数据库安全服务

用户指南

文档版本 04

发布日期 2023-05-15

华为云计算技术有限公司

商标声明


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。

目 录

1 产品介绍

1.1 什么是数据库安全服务?

数据库安全服务，即DBSS（Database Security Service），提供旁路模式数据库安全审计服务功能，通过实时记录用户访问数据库行为，形成细粒度的审计报告，对风险行为和攻击行为进行实时告警。同时，数据库安全审计可以生成满足数据安全标准（例如Sarbanes-Oxley）的合规报告，对数据库的内部违规和不正当操作进行定位追责，保障数据资产安全。

支持的数据库

数据库安全审计可以为管理控制台上的以下数据库提供旁路模式的数据库审计功能：

- 云数据库
- 弹性云服务器（Elastic Cloud Server，ECS）的自建数据库
- 裸金属服务器（Bare Metal Server，BMS）的自建数据库

数据库安全审计支持数据库类型及版本如表1-1所示。

表 1-1 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	• 5.0、5.1、5.5、5.6、5.7 • 8.0（8.0.11及以前的子版本） • 8.0.20 • 8.0.23
Oracle	• 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

数据库类型	版本
PostgreSQL	• 7.4 • 8.0 8.0、8.1、8.2、8.3、8.4 • 9.0 9.0、9.1、9.2、9.3、9.4、9.5、9.6 • 10.0 10.0、10.1、10.2、10.3、10.4、10.5 • 11.0 • 12.0 • 13.0 • 14.0
SQL Server	• 2008、2008R2 • 2012 • 2014 • 2016 • 2017
DWS	• 1.5
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0
TAURUS	MySQL 8.0

服务特点

- 支持备份和恢复数据库审计日志，满足审计数据保存期限要求
- 支持风险分布、会话统计、会话分布、SQL分布的实时监控能力
- 提供风险行为和攻击行为实时告警能力，及时响应数据库攻击
- 帮助您对内部违规和不正当操作进行定位追责，保障数据资产安全

数据库安全审计采用数据库旁路部署方式，在不影响用户业务的前提下，可以对数据库进行灵活的审计。

- 基于数据库风险操作，监视数据库登录、操作类型（数据定义、数据操作和数据控制）和操作对象，有效对数据库进行审计。
- 从风险、会话、SQL注入等多个维度进行分析，帮助您及时了解数据库状况。
- 提供审计报表模板库，可以生成日报、周报或月报审计报表（可设置报表生成频率）。同时，支持发送报表生成的实时告警通知，帮助您及时获取审计报表。

1.2 功能特性

数据库安全审计提供用户行为发现审计、多维度分析、实时告警和报表功能。

- 用户行为发现审计
  - 关联应用层和数据库层的访问操作。
  - 提供内置或自定义隐私数据保护规则，防止审计日志中的隐私数据（例如，帐号密码）在控制台上以明文显示。
- 多维度线索分析
  - 行为线索

    支持审计时长、语句总量、风险总量、风险分布、会话统计、SQL分布等多维度的快速分析。
  - 会话线索

    支持根据时间、数据库用户、客户端等多角度进行分析。
  - 语句线索

    提供时间、风险等级、数据用户、客户端IP、数据库IP、操作类型、规则等多种语句搜索条件。
- 风险操作、SQL注入实时告警
  - 风险操作

    支持通过操作类型、操作对象、风险等级等多种元素细粒度定义要求监控的风险操作行为。
  - SQL注入

    数据库安全审计提供SQL注入库，可以基于SQL命令特征或风险等级，发现数据库异常行为立即告警。
  - 系统资源

    当系统资源（CPU、内存和磁盘）占用率达到设置的告警阈值时立即告警。
- 针对各种异常行为提供精细化报表
  - 会话行为

    提供客户端和数据库用户会话分析报表。
  - 风险操作

    提供风险分布情况分析报表。

1.3 产品优势

数据库安全审计提供的旁路模式数据库审计功能，可以对风险行为进行实时告警。同时，通过生成满足数据安全标准的合规报告，可以对数据库的内部违规和不正当操作进行定位追责，保障数据资产安全。

- 部署简单

  采用数据库旁路部署方式，操作简单，快速上手。
- 全量审计

  支持对管理控制台上的RDS、ECS/BMS自建的数据库进行审计。

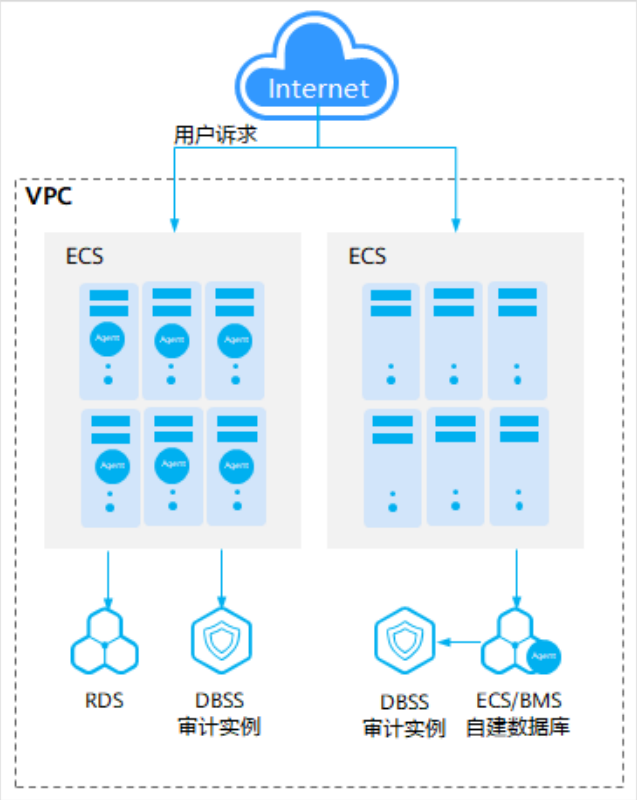
- 快速识别
  实现99%+的应用关联审计、完整的SQL解析、精确的协议分析。
- 高效分析
  每秒万次入库、海量存储、亿级数据秒级响应。
- 三权分立
  系统管理员，安全管理员，审计管理员权限分离，满足审计安全需求。

1.4 部署架构

数据库安全审计采用数据库旁路部署方式，支持对管理控制台上的RDS、ECS/BMS自建的数据库进行审计。

数据库安全审计部署架构如图1-1所示。

图 1-1 数据库安全审计部署架构



数据库安全审计的Agent部署说明如下：

- ECS/BMS自建数据库：在数据库端部署Agent
- RDS关系型数据库：在应用端或代理端部署Agent

1.5 服务版本规格

数据库安全审计提供了基础版、专业版和高级版三种服务版本。您可以根据业务需求选择相应的服务版本。

各版本的性能规格说明如表1-2所示。

表 1-2 数据库安全审计版本性能规格说明

版本	支持的数据库实例	系统资源要求	性能参数
基础版	最多支持3个数据库实例	• CPU：4U • 内存：16GB • 硬盘：560GB	• 吞吐量峰值：3,000条/秒 • 入库速率：360万条/小时 • 4亿条在线SQL语句存储 • 50亿条归档SQL语句存储
专业版	最多支持6个数据库实例	• CPU：8U • 内存：32GB • 硬盘：1T	• 吞吐量峰值：6,000条/秒 • 入库速率：720万条/小时 • 6亿条在线SQL语句存储 • 100亿条归档SQL语句存储

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IP_1和IP_2，IP_1有一个数据库端口，则为1个数据库实例；IP_2有3个数据库端口，则为3个数据库实例。IP_1和IP_2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，请退订后重新申请。
- 云原生版仅支持在RDS控制台购买。
- 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。

1.6 使用约束

在使用数据库安全审计前，您需要了解数据库安全审计的使用限制。

支持的数据库类别

数据库安全审计可以为管理控制台上的以下数据库提供旁路模式的审计功能：

- 云数据库
- 弹性云服务器（Elastic Cloud Server ，ECS）的自建数据库
- 裸金属服务器（Bare Metal Server，BMS）的自建数据库

支持安装 Agent 数据库类型及版本

支持的数据库类型及版本如表1-3所示。

表 1-3 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	• 5.0、5.1、5.5、5.6、5.7 • 8.0（8.0.11及以前的子版本） • 8.0.20 • 8.0.23
Oracle	• 11g 11.1.0.6.0 、11.2.0.1.0 、11.2.0.2.0、11.2.0.3.0、11.2.0.4.0 • 12c 12.1.0.2.0 、12.2.0.1.0 • 19c
PostgreSQL	• 7.4 • 8.0 8.0、8.1、8.2、8.3、8.4 • 9.0 9.0、9.1、9.2、9.3、9.4、9.5、9.6 • 10.0 10.0、10.1、10.2、10.3、10.4、10.5 • 11.0 • 12.0 • 13.0 • 14.0
SQL Server	• 2008、2008R2 • 2012 • 2014 • 2016 • 2017
DWS	• 1.5
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0
TAURUS	MySQL 8.0

Agent 支持的操作系统

使用数据库安全审计功能，必须在数据库节点或应用节点安装Agent。数据库安全审计的Agent可运行在Linux64位和Windows64位操作系统上。

- 数据库安全审计的Agent支持的Linux系统版本如表1-4所示。

  表 1-4 Agent 支持的 Linux 系统版本说明

系统名称	系统版本
CentOS	• CentOS 7.0 (64bit) • CentOS 7.1 (64bit) • CentOS 7.2 (64bit) • CentOS 7.3 (64bit) • CentOS 7.4 (64bit) • CentOS 7.5 (64bit) • CentOS 7.6 (64bit) • CentOS 7.8 (64bit) • CentOS 8.0 (64bit)
Debian	• Debian 7.5.0 (64bit) • Debian 8.2.0 (64bit) • Debian 8.8.0 (64bit) • Debian 9.0.0 (64bit)
Fedora	• Fedora 24 (64bit) • Fedora 25 (64bit)
SUSE	• SUSE 11 SP4 (64bit) • SUSE 12 SP1 (64bit) • SUSE 12 SP2 (64bit)
Ubuntu	• Ubuntu 14.04 (64bit) • Ubuntu 16.04 (64bit) • Ubuntu 18.04 (64bit) • Ubuntu 20.04 (64bit)
EulerOS	• Euler 2.2 (64bit) • Euler 2.3 (64bit)
Oracle Linux	• Oracle Linux 6.9 (64bit) • Oracle Linux 7.4 (64bit)

- 数据库安全审计的Agent支持的Windows系统版本如下所示：
  - Windows Server 2008 R2(64bit)
  - Windows Server 2012 R2(64bit)

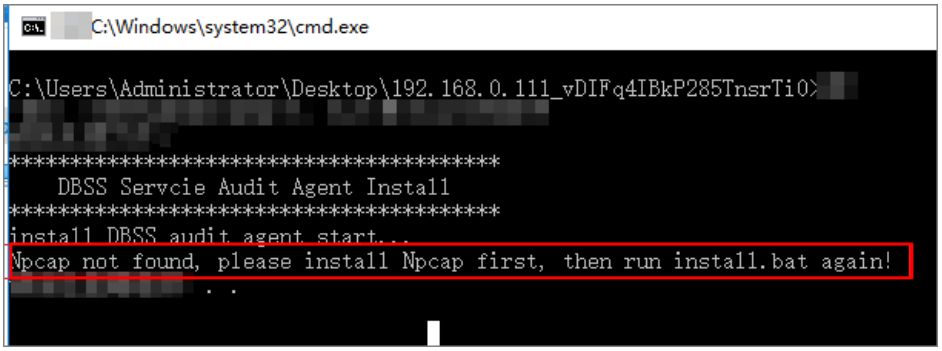
- Windows Server 2016(64bit)
- Windows 7(64bit)
- Windows 10(64bit)

说明

DBSS Agent的运行依赖Npcap，如果安装过程中提示"Npcap not found，please install Npcap first"，请安装Npcap后，再安装DBSS Agent。

Npcap下载链接：**https://npcap.com/#download**

图 1-2 Npcap not found



其他约束条件

- 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。
- 申请数据库安全审计实例配置VPC时，需与待安装Agent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。
- 部分SQLserver中的复杂declare语句、select函数和包含系统无法识别的符号语句可能无法解析。

1.7 DBSS 权限管理

如果您需要对云服务平台上创建的DBSS 资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制云服务资源的访问。

通过IAM，您可以在帐号中给员工创建IAM用户，并授权控制他们对云服务资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有DBSS的使用权限，但是不希望他们拥有删除DBSS等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用DBSS，但是不允许删除DBSS的权限，控制他们对DBSS资源的使用范围。

如果帐号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用DBSS服务的其它功能。

IAM是云服务平台提供权限管理的基础服务，无需付费即可使用，您只需要为您帐号中的资源进行付费。

关于IAM的详细介绍，请参见**IAM产品简介**。

DBSS 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

DBSS部署时通过物理区域划分，为项目级服务。授权时，“授权范围”需要选择“指定区域项目资源”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果“授权范围”选择“所有资源”，则该权限在所有区域项目中都生效。访问DBSS时，需要先切换至授权区域。

权限根据授权精细程度分为角色和策略。

- 角色：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。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于云服务平台各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对ECS服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，权限的最小粒度为API授权项（action），DBSS支持的API授权项请参见策略支持的授权项。

表 1-5 DBSS 系统角色

角色名称	描述	依赖关系
DBSS System Administrator （数据库安全服务系统管理员，拥有操作数据库安全服务系统资源的权限）	● 数据库安全审计操作权限： – 购买实例。 – 开启、关闭、重启实例。 – 获取实例列表。 – 获取基本信息。 – 获取审计概况。 – 获取监控信息。 – 获取操作日志。 – 数据库管理。 – Agent管理。 – 邮件设置。 – 备份与恢复。	进行付费操作（例如，购买DBSS实例、续费）时需要同时具有BSS Administrator角色、VPC Administrator角色和ECS 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。 ● BSS Administrator：对帐号中心、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。

角色名称	描述	依赖关系
DBSS Audit Administrator （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）	• 数据库安全审计操作权限： – 获取实例列表。 – 获取基本信息。 – 获取审计概况。 – 获取报表结果。 – 获取规则信息。 – 获取语句信息。 – 获取会话信息。 – 获取监控信息。 – 获取操作日志。 – 获取数据库列表。 – 报表管理。	无
DBSS Security Administrator （数据库安全服务安全管理员，拥有设置数据库安全服务安全策略的权限）	• 数据库安全审计操作权限： – 获取实例列表。 – 获取基本信息。 – 获取审计概况。 – 获取报表结果。 – 获取规则信息。 – 获取语句信息。 – 获取会话信息。 – 获取监控信息。 – 获取操作日志。 – 获取数据库列表。 – 审计规则设置。 – 告警通知设置。 – 报表管理。	无

表1-6列出了DBSS常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 1-6 常用操作与系统权限的关系

操作	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
购买实例	√	×	√

操作	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
开启、关闭、重启实例	√	×	×
获取实例列表	√	×	×
获取基本信息	√	√	√
获取审计概况	√	√	√
获取监控信息	√	√	√
获取操作日志	√	√	√
数据库管理	√	×	×
Agent管理	√	×	×
邮件设置	√	×	×
备份与恢复	√	√	×
获取报表结果	√	√	√
获取规则信息	√	√	√
获取语句信息	√	√	√
获取会话信息	√	√	√
获取数据库列表	√	√	√
报表管理	×	√	×
审计规则设置	×	×	√
告警通知设置	×	×	×

1.8 与其他云服务的关系

与弹性云服务器的关系

数据库安全服务实例创建在弹性云服务器上，用户可以通过该实例，为弹性云服务器上的自建数据库提供安全审计功能。

与关系型数据库的关系

数据库安全服务可以为关系型数据库服务中的RDS实例提供安全审计功能。

与裸金属服务器的关系

数据库安全服务可以为裸金属服务器上的自建数据库提供安全审计功能。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）记录数据库安全服务相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见《云审计服务用户指南》。

表 1-7 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

与对象存储服务的关系

对象存储服务（Object Storage Service，简称OBS）是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力。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。

与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management，简称IAM）为数据库安全服务提供了权限管理的功能。

需要拥有DBSS System Administrator权限的用户才能使用DBSS。

如需开通该权限，请联系拥有Security Administrator权限的用户，详细内容请参考《统一身份认证服务用户指南》。

2 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管理控制台上的ECS/BMS自建数据库和RDS关系型数据库进行审计。

