数据库安全服务(DBSS)

用户指南

文档版本 35

发布日期 2024-05-13

华为技术有限公司

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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

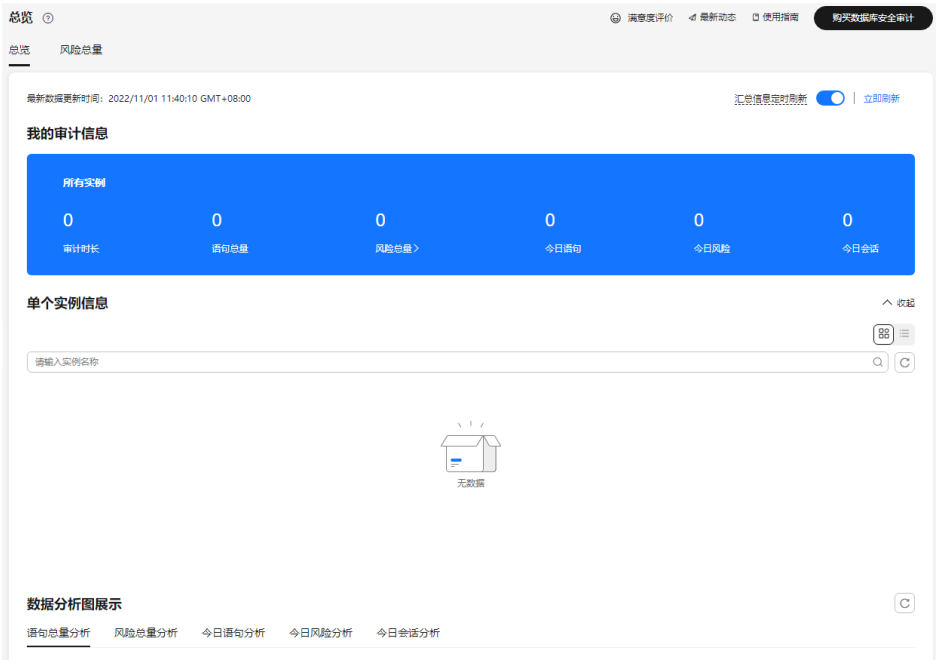
1 总览

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

步骤1 登录管理控制台。

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

图 1-1 进入总览



步骤3 单击右上角“汇总信息定时刷新”开关，可开启审计信息定时刷新。

说明

开启后，系统按照预设规则每间隔1小时对全量审计信息进行刷新。

----结束

我的审计信息

展示对所有实例扫描检测的统计展示。

表 1-1 参数说明

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

单个实例信息

按照单个实例的维度统计展示实例审计情况，默认展示10条，超过数量分页显示。

数据分析图展示

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

单击右上角可切换统计图展示样式。

TOP5 语句总量

展示历史审计中使用语句最多排列前5的实例。

图 1-2 TOP5 语句总量

风险级别总体分析

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

说明

支持自定义时间段查看总体风险，点击右上角的 图标选择时间区间。

风险规则总体分析

统计所有风险规则命中的次数，并且在右侧从高至低排列风险规则命中次数最高的五个规则。

其他风险角度分析

可以从以下三个方向查看分析报告：

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

2 开通并使用数据库安全审计（安装 Agent）

2.1 流程指引

本节内容指引您快速启用数据库安全审计服务DBSS。

背景信息

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

须知

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

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

免 Agent 方式审计数据库

部分数据库类型及版本支持免安装Agent方式，如**表2-1**所示。

表 2-1 支持免 Agent 安装的关系型数据库

数据库类型	支持的版本
GaussDB for MySQL	默认都支持
RDS for SQLServer	默认都支持

数据库类型	支持的版本
RDS for MySQL	● 5.6（5.6.51.1及以上版本） ● 5.7（5.7.29.2及以上版本） ● 8.0（8.0.20.3及以上版本）
GaussDB(DWS)	● 8.2.0.100及以上版本
PostgreSQL	● 14（14.4及以上版本） ● 13（13.6及以上版本） ● 12（12.10及上版本） ● 11（11.15及以上版本） ● 9.6（9.6.24及以上版本） ● 9.5（9.5.25及以上版本）
RDS for MariaDB	默认都支持

说明

- 免安装Agent模式配置简单、易操作，但较之安装了Agent的DBSS实例，支持的功能上存在如下差异：
  - 统计会话数量时，无法统计成功登录、与失败登录的会话个数。
  - 无法获取数据库访问时客户端的端口号。
- 由于GaussDB(DWS)服务具有日志审计开关的权限控制策略，只有华为云账号或拥有Security Administrator权限的用户才能开启或者关闭DWS数据库审计开关。

图 2-1 免 Agent 安装流程

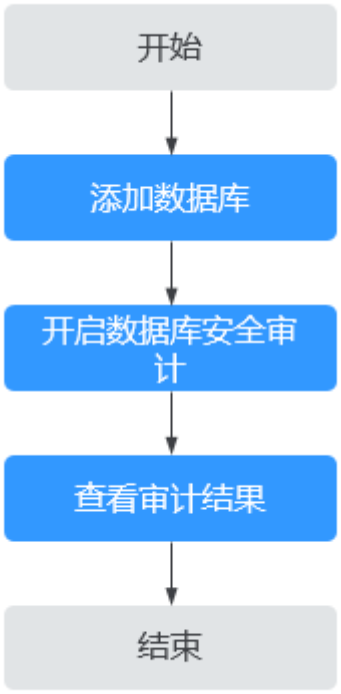


表 2-2 快速使用数据库安全审计操作步骤

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

通过 Agent 方式审计数据库

非**表2-1**中的数据库类型及版本，需采用安装Agent方式开启DBSS服务。

图 2-2 快速使用数据库安全审计流程图

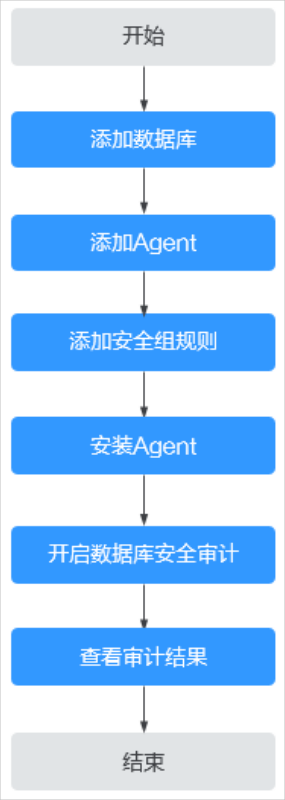


表 2-3 快速使用数据库安全审计操作步骤

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

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

相关操作

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

效果验证

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

2.2 购买数据库安全审计

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。

  数据库安全审计的Agent安装节点，请参见：**如何选择数据库安全审计的Agent安装节点？**。

系统影响

数据库安全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。

须知

请确认购买实例的账号具有“DBSS System Administrator”、“VPC Administrator”、“ECS Administrator”和“BSS 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：对账号中心、费用中心、资源中心中的所有菜单项执行任意操作。项目级角色，在同项目中勾选。
- ECS Administrator：对弹性云服务器的所有执行权限。项目级角色，在同项目中勾选。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在界面右上角，单击“购买数据库安全审计”。

步骤4 选择“区域”、“项目”、“可用区”和“性能规格”，如图2-3所示。

图 2-3 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2-4所示。

表 2-4 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
专业版	最多支持6个数据库实例	• CPU：8U • 内存：32GB • 硬盘：1,084GB	• 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

版本	支持的数据库实例	系统资源要求	性能参数
高级版	最多支持30个数据库实例	• CPU：16U • 内存：64GB • 硬盘：2,108GB	• 吞吐量峰值：30,000条/秒 • 入库速率：1,080万条/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。
- 云原生版仅支持在RDS控制台购买。
- 本表中的系统资源要求，是指购买数据库安全审计实例时会消耗的系统资源。购买时，用户的系统需要满足审计版本对应的配置。
- 本表中在线SQL语句的条数，是按照每条SQL语句的容量为1KB来计算的。

步骤5 设置数据库安全审计参数，如图2-4所示，相关参数说明如表2-5所示。

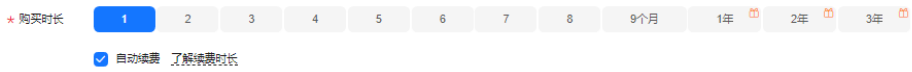
图 2-4 设置数据库安全审计参数

表 2-5 数据库安全审计实例参数说明

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

步骤6 选择“购买时长”，如**图2-5**所示。

图 2-5 选择实例购买时长



勾选“自动续费”后，当购买的数据库安全审计实例到期时，如果账号余额充足，DBSS将自动为该实例续费，您可以继续使用该实例。自动续费的周期说明如**表2-6**所示。

表 2-6 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7 （可选）为数据库安全审计实例添加标签。如您的组织已经设定数据库安全服务的相关标签策略，则需按照标签策略规则为数据库安全审计实例添加标签。标签如果不符合标签策略的规则，则可能会导致数据库安全审计实例创建失败，请联系组织管理员了解标签策略详情。

步骤8 确认当前配置无误后，单击“立即购买”。

如果您对价格有疑问，可以单击“了解计费详情”，了解产品价格。

步骤9 在“详情”页面，阅读《数据库安全审计安全免责声明》后，勾选“我已阅读并同意《数据库安全审计安全免责声明》”，单击“提交”。

步骤10 在购买页面，请选择付款方式进行付款。

步骤11 成功付款后，在数据库安全审计实例列表界面，可以查看数据库安全审计实例的创建情况。

----结束

后续处理

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

2.3 步骤一：添加数据库

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

数据库安全审计支持审计的数据库类型及版本，请参见**支持的数据库类型及版本**。

前提条件

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

步骤3 在左侧导航树中，选择“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，配置数据库的信息。

表 2-7 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

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 ● SQL Service ● DWS ● GaussDB(for MYSQL) ● GaussDB ● DAMENG ● KINGBASE ● MongoDB ● Hbase ● SHENTONG ● GBase 8a ● GBase XDM Cluster ● Greenplum ● HighGo ● MariaDB ● Hive ● DDS ● GBase 8s ● TDSQL **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 – 8.0.25 – 当“数据库类别”为“RDS数据库”时，自动关联获取数据库列表，按需选择实例，Agent免安装。 ● 当“数据库类型”选择“ORACLE”时，您可以选择以下版本： – 11g – 12c – 19c ● 当“数据库类型”选择“POSTGRESQL”时，您可以选择以下版本： – 7.4 – 8.0 8.0、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 ● 当“数据库类型”选择“SQLSERVER”时，您可以选择以下版本： – 2008 – 2012 – 2014 – 2016 – 2017 ● 当“数据库类型”选择“DWS”时，您可以选择以下版本： – 1.5 – 8.1	5.0

参数名称	说明	取值样例
	• 当“数据库类型”选择“GaussDB(for MySQL)”时，您可以选择以下版本： – 当“数据库类别”为“自建数据库”时，可选择“MySQL 8.0” – 当“数据库类别”为“RDS数据库”时，自动关联获取数据库列表，按需选择实例，Agent免安装。 • 当“数据库类型”选择“GaussDB”时，您可以选择以下版本： – 1.4企业版 – 1.3企业版 – 2.8企业版 – 3.223企业版 • 当“数据库类型”选择“DAMENG”时，您可以选择以下版本： – DM8 • 当“数据库类型”选择“KINGBASE”时，您可以选择以下版本： – V8 • 当“数据库类型”选择“Hbase”时，您可以选择以下版本： – 1.3.1 – 2.2.3 • 当“数据库类型”选择“SHENTONG”时，您可以选择以下版本： – V7.0 • 当“数据库类型”选择“GBase 8a”时，您可以选择以下版本： – v8.5 • 当“数据库类型”选择“GBase 8s”时，您可以选择以下版本： – v8.8 • 当“数据库类型”选择“Greenplum”时，您可以选择以下版本： – v6.0 • 当“数据库类型”选择“HighGo”时，您可以选择以下版本： – v6.0 • 当“数据库类型”选择“MongoDB”时，您可以选择以下版本： – v5.0	

参数名称	说明	取值样例
	● 当“数据库类型”选择“MariaDB”时，您可以选择以下版本： – 10.6 ● 当“数据库类型”选择“Hive”时，您可以选择以下版本： – 1.2.2 – 2.3.9 – 3.1.2 – 3.1.3 ● 当“数据库类型”选择“TDSQL”时，您可以选择以下版本： – 10.3.17.3.0	
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

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

说明

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

----结束

2.4 步骤二：添加 Agent

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

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）
- GaussDB(DWS)：8.2.0.100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2-6和图2-7所示。

图 2-6 一个应用端连接多个 ECS/BMS 自建数据库

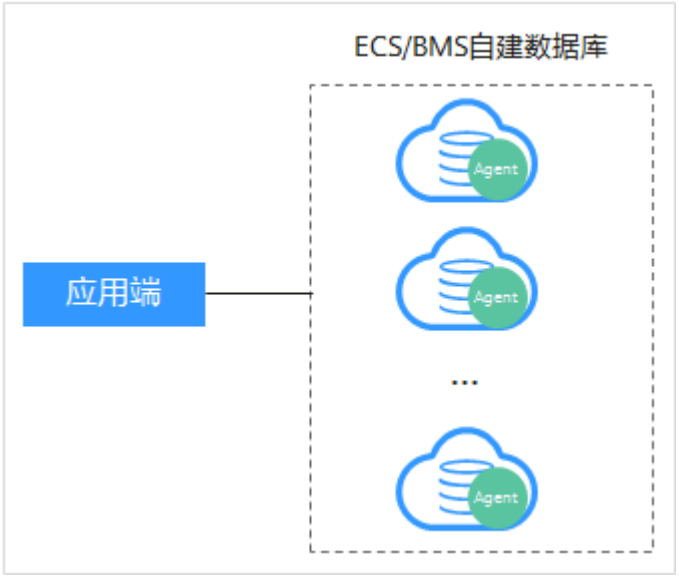
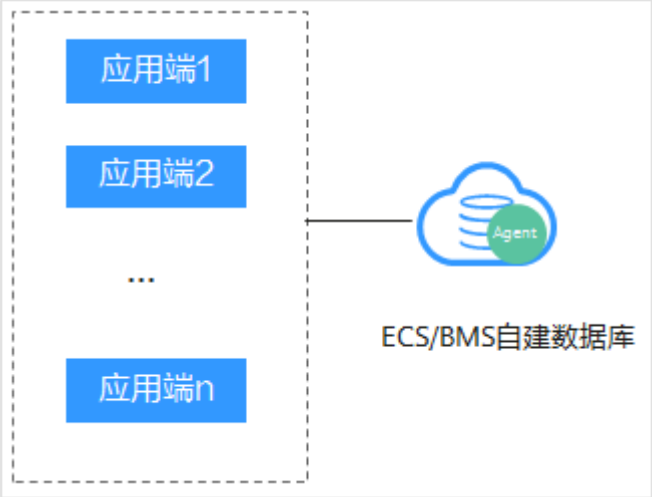


