oracle	\sim

步骤5设置"风险扫描策略"。

- 1. 在"扫描管理"页签,单击"添加策略"。
- 2. 在"添加策略"对话框中,设置扫描策略信息,单击"确定"。

图 17-37 添加策略

添加策略		×
* 策略名称:	demo	
类型:	ORACLE	\sim
策略标签:	CVE风险 授权风险 系统风险 认证风险	
类型详情: ♥ 数据 ♥ 默 ♥ pub ♥ pub ♥ pub ♥ conn ♥ reso ♥ 授予	i库链接信息的访问权限 的系统表空间 员权限的级联授权 lic对象权限设置 lic系统权限设置 F管理员权限的角色 nect角色授权 级联授权 ipublic权限的角色	
	取消	确定

表17-15 添加策略参数说明

参数	说明					
策略名称	设置风险扫描策略名称。					
类型	显示数据库类型,根据当前所选资产确定。					
策略标签	- 设置风险扫描策略,支持对每个策略标签进行设置:					
	■ CVE风险					
	■ 授权风险					
	■ 系统风险					
	■ 认证风险 - 单击标签后,在类型详情中勾选需要扫描的具体风险项。					

参数	说明
类型详情	勾选需要扫描的具体风险项。

步骤6执行"风险扫描任务"。

- 1. 在"扫描管理"页签,单击"风险扫描"。
- 2. 在风险扫描对话框中,选择资产用户和策略名称,单击"开始扫描"。 在扫描进程中可以查看具体扫描项和风险等级。

图 17-38 风险扫描

风险扫描				×
* 资产用户:	sys as sysdba	~	开始扫描	
* 策略名称:	默认Oracle策略	~		
扫描进程:				
正在扫描【oracle】	空口令角色: 低风险			
正在扫描 [oracle]	过期未登录的帐号: 无风险			
正在扫描【oracle】	远程操作系统非安全认证: 无风险			
正在扫描【oracle】	基于远程操作系统的角色的设置: 无风险			
正在扫描【oracle】	数据字典访问权限: 无风险			
扫描完成				

步骤7执行"弱口令检查"。

1. 在"扫描管理"页签,单击"弱口令检测"。

2. 在弱口令检测对话框中,单击"开始检测",查看资产是否存在弱口令账号。

图 17-39 风险扫描

弱口令检测-19 33	Х
正在检测【oracle】弱口令:	
未检测到风险	
检测结束	
共耗时: 2 秒 862 室秒	
取消检测开	始检测

- 步骤8 查看"风险扫描结果"。
 - 1. 单击"风险报告"页签。
 - 找到目标报告,单击"详情"。在查看报表页面,可以查看报表的详细统计信息。

图 17-40 查看报表



3. 单击"导出报表",选择报表格式,将报表下载到本地。

----结束

17.2.5.2 进行风险管理

风险管理提供风险日志查询统计、风险日志处理功能。对绑定资产进行风险日志信息检索,并可以将误报的风险操作加入虚拟补丁例外规则。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"风险管控 > 风险管理"。
- 步骤3 在顶部的"当前已选择资产"下拉栏中,选择目标资产。

图 17-41 风险管理

风险管控 / 风险管理	当前已选择资产	mysql_1	51 V 1				
统计事件 2							5
时间范围: 最近一周	✓ 查询						加入虚拟补丁规则例外
			4 时间	资产客户端IP	数据库用户 表		动作 操作
			0 2023-05-31 09:31	1 44	root		阻断详情目回放
木认证/认证超时						总共1条	< 1 > 15条/页 >
• 无风险 66							
全部记录							

步骤4 在"时间范围"下拉栏中选择查询时间,单击"查询"。

步骤5 单击风险类型名称,在右侧查看具体风险列表。

- 查看详情:单击"详情",查看风险的详细信息,包括资产信息、访问信息和 SQL执行信息等。
- 回放信息:单击"回放",查看SQL执行的请求和应答过程。
- **步骤6**(可选)如果判断此风险是误报,您可以选择风险后,单击"加入虚拟补丁规则例 外"。更多信息请参考<mark>设置虚拟补丁</mark>。

----结束

17.2.6 报表分析

17.2.6.1 添加并生成报表

在配置报表页面,您可以执行添加报表模板,生成报表,设置定时生成报表等操作。

操作步骤

步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。

步骤2 在左侧导航栏中,选择"报表分析 > 报表配置"。

步骤3添加"报表模板"。
1. 单击"添加",在添加报表对话框中,设置报表信息。

图 17-42 添加报表

添加报表		×
报表类型: 默认:	QB ∨	
类型	描述	
DPA	○ DPA数据库管理活动(HDPA保护的数据库进行的DDL和DCL论问、) ○ DPA数据库请求异常分析(HDPA保护的数据库进行的超出箱商语句、)	
SOX	○ SOX数编考管理活动(HISOX保护的数据库进行的DDL和DCL论问,) ○ SOX数编串请求异常分析(HISOX保护的数据库进行的超出指断语句范围的,)	
	○ SOX活動用户(RISOX保护的設備準进行的活動状态的用户的访问描知的計。) ○ SOX活動用户(表積)(RISOX保护的設備準进行的活動状态的用户的访问描知统计(表指),)
等级层边	● 等保数编集管理活動对等级保护的数据常进行的DDI和DCL访问。) ● 等保数编集集求异集分析(对等级保护的数据常进行的超出策略语句范围的。)	
	○ 等保護動用户(均等吸留)中的股票库进行的活动状态的用户的访问情况统计。) ○ 等保護動用户 (素格) (对等吸促)中的股票库进行的活动状态的用户的访问情况统计 (表格) 。)
医疗防体支	○ HIS数据書管理透动(HHS保护的数据库进行的DDL和DCLib问。) ○ HIS数据率请求异常分析(对HIS保护的数据库进行的超出策略语句范围的。)	
CONTA LEG	○ HIS運動用户図HIS限中的設調率进行的活动状态的用户的访问情况能计。)	
	取调	确定