须知

- 申请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。

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

图 2-1 快速使用数据库安全审计流程图

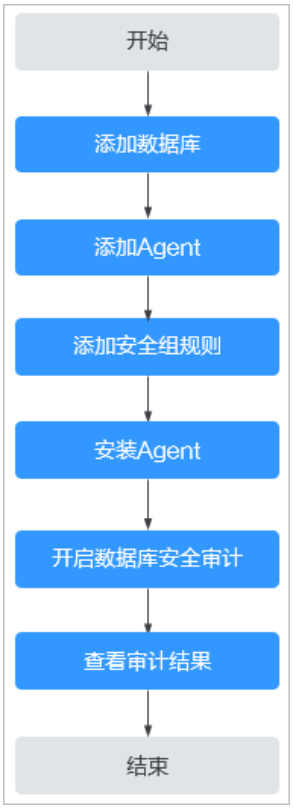


表 2-1 快速使用数据库安全审计操作步骤

步骤	配置操作	说明
1	添加数据库	申请数据库安全审计后，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	添加的数据库开启审计功能后，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，请根据您在管理控制台上实际部署的数据库选择Agent添加方式。
4	安装Agent（Linux操作系统）	添加Agent后，您需要下载Agent，并根据Agent的添加方式在数据库端或应用端安装Agent。
5	开启数据库安全审计	Agent安装成功后，您还需要开启数据库安全审计功能，将添加的数据库连接到数据库安全审计实例，才能使用数据库安全审计功能。

步骤	配置操作	说明
6	查看审计结果	数据库安全审计默认提供一条“全审计规则”的审计范围，可以对连接数据库安全审计实例的所有数据库进行审计。开启数据库安全审计后，您可以在数据库安全审计界面查看被添加的数据库的审计结果。

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。

3 申请数据库安全审计实例

在使用数据库安全审计功能前，您需要申请数据库安全审计实例。

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。

系统影响

数据库安全审计为旁路模式审计，不影响用户业务，与本地审计工具不冲突。

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 ☰，选择“安全 > 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“申请数据库安全审计实例”。

步骤4 在申请实例界面，选择“可用区”和“性能规格”。

- 可用区：提交申请时，如果提示“可用区资源已售罄”，请切换可用区再进行操作。
- 性能规格：支持的规格与性能参数请查看**服务版本规格**。

步骤5 设置数据库安全审计参数，相关参数说明如**表3-1**所示。

表 3-1 数据库安全审计实例参数说明

参数名称	说明	取值样例
虚拟私有云	可以选择使用已有的虚拟私有云（Virtual Private Cloud，VPC）网络，或者单击“查看虚拟私有云”创建新的虚拟私有云。 **说明** • 请选择Agent安装节点（应用端或数据库端）所在的VPC。 • 不支持修改VPC。若要修改，请退订后重新申请。 更多有关虚拟私有云的信息，请参见《虚拟私有云用户指南》。	vpc-sec
安全组	界面显示实例已配置的安全组。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》。	sg
子网	界面显示所有可选择的子网。 更多有关子网的信息，请参见《虚拟私有云用户指南》。	public_subnet
实例名称	您可以自定义实例的名称。	DBSS-test

步骤6 确认当前配置无误后，单击“立即申请”。

步骤7 在详情确认页面，单击“提交”。

在“数据库安全审计 > 实例列表”，可以查看数据库安全审计实例的创建情况。

当申请实例的“运行状态”为“运行中”时，说明实例申请成功。

----结束

4 步骤一：添加数据库

数据库安全审计支持对管理控制台上的RDS关系型数据库、ECS/BMS自建数据库进行审计。申请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。

前提条件

已成功申请数据库安全审计实例，且实例的状态为“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 ☰，选择“安全 > 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”。

步骤6 在弹出的对话框中，设置数据库的信息，如图4-1所示，相关参数说明如表 数据库参数说明所示。

图 4-1 “添加数据库”对话框

表 4-1 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。	RDS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：fe80:0000:0000:0000:0000:0000:0000:0000
数据库类型	支持的数据库类型，您可以选择以下类型： ● MYSQL ● ORACLE ● POSTGRESQL ● SQLSERVER ● DWS ● TAURUS ● GaussDB ● DAMENG ● KINGBASE ● SHENTONG ● GBase 8a ● GBase XDM Cluster ● Greenplum ● HighGo ● Mariadb ● Hive **说明** ● 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。	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	支持的数据库版本。 ● 当“数据库类型”选择“MYSQL”时，您可以选择以下版本： – 5.0、5.1、5.5、5.6、5.7 – 8.0（8.0.11及以前的子版本） – 8.0.20 – 8.0.23 ● 当“数据库类型”选择“ORACLE”时，您可以选择以下版本： – 11g – 12c – 19c ● 当“数据库类型”选择“POSTGRESQL”时，您可以选择以下版本： – 7.4 – 8.0 8.0、8.1、8.2、8.3、8.4 – 9.0 9.0、9.1、9.2、9.3、9.4、9.5、9.6 – 10.0 10.0、10.1、10.2、10.3、10.4、10.5 – 11.0 – 12.0 – 13.0 ● 当“数据库类型”选择“SQLSERVER”时，您可以选择以下版本： – 2008 – 2012 – 2014 – 2016 – 2017 ● 当“数据库类型”选择“DWS”时，您可以选择以下版本： – 1.5 ● 当“数据库类型”选择“TAURUS”时，您可以选择以下版本： – MySQL 8.0 ● 当“数据库类型”选择“GaussDB”时，您可以选择以下版本： – 1.4企业版	5.0

参数名称	说明	取值样例
	• 当“数据库类型”选择“DAMENG”时，您可以选择以下版本： – DM8 • 当“数据库类型”选择“KINGBASE”时，您可以选择以下版本： – V8	
实例名	您可以指定需要审计的数据库的实例名称。 **说明** • 如果实例名为空，数据库安全审计将审计数据库中所有的实例。 • 如果填写实例名，数据库安全审计将审计填写的实例，最多可填写5个实例名，且实例名以“;”分隔。	-
选择字符集	支持的数据库字符集的编码格式，您可以选择以下编码格式： • UTF-8 • GBK	UTF-8
操作系统	添加的数据库运行的操作系统，您可以选择以下操作系统： • LINUX64	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，如图4-2所示。

图 4-2 数据库添加完成

说明

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

----结束

5 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。

完成添加Agent后，您还需要为Agent安装节点所在的安全组添加入方向规则TCP协议（8000端口）和UDP协议（7000-7100端口），使Agent与审计实例之间的网络连通，数据库安全审计才能对添加的数据库进行审计。

说明

目前仅如下几种类型数据库支持免Agent审计。

- 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）

前提条件

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已成功添加数据库。

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5-1和图5-2所示。

图 5-1 一个应用端连接多个 ECS/BMS 自建数据库

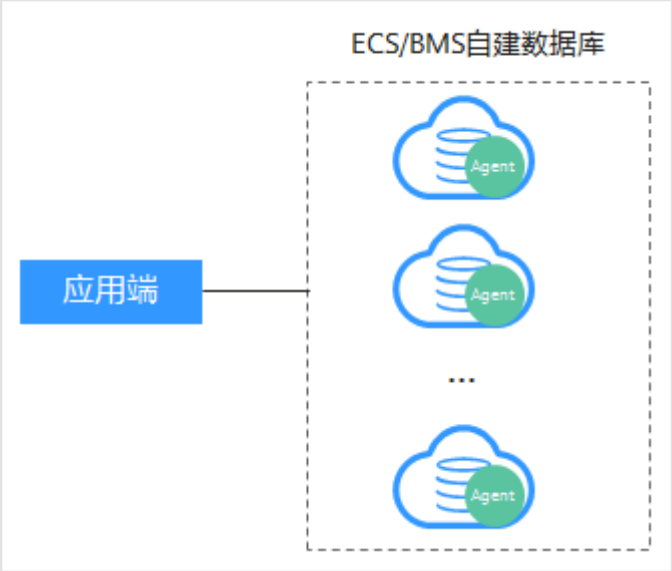
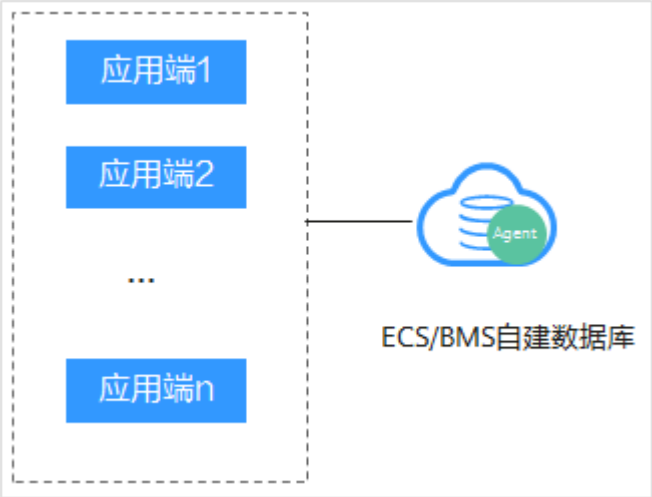


图 5-2 多个应用端连接同一个 ECS/BMS 自建数据库



- RDS关系型数据库的常见部署场景如图5-3和图5-4所示。

图 5-3 一个应用端连接多个 RDS

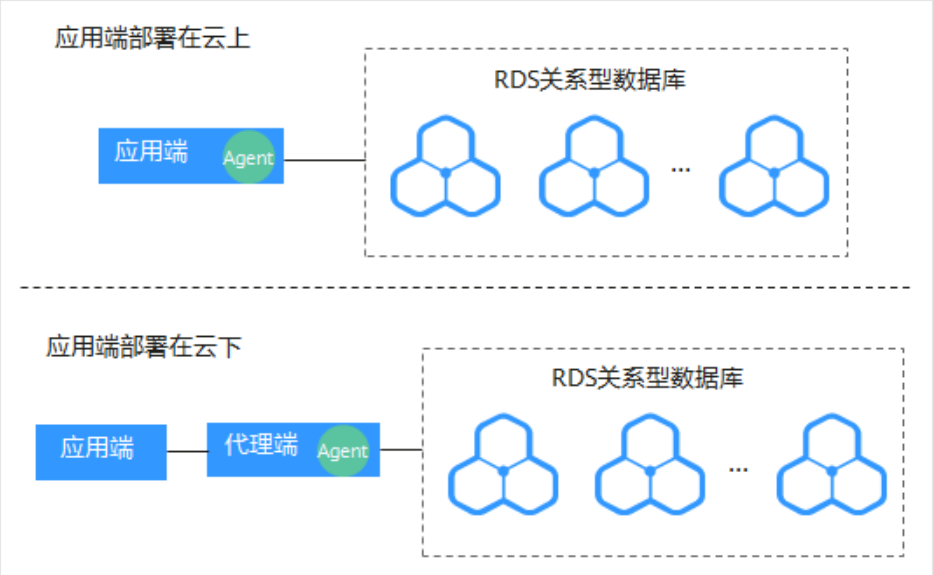
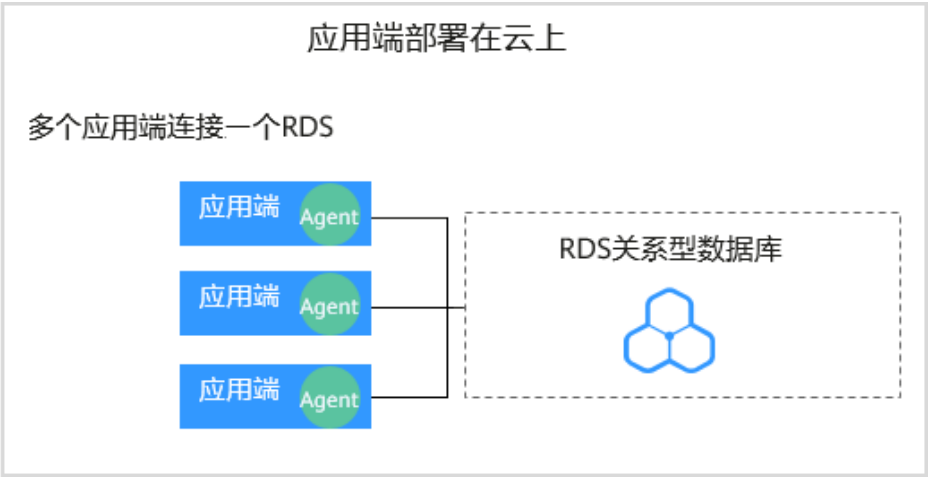


图 5-4 多个应用端连接同一个 RDS



添加Agent方式的详细说明如表5-1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需在数据库端添加。

表 5-1 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	可以审计所有访问该数据库的应用端的所有访问记录。	• 在数据库端添加Agent。 • 当某个应用端连接多个ECS/BMS自建数据库时，所有连接该应用端的数据库都需要添加Agent。
RDS关系型数据库	应用端（应用端部署在云上）	可以审计该应用端与其连接的所有数据库的访问记录。	• 在应用端添加Agent。 • 当某个应用端连接多个RDS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选择“安装节点类型”后，其余RDS添加Agent时，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时，所有连接该RDS的应用端都需要添加Agent。
	代理端（应用端部署在云下）	只能审计代理端与后端数据库之间的访问记录，无法审计应用端与后端数据库的访问记录。	• 在应用端添加Agent。 • “安装节点IP”需要配置为代理端的IP地址。

添加 Agent（ECS/BMS 自建数据库）

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 ☰，选择“安全 > 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Agent的数据库所属的实例。

步骤5 在添加的数据库所在行的“Agent”列，单击“添加Agent”。

步骤6 在弹出的“添加Agent”对话框中，选择添加方式，如**图5-5**所示，相关参数说明如**表5-2**所示。

图 5-5 在数据库端添加 Agent

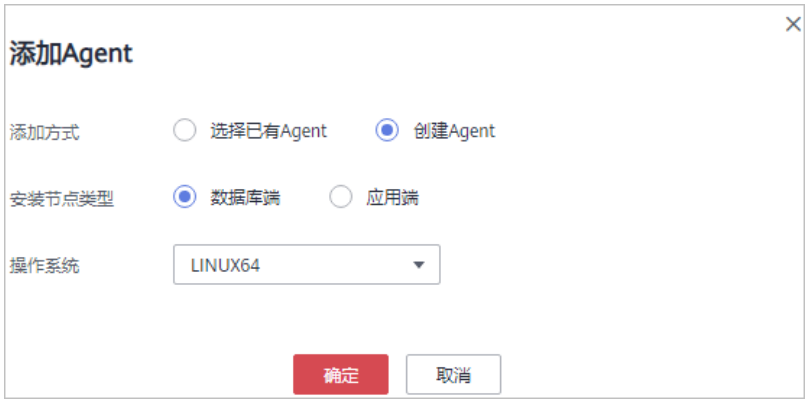


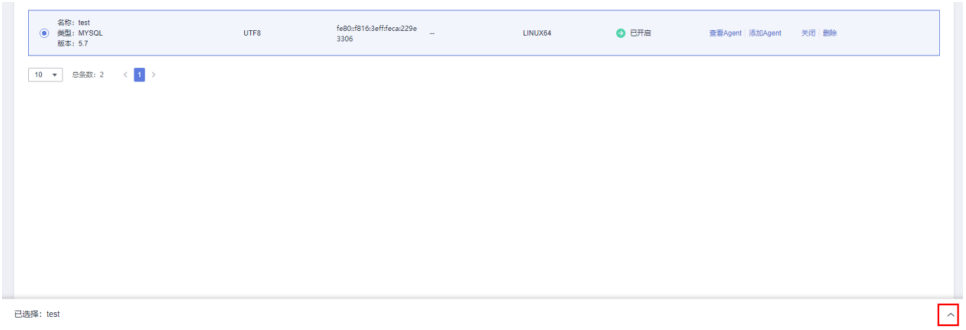
表 5-2 添加 Agent 参数说明（ECS/BMS 自建数据库）

参数名称	说明	取值样例
添加方式	您可以选择Agent的添加方式。 • 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
安装节点类型	当“添加方式”选择“创建Agent”时，需配置该参数。 审计ECS/BMS自建数据库，选择“数据库端”。	数据库端
操作系统	指待审计的数据库的操作系统，支持。 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LINUX64_X86或者LINUX64_ARM架构版本。	LINUX64-X86

步骤7 单击“确定”，Agent添加成功。

步骤8 单击“数据库列表”页面下方的 ^ 展开该数据库的详细信息，查看添加的Agent信息。

图 5-6 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“More”选择“删除”，删除Agent后，再重新添加Agent。

----结束

添加 Agent（RDS 关系型数据库）

说明

对于数据库类型为“MYSQL”和“GaussDB(for MySQL)”的RDS关系型数据库，在添加数据库成功后Agent免安装，您可以直接进行步骤四：添加安全组规则。

当某个应用端连接了多个RDS时， 请按以下方式添加Agent：

- 连接该应用端所有的RDS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，请选择“选择已有Agent”添加方式。

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 ☰，选择“安全 > 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Agent的数据库所属的实例。

步骤5 在添加的数据库所在行的“Agent”列，单击“添加Agent”。

步骤6 在弹出的“添加Agent”对话框中，选择添加方式，如图5-7和图5-8所示，相关参数说明如表5-3所示。

- “添加方式”选择“选择已有Agent”

