

# 数据库审计

# 目录

## 产品介绍

产品定义.....	3
产品优势.....	3
功能特性.....	4
应用场景.....	5
部署架构.....	5
产品规格.....	7
术语解释.....	8
使用限制.....	8
该产品与其他服务的关系.....	13

## 计费说明

计费概述.....	14
计费模式.....	14
计费项.....	15
变更规格.....	17
欠费.....	18

## 快速入门

购买数据库审计实例.....	19
登录数据库审计实例.....	21
审计天翼云上数据库（免Agent）.....	22
审计云上自建数据库（安装Agent）.....	25

## 用户指南

实例管理.....	29
总览.....	41
数据库审计资产管理.....	50
Agent管理.....	53
审计规则配置.....	57
查询审计内容.....	65
报表中心.....	67
设置告警通知.....	70
其他操作.....	72

# 目录

## 最佳实践

审计云上自建数据库.....	78
审计云数据库.....	79

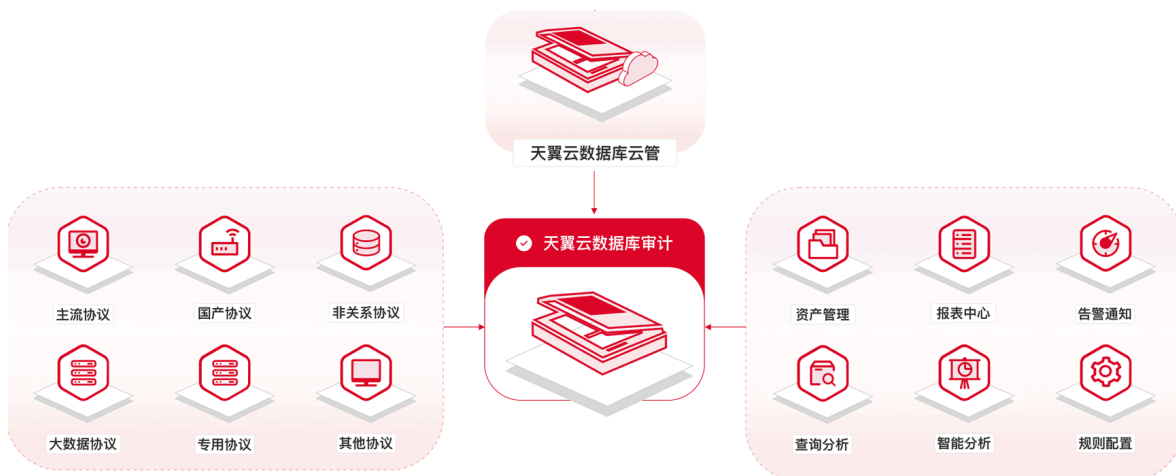
## 常见问题

产品咨询.....	83
购买问题.....	85
功能类问题.....	86
Agent问题.....	90
使用类问题.....	91
故障类.....	92
日志类问题.....	93

# 产品介绍

## 产品定义

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



## 支持的数据库类型

数据库协议	数据库类型
国产数据库协议	DM、GBase、Kingbase、OSCAR、K-DB、OceanBase、PolarDB、PolarDB-X、TiDB、Analytic DB、GaussDB、HighGo DB、Percona、Vastbase、teleDB-MySQL、teleDB-PostgreSQL。
主流数据库协议	Oracle、MySQL、DB2、SQL server、PostgreSQL、Informix、MariaDB、Sybase ASE、Teradata、Sybase IQ、HANA、libra、Vertica、Clickhouse。
非关系协议	MongoDB、Redis、Graphbase、ArangoDB、OrientDB、Neo4j。
大数据协议	Hive、Hbase(Thrift)、Hbase(Protobuf)、Spark SQL(RESTful)、Spark SQL(Thrift)、GreenPlum、Cassandra、Impala、SSDB、HDFS、TDSQL-C、TBase、MAX COMPUTE。

## 产品优势

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

## 支持海量数据库协议

- 支持40余种协议，包括关系型协议、非关系型协议、大数据协议及其他常见协议。
- 支持国内外主流数据库，包括传统的数据库系统、大数据系统和Web系统等。

# 产品介绍

## 数据库安全分析

内置丰富的漏洞规则，在审计过程中通过规则匹配发现数据库的配置不合理项和安全漏洞，并可根据漏洞情况提供合理的安全建议和审计规则。

### 智能关联分析

同时提取Web业务端和数据库端的协议流量，提取出具体业务操作请求URL、POST/GET值、业务账号、原始客户端IP、MAC地址、提交参数等。通过智能自动多层关联，关联出每条SQL语句所对应URL以及其原始客户端IP地址等信息，实现追踪溯源。

### 双向审计

双向审计不但包含了SQL语句执行状态、返回行数、执行时长等基本信息，同时包含数据库的返回结果内容。

功能简单、易上手

采用数据库旁路部署方式是一种简单且快速上手的数据库审计部署方式，该部署方式是在数据库服务器之外设置一个独立的审计服务器，通过旁路方式捕获数据库的操作和日志信息，实现对数据库的实时监控和记录。同时方便用户快速上手，对数据库实例操作简单。

### 天翼云自建数据库全量审计

支持对管理控制台上自建的数据库进行审计，同时也兼容国内外常见数据库。

### 数据库行为模型分析

通过自动学习建立数据库行为模型，行为模型基于“总-分”逻辑分析思维，逐层展示整个数据库的行为状态。通过行为模型的变更分析，可方便用户掌握最新访问动态。

## 功能特性

---

### 记录数据库活动

记录一切对数据库的访问行为，记录维度包括客户端信息、服务端信息、操作信息、操作状态、返回结果集、SQL模板等。

### 存储数据库行为记录

存储记录行为时产生的日志，包括审计日志、会话日志、告警日志，还包括系统的相关配置，如人员权限配置、系统引擎配置等。

### 查询数据库审计日志

在已有的日志中查询某些关键信息，完成事件溯源，一般支持时间、类型、数据库实例名、操作结果、客户端、服务端等查询维度。

### 风险和威胁告警

将数据库访问的行为与安全规则库进行匹配，根据匹配的结果进行告警，一般包含页面告警、外送告警（短信、邮件）。

### 数据库性能分析

通过SQL执行时间统计数据库性能情况，分析潜在性能问题的根因，定位关键资产，可作为用户数据库性能调优的决策辅助。

## 应用场景

### 响应合规需求

应等保及其他行业政策要求，产品可以覆盖对于数据库系统的安全审计工作，内置丰富报表，快速轻松通过合规审查。

### 防范数据泄露

产品内置900多条安全规则，可精准识别拖库、撞库、暴力破解、大流量返回等容易导致数据泄露的安全问题，双向审计功能保证对于数据库的请求和返回全面审计，在数据泄露发生的初始阶段进行告警和遏制。

### 监测SQL注入事件

天翼云数据库审计内置丰富的SQL注入规则，可以精准识别包括布尔盲注、OR注入、SLEEP时间盲注、BENCHMARK时间盲注、GENERATE\_SERIES时间盲注、RECEIVE\_MESSAGE时间盲注、WAITFOR时间盲注、GET\_LOCK时间盲注、CTXSYS\_DRITHSX\_SN报错注入等在内的SQL注入，及时告警，有效切断持续的外部攻击。

### 监测漏洞攻击事件

外部不法分子可能会利用漏洞扫描设备探测到数据库存在的漏洞，进而利用漏洞窃取数据，天翼云数据库审计内置漏洞攻击安全规则，可监测缓冲区溢出、存储过程滥用、隐通道攻击、拒绝服务攻击等多类型的漏洞攻击。

