天翼云·数据库安全服务

用户使用指南

天翼云科技有限公司

目 录

1 产品简介

1.1 产品定义

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。

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：

- 关系型数据库（Relational Database Service，RDS）
- 云主机（Elastic Cloud Server ，ECS）的自建数据库
- 物理机（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） • 8.0.23 • 8.0.25
Oracle (因 Oracle 为闭源协议，适配版本复杂，如您需审计 Oracle 数据库，请先联系客服人员)	• 11g 11.1.0.6.0 、11.2.0.1.0 、11.2.0.2.0、11.2.0.3.0、11.2.0.4.0 • 12c 12.1.0.2.0 、12.2.0.1.0 • 19c
PostgreSQL	• 7.4 • 8.0

数据库类型	版本
	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
SQL Server	• 2008、2008R2 • 2012 • 2014 • 2016 • 2017
DWS	• 1.5 • 8.1
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0
Greenplum	V6.0
HighGo	V6.0
TAURUS	MySQL 8.0
GaussDB	1.4 企业版
DAMENG	DM8
KINGBASE	V8
MongoDB	V5.0

1.2 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。

1.3 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

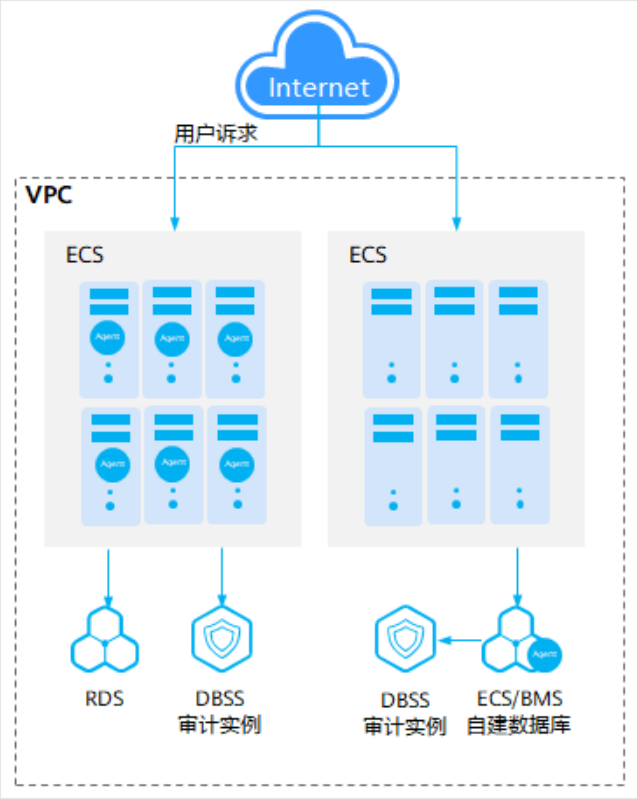
提供风险分布情况分析报表。

1.4 应用场景

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 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：500GB	• 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：1000GB • 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
高级版	最多支持 30 个数据库实例	• CPU：16U • 内存：64GB • 硬盘：2000GB • 硬盘：2T	• 吞吐量峰值：30,000 条/秒 • 入库速率：1080 万条/小时 • 15 亿条在线 SQL 语句存储 • 600 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。

1.6 术语解释

可用区（AZ）

一个可用区是一个或多个物理数据中心的集合，有独立的风火水电，AZ 内逻辑上再将计算、网络、存储等资源划分成多个集群。一个 Region 中的多个 AZ 间通过高速光纤相连，以满足用户跨 AZ 构建高可用性系统的需求。

非关系型数据库

按照非关系型数据结构来联系和组织的数据库。按不同的数据结构，可细分为以下几种：键值存储数据库（key-value）、列存储（Column-oriented）数据库、面向文档（Document-Oriented）数据库、图形数据库。常用非关系型数据库有：Memcached、Redis、MongoDB、Cassandra、HBase、MemacheDB、BerkeleyDB 等。

非系统数据库

非系统数据库是指除系统数据库以外的数据库，比如用户自建数据库。

内存数据库

将数据放在内存中直接操作的数据库。相对于磁盘，内存的数据读写速度要高出几个数量级，将数据保存在内存中相比从磁盘上访问能够极大地提高应用的性能。

SQL 注入

SQL 注入攻击是一种常见的 Web 攻击方法，攻击者通过把 SQL 命令注入到 Web 后台数据库的查询字符串中，最终达到欺骗服务器执行恶意 SQL 命令的目的。例如可以从数据库获取敏感信息，或者利用数据库的特性执行添加用户、导出文件等一系列恶意操作，甚至有可能获取数据库乃至系统用户最高权限。

正则表达式

用于指定和识别文本字符串（如特定字符，单词或字符模式）的一种简洁而灵活的方式。正则表达式模式是包含下列字段的对象：名称和正则表达式定义字符串。

1.7 使用限制

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。

支持的数据库类型

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：

- 关系型数据库（Relational Database Service，RDS）
- 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

- 云主机（Elastic Cloud Server ，ECS）的自建数据库
- 物理机（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 1-3 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） • 8.0.23 • 8.0.25
Oracle (因 Oracle 为闭源协议，适配版本复杂，如您需审计 Oracle 数据库，请先联系客服人员)	• 11g 11.1.0.6.0 、11.2.0.1.0 、11.2.0.2.0、11.2.0.3.0、11.2.0.4.0 • 12c 12.1.0.2.0 、12.2.0.1.0 • 19c
PostgreSQL	• 7.4 • 8.0 8.0、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
SQL Server	• 2008、2008R2 • 2012 • 2014 • 2016 • 2017
DWS	• 1.5 • 8.1
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
TAURUS	MySQL 8.0
GaussDB	1.4 企业版
DAMENG	DM8
KINGBASE	V8
MongoDB	V5.0

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 6.3 (64bit) • CentOS 6.5 (64bit) • CentOS 6.8 (64bit) • CentOS 6.9 (64bit) • 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)
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)
OpenSUSE	• SUSE 13 (64bit) • SUSE 15 (64bit)

系统名称	系统版本
	• SUSE 42 (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) • Euler 2.5 (64bit)
OpenEuler	• OpenEuler 20.03 (64bit)
Oracle Linux	• Oracle Linux 6.9 (64bit) • Oracle Linux 7.4 (64bit)
RedHat	• Red Hat Enterprise Linux 7.4 (64bit) • Red Hat Enterprise Linux 7.6 (64bit)
NeoKylin	• NeoKylin 7.0 (64bit)
Kylin	• Kylin Linux Advanced Server release V10 (64bit)
Uniontech OS	• Uniontech OS Server 20 Enterprise (64bit)

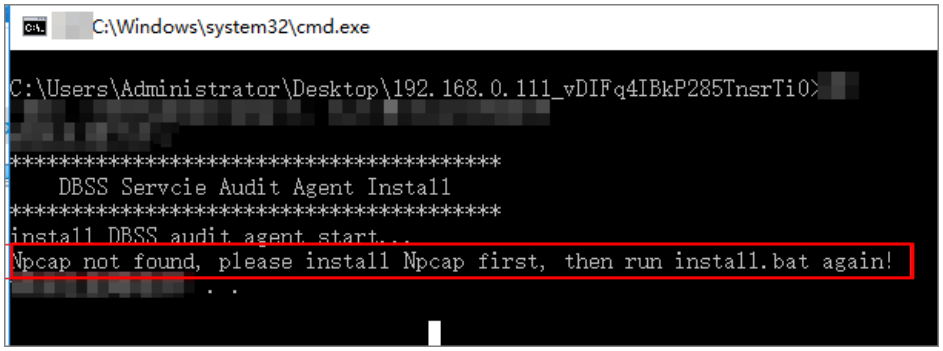
- 数据库安全审计的 Agent 支持的 Windows 系统版本如下所示：
  - Windows Server 2008 R2(64bit)
  - Windows Server 2012 R2(64bit)
  - Windows Server 2016(64bit)
  - Windows 7(64bit)
  - Windows 10(64bit)

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



1.8 该产品与其他服务的关系

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。

与物理机的关系

数据库安全服务可以为物理机上的自建数据库提供安全审计功能。

2 计费说明

计费项

数据库安全服务根据您选择 DBSS 实例规格和使用时长计费

表2-1 计费项信息

计费项	计费说明
DBSS 实例	实例版本，购买时长以及所购买的实例数量。

计费模式

数据库安全服务只提供包月的计费模式。

变更配置

如果您需要变更 DBSS 实例规格，可以先退订当前 DBSS 实例后，再重新购买 DBSS。

退订：若购买数据库安全服务后，需停止使用，请执行退订操作。

续费

包周期购买的版本到期后，您可以单击右上角“续费”，跳转至续费管理页面完成续费，延长使用期。

为避免版本到期未及时续费，导致安全风险，建议开通自动续费。开通自动续费后，系统将根据配置自动续费，无需手动操作。

3 用户指南

3.1 数据库安全审计使用指导

3.1.1 购买数据库安全审计

使用数据库安全审计功能前，您需要购买数据库安全审计。数据库安全审计提供包年/包月计费方式。

约束与限制

- 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。

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。

前提条件

确认实例账号具有相关权限。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计”，进入数据库安全审计“总览”界面。

步骤 5 在界面右上角，单击“购买数据库安全审计”。

步骤 6 选择“区域”、“项目”、“可用区”和“性能规格”，如图 3-1 所示。

图3-1 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 3-1 所示。

表3-1 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：500GB	• 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
高级版	最多支持 30 个数据库实例	• CPU：16U • 内存：64GB • 硬盘：2T	• 吞吐量峰值：30,000 条/秒 • 入库速率：1080 万条/小时 • 15 亿条在线 SQL 语句存储 • 600 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 7　设置数据库安全审计参数，如图 3-2 所示，相关参数说明如表 3-2 所示。

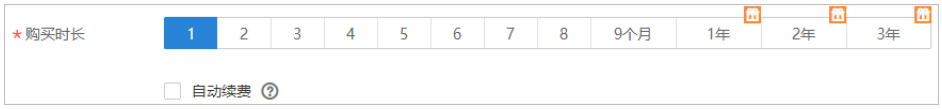
图3-2 设置数据库安全审计参数

表3-2 数据库安全审计实例参数说明

参数名称	说明
虚拟私有云	您可以选择使用区域中已有的虚拟私有云（Virtual Private Cloud，VPC）网络，或者单击“查看虚拟私有云”，跳转到 VPC 管理控制台创建新的虚拟私有云。 说明 • 请选择 Agent 安装节点（应用端或数据库端）所在的 VPC。 • 不支持修改 VPC。若要修改，请退订后重购。
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。
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。

