

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



HUAWEI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：<https://www.huaweicloud.com/>

目录

1 总览	1
2 开通并使用数据库安全审计（安装 Agent）	4
2.1 流程指引.....	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）.....	29
2.5.3 安装 Agent（Windows 操作系统）.....	33
2.6 步骤四：添加安全组规则.....	40
2.7 步骤五：开启数据库安全审计.....	42
3 开通并使用数据库安全审计（免安装 Agent）	44
3.1 流程指引.....	44
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.....	78
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.....	91
5.2 步骤二：登录实例 web 控制台.....	96
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.....	98
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.....	100
5.3.3 自定义策略阻断举例.....	103
5.3.4 客户端语句过滤白名单配置举例.....	107
5.3.5 虚拟补丁防护配置举例.....	112
5.3.6 业务字典配置举例.....	114
5.3.7 Web 安全客户端配置举例.....	118
5.3.8 工单审批配置举例.....	122
6 升级数据库审计实例版本.....	130
7 配置审计规则.....	131
7.1 添加审计范围.....	131
7.2 添加 SQL 注入规则.....	133
7.3 管理 SQL 注入规则.....	135
7.4 添加风险操作.....	139
7.5 配置隐私数据保护规则.....	142
7.6 SQL 白名单.....	145
7.6.1 添加 SQL 白名单.....	145
7.6.2 管理 SQL 白名单.....	146
8 查看审计结果.....	148
8.1 查看 SQL 语句详细信息.....	148
8.2 查看会话分布.....	151
8.3 查看审计总览信息.....	152
8.4 查看审计报告.....	155
8.5 查看趋势分析.....	160
9 通知设置管理.....	163
9.1 设置邮件通知.....	163
9.2 设置告警通知.....	164
10 查看监控信息.....	167
10.1 查看系统监控信息.....	167
10.2 查看告警信息.....	168
11 备份和恢复数据库审计日志.....	171
12 其他操作.....	178
12.1 管理数据库安全审计实例.....	178
12.2 查看实例概览信息.....	180
12.3 管理添加的数据库和 Agent.....	182
12.4 卸载 Agent.....	184
12.5 管理审计范围.....	185
12.6 查看 SQL 注入检测信息.....	187
12.7 管理风险操作.....	188
12.8 管理隐私数据保护规则.....	190
12.9 管理审计报告.....	192

12.10 管理备份的审计日志.....	194
12.11 查看操作日志.....	195
13 云审计服务支持的关键操作.....	197
13.1 如何查看云审计日志.....	197
13.2 云审计服务支持的 DBSS 操作列表.....	198
14 监控.....	199
14.1 DBSS 监控指标说明.....	199
14.2 设置监控告警规则.....	201
14.3 查看监控指标.....	202
15 共享 VPC.....	204
16 数据库安全加密管理.....	209
16.1 数据库安全加密实例管理.....	209
16.2 系统管理员操作指导.....	212
16.2.1 平台管理.....	212
16.2.1.1 网络配置.....	212
16.2.1.2 升级系统版本.....	215
16.2.1.3 备份与恢复配置信息.....	217
16.2.1.4 查看平台信息.....	218
16.2.1.5 查看高可用信息.....	219
16.2.2 修改安全口令.....	220
16.2.3 初始化密钥.....	220
16.2.4 添加数据资产.....	222
16.2.5 业务测试和分析.....	230
16.2.6 敏感数据发现.....	233
16.2.6.1 扫描资产的敏感数据.....	233
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.....	241
16.2.6.6 新增行业模板.....	244
16.2.7 数据加密和解密.....	245
16.2.7.1 设置加密参数.....	246
16.2.7.2 查看加密算法.....	246
16.2.7.3 仿真加密测试.....	246
16.2.7.4 配置加密队列.....	248
16.2.7.5 管理授权.....	250
16.2.7.6 仿真解密测试.....	252
16.2.7.7 配置解密队列.....	253
16.2.7.8 加密表管理.....	255
16.2.7.9 回滚表结构.....	257
16.2.7.10 安装 Bypass 插件.....	258

16.2.7.11 查询应用访问记录.....	259
16.2.8 动态脱敏.....	259
16.2.8.1 新增自定义脱敏算法.....	259
16.2.8.2 创建脱敏规则.....	261
16.2.8.3 配置脱敏白名单.....	263
16.2.9 密钥管理.....	265
16.2.9.1 更新数据源密钥 DSK.....	265
16.2.9.2 配置 KMS 对接.....	266
16.2.9.3 查看密钥信息.....	267
16.2.10 系统管理.....	267
16.2.10.1 手动创建账号.....	268
16.2.10.2 组织架构管理.....	270
16.2.10.2.1 创建组织部门.....	270
16.2.10.2.2 手动创建成员.....	271
16.2.10.3 系统运维.....	272
16.2.10.3.1 查看系统监控.....	272
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.....	275
16.2.10.4 查看消息通知.....	275
16.2.10.5 系统设置.....	275
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.....	277
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.....	279
16.4 审计管理员操作指导.....	281
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.....	283
17.1 数据库运维实例管理.....	283
17.2 系统管理员操作指南.....	286
17.2.1 首页信息.....	286
17.2.2 资产管理.....	287
17.2.2.1 添加数据资产.....	287
17.2.2.2 手动添加账号.....	291
17.2.2.3 误删恢复.....	292
17.2.3 策略防护.....	293
17.2.3.1 概述.....	293

17.2.3.2 策略设置.....	293
17.2.3.2.1 管理基本配置.....	293
17.2.3.2.2 管理集合配置.....	294
17.2.3.3 自定义策略.....	295
17.2.3.3.1 添加 SQL 策略.....	295
17.2.3.3.2 添加包过滤策略.....	300
17.2.3.3.3 启用或禁用策略.....	302
17.2.3.3.4 添加客户端语句过滤白名单.....	303
17.2.3.4 设置虚拟补丁.....	304
17.2.4 审计日志.....	306
17.2.4.1 查看审计日志信息.....	306
17.2.4.2 回放审计日志语句.....	306
17.2.4.3 添加业务字典.....	307
17.2.4.4 启用业务字典功能.....	311
17.2.5 风险管控.....	312
17.2.5.1 执行风险扫描.....	312
17.2.5.2 进行风险管理.....	316
17.2.6 报表分析.....	316
17.2.6.1 添加并生成报表.....	316
17.2.6.2 下载并查看报表.....	319
17.2.7 运维管理.....	319
17.2.7.1 审批运维工单.....	319
17.2.7.2 管理运维人员.....	320
17.2.8 设备管理.....	321
17.2.8.1 Bypass 设置.....	321
17.2.9 日志设置.....	322
17.2.9.1 配置日志保存方式.....	322
17.2.9.2 备份还原日志.....	322
17.2.9.2.1 自动备份.....	322
17.2.9.2.2 手动备份.....	323
17.2.9.2.3 还原日志.....	324
17.2.10 系统管理.....	324
17.2.10.1 查看平台信息.....	324
17.2.10.2 手动创建账号.....	325
17.2.10.3 诊断系统实时情况.....	326
17.2.10.4 升级系统版本.....	327
17.2.10.5 时间配置.....	328
17.2.10.6 查看设备状态.....	329
17.2.10.7 网络配置.....	330
17.2.10.7.1 配置网卡信息.....	330
17.2.10.7.2 配置路由信息.....	332
17.2.10.8 查看和配置消息中心.....	333

17.3 安全管理员操作指南.....	334
17.3.1 设置审批架构.....	334
17.3.2 系统管理.....	336
17.3.2.1 审核账号.....	336
17.3.2.2 角色管理.....	336
17.3.2.3 启用安全配置.....	337
17.3.2.3.1 设置用户登录安全.....	337
17.3.2.3.2 设置账号密码安全.....	338
17.3.2.3.3 启用网络访问安全配置.....	338
17.4 审计管理员操作指南.....	339
17.4.1 查看操作审计日志.....	339
17.5 数据库操作员操作指南.....	340
17.5.1 发起运维工单申请.....	340
17.5.2 通过 Web 安全客户端访问资产.....	342
18 权限管理.....	344
18.1 创建用户并授权使用 DBSS.....	344
18.2 DBSS 自定义策略.....	346
18.3 DBSS 权限及授权项.....	347
18.4 FullAccess 敏感权限配置.....	348

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。


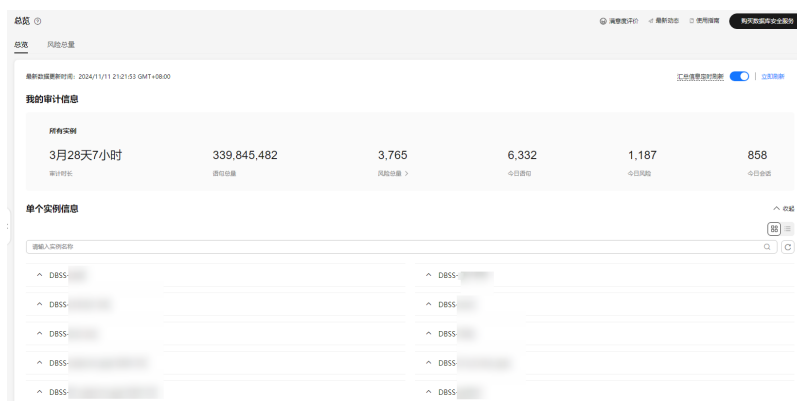
步骤2 在页面上方选择“区域”后，单击页面左上方的 ，选择“安全与合规 > 数据库安全服务”，进入数据库安全审计“总览”界面。

图 1-1 进入总览



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



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。

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。

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
MySQL	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 2008 • 2012 • 2014 • 2016 • 2017
GaussDB(for MySQL)	8.0
DWS	<ul style="list-style-type: none"> • 1.5 • 8.1
DAMENG	DM8
KINGBASE	V8
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0

数据库类型	版本
Greenplum	V6.0
HighGo	V6.0
GaussDB	<ul style="list-style-type: none">• 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)	<ul style="list-style-type: none">• 1.3.1• 2.2.3
Hive (华为云审计实例: 23.02.27.182148 及其之后的版本支持)	<ul style="list-style-type: none">• 1.2.2• 2.3.9• 3.1.2• 3.1.3
MariaDB	10.6
TDSQL	10.3.17.3.0
Vastbase	G100 V2.2
TiDB	<ul style="list-style-type: none">• 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骤

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	<p>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。</p> <p>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，请参见配置审计规则。</p>

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[无法使用数据库安全审计](#)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。

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](#)。

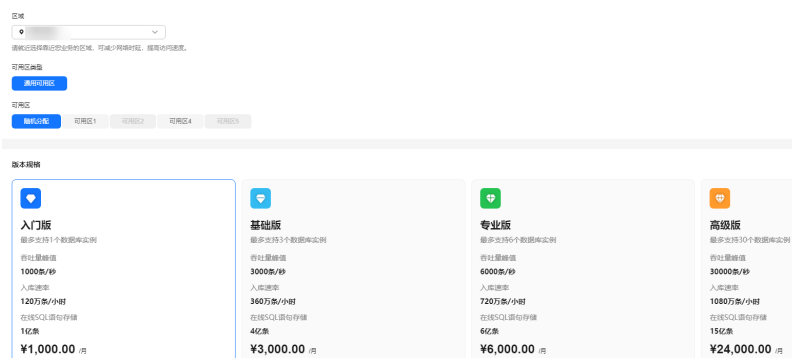
步骤2 进入[数据库安全审计购买页面](#)。

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



各版本的性能规格说明如[表2-3](#)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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 [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 [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 [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，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 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	<p>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。</p> <p>说明</p> <ul style="list-style-type: none"> 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。 <p>更多有关虚拟私有云的信息，请参见《虚拟私有云用户指南》。</p>
安全组	<p>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。</p> <p>更多有关安全组的信息，请参见《虚拟私有云用户指南》。</p>
子网	<p>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。</p>
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	<p>该参数针对企业用户使用。</p> <p>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。</p> <p>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》。</p>

参数名称	说明
标签	<p>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。</p> <p>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。</p>

步骤7 选择“购买时长”，如图2-5所示。

图 2-5 选择实例购买时长



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2-5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

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



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 00:0000:0000 0:0000:0000: 0000

参数名称	说明	取值样例
数据库类型	<p>支持的数据库类型，您可以选择以下类型：</p> <ul style="list-style-type: none"> ● 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 <p>说明</p> <ul style="list-style-type: none"> ● 当数据库类型选择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。 	MYSQL
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	<p>支持的数据库版本。</p> <ul style="list-style-type: none">当“数据库类型”选择“MySQL”时，您可以选择以下版本：<ul style="list-style-type: none">5.0、5.1、5.5、5.6、5.78.0（8.0.11及以前的子版本）8.0.308.0.358.1.08.2.0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：<ul style="list-style-type: none">11g12c19c当“数据库类型”选择“PostgreSQL”时，您可以选择以下版本：<ul style="list-style-type: none">7.48.0、8.1、8.2、8.3、8.49.0、9.1、9.2、9.3、9.4、9.5、9.610.0、10.1、10.2、10.3、10.4、10.511.012.013.014.0当“数据库类型”选择“SQLServer”时，您可以选择以下版本：<ul style="list-style-type: none">20082012201420162017当“数据库类型”选择“DWS”时，您可以选择以下版本：<ul style="list-style-type: none">1.58.1当“数据库类型”选择“GaussDB(for MySQL)”时，您可以选择以下版本：	5.0

参数名称	说明	取值样例
	<ul style="list-style-type: none"> - 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： <ul style="list-style-type: none"> - 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： <ul style="list-style-type: none"> - DM8 ● 当“数据库类型”选择“KINGBASE”时，您可以选择以下版本： <ul style="list-style-type: none"> - V8 ● 当“数据库类型”选择“HBase”时，您可以选择以下版本： <ul style="list-style-type: none"> - 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： <ul style="list-style-type: none"> - v7.0 ● 当“数据库类型”选择“GBase 8a”时，您可以选择以下版本： <ul style="list-style-type: none"> - v8.5 ● 当“数据库类型”选择“GBase XDM Cluster”时，您可以选择以下版本： <ul style="list-style-type: none"> - v8.0 ● 当“数据库类型”选择“GBase 8s”时，您可以选择以下版本： <ul style="list-style-type: none"> - v8.8 ● 当“数据库类型”选择“Greenplum”时，您可以选择以下版本： <ul style="list-style-type: none"> - v6.0 ● 当“数据库类型”选择“HighGo”时，您可以选择以下版本： <ul style="list-style-type: none"> - 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
	<ul style="list-style-type: none"> - v5.0 ● 当“数据库类型”选择“MariaDB”时，您可以选择以下版本： <ul style="list-style-type: none"> - 10.6 ● 当“数据库类型”选择“Hive”时，您可以选择以下版本： <ul style="list-style-type: none"> - 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： <ul style="list-style-type: none"> - 10.3.17.3.0 ● 当“数据库类型”选择“Vastbase”时，您可以选择以下版本： <ul style="list-style-type: none"> - G100 V2.2 ● 当“数据库类型”选择“TiDB”时，您可以选择以下版本： <ul style="list-style-type: none"> - V4 - V5 - V6 - V7 - V8 	
实例名	<p>您可以指定需要审计的数据库的实例名称。</p> <p>说明</p> <ul style="list-style-type: none"> ● 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	<p>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：</p> <ul style="list-style-type: none"> ● UTF-8 ● GBK 	UTF-8
操作系统	<p>添加的数据库运行的操作系统，您可以选择以下操作系统：</p> <ul style="list-style-type: none"> ● 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

数据库名称	选择字符集	IP地址/端口	实例名	操作系统	审计状态	Agent	操作
名称: MySQL 类型: MySQL 版本: 5.0	UTF8	3306	-	LINUX64	已启用	安装Agent 添加Agent	开启 删除

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及以上版本）
 - 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

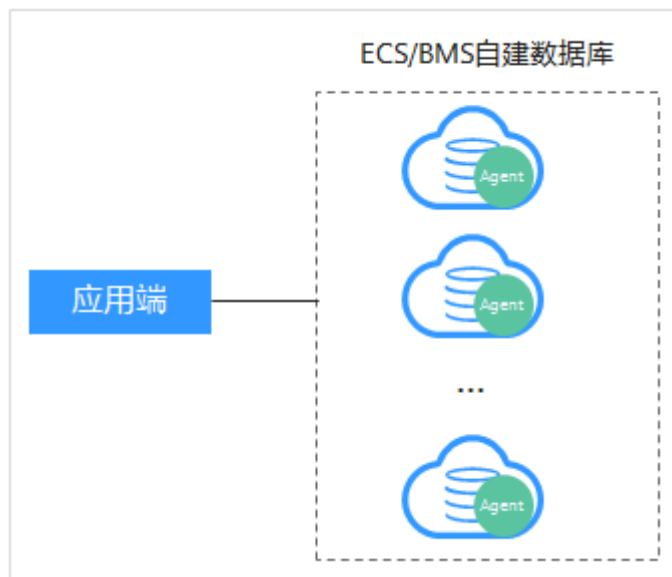
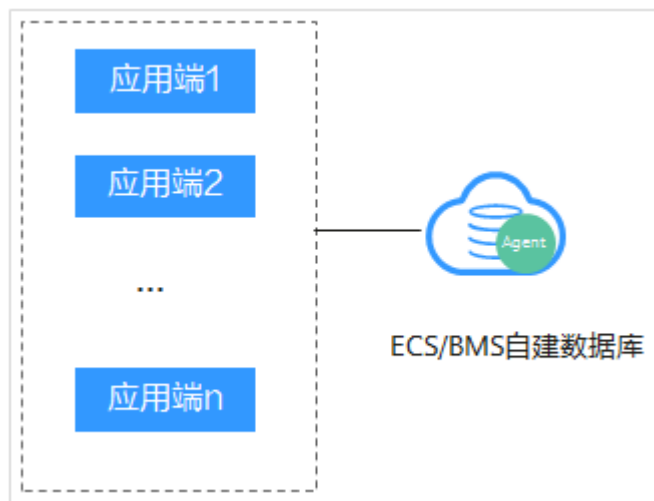


图 2-9 多个应用端连接同一个 ECS/BMS 自建数据库



- 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

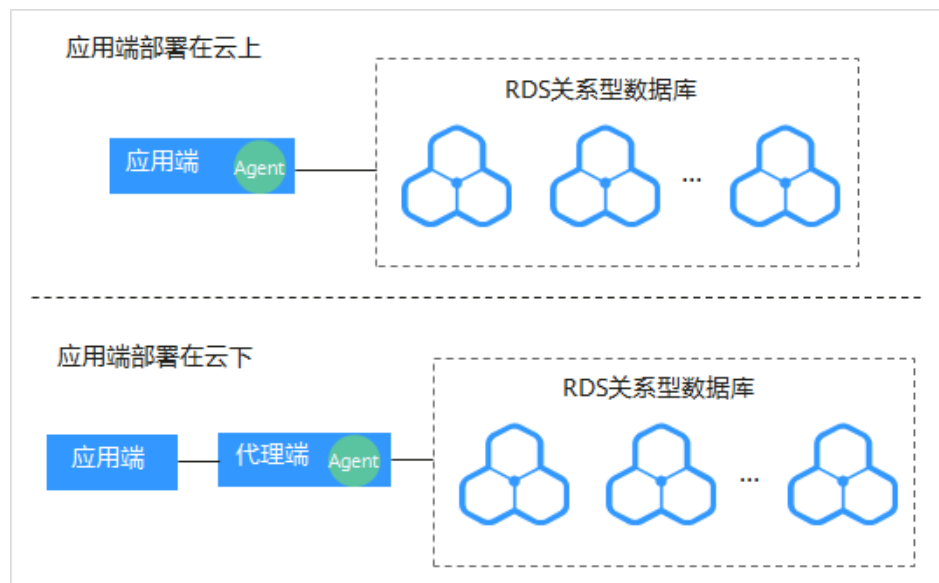
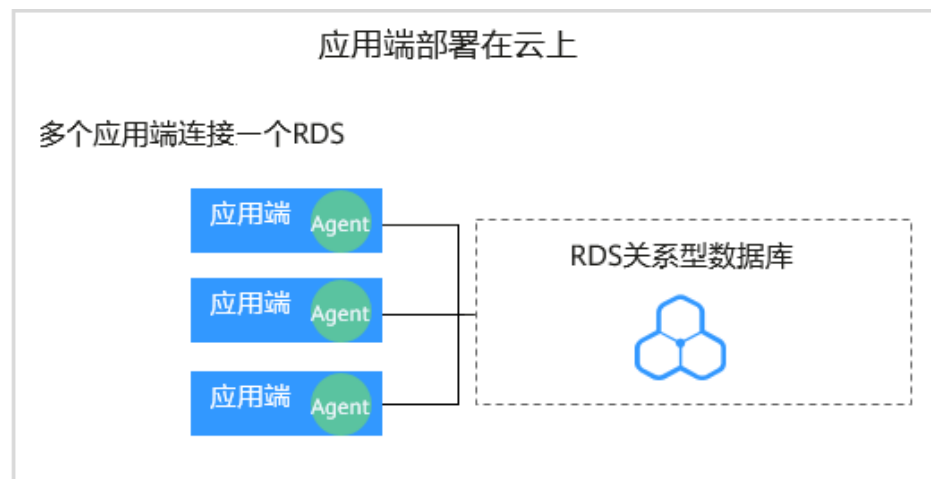


图 2-11 多个应用端连接同一个 RDS



添加Agent方式的详细说明如[表2-7](#)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](#)。


表 2-7 添加 Agent 方式说明

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。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 在应用端添加Agent。 “安装节点IP”需要配置为代理端的IP地址。

添加 Agent（ECS/BMS 自建数据库）

步骤1 请参见**步骤一**添加数据库。

步骤2 [登录管理控制台](#)。

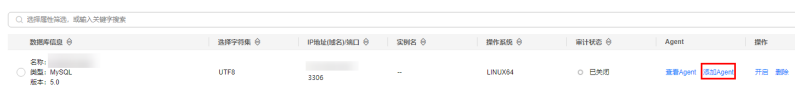
步骤3 在页面上方选择“区域”后，单击页面左上方的 ，选择“安全与合规 > 数据库安全服务 DBSS”，进入数据库安全审计“总览”界面。

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



步骤7 在弹出的“添加Agent”对话框中，选择添加方式，如图2-13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

CPU阈值(%)

内存阈值(%)

表 2-8 添加 Agent 参数说明（ECS/BMS 自建数据库）

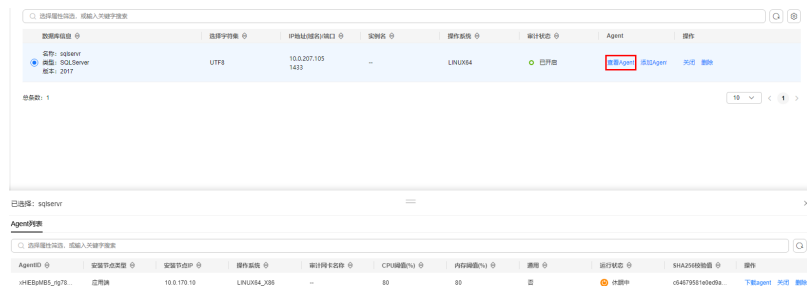
参数名称	说明	取值样例
添加方式	<p>您可以选择Agent的添加方式。</p> <ul style="list-style-type: none"> 选择已有Agent 当某个应用端连接了多个数据库时，如果该应用端的一个数据库已经添加了Agent。其他数据库在添加Agent时，只需要选择“选择已有Agent”添加方式。 创建Agent 如果待添加Agent的数据库需要创建Agent，请创建新的Agent。 	创建Agent
数据库名称	可选参数。当“添加方式”选择“选择已有Agent”时，可以选择实例下已添加Agent的数据库。	test1
Agent ID	<p>当“添加方式”选择“选择已有Agent”时，需配置该参数。</p> <p>您可以选择实例下已添加的Agent ID，Agent ID由系统自动生成。</p>	-
安装节点类型	<p>当“添加方式”选择“创建Agent”时，需配置该参数。</p> <p>审计ECS/BMS自建数据库，可以选择“数据库端”或“应用端”。</p>	数据库端

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。 IP地址必须为应用端节点的内网IP地址，支持IPv4和IPv6格式。	192.168.1.1
操作系统	当“添加方式”选择“创建Agent”时，需配置该参数。 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。	LINUX64_X86
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



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[步骤一添加数据库](#)。

步骤2 [登录管理控制台](#)。

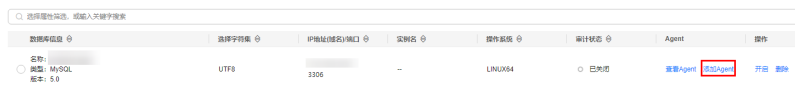
步骤3 在页面上方选择“区域”后，单击页面左上方的 ，选择“安全与合规 > 数据库安全服务 DBSS”，进入数据库安全审计“总览”界面。

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[图2-16](#)和[图2-17](#)所示，相关参数说明如[表2-9](#)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[在什么场景下需要选择“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

* Agent ID

CPU阈值(%)

内存阈值(%)

- “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Agent

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(%) 内存阈值(%)

操作系统

表 2-9 添加 Agent 参数说明（RDS 关系型数据库）

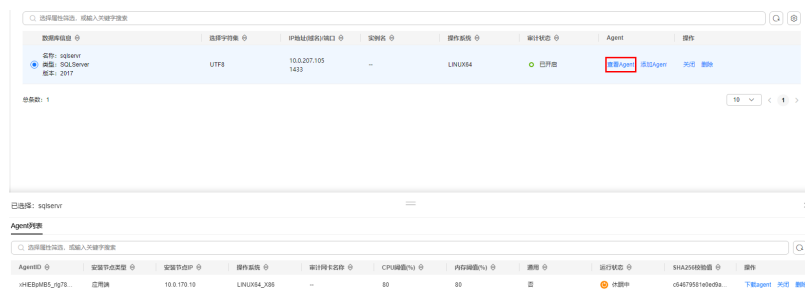
参数名称	说明	取值样例
添加方式	<p>您可以选择Agent的添加方式。</p> <ul style="list-style-type: none"> 选择已有Agent 当某个应用端连接了多个数据库时，如果该应用端的一个数据库已经在应用端添加了Agent。其他数据库在添加Agent时，只能选择“选择已有Agent”添加方式。 创建Agent 如果待添加Agent的数据库需要创建Agent，请创建新的Agent。 	创建Agent
数据库名称	可选参数。当“添加方式”选择“选择已有Agent”时，可以选择实例下已添加Agent的数据库。	tesT
Agent ID	<p>当“添加方式”选择“选择已有Agent”时，需配置该参数。</p> <p>您可以选择实例下已添加的Agent ID，Agent ID由系统自动生成。</p>	-
安装节点类型	<p>当“添加方式”选择“创建Agent”时，需配置该参数。</p> <p>审计RDS关系型数据库，只能选择“应用端”。</p>	应用端
安装节点IP	<p>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。</p> <p>IP地址必须为应用端节点的内网IP地址，支持IPv4和IPv6格式。</p> <p>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。</p>	192.168.1.1

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。 指待审计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。 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。	80
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。 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。	80
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。 指待审计的应用端节点的操作系统，可以选择“LINUX64_X86”、“LINUX64_ARM”、“WINDOWS64”。	“LINUX64_X86”

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



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](#)。

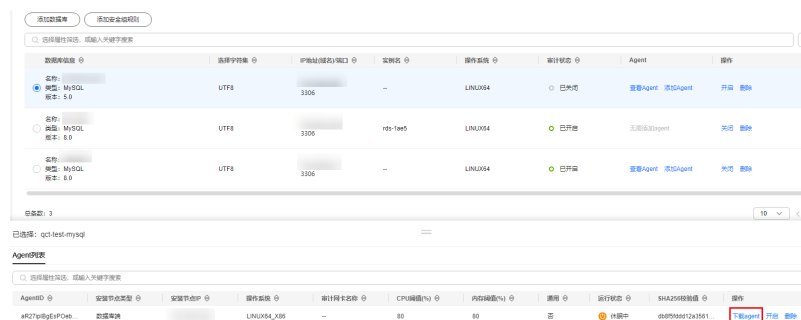
步骤3 在页面上方选择“区域”后，单击页面左上方的 ，选择“安全与合规 > 数据库安全服务 DBSS”，进入数据库安全审计“总览”界面。

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



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[安装Agent（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

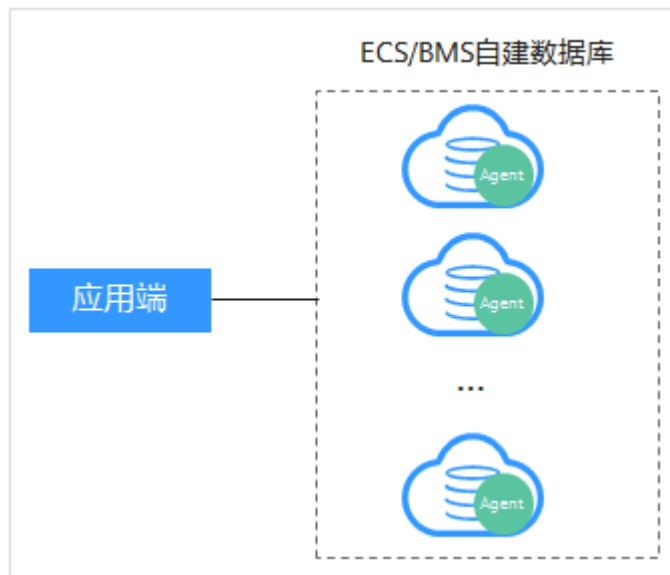
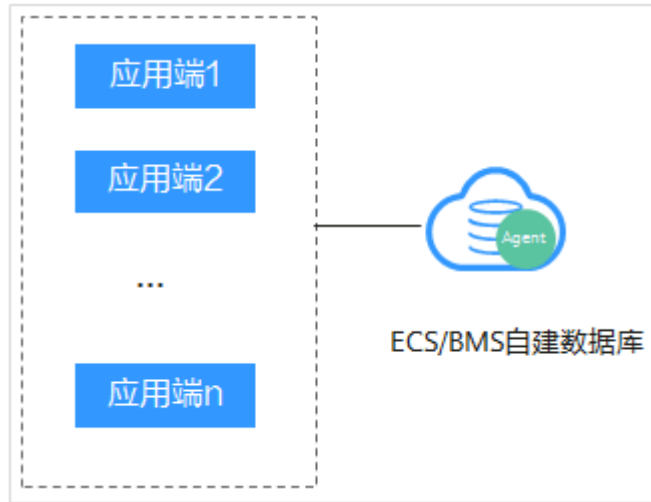