### 监测账号安全隐患

数据库账号安全隐患同样会导致数据安全事件，天翼云数据库审计能够监测数据库账号异常登录的行为，例如撞库、暴力破解、口令失效等，杜绝因数据库账号存在安全隐患导致的恶性事件。

### 监测数据泄露事件

数据库访问对应的返回结果中，包含大量的价值信息，单次操作访问的数据量过大、数据导出操作过于频繁也可能指向数据泄露，天翼云数据库审计能够监测众多可能导致数据泄露的操作，包括撞库、数据库外联、大流量返回、非授权访问等。

### 监测违规操作事件

部分主体的内部工作人员会存在违规行为，联合外部攻击者，共同窃取价值数据谋取私利，天翼云数据库审计能够监测应用账号违规操作、运维人员违规操作、数据库探测等具备潜在内部违规风险的行为。

### 提升安全意识

详细分析报表定期发送，全面了解数据库性能、语句、访问、会话、告警等多方情况，智能学习数据库行为习惯，对于超出基线的行为及时预警，防患于未然。

## 部署架构

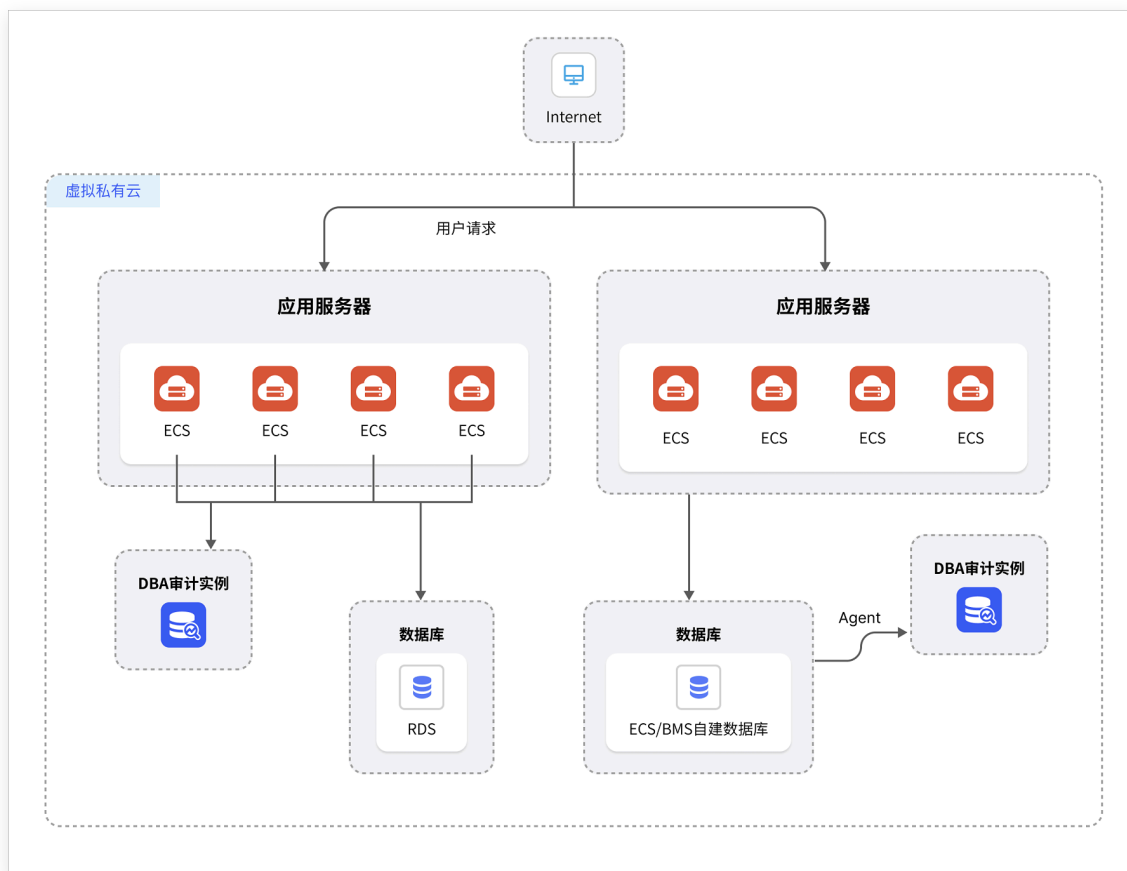
### 天翼云数据库审计架构图

天翼云数据库审计从产品部署架构可以自下而上分为数据采集、协议解析、风险识别、数据存储四个部分，在管理控制侧分成日志查询、仪表盘与报表、数据开发和分布式统一管理。

- 数据采集层的功能是接入需要审计的流量信息，并对流量二三层网络协议和TCP层协议进行解析，提取IP、端口等信息，并根据过滤规则去除不需要进行审计的流量。

# 产品介绍

- 协议解析层的功能是按照各种不同数据库的传输协议解析数据包中包含的有效信息，提取出数据库名称、SQL语句、客户端工具等信息，天翼云数据库审计在协议解析领域已积累十三年的解析经验，对数据库协议有着较深的理解，对协议的解析精确且全面。
- 风险识别功能将解析出来的SQL语句和安全规则进行匹配，以此来发现SQL语句中存在的可疑风险；规则匹配是采用基于DFA状态机的AC算法，该算法实现多条安全规则只需进行一次匹配，实现了高效的规则匹配。如果规则匹配的过程中没有发现风险，那么需要将SQL预计进行字段标准化形成一条审计日志，如果发现了风险，还会根据风险级别相应的产生一条标准化的告警日志，为了达到审计日志和告警日志可回溯，需要将日志进行存储，此时入库程序就会将产生的日志存储到磁盘当中。
- 当需要查询审计日志和风险日志时，天翼云数据库审计的数据输出模块提供了Web端查询功能，并可将这些日志信息通过Syslog、Kafka等方式发送到第三方平台。同时天翼云数据库审计的系统管理模块提供丰富的管理功能，包括了规则管理、软件升级等功能。



# 产品介绍

## 产品规格

- 在“一类节点”区域，数据库审计提供了标准版、专业版、高级版和旗舰版四种服务版本，您可以根据业务需求选择相应的服务版本。

### 说明

在“一类节点”区域，购买数据库审计无需再配套开通云服务器。

分类	标准版	高级版	企业版	旗舰版
支持的数据库实例个数	3个	6个	12个	30个
吞吐量峰值	3,000条/秒	6,000条/秒	12,000条/秒	35,000条/秒
入库速率	360万条/小时	720万条/小时	1440万条/小时	1440万条/小时
支持的SQL语句存储量	<ul style="list-style-type: none"><li>4亿条在线SQL语句存储。</li><li>50亿条归档SQL语句存储。</li></ul>	<ul style="list-style-type: none"><li>6亿条在线SQL语句存储。</li><li>100亿条归档SQL语句存储。</li></ul>	<ul style="list-style-type: none"><li>10亿条在线SQL语句存储。</li><li>200亿条归档SQL语句存储。</li></ul>	<ul style="list-style-type: none"><li>16亿条在线SQL语句存储。</li><li>200亿条归档SQL语句存储。</li></ul>
资源需求	<ul style="list-style-type: none"><li>CPU: 4U</li><li>内存: 16GB</li><li>硬盘: 512GB</li></ul>	<ul style="list-style-type: none"><li>CPU: 8U</li><li>内存: 32GB</li><li>硬盘: 1TB</li></ul>	<ul style="list-style-type: none"><li>CPU: 16U</li><li>内存: 64GB</li><li>硬盘: 2TB</li></ul>	<ul style="list-style-type: none"><li>CPU: 16U</li><li>内存: 64GB</li><li>硬盘: 5TB</li></ul>

