

数据库安全服务 (DBSS)

最佳实践

文档版本 16
发布日期 2024-08-12



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

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

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

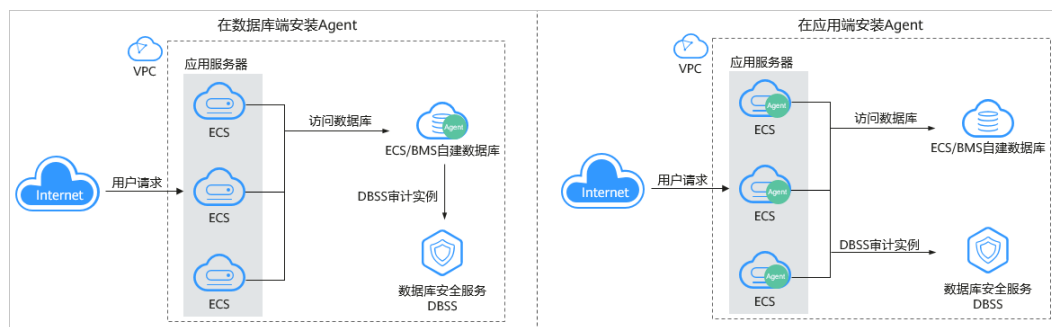
| | |
|--|-----------|
| 1 审计 ECS 自建数据库 | 1 |
| 2 审计 RDS 关系型数据库 (安装 Agent) | 8 |
| 3 审计 RDS 关系型数据库 (免安装 Agent) | 17 |
| 4 容器化部署数据库安全审计 Agent | 22 |
| 4.1 场景说明..... | 22 |
| 4.2 添加数据库并导出数据库配置..... | 23 |
| 4.3 在 CCE 集群节点中安装 Agent..... | 25 |
| 4.3.1 导入对象存储卷..... | 25 |
| 4.3.2 创建配置项..... | 27 |
| 4.3.3 创建 Agent 守护进程集工作负载..... | 28 |
| 4.4 开启数据库安全审计..... | 34 |
| 4.5 查看审计结果..... | 34 |
| 5 数据库慢 SQL 检测 | 37 |
| 6 数据库拖库检测 | 41 |
| 7 数据库脏表检测 | 46 |
| 8 Oracle RAC 集群审计配置最佳实践 | 50 |
| 9 数据库安全审计等保最佳实践 | 58 |
| 10 数据库审计实例规则配置最佳实践 | 62 |

1 审计 ECS 自建数据库

数据库安全审计采用旁路部署模式，通过在**数据库**或**应用系统服务器**上部署数据库安全审计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，实现对ECS/BMS自建数据库的安全审计。

审计ECS/BMS自建数据库架构图如**图1-1**所示。

图 1-1 审计 ECS/BMS 自建数据库架构图



场景说明

假设您在华为云的弹性云服务器（Elastic Cloud Server，以下简称ECS）上自建了一个数据库，数据库的详细信息如**表1-1**所示，您需要对该数据库内部违规和不正当操作进行定位追责，满足等保测评数据库审计需求。本章节详细介绍该场景下，在**数据库端安装Agent**，开启数据库安全审计功能和验证审计结果的操作。

表 1-1 ECS 自建数据库信息说明

| | |
|---------|-------------|
| 数据库类型 | MySQL |
| 数据库版本 | 5.7 |
| 数据库IP地址 | 192.168.1.5 |
| 端口 | 3306 |
| 操作系统 | LINUX64 |

约束与限制

- 使用数据库安全审计需要关闭数据库的SSL。
- 待审计数据库与数据库安全审计需要在同一区域。
- 购买数据库安全审计配置“VPC”参数时，需与Agent安装节点所在VPC相同。
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？](#)。

步骤一：购买数据库安全审计

您需要根据您的业务需求购买数据库安全审计规格并配置数据库安全审计参数，详细操作请参见[购买数据库安全审计](#)。

📖 说明

为保证审计功能的正常使用，购买数据库安全审计配置“VPC”参数时，请与Agent安装节点所在VPC相同。

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？](#)。

步骤二：添加数据库并开启审计

购买数据库安全审计后，您需要先将目标数据库添加至数据库安全审计实例并开启该数据库的审计功能。

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，并单击“添加数据库”。

步骤5 在弹出的对话框中，按[表1-1](#)所示信息填写数据库参数，如[图1-2](#)所示。

图 1-2 “添加数据库”对话框

| | | | |
|---------|---------|---------|-------------|
| * 数据库类别 | 自建数据库 | * 数据库类型 | MYSQL |
| * 数据库名称 | test | * IP地址 | 192.168.1.5 |
| * 端口 | 3306 | * 数据库版本 | 5.7 |
| 实例名 | | * 选择字符集 | UTF-8 |
| * 操作系统 | LINUX64 | | |

确定 取消

步骤6 单击“确定”，该数据库添加到数据库列表中，且“审计状态”为“已关闭”。

步骤7 在该数据库所在行的“操作”列，单击“开启”，开启审计功能。

----结束

步骤三：添加 Agent

步骤1 在数据库所在行的“Agent”列，单击“添加Agent”，如**图1-3**所示。

图 1-3 添加 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：db05 类型：MYSQL 版本：5.7 | UTF8 | 192.168.0.73 3306 | -- | LINUX64 | 已开启 | 添加Agent | 关闭 删除 |
| 2 | 名称：awde 类型：MYSQL 版本：5.0 | UTF8 | .32.3 12 | -- | LINUX64 | 已关闭 | 添加Agent | 开启 删除 |
| 3 | 名称：test 类型：MYSQL 版本：5.7 | UTF8 | 192.168.1.5 3306 | -- | LINUX64 | 已开启 | 添加Agent | 关闭 删除 |

步骤2 在弹出的对话框中，选择添加方式。

图 1-4 在数据库端添加 Agent

添加Agent ✕

添加方式 选择已有Agent 创建Agent

安装节点类型 数据库端 应用端

操作系统

步骤3 单击“确定”，Agent添加成功。

----结束

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。

- 如果该安全组已配置安装节点的入方向规则，请执行**步骤五：安装Agent**。
- 如果该安全组未配置安装节点的入方向规则，请按照本节内容进行配置。

📖 说明

安全组规则也可以在成功安装Agent后进行添加。

- 步骤1** 获取**安装节点IP地址**。
- 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1-5**所示。

图 1-5 添加安全组规则



- 步骤4** 单击“前往处理”，进入“安全组”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**Q**或按“Enter”，列表显示“default”安全组信息。
- 步骤6** 单击“default”，进入“基本信息”页面。
- 步骤7** 选择“入方向规则”页签，单击“添加规则”，如**图1-6**所示。

图 1-6 添加规则



- 步骤8** 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，如**图1-7**所示。

图 1-7 “添加加入方向规则”对话框 (ECS)



步骤9 单击“确定”，完成添加加入方向规则。

----结束

步骤五：安装 Agent

添加安全规则后，您需要下载Agent包并将下载的Agent安装包上传到待安装Agent的节点上进行安装。使添加的数据库连接到数据库安全审计实例，数据库安全审计才能对添加的数据库进行审计。

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和安装Agent。

步骤1 登录控制台进入数据库安全服务。

步骤2 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3 在“选择实例”下拉框中，选择需要下载Agent的数据库所属实例。

步骤4 单击该数据库左侧的 ▾ 展开Agent的详细信息，在Agent所在行的“操作”列，单击“下载agent”，如图1-8所示。

将Agent安装包下载到本地。

图 1-8 下载 Agent



步骤5 使用跨平台传输工具（例如WinSCP），将下载的Agent安装包“xxx.tar”上传到待安装Agent的节点（即图1-8中的“安装节点IP”）。

步骤6 使用跨平台远程访问工具（例如PuTTY）以root用户通过SSH方式，登录该安装节点。

步骤7 执行以下命令，进入Agent安装包“xxx.tar”所在目录。

步骤8 cd Agent安装包所在目录

步骤9 执行以下命令，解压缩“xxx.tar”安装包。

步骤10 `tar -xvf xxx.tar`

步骤11 执行以下命令，进入“install.sh”脚本所在目录。

步骤12 `cd install.sh脚本所在目录`

步骤13 执行以下命令，安装Agent。

步骤14 `sh install.sh`

步骤15 如果界面回显以下信息，说明安装成功。

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

----结束

步骤六：验证 Agent 与数据库安全审计实例之间的网络通信正常

待审计的数据库与数据库安全审计实例连接成功后，您需要验证Agent与数据库安全审计实例之间的网络通信是否正常。

步骤1 在安装Agent的节点执行一条SQL语句或对数据库进行操作（例如，“Select 1;”）。

步骤2 在左侧导航树中，选择“总览”，进入“总览”界面。

步骤3 在“选择实例”下拉列表框中，选择需要查看数据库慢SQL语句信息的实例。

步骤4 选择“语句”页签。

步骤5 SQL语句列表将显示登录数据库操作的记录，如图1-9所示。

如果不能查询到SQL语句，请您参照[如何处理Agent与数据库安全审计实例之间通信异常?](#)进行排查。

图 1-9 查看 SQL 语句

| 序号 | SQL语句 | 客户端IP | 数据库IP | 数据库用户 | 风险等级 | 规则 | 操作类型 | 生成时间 | 操作 |
|----|--------|--------------|--------------|-------|------|--------|--------|-------------------------------|----|
| 1 | LOGOUT | 192.168.0.62 | 192.168.0.78 | root | -- | 全审计... | LOGOUT | 2020/04/03 10:55:07 GMT+08:00 | 详情 |

----结束

步骤七：查看审计结果

验证成功后，您可参照本节内容在总览界面查看审计结果信息，同时也可根据需求在报表界面进行设置生成报表、下载或预览报表。

步骤1 查看总览信息。

进入总览入口，如图1-10所示，查看总览信息。

在总览界面，展示了该实例的审计时长、SQL语句总量、风险总量以及今日语句、今日风险、今日会话量

您可以选择“语句”或“会话”页签，分别查看SQL语句信息和会话分布图。

图 1-10 进入总览入口




步骤2 生成报表、下载或预览报表。

1. 参照图1-11进入报表管理界面。

图 1-11 进入报表管理入口



2. 在左侧导航树中，选择“报表”。
3. 在“选择实例”下拉列表框中，选择需要生成审计报表的实例。选择“报表管理”页签。
4. 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”。
5. 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。
6. 单击“确定”。

系统跳转到“报表结果”页面，您可以查看报表的生成进度。报表生成后，您可以“预览”或“下载”报表，如图1-12所示。

须知

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

图 1-12 预览或下载报表

| 报表名称 | 关联数据库 | 报表类型 | 生成时间 | 格式 | 状态 | 操作 |
|---------|-------|------|-------------------------------|-----|------|----------|
| DDL命令报表 | 全部数据库 | 实时报表 | 2020/03/13 16:46:22 GMT+08:00 | pdf | 100% | 预览 下载 删除 |
| DDL命令报表 | 全部数据库 | 实时报表 | 2020/03/13 16:44:54 GMT+08:00 | pdf | 100% | 预览 下载 删除 |

----结束

2 审计 RDS 关系型数据库 (安装 Agent)

方案概述

本文档介绍了如何对关系型数据库 (应用部署于ECS) 进行安全审计。对于部分关系型数据库, DBSS服务支持免安装Agent模式, 无需安装Agent, 即可开启数据库安全审计。

- 如果您需要安全审计的数据库类型如表2-1所示, 请参见[审计RDS关系型数据库 \(免安装Agent\)](#)。

表 2-1 支持免 Agent 安装的关系型数据库

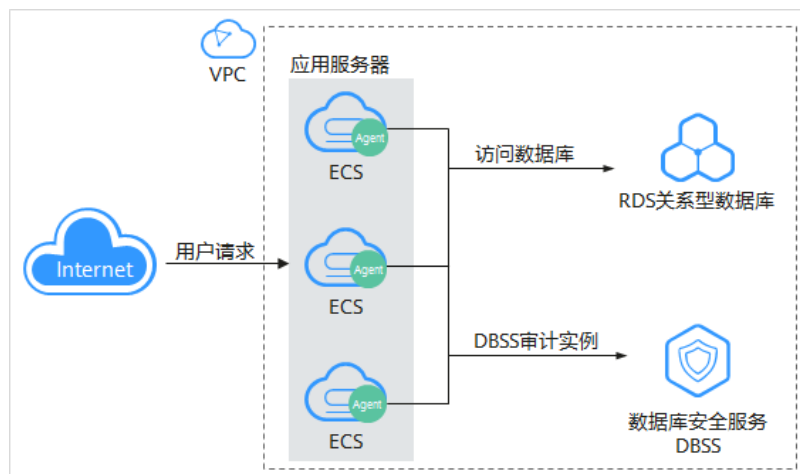
| 数据库类型 | 支持的版本 |
|--|---|
| GaussDB for MySQL | 默认都支持 |
| RDS for SQLServer (华为云审计实例: 23.02.27.182148 及其之后的版本支持) | 默认都支持 |
| RDS for MySQL | <ul style="list-style-type: none">5.6 (5.6.51.1及以上版本)5.7 (5.7.29.2及以上版本)8.0 (8.0.20.3及以上版本) |
| GaussDB(DWS) | <ul style="list-style-type: none">8.2.0.100及以上版本 |
| PostgreSQL (华为云审计实例: 23.04.17.123301 及其之后的版本支持) | <ul style="list-style-type: none">14 (14.4及以上版本)13 (13.6及以上版本)12 (12.10及以上版本)11 (11.15及以上版本)9.6 (9.6.24及以上版本)9.5 (9.5.25及以上版本) |
| RDS for MariaDB | 默认都支持 |

- 如果您需要安全审计的数据库类型不在表2-1范围内, 请参见本节内容。

方案架构

数据库安全审计采用旁路部署模式，通过在访问数据库的应用系统服务器上部署数据库安全审计Agent，获取访问数据库流量，Agent将获取的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，实现对数据库的安全审计。

图 2-1 审计 RDS 关系型数据库 (安装 Agent) 架构图



本文以POSTGRESQL 7.4版本的关系型数据库为例，详细信息如表1所示，您需要对该数据库内部违规和不正当操作进行定位追责，满足等保测评数据库审计需求。本节详细介绍该场景下开启数据库安全审计功能和验证审计结果的具体操作。