步骤 8　选择“购买时长”，如图 3-3 所示。

图3-3 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，如果帐号余额充足，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 3-3 所示。

表3-3 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 年	1 年

步骤 9 确认当前配置无误后，单击“立即购买”。

步骤 10 在“详情”页面，阅读《数据库安全审计用户服务协议》后，勾选“我已阅读并同意《数据库安全审计用户服务协议》”，单击“提交”。

步骤 11 在购买页面，请选择付款方式进行付款。

步骤 12 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

3.1.2 步骤一：添加数据库

数据库安全审计支持对云上的 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。

前提条件

已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 5 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 6 在数据库列表框左上方，单击“添加数据库”。

步骤 7 在弹出的对话框中，设置数据库的信息，如图 3-4 所示，相关参数说明如表 数据库参数说明所示。

图3-4 “添加数据库”对话框

表3-4 数据库参数说明

参数名称	说明	取值样例
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 • MongoDB • Hbase	MYSQL

参数名称	说明	取值样例
	• SHENTONG • GBase 8a • GBase XDM Cluster • Greenplum • HighGo • Mariadb 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。	
端口	添加的数据库的端口。	3306
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： • 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：	5.0

参数名称	说明	取值样例
	– 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 • 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 • WINDOWS64	LINUX64
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”。	RDS 数据库

步骤 8 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 3-5 所示。

图3-5 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

3.1.3 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

- 已成功购买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 3-6 和图 3-7 所示。

图3-6 一个应用端连接多个 ECS/BMS 自建数据库

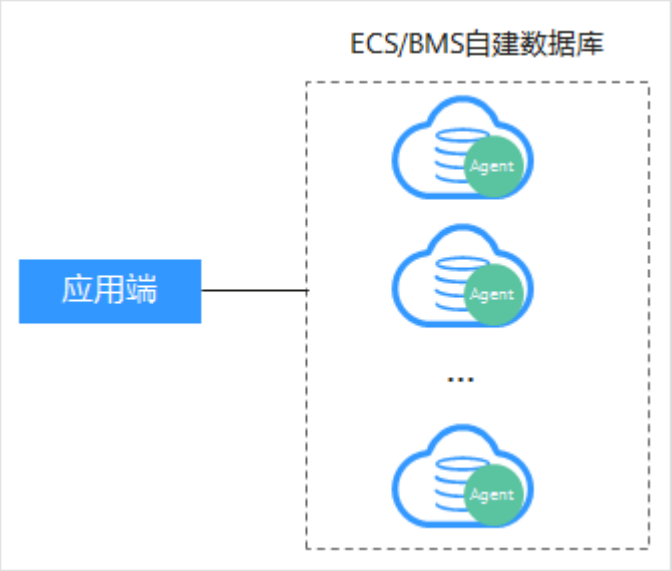
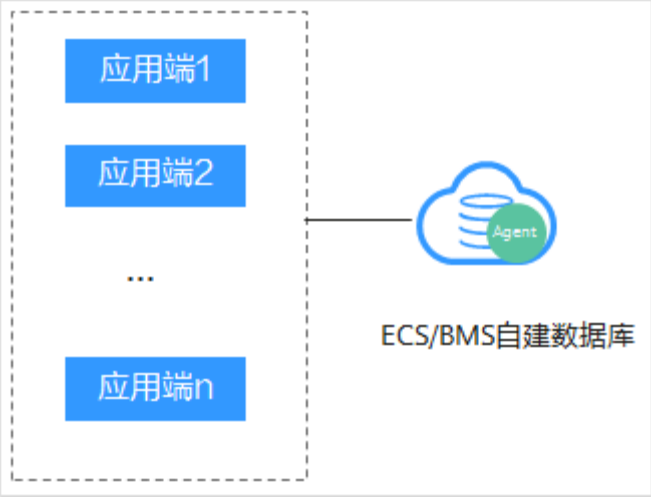


图3-7 多个应用端连接同一个 ECS/BMS 自建数据库



- RDS 关系型数据库的常见部署场景如图 3-8 和图 3-9 所示。

图3-8 一个应用端连接多个 RDS

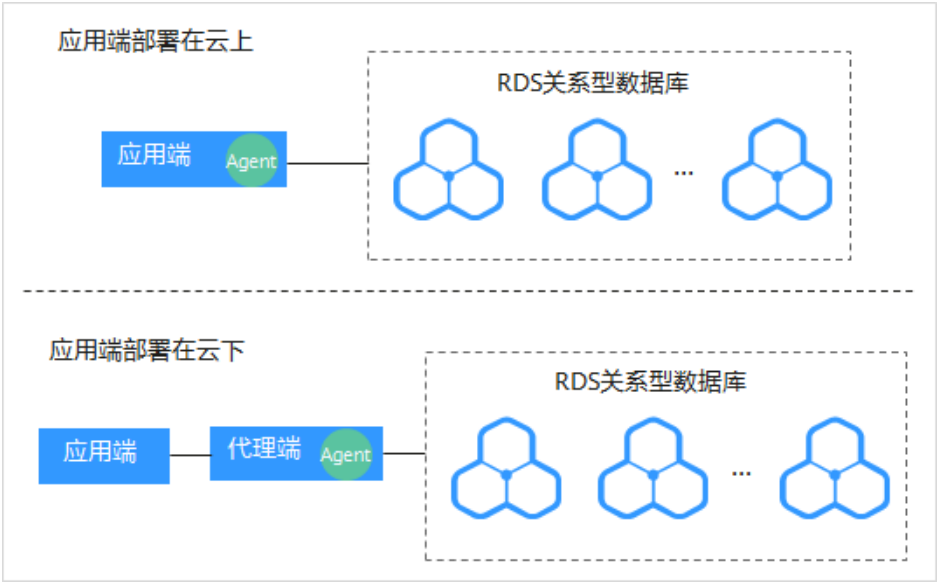
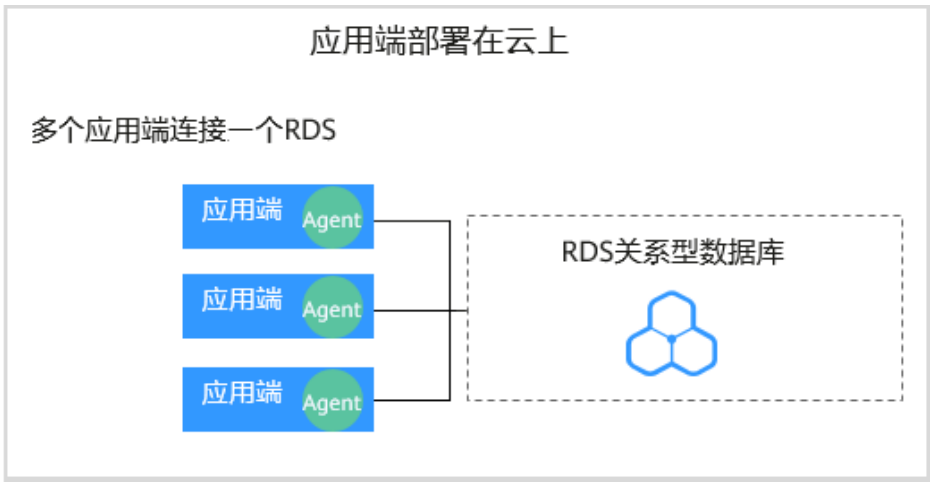


图3-9 多个应用端连接同一个 RDS



添加 Agent 方式的详细说明如表 3-5 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3-5 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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 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”。

步骤 7 在弹出的“添加 Agent”对话框中，选择添加方式，如图 3-10 所示，相关参数说明如表 3-6 所示。

图3-10 在数据库端添加 Agent

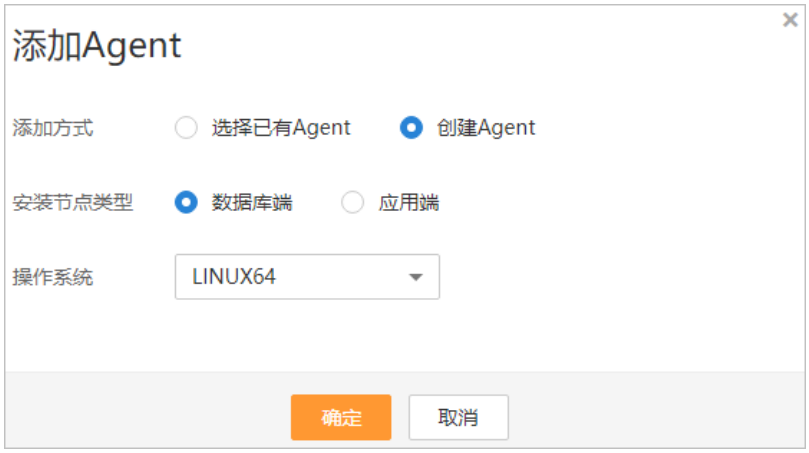


表3-6 添加 Agent 参数说明（ECS/BMS 自建数据库）

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
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 8 单击“确定”，Agent 添加成功。

步骤 9 单击数据库左侧的 展开该数据库的详细信息，查看添加的 Agent 信息，如图 3-11 所示。

图3-11 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三：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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 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”。

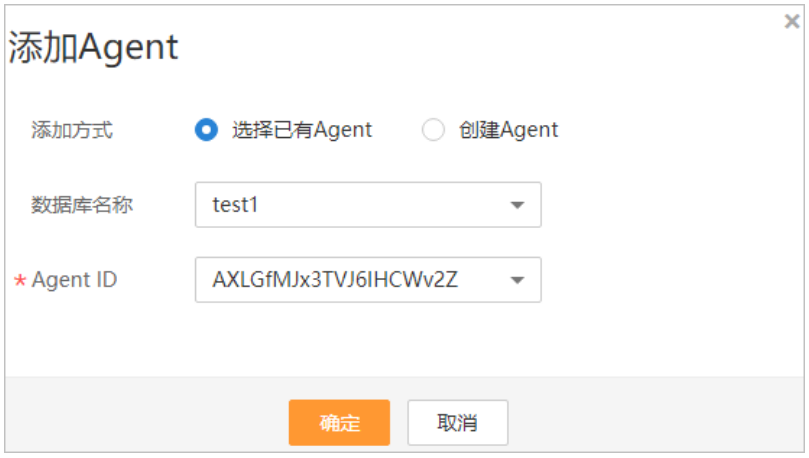
步骤 7 在弹出的“添加 Agent”对话框中，选择添加方式，如图 3-12 和图 3-13 所示，相关参数说明如表 3-7 所示。