  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 5-7 选择已有 Agent

- “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 5-8 在应用端添加 Agent

表 5-3 添加 Agent 参数说明（RDS 关系型数据库）

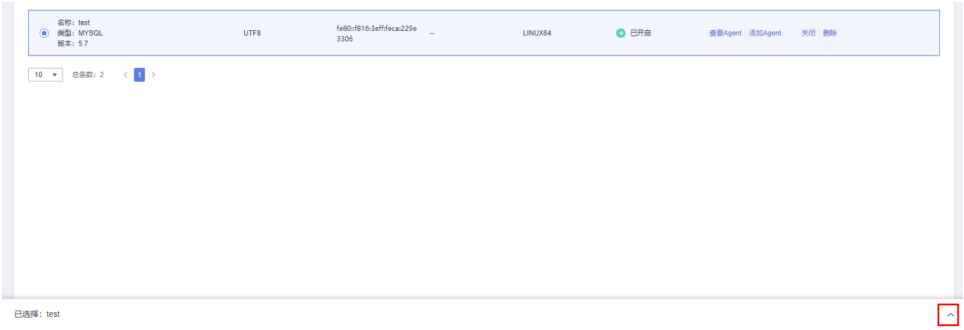
参数名称	说明	取值样例
添加方式	您可以选择Agent的添加方式。 • 选择已有Agent 当某个应用端连接了多个数据库时，如果该应用端的一个数据库已经在应用端添加了Agent。其他数据库在添加Agent时，只需要选择“选择已有Agent”添加方式。 • 创建Agent 如果待添加Agent的数据库需要创建Agent，请创建新的Agent。	创建Agent

参数名称	说明	取值样例
安装节点类型	当“添加方式”选择“创建Agent”时，需配置该参数。 审计RDS关系型数据库，需要选择“应用端”。	应用端
安装节点IP	“安装节点类型”选择“应用端”时，需配置该参数。安装节点IP只能填写一个，每个Agent安装节点IP不同。 IP地址为应用端内网IP地址。 IP必须为内网IP地址，支持IPv4和IPv6格式。 **须知** 当审计RDS关系型数据库且应用端在云下时，代理端将作为应用端，此时，“安装节点IP”需要配置为代理端的IP地址。	192.168.1.1
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”或“WINDOWS64”。	LINUX64

步骤7 单击“确定”，Agent添加成功。

步骤8 单击“数据库列表”页面下方的 ^ 展开该数据库的详细信息，查看添加的Agent信息。

图 5-9 Agent 已添加完成



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“More”选择“删除”，删除Agent后，再重新添加Agent。

----结束

后续处理

Agent添加完成后，您还需要根据Agent的添加方式在数据库端或应用端安装Agent，将添加的数据库连接到数据库安全审计实例，数据库安全审计才能对添加的数据库进行审计。有关安装Agent的详细操作，请参见**安装Agent**。

6 步骤三：下载并安装 Agent

6.1 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AgentID，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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 数据库已成功添加Agent。

操作步骤

步骤1 登录管理控制台。

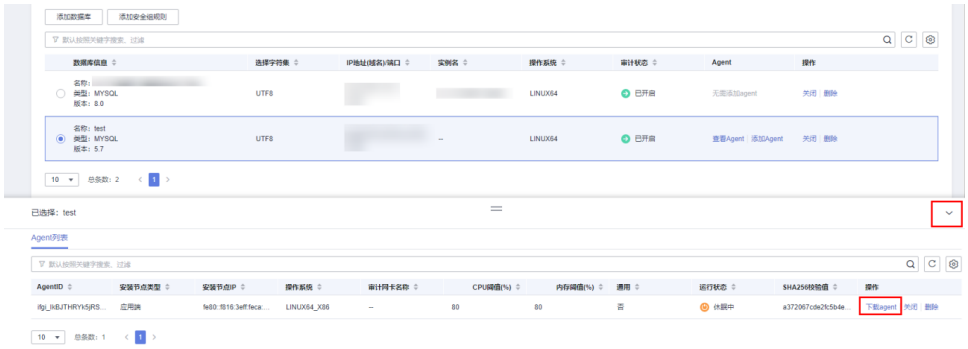
步骤2 在页面上方选择“区域”后，单击 ☰，选择“安全 > 数据库安全服务 DBSS”，进入数据库安全审计“总览”界面。

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，选择需要下载Agent的数据库所属的实例。

步骤5 单击“数据库列表”列表页面下方的 ^ 展开Agent的详细信息，在Agent所在行的“操作”列，单击“下载agent”。将Agent安装包下载到本地。

图 6-1 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

6.2 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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 数据库已成功添加Agent。
- 已获取Linux操作系统Agent安装包。
- 安装Agent节点的运行系统满足Linux系统版本要求。

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6-2**和**图6-3**所示。

图 6-2 一个应用端连接多个 ECS/BMS 自建数据库

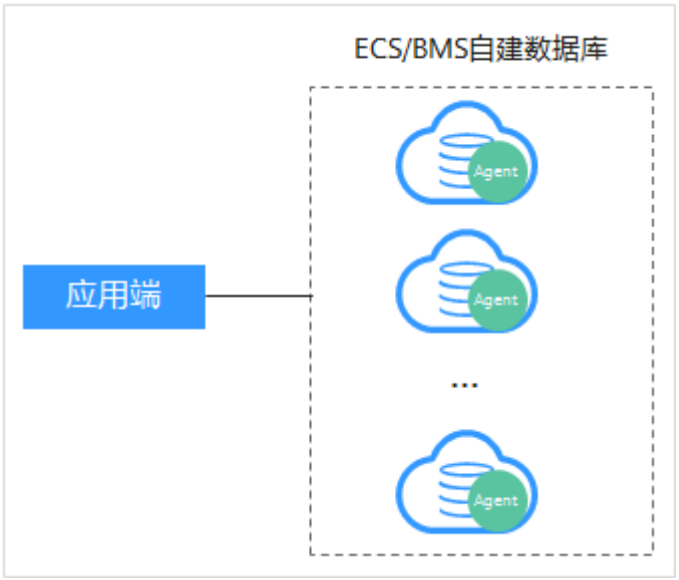
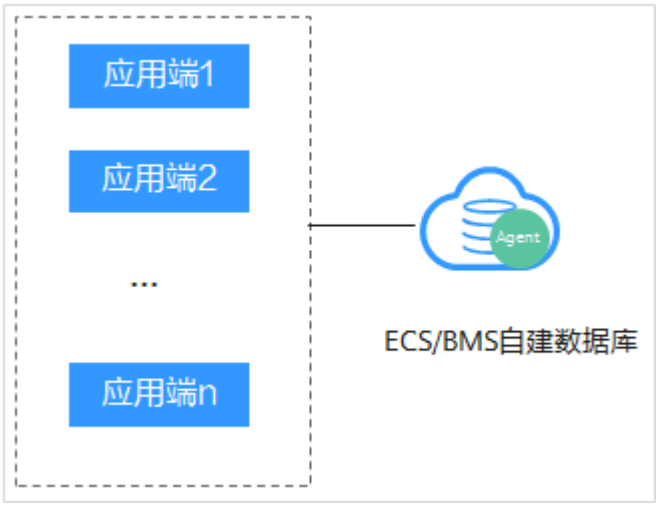


图 6-3 多个应用端连接同一个 ECS/BMS 自建数据库



- RDS关系型数据库的常见部署场景如图6-4和图6-5所示。

图 6-4 一个应用端连接多个 RDS

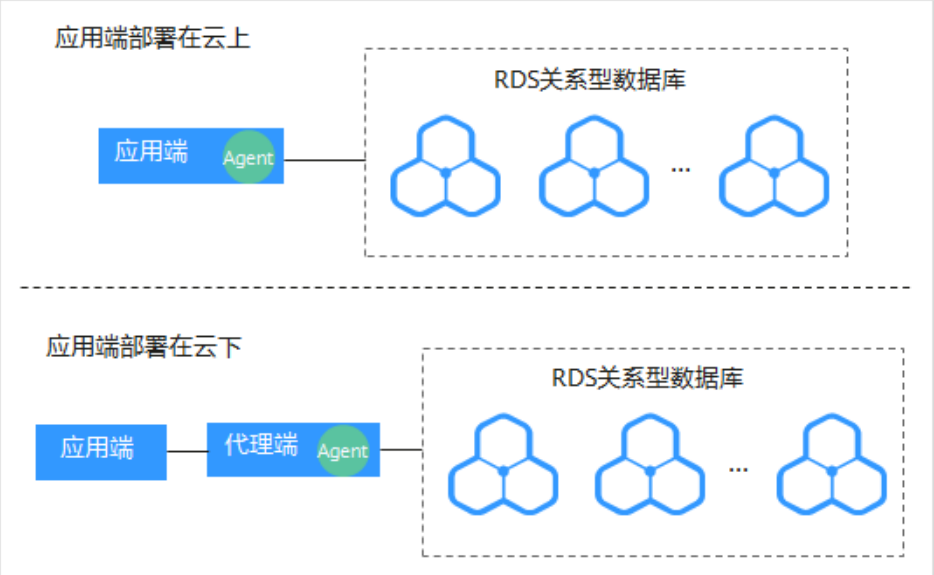
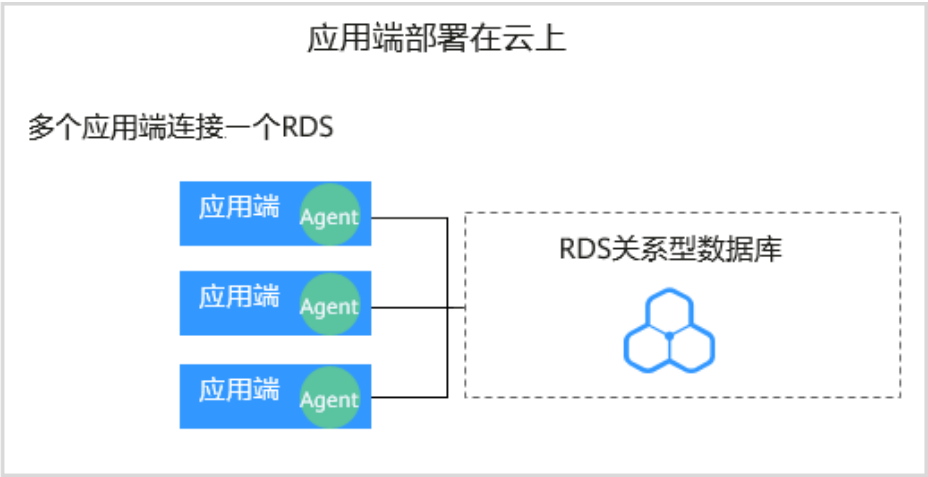


图 6-5 多个应用端连接同一个 RDS



安装Agent节点的详细说明如表6-1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 6-1 安装 Agent 场景说明

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

安装 Agent

说明

在您安装新版Agent的时候，需要您为当前安装的Agent自定义一个密码。

请您根据数据库类型以及数据库的部署环境，在相应节点上安装Agent。

步骤1 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2 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3 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4 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5 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               _9syBZIsBbeAhEFqE_hhD]#
```

步骤6 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7**。
- 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7**。

步骤7 执行以下命令，安装Agent。

sh install.sh

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

说明

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

界面回显以下信息，说明安装成功。否则，说明Agent安装失败。

```
start agent
starting audit agent
audit agent started
start success
install dbss audit agent done!
```

须知

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

步骤8 执行以下命令，查看Agent程序的运行状态。

service audit_agent status

如果界面回显以下信息，说明Agent程序运行正常。

