

数据库安全服务

常见问题

文档版本 21
发布日期 2024-04-10



版权所有 © 华为技术有限公司 2024。保留一切权利。

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

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为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 产品咨询类	1
1.1 什么是数据库安全审计？	1
1.2 数据库安全审计和 RDS SQL 审计有什么区别？	1
1.3 数据库安全服务支持哪些性能规格？	1
1.4 数据库安全服务可以对华为云上的哪些数据库提供保护？	2
1.5 数据库安全服务支持哪些类型的数据库？	2
1.6 为什么购买实例后不能马上查看创建中的实例？	2
1.7 数据库安全服务到期后不续费会影响业务吗？	2
1.8 数据库安全审计是否支持审计云下数据库和非华为云上数据库？	2
1.9 什么是区域和可用区？	3
1.10 数据库安全服务是否支持数据实时脱敏？	4
1.11 购买 DBSS 服务后添加的数据库不在同一子网有什么影响？	4
2 购买类	5
2.1 购买实例时如何选择“子网”？	5
2.2 购买实例时为何要选择 VPC？	5
2.3 同一区域可以购买多少个数据库安全审计实例？	5
2.4 购买实例时提示配额不足时如何处理？	5
2.5 如何为数据库安全审计续费？	5
2.6 如何退订数据库安全服务？	6
3 功能类	8
3.1 数据库安全审计可以跨可用区使用吗？	8
3.2 数据库安全审计（旁路模式）是否会影响业务？	8
3.3 数据库安全审计支持多个账号共享使用吗？	8
3.4 数据库安全审计可以应用于哪些场景？	8
3.5 支持的数据库类型	9
3.6 数据库安全审计支持数据库部署在哪些操作系统上？	10
3.7 数据库安全审计支持双向审计吗？	12
3.8 数据库安全审计可以审计不同 VPC 的数据库吗？	13
3.9 数据库安全审计支持 TLS 连接的应用吗？	13
3.10 数据库安全审计的审计数据可以保存多久？	13
3.11 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？	14
3.12 每天发送告警总条数与每天收到的邮件数是相同的吗？	14

3.13 为什么不能在线预览数据库安全审计报表?	14
3.14 在业务侧使用中间件会影响数据库安全审计功能吗?	14
3.15 DBSS 服务能否对第三方工具执行的 SQL 语句进行捕捉?	15
3.16 DBSS 服务是否支持线下部署?	15
3.17 数据库安全服务实例所属 VPC 是否可以更改?	15
3.18 如何对接 DBSS 服务审计的数据?	15
3.19 云服务首页提示 DBSS 服务预测容量不足如何处理?	17
4 Agent 相关.....	18
4.1 数据库安全审计的 Agent 提供哪些功能?	18
4.2 数据库安全审计的 Agent 可以安装在哪些 Windows 操作系统上?	18
4.3 数据库安全审计的 Agent 可以安装在哪些 Linux 操作系统上?	19
4.4 数据库安全审计 Agent 的进程名称是什么?	21
4.5 (Linux 操作系统) 安装 Agent 时没有安装脚本执行权限, 如何处理?	21
4.6 (Linux 操作系统) 数据库安全审计 Agent 客户端日志保存在哪里?	21
4.7 添加 Agent 时, 在什么场景下需要选择“选择已有 Agent”添加方式?	21
4.8 当数据库安全审计 Agent 的运行状态为“休眠中”时, 如何处理?	22
4.9 待审计的 RDS 如果连接了多台 ECS, 如何部署 Agent?	22
4.10 如何选择数据库安全审计的 Agent 安装节点?	23
4.11 如何运行数据库安全审计 Agent 程序?	24
4.12 如何查看数据库安全审计 Agent 的运行状态?	24
4.13 如何下载数据库安全审计的 Agent?	25
4.14 如何卸载数据库安全审计 Agent 程序?	26
4.15 如何修改 Agent 的 CPU 和内存的阈值?	27
4.16 如何安装 Agent (Linux 操作系统)?	28
4.17 如何安装 Agent (Windows 操作系统)?	30
4.18 如何处理 Agent 与数据库安全审计实例之间通信异常?	34
4.19 Agent 运行时消耗安装节点多少资源?	36
4.20 Agent 安装失败如何处理?	36
4.21 Agent 安装报错“unsupport this Linux version, please check your Linux version with install document!”如何解决?	36
5 操作类.....	38
5.1 如何配置数据库安全审计?	38
5.2 如何关闭数据库 SSL?	39
5.3 如何设置数据库安全审计的 INSERT 审计策略?	39
5.4 如何验证已完成数据库安全审计配置?	40
5.5 如何对所有数据库设置数据库安全审计规则?	40
5.6 如何查看数据库安全审计的版本信息?	40
5.7 如何查看数据库安全审计所有的告警信息?	41
5.8 PC 通过内网访问 RDS (即应用端在云下) 时, 如何使用数据库安全审计?	41
6 故障排查.....	42
6.1 数据库安全审计运行正常但无审计记录.....	42
6.2 无法使用数据库安全审计.....	44

6.3 告警邮件异常.....	46
6.4 无法进入数据库安全服务购买页.....	47
6.5 数据库安全服务实例审计 Postgres 的 RDS 数据库没有审计数据怎么办?	48
6.6 数据库安全服务自动备份失败, 失败码: Export backup file failed。.....	48
7 日志类.....	49
7.1 数据库安全审计的操作日志是否可以迁移?	49
7.2 数据库安全审计的操作日志默认保存多久?	49
7.3 如何查看数据库安全审计的用户操作日志?	49
7.4 数据库安全审计的日志处理机制是什么?	50
7.5 数据库安全审计的审计日志是否支持备份?	50
7.6 数据库安全审计的审计日志支持直接转存 OBS 吗?	52
7.7 备份时持续显示“正在上传备份文件”	52
A 修订记录.....	53

1 产品咨询类

1.1 什么是数据库安全审计？

数据库安全服务（Database Security Service，DBSS）是一个智能的数据库安全服务，基于大数据分析技术，提供数据库审计，SQL注入攻击检测，风险操作识别等功能，保障云上数据库的安全。

数据库安全审计提供旁路模式数据库安全审计功能，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。

1.2 数据库安全审计和 RDS SQL 审计有什么区别？

DBSS审计和RDS SQL审计存在功能和范围上的差异，如表1-1所示。

表 1-1 差异比较

审计	功能	范围
RDS SQL 审计	只记录SQL访问操作。	应用于使用RDS数据库场景。
DBSS审计	审计所有的数据库风险操作。在记录SQL访问的基础上进行安全检测、统计分析、风险识别、生成报表等功能，保障云上数据库的安全。	应用于所有数据库场景，包括用户自建数据库。

1.3 数据库安全服务支持哪些性能规格？

数据库安全服务支持专业版和高级版两种服务版本。您可以根据业务需求选择相应的服务版本。

数据库安全审计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
专业版	最多支持6个数据库实例	<ul style="list-style-type: none">• CPU: 8U• 内存: 32GB• 硬盘: 1000GB	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• CPU: 16U• 内存: 64GB• 硬盘: 2000GB	<ul style="list-style-type: none">• 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

1.4 数据库安全服务可以对华为云上的哪些数据库提供保护？

数据库安全服务可以对相同虚拟私有云及其子网下的ECS自建数据库、BMS自建数据库以及RDS关系型数据库提供保护。在非同一虚拟私有云及其子网下的ECS自建数据库、BMS自建数据库和RDS关系型数据库，由于网络限制的原因不能对其提供保护。

1.5 数据库安全服务支持哪些类型的数据库？

数据库安全服务支持华为云的以下数据库：

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

1.6 为什么购买实例后不能马上查看创建中的实例？

购买数据库安全审计时，由于数据库安全审计实例所在的虚拟机创建系统盘和网络配置需要少许时间，所以需要在虚拟机配置完成才能查看创建中的实例。

1.7 数据库安全服务到期后不续费会影响业务吗？

购买的数据库安全服务到期后，如果未续费，您将不能使用数据库安全服务，不影响您的业务。为了数据库安全和资产安全，建议您续费使用数据库安全服务。

1.8 数据库安全审计是否支持审计云下数据库和非华为云上数据库？

数据库安全审计暂不支持审计云下数据库和非华为云上数据库，支持对云上的以下数据库提供旁路模式的数据库审计功能：

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

数据库安全审计支持的数据库类型及版本，请参见：[数据库安全审计支持哪些数据库？](#)。

1.9 什么是区域和可用区？

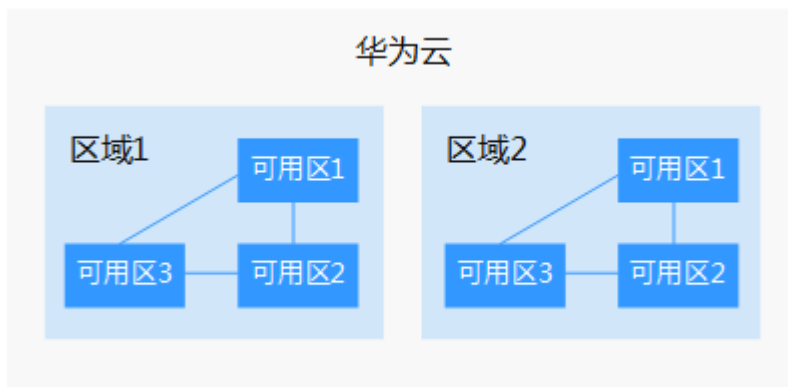
什么是区域、可用区？

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ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。

[图1-1](#)阐明了区域和可用区之间的关系。

图 1-1 区域和可用区



目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

如何选择区域？

选择区域时，您需要考虑以下几个因素：

- 地理位置
 - 一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。
 - 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。