- 在“二类节点”区域，数据库审计提供以下实例规格，请您参照下表选择需要的实例规格。

支持的数据库实例个数	推荐云主机的资源需求		
3个	CPU: 4U	内存: 16GB	硬盘: 500GB
6个	CPU: 8U	内存: 16GB	硬盘: 1TB
9个	CPU: 8U	内存: 16GB	硬盘: 1TB
12个	CPU: 16U	内存: 32GB	硬盘: 2TB
15个	CPU: 16U	内存: 32GB	硬盘: 2TB
18个	CPU: 16U	内存: 32GB	硬盘: 3TB
21个	CPU: 16U	内存: 32GB	硬盘: 3TB
24个	CPU: 16U	内存: 32GB	硬盘: 3TB
27个	CPU: 16U	内存: 64GB	硬盘: 4TB
30个	CPU: 16U	内存: 64GB	硬盘: 4TB

# 产品介绍

## 术语解释

### Agent

本文中所述的Agent指的是审计代理插件，是安装在数据库系统或者业务系统上的插件，其功能是捕获访问数据库系统的数据包，并将数据包发送至数据库审计。

### Kafka

Kafka是一种高吞吐量的分布式发布订阅消息系统，可以处理消费者规模的网站中所有动作流数据。这些数据通常由于吞吐量要求而通过处理日志和日志聚合来解决。

### SNMP

SNMP是简单网络管理协议（Simple Network Management Protocol）的简称，是标准IP网络管理协议，支持目前主流的网络管理系统。

### SQL

SQL是结构化查询语言（Structured Query Language）的简称，是一种数据库查询和程序设计语言，用于存取数据以及查询、更新和管理关系数据库系统；同时也是数据库脚本文件的扩展名。

### Syslog

Syslog是一种行业标准的协议，可用来记录设备的日志。Syslog日志消息既可以记录在本地文件中，也可以通过网络发送到接收Syslog的服务器。服务器可以对多个设备的Syslog消息进行统一的存储，或者解析其中的内容做相应的处理。常见的应用场景是网络管理工具、安全管理系统、日志审计系统。

### 数据库

数据库（Database）是用于存放数据的仓库，按照一定的数据结构（即数据的组织形式或数据之间的联系）来组织、存储，用户可以通过数据库提供的多种方法来管理数据库中的数据。

### 规则

本文中所述的规则是指根据一些特征（如客户端、服务端、SQL语句）定义的危险行为（安全规则）及可以信任的行为（过滤规则）。当系统审计到对数据库的操作匹配安全规则时会触发告警，对于匹配过滤规则的行为则不进行审计。

### 资产

本文中所述的资产是指系统需要审计管理的数据库系统。

## 使用限制

### 支持的数据库

### 支持的数据库类型

数据库协议	数据库类型
国产数据库协议	DM、GBase、Kingbase、OSCAR、K-DB、OceanBase、PolarDB、PolarDB-X、TiDB、AnalyticDB、GaussDB、HighGo DB、Percona、Vastbase、teleDB-MySQL、teleDB-PostgreSQL

# 产品介绍

数据库协议	数据库类型
主流数据库协议	Oracle、MySQL、DB2、SQL server、PostgreSQL、Informix、MariaDB、Sybase ASE、Teradata、Sybase IQ、HANA、libra、Vertica、Clickhouse
非关系协议	MongoDB、Redis、Graphbase、ArangoDB、OrientDB、Neo4j
大数据协议	Hive、Hbase(Thrift)、Hbase(Protobuf)、Spark SQL(RESTful)、Spark SQL(Thrift)、GreenPlum、Cassandra、Impala、SSDB、HDFS、TDSQL-C、TBase、MAX COMPUTE

## 支持免Agent安装的数据数据库

天翼云如下数据库支持通过免Agent安装的方式进行数据库审计，快速使用请参考：[如何免Agent安装审计天翼云上数据库](#)。

数据库类型	支持的版本
<a href="#">天翼云关系数据库MySQL版</a>	所有版本
<a href="#">天翼云关系数据库PostgreSQL版</a>	所有版本
<a href="#">天翼云关系数据库SQL Server版</a>	所有版本
<a href="#">天翼云文档数据库服务</a>	所有版本
<a href="#">天翼云云数据库Clickhouse</a>	所有版本

## 需要安装Agent的数据库

数据库类型	支持的版本
Oracle	21c、19c、18c、12c、11g、10g、9i、8i
MySQL	8.0、5.7、5.6、5.5、5.1、5.0、4.1、4.0
SQL Server	2019、2017、2016、2014、2012、2008、2005、2000
SyBase ASE	12.5、11.9
DB2	v11.5、v11.1、v10.5、v9.7、v9.5、v8.2、v8.1、v8.0
infomix	IDS9
Oscar	5.7、5.5
达梦数据库（DM）	DM8、DM7
Cache	2021、2016、2010
Postgre SQL	14、13、12、11、10、9
Teradata	所有版本
人大金仓（Kingbase）	V8、V7、V6
Gbase（南大通用）	8.8s、8.5a
mariaDB	10.3、10.2、10.1、10.0、5.5、5.3、5.2、5.1
Hana	2.0、1.0

## 产品介绍

数据库类型	支持的版本
GaussDB	300、200、100
librA	6
K-DB	11
SyBase IQ	15.4
TiDB	4.X、5.X
Vertica	11、10、9、8、7
Ocean Base	4.X、3.X、2.X
PolarDB	兼容oracle语法版本、PostgreSQL版本、MySQL版本
PolarDB-X	2.0/MySQL5.7、1.0/MySQL5、1.0/MySQL8
AnalyticDB	PostgreSQL版本、MySQL版本
TBase	v2
HighGo (瀚高)	6.0
TDSQL-C MySQL	8.0、5.7
TDSQL-C PostgreSQL	14、10
Percona-MySQL	8.0、5.7、5.6
Vastbase	2.X
Clickhouse-MySQL	所有版本
teleDB-MySQL	所有版本
teleDB-PostgreSQL	所有版本
MongoDB	5.X、4.X、3.X、2.X
Hbase (Protobuf)	所有版本
Hbase (Thrift)	Thrift1、Thrift2
Hive	3.X、2.X、1.X
Redis	所有版本
Elasticsearch	所有版本
Cassandra	3.X
HDFS	所有版本
Impala	3.X
GraphBase	6
Greenplum	5、6
Spark SQL(Thrift)	2.X、1.X
Spark SQL(RESTful)	2.X、1.X
SSDB	所有版本

# 产品介绍

数据库类型	支持的版本
ArangoDB	3.4.9
Neo4j	4.2.0
OrientDB	3.1.6
Percona-MongoDB	5.X、4.X
Hbase (Protobuf)	所有版本
Hbase (Thrift)	Thrift1、Thrift2
Hive	3.X、2.X、1.X

## Agent支持的版本

操作系统	操作系统位数	支持版本
Ubuntu	X64	14.04、16.04、18.04、20.04
Debian	X64	7.6、8.7、9.5、10.11、11.2
CentOS	X64	5.11、6.0、7.4、7.6、8
RedHat	X64	6.5、7.0、7.5
SUSE	X64	11SP4、12SP4
Solaris X86	X86	5.10、5.11
Solaris Sparc	X64	5.10
AIX	-	5.3、6.1、7.1
Windows	X64	Windows7、Windows10
Windows	X86	Windows7
Windows Server	X64	2003、2008、2012、2016、2022
EulerOS (欧拉)	x64	EulerOS 2.0 SP9
银河麒麟	aarch64	v10服务器版
兆芯cpu+银河麒麟系统	x64	v10服务器版
兆芯cpu+中标麒麟系统	x64	7
兆芯cpu+统信UOS	x86	v20
海光cpu+统信UOS	x64	v20
鲲鹏cpu+统信UOS	aarch64	v20