表 17-16 添加报表

参数	说明
报表类型	选择一种报表类型,支持的类型包括检索、默认报 告、其他。
选择报表项目	在描述中选择一个报表项目。 说明 仅支持选择一个报表项目。

2. 单击"确定",创建报表模板。

步骤4 如果需要根据报表模板"直接生成报表",请参考此步骤:

- 1. 找到目标报表模板,单击生"成报表"。
- 2. 在左侧导航栏中,选择"报表分析 > 报表查看"。
- 3. 单击"下载",将报表下载到本地。具体操作,请参见**下载并查看报表**。

图 17-43 生成报表

报表列表							
+ 添加						时间排序	分类排序
报表名称	报表类型	修改时间	定时发送	报表来源	操作		
- 检索-视图							
概要_周报	概要	2017-08-29	禁用	手动输入	编辑 生成报表	定时报表配置	删除
概要_日报	概要	2017-08-29	禁用	手动输入	编辑 生成报表	定时报表配置	删除

步骤5 如果需要根据报表模板"定时发送报表",请参考此步骤:

- 1. 找到目标报表模板,单击"定时报表配置"。
- 2. 在定时报表配置对话框中,设置定时报表生成。

图 17-44 定时报表配置

定时报表配置(需重启或等待24小时后使用)	Х
启用计划: 🗹 启用计划	
频率设置: 🔵 执行一次 💿 重复执行	
定时设置: 🔵 每日计划 💿 每周计划 🔵 每月计划	
设置:每个周的: 周一	
整点设置: 9 / 整点	
开始日期: 2023-05-11	
取消	● 定

表 17-17 定时报表配置

参数	说明
启用计划	勾选启用计划,开启定时生成报表。
频率设置	选择定时发送报表次数。可选项包括: - 执行一次 - 重复执行
定时设置	设置周期生成时间。可选项包括: - 每日计划:设置每日的具体时间生成报表。 - 每周计划:设置每周的具体时间生成报表。 - 每月计划:设置每月的具体时间生成报表。
开始时间	选择开始执行定时报表的日期。

3. 单击确定。

配置完成后,系统将在指定时间在"报表分析 > 报表查看"页面生成报表。

----结束

相关操作

您可以根据需要进行以下管理操作:

• 编辑报表模板:找到目标报表模板,单击"编辑",修改报表模板。

● 删除报表模板:找到目标报表模板,单击"删除",删除报表模板。

17.2.6.2 下载并查看报表

生成报表后,您可以在报表查看页面下载查看报表。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏中,选择"报表分析 > 报表查看"。
- 步骤3 (可选)在报表类型中选择目标报表类型,单击"查询",搜索指定类型报表。
- 步骤4 找到目标报表,单击"下载"。
- 步骤5 解压下载的zip压缩包,查看报表信息。

----结束

17.2.7 运维管理

17.2.7.1 审批运维工单

数据库操作员对资产进行运维操作时,需要提交运维工单。管理员在工单审批页面审 批后,数据库操作员才能进行相关操作。

前提条件

在审批前数据库操作员已经发起运维工单,具体操作请参见发起运维工单申请。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"运维管理 > 工单审批"。
- 步骤3 找到目标工单申请,单击"审批"进行编辑。
- 步骤4 在编辑审批对话框中,设置审批意见,并单击"同意"(或者单击驳回)。

🗀 说明

如果是SQL脚本,可以单击脚本名称,下载到本地进行审批。

图 17-45 审批工单

编辑审批									×
* 申请名称:	datadmin工单申请								
* 资产名称:	oracle_zz(10 521)	\vee		数据库实例名:	orcl				
客户端工具:	安全客户端			客户端IP:	1 5				
是否开启授权码:			申请操作时间:	2022-03-25 14:1	8:22 ~	2022-04-05 14	1:18:22		
申请事由:				备注:				11	
* 审批意见:	审批通过							11	
操作方式 操	作语句	操作命令	操作对象-表	操	作对象-列	s	QL脚本		
常规操作		SELECT							
							同意	驳回	取消

----结束

操作结果

如果审批同意,运维操作员可以进行后续运维操作。如果被驳回,运维操作员无法进 行后续运维操作。

17.2.7.2 管理运维人员

在人员管理页面查看运维人员信息。如果添加资产时开启了Web认证,还需对运维人员进行目标资产授权,授权后才可访问资产。

背景信息

请确保已添加资产账号信息,具体操作请参见添加数据资产。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"运维管理 > 人员管理"。
- 步骤3 在账号列表中,查看数据库操作员相关信息。
- 步骤4 授权数据库操作员访问数据资产,请参考此步骤。
 - 1. 找到目标数据库操作员,单击"配置中心"。
 - 2. 在账号设置对话框中,对数据库操作员进行目标资产账号授权。

图 17-46 关联数据资产

账号设置							×
资产名称 (按名称排序)	资产类型	资产IP	资产端口	授权状态	密码代填	授权账号 (账户名-实例名)	
创意团队my_1	MYSQL	192 120	3306			test-test	
运维测试192.1	MYSQL	192 251	3306			请选择授权账号	
						< [1) >

表 17-18 关联数据资产

参数	说明
授权账号	选择已添加的资产账号。 如果资产没有设置账号,请先添加账号。具体操作,请参见 <mark>手动</mark> <mark>添加账号</mark> 。
授权状态	打开授权状态。
密码代填	打开密码代填。开启后,通过安全客户端无需密码直接访问资 产。

----结束

相关操作

配置完成后,运维人员可以通过安全客户端访问资产。具体操作,请参见<mark>通过Web安</mark> 全客户端访问资产。

17.2.8 设备管理

17.2.8.1 Bypass 设置

支持进行系统一键Bypass设置,以便在系统发生故障时,跳过系统以维持业务的正常运行,并在不影响业务的前提下排查系统问题。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"设备管理 > Bypass"。
- 步骤3 在Bypass页面,开启Bypass开关。

系统一键Bypass:开启启动按钮,系统进入Bypass状态。所有策略将自动失效,直至 手动关闭。

----结束

17.2.9 日志设置

日志管理包括配置日志保存方式和备份还原日志等。

17.2.9.1 配置日志保存方式

该模块是对日志的存放位置、日志保存时间及对业务日志的删除进行配置。日志存放 方式包括集中管理和本地记录,集中管理会将操作日志发送到集中管理设备。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"日志设置 > 日志配置"。
- 步骤3 如需配置日志集中管理,请参考此步骤操作:

图 17-47 日志配置

	✔ 启用日志集中管理	✔ 本地继续记录日志		
日志集中管理地址:				
	保存			
*日志保存时间:	六个月		~	保存
清除业务日志:	清除业务日志			

- 1. 勾选"启用集中管理",同时也可勾选本地继续记录日志。
- 2. 在集中管理地址输入框中,设置集中管理设备IP。
- 3. 单击"保存"。
- 重启服务或者重启设备,使配置生效。
 重启设备影响业务运行,建议在业务运行低谷时执行此操作。
- 步骤4 如需配置日志定期删除,请参考此步骤操作:
 - 1. 在日志保存时间下拉栏中,选择"日志保留时间"。
 - 2. 单击保存,到期后系统自动删除日志。
- 步骤5 如需清除业务日志,单击"清除业务日志"。

----结束

17.2.9.2 备份还原日志

系统支持对本地日志进行备份和还原产品日志信息,备份包括自动备份、手动备份两 种方式。

17.2.9.2.1 自动备份

配置自动备份,系统会定时自动备份产品日志。

文档版本 01 (2024-11-28)

操作步骤

步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。

- **步骤2** 在左侧导航栏,选择"日志设置 > 备份还原"。
- 步骤3 在备份配置区域,设置自动备份方式。

图 17-48 自动备份

备份配置		
备份方式:	自动备份	\vee
状态:	● 启用 ○ 禁用	
备份时间:	在每天的 1 (0~23)点备份昨天日志	
e	保存	

表 17-19 自动备份

参数	说明
备份方式	选择自动备份。
状态	选择启用。
备份时间	设置每天的备份时间。

步骤4 单击"保存"。

----结束

17.2.9.2.2 手动备份

配置手动备份,系统会立即创建全量的产品日志备份文件或增量的产品日志备份文 件。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"日志管理 > 备份还原"。
- 步骤3 在备份配置区域,设置手动备份方式。

图 17-49 手动备份

备份方式:	手动备份		\sim
Į,	曾星备份	备份全部	

手动备份支持全量备份和增量备份两种方式:

- 单击"备份全部",手动备份当前零点以前的所有的日志。
- 单击"增量备份",手动备份从上次备份后时间节点到当前零点前的所有日志备份。

----结束

17.2.9.2.3 还原日志

在备份文件列表,展示日志备份记录。您可用通过备份日志文件进行还原操作。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 找到目标备份文件,单击"还原"。

🗋 说明

如果是远程备份日志,需要先单击下载将备份文件下载到设备。

步骤3 在确认提示框中,单击"确定"。

▲ 注意

还原后系统数据是备份文件的当时状态,新变更的信息会丢失,请谨慎操作!还原后 需要重启服务。

----结束

17.2.10 系统管理

17.2.10.1 查看平台信息

平台管理模块包括设备授权、账号管理与网络设置。

在使用系统前,您需要为系统进行授权。完成设备授权后,您可以在平台信息页面, 查看系统基本信息和授权信息。

17.2.10.2 手动创建账号

系统默认已经创建系统管理员(sysadmin)账号、安全管理员(secadmin)、审计管理员(audadmin)、数据库操作员(datadmin)账号。如果有多个员工需要使用系统,建议您为每个员工单独创建账号,便于管理。

背景信息

账号的权限由角色决定,系统默认创建系统管理员、审计管理员、安全管理员和数据 库操作员角色。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"系统管理 > 账号管理"。
- 步骤3 单击右上角的"新建账号",配置账号参数。

图 17-50 新建账号

新建账号		Х
* 账号:	demo_user	
* 密码:	•••••	
* 密码确认:	••••••	
* 使用人:	<u>*</u>	
* 角色:	系統管理员 🗸 🗸	
* 电话:	1300000000	
* 邮箱:	zhangsan@com	
使用期限:	 永久 ○ 定义期限 	
备注说明:	请输入备注说明	
	0/200	
	取消	提交审核

表 17-20 新建账号

参数	说明
账号	填写自定义账号名称。

参数	说明
密码/密码确认	● 填写账号登录密码。
	 说明:密码最小长度为6个字符,且需要同时包含数字、字符、大写字母、小写字母。
使用人	填写使用人员姓名。
角色	在下拉栏中选中角色。支持系统管理员、审计管理员、安全管理 员和数据库操作员。
电话	使用人员联系电话。
邮箱	使用人员联系邮箱。
使用期限	配置账号的有效期限。支持以下选项: ● 永久:账号不会过期停用。 ● 定义期限:选由后 沿置时间期限 到期停用账号
	▼ 定入规模·处于归,这直时可规限,到规序用账号。 植空帐早的描述信自
田江坑明	堤 つ 炊 ち い 油 心 に ふ。

步骤4 单击"提交审核"。

----结束

操作结果

创建账号后,您可以在账号列表进行查看。

🛄 说明

创建的账号通过审批才能使用,详情请参见<mark>审核账号</mark>。

相关操作

根据需要您还可以进行以下管理操作:

- 修改账号信息:单击"编辑",修改账号信息。
- 删除单个账号:单击"删除",删除账号。
- 批量删除账号:选中账号后,单击"批量操作",在下拉框中选择"删除"。
- 初始化密码:选中账号后,单击"批量操作",在下拉框中选择"重置密码", 系统自动为账号修改密码。

🛄 说明

对于系统默认账号,不支持执行以上管理操作。

17.2.10.3 诊断系统实时情况

支持实时查看系统内核,CPU、内存、磁盘、网卡等资源情况。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"系统管理 > 系统诊断"。
- 步骤3 单击实时诊断的下拉框,选择您需要诊断的服务。

诊断项目包括内核、cpu&mem、磁盘、网卡、端口、ping。

步骤4 单击"执行",进行系统诊断。

图 17-51 系统诊断

artist:	内相差年		ц т				
	Linux version 3,10 on Oct 19 16:18:5	0.0-1160.el7.x86_6 9 UTC 2020	i4 (mockbuild@kbuilde	nbays.centos.org) (gcc	version 4.8.5 20150623 (Re	d Hat 4.8.5-44) (GCC)) #1 SMP 1	N