- 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
- 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。
- 资源的价格
不同区域的资源价格可能有差异，请参见[华为云服务价格详情](#)。

如何选择可用区？

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参见[地区和终端节点](#)。

1.10 数据库安全服务是否支持数据实时脱敏？

暂不支持实时脱敏。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，来防止数据库用户敏感信息泄露。详情请参见[配置隐私数据保护规则](#)。

1.11 购买 DBSS 服务后添加的数据库不在同一子网有什么影响？

购买DBSS服务后添加的多个数据库不在同一子网，但只要在同一VPC，添加的所有数据库可进行正常审计，不受子网影响。

2 购买类

2.1 购买实例时如何选择“子网”？

需要选择与数据库同一VPC的子网。

2.2 购买实例时为何要选择 VPC？

对于非云上的数据库，Agent和DBSS实例之间的网络需要通过VPC互通。DBSS实例的VPC和安装Agent的节点如果在不同VPC，将导致无法审计。

2.3 同一区域可以购买多少个数据库安全审计实例？

- 基础版：最多支持3个数据库实例。
- 专业版：最多支持6个数据库实例。
- 高级版：最多支持30个数据库实例。

2.4 购买实例时提示配额不足时如何处理？

当您在购买数据库安全审计时，界面提示配额不足，请您提交工单申请配额。

提交工单的详细操作，请参见：[提交工单](#)。

2.5 如何为数据库安全审计续费？


在数据库安全审计到期前，用户可以通过续费操作继续使用数据库安全服务。


前提条件

- 登录管理控制台的账号已授权DBSS System Administrator、ECS Administrator、VPC Administrator和DBSS Administrator权限策略，或授权Tenant Administrator权限策略。
- 已成功购买数据库安全审计实例。

数据库安全审计续费

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击 ，选择“安全与合规 > 数据库安全服务”，进入数据库安全审计“总览”界面。

步骤4 在左侧导航树中，选择“实例列表”。

步骤5 在需要续费的实例所在行中，单击“续费”。

有关续费的详细操作，请参见[续费管理](#)。

----结束

2.6 如何退订数据库安全服务？

数据库安全服务仅支持包年/包月付费方式，购买的实例不能直接删除，不支持修改规格，仅支持退订。

系统影响

执行退订操作后，将清除实例的审计记录和日志。已经备份到OBS桶中的审计日志不会清除。

前提条件

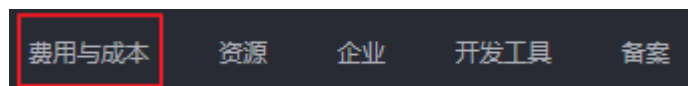
- 登录管理控制台的账号已授权DBSS System Administrator、ECS Administrator、VPC Administrator和BSS Administrator角色。
- 已成功购买数据库安全审计实例。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 在界面右上方，单击“费用与成本”，进入“费用中心”界面。

图 2-1 费用与成本



步骤3 在左侧导航树上，选择“订单管理 > 退订与退换货”。

有关退订的详细操作，请参见[退订管理](#)。退订后可重新购买，请参见[购买数据库安全审计](#)。

图 2-2 退订与退换货



----结束

3 功能类

3.1 数据库安全审计可以跨可用区使用吗？

待审计的数据库和购买的数据库安全审计实例必须在同一区域，您才能使用数据库安全审计。如果待审计的数据库和购买的数据库安全审计实例在同一区域，但不在同一可用区，则您可以使用数据库安全审计。

例如，您在某个区域的“可用区1”购买了数据库安全审计，待审计的数据库部署在该区域的“可用区2”或“可用区3”，则您可以使用购买的数据库安全审计。

3.2 数据库安全审计（旁路模式）是否会影响业务？

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

3.3 数据库安全审计支持多个账号共享使用吗？

数据库安全审计不支持多个账号共享使用。例如，如果您在某个区域通过注册华为云创建了2个账号（“domain1”和“domain2”），当您在“domain1”账号下购买了数据库安全审计，则“domain2”账号不能使用“domain1”的数据库安全审计。

在同一区域，一个账号的在IAM上创建的所有IAM用户都可以共用该账号下的数据库安全审计。例如，您在某个区域通过注册华为云创建了1个账号（“domain1”），且“domain1”账号在IAM中创建了2个IAM用户（“sub-user01”、“sub-user02”），如果您授权了“sub-user01”和“sub-user02”用户DBSS的权限策略，则这2个IAM用户都可以使用“domain1”的数据库安全审计。

3.4 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前提下，可以对华为云上的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。
- 提供审计报告模板库，可以生成日报、周报或月报审计报告（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告。

3.5 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3-1所示。

表 3-1 数据库安全审计支持的数据库类型和版本

数据库类型	版本
MySQL	<ul style="list-style-type: none"> • 5.0、5.1、5.5、5.6、5.7 • 8.0（8.0.11及以前的子版本） • 8.0.20 • 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)	<ul style="list-style-type: none"> • 11g 11.1.0.6.0、11.2.0.1.0、11.2.0.2.0、11.2.0.3.0、11.2.0.4.0 • 12c 12.1.0.2.0、12.2.0.1.0 • 19c
PostgreSQL	<ul style="list-style-type: none"> • 7.4 • 8.0 8.0、8.1、8.2、8.3、8.4 • 9.0 9.0、9.1、9.2、9.3、9.4、9.5、9.6 • 10.0 10.0、10.1、10.2、10.3、10.4、10.5 • 11.0 • 12.0 • 13.0 • 14.0
SQL Server	<ul style="list-style-type: none"> • 2008、2008R2 • 2012 • 2014 • 2016 • 2017
DWS	<ul style="list-style-type: none"> • 1.5 • 8.1

数据库类型	版本
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0
Greenplum	V6.0
HighGo	V6.0
GaussDB(for MYSQL)	MySQL 8.0
GaussDB	1.4企业版
DAMENG	DM8
KINGBASE	V8
MongoDB	V5.0
DDS	4.0
Hbase (华为云审计实例: 23.02.27.182148 及其之后的版本支持)	1.3.1 2.2.3
Hive	1.2.2 2.3.9 3.1.2 3.1.3

3.6 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3-2](#)所示。

表 3-2 Agent 支持的 Linux 系统版本说明

系统名称	系统版本
CentOS	<ul style="list-style-type: none"> ● CentOS 7.0 (64bit) ● CentOS 7.1 (64bit) ● CentOS 7.2 (64bit) ● CentOS 7.3 (64bit) ● CentOS 7.4 (64bit) ● CentOS 7.5 (64bit) ● CentOS 7.6 (64bit) ● CentOS 7.8 (64bit) ● CentOS 7.9 (64bit) ● CentOS 8.0 (64bit) ● CentOS 8.1 (64bit) ● CentOS 8.2 (64bit)
Debian	<ul style="list-style-type: none"> ● Debian 7.5.0 (64bit) ● Debian 8.2.0 (64bit) ● Debian 8.8.0 (64bit) ● Debian 9.0.0 (64bit) ● Debian 10.0.0 (64bit)
Fedora	<ul style="list-style-type: none"> ● Fedora 24 (64bit) ● Fedora 25 (64bit) ● Fedora 29 (64bit) ● Fedora 30 (64bit)
OpenSUSE	<ul style="list-style-type: none"> ● SUSE 13 (64bit) ● SUSE 15 (64bit) ● SUSE 42 (64bit)
SUSE	<ul style="list-style-type: none"> ● SUSE 11 SP4 (64bit) ● SUSE 12 SP1 (64bit) ● SUSE 12 SP2 (64bit)
Ubuntu	<ul style="list-style-type: none"> ● Ubuntu 14.04 (64bit) ● Ubuntu 16.04 (64bit) ● Ubuntu 18.04 (64bit) ● Ubuntu 20.04 (64bit)
EulerOS	<ul style="list-style-type: none"> ● Euler 2.2 (64bit) ● Euler 2.3 (64bit) ● Euler 2.5 (64bit)

系统名称	系统版本
OpenEuler	<ul style="list-style-type: none"> OpenEuler 20.03 (64bit)
Oracle Linux	<ul style="list-style-type: none"> Oracle Linux 6.9 (64bit) Oracle Linux 7.4 (64bit)
Red Hat	<ul style="list-style-type: none"> Red Hat Enterprise Linux 7.4 (64bit) Red Hat Enterprise Linux 7.6 (64bit)
NeoKylin	<ul style="list-style-type: none"> NeoKylin 7.0 (64bit)
Kylin	<ul style="list-style-type: none"> Kylin Linux Advanced Server release V10 (64bit)
Uniontech OS	<ul style="list-style-type: none"> Uniontech OS Server 20 Enterprise (64bit)
Huawei Cloud Euler	<ul style="list-style-type: none"> Huawei Cloud Euler 2.0 (64bit)
KylinSec	<ul style="list-style-type: none"> KylinSec 3.4 (64bit)

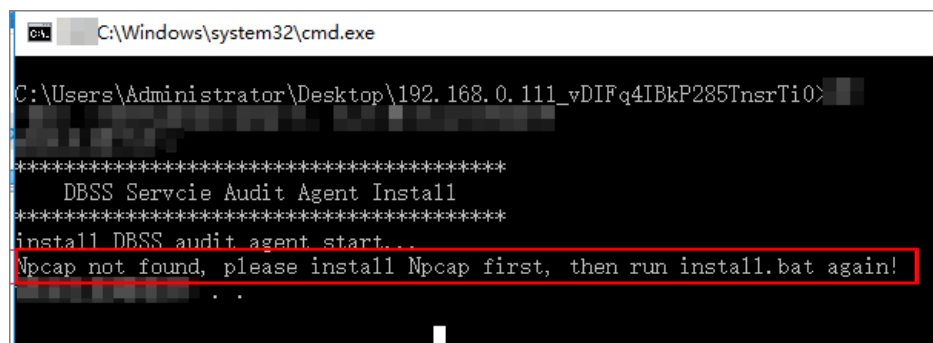
- 数据库安全审计的Agent支持的Windows系统版本如下所示：
 - Windows Server 2008 R2(64bit)
 - Windows Server 2012 R2(64bit)
 - Windows Server 2016(64bit)
 - Windows Server 2019(64bit)
 - Windows 7(64bit)
 - Windows 10(64bit)