- “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3-12 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3-13 在应用端添加 Agent

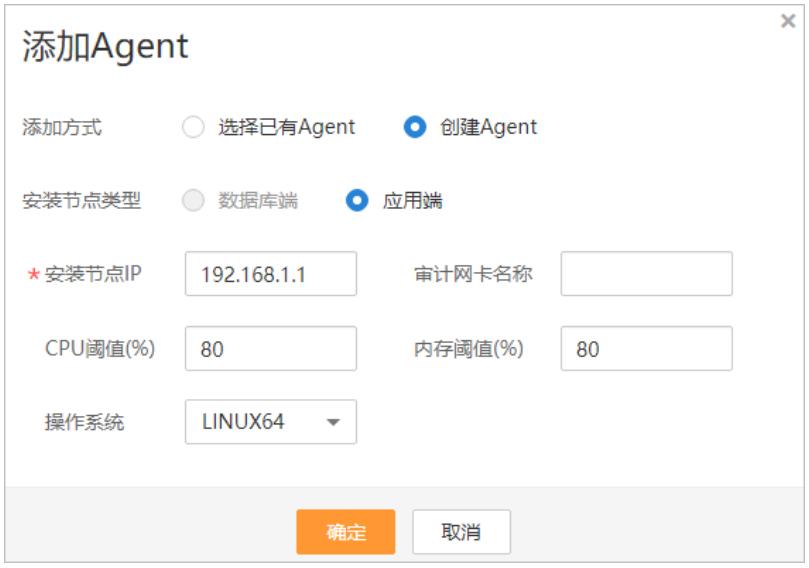


表3-7 添加 Agent 参数说明（RDS 关系型数据库）

参数名称	说明	取值样例

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
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

参数名称	说明	取值样例
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 8 单击“确定”，Agent 添加成功。

步骤 9 单击数据库左侧的 展开该数据库的详细信息，查看添加的 Agent 信息，如图 3-14 所示。

图3-14 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 3.1.5.2 安装 Agent（Linux 操作系统）。

3.1.4 步骤三：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

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 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 在数据库列表的上方，单击“添加安全组规则”。

步骤 7 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 8 单击“前往处理”，进入“安全组”列表界面。

步骤 9 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 10 单击“default”，进入“基本信息”页面。

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#dbss_01_0354/li0918135319384 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 3.1.5.1 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 12。

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”，如图 3-15 所示。

图3-15 添加规则

2. 在“添加入方向规则”对话框中，为#dbss_01_0354/fig133221637175316 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 3-16 所示。

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3-16 “添加入方向规则”对话框

3. 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

3.1.5 步骤三：下载并安装 Agent

3.1.5.1 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 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

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 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 单击数据库左侧的展开 Agent 的详细信息，在 Agent 所在行的“操作”列，单击“下载 agent”，如图 3-17 所示。将 Agent 安装包下载到本地。

图3-17 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

3.1.5.2 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。

前提条件

- 已成功购买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 3-18 和图 3-19 所示。

图3-18 一个应用端连接多个 ECS/BMS 自建数据库

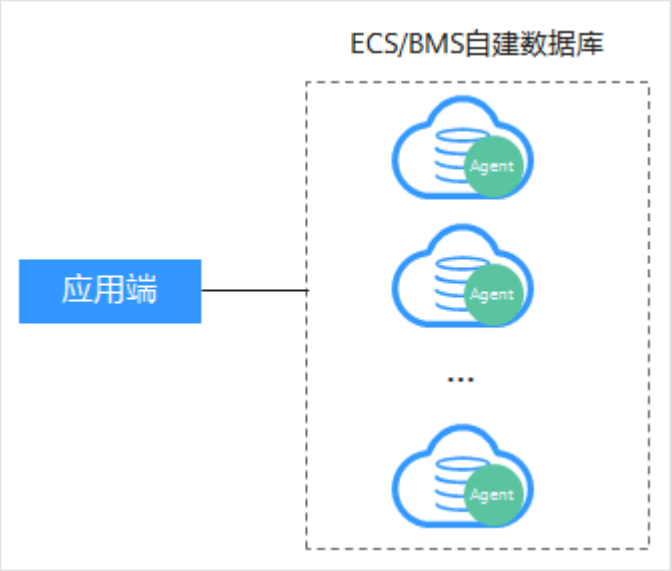
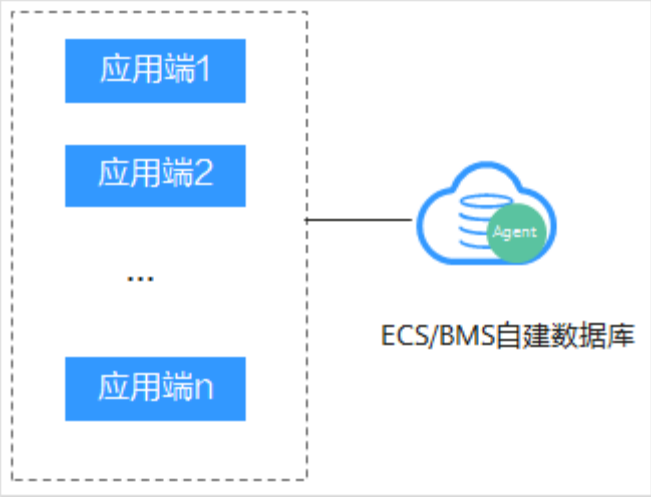


图3-19 多个应用端连接同一个 ECS/BMS 自建数据库



- RDS 关系型数据库的常见部署场景如图 3-20 和图 3-21 所示。

图3-20 一个应用端连接多个 RDS

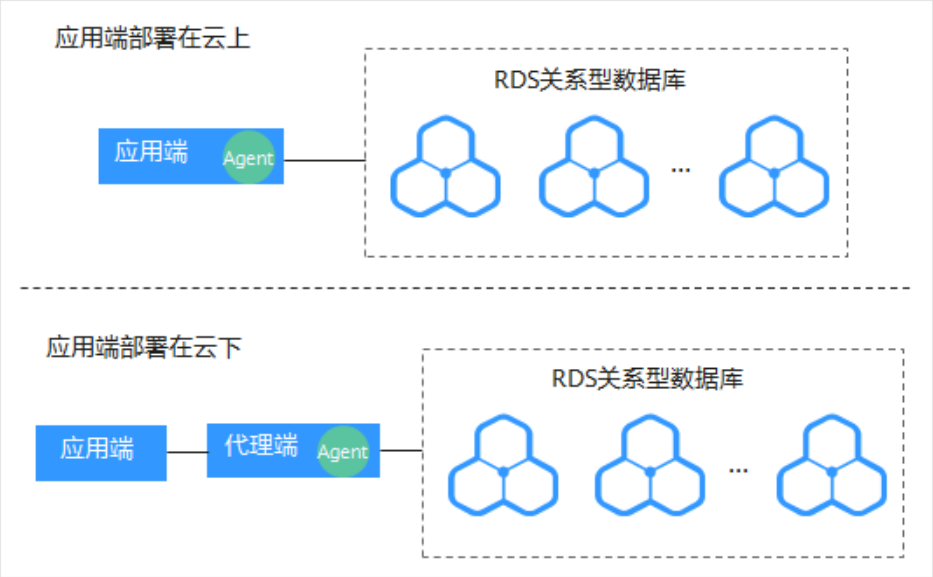
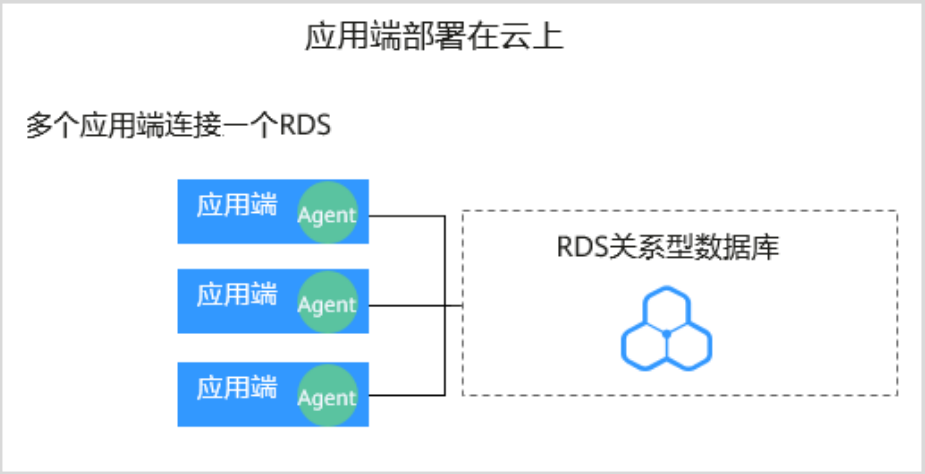


图3-21 多个应用端连接同一个 RDS



安装 Agent 节点的详细说明如表 3-8 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3-8 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

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*

步骤 4 执行以下命令，解压缩“xxx.tar.gz”安装包。

tar -xvf *xxx.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*

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

说明

用户系统是 Ubantu 时，执行以下命令安装 Agent。

bash install.sh

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。

```
audit agent is running.
```

----结束

3.1.5.3 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 3.1.5.2 安装 Agent（Linux 操作系统）。