图 2-21 多个应用端连接同一个 ECS/BMS 自建数据库



- 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

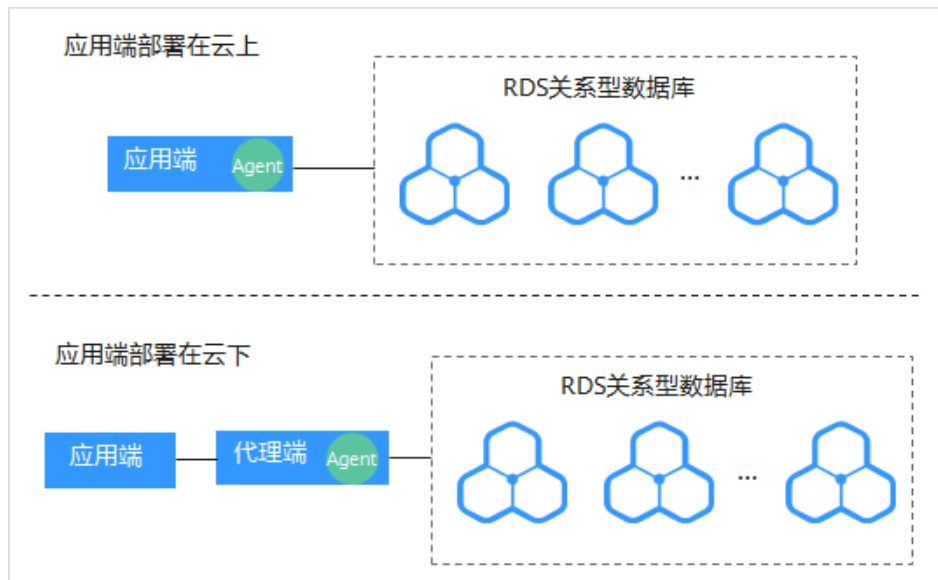
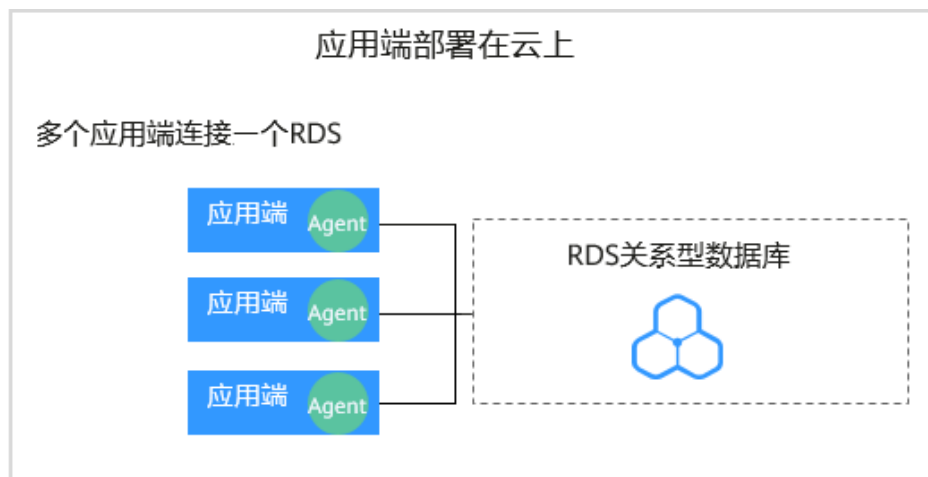


图 2-23 多个应用端连接同一个 RDS



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。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 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

```
[root@ecs-test ~]#  
[root@ecs-test ~]# cd /agent  
[root@ecs-test agent]# ll  
total 5080  
-rw-r--r-- 1 root root 5199159 Oct 25 09:47 _9syBZIsBbeAhEFqE_hhD.tar.gz  
[root@ecs-test agent]#
```

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-r--r-- 1 root root 308 Oct 25 09:45 uninstall.sh  
drwxr-xr-x 2 root root 4096 Oct 25 09:50 utils  
root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_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。

ll

- 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[步骤9](#)。

步骤9 执行以下命令，安装Agent。

sh install.sh

```
[root@ecs-test ~]# 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 : █
```

说明

- 用户系统是Ubuntu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 ~]# service audit_agent status
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[步骤二：添加Agent](#)。
- 有关卸载Agent的详细操作，请参见[卸载Agent](#)。

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[安装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

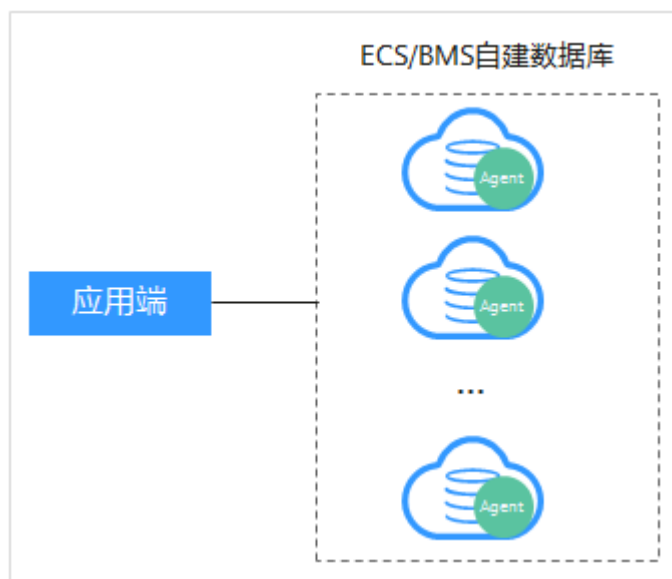
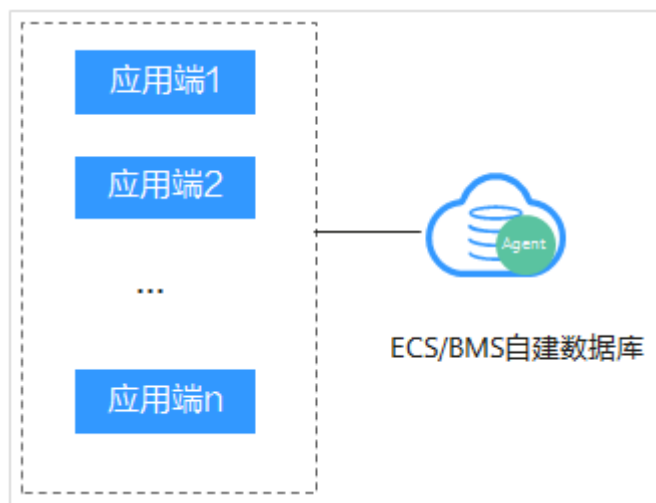


图 2-25 多个应用端连接同一个 ECS/BMS 自建数据库



- 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

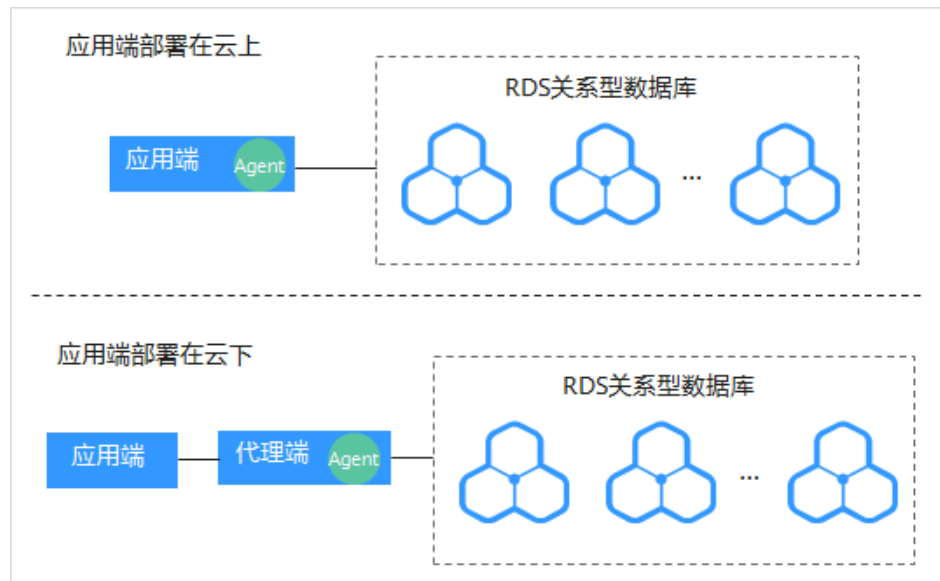
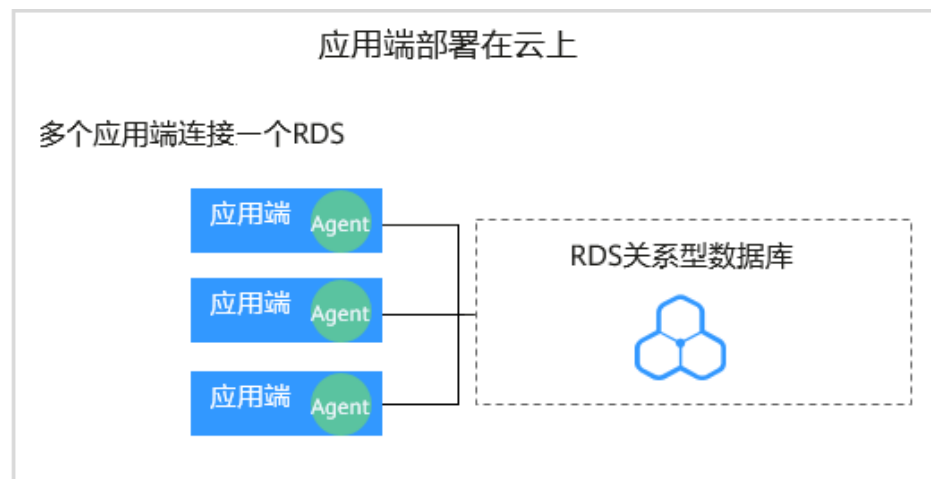


图 2-27 多个应用端连接同一个 RDS



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。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 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。

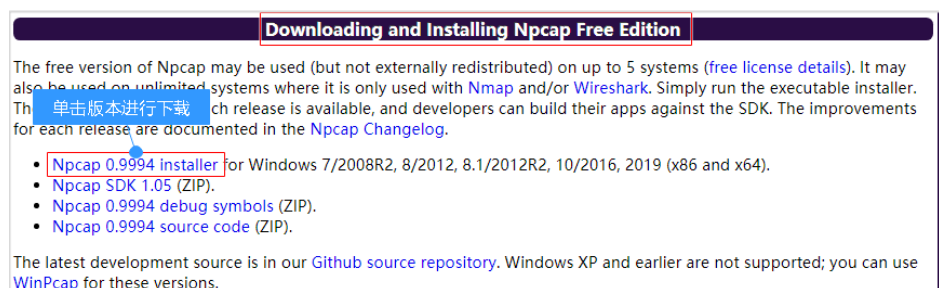
安装 Agent

步骤1 请参见步骤二添加Agent。

步骤2 在Windows主机安装“Npcap”软件。

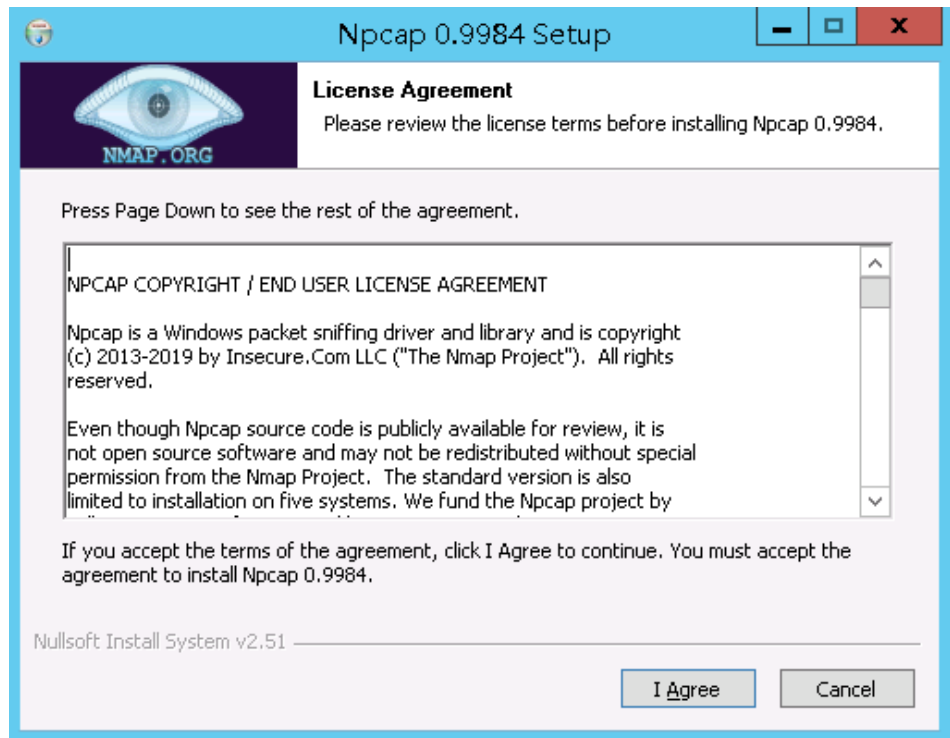
- 如果该Windows主机已安装“Npcap”，请执行步骤4。
- 如果该Windows主机未安装“Npcap”，请执行以下步骤：
 - 请前往<https://nmap.org/npcap/>下载Npcap最新软件安装包。

图 2-28 下载 npcap



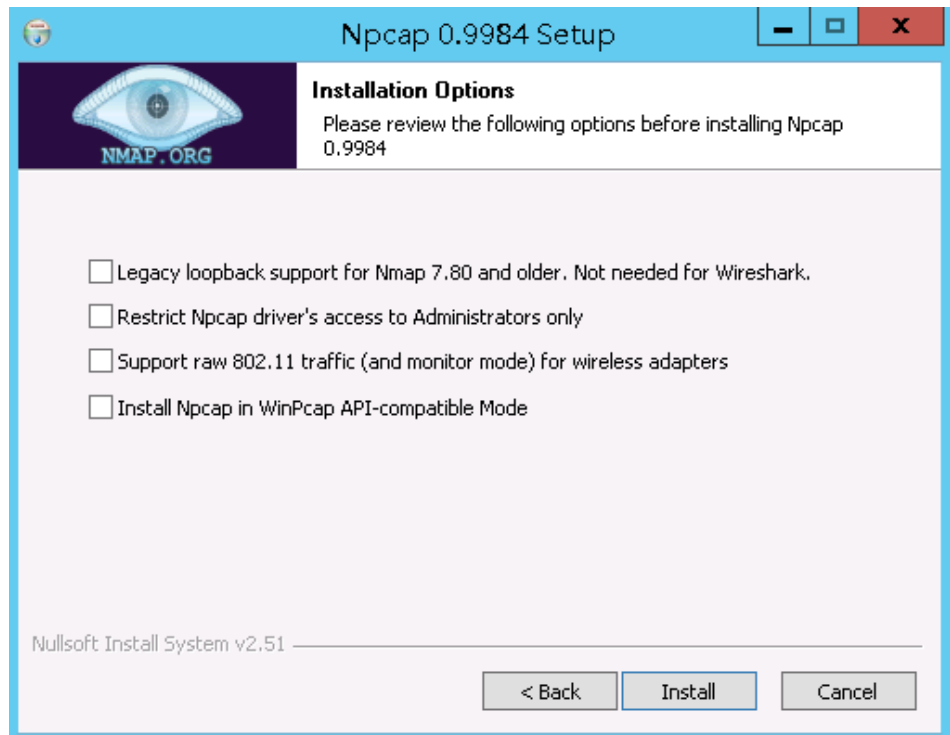
- 将下载好的npcap-xxxx.exe软件安装包上传至需要安装agent的虚拟机。
- 双击npcap软件安装包。
- 在弹出的对话框中，单击“I Agree”，如图2-29所示。

图 2-29 同意安装“Npcap”

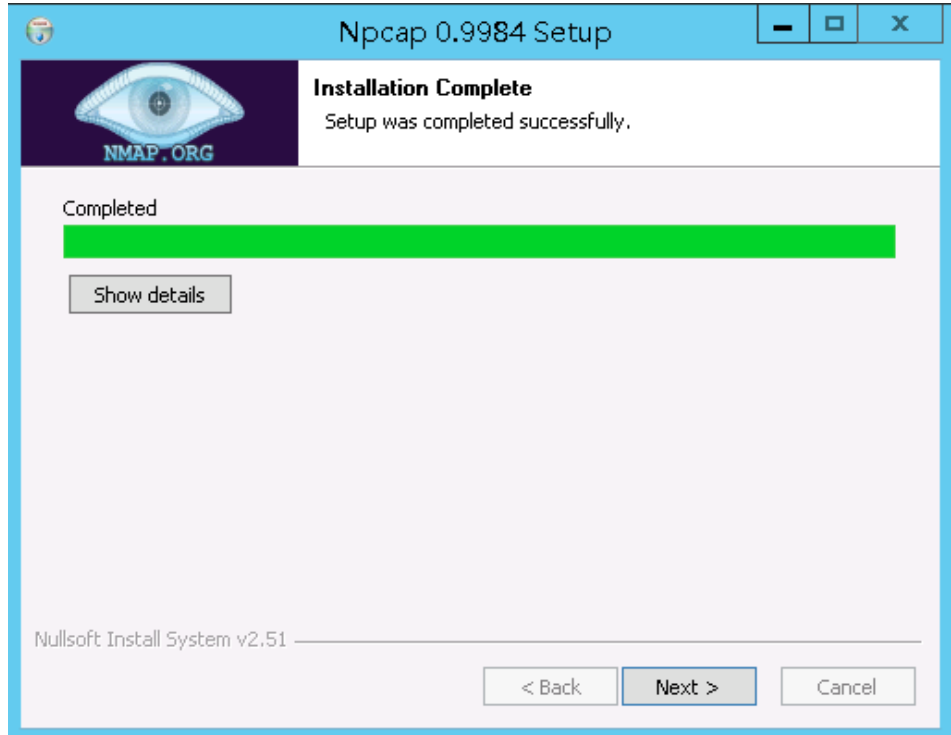


- e. 在弹出的对话框中，单击“Install”，不勾选安装选项，如图2-30所示。

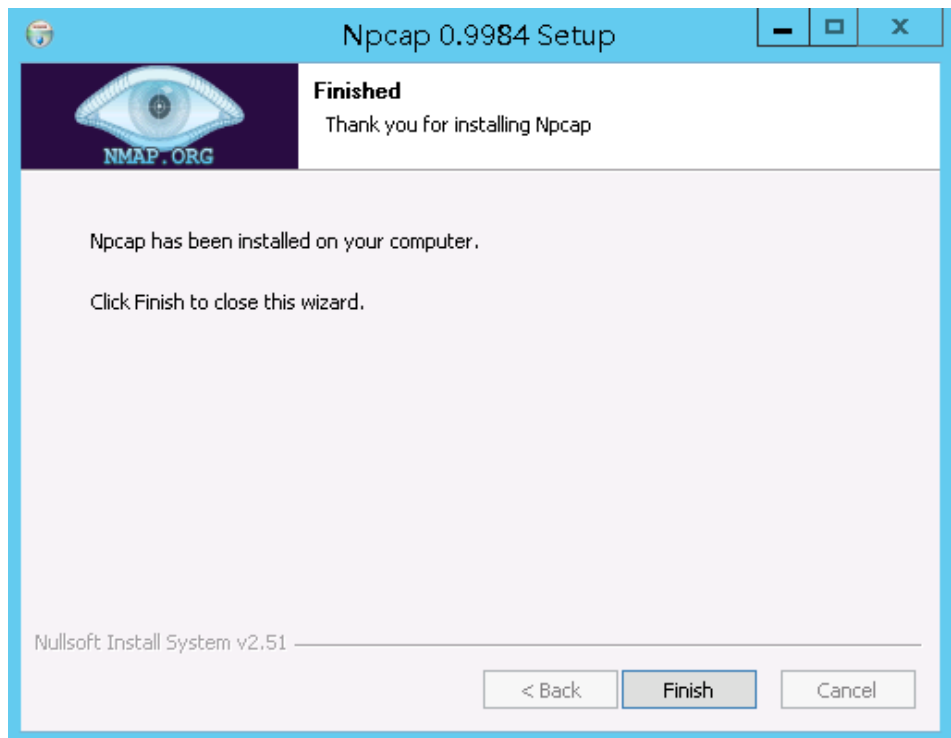
图 2-30 安装“Npcap”



- f. 在弹出的对话框中，单击“Next”。



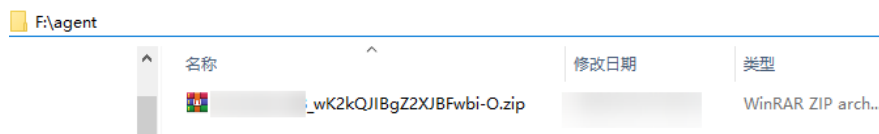
g. 单击“Finish”，完成安装。



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



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



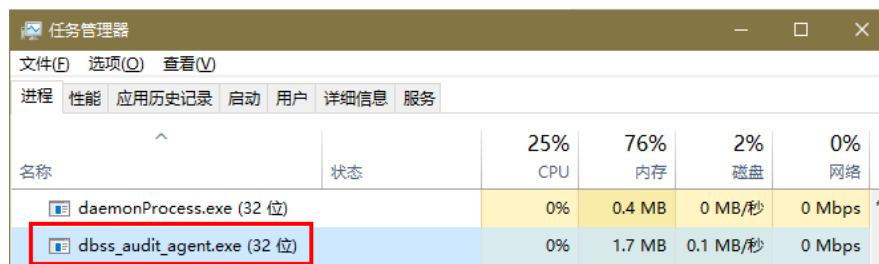
步骤7 安装成功，界面如图2-33所示，按任意键结束安装。

图 2-33 Agent 安装成功



步骤8 安装完成后，在Windows任务管理器中查看“dbss_audit_agent”进程，如下图图 2-34所示。

图 2-34 查看 dbss_audit_agent 进程



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[步骤二：添加Agent](#)。
- 有关卸载Agent的详细操作，请参见[卸载Agent](#)。
- 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接，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。

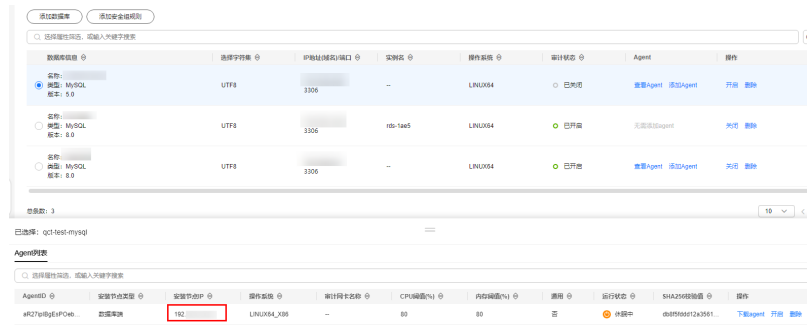
步骤4 在左侧导航树中，选择“数据库列表”，进入“数据库列表”界面。

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”。

图 2-35 安装节点 IP



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) 点击进入方向规则，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](#)

取消 前往处理

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



步骤11 选择“入方向规则”，检查安全组的入方向规则。

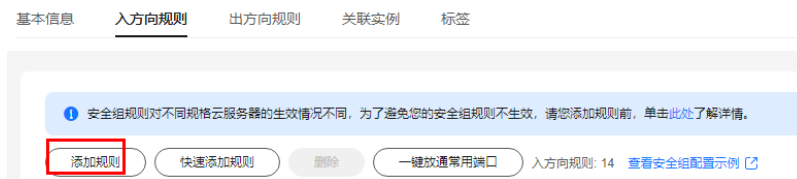
请检查该安全组的入方向规则是否已为安装节点IP配置了TCP协议（端口为8000）和UDP协议（端口为7000-7100）规则。

- 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



2. 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



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[查看审计结果](#)。

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[步骤四](#)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。

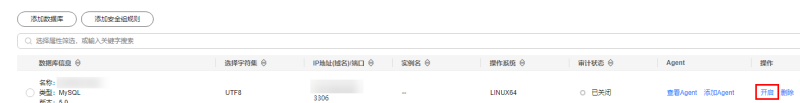
步骤5 在左侧导航栏中，选择“数据库列表”，进入“数据库列表”界面。

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 2-40 开启数据库审计功能




----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

序号	SQL语句	客户端IP	数据库IP	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	--	全审计规则	SHOW	2020/07/06 17:01:05 GMT+08:00	详情

- 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[表3-1](#)所示。

表 3-1 支持免 Agent 安装的关系型数据库

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	<ul style="list-style-type: none">• 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)	<ul style="list-style-type: none">• 8.2.0.100及以上版本
PostgreSQL (华为云审计实例：23.04.17.123301 及其之后的版本支持) 须知 当SQL语句大小超过4KB审计时会被截断，会导致审计到的SQL语句不完整。	<ul style="list-style-type: none">• 14（14.4及以上版本）• 13（13.6及以上版本）• 12（12.10及以上版本）• 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	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

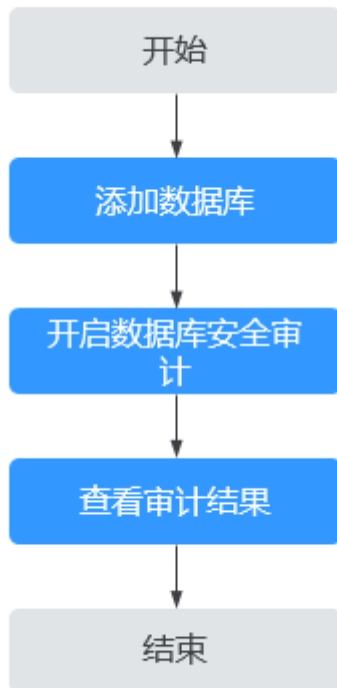


表 3-2 快速使用数据库安全审计操作步骤

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 配置审计规则 。

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](#)。

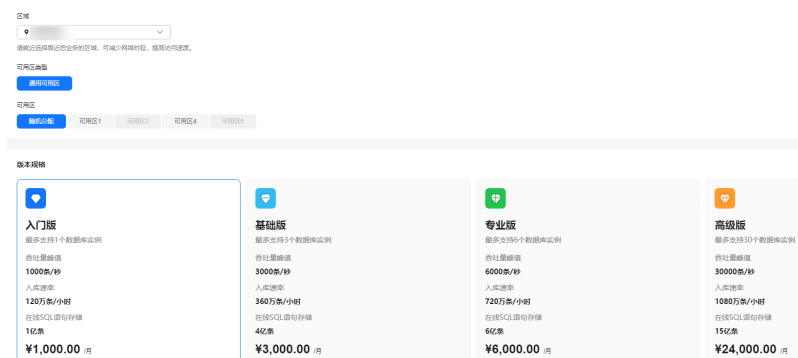
步骤2 进入[数据库安全审计购买页面](#)。

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



各版本的性能规格说明如表3-3所示。

表 3-3 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 [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 [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 [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 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 [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，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

参数名称	说明
虚拟私有云	<p>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。</p> <p>说明</p> <ul style="list-style-type: none"> 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。 <p>更多有关虚拟私有云的信息，请参见《虚拟私有云用户指南》。</p>

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《企业管理用户指南》。
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



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



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 00:0000:0000 0:0000:0000: 0000

参数名称	说明	取值样例
数据库类型	<p>支持的数据库类型，您可以选择以下类型：</p> <ul style="list-style-type: none"> ● 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 <p>说明</p> <ul style="list-style-type: none"> ● 当数据库类型选择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。 	MYSQL
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	<p>支持的数据库版本。</p> <ul style="list-style-type: none"> ● 当“数据库类型”选择“MySQL”时，您可以选择以下版本： <ul style="list-style-type: none"> - 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： <ul style="list-style-type: none"> - 11g - 12c - 19c ● 当“数据库类型”选择“PostgreSQL”时，您可以选择以下版本： <ul style="list-style-type: none"> - 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： <ul style="list-style-type: none"> - 2008 - 2012 - 2014 - 2016 - 2017 ● 当“数据库类型”选择“DWS”时，您可以选择以下版本： <ul style="list-style-type: none"> - 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： 	5.0

参数名称	说明	取值样例
	<ul style="list-style-type: none"> - 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： <ul style="list-style-type: none"> - 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： <ul style="list-style-type: none"> - DM8 ● 当“数据库类型”选择“KINGBASE”时，您可以选择以下版本： <ul style="list-style-type: none"> - V8 ● 当“数据库类型”选择“HBase”时，您可以选择以下版本： <ul style="list-style-type: none"> - 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： <ul style="list-style-type: none"> - v7.0 ● 当“数据库类型”选择“GBase 8a”时，您可以选择以下版本： <ul style="list-style-type: none"> - v8.5 ● 当“数据库类型”选择“GBase XDM Cluster”时，您可以选择以下版本： <ul style="list-style-type: none"> - v8.0 ● 当“数据库类型”选择“GBase 8s”时，您可以选择以下版本： <ul style="list-style-type: none"> - v8.8 ● 当“数据库类型”选择“Greenplum”时，您可以选择以下版本： <ul style="list-style-type: none"> - v6.0 ● 当“数据库类型”选择“HighGo”时，您可以选择以下版本： <ul style="list-style-type: none"> - 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
	<ul style="list-style-type: none"> - v5.0 ● 当“数据库类型”选择“MariaDB”时，您可以选择以下版本： <ul style="list-style-type: none"> - 10.6 ● 当“数据库类型”选择“Hive”时，您可以选择以下版本： <ul style="list-style-type: none"> - 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： <ul style="list-style-type: none"> - 10.3.17.3.0 ● 当“数据库类型”选择“Vastbase”时，您可以选择以下版本： <ul style="list-style-type: none"> - G100 V2.2 ● 当“数据库类型”选择“TiDB”时，您可以选择以下版本： <ul style="list-style-type: none"> - V4 - V5 - V6 - V7 - V8 	
实例名	<p>您可以指定需要审计的数据库的实例名称。</p> <p>说明</p> <ul style="list-style-type: none"> ● 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	<p>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：</p> <ul style="list-style-type: none"> ● UTF-8 ● GBK 	UTF-8
操作系统	<p>添加的数据库运行的操作系统，您可以选择以下操作系统：</p> <ul style="list-style-type: none"> ● 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 3-7 数据库添加完成

数据库名称	选择字符集	IP地址(端口)/端口	实例名	操作系统	审计状态	Agent	操作
名称: MySQL 版本: 5.0	UTF8	3306	-	LINUX64	已开启	安装Agent 添加Agent	开启 删除

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[查看审计结果](#)。

开启审计

步骤1 请参见[步骤三](#)安装Agent。

步骤2 请参见[步骤四](#)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


数据库名称	选择字符集	IP地址(端口)/端口	实例名	操作系统	审计状态	Agent	操作
名称: MySQL 版本: 5.0	UTF8	3306	-	LINUX64	已开启	安装Agent 添加Agent	开启 删除

----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 3-9 查看 SQL 语句

序号	SQL语句	客户端IP	数据库IP	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	--	全审计规则	SHOW	2020/07/06 17:51:05 GMT+08:00	详情

----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[提交工单](#)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”。

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，可减少网络时延，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

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

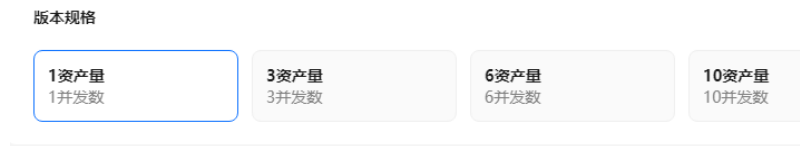


表 4-2 数据库安全加密版本性能规格说明

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	<ul style="list-style-type: none">CPU: 8U内存: 16GB	<ul style="list-style-type: none">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	<ul style="list-style-type: none">CPU: 8U内存: 16GB	<ul style="list-style-type: none">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	<ul style="list-style-type: none">CPU: 16U内存: 32GB	<ul style="list-style-type: none">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	<ul style="list-style-type: none">CPU: 16U内存: 32GB	<ul style="list-style-type: none">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 [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。