📖 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 3-1 Npcap not found



3.7 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。

3.8 数据库安全审计可以审计不同 VPC 的数据库吗？

数据库安全审计支持审计不同VPC的数据库。当您需要审计不同VPC的数据库时，需要VPC互相通信，可以通过在VPC间建立对等连接的方式实现。请参考[创建同一账户下的对等连接](#)进行配置。

3.9 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。

3.10 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。未开启备份时，存储在审计实例上，原则上保存时间为180天，这取决于日志量大小。如果日志量较大，会以滚动删除的方式删除存放时间最久的日志以保证磁盘空间使用率。开启备份时，会同时保存在obs桶里，此时保存的时间会对应着obs存储的时间。

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

- 根据业务数据库审计数据实际情况，选择购买的数据库安全审计版本
 - 审计数据容量较小：购买基础版
 - 审计数据容量较大：购买专业版或高级版
 数据库安全审计各版本的规格说明如所[表3-3](#)示。
- 备份审计日志

有关备份审计日志的详细操作，请参见[备份数据库审计日志](#)。

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	<ul style="list-style-type: none"> ● CPU：8U ● 内存：32GB ● 硬盘：1000GB 	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● CPU：16U ● 内存：64GB ● 硬盘：2000GB 	<ul style="list-style-type: none"> ● 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IP₁和IP₂，IP₁有一个数据库端口，则为1个数据库实例；IP₂有3个数据库端口，则为3个数据库实例。IP₁和IP₂合计为4个数据库实例，选择服务版本规格时需要大于或等于4个数据库实例，即选用专业版（最多支持审计6个数据库实例）。
- 不支持修改规格。若要修改，请退订后重购。
- 云原生版仅支持在RDS控制台购买。
- 本表中的系统资源要求，是指购买数据库安全审计实例时会消耗的系统资源。购买时，用户的系统需要满足审计版本对应的配置。
- 本表中在线SQL语句的条数，是按照每条SQL语句的容量为1KB来计算的。

3.11 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。

3.12 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。

3.13 为什么不能在线预览数据库安全审计报告？

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

3.14 在业务侧使用中间件会影响数据库安全审计功能吗？

不会影响使用数据库安全审计。

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

数据库安全审计采用旁路模式部署，通过Agent（数据库节点或应用节点安装Agent）获取访问数据库流量、将流量数据上传到审计系统、接收审计系统配置命令和上报数据库状态监控数据，从而实现数据库安全审计功能。

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

如果您的数据库安全审计没有审计数据，请参见以下内容进行排查：

- [无法使用数据库安全审计。](#)
- [数据库安全审计运行正常但无审计记录。](#)

3.15 DBSS 服务能否对第三方工具执行的 SQL 语句进行捕捉？

可以。DBSS服务审计的数据是Agent接入的全量日志和流量数据，与工具无关。

3.16 DBSS 服务是否支持线下部署？

不支持。数据库安全服务需要部署在您所使用的云上的服务器中，您需要将相关的业务迁移至目标云上。

3.17 数据库安全服务实例所属 VPC 是否可以更改？

不可以。实例所属的VPC是由私网网段、路由表和至少一个子网组成，拥有独立的安全组和网络ACL来保障云资源安全，详情请参见[什么是虚拟私有云](#)。

若有VPC的变更需求，可通过申请退订变更或[提交工单](#)提交工单申请VPC对接：

- 退订变更：对想要变更的VPC对应实例参照[如何退订数据库安全服务？](#)进行退订，退订后在目标VPC重新[购买数据库安全审计](#)（建议）。
- VPC对接：通过[提交工单](#)提交工单申请目标VPC人工对接。


3.18 如何对接 DBSS 服务审计的数据？

您可在数据库安全服务中开启自动备份，将审计数据备份至OBS桶。

📖 说明

自动备份前，您需要完成OBS细粒度授权，详情请参见[备份和恢复审计日志](#)。

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3-4](#)所示。

图 3-2 “设置自动备份”对话框

设置自动备份

1. 审计日志将备份到对象存储服务的OBS桶中，OBS桶按照存储用量收费，由对象存储服务结算。
2. 开启自动备份，请先选择OBS桶作为审计日志备份桶，DBSS服务将获取该桶的读写权限。

自动备份

备份周期

开始时间

桶名称 C 跳转到该桶 | 创建默认桶

可选择已有OBS桶或默认桶，默认桶不存在时将被自动创建
 OBS服务默认使用按需计费模式，不同区域及计费项产生费用不同。 [了解计费详情](#)

文件导出目录

自动备份授权 同意DBSS服务获取该OBS桶读写权限，用于审计日志备份导出
注：授权成功后预计15分钟，自动备份才会生效

取消
确定

表 3-4 自动备份参数说明

参数名称	说明	取值样例
自动备份	开启或关闭自动备份。 <ul style="list-style-type: none"> ● : 开启 ● : 关闭 	
备份周期	选择自动备份的周期，可以选择： <ul style="list-style-type: none"> ● 每天 ● 每小时 	每天
开始时间	单击 ，选择开始备份的时间。	2020/01/14 20:27:08
桶名称	设置备份使用的OBS桶名称，可以选择： <ul style="list-style-type: none"> ● 创建默认桶 ● 选择已有桶 说明 <ul style="list-style-type: none"> ● 单击“创建默认桶”，将进行OBS授权，用于审计日志备份导出。 ● 审计日志只能导出到DBSS服务创建的桶。 	20f18-7a5a-4042
文件导出目录	在OBS桶中创建备份文件的目录。	test

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

开启备份后通过对接OBS桶的接口实现对接数据库安全服务的审计数据，详情请参见OBS的[API概览](#)。

3.19 云服务首页提示 DBSS 服务预测容量不足如何处理？

DBSS实例磁盘不支持单独扩容，磁盘容量预测无法满足保存至少180天日志的合规要求时，需要进行备份。

此告警为提醒用户实例磁盘使用阈值较高，建议按小时备份。如果已开启了备份，则可忽略该告警。

4 Agent 相关

4.1 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 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：

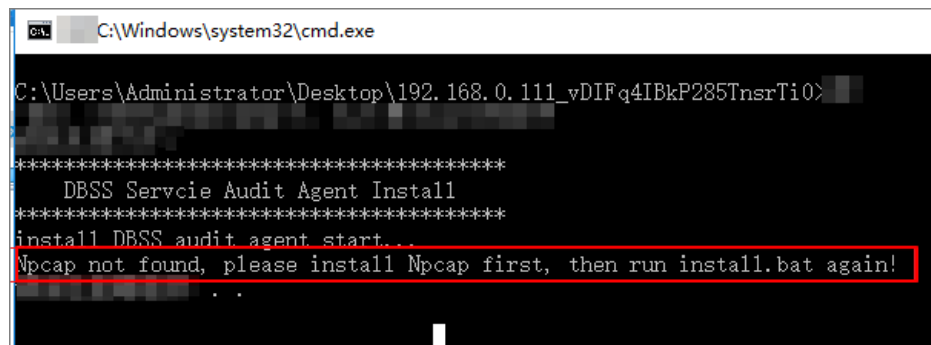
- Windows Server 2008 R2(64bit)
- Windows Server 2012 R2(64bit)
- Windows Server 2016(64bit)
- Windows Server 2019(64bit)
- Windows 7(64bit)
- Windows 10(64bit)

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



4.3 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4-1所示。

表 4-1 Agent 支持的 Linux 系统版本说明

系统名称	系统版本
CentOS	<ul style="list-style-type: none"> ● CentOS 7.0 (64bit) ● CentOS 7.1 (64bit) ● CentOS 7.2 (64bit) ● CentOS 7.3 (64bit) ● CentOS 7.4 (64bit) ● CentOS 7.5 (64bit) ● CentOS 7.6 (64bit) ● CentOS 7.8 (64bit) ● CentOS 7.9 (64bit) ● CentOS 8.0 (64bit) ● CentOS 8.1 (64bit) ● CentOS 8.2 (64bit)

系统名称	系统版本
Debian	<ul style="list-style-type: none"> • Debian 7.5.0 (64bit) • Debian 8.2.0 (64bit) • Debian 8.8.0 (64bit) • Debian 9.0.0 (64bit) • Debian 10.0.0 (64bit)
Fedora	<ul style="list-style-type: none"> • Fedora 24 (64bit) • Fedora 25 (64bit) • Fedora 29 (64bit) • Fedora 30 (64bit)
OpenSUSE	<ul style="list-style-type: none"> • SUSE 13 (64bit) • SUSE 15 (64bit) • SUSE 42 (64bit)
SUSE	<ul style="list-style-type: none"> • SUSE 11 SP4 (64bit) • SUSE 12 SP1 (64bit) • SUSE 12 SP2 (64bit)
Ubuntu	<ul style="list-style-type: none"> • Ubuntu 14.04 (64bit) • Ubuntu 16.04 (64bit) • Ubuntu 18.04 (64bit) • Ubuntu 20.04 (64bit)
EulerOS	<ul style="list-style-type: none"> • Euler 2.2 (64bit) • Euler 2.3 (64bit) • Euler 2.5 (64bit)
OpenEuler	<ul style="list-style-type: none"> • OpenEuler 20.03 (64bit)
Oracle Linux	<ul style="list-style-type: none"> • Oracle Linux 6.9 (64bit) • Oracle Linux 7.4 (64bit)
Red Hat	<ul style="list-style-type: none"> • Red Hat Enterprise Linux 7.4 (64bit) • Red Hat Enterprise Linux 7.6 (64bit)
Neokylin	<ul style="list-style-type: none"> • Neokylin 7.0 (64bit)
Kylin	<ul style="list-style-type: none"> • Kylin Linux Advanced Server release V10 (64bit)
Uniontech OS	<ul style="list-style-type: none"> • Uniontech OS Server 20 Enterprise (64bit)
Huawei Cloud Euler	<ul style="list-style-type: none"> • Huawei Cloud Euler 2.0 (64bit)
KylinSec	<ul style="list-style-type: none"> • KylinSec 3.4 (64bit)