前提条件

- 已成功购买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 3-22 和图 3-23 所示。

图3-22 一个应用端连接多个 ECS/BMS 自建数据库

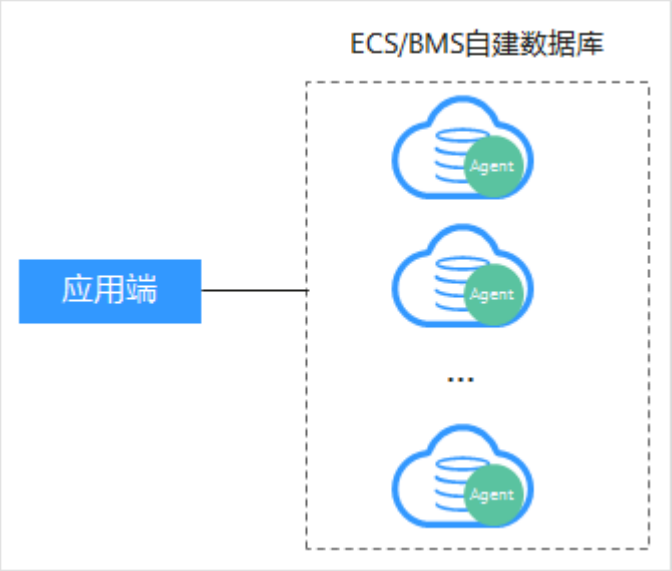
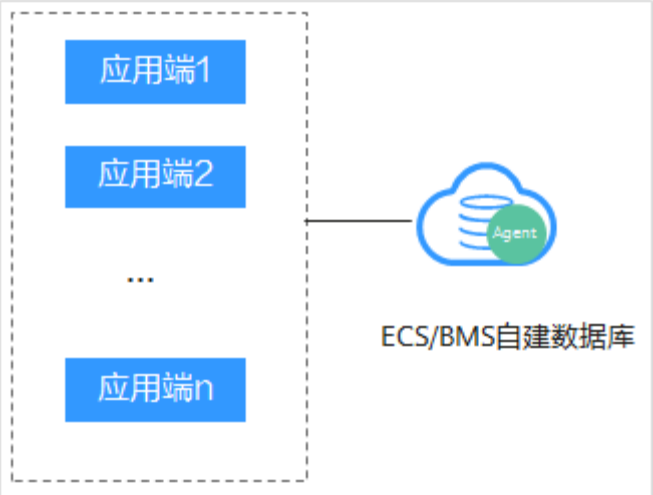


图3-23 多个应用端连接同一个 ECS/BMS 自建数据库



- RDS 关系型数据库的常见部署场景如图 3-24 和图 3-25 所示。

图3-24 一个应用端连接多个 RDS

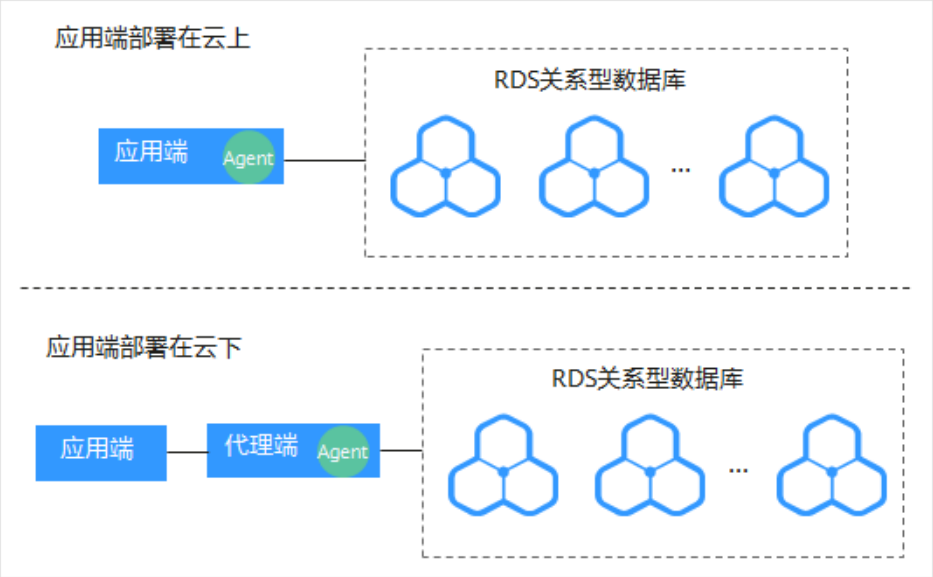
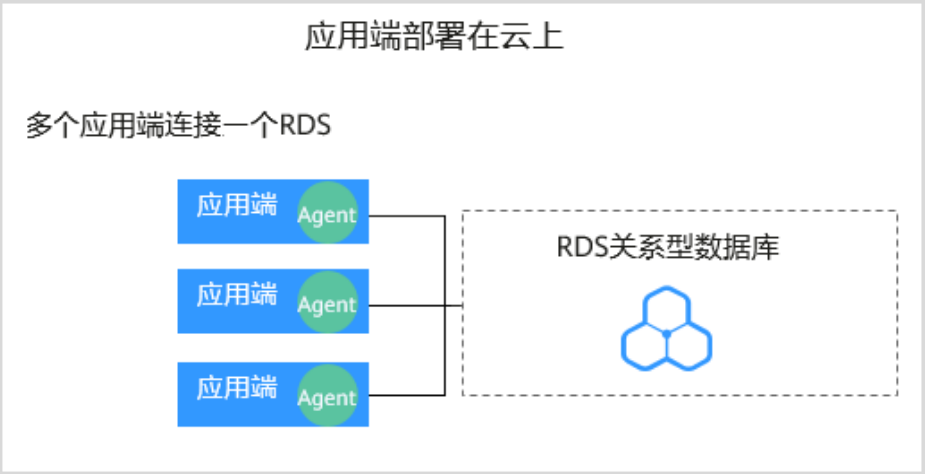


图3-25 多个应用端连接同一个 RDS



安装 Agent 节点的详细说明如表 3-9 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3-9 安装 Agent 场景说明

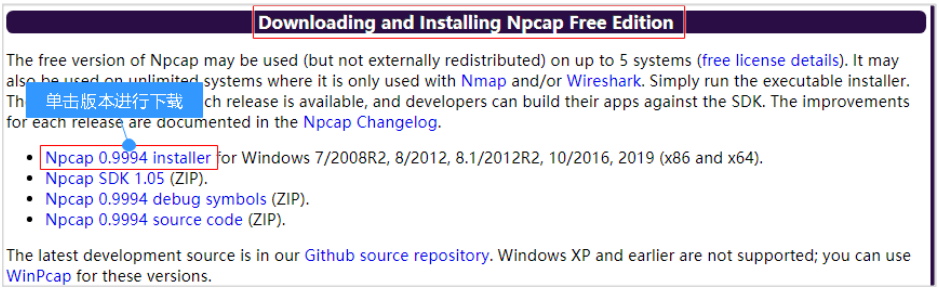
使用场景	Agent 安装节点	审计功能说明	注意事项
ECS/BMS 自建数据库	数据库端	可以审计所有访问该数据库的应用端的所有访问记录。	• 在数据库端安装 Agent。 • 当某个应用端连接多个 ECS/BMS 自建数据库时，需要在所有连接该应用端的数据库端安装 Agent。
RDS 关系型数据库	应用端（应用端部署在云上）	可以审计该应用端与其连接的所有数据库的访问记录。	• 在应用端安装 Agent。 • 当多个应用端连接同一个 RDS 时，所有连接该 RDS 的应用端都需要安装 Agent。
RDS 关系型数据库	代理端（应用端部署在云下）	只能审计代理端与后端数据库之间的访问记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

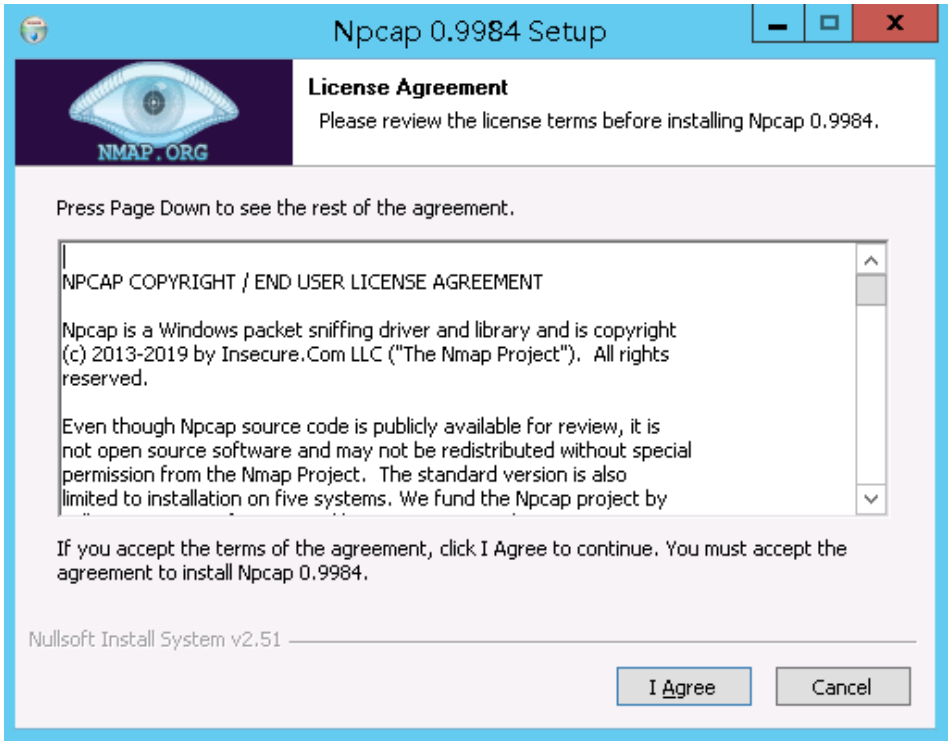
- 如果该 Windows 主机已安装“Npcap”，请执行步骤 2。
- 如果该 Windows 主机未安装“Npcap”，请执行以下步骤：
  a. 请前往 https://nmap.org/npcap/下载 Npcap 最新软件安装包。