图 2-7 多个应用端连接同一个 ECS/BMS 自建数据库



- RDS关系型数据库的常见部署场景如图2-8和图2-9所示。

图 2-8 一个应用端连接多个 RDS

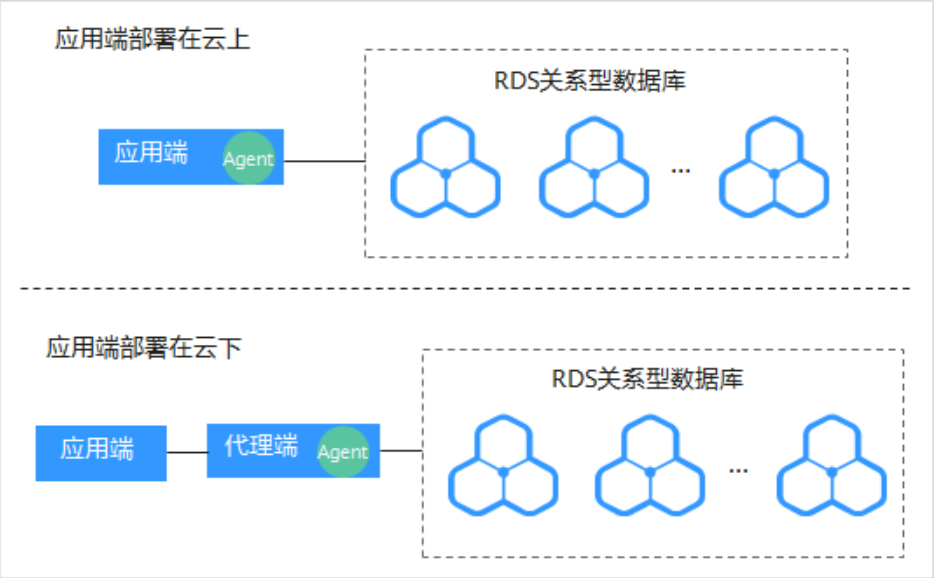
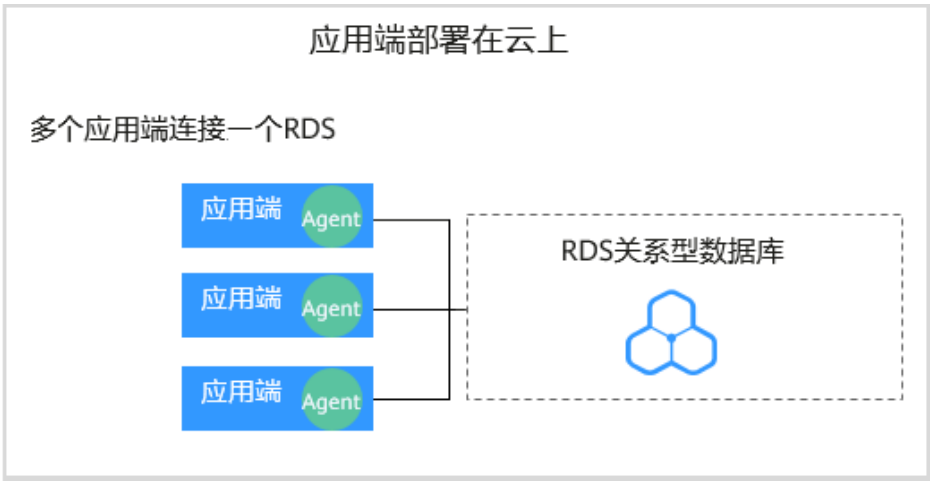


图 2-9 多个应用端连接同一个 RDS



添加Agent方式的详细说明如表2-8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需在数据库端添加。

表 2-8 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。

使用场景	Agent安装节点	审计功能说明	注意事项
	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，单击页面左上方的 ☰，选择“安全与合规 > 数据库安全服务”，进入数据库安全审计“总览”界面。

步骤3 在左侧导航树中，选择“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2-10所示，相关参数说明如表2-9所示。

图 2-10 在数据库端添加 Agent

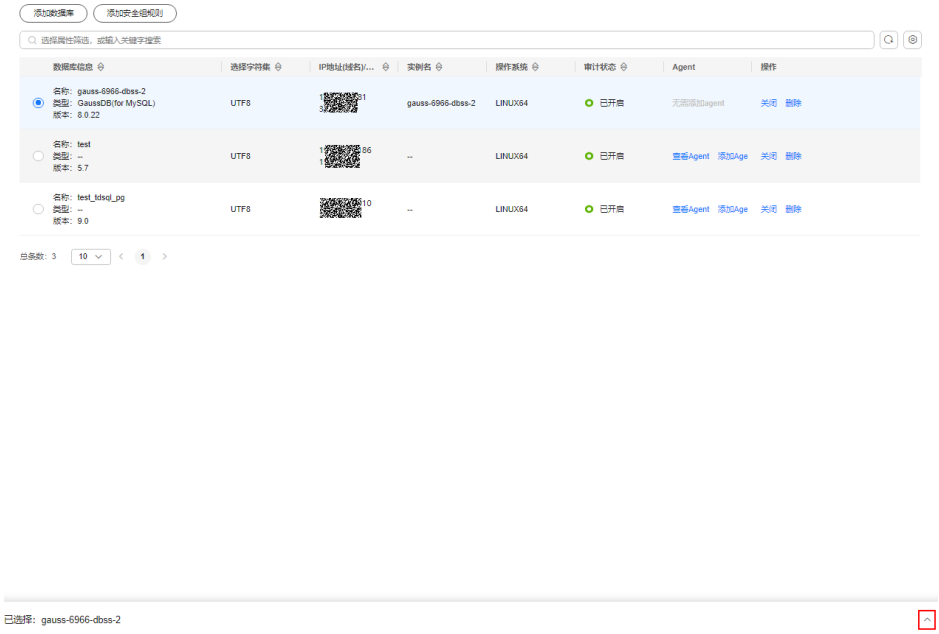
表 2-9 添加 Agent 参数说明（ECS/BMS 自建数据库）

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
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”。	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”。	80

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 2-11 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，单击页面左上方的 ☰，选择“安全与合规 > 数据库安全服务”，进入数据库安全审计“总览”界面。

步骤3 在左侧导航树中，选择“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2-12和图2-13所示，相关参数说明如表2-10所示。

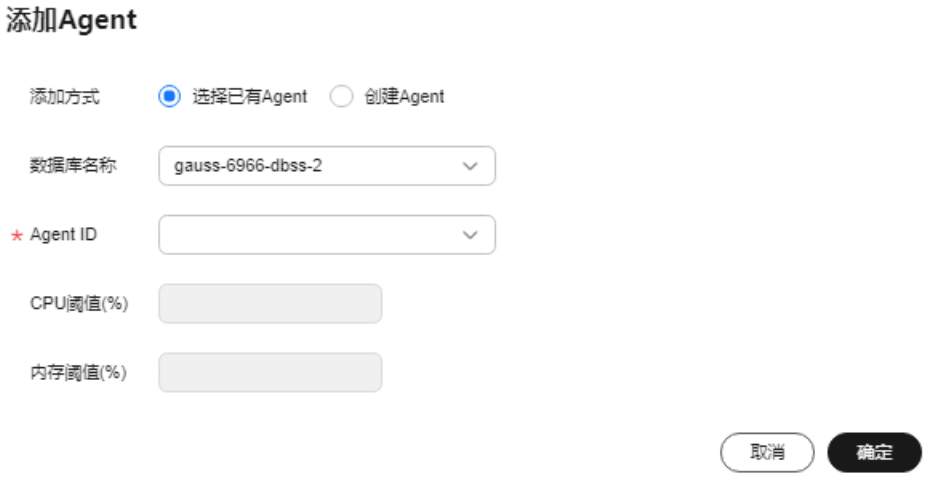
- “添加方式”选择“选择已有Agent”

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

  说明

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

  图 2-12 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 2-13 在应用端添加 Agent

表 2-10 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
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。

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

2.5 步骤三：下载并安装 Agent

2.5.1 下载 Agent

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。

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。**

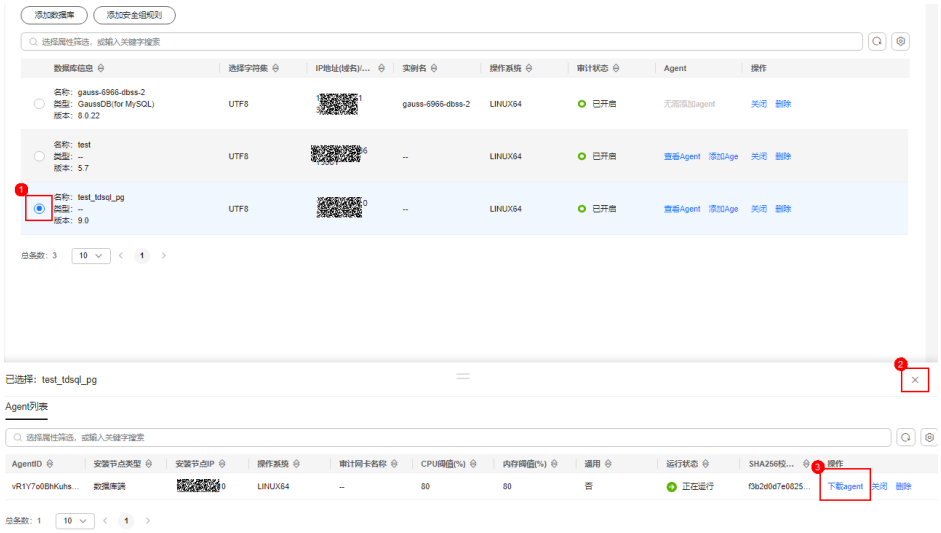
步骤2 在页面上方选择“区域”后，单击页面左上方的 ，选择“安全与合规 > 数据库安全服务”，进入数据库安全审计“总览”界面。

步骤3 在左侧导航树中，选择“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 2-14 下载 Agent



请根据安装Agent节点的操作系统类型，选择下载相应的Agent安装包。

- Linux操作系统
  在“操作系统”为“LINUX64”的数据库中下载Agent安装包
- Windows操作系统
  在“操作系统”为“WINDOWS64”的数据库中下载Agent安装包

----结束

2.5.2 安装 Agent（Linux 操作系统）

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

前提条件

- 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。有关Linux系统版本的要求，请参见**Agent可以安装在哪些Linux操作系统上?**

常见安装场景

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

- ECS/BMS自建数据库的常见部署场景如**图2-15**和**图2-16**所示。

图 2-15 一个应用端连接多个 ECS/BMS 自建数据库

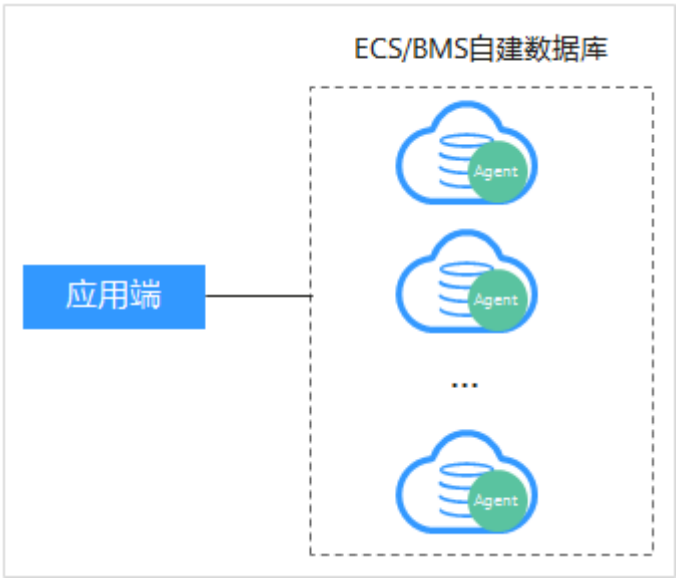
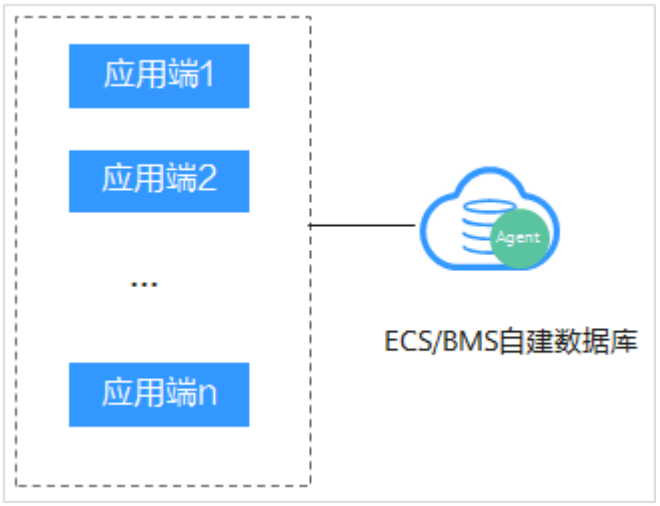


图 2-16 多个应用端连接同一个 ECS/BMS 自建数据库



- RDS关系型数据库的常见部署场景如图2-17和图2-18所示。

图 2-17 一个应用端连接多个 RDS

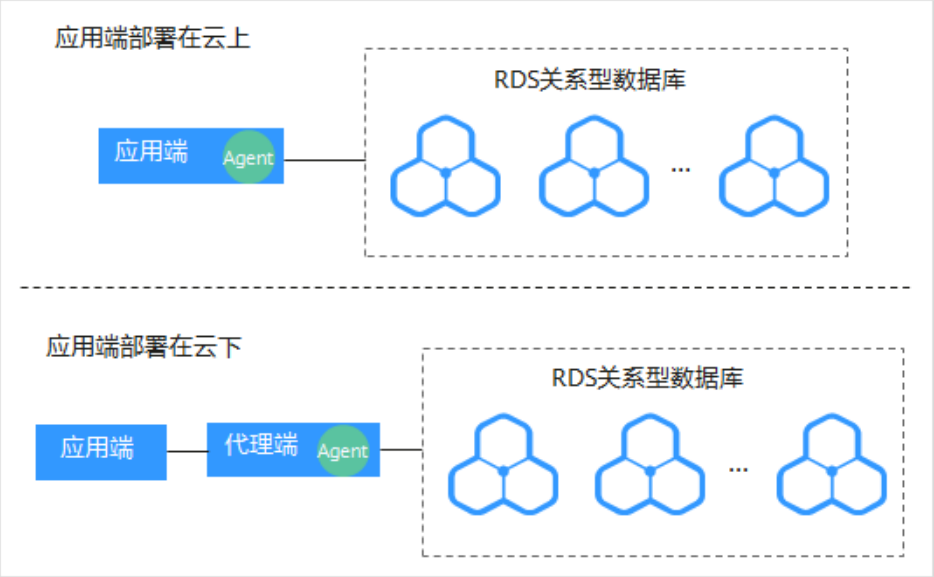
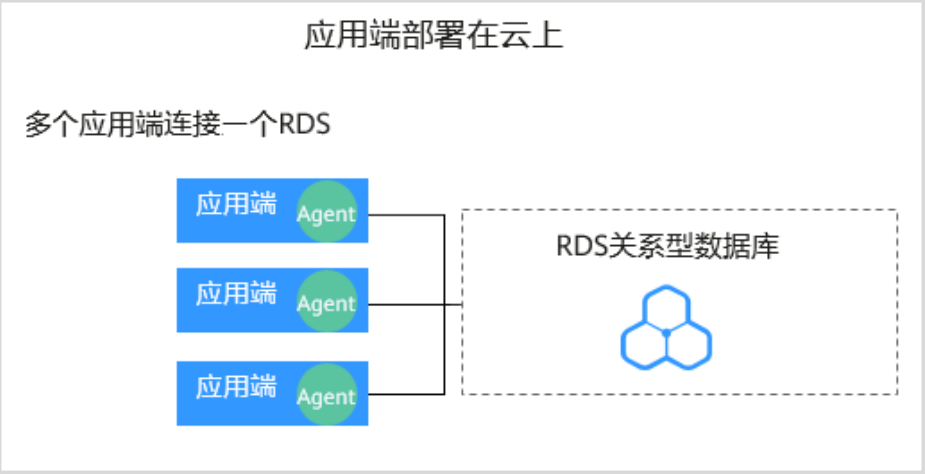