安全组

Sys-FullAccess [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IPv4地址

自动分配IP地址

弹性IP(可选)

-请选择-

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Ipv4地址	选择Ipv4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

确认密码

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： <ul style="list-style-type: none"> • 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、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



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表4-5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。
 - 选择“余额支付”。
 - 单击“确认付款”，完成购买操作。
- 申请线上合同请款后支付
 - 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。

出厂默认用户名如表1 系统默认账号信息所示，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 系统管理员操作指导 。
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 安全管理员操作指导 。
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 审计管理员操作指导 。

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。

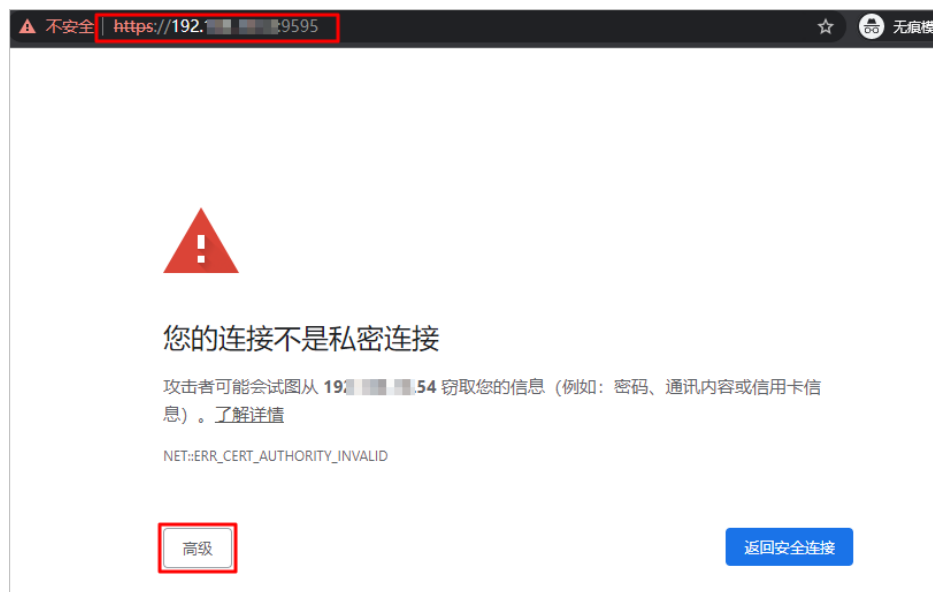
操作步骤

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。

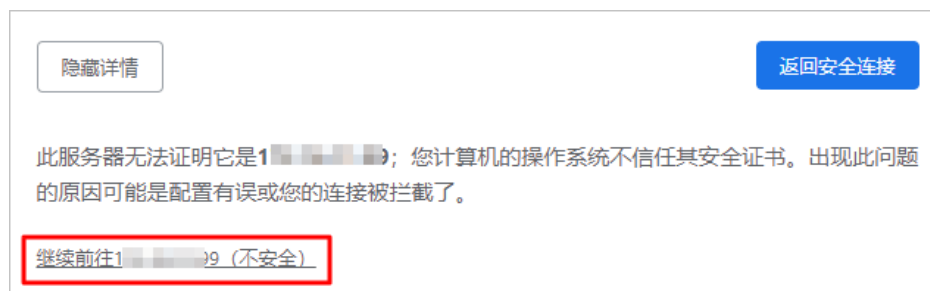
步骤2 （可选）在安全告警页面，单击“高级”。

图 4-6 安全告警



步骤3 (可选) 在详情说明中, 单击继续前往xx.xx.xx.xx (不安全)。

图 4-7 继续前往



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



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”，新密码规则如表4-7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 4-7 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： <ul style="list-style-type: none">● 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图4-9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[初始化密钥](#)。
2. 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[新增行业模板](#)和[新增自定义数据类型](#)。
4. (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](#)。
5. (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](#)。
6. (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[在结果中创建加密队列](#)。

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[配置加密队列](#)。

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[管理授权](#)。

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。

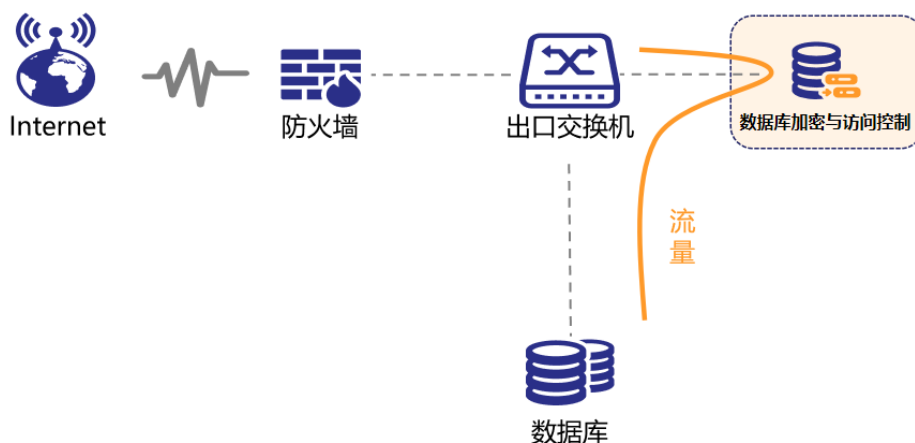
加密功能典型配置

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[图4-10](#)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”。
4. 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

添加数据源

* 数据源名称: demo

* 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

* 数据源端口: 3310

* 代理地址: eth1:172.

* 代理端口: 14099 自动分配
(范围: 1025-65535)

账号管理

* 数据库/实例名/SID/服务名/模式: doc_demo

* 数据库账号: root

* 数据库密码: *****

加密配置 >

取消 测试数据库连接 测试账号权限 测试主机连接 测试日志连接 保存

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 4-12 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。

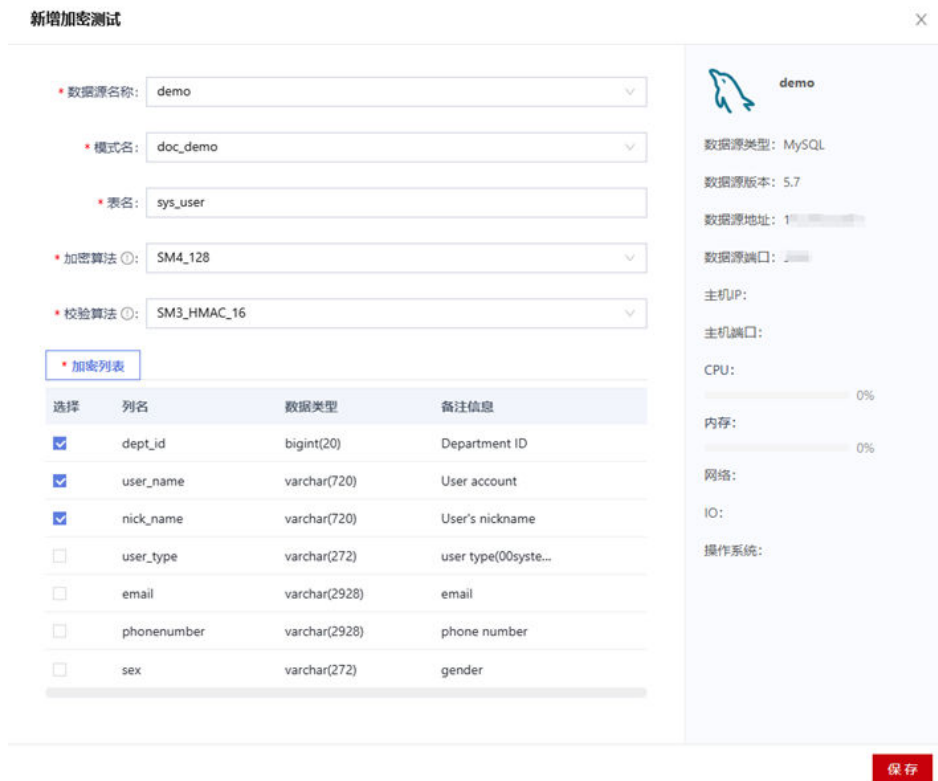
执行开始后，系统自动扫描识别敏感数据。扫描时间和需要扫描的数据量有关，数据量越多，需要扫描的时间越长，您可以在页面查看扫描进度。

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。

图 4-13 新增加密测试



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。

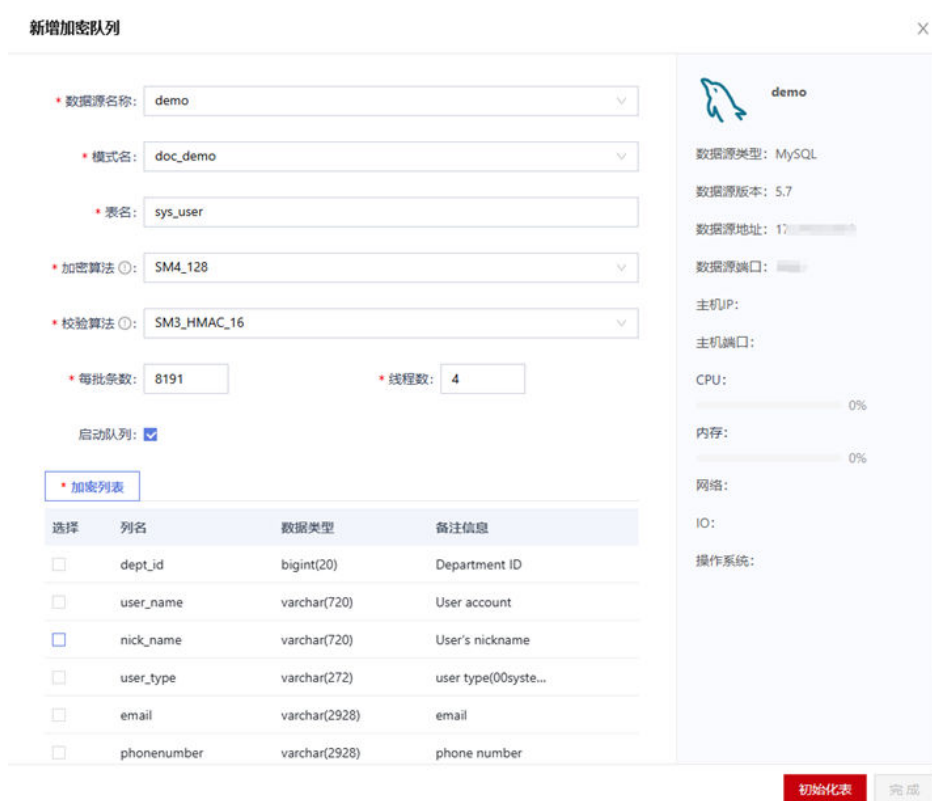
说明

- 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。

图 4-14 新增加密队列



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 4-15 客户端授权

The screenshot shows a dialog box titled "客户端授权" (Client Authorization) with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- IP范围** (IP Range): A label followed by a search icon. Below it are two input boxes. The first contains "196.168.0.100-196.168.0.120" and has a plus icon on the right. The second contains "196.168.1.100-196.168.1.120" and has minus and plus icons on the right.
- 时间点范围** (Time Range): A label followed by a search icon. Below it are two input boxes. The first contains "00" and the second contains "23".
- 星期范围** (Day Range): A label followed by a search icon. Below it are two dropdown menus. The first is set to "星期一" (Monday) and the second is set to "星期天" (Sunday).
- At the bottom right, there are three buttons: "取消" (Cancel), "清空" (Clear), and "保存" (Save).

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

- 找到目标加密数据库表，单击“用户授权”。
- 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”。

图 4-16 用户授权

The screenshot shows a dialog box titled "用户授权" (User Authorization) with a close button (X) in the top right corner. The dialog contains the following elements:

- A search input field with the placeholder text "请输入用户名" (Please enter the username) and a search icon.
- A table with two columns: "用户" (User) and "权限" (Permissions). The table lists four users: "root", "mysql.infoschema", "mysql.session", and "mysql.sys". Each user row has four checkboxes for permissions: "查询" (Query), "添加" (Add), "编辑" (Edit), and "删除" (Delete).
- At the bottom right, there are three buttons: "取消" (Cancel), "清空" (Clear), and "保存" (Save).

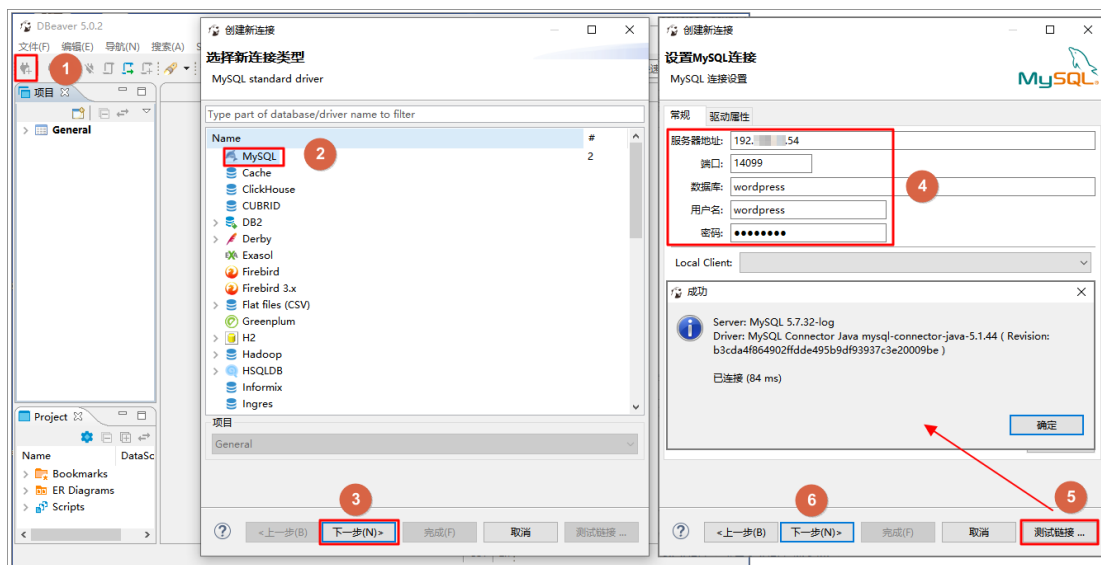
步骤六：通过代理连接数据库

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连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



1. 单击图标。
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

user_id	dept_id	user_name	nick_name	user_type	email	phonenumber	sex	avatar
1	103	admin	管理员	00	@163.com	15888888888	1	
2	105	ry	普通	00	@qq.com	15666666666	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

user_id	dept_id	user_name	nick_name	user_type	email	phonenumber	sex	avatar
1	103	admin	管理员	00	[NULL]	[NULL]	1	
2	105	ry	普通	00	[NULL]	[NULL]	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

user_id	dept_id	user_name	nick_name	user_type	email	phonenumber	sex
1	103	admin		00	[NULL]	[NULL]	1
2	105	ry		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

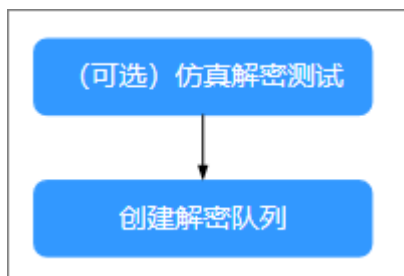
user_name	nick_name	user_type	email	phonenumber	sex
admin		00	00002F50F6A9ED206D6746551FCFC	00006C1C8EA0E32B7B3C110C	1
ry		00	00002F50F6E9AA3D206B44B0040C	00006C1C80AEED2575321F0E	1

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图4-22所示。

图 4-22 解密操作流程



1. （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](#)。
2. 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[场景一：加密操作流程及加密功能典型配置](#)。

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

新增解密测试

* 数据源名称: demo

* 模式名: doc_demo

* 表名: sys_user

* 加密算法: SM4_128

* 校验算法: SM3_HMAC_16

* 加密列表

选择	列名	数据类型	备注信息
<input type="checkbox"/>	dept_id	bigint(20)	Department ID
<input type="checkbox"/>	user_name	varchar(720)	User account
<input type="checkbox"/>	nick_name	varchar(720)	User's nickname
<input type="checkbox"/>	user_type	varchar(272)	user type(00system...
<input checked="" type="checkbox"/>	email	varchar(2928)	email
<input checked="" type="checkbox"/>	phonenumber	varchar(2928)	phone number
<input type="checkbox"/>	sex	varchar(272)	gender

demo

数据源类型: MySQL

数据源版本: 5.7

数据源地址: 1

数据源端口:

主机IP:

主机端口:

CPU: 0%

内存: 0%

网络:

IO:

操作系统:

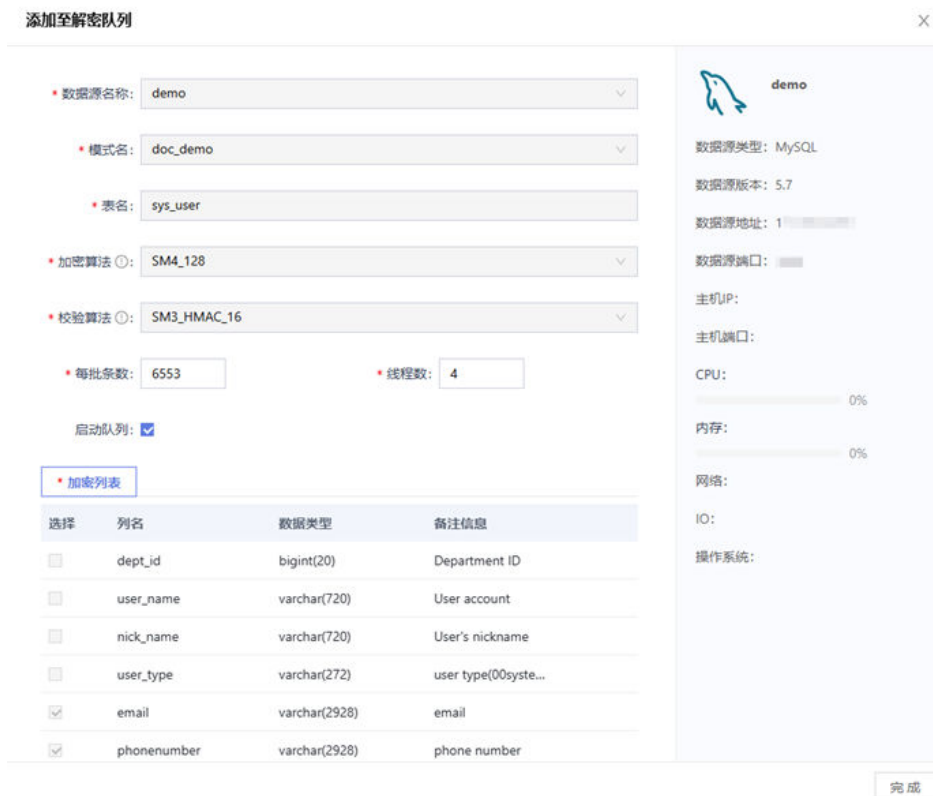
保存

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。
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。

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”。
4. 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



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，示例如下图4-25所示，表示数据库表已经恢复。

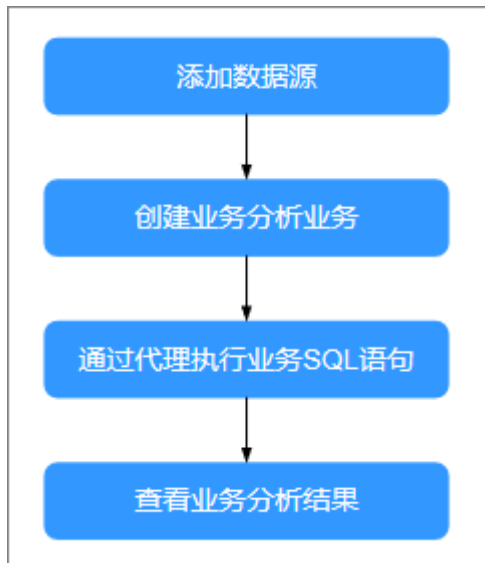
图 4-25 通过代理查询结果

	user_id	dept_id	user_name	nick_name	user_type	email	phonenumber	sex	avatar
1	1	103	admin	管理员	00	@163.com	15888888888	1	
2	2	105	ry	普通	00	@qq.com	15666666666	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，业务测试流程如图4-26所示。

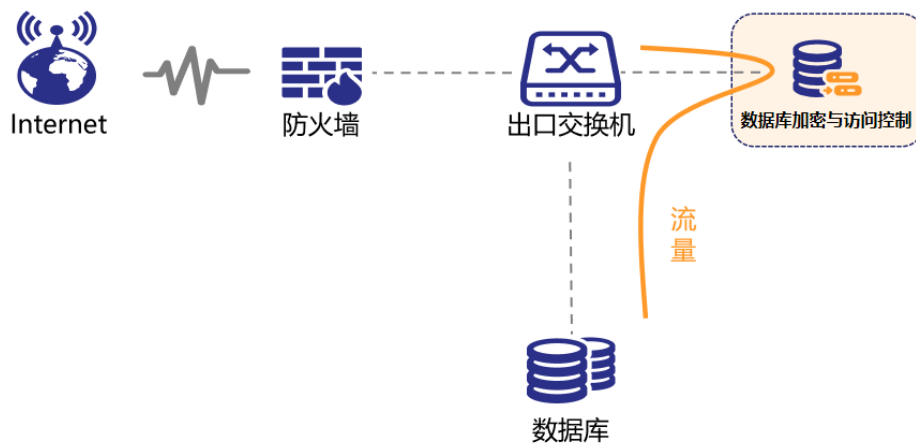
图 4-26 业务测试流程



组网说明

数据库加密与访问控制采用反向代理方式，典型组网如下图4-27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”。

- 在“添加数据源”对话框中，设置资产信息。

图 4-28 添加数据源

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。

- 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。
- 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。
- 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

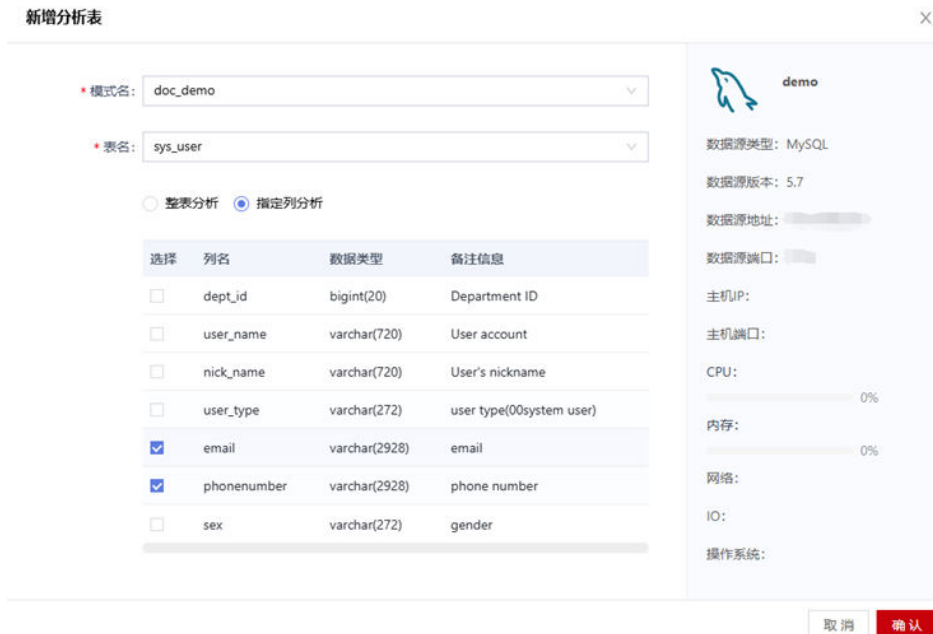
在加密之前，创建业务分析任务，测试业务SQL是否支持。


- 使用sysadmin用户[登录实例Web控制台](#)。
- 在左侧导航栏，选择“业务测试 > 业务分析”。
- 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

- 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



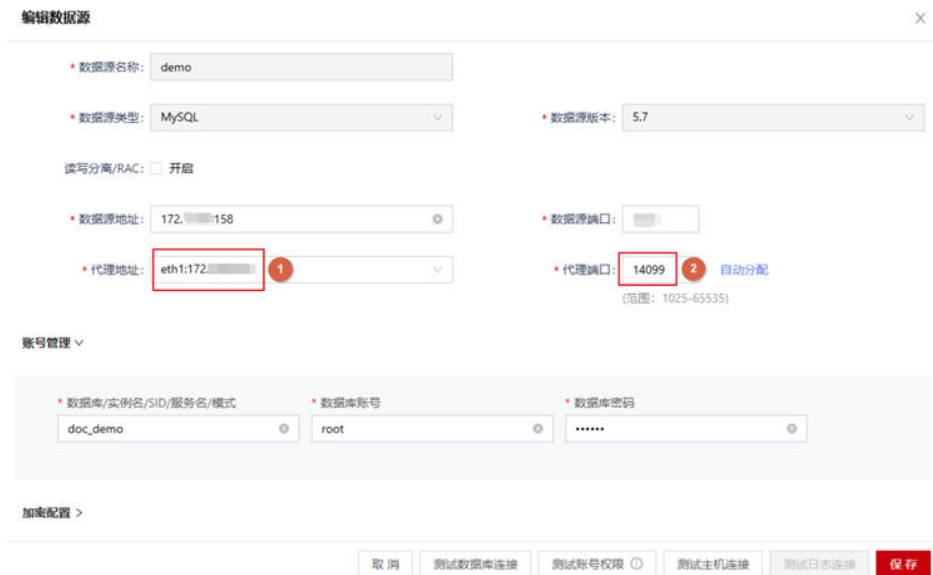
找到目标表格，单击启动按钮。

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](#)。
2. 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



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



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

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=DBBeaver ...

5. 查看阻断的SQL语句和系统建议。

图 4-34 阻断 SQL 语句

模式名	表名	分析列	状态	异常记录	分析	操作
doc_demo	sys_user	email.phonenumber	分析中	1		查看日志

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

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

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

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

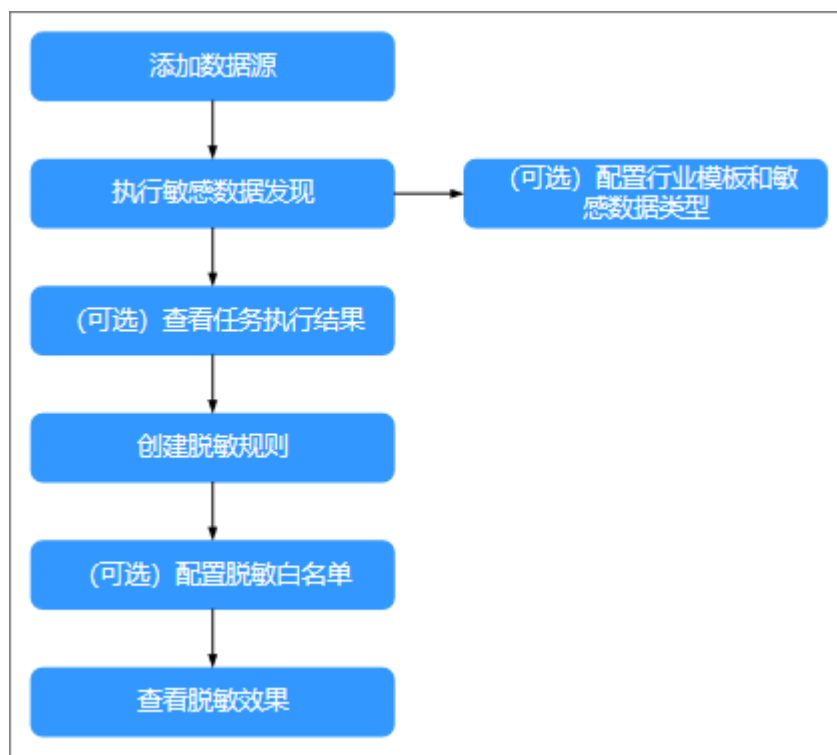
业务测试结果表明此数据库表如果加密的话将影响业务的SQL语句运行，所以不建议对此数据库表进行加密操作。

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，动态脱敏流程如图4-37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[添加数据资产](#)。
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[新增行业模板](#)和[新增自定义数据类型](#)。
3. 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](#)。
4. （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[在结果中创建脱敏规则](#)。

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”。
4. 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 4-38 添加数据源

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. 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

添加脱敏规则

* 规则名称: 脱敏demo

* 模式名: doc_demo

* 表名: sys_user

* 脱敏列表

列名	数据类型	命中率	脱敏算法 ①
phone	手机号码	100%	部分遮蔽
tel	固定电话号码	100%	部分遮蔽

取消 保存

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”。

图 4-41 添加白名单

添加白名单 ×

数据源: demo

数据库用户名:

IP范围 ⓘ: ⓘ ⓘ

授权开始时间: ⓘ

授权结束时间: ⓘ

放行规则: 全部规则 指定规则

支持配置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。

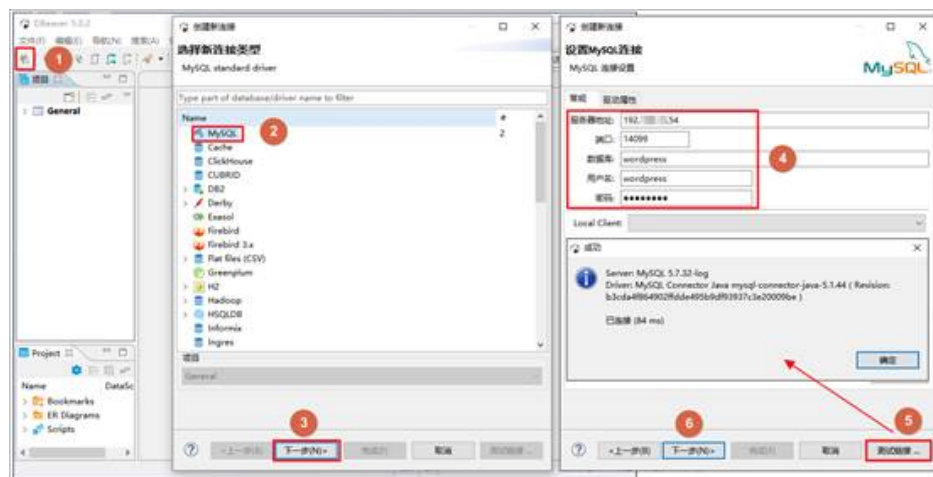
步骤五：通过代理连接数据库

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连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 4-42 通过代理连接数据库



1. 单击 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
1	158****8628	0571*****500	[blurred]
2	183****8185	0571*****500	[blurred]
3	170****7826	0571*****500	[blurred]

2. 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	
2	1833 88185	0571-88 2500	
3	1701 07826	0571-88 2500	

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[提交工单](#)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”。

步骤4 选填购买相关信息。

图 5-1 基础配置



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	选择购买实例的计费模式。
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