图3-26 下载 npcap



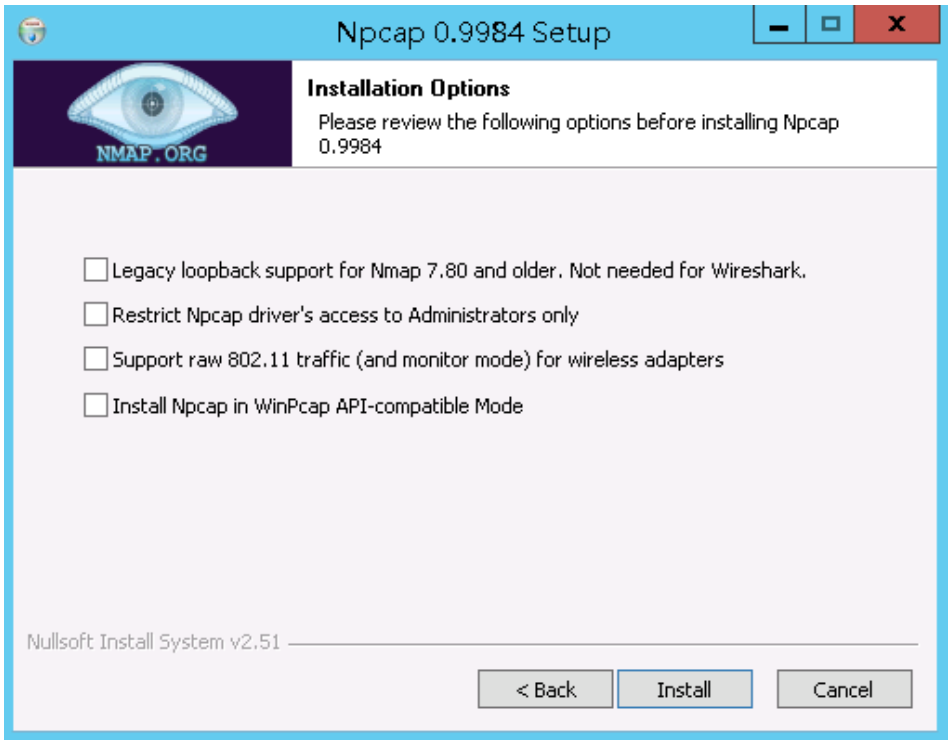
  b. 将下载好的 npcap-*xxxx*.exe 软件安装包上传至需要安装 agent 的虚拟机。
  c. 双击 npcap 软件安装包。
  d. 在弹出的对话框中，单击“I Agree”，如图 3-27 所示。

图3-27 同意安装“Npcap”

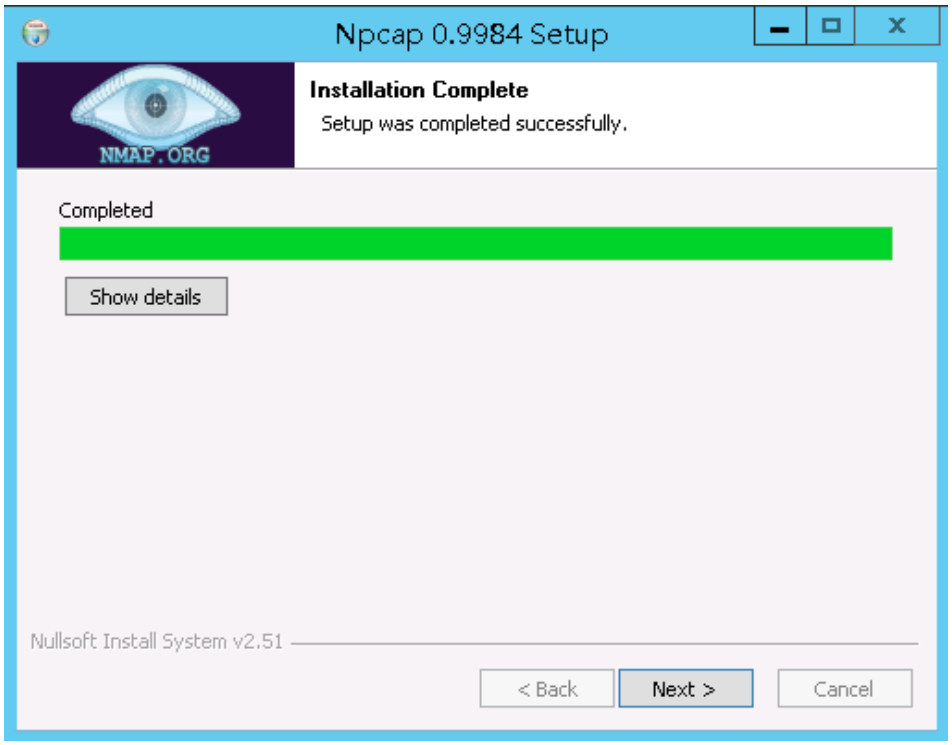


e. 在弹出的对话框中，单击“Install”，不勾选安装选项，如图 3-28 所示。

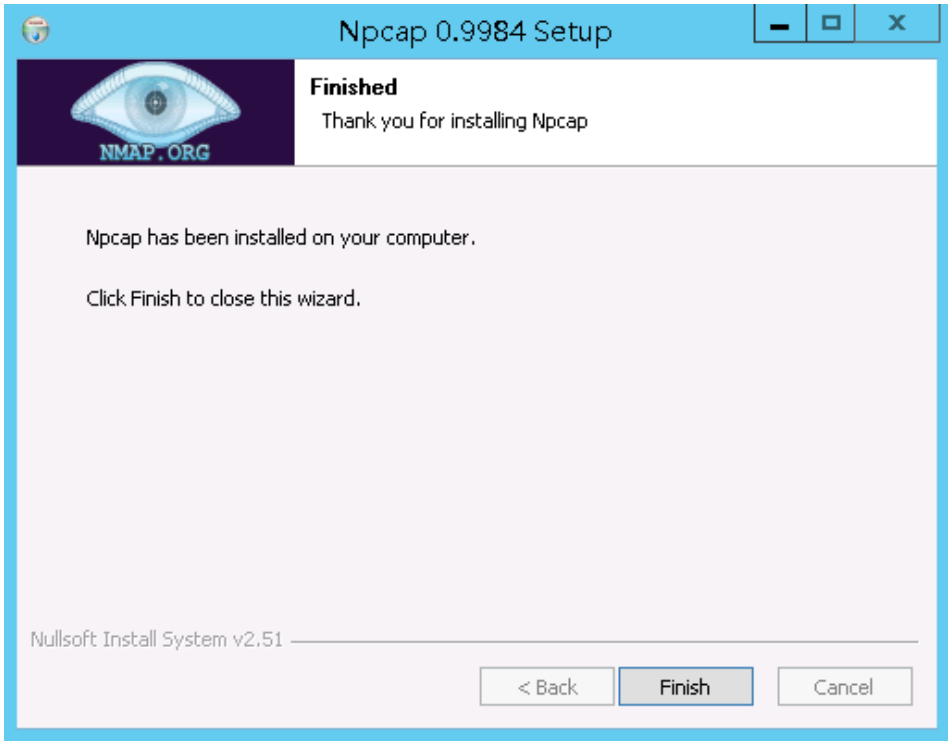
图3-28 安装“Npcap”



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 3-29 所示，按任意键结束安装。

图3-29 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

3.1.6 步骤四：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 3.1.7.1 查看审计总览信息。

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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 5 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 6 在待开启审计所在行的“操作”列，单击“开启”，如图 3-30 所示，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3-30 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“数据库安全审计 > 总览”，进入数据库安全审计“总览”界面。

步骤 4 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 5 选择“语句”页签。

步骤 6 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”，SQL 语句列表将显示步骤 1 中输入的 SQL 语句。

----结束

3.1.7 步骤五：查看审计结果

3.1.7.1 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

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 总览”，进入数据库安全审计“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，选择需要查看审计总览信息的实例。

步骤 7 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，如图 3-31、图 3-32、图 3-33 和图 3-34 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3-31 查看审计概况

图3-32 风险分布

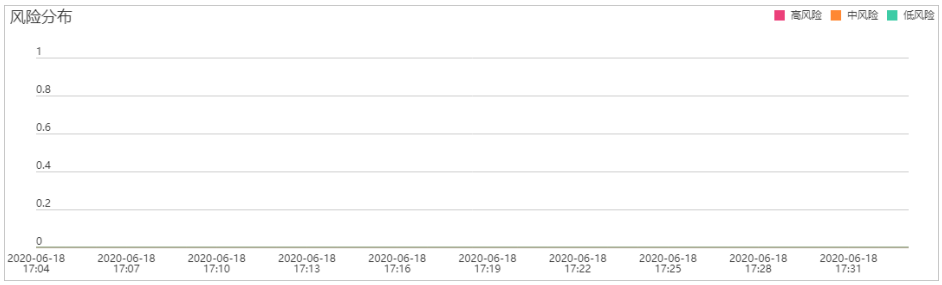


图3-33 会话统计

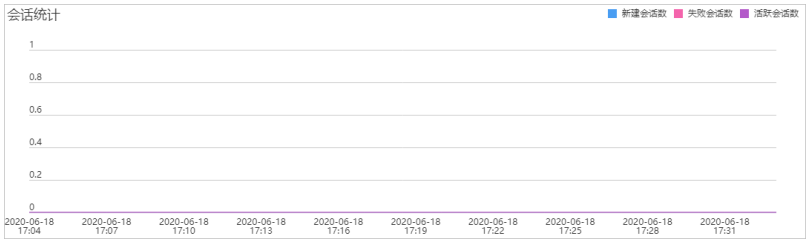
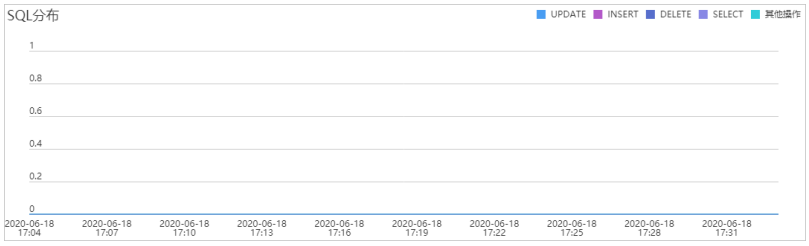


图3-34 SQL 分布



----结束

3.1.7.2 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

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 总览”，进入数据库安全审计“总览”界面。

步骤 5 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 6 选择“语句”页签。

步骤 7 查询 SQL 语句信息，如图 3-35 所示。

图3-35 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”（“全部”、“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，单击“搜索”，列表显示该时间段的 SQL 语句。
- 选择“风险等级”（“全部”、“高”、“中”、“低”或“信任”），单击“搜索”，列表显示该级别的 SQL 语句。
- 单击“高级选项”后的，输入相关信息，如图 3-36 所示，单击“提交”，列表显示该选项的 SQL 语句。

说明

一次查询最多可查询 10,000 条记录。

图3-36 高级选项信息

步骤 8 在需要查看详情的 SQL 语句所在行的“操作”列，单击“详情”。

步骤 9 在“详情”提示框中，查看 SQL 语句的详细信息，相关参数说明如表 3-10 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。

表3-10 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	执行 SQL 语句所在的数据库的 IP 地址。

参数名称	说明
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。
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

3.1.7.3 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

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 总览”，进入数据库安全审计“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，选择需要查看会话信息的实例。