表 2-2 数据库示例信息说明

| | |
|-----------------------|---------------|
| 数据库类型 | POSTGRESQL |
| 数据库版本 | 7.4 |
| 数据库IP地址 | 192.168.1.31 |
| 应用端IP地址 (安装节点IP地址) | 192.168.1.132 |
| 端口 | 8000 |
| 操作系统 | LINUX64 |

约束与限制

- 使用数据库安全审计需要关闭数据库的SSL。
- 待审计数据库与数据库安全审计需要在同一区域。
- 购买数据库安全审计配置“VPC”参数时，需与Agent安装节点所在VPC相同。

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？](#)。

步骤一：购买数据库安全审计

您需要根据您的业务需求购买数据库安全审计规格并配置数据库安全审计参数，详细操作请参见[购买数据库安全审计](#)。

说明


为保证审计功能的正常使用，购买数据库安全审计配置“VPC”参数时，请与Agent安装节点所在VPC相同。

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？](#)。

步骤二：添加数据库并开启审计

购买成功后，您需要先将目标数据库添加至数据库安全审计实例并开启该数据库的审计功能。

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，并单击“添加数据库”。

步骤5 在弹出的对话框中，按[表2-2](#)所示信息填写数据库参数，如[图2-2](#)所示。

数据库安全审计支持“UTF-8”和“GBK”两种数据库字符集的编码格式，请根据业务情况选择编码格式。

图 2-2 “添加数据库”对话框



步骤6 单击“确定”，该数据库添加到数据库列表中，且“审计状态”为“已关闭”。

步骤7 在该数据库所在行的“操作”列，单击“开启”，开启审计功能。

----结束

步骤三：添加 Agent

步骤1 在数据库所在行的“Agent”列，单击“添加Agent”，如图2-3所示。

图 2-3 添加 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: db05 类型: MYSQL 版本: 5.7 | UTF8 | 192.168.0.73 3306 | -- | LINUX64 | 已开启 | 添加Agent | 关闭 删除 |
| 2 | 名称: test 类型: POSTGRESQL 版本: 7.4 | UTF8 | 192.168.1.31 8000 | -- | WINDOWS64 | 已开启 | 添加Agent | 关闭 删除 |

步骤2 在弹出的对话框中，选择添加方式。

- 方式一：选择“创建Agent”

如果数据库安全审计实例的数据库未添加Agent，您需要创建新的Agent。

“安装节点类型”选择“应用端”，“安装节点IP”输入表2-2所示的应用端IP地址，如图2-4所示。

图 2-4 在应用端添加 Agent

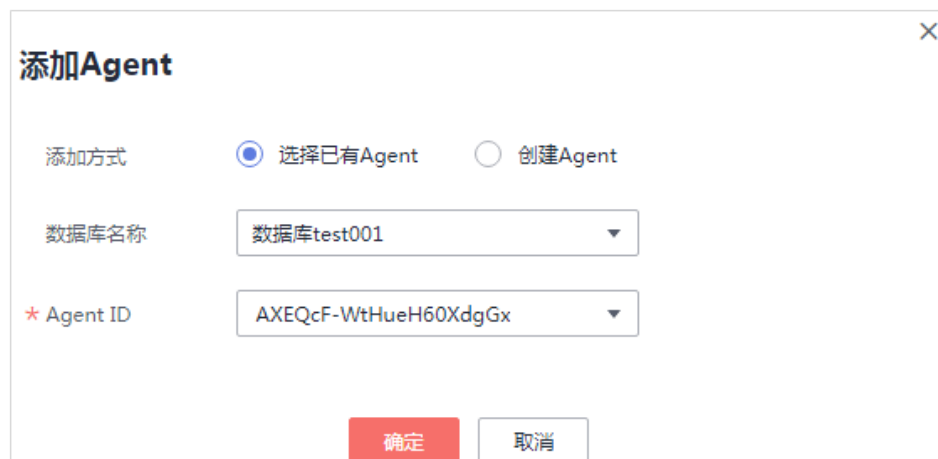
- 方式二：“选择已有Agent”如图2-5所示。

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 2-5 选择已有 Agent



步骤3 单击“确定”，Agent添加成功。

----结束

步骤四：添加安全组规则

Agent添加完成后，您需要为数据库安全审计实例所在的安全组添加入方向规则TCP协议（8000端口）和UDP协议（7000-7100端口），使Agent与审计实例之间的网络连接，数据库安全审计才能对添加的数据库进行审计。

- 如果该安全组已配置安装节点的入方向规则，请执行[步骤五：安装Agent](#)。
- 如果该安全组未配置安装节点的入方向规则，请按照本节内容进行配置。

📖 说明

安全组规则也可以在成功安装Agent后进行添加。

步骤1 获取[安装节点IP地址](#)。


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 2-6](#)所示。

图 2-6 添加安全组规则



步骤4 单击“前往处理”，进入“安全组”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“基本信息”页面。

步骤7 选择“入方向规则”页签，单击“添加规则”，如图2-7所示。

图 2-7 添加规则



步骤8 在弹出的“添加入方向规则”对话框中，为表2-2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2-8所示。

图 2-8 “添加入方向规则”对话框



步骤9 单击“确定”，完成添加入方向规则。

----结束

步骤五：安装 Agent

添加安全组规则后，您需要下载Agent包并将下载的Agent安装包上传到待安装Agent的节点上进行安装。使添加的数据库连接到数据库安全审计实例，数据库安全审计才能对添加的数据库进行审计。


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和安装Agent。

步骤1 登录控制台进入数据库安全服务。

步骤2 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3 在“选择实例”下拉框中，选择需要下载Agent的数据库所属实例。

步骤4 单击该数据库左侧的  展开Agent的详细信息，在Agent所在行的“操作”列，单击“下载agent”，如图2-9所示。

将Agent安装包下载到本地。

图 2-9 下载 Agent



| AgentID | 安装节... | 安装节... | 操作系统 | 审计网... | CPU脚... | 内存脚... | 通用 | 运行状态 | 操作 |
|----------------------|--------|--------------|---------|--------|---------|--------|----|------|-------------------|
| AXGHb4BA7I_qYlmCkNo- | 应用端 | 192.168.1... | LINUX64 | -- | 80 | 80 | 否 | 休眠中 | 下载agent 关闭 删除 |

步骤5 使用跨平台传输工具（例如WinSCP），将下载的Agent安装包“xxx.tar”上传到待安装Agent的节点（即图2-9中的“安装节点IP”）。

步骤6 使用跨平台远程访问工具（例如PuTTY）以root用户通过SSH方式，登录该安装节点。

步骤7 执行以下命令，进入Agent安装包“xxx.tar”所在目录。

```
cd Agent安装包所在目录
```

步骤8 执行以下命令，解压缩“xxx.tar”安装包。

```
tar -xvf xxx.tar
```

步骤9 执行以下命令，进入“install.sh”脚本所在目录。

```
cd install.sh脚本所在目录
```

步骤10 执行以下命令，安装Agent。

```
sh install.sh
```

如果界面回显以下信息，说明安装成功。

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

----结束

步骤六：验证 Agent 与数据库安全审计实例之间的网络通信正常

待审计的数据库与数据库安全审计实例连接成功后，您需要验证Agent与数据库安全审计实例之间的网络通信是否正常。

步骤1 在安装Agent的节点执行一条SQL语句或对数据库进行操作（例如，“Select 1;”）。

步骤2 在左侧导航树中，选择“总览”，进入“总览”界面。

步骤3 在“选择实例”下拉列表框中，选择需要查看数据库慢SQL语句信息的实例。

步骤4 选择“语句”页签。

步骤5 SQL语句列表将显示登录数据库操作的记录，如图2-10所示。

如果不能查询到SQL语句，请您参照[如何处理Agent与数据库安全审计实例之间通信异常？](#)进行排查。

图 2-10 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 | LOGOUT | 192.168.0.62 | 192.168.0.78 | root | - | 全审计 | LOGOUT | 2020/04/03 10:55:07 GMT+08:00 | 详情 |

----结束

步骤七：查看审计结果

验证成功后，您可参照本节内容在总览界面查看审计结果信息，同时也可根据需求在报表界面进行设置生成报表、下载或预览报表。

步骤1 查看总览信息。

进入总览入口，如图2-11所示，查看总览信息。

在总览界面，展示了该实例的审计时长、SQL语句总量、风险总量以及今日语句、今日风险、今日会话量

您可以选择“语句”或“会话”页签，分别查看SQL语句信息和会话分布图。

图 2-11 进入总览入口




步骤2 生成报表、下载或预览报表。

1. 参照图2-12进入报表管理界面。

图 2-12 进入报表管理入口



2. 在左侧导航树中，选择“报表”。
3. 在“选择实例”下拉列表框中，选择需要生成审计报表的实例。选择“报表管理”页签。
4. 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”。

5. 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。
6. 单击“确定”。

系统跳转到“报表结果”页面，您可以查看报表的生成进度。报表生成后，您可以“预览”或“下载”报表，如 [图2-13](#) 所示。

须知

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

图 2-13 预览或下载报表

| 报表名称 | 关联数据库 | 报表类型 | 生成时间 | 格式 | 状态 | 操作 |
|---------|-------|------|-------------------------------|-----|---|--|
| DDL命令报表 | 全部数据库 | 实时报表 | 2020/03/13 16:46:22 GMT+08:00 | pdf | <div style="width: 100%;"><div style="width: 100%;"></div></div> 100% | 预览 下载 删除 |
| DDL命令报表 | 全部数据库 | 实时报表 | 2020/03/13 16:44:54 GMT+08:00 | pdf | <div style="width: 100%;"><div style="width: 100%;"></div></div> 100% | 预览 下载 删除 |

---结束

3 审计 RDS 关系型数据库 (免安装 Agent)

方案概述

本文档介绍了如何对关系型数据库 (应用部署于ECS) 进行安全审计。对于部分关系型数据库, DBSS服务支持免安装Agent模式, 无需安装Agent, 即可开启数据库安全审计。

- 如果您需要安全审计的数据库类型如[表3-1](#)所示, 请参见本节内容。

表 3-1 支持免 Agent 安装的关系型数据库

| 数据库类型 | 支持的版本 |
|--|---|
| GaussDB for MySQL | 默认都支持 |
| RDS for SQLServer (华为云审计实例: 23.02.27.182148 及其之后的版本支持) | 默认都支持 |
| RDS for MySQL | <ul style="list-style-type: none">5.6 (5.6.51.1及以上版本)5.7 (5.7.29.2及以上版本)8.0 (8.0.20.3及以上版本) |
| GaussDB(DWS) | <ul style="list-style-type: none">8.2.0.100及以上版本 |
| PostgreSQL (华为云审计实例: 23.04.17.123301 及其之后的版本支持) | <ul style="list-style-type: none">14 (14.4及以上版本)13 (13.6及以上版本)12 (12.10及以上版本)11 (11.15及以上版本)9.6 (9.6.24及以上版本)9.5 (9.5.25及以上版本) |
| RDS for MariaDB | 默认都支持 |

- 如果您需要安全审计的数据库类型不在[表3-1](#)范围内, 请参见[审计RDS关系型数据库 \(安装Agent\)](#)。

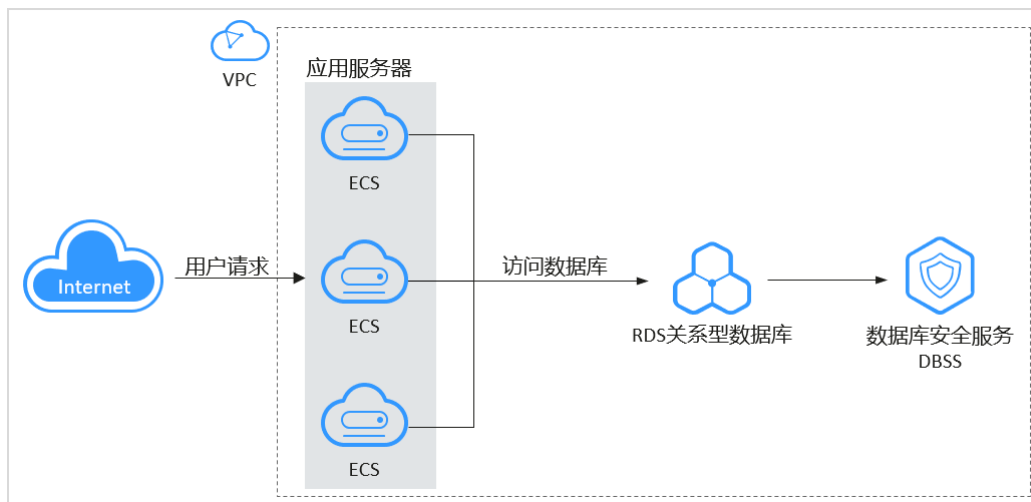
说明

- 免安装Agent模式配置简单、易操作，但较之安装了Agent的DBSS实例，支持的功能上存在如下差异：
 - 统计会话数量时，无法统计成功登录、与失败登录的会话个数。
 - 无法获取数据库访问时客户端的端口号。
- 由于GaussDB(DWS)服务具有日志审计开关的权限控制策略，只有华为云账号或拥有 Security Administrator权限的用户才能开启或者关闭DWS数据库审计开关。
- GaussDB默认不开启ddl，用户需要需按GaussDB用户手册开启（audit_system_object = 130023423）配置，同时该配置页中需保证日期格式为yyyy-MM-dd HH:mm:ss+Z（datastyle=ISO,YMD），操作请参考：[GaussDB开发指南](#)。

方案架构

数据库（GaussDB for MySQL或RDS for MySQL指定版本）将日志传送给DBSS，经过日志数据解析保存至DBSS实例日志库中，进行安全分析、聚合统计、合规分析等操作，实现对数据库的安全审计。

图 3-1 审计 RDS 关系型数据库 (免安装 Agent) 架构图



本文以GaussDB for MySQL为例，详细信息如表2所示，您需要对该数据库内部违规和不正当操作进行定位追责，满足等保测评数据库审计需求。本节详细介绍该场景下开启数据库安全审计功能和验证审计结果的具体操作。