----结束

17.2.10.4 升级系统版本

通过此功能升级版本,维护系统正常运行。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"系统管理 > 系统升级"。
- 步骤3 在页面右上角,单击"上传升级脚本"。
- 步骤4 在对话框中,单击"点击或将文件拖拽到这里上传",上传系统升级包。

图 17-52 升级系统

反本变	ē.	>
	点击或将文件拖拽到这里上传	
	 注意 (1)执行升级脚本前将自动备份当前系统,若升级失败将自动回滚; (2)升级结束可能会自动更启应用或系统; (3)文件格式需为gpg; (4)单次仅上传1个文件,文件大小不超过2GB。 	

步骤5 单击"升级"。

----结束

操作结果

在版本变更历史中,查看系统的升级记录。

17.2.10.5 时间配置

系统支持手动修改服务器时间,或者通过NTP服务器同步服务器时间。 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Web控制 台。

取消

升级

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"系统管理 > 时间配置"。
- **步骤3** 如需手动修改系统时间,请参考此步骤:

图 17-53 手动修改系统时间

日期和时间					
	* 时间:	2021-11-08 15:43:13			
	 注意 	意: 修改或同步时间可能导行	改測遊麟当前	的页面合话失效	 设置后需要重新登录系统。
		保存			

- 在日期和时间区域,单击时间的下拉栏,在提示框中选择日期和时间,单击"确 定"。
- 2. 单击"保存",完成系统时间修改。
- 3. 完成后系统将自动重启Web服务,设置后需要重新登录系统。

步骤4 如果需要启用时间同步服务,请参考此步骤:

图 17-54 启用时间同步服务

主服务器		
	• IP:	19 00
	• 跳口:	123
	自动局步:	
	0 2	"意:设置"自动局步"后,系统会每天和时间服务器局步一次。
		保存 同步
备用服务器		
	• IP::	19 10
	• 190:	123
	自动同步:	
	0 1	章:设置"自动同步"后,系统会每天和时间服务器同步一次。
		保存 同步

- 1. 在主服务器区域,设置时间服务器的IP和端口。
- 2. 打开自动同步开关。
- 单击"保存",启用时间同步服务。
 启用后,系统会在每天的00:05分和时间服务器同步一次。单击"同步",系统立即同步时间。
- 如果需要设置备用时间服务器,参考主服务器设置,在备用服务器中设置备份时 间服务器。

----结束

17.2.10.6 查看设备状态

您可以通过设备状态页面,查看系统的资源使用情况,方便排查问题。同时支持进行 重启服务、重启/关闭设备等管理操作。

操作步骤

步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。

文档版本 01 (2024-11-28)

步骤2 在左侧导航栏,选择"系统管理 > 系统运维"。

步骤3 查看设备的"运行时间"、"CPU使用率"、"内存使用率"、"网卡吞吐量"、 "磁盘使用情况等"信息。

图 17-55 查看设备状态

	100 (red 27 state			Acard Book Acard
-	OVERED		m edemenu	ARREN IN THESE IN
() () () () () () () () () () () () () (~ ·		-	
6.				
1 255 10	1 11% w		1 1	
OPUERUE	NREAL STREET	the sales taken taken taken in	alter after table table	who take take take take
Instation (Protection				
199				
- 0	777			al.
	1			
		a salar taken salar taken ta	this suiter taken to	
POWTEN				
111KB	1154	arrest		
aveneti	1000		((#(% (%/23)	726
And A Contract of	and have		changing and of the lot	1.000

表 17-21 查看设备状态

参数	说明
系统概况	展示系统实时的CPU使用率与内存使用率。
CPU使用率	展示最近15分钟系统CPU使用率的变化情况。
内存使用率	展示最近15分钟系统内存使用率的变化情况。
吞吐量	展示最近15分钟系统网卡的吞吐量变化情况。
磁盘使用情况	展示各文件系统与挂载点的使用情况。

步骤4 (可选)在页面的右上角,进行重启服务、重启/关闭设备等操作。

重启服务、重启/关闭设备的操作影响业务的运行,建议在业务低谷运行时执行本操 作。

----结束

17.2.10.7 网络配置

您可在"系统管理 > 网络设置"页面配置设备的网卡信息、DNS和路由信息。

17.2.10.7.1 配置网卡信息

通过配置网络信息,修改设备网络IP地址、路由等信息,从而接入业务网络环境。 系统的网络设置功能,支持配置网卡信息、DNS服务器和路由策略信息等。

- 网卡信息:包括网络IP地址、网关地址等信息,一般在初次安装部署或者网络环境变更时,需要配置。
- DNS服务器:设置DNS服务器地址,如果资产为域名时,必须要配置DNS服务器。

• 路由策略信息:配置路由策略,一般在多网卡环境下,需要配置。

🗀 说明

请根据网络环境规划配置设备的网络信息,如果网络配置错误,您可能无法通过网络Web访问 设备。此时,您需要直连设备后,重新配置网络信息。

前提条件

已经获取设备需要配置的IP地址等网络信息。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"系统管理 > 网络设置"。
- 步骤3 在网卡列表区域,找到目标网卡,单击"编辑"。
- 步骤4 在"编辑"对话框中,设置网卡信息。

图 17-56 配置网络地址

1.输入IP 2.修改网 同!	雨,调嘲保您输入的IP可用: 关地址前,请确保您了解网关地址对网络的影响,谨慎操作,避免新
可口名称:	ens32
网口类型:	管理ロ ~ ~
• IP地址:	1 61
子阿掩码:	2 5.0
网关地址:	1

表 17-22 配置网络地址

参数	说明
网口名称	默认网口名称,无法更改。
网口类型	选择网口类型。网口类型包括: • 管理口 • 未做用途

参数	说明
IP地址	您的设备IP地址。根据您的网络规划决定,需要和数据库等数据资产 互通。
子网掩码	设置您的子网掩码。根据您的网络规划决定。
网关地址	您的网关地址。