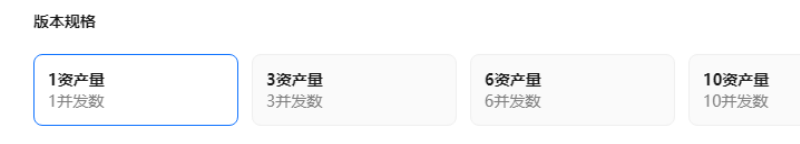


表 5-2 数据库安全运维版本性能规格说明

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	<ul style="list-style-type: none">CPU: 4U内存: 8GB	<ul style="list-style-type: none">性能: 25000QPS最大并发连接数: 3000
3资产量	最多支持3个数据库	<ul style="list-style-type: none">CPU: 4U内存: 8GB	<ul style="list-style-type: none">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	<ul style="list-style-type: none"> CPU：8U 内存：16GB 	<ul style="list-style-type: none"> 性能：35000QPS 最大并发连接数：5000
10资产量	最多支持10个数据库	<ul style="list-style-type: none"> CPU：8U 内存：16GB 	<ul style="list-style-type: none"> 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

建议VPC选择时，尽量与Agent安装节点所在VPC相同。

子网

subnet-default

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-FullAccess

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

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Ipv4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

^ 高级配置

实例名称

实例类型

主备

备注(可选)

登录信息

用户名

sysadmin

登录密码

确认密码

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： <ul style="list-style-type: none"> • 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、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



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表5-5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。
 - 选择“余额支付”。
 - 单击“确认付款”，完成购买操作。
- 申请线上合同请款后支付
 - 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。

表 5-6 权限说明

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 系统管理员操作指南 。
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。 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 安全管理员操作指南 。
audadmin	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 审计管理员操作指南 。
datadmin	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 数据库操作员操作指南 。

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>。

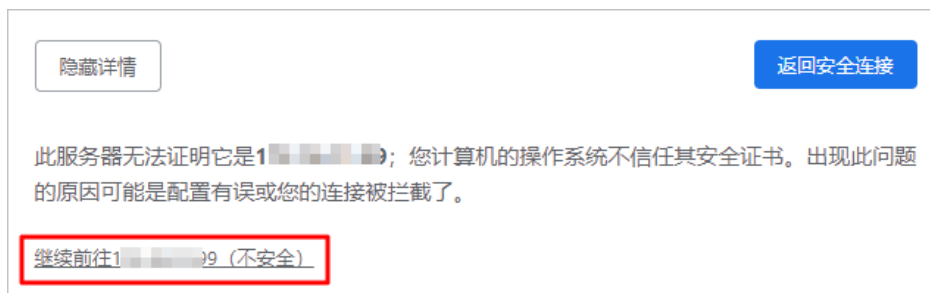
步骤2 （可选）在安全告警页面，单击“高级”。

图 5-6 安全告警



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

图 5-7 进入登录页面



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

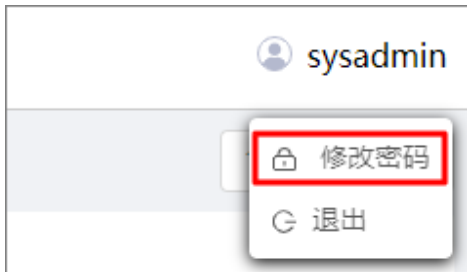
初次登录系统，您需要修改默认密码。具体操作请参见[修改登录密码](#)。

----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



步骤2 在修改密码对话框中，修改密码并单击“确定”。

表 5-7 参数说明

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： <ul style="list-style-type: none">• 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。

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

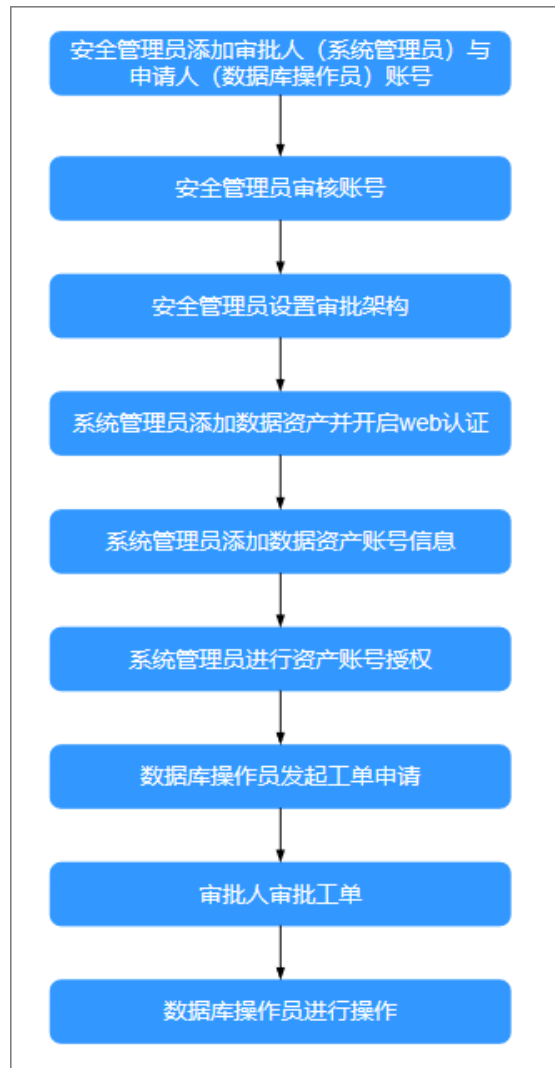
5.3 步骤三：系统功能配置及使用场景举例

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，流程如图5-9所示。

图 5-9 运维人员操作管理流程

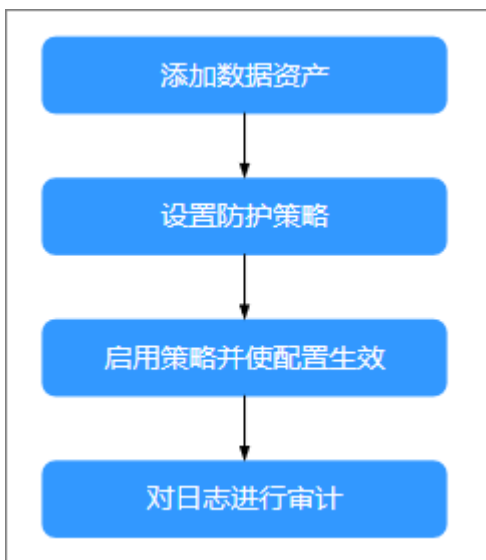


1. 安全管理员需先添加审批人（系统管理员）与申请人（数据库操作员）账号。具体说明请参见[手动创建账号](#)。
2. 新增的账号需先经安全管理员审核通过。具体说明请参见[审核账号](#)。
3. 安全管理员设置审批架构，设置审批人与申请人。具体说明请参见[设置审批架构](#)。
4. 系统管理员需给目标资产开启Web认证，以便后续能给数据库操作员进行资产认证授权。具体说明请参见[添加数据资产](#)。
5. 系统管理员添加数据资产账号信息，用于给数据库操作员资产认证授权。具体说明请参见[手动添加账号](#)。
6. 系统管理员找到目标数据库操作员，并进行资产授权操作。具体说明请参见[管理运维人员](#)。
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[审批运维工单](#)。
9. 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[图5-10](#)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[添加数据资产](#)。
2. 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](#)。
4. 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[图1 反向代理组网](#)所示。

图 5-11 反向代理组网

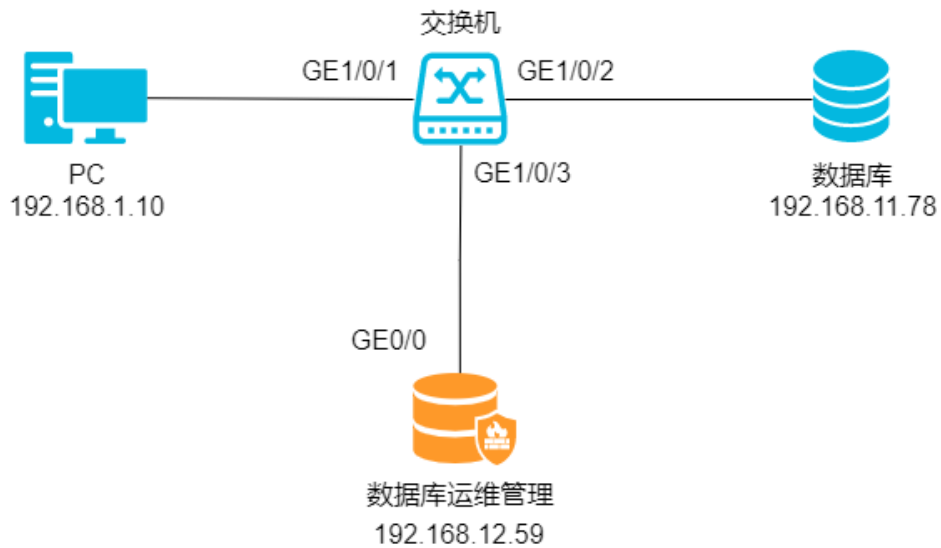


表 5-8 组网说明

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	<ul style="list-style-type: none">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



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

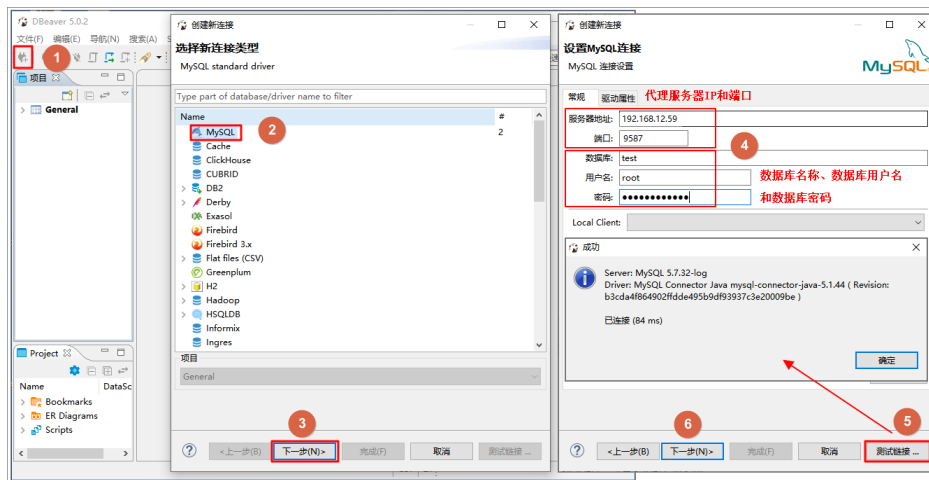
本文以“DBeaver工具”为例，通过数据库运维管理系统代理连接到数据库。

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[图4 通过代理连接数据库](#)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
...

----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

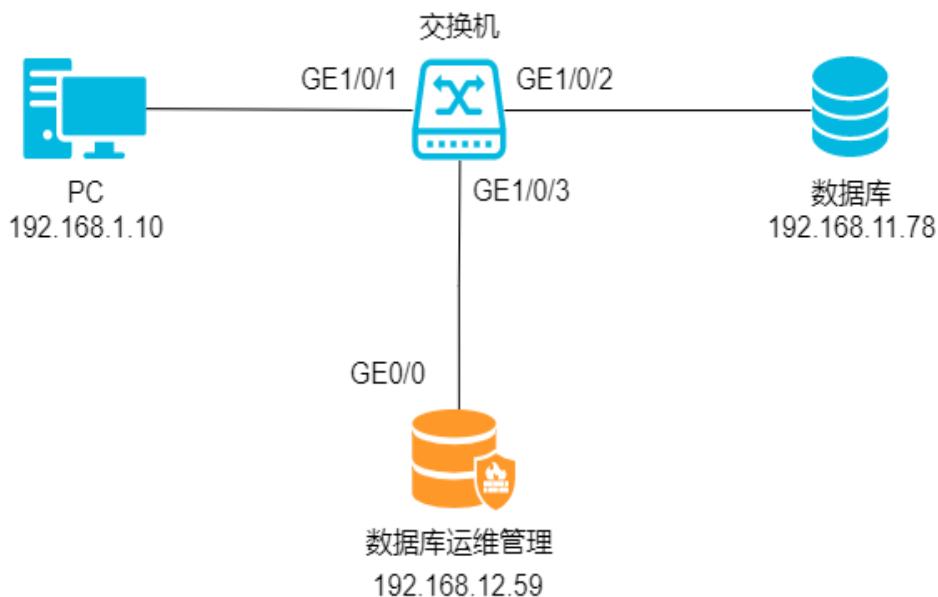


表 5-9 组网说明

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	<ul style="list-style-type: none">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: 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 确定

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

响应动作: 阻断

记录日志:

锁定时间:

资产信息(源)

资产客户端IP: 包含任意 请输入

操作系统用户: 包含任意 请输入

数据库用户组: 包含任意 请选择

资产客户端MAC: 请输入

应用用户组: 包含任意 请输入

应用用户: 包含任意 请输入

主机名: 包含任意 请输入

数据库用户: 包含任意 root x

资产客户端: 包含任意 请输入

应用客户端IP: 包含任意 请输入

时间组: 包含任意 请输入

目标信息

目标表: 包含任意 user x

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

取消 确定

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。

说明

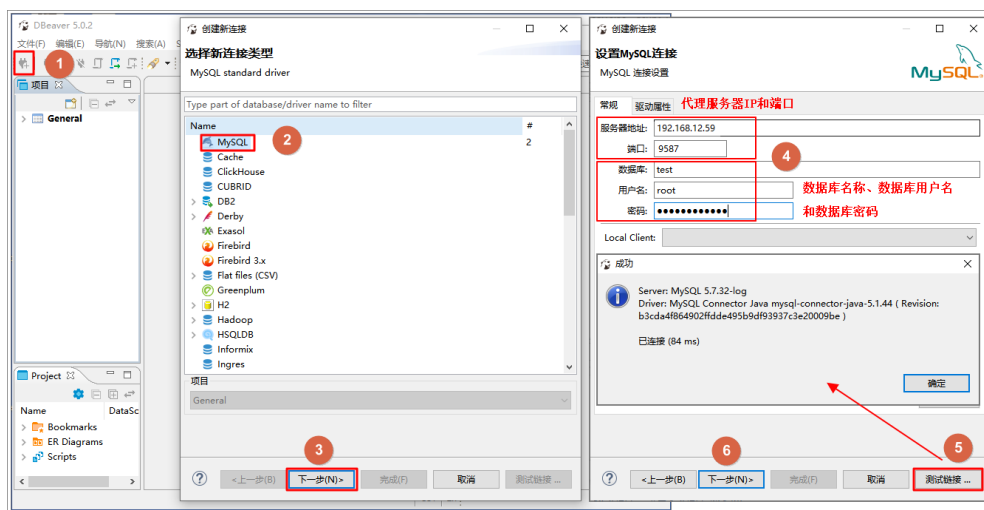
每次修改策略组，都需要在策略设置中单击策略应用，使策略修改生效。


----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 通过代理连接数据库



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”。

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。

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

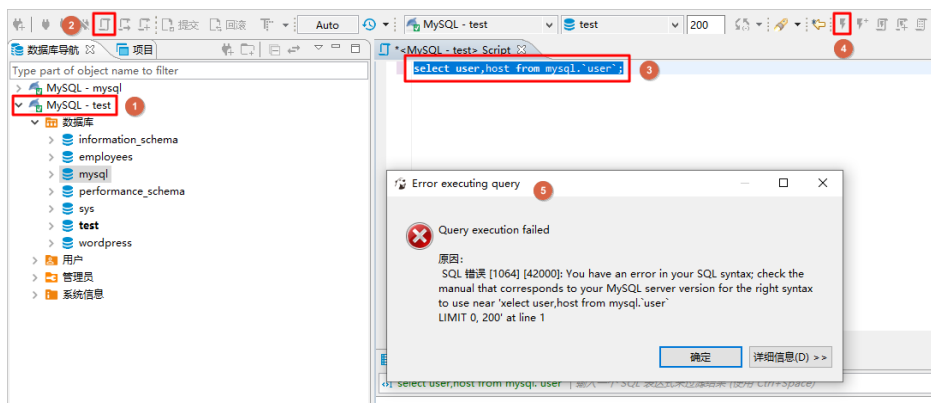
验证配置效果

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 如图5-21所示，查询操作被阻断。

图 5-21 查询 user 表及结果



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
...

----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。

本示例组网情况如图1 [反向代理组网](#)所示。

图 5-23 反向代理组网

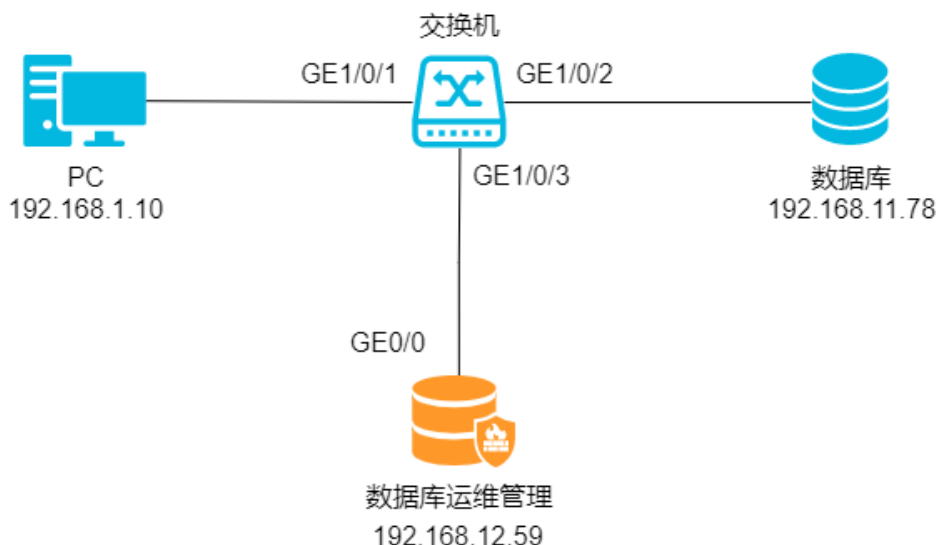


表 5-10 组网说明

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	<ul style="list-style-type: none"> 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

The screenshot shows the '添加资产' (Add Asset) dialog box with the following configuration:

- 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:
- 识别恢复配置:
- 部署模式: 反向代理
- 端口: 9587

Buttons at the bottom: 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

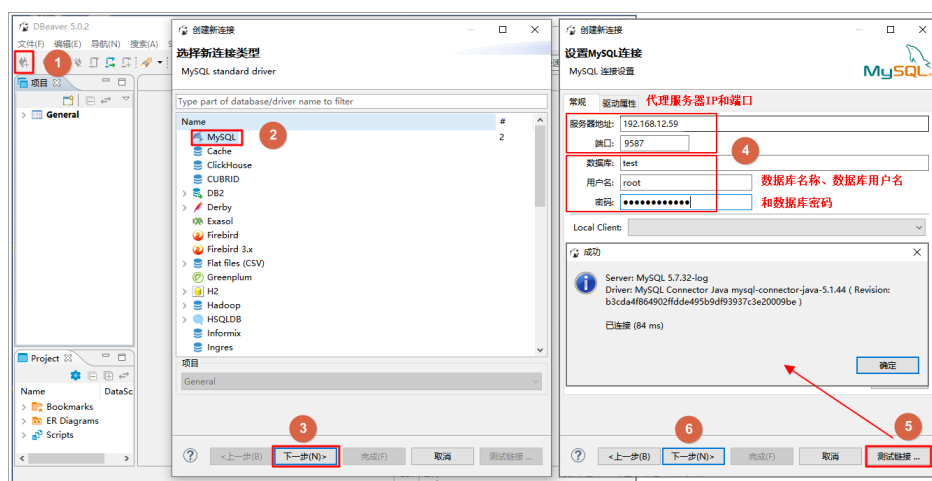
本文以“DBeaver工具”为例，通过数据库运维安全管理系统代理连接到数据库。

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[图4 通过代理连接数据库](#)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。

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内容如图5-27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



添加客户端语句过滤白名单

* SQL: SET NAMES utf8mb4

* 工具: dbeaver

数据库: MySql

状态: 启用

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

图 5-30 反向代理组网示例

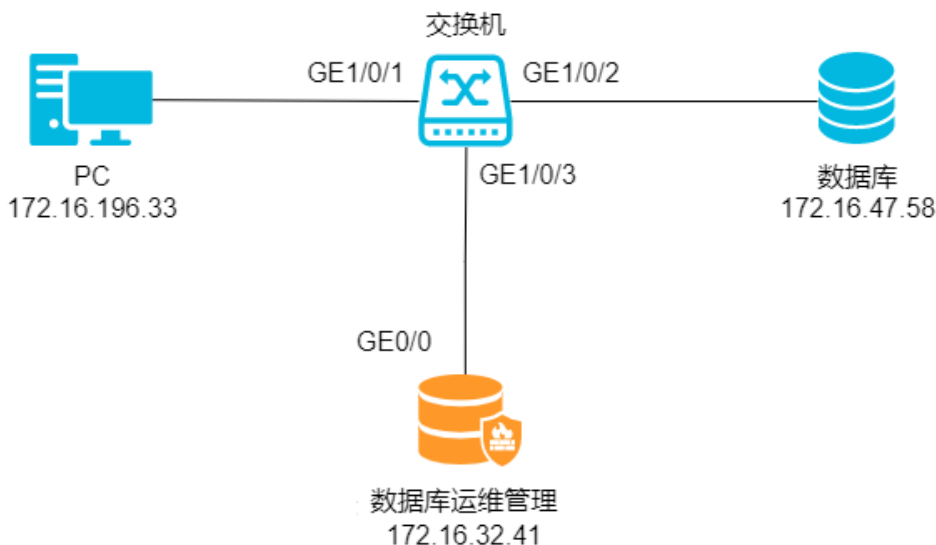


表 5-11 组网参数说明

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	<ul style="list-style-type: none"> 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

The screenshot shows a '添加资产' (Add Asset) dialog box with the following fields and options:

- 资产名称: demo
- 资产类型: Oracle
- 资产IP: 172.16.47.58
- 资产端口: 1521
- 数据库/实例名: dbrsv2
- 数据库账号: sys as sysdba
- 数据库密码: *****
- web认证:
- 设备恢复配置:
- 部署模式: 反向代理
- 端口: 9001
- RAC:

At the bottom right, there are three buttons: '测试连接' (Test Connection), '保存' (Save), and '取消' (Cancel).

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  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

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			X		
资产名称:		数据库:		数据库用户:	
数据库IP:		资产客户端:		资产客户端IP:	
资产客户端端口:		操作:		执行时长(毫秒):	
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:		操作对象:	-
匹配的策略:	入侵[SQL注入]->SYS.KUPP\$PROC包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

图 5-34 反向代理组网

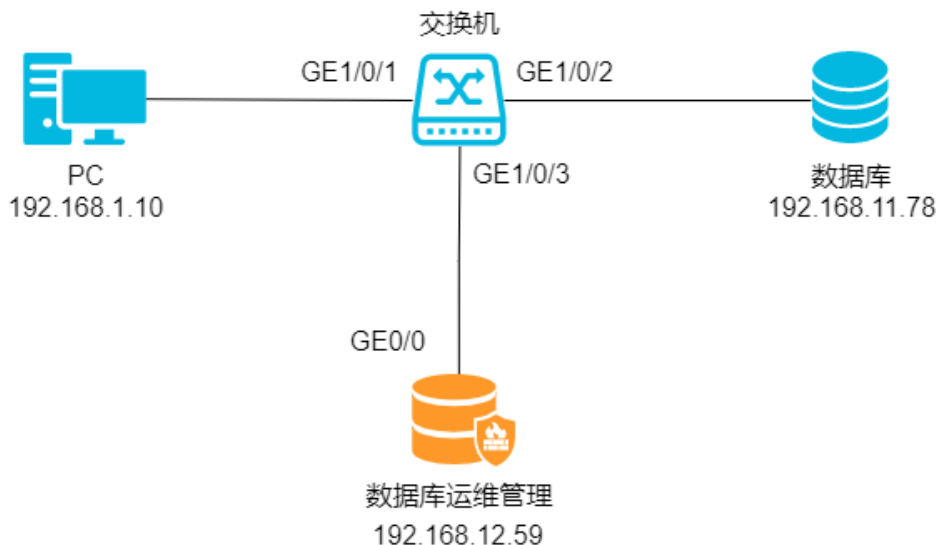


表 5-12 组网说明

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	<ul style="list-style-type: none"> 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 ×

* 资产名称: * 资产类型:

* 资产IP: * 资产端口:

* 数据库/实例名: * 数据库账号: * 数据库密码:

web认证: 识别恢复配置:

部署模式: 反向代理 * 端口:

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

----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地址: 192.168.1.10

* IP类型: 客户端IP

* 业务名称: 测试部门


状态:

取消 确定

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

* 操作: SELECT

* 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



----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(172.16.47.58)	全部审计	无风险	SHOW	网站数据库(172.16.47.58)	2021-11-16 16:22:52
root	测试部门(172.16.47.58)	全部审计	无风险	查询(SELECT)	网站数据库(172.16.47.58)	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	数据库用户: SYS
数据库IP:	网站数据库(172.16.47.58)	资产客户端IP: 测试部门(172.16.47.58)
资产客户端端口:	42744	资产客户端MAC: 00-00-00-00-00-00
操作:	查询(SELECT)	数据库MAC: 00-00-00-00-00-00
	执行时长(毫秒): 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

图 5-43 反向代理组网

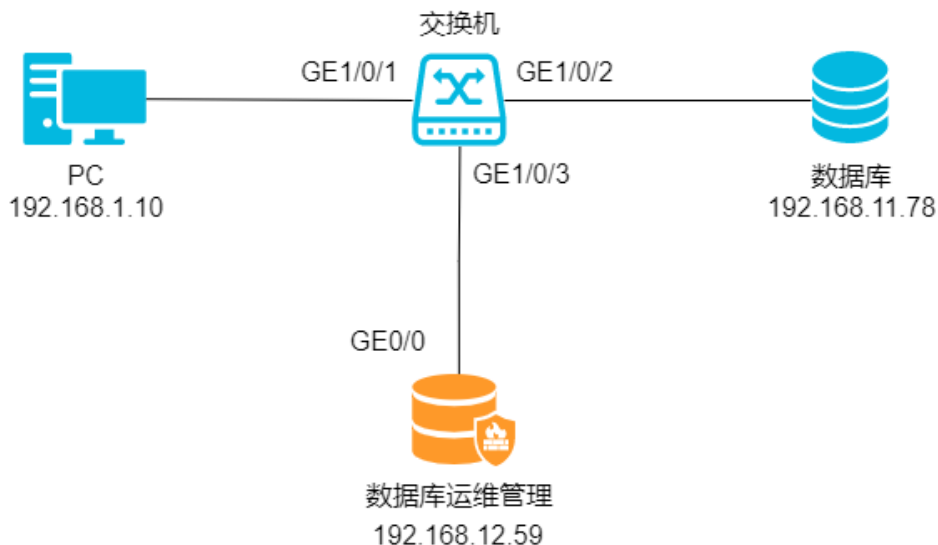


表 5-13 组网说明

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	<ul style="list-style-type: none"> 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

The screenshot shows the '添加资产' (Add Asset) dialog box with the following configuration:

- 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:
- 识别恢复配置:
- 部署模式: 反向代理
- 端口: 9587

Buttons at the bottom: 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

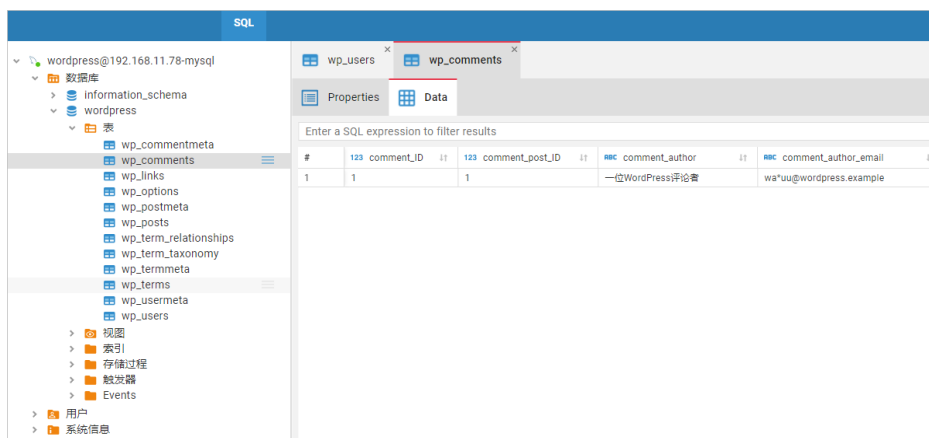


步骤2 使用数据库操作员账号（例如datadmin）登录数据库运维管理系统。

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



- 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



----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

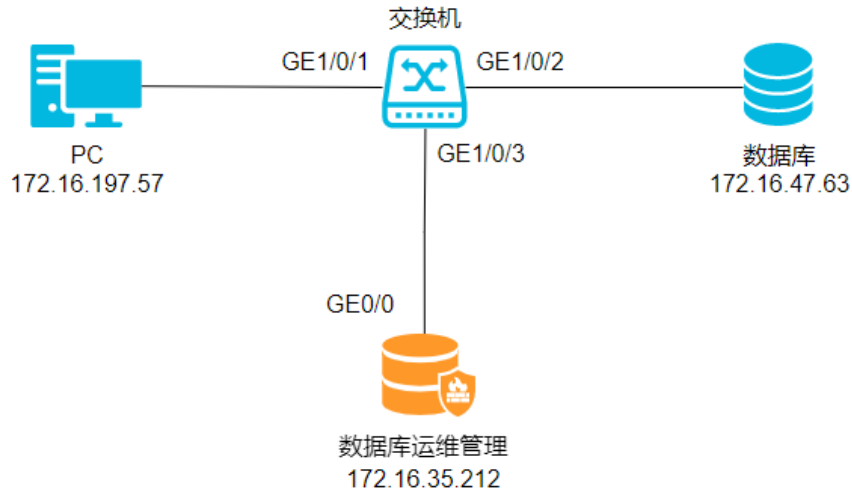


表 5-14 组网说明

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	<ul style="list-style-type: none">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

The screenshot shows a '添加资产' (Add Asset) dialog box. It includes the following fields and controls:

- Asset Name: mysql_172.16.47.63
- Asset Type: MySQL
- Asset IP: 172.16.47.63
- Asset Port: 6003
- Database Instance Name: (empty)
- Database Account: (empty)
- Database Password: (empty)
- Web Authentication:
- Ignore Replication Configuration:
- Deployment Mode: 反向代理
- Port: 9018
- Buttons: 测试连接 (Test Connection), 保存 (Save), 取消 (Cancel)

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。

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

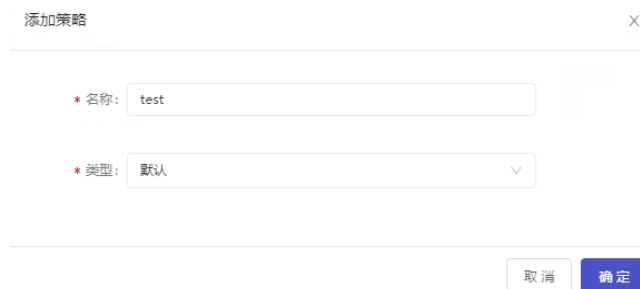


3. 创建完成后，单击策略组名称，修改策略信息，单击右上角的“保存”。

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+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



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

The screenshot shows a configuration page for a strategy. It is divided into three main sections: '策略汇总' (Strategy Summary) at the top right with '保存' (Save) and '清空' (Clear) buttons; '基本信息' (Basic Information) in the middle, containing fields for '策略名称' (Strategy Name) set to 'test', '风险等级' (Risk Level) set to '高风险' (High Risk), and '响应动作' (Response Action) set to '阻断' (Block); and '资产信息(源)' (Asset Information) and '目标信息' (Target Information) at the bottom. The '资产信息' section includes fields for '资产客户端IP', '操作系统用户', '数据库用户组', '资产客户端MAC', '应用用户组', and '应用用户'. The '目标信息' section includes fields for '目标表', '影响行数', '表组', '数据库', and '字段'. Several dropdown menus are present, many with '包含任意' (Include any) selected. The '策略名称' and '风险等级' fields are highlighted with a red box in the original image.