图 2-18 多个应用端连接同一个 RDS



安装Agent节点的详细说明如表2-11所示。

须知

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

表 2-11 安装 Agent 场景说明

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

安装 Agent

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 [redacted]_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 [redacted]_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!
```

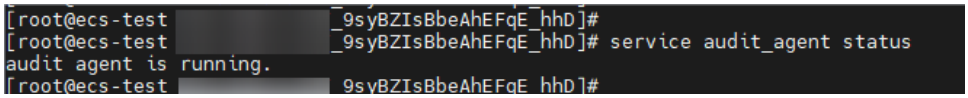
须知

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。




```
audit agent is running.
```

----结束

相关操作

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

2.5.3 安装 Agent（Windows 操作系统）

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

前提条件

- 数据库已成功添加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。有关Windows系统版本的要求，请参见**Agent可以安装在哪些Windows操作系统上?** 。

常见安装场景

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

- ECS/BMS自建数据库的常见部署场景如**图2-19**和**图2-20**所示。

图 2-19 一个应用端连接多个 ECS/BMS 自建数据库

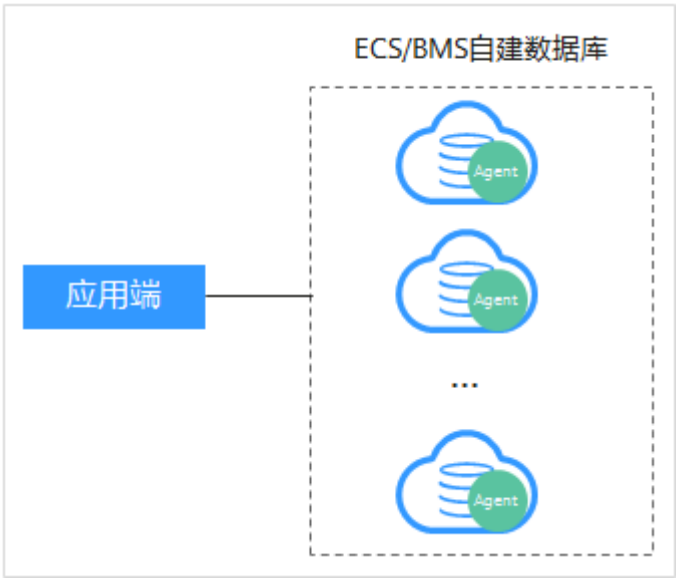
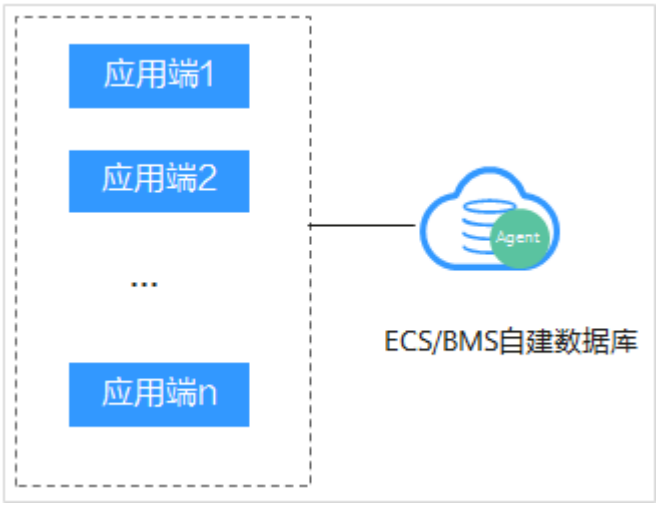


图 2-20 多个应用端连接同一个 ECS/BMS 自建数据库



- RDS关系型数据库的常见部署场景如图2-21和图2-22所示。

图 2-21 一个应用端连接多个 RDS

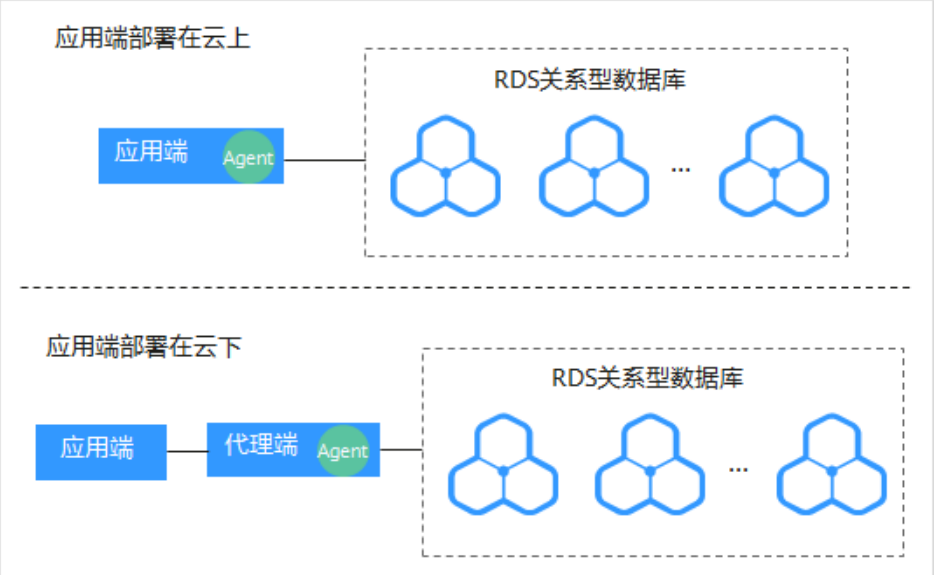
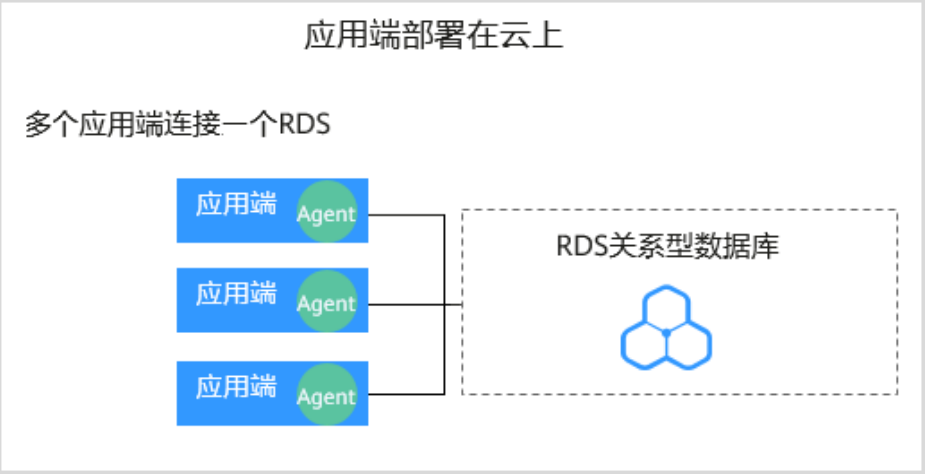


图 2-22 多个应用端连接同一个 RDS



安装Agent节点的详细说明如表2-12所示。

须知

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

表 2-12 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。

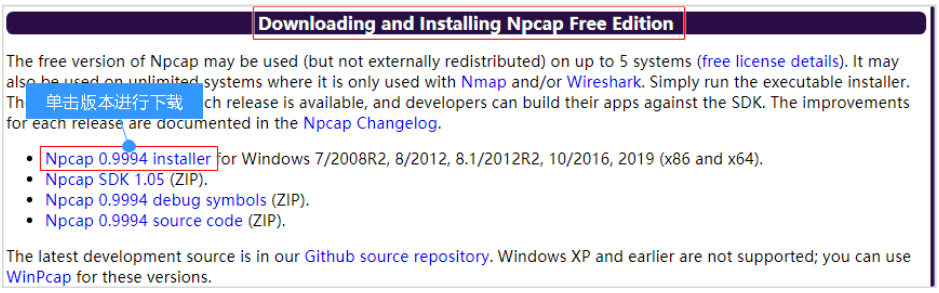
安装 Agent

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 2-23 下载 npcap

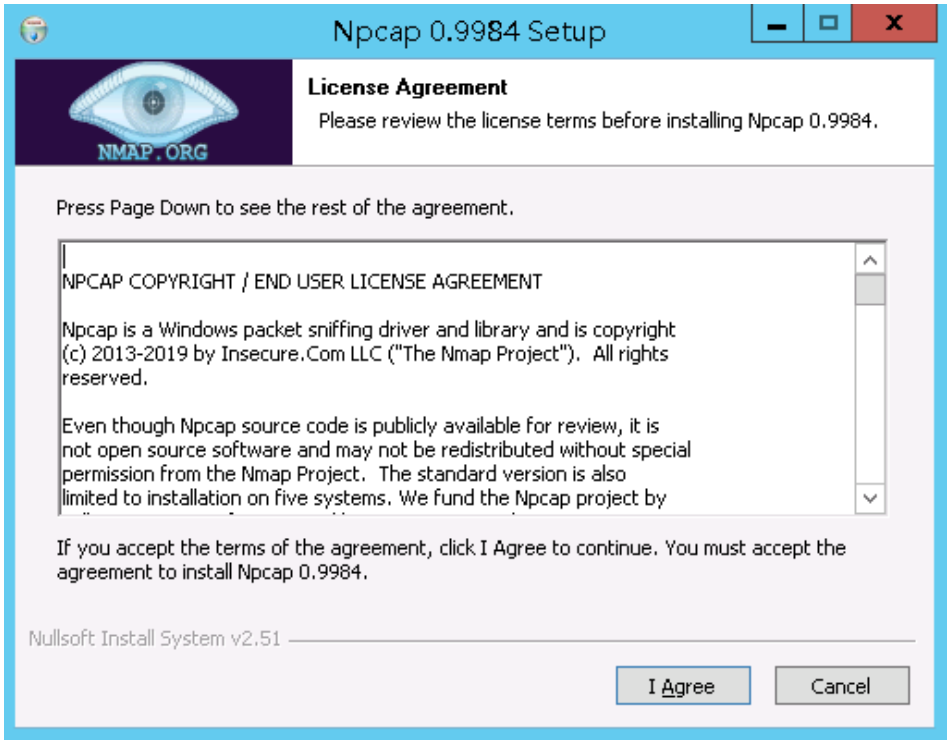
  

  b. 将下载好的npcap-*xxxx*.exe软件安装包上传至需要安装agent的虚拟机。

  c. 双击npcap软件安装包。

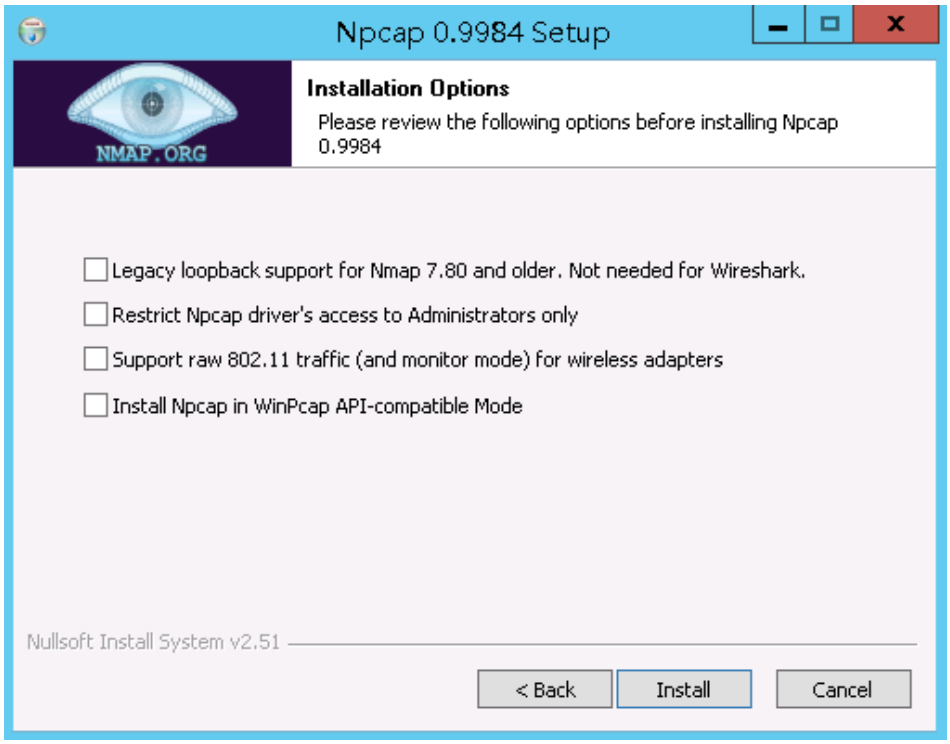
  d. 在弹出的对话框中，单击“I Agree”，如**图2-24**所示。

图 2-24 同意安装“Npcap”

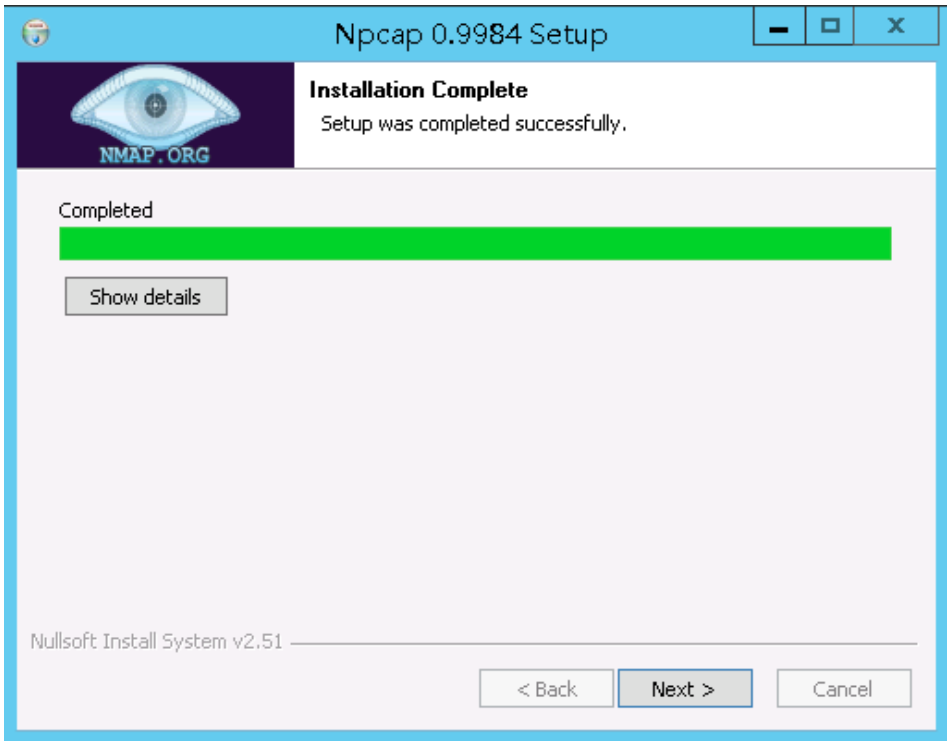


e. 在弹出的对话框中，单击“Install”，不勾选安装选项，如图2-25所示。

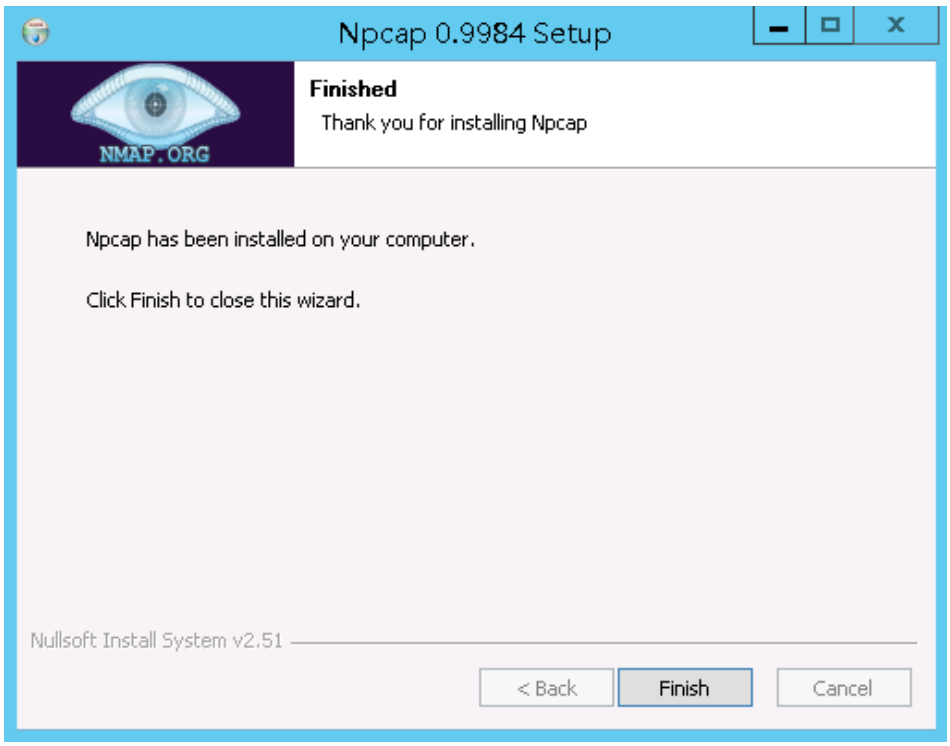
图 2-25 安装“Npcap”



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。

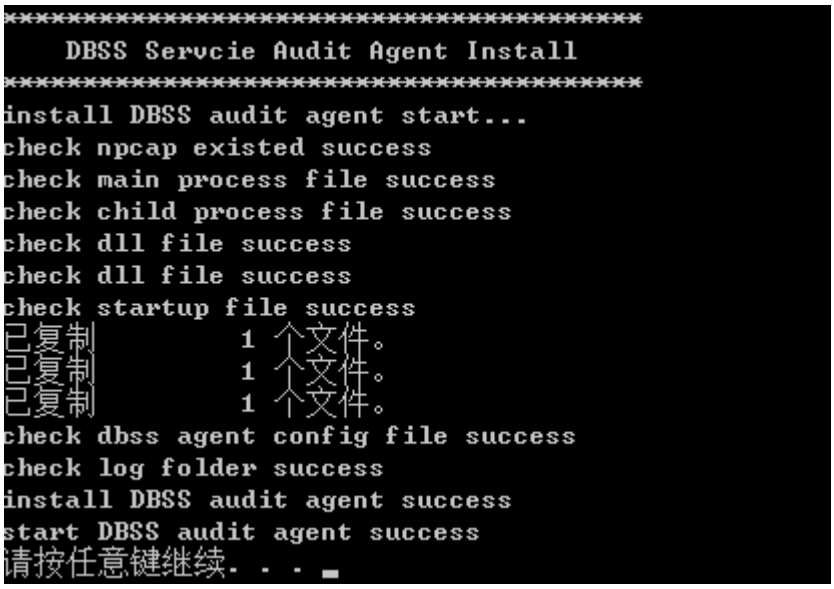
步骤3 将下载的Agent安装包“xxx.zip”复制到该主机任意一个目录下。

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2-26所示，按任意键结束安装。

图 2-26 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

2.6 步骤四：添加安全组规则

Agent添加完成后，您需要为数据库安全审计实例所在的安全组添加入方向规则TCP协议（8000端口）和UDP协议（7000-7100端口），使Agent与审计实例之间的网络连通，数据库安全审计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 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > 数据库安全服务”，进入数据库安全审计“总览”界面。

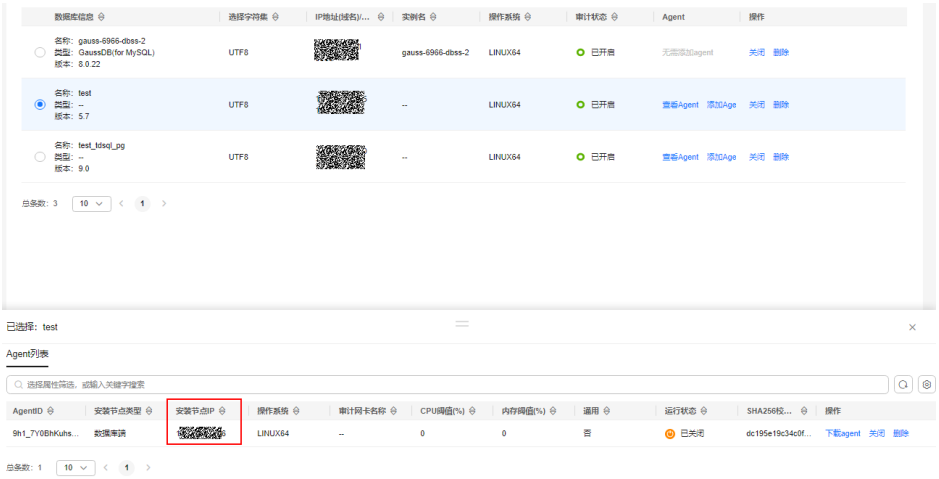
步骤3 在左侧导航树中，选择“数据库安全审计 > 数据库列表”，进入“数据库列表”界面。

步骤4 在“选择实例”下拉列表框中，选择需要添加安全组规则的数据库所属的实例。

步骤5 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2-27所示。

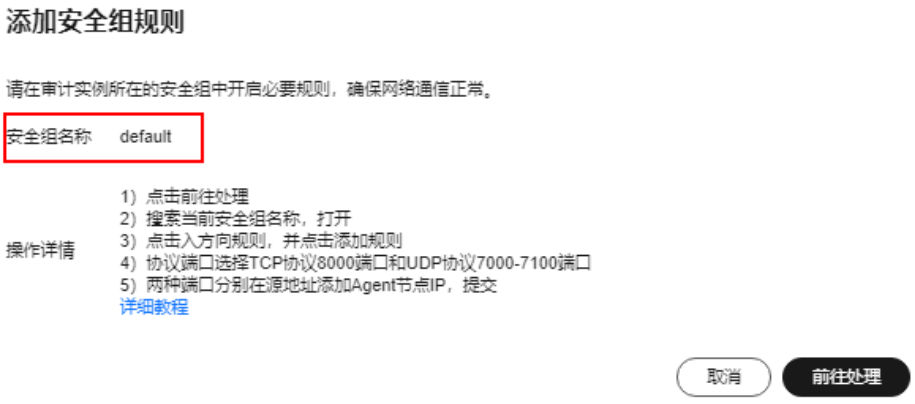
图 2-27 安装节点 IP



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），如图2-28所示。

图 2-28 添加安全组规则



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**步骤5**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”。

图 2-29 添加规则

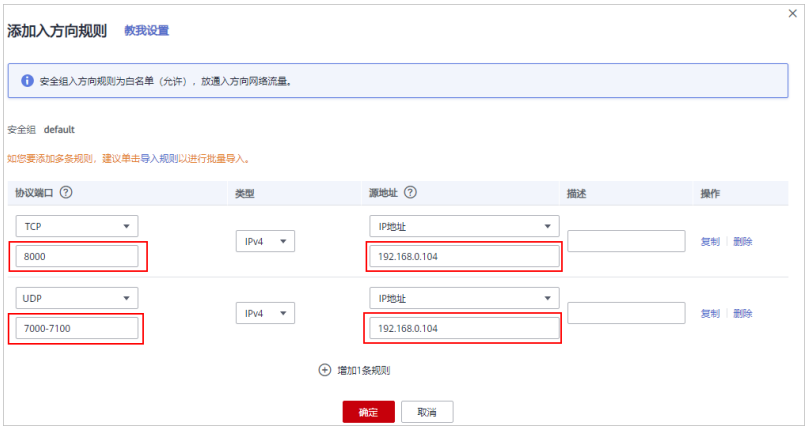
2. 在“添加入方向规则”对话框中，为**图2-27**中的安装节点IP添加TCP协议（端口为8000）和UDP协议（端口为7000-7100）规则，如**图2-30**所示。

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 2-30 “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

2.7 步骤五：开启数据库安全审计

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

前提条件

- 已成功添加并安装Agent，且Agent的运行状态为“正在运行”。
- 数据库安全审计实例已成功添加安全组规则。

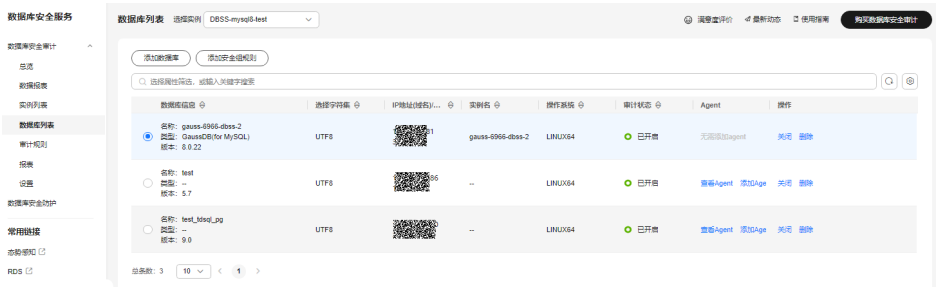
开启审计

步骤1 **登录管理控制台。**

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

步骤3 在左侧导航栏中，选择“数据库列表”，进入“数据库列表”界面。

图 2-31 进入“数据库列表”界面



步骤4 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5 在待开启审计所在行的“操作”列，单击“开启”，开启审计功能。

审计功能开启后，该数据库的“审计状态”为“已开启”，不需要重启数据库。

图 2-32 开启数据库审计功能

----结束

验证审计效果

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

步骤2 **登录管理控制台。**

步骤3 在页面上方选择“区域”后，单击页面左上方的 ，选择“安全与合规 > 数据库安全服务”，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”，SQL语句列表将显示**步骤1**中输入的SQL语句。

图 2-33 查看 SQL 语句

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

----结束

3 开通并使用数据库安全审计（免安装 Agent）

3.1 流程指引

背景信息

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

须知

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

免 Agent 方式审计数据库

部分数据库类型及版本支持免安装Agent方式，如**表3-1**所示。

表 3-1 支持免 Agent 安装的关系型数据库

数据库类型	支持的版本
GaussDB for MySQL	默认都支持
RDS for SQLServer	默认都支持

数据库类型	支持的版本
RDS for MySQL	• 5.6（5.6.51.1及以上版本） • 5.7（5.7.29.2及以上版本） • 8.0（8.0.20.3及以上版本）
GaussDB(DWS)	• 8.2.0.100及以上版本
PostgreSQL	• 14（14.4及以上版本） • 13（13.6及以上版本） • 12（12.10及上版本） • 11（11.15及以上版本） • 9.6（9.6.24及以上版本） • 9.5（9.5.25及以上版本）
RDS for MariaDB	默认都支持

说明

- 免安装Agent模式配置简单、易操作，但较之安装了Agent的DBSS实例，支持的功能上存在如下差异：
  - 统计会话数量时，无法统计成功登录、与失败登录的会话个数。
  - 无法获取数据库访问时客户端的端口号。
- 由于GaussDB(DWS)服务具有日志审计开关的权限控制策略，只有华为云账号或拥有Security Administrator权限的用户才能开启或者关闭DWS数据库审计开关。

图 3-1 免 Agent 安装流程

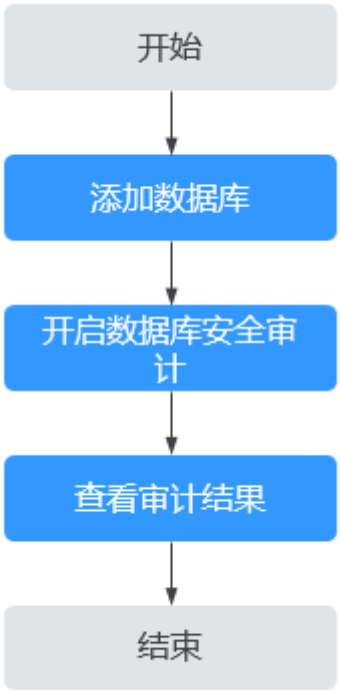


表 3-2 快速使用数据库安全审计操作步骤

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

3.2 购买数据库安全审计

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。

  数据库安全审计的Agent安装节点，请参见：**如何选择数据库安全审计的Agent安装节点?** 。

系统影响

数据库安全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。

须知

请确认购买实例的账号具有“DBSS System Administrator”、“VPC Administrator”、“ECS Administrator”和“BSS 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：对账号中心、费用中心、资源中心中的所有菜单项执行任意操作。项目级角色，在同项目中勾选。
- ECS Administrator：对弹性云服务器的所有执行权限。项目级角色，在同项目中勾选。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在界面右上角，单击“购买数据库安全审计”。

步骤4 选择“区域”、“项目”、“可用区”和“性能规格”，如**图3-2**所示。

图 3-2 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3-3**所示。

表 3-3 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
专业版	最多支持6个数据库实例	• CPU：8U • 内存：32GB • 硬盘：1,084GB	• 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：2,108GB	• 吞吐量峰值：30,000条/秒 • 入库速率：1,080万条/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。
- 云原生版仅支持在RDS控制台购买。
- 本表中的系统资源要求，是指购买数据库安全审计实例时会消耗的系统资源。购买时，用户的系统需要满足审计版本对应的配置。
- 本表中在线SQL语句的条数，是按照每条SQL语句的容量为1KB来计算的。

步骤5 设置数据库安全审计参数，如图3-3所示，相关参数说明如表3-4所示。

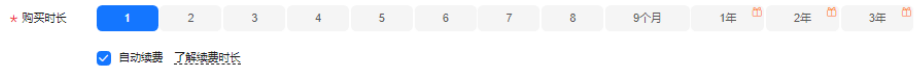
图 3-3 设置数据库安全审计参数

表 3-4 数据库安全审计实例参数说明

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

步骤6 选择“购买时长”，如图3-4所示。

图 3-4 选择实例购买时长



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

表 3-5 自动续费周期说明

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