## 数据库加密通讯协议审计能力支持情况

数据库类型	加密方式	加密套件	DBAudit
Oracle	高级安全(Oracle Advanced Security)	AES-256	支持
	SSL	SSL_RSA_WITH_AES_256_CBC_SHA	支持

## 产品介绍

数据库类型	加密方式	加密套件	DBAudit	
		SSL_RSA_WITH_3DES_EDE_CBC_SHA	支持	
		TLS_RSA_WITH_AES_256_CBC_SHA	需提供证书和密码，二次验证	
		TLS_RSA_WITH_AES_256_CBC_SHA256	需提供证书和密码，二次验证	
		TLS_RSA_WITH_AES_128_CBC_SHA256	需提供证书和密码，二次验证	
		TLS_RSA_WITH_AES_128_CBC_SHA	需提供证书和密码，二次验证	
		TLS_RSA_WITH_AES_256_GCM_SHA256	需提供证书和密码，二次验证	
		TLS_RSA_WITH_3DES_EDE_CBC_SHA	需提供证书和密码，二次验证	
	高级安全(Oracle Advanced Security)	AES-256	支持	
	SSL	SSL_RSA_WITH_AES_256_CBC_SHA	支持	
		TLS_RSA_WITH_AES_256_CBC_SHA	支持	
		TLS_RSA_WITH_AES_256_CBC_SHA256	支持	
		TLS_RSA_WITH_AES_128_CBC_SHA256	支持	
		TLS_RSA_WITH_AES_128_CBC_SHA	支持	
		TLS_RSA_WITH_AES_256_GCM_SHA256	需提供证书和密码，二次验证	
		SSL_RSA_WITH_3DES_EDE_CBC_SHA	需提供证书和密码，二次验证	
		TLS_RSA_WITH_3DES_EDE_CBC_SHA	需提供证书和密码，二次验证	
		SQL Server	SSL	TLS_RSA_WITH_3DES_EDE_CBC_SHA
		TLS_RSA_WITH_AES_128_CBC_SHA		需提供证书和密码，二次验证
MySQL	SSL	TLS_RSA_WITH_3DES_EDE_CBC_SHA	支持	
		TLS_RSA_WITH_AES_128_CBC_SHA	支持	
		TLS_RSA_WITH_AES_256_CBC_SHA	支持	
		TLS_RSA_WITH_3DES_EDE_CBC_SHA	支持	
		TLS_RSA_WITH_AES_128_CBC_SHA	支持	
		TLS_RSA_WITH_AES_256_CBC_SHA	支持	
		TLS_RSA_WITH_3DES_EDE_CBC_SHA	支持	
		TLS_RSA_WITH_AES_128_CBC_SHA	支持	
		TLS_RSA_WITH_AES_256_CBC_SHA	支持	
		TLS_RSA_WITH_AES_128_CBC_SHA256	支持	
		TLS_RSA_WITH_AES_256_CBC_SHA256	支持	
		TLS_RSA_WITH_AES_128_GCM_SHA256	支持	
		TLS_RSA_WITH_AES_256_GCM_SHA256	支持	
Hive	Kerberos认证	全部通讯加密	支持	

## 产品介绍

数据库类型	加密方式	加密套件	DBAudit
hdfs	Kerberos认证	全部通讯加密	支持
PostgreSQL	Kerberos认证	全部通讯加密	支持

### 支持的区域

区域	一类节点	二类节点
华东地区	杭州2/杭州7/合肥2/华东1/九江/南昌5/南京3/上海36/上海7/芜湖2/芜湖4	杭州/南昌/上海4/苏州/芜湖
华南地区	长沙42/郴州2/海口2/华南2/南宁2/南宁23/武汉41/厦门3	长沙2/福州1/广州4/海口/南宁/深圳/武汉2
西北地区	兰州2/乌鲁木齐27/西安4/西安7/中卫2/中卫5	兰州/乌鲁木齐/西安2/西宁/中卫
西南地区	成都4/重庆2/贵州3/昆明2/拉萨3/西南1/西南2-贵州	成都3/重庆/贵州1/昆明
北方地区	北京5/华北2/晋中/内蒙6/青岛20/石家庄20/太原4/郑州5	北京2/长春/哈尔滨/华北/内蒙3/青岛/沈阳3/石家庄/太原/天津/郑州

## 该产品与其他服务的关系

### 与统一身份认证服务的关系

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

# 计费说明

## 计费概述

### 计费模式

数据库审计服务仅提供**包年/包月**计费模式。

**包年/包月**是一种预付费模式，即先付费再使用，按照订单的购买周期进行结算，因此在购买之前，您必须确保账户余额充足。

### 计费项

数据库审计的计费项由**云主机、系统盘、数据盘**组成。

如需了解每种计费项的计费因子、计费公式等信息，请参见[计费项](#)。

### 续费

包年/包月数据库审计在到期后会**影响云服务器的正常运行**。如果您想继续使用数据库审计，需要在规定的时间内为服务进行续费，否则资源将会自动释放，数据也可能会丢失。

### 停止计费

当云服务资源不再使用时，可以将他们退订或删除，从而避免继续收费。

## 计费模式

### 适用场景

包年/包月计费模式需要用户预先支付一定时长的费用，适用于长期、稳定的业务需求。以下是一些适用于包年/包月计费模式的业务场景：

- **稳定业务需求**：对于长期运行且资源需求相对稳定的业务，如企业官网、在线商城、博客等，包年/包月计费模式能提供较高的成本效益。
- **长期项目**：对于周期较长的项目，如科研项目、大型活动策划等，包年/包月计费模式可以确保在整个项目周期内资源的稳定使用。
- **业务高峰预测**：如果能预测到业务高峰期，如电商促销季、节假日等，可提前购买包年/包月资源以应对高峰期的需求，避免资源紧张。
- **数据安全要求高**：对于对数据安全性要求较高的业务，包年/包月计费模式可确保资源的持续使用，降低因资源欠费而导致的数据安全风险。

### 适用计费项

根据所选购买区域，计费项略有不同：

- 在“一类节点”区域，通过数据库审计版本、数据盘扩容大小进行计费：

计费项	说明
数据库审计版本	购买的数据库审计版本，目前可选标准版、高级版、企业版和旗舰版。
数据盘扩容	购买数据盘扩容的存储大小。

# 计费说明

- 在“二类节点”区域，通过数据库审计实例个数、配套的云主机进行计费：

计费项	说明
数据库审计实例个数	购买的数据库审计实例个数。
云主机	开通数据库审计需要同步开通云主机，涉及购买云主机的规格、系统盘及数据盘。

在购买云服务页面底部，您将看到所需费用的明细。

## 计费周期

包年/包月资源的计费周期是根据您购买的时长来确定的（以UTC+8时间为准）。一个计费周期的起点是您开通或续费资源的时间（精确到秒），终点则是到期日的23:59:59。

例如，如果您在2024/03/08 15:50:04购买了一个时长为一个月的数据库审计，那么其计费周期为：2024/03/08 15:50:04 ~ 2024/04/08 23:59:59。