步骤5 单击"确定",完成配置。

步骤6 配置DNS服务。

如果需要用到域名解析服务,例如数据库地址使用了域名,需要配置DNS服务。

- 1. 在右上角,单击设置DNS。
- 2. 在设置DNS对话框中,配置主DNS和备DNS信息。
- 3. 单击"确定"。

----结束

17.2.10.7.2 配置路由信息

如果设备存在多网卡,需要根据网络规划方案配置路由策略信息。 修改路由信息前,请确保您了解路由对网络的影响,谨慎操作,避免断网。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"系统管理 > 网络设置"。
- 步骤3 在路由列表区域,单击"添加路由"。
- 步骤4 在"添加路由"对话框中,设置路由信息。

图 17-57 配置网络地址

 目标地址: 	19)	
•子网掩码:	25	
下一跳地址:	19]	
接口 :	 目动 ()选择接口 	

表 17-23 配置网络地址

参数	说明
目标地址	即目标网络IP地址。
子网掩码	配置目标地址的子网掩码。
下一跳地址	配置下一跳地址,一般是网关地址。
接口	选择接口方式: 自动:系统根据目标地址,自动选择流量外发网卡。 选择接口:手动选择流量外发的网卡。

步骤5 单击"确定",完成配置。

----结束

17.2.10.8 查看和配置消息中心

在消息中心,您可以查看系统的通知告警等消息,配置推送的消息类型、消息模板和 接收角色等。

操作步骤

- 步骤1 使用系统管理员sysadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"系统管理 > 消息中心"。

也可在页面右上角,单击"消息中心",进入"消息中心"页面。

图 17-58 消息中心



步骤3 在消息中心页面查看最近的通知告警等信息。

步骤4 单击右上角的"消息管理",配置需要接收的消息。

- ①: 消息开关,配置是否需要推送此类型消息。
 - ②:单击编辑,编辑推送的消息模板。

• ③:单击修改,设置消息接收的角色,仅部分消息类型支持配置。

图 17-59 消息管理

 ◆ 账号到期预警 ① 账号到期预警 	 ◆ 授权到期预警 ● 授权到期预警
你的账号将在[[Time]]到期,为了不影响 使用,请尽快更改有效期!	授权即将于[[Time]]到期,为了不影响使 用,请尽快重新授权[[Link]]
接收:默认角色	接收:未设置 修改 3 编辑

----结束

17.3 安全管理员操作指南

17.3.1 设置审批架构

根据业务需求设置合理的审批架构,对数据库操作员申请人设置相应的系统管理员审 批人,以增强操作流程的安全性。

请确保已为对应人员创建账号,具体操作请参见手动创建账号。

操作步骤

- 步骤1 使用安全管理员secadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,选择"用户管理 > 审批架构"。
- 步骤3 单击右侧"添加"。
- **步骤4** 在"添加成员信息"弹框填写信息。 请先添加**系统管理员**审批人账号,随后添加数据库操作员申请人账号。

图 17-60 添加成员信息

添加成员信息			×
* 成员姓名:	李		
* 账号:	操作员1	~	
角色:	数据库操作员	\vee	
* 上级审批人:	小明	~	
☆取行.			
цн J:	XCP		
职位:	XXX		
		取	消 确定

表 17-24 添加成员信息

参数	说明
成员姓名	通过选择账号自动获取。也可修改自动获取的姓名,修改后账号 信息同步改动。
账号	在下拉框中选择账号。
角色	通过选择账号自动获取。
上级审批人	在下拉框中选取 数据库操作员 的上级审批人。上级审批人为已添 加的系统管理员账号。
部门	填写成员部门信息。
职位	填写成员职位信息。

步骤5 单击"确定"。

- 步骤6 单击页面左侧的审批架构,在成员列表查看到审批人信息,您还可进行如下操作:
 - 修改审批人信息:单击编辑,修改审批人信息。
 - 删除审批人:单击删除,删除审批人。删除前请先确保其下申请人已清理或转移。
 - 批量删除审批人:勾选目标审批人,单击删除。
- **步骤7** 单击页面左侧的组织架构旁的 ∨ 展开组织架构,单击目标审批人,查看其管理的成员,您还可进行如下操作:
 - 修改申请人信息:单击编辑,修改申请人信息。
 - 删除申请人:单击删除,删除申请人。

• 批量删除申请人:勾选目标申请人,单击删除。

----结束

17.3.2 系统管理

17.3.2.1 审核账号

创建账号后,需要安全管理员审核通过后,才能够正常使用。系统支持手动审核和自 动审核两种方式。

前提条件

您已经创建新的用户账号,具体操作请参见手动创建账号。

背景信息

默认情况下需要安全管理员手动审核账号,您也可以打开自动审核开关,自动通过账 号。

图 17-61 自动审核

自动审核	通过	拒绝	C	⊘	Ì	
------	----	----	---	---	---	--

操作步骤

- 步骤1 使用安全管理员secadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"系统管理 > 账号审核"。
- 步骤3 找到需要审核的账号,单击"通过"。
- 步骤4 在提示框中,单击"确定"。

----结束

17.3.2.2 角色管理

系统已经默认创建系统管理员、审计管理员、安全管理员与数据库操作员角色。

操作步骤

- 步骤1 使用安全管理员secadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"系统管理 > 角色管理"。

步骤3 查看内置角色相关信息。

图 17-62 查看角色

角色名称	创建省	创建时间	说明	启用状态	操作
数据库操作员	-	2022-08-20 16:47:23	数据库操作员		
安全管理员		2019-06-13 14:21:48	安全管理员		
审计管理员		2019-06-13 14:21:48	审计管理员		
系统管理员		2019-06-13 14:21:48	系统管理员		

----结束

17.3.2.3 启用安全配置

安全管理员可以通过用户登录安全设置、账号密码安全设置以及网络访问安全配置三方面保障系统自身的安全性。

17.3.2.3.1 设置用户登录安全

操作步骤

- 步骤1 使用安全管理员secadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"系统管理 > 系统设置"。
- 步骤3 在用户登录安全设置区域,设置用户登录的安全性。