步骤7 （可选）为数据库安全审计实例添加标签。如您的组织已经设定数据库安全服务的相关标签策略，则需按照标签策略规则为数据库安全审计实例添加标签。标签如果不符合标签策略的规则，则可能会导致数据库安全审计实例创建失败，请联系组织管理员了解标签策略详情。

步骤8 确认当前配置无误后，单击“立即购买”。

如果您对价格有疑问，可以单击“了解计费详情”，了解产品价格。

步骤9 在“详情”页面，阅读《数据库安全审计安全免责声明》后，勾选“我已阅读并同意《数据库安全审计安全免责声明》”，单击“提交”。

步骤10 在购买页面，请选择付款方式进行付款。

步骤11 成功付款后，在数据库安全审计实例列表界面，可以查看数据库安全审计实例的创建情况。

----结束

后续处理

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

3.3 步骤一：添加数据库

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

数据库安全审计支持审计的数据库类型及版本，请参见**支持的数据库类型及版本**。

前提条件

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

步骤3 在左侧导航树中，选择“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，配置数据库的信息。

表 3-6 数据库参数说明

参数名称	说明	取值样例
数据库类别	选择添加的数据库类别，“RDS数据库”或“自建数据库”。 **说明** 当您选择“RDS数据库”类型时，可以直接选择您需要添加至数据库安全服务防护的数据库。	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

参数名称	说明	取值样例
数据库类型	支持的数据库类型，您可以选择以下类型： ● MYSQL ● ORACLE ● PostgreSQL ● SQL Service ● DWS ● GaussDB(for MYSQL) ● GaussDB ● DAMENG ● KINGBASE ● MongoDB ● Hbase ● SHENTONG ● GBase 8a ● GBase XDM Cluster ● Greenplum ● HighGo ● MariaDB ● Hive ● DDS ● GBase 8s ● TDSQL **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 – 8.0.25 – 当“数据库类别”为“RDS数据库”时，自动关联获取数据库列表，按需选择实例，Agent免安装。 ● 当“数据库类型”选择“ORACLE”时，您可以选择以下版本： – 11g – 12c – 19c ● 当“数据库类型”选择“POSTGRESQL”时，您可以选择以下版本： – 7.4 – 8.0 8.0、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 ● 当“数据库类型”选择“SQLSERVER”时，您可以选择以下版本： – 2008 – 2012 – 2014 – 2016 – 2017 ● 当“数据库类型”选择“DWS”时，您可以选择以下版本： – 1.5 – 8.1	5.0

参数名称	说明	取值样例
	• 当“数据库类型”选择“GaussDB(for MySQL)”时，您可以选择以下版本： – 当“数据库类别”为“自建数据库”时，可选择“MySQL 8.0” – 当“数据库类别”为“RDS数据库”时，自动关联获取数据库列表，按需选择实例，Agent免安装。 • 当“数据库类型”选择“GaussDB”时，您可以选择以下版本： – 1.4企业版 – 1.3企业版 – 2.8企业版 – 3.223企业版 • 当“数据库类型”选择“DAMENG”时，您可以选择以下版本： – DM8 • 当“数据库类型”选择“KINGBASE”时，您可以选择以下版本： – V8 • 当“数据库类型”选择“Hbase”时，您可以选择以下版本： – 1.3.1 – 2.2.3 • 当“数据库类型”选择“SHENTONG”时，您可以选择以下版本： – V7.0 • 当“数据库类型”选择“GBase 8a”时，您可以选择以下版本： – v8.5 • 当“数据库类型”选择“GBase 8s”时，您可以选择以下版本： – v8.8 • 当“数据库类型”选择“Greenplum”时，您可以选择以下版本： – v6.0 • 当“数据库类型”选择“HighGo”时，您可以选择以下版本： – v6.0 • 当“数据库类型”选择“MongoDB”时，您可以选择以下版本： – v5.0	

参数名称	说明	取值样例
	• 当“数据库类型”选择“MariaDB”时，您可以选择以下版本： – 10.6 • 当“数据库类型”选择“Hive”时，您可以选择以下版本： – 1.2.2 – 2.3.9 – 3.1.2 – 3.1.3 • 当“数据库类型”选择“TDSQL”时，您可以选择以下版本： – 10.3.17.3.0	
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

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

说明

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

----结束

3.4 步骤二：开启数据库安全审计

数据库安全审计默认提供一条“全审计规则”的审计范围，可以对成功连接数据库安全审计实例的所有数据库进行安全审计。开启数据库安全审计后，您可以查看被添加的数据库的审计结果。详细操作，请参见**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”。
- 数据库安全审计实例已成功添加安全组规则。

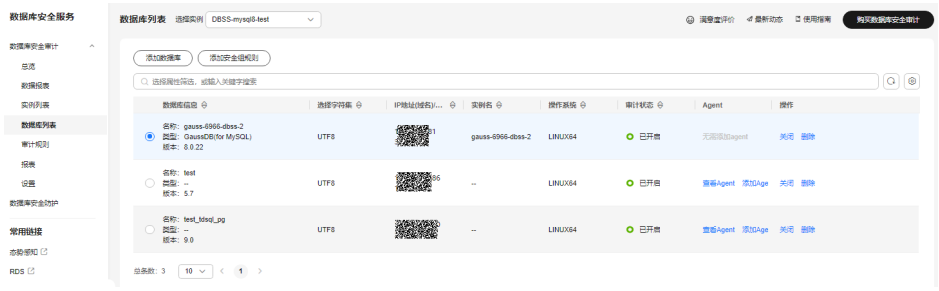
开启审计

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，选择“数据库列表”，进入“数据库列表”界面。

图 3-5 进入“数据库列表”界面

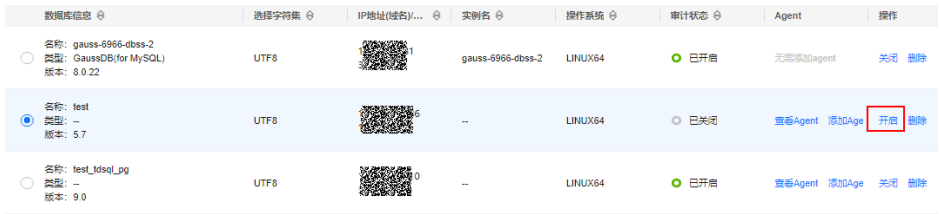


步骤4 在选择实例下拉框中，选择需要开启审计的数据库安全审计实例。

步骤5 在待开启审计所在行的“操作”列，单击“开启”，开启审计功能。

审计功能开启后，该数据库的“审计状态”为“已开启”，不需要重启数据库。

图 3-6 开启数据库审计功能



----结束

验证审计效果

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

步骤2 登录管理控制台。

步骤3 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > 数据库安全服务”，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”，SQL语句列表将显示**步骤1**中输入的SQL语句。

图 3-7 查看 SQL 语句

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

----结束

4 升级数据库审计实例版本

本章节指导您如何升级您的数据库实例版本。

前提条件

- 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。
- 数据库安全审计实例已成功添加安全组规则。
- 数据库实例版本低于当前最新版本。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“实例列表”，进入“实例列表”界面。

步骤4 在“版本”列单击“升级”。

图 4-1 升级实例版本

步骤5 在弹出的对话框中单击“是”，开始实例版本升级。

----结束

5 配置审计规则

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

步骤3 在左侧导航树中，选择“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5-1所示，相关参数说明如表5-1所示。

图 5-1 “添加审计范围”对话框

表 5-1 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“**ALL（全部数据库）**”或选择待添加审计范围的数据库。	db03
数据库账户	可选参数。输入数据库的用户名。 可增加多个账户，多个账户间用逗号隔开。	-

参数名称	说明	取值样例
操作类型	审计范围的操作类型，包括“登录”和“操作”。 当选择“操作”时，可以选择“全部操作”，或选择“数据定义”、“数据操作”或“数据控制”的操作。	登录
数据库账户	可选参数。输入数据库的账户名。 可增加多个账户，多个账户间用逗号隔开。	-
例外IP	可选参数。输入不需要对数据库操作行为进行审计的IP地址。 **说明** 例外IP规则高于源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。

5.2 添加 SQL 注入规则

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

前提条件

- 已成功购买数据库安全审计实例，且实例的状态为“运行中”。
- 已成功添加数据库并开启审计功能。
- 已成功添加数据库。

操作步骤

步骤1 登录管理控制台。

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

步骤3 单击“添加SQL注入规则”，在弹窗中填写相关信息。

图 5-2 添加 SQL 注入规则

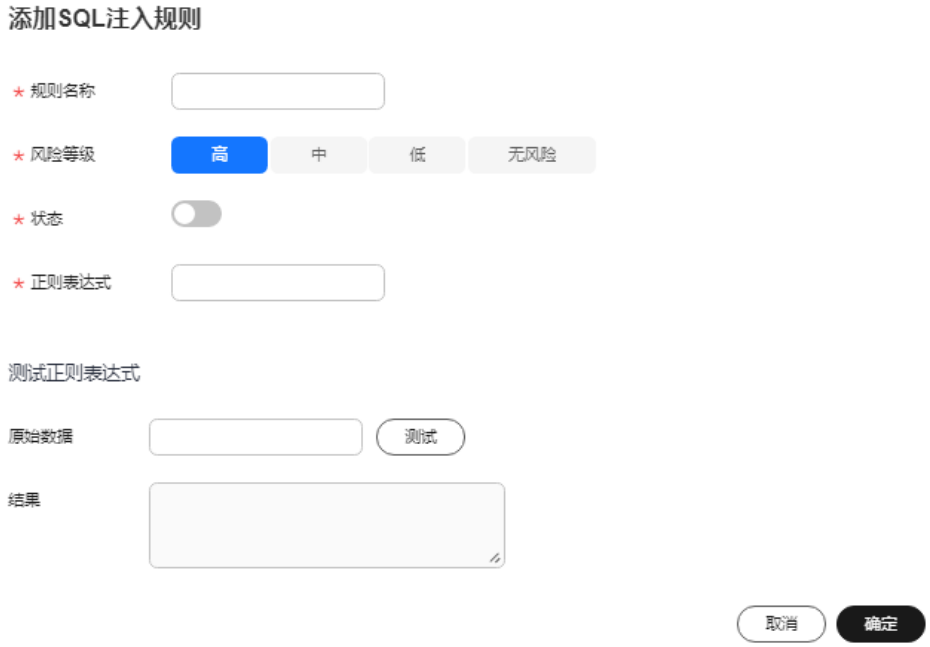


表 5-2 SQL 注入规则参数说明

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

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

步骤4 填写完成，确认信息无误，单击“确定”，添加完成，新增的SQL注入规则默认为SQL注入列表第一条。

----结束

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

步骤3 在左侧导航树中，选择“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“设置优先级”，在弹出的窗口中单击“优先级”的选框选择想要设置的优先等级，数字越小优先级越高，选择完成，单击“确定”完成设置。

图 5-3 设置优先级

步骤7 在SQL注入检测规则所在行的“操作”列，单击“禁用”。

图 5-4 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”。

步骤8 单击“操作”列的“编辑”，可对目标规则的参数进行编辑；参数说明如**表5-3**所示，编辑完成，确认信息无误，单击“确定”，完成修改。

图 5-5 编辑 SQL 注入规则

表 5-3 SQL 注入规则参数说明

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

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

步骤9 单击“操作”列的“删除”，对目标规则进行删除。

----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 5-6 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”。

5.4 添加风险操作

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

须知

一条审计数据只能命中风险操作中的一个规则。

前提条件

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

步骤3 在左侧导航树中，选择“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“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6 选择“风险操作”页签。

步骤7 在风险操作列表左上方，单击“添加风险操作”。

步骤8 在“添加风险操作”界面，设置基本信息和客户端IP地址，如图5-7所示，相关参数说明如表5-4所示。

图 5-7 设置基本信息和客户端 IP 地址

表 5-4 风险操作参数说明

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

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

步骤9 设置操作类型、操作对象、执行结果，如图5-8所示，相关参数说明如表5-5所示。

图 5-8 设置操作类型、操作对象和执行结果

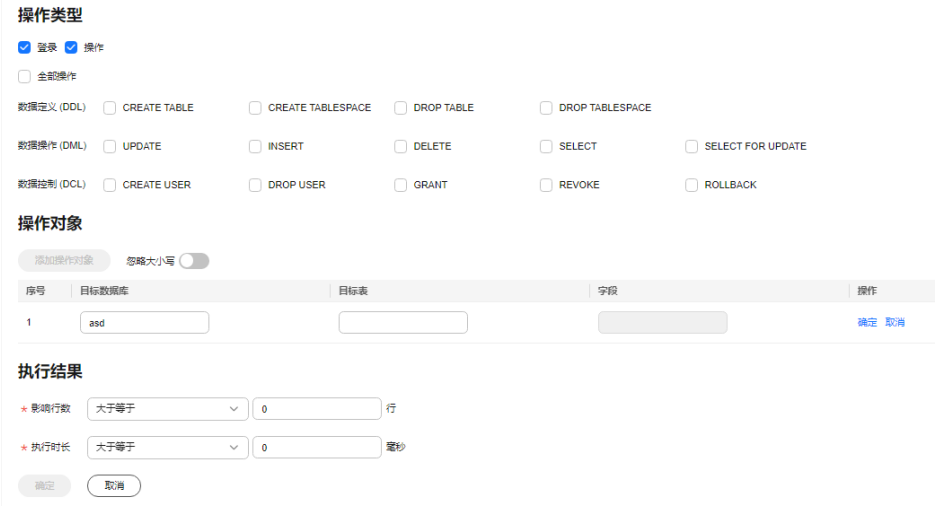


表 5-5 参数说明

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

步骤10 单击“保存”。

----结束

5.5 配置隐私数据保护规则

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

前提条件

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