表 3-2 数据库示例信息说明

| | |
|----------|-------------------|
| 数据库类别 | RDS数据库 |
| 数据库类型 | GaussDB for MySQL |
| 兼容的数据库版本 | MySQL 8.0 |
| 数据库IP地址 | 192.168.0.237 |
| 数据库端口 | 3306 |

约束与限制

待审计数据库与数据库安全审计需要在同一区域。


步骤一：购买数据库安全审计

您需要根据您的业务需求购买数据库安全审计规格并配置数据库安全审计参数，详细操作请参见[购买数据库安全审计](#)。

步骤二：添加数据库并开启审计

购买成功后，您需要先将目标数据库添加至数据库安全审计实例并开启该数据库的审计功能。

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，并单击“添加数据库”。

步骤5 在弹出的对话框中，按[表3-2](#)所示信息填写数据库参数，如[图3-2](#)所示。

图 3-2 添加数据库



步骤6 单击“确定”，该数据库添加到数据库列表中，且“审计状态”为“已关闭”。

图 3-3 数据库列表



步骤7 在数据库列表栏，查看“Agent”列的提示信息：

- 如果提示“无需添加agent”，表示该数据库版本支持免安装Agent模式。此时，请直接执行**步骤8**。

图 3-4 无需添加 Agent



- 如果提示“添加Agent”，表示该数据库版本需安装Agent才能启用安全审计。此时，请单击“添加Agent”，按界面提示操作，具体操作指导请参见[审计RDS关系型数据库 \(安装Agent\)](#)。

图 3-5 添加 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: db05 类型: MYSQL 版本: 5.7 | UTF8 | 192.168.0.73 3306 | -- | LINUX64 | 已开启 | 添加Agent | 关闭 删除 |
| 2 | 名称: test 类型: POSTGRESQL 版本: 7.4 | UTF8 | 192.168.1.31 8000 | -- | WINDOW564 | 已开启 | 添加Agent | 关闭 删除 |

步骤8 在该数据库所在行的“操作”列，单击“开启”，开启审计功能。

图 3-6 开启审计



----结束

步骤三：查看审计结果

您可参照本节内容在总览界面查看审计结果信息，同时也可根据需求在报表界面进行设置，生成报表、下载或预览报表。

步骤1 查看总览信息。

进入总览入口，如**图3-7**所示，查看总览信息。

在总览界面，展示了该实例的审计时长、SQL语句总量、风险总量以及今日语句、今日风险、今日会话量

您可以选择“语句”或“会话”页签，分别查看SQL语句信息和会话分布图。

图 3-7 进入总览入口




步骤2 生成报表、下载或预览报表。

1. 参照图3-8进入报表管理界面。

图 3-8 进入报表管理入口



2. 在左侧导航树中，选择“报表”。
3. 在“选择实例”下拉列表框中，选择需要生成审计报表的实例。选择“报表管理”页签。
4. 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”。
5. 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。
6. 单击“确定”。

系统跳转到“报表结果”页面，您可以查看报表的生成进度。报表生成后，您可以“预览”或“下载”报表，如图3-9所示。

须知

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

图 3-9 预览或下载报表

| 报表名称 | 关联数据库 | 报表类型 | 生成时间 | 格式 | 状态 | 操作 |
|---------|-------|------|-------------------------------|-----|------|--------------|
| DDL命令报表 | 全部数据库 | 实时报表 | 2020/03/13 16:46:22 GMT+08:00 | pdf | 100% | 预览 下载 删除 |
| DDL命令报表 | 全部数据库 | 实时报表 | 2020/03/13 16:44:54 GMT+08:00 | pdf | 100% | 预览 下载 删除 |

----结束

4 容器化部署数据库安全审计 Agent

4.1 场景说明

数据库安全审计支持批量部署流量采集Agent，针对大规模业务场景（容器化部署应用、数据库（RDS关系型数据库）数量多），能够显著提升产品配置的效率，降低配置的复杂度，减少运维人员的日常维护压力。

假设您的数据库信息和容器集群信息如表4-1所示，您需要审计该集群连接的数据库，并使用购买的数据库安全审计帮助您满足等保合规要求，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。本手册详细介绍该场景下，开启数据库安全审计功能和查看审计结果的操作。

须知

- 每个连接数据库的CCE集群，都需要在集群节点上安装Agent，当您有多个集群时，导出数据库配置后，请参见[在CCE集群节点中安装Agent](#)为每个连接数据库的CCE集群安装Agent。
- 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。

表 4-1 待审计数据库和 CCE 集群信息

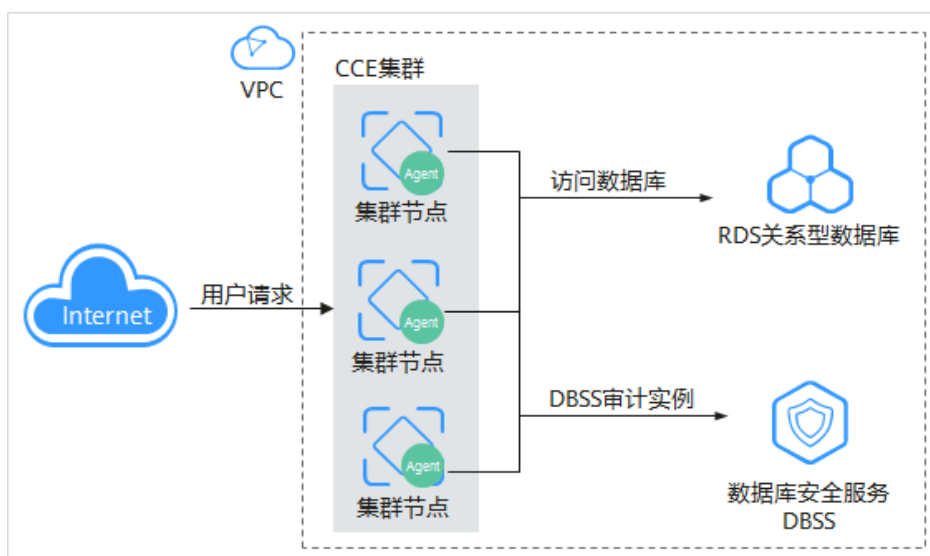
| | |
|-------|---|
| 集群名称 | scc-cmv-bj4 |
| 命名空间 | default 说明 可根据您的业务需要选择集群中已有命名空间或新建命名空间。命名空间（Namespace）是对一组资源和对象的抽象整合。在同一个集群内可创建不同的命名空间，不同命名空间中的数据彼此隔离。使得它们既可以共享同一个集群的服务，也能够互不干扰。 |
| 数据库类别 | RDS关系型数据库 |
| 数据库类型 | MySQL |
| 数据库版本 | 5.0 |

| | |
|---------|----------------------------|
| 数据库IP地址 | 192.168.1.31,192.168.0.159 |
| 端口 | 3306 |
| 操作系统 | LINUX64 |

数据库安全审计工作原理

数据库安全审计采用旁路部署模式，通过在访问数据库的应用系统服务器上部署数据库审计Agent，获取访问日志数据用于日志审计，实现对RDS关系型数据库的审计。

图 4-1 应用架构



4.2 添加数据库并导出数据库配置

在本章节中，您需要将待审计的数据库添加至数据库安全审计实例并开启数据库的审计功能，开启审计功能后再将数据库配置导入 OBS 桶。

约束与限制


- 在添加数据库前，您需要梳理集群工作负载中绑定的数据库，并注意以下规则：
 - 相同的数据库不能同时添加在多个不同审计实例上
 - 同一个工作负载所访问的数据库，必须添加在同一个审计实例中
 - 多个工作负载所访问的数据库有交集时，这些工作负载所访问的所有数据库必须添加在同一个审计实例中。
- 数据库安全审计实例配置有如下变动时，您必须重新“导出数据库配置”并重新“导入对象存储卷”和“添加云存储”。
变动包括：购买数据库安全审计实例、添加数据库、删除数据库。
- 使用数据库安全审计需要关闭数据库的 SSL。

添加数据库并开启审计

购买数据库安全审计后，您需要将待审计的数据库添加至数据库安全审计实例并开启数据库的审计功能。

购买数据库安全审计的详细操作请参见：[购买数据库安全审计](#)。

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，并单击“添加数据库”。

步骤5 在弹出的对话框中，按[表4-1](#)所示信息填写数据库参数，如[图4-2](#)所示。

数据库安全审计支持“UTF-8”和“GBK”两种数据库字符集的编码格式，请根据业务情况选择编码格式。

图 4-2 “添加数据库”对话框



步骤6 单击“确定”，该数据库添加到数据库列表中，且“审计状态”为“已关闭”。

步骤7 在该数据库所在行的“操作”列，单击“开启”，开启审计功能。

----结束

导出数据库配置

开启审计功能后，您需要将数据库配置导入OBS桶。

步骤1 在左侧导航树中，选择“实例列表”，进入“实例列表”界面。

步骤2 单击“导出数据库配置”。

图 4-3 导出数据库配置



须知

- “导出数据库配置”为隐藏按钮，请在“实例列表”界面的访问链接后面添加“? exportCfg”，添加完成后，按“Enter”进行访问。
- 数据库配置包含：待审计数据库配置信息和数据库安全审计Agent。

步骤3 在弹出的对话框中，单击“确定”，同意授权。

步骤4 同意授权后，DBSS将在对象存储服务为您创建名为“dbss-audit-agent-*{projectid}*”的桶。

说明

数据库安全审计实例配置有如下变动时，您必须重新导出数据库配置。

变动包括：购买数据库安全审计实例、添加数据库、删除数据库。

----结束

4.3 在 CCE 集群节点中安装 Agent

4.3.1 导入对象存储卷

导出数据库配置后，您需要为待审计数据库连接的集群在对象存储卷中导入数据库配置 (dbss-audit-agent-*{projectid}*)，用于Agent容器工作负载的云存储中，实现批量部署数据库安全审计Agent。

准备工作

为了确保挂载方式使用对象存储桶的可靠性和稳定性，请在创建对象存储前先配置密钥。

本章节操作适配云容器引擎 CCE服务旧版Console，请您在控制台切换至旧版CCE Console，具体切换步骤如图所示。

图 4-4 切换云容器引擎服务至旧版 Console



操作步骤


- 步骤1 登录管理控制台。
- 步骤2 在页面上方选择“区域”后，单击 ，选择“容器 > 云容器引擎”，进入云容器引擎“总览”界面。
- 步骤3 在左侧导航树中选择“资源管理 > 存储管理”，选择“对象存储卷”页签，单击“导入”。
- 步骤4 在弹出的“导入对象存储”对话框中，从列表里选择要导入的对象存储（dbss-audit-agent-*{projectid}*）。

图 4-5 “导入对象存储”对话框



- 步骤5 按表4-1所示信息选择导入对象存储的集群和命名空间，如图4-5所示。
 - 步骤6 单击“确定”。
- 在对象存储卷列表中，会新创建一条对象存储卷。

说明

当数据库配置有变动时，您需要重新导出数据库配置、导入对象存储和挂载云存储。

----结束

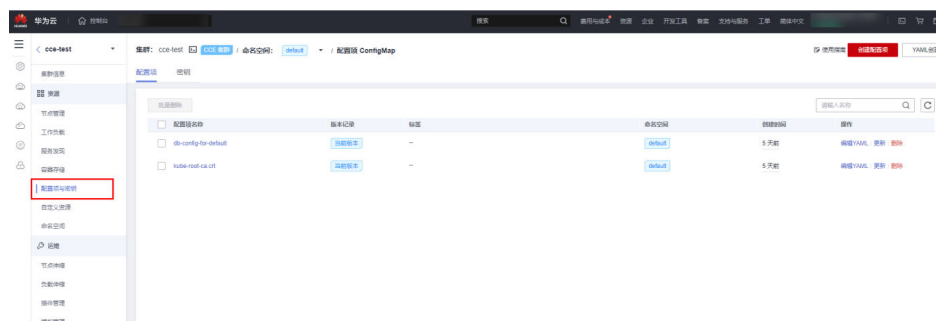
4.3.2 创建配置项

用于存储工作负载所需待审计的数据库信息，在Agent容器工作负载中作为文件使用。

操作步骤

步骤1 在左侧导航树中，选择“配置中心 > 配置项”，单击“创建配置项”，如图4-6所示。

图 4-6 进入创建配置项入口



步骤2 在“创建配置项”页面中，设置配置参数。如图4-7所示，相关参数如表4-2所示。

图 4-7 设置配置参数

The screenshot shows the 'Create Configuration Item' form. It includes the following fields:

- 配置名称** (Configuration Name): db-config-for-default
- 所属集群** (Cluster): scc-cmv-bj4
- 集群命名空间** (Cluster Namespace): default
- 描述** (Description): 请输入描述信息 (Please enter description information)
- 配置数据** (Configuration Data): A table with columns 'Key' (键) and 'Value' (值). The key 'db_config' has the value '192.168.1.31,192.168.0.159'.