## 计费项

### 版本规格

- 在“一类节点”区域，数据库审计提供了标准版、专业版、高级版和旗舰版四种服务版本，您可以根据业务需求选择相应的服务版本。

#### 说明

在“一类节点”区域，购买数据库审计无需再配套开通云服务器。

分类	标准版	高级版	企业版	旗舰版
支持的数据库实例个数	3个	6个	12个	30个
吞吐量峰值	3,000条/秒	6,000条/秒	12,000条/秒	35,000条/秒
入库速率	360万条/小时	720万条/小时	1440万条/小时	1440万条/小时
支持的SQL语句存储量	<ul style="list-style-type: none"><li>4亿条在线SQL语句存储。</li><li>50亿条归档SQL语句存储。</li></ul>	<ul style="list-style-type: none"><li>6亿条在线SQL语句存储。</li><li>100亿条归档SQL语句存储。</li></ul>	<ul style="list-style-type: none"><li>10亿条在线SQL语句存储。</li><li>200亿条归档SQL语句存储。</li></ul>	<ul style="list-style-type: none"><li>16亿条在线SQL语句存储。</li><li>200亿条归档SQL语句存储。</li></ul>
资源需求	<ul style="list-style-type: none"><li>CPU：4U</li><li>内存：16GB</li><li>硬盘：512GB</li></ul>	<ul style="list-style-type: none"><li>CPU：8U</li><li>内存：32GB</li><li>硬盘：1TB</li></ul>	<ul style="list-style-type: none"><li>CPU：16U</li><li>内存：64GB</li><li>硬盘：2TB</li></ul>	<ul style="list-style-type: none"><li>CPU：16U</li><li>内存：64GB</li><li>硬盘：5TB</li></ul>

- 在“二类节点”区域，数据库审计提供以下实例规格，请您参照下表选择需要的实例规格。

支持的数据库实例个数	推荐云主机的资源需求		
3个	CPU：4U	内存：16GB	硬盘：500GB

# 计费说明

支持的数据库实例个数	推荐云主机的资源需求		
6个	CPU: 8U	内存: 16GB	硬盘: 1TB
9个	CPU: 8U	内存: 16GB	硬盘: 1TB
12个	CPU: 16U	内存: 32GB	硬盘: 2TB
15个	CPU: 16U	内存: 32GB	硬盘: 2TB
18个	CPU: 16U	内存: 32GB	硬盘: 3TB
21个	CPU: 16U	内存: 32GB	硬盘: 3TB
24个	CPU: 16U	内存: 32GB	硬盘: 3TB
27个	CPU: 16U	内存: 64GB	硬盘: 4TB
30个	CPU: 16U	内存: 64GB	硬盘: 4TB

## 产品价格

- 在“一类节点”区域，数据库审计计费项有数据库安全审计实例规格和存储扩容两个部分，可详见下表。

### 说明

- 标\*的计费项为必选计费项。
- 包年购买，每年的年付价格为10个月的月付价格总和。

计费项	支持的规格	月计费价格	年计费价格
*数据库审计标准版	支持3个数据库审计实例	3,000元/月	30,000元/年
*数据库审计高级版	支持6个数据库审计实例	5,400元/月	54,000元/年
*数据库审计企业版	支持12个数据库审计实例	9,600元/月	96,000元/年
*数据库审计旗舰版	支持30个数据库审计实例	22,500元/月	225,000元/年
存储扩容	每份存储扩容增加数据盘 内存: 1TB	500元/月	5,000元/年

- 在“二类节点”区域，数据库审计计费项有数据库安全审计实例规格、云主机和硬盘三个部分，可详见下表。

云主机为配套开通项，可在数据库审计实例购买页同步购买并开通。

### 说明

- 标\*的计费项为必选计费项。
- 数据库审计实例包年购买，每年的年付价格为10个月的月付价格总和。

计费项	计费基准	月计费价格	年计费价格
*数据库审计实例	实例个数	650元/个/月	6,500元/个/年
*云主机	云主机实例规格	以订单页显示金额为准	以订单页显示金额为准

# 计费说明

计费项	计费基准	月计费价格	年计费价格
*系统盘/数据盘	存储容量	以订单页显示金额为准	以订单页显示金额为准

## 变更规格

数据库审计支持升级实例版本或存储扩容大小。

## 约束限制

- 若首次进行实例存储扩容，则无法和实例版本一起升级，请分批次升级。
- 数据库审计实例只支持升配不支持降配。

## 升级步骤

1. 登录数据库审计控制台。
2. 选择需要升级的实例，选择“更多 > 变更规格”。

### 注意

“一类节点”区域的实例，只有运行状态为“关机中”可以执行升级操作。若实例未关闭则需要关闭实例。



3. 在跳转的页面中选择需要升级的版本和数据盘扩容大小。



4. 选择完成后，勾选“我已阅读并同意《天翼云数据库审计产品服务协议》”，单击“提交订单”。

# 计费说明

## 注意

“二类节点”区域的实例，数据库审计实例控制台不支持直接对您的云主机规格进行升级，若需升级云主机配置请自行参考[云主机变更规格](#)。

## 欠费

---

### 欠费说明

欠费后天翼云数据库审计会自动停止，您所占用的存储空间资源仍会继续扣费，因此欠费余额会累计。如果您在15天内充值补足欠款，服务会自动启用。

当欠费超过15天，将视为您主动放弃该服务，您保存在天翼云数据库审计的全部数据将会被销毁，销毁后数据不可恢复。因此请您及时关注账户余额并及时续费以保证您的服务不受到影响。

若您确认不再使用天翼云数据库审计服务，请务必及时删除存储于数据库审计的数据。

### 续费说明

若是已购买资源包后欠费，请在15天内再次订购相应的资源包或保证帐号中的余额充足。

若是未购买资源包后欠费，请在15天内充值补足欠款并保证帐号中的余额充足。

## 购买数据库审计实例

### 支持的区域

根据所选购买区域，购买步骤略有不同，数据库审计支持的区域请参见[支持的区域](#)。

### 前提条件

购买数据库审计前，您需要[注册天翼云账号](#)并完成[实名认证](#)。

### 购买步骤（一类节点）

1. 登录天翼云控制中心。
2. 选择“安全 > 数据库审计”，进入数据库审计实例管理页面。
3. 单击右上角的“立即购买”，进入数据库审计实例购买页。
4. 在订购页面，配置实例相关参数。

参数	说明
地域	选择数据库审计实例的地域。 尽量选择距离您更近的地域以提高访问速；购买完成后不支持修改地域。
可用区域	部分地域拥有多个可用区，选择其中一个可用区购买数据库审计实例；购买完成后不支持修改可用区。
CPU分类	选择实例的CPU架构。部分地域提供了X86和ARM架构，实际支持情况以订购页为准。
数据库审计名称	支持自定义数据库审计实例的名称。
版本	选择数据库审计的版本，版本说明详见 <a href="#">产品规格</a> 。
企业项目	选择实例所属的企业项目。 企业项目通过将云资源、带有权限的用户组绑定到一起，用户使用企业项目内云资源时，权限将受用户组的权限制。
虚拟私有云	选择实例所在的虚拟私有云。 如果没有可选的虚拟私有云，单击“配置虚拟私有云”立即跳转到虚拟私有云控制台进行创建，详细操作请参见 <a href="#">创建虚拟私有云VPC</a> 。
子网	选择实例所在的子网。 如果没有可选的子网，单击“配置子网”立即跳转到子网控制台进行创建，详细操作请参见 <a href="#">创建子网</a> 。
数据盘扩容	按需选择需要扩容的数据盘大小。

5. 选择“购买时长”，拖动时间轴设置购买时长。

支持开启“到期自动续费”，当服务到期前，系统会自动按照默认的续订周期生成续费订单并进行续费，无须用户手动续费。

6. 确认参数配置无误后，阅读《天翼云数据库审计产品服务协议》并勾选“我已阅读并同意《天翼云数据库审计产品服务协议》”，单击“提交订单”。

# 快速入门

7. 在订单详情页确认内容是否正确，确认无误后单击“立即支付”，在后续跳转页中完成支付即成功购买数据库审计服务。

## 购买步骤（二类节点）

1. 登录天翼云控制中心。
2. 选择“安全 > 数据库审计”，进入数据库审计实例管理页面。
3. 单击右上角的“立即购买”，进入数据库审计实例购买页。
4. 在订购页面，配置实例相关参数。