步骤 7 选择“会话”页签。

步骤 8 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”、“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会话信息。

----结束

3.1.7.4 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

- 已成功购买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 3-11 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3-11 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。
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。

报表模板名称	报表类型	说明
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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 报表”，进入报表界面。

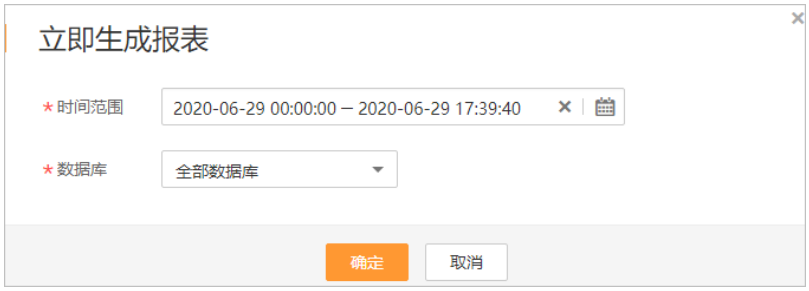
步骤 5 在“选择实例”下拉列表框中，选择需要生成审计报表的实例。

步骤 6 选择“报表管理”页签。

步骤 7 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”，如#dbss_01_0248/fig1155923804811 所示。

步骤 8 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，如图 3-37 所示。

图3-37 “立即生成报表”对话框



步骤 9 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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 报表”，进入数据库安全审计“报表”界面。

步骤 5 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 6 选择“报表管理”页签。

步骤 7 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 3-38 所示。

图3-38 设置任务

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

步骤 8 在弹出的对话框中，设置计划任务参数，如图 3-39 所示，相关参数说明如表 3-12 所示。

图3-39 “计划任务”对话框

表3-12 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	
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，当数据库生成报表时，数据库安全审计将发送通知邮件。 • ：开启 • ：关闭	
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

参数名称	说明	取值样例
	• 周期执行	
执行时间	选择报表执行的时间点。	10 点
格式	当前支持 PDF 格式。	PDF
数据库	选择执行报表任务的数据库。	-

步骤 9 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 单击右上角的，选择区域。

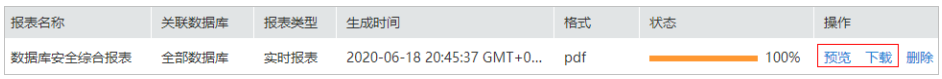
步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 报表”，进入数据库安全审计“报表”界面。

步骤 5 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 6 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 3-40 所示，在线预览报表结果，或下载并查看报表。

图3-40 预览或下载报表



----结束

3.1.8 配置审计规则

3.1.8.1 添加审计范围

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

须知

全审计规则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

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 审计规则”，进入审计规则界面。

步骤 5 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 6 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 7 在弹出的对话框中，设置审计范围，如图 3-41 所示，相关参数说明如表 3-13 所示。

图3-41 “添加审计范围”对话框

表3-13 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
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。	-
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 8 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。

3.1.8.2 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

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 审计规则”，进入审计规则界面。

步骤 5 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 6 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 7 在 SQL 注入检测规则所在行的“操作”列，单击“禁用”，如图 3-42 所示。

图3-42 禁用 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	布尔型SQL注入	正则表达式	高	已启用	禁用
2	UNION联合查询SQL注入	正则表达式	中	已启用	禁用

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”，如图 3-43 所示，启用该规则。

图3-43 启用 SQL 注入检测规则

启用 SQL 注入检测成功，该 SQL 注入检测规则的状态为“已启用”。

3.1.8.3 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

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 审计规则”，进入审计规则界面。

步骤 5 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 6 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 7 选择“风险操作”页签。

步骤 8 在风险操作列表左上方，单击“添加风险操作”。

步骤 9 在“添加风险操作”界面，设置基本信息和客户端 IP 地址，如图 3-44 所示，相关参数说明如表 3-14 所示。

图3-44 设置基本信息和客户端 IP 地址

表3-14 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 10　设置操作类型、操作对象、执行结果，如图 3-45 所示，相关参数说明如表 3-15 所示。

图3-45 设置操作类型、操作对象和执行结果

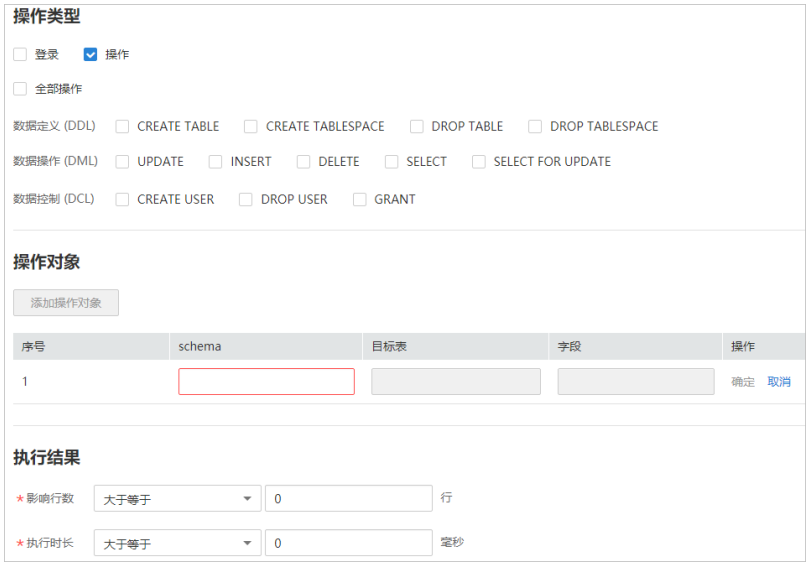


表3-15 参数说明

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 11　单击“保存”。

----结束

3.1.8.4 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

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 审计规则”，进入审计规则界面。

步骤 5 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 6 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 7 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 8 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 3-46 所示，相关参数说明如表 3-16 所示。

图3-46 “添加自定义规则”对话框

表3-16 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 9 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 3-47 所示。

图3-47 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。

3.1.9 设置邮件和告警通知

3.1.9.1 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

已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 设置”，进入设置界面。

步骤 5 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 6 设置邮件通知，如图 3-48 所示，相关参数说明如表 3-17 所示。

图3-48 设置邮件通知

表3-17 邮件通知参数说明

参数名称	说明	取值样例

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。	
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 7 单击“应用”。

----结束

相关操作

有关开启报表邮件通知的详细操作，请参见 dbss_01_0248.xml#dbss_01_0248/section93781444126。

3.1.9.2 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，您可以收到告警的通知邮件。您可以开启或关闭告警通知、设置告警的风险等级以及系统资源的告警信息。

前提条件

已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 设置”，进入设置界面。

步骤 5 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 6 选择“告警通知”页签。

步骤 7 设置告警通知，如图 3-49 所示，相关参数说明如表 3-18 所示。

图3-49 设置告警通知

表3-18 告警通知参数说明

参数名称	说明	取值样例
告警通知	开启或关闭告警通知。数据库安全审计默认开启告警通知，当数据库发生设置的告警事件时，数据库安全审计将发送告警通知邮件。 •  ：开启 •  ：关闭	 -
告警方式	当前支持邮件通知的告警方式。	邮件通知
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
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

参数名称	说明	取值样例
	• 高 • 中 • 低	
CPU 告警阈值(%)	设置审计实例系统资源 CPU 告警的阈值。当超过该阈值时，产生告警通知。	80
内存告警阈值(%)	设置审计实例系统资源内存告警的阈值。当超过该阈值时，产生告警通知。	80
磁盘告警阈值(%)	设置审计实例系统资源磁盘告警的阈值。当超过该阈值时，产生告警通知。	80

步骤 8 单击“应用”，完成设置。

----结束

3.1.10 查看监控信息

3.1.10.1 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

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 5 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 6 查看系统监控信息，如#dbss_01_0208/fig75451433958 所示。查看系统监控信息。

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。

----结束

3.1.10.2 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

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 5 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 6 查看告警信息，相关参数说明如表 3-19 所示。

表3-19 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“时间”（“全部”、“近 30 分钟”、“近 1 小时”、“近 24 小时”、“近 7 天”或“近 30 天”），或单击，选择开始时间和结束时间，单击“确认”，列表显示该时间段的告警信息。
- 选择“风险等级”（“全部”、“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。

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。

3.1.11 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

- 已成功购买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。

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。

自动备份数据库审计日志

步骤 1 登录管理控制台。

步骤 2 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 设置”，进入“设置”界面。

步骤 5 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 6 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 3-50 所示，相关参数说明如表 3-20 所示。

图3-50 “设置自动备份”对话框

表3-20 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
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 7 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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 设置”，进入设置界面。

步骤 5 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 6 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”。

步骤 7 在弹出的提示框中，单击“确定”。

----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。

步骤 1 登录管理控制台。

步骤 2 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 设置”，进入设置界面。

步骤 5 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 6 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。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”。
- 导出目录：在 OBS 桶中创建风险导出文件的目录。

----结束

3.1.12 其他操作

3.1.12.1 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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 5 查看数据库安全审计实例信息，如图 3-51 所示，相关参数说明如表 3-21 所示。

图3-51 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3-21 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

参数名称	说明
	• 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

3.1.12.2 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

已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 5 单击需要查看信息的实例名称，进入实例概览页面。

步骤 6 查看实例的“基本信息”、“网络配置信息”和“关联数据库”，如图 3-52 所示，相关参数说明如表 3-22 所示。

图3-52 查看实例概览信息

表3-22 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

类别	参数名称	说明
		• 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	当前实例的版本。
	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。
	计费模式	实例的计费模式。
	创建时间	实例创建的时间。
	剩余天数	实例可以使用的剩余天数。
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。
	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

3.1.12.3 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

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 5 查看数据库信息，如图 3-53 所示，相关参数说明如表 3-23 所示。

图3-53 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3-23 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。	-

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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 5 在“选择实例”下拉列表框中，选择查看的 Agent 所属的实例。

步骤 6 单击数据库左侧的展开 Agent 的详细信息，如图 3-54 所示，相关参数如表 3-24。

图3-54 查看数据库和 Agent 信息

表3-24 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**

参数名称	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

3.1.12.4 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

3.1.12.5 管理审计范围

添加审计范围后，您可以查看审计范围信息，启用、编辑、禁用或删除审计范围。

前提条件

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 审计规则”，进入审计规则界面。

步骤 5 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 6 查看审计范围信息，如图 3-55 所示，相关参数说明如表 3-25 所示。