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。

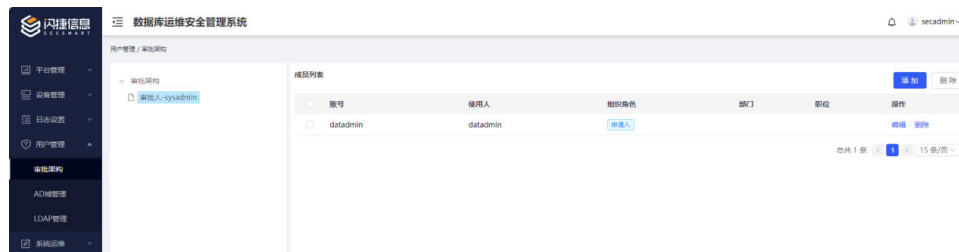
步骤4 在添加成员信息弹框填写信息。

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



----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

发起审批

* 申请名称:

* 资产名称: 数据库实例名:

客户端工具: 客户端IP:

是否开启授权码: * 申请操作时间:

申请事由: 备注:

<input type="checkbox"/>	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
<input type="checkbox"/>	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:

* 审批意见:

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



	id	prefecture	Home_return_permit	Sex	National	county
1	1	和静县	M92386054	男	京族	资阳
2	2	甘德县	M48107235	女	德昂族	龙岩
3	3	昌江黎族自治县	M57036298	男	朝鲜族	黑河
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县	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	常德
11	11	乌拉特后旗	H56947318	女	佤族	吐鲁番
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



----结束

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。

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，如图7-1所示，相关参数说明如表7-1所示。

图 7-1 “添加审计范围”对话框

添加审计范围

* 名称

* 数据库名称

操作类型 登录 操作

数据库账户

例外IP 请输入IP/IP段，多个请以换行符相隔，不可重复(默认全审计)：

源IP 请输入IP/IP段，多个请以换行符相隔，不可重复(默认全审计)：

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)：

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。	-

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”，您可以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

* 风险等级 高 中 低 无风险

* 状态

* 正则表达式

测试正则表达式

原始数据 测试

结果

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： <ul style="list-style-type: none"> 高 中 低 无风险 	中
状态	开启或关闭当前SQL注入规则。 <ul style="list-style-type: none"> <input checked="" type="checkbox"/> : 开启 <input type="checkbox"/> : 关闭 	<input checked="" type="checkbox"/>

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。 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。	628307
结果	显示测试的结果： <ul style="list-style-type: none"> 命中 未命中 说明 <ul style="list-style-type: none"> 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。 	命中

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

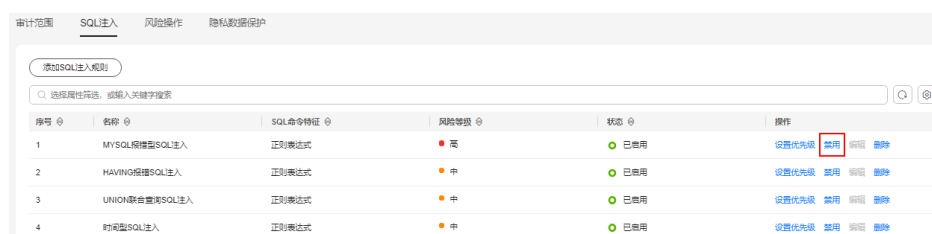
SQL注入规则默认开启，您可以根据使用需要禁用SQL注入规则。禁用SQL注入规则后，该审计规则在审计中将不生效。

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



序号	名称	SQL命令特征	风险等级	状态	操作
1	MySQL扫描型SQL注入	正则表达式	高	已禁用	设置优先级 禁用 编辑 删除
2	HAVING扫描型SQL注入	正则表达式	中	已禁用	设置优先级 禁用 编辑 删除
3	UNION联合查询SQL注入	正则表达式	中	已禁用	设置优先级 禁用 编辑 删除
4	时间型SQL注入	正则表达式	中	已禁用	设置优先级 禁用 编辑 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




序号	名称	SQL命令特征	风险等级	状态	操作
1	test40403	正则表达式	低	已禁用	设置优先级 启用 编辑 删除
2	MySQL扫描型SQL注入	正则表达式	高	已禁用	设置优先级 禁用 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”。

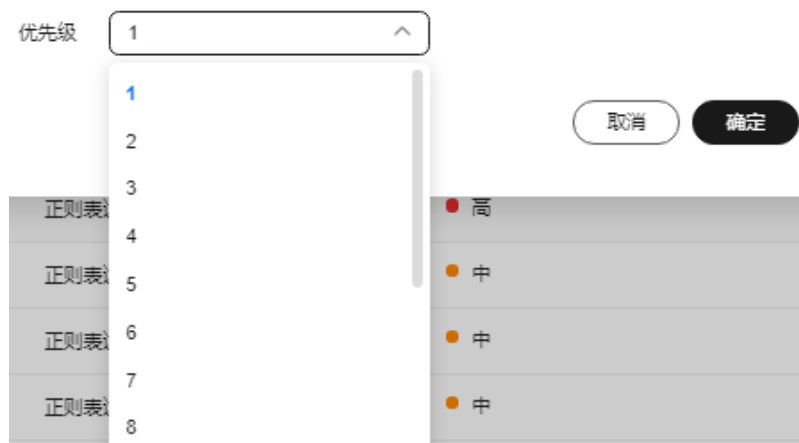
----结束

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



----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

* 风险等级 高 中 低 无风险

* 状态

* 正则表达式

测试正则表达式

原始数据 测试

结果

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： <ul style="list-style-type: none"> • 高 • 中 • 低 • 无风险 	中
状态	开启或关闭当前SQL注入规则。 <ul style="list-style-type: none"> • <input checked="" type="checkbox"/> : 开启 • <input type="checkbox"/> : 关闭 	<input checked="" type="checkbox"/>
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。 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。	628307


参数名称	参数说明	取值样例
结果	显示测试的结果： <ul style="list-style-type: none"> 命中 未命中 说明 <ul style="list-style-type: none"> 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。 	命中

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	名称	SQL命令特征	风险等级	状态	操作
1	A	正则表达式	高	已禁用	设置优先级 禁用 删除
2	MYSQL数据库SQL注入	正则表达式	高	已启用	设置优先级 禁用 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 全部数据库 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

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： <ul style="list-style-type: none"> • 高 • 中 • 低 • 无风险 	高
状态	开启或关闭风险操作。 <ul style="list-style-type: none"> •  : 开启 •  : 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。 IP地址支持IPv4（例如，192.168.1.1）和IPv6（例如，fe80:0000:0000:0000:0000:0000:0000）格式。	192.168.0.0

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

忽略大小写

序号	目标数据库	目标表	字段	操作
1	<input type="text" value="asd"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

执行结果

* 影响行数 行

* 执行时长 毫秒

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： <ul style="list-style-type: none"> • 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 。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，如图7-10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

示例 原始审计日志: alter user dba with password 'mypassword';
 当设置正则表达式为: password [""].*[""]替换值为: password ***时
 脱敏后的日志为: 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。	###

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



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。

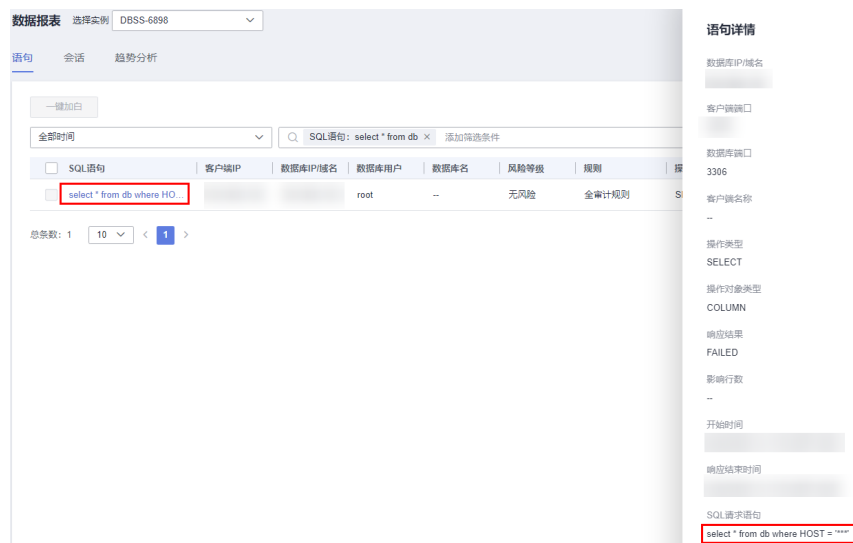
`select * from db where HOST="护照号";`

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

序号	规则名称	规则类型	正则表达式	替换值	状态	操作
1	防护等	默认	-	---	已启用	禁用 编辑 删除
2	军警证号	默认	-	---	已启用	禁用 编辑 删除
3	医保	默认	-	---	已启用	禁用 编辑 删除
4	银行卡号	默认	-	---	已启用	禁用 编辑 删除
5	身份证号	默认	-	---	已启用	禁用 编辑 删除
6	GP号簿号	默认	-	---	已启用	禁用 编辑 删除
7	test	自定义	password	---	已启用	禁用 编辑 删除

- 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

序号	规则名称	规则类型	正则表达式	替换值	状态	操作
1	防护等	默认	-	---	已启用	禁用 编辑 删除
2	军警证号	默认	-	---	已启用	禁用 编辑 删除
3	医保	默认	-	---	已启用	禁用 编辑 删除
4	银行卡号	默认	-	---	已启用	禁用 编辑 删除
5	身份证号	默认	-	---	已启用	禁用 编辑 删除
6	GP号簿号	默认	-	---	已启用	禁用 编辑 删除
7	test	自定义	password	---	已启用	禁用 编辑 删除

- 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

序号	规则名称	规则类型	正则表达式	替换值	状态	操作
1	防护等	默认	-	---	已启用	禁用 编辑 删除
2	军警证号	默认	-	---	已启用	禁用 编辑 删除
3	医保	默认	-	---	已启用	禁用 编辑 删除
4	银行卡号	默认	-	---	已启用	禁用 编辑 删除
5	身份证号	默认	-	---	已启用	禁用 编辑 删除
6	GP号簿号	默认	-	---	已启用	禁用 编辑 删除
7	test	自定义	password	---	已启用	禁用 编辑 删除

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。

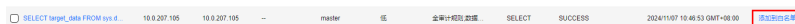
步骤4 在“选择实例”下拉列表框中，选择需要查看会话信息的实例。

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



- 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 7-17 添加 SQL 白名单

添加SQL白名单

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。
- 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”。

图 7-18 一键加白



- 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SQL白名单

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。

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。

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	客户端IP	数据库IP地址	数据库用户	数据库名	风险等级	规则	操作类型	输出结果	生成时间	操作
SET DEADLOCK_PRIORITY -10			-	master	无风险	数据库规则	SET	SUCCESS		查看详情
SELECT target_sma FROM sys.t...			-	master	无风险	数据库规则	SELECT	SUCCESS		查看详情
SET DEADLOCK_PRIORITY -10			-	master	无风险	数据库规则	SET	SUCCESS		查看详情
ALTER EVENT SESSION [name]...			-	master	无风险	数据库规则	ALTER	SUCCESS		查看详情

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，列表显示该时间段的SQL语句。

- 选择“风险等级”（“（全选）”、“高”、“中”、“低”或“无风险”），单击 ，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



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，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



----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[配置审计规则](#)。

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

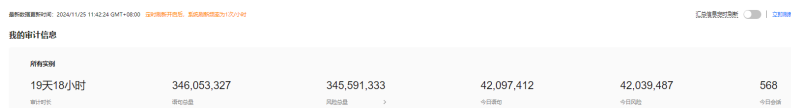
步骤1 [登录管理控制台](#)。


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



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



- 数据分析图展示



单击“”或“”，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

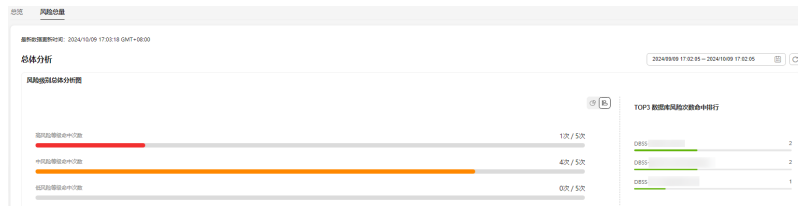


步骤4 单击上方“风险总量”，进入“风险总量”界面。单击“📅”，选择时间范围，查看指定时间段的所有数据库安全审计实例的风险分析。

- 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、中风险等级命中次数和低风险等级命中次数，另外还展示数据库风险次数命中排行TOP3。

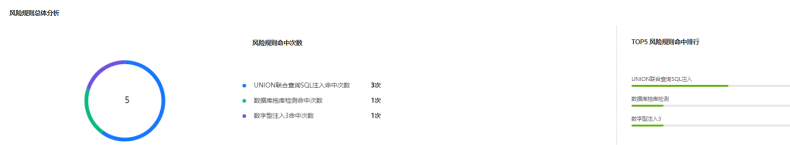
图 8-7 风险级别总体分析



- 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



- 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中风险规则的分析情况。

图 8-11 数据库统计分析



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。


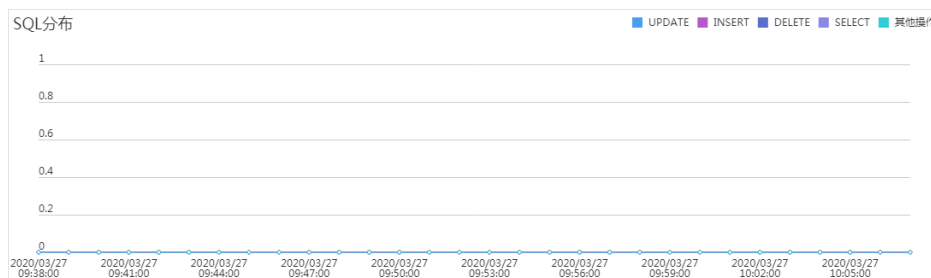
- 在“选择数据库”下拉列表框中，选择“全部数据库”或指定的数据库，可以查看实例中所有的数据库或指定的某个数据库的总览信息。
- 选择审计的时间（“近30分钟”、“近1小时”、“今日”、“近7天”或“近30天”）；或者单击 ，选择开始时间和结束时间，查看指定的时间段的总览信息。

图 8-12 SQL 分布



----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[配置审计规则](#)。

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”。

- 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。

- 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”。

图 8-13 报表模板列表



报表模板名称	关联数据库	类型	描述	计划任务状态	操作
数据库安全综合报表	全部数据库	综合报表	数据库安全综合报表	<input checked="" type="radio"/> 已开启 (每天)	设置任务 立即生成报表
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	<input type="radio"/> 已关闭 (每周)	设置任务 立即生成报表
SOX 审计跟踪报表	全部数据库	合规报表	SOX 审计跟踪报表	<input type="radio"/> 已关闭 (每周)	设置任务 立即生成报表
数据库操作事件分析报表	全部数据库	数据库事件报表	数据库操作事件分析报表	<input type="radio"/> 已关闭 (每周)	设置任务 立即生成报表
客户端操作分析报表	全部数据库	客户端事件报表	客户端操作分析报表	<input type="radio"/> 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	数据库操作事件报表	DDL 命令报表	<input type="radio"/> 已关闭 (每周)	设置任务 立即生成报表
DCL 命令报表	全部数据库	数据库操作事件报表	DCL 命令报表	<input type="radio"/> 已关闭 (每周)	设置任务 立即生成报表
DML 命令报表	全部数据库	数据库操作事件报表	DML 命令报表	<input type="radio"/> 已关闭 (每周)	设置任务 立即生成报表


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

图 8-14 “立即生成报表”对话框



立即生成报表 ✕

* 时间范围 


* 数据库

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。

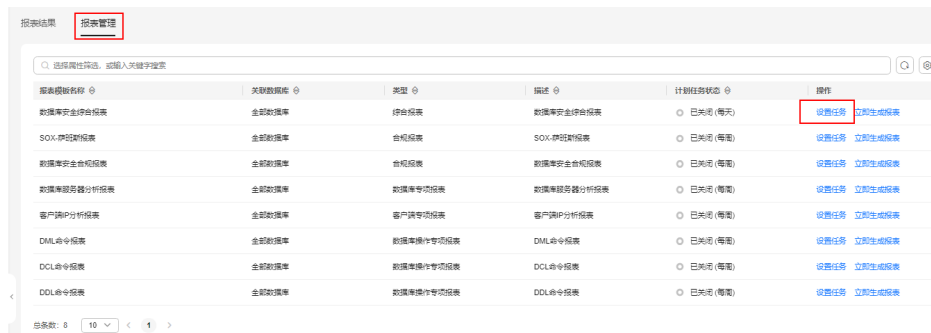
步骤3 在左侧导航树中，选择“报表”。

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









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

图 8-16 “计划任务”对话框



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	<p>开启或关闭计划任务。</p> <ul style="list-style-type: none">  : 开启  : 关闭 	
消息通知	<p>开启或关闭消息通知。</p> <p>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SMN价格详情。</p> <ul style="list-style-type: none">  : 开启  : 关闭 	
消息通知主题	<ul style="list-style-type: none"> 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。 <p>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》。</p>	-
报表类型	<p>选择生成的报表类型，可以选择：</p> <ul style="list-style-type: none"> 日报 周报 月报 	周报
执行方式	<p>选择报表执行的方式，可以选择：</p> <ul style="list-style-type: none"> 执行一次 周期执行 	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、下载审计报告

预览或下载审计报告前，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。

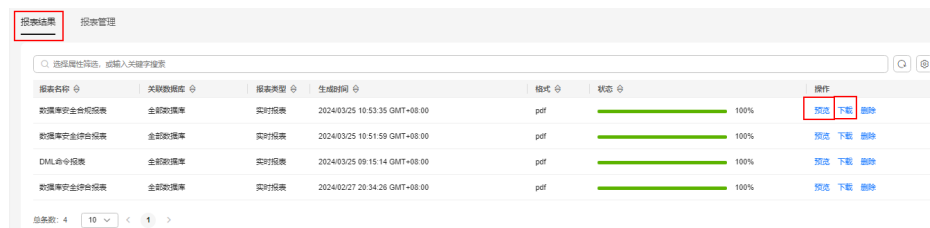
步骤2 在页面上方选择“区域”后，单击页面左上方的，选择“安全与合规 > 数据库安全服务 DBSS”，进入数据库安全审计“总览”界面。

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”，如图8-17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



报表名称	关联数据库	报表类型	生成时间	格式	状态	操作
数据库安全合规报表	全部数据库	实时报表	2024/03/25 10:53:35 GMT+08:00	pdf	100%	预览 下载 删除
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%	预览 下载 删除
DML命令报表	全部数据库	实时报表	2024/03/25 09:15:14 GMT+08:00	pdf	100%	预览 下载 删除
数据库安全综合报表	全部数据库	实时报表	2024/02/27 20:34:26 GMT+08:00	pdf	100%	预览 下载 删除

----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




- 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，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

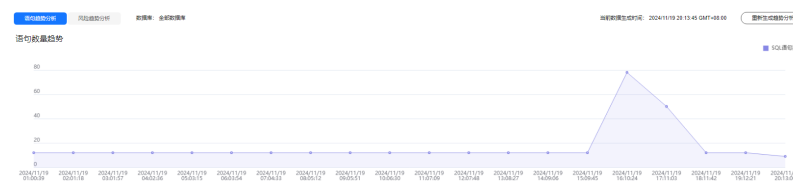


图 8-20 会话统计

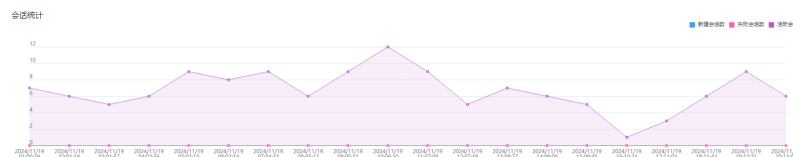


图 8-21 SQL 分布

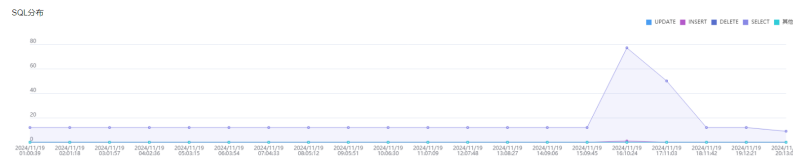


图 8-22 风险分布

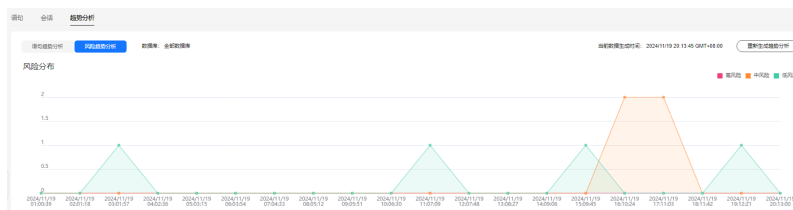


图 8-23 SQL 注入趋势



图 8-24 风险操作趋势



---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。

图 9-1 设置邮件通知



表 9-1 邮件通知参数说明

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。 <ul style="list-style-type: none"> : 开启 : 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



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	<p>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。</p> <ul style="list-style-type: none"> ：关闭 ：开启 	
消息通知主题	<ul style="list-style-type: none"> 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。 <p>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》。</p>	-
每天发送告警总条数	<p>每天允许发送的告警总条数。</p> <p>须知</p> <ul style="list-style-type: none"> 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。 	30
告警风险等级	<p>选择产生告警通知的风险日志告警风险等级，可以选择：</p> <ul style="list-style-type: none"> 高 中 低 	高
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。


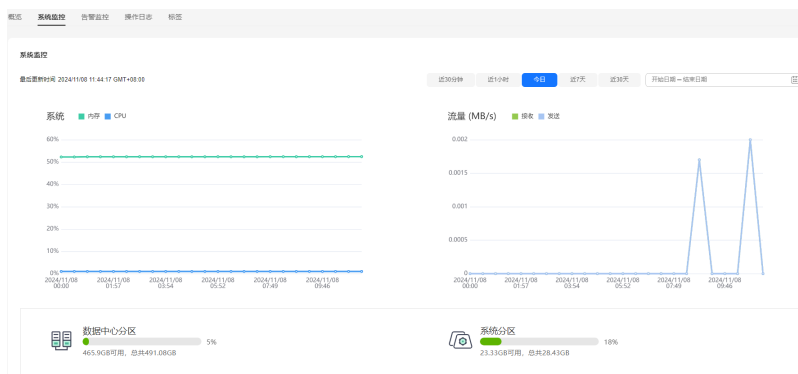
选择审计的时间（“近30分钟”、“近1小时”、“今日”、“近7天”或“近30天”）；或者单击，选择开始时间和结束时间，查看指定的时间段的系统监控信息。

图 10-1 查看系统监控信息



----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[设置告警通知](#)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

发生时间	告警类型	告警风险等级	发生时间	确认状态	操作
2024-11-08 10:47:27 GMT+08:00	风险检测告警	高风险	--	未确认	确认 删除
2024-11-08 10:31:04 GMT+08:00	风险检测告警	高风险	--	未确认	确认 删除
2024-11-08 10:29:59 GMT+08:00	风险检测告警	高风险	--	未确认	确认 删除
2024-11-08 10:28:53 GMT+08:00	风险检测告警	高风险	--	未确认	确认 删除
2024-11-08 10:28:53 GMT+08:00	风险检测告警	高风险	--	未确认	确认 删除

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： <ul style="list-style-type: none">• 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： <ul style="list-style-type: none">• 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： <ul style="list-style-type: none">• 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 ，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

发生时间	告警类型	告警风险等级	恢复时间	确认状态	描述	操作
<input type="checkbox"/> 2024/11/08 14:53:13 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 14:49:56 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 14:47:45 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 14:46:40 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 14:46:34 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 14:40:07 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 14:40:07 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 10:47:27 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 10:31:04 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 10:29:59 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 10:28:53 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input checked="" type="checkbox"/> 2024/11/08 10:28:53 GMT+08:00	风险规则告警	高风险	--	已确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除

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

告警列表

批量确认

今日

选择属性在筛选，或输入关键字搜索

发生时间	告警类型	告警风险等级	恢复时间	确认状态	描述	操作
<input checked="" type="checkbox"/> 2024/11/08 14:53:13 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input checked="" type="checkbox"/> 2024/11/08 14:49:56 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input checked="" type="checkbox"/> 2024/11/08 14:47:45 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input checked="" type="checkbox"/> 2024/11/08 14:46:40 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除

- 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

告警列表

今日

选择属性在筛选，或输入关键字搜索

发生时间	告警类型	告警风险等级	恢复时间	确认状态	描述	操作
<input type="checkbox"/> 2024/11/08 14:53:13 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 14:49:56 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 14:47:45 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 14:46:40 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 14:46:34 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 14:40:07 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 14:40:07 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 10:47:27 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 10:31:04 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 10:29:59 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 10:28:53 GMT+08:00	风险规则告警	高风险	--	未确认	Risk SQL_Risk Level: HIGH_Risk...	确认 删除
<input type="checkbox"/> 2024/11/08 10:28:53 GMT+08:00	风险规则告警	高风险	--	已确认	Risk SQL_Risk Level: HIGH_Risk...	删除

删除告警信息

删除该告警信息将不会记录。

即将删除以下告警信息

发生时间	告警类型	告警风险等级
2024/11/08 10:28:53	风险规则告警	高风险

取消 确认

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:PutObjectAcl",
        "obs:object:GetObjectVersion",
        "obs:object:GetObject",
        "obs:object:GetObjectVersionAcl",
        "obs:bucket:HeadBucket",

```

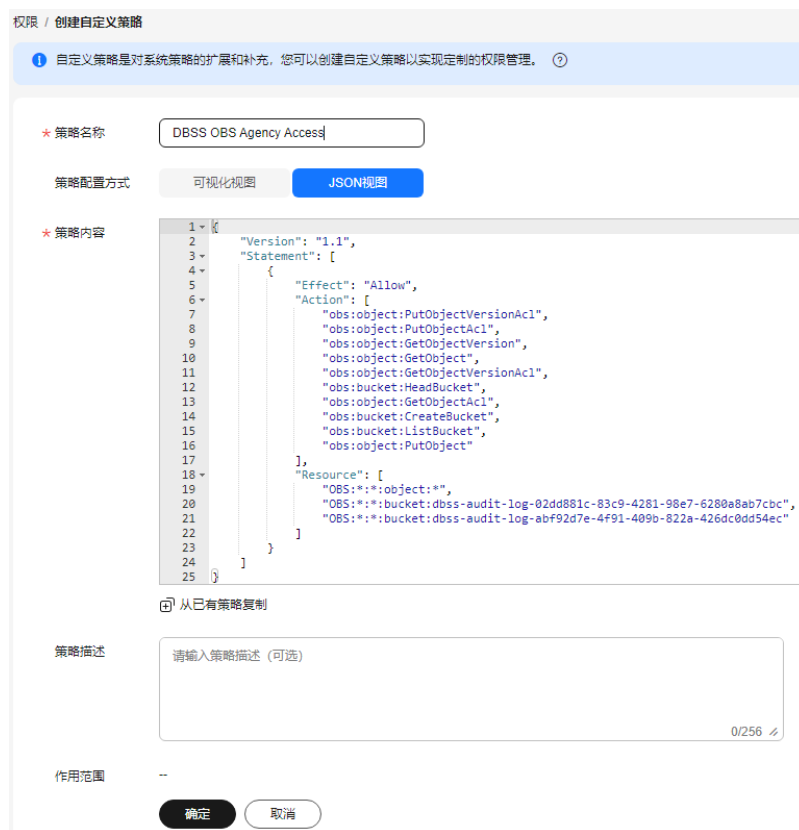
```

"obs:object:GetObjectAcl",
"obs:bucket:CreateBucket",
"obs:bucket:ListBucket",
"obs:object:PutObject"
],
"Resource": [
"OBS:*:*:object:*",
"OBS:*:*:bucket:OBS桶1的名称",
"OBS:*:*:bucket:OBS桶2的名称" //可添加多个桶。
]
}
]
}

```

如图11-1所示。配置完成后单击“确定”。

图 11-1 创建自定义策略



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”。如图11-2所示。

图 11-2 创建委托

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**图11-3**所示。单击右下角的“下一步”。

图 11-3 选择策略

名称	类型
DBSS OBS Agency Access	自定义策略
AA4 FullAccess	系统策略
AA4 ReadOnlyAccess	系统策略

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**图11-4**所示，单击“完成”后等待15分钟授权生效。


图 11-4 完成授权

名称	作用范围	类型	描述
DBSS OBS Agency Access	所有资源	自定义策略	

----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(OBS)桶中，OBS桶按照存储用量收费，由对象存储服务结算。
2. 开启自动备份，请先选择OBS桶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





开始时间

桶名称 [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

自动备份授权 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：授权成功后预计15分钟，自动备份才会生效

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。 <ul style="list-style-type: none"> ：开启 ：关闭 	
备份周期	选择自动备份的周期，可以选择： <ul style="list-style-type: none"> 每天 每小时 	每天
开始时间	单击  ，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： <ul style="list-style-type: none"> 创建默认桶 选择已有桶 说明 <ul style="list-style-type: none"> 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-4042
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	设置自动备份任务时，请先进行自动备份授权。勾选自动备份授权后，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。	勾选

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	备份时间	文件大小	备份方式	备份范围	实例ID	任务状态	操作
auto_backup_20241107...	20241107...	20 Byte	自动备份	20241107 00:00:00 GMT+08:00-20241107 23:59:59 GM...	58669db348539336239f1e2219c7f0431d...	自动	恢复日志 删除
auto_backup_20241106...	20241106...	20 Byte	自动备份	20241106 00:00:00 GMT+08:00-20241106 23:59:59 GM...	58669db348539336239f1e2219c7f0431d...	自动	恢复日志 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



---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。


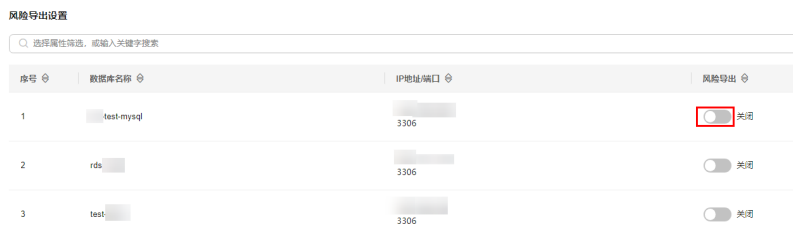
步骤5 在需要导出风险日志的数据库右侧操作栏单击 ，开启风险导出。

图 11-8 开启风险导出



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。勾选风险导出授权后，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. 风险日志将导出到对象存储服务的OBS桶中，OBS桶按照存储用量收费，由对象存储服务结算。
2. 开启风险导出，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 [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

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 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

实例名称/资源ID	状态	实例规格	计费模式	版本	已关联数据库实例总数	企业项目	操作
DBSS-	运行中	入门版	包年/包月 按天按量计费	24.09.03.141647	0/1	default	配置审计规则 续费 更多
DBSS-	运行中	入门版	包年/包月	24.09.03.141647	1/1	default	配置审计规则 续费 更多

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： <ul style="list-style-type: none">• 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： <ul style="list-style-type: none">• 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

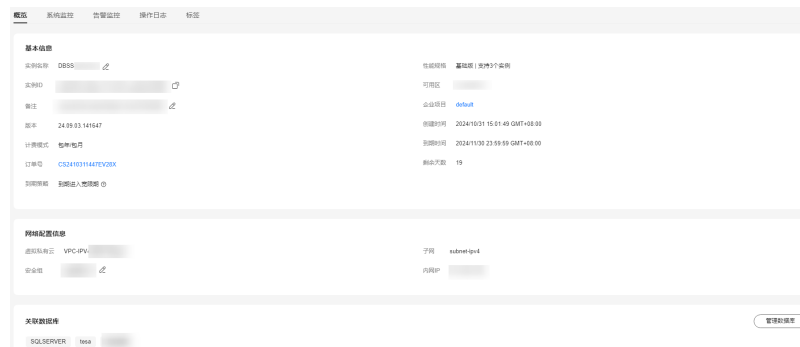




表 12-2 实例概览信息参数说明

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  ，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： <ul style="list-style-type: none"> • 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  ，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： <ul style="list-style-type: none"> • 自动续费 • 到期进入宽限期
	剩余天数	实例到期剩余天数。
网络配置信息	虚拟私有云	实例所在的虚拟私有云。
	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 步骤一：添加数据库 。

----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： <ul style="list-style-type: none"> • 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。