步骤3 在左侧导航树中，选择“审计规则”。

步骤4 在“选择实例”下拉列表框中，选择需要配置隐私数据保护规则的实例。

步骤5 选择“隐私数据保护”页签。

说明

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

步骤6 开启或关闭“存储结果集”和“隐私数据脱敏”。

- 存储结果集

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

  如果用于PCI DSS/PCI 3DS CSS认证，禁止开启。

  注：结果集存储只支持agent方式审计数据库。

- 隐私数据脱敏

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

步骤7 单击“添加自定义规则”，在弹出“添加自定义规则”对话框中设置数据脱敏规则，如图5-9所示，相关参数说明如表5-6所示。

图 5-9 “添加自定义规则”对话框

表 5-6 自定义规则参数说明

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

步骤8 单击“确定”。

规则列表中新增一条状态为“已启用”的脱敏规则。

----结束

效果验证

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

步骤1 开启“隐私数据脱敏”，并确保“护照号”规则已启用，如图5-10所示。

图 5-10 规则已启用

步骤2 使用MySQL数据库自带的客户端，以**root**用户登录数据库。

步骤3 在数据库客户端，输入一条SQL请求语句。

select * from db where HOST="*护照号*";

步骤4 在左侧导航树中，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。

6 查看审计结果

6.1 查看 SQL 语句详细信息

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

前提条件

- 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。
- 数据库安全审计实例已成功添加安全组规则。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏选择“数据报表”，进入“数据报表”页面。

步骤4 在“选择实例”下拉列表框中，选择需要查看SQL语句信息的实例。

步骤5 选择“语句”页签。

步骤6 查询SQL语句信息。

图 6-1 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”、“今日”、“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7 在需要查看详情的SQL语句所在行的“操作”列，单击“详情”。

图 6-2 查看 SQL 语句详情

步骤8 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6-1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。

表 6-1 SQL 语句详情参数说明

参数名称	说明
会话ID	SQL语句的ID，由系统自动生成。
数据库实例	SQL语句所在的数据库实例。
数据库类型	执行SQL语句所在的数据库的类型。
数据库用户	执行SQL语句的数据库用户。
客户端MAC地址	执行SQL语句所在客户端MAC地址。
数据库MAC地址	执行SQL语句所在数据库MAC地址。
客户端IP	执行SQL语句所在客户端的IP地址。
数据库IP/域名	执行SQL语句所在的数据库的IP地址/域名。
客户端端口	执行SQL语句所在的客户端的端口。
数据库端口	执行SQL语句所在的数据库的端口。
客户端名称	执行SQL语句所在客户端名称。
操作类型	SQL语句的操作类型。
操作对象类型	SQL语句的操作对象的类型。
响应结果	执行SQL语句的响应结果。

参数名称	说明
影响行数	执行SQL语句的影响行数。
开始时间	SQL语句开始执行的时间。
响应结束时间	SQL语句结束的时间。
SQL请求语句	SQL语句的名称。
请求结果	SQL语句请求执行的结果。

----结束

相关操作

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

6.2 查看会话分布

添加的数据库连接到数据库安全审计实例后，您可以查看该数据库的会话分布情况。

前提条件

- 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。
- 数据库安全审计实例已成功添加安全组规则。

操作步骤

步骤1 **登录管理控制台。**

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

步骤3 在左侧导航栏选择“数据报表”，进入“数据报表”页面。

步骤4 在“选择实例”下拉列表框中，选择需要查看会话信息的实例。

步骤5 选择“会话”页签。

步骤6 查看会话分布表。

- 在“选择数据库”下拉列表框中，选择“全部数据库”或指定的数据库，可以查看实例中所有的数据库或指定的某个数据库的会话信息。

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

----结束

6.3 查看审计总览信息

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

前提条件

- 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。
- 数据库安全审计实例已成功添加安全组规则。
- 数据库实例版本在23.05.23.193055及以上，此章节内容请参见**查看趋势分析**。

操作步骤

步骤1 **登录管理控制台。**

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

步骤3 在左侧导航栏选择“数据报表”，进入“数据报表”页面。

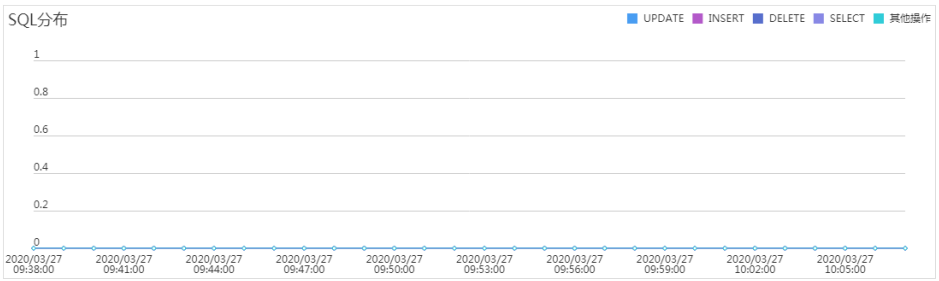
步骤4 选择“趋势分析”页签，进入“趋势分析”页面。

步骤5 在“选择实例”下拉列表框中，选择需要查看审计总览信息的实例。

步骤6 查看数据库的总体审计情况，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 6-3 SQL 分布



----结束

相关操作

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

6.4 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。
- 数据库安全审计实例已成功添加安全组规则。

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6-2**所示。用户可根据实际业务情况生成报表、设置报表的执行任务。

表 6-2 报表说明

报表模板名称	报表类型	说明
数据库安全综合报表	综合报表	提供数据库整体审计状况，主要从风险分布、会话分布和登录状况等几个维度进行审计分析，为数据库管理提供整体审计状况依据。
数据库安全合规报表	合规报表	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 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 在页面上方选择“区域”后，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“报表”。

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”。

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。

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

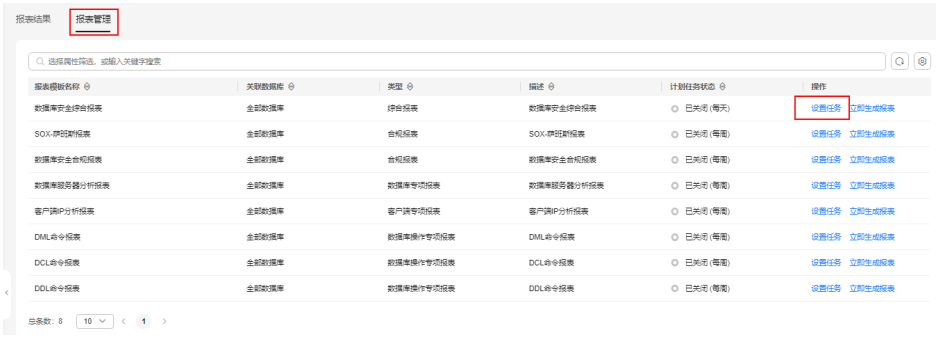
步骤3 在左侧导航树中，选择“报表”。

步骤4 在“选择实例”下拉列表框中，选择需要设置执行任务的报表的实例。

步骤5 选择“报表管理”页签。

步骤6 在需要立即生成报表的模板所在行的“操作”列，单击“设置任务”，如图6-4所示。

图 6-4 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6-5所示，相关参数说明如表6-3所示。

图 6-5 “计划任务”对话框

表 6-3 计划任务参数说明

参数名称	说明	取值样例
启动任务	开启或关闭计划任务。 •  ：开启 •  ：关闭	
消息通知	开启或关闭消息通知。 消息通知触发的消息由消息通知服务发送，消息通知服务为收费服务，价格详情请参见**SMN价格详情**。 •  ：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	周期执行
执行时间	选择报表执行的时间点。	10点
数据库	选择执行报表任务的数据库。	-

步骤8 单击“确定”。

----结束

步骤二：预览、下载审计报表

预览或下载审计报表前，请确认报表的“状态”为“100%”。

须知

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

步骤1 **登录管理控制台。**

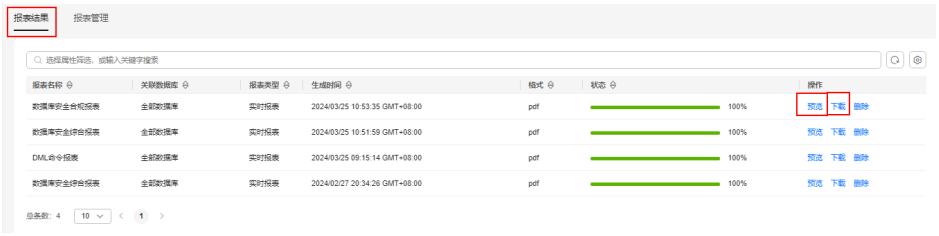
步骤2 在页面上方选择“区域”后，单击页面左上方的 ，选择“安全与合规 > 数据库安全服务”，进入数据库安全审计“总览”界面。

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6-6所示，在线预览报表结果，或下载并查看报表。

图 6-6 预览或下载报表



----结束

相关操作

[为什么不能在线预览数据库安全审计报表?]

6.5 查看趋势分析

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

前提条件

- 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。
- 数据库安全审计实例已成功添加安全组规则。
- 数据库实例23.05.23.193055及以上版本支持该功能。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏选择“数据报表”，进入“数据报表”页面。

步骤4 选择“趋势分析”页签，进入“趋势分析”页面。

步骤5 在“选择实例”下拉列表框中，选择需要查看审计总览信息的实例。

步骤6 查看数据库的总体趋势情况。

- 单击控制台右侧的“重新生成趋势分析”。
- 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 6-7 重新生成趋势分析

----结束

7 设置告警通知

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

步骤3 在左侧导航树中，选择“设置”。

步骤4 在“选择实例”下拉列表框中，选择需要设置邮件通知的实例。

步骤5 设置邮件通知，相关参数说明如**表7-1**所示。

图 7-1 设置邮件通知

表 7-1 邮件通知参数说明

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

步骤6 单击“应用”。

----结束

7.2 设置告警通知

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

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

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

前提条件

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

步骤3 在左侧导航树中，选择“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7-2**所示。

图 7-2 设置告警通知

表 7-2 告警通知参数说明

参数名称	说明	取值样例
消息通知	开启或关闭消息通知。数据库安全审计的告警基础功能免费，触发产生的告警消息由消息通知发送，可能会产生少量费用，具体的收费详情，请参见**SMN价格详情**。 ●  ：开启 ●  ：关闭	
消息通知主题	● 通过下拉框选择已有的主题，或者单击“查看消息通知主题”创建新的主题，具体操作请参见**创建主题**。 ● 每个消息通知主题可添加多个订阅，并可选择多种订阅终端（例如短信、邮件等），详细订阅说明请参见**添加订阅**。 **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
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

8 查看监控信息

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

步骤3 在左侧导航树中，选择“实例列表”，进入“实例列表”界面。

步骤4 单击需要查看系统监控信息的实例名称，进入实例概览页面。

步骤5 选择“系统监控”页签，进入系统监控页面。