表 4-2 配置参数说明

| 参数 | 参数说明 | 取值样例 |
|------|-------------------------|-----------------------|
| 配置名称 | 新建的配置名称，同一个命名空间里命名必须唯一。 | db-config-for-default |
| 所属集群 | 选择需要进行审计的集群。 | scc-cmv-bj4 |

| 参数 | 参数说明 | 取值样例 |
|--------|--|---|
| 集群命名空间 | 根据业务需要选择该集群下设置的命名空间。 | default |
| 描述 | 配置项的描述信息。 | - |
| 配置数据 | 用于存储工作负载所需数据库IP地址。 1. 单击“添加和更多配置数据”。 2. 输入“键”：db_config。 3. 输入“值”：需要被审计的数据库IP，涉及多个IP以“,”分隔。 | 键：db_config 值： 192.168.1.31,192.168.0.15 9 |

说明

若还需要为VPC配置，则单击“添加更多配置数据”，输入“键”、“值”。

- 键：vpc_config
- 值：工作负载所属的CCE集群的vpc id

步骤3 单击“创建”。

----结束

4.3.3 创建 Agent 守护进程集工作负载

配置项创建完成后，您需要把数据库安全审计Agent和待审计数据库信息部署到创建的Agent守护进程集中，使待审计的数据库成功连接到数据库安全审计实例，开启数据库安全审计功能。

创建 Agent 守护进程集

步骤1 在左侧导航树中，选择“工作负载 > 守护进程集”，单击“创建守护进程集”，如图4-8所示。

图 4-8 创建守护进程集工作负载



步骤2 设置工作负载基本信息，如图4-9所示，参数说明如表4-3所示。

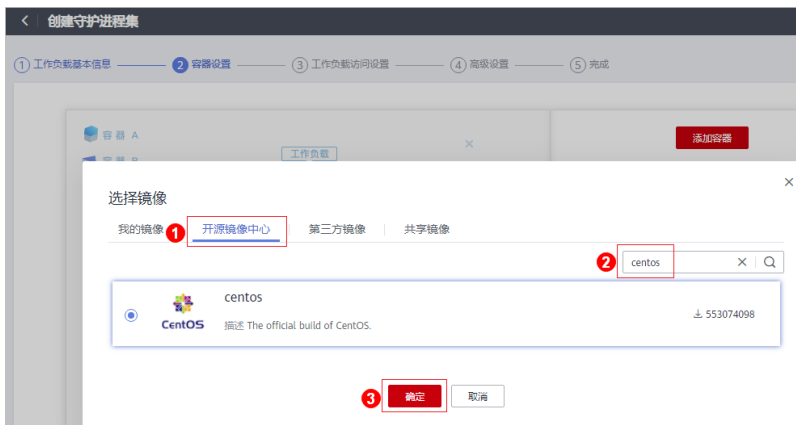
图 4-9 工作负载基本信息

表 4-3 工作负载基本信息参数说明

| 参数 | 说明 | 取值样例 |
|--------|-------------------|--------------|
| 工作负载名称 | 新建工作负载的名称，命名必须唯一。 | agent-docker |
| 集群名称 | 待审计数据库连接的集群。 | scc-cmv-bj4 |
| 命名空间 | 待审计数据库连接的集群的命名空间。 | default |

步骤3 单击“下一步，容器设置 > 添加容器”，在弹出的对话框中，选择“开源镜像中心 > centos”，如图4-10所示，选择后单击“确认”。

图 4-10 选择“centos”镜像



步骤4 设置“centos”镜像参数。

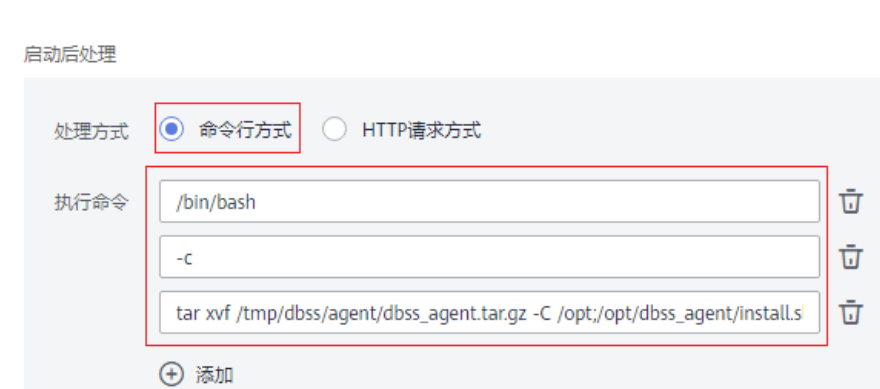
- 展开“基本信息”页签，“镜像版本”选择“centos7.5.1804”，其他保持默认即可。
若所在区域暂不支持选择“centos7.5.1804”版本，请参照[更换镜像版本](#)变更为目标镜像版本。
- 展开“生命周期”页签，设置容器启动和运行时需要的命令。输入以下参数，其他保持默认。
 - 启动命令：容器启动时执行的命令。
`/bin/bash`
`-c`

`while true; do sleep 10; done;`



- 启动后处理：容器成功运行后执行的命令。
 - 处理方式：根据您实际的CPU架构类型选择对应的安装包并执行如下命令
 - CPU为X86架构，请执行如下命令：
`/bin/bash`
`-c`
`tar xvf /tmp/dbss/agent/audit_agent-x86_64-linux-cce.tar.gz -C /opt;/opt/dbss_agent/install.sh;rm -rf /opt/dbss_agent`
 - CPU为ARM架构，请执行如下命令：
`/bin/bash`
`-c`
`tar xvf /tmp/dbss/agent/audit_agent-aarch64-linux-cce.tar.gz -C /opt;/opt/dbss_agent/install.sh;rm -rf /opt/dbss_agent`

图 4-11 容器运行时命令参数



3. 展开“数据存储”页签，为容器挂载额外存储。

- a. 选择“本地磁盘”页签，单击“添加本地磁盘”，在弹出的对话框中，输入以下参数，其他保持默认，如图4-12所示。
- 存储类型：配置项。
 - 配置项：[创建配置项](#)中创建的配置项名称。
 - 挂载路径：挂载配置文件到指定容器目录（/tmp/dbss/db）。

图 4-12 “添加本地磁盘”对话框



- b. 单击“确定”。
- c. 选择“云存储”页签，单击“添加云存储”，在弹出的对话框中，输入以下参数，其他保持默认，如图4-13所示。
- 云存储类型：对象存储
 - 分配方式：使用已有存储
 - 云存储名称：[导入对象存储卷](#)中创建的对象存储PVC名称。
 - 挂载路径：将数据存储挂载到容器上的路径（/tmp/dbss/agent）

图 4-13 “添加云存储”对话框



- d. 单击“确定”。

说明

当数据库配置有变动时，您需要重新挂载云存储并卸载之前配置的云存储。

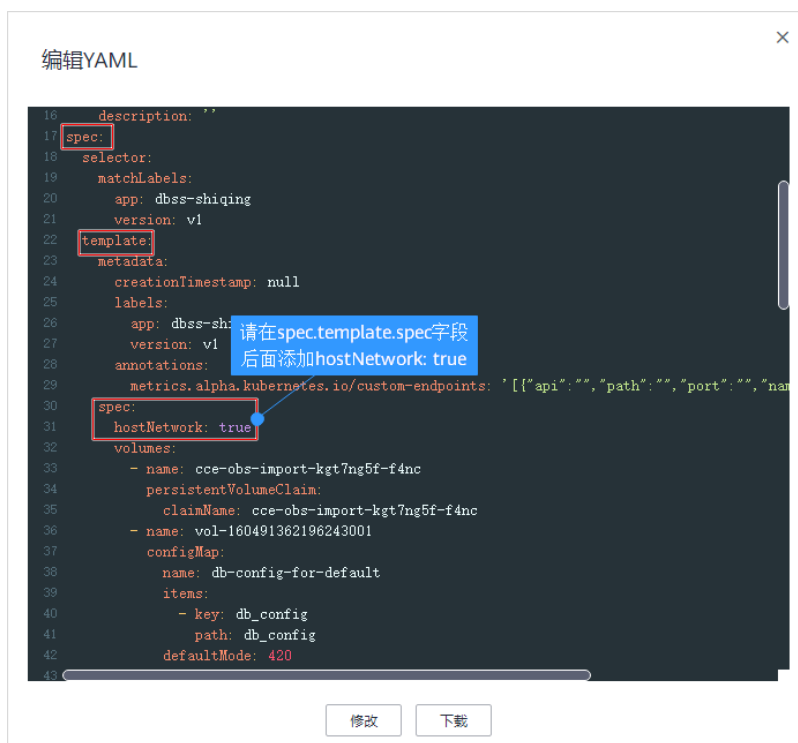
操作步骤：单击工作负载名称，进入工作负载详细信息界面，选择“更新升级 > 高级设置 > 数据存储 > 云存储 > 添加云存储”，添加云存储。

步骤5 工作负载访问设置和高级设置不需要配置，单击“下一步：工作负载访问设置 > 下一步：高级设置 > 创建”，完成创建守护进程工作负载。

步骤6 完成创建后，请返回“工作负载 > 守护进程集”界面，在工作负载列表的“操作”列，单击“更多 > 编辑YAML”。

步骤7 在弹出的“编辑YAML”对话框中，请在spec.template.spec字段后面添加“hostNetwork: true”，如图4-14所示。

图 4-14 编辑 YAML



步骤8 单击“修改”，完成编辑YAML。

步骤9 查看守护进程集工作负载状态。

在工作负载列表中，当工作负载的状态为“运行中”时，表示Agent容器工作负载创建成功。

图 4-15 守护进程集工作负载创建成功

| <input type="checkbox"/> | 工作负载名称 | 状态 | 外部访问地址 | 关联节点数(正常/全部) | 命名空间 | 创建时间 | 操作 |
|--------------------------|--------------|-----|--------|--------------|---------|-------------------|--------------|
| <input type="checkbox"/> | client | 运行中 | -- | 3/3 | default | 2020/04/03 11:... | 日志 升级 更多 |
| <input type="checkbox"/> | agent-docker | 运行中 | -- | 3/3 | default | 2020/04/02 20:... | 日志 升级 更多 |

步骤10 等待2~3分钟，部署生效后返回数据库安全服务控制台。查看Agent状态。

在“数据库列表 > Agent列表”中，当“Agent”“通用”为“是”；“运行状态为”“正在运行”时，如图4-16所示，表示Agent与数据库安全审计实例连接成功。

图 4-16 数据库安全审计连接成功

| 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: mysql-003 类型: MySQL 版本: 5.0 | UTF8 | 192.168.0.177 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负载(%) | 内存峰值(%) | 通用 | 运行状态 | 操作 |
|----------------------|--------|-----------|---------|--------|----------|---------|----|------|----|
| AXDcm1tr3FJ_xcpgqJMs | 应用端 | 10.0.0.74 | LINUX64 | - | 90 | 90 | 是 | 正在运行 | 关闭 |
| AXDcm1hp3FJ_xcpgqJMt | 应用端 | 10.0.0.60 | LINUX64 | - | 90 | 90 | 是 | 正在运行 | 关闭 |

----结束

更换镜像版本

若所在区域暂不支持“centos7.5.1804”版本，请参照以下步骤更换为目标镜像版本“centos7.5.1804”。

步骤1 配置镜像名称。

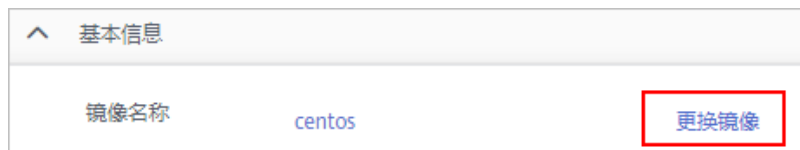
1. 在管理控制台选择“容器 > 容器镜像服务”进入容器镜像服务界面（建议新打开一个窗口进行配置）。
2. 在左侧导航树中，选择“镜像资源 > 镜像中心”，进入“镜像中心”界面。
3. 单击“镜像加速器”，在弹出的“镜像加速器”弹框中，复制加速器地址（不需要“https://”），并在地址尾端添加“/library/centos:centos7.5.1804”。

例如：7b01ab6xxxxfb06b2.mirror.swr.myhuaweicloud.com/library/centos:centos7.5.1804

步骤2 更换镜像版本。

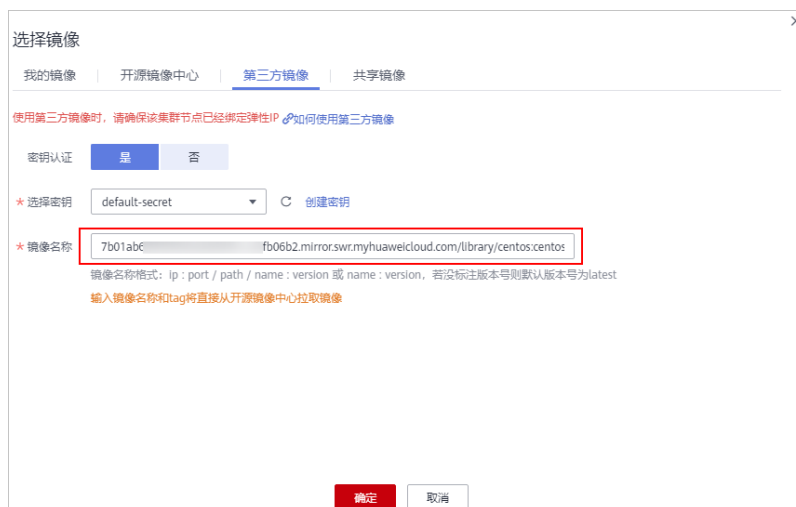
1. 返回设置“centos”镜像参数界面。
2. 单击“镜像名称”栏的“更换镜像”，在弹出的“选择镜像”弹框中，选择“第三方镜像”页签。

图 4-17 更换镜像



3. 在“镜像名称”的输入框中输入**镜像名称**，如图4-18所示。

图 4-18 更换镜像版本



4. 单击“确定”。

----结束

4.4 开启数据库安全审计

待审计的数据库与数据库安全审计实例连接成功后，您需要返回数据库安全服务并开启数据库安全审计。

操作步骤

步骤1 返回数据库安全服务控制台。

步骤2 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3 在待开启数据库安全审计行的“操作”列，单击“开启”。

----结束

4.5 查看审计结果

待审计的数据库与数据库安全审计实例连接成功后，您还需要验证Agent与数据库安全审计实例之间的网络通信是否正常。通信正常，才能正常使用数据库安全审计功能。

验证 Agent 与数据库安全审计实例之间的网络通信正常

安装Agent成功后，在数据库上执行一条SQL语句，稍等几分钟后，登录数据库安全服务控制台，查看操作的SQL语句。

步骤1 登录应用服务器对数据库执行一条SQL语句（例如，“select 1;”）。

步骤2 登录数据库安全服务控制台。

步骤3 在左侧导航树中，选择“总览”，进入“总览”界面。

步骤4 选择“语句”页签。

步骤5 SQL语句列表将显示**步骤1**执行SQL语句的记录，如**图4-19**所示。

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。

图 4-19 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 | select 1; | 192.168.0.140 | 192.168.0.225 | root | -- | 全审计规则 | SHOW | 2020/07/06 17:01:05 GMT+08:00 | 详情 |