```
[root@ecs-test                _9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test                _9syBZIsBbeAhEFqE_hhD]# service audit_agent status
audit agent is running.
[root@ecs-test                9syBZIsBbeAhEFqE_hhD]#
audit agent is running.
```

----结束

6.3 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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 数据库已成功添加Agent
- 已获取Windows操作系统Agent安装包。
- 安装Agent节点的运行系统满足Windows系统版本要求。

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6-6**和**图6-7**所示。

图 6-6 一个应用端连接多个 ECS/BMS 自建数据库

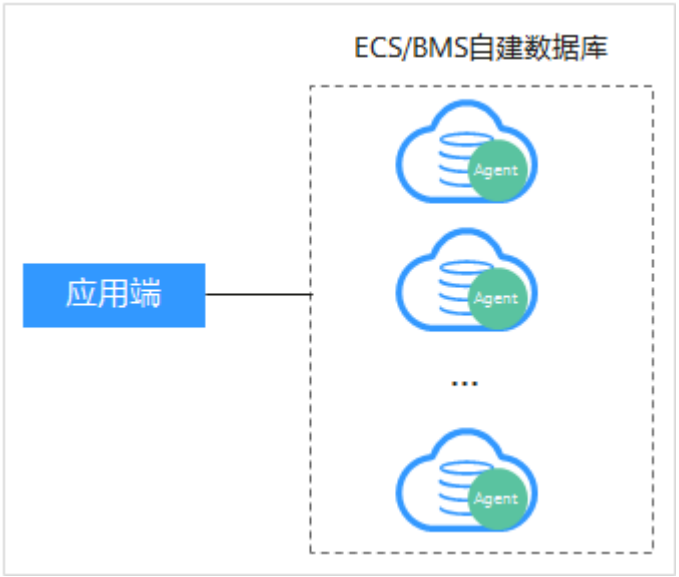
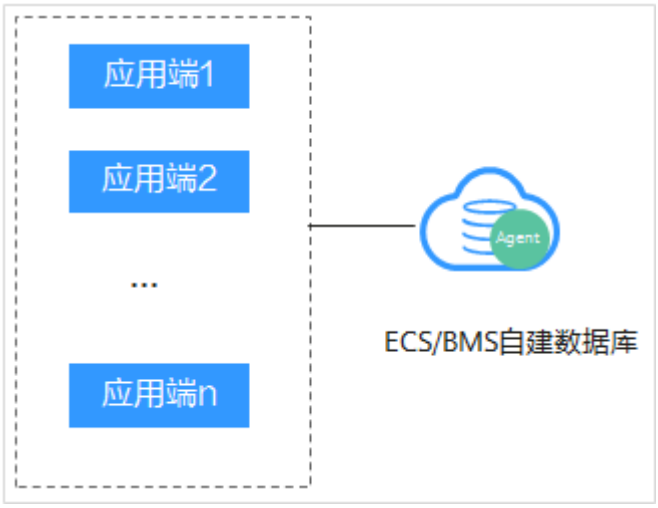


图 6-7 多个应用端连接同一个 ECS/BMS 自建数据库



- RDS关系型数据库的常见部署场景如图6-8和图6-9所示。

图 6-8 一个应用端连接多个 RDS

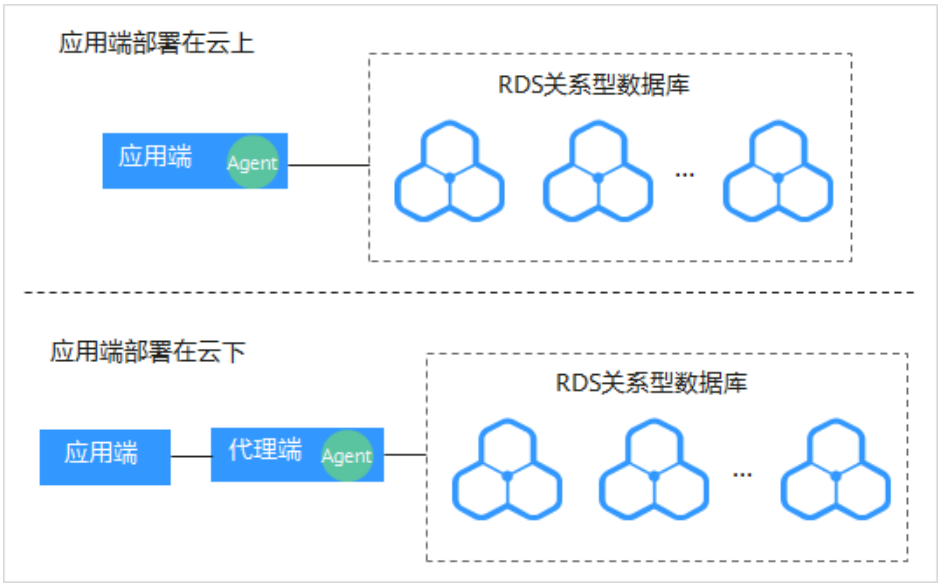
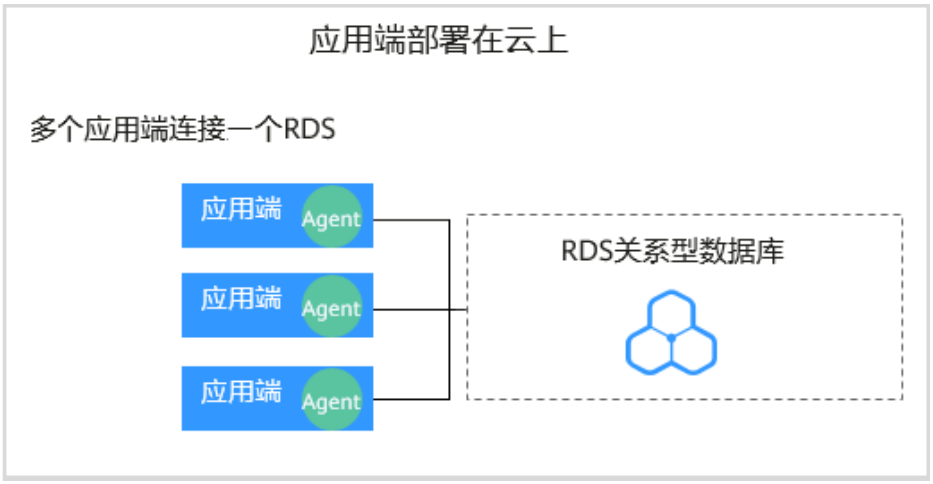


图 6-9 多个应用端连接同一个 RDS



安装Agent节点的详细说明如表6-2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 6-2 安装 Agent 场景说明

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

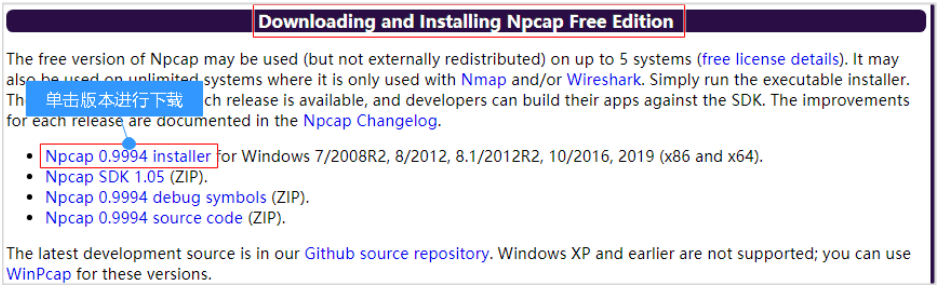
安装 Agent

步骤1 在Windows主机安装“Npcap”软件。

- 如果该Windows主机已安装“Npcap”，请执行**步骤2**。
- 如果该Windows主机未安装“Npcap”，请执行以下步骤：

a. 请前往**https://nmap.org/npcap/**下载Npcap最新软件安装包。

图 6-10 下载 npcap

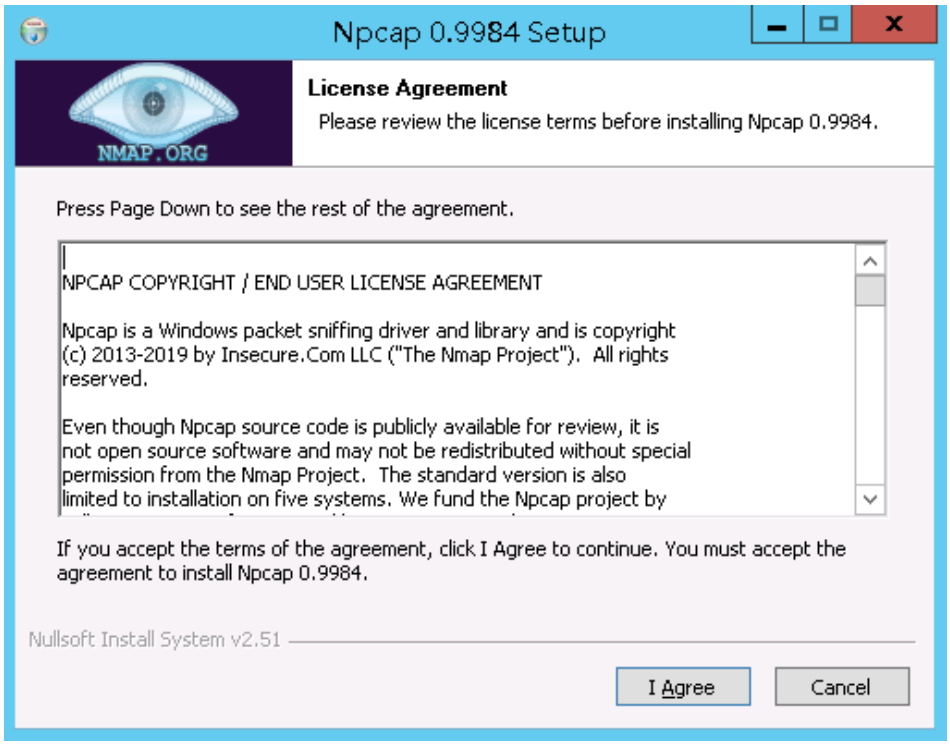


b. 将下载好的npcap-*xxxx*.exe软件安装包上传至需要安装agent的虚拟机。

c. 双击npcap软件安装包。

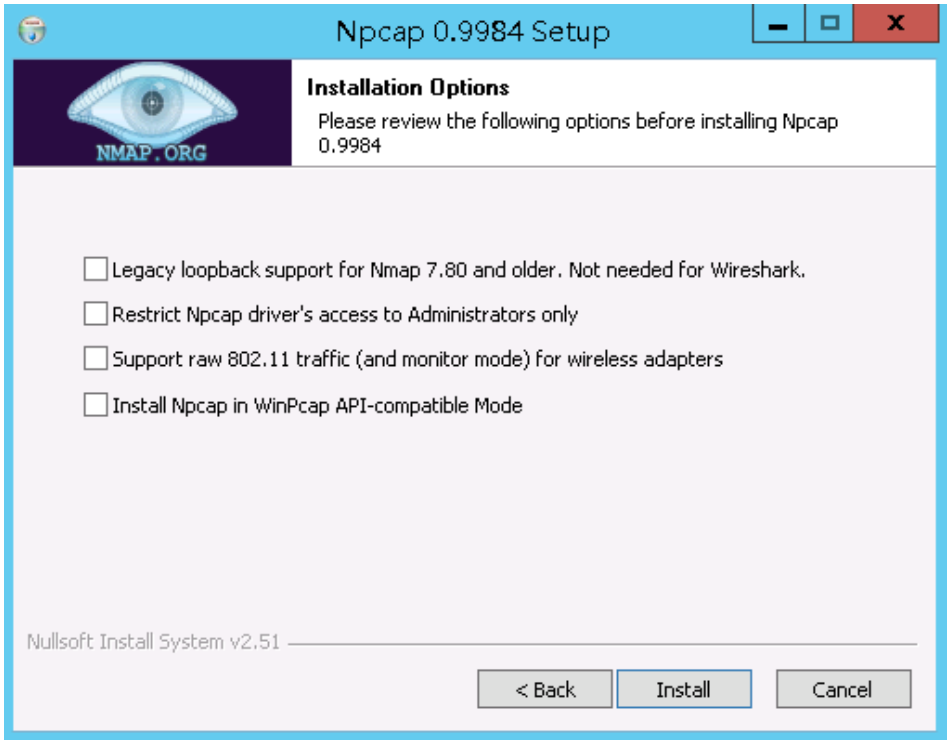
d. 在弹出的对话框中，单击“I Agree”，如**图6-11**所示。

图 6-11 同意安装“Npcap”

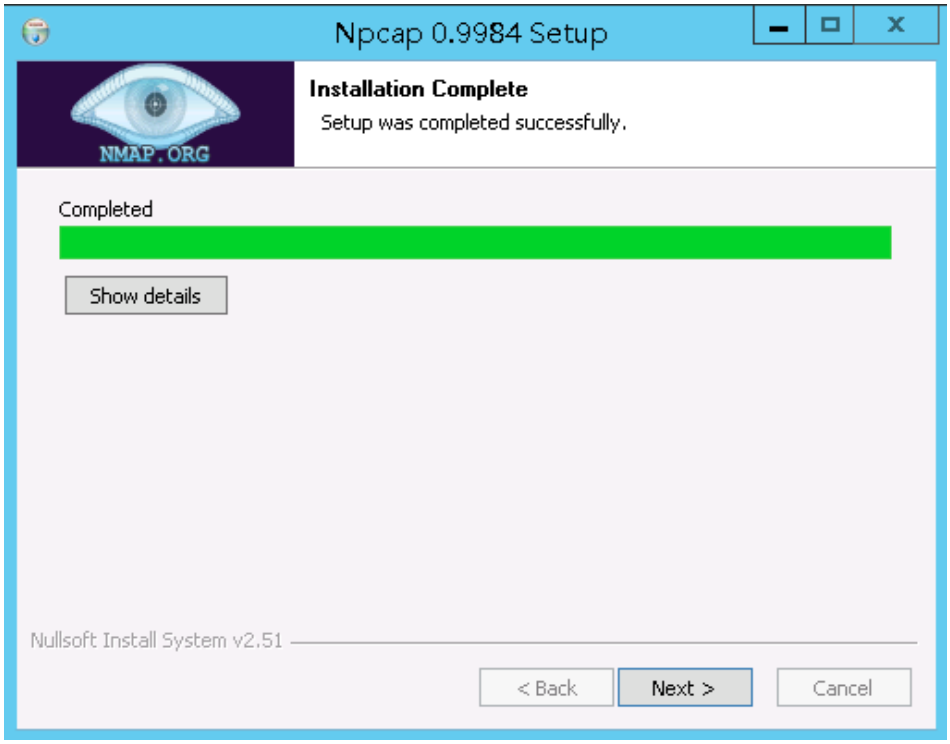


e. 在弹出的对话框中，单击“Install”，不勾选安装选项，如**图6-12**所示。

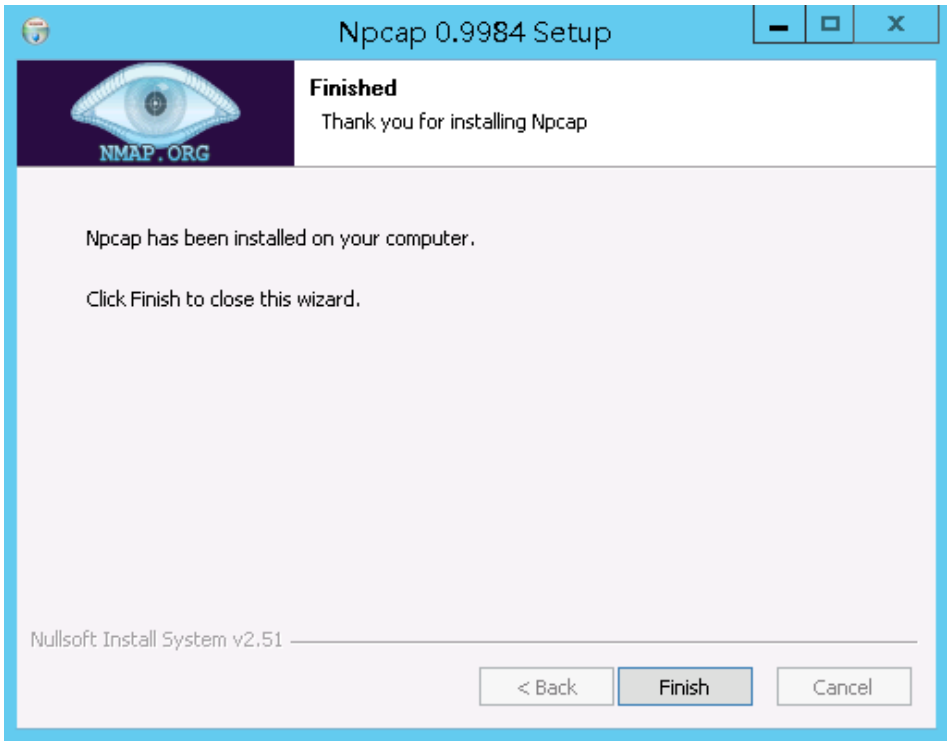
图 6-12 安装“Npcap”



f. 在弹出的对话框中，单击“Next”。



g. 单击“Finish”，完成安装。



步骤2 以“Administrator”用户登录到Windows主机。

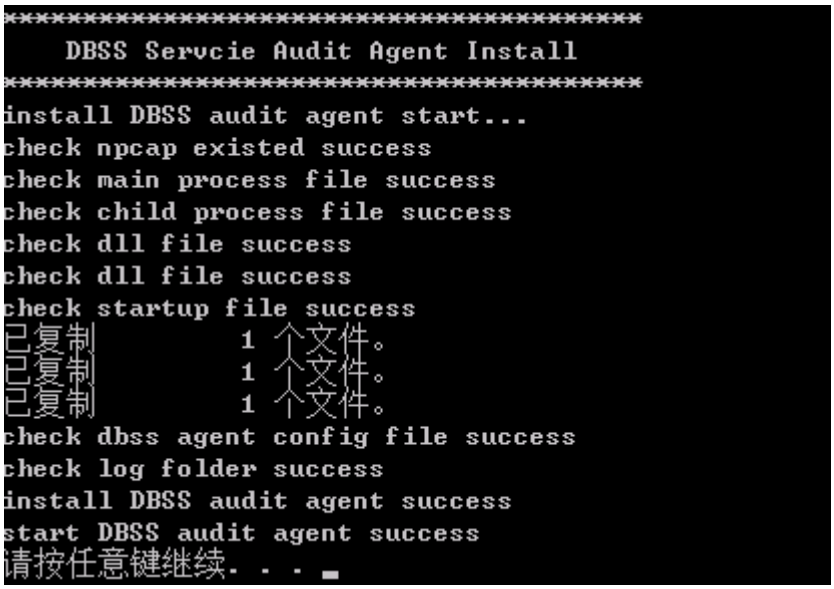
步骤3 将下载的Agent安装包“xxx.zip”复制到该主机任意一个目录下。

步骤4 进入Agent安装包所在目录，并解压缩安装包。

步骤5 进入解压后的文件夹，双击“install.bat”执行文件。

步骤6 安装成功，界面如图6-13所示，按任意键结束安装。

图 6-13 Agent 安装成功



步骤7 安装完成后，在Windows任务管理器中查看“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

7 步骤四：添加安全组规则

Agent添加完成后，您需要为数据库安全审计实例所在的安全组添加入方向规则TCP协议（8000端口）和UDP协议（7000-7100端口），使Agent与审计实例之间的网络连通，数据库安全审计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成功安装Agent后进行添加。

前提条件

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 数据库已成功添加Agent。

添加安全组规则

步骤1 登录管理控制台。

步骤2 在左侧导航树中，选择“数据库安全审计 > 数据库列表”，进入“数据库列表”界面。

步骤3 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4 记录**Agent安装节点IP信息。**

单击数据库左侧的展开Agent的详细信息，并记录“安装节点IP”。

步骤5 在数据库列表的上方，单击“添加安全组规则”。

步骤6 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）。

步骤7 单击“前往处理”，进入“安全组”列表界面。

步骤8 在列表右上方的搜索框中输入安全组“default”后，单击或按“Enter”，列表显示“default”安全组信息。

步骤9 单击“default”，进入“基本信息”页面。

步骤10 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**步骤4**的安装节点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**下载Agent**。
- 如果该安全组未配置安装节点的入方向规则，请执行**步骤11**。

步骤11 为安装节点添加入方向安全规则。

1. 单击“确定”，完成添加入方向规则。

   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，将添加的数据库连接到数据库安全审计实例，才能开启数据库安全审计功能。

----结束

8 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

- 已成功添加并安装Agent，且Agent的运行状态为“正在运行”。

开启审计

步骤1 登录管理控制台。

步骤2 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3 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4 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 8-1 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 在左侧导航树中，选择“总览”，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“时间”所在行右侧，单击，选择开始时间和结束时间，单击“提交”。

图 8-2 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

----结束

9 添加审计范围

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

须知

全审计规则大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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已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 ☰，选择“安全 > 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。
- 全审计规则大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9-1所示，相关参数说明如表9-1所示。

图 9-1 “添加审计范围”对话框

表 9-1 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	选择待添加审计范围的数据库。	db03
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。

10 启用或禁用 SQL 注入检测

数据库安全审计的SQL注入检测默认开启，您可以禁用或启用SQL注入的检测规则。

须知

一条审计数据只能命中SQL注入检测中的一个规则。

前提条件

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- SQL注入检测的状态为“已禁用”时，可以启用SQL注入检测。
- SQL注入检测的状态为“已启用”时，可以禁用SQL注入检测。

禁用 SQL 注入检测

SQL注入检测默认开启，您可以根据使用需要禁用SQL注入检查规则。禁用SQL注入检测规则后，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 ☰，选择“安全 > 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注入检测的实例。

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 在SQL注入检测规则所在行的“操作”列，单击“禁用”。

图 10-1 禁用 SQL 注入检测规则

禁用SQL注入检测成功，该SQL注入检测规则的状态为“已禁用”。

----结束

后续处理

禁用SQL注入检测规则后，如果您需要启动该规则，请在SQL注入检测规则所在行的“操作”列，单击“启用”，启用该规则。

图 10-2 启用 SQL 注入检测规则

序号	名称	SQL命令特征	风险等级	状态	操作
1	UNION联合查询SQL注入	正则表达式	中	已禁用	启用
2	HAVING报错SQL注入	正则表达式	中	已启用	禁用

启用SQL注入检测成功，该SQL注入检测规则的状态为“已启用”。

11 添加风险操作

添加的数据库开启审计功能后，您可以通过添加风险操作，设置被添加的数据库需要审计的风险操作。

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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已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 ☰，选择“安全 > 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。选择“风险操作”页签。在风险操作列表左上方，单击“添加风险操作”。

步骤5 在“添加风险操作”界面，设置基本信息和客户端IP地址，如图11-1所示，相关参数说明如表11-1所示。

图 11-1 设置基本信息和客户端 IP 地址

表 11-1 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
风险级别	选择风险操作的级别，可以选择以下级别： • 高 • 中 • 低 • 无风险	高
状态	开启或关闭风险操作。	
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，fe80:0000:0000:0000:0000:0000:0000:0000）格式。	192.168.0.0

步骤6 设置操作类型、操作对象、执行结果，如图11-2所示，相关参数说明如表11-2所示。

图 11-2 设置操作类型、操作对象和执行结果

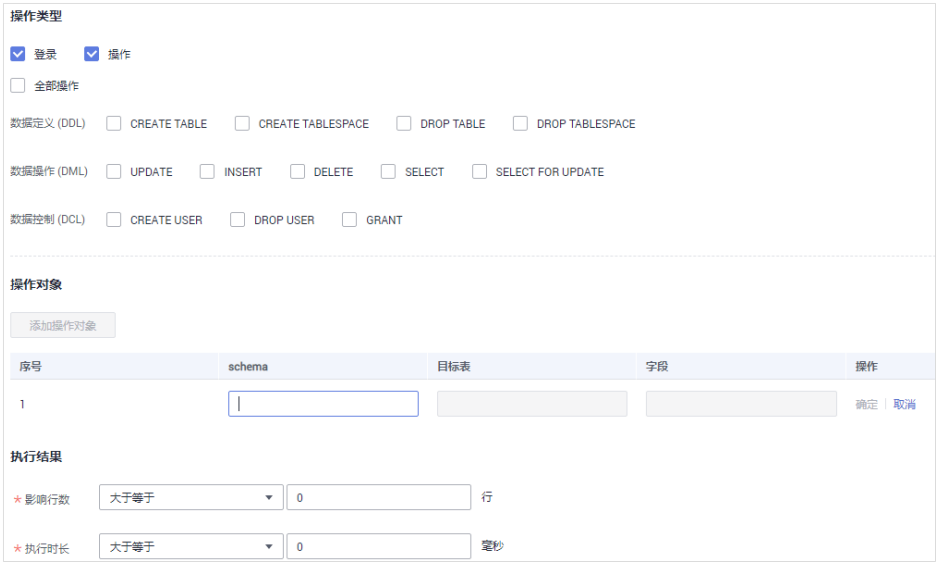


表 11-2 参数说明

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“schema”、“目标表”和“字段”信息。单击“确定”，添加操作对象。	-
执行结果	设置“影响行数”和“执行时长”的执行条件后，输入行数和时长值，执行条件包括： ● 大于 ● 小于 ● 等于 ● 大于等于 ● 小于等于	-

步骤7 单击“保存”。

----结束

12 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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已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 ☰，选择“安全 > 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。

- 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12-1所示，相关参数说明如表12-1所示。

图 12-1 “添加自定义规则”对话框

表 12-1 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12-2所示。

图 12-2 开启隐私数据保护

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 在左侧导航树中，选择“总览”，进入“总览”界面。

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 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。选择“语句”页签。

步骤7 根据筛选条件，查询输入的SQL语句。

步骤8 在该SQL语句所在行的“操作”列，单击“详情”。

步骤9 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。

----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。

- 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。

13 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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已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 ☰，选择“安全 > 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“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4 选择“语句”页签。

步骤5 查询SQL语句信息。

图 13-1 查询 SQL 语句

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”、“近30分钟”、“近1小时”、“近24小时”、“近7天”或“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“信任”），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6 在需要查看详情的SQL语句所在行的“操作”列，单击“详情”。

图 13-2 查看 SQL 语句详情

步骤7 在“详情”提示框中，查看SQL语句的详细信息，如图13-3所示，相关参数说明如表13-1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 13-3 “详情”提示框

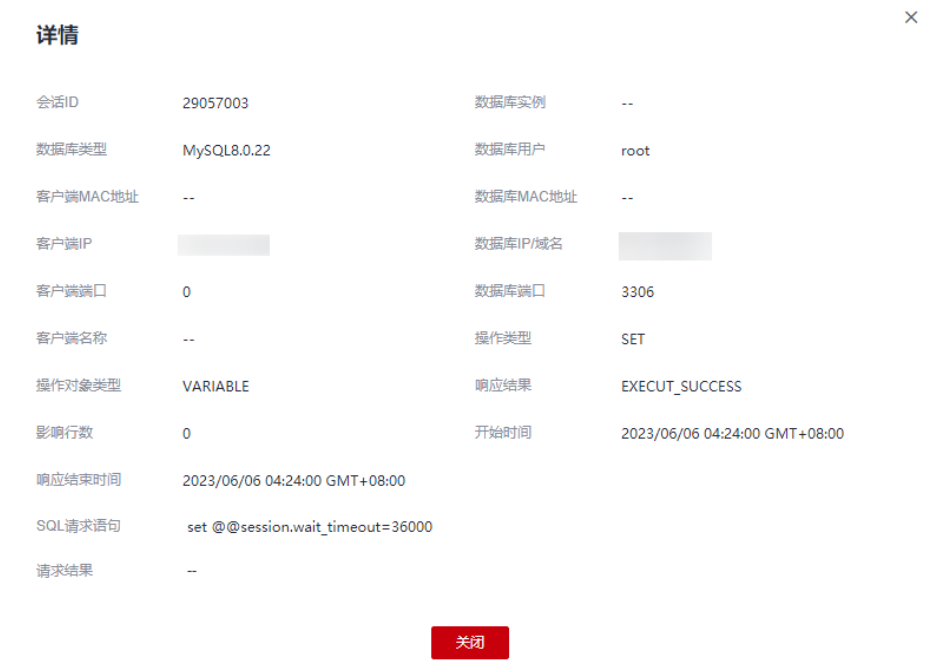


表 13-1 SQL 语句详情参数说明

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。

参数名称	说明
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

14 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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已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 ☰，选择“安全 > 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“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4 选择“会话”页签。

步骤5 查看会话分布表，如图14-1所示。

- 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 14-1 会话分布表

----结束

15 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，包括数据库的总体审计情况、风险分布、会话统计以及SQL分布情况。

前提条件

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已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 ☰，选择“安全 > 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“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4 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 15-1 查看审计概况

图 15-2 风险分布

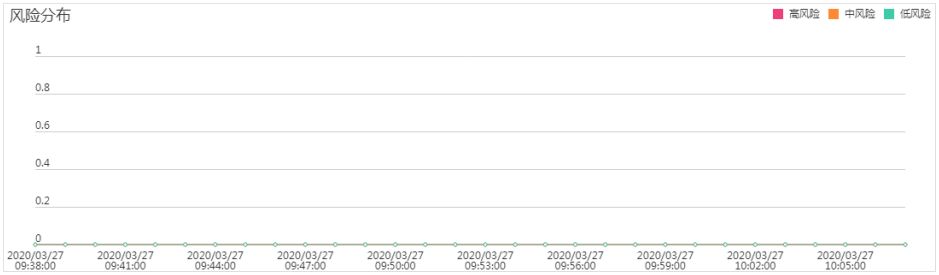
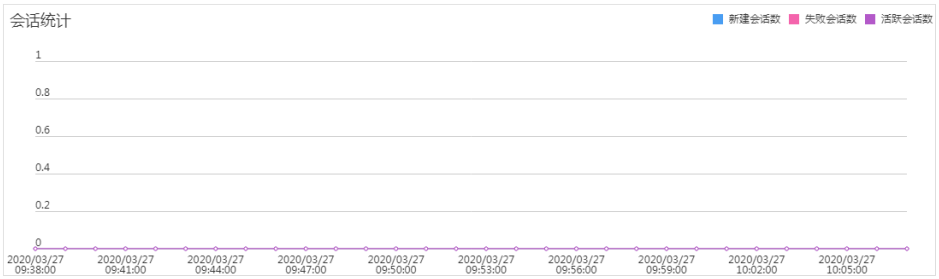


图 15-3 会话统计



----结束

16 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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已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16-1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 16-1 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	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。

报表模板名称	报表类型	说明
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。

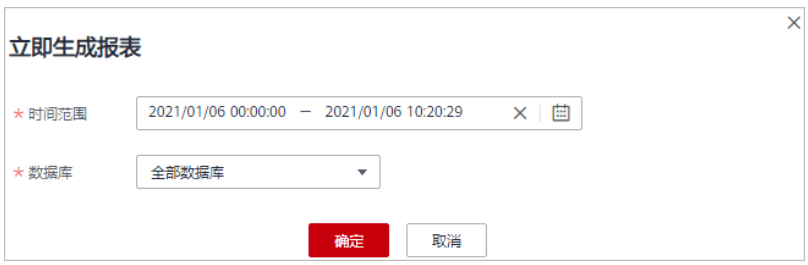
步骤5 选择“报表管理”页签。