图3-55 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3-25 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

3.1.12.6 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

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 审计规则”，进入审计规则界面。

步骤 5 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 6 查看 SQL 注入检测信息，如图 3-56 所示，相关参数如表 3-26 所示。

图3-56 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	布尔型SQL注入	正则表达式	高	已禁用	启用
2	UNION联合查询SQL注入	正则表达式	中	已启用	禁用
3	时间型SQL注入	正则表达式	中	已启用	禁用
4	MYSQL报错型SQL注入	正则表达式	高	已启用	禁用
5	HAVING报错SQL注入	正则表达式	中	已启用	禁用
6	恒等式SQL注入	正则表达式	高	已启用	禁用

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3-26 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

3.1.12.7 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，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

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 审计规则”，进入审计规则界面。

步骤 5 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 6 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3-57 设置风险操作的优先级

步骤 7 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”。

步骤 8 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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 审计规则”，进入审计规则界面。

步骤 5 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 6 选择“风险操作”页签。

步骤 7 查看风险操作信息，相关参数说明如表 3-27 所示。

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3-27 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

参数名称	说明
	• 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

3.1.12.8 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

已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 审计规则”，进入审计规则界面。

步骤 5 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 6 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 7 查看规则信息，如图 3-58 所示，相关参数说明如表 3-28 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3-58 查看脱敏规则信息

表3-28 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

3.1.12.9 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

- 已成功购买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 单击右上角的，选择区域。

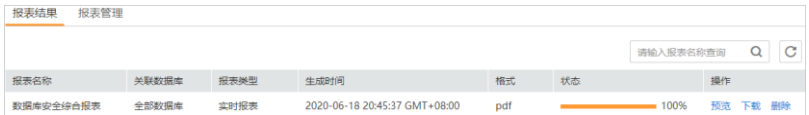
步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 报表”，进入报表界面。

步骤 5 在“选择实例”下拉列表框中，选择查看报表信息的实例。

步骤 6 查看报表信息，如图 3-59 所示。

图3-59 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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 报表”，进入报表界面。

步骤 5 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 6 选择“报表管理”页签。

步骤 7 查看报表模板信息，如图 3-60 所示。

图3-60 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
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

3.1.12.10 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

- 已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 设置”，进入设置界面。

步骤 5 在“选择实例”下拉列表框中，选择需要查看日志的实例。

步骤 6 选择“备份与恢复”页签。

步骤 7 查看备份的审计日志信息，相关参数说明如表 3-29 所示。查看报表模板信息，相关参数说明如表 3-29 所示。

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3-29 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

3.1.12.11 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

已成功购买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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 5 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 6 选择“操作日志”页签，进入操作日志列表页面。

步骤 7 查看操作日志，相关参数说明如表 3-30 所示。查看操作日志，相关参数说明如表 3-30 所示。

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3-30 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

3.2 云审计服务支持的关键操作

3.2.1 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”，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 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。

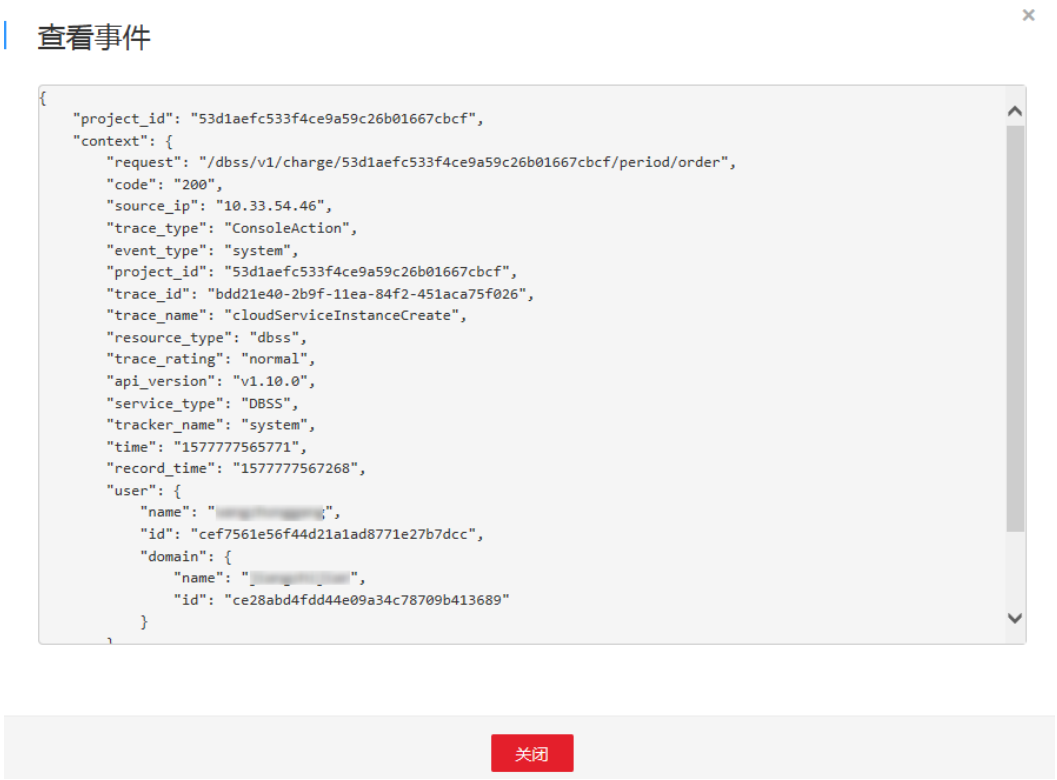
步骤 5 单击“查询”，查看对应的操作事件。

步骤 6 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 3-61 所示。

图3-61 展开记录

步骤 7 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，如图 3-62 所示，显示了该操作事件结构的详细信息。

图3-62 查看事件



----结束

3.2.2 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 3-31 所示。

表3-31 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

3.3 监控

3.3.1 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3-32 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
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

3.3.2 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

已购买DBSS实例。

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，选择告警规则“归属企业项目”。

步骤 6 在“资源类型”下拉列表框中选择“数据库安全服务”，选择“维度”、“监控范围”，设置告警模板、是否发送通知，如图 3-63 所示。

图3-63 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

3.3.3 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 3.3.2 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 > 数据库安全服务”，进入“云服务监控”页面。

步骤 4 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。

----结束

4 常见问题

4.1 数据库安全审计功能类

4.1.1 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。

4.1.2 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 4-1 所示。

表4-1 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） • 8.0.23
Oracle (因 Oracle 为闭源协议，适配版本复杂，如您需审计 Oracle 数据库，请先联系客服人员)	• 11g 11.1.0.6.0 、11.2.0.1.0 、11.2.0.2.0、11.2.0.3.0、11.2.0.4.0 • 12c 12.1.0.2.0 、12.2.0.1.0 • 19c
PostgreSQL	• 7.4 • 8.0

数据库类型	版本
	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
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
Greenplum	V6.0
HighGo	V6.0
TAURUS	MySQL 8.0
DAMENG	DM8
KINGBASE	V8
MongoDB	V5.0

4.1.3 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 4-2 所示。

表4-2 Agent 支持的 Linux 系统版本说明

系统名称	系统版本
CentOS	• CentOS 6.3 (64bit) • CentOS 6.5 (64bit) • CentOS 6.8 (64bit) • CentOS 6.9 (64bit) • 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)
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)
OpenSUSE	• SUSE 13 (64bit) • SUSE 15 (64bit) • SUSE 42 (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) • Euler 2.5 (64bit)
OpenEuler	• OpenEuler 20.03 (64bit)
Oracle Linux	• Oracle Linux 6.9 (64bit) • Oracle Linux 7.4 (64bit)
RedHat	• Red Hat Enterprise Linux 7.4 (64bit) • Red Hat Enterprise Linux 7.6 (64bit)
NeoKylin	• NeoKylin 7.0 (64bit)

系统名称	系统版本
Kylin	• Kylin Linux Advanced Server release V10 (64bit)
Uniontech OS	• Uniontech OS Server 20 Enterprise (64bit)

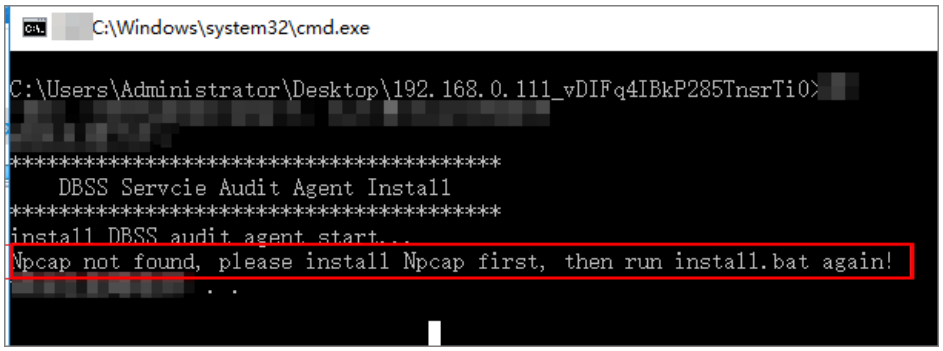
- 数据库安全审计的 Agent 支持的 Windows 系统版本如下所示：
  - Windows Server 2008 R2(64bit)
  - Windows Server 2012 R2(64bit)
  - Windows Server 2016(64bit)
  - Windows 7(64bit)
  - Windows 10(64bit)

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4-1 Npcap not found



4.1.4 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。

4.1.5 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。

4.1.6 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。

表4-3 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：500GB	• 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
高级版	最多支持 30 个数据库实例	• CPU：16U • 内存：64GB • 硬盘：2T	• 吞吐量峰值：30,000 条/秒 • 入库速率：1080 万条/小时 • 15 亿条在线 SQL 语句存储 • 600 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。