---结束

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，可以对成功连接数据库安全审计的所有数据库进行安全审计。待审计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总体审计情况、风险分布、会话统计、SQL分布情况以及审计报告。

您也可以根据业务实际情况配置审计规则，详情请参见：[配置审计规则](#)。

步骤1 查看审计总览信息。

1. 进入总览入口，如**图4-20**所示，查看总览信息。

图 4-20 进入总览入口




2. 选择“语句”或“会话”页签，分别查看SQL语句详细信息和会话分布图情况。

步骤2 查看审计报告。

1. 进入报表管理入口，如**图4-21**所示。

图 4-21 进入报表管理入口



2. 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”。
3. 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。
4. 单击“确定”。

系统跳转到“报表结果”页面，您可以查看报表的生成进度。报表生成后，您可以“预览”或“下载”报表，如图4-22所示。

须知

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

图 4-22 预览或下载报表

| 报表名称 | 关联数据库 | 报表类型 | 生成时间 | 格式 | 状态 | 操作 |
|---------|-------|------|-------------------------------|-----|---|--|
| DDL命令报表 | 全部数据库 | 实时报表 | 2020/03/13 16:46:22 GMT+08:00 | pdf | <div style="width: 100%;"><div style="width: 100%;"></div></div> 100% | 预览 下载 删除 |
| DDL命令报表 | 全部数据库 | 实时报表 | 2020/03/13 16:44:54 GMT+08:00 | pdf | <div style="width: 100%;"><div style="width: 100%;"></div></div> 100% | 预览 下载 删除 |

----结束

5 数据库慢 SQL 检测

操作场景

数据库安全审计默认提供一条“数据库慢SQL检测”的风险操作，用于检测原始审计日志的响应时间大于1秒的SQL语句。

通过数据库慢SQL检测，您可获知执行耗时长、影响行数、执行该SQL语句的数据库信息并根据实际需求对慢SQL进行优化。

数据库安全审计支持以下执行语句类型检测：

- 数据定义（DDL）：
 - CREATE TABLE
 - CREATE TABLESPACE
 - DROP TABLE
 - DROP TABLESPACE
- 数据操作（DML）：
 - INSERT
 - UPDATE
 - DELETE
 - SELECT
 - SELECT FOR UPDATE
- 数据控制（DCL）：
 - CREATE USER
 - DROP USER
 - GRANT

查看慢 SQL 检测结果

数据库慢SQL检测开启后，您可以在“总览 > 语句”中查看执行效率低的语句及语句详细信息。

步骤1 登录管理控制台。


步骤2 在页面上方选择“区域”后，单击 ，选择“安全与合规 > 数据库安全服务”。

步骤3 在左侧导航树中，选择“总览”，进入“总览”界面。

步骤4 在“选择实例”下拉列表框中，选择需要查看数据库慢SQL语句信息的实例。

步骤5 选择“语句”页签。

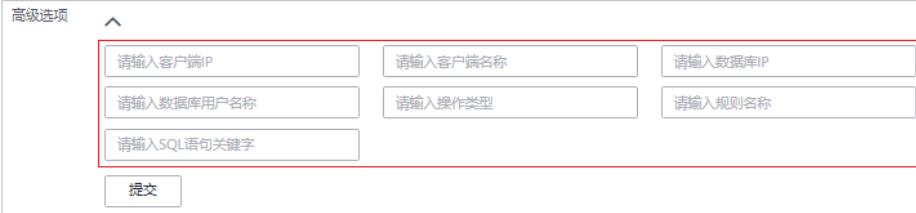
步骤6 您可以按照以下方法，查询指定的SQL语句。

- 选择“时间”（“全部”、“近30分钟”、“近1小时”、“近24小时”、“近7天”或“近30天”），或者单击，选择开始时间和结束时间，单击“提交”，列表显示该时间段的SQL语句。
- 选择“风险等级”（“低”，数据库慢SQL规则默认为低），单击“提交”，列表显示该级别的SQL语句。
- 单击“高级选项”后的▼，输入相关信息，如[图5-1](#)所示，单击“搜索”，列表显示该选项的SQL语句。

说明

一次查询最多可查询10,000条记录。

图 5-1 高级选项信息



高级选项

请输入客户端IP 请输入客户端名称 请输入数据库IP

请输入数据库用户名称 请输入操作类型 请输入规则名称

请输入SQL语句关键字

提交

步骤7 在需要查看详情的慢SQL语句所在行的“操作”列，单击“详情”，如[图5-2](#)所示。

图 5-2 查看慢 SQL 语句详情

| 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 | SELECT * FROM Information_schema.T... | 10.159.19.246 | 192.168.0.177 | root | 低 | 全审计视图数据库慢SQL检测 | SELECT | 2020/11/05 16:11:42 GMT+08:00 | 详情 |

步骤8 在详情提示框中，查看慢SQL语句的详细信息，如[图5-3](#)所示，相关参数说明如[表5-1](#)所示。

图 5-3 “详情”提示框



表 5-1 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 | 执行SQL语句所在的数据库的IP地址。 |
| 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。 |
| 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

查看数据库慢 SQL 检测规则

您可以在“审计规则 > 风险操作”中查看数据库慢SQL检测规则，并根据需要执行以下操作：

图 5-4 数据库慢 SQL 检测



- 启用
在数据库慢SQL检测规则所在行的“操作”列，单击“启用”，数据库安全审计将对该规则进行审计。
- 编辑
在数据库慢SQL检测规则所在行的“操作”列，单击“编辑”，在风险操作界面，您可以修改数据库慢SQL检测规则。
- 禁用
在数据库慢SQL检测规则所在行的“操作”列，单击“禁用”，在弹出的对话框中，单击“确定”，可以禁用该数据库慢SQL检测规则。禁用数据库慢SQL检测规则后，该规则将不在审计中执行。
- 删除
在数据库慢SQL检测规则所在行的“操作”列，单击“删除”，在弹出的对话框中，单击“确定”，可以删除该规则。删除数据库慢SQL检测规则后，如果需要对该规则进行安全审计，请重新添加**数据库慢SQL检测规则**。详细操作步骤，请参见：[添加风险操作](#)。

6 数据库拖库检测

操作场景

数据库安全审计默认提供一条“数据库拖库检测”的风险操作，用于检测原始审计日志疑似拖库的SQL语句，及时发现数据安全风险。

通过数据库拖库检测，您可获知执行耗时长、影响行数、执行该SQL语句的数据库信息。

数据库安全审计支持以下执行语句类型检测：

- 数据定义（DDL）：
 - CREATE TABLE
 - CREATE TABLESPACE
 - DROP TABLE
 - DROP TABLESPACE
- 数据操作（DML）：
 - INSERT
 - UPDATE
 - DELETE
 - SELECT
 - SELECT FOR UPDATE
- 数据控制（DCL）：
 - CREATE USER
 - DROP USER
 - GRANT

配置数据库拖库检测

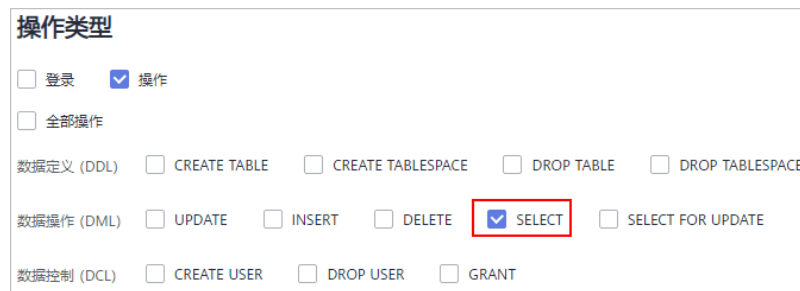
在启用数据库拖库检测规则前，还需要用户根据业务实际需求添加待审计的数据库、客户端IP/IP段、操作类型、操作对象及执行结果。

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击 ，选择“安全与合规 > 数据库安全服务”。

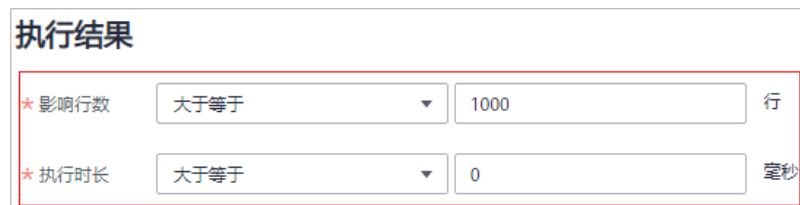
- 步骤3** 在左侧导航树中，选择“审计规则”，进入“审计规则”界面。
- 步骤4** 在“选择实例”下拉列表框中，选择需要配置数据库拖库检测的实例。
- 步骤5** 选择“风险操作”页签。
- 步骤6** 在数据库拖库检测行的“操作”列，单击“编辑”，进入“编辑风险操作”界面。
- 步骤7** （可选）配置“客户端IP/IP段”，不配置系统默认检测全部。
- 步骤8** “操作类型”：选择“SELECT”。

图 6-1 操作类型



- 步骤9** （可选）设置“操作对象”，不配置系统默认检测全部。
 1. 单击操作对象后，输入“目标数据库”、“目标表”和“字段”信息。
 2. 单击“确定”。
- 步骤10** 配置“执行结果”区域中的“影响行数”和“执行时长”。

图 6-2 执行结果



须知

当您的应用程序发生变化（如：服务升级、代码变更）时，需要根据实际情况修改“影响行数”的参数，以免审计不完全。

- 步骤11** 单击“保存”。

----结束

查看数据库拖库检测结果

数据库拖库检测开启后，您可以在“总览 > 语句”中，查看原始审计日志疑似拖库的SQL语句。

- 步骤1** 登录管理控制台。



步骤2 在页面上方选择“区域”后，单击 ，选择“安全与合规 > 数据库安全服务”。

步骤3 在左侧导航树中，选择“总览”，进入“总览”界面。

步骤4 在“选择实例”下拉列表框中，选择需要查看数据库拖库检测语句信息的实例。

步骤5 选择“语句”页签。

步骤6 您可以按照以下方法，查询指定的SQL语句。

- 选择“时间”（“全部”、“近30分钟”、“近1小时”、“近24小时”、“近7天”或“近30天”），或者单击 ，选择开始时间和结束时间，单击“提交”，列表显示该时间段的SQL语句。
- 选择“风险等级”（“高”，数据库拖库检测规则默认为高），单击“提交”，列表显示该级别的SQL语句。
- 单击“高级选项”后的 ，输入相关信息，如**图6-3**所示，单击“搜索”，列表显示该选项的SQL语句。

说明

一次查询最多可查询10,000条记录。

图 6-3 高级选项信息



高级选项 

请输入客户端IP 请输入客户端名称 请输入数据库IP

请输入数据库用户名称 请输入操作类型 请输入规则名称

请输入SQL语句关键字

步骤7 在需要查看数据库拖库检测详情的SQL语句所在行的“操作”列，单击“详情”，如**图6-4**所示。

图 6-4 查看拖库检测详情

| 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 | select tttttttt1.SalesOrderID, tttttttt... | 192.168.0.223 | 192.168.0.78 | root | 高 | 全审计规则_数据库拖库检测 | SELECT | 2020/10/29 14:31:32 GMT+08:00 | 详情 |
| 2 | select tttttttt1.SalesOrderID, tttttttt... | 192.168.0.223 | 192.168.0.78 | root | 高 | 全审计规则_数据库拖库检测 | SELECT | 2020/10/29 14:31:32 GMT+08:00 | 详情 |

步骤8 在详情提示框中，查看数据库拖库SQL语句的详细信息，如**图6-5**所示，相关参数说明如**表6-1**所示。

图 6-5 “详情”提示框

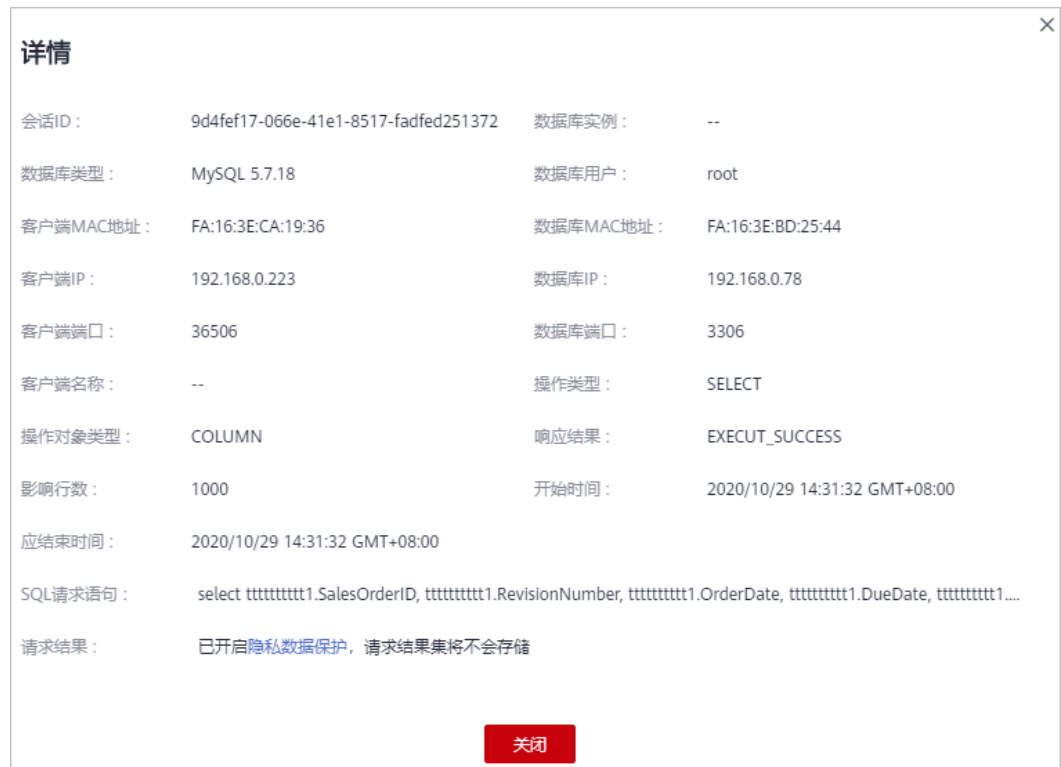


表 6-1 SQL 语句详情参数说明

| 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 | 执行SQL语句所在的数据库的IP地址。 |
| 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。 |
| 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