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 16-1 报表模板列表

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 16-2 “立即生成报表”对话框



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 ☰，选择“安全 > 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16-3所示。

图 16-3 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16-4所示，相关参数说明如表16-2所示。

图 16-4 “计划任务”对话框

表 16-2 计划任务参数说明

参数名称	说明	取值样例
启动任务	开启或关闭计划任务。 ●  ：开启 ●  ：关闭	
消息通知	开启或关闭消息通知。 ●  ：开启 ●  ：关闭	
消息通知主题	单击下拉列表选择已创建的主题或者单击“查看消息通知主题”创建新的主题，用于配置接收告警通知的终端。 更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。	-
报表类型	选择生成的报表类型，可以选择： ● 日报 ● 周报 ● 月报	周报
执行方式	选择报表执行的方式，可以选择： ● 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、下载审计报表

预览或下载审计报表前，请确认报表的“状态”为“100%”。

须知

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

步骤1 登录管理控制台。

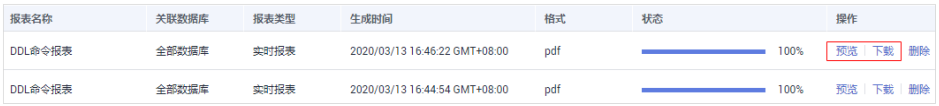
步骤2 在页面上方选择“区域”后，单击 ，选择“安全 > 数据库安全服务 DBSS”，进入数据库安全审计“总览”界面。

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16-5所示，在线预览报表结果，或下载并查看报表。

图 16-5 预览或下载报表



----结束

17 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。
- 您还可以为设置的报表任务开启消息通知，及时获取报表生成结果。有关开启报表消息通知的详细操作，请参见**查看审计报表**。

前提条件

已成功申请数据库安全审计实例，且实例的状态为“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 ☰，选择“安全 > 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17-1**所示。

图 17-1 设置告警通知

表 17-1 告警通知参数说明

参数名称	说明	取值样例
消息通知	开启或关闭消息通知。	
消息通知主题	单击下拉列表选择已创建的主题或者单击“查看消息通知主题”创建新的主题，用于配置接收告警通知的终端。 **说明** 在选择主题前，请确保您主题中订阅状态为“已确认”，即当前订阅终端可用，否则可能不能收到告警通知。 更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。	-
每天发送告警总条数	每天允许发送的告警总条数。 **须知** • 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

参数名称	说明	取值样例
告警风险等级	选择产生告警通知的风险日志告警风险等级，可以选择： ● 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

18 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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已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 ☰，选择“安全 > 数据库安全服务 DBSS”，进入数据库安全审计“总览”界面。

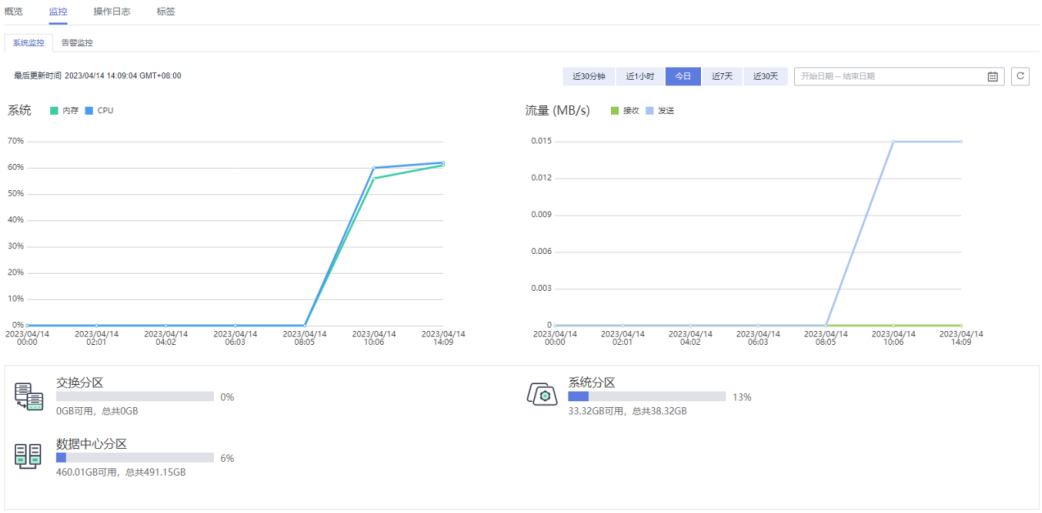
步骤3 在左侧导航树中，选择“实例列表”，进入“实例列表”界面。

步骤4 单击需要查看系统监控信息的实例名称，选择“监控”页签，进入系统监控页面。

步骤5 查看系统监控信息，如图18-1所示。

选择审计的时间（“近30分钟”、“近1小时”、“近24小时”、“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 18-1 查看系统监控信息



----结束

19 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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已成功开启数据库安全审计功能。
- 已设置告警通知。

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 ☰，选择“安全 > 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“监控 > 告警监控”，进入告警监控页面。

步骤5 查看告警信息，如图19-1所示，相关参数说明如表19-1所示。

图 19-1 查看告警信息

表 19-1 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： • 风险规则告警 • CPU异常 • 内存异常 • 磁盘异常 • 审计容量不足
告警风险等级	告警的风险等级，包括： • 高风险 • 中风险 • 低风险
恢复时间	恢复告警的时间。
确认状态	告警的确认状态。单击，可以筛选“未确认”或“已确认”状态的告警信息。
描述	告警的相关描述信息。

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”或“近30天”），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。

----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。

图 19-2 确认告警信息

说明

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。

20 管理数据库安全审计实例

成功申请数据库安全审计实例后，您可以查看实例信息，开启、重启、关闭或删除实例。

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”。
- 开启实例和删除实例前，请确认实例的状态为“已关闭”。

删除实例

当您不需要使用某个实例时，可以删除该实例。删除时可以选择同时删除该实例绑定的弹性IP。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击，选择“安全 > 数据库安全服务”，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“实例列表”，进入“实例列表”界面。

步骤5 在需要删除的实例所在行的“操作”列，选择“更多 > 删除”。

步骤6 在弹出的提示框中，单击“确定”。

----结束

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，选择“安全 > 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20-1**所示。

图 20-1 查看数据库安全审计实例信息

说明

- 单击实例名称，可以查看该实例的概览信息。
- 在列表右上方“全部状态”下拉列表框中选择实例的状态，或输入实例名称的关键字，可以搜索指定的实例。

表 20-1 实例信息参数说明

参数名称	说明
实例名称/ID	实例的名称和ID。实例ID由系统自动生成。
实例规格	实例的规格。
状态	实例当前的运行状态，包括： ● 运行中 ● 创建中 ● 故障 ● 已关闭 ● 已冻结 ● 公安冻结 ● 违规冻结 ● 未实名认证冻结 ● 合作伙伴冻结 ● 创建失败
已关联数据库/数据库总数	实例的已关联的数据库和实例可以支持关联的数据库总数。
操作	对该实例进行相关操作： ● 配置审计规则 ● 开启 ● 关闭 ● 重启 ● 查看详情 ● 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，实例列表不在显示该条实例。

- 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

21 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

已成功申请数据库安全审计实例，且实例的状态为“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 ☰，选择“安全 > 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”，如图21-1所示，相关参数说明如表21-1所示。

图 21-1 查看实例概览信息

表 21-1 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。
	状态	实例当前的运行状态，包括： ● 运行中 ● 创建中 ● 故障 ● 已关闭 ● 已冻结 ● 公安冻结 ● 违规冻结 ● 未实名认证冻结 ● 合作伙伴冻结 ● 创建失败
	实例ID	实例的ID，由系统自动生成。
	可用区	实例所在的可用区。
	版本	您创建DBSS实例时对应的DBSS实例版本，您不同时间创建的DBSS实例的版本可能会有差别。 DBSS实例版本影响的范围： ● 支持的数据库类别 ● 支持的数据库版本
	备注	实例的备注信息。单击备注后的，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。
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。
	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。

----结束

22 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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已成功添加数据库。
- 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 ☰，选择“安全 > 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22-1所示。

图 22-1 查看数据库和 Agent 信息

说明

在列表右上方“全部审计状态”下拉列表框中选择数据库的审计状态，或输入数据库的关键字，可以搜索指定的数据库。

表 22-1 数据库信息参数说明

参数名称	说明	取值样例
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。	UTF8
IP地址/端口	数据库的IP地址。	192.168.0.104 3306
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。	LINUX64
审计状态	数据库的审计状态，包括： • 已开启 • 已关闭	已开启
Agent	单击“添加Agent”，可以为数据库添加Agent。	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“确定”，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 ☰，选择“安全 > 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，如**图 查看数据库和Agent信息**所示，相关参数如**表 Agent参数说明所示**。

图 22-2 查看数据库和 Agent 信息

表 22-2 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。
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。
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“确定”，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

23 卸载 Agent

在数据库端或应用端的节点安装Agent后，当不需要停止审计数据库时，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

24 管理审计范围

添加审计范围后，您可以查看审计范围信息，启用、编辑、禁用或删除审计范围。

前提条件

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已成功添加审计范围。
- 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 ☰，选择“安全 > 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24-1所示。

图 24-1 查看审计范围信息

说明

在列表右上方输入审计范围名称的关键字，可以搜索指定的审计范围。

表 24-1 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。
数据库帐户	数据库的用户名。
状态	审计范围的状态，包括： ● 已启用 ● 已禁用

说明

根据需要，您还可以对审计范围执行以下操作：

- 启用

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

- 编辑（仅自定义创建审计范围的支持）

  在需要编辑的审计范围所在行的“操作”列，单击“编辑”，在弹出的对话框中，您可以修改审计范围。

- 禁用

  在需要禁用的审计范围所在行的“操作”列，单击“禁用”，在弹出的对话框中，单击“确定”，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

25 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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已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 ☰，选择“安全 > 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，如图25-1所示，相关参数如表25-1所示。

图 25-1 查看 SQL 注入检测信息

说明

- 在列表右上方“全部风险等级”下拉列表框中选择SQL注入的风险等级，或输入SQL注入名称的关键字，可以搜索指定的SQL注入检测规则。
- 在“操作”列单击设置优先级，可以修改SQL注入规则的优先级。

表 25-1 SQL 注入检测信息参数说明

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

----结束

26 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，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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已成功添加风险操作。
- 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 ☰，选择“安全 > 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 26-1 设置风险操作的优先级

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。

----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 ☰，选择“安全 > 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26-1所示。

图 26-2 查看风险操作信息

说明

在列表右上方“全部风险等级”下拉列表框中选择风险操作的等级，或输入风险操作名称的关键字，可以搜索指定的风险操作。

表 26-1 风险操作信息参数说明

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

说明

根据需要，您还可以对风险操作执行以下操作：

- 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，单击“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“确定”，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”列，单击“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

27 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

已成功申请数据库安全审计实例，且实例的状态为“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 ☰，选择“安全 > 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27-1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。
- 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 27-1 查看脱敏规则信息

表 27-1 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。
规则类型	该规则的类型，包括 • 默认 • 自定义
正则表达式	该规则的正则表达式。
替换值	正则表达式脱敏后对应的替换值。
状态	该规则的启用状态，包括： • 已启用 • 已禁用

说明

根据需要，您还可以对规则执行以下操作：

- 禁用

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

- 编辑

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

- 删除

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

----结束

28 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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已成功开启数据库安全审计功能。
- 已生成审计报表。

查看报表信息

步骤1 登录管理控制台。

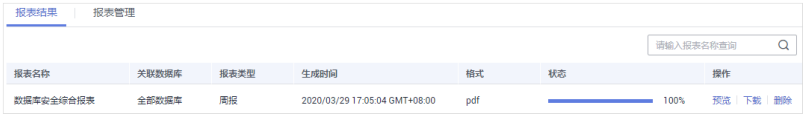