参数	说明
地域	选择数据库审计实例的地域。 尽量选择距离您更近的地域以提高访问速；购买完成后不支持修改地域。
可用区域	部分地域拥有多个可用区，选择其中一个可用区购买数据库审计实例；购买完成后不支持修改可用区。
CPU分类	选择实例的CPU架构。部分地域提供了X86和ARM架构，实际支持情况以订购页为准。
数据库审计名称	输入该数据库审计实例的名称。
实例数量	选择数据库审计的实例数量。
配套弹性云主机	配置数据库审计实例所需的云主机规格，不同实例规格所需的云主机规格详见 <a href="#">产品规格</a> 。 <ul style="list-style-type: none"><li>• 数据库审计-云主机：云主机的规格，即CPU、内存规格。不支持升降配。</li><li>• 系统盘：云主机的系统盘规格，根据您服务自身需求选择具体容量大小，不支持降配。</li><li>• 数据盘：云主机的数据盘规格，根据您服务自身需求选择具体容量大小，不支持降配。</li></ul>
虚拟私有云	选择数据库审计实例所属的VPC。
安全组	选择数据库审计实例所属的安全组。为正常使用数据库审计，请手动开通如下安全组规则：TCP协议1443、13001与13002入方向。
子网	选择数据库审计实例所属的子网。
弹性IP	绑定数据库审计实例的弹性IP。 若购买时未绑定弹性IP，等开通完成后，请在云主机手动同步绑定选择的弹性IP，具体操作请参考： <a href="#">绑定弹性公网IP</a> 。
管理员初始帐号	为数据库审计实例的超级管理员设置初始密码。 <ul style="list-style-type: none"><li>• 用户名：默认为超级管理员admin，不支持修改。</li><li>• 登录密码：设置初始密码。</li><li>• 确认密码：二次确认密码。</li></ul>

5. 选择“购买时长”，拖动时间轴设置购买时长。

支持开启“到期自动续费”，当服务到期前，系统会自动按照默认的续订周期生成续费订单并进行续费，无须用户手动续费。

6. 确认参数配置无误后，阅读《天翼云数据库审计产品服务协议》并勾选“我已阅读并同意《天翼云数据库审计产品服务协议》”，单击“提交订单”。
7. 在订单详情页确认内容是否正确，确认无误后单击“立即支付”，在后续跳转页中完成支付即成功购买数据库审计服务。

后续操作

购买完成后，首次登录实例需要使用admin账户登录，具体请参见[用户管理](#)章节。

## 登录数据库审计实例

### 设置安全组策略

若数据库审计绑定了EIP，在用户通过EIP访问数据库审计实例之前需要配置安全组策略，编辑入向策略，才可通过EIP直接访问数据库审计实例。

说明

- 安全组是一个逻辑上的分组，为同一个虚拟私有云内具有相同安全保护需求，并相互信任的弹性云服务器和数据库审计实例提供访问策略。
- 为了保障数据库审计的安全性和稳定性，在使用数据库审计实例之前，您需要设置安全组，添加规则允许需访问数据库审计的IP地址和端口。

### 数据库审计实例开放端口说明

端口	用途	说明
1443	门户端口、心跳端口	访问数据库审计门户页面并保持心跳连接，需开放该端口的出入方向规则。
13001	流量转发	数据库资产与数据库审计的13001端口建立连接负责流量转发，需开放该端口的出入方向规则。
13002	连接控制	数据库资产与数据库审计的13002端口建立连接负责控制部分，包含接收天翼云数据库审计下发的资产和其他配置，需开放该端口的出入方向规则。

### 登录实例

购买数据库审计实例后，用户在数据库审计实例页面，点击实例右上角的“管理”即可单点登录进入数据库实例Web控制台。

支持“外网地址登录”、“内网地址登录”。

#### 外网地址登录

注意

外网地址登录需要给实例绑定弹性IP。

1. 登录[数据库审计控制台](#)。

# 快速入门

2. 找到需要登录的实例，单击“管理 > 外网地址登录”。



## 内网地址登录

### 注意

内网地址登录需要确保客户端（个人电脑、手机、平板等）与数据库审计实例网络互通。可通过VPN方式打通客户端与实例的网络，具体操作请参见[客户端远程连接VPC-VPN连接](#)。

1. 登录[数据库审计控制台](#)。
2. 找到需要登录的实例，单击“管理 > 内网地址登录”。



## 审计天翼云上数据库（免Agent）

### 操作场景

天翼云关系数据库MySQL版、关系数据库PostgreSQL版、关系数据库SQL Server版、文档数据库服务支持通过免Agent安装的方式进行数据库审计。

### 前提条件

通过免Agent方式审计天翼云上数据库之前，首先需要开启SQL审计日志功能：

- 关系数据库MySQL版：具体操作请参考[关系型数据库MySQL版-开启SQL审计日志](#)。（II类资源池中仅支持一类节点的资源池）
- 关系数据库PostgreSQL版：具体操作请参考[关系数据库PostgreSQL版-数据库审计设置](#)。
- 关系数据库SQL Server版：具体操作请参考[关系数据库SQL Server版-开启审计日志](#)。
- 文档数据库服务：具体操作请参考[文档数据库服务-开启审计日志](#)。

# 快速入门

- 云数据库Clickhouse：无需单独配置审计日志开启，可直接在数据库审计中添加资产采集。

## 步骤一：购买数据库审计实例

请根据您的业务需求选购数据库审计规格，数据库安全审计参数及详细操作请参见[购买数据库审计实例](#)。

### 注意

数据库审计实例、数据库实例，需要在同一区域。

## 步骤二：启用天翼云RDS日志

### 说明

最新版本的数据数据库审计实例，购买后已自动开启天翼云RDS日志采集功能。若实例已开启该功能，可跳过该步骤。

1. 登录数据库审计实例。
2. 在左侧导航栏选择“系统管理 > 系统配置 > 日志采集方式”。
3. 确保已启用天翼云RDS日志采集。若未启用，单击“修改”按钮，在弹出的日志采集方式对话框中进行修改。