图 17-63 平台登录安全设置

平台登录安全设置	
安全管理方式:	● 安全模式 (https) 更新证书
动态验证码:	
空闲超时登出:	30 分钟
多点登录:	 ● 是 ○ 否
登录安全策略:	3分钟内,同一账号连续提交错误3次,锁定5分钟;10分钟内,同一IP连续提交错误10次,锁定10分钟。
OTP验证:	
UKey验证(证书认证):	

表17-25 平台登录安全设置

参数	说明
安全管理方式	支持使用HTTPS安全模式。
动态验证码	 选择登录时是否启用动态验证码。 启用后,系统登录时,输入正确的动态验证码是必要条件之一,可以防暴力破解密码。
空闲超时登出	设置账号超时自动退出时间。
多点登录	设置是否支持多点登录功能。 • 是:同账号支持在多个地方同时登录。 • 否:一个账号登录后,不能在其他地方登录。

参数	说明
登录安全策略	选择是否启用登录安全策略,防止账号被暴力破解。 例如,用户账号如果在3分钟内,登录信息连续输入错误3次,则 此账号在5分钟内将被锁定,无法登录到系统。
OTP验证	选择是否需要输入动态口令验证。
Ukey验证(证 书认证)	启用后,用户需将存储有证书的UKey插上设备,以实现身份认 证。

步骤4 单击"确定"。

----结束

17.3.2.3.2 设置账号密码安全

操作步骤

- 步骤1 使用安全管理员secadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"系统管理 > 系统设置"。
- 步骤3 在账号密码安全设置区域,设置密码安全要求。

图 17-64 账号密码安全设置

账号密码安全设置

初次登录强制更改密码:

密码有效期:

30 天

步骤4单击"确定"。

----结束

17.3.2.3.3 启用网络访问安全配置

操作步骤

- 步骤1 使用安全管理员secadmin账号登录数据库运维管理系统。
- **步骤2** 在左侧导航栏,选择系统运维 > 系统设置。
- 步骤3 单击安全配置页签。
- 步骤4 在网络访问安全设置区域,设置网络访问限制。

文档版本 01 (2024-11-28)

图 17-65 网络访问安全设置

网络访问安全设置		
登录IP限制:	 ● 接受所有IP ● 限制IP 	
网络权限配置:	□ 禁止ICMP探测 □ 禁止SSH登录	
HOST代理白名单:		仅支持IPv4格式; 接受多个IP地址或域名以换行分隔 格式示例: 192.168.0.1 www.xxx.com
	自动添加	
	确定重置	

表17-26网络访问安全设置

参数	说明
登录IP限制	设置是否限制访问来源:
	● 接受所有IP:不限制访问来源。
	 限制IP: 仅支持允许登录IP地址名单中的IP访问数据库加密 与访问控制的Web控制台。
允许登录IP地址	填写允许登录的IP地址,多个地址用换行隔开。
网络权限配置	设置是否禁止ICMP探测和SSH登录。
	 启用禁止ICMP探测:关闭ICMP功能,则其他设备无法ping 系统。
	● 启用禁止SSH登录:禁止SSH访问系统。
	说明 禁止SSH登录后,运维人员将不能通过SSH访问服务器后台。
HOST代理白名单	填写HOST代理白名单,支持IP地址或域名。

步骤5 单击"确定"生效。

----结束

17.4 审计管理员操作指南

系统会保存所有的操作记录,审计管理员可以定期检查系统日志,审查操作的合规性 以保障系统的安全性。

17.4.1 查看操作审计日志

通过查看系统操作审计日志,检查系统操作的合规性,保障系统安全。

操作步骤

步骤1 使用安全管理员audadmin账号登录数据库运维管理系统。

步骤2 在左侧导航栏,选择"日志管理"。

文档版本 01 (2024-11-28)

步骤3 单击"操作日志"。

步骤4 可选: 设置过滤条件,单击^Q,查询对应操作审计日志。

图 17-66 设置过滤条件

2023-05-04 11:34:07 ~ 2023-05-11 11:34:07		操作账号	IP.	内容等搜索	Q
---	--	------	-----	-------	---

步骤5 在列表查看系统各用户的登录登出和各种操作日志信息。

----结束

17.5 数据库操作员操作指南

数据库运维人员,通过安全客户端进行日常运维。通过运维工单申请高风险操作。

17.5.1 发起运维工单申请

数据库操作员在运维操作前,需要先发起工单申请。

前提条件

请确保已设置好审批架构,为数据库操作员设置相应审批人,详情参见<mark>设置审批架</mark> <mark>构</mark>。

操作步骤

- 步骤1 使用安全管理员datadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"运维管理 > 工单申请"。
- 步骤3 单击"工单申请",在"发起审批"对话框中,设置工单信息。
 - 1. 配置工单信息。

图 17-67 发起审批

发起审批						×
* 申请名称:	datadmin工单申请					
* 资产名称:	oracle_zz(1 21)		数据库实例名:	orcl		
客户端工具:	安全客户端		客户端IP:	100.0		
是否开启授权码:		*申请操作时间:	2022-03-25 14:18	8:22 ~ 2022-04-05 14:18	:22 🗎	
申请事由:		le.	雷注:		li.	
					添加	删除
操作方式	操作语句操作命令	操作对象-表	操作对象-列	SQL脚本	操作	

表 17-27 发起审批

参数	说明	
申请名称	运维工单申请名称。	
资产名称	在下拉栏中选择需要运维的数据资产。数据资产需要已经添 加到系统。	
数据库实例名	设置数据库名称或者实例名称。	
客户端工具	设置访问数据库的客户端工具名称。	
客户端IP	设置访问数据库的客户端IP。	
是否开启授权码	开启授权码 开启授权码,申请审批通过后将获取授权码,后续需通过唯一授权码进行使用人员身份认定。	
申请操作时间	设置运维操作的时间范围。	
申请事由	设置运维操作事由。	
备注	设置申请的备注信息。	

2. 单击"添加",配置数据库操作,单击"确定"。

图 17-68 添加操作

添加操作	Х
操作方式: (•) 常规操作 () 操作语句 () SQL脚本	
* 操作命令: SELECT ×	
操作对象-表: 请输入	
操作对象-列: 请输入	
	取消 确定