4.4 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”。

4.5 （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
```

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

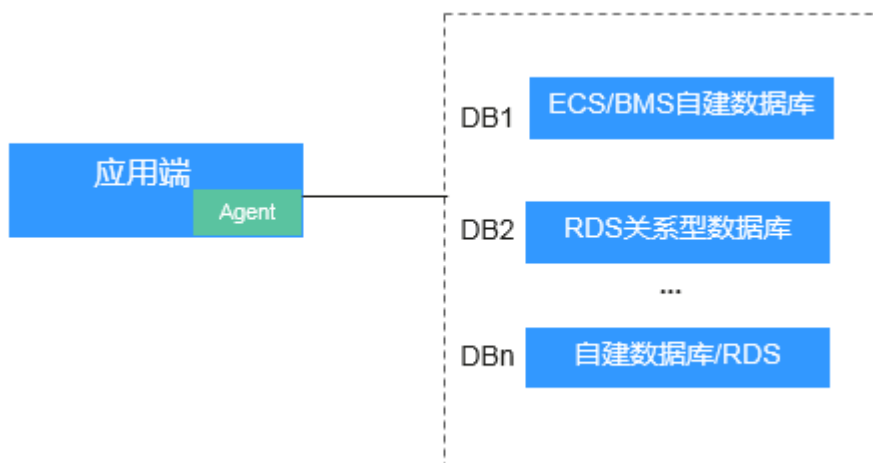
Agent客户端日志存放路径为：“/opt/dbss_audit_agent/log/audit_agent.log”

4.7 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4-2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。有关安装节点的详细介绍，请参见[如何选择数据库安全审计的Agent安装节点？](#)。

图 4-2 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

4.8 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”。

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。

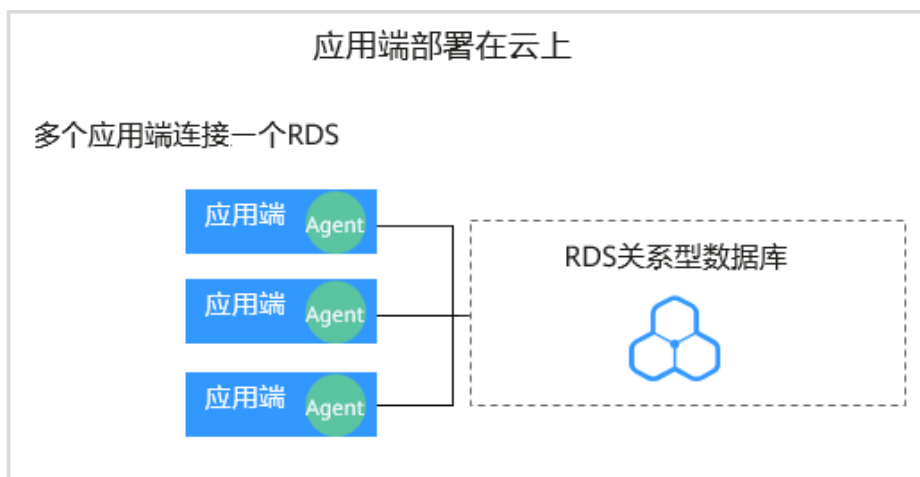
请您安装Agent后，再查看该Agent的运行状态。有关安装Agent的详细操作，请参见[安装Agent](#)。

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

4.9 待审计的 RDS 如果连接了多台 ECS，如何部署 Agent？

当待审计的RDS连接了多台ECS，即多个应用端（ECS）连接同一个RDS时，所有的应用端都需要部署Agent，如[图4-3](#)所示。

图 4-3 多个应用端连接同一个 RDS



在完成添加数据库操作后，请您参照以下步骤部署Agent：

1. 添加Agent。
所有连接RDS的ECS都需要添加Agent。
有关添加Agent的详细操作，请参见[添加Agent](#)。
2. 安装Agent。
下载Agent后，需要在所有连接RDS的ECS上安装Agent。
有关安装Agent的详细操作，请参见[安装Agent](#)。

4.10 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4-2](#)所示。有关安装Agent的详细操作，请参见[安装Agent](#)。

表 4-2 数据库安全审计 Agent 安装说明

Agent安装节点	使用场景	审计功能说明	注意事项
数据库端	ECS/BMS自建数据库	可以审计所有访问该数据库的应用端的所有访问记录。	添加Agent时，“安装节点类型”选择“数据库端”。
应用端	无法登录到数据库节点的部署环境（例如，RDS关系型数据库）	可以审计该应用端与其连接的所有数据库的访问记录。	<ul style="list-style-type: none"> • 添加Agent时，“安装节点类型”选择“应用端”。 • 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。

Agent安装节点	使用场景	审计功能说明	注意事项
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
- 应用端

须知

当某个应用端连接了多个数据库时，如果该应用端的一个数据库已经在应用端添加了Agent。其他数据库在添加Agent时，只需要选择“选择已有Agent”添加方式。详细介绍，请参见[添加Agent时，在什么场景下需要选择“选择已有Agent”添加方式？](#)。

- 代理端

须知

安装节点IP需要配置为代理的IP地址。

4.11 如何运行数据库安全审计 Agent 程序？

成功添加数据库且开启审计后，请参照以下操作步骤，运行Agent程序。

步骤1 [登录管理控制台](#)。

步骤2 在“选择实例”下拉列表框中，选择需要运行的数据库实例。

步骤3 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”，将Agent安装包下载到本地。

步骤4 安装Agent。

有关安装Agent的详细操作，请参见[安装Agent](#)。

----结束

4.12 如何查看数据库安全审计 Agent 的运行状态？

安装节点安装Agent程序后，请参照以下操作步骤，查看Agent程序的运行状态。Agent程序的运行状态如[表4-3](#)所示。

Linux 操作系统

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，查看Agent程序的运行状态。

```
service audit_agent status
```

如果界面回显以下信息，说明Agent程序运行正常。

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

----结束

Windows 操作系统

步骤1 进入Agent安装文件的目录。

步骤2 双击“status.bat”执行文件，查看Agent的运行状态。

----结束

表 4-3 Agent 运行状态

状态	说明
正在运行	该安装节点的Agent程序正在运行。
已关闭	该安装节点的Agent程序已关闭。单击右侧操作栏的“开启”，可运行该Agent。 说明 Agent程序在CPU占用过高时将休眠，运行状态显示“已关闭”。请检查CPU使用率是否超过Agent配置的CPU阈值，更改阈值或扩容内存以解决该问题。Agent程序将在CPU使用率低于阈值后自动重启。
休眠中	添加Agent后，Agent的初始运行状态为“休眠中”。 如需更改状态，请参考 当数据库安全审计Agent的运行状态为“休眠中”时，如何处理？ 。

4.13 如何下载数据库安全审计的 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](#)。

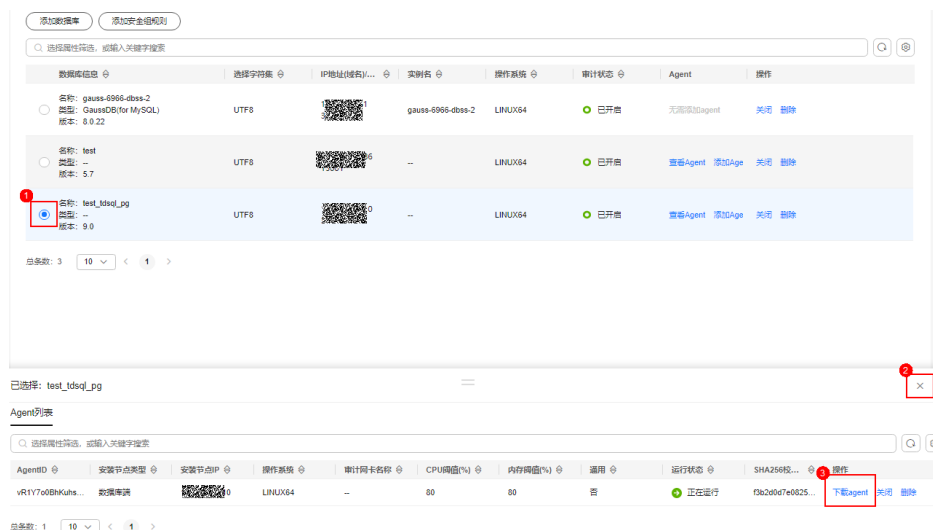
步骤2 在页面上方选择“区域”后，单击页面左上方的 ，选择“安全与合规 > 数据库安全服务”，进入数据库安全审计“总览”界面。

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 4-4 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

4.14 如何卸载数据库安全审计 Agent 程序？

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

前提条件

已在安装节点安装了Agent程序。

在 Linux 操作系统上卸载 Agent

步骤1 使用跨平台远程访问工具（例如PuTTY）以root用户通过SSH方式，登录已安装Agent的节点。

步骤2 执行以下命令，进入Agent安装包“xxx.tar.gz”解压后所在目录。