```
ll
```

- 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[步骤4](#)。

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



序号	名称	例外IP	源IP	源端口	数据库名称	数据库账户	状态	操作
1	update	any	any	any	全部数据库	any	<input type="radio"/> 已禁用	启用 编辑 删除
2	全库审计规则	any	any	any	--	any	<input checked="" type="radio"/> 已启用	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： <ul style="list-style-type: none"> 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

序号	名称	SQL命令特征	风险等级	状态	操作
1	WebSQL注入	正则表达式	低	已启用	设置优先级 禁用 编辑 删除
2	MySQL数据库SQL注入	正则表达式	高	已禁用	设置优先级 禁用 编辑 删除
3	HAVING数据库SQL注入	正则表达式	中	已禁用	设置优先级 禁用 编辑 删除
4	UNION联合查询SQL注入	正则表达式	中	已禁用	设置优先级 禁用 编辑 删除
5	时间型SQL注入	正则表达式	中	已禁用	设置优先级 禁用 编辑 删除
6	模糊型SQL注入1	正则表达式	高	已禁用	设置优先级 禁用 编辑 删除
7	模糊型SQL注入2	正则表达式	高	已禁用	设置优先级 禁用 编辑 删除
8	布尔型SQL注入	正则表达式	高	已禁用	设置优先级 禁用 编辑 删除
9	时间型SQL注入2	正则表达式	高	已禁用	设置优先级 禁用 编辑 删除
10	暴力注入	正则表达式	高	已禁用	设置优先级 禁用 编辑 删除

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： <ul style="list-style-type: none"> 高 中 低 无风险
状态	SQL注入检测的状态，包括： <ul style="list-style-type: none"> 已启用 已禁用
操作	SQL注入规则的操作，包括： <ul style="list-style-type: none"> 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

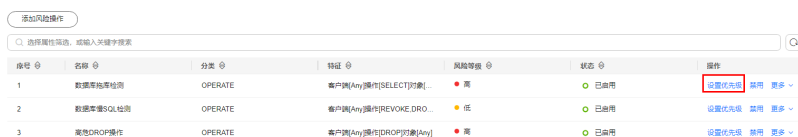
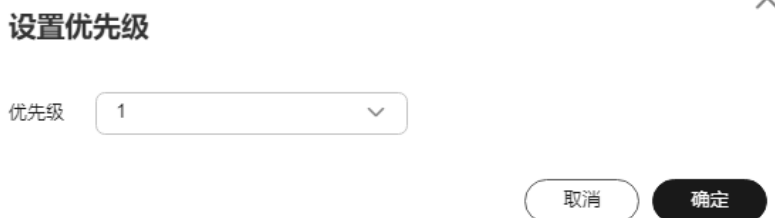


图 12-5 展示了数据库安全审计“总览”界面中的“风险操作”列表。列表包含以下列：操作 ID、名称、分类、特征、风险等级、状态和操作。其中，操作 ID 为 1 的“数据库连接检测”操作，其“操作”列中的“设置优先级”按钮被红色框选中。

操作 ID	名称	分类	特征	风险等级	状态	操作
1	数据库连接检测	OPERATE	客户端[Any]操作[SELECT]对象...	高	已启用	设置优先级 禁用 更多
2	数据库重连SQL检测	OPERATE	客户端[Any]操作[REVOKE.DRO...	低	已启用	设置优先级 禁用 更多
3	高危DROP操作	OPERATE	客户端[Any]操作[DROP]对象[Any]	高	已启用	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



----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

序号	名称	分类	特征	风险等级	状态	操作
1	数据库高危操作	OPERATE	客户端[Any]操作[SELECT]匹配...	高	已启用	设置优先级 禁用 更多
2	数据库高危SQL语句	OPERATE	客户端[Any]操作[REVOKE, DRO...	低	已禁用	设置优先级 禁用 更多
3	高危DROP操作	OPERATE	客户端[Any]操作[DROP]匹配[Any]	高	已禁用	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： <ul style="list-style-type: none"> 高 中 低 无风险
状态	风险操作的状态，包括： <ul style="list-style-type: none"> 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：

- 启用**
 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。

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



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	该规则的类型，包括 <ul style="list-style-type: none">• 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： <ul style="list-style-type: none">• 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](#)。

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

报表名称	关联数据库	报表类型	生成时间	格式	状态	操作
数据库安全综合报表	全部数据库	实时报表	20241108 09:51:27 GMT+08:00	pdf	100%	预览 下载 删除
数据库安全综合报表	全部数据库	日报	20241010 16:05:20 GMT+08:00	pdf	100%	预览 下载 删除
数据库安全综合报表	全部数据库	日报	20240906 16:13:37 GMT+08:00	pdf	100%	预览 下载 删除
客户操作分析报表	全部数据库	实时报表	20240730 16:12:34 GMT+08:00	pdf	100%	预览 下载 删除
数据库服务器分析报表	全部数据库	实时报表	20240730 16:11:47 GMT+08:00	pdf	100%	预览 下载 删除
客户操作分析报表	全部数据库	实时报表	20240730 16:10:43 GMT+08:00	pdf	100%	预览 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

报表模板名称	关联数据库	类型	描述	计划任务状态	操作
数据库安全综合报表	全部数据库	综合报表	数据库安全综合报表	已开启 (每天)	设置任务 立即生成报表
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 缺陷检测报表	全部数据库	合规报表	SOX 缺陷检测报表	已关闭 (每周)	设置任务 立即生成报表
数据库操作分析报表	全部数据库	数据库专项报表	数据库操作分析报表	已关闭 (每周)	设置任务 立即生成报表
客户操作分析报表	全部数据库	客户操作专项报表	客户操作分析报表	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	数据库操作专项报表	DDL命令报表	已关闭 (每周)	设置任务 立即生成报表
DCL命令报表	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命令报表	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 立即生成报表

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



日志名称	备份时间	文件大小	备份方式	备份范围	sha256	任务状态	操作
auto_backup_20241111...	2024/11/11...	20 Byte	自动备份	2024/11/11 00:00:00 GMT+08:00-2024/11/11 23:59:59 GM...	59869db34853933b239f1a2219fd7d...	自动备份完成	恢复日志 删除
auto_backup_20241110...	2024/11/10...	20 Byte	自动备份	2024/11/10 00:00:00 GMT+08:00-2024/11/10 23:59:59 GM...	59869db34853933b239f1a2219fd7d...	自动备份完成	恢复日志 删除
auto_backup_20241109...	2024/11/11...	20 Byte	自动备份	2024/11/09 00:00:00 GMT+08:00-2024/11/09 23:59:59 GM...	59869db34853933b239f1a2219fd7d...	自动备份完成	恢复日志 删除
auto_backup_20241108...	2024/11/10...	20 Byte	自动备份	2024/11/08 00:00:00 GMT+08:00-2024/11/08 23:59:59 GM...	59869db34853933b239f1a2219fd7d...	自动备份完成	恢复日志 删除
auto_backup_20241107...	2024/11/10...	20 Byte	自动备份	2024/11/07 00:00:00 GMT+08:00-2024/11/07 23:59:59 GM...	59869db34853933b239f1a2219fd7d...	自动备份完成	恢复日志 删除
auto_backup_20241106...	2024/11/10...	20 Byte	自动备份	2024/11/06 00:00:00 GMT+08:00-2024/11/06 23:59:59 GM...	59869db34853933b239f1a2219fd7d...	自动备份完成	恢复日志 删除
auto_backup_20241105...	2024/11/10...	20 Byte	自动备份	2024/11/05 00:00:00 GMT+08:00-2024/11/05 23:59:59 GM...	59869db34853933b239f1a2219fd7d...	自动备份完成	恢复日志 删除
auto_backup_20241104...	2024/11/10...	20 Byte	自动备份	2024/11/04 00:00:00 GMT+08:00-2024/11/04 23:59:59 GM...	59869db34853933b239f1a2219fd7d...	自动备份完成	恢复日志 删除
auto_backup_20241103...	2024/11/10...	20 Byte	自动备份	2024/11/03 00:00:00 GMT+08:00-2024/11/03 23:59:59 GM...	59869db34853933b239f1a2219fd7d...	自动备份完成	恢复日志 删除
auto_backup_20241102...	2024/11/10...	20 Byte	自动备份	2024/11/02 00:00:00 GMT+08:00-2024/11/02 23:59:59 GM...	59869db34853933b239f1a2219fd7d...	自动备份完成	恢复日志 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



用户名	发生时间	功能	操作	操作对象	描述	结果
security_dbss_0048254	2024/11/12 15:11:34 GMT+08:00	数据库列表	下载预览	F3q2H5M8R5Y2aT7jAkY	下载审计客户端	成功
security_dbss_0048254	2024/11/12 15:11:33 GMT+08:00	数据库列表	创建	F3q2H5M8R5Y2aT7jAkY	添加新的审计Agent	成功
security_dbss_0048254	2024/11/12 15:11:27 GMT+08:00	数据库列表	更新	mysql	开启审计客户端	成功
security_dbss_0048254	2024/11/12 15:11:24 GMT+08:00	数据库列表	创建	mysql	创建新的数据库	成功

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2 在左侧导航树中，单击 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务信息页面。

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。

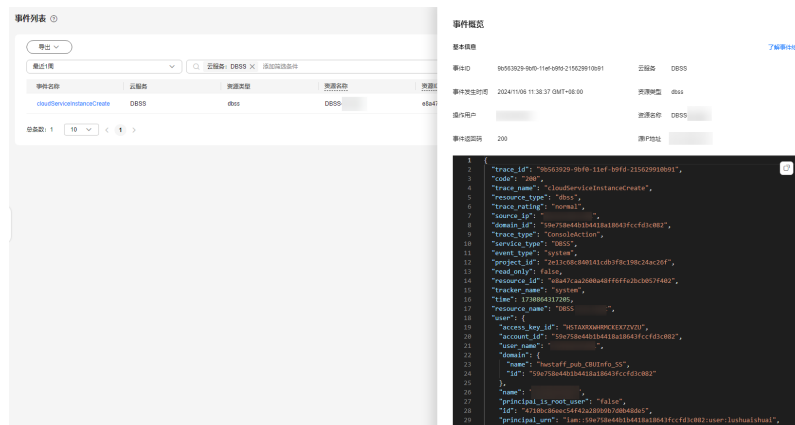
图 13-1 事件列表



事件名称	云服务	资源类型	资源名称	资源ID	操作用户	事件属性	事件时间
cloudServiceInstanceCreate	DBSS	dbss	DBSS	6ba47ca2260a4489f9		normal	20241106 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



----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_util	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_util	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_process_status	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 <ul style="list-style-type: none"> 0：进程状态异常 1：进程状态正常 	数据库审计实例	1分钟
hx_port_status	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 <ul style="list-style-type: none"> 0：端口状态异常 1：端口状态正常 	数据库审计实例	1分钟
hx_proxy_num	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_proxy_status	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 <ul style="list-style-type: none"> 0：代理状态异常 1：代理状态正常 	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_qps	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_rps	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_active_connections_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“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



该截图显示了一个名为“设置告警规则名称”的表单。表单包含两个输入框：

- 第一个输入框，左侧有红色的星号“*”和文字“名称”，框内已输入“alarm-igxc”。
- 第二个输入框，左侧有文字“描述”，框内为空白。

 在第二个输入框的右下角，有一个字符计数器和删除图标，显示为“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”，如图14-2所示。

图 14-2 设置 DBSS 监控告警规则

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[设置监控告警规则](#)。

操作步骤

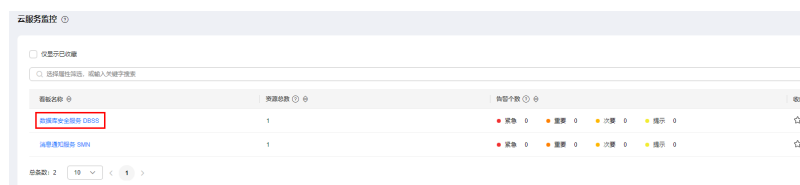
步骤1 [登录管理控制台](#)。

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



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



---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。

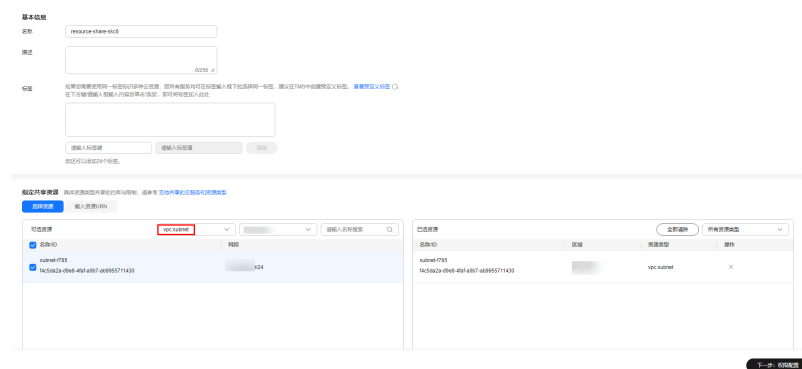
步骤2 单击页面左上角的 ，选择“管理与监管 > 资源访问管理 RAM”，进入“资源访问管理”页面。

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。

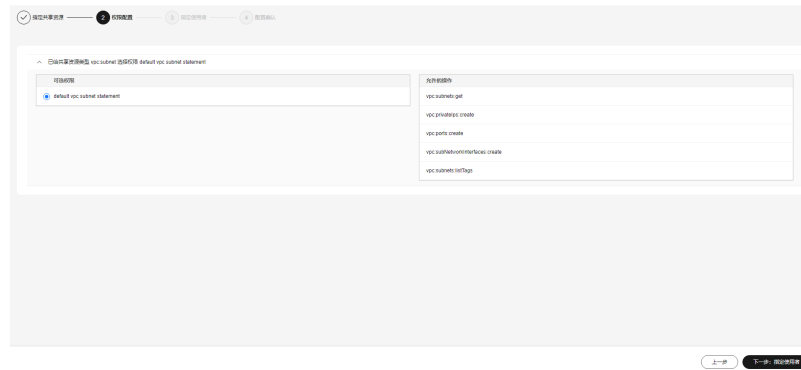
步骤5 选择资源类型为“vpc: subnet”，选择对应区域，勾选需进行共享的VPC。单击“下一步：权限配置”。

图 15-1 指定共享资源



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



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

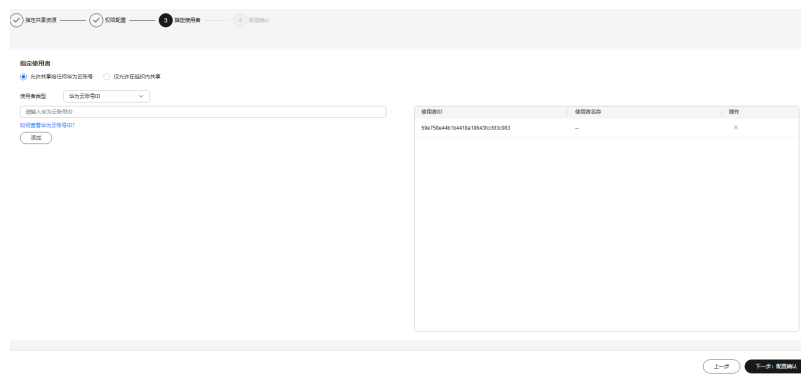
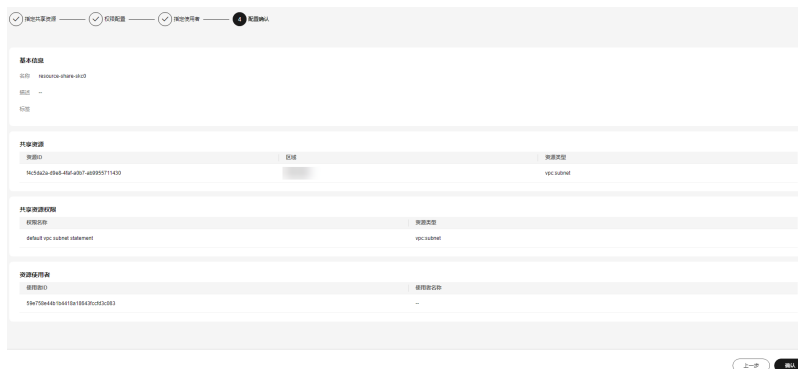


表 15-1 参数说明

参数名称	参数说明
使用者类型	<ul style="list-style-type: none"> 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



---结束

使用 VPC

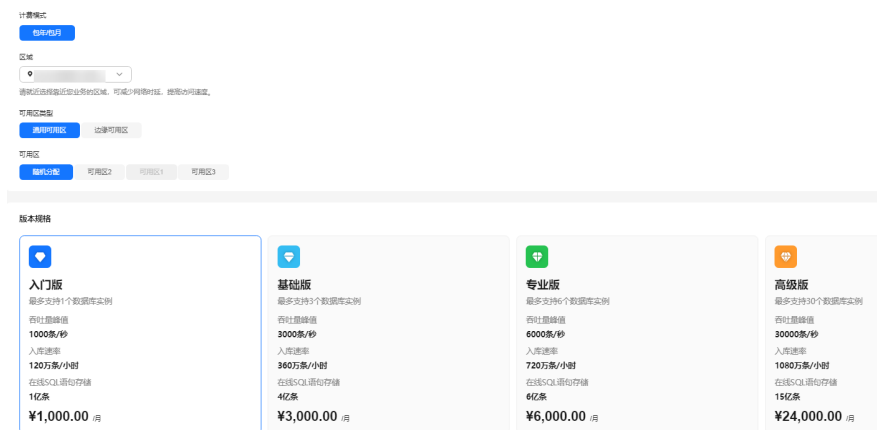
步骤1 登录管理控制台。

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”。

步骤4 选择“区域”、“可用区类型”、“可用区”和“性能规格”。

图 15-5 选择可用区和性能规格



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表15-2所示。

表 15-2 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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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 设置数据库安全审计参数

* 虚拟私有云 [查看虚拟私有云](#)

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。

i 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 [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

备注

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	<p>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。</p> <p>说明</p> <ul style="list-style-type: none"> 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。 <p>更多有关虚拟私有云的信息, 请参见《虚拟私有云用户指南》。</p>
安全组	<p>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。</p> <p>更多有关安全组的信息, 请参见《虚拟私有云用户指南》。</p>
子网	<p>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。</p>
实例名称	<p>您可以自定义实例的名称。</p>


----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

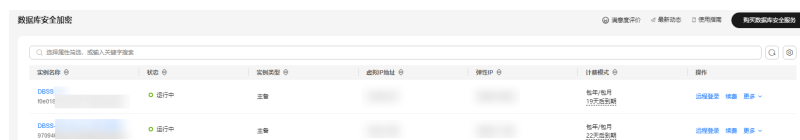
通过管理控制台可登录实例侧，同时可对实例进行重启、关闭、解绑EIP等操作。

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

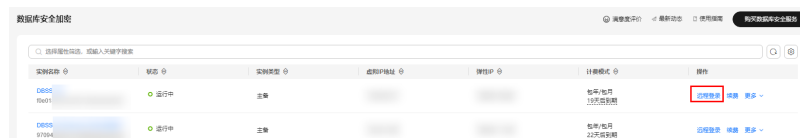


----结束

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



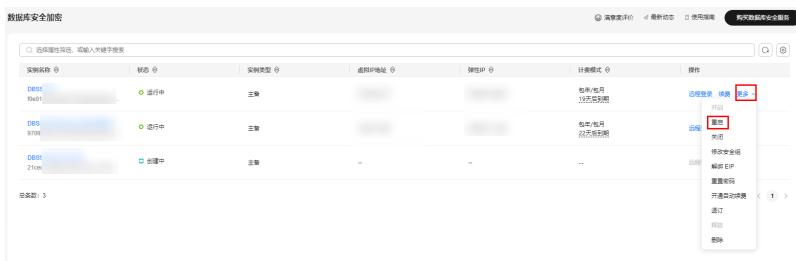
步骤2 跳转至登录页面，输入实例的账号密码，单击“登录”进入数据库加密控制台。

----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



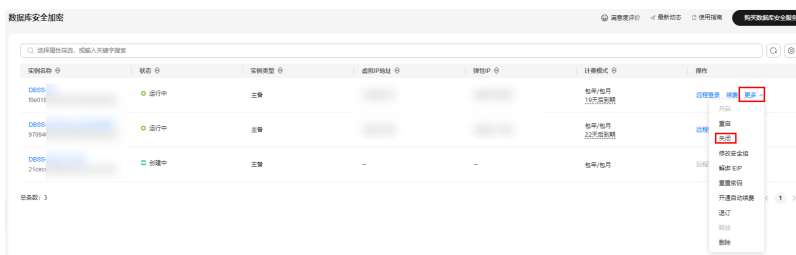
步骤2 在弹窗中确认重启，单击“确认”，实例开始自动执行重启。

----结束

关闭实例

步骤1 在目标实例“操作”列选择“更多 > 关闭”。

图 16-4 关闭数据库安全加密实例



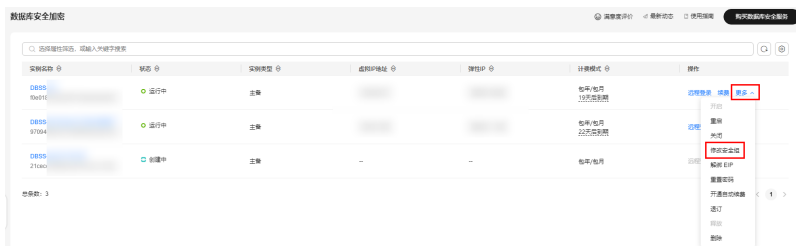
步骤2 在弹窗中确认关闭，单击“确认”，实例开始自动执行关闭。

----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 16-5 数据库安全加密实例修改安全组



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

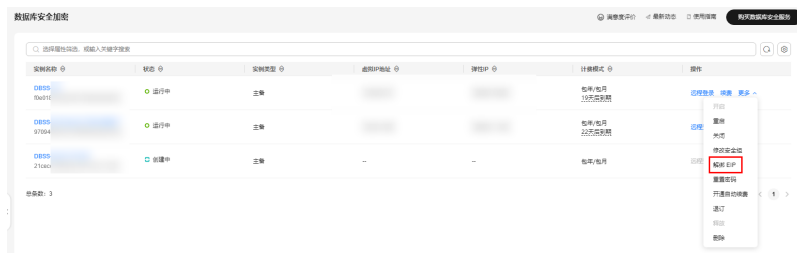
只能选择已有的安全组。

----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



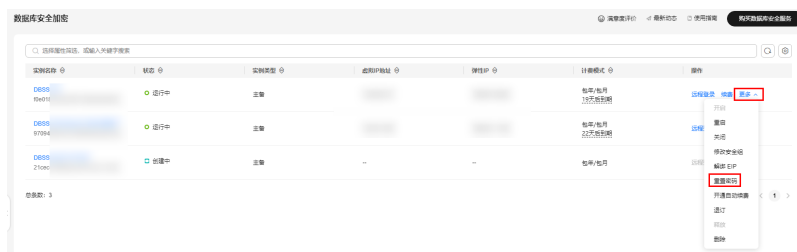
步骤2 在弹窗中确认解绑，单击“确认”，实例将解绑EIP。

----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



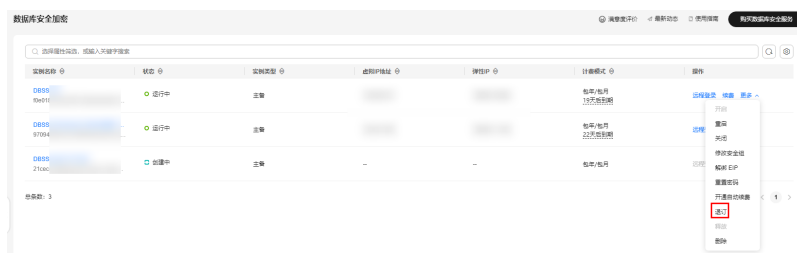
步骤2 在弹窗中输入需要修改的密码，单击“确定”，修改密码完成。

----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



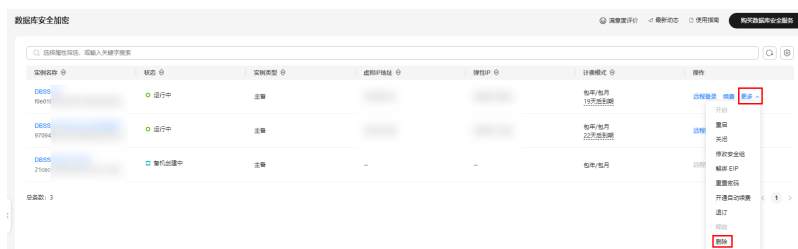
步骤2 在弹窗中确认退订信息，单击“是”，完成退订。

----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



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](#)。
- 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[图16-10](#)所示。

图 16-10 编辑网口

编辑网口

网口名称: eth0

* 网口类型: 业务口

网口描述: 请输入

* 地址类型: IPv4

IPv4配置

* IP地址及子网掩码: 172.17.0.1 : 255.255.255.0

+ 添加(1/10)

网关: 172.17.0.1

DNS: 172.17.0.1

取消 确认

- 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。

参数	说明
网口类型	选择网口类型。网口类型包括： <ul style="list-style-type: none">• 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： <ul style="list-style-type: none">• 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

✕

! 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:

* 子网掩码: ▾

下一跳地址:

* 选择接口: ▾

取消
确认

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： <ul style="list-style-type: none"> ● IPv4 ● IPv6
目标地址	即目标网络IP地址。
子网掩码 (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。

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。

📖 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[备份与恢复配置信息](#)。

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“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”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，升级包请联系技术支持获取。

图 16-12 上传升级包



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



- c. 单击“确定”。
- 周期性自动备份：
 - a. 在周期备份区域，单击设置。


图 16-14 配置自动备份



- b. 在设置周期备份对话框中，配置周期备份信息，配置信息如表16-3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： <ul style="list-style-type: none"> ▪ 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。

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:

* 确认安全口令:

- 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[初始化密钥](#)所示。

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[表16-6](#)所示。

图 16-16 初始化密钥

初始化密钥

● 密钥来源设置后不可修改, 请谨慎选择

* 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