步骤6 查看系统监控信息，如图8-1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 8-1 查看系统监控信息

----结束

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

步骤3 在左侧导航树中，选择“实例列表”，进入“实例列表”界面。

步骤4 单击需要查看告警信息的实例名称，选择“告警监控”，进入告警监控页面。

步骤5 查看告警信息，如图8-2所示，相关参数说明如表8-1所示。

图 8-2 查看告警信息

表 8-1 告警信息参数说明

参数名称	说明
发生时间	告警发生的时间。
告警类型	告警的类型，包括： ● 审计流量超限 ● CPU异常 ● 内存异常 ● 磁盘异常 ● 审计容量不足 ● 日志备份OBS失败 ● Agent异常
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”、“近30天”或自定义时间），单击，列表显示该时间段的告警信息。
- 选择“告警风险等级”（“全选”、“高”、“中”或“低”），列表显示该级别的告警信息。
- 选择“告警类型”，列表显示该类型的告警信息。

----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。

9 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。

OBS 细粒度授权

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

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“管理与监管 > 统一身份认证服务”。

步骤3 选择左侧导航树的“权限管理 > 授权”，单击右上角的“创建自定义策略”。

步骤4 填写策略参数。策略名称为“DBSS OBS Agency Access”，策略配置方式选择“JSON视图”。填写策略内容如下：

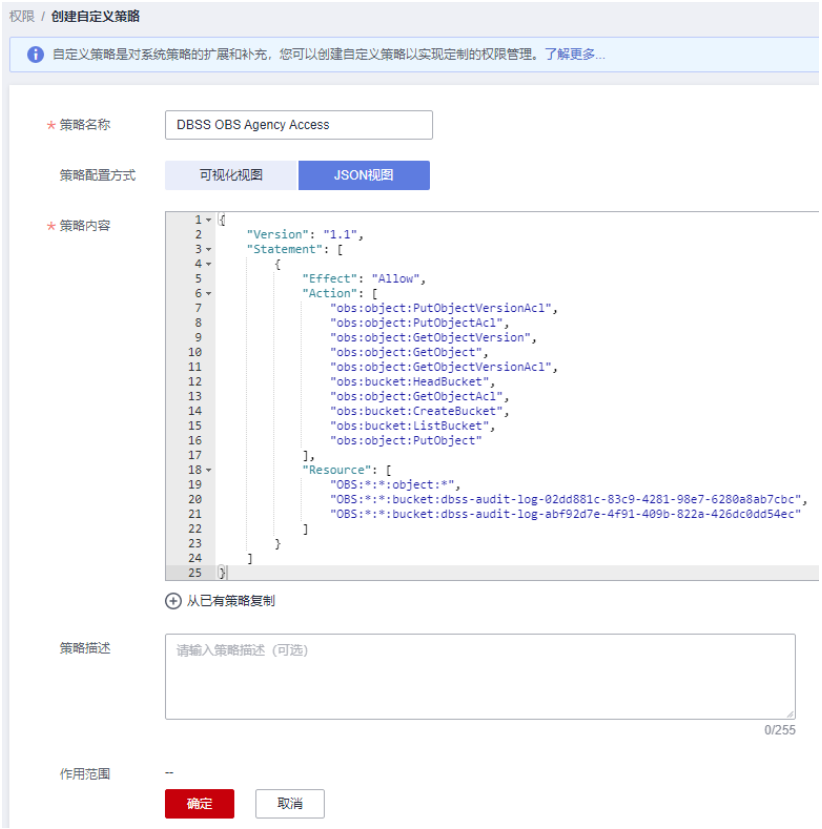
```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "obs:object:PutObjectVersionAcl",
        "obs:object:PutObjectAcl",
        "obs:object:GetObjectVersion",
        "obs:object:GetObject",
        "obs:object:GetObjectVersionAcl",
        "obs:bucket:HeadBucket",
        "obs:object:GetObjectAcl",
        "obs:bucket:CreateBucket",
```



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

如图9-1所示。配置完成后单击“确定”。

图 9-1 创建自定义策略



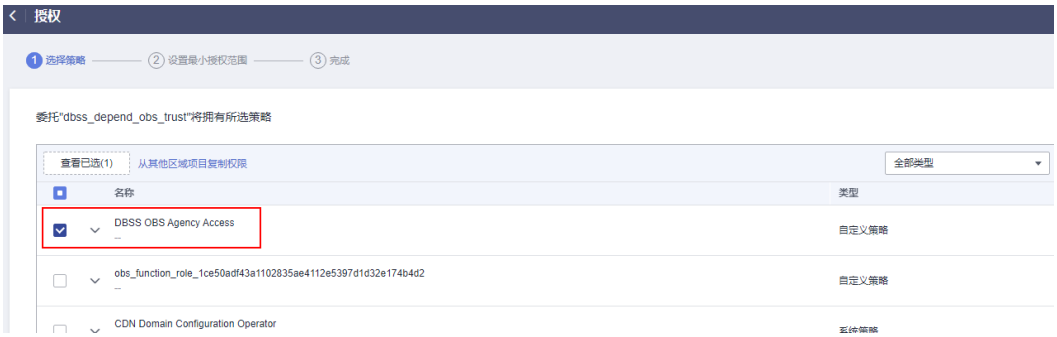
步骤5 选择左侧导航树上的“委托”，单击右上角“创建委托”。

步骤6 填写委托参数。委托名称为“dbss_depend_obs_trust”，委托类型选择“云服务”，云服务选择“DBSS”。如图9-2所示。

图 9-2 创建委托

步骤7 单击“下一步”，勾选**步骤4**中创建的自定义策略，将权限（DBSS OBS Agency Access）添加到委托（dbss_depend_obs_trust）中，如**图9-3**所示。单击右下角的“下一步”。

图 9-3 选择策略



步骤8 授权范围选择“所有资源”，单击右下角的“确定”，显示授权成功如**图9-4**所示，单击“完成”后等待15分钟授权生效。

图 9-4 完成授权

----结束

自动备份数据库审计日志

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“设置”。

步骤4 在“选择实例”下拉列表框中，选择需要设置备份的实例，选择“备份与恢复”页签。

步骤5 单击“修改自动备份设置”，在弹出的对话框中，设置自动备份参数，相关参数说明如表9-1所示。

图 9-5 “设置自动备份”对话框

表 9-1 自动备份参数说明

参数名称	说明	取值样例
自动备份	开启或关闭自动备份。 •  ：开启 •  ：关闭	
备份周期	选择自动备份的周期，可以选择： • 每天 • 每小时	每天

参数名称	说明	取值样例
开始时间	单击，选择开始备份的时间。	2020/01/14 20:27:08
桶名称	设置备份使用的OBS桶名称，可以选择： • 创建默认桶 • 选择已有桶 **说明** • 单击“创建默认桶”，将进行OBS授权，用于审计日志备份导出。 • 审计日志只能导出到DBSS服务创建的桶。	20f18-7a5a-4042
文件导出目录	在OBS桶中创建备份文件的目录。	test

步骤6 单击“确定”，设置完成。

说明

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

----结束

恢复数据库审计日志

数据库审计日志备份成功后，您可以根据需要恢复数据库的审计日志。

须知

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

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“设置”。

步骤4 在“选择实例”下拉列表框中，选择需要恢复日志的实例，选择“备份与恢复”页签。

步骤5 在需要恢复数据库审计的备份日志所在的“操作”列，单击“恢复日志”。

步骤6 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。

说明

开启风险导出前，需进行**OBS细粒度授权**。

步骤1 **登录管理控制台。**

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

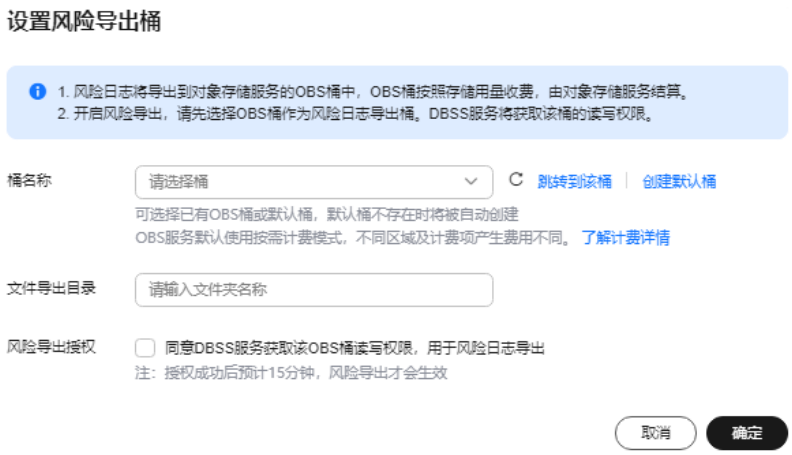
步骤3 在左侧导航树中，选择“设置”。

步骤4 在“选择实例”下拉列表框中，选择需要导出风险的实例，选择“风险导出”页签。

步骤5 在需要导出风险日志的数据库右侧操作栏单击，开启风险导出。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。

图 9-6 自动创建 OBS 桶



----结束

10 其他操作

10.1 管理数据库安全审计实例

成功购买数据库安全审计实例后，您可以查看实例信息，开启、重启或关闭实例。

前提条件

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

查看实例信息

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > 数据库安全服务”，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10-1所示。

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 10-1 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。
计费模式	实例的计费模式（包年/包月）和到期时间。
版本	数据库安全审计的实例版本。

参数名称	说明
状态	实例当前的运行状态，包括： ● 运行中 ● 创建中 ● 故障 ● 已关闭 ● 已冻结 ● 公安冻结 ● 违规冻结 ● 未实名认证冻结 ● 合作伙伴冻结 ● 创建失败
已关联数据库/数据库总数	实例的已关联的数据库和实例可以支持关联的数据库总数。
企业项目	该实例的企业项目名称。
操作	对该实例进行相关操作： ● 配置审计规则 ● 开启 ● 关闭 ● 重启 ● 查看详情 ● 查看监控指标 ● 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

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

步骤3 在左侧导航树中，选择“实例列表”，进入“实例列表”界面。

步骤4 单击需要查看信息的实例名称，进入实例概览页面。

步骤5 查看实例的“基本信息”、“网络配置信息”和“关联数据库”，相关参数说明如表10-2所示。

表 10-2 实例概览信息参数说明

类别	参数名称	说明
基本信息	实例名称	实例的名称。单击名称后的✎，可以修改实例名称。
	版本	当前实例的版本。

类别	参数名称	说明
	备注	实例的备注信息。单击备注后的，可以修改备注信息。
	计费模式	实例的计费模式。
	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。有关添加数据库的详细操作，请参见**步骤一：添加数据库**。

----结束

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

步骤3 在左侧导航树中，选择“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10-3**所示。

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 10-3 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，单击页面左上方的 ☰，选择“安全与合规 > 数据库安全服务”，进入数据库安全审计“总览”界面。

步骤3 在左侧导航树中，选择“数据库列表”，进入“数据库列表”界面。

步骤4 在“选择实例”下拉列表框中，选择查看的Agent所属的实例。

步骤5 单击数据库左侧的 ⌄ 展开Agent的详细信息，相关参数如表 Agent参数说明所示。

表 10-4 Agent 参数说明

参数名称	说明
Agent ID	Agent的ID，由系统自动生成。
安装节点类型	安装节点的类型，包括“数据库端”或“应用端”。
安装节点IP	安装Agent的节点的IP地址。
操作系统	安装Agent运行的操作系统。
审计网卡名称	安装节点的网卡名称。
CPU阈值(%)	安装节点的CPU阈值，缺省值为“80”。 **说明** 当安装节点的CPU超过设定的阈值时，Agent将停止工作。您可以直接升级服务器的CPU。
内存阈值(%)	安装节点的内存阈值，缺省值为“80”。 **说明** 当安装节点的内存超过设定的阈值时，Agent将停止工作。您可以直接升级服务器的内存。
通用	Agent是否为通用Agent。
SHA256校验值	Agent安装包的校验值。
运行状态	安装节点的运行状态。

说明

您可以根据使用需求，对添加的Agent执行以下操作：

- 关闭
  - 在需要关闭的Agent所在行的“操作”列，单击“关闭”后，在弹出的提示框中，单击“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

10.4 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

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

步骤3 在左侧导航树中，选择“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10-5所示。

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 10-5 审计范围信息参数说明

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

说明

根据需要，您还可以对审计范围执行以下操作：

- 启用

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

- 编辑（仅自定义创建审计范围的支持）

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

- 禁用

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

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

步骤3 在左侧导航树中，选择“审计规则”。

步骤4 在“选择实例”下拉列表框中，选择需要查看SQL注入检测信息的实例。选择“SQL注入”页签。

步骤5 查看SQL注入检测信息，相关参数如表10-6所示。

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 10-6 SQL 注入检测信息参数说明

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

----结束

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

步骤3 在左侧导航树中，选择“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”。

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，单击页面左上方的 ☰，选择“安全与合规 > 数据库安全服务”，进入数据库安全审计“总览”界面。