```
cd Agent安装包解压后所在目录
```

步骤3 执行以下命令，查看是否有卸载脚本“uninstall.sh”的执行权限。

```
ll
```

- 如果有卸载脚本的执行权限，请执行**步骤4**。
- 如果没有卸载脚本的执行权限，请执行以下操作：
 - a. 执行以下命令，添加卸载脚本执行权限。

```
chmod +x uninstall.sh
```
 - b. 确认有安装脚本执行权限后，请执行**步骤4**。

步骤4 执行以下命令，卸载Agent。

```
sh uninstall.sh
```

如果界面回显以下信息，说明卸载成功。

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

----结束

在 Windows 操作系统上卸载 Agent

步骤1 进入Agent安装文件的目录。

步骤2 双击“uninstall.bat”执行文件，卸载Agent。

步骤3 验证Agent已卸载成功。

1. 打开任务管理器，查看“dbss_audit_agent”进程已停止。
2. 查看Agent安装目录，安装目录内容已经全部删除。

----结束

4.15 如何修改 Agent 的 CPU 和内存的阈值？

数据库安全审计Agent的CPU阈值和内存阈值用户不能直接修改：

- Agent安装在数据库端的用户，若有需求，请您联系技术支持修改数据库安全审计Agent的阈值。

- Agent安装在应用端的用户，您可以按照以下操作步骤在添加Agent时，配置CPU阈值和内存阈值。

步骤1 登录安装Agent的节点，[卸载Agent程序](#)。

步骤2 登录数据库安全服务控制台。

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。

步骤4 在“选择实例”下拉框中，选择需要修改AgentCPU阈值和内存阈值的实例。

步骤5 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，如[图4-5](#)所示，删除已添加的Agent。

图 4-5 删除 Agent

序号	数据库信息	选择字符集	IP地址/端口	实例名	操作系统	审计状态	Agent	操作
1	名称: tesT 类型: MYSQL 版本: 5.7	UTF8	192.168.0.104 3306	--	LINUX64	已开启	添加Agent	关闭 删除

AgentID	安装节点类型	安装节点IP	操作系统	审计网卡名称	CPU阈值(%)	内存阈值(%)	通用	运行状态	操作
AXRTayECzoA3BGe6TH2A	应用端	192.168.0.131	LINUX64	--	80	80	否	正在运行	下载Agent 关闭 删除

步骤6 重新[添加Agent](#)。请根据您的业务需求，设置CPU阈值和内存阈值。

CPU阈值和内存阈值系统默认为80%。当Agent程序检测到服务器上的内存或CPU超过设定的阈值时，Agent将立即停止运行。

步骤7 [下载Agent](#)。

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。重新添加Agent后，必须重新下载和安装Agent。

步骤8 [安装Agent（Linux操作系统）](#)或[安装Agent（Windows操作系统）](#)。

----结束

4.16 如何安装 Agent（Linux 操作系统）？

安装Agent后，您才能开启数据库安全审计功能，对待审计的数据库进行审计。

本节介绍如何在Linux系统上安装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。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？](#)。

安装 Agent

📖 说明

在您安装新版Agent的时候，需要您为当前安装的Agent自定义一个密码。

请您根据数据库类型以及数据库的部署环境，在相应节点上安装Agent。

- 步骤1** 将下载的Agent安装包“xxx.tar.gz”上传到待安装Agent的节点（例如使用WinSCP工具）。
- 步骤2** 使用跨平台远程访问工具（例如PuTTY）以root用户通过SSH方式，登录该节点。
- 步骤3** 执行以下命令，进入Agent安装包“xxx.tar.gz”所在目录。

cd Agent安装包所在目录

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

- 步骤4** 执行以下命令，解压缩“xxx.tar.gz”安装包。

tar -xvf xxx.tar.gz

```
[root@ecs-test agent]#  
[root@ecs-test agent]# tar -xvf _9syBZIsBbeAhEFqE_hhD.tar.gz
```

- 步骤5** 执行以下命令，进入解压后的目录。

cd 解压后的目录

```
root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]#  
root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]#  
root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]# chmod +x install.sh  
root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]#  
root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]# ll  
total 36  
drwxr-xr-x 2 root root 4096 Oct 25 09:50 bin  
drwxr-xr-x 2 root root 4096 Oct 25 09:50 boot  
drwxr-xr-x 2 root root 4096 Oct 25 09:50 cert  
drwxr-xr-x 2 root root 4096 Oct 25 09:50 conf  
drwxr-xr-x 2 root root 4096 Oct 25 09:50 crond  
-rwxr-xr-x 1 root root 527 Oct 25 09:45 install.sh  
drwxr-xr-x 2 root root 4096 Oct 25 09:50 lib  
-rw-r--r-- 1 root root 308 Oct 25 09:45 uninstall.sh  
drwxr-xr-x 2 root root 4096 Oct 25 09:50 utils  
root@ecs-test 192.168.0.107_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 192.168.0.107_9syBZIsBbeAhEFqE_hhD]#  
[root@ecs-test 192.168.0.107_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Ubuntu时，执行以下命令安装Agent：**bash install.sh**
- Agent程序是以DBSS普通用户运行的，在首次安装Agent时，需要创建Agent用户，执行sh install.sh命令后，需要您自行设置DBSS用户的密码。

界面回显以下信息，说明安装成功。否则，说明Agent安装失败。

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

须知

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

步骤8 执行以下命令，查看Agent程序的运行状态。

```
service audit_agent status
```

如果界面回显以下信息，说明Agent程序运行正常。

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

----结束

4.17 如何安装 Agent（Windows 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，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。

安装Agent后，您才能开启数据库安全审计功能，对待审计的数据库进行审计。

本节介绍如何在Windows操作系统上安装Agent。

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。

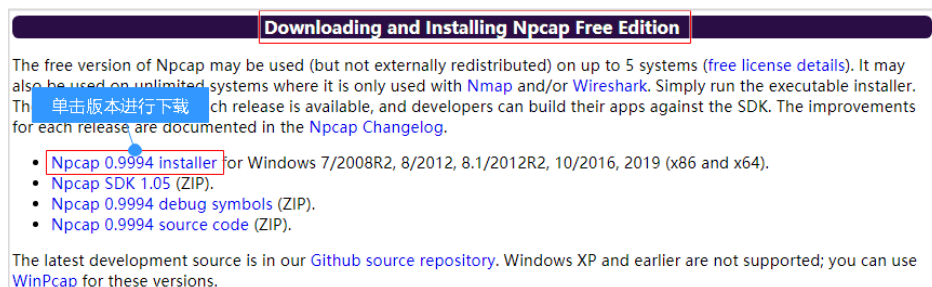
安装 Agent

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：

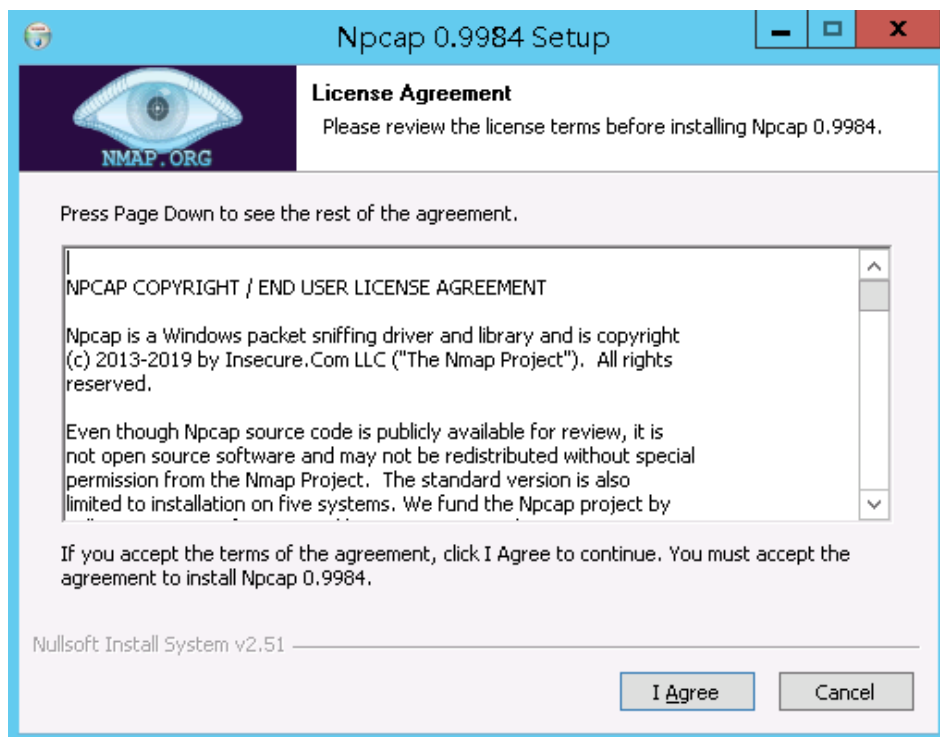
- a. 请前往<https://nmap.org/npcap/>下载Npcap最新软件安装包。