表 17-28 添加操作

参数		- 说明	
操作方常规操		- 使用常规的SQL操作,支持设置以下参数:	
IL 1'F	1F	■ 操作命令:选择SQL操作关键字。	
		■ 操作对象-表:设置数据库表名称。	
		■ 操作对象-列:设置数据库列名称。	

参数	-	说明
操作	晤 -	在操作语句中直接输入具体的操作语句。
SQI 本	_脚 –	在SQL脚本,单击请选择在本地选择SQL脚本。 在SQL脚本详情中可以查看脚本内容。

3. 单击"确定"。

步骤4 找到待提交工单,单击"提交",在"确认"提示框中单击"确定"。

----结束

相关操作

根据需要您还可以进行如下操作:

- 查看工单详情:单击目标工单栏的查看,查看工单详情。
- 撤销工单申请:单击目标工单栏的撤销,撤销工单申请。
- 条件查询工单:在条件查询框设置不同条件,进行查询。
- 再次发起审批:单击目标工单栏的再次申请,原工单可以作为模板,您修改相关 信息后,再次发起审批。
- 收藏审批:单击目标工单栏的收藏,收藏审批工单,便于后续使用。

待工单申请审批通过后,可通过安全管理客户端对数据库进行相应操作,详情请参见 通过Web安全客户端访问资产。

17.5.2 通过 Web 安全客户端访问资产

数据库操作员可以通过Web安全客户端访问资产。

在使用Web安全客户端前,需要系统管理员已经将数据库操作员和资产关联起来。具体操作,请参见<mark>管理运维人员</mark>。

操作步骤

- 步骤1 使用安全管理员datadmin账号登录数据库运维管理系统。
- 步骤2 在左侧导航栏,选择"运维管理 > 安全客户端"。
- 步骤3 单击Web安全客户端右侧的"查看"。
- 步骤4 将光标移动到资产名上并单击 ——。
- 步骤5 单击"Edit Connection"。
- **步骤6**单击"OPTIONS"页签,进行连接设置。如果为数据库操作员开启了密码代填,则可 跳过此步骤。
 - 填写User name数据库账号与User password数据库密码。
 - 单击 TEST CONNECTION,测试连接是否成功。
- 步骤7 (可选)单击"DRIVER PROPERTIES"页签,进行驱动属性添加。

步骤8 (可选)单击"SSH TUNNEL"页签,进行SSH隧道通信设置。

步骤9 单击 "SAVE"保存, 成功创建连接。

图 17-69 资产链接

> 🛃 system@oracle_zz-oracle

----结束

相关操作

连接成功后,如果要进行运维操作,请先发起工单申请,详情参见<mark>发起运维工单申</mark> 请。

18 _{权限管理}

18.1 创建用户并授权使用 DBSS

如果您需要对您所拥有的DBSS进行精细的权限管理,您可以使用<mark>统一身份认证服务</mark> (Identity and Access Management,简称IAM),通过IAM,您可以:

- 根据企业的业务组织,在您的华为云账号中,给企业中不同职能部门的员工创建 IAM用户,让员工拥有唯一安全凭证,并使用DBSS资源。
- 根据企业用户的职能,设置不同的访问权限,以达到用户之间的权限隔离。
- 将DBSS资源委托给更专业、高效的其他华为云账号或者云服务,这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求,不需要创建独立的IAM用户,您可以跳过本章 节,不影响您使用DBSS服务的其它功能。

本章节为您介绍对用户授权的方法,操作流程如图18-1所示。

前提条件

给用户组授权之前,请您了解用户组可以添加的DBSS权限,并结合实际需求进行选择,DBSS系统策略如<mark>表18-1</mark>所示。DBSS支持的系统权限,请参见:DBSS系统权限。若您需要对除DBSS之外的其它服务授权,IAM支持服务的所有权限请参见系统权限。

表 1	8-1	DBSS	系统权限
-----	-----	------	------

系统角色/策 略名称	描述	类别	依赖关系
DBSS Audit Administrato r	数据库安全服务 审计管理员,拥 有审核数据库安 全服务日志信息 的权限。	系统角色	无。
DBSS FullAccess	数据库安全服务 所有权限。	系统策略	

系统角色/策 略名称	描述	类别	依赖关系
DBSS ReadOnlyAcc ess	数据库安全服务 只读权限,拥有 该权限的用户仅 能查看数据库安 全服务,不具备 服务配置权限。	系统策略	

示例流程



图 18-1 给用户授权服务权限流程

1. 创建用户组并授权

在IAM控制台创建用户组,并授予数据库安全服务管理员权限"DBSS Security Administrator"。

2. 创建用户并加入用户组

在IAM控制台创建用户,并将其加入1中创建的用户组。

3. 用户登录并验证权限

新创建的用户登录控制台,切换至授权区域,验证权限:

验证方式(参考):您可以尝试开启或关闭实例,此时如果提示"您的权限不足",则表示设置的"DBSS Security Administrator"数据库安全服务安全管理员角色已生效。

18.2 DBSS 自定义策略

如果系统预置的DBSS权限,不满足您的授权要求,可以创建自定义策略。自定义策略 中可以添加的授权项(Action)请参考DBSS权限及授权项。

目前华为云支持以下两种方式创建自定义策略:

- 可视化视图创建自定义策略:无需了解策略语法,按可视化视图导航栏选择云服
 务、操作、资源、条件等策略内容,可自动生成策略。
- JSON视图创建自定义策略:可以在选择策略模板后,根据具体需求编辑策略内容;也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见:创建自定义策略。本章为您介绍常用的DBSS自定义策略样例。

DBSS 自定义策略样例

{

示例1:授权用户查询数据库审计列表

```
"Version": "1.1",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "dbss:auditInstance:list"
        ]
    }
]
```