步骤3 在左侧导航树中，选择“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10-7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 10-7 风险操作信息参数说明

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

说明

根据需要，您还可以对风险操作执行以下操作：

- 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

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

步骤3 在左侧导航树中，选择“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10-8所示。

说明

- 存储结果集

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

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

表 10-8 脱敏规则信息参数说明

参数名称	说明
规则名称	该规则的名称。
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

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

步骤3 在左侧导航树中，选择“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。

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，单击页面左上方的 ☰，选择“安全与合规 > 数据库安全服务”，进入数据库安全审计“总览”界面。

步骤3 在左侧导航树中，选择“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。

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

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

步骤3 在左侧导航树中，选择“设置”。

步骤4 在“选择实例”下拉列表框中，选择需要查看日志的实例。

步骤5 选择“备份与恢复”页签。

步骤6 查看备份的审计日志信息，相关参数说明如表10-9所示。

在列表右上方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 10-9 审计日志参数说明

参数名称	说明
日志名称	日志的名称，由系统自动生成。
备份时间	执行日志备份操作的时间。
文件大小	日志的文件大小。
备份方式	日志的备份方式。
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

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

步骤3 在左侧导航树中，选择“实例列表”。

步骤4 单击需要查看操作日志的实例名称，进入实例概览页面。

步骤5 选择“操作日志”页签，进入操作日志列表页面。

步骤6 查看操作日志，相关参数说明如表10-10所示。

说明

可选择时间“近30分钟”、“近1小时”、“今日”、“近7天”或“近30天”或自定义时间段。

表 10-10 操作日志参数说明

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

----结束

11 云审计服务支持的关键操作

11.1 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。

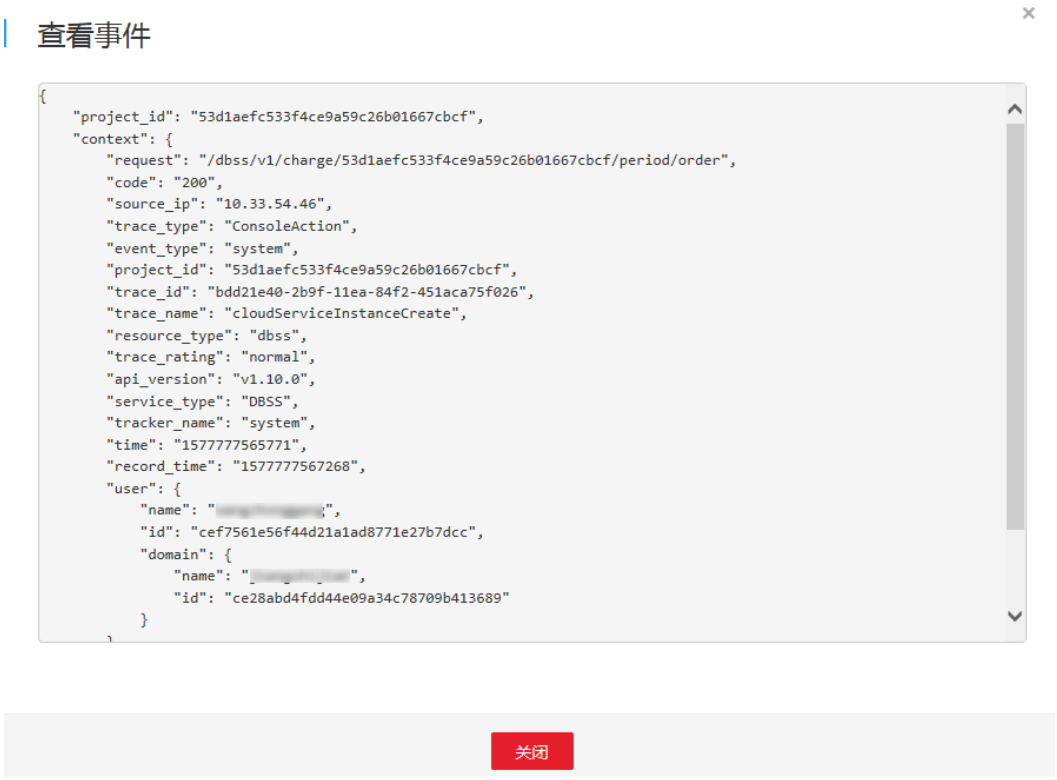
步骤5 单击“查询”，查看对应的操作事件。

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11-1所示。

图 11-1 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11-2所示，显示了该操作事件结构的详细信息。

图 11-2 查看事件



----结束

11.2 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11-1所示。

表 11-1 云审计服务支持的数据库安全服务操作列表

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

12 监控

12.1 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 12-1 数据库安全服务支持的监控指标

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

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
mem_util	内存使用率	该指标用于统计测量对象的内存利用率。 单位：百分比 采集方式：100%减去空闲内存占比	0～100% 值类型：Float	数据库审计实例	1分钟
disk_util	磁盘使用率	该指标用于统计测量对象的磁盘利用率。 单位：百分比 采集方式：100%减去空闲磁盘占比	0～100% 值类型：Float	数据库审计实例	1分钟
hx_process_status	防护实例进程状态	该指标用于展示防护实例的进程状态。 **说明** 该防护实例已不再维护。	0/1 ● 0：进程状态异常 ● 1：进程状态正常	数据库审计实例	1分钟
hx_port_stats	防护实例端口状态	该指标用于展示防护实例的端口状态。 **说明** 该防护实例已不再维护。	0/1 ● 0：端口状态异常 ● 1：端口状态正常	数据库审计实例	1分钟
hx_proxy_num	防护实例代理数量	该指标用于展示防护实例的代理数量。 **说明** 该防护实例已不再维护。	≥0	数据库审计实例	1分钟
hx_proxy_status	防护实例代理状态	该指标用于展示防护实例的代理状态。 **说明** 该防护实例已不再维护。	0/1 ● 0：代理状态异常 ● 1：代理状态正常	数据库审计实例	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
hx_qps	防护实例每秒查询数	该指标用于展示防护实例的每秒查询数。 **说明** 该防护实例已不再维护。	≥0	数据库审计实例	1分钟
hx_rps	防护实例每秒请求数	该指标用于展示防护实例的每秒请求数。 **说明** 该防护实例已不再维护。	≥0	数据库审计实例	1分钟
hx_active_connections_num	防护实例活跃连接数	该指标用于展示防护实例的活跃连接数。 **说明** 该防护实例已不再维护。	≥0	数据库审计实例	1分钟

12.2 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12-1所示。

图 12-1 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

12.3 查看监控指标

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

前提条件

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“管理与监管 > 云监控服务 CES”。

步骤3 在左侧导航树栏，选择“云服务监控 > 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

13 共享 VPC

操作场景

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

创建 VPC

步骤1 登录管理控制台。

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

步骤3 单击页面左侧“我的共享 > 共享管理”，进入“共享管理”页面。

步骤4 单击页面右上角的“创建共享”，进入“创建共享”页面。

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

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

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

表 13-1 参数说明

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

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

----结束

使用 VPC

步骤1 登录管理控制台。

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

步骤3 在界面右上角，单击“购买数据库安全审计”。

步骤4 选择“区域”、“项目”、“可用区”和“性能规格”，如图13-1所示。

图 13-1 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13-2所示。

表 13-2 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
专业版	最多支持6个数据库实例	• CPU：8U • 内存：32GB • 硬盘：1,084GB	• 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：2,108GB	• 吞吐量峰值：30,000条/秒 • 入库速率：1,080万条/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。
- 云原生版仅支持在RDS控制台购买。
- 本表中的系统资源要求，是指购买数据库安全审计实例时会消耗的系统资源。购买时，用户的系统需要满足审计版本对应的配置。
- 本表中在线SQL语句的条数，是按照每条SQL语句的容量为1KB来计算的。

步骤5 选择数据库安全审计的虚拟私有云及子网，相关参数说明如**表13-3**所示。

图 13-2 设置数据库安全审计参数

表 13-3 数据库安全审计实例参数说明

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

参数名称	说明
安全组	您可以选择区域中已有的安全组，或者在VPC管理控制台创建新的安全组。选择实例的安全组后，该实例将受到该安全组访问规则的保护。 更多有关安全组的信息，请参见《 虚拟私有云用户指南 》。
子网	您可以选择VPC中已配置的子网，或者在VPC管理控制台为VPC创建新的子网。
实例名称	您可以自定义实例的名称。

----结束

14 权限管理

14.1 创建用户并授权使用 DBSS

如果您需要对您所拥有的DBSS进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用DBSS资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将DBSS资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用DBSS服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如**图14-1**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的DBSS权限，并结合实际需求进行选择，DBSS系统策略如**表14-1**所示。DBSS支持的系统权限，请参见：**DBSS系统权限**。

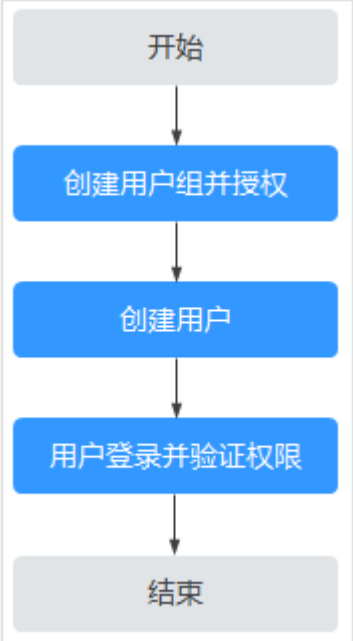
表 14-1 DBSS 系统权限

系统角色/策略名称	描述	类别	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。	系统角色	无。
DBSS FullAccess	数据库安全服务所有权限。	系统策略	

系统角色/策略名称	描述	类别	依赖关系
DBSS ReadOnlyAccess	数据库安全服务只读权限，拥有该权限的用户仅能查看数据库安全服务，不具备服务配置权限。	系统策略	

示例流程

图 14-1 给用户授权服务权限流程



1. **创建用户组并授权**

   在IAM控制台创建用户组，并授予数据库安全服务管理员权限“DBSS Security Administrator”。

2. **创建用户并加入用户组**

   在IAM控制台创建用户，并将其加入**1**中创建的用户组。

3. **用户登录**并验证权限

   新创建的用户登录控制台，切换至授权区域，验证权限：

   验证方式（参考）： 您可以尝试开启或关闭实例，此时如果提示“您的权限不足”，则表示设置的“DBSS Security Administrator”数据库安全服务安全管理员角色已生效。

14.2 DBSS 自定义策略

如果系统预置的DBSS权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考**DBSS权限及授权项**。

DBSS 自定义策略样例

- 示例1：授权用户查询数据库审计列表

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "dbss:auditInstance:list"
         ]
      }
   ]
}
```