图 4-6 下载 npcap



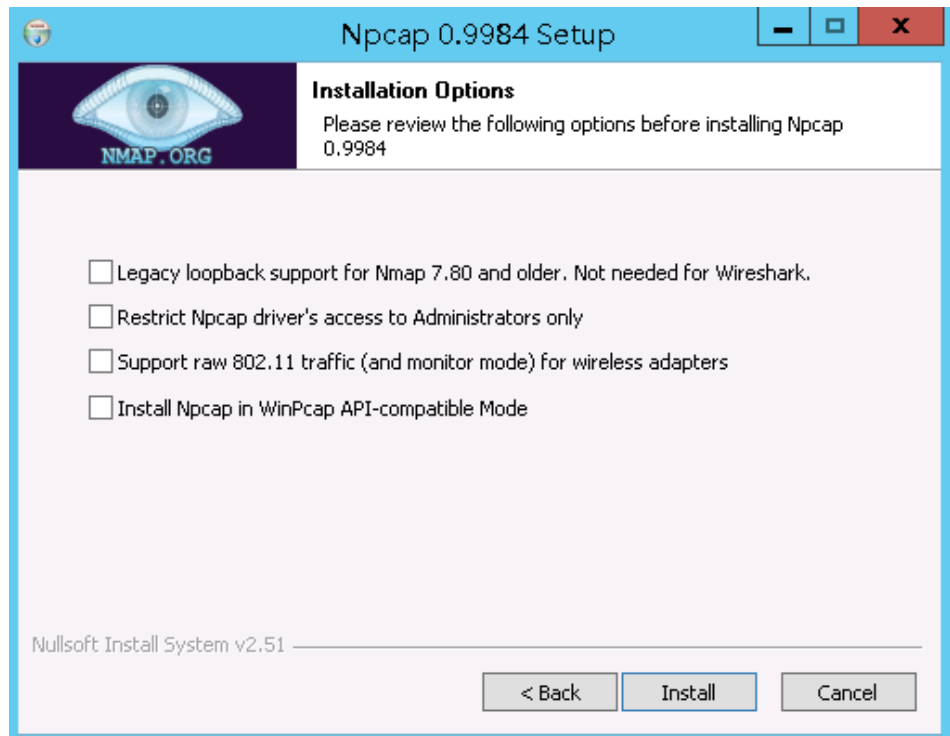
- b. 将下载好的npcap-xxxx.exe软件安装包上传至需要安装agent的虚拟机。
c. 双击npcap软件安装包。
d. 在弹出的对话框中，单击“I Agree”，如图4-7所示。

图 4-7 同意安装“Npcap”

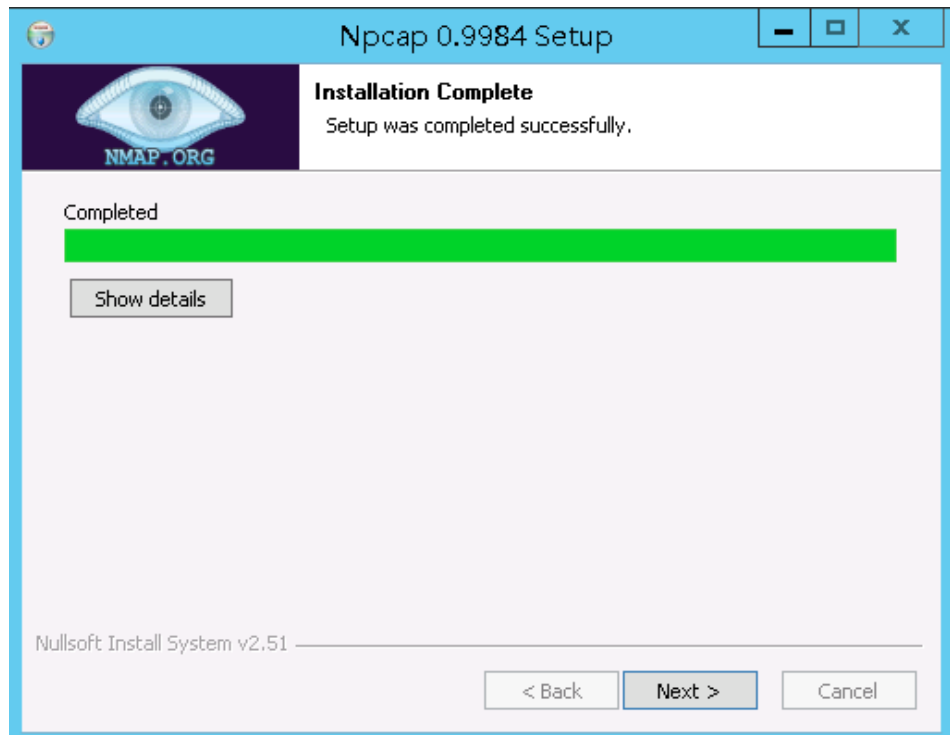


- e. 在弹出的对话框中，单击“Install”，不勾选安装选项，如图4-8所示。

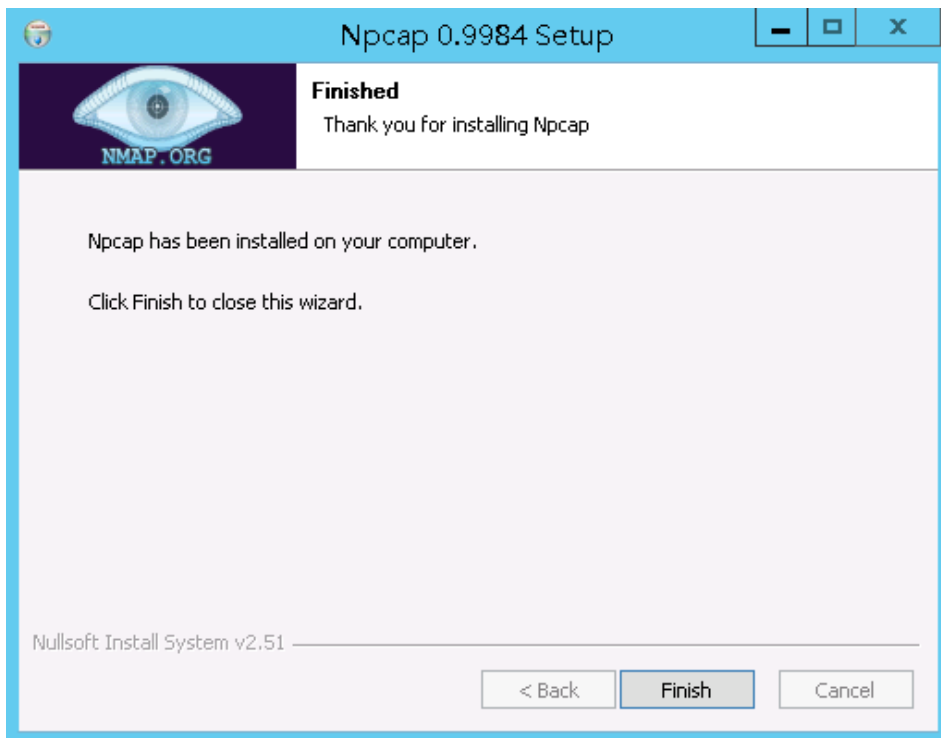
图 4-8 安装 “Npcap”



- 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4-9所示，按任意键结束安装。

图 4-9 Agent 安装成功

```
*****
DBSS Service Audit Agent Install
*****
install DBSS audit agent start...
check npcap existed success
check main process file success
check child process file success
check dll file success
check dll file success
check startup file success
已复制      1 个文件。
已复制      1 个文件。
已复制      1 个文件。
check dbss agent config file success
check log folder success
install DBSS audit agent success
start DBSS audit agent success
请按任意键继续. . .
```

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

4.18 如何处理 Agent 与数据库安全审计实例之间通信异常？

故障现象


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

建议您按照本章节的操作步骤进行处理：

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

检查添加的数据库信息以及审计状态

步骤1 [登录管理控制台](#)。

步骤2 在页面上方选择“区域”后，单击页面左上方的，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，选择需要排查的数据库所属的实例。

步骤5 检查待审计的数据库信息。

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

步骤6 检查待审计的数据库的审计状态。

- 如果“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”。

步骤2 在数据库列表的上方，单击“添加安全组规则”。

步骤3 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4-10](#)所示。

图 4-10 添加安全组规则

添加安全组规则

请在审计实例所在的安全组中开启必要规则，确保网络通信正常。

安全组名称 default


操作详情

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

取消

前往处理

步骤4 单击“前往处理”，进入“安全组”列表界面。

步骤5 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6 单击“default”，进入“入方向规则”页面。

步骤7 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8**。

步骤8 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”。
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。
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。

4.19 Agent 运行时消耗安装节点多少资源？

Agent在运行时消耗一定的系统资源（CPU不超过5%，内存不超过300MB），并有以下两个监控措施：

- 监控系统整体的CPU和内存。当CPU或内存超过设定的阈值（默认80%），Agent将停止运行，不进行流量获取。
- 监控Agent进程本身的CPU和内存。

4.20 Agent 安装失败如何处理？

如果Agent安装失败，请先检查选择的Agent ID是否正确。如果Agent ID设置无误，请按下方指导，先卸载再重装Agent：

- 步骤1 在目标数据库[卸载Agent](#)。
- 步骤2 参照[添加Agent](#)进行重新添加。
- 步骤3 添加后[下载Agent](#)。
- 步骤4 重新[安装Agent（Linux操作系统）](#)或[安装Agent（Windows操作系统）](#)。

----结束

4.21 Agent 安装报错“unsupport this Linux version, please check your Linux version with install document!”如何解决？

由于在[添加Agent](#)时，“安装节点IP”所填写的IP地址为公网IP地址，因此，在下载Agent后进行安装时会报“unsupport this Linux version, please check your Linux version with install document!”的错误信息，您需要对目标Agent进行卸载重装。详细步骤如下：