## 系统配置

许可证 **日志采集方式**

**日志采集方式** 建议关闭不必要的日志采集方式，可减少资源的浪费

接收镜像流量：启用

接收Agent流量：启用

**天翼云RDS日志：启用**

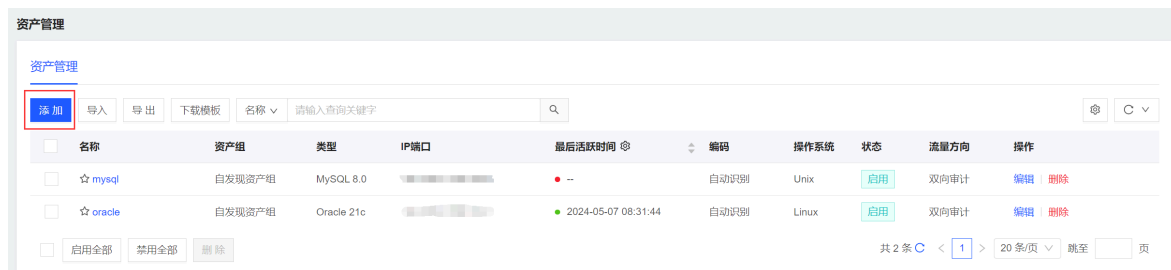
修改

## 步骤三：添加数据库资产

1. 登录数据库审计实例。

# 快速入门

2. 在左侧导航栏选择“资产 > 资产管理”，单击“添加”。



3. 在弹出的“添加资产”窗口配置数据库信息。

参数填写规则说明如下：

参数	参数说明
保存时启用推荐的规则	<ul style="list-style-type: none"><li>勾选此选项，则保存时添加的资产会使用系统推荐的规则。</li><li>不勾选此选项，保存时添加的资产不会使用系统推荐的规则。</li></ul>
类型	<ul style="list-style-type: none"><li>关系数据库MySQL版：请选择“天翼云RDS &gt; Teledb-MySQL &gt; 所有版本”。</li><li>关系数据库PostgreSQL版：请选择“天翼云RDS &gt; PostgreSQL &gt; 所有版本”。</li><li>关系数据库SQL Server版：请选择“天翼云RDS &gt; SQL Server &gt; 所有版本”。</li><li>文档型数据库：请选择“天翼云RDS &gt; MongoDB &gt; 所有版本”。</li><li>云数据库Clickhouse：请选择“天翼云RDS &gt; Clickhouse HTTP &gt; 所有版本”。</li></ul>
实例ID	填写数据库实例ID，请前往对应数据库控制台获取“实例ID”。
资产组	设置资产所属的资产组。
名称	填写资产的名称，必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过64字符。
IP端口	填写数据库实例的IP及端口号，请前往对应数据库控制台获取“连接地址”。
状态	点击“更多配置”，可配置审计状态，默认为“启用”。

4. 配置完成后，单击“保存”即可纳管天翼云上数据库并审计。

后续操作

- 若需要配置审计规则，请参考[审计规则配置](#)。
- 查看审计结果，请参考[查询审计内容](#)。

# 快速入门

## 审计云上自建数据库（安装Agent）

### 使用流程

操作步骤	操作说明
步骤一：购买数据库审计实例	根据实际业务情况，选购合适规格的数据库审计实例，详情请参见 <a href="#">购买数据库审计实例</a> 。
步骤二：添加资产	添加系统需要审计的数据库，详情请参见 <a href="#">资产管理</a> 。
步骤三：安装Agent	添加Agent对数据库进行审计，详情请参见 <a href="#">Agent管理</a> 。
步骤四：配置规则	配置数据库的安全规则和过滤规则，详情请参见 <a href="#">规则配置</a> 。
步骤五：订阅报表的设置告警通知	便于管理员及时了解数据库的运行状态及安全告警信息，详情请参见 <a href="#">报表订阅</a> 和 <a href="#">告警通知</a> 。

### 添加数据库资产

#### 支持的数据库

支持的数据库类型及版本请参见[使用限制](#)。

#### 添加资产

添加资产包括单个添加和批量导入两种方式。

1. 在左侧菜单栏选择“资产 > 资产管理”进入“资产管理”页面，选择“资产管理”页签，单击“添加”。

#### 资产管理

名称	资产组	类型	IP端口	编码	操作系统	状态	流量方向	操作
☆ 10.123.36.40	缺省资产组	MySQL 8.0	10.123.36.40:3323	自动识别	Linux	启用	双向审计	编辑   删除

2. 在弹出的“添加资产”窗口编辑相关信息。

参数填写规则可参见下表。

参数	参数说明
保存时启用推荐的规则	勾选此选项，则保存时添加的资产会使用系统推荐的规则；不勾选此选项，保存时添加的资产不会使用系统推荐的规则。
类型	设置资产类型，包括关系型、非关系型、大数据、图形、全文、文档、键值、其他等。
资产组	设置资产所属的资产组。
名称	填写资产的名称，必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过64字符。

# 快速入门

参数	参数说明
操作系统	设置资产所在主机的操作系统。
IP端口	设置资产所在主机的IP及端口号。

## 说明

- 本地运维行为审计是指通过安装本地Agent捕获本地数据库客户端程序中实际响应的SQL指令，实现对本地运维人员数据库操作行为的审计，支持Oracle、PostgreSQL、MySQL、SQL Server等主流数据库。
- 当使用本地运维行为审计方式时，需要添加回环IP地址127.0.0.1和端口号，端口号需根据数据库类型进行填写。
- 如果使用的IP类型为IPv6，IP地址需填写为“::1”。

- 如需配置其他更多信息，可点击“更多配置”，选择单向审计或双向审计，设置加密协议审计。参数填写规则可参见下表。

参数	参数说明
流量方向	<ul style="list-style-type: none"><li>单向审计：审计内容包括请求信息、客户端信息、服务端信息，不包括返回结果集。</li><li>双向审计：审计内容包括请求信息、客户端信息、服务端信息、返回结果集。</li></ul>
保存行数	取值范围：0~999，0表示不保存返回结果。最大保存内容为64KB。
最大保存长度	取值范围：1~64KB，确保整行显示。
解密私钥	加密协议导入解密私钥，目前支持MySQL、SQL Server、HTTPS加密解析，证书支持导入和编辑两种方式。
证书密码	安全证书的密码。

- 配置完成后，单击“保存”即可完成资产添加。

## 说明

资产添加之后，需要确认部署模式。若选择流量代理模式，需要部署Agent程序才能完成数据库审计。

## 安装Agent

本文以“通过SSH远程安装Agent”为例介绍如何安装Agent，更多安装Agent的方法请参[Agent管理](#)。

### 通过SSH远程安装Agent

您可以通过SSH协议将Agent自动安装到需要审计的服务器上，目前仅支持Linux系统。

在界面上输入需要审计的服务器IP、SSH端口、root用户名、密码，天翼云数据库审计通过scp协议将agent安装包传输到宿主机上并自动安装。

- 在菜单栏选择“系统管理 > Agent管理”进入“Agent管理”页面，选择“Agent安装”页签。

# 快速入门

- 单击“开始安装”进入通过SSH远程安装Agent页面，编辑审计服务器IP，并添加安装Agent的服务器，单击“安装”。

填写参数说明请参见下表：

参数	参数说明
审计服务器IP	默认为当前的审计服务器IP，用户可以根据需要修改。
安装Agent的服务器	输入需要安装Agent的服务器IP及该服务器root账户的密码，默认端口为22，用户可以根据实际情况修改。 <ul style="list-style-type: none"><li>支持表单格式和文本格式输入。</li><li>支持IPv4和IPv6。</li><li>最多填写20个。</li></ul>

## 说明

单击“安装状态”可进入“安装状态”查看页面，可进行以下操作：

- 单击“卸载”可远程卸载已经成功安装了Agent。
- 单击“重新安装”可对未成功安装Agent的服务器重新安装。
- 将光标悬停至“安装失败”后的图标，查看安装失败原因。
- 若您的业务部署在一类节点的资源池上，审计服务器IP需改为数据库审计所在的VPC组的公网IP。（一类节点可参考[支持的区域](#)）

## 配置规则

### 规则配置

规则配置是指根据一些特征（如客户端、服务端、SQL语句）定义危险行为（安全规则）、可以信任的行为（信任规则）和不审计的行为（过滤规则）。当系统审计到对数据库的操作匹配过滤规则的行为则不进行审计，对应匹配信任规则时不会触发告警，对应匹配安全规则时会触发告警。

系统匹配规则的顺序为：

- 过滤规则
- 信任规则
- 安全规则

### 配置过滤规则

过滤规则的功能是根据某些特定的条件过滤一些操作，系统对这些操作不审计，从而节省设备的磁盘空间，将有限的资源用来存储更有价值的审计数据。过滤规则的过滤方式有三种：

- 按IP过滤：设置某些IP地址为信任的IP地址，系统对这些IP地址发起的SQL请求不审计。
- 按SQL模板过滤：设置SQL模板为可信任的模板，当访问的SQL语句的模板是设置的过滤模板，则不进行审计。
- 按规则过滤：指按照特定的条件进行审计过滤，规则包括客户端信息、服务端信息、SQL请求和SQL结果等条件。