- 示例2：拒绝用户删除数据库审计实例

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循**Deny优先原则**。

  如果您给用户授予“DBSS FullAccess”的系统策略，但不希望用户拥有“DBSS FullAccess”中定义的删除数据库审计实例权限，您可以创建一条拒绝删除数据库审计实例的自定义策略，然后同时将“DBSS FullAccess”和拒绝策略授予用户，根据Deny优先原则，则用户可以对DBSS执行除了删除数据库审计实例外的所有操作。拒绝策略示例如下：

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

- 示例3：多个授权项策略

  一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下：

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "dbss:defendInstance:eipOperate",
            "dbss:auditInstance:getSpecification"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "hss:accountCracks:unblock",
            "hss:commonIPs:set"
         ]
```

```
    }
  ]
}
```

14.3 DBSS 权限及授权项

如果您需要对您所拥有的数据库安全服务进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，IAM），如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用DBSS服务的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。策略支持的操作与API相对应，授权项列表说明如下：

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。
- 依赖的授权项：部分Action存在对其他Action的依赖，需要将依赖的Action同时写入授权项，才能实现对应的权限功能。

DBSS支持的自定义策略授权项如**表14-2**所示：

表 14-2 授权列表

权限	授权项
查询数据库安全审计实例列表	dbss:auditInstance:list
获取数据库安全审计实例的可用规格	dbss:auditInstance:getSpecification
查询数据库安全防护实例列表	dbss:defendInstance:list
删除数据库安全审计实例	dbss:auditInstance:delete
按需购买数据库安全防护实例	dbss:defendInstance:createOnDemand
按需购买数据库安全审计实例	dbss:auditInstance:createOnDemand
按包周期购买数据库安全审计实例	dbss:auditInstance:createOnOrder
重启数据库安全防护实例	dbss:defendInstance:reboot
启动数据库安全审计实例	dbss:auditInstance:start
关闭数据库安全审计实例	dbss:auditInstance:stop
重启数据库安全审计实例	dbss:auditInstance:reboot

权限	授权项
启动数据库安全防护实例	dbss:defendInstance:start
关闭数据库安全防护实例	dbss:defendInstance:stop

14.4 FullAccess 敏感权限配置

DBSS的full权限集涉及部分用户的敏感权限，比如订单支付、obs桶创建和文件上传、委托的创建及委托权限设置等。

这部分权限对用户资产影响较大，故不在系统预制权限集中添加，需通过说明文档方式，由用户手动添加。

相关敏感权限说明如表14-3所示，权限详情如下：

```
"obs:bucket:CreateBucket",
"obs:object:PutObject",
"bss:order:pay",
"iam:agencies:createAgency",
"iam:permissions:grantRoleToAgency",
"iam:permissions:grantRoleToAgencyOnEnterpriseProject",
"iam:permissions:grantRoleToAgencyOnDomain",
"iam:permissions:grantRoleToAgencyOnProject"
```

表 14-3 敏感权限说明

敏感权限项	使用场景说明	是否为global权限	敏感权限规避措施
obs:bucket:CreateBucket	• agent在CCE场景部署时，如果上传的obs桶不存在，则会调用该接口创建obs桶。上传的obs桶名固定为:dbss-audit-agent-{project_id}，project_id为当前实例所在的项目id。 • 备份和风险导出功能场景，如果选择的桶不存在，则会创建obs桶。	是	• 如不涉及权限使用场景，可以不配置该权限。 • 如涉及，可以提前使用有权限的账号创建要使用的obs桶即可。
obs:object:PutObject	agent在CCE场景部署时，将实例配置信息上传到obs桶。	是	• 如不涉及权限使用场景，可以不配置该权限。 • 如需使用，必须配置该权限才能将实例信息正常导出，无规避措施。

敏感权限项	使用场景说明	是否为global权限	敏感权限规避措施
iam:agencies:createAgency iam:permissions:grantRoleToAgency iam:permissions:grantRoleToAgencyOnEnterpriseProject iam:permissions:grantRoleToAgencyOnDomain iam:permissions:grantRoleToAgencyOnProject	• 备份和风险导出场景，创建名为"dbss_depend_obs_trust"的委托并对其授予obs操作相关权限。 • dws免agent场景，dws会创建名为"DWSAccessLTS"的委托，并对其授予访问lts的权限，用于将审计日志上传到租户的lts中。dbss会创建名为"dbss_dws_lts_trust"的委托，并对其授予lts访问权限，用于后续从lts下载审计日志。	是	• 如不涉及权限使用场景，可以不配置该权限。 • 使用有权限的账号开启该功能。
bss:order:pay	购买审计实例时，进行订单支付。	否	• 如不涉及权限使用场景，可以不配置该权限。 • 使用有权限的账号提前购买实例。

A 修订记录

发布日期	修改说明
2024-05-13	第三十五次正式发布。 ● 新增**共享VPC**章节。 ● **配置隐私数据保护规则**补充结果集存储只支持agent方式审计数据库的说明。
2024-04-10	第三十四次正式发布。 控制台新风格升级。
2023-06-30	第三十三次正式发布。 新增如下章节： **查看趋势分析**章节； 5.4-升级数据库审计实例版本章节。
2022-11-30	第三十二次正式发布。 新增章节5.1-总览。
2022-11-16	第三十一次正式发布。 新增自动备份的延时说明。
2022-06-08	第三十次正式发布。 DBSS对接CES功能上线，新增章节： ● **DBSS监控指标说明** ● **设置监控告警规则** ● **查看监控指标**
2022-03-24	第二十九次正式发布。 手动备份审计日志功能下线。 ● **购买数据库安全审计**：新增参数“企业项目”。 ● 5.9-备份和恢复数据库审计日志：新增“OBS细粒度授权”操作；自动备份时，备份周期可选“每天”和“每小时”。

发布日期	修改说明
2022-01-07	第二十八次正式发布。 **表2-7**：新增“数据库类型”选择“MySQL”时，自动关联获取数据库列表，按需选择即可的说明。
2021-08-30	第二十七次正式发布。 修改内容：将服务列表入口“安全”修改为“安全与合规”。 新增内容如下： • **添加SQL注入规则**：新增“添加SQL注入规则”。 • **添加数据库**：新增选择GaussDB(for MySQL)时自动关联库内所有实例说明。 • **添加Agent（ECS/BMS自建数据库）**：数据库端添加Agent时，新增阈值自定义功能。 • **操作步骤**：告警信息新增“Agent异常”筛选。
2021-04-19	第二十六次正式发布。 • **安装Agent（Linux操作系统）**，修改Agent安装包命名。 • **管理添加的数据库和Agent**，新增“SHA256校验值”，校验Agent包的完整性。 • **卸载Agent**，修改Agent安装包命名。
2021-03-22	第二十五次正式发布。 • **步骤二：添加Agent**，优化相关内容描述。 • **添加风险操作**，优化相关内容描述。
2021-01-19	第二十四次正式发布。 优化数据库安全审计步骤流程。
2020-12-18	第二十三次正式发布。 • 新增**步骤四：添加安全组规则**。 • **流程指引**，新增添加安全组规则描述。 • **步骤二：添加Agent**，优化相关内容描述。 • **步骤三：下载并安装Agent**，优化相关内容描述。 • 5.6-查看审计结果，新增前提条件。
2020-12-15	第二十二次正式发布。 **步骤一：添加数据库**，优化相关内容描述。
2020-11-27	第二十一次正式发布。 **添加审计范围**，审计范围新增“例外IP”功能。

发布日期	修改说明
2020-10-14	第二十次正式发布。 **购买数据库安全审计**，新增购买数据库安全审计实例时选择VPC的说明描述。
2020-09-23	第十九次正式发布。 **添加风险操作**，新增一条默认风险操作“数据库拖库检测”。
2020-09-01	第十八次正式发布。 • **查看SQL语句详细信息**，新增审计语句和结果集字数长度限制。 • **创建用户并授权使用DBSS**，优化相关内容描述。
2020-07-31	第十七次正式发布。 • **设置告警通知**，告警通知方式变更，对接SMN服务，通知方式多样化。 • 下线“设置邮件通知”章节。
2020-07-08	第十六次正式发布。 • **安装Agent（Linux操作系统）**，优化相关内容描述。 • **安装Agent（Windows操作系统）**，优化相关内容描述。
2020-06-29	第十五次正式发布。 **购买数据库安全审计**，优化相关内容描述。
2020-06-18	第十四次正式发布。 • **添加审计范围**，优化相关内容描述。 • **设置告警通知**，优化相关内容描述。
2020-06-05	第十三次正式发布。 • **添加审计范围**，新增审计范围的操作类型。 • **查看告警信息**，新增“日志备份OBS失败”告警类型。
2020-05-20	第十二次正式发布。 **购买数据库安全审计**，优化相关内容描述。
2020-05-06	第十一次正式发布。 • **步骤二：添加Agent**，优化相关内容描述。 • **下载Agent**，优化相关内容描述。
2020-04-10	第十次正式发布。 更新界面截图。

发布日期	修改说明
2020-03-20	第九次正式发布。 修改**管理数据库安全审计实例**，新增实例运行状态。
2020-03-16	第八次正式发布。 ● 新增字符集“GBK”，oracle数据库增加“19c”版本。 ● “数据库安全防护故障排查”调整为FAQ。 ● “数据库安全审计故障排查”调整为FAQ。
2020-03-03	第七次正式发布。 ● 修改**购买数据库安全审计**，新增实例创建失败相关内容。 ● 修改**步骤一：添加数据库**，优化相关内容描述。 ● 修改**管理数据库安全审计实例**，优化相关内容描述。
2020-02-21	第六次正式发布。 新增数据库安全审计Windows相关描述。
2020-01-21	第五次正式发布。 ● **设置告警通知**，优化内容描述。 ● 5.9-备份和恢复数据库审计日志，优化内容描述。
2019-12-23	第四次正式发布。 补充支持IPv6相关内容描述。
2019-12-03	第三次正式发布。 ● 新增数据库安全审计服务内容。 ● 删除数据库安全防护服务内容。
2019-01-15	第二次正式发布。 调整文档大纲，优化内容描述。
2018-05-31	第一次正式发布。