• 示例2: 拒绝用户删除数据库审计实例

拒绝策略需要同时配合其他策略使用,否则没有实际作用。用户被授予的策略 中,一个授权项的作用如果同时存在Allow和Deny,则遵循**Deny优先原则**。

如果您给用户授予"DBSS FullAccess"的系统策略,但不希望用户拥有"DBSS FullAccess"中定义的删除数据库审计实例权限,您可以创建一条拒绝删除数据库 审计实例的自定义策略,然后同时将"DBSS FullAccess"和拒绝策略授予用户, 根据Deny优先原则,则用户可以对DBSS执行除了删除数据库审计实例外的所有操 作。拒绝策略示例如下:

• 示例3: 多个授权项策略

一个自定义策略中可以包含多个授权项,且除了可以包含本服务的授权项外,还 可以包含其他服务的授权项,可以包含的其他服务必须跟本服务同属性,即都是 项目级服务或都是全局级服务。多个授权语句策略描述如下:

```
{

"Version": "1.1",

"Statement": [

{

"Effect": "Allow",
```

	},	"Action": ["dbss:defendInstance:eipOperate", "dbss:auditInstance:getSpecification"]
	{	"Effect": "Allow"
		"Action": [
		"hss:accountCracks:unblock", "hss:commonIPs:set"
	'']
]	ł	

18.3 DBSS 权限及授权项

如果您需要对您所拥有的数据库安全服务进行精细的权限管理,您可以使用统一身份 认证服务(Identity and Access Management,IAM),如果华为云账号已经能满足 您的要求,不需要创建独立的IAM用户,您可以跳过本章节,不影响您使用DBSS服务 的其它功能。

默认情况下,新建的IAM用户没有任何权限,您需要将其加入用户组,并给用户组授 予策略或角色,才能使用户组中的用户获得相应的权限,这一过程称为授权。授权 后,用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度,分为<mark>角色和策略</mark>。角色以服务为粒度,是IAM最初提供的 一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细,可以精确 到某个操作、资源和条件,能够满足企业对权限最小化的安全管控要求。

支持的授权项

策略包含系统策略和自定义策略,如果系统策略不满足授权要求,管理员可以创建自 定义策略,并通过给用户组授予自定义策略来进行精细的访问控制。策略支持的操作 与API相对应,授权项列表说明如下:

- 权限:允许或拒绝某项操作。
- 授权项:自定义策略中支持的Action,在自定义策略中的Action中写入授权项, 可以实现授权项对应的权限功能。
- 依赖的授权项:部分Action存在对其他Action的依赖,需要将依赖的Action同时写 入授权项,才能实现对应的权限功能。

DBSS支持的自定义策略授权项如表18-2所示:

表 18-2 授权列表

权限	授权项
查询数据库安全审计实例列表	dbss:auditInstance:list
获取数据库安全审计实例的可用规 格	dbss:auditInstance:getSpecification
查询数据库安全防护实例列表	dbss:defendInstance:list
绑定或解绑EIP	dbss:defendInstance:eipOperate

权限	授权项
删除数据库安全防护实例	dbss:defendInstance:delete
删除数据库安全审计实例	dbss:auditInstance:delete
按需购买数据库安全防护实例	dbss:defendInstance:createOnDemand
按需购买数据库安全审计实例	dbss:auditInstance:createOnDemand
按包周期购买数据库安全防护实例	dbss:defendInstance:createOnOrder
按包周期购买数据库安全审计实例	dbss:auditInstance:createOnOrder
重启数据库安全防护实例	dbss:defendInstance:reboot
启动数据库安全审计实例	dbss:auditInstance:start
关闭数据库安全审计实例	dbss:auditInstance:stop
重启数据库安全审计实例	dbss:auditInstance:reboot
启动数据库安全防护实例	dbss:defendInstance:start
关闭数据库安全防护实例	dbss:defendInstance:stop

18.4 FullAccess 敏感权限配置

DBSS的full权限集涉及部分用户的敏感权限,比如订单支付、obs桶创建和文件上传、委托的创建及委托权限设置等。

这部分权限对用户资产影响较大,故不在系统预置权限集中添加,需通过说明文档方 式,由用户手动添加。

相关敏感权限说明如表18-3所示,权限详情如下:

"obs:bucket:CreateBucket", "obs:object:PutObject", "bss:order:pay", "iam:agencies:createAgency", "iam:permissions:grantRoleToAgency", "iam:permissions:grantRoleToAgencyOnEnterpriseProject", "iam:permissions:grantRoleToAgencyOnDomain",

"iam:permissions:grantRoleToAgencyOnProject"

表 18-3 敏感权限说明

敏感权限项	使用场景说明	是否为 g bal bal	敏感权限规避措施
obs:bucket:Create Bucket	 agent在CCE场景部署 时,如果上传的obs桶不 存在,则会调用该接口 创建obs桶。上传的obs 桶名固定为:dbss-audit- agent-{project_id}, project_id为当前实例所 在的项目id。 备份和风险导出功能场 景,如果选择的桶不存 在,则会创建obs桶。 	是	 如不涉及权限使用场景,可以不配置该权限。 如涉及,可以提前使用有权限的账号创建要使用的obs桶即可。
obs:object:PutObje ct	agent在CCE场景部署时, 将实例配置信息上传到obs 桶。	是	 如不涉及权限使用场景,可以不配置该权限。 如需使用,必须配置该权限才能将实例信息正常导出,无规避措施。
iam:agencies:creat eAgency iam:permissions:gr antRoleToAgency iam:permissions:gr antRoleToAgency OnEnterpriseProje ct iam:permissions:gr antRoleToAgency OnDomain iam:permissions:gr antRoleToAgency OnProject	 备份和风险导出场景, 创建名为 "dbss_depend_obs_trus t"的委托并对其授予obs 操作相关权限。 dws免agent场景,dws 会创建名为 "DWSAccessLTS"的委 托,并对其授予访问ts 的权限,用于将审计日 志上传到租户的lts中。 dbss会创建名为 "dbss_dws_lts_trust"的 委托,并对其授予lts访 问权限,用于后续从lts 下载审计日志。 	是	 如不涉及权限使用场景,可以不配置该权限。 使用有权限的账号开启该功能。
uss:order:pay	支付。	Ĥ	 如不涉及权限使用场 景,可以不配置该权 限。 使用有权限的账号提前 购买实例。