4.1.7 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。

4.1.8 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。

4.1.9 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。

4.2 数据库安全审计 Agent 相关

4.2.1 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

4.2.2 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：

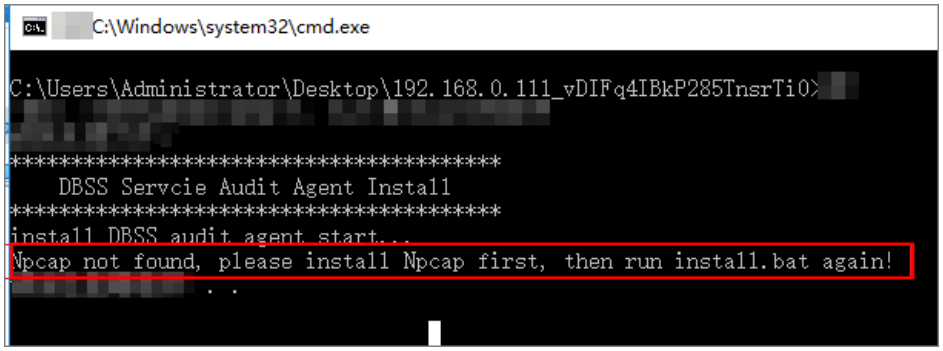
- Windows Server 2008 R2(64bit)
- Windows Server 2012 R2(64bit)
- Windows Server 2016(64bit)
- Windows 7(64bit)
- Windows 10(64bit)

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4-2 Npcap not found



4.2.3 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 4-4 所示。

表4-4 Agent 支持的 Linux 系统版本说明

系统名称	系统版本
CentOS	• CentOS 6.3 (64bit) • CentOS 6.5 (64bit) • CentOS 6.8 (64bit) • CentOS 6.9 (64bit) • 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)
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)
OpenSUSE	• SUSE 13 (64bit) • SUSE 15 (64bit) • SUSE 42 (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) • Euler 2.5 (64bit)
OpenEuler	• OpenEuler 20.03 (64bit)
Oracle Linux	• Oracle Linux 6.9 (64bit) • Oracle Linux 7.4 (64bit)
RedHat	• Red Hat Enterprise Linux 7.4 (64bit) • Red Hat Enterprise Linux 7.6 (64bit)
NeoKylin	• NeoKylin 7.0 (64bit)
Kylin	• Kylin Linux Advanced Server release V10 (64bit)
Uniontech OS	• Uniontech OS Server 20 Enterprise (64bit)

4.2.4 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”。

4.2.5（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

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

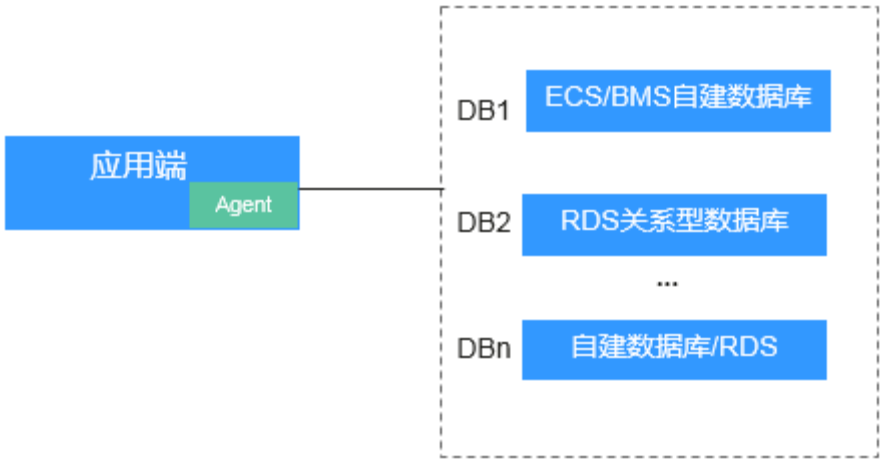
Agent 客户端日志存放路径为：“/opt/dbss_audit_agent/log/audit_agent.log”

4.2.7 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 4-3 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 4-4 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4-3 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4-4 选择已有 Agent

4.2.8 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 4-5 所示。

图4-5 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 4-6 所示。

图4-6 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 4.2.10 如何处理 Agent 与数据库安全审计实例之间通信异常？章节进行处理。

4.2.9 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 4-5 所示。

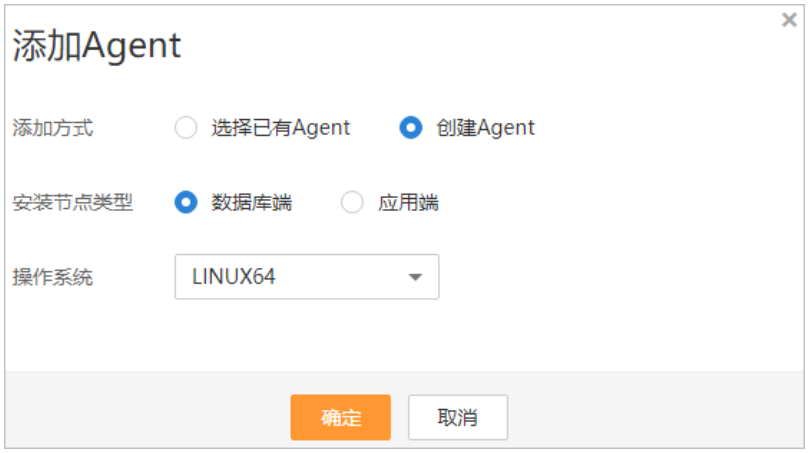
表4-5 数据库安全审计 Agent 安装说明

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”，如图 4-7 所示。
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 4-8 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 4-9 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4-7 在数据库端添加 Agent



- 应用端

图4-8 在应用端添加 Agent

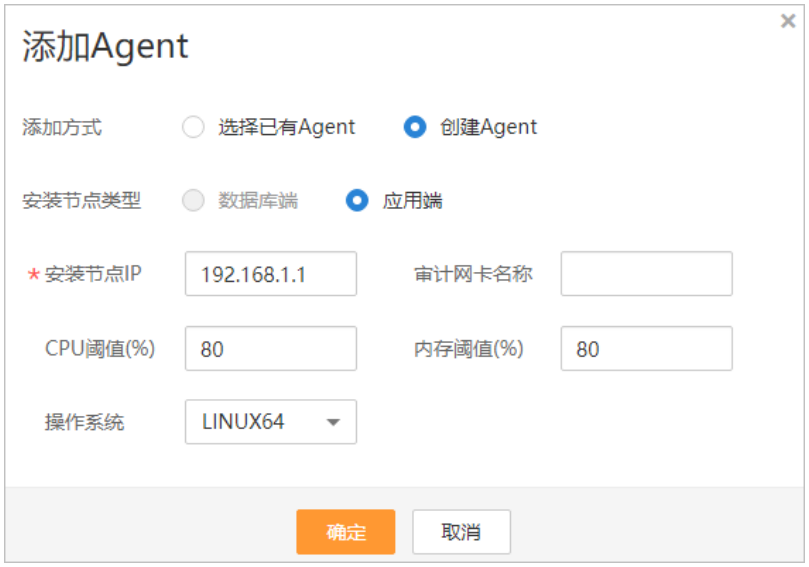


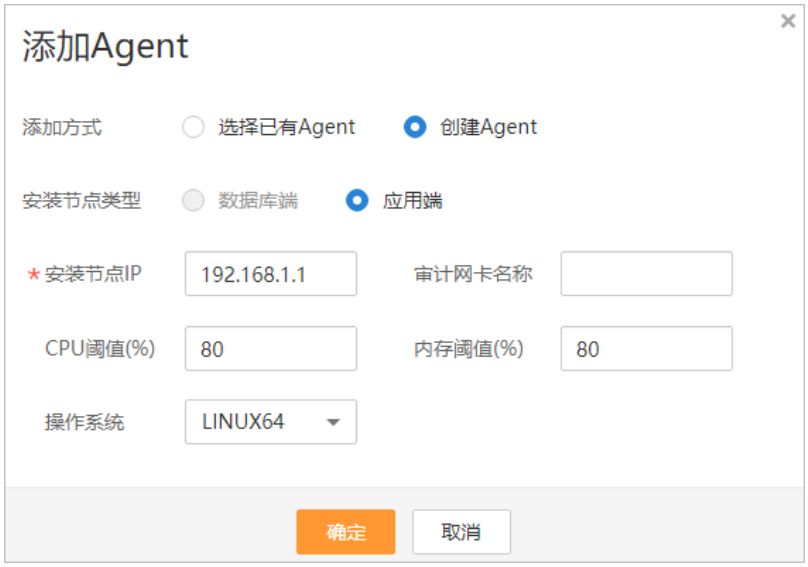
图4-9 选择已有 Agent

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

- 代理端

图4-10 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。

4.2.10 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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 5 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 6 检查待审计的数据库信息，如图 4-11 所示。

图4-11 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 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 检查待审计的数据库的审计状态，如图 4-12 所示。

图4-12 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 4-13 所示。

图4-13 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）。

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 4-14 所示。

图4-14 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 4-15 所示。

图4-15 “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。

4.3 数据库安全审计操作类

4.3.1 如何关闭数据库 SSL？

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。

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

4.3.2 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 4-16 所示。

图4-16 风险操作应用到连接到实例的所有数据库

4.3.3 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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 5 单击需要查看信息的实例名称，进入实例概览页面。

步骤 6 查看实例版本信息，如图 4-17 所示。

图4-17 查看实例版本信息

----结束

4.3.4 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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 5 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 6 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“时间”（“全部”、“近 30 分钟”、“近 1 小时”、“近 24 小时”、“近 7 天”或“近 30 天”），或单击，选择开始时间和结束时间，单击“确认”，列表显示该时间段的告警信息。
- 选择“风险等级”（“全部”、“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

4.4 数据库安全审计故障排查类

4.4.1 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

4.5 日志类

4.5.1 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 4.5.2 数据库安全审计的操作日志默认保存多久？。

4.5.2 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。

4.5.3 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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 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 5 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 6 选择“操作日志”页签，进入操作日志列表页面。

步骤 7 查看操作日志，相关参数说明如表 4-6 所示。查看操作日志，相关参数说明如表 4-6 所示。

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4-6 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

4.5.4 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。

4.5.5 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 单击右上角的，选择区域。

步骤 3 选择“安全 > 数据库安全服务”，进入数据库安全防护实例列表界面。

步骤 4 在左侧导航树中，选择“数据库安全审计 > 设置”，进入“设置”界面。

步骤 5 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 6 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 4-18 所示，相关参数说明如表 4-7 所示。

图4-18 “设置自动备份”对话框

表4-7 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
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 7　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

A 修订记录

发布日期	修改说明
2023-05-23	第二次正式发布。 新增支持的数据库类型，详情查看 1.1 产品定义章节。
2021-09-10	第一次正式发布。