步骤2 在页面上方选择“区域”后，单击 ☰，选择“安全 > 数据库安全服务 DBSS”，进入数据库安全审计“总览”界面。

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 28-1 查看报表信息



说明

- 在列表右上方输入报表名称，可以搜索指定的报表。
- 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 ☰，选择“安全 > 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，如图28-2所示。

图 28-2 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 (每周)	设置任务 | 立即生成报表
SOX-萨班斯报表	全部数据库	合规报表	SOX-萨班斯报表	已关闭 (每周)	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
数据库服务器分析报表	全部数据库	数据库专项报表	数据库服务器分析报表	已关闭 (每周)	设置任务 | 立即生成报表
客户端IP分析报表	全部数据库	客户端专项报表	客户端IP分析报表	已关闭 (每周)	设置任务 | 立即生成报表
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
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
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

29 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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 已成功开启数据库安全审计功能。
- 已成功备份审计日志。

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 ☰，选择“安全 > 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，如图29-1所示，相关参数说明如表29-1所示。

图 29-1 查看备份审计日志信息

在列表右上方单击 📅，选择开始时间和结束时间，可以查看指定的时间段的备份日志。

表 29-1 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。
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

30 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

已成功申请数据库安全审计实例，且实例的状态为“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 ☰，选择“安全 > 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，如图30-1所示，相关参数说明如表30-1所示。

图 30-1 查看操作日志

说明

选择时间（“近30分钟”、“近1小时”、“近24小时”、“近7天”或“近30天”）；或者单击 📅，选择开始时间和结束时间，列表显示指定时间段的操作日志。

表 30-1 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

31 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 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤3 单击事件列表上方的“Region”，设置对应的操作事件条件。

当前事件列表支持四个维度的组合查询，详细信息如下：

- “事件类型”、“事件来源”、“资源类型”和“筛选类型”。
  - 在下拉框中选择查询条件。其中，“事件来源”选择“DBSS”。
  - 筛选类型选择事件名称时，还需选择某个具体的事件名称。
  - 选择资源ID时，还需选择或者手动输入某个具体的资源ID。
  - 选择资源名称时，还需选择或手动输入某个具体的资源名称。
- “操作用户”：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
- “事件级别”：可选项为“所有事件级别”、“normal”、“warning”、“incident”，只可选择其中一项。
- 可在页面右上角选择查询最近1小时、最近1天、最近1周及自定义时间段的操作事件。

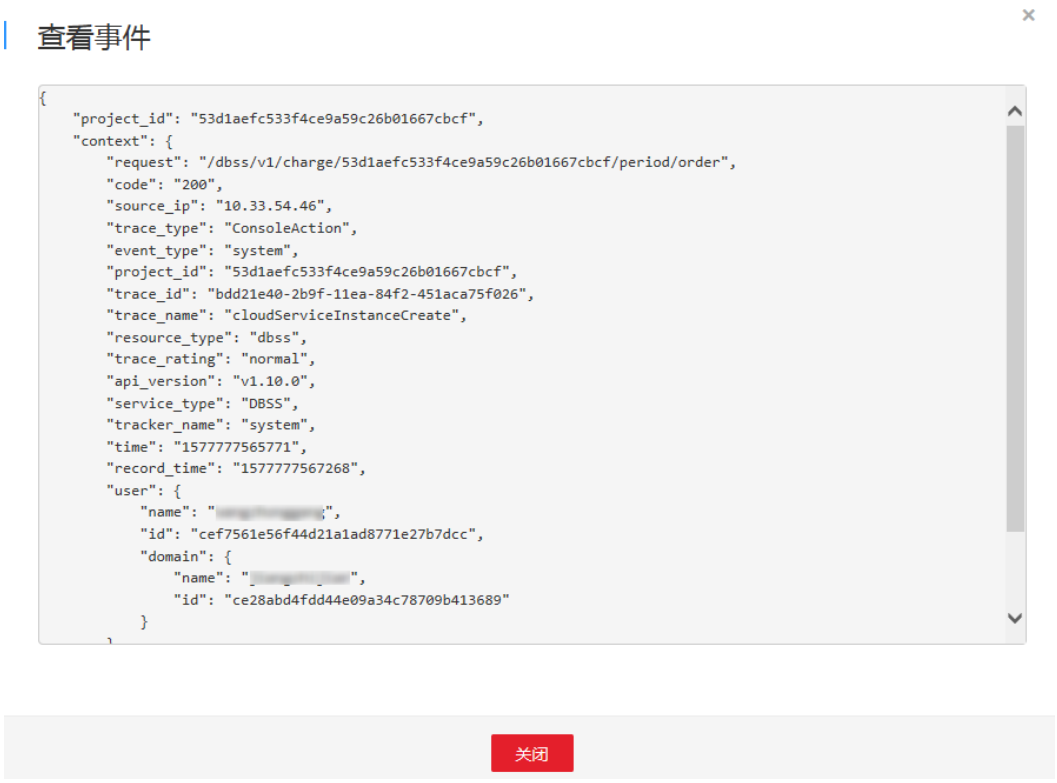
步骤4 单击“查询”，查看对应的操作事件。

步骤5 在需要查看的记录左侧，单击 展开该记录的详细信息，展开记录如图31-1所示。

图 31-1 展开记录

步骤6 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，如图31-2所示，显示了该操作事件结构的详细信息。

图 31-2 查看事件



----结束

32 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32-1所示。

表 32-1 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

33 常见问题

33.1 功能类

33.1.1 数据库安全审计（旁路模式）是否会影响业务?

不影响。数据库安全审计是数据库安全服务提供的旁路模式数据库审计功能，只对数据库进行审计，不影响用户业务，与本地审计工具不冲突。

33.1.2 数据库安全审计可以应用于哪些场景?

数据库安全审计采用数据库旁路部署方式，在不影响用户业务的提前下，可以对管理控制台上的RDS、ECS/BMS自建的数据库进行灵活的审计。

- 基于数据库风险操作，监视数据库登录、操作类型（数据定义、数据操作和数据控制）和操作对象，有效对数据库进行审计。
- 从风险、会话、SQL注入等多个维度进行分析，帮助您及时了解数据库状况。
- 提供审计报表模板库，可以生成日报、周报或月报审计报表（可设置报表生成频率）。同时，支持发送报表生成的实时告警通知，帮助您及时获取审计报表。

33.1.3 支持的数据库类型

数据库安全审计支持数据库类型及版本如**表33-1**所示。

表 33-1 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	• 5.0、5.1、5.5、5.6、5.7 • 8.0（8.0.11及以前的子版本） • 8.0.20 • 8.0.23

数据库类型	版本
Oracle	• 11g 11.1.0.6.0 、11.2.0.1.0 、11.2.0.2.0、11.2.0.3.0、11.2.0.4.0 • 12c 12.1.0.2.0 、12.2.0.1.0 • 19c
PostgreSQL	• 7.4 • 8.0 8.0、8.1、8.2、8.3、8.4 • 9.0 9.0、9.1、9.2、9.3、9.4、9.5、9.6 • 10.0 10.0、10.1、10.2、10.3、10.4、10.5 • 11.0 • 12.0 • 13.0 • 14.0
SQL Server	• 2008、2008R2 • 2012 • 2014 • 2016 • 2017
DWS	• 1.5
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0
TAURUS	MySQL 8.0

33.1.4 数据库安全审计支持数据库部署在哪些操作系统上?

您需要在数据库端、应用端或代理端安装Agent，将添加的数据库连接到数据库安全审计实例。

数据库安全审计的Agent可运行在Linux64位和Windows64位操作系统上，安装节点的操作系统说明如下所示。

- 数据库安全审计的Agent支持的Linux系统版本如表33-2所示。

表 33-2 Agent 支持的 Linux 系统版本说明

系统名称	系统版本
CentOS	• CentOS 7.0 (64bit) • CentOS 7.1 (64bit) • CentOS 7.2 (64bit) • CentOS 7.3 (64bit) • CentOS 7.4 (64bit) • CentOS 7.5 (64bit) • CentOS 7.6 (64bit) • CentOS 7.8 (64bit) • CentOS 8.0 (64bit)
Debian	• Debian 7.5.0 (64bit) • Debian 8.2.0 (64bit) • Debian 8.8.0 (64bit) • Debian 9.0.0 (64bit)
Fedora	• Fedora 24 (64bit) • Fedora 25 (64bit)
SUSE	• SUSE 11 SP4 (64bit) • SUSE 12 SP1 (64bit) • SUSE 12 SP2 (64bit)
Ubuntu	• Ubuntu 14.04 (64bit) • Ubuntu 16.04 (64bit) • Ubuntu 18.04 (64bit) • Ubuntu 20.04 (64bit)
EulerOS	• Euler 2.2 (64bit) • Euler 2.3 (64bit)
Oracle Linux	• Oracle Linux 6.9 (64bit) • Oracle Linux 7.4 (64bit)

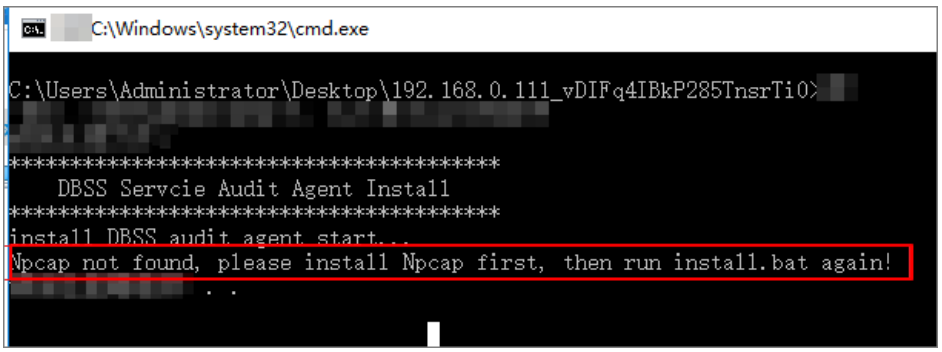
- 数据库安全审计的Agent支持的Windows系统版本如下所示：
  - Windows Server 2008 R2(64bit)
  - Windows Server 2012 R2(64bit)
  - Windows Server 2016(64bit)
  - Windows 7(64bit)
  - Windows 10(64bit)

说明

DBSS Agent的运行依赖Npcap，如果安装过程中提示"Npcap not found，please install Npcap first"，请安装Npcap后，再安装DBSS Agent。

Npcap下载链接：**https://npcap.com/#download**

图 33-1 Npcap not found



33.1.5 数据库安全审计支持双向审计吗?

数据库安全审计支持双向审计。双向审计是对数据库的请求和响应都进行审计。

数据库安全审计默认使用双向审计。

33.1.6 数据库安全审计支持 TLS 连接的应用吗?

不支持。TLS（Transport Layer Security）连接的应用是加密的，无法使用数据库安全审计功能。

33.1.7 数据库安全审计的审计数据可以保存多久?

数据库安全审计支持将在线和归档的审计数据至少保存180天的功能。

您可以在数据库安全审计的“总览”界面，通过选择数据库和审计周期，查看对应时间段的审计数据。

由于审计数据存放在日志数据库中，而日志数据库的硬盘容量可能影响保存时长。为了确保审计数据满足保存时长要求，建议您通过以下方式处理：

- 根据业务数据库审计数据实际情况，选择申请的数据库安全审计版本
  - 审计数据容量较小：申请基础版
  - 审计数据容量较大：申请专业版或高级版

  数据库安全审计各版本的规格说明如所**表33-3**示。
- 备份审计日志

表 33-3 数据库安全审计版本性能规格说明

版本	支持的数据库实例	系统资源要求	性能参数
基础版	最多支持3个数据库实例	• CPU：4U • 内存：16GB • 硬盘：560GB	• 吞吐量峰值：3,000条/秒 • 入库速率：360万条/小时 • 4亿条在线SQL语句存储 • 50亿条归档SQL语句存储
专业版	最多支持6个数据库实例	• CPU：8U • 内存：32GB • 硬盘：1T	• 吞吐量峰值：6,000条/秒 • 入库速率：720万条/小时 • 6亿条在线SQL语句存储 • 100亿条归档SQL语句存储

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IP_1和IP_2，IP_1有一个数据库端口，则为1个数据库实例；IP_2有3个数据库端口，则为3个数据库实例。IP_1和IP_2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，请退订后重新申请。
- 云原生版仅支持在RDS控制台购买。
- 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。

33.1.8 数据库安全审计发生异常，多长时间用户可以收到告警通知?

在数据库安全审计正常运行的情况下，从系统发生异常到收到告警通知最大时延不超过5分钟。

当您设置告警通知后，在数据库安全审计正常运行的情况下，当数据库安全审计实例资源（CPU、内存和磁盘）超过设置的告警阈值时，系统产生告警通知。用户约在5分钟内可以收到告警通知。

33.1.9 每天发送告警总条数与每天收到的邮件数是相同的吗?

是的。一条告警信息对应一个通知邮件。

33.1.10 为什么不能在线预览数据库安全审计报表?

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

33.1.11 在业务侧使用中间件会影响数据库安全审计功能吗?

不会影响使用数据库安全审计。

中间件是介于应用系统和操作系统之间的一类软件，通常在操作系统、网络和数据库之上，应用软件的下层，是为处于上层的应用软件提供运行与开发的环境，帮助用户灵活、高效地开发和集成复杂的应用软件。

数据库安全审计采用旁路模式部署，通过Agent（数据库节点或应用节点安装Agent）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，从而实现数据库安全审计功能。

因此，您在业务侧使用中间件不影响数据库安全审计功能，不会导致Agent监听SQL失败或者审计没有数据。

如果您的数据库安全审计没有审计数据，请参见以下内容进行排查：

33.2 Agent 相关

33.2.1 数据库安全审计的 Agent 提供哪些功能?

使用数据库安全审计功能，必须在数据库节点或应用节点安装Agent。

数据库安全审计的Agent主要提供以下功能：

- 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
- 上报数据库状态监控数据

33.2.2 数据库安全审计的 Agent 可以安装在哪些 Windows 操作系统上?

使用数据库安全审计功能，必须在数据库节点或应用节点安装Agent。

数据库安全审计的Agent支持安装在以下Windows操作系统上：

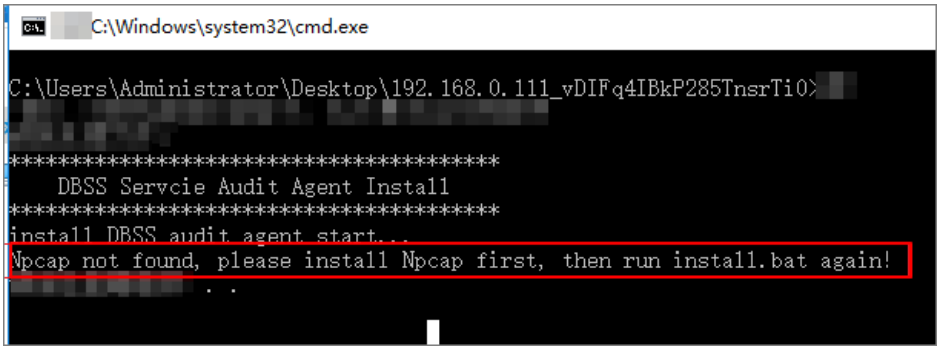
- Windows Server 2008 R2(64bit)
- Windows Server 2012 R2(64bit)
- Windows Server 2016(64bit)
- Windows 7(64bit)
- Windows 10(64bit)

说明

DBSS Agent的运行依赖Npcap，如果安装过程中提示"Npcap not found，please install Npcap first"，请安装Npcap后，再安装DBSS Agent。

Npcap下载链接：**https://npcap.com/#download**

图 33-2 Npcap not found



33.2.3 数据库安全审计的 Agent 可以安装在哪些 Linux 操作系统上?

使用数据库安全审计功能，必须在数据库节点或应用节点安装Agent。

数据库安全审计的Agent支持安装在Linux64位操作系统，系统版本说明如**表33-4**所示。

表 33-4 Agent 支持的 Linux 系统版本说明

系统名称	系统版本
CentOS	• CentOS 7.0 (64bit) • CentOS 7.1 (64bit) • CentOS 7.2 (64bit) • CentOS 7.3 (64bit) • CentOS 7.4 (64bit) • CentOS 7.5 (64bit) • CentOS 7.6 (64bit) • CentOS 7.8 (64bit) • CentOS 8.0 (64bit)
Debian	• Debian 7.5.0 (64bit) • Debian 8.2.0 (64bit) • Debian 8.8.0 (64bit) • Debian 9.0.0 (64bit)
Fedora	• Fedora 24 (64bit) • Fedora 25 (64bit)

系统名称	系统版本
SUSE	• SUSE 11 SP4 (64bit) • SUSE 12 SP1 (64bit) • SUSE 12 SP2 (64bit)
Ubuntu	• Ubuntu 14.04 (64bit) • Ubuntu 16.04 (64bit) • Ubuntu 18.04 (64bit) • Ubuntu 20.04 (64bit)
EulerOS	• Euler 2.2 (64bit) • Euler 2.3 (64bit)
Oracle Linux	• Oracle Linux 6.9 (64bit) • Oracle Linux 7.4 (64bit)

33.2.4 数据库安全审计 Agent 的进程名称是什么?

Linux 操作系统

Agent客户端进程名称为：“/opt/dbss_audit_agent/bin/audit_agent”

安装Agent后，您可以参照以下操作步骤，查看Agent程序的运行状态。

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Agent的安装节点。

步骤2 执行以下命令，查看Agent程序的运行状态。

ps -ef|grep audit_agent

- 如果界面回显以下信息，说明Agent程序运行正常。
  ```
  /opt/dbss_audit_agent/bin/audit_agent
  ```
- 如果界面无回显信息，说明Agent程序运行异常。

----结束

Windows 操作系统

Agent安装完成后，在Windows任务管理器中，可以查看Agent的进程“dbss_audit_agent”。

33.2.5 （Linux 操作系统）安装 Agent 时没有安装脚本执行权限，如何处理?

如果在安装Agent时，没有安装脚本的执行权限，请在安装Agent的节点上执行以下命令，添加安装脚本的执行权限：

chmod +x install.sh

33.2.6 （Linux 操作系统）数据库安全审计 Agent 客户端日志保存在哪里?

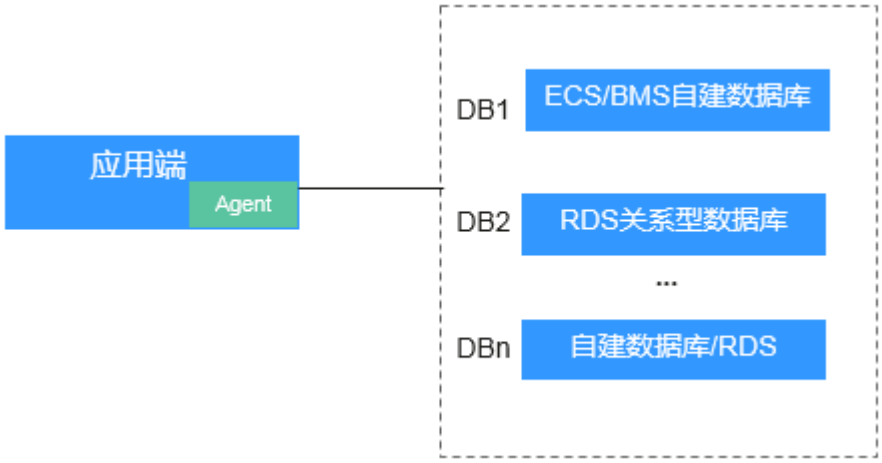
Agent客户端日志存放路径为：“/opt/dbss_audit_agent/log/audit_agent.log”

33.2.7 添加 Agent 时，在什么场景下需要选择“选择已有 Agent”添加方式?

当某个应用端连接了多个数据库时，如图33-3所示。如果连接该应用端的某个数据库（例如“DB1”），已在应用端添加了Agent（即“DB1”数据库在添加Agent时，“安装节点类型”选择“应用端”）。则连接该应用端的其他数据库在添加Agent时，只需要选择“选择已有Agent”添加方式（即选择“DB1”已添加的Agent），如图33-4所示。

如果您已在该应用端安装了Agent，则该数据库添加Agent后，数据库安全审计即可对其进行审计。

图 33-3 一个应用端连接了多个数据库



说明

连接的数据库类型包括：