查看数据库拖库检测规则

您可以在“审计规则 > 风险操作”中查看数据库慢SQL检测规则，并根据需要执行以下操作：

图 6-6 数据库慢 SQL 检测



- 启用**

在数据库拖库检测规则所在行的“操作”列，单击“启用”，数据库安全审计将对该规则进行审计。
- 编辑**

在数据库拖库检测规则所在行的“操作”列，单击“编辑”，在风险操作界面，您可以修改数据库拖库检测规则。
- 禁用**

在数据库拖库检测规则所在行的“操作”列，单击“禁用”，在弹出的对话框中，单击“确定”，可以禁用该数据库拖库检测规则。禁用数据库拖库检测规则后，该规则将不在审计中执行。
- 删除**

在数据库拖库检测规则所在行的“操作”列，单击“删除”，在弹出的对话框中，单击“确定”，可以删除该规则。删除数据库拖库检测规则后，如果需要对规则进行安全审计，请重新添加数据库拖库检测规则。详细操作步骤，请参见：[添加风险操作](#)。

7 数据库脏表检测

操作场景

数据库安全审计规则可增加一条“数据库脏表检测”的高风险操作。用户预设无用的库、表或列作为“脏表”，无风险程序不会访问用户自建的“脏表”，用于检测访问“脏表”的可能的恶意程序。

通过数据库脏表检测，可以帮助您监控识别访问“脏表”的SQL语句，及时发现数据安全风险。

前提条件

用户需要在待审计的实例中添加无用的数据库、表或字段，作为脏表检测的对象。

配置数据库脏表检测

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击 ，选择“安全与合规 > 数据库安全服务”。

步骤3 在左侧导航树中，选择“审计规则”，进入“审计规则”界面。

步骤4 在“选择实例”下拉列表框中，选择需要配置数据库脏表检测的实例。

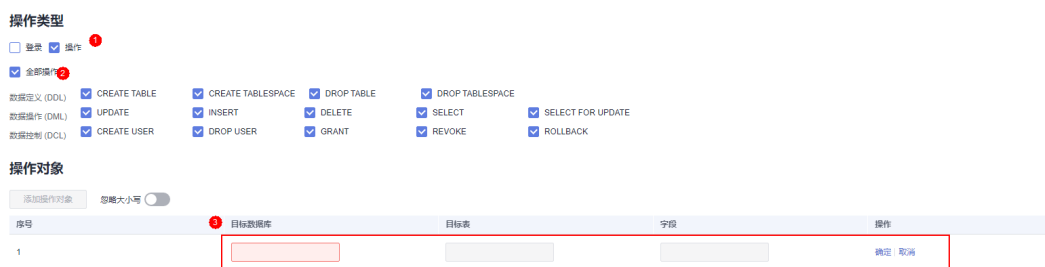
步骤5 选择“风险操作”页签。单击“添加风险操作”增加脏表检测规则。

步骤6 基本信息中将“风险等级”配置为“高”。

步骤7 （可选）配置“客户端IP/IP段”，不配置系统默认检测全部。

步骤8 配置操作类型，选择“操作”和“全部操作”。配置操作对象填写实例中添加无用的数据库、表或字段，如图7-1所示。

图 7-1 添加脏表检测规则



步骤9 单击“保存”。

----结束

查看数据库脏表检测结果

数据库脏表检测开启后，您可以在“总览 > 语句”中，查看原始审计日志访问脏表的SQL语句。

步骤1 登录管理控制台。



步骤2 在页面上方选择“区域”后，单击 ，选择“安全与合规 > 数据库安全服务”。

步骤3 在左侧导航树中，选择“总览”，进入“总览”界面。

步骤4 在“选择实例”下拉列表框中，选择需要查看数据库脏表检测语句信息的实例。

步骤5 选择“语句”页签。

步骤6 您可以按照以下方法，查询指定的SQL语句。

- 选择“时间”（“全部”、“近30分钟”、“近1小时”、“近24小时”、“近7天”或“近30天”），或者单击 ，选择开始时间和结束时间，单击“提交”，列表显示该时间段的SQL语句。
- 选择“风险等级”（“高”，数据库脏表检测规则默认为高），单击“提交”，列表显示该级别的SQL语句。
- 单击“高级选项”后的 ，输入相关信息，如 [图7-2](#)所示，单击“搜索”，列表显示该选项的SQL语句。

说明

一次查询最多可查询10,000条记录。

图 7-2 高级选项信息



高级选项

| | | |
|-------------|----------|----------|
| 请输入客户端IP | 请输入客户端名称 | 请输入数据库IP |
| 请输入数据库用户名称 | 请输入操作类型 | 请输入规则名称 |
| 请输入SQL语句关键字 | | |

提交

步骤7 在需要查看数据库脏表检测详情的SQL语句所在行的“操作”列，单击“详情”，在详情提示框中，查看数据库访问脏表的SQL语句的详细信息，如 [图7-3](#)所示，相关参数说明如 [表7-1](#)所示。

图 7-3 “详情”提示框



表 7-1 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 | 执行SQL语句所在的数据库的IP地址。 |
| 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。 |
| 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

查看脏表检测规则

您可以在“审计规则 > 风险操作”中查看数据库脏表检测规则，并根据需要执行以下操作：

- 启用
在数据库脏表检测规则所在行的“操作”列，单击“启用”，数据库安全审计将对该规则进行审计。
- 编辑
在数据库脏表检测规则所在行的“操作”列，单击“编辑”，在风险操作界面，您可以修改数据库脏表检测规则。
- 禁用
在数据库脏表检测规则所在行的“操作”列，单击“禁用”，在弹出的对话框中，单击“确定”，可以禁用该数据库脏表检测规则。禁用数据库脏表检测规则后，该规则将不在审计中执行。
- 删除
在数据库脏表检测规则所在行的“操作”列，单击“删除”，在弹出的对话框中，单击“确定”，可以删除该规则。删除数据库脏表检测规则后，如果需要对该规则进行安全审计，请重新添加数据库脏表检测规则。详细操作步骤，请参见：[添加风险操作](#)。

8 Oracle RAC 集群审计配置最佳实践

在使用Oracle RAC集群的DBSS时，RAC集群中的每一个节点都是作为一个独立的数据库，在配置时需要为集群中的每一个节点安装Agent，以实现网络流量的转发。

配置说明

由于添加的实例数受购买的DBSS版本所限制，因此配置前需确认已购买版本所支持添加的最大实例数是否与RAC集群节点数一致或多于节点数。

示例：

- 若您的RAC集群节点不超过3个，则您购买基础版即可满足需求；
- 若您的RAC集群节点不超过6个，则您购买专业版即可满足需求；
- 若您的RAC集群中超过6个节点，则您需购买高级版才可满足需求；

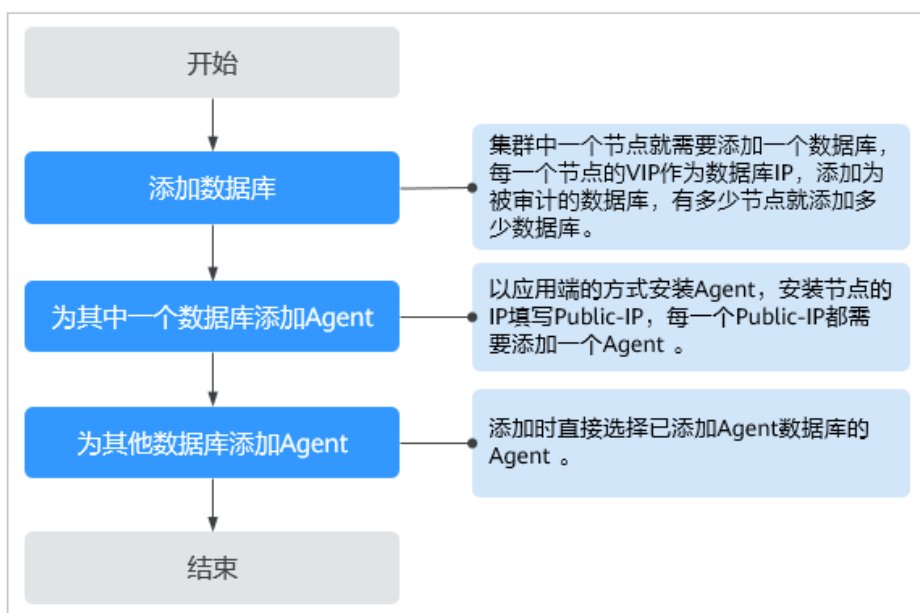
表 8-1 DBSS 版本性能及规格说明

| 版本 | 支持的数据库实例 | 系统资源要求 | 性能参数 |
|-----|-------------|---|---|
| 基础版 | 最多支持3个数据库实例 | <ul style="list-style-type: none"> ● CPU: 4U ● 内存: 16GB ● 硬盘: 500GB | <ul style="list-style-type: none"> ● 吞吐量峰值: 3,000条/秒 ● 入库速率: 360万条/小时 ● 4亿条在线SQL语句存储 ● 50亿条归档SQL语句存储 |
| 专业版 | 最多支持6个数据库实例 | <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 |

| 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 | <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 |

配置流程

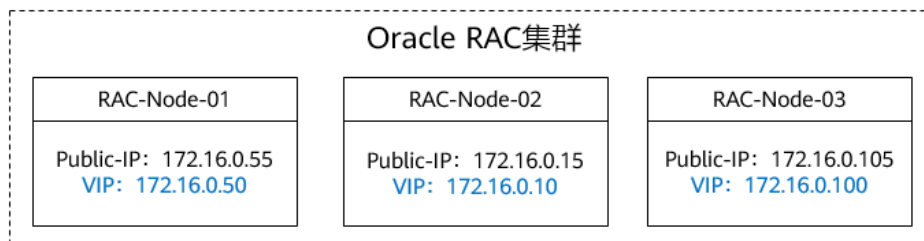
通过添加数据库和Agent即可完成RAC集群的审计配置。



前提条件

- 已购买DBSS实例。
- 需要准备好集群内所有节点的Public-IP和VIP两个字段值。

示例：准备开启DBSS的Oracle RAC集群有三个节点。



操作步骤

- 步骤1** 登录华为云控制台后进入数据库安全服务，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2 在“选择实例”下拉列表框中，选择需要添加数据库的实例，在数据库列表框左上方，单击“添加数据库”。

步骤3 在弹出的对话框中，填写RAC集群数据库的信息。

示例：添加RAC集群节点RAC-Node-01的数据库。

图 8-1 添加 Oracle 数据库

表 8-2 数据库参数说明

| 参数名称 | 参数说明 | 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”。 | 自建数据库 |
| 数据库类型 | 支持的数据库类型。 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。 | ORACLE |
| 数据库名称 | 您可以自定义添加的数据库的名称。 | test01 |
| IP地址 | 添加的数据库的IP地址。 填写预先准备好的集群节点的VIP字段值。 | 172.16.0.50 |
| 端口 | 添加的数据库开放的端口。 Oracle数据库端口默认值为1521。 | 1521 |
| 数据库版本 | 支持的数据库版本。 <ul style="list-style-type: none"> “数据库类型”选择“ORACLE”，根据需求可以选择以下版本： <ul style="list-style-type: none"> - 11g - 12c - 19c | 11g |

| 参数名称 | 参数说明 | 取值样例 |
|-------|---|---------|
| 实例名 | 您可以指定需要审计的数据库的实例名称。 说明 <ul style="list-style-type: none"> 如果实例名为空，数据库安全审计将审计数据库中所有的实例。 如果填写实例名，数据库安全审计将审计填写的实例，最多可填写5个实例名，且实例名以“;”分隔。 | - |
| 选择字符集 | 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： <ul style="list-style-type: none"> UTF-8 GBK | UTF-8 |
| 操作系统 | 添加的数据库运行的操作系统，根据所使用的数据库类型选择操作系统： <ul style="list-style-type: none"> LINUX64 WINDOWS64 | LINUX64 |

步骤4 确认无误，单击“确认”，添加RAC-Node-01节点的数据库完成。

参照**步骤3**将RAC-Node-02、RAC-Node-03节点依次完成添加，所有数据库添加完成后在数据库列表查看已添加的数据库，如图8-2所示。

示例：已完成集群内所有节点的数据库添加，分别是：test01、test02、test03。

图 8-2 集群节点全部添加完成



步骤5 单击已添加的任一数据库的“添加Agent”。

示例：首先为test01数据库添加Agent。

图 8-3 添加 Agent



步骤6 在弹窗中填写添加Agent的相关信息，参数说明如表8-3所示。

示例：添加节点RAC-Node-01的Agent。

图 8-4 填写添加 Agent 的信息

表 8-3 首次添加 Agent 的参数说明

| 参数名称 | 参数说明 | 取值样例 |
|--------|---|-------------|
| 添加方式 | 添加Agent的方式 <ul style="list-style-type: none"> 选择已有Agent。 创建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。 <ul style="list-style-type: none"> 数据库端 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。 配置RAC集群时，填写集群节点Public-IP字段的值。 | 172.16.0.55 |
| 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。 | test-rac-01 |

| 参数名称 | 参数说明 | 取值样例 |
|-----------|--|-------------|
| CPU阈值 (%) | <p>可选参数。“安装节点类型”选择“应用端”时，可以配置该参数。</p> <p>指待审计的应用端节点的CPU阈值，默认值为“80”。</p> <p>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。</p> | 80 |
| 内存阈值 (%) | <p>可选参数。“安装节点类型”选择“应用端”时，可以配置该参数。</p> <p>指待审计的应用端节点的内存阈值，默认值为“80”。</p> <p>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。</p> | 80 |
| 操作系统 | <p>可选参数。“安装节点类型”选择“应用端”时，可以配置该参数。</p> <p>指待审计的应用端节点的操作系统，可以选择“LINUX64”或“WINDOWS64”。</p> | LINUX64_X86 |