- 步骤1 在目标数据库[卸载Agent](#)。

步骤2 参照[添加Agent](#)进行重新添加，在“安装节点IP”一栏填写能正常使用的内网IP地址。

步骤3 添加后[下载Agent](#)。

----结束

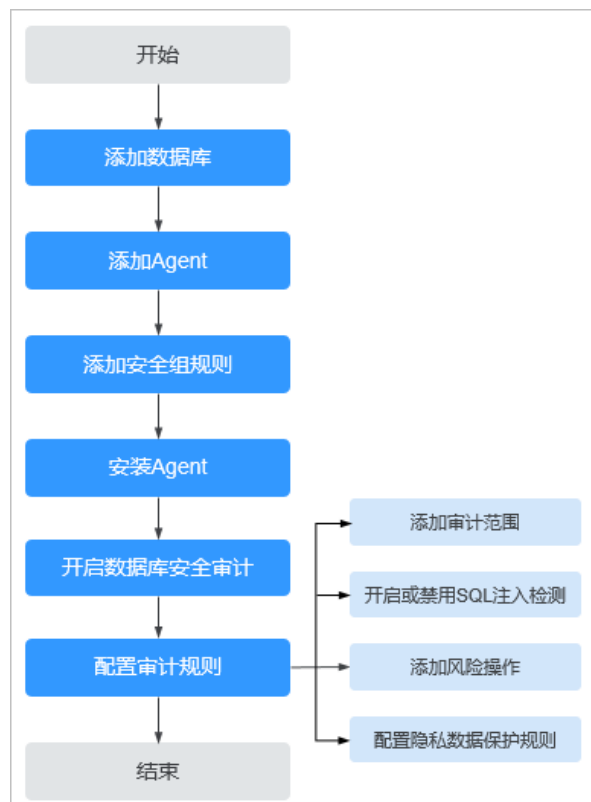
5 操作类

5.1 如何配置数据库安全审计？

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到数据库安全审计实例中，并在数据库端、应用端或代理端安装Agent。当待审计的数据库连接到数据库安全审计实例后，数据库安全审计才能对待审计的数据库进行审计。

数据库安全审计的配置操作流程如图5-1所示。

图 5-1 数据库安全审计配置流程图



5.2 如何关闭数据库 SSL?

操作场景

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

操作步骤

以MySQL数据库自带的客户端为例说明，操作步骤如下：

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

步骤2 执行以下命令，查看MySQL数据库连接的方式。

```
\s
```

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

步骤3 以SSL模式登录MySQL数据库。

1. 执行以下命令，退出MySQL数据库。

```
exit
```

2. 以root用户重新登录MySQL数据库。

在登录命令后添加以下参数：

```
--ssl-mode=DISABLED
```

或

```
--ssl=0
```

须知

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

3. 执行以下命令，查看MySQL数据库连接的方式。

```
\s
```

如果界面回显类似以下信息，说明MySQL数据库已关闭SSL。

```
SSL: Not in use
```

----结束

5.3 如何设置数据库安全审计的 INSERT 审计策略?


在添加风险操作时，您可以添加INSERT审计策略。

5.4 如何验证已完成数据库安全审计配置？

开启数据库安全审计功能后，请参考以下操作步骤验证已正确配置数据库安全审计。

步骤1 在安装Agent的节点输入一条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“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 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**输入的SQL语句，如**图5-2**所示。

图 5-2 查看 SQL 语句

序号	SQL语句	客户端IP	数据库IP	数据库用户	风险等级	规则	操作类型	生成时间	操作
1	show databases	192.168.0.140	192.168.0.225	root	--	全审计规则	SHOW	2020/07/06 17:01:05 GMT+08:00	详情

- 如果SQL语句列表中显示输入的SQL语句，说明已正确配置数据库安全审计。
- 如果SQL语句列表中未显示输入的SQL语句，说明数据库安全审计功能无法使用，请按以下方法处理：
 - 关闭数据库的SSL。数据库开启SSL时，将不能使用数据库安全审计功能。请参照[如何关闭数据库SSL?](#) 章节关闭数据库SSL。
 - 请参照[Agent与数据库安全审计实例之间通信异常](#) 章节排查处理。

---结束

5.5 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。

5.6 如何查看数据库安全审计的版本信息？

请参照以下操作步骤查看数据库安全审计的版本信息。

步骤1 [登录管理控制台](#)。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ，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 查看实例版本信息。

----结束

5.7 如何查看数据库安全审计所有的告警信息？

请参照以下操作步骤查看数据库安全审计的告警信息。

步骤1 [登录管理控制台](#)。


步骤2 在页面上方选择“区域”后，单击页面左上方的，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“监控 > 告警监控”，进入告警监控页面。

步骤5 查看告警信息。

您可以按照以下方法，查询指定的告警信息。

- 选择“发生时间范围”（“近30分钟”、“近1小时”、“今日”、“近7天”、“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

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

当PC通过专线内网访问RDS时，您可以将Agent安装到自建的代理端。此时，PC通过代理端访问数据库，数据库安全审计只能审计代理与后端数据库之间的访问记录，无法审计应用端与后端数据库的访问记录。

有关Agent安装节点的详细介绍，请参见[如何选择数据库安全审计的Agent安装节点？](#)。

6 故障排查

6.1 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。

搜索SQL语句的详细操作，请参见[查看SQL语句详细信息](#)。

- 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。

搜索SQL语句的详细操作，请参见[查看SQL语句详细信息](#)。

- 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

6.2 无法使用数据库安全审计

问题现象


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

建议您按照本章节的操作步骤排查无法审计SQL语句的原因并进行修改。

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

检查数据库信息是否正确以及数据库的审计是否已开启

步骤1 [登录管理控制台](#)。

步骤2 在页面上方选择“区域”后，单击页面左上方的，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”，进入数据库列表页面。

步骤4 在“实例列表”下拉列表框中选择数据库所在的实例。

步骤5 查看数据库信息。

步骤6 检查数据库信息是否正确。

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

步骤7 检查数据库的审计是否已开启。

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

---结束

检查审计范围中对应数据库是否已启用

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

- 如果“状态”为“已启用”，请执行[检查数据库的Agent程序运行状态](#)。
- 如果“状态”为“已禁用”，请单击“启用”，启用数据库对应的审计范围规则。

- 如果问题已解决，结束操作。
- 如果问题仍存在，请执行[检查数据库的Agent程序运行状态](#)。

检查数据库的 Agent 程序运行状态

步骤1 使用跨平台远程访问工具（例如PuTTY）以root用户通过SSH方式，登录Agent的安装节点。

步骤2 执行以下命令，查看Agent程序的运行状态。

ps -ef|grep audit_agent

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

步骤3 执行以下命令，重新启动Agent。

service audit_agent restart

- 如果问题已解决，结束操作。
- 如果问题仍存在，请执行[步骤4](#)。

步骤4 执行以下命令，检查Agent与数据库安全审计实例之间的通信状态。

tailf /opt/dbss_audit_agent/log/audit_agent.log

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

图 6-1 通信正常

```

-]# tailf /opt/dbss_audit_agent/log/audit_agent.log
7:37 INFO [websocket_message_handle.cpp:357] send config data capture result begin...
7:37 INFO [websocket_message_handle.cpp:359] send config data capture result success
7:37 INFO [websocket_message_handle.cpp:116] audit ethernet is: eth0
7:37 INFO [websocket_message_handle.cpp:149] libpcap filter policy is: port 3306 and (src host 192.168.0.118 or dst host 192.168.0.118)
7:37 INFO [catch_data_package.cpp:119] init libpcap tool begin...
7:37 INFO [catch_data_package.cpp:155] init libpcap tool success
7:37 INFO [udp_communication.cpp:28] init udp connection begin...
7:37 INFO [udp_communication.cpp:51] init udp connection success!
7:37 INFO [catch_data_package.cpp:167] catch data packet begin...
7:39 INFO [websocket_message_handle.cpp:430] send heart beat begin
    
```

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

图 6-2 通信异常

```

AWdmb74cL5BfUhrp8-t]# tail /opt/dbss_audit_agent/log/audit_agent.log
INFO [websocket.cpp:1608] create websocket thread begin...
INFO [websocket.cpp:1620] create websocket thread success
INFO [websocket_connection_handle.cpp:278] setup websocket connection success
INFO [websocket_connection_handle.cpp:169] send authentication request packet with websocket...
INFO [websocket_connection_handle.cpp:126] create authentication request packet begin...
INFO [websocket_connection_handle.cpp:25] encrypt verify info by public key begin...
INFO [websocket_connection_handle.cpp:53] encrypt verify info by public key success
INFO [websocket_connection_handle.cpp:158] create authentication request packet success
INFO [websocket_connection_handle.cpp:172] authentication request packet is: {"body":{"agentid":"AWdmb74cL5BfUH
":"EulerOS","ostype":"Linux","osver":"3.10.0-327.36.58.4.x86_64","verify":"IHGavbph0aqK6Q+saLeIaIMLRBIA/537uGRgQqJ
icJUMk5sz1VSLHZwidlMraDnczItXe4NM1wn//fzcZdj9qeendgh0B1v3CXpD0zY35MouLkfbauoLqdMipwrNw5utJD55id5Qn0vfgunuZJWtc2A
0QTb2cL10iEKGHlteQ=="},"code":1,"id":"98c43f29-e302-402a-9e75-321b2f6e86c2","method":"request","time":1543807412}
ERROR [websocket_connection_handle.cpp:177] send authentication request packet failed, retry 30 seconds later!
    
```

----结束

检查数据库安全审计实例安全组规则是否开放

步骤1 进入数据库安全服务管理界面。

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

步骤3 在“实例列表”下拉列表框中选择数据库所在的实例。


步骤4 记录Agent安装节点IP信息。

单击数据库左侧的 ▾ 展开Agent的详细信息，并记录“安装节点IP”。

步骤5 在数据库列表的上方，单击“添加安全组规则”。

步骤6 在弹出的弹框中，记录数据库审计实例的“安全组名称”（例如default）。

步骤7 单击“前往处理”，进入“安全组”列表界面。

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

步骤9 单击“default”，进入“入方向规则”页面。

步骤10 检查安全组的入方向规则。

请检查该安全组的入方向规则是否已为**步骤4**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安装节点的入方向规则，请执行**效果验证**。
- 如果该安全组未配置安装节点的入方向规则，请执行**步骤11**。