- 全是ECS/BMS自建数据库
- 全是RDS关系型数据库
- ECS/BMS自建数据库与RDS关系型数据库

图 33-4 选择已有 Agent

33.2.8 当数据库安全审计 Agent 的运行状态为“休眠中”时，如何处理?

待审计的数据库添加Agent后，该Agent的初始运行状态为“休眠中”，如图33-5所示。

图 33-5 Agent 添加完成

添加Agent后，您还需要在安装节点上安装Agent，才能使用数据库安全审计。

请您安装Agent后，再查看该Agent的运行状态。

- 如果安装Agent后Agent正常运行，则该Agent的运行状态，如图33-6所示。

  图 33-6 Agent 运行正常

- 如果安装Agent后，该Agent的运行状态仍为“休眠中”，请参照**Agent与数据库安全审计实例之间通信异常**章节进行处理。

33.2.9 如何选择数据库安全审计的 Agent 安装节点?

数据库安全审计的Agent可以安装在数据库端、应用端和代理端。建议您按“数据库端 > 应用端 > 代理端”优先级顺序选择Agent的安装节点。

在各节点上安装Agent的详细说明如表33-5所示。

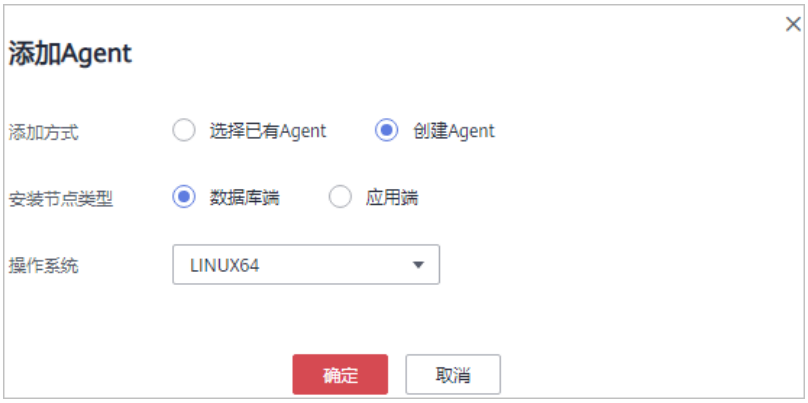
表 33-5 数据库安全审计 Agent 安装说明

Agent安装节点	使用场景	审计功能说明	注意事项
数据库端	ECS/BMS自建数据库	可以审计所有访问该数据库的应用端的所有访问记录。	添加Agent时，“安装节点类型”选择“数据库端”。
应用端	无法登录到数据库节点的部署环境（例如，RDS关系型数据库）	可以审计该应用端与其连接的所有数据库的访问记录。	• 添加Agent时，“安装节点类型”选择“应用端”，如图33-8所示。 • 当某个应用端连接了多个数据库时，如果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，只需要选择“选择已有Agent”添加方式，如图33-9所示。
代理端	无法登录到数据库节点，且不能在应用端安装Agent的部署环境（例如，RDS关系型数据库且应用端在云下）	只能审计代理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。	添加Agent时，需要将该代理端作为应用端，即“安装节点类型”选择“应用端”，且“安装节点IP”需要配置为该代理的IP地址。

添加 Agent 方式说明

- 数据库端

  图 33-7 在数据库端添加 Agent

- 应用端

图 33-8 在应用端添加 Agent

图 33-9 选择已有 Agent

须知

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，只需要选择“选择已有Agent”添加方式。详细介绍，请参见**添加Agent时，在什么场景下需要选择“选择已有Agent”添加方式?** 。

- 代理端

图 33-10 在应用端添加 Agent

须知

安装节点IP需要配置为代理的IP地址。

33.2.10 如何下载数据库安全审计的 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AgentID，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

- 已成功申请数据库安全审计实例，且实例的状态为“运行中”。
- 数据库已成功添加Agent。

操作步骤

步骤1 登录管理控制台。

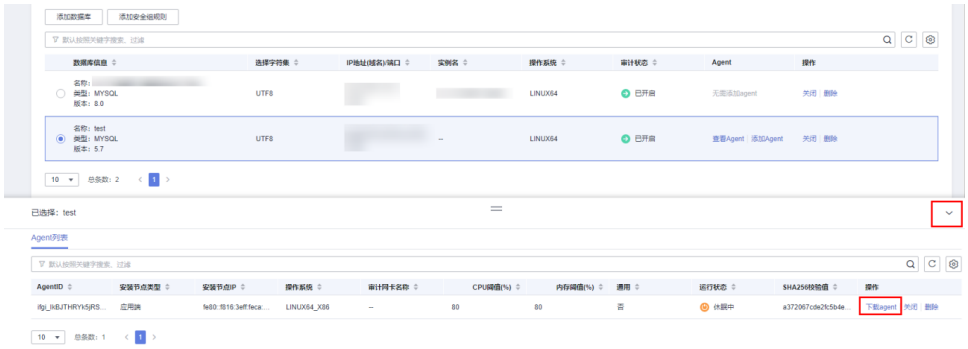
步骤2 在页面上方选择“区域”后，单击 ☰，选择“安全 > 数据库安全服务 DBSS”，进入数据库安全审计“总览”界面。

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，选择需要下载Agent的数据库所属的实例。

步骤5 单击“数据库列表”列表页面下方的 ^ 展开Agent的详细信息，在Agent所在行的“操作”列，单击“下载agent”。将Agent安装包下载到本地。

图 33-11 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

33.2.11 如何卸载数据库安全审计 Agent 程序?

在数据库端或应用端的节点安装Agent后，当不需要停止审计数据库时，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

33.2.12 如何处理 Agent 与数据库安全审计实例之间通信异常?

故障现象

在数据库端或应用端安装Agent后，在数据库上输入SQL语句，SQL语句列表中未显示该SQL语句。

建议您按照本章节的操作步骤进行处理：

- **检查添加的数据库信息以及审计状态**
- **检查数据库安全审计实例的安全组规则**
- **检查安装节点的Agent程序运行状态**

检查添加的数据库信息以及审计状态

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 ☰，选择“安全 > 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，选择需要排查的数据库所属的实例。

步骤5 检查待审计的数据库信息，如图33-12所示。

图 33-12 查看待审计的数据库信息

- 如果数据库信息正确，请执行**步骤6**。
- 如果数据库信息错误，请先单击“删除”，删除该数据库，再单击“添加数据库”，重新添加数据库。
  - 如果问题已解决，结束操作。
  - 如果问题仍存在，请执行**步骤6**。

步骤6 检查待审计的数据库的审计状态，如**图33-13**所示。

图 33-13 查看待审计的审计状态

- 如果“审计状态”为“已开启”，请执行**检查数据库安全审计实例的安全组规则**。
- 如果“审计状态”为“已关闭”，请单击“开启”，开启数据库审计。
  - 如果问题已解决，结束操作。
  - 如果问题仍存在，请执行**检查数据库安全审计实例的安全组规则**。

----结束

检查数据库安全审计实例的安全组规则

步骤1 单击数据库左侧的 ⌄ 展开Agent的详细信息，并记录“安装节点IP”，如**图33-14**所示。

图 33-14 记录安装节点 IP 信息

步骤2 在左侧导航树中，选择“数据库安全审计 > 实例列表”，进入实例列表界面。

步骤3 单击需要处理的实例名称，进入实例概览页面。

步骤4 在“网络配置信息”区域，记录数据库安全审计实例的“安全组”（例如default），如**图33-15**所示。

图 33-15 获取数据库安全审计实例所在的安全组

步骤5 单击页面左上方的 ☰，选择“网络 > 虚拟私有云 VPC”，进入虚拟私有云列表界面。

步骤6 在左侧导航树中，选择“访问控制 > 安全组”，进入安全组列表界面。

步骤7 在列表右上方的搜索框中输入**步骤4**中记录的安全组“default”后，单击 🔍 或按“Enter”，列表显示“default”安全组信息。

步骤8 单击“default”，进入“入方向规则”页面。

步骤9 检查“default”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**步骤1**中的安装节点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入方向规则，请执行**检查安装节点的Agent程序运行状态**。
- 如果该安全组未配置入方向规则，请执行**步骤10**。

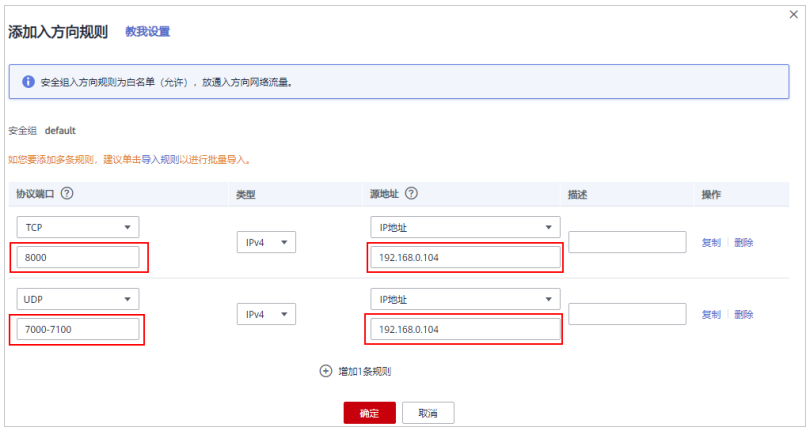
步骤10 添加数据库安全审计实例安全组的入方向规则。

1. 单击“添加规则”，如**图33-16**所示。

图 33-16 添加规则

2. 在“添加入方向规则”对话框中，为**步骤1**中安装节点IP添加TCP协议（端口为8000）和UDP协议（端口为7000-7100）规则，如**图33-17**所示。

图 33-17 “添加入方向规则”对话框



3. 单击“确定”。
   - 如果问题已解决，结束操作。
   - 如果问题仍存在，请执行**检查安装节点的Agent程序运行状态**。

----结束

检查安装节点的 Agent 程序运行状态

- Linux操作系统
  a. 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Agent的安装节点。
  b. 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，请执行**效果验证**。

       ```
       audit agent is running.
       ```

     - 如果界面无回显信息，说明Agent程序运行异常，请执行以下命令，重新启动Agent后，再执行**效果验证**。

       service audit_agent restart

- Windows操作系统
  a. 打开任务管理器。
  b. 查看“dbss_audit_agent”进程运行状态。

     - 如果进程正在运行，请执行**效果验证**。
     - 如果进程停止，请进入Agent安装文件的目录，双击“start.bat”执行文件，开启审计进程后，再执行**效果验证**。

效果验证

在数据库中输入一条SQL语句后，在“总览 > 语句”高级选项中搜索执行的语句。

- 如果可以搜索到输入的SQL语句信息，说明问题已解决。
- 如果不能搜索到输入的SQL语句信息，说明问题仍存在，请联系技术支持。

33.3 操作类

33.3.1 如何关闭数据库 SSL?

操作场景

- 通过“免安装Agent”方式审计数据库时，不需要执行关闭数据库SSL操作。请跳过本章节。
- 通过“安装Agent”方式审计数据库时，关闭数据库的SSL是必要操作。如果您开启了数据库SSL，将无法获取审计数据。

操作步骤

以MySQL数据库自带的客户端为例说明，操作步骤如下：

步骤1 使用MySQL数据库自带的客户端，以**root**用户登录MySQL数据库。

步骤2 执行以下命令，查看MySQL数据库连接的方式。

\s

- 如果界面回显类似以下信息，说明MySQL数据库已关闭SSL。
  ```
  SSL:            Not in use
  ```
- 如果界面回显类似以下信息，说明MySQL数据库已开启SSL，请执行**步骤3**。
  ```
  SSL:            Cipher in use is XXX-XXX-XXXXXX-XXX
  ```

步骤3 以SSL模式登录MySQL数据库。

1. 执行以下命令，退出MySQL数据库。

   exit

2. 以**root**用户重新登录MySQL数据库。

   在登录命令后添加以下参数：

   --ssl-mode=DISABLED

   或

   --ssl=0

   须知

   以SSL模式登录MySQL数据库，只能关闭本次SSL。当需要使用数据库安全审计功能时，请以本步骤登录MySQL数据库。

3. 执行以下命令，查看MySQL数据库连接的方式。

   \s

   如果界面回显类似以下信息，说明MySQL数据库已关闭SSL。
   ```
   SSL:            Not in use
   ```

----结束

33.3.2 如何对所有数据库设置数据库安全审计规则?

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

在添加风险操作时，您也可以将添加的风险操作应用到连接数据库审计实例的所有数据库，如图33-18所示。

图 33-18 风险操作应用到连接到实例的所有数据库

33.3.3 如何查看数据库安全审计的版本信息?

请参照以下操作步骤查看数据库安全审计的版本信息。

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 ☰，选择“安全 > 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 查看实例版本信息，如图33-19所示。

图 33-19 查看实例版本信息

----结束

33.3.4 如何查看数据库安全审计所有的告警信息?

请参照以下操作步骤查看数据库安全审计的告警信息。

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 ，选择“安全 > 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“监控 > 告警监控”，进入告警监控页面。

步骤5 查看告警信息，如图33-20所示。

图 33-20 查看告警信息

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”或“近30天”），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。

----结束

33.3.5 PC 通过内网访问 RDS（即应用端在云下）时，如何使用数据库安全审计?

当PC通过专线内网访问RDS时，您可以将Agent安装到自建的代理端。此时，PC通过代理端访问数据库，数据库安全审计只能审计代理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。

33.4 故障排查

33.4.1 数据库安全审计运行正常但无审计记录

故障现象

数据库安全审计实例功能正常，当触发数据库流量后，在SQL语句列表页面搜索执行的语句，不能搜索到相关的审计信息。

可能原因

- 数据库已开启SSL。
- 数据库SQL SERVER协议已开启强行加密。
- 数据量过大，造成Agent进程假死。建议重启容器或优化审计规则以减少数据量。

说明

- 数据库开启SSL时，将不能使用数据库安全审计功能。
- 数据库开启强行加密，数据库安全审计将无法获取文件内容进行分析。

关闭数据库 SSL

以MySQL数据库自带的客户端为例说明，操作步骤如下：

步骤1 使用MySQL数据库自带的客户端，以**root**用户登录MySQL数据库。

步骤2 执行以下命令，查看MySQL数据库连接的方式。

\s

- 如果界面回显类似以下信息，说明MySQL数据库已关闭SSL，请执行**步骤4**。
  ```
  SSL:            Not in use
  ```
- 如果界面回显类似以下信息，说明MySQL数据库已开启SSL，请执行**步骤3**。
  ```
  SSL:            Cipher in use is XXX-XXX-XXXXXX-XXX
  ```

步骤3 以SSL模式登录MySQL数据库。

1. 执行以下命令，退出MySQL数据库。

   exit

2. 以**root**用户重新登录MySQL数据库。

   在登录命令后添加以下参数：

   --ssl-mode=DISABLED

   或

   --ssl=0

   须知

   以SSL模式登录MySQL数据库，只能关闭本次SSL。当需要使用数据库安全审计功能时，请以**步骤3.2**方式登录MySQL数据库。

3. 执行以下命令，查看MySQL数据库连接的方式。

   \s

   如果界面回显类似以下信息，说明MySQL数据库已关闭SSL。请执行**步骤4**。
   ```
   SSL:            Not in use
   ```

步骤4 输入一条SQL语句后，在SQL语句列表页面搜索执行的语句。

- 如果可以搜索到输入的SQL语句信息，说明问题已解决。
- 如果不能搜索到输入的SQL语句信息，说明问题仍存在，请执行**关闭SQL SERVER协议的强行加密**。

----结束

关闭 SQL SERVER 协议的强行加密

步骤1 打开SQL Server Configuration Manager配置管理器。

步骤2 选择“SQL Server网络配置”。

步骤3 右键单击“MSSQLSERVER的协议”，选择“属性”。

步骤4 在弹出的弹框中，选择“标志”页签，关闭数据库的强行加密。

步骤5 重启SQL Server服务，使得修改的配置生效。

步骤6 输入一条SQL语句后，在SQL语句列表页面搜索执行的语句。

- 如果可以搜索到输入的SQL语句信息，说明问题已解决。
- 如果不能搜索到输入的SQL语句信息，说明问题仍存在，请联系技术支持。

----结束

33.4.2 无法使用数据库安全审计

问题现象

触发数据库流量后，在SQL语句列表页面搜索执行的语句，不能搜索到相关的审计信息。

建议您按照本章节的操作步骤排查无法审计SQL语句的原因并进行修改。

- **检查数据库信息是否正确以及数据库的审计是否已开启**
- **检查审计范围中对应数据库是否已启用**
- **检查数据库的Agent程序运行状态**
- **检查数据库安全审计实例安全组规则是否开放**

检查数据库信息是否正确以及数据库的审计是否已开启

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 ☰，选择“安全 > 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”，进入数据库列表页面。

步骤4 在“实例列表”下拉列表框中选择数据库所在的实例。

步骤5 查看数据库信息，如图33-21所示。

图 33-21 查看待审计数据库的信息

步骤6 检查数据库信息是否正确。

- 如果数据库信息正确，请执行**步骤7**。
- 如果数据库信息错误，请先单击“删除”，删除该数据库，再单击“添加数据库”，重新添加该数据库。
  - 如果问题已解决，结束操作。
  - 如果问题仍存在，请执行**步骤7**。

步骤7 检查数据库的审计是否已开启。

- 如果“审计状态”为“已开启”，请执行**检查审计范围中对应数据库是否已启用**。
- 如果“审计状态”为“已关闭”，请单击“开启”，开启数据库审计。
  - 如果问题已解决，结束操作。
  - 如果问题仍存在，请执行**检查审计范围中对应数据库是否已启用**。

----结束

检查审计范围中对应数据库是否已启用

在左侧导航树中，选择“数据库安全审计 > 审计规则”，进入审计范围列表页面，如**图33-22**所示。

图 33-22 审计范围信息

- 如果“状态”为“已启用”，请执行**检查数据库的Agent程序运行状态**。
- 如果“状态”为“已禁用”，请单击“启用”，启用数据库对应的审计范围规则。
  - 如果问题已解决，结束操作。
  - 如果问题仍存在，请执行**检查数据库的Agent程序运行状态**。

检查数据库的 Agent 程序运行状态

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Agent的安装节点。

步骤2 执行以下命令，查看Agent程序的运行状态。

ps -ef|grep audit_agent

- 如果界面回显以下信息，说明Agent程序运行正常，请执行**步骤4**。
  ```
  /opt/dbss_audit_agent/bin/audit_agent
  ```
- 如果界面无回显信息，说明Agent程序运行异常，请执行**步骤3**。

步骤3 执行以下命令，重新启动Agent。

service audit_agent restart

- 如果问题已解决，结束操作。
- 如果问题仍存在，请执行**步骤4**。

步骤4 执行以下命令，检查Agent与数据库安全审计实例之间的通信状态。

tailf /opt/dbss_audit_agent/log/audit_agent.log

- 如果界面回显类似以下信息，说明Agent与数据库安全审计实例之间通信正常，请执行**效果验证**。

图 33-23 通信正常