步骤7 单击“确认”，完成RAC-Node-01节点的Agent添加。

参照**步骤6**操作继续在test01数据库添加RAC-Node-02、RAC-Node-03节点的Agent，添加完成后展开test01数据库确认全部节点的Agent添加完成，如图8-5所示。

示例：已完成RAC集群所有节点在test01数据库的Agent添加，Agent ID分别为：p7U_dIQBUQf7E9XurmjX、rLVIdIQBUQf7E9Xug2iQ、rrVIdIQBUQf7E9Xu3Wja。

图 8-5 查看添加的 Agent

| 名称 | 选择字符集 | IP地址/端口 | 实例名 | 操作系统 | 审计状态 | Agent | 操作 | | | |
|-------------------------------------|---------|----------------------|-------------|-------------|---------|---------|-------|------|-----------------|------------------|
| 名称: test01 类型: ORACLE 版本: 11g | UTF8 | 172.16.0.50 1521 | -- | LINUX64 | 已关闭 | 添加Agent | 开启 删除 | | | |
| AgentID | 安装节点... | 安装节点IP | 操作系统 | 审计网未... | CPU阈... | 内存阈... | 通用 | 运行状态 | SHA256校验值 | 操作 |
| p7U_dIQBUQf7E9XurmjX | 应用端 | 172.16.0.55 | LINUX64_... | test-rac-01 | 80 | 80 | 否 | 休眠中 | d4c8a188468... | 下载agent 关闭 删除... |
| rLVIdIQBUQf7E9Xug2iQ | 应用端 | 172.16.0.15 | LINUX64_... | test-rac-02 | 80 | 80 | 否 | 休眠中 | f30822677749... | 下载agent 关闭 删除... |
| rrVIdIQBUQf7E9Xu3Wja | 应用端 | 172.16.0.105 | LINUX64_... | test-rac-03 | 80 | 80 | 否 | 休眠中 | a892e55ff96a... | 下载agent 关闭 删除... |
| 名称: test02 类型: ORACLE 版本: 11g | UTF8 | 172.16.0.10 1521 | -- | LINUX64 | 已关闭 | 添加Agent | 开启 删除 | | | |
| 名称: test03 类型: ORACLE 版本: 11g | UTF8 | 172.16.0.100 1521 | -- | LINUX64 | 已关闭 | 添加Agent | 开启 删除 | | | |

步骤8 test01数据库的Agent全部添加完成后，需为test02、test03集群数据库添加Agent。单击test02数据库“Agent”列的“添加Agent”。

步骤9 在弹窗中填写添加Agent的相关信息，参数说明如表8-4所示。

示例：为test02数据库添加Agent。

说明

test02数据库添加的Agent需与test01数据库添加的Agent保持一致，直接选择test01数据库已添加的Agent即可。

图 8-6 添加已有的 Agent

表 8-4 添加已有 Agent 的参数说明

| 参数名称 | 参数说明 | 取值样例 |
|---------|---|----------------------|
| 添加方式 | 添加Agent的方式 <ul style="list-style-type: none"> 选择已有Agent。 创建Agent | 选择已有Agent |
| 数据库名称 | 选择已添加Agent的数据库。 示例： 在集群中test01数据库已添加Agent，因此选择test01数据库。 | test01 |
| AgentID | 在选择的数据库中选择添加的Agent ID。 示例： 在test01数据库累计添加了三个节点的Agent，单次任一选择一个即可，需依次完成三个Agent的添加。 | p7U_dIQBUQf7E9XurmjX |

步骤10 单击“确认”，完成已有Agent在test02数据库的添加。

参照**步骤8**和**步骤9**完成另外两个Agent的添加，添加完成后，确认test01数据库与test02数据库中的Agent完全保持一致。

图 8-7 确认 Agent 保持一致

| 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 | | | |
|-------------------------------------|-------|---------------------|-------------|-------------|------|---------|-------|-----|-----------------|-----------------|
| 名称: test01 类型: ORACLE 版本: 11g | UTF8 | 172.16.0.50 1521 | -- | LINUX64 | 已关闭 | 添加Agent | 开启 删除 | | | |
| AgentID | | | | | | | | | | |
| p7U_dIQBUQ7E9XurmpX | 应用端 | 172.16.0.55 | LINUX64_... | test-rac-01 | 80 | 80 | 否 | 休眠中 | d4c8a188468... | 下载agent 关闭 删除.. |
| rLVidiQBUIQ7E9Xug2IQ | 应用端 | 172.16.0.15 | LINUX64_... | test-rac-02 | 80 | 80 | 否 | 休眠中 | f30822677749... | 下载agent 关闭 删除.. |
| rVidiQBUIQ7E9Xu3Vjja | 应用端 | 172.16.0.105 | LINUX64_... | test-rac-03 | 80 | 80 | 否 | 休眠中 | a892e55f96a... | 下载agent 关闭 删除.. |
| 名称: test02 类型: ORACLE 版本: 11g | UTF8 | 172.16.0.10 1521 | -- | LINUX64 | 已关闭 | 添加Agent | 开启 删除 | | | |
| AgentID | | | | | | | | | | |
| p7U_dIQBUQ7E9XurmpX | 应用端 | 172.16.0.55 | LINUX64_... | test-rac-01 | 80 | 80 | 否 | 休眠中 | d4c8a188468... | 下载agent 关闭 删除.. |
| rLVidiQBUIQ7E9Xug2IQ | 应用端 | 172.16.0.15 | LINUX64_... | test-rac-02 | 80 | 80 | 否 | 休眠中 | f30822677749... | 下载agent 关闭 删除.. |
| rVidiQBUIQ7E9Xu3Vjja | 应用端 | 172.16.0.105 | LINUX64_... | test-rac-03 | 80 | 80 | 否 | 休眠中 | a892e55f96a... | 下载agent 关闭 删除.. |

步骤11 参照步骤8~步骤10完成test03数据库的Agent添加，完成后确认RAC集群内所有数据库的Agent均保持一致。

示例：集群部署完成后，test01、test02、tes03三个数据库所添加的Agent保持一致，且与集群节点数保持一致。

图 8-8 集群内所有 Agent 保持一致

| 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 | | | |
|-------------------------------------|-------|----------------------|-------------|-------------|------|---------|-------|-----|-----------------|-----------------|
| 名称: test01 类型: ORACLE 版本: 11g | UTF8 | 172.16.0.50 1521 | -- | LINUX64 | 已关闭 | 添加Agent | 开启 删除 | | | |
| AgentID | | | | | | | | | | |
| p7U_dIQBUQ7E9XurmpX | 应用端 | 172.16.0.55 | LINUX64_... | test-rac-01 | 80 | 80 | 否 | 休眠中 | d4c8a188468... | 下载agent 关闭 删除.. |
| rLVidiQBUIQ7E9Xug2IQ | 应用端 | 172.16.0.15 | LINUX64_... | test-rac-02 | 80 | 80 | 否 | 休眠中 | f30822677749... | 下载agent 关闭 删除.. |
| rVidiQBUIQ7E9Xu3Vjja | 应用端 | 172.16.0.105 | LINUX64_... | test-rac-03 | 80 | 80 | 否 | 休眠中 | a892e55f96a... | 下载agent 关闭 删除.. |
| 名称: test02 类型: ORACLE 版本: 11g | UTF8 | 172.16.0.10 1521 | -- | LINUX64 | 已关闭 | 添加Agent | 开启 删除 | | | |
| AgentID | | | | | | | | | | |
| p7U_dIQBUQ7E9XurmpX | 应用端 | 172.16.0.55 | LINUX64_... | test-rac-01 | 80 | 80 | 否 | 休眠中 | d4c8a188468... | 下载agent 关闭 删除.. |
| rLVidiQBUIQ7E9Xug2IQ | 应用端 | 172.16.0.15 | LINUX64_... | test-rac-02 | 80 | 80 | 否 | 休眠中 | f30822677749... | 下载agent 关闭 删除.. |
| rVidiQBUIQ7E9Xu3Vjja | 应用端 | 172.16.0.105 | LINUX64_... | test-rac-03 | 80 | 80 | 否 | 休眠中 | a892e55f96a... | 下载agent 关闭 删除.. |
| 名称: test03 类型: ORACLE 版本: 11g | UTF8 | 172.16.0.100 1521 | -- | LINUX64 | 已关闭 | 添加Agent | 开启 删除 | | | |
| AgentID | | | | | | | | | | |
| p7U_dIQBUQ7E9XurmpX | 应用端 | 172.16.0.55 | LINUX64_... | test-rac-01 | 80 | 80 | 否 | 休眠中 | d4c8a188468... | 下载agent 关闭 删除.. |
| rLVidiQBUIQ7E9Xug2IQ | 应用端 | 172.16.0.15 | LINUX64_... | test-rac-02 | 80 | 80 | 否 | 休眠中 | f30822677749... | 下载agent 关闭 删除.. |
| rVidiQBUIQ7E9Xu3Vjja | 应用端 | 172.16.0.105 | LINUX64_... | test-rac-03 | 80 | 80 | 否 | 休眠中 | a892e55f96a... | 下载agent 关闭 删除.. |

步骤12 集群数据库及Agent配置完成后，可继续完成添加安全组规则、下载及安装Agent、开启审计等操作。

操作详情请参见[添加安全组规则](#)、[下载并安装Agent](#)、[开启数据库安全审计](#)。

----结束

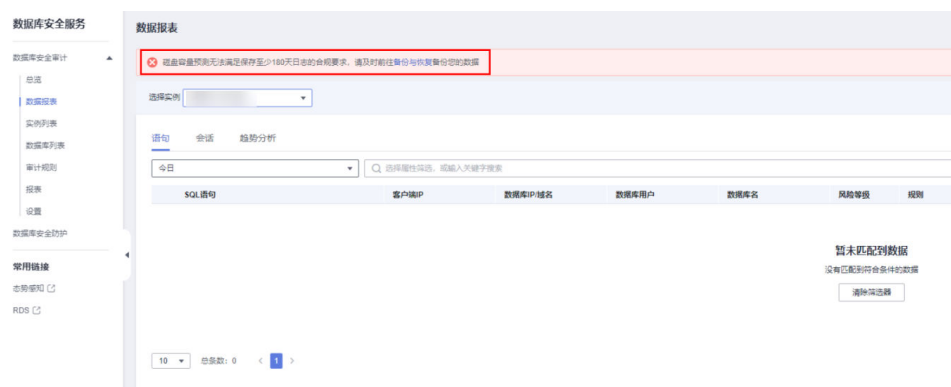
9 数据库安全审计等保最佳实践

DBSS可以从审计日志的天数、审计合规的报表、审计日志的隐私合规的配置来进一步满足等保合规。

审计日志天数的合规配置

相关审计法规规定，审计日志至少保留半年。DBSS服务会自动预测审计实例的剩余存储空间是否能够满足半年审计日志的合规要求，若不满足会给出界面提示。

图 9-1 磁盘不足提示



当出现如图9-1所示提示时，请开启自动备份，开启备份详情请参见[自动备份数据库审计日志](#)。

说明

- 开启自动备份时，备份周期优先选择“每小时”。
- 若每天的备份文件大小总和小于50MB时，建议选择“每天”。

审计报表的合规配置

为了能够更及时、准确的了解合规状况，建议开启审计报表计划任务。

建议您优先设置如图9-2所示的报表计划任务。

图 9-2 报表合规设置项

| 报表模板名称 | 关联数据库 | 类型 | 描述 | 计划任务状态 | 操作 |
|--------------|-------|-----------|--------------|---------|-------------|
| 数据库安全审计报表 | 全部数据库 | 综合报表 | 数据库安全审计报表 | 已关闭(每周) | 设置任务 立即生成报表 |
| SOX-萨班斯报表 | 全部数据库 | 合规报表 | SOX-萨班斯报表 | 已关闭(每周) | 设置任务 立即生成报表 |
| 数据库安全合规报表 | 全部数据库 | 合规报表 | 数据库安全合规报表 | 已关闭(每周) | 设置任务 立即生成报表 |
| 数据库服务器审计分析报表 | 全部数据库 | 数据库专项报表 | 数据库服务器审计分析报表 | 已关闭(每周) | 设置任务 立即生成报表 |
| 客户端IP分析报表 | 全部数据库 | 客户端专项报表 | 客户端IP分析报表 | 已关闭(每周) | 设置任务 立即生成报表 |
| DDL命令报表 | 全部数据库 | 数据库操作专项报表 | DDL命令报表 | 已关闭(每周) | 设置任务 立即生成报表 |
| DCL命令报表 | 全部数据库 | 数据库操作专项报表 | DCL命令报表 | 已关闭(每周) | 设置任务 立即生成报表 |
| DML命令报表 | 全部数据库 | 数据库操作专项报表 | DML命令报表 | 已关闭(每周) | 设置任务 立即生成报表 |

单击“设置任务”可对计划任务的参数进行设置，参数说明如表9-1所示。

图 9-3 选择计划任务参数

计划任务

消息通知触发的消息由消息通知服务发送，可能产生少量费用，具体费用由消息通知服务结算。[了解计费详情](#)

* 启动任务

* 消息通知

* 消息通知主题 [查看消息通知主题](#)
下拉框只展示订阅状态为“已确认”的消息通知主题。







* 报表类型

* 执行方式

* 执行时间

* 数据库

表 9-1 计划任务参数说明

| 参数名称 | 参数说明 | 取值样例 |
|--------|--|---|
| 启动任务 | 启动当前任务的开关。 <ul style="list-style-type: none"> 关闭:  开启:  |  |
| 消息通知 | 生成报表后是否发送通知。 <ul style="list-style-type: none"> 关闭:  开启:  |  |
| 消息通知主题 | “消息通知”选择开启时在此项选择预设的消息通知主题。 | - |
| 报表类型 | 选择报表生成的周期类型。 <ul style="list-style-type: none"> 日报: 若每天审计日志量超过1000万条, 建议选择日报。 周报: 若每天的审计日志量超过1万但不超过1000万条, 建议选择周报。 月报: 若每天审计日志量不超过1万条, 可以选择月报。 | 周报 |
| 执行方式 | 计划任务创建后执行的次数。 <ul style="list-style-type: none"> 周期执行: 按照报表类型循环周期性执行。 执行一次: 计划任务执行一次之后不再执行。 | 周期执行 |
| 执行时间 | 目标任务执行的具体时间点, 可选择24小时内的任一整点时间。 创建任务后紫铜自动执行, 建议选择在工作负载较低的时间段, 如: 凌晨。 | 2点 |
| 数据库 | 选择需要执行目标任务的数据库, 可选择全部数据库, 也可选择具体的单个数据库。 | 全部数据库 |