步骤11 为安装节点添加入方向安全规则。

1. 在入方向规则页面，单击“添加规则”。
2. 在“添加入方向规则”对话框中，为安装节点IP添加TCP协议（端口为8000）和UDP协议（端口为7000-7100）规则。
3. 单击“确定”，完成添加入方向规则。

----结束

效果验证

在数据库中输入一条SQL语句后，在SQL语句列表页面搜索执行的语句。

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

6.3 告警邮件异常

故障现象

- 数据库安全审计实例功能正常，邮件收到高风险语句告警，但控制台未显示高风险SQL语句。
- 告警邮件发送延迟。

可能原因

审计日志量超过了实例的处理能力，导致数据审计的延迟。

处理建议

- 新增DBSS实例，分担当前数据审计流量或者更改审计规则，优化缩小审计范围。
- 制定自动小时备份任务，避免数据量存储磁盘达到85%触发日志清理机制。

6.4 无法进入数据库安全服务购买页

故障现象

使用FullAccess权限的账号进入购买页面报错

可能原因

IAM主账号开启细粒度鉴权，权限不够无法进入购买页。

处理建议

给子账户添加以下权限：

tms:predefineTags:list

bss:order:pay

bss:order:view

bss:order:update

bss:balance:view

vpc:vpcs:list

smn:topic:list

ces:metricData:create

gaussdb:instance:list

gaussdb:instance:modifyTraceSQLPolicy

eps:resources:list

rds:instance:list

dws:openAPICluster:list

rds:auditlog:operate

dws:cluster:setSecuritySettings

dws:ltsAccess:get

dws:ltsAccess:operate

dws:createAgency:create

6.5 数据库安全服务实例审计 Postgres 的 RDS 数据库没有审计数据怎么办？

故障现象

DBSS实例审计Postgres的RDS数据库没有审计数据

可能原因

- DBSS审计实例配置不正确，请重新检查配置
- 若配置没有问题，还是没有审计数据，那就需要在连接数据库实例的时候用非SSL的方式去连接。

解决办法

使用如下命令，连接数据库：

```
psql -h xxx.xxx.xxx -p 5432 "dbname=postgres user=root sslmode=disable"
```

6.6 数据库安全服务自动备份失败，失败码：Export backup file failed。

DBSS自动备份失败。失败码：Export backup file failed

形成原因

DBSS磁盘空间占满后会自动备份失败，需要修改自动备份规则，设置日志保留时间。需要及时删除不需要的备份来腾出空间。

7 日志类

7.1 数据库安全审计的操作日志是否可以迁移？

不可以。数据库安全审计当前不支持迁移数据库操作日志。

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


7.2 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。

7.3 如何查看数据库安全审计的用户操作日志？

请参照以下操作步骤，查看用户在数据库安全审计系统的操作日志。

步骤1 [登录管理控制台](#)。

步骤2 在页面上方选择“区域”后，单击页面左上方的，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7-1](#)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 7-1 操作日志参数说明

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

----结束

7.4 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。


7.5 数据库安全审计的审计日志是否支持备份？

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

请参照以下操作步骤，自动备份审计日志。

自动备份数据库审计日志

步骤1 [登录管理控制台](#)。

步骤2 在页面上方选择“区域”后，单击页面左上方的，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7-2所示。

图 7-1 “设置自动备份”对话框

设置自动备份

1. 审计日志将备份到对象存储服务的OBS桶中，OBS桶按照存储用量收费，由对象存储服务结算。
2. 开启自动备份，请先选择OBS桶作为审计日志备份桶，DBSS服务将获取该桶的读写权限。

自动备份

备份周期

开始时间

桶名称 C 跳转到该桶 | 创建默认桶





可选择已有OBS桶或默认桶，默认桶不存在时将被自动创建
 OBS服务默认使用按需计费模式，不同区域及计费项产生费用不同。 [了解计费详情](#)

文件导出目录

自动备份授权 同意DBSS服务获取该OBS桶读写权限，用于审计日志备份导出
注：授权成功后预计15分钟，自动备份才会生效

取消
确定

表 7-2 自动备份参数说明

参数名称	说明	取值样例
自动备份	开启或关闭自动备份。 <ul style="list-style-type: none">  : 开启  : 关闭 	
备份周期	选择自动备份的周期，可以选择： <ul style="list-style-type: none"> 每天 每小时 	每天
开始时间	单击  ，选择开始备份的时间。	2020/01/14 20:27:08
桶名称	设置备份使用的OBS桶名称，可以选择： <ul style="list-style-type: none"> 创建默认桶 选择已有桶 说明 <ul style="list-style-type: none"> 单击“创建默认桶”，将进行OBS授权，用于审计日志备份导出。 审计日志只能导出到DBSS服务创建的桶。 	20f18-7a5a-4042
文件导出目录	在OBS桶中创建备份文件的目录。	test

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

7.6 数据库安全审计的审计日志支持直接转存 OBS 吗？

不支持。数据库安全审计的审计日志是存放在日志数据库中的。若您需要将日志保存于对象存储服务（OBS），请登录数据库安全服务控制台，设置备份审计日志。备份数据库审计日志的详细操作步骤，请参见[备份数据库审计日志](#)。

数据库安全审计支持**手动备份**和**自动备份**两种模式。

自动备份支持“每天”、“每周”、“每月”三种备份周期备份审计日志。

手动备份支持“备份最近24小时日志”、“最近7天日志”、“最近30天日志”和“全部日志”四种备份范围。

当您的日志量比较大时，建议您按**每天**来自动备份日志。

日志备份到OBS，服务会自动为您创建桶。桶按照存储量收费。有关OBS的计费详情，请参见[价格详情](#)。

7.7 备份时持续显示“正在上传备份文件”

备份数据较大将导致备份速度缓慢，建议您按小时进行备份。

A 修订记录

发布日期	修改说明
2024-04-10	第二十一正式发布。 控制台新风格升级。
2023-04-07	第二十次正式发布。 新增 无法进入数据库安全服务购买页
2022-11-01	第十九次正式发布。 修改 如何退订数据库安全服务?
2022-06-21	第十八次正式发布。 <ul style="list-style-type: none"> 新增告警邮件异常。 新增备份时持续显示“正在上传备份文件”。 优化部分常见问题描述。
2022-05-12	第十七次正式发布。 <ul style="list-style-type: none"> 新增数据库安全审计和RDS SQL审计有什么区别?。 新增同一区域可以购买多少个数据库安全审计实例?。 优化部分常见问题描述。
2022-03-18	第十六次正式发布。 <ul style="list-style-type: none"> 新增购买实例时为何要选择VPC?。 新增云服务首页提示DBSS服务预测容量不足如何处理?。
2021-11-03	第十五次正式发布。 修改部分常见问题的问答描述。 数据库安全服务支持哪些性能规格? ，更新支持的硬盘规格。

发布日期	修改说明
2021-10-20	<p>第十四次正式发布。</p> <p>修改部分常见问题的问答描述。</p> <ul style="list-style-type: none"> • 新增数据库安全审计可以审计不同VPC的数据库吗？。 • 数据库安全审计的Agent可以安装在哪些Linux操作系统上？，新增Agent支持以下版本的操作系统： <ul style="list-style-type: none"> - Fedora 29 (64bit) - Fedora 30 (64bit) - SUSE 13 (64bit) - SUSE 15 (64bit) - SUSE 42 (64bit) - Euler 2.5 (64bit) - OpenEuler 20.03 (64bit) - Red Hat Enterprise Linux 7.4 (64bit) - Red Hat Enterprise Linux 7.6 (64bit) - NeoKylin 7.0 (64bit) - Kylin Linux Advanced Server release V10 (64bit) - Uniontech OS Server 20 Enterprise (64bit)
2021-04-19	<p>第十三次正式发布。</p> <p>数据库安全审计的Agent可以安装在哪些Linux操作系统上？，新增Agent支持CentOS 7.9、CentOS 8.1、CentOS 8.2和Debian 10.0.0版本。</p>
2021-03-22	<p>第十二次正式发布。</p> <ul style="list-style-type: none"> • 新增Agent运行时会消耗安装节点多少资源？ • 如何配置数据库安全审计？，优化相关内容描述。 • 数据库安全审计运行正常但无审计记录，新增关闭SQL SERVER 协议的强行加密Section。
2021-01-19	<p>第十一次正式发布。</p> <p>新增数据库安全审计的审计日志支持直接转存OBS吗？。</p>
2020-12-18	<p>第十次正式发布。</p> <ul style="list-style-type: none"> • 如何处理Agent与数据库安全审计实例之间通信异常？，优化添加加入方向安全组规则。 • 无法使用数据库安全审计，优化添加加入方向安全组规则。
2020-05-20	<p>第九次正式发布。</p> <p>数据库安全审计的审计数据可以保存多久？，优化相关内容描述。</p>
2020-04-22	<p>第八次正式发布。</p> <p>数据库安全审计的Agent可以安装在哪些Linux操作系统上？，新增Agent支持CentOS 7.6 (64bit) 版本。</p>

发布日期	修改说明
2020-03-16	第七次正式发布。 调整了文档大纲。 <ul style="list-style-type: none">• 如何修改Agent的CPU和内存的阈值?• 如何安装Agent (Linux操作系统)?• 如何安装Agent (Windows操作系统)?• 如何处理Agent与数据库安全审计实例之间通信异常?
2020-02-24	第六次正式发布。 新增数据库安全审计Windows相关描述。
2019-12-23	第五次正式发布。 补充支持IPv6相关内容描述。
2019-12-03	第四次正式发布。 <ul style="list-style-type: none">• 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。
2019-08-26	第三次正式发布。 新增 什么是区域、可用区? 。
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。