取消 初始化

表 16-6 初始化密钥

参数	说明
RK密钥来源	<p>配置RK（根密钥）来源，支持以下来源：</p> <ul style="list-style-type: none"> 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。 <p>配置后，在密钥平台中选择平台厂商。</p> <p>说明 KMS需要的权限：KMS CMKFullAccess。</p>
DSK密钥来源	<p>配置DSK密钥来源，支持以下来源：</p> <ul style="list-style-type: none"> 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。 <p>配置后，在密钥平台中选择平台厂商。</p> <p>说明 KMS需要的权限：KMS CMKFullAccess。</p>
DEK密钥来源	<p>配置DEK密钥来源，支持以下来源：</p> <ul style="list-style-type: none"> 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。 <p>配置后，在密钥平台中选择平台厂商。</p> <p>说明 KMS需要的权限：KMS CMKFullAccess。</p>

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 performance_schema.*	select insert create update delete drop alter index
RDS_MYSQL	mysql.user performance_schema.*	select 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_PART_KEY_COLUMNS SYS.ALL_IND_COLUMNS SYS.ALL_INDEXES 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_PosgreSQL	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
GAUSSDB	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
KINGBASE 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
KINGBASE 8.3	sys_catalog.sys_class sys_catalog.sys_index 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	用户必须是表的owner或者是dba
Oracle	SYS.ALL_SUBPART_KEY_COLUMNS 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_INDEXES SYS.V_\$INSTANCE SYS.DBMS_LOB SYS.DBMS_METADATA DBA_TABLES DBA_TAB_COLS	用户角色必须是dba

数据库	需要select权限的系统表名	数据库账号权限
SQLserver	sys.tables sys.indexes sys.index_columns sys.default_constraints sys.systypes sys.extended_properties sys.foreign_key_columns sys.check_constraints sys.foreign_keys 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	schemaSelect schemaInsert schmeaUpdate schemaAlter createTable VIEW SERVER STATE 加密表的select 加密表的insert 加密表的alter

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 使用约束 。
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	<p>设置代理端口。运维人员通过代理IP + 代理端口访问数据库。</p> <ul style="list-style-type: none"> 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。 <p>可单击“自动分配”，由系统自动分配空闲的代理端口。</p>
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	<ul style="list-style-type: none"> 设置资产加密方式，可选项如下： <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 设置用户没有权限访问数据库时看到结果。可选项如下： <ul style="list-style-type: none"> 密文：查看到密文信息，编码格式为BASE64或者十六进制，具体请参见设置加密参数。 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，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密，资源使用率超过阈值后停止加密，降低对业务的影响。如果条件允许，建议配置。	
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[表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[图16-17](#)所示。

图 16-17 数据源列表

数据源名称	数据源类型/版本号	数据源地址/端口	代理地址/端口	数据源连接状态	策略配置	启用/停用	操作
demo	MySQL5.7	172.17.0.1:3306	172.17.0.1:14099	已启用		<input checked="" type="checkbox"/>	编辑 删除

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 ，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 ，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符串。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：

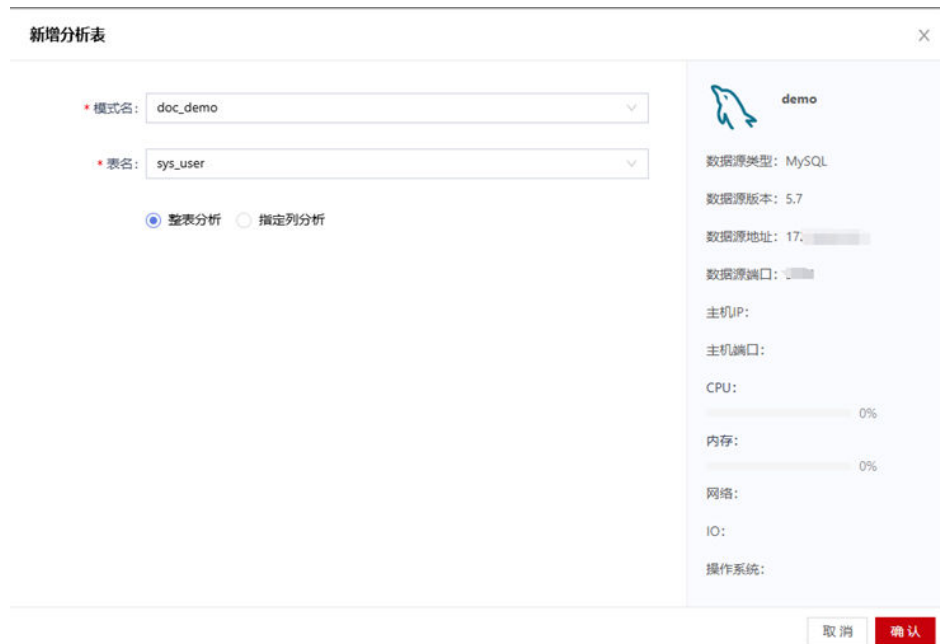
1. 在左侧导航栏，选择“业务测试 > 业务分析”。
2. 在页面左侧数据源处，单击目标数据源。

图 16-18 选择数据源



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



4. 找到目标表格，单击“启动”。

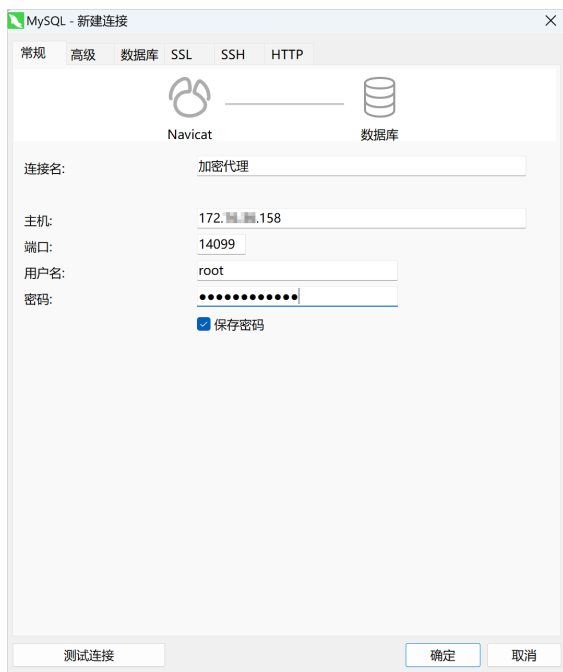
图 16-20 启动

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		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。

1. 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。
2. 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



3. 在数据库工具上执行异常SQL语句。
例如执行以下语句：

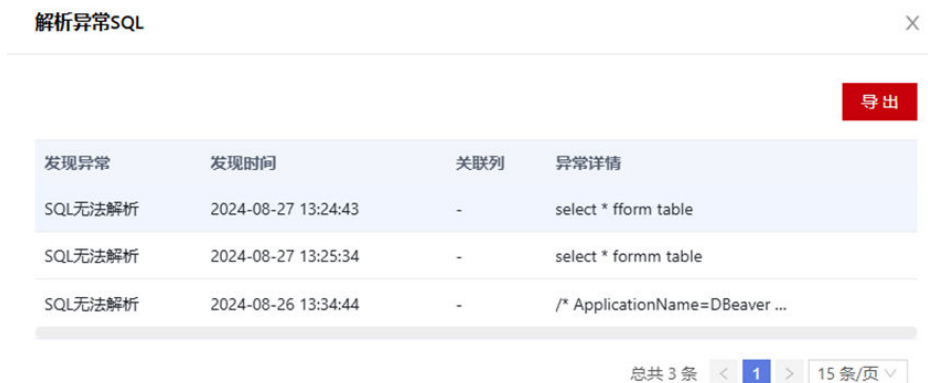
表 16-10 异常示例

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



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		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

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

5. 单击“分析报表”，可用查看系统对此表格的加密建议。

如图16-25所示，如果用户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

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

----结束

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。

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 新增行业模板 。 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。
需要发现的数据类型	手动选中需要扫描的数据类型。 仅在敏感数据类型选择为不使用模板时，此参数可以设置。

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  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”。

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

数据源名称	模式	表名	表列数	是否可加密	不可加密原因	敏感数据发现时间	操作
demo	dbcc_demo	sys_user	8	✔	-	2024-06-27 11:48:45	编辑 添加加密列 添加敏感数据

步骤6 对于数据库表, 单击“编辑”, 可以查看表字段信息。

如**图16-28**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。

图 16-28 编辑表字段信息

编辑 X

表字段信息

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 <input type="button" value="v"/>
dept_id	BIGINT	20	0%	未命中	无 <input type="button" value="v"/>
user_name	VARCHAR	720	0%	未命中	无 <input type="button" value="v"/>
nick_name	VARCHAR	720	0%	未命中	无 <input type="button" value="v"/>
user_type	VARCHAR	272	0%	未命中	无 <input type="button" value="v"/>
email	VARCHAR	2928	100%	电子邮箱地址: 100%	电子邮... <input type="button" value="v"/>
phonenumber	VARCHAR	2928	100%	手机号码: 100%	手机号码 <input type="button" value="v"/>
sex	VARCHAR	272	0%	未命中	无 <input type="button" value="v"/>

总共 8 条 1 15 条/页

----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，示例如图16-29所示。

图 16-29 加密前查询结果

	123 user_id <input type="button" value="v"/>	123 dept_id <input type="button" value="v"/>	abc user_name <input type="button" value="v"/>	abc nick_name <input type="button" value="v"/>	abc user_type <input type="button" value="v"/>	abc email <input type="button" value="v"/>	abc phonenumber <input type="button" value="v"/>	abc sex <input type="button" value="v"/>	abc avatar <input type="button" value="v"/>
1	1	103	admin	管理员	00	@163.com	15888888888	1	
2	2	105	ry	管理员	00	@qq.com	15666666666	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

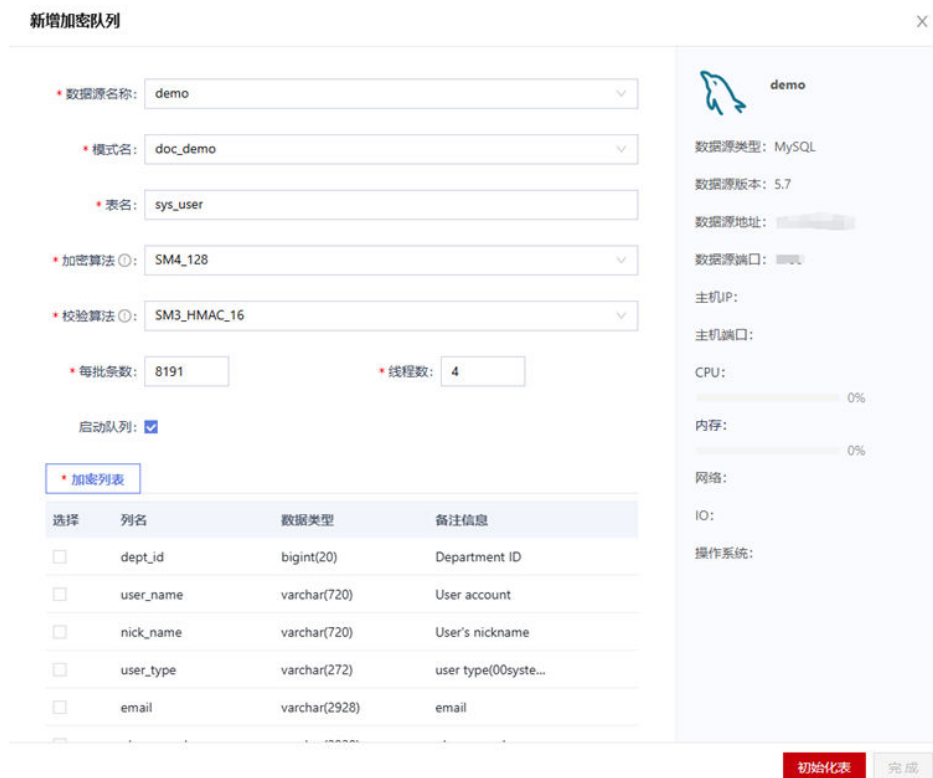
- 步骤1 使用系统管理员sysadmin账号[登录实例Web控制台](#)。
- 步骤2 在左侧导航栏，选择“敏感数据发现 > 敏感数据扫描”。
- 步骤3 在扫描任务列表页面，找到目标数据资产，单击“查看”。
- 步骤4 在扫描结果列表页面，找到目标数据库表，单击“添加加密队列”。

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 查看加密算法 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 查看加密算法 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

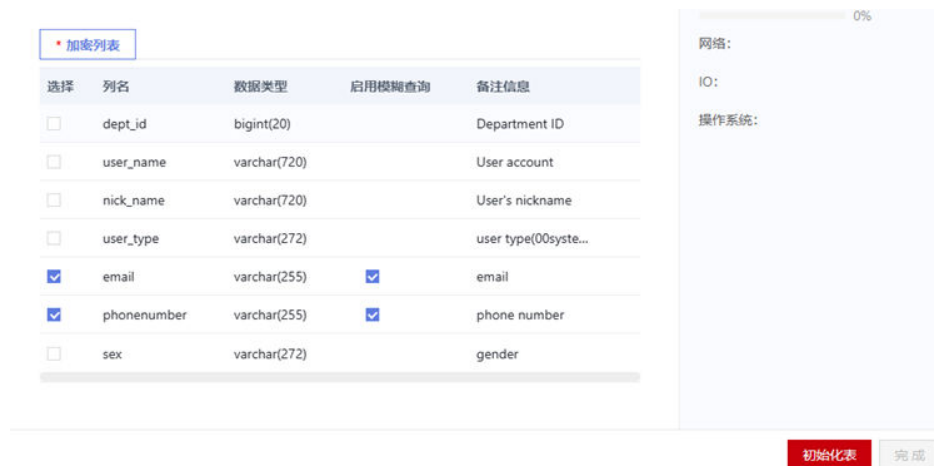


步骤6 单击“加密列表”页签，勾选需要加密的列名称，并设置是否启用模糊查询功能。

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（varchar）。其它类型不支持。

图 16-31 选择加密列



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

队列名	IP地址	端口号	实例名	加密模式	被加密表名	被加密列名	创建时间	启动	状态	操作
加密-root-Mysql-5.7	10.10.10.10	3306	doc_demo	doc_demo	sys_user	email,phonenumber	2024-08-27 15:19:37	<input checked="" type="checkbox"/>	已移出	详情 添加至解密队列

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

	user_id	dept_id	user_name	nick_name	user_type	email	phonenumber	sex
1	103	admin1	aa	00	IEC9Yin7WLo5icdW4BVGzTR6G2tbcsc2Ylq2YFRUz	IEC9YU/9Krw/UcZQ485DhmoSSMUNEHOY1GGW5Kwe	1	
2	105	admin2	aa	00	IEC9Yin7WLo5icdW4BVGzTR6G2tbcsc2Ylq2YFRUz	IEC9Z0/9Krw/UcZQ48gggt+ihz.NuPWj1DOYzPhZz	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[图16-34](#)所示。

图 16-34 脱敏前查询结果

	ABC phone	ABC tel	ABC email
1	1585-88628	0571-88-2500	
2	1833-88185	0571-88-2500	
3	1701-07826	0571-88-2500	

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[新增行业模板](#)。

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。

表 16-14 添加脱敏规则

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

添加脱敏规则

* 规则名称: 脱敏demo

* 模式名: doc_demo

* 表名: sys_user

* 脱敏列表

列名	数据类型	命中率	脱敏算法
phone	手机号码	100%	部分遮蔽
tel	固定电话号码	100%	部分遮蔽

取消 保存

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
1	158****8628	0571*****500	[Redacted]
2	183****8185	0571*****500	[Redacted]
3	170****7826	0571*****500	[Redacted]

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”。

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 匹配列名

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。

- 匹配数据内容

图 16-38 匹配数据内容

添加自定义类型
✕

* 数据类型名称:

* 定义方式: 列名 数据内容

* 正则表达式:

! 只支持字符串正则匹配

备注说明:

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

添加行业模板

* 行业模板名称: 官网模板

备注说明: 官网涉及的敏感数据 9 / 200

安全策略: 脱敏策略

敏感数据选择: 全选

<input type="checkbox"/> 姓名(简体中文)	<input type="checkbox"/> 身份证号(中国大陆)	<input type="checkbox"/> 护照号
<input type="checkbox"/> 军官证号	<input type="checkbox"/> 港澳通行证号	<input checked="" type="checkbox"/> 地址(中文)
<input checked="" type="checkbox"/> 电子邮箱地址	<input type="checkbox"/> 邮政编码	<input type="checkbox"/> 固定电话号码
<input checked="" type="checkbox"/> 手机号码	<input type="checkbox"/> 组织机构代码	<input type="checkbox"/> 统一社会信用代码

脱敏算法选择:

数据类型	脱敏算法
地址(中文)	部分遮蔽
电子邮箱地址	部分遮蔽
手机号码	部分遮蔽

取消 保存

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： <ul style="list-style-type: none"> • 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	包含敏感数据类型	备注说明	策略应用	操作
官网模板	手机号码、电子邮箱地址、地...	官网涉及的敏感数据		编辑 复制 删除
默认类型模板	邮政编码、护照号、电子邮箱...	-		复制
企事业单位敏感信息模板	电子邮箱地址、固定电话号码...	-		复制
个人敏感信息模板	电子邮箱地址、港澳通行证号...	-		复制

- 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

user_id	dept_id	user_name	nick_name	user_type	email	phonenumber	sex	avatar
1	103	000072C522716F38D943	若依	00	000061D80F293773D3B1C40617494D	00000229477203978C5EA9353	1	
2	105	000061D8CFB2B292E4B	若依	00	000061D80F69706E9EBDC62E9622BB	000002294792E3776CBE49D51	1	

----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[初始化密钥](#)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](#)。

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

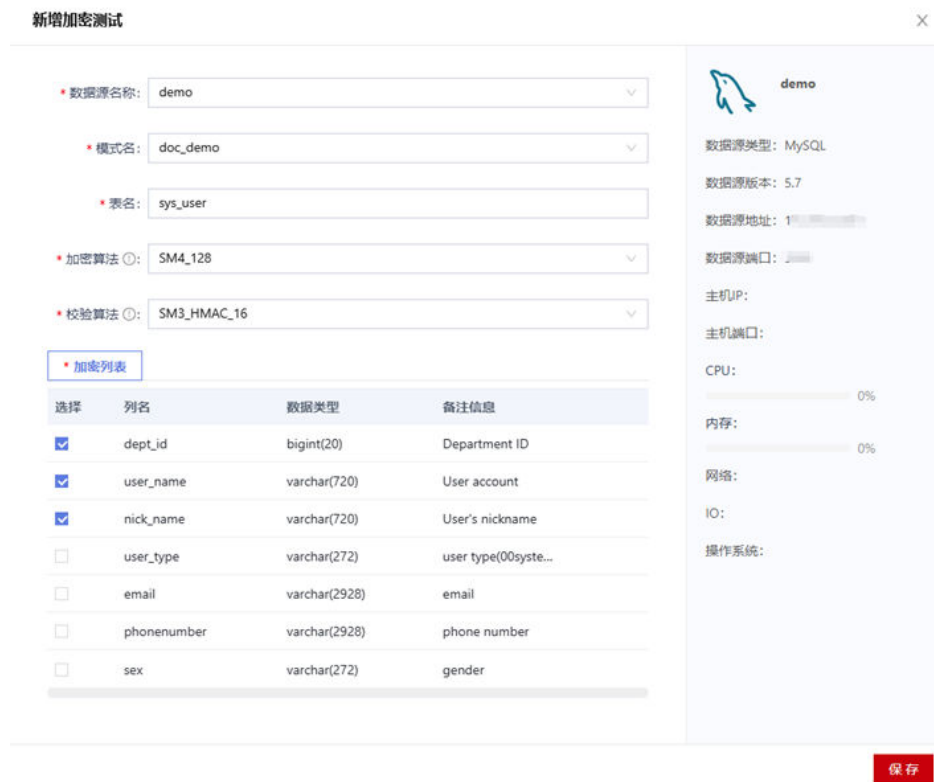


表 16-19 仿真测试

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 查看加密算法 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 查看加密算法 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[仿真加密测试](#)。

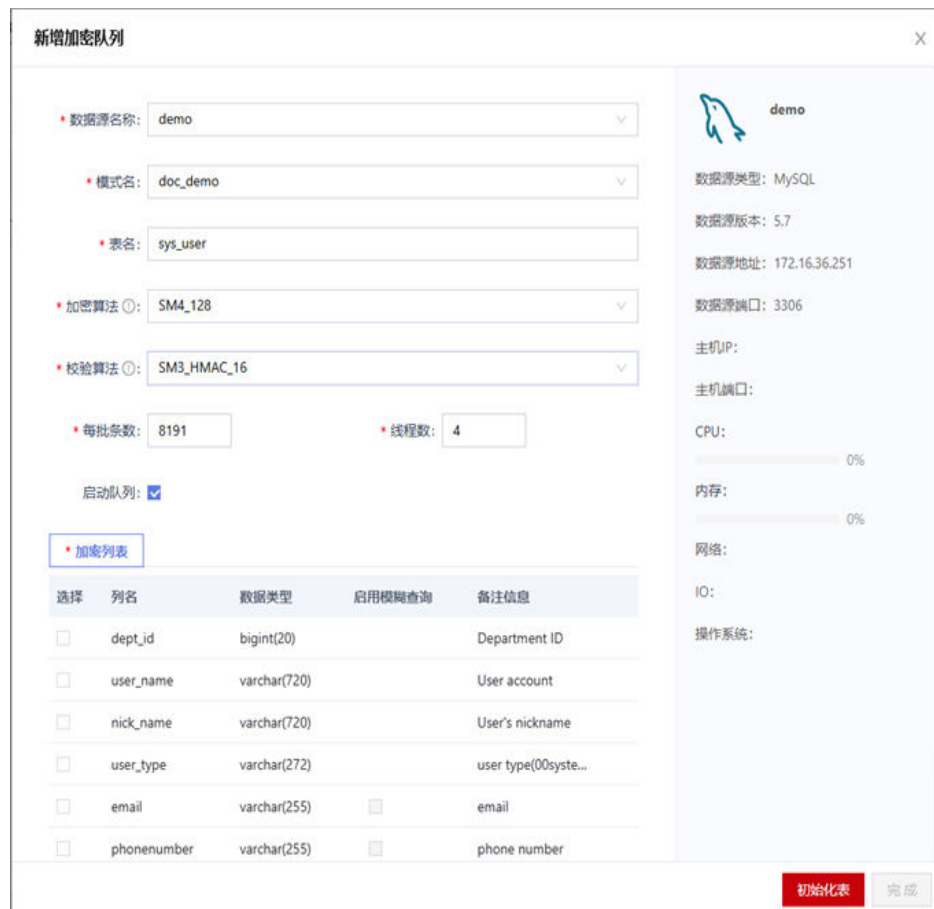
操作步骤

- 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 查看加密算法 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 查看加密算法 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



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





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。

----结束

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

队列名	IP地址	端口号	实例名	加密模式	被加密表名	被加密列名	创建时间	启动	状态	操作
加密-root_MySQL-5.7	192.168.1.100	3306	doc_demo	doc_demo	sys_user	email,phonenumber	2024-08-27 15:19:37		已移除	详情 删除 添加新加密队列

- 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

id	user_id	dept_id	nk user_name	nk nick_name	nk user_type	nk email	nk phonenumber	nk sex
1	103	admin1	aa	00	IECYkn7WLe5IcdW4BVGt1RiGX2bcsc2Ylq2YF8Uz	IECY9U/5Xnw/UcZQ485DhmoSSMUjNEH0Y1GGW5Kwe	1	
2	105	admin2	aa	00	IECYkn7WLe5IcdW4BVGt1RiGX2bcsc2Ylq2YF8Uz	IECY9U/5Xnw/UcZQ485DhmoSSMUjNEH0Y1GGW5Kwe	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[设置客户端授权](#)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： <ul style="list-style-type: none"> • 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

客户端授权
✕

IP范围 ⓘ: ✕ -

✕ - +

时间点范围: ⓘ - ⓘ

星期范围: ⓘ - ⓘ

取消
清空
保存

📖 说明

- IP地址范围支持设置起始IP和结束IP，单击 \oplus 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](#)。

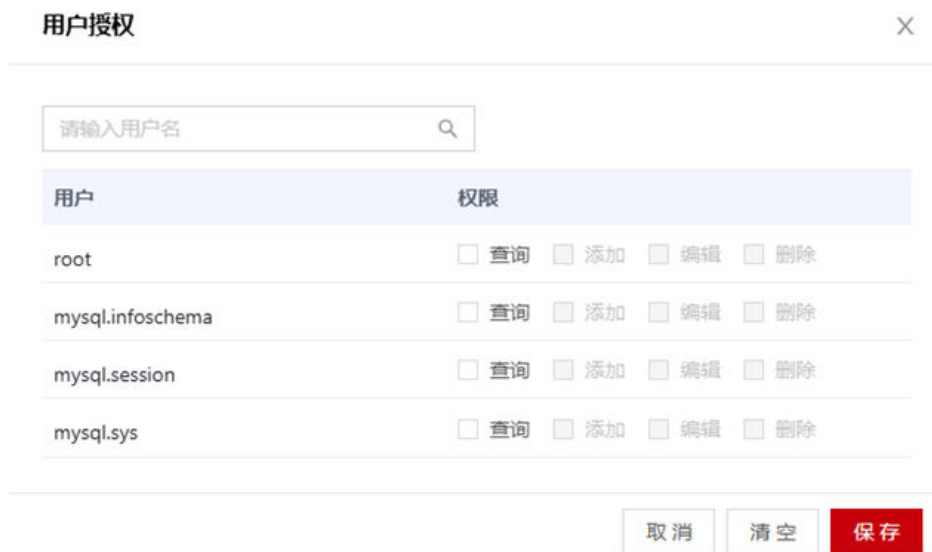
步骤2 在左侧导航栏中，选择“数据加密 > 授权管理”。

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



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[配置加密队列](#)。

操作步骤

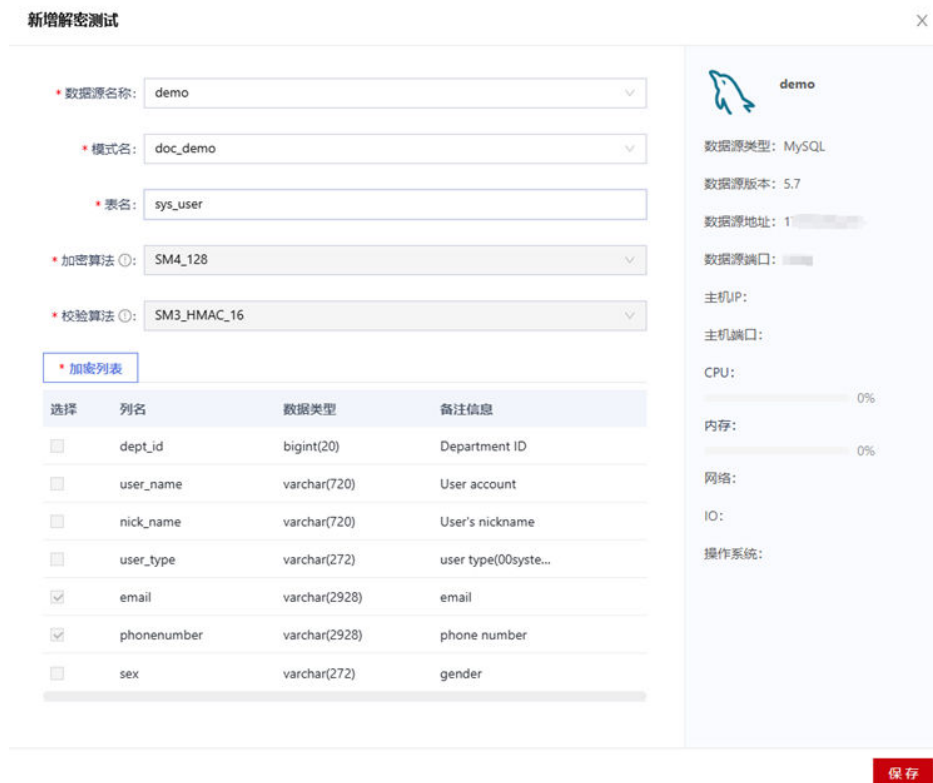
步骤1 使用系统管理员sysadmin账号[登录实例Web控制台](#)。

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



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。

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[仿真解密测试](#)。

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

添加至解密队列

* 数据源名称: demo

* 模式名: doc_demo

* 表名: sys_user

* 加密算法: SM4_128

* 校验算法: SM3_HMAC_16

* 每批条数: 6553

* 线程数: 4

启动队列:

* 加密列表

选择	列名	数据类型	备注信息
<input type="checkbox"/>	dept_id	bigint(20)	Department ID
<input type="checkbox"/>	user_name	varchar(720)	User account
<input type="checkbox"/>	nick_name	varchar(720)	User's nickname
<input type="checkbox"/>	user_type	varchar(272)	user type(00system...
<input checked="" type="checkbox"/>	email	varchar(2928)	email
<input checked="" type="checkbox"/>	phonenumber	varchar(2928)	phone number

demo

数据源类型: MySQL

数据源版本: 5.7

数据源地址: 1

数据源端口:

主机IP:

主机端口:

CPU: 0%

内存: 0%

网络:

IO:

操作系统:

完成

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

添加索引

此操作执行过程中会暂时锁表，请确认执行

选择列: NAME

索引名称: test

索引长度: 100 (范围: 1~3072)

注释: 请输入 0 / 500

预览

SQL预览