```
-]# tailf  /opt/dbss_audit_agent/log/audit_agent.log
':37 INFO  [websocket_message_handle.cpp:357] send config data capture result begin...
':37 INFO  [websocket_message_handle.cpp:359] send config data capture result success
':37 INFO  [websocket_message_handle.cpp:136] audit ethernet is: eth0
':37 INFO  [websocket_message_handle.cpp:149] libpcap filter policy is: port 3306 and (src host 192.168.0.118 or dst host 192.168.0.118)
':37 INFO  [catch_data_package.cpp:119] init libpcap tool begin...
':37 INFO  [catch_data_package.cpp:155] init libpcap tool success
':37 INFO  [udp_communication.cpp:28] init udp connection begin...
':37 INFO  [udp_communication.cpp:51] init udp connection success!
':37 INFO  [catch_data_package.cpp:167] catch data packet begin...
':39 INFO  [websocket_message_handle.cpp:430] send heart beat begin
```

- 如果界面回显类似以下信息，说明Agent与数据库安全审计实例之间通信异常，请**检查数据库安全审计实例安全组规则是否开放**。

图 33-24 通信异常

```
AWdimb74cL5BfUHrp8-tJ# tail /opt/dbss_audit_agent/log/audit_agent.log
INFO  [websocket.cpp:1608] create websocket thread begin...
INFO  [websocket.cpp:1620] create websocket thread success
INFO  [websocket_connection_handle.cpp:278] setup websocket connection success
INFO  [websocket_connection_handle.cpp:169] send authentication request packet with websocket...
INFO  [websocket_connection_handle.cpp:126] create authentication request packet begin...
INFO  [websocket_connection_handle.cpp:25] encrypt verify info by public key begin...
INFO  [websocket_connection_handle.cpp:53] encrypt verify info by public key success
INFO  [websocket_connection_handle.cpp:158] create authentication request packet success
INFO  [websocket_connection_handle.cpp:172] authentication request packet is: {"body":{"agentid":"AWdimb74cL5BfUH
':"EulerOS","ostype":"Linux","osver":"3.10.0-327.36.58.4.x86_64","verify":"IHGabvph0aqK6Q+saLeIaIMLRBIA/S37uGRgQqJ
cJUMWkSsz1VSlHZwidlMraDnczItXe4NMiwn//fzcZdj9qeendGh0BIv3CXpdDDzY3SMoUlkfbauolqdMIpwrNw5utJD55id5Qn0vfgunuZJWTc2A
'OQTb2Cli0iEKGHLteQ=="},"code":1,"id":"98c43f29-e302-402a-9e75-321b2f6e86c2","method":"request","time":1543807412}
ERROR [websocket_connection_handle.cpp:177] send authentication request packet failed, retry 30 seconds later!
```

----结束

检查数据库安全审计实例安全组规则是否开放

步骤1 进入数据库安全服务管理界面。

步骤2 在左侧导航树中，选择“数据库安全审计 > 数据库列表”，进入数据库列表页面。

步骤3 在“实例列表”下拉列表框中选择数据库所在的实例。

步骤4 记录**Agent安装节点IP信息。**

单击数据库左侧的 ⌄ 展开Agent的详细信息，并记录“安装节点IP”，如**图33-25**所示。

图 33-25 安装节点 IP

步骤5 **记录待审计的数据库所在的安全组信息。**

1. 在左侧导航树中，选择“数据库安全审计 > 实例列表”，进入实例列表页面。
2. 单击需要处理的实例名称，进入实例概览页面。

3. 在“网络配置信息”区域，记录数据库安全审计实例的“安全组”（例如default），如图33-26所示。

图 33-26 获取待审计数据库所在的安全组信息

步骤6 进入安全组的规则页面。

1. 单击页面左上方的 ☰，选择“网络 > 虚拟私有云 VPC”，进入虚拟私有云列表界面。
2. 在左侧导航树中，选择“访问控制 > 安全组”，进入安全组列表界面。
3. 在列表右上方的搜索框中输入5.c中记录的安全组“default”后，单击 🔍 或按“Enter”，列表显示“default”安全组信息。
4. 单击“default”，进入“入方向规则”页面。
5. 检查“default”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步骤4中的安装节点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入方向规则，请执行效果验证。
   - 如果该安全组未配置入方向规则，请执行步骤7。

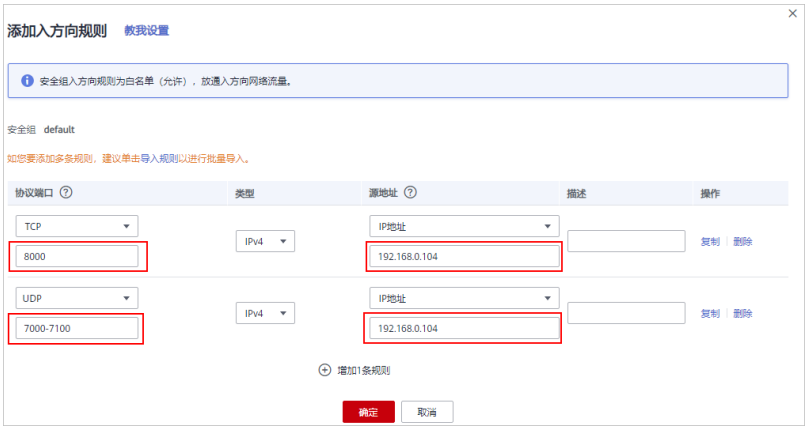
步骤7 为安装节点添加入方向安全规则。

1. 在入方向规则页面，单击“添加规则”，如图33-27所示。

图 33-27 添加规则-0

2. 在“添加入方向规则”对话框中，为图33-25中的安装节点IP添加TCP协议（端口为8000）和UDP协议（端口为7000-7100）规则，如图33-28所示。

图 33-28 添加入方向规则



3. 单击“确定”，完成添加入方向规则。

----结束

效果验证

在数据库中输入一条SQL语句后，在SQL语句列表页面搜索执行的语句。

- 如果可以搜索到输入的SQL语句信息，说明问题已解决。
- 如果不能搜索到输入的SQL语句信息，说明问题仍存在，请联系技术支持。

33.5 日志类

33.5.1 数据库安全审计的操作日志是否可以迁移?

不可以。数据库安全审计当前不支持迁移数据库操作日志。

您可以查看数据库安全审计的操作日志，有关查看数据库安全审计操作日志的详细操作，请参见**数据库安全审计的操作日志默认保存多久?** 。

33.5.2 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会一直保存。

33.5.3 如何查看数据库安全审计的用户操作日志?

请参照以下操作步骤，查看用户在数据库安全审计系统的操作日志。

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 ☰，选择“安全 > 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，如图33-29所示，相关参数说明如表33-6所示。

图 33-29 查看操作日志

说明

选择时间（“近30分钟”、“近1小时”、“近24小时”、“近7天”或“近30天”）；或者单击，选择开始时间和结束时间，列表显示指定时间段的操作日志。

表 33-6 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

33.5.4 数据库安全审计的日志处理机制是什么?

数据库安全审计的审计日志存放在日志数据库中，日志的处理机制说明如下：

- 当日志数据库的磁盘空间使用率达到85%及以上时，系统将自动循环删除存放时间最久的审计日志（每次删除一天的审计日志），直至磁盘空间使用率为85%以下。
- 当日志数据库的磁盘空间使用率达到90%及以上时，数据库安全审计将停止审计功能，系统将不保存新生成的审计日志。

33.5.5 数据库安全审计的审计日志是否支持备份?

数据库安全审计支持手动和自动两种备份方式。备份日志后，审计日志将备份到对象存储服务上，并自动为您创建桶，桶按用量需要单独收费。

请参照以下操作步骤，自动备份审计日志。

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 ☰，选择“安全 > 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“设置自动备份”，在弹出的对话框中，设置自动备份参数，如图33-30所示，相关参数说明如表33-7所示。

图 33-30 “设置自动备份”对话框

表 33-7 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。	
备份周期	选择自动备份的周期，可以选择： • 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
预计下次备份时间	预计下次自动备份开始时间。	2020/01/15 20:21:29

参数名称	说明	取值样例
Access Key ID(AK)	输入访问密钥的AK。	-
Secret Access Key(SK)	输入访问密钥的SK。	-

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