审计日志隐私的合规配置

由于审计日志中的SQL请求语句和结果集中可能包含用户的隐私数据, 建议对审计日志开启隐私数据保护, 以防止违反隐私保护相关合规要求。

通过配置如下可满足隐私数据的合规要求:

- 开启“隐私数据脱敏”开关: 开启后会对审计日志中的隐私数据进行脱敏存储。
- 关闭“存储结果集”开关: 关闭后, 审计日志含有隐私信息的结果集将不会存储到审计日志中。
- 开启所有的隐私保护规则。

图 9-4 审计日志隐私合规配置



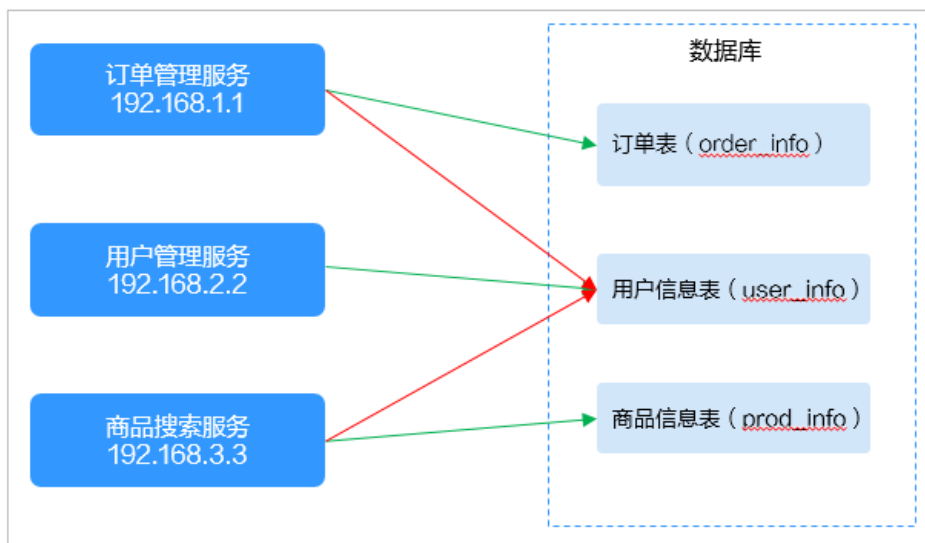
10 数据库审计实例规则配置最佳实践

建议您开启风险告警，配置了风险告警后，当数据库访问触发了审计规则时，DBSS才能及时将风险通知给您，操作详情请参见[设置告警通知](#)。

场景一：核心资产数据库表的异常访问、告警

示例：某电商网站后台分为多个微服务，分别为订单管理服务、用户管理服务、商品搜索服务等，各服务部署在不同的服务节点上，有不同IP地址，如图10-1所示。

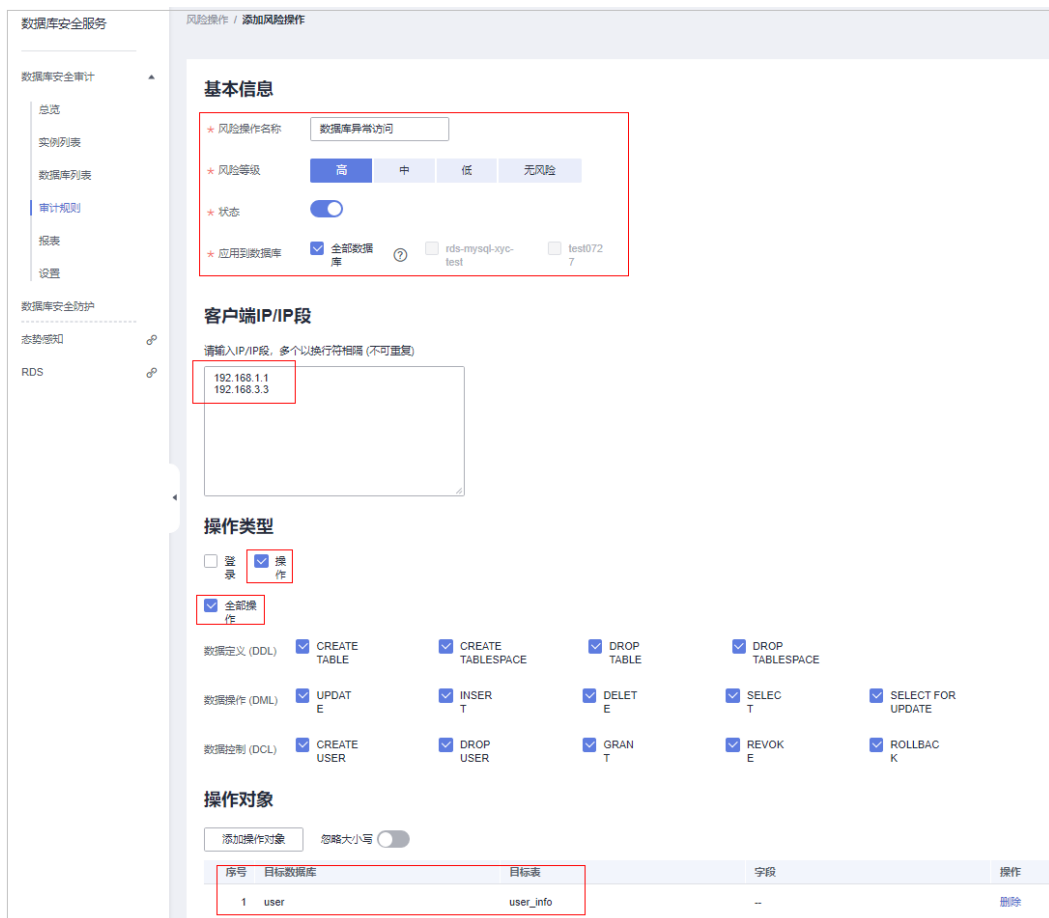
图 10-1 服务器部署拓扑图



绿色箭头为正常访问路径，如果订单管理服务或商品搜索服务两个节点被攻陷，攻击者会从这两个节点去访问数据库的用户信息表，意图窃取用户信息，就属于数据库的异常访问。

在DBSS中可通过如下规则设置来检测数据库异常访问情况：

图 10-2 添加数据库异常访问

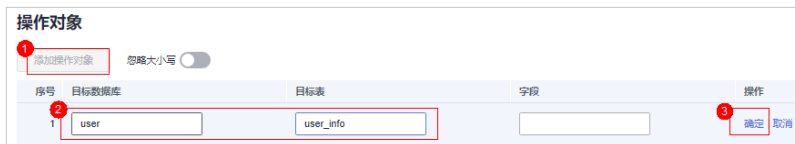


如图10-2所示填写的规则表示从192.168.1.1或192.168.3.3上发起的所有针对user_info表的操作都是“高风险”。

设置该规则后，所有异常访问或窃取表user_info的行为都会被审计，并且触发风险告警。

添加“操作对象”时，单击“添加操作对象”，填写“目标数据库”和“目标表”，单击“确认”，完成添加。

图 10-3 添加检测异常行为的目标表



场景二：利用 DBSS 进行应用程序的 SQL 语句性能优化

示例：某应用上线之后发现当用户执行某些操作时总会出现界面长时间卡顿。经定位，发现后台应用访问数据库时出现好几秒的时延，但未定位到具体是哪些语句导致。

此时可利用DBSS的“数据库慢SQL检测”规则进行辅助定位，帮助开发人员进行性能优化。

操作步骤如下：

步骤1 登录DBSS控制台，进入风险操作页面。

图 10-4 进入风险操作页面



步骤2 单击“数据库慢SQL检测”项“操作”列的“编辑”，在编辑页面的底部设置执行时长规则设置为大于1000毫秒。

图 10-5 设置执行时长

执行结果

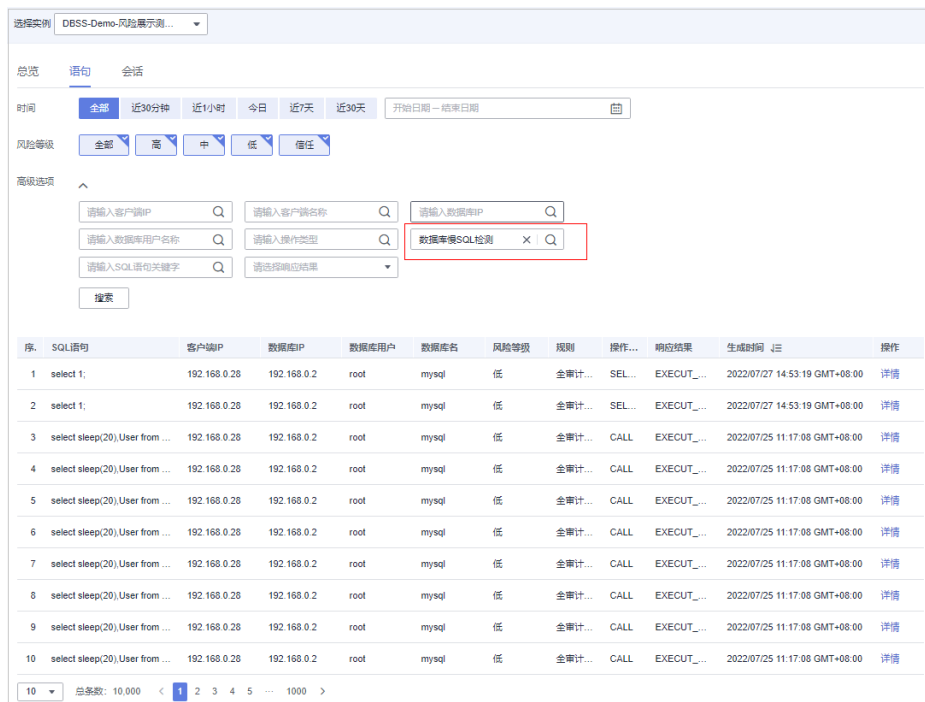
* 影响行数 行

* 执行时长 毫秒

步骤3 单击“确认”，完成设置。

步骤4 设置完成后，待运行一段时间，在语句页面下的规则名称搜索框中填入“数据库慢SQL检测”对检测情况进行检索。

图 10-6 检索慢 SQL 检索情况



说明

- 您可对检索的结果进行分析，对可进行优化的SQL进行优化。
- 若需要进行多轮优化，您可对规则中的“执行时长”字段进行修改，逐步缩小时间，直到达成性能提升的目标。

----结束

场景三：解决 SQL 注入风险的告警误报

DBSS提供SQL注入检测功能，并内置了一些SQL注入检测规则。您也可以自行添加SQL注入检测规则。

示例：若某些语句命中了SQL注入规则，但是经分析发现该语句并不是一条攻击语句，是自己程序生成的合法语句，如图10-7所示。

图 10-7 SQL 注入误报



为了避免DBSS对误报SQL的持续告警，您可以通过设置白名单来解决该误报问题。

📖 说明

风险规则的优先级高于SQL注入规则。

如图10-7所示，执行的SQL语句如下：

```
SELECT COUNT(*) FROM information_schema.TABLES WHERE TABLE_SCHEMA = 'adventureworks' UNION SELECT COUNT(*) FROM information_schema.COLUMNS WHERE TABLE_SCHEMA = 'adventureworks' UNION SELECT COUNT(*) FROM information_schema.ROUTINES WHERE ROUTINE_SCHEMA = 'adventureworks'
```

分析语句关键信息：该语句用SELECT语句访问information_schema库的TABLES表。

配置操作

步骤1 进入风险操作页面。

图 10-8 进入风险操作



步骤2 单击添加风险操作，填写规则信息。

图 10-9 填写规则信息

The screenshot shows a configuration page for a rule. It is divided into several sections:

- 基本信息 (Basic Information):** Includes fields for '风险操作名称' (Risk Operation Name) set to '信任语句' (Trust Statement), '风险等级' (Risk Level) set to '无风险' (No Risk), '状态' (Status) as a toggle switch, and '应用到数据库' (Apply to Database) with checkboxes for '全部数据库' (All Databases), '213', 'mysql', and 'rds-16d7-qct-1025'.
- 客户端IP/IP段 (Client IP/Segment):** A text input field for IP addresses.
- 操作类型 (Operation Type):** A list of checkboxes for various database operations. '操作' (Operation) and 'SELECT' are checked.
- 操作对象 (Operation Object):** A table with columns for '序号' (Serial Number), '目标数据库' (Target Database), '目标表' (Target Table), '字段' (Field), and '操作' (Operation). One entry is shown: '1', 'information_schema', 'TABLES', and a '删除' (Delete) button.

如图10-9所示，填写的规则表示：在information_schema库的TABLES表执行的SELECT语句为无风险。

添加“操作对象”时，单击“添加操作对象”，填写“目标数据库”和“目标表”，单击“确认”，完成添加。

图 10-10 添加 SQL 注入白名单操作对象

The screenshot shows a dialog box titled '添加操作对象' (Add Operation Object). It contains a table with columns: '序号' (Serial Number), '目标数据库' (Target Database), '目标表' (Target Table), '字段' (Field), and '操作' (Operation). The table has one row with '1', 'information_schema', 'TABLES', and empty fields for '字段' and '操作'. There are '确定' (Confirm) and '取消' (Cancel) buttons at the bottom right. Red circles and boxes highlight the '添加操作对象' button, the input fields, and the '确定' button.

步骤3 单击下方“确认”，添加规则成功。

设置完成后，再次检测到该语句时，优先命中该条规则，识别为无风险将不再告警。

----结束