```
ALTER TABLE `TEST`.`ddm_rules5` ADD INDEX `test`(`NAME` (100) ) USING BTREE
```

取消 保存

步骤8 单击“保存”。

----结束

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

The screenshot shows a '添加列' (Add Column) dialog box. It contains the following fields and options:

- A warning message: "此操作执行过程中会暂时锁表，请确认后执行" (This operation will temporarily lock the table during execution, please confirm before executing).
- Column name: 'name' (with a dropdown arrow).
- Data type: 'VARCHAR' (with a dropdown arrow).
- Non-null status: '非空' (Non-null) with radio buttons for '是' (Yes) and '否' (No), where '否' is selected.
- Default value: ''name'' (with a dropdown arrow).
- Column length: '10' (with a dropdown arrow).
- Comment: '请输入' (Please enter) in a text area with a character count '0 / 50'.
- A '预览' (Preview) button.
- At the bottom right, there are '取消' (Cancel) and '保存' (Save) buttons.

The SQL preview on the right shows the following statement:

```
ALTER TABLE `TEST`.`ddm_rules5` ADD COLUMN `name` VARCHAR(10) DEFAULT 'name' NULL
```

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。

图 16-54 初始化表

新增加密队列

* 数据源名称: demo

* 模式名: doc_demo

* 表名: sys_user

* 加密算法: SM4_128

* 校验算法: SM3_HMAC_16

* 每批条数: 8191 * 线程数: 4

启动队列:

* 加密列表

选择	列名	数据类型	备注信息
<input type="checkbox"/>	dept_id	bigint(20)	Department ID
<input type="checkbox"/>	user_name	varchar(720)	User account
<input checked="" type="checkbox"/>	nick_name	varchar(720)	User's nickname
<input type="checkbox"/>	user_type	varchar(272)	user type(00system...
<input type="checkbox"/>	email	varchar(2928)	email
<input type="checkbox"/>	phonenumber	varchar(2928)	phone number

demo

数据源类型: MySQL

数据源版本: 5.7

数据源地址: 17...

数据源端口: ...

主机IP:

主机端口:

CPU: 0%

内存: 0%

网络:

IO:

操作系统:

初始化表 完成

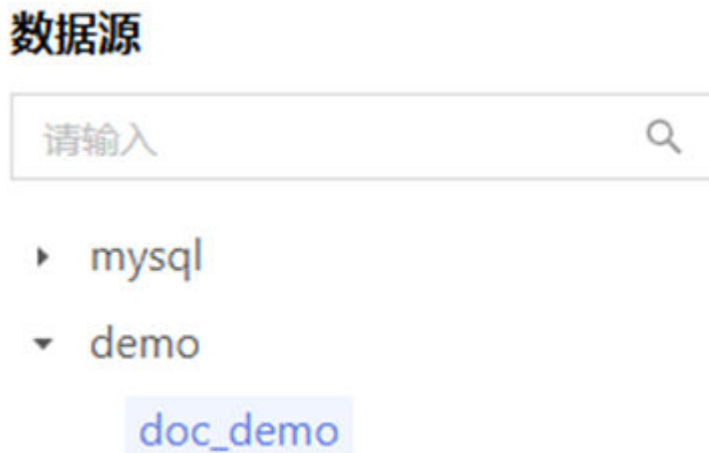
操作步骤

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。

图 16-55 选择模式



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。

图 16-56 添加自定义算法

添加自定义算法 X

* 算法名称:

* 关联数据类型:

算法类型: 字符串

保留前 字符 保留后 字符

* 遮蔽符号:

备注说明:

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

算法名称	算法属性	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。

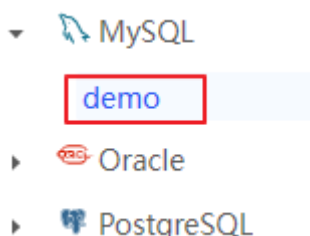
操作步骤

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



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。

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 新增自定义数据类型 。
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 新增自定义脱敏算法 。

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

* 数据类型: 电子邮箱地址

* 脱敏算法: 部分遮蔽

取消 保存

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	部分遮蔽	<input checked="" type="checkbox"/>	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

user_id	dept_id	user_name	nick_name	user_type	email
1					1***3@163.com
2					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。

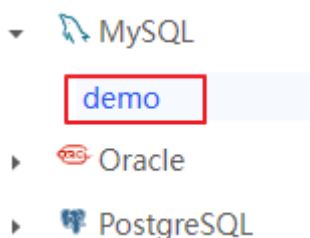
操作步骤

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



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	<ul style="list-style-type: none">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

添加白名单

数据源: demo

数据库用户名: root

IP范围: 请输入

授权开始时间: 2024-08-27 16:31:14

授权结束时间: 2024-08-31 16:31:22

放行规则: 全部规则 指定规则

取消 保存

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[初始化密钥](#)。

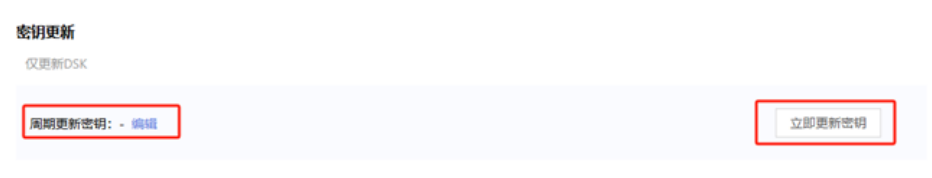
操作步骤

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



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[表16-25](#)所示。

图 16-65 修改密钥更新周期



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： <ul style="list-style-type: none"> - 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[查看密钥信息](#)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”。

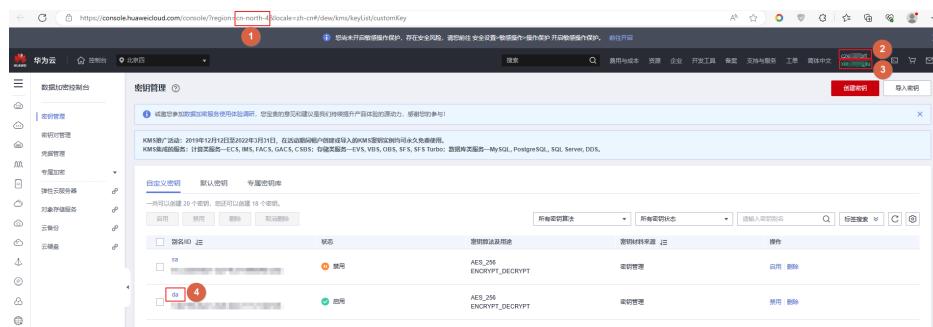
步骤3 单击“华为云”页签。

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 图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



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[初始化密钥](#)。

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



----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

The screenshot shows a 'New Account' dialog box with the following fields and options:

- * 账号:** assetmanager
- * 密码:** [masked]
- * 确认密码:** [masked]
- 使用人:** 张三
- * 关联角色:** 系统管理员
- 电话:** 13000000000
- 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 characters)

Buttons at the bottom: 取消 (Cancel), 提交审核 (Submit for Review)

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。 <ul style="list-style-type: none">● 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。 <ul style="list-style-type: none">● 永久：账号永久有效。● 定义期限：账号在使用期限前有效。
时间期限	<ul style="list-style-type: none">● 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

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。

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

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



----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。

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



- 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公告等消息，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，查看最近的通知公告等信息。

图 16-75 消息中心



----结束

16.2.10.5 系统设置

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



----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



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。
2. 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

1. 在NTP服务器地址输入框填入时间服务器的IP或域名。
2. 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。

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[图16-79](#)所示。

图 16-79 查看角色列表

角色名称	创建者	创建时间	说明	启用状态	操作
安全管理员	-	2019-06-13 14:21:48	安全管理员	<input checked="" type="checkbox"/>	
审计管理员	-	2019-06-13 14:21:48	审计管理员	<input checked="" type="checkbox"/>	
系统管理员	-	2019-06-13 14:21:48	系统管理员	<input checked="" type="checkbox"/>	

----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

 确定开启自动审核吗

取消

确认

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

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	<ul style="list-style-type: none">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	<p>设置是否支持多端登录功能。</p> <ul style="list-style-type: none">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	<ul style="list-style-type: none">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
双因子安全认证	设置登录认证方式。 <ul style="list-style-type: none"> 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



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



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： <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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



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。

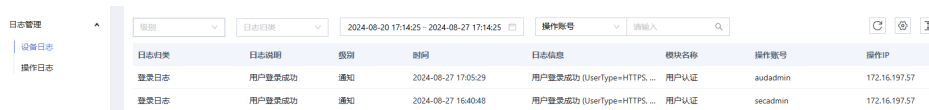
操作步骤

步骤1 使用审计管理员audadmin账号[登录实例Web控制台](#)

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



The screenshot shows the 'Device Logs' interface. At the top, there are search filters for '日志名称' (Log Name), '日志日期' (Log Date) with a date range of '2024-08-20 17:14:25 - 2024-08-27 17:14:25', and '操作账号' (Operation Account). Below the filters is a table with the following data:

日志名称	日志日期	级别	时间	日志信息	模块名称	操作账号	操作IP
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	172.16.197.57
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	172.16.197.57

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

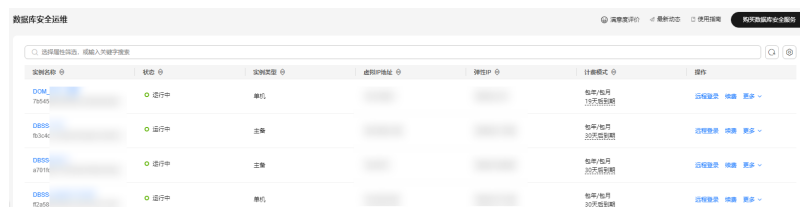
通过管理控制台可登录实例侧，同时可对实例进行重启、关闭、解绑EIP等操作。

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

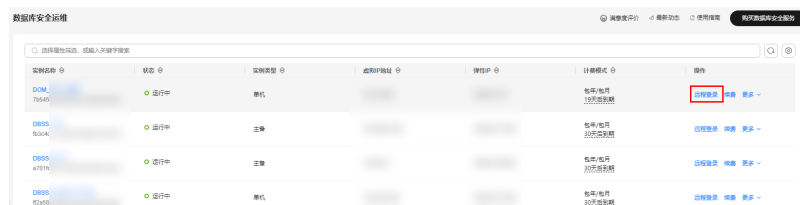


----结束

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



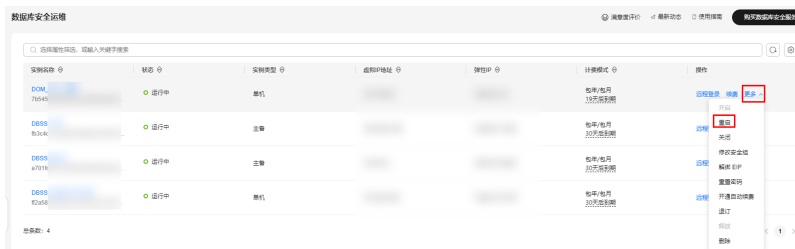
步骤2 跳转至登录页面，输入实例的账号密码，单击“登录”进入数据库运维控制台。

----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



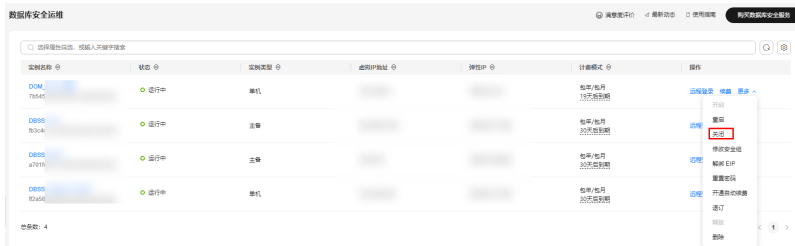
步骤2 在弹窗中确认重启，单击“确认”，实例开始自动执行重启。

----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



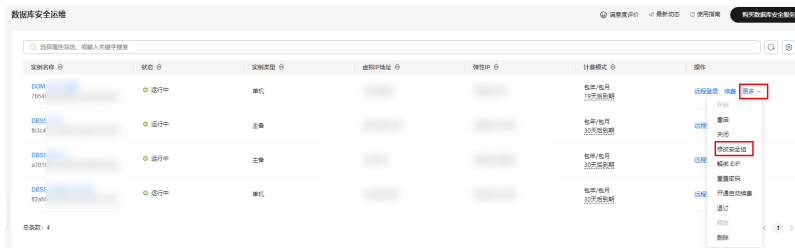
步骤2 在弹窗中确认关闭，单击“确认”，实例开始自动执行关闭。

----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



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

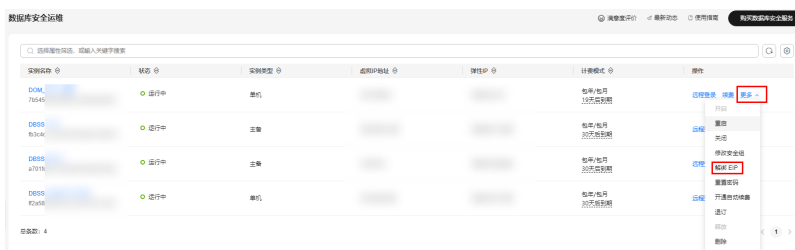
只能选择已有的安全组。

----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



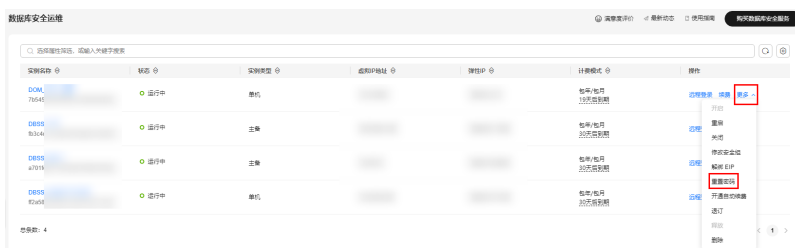
步骤2 在弹窗中确认解绑，单击“确认”，实例将解绑EIP。

----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



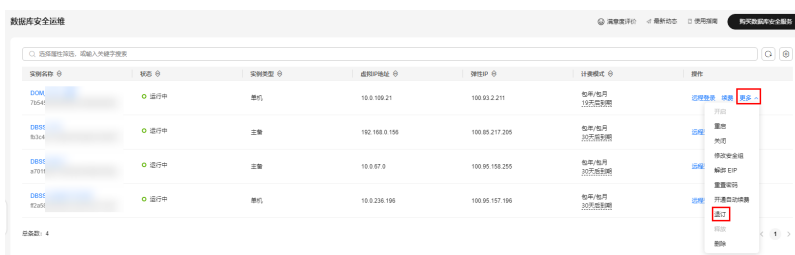
步骤2 在弹窗中输入需要修改的密码，单击“确定”，修改密码完成。

----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



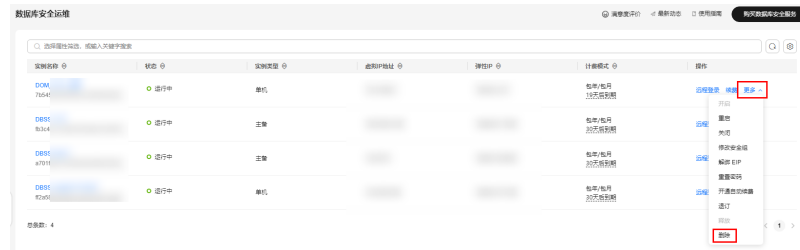
步骤2 在弹窗中确认退订信息，单击“是”，完成退订。

----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



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				
		协议解析单向	协议解析双向	风险扫描	密码代填	web认证
数据库	版本					
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)	√	√	×	√	√
	5.6	√	√	×	√	√
	5.7.29	√	√	×	√	√
	5.7.36	√	√	×	√	√
	5.7.32	√	√	×	√	√
	8.0.21	√	√	×	√	√
	8.0.22	√	√	×	√	√
	8.0.27	√	√	×	√	√
	8.0.28	√	√	×	√	√
SQL Server	2008	√	√	√	×	√
	2014	√	√	√	×	√
	2019	√	√	√	×	√
DB2	8	√	×	√	√	√
	10	√	×	√	√	√
DM7	7.1.2	√	×	√	√	√
DM8	8.1.2.84	√	×	×	√	√
PostgreSQL	10	√	√	×	×	√
	12.2	√	√	×	√	×

兼容性软件名称	兼容版本情况	功能差异化描述				
	9.6.6	√	×	×	×	√
	12.4	√	√	×	√	√
	12.3	√	√	×	√	√
Hive	1.1	√	×	×	×	×
	2.1.1	√	√	×	×	×
Kingbase	7.1.2.0480	√	×	×	×	×
GaussDB	100	√	×	×	×	×
	200	√	×	×	×	×
TDSQL	10.3.14.6.0_D014	√	√	×	×	×
TBase (TBase (PG)	V2.15.17.3.6	√	√	×	×	×
GreemPlum	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

* 资产名称: oracle_zz * 资产类型: Oracle

* 资产IP: 172.17.0.10 * 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: 策略恢复配置:

部署模式: 反向代理 * 端口: 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 通过Web安全客户端访问资产 。
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 误删恢复 。
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。

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

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	<ul style="list-style-type: none"> 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



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



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+。
- 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



- 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[图17-16](#)所示。

图 17-16 选择资产客户端 IP 集

策略详情

命中策略后记录结果集:

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

操作系统用户: 包含任意

----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

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 ： <ul style="list-style-type: none"> - 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

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



2. 设置策略名称和类型，单击“确定”。

图 17-20 添加策略

表 17-6 添加策略

参数	说明
名称	自定义策略名称。
类型	<ul style="list-style-type: none"> - 可选择默认、优先级、白名单和黑名单四种类型： <ul style="list-style-type: none"> ▪ 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



4. 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

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。

- 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



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 ，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 ，复制整个策略。
 - 删除策略：鼠标移动到策略，单击 ，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

The screenshot shows a configuration form for a strategy. At the top right, there are '保存' (Save) and '清空' (Clear) buttons. The form includes the following fields:

- 策略汇总 (Strategy Summary)
- 协议 (Protocol): TCP (dropdown menu)
- 响应动作 (Response Action): 放行 (selected, radio button) / 阻断 (radio button)
- 源ip (Source IP): 192.168.1.100
- 源端口 (Source Port): 请输入 (Please enter)
- 目的ip (Destination IP): 192.168.1.200
- 目的端口 (Destination Port): 22 x

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，此端口可不填）。
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：

- 编辑策略：鼠标移动到策略，单击，修改策略名称。
- 删除策略：鼠标移动到策略，单击，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



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

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 。
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

The screenshot shows a configuration form for adding a SQL attack strategy. The fields are as follows:

- * 名称:** CVE-2017-10292: Vulnerability in Oracle RDBMS Security Component
- * 攻击类型:** SQL注入
- * 状态:** 启用
- * 响应动作:** 通过
- * 关键字:** grant&identified by
注: 仅自定义策略修改才生效!
- 特征:** (\s|^)grant(?:\s?(\s+\s+?))?(?:\s?identified\sby
注: 仅自定义策略修改才生效!
- * 详细:** Exploit database CVEs

At the bottom right, there are two buttons: '取消' (Cancel) and '确定' (Confirm).

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[进行风险管理](#)。

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 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[管理基本配置](#)。

----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



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	172.17.0.44	默认策略	无风险	LOGOUT	通过	172.17.0.1	2023-05-31 14:04:06	详情 回放
root	172.17.0.44	默认策略	无风险	LOGOUT	通过	172.17.0.1	2023-05-31 14:04:06	详情 回放
SYS	127.0.0.1	默认策略	无风险	LOGOUT	通过	172.17.0.1	2023-05-31 10:19:21	详情 回放
SYS	127.0.0.1	默认策略	无风险	LOGOUT	通过	172.17.0.1	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

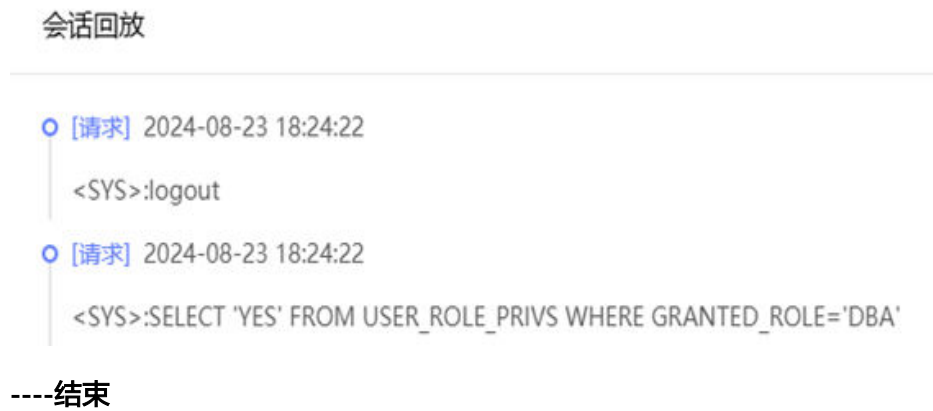
如果在查看审计日志时部分内容不好识别，您可以通过回放审计日志涉及的语句了解信息。

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



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: 192.168.1.93

* IP类型: 服务端IP

* 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。 <ul style="list-style-type: none">• 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

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。 <ul style="list-style-type: none"> 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

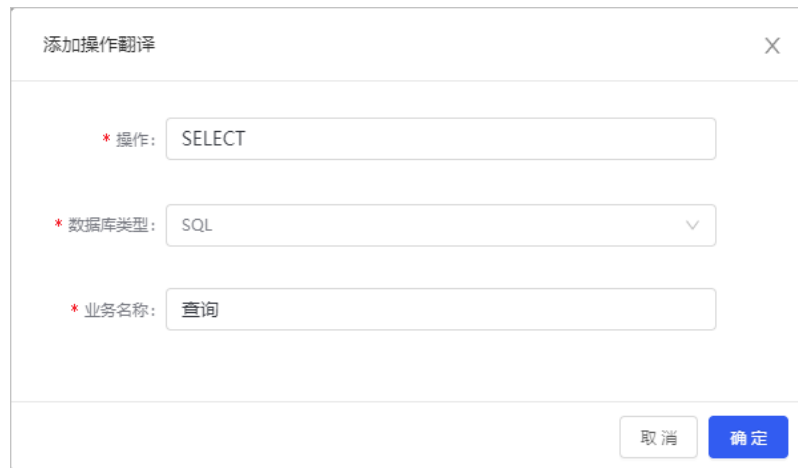
步骤1 使用系统管理员sysadmin账号[登录数据库运维管理系统](#)。

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

* 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

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。 <ul style="list-style-type: none"> 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”。

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



----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

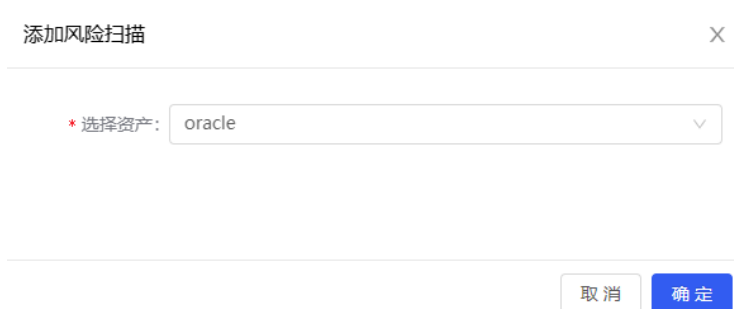
步骤1 使用系统管理员sysadmin账号[登录数据库运维管理系统](#)。

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



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

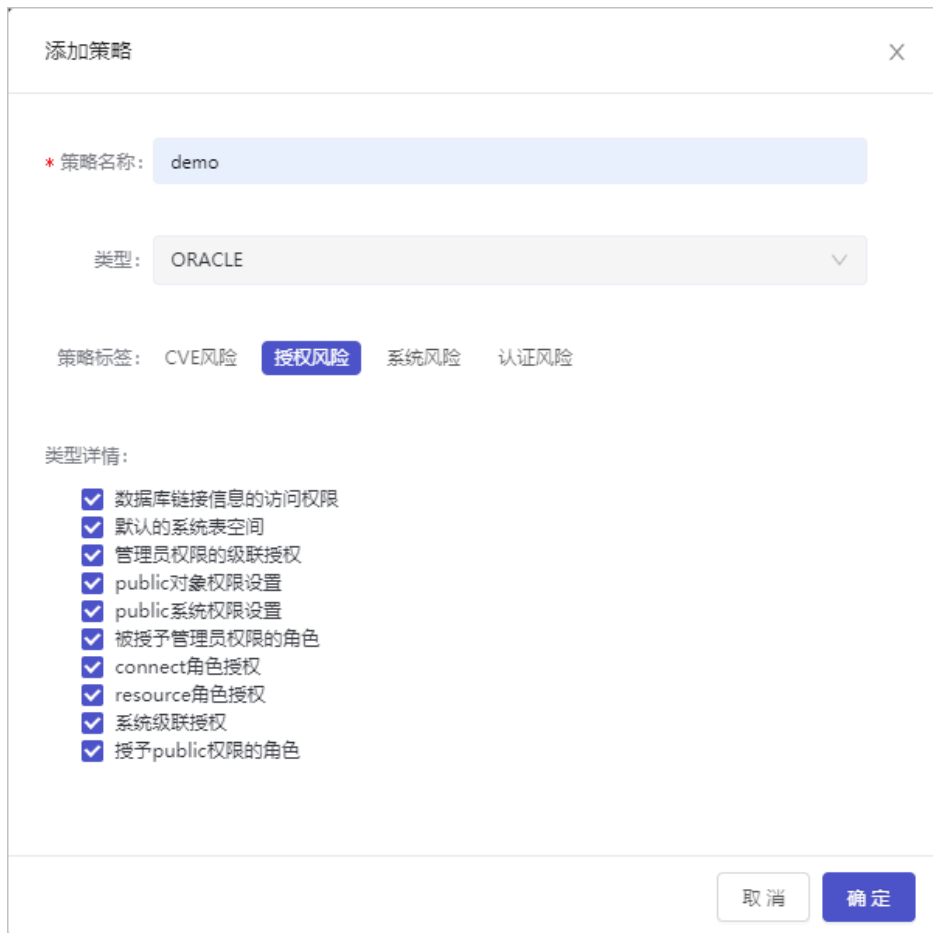


表 17-15 添加策略参数说明

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	<ul style="list-style-type: none"> - 设置风险扫描策略，支持对每个策略标签进行设置： <ul style="list-style-type: none"> ▪ 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

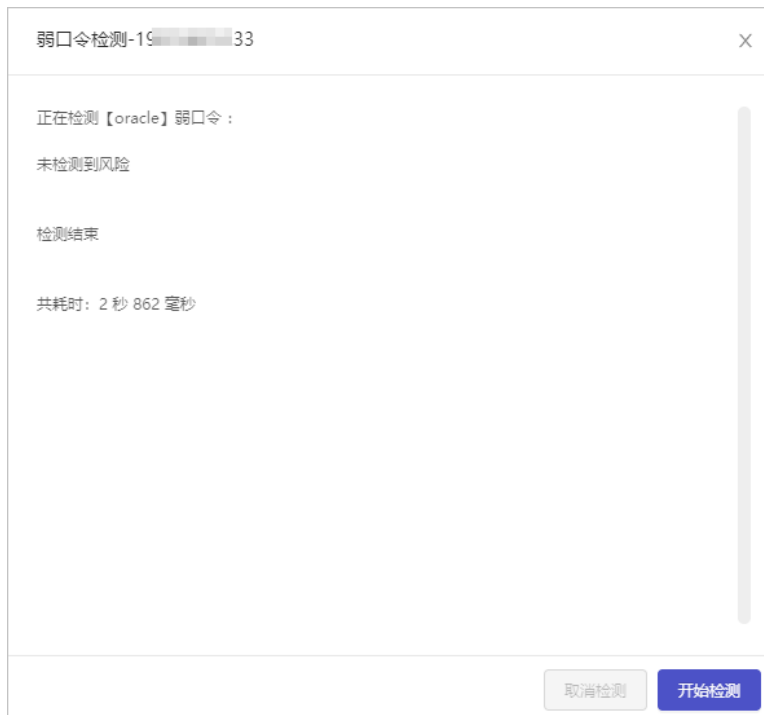


步骤7 执行“弱口令检查”。

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



步骤8 查看“风险扫描结果”。

1. 单击“风险报告”页签。
2. 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。

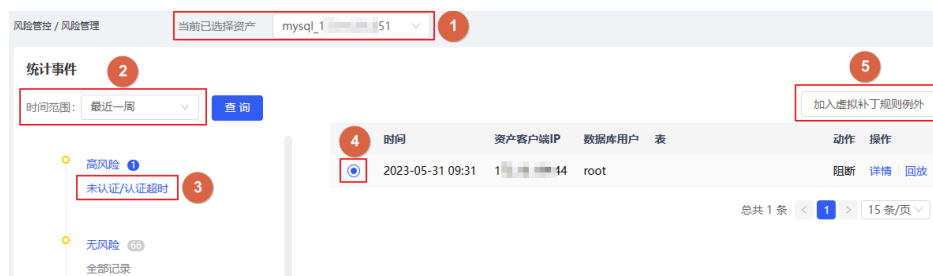
操作步骤

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



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[设置虚拟补丁](#)。

----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



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



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

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) 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 14:18:22 ~ 2022-04-05 14:18:22

申请事由: 备注:

* 审批意见: 审批通过

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		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。
 - 找到目标数据库操作员，单击“配置中心”。
 - 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



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 手动添加账号 。
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[通过Web安全客户端访问资产](#)。

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

图 17-47 展示了日志配置界面。界面顶部有两个复选框，均已勾选：'启用日志集中管理' 和 '本地继续记录日志'。下方有一个输入框，用于填写'日志集中管理地址'，右侧有一个蓝色的'保存'按钮。再下方是一个下拉菜单，用于选择'日志保存时间'，当前显示为'六个月'，右侧也有一个蓝色的'保存'按钮。最底部有一个'清除业务日志'的按钮。

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”。
4. 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。

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

状态: 启用 禁用

备份时间: 在每天的 1 (0~23)点备份昨天日志

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



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

The screenshot shows a 'New Account' form with the following fields and values:

- * 账号: demo_user
- * 密码: [masked]
- * 密码确认: [masked]
- * 使用人: 张三
- * 角色: 系统管理员
- * 电话: 13000000000
- * 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)

Buttons: 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	<ul style="list-style-type: none">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： <ul style="list-style-type: none">永久：账号不会过期停用。定义期限：选中后，设置时间期限，到期停用账号。
备注说明	填写账号的描述信息。

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[审核账号](#)。

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



----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



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。

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



1. 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



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。
3. 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。
4. 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](#)。

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



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

编辑网口

1. 输入IP前，请确保您输入的IP可用；
2. 修改网关地址前，请确保您了解网关地址对网络的影响，谨慎操作，避免断网！

网口名称：ens32

网口类型：管理口

IP地址：192.168.1.61

子网掩码：255.255.255.0

网关地址：192.168.1.1

取消 确定

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： <ul style="list-style-type: none">• 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

添加路由

● 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！

目标地址: 192.168.1.1

子网掩码: 255.255.255.0

下一跳地址: 192.168.1.1

接口: 自动 选择接口

取消 确定

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： <ul style="list-style-type: none">● 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



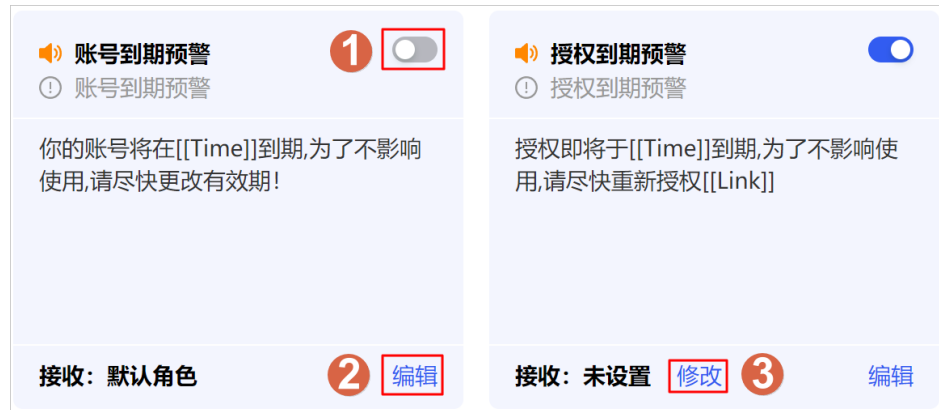
步骤3 在消息中心页面查看最近的通知告警等信息。

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



----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

* 上级审批人: 小明

部门: xx部

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



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	创建者	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	<input checked="" type="checkbox"/>	
安全管理员	-	2019-06-13 14:21:48	安全管理员	<input checked="" type="checkbox"/>	
审计管理员	-	2019-06-13 14:21:48	审计管理员	<input checked="" type="checkbox"/>	
系统管理员	-	2019-06-13 14:21:48	系统管理员	<input checked="" type="checkbox"/>	

---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: 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	<ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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

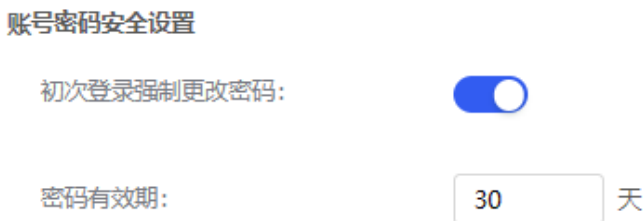
操作步骤

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



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。

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

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： <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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”。

步骤3 单击“操作日志”。


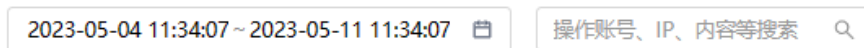
步骤4 可选： 设置过滤条件，单击 ，查询对应操作审计日志。

图 17-66 设置过滤条件



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[设置审批架构](#)。

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

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，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。

- 单击“添加”，配置数据库操作，单击“确定”。

图 17-68 添加操作

表 17-28 添加操作

参数		说明
操作方式	常规操作	- 使用常规的SQL操作，支持设置以下参数： <ul style="list-style-type: none"> 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
	操作语句	- 在操作语句中直接输入具体的操作语句。
	SQL脚本	- 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[管理运维人员](#)。

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[发起运维工单申请](#)。

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[统一身份认证服务](#)（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[表18-1](#)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](#)。

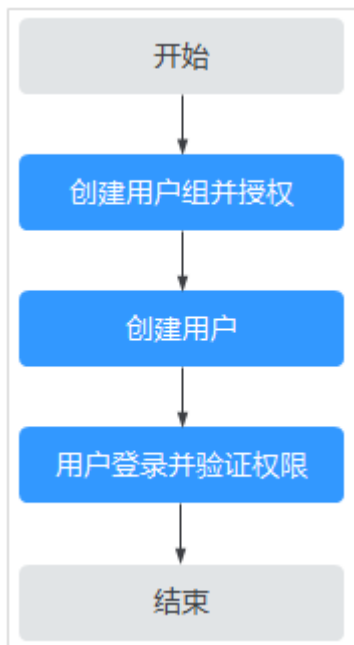
表 18-1 DBSS 系统权限

系统角色/策略名称	描述	类别	依赖关系
DBSS Auditor	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 ReadOnlyAccess	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：

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "dbss:auditInstance:delete"
      ],
      "Effect": "Deny"
    }
  ]
}
```

- 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:unlock",
      "hss:commonIPs:set"
    ]
  }
]
}

```

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**角色**和**策略**。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 global 权限	敏感权限规避措施
obs:bucket:CreateBucket	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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:PutObject	agent在CCE场景部署时，将实例配置信息上传到obs桶。	是	<ul style="list-style-type: none"> 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:createAgency iam:permissions:grantRoleToAgency iam:permissions:grantRoleToAgencyOnEnterpriseProject iam:permissions:grantRoleToAgencyOnDomain iam:permissions:grantRoleToAgencyOnProject	<ul style="list-style-type: none"> 备份和风险导出场景，创建名为"dbss_depend_obs_trust"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lts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	<ul style="list-style-type: none"> 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。
bss:order:pay	购买审计实例时，进行订单支付。	否	<ul style="list-style-type: none"> 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。