具体操作步骤请参考[过滤规则](#)章节。

## 配置信任规则

1. 在左侧菜单栏中选择“规则配置 > 信任规则”进入“信任规则”页面。
2. 单击“新增”，在弹出的新增规则对话框中编辑相关信息，具体参数请参考[信任规则](#)章节。
3. 配置完成后，单击“保存”即可完成信任规则的配置。

## 配置安全规则

内置规则不可更改，默认为推荐规则，您可以通过单击界面右上角的“推荐”按钮切换到全部规则。

## 说明

内置规则包含特征规则及其他非特征规则，特征规则不可进行克隆和删除操作，非特征规则可进行克隆操作。

您可以管理自定义的规则，新增自定义安全规则的操作方法如下：

1. 在菜单栏选择“规则配置 > 安全规则”进入“安全规则”页面，选择“规则管理”页签。
2. 单击“新增”，在弹出的对话框中填写相关参数，具体参数请参考[安全规则](#)章节。
3. 填写完成后单击“保存”即可完成安全规则新增任务。

## 实例管理

### 升级数据库审计实例版本

数据库审计在上线新版本后，支持您在控制台升级实例版本。

#### 操作步骤

1. 登录[数据库审计实例控制台](#)。
2. 在数据库审计实例界面，选择需要升级并且“可升级”的数据库实例，单击“升级”按钮。



3. 在弹出的对话框中单击“确认”，实例开始进行自动升级并且实例的状态会变为“升级中”。
4. 待实例状态变为“运行中”即表示升级已经结束。

### 修改子网

支持修改“已关机”状态的数据库审计实例的子网信息。

#### 操作步骤

1. 登录[数据库审计实例控制台](#)。
2. 在数据库审计实例界面，选择“更多 > 修改子网”。
3. 选择子网。

如果没有可选的子网，单击“创建子网”立即跳转到“[网络控制台](#)”进行创建，详细操作请参见[创建子网](#)。

### 标签管理

标签是对实例的标识。基于标签，您可以实现对实例的便捷搜索和整理。标签由键值对（Key-Value）组成，您可以为实例绑定和解绑标签，在控制台中通过标签快速查找实例。

#### 约束限制

- 每个实例最多可绑定10个标签。
- 每个实例下的标签键是唯一的，不可绑定相同标签键。
- 不支持修改标签，可以解绑标签后，绑定新的标签。

# 用户指南

## 绑定标签

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > 数据库审计”，进入数据库审计实例管理页面。
4. 选择需要添加标签的数据库审计实例，单击“标签”旁的编辑按钮。



5. 在弹出的编辑标签窗口中，填写标签键和值。  
方式一：在输入框中输入新的标签键和值，新增标签。  
方式二：下拉选择已有标签。
6. 配置完成后，单击“确定”，绑定标签完成。
7. 标签绑定成功后，鼠标点击实例信息的“标签”数量，可查询标签绑定情况。

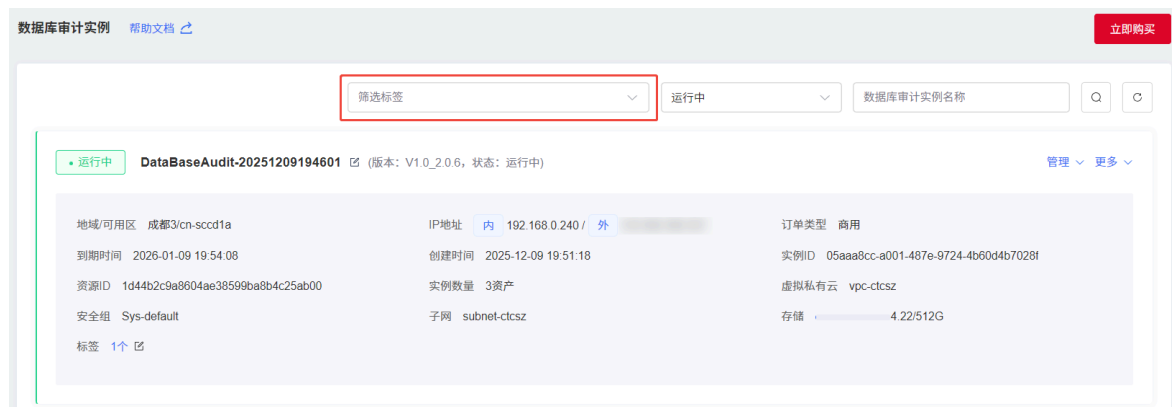


## 使用标签筛选实例

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > 数据库审计”，进入数据库审计实例管理页面。

# 用户指南

4. 单击“筛选标签”。



5. 在“标签筛选”弹窗中，下拉选择已有标签。

6. 单击“确定”，执行筛选标签操作，列表将展示标签筛选结果。筛选结果返回包含所选择的多项键值的实例。

## 解绑标签

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > 数据库审计”，进入数据库审计实例管理页面。
4. 选择需要解绑标签的数据库审计实例，单击“标签”旁的编辑按钮。
5. 在弹出的编辑标签窗口中，单击目标标签操作列的“删除”。

## 编辑标签



标签键	标签值	操作
test-osm	test-osm	删除

+ 您还可以添加9个标签

取消

确定

6. 单击“确定”，解绑标签完成。

## 权限管理

天翼云提供统一身份认证（Identity and Access Management，简称IAM）服务，是提供用户进行权限管理的基础服务，可以帮助您安全的控制云服务和资源的访问及操作权限。通过IAM服务定义企业项目、创建子用户，轻松实现IAM子用户对数据库审计资源的访问控制、权限分配等。

默认情况下，天翼云主账号拥有管理员权限，而主账号创建的IAM用户没有任何权限。IAM用户需要加入用户组，并给用户组授权相应策略后，IAM用户才能获得策略对应的权限，才可以基于被授予的权限对云服务进行操作。

数据库审计支持企业项目管理，若您需要对数据库审计资源进行分组和管理，形成逻辑隔离，您可以创建企业项目，并将资源划分至不同的企业项目中，不同的企业项目可以绑定不同的用户组，并给用户组授予数据库审计产品的权限策略（包括系统策略和自定义策略），从而实现对特定资源的授权。

### 说明

仅“一类节点”区域的实例支持企业项目管理。

## IAM应用场景

IAM策略主要面向同一主账号下，对不同IAM用户授权的场景：

- 您可以为不同操作人员或应用程序创建不同IAM用户，并授予IAM用户刚好能完成工作所需的权限，比如查看权限，进行最小粒度授权管理。
- 新创建的IAM用户可以使用自己的登录名和密码登录控制台，实现多用户协同操作时无需分享账号密码的安全要求。

### 数据库审计IAM策略说明

天翼云为数据库审计提供如下**系统策略**。如果系统策略不满足授权要求，可以创建**自定义策略**，自定义策略是对系统策略的扩展和补充，详情请参见[创建自定义策略](#)。

策略名称	策略描述	类别	授权范围
数据库审计admin策略	数据库审计admin策略，拥有产品所有操作权限。	系统策略	全局级
数据库审计系统管理员策略	数据库审计系统管理员策略。	系统策略	全局级
数据库审计审计员策略	数据库审计审计员策略，只具备查看权限。	系统策略	全局级
数据库审计安全员策略	数据库审计安全员策略。	系统策略	全局级
数据库审计业务管理员策略	数据库审计业务员管理员策略，仅支持使用数据库审计实例，不支持订购相关操作。	系统策略	全局级

### 数据库审计权限及授权项

策略支持的操作与授权项相对应，授权项列表说明如下：

- 权限：允许或拒绝IAM用户某项操作。
- 授权项：授权操作对应的权限三元组，创建自定义策略时，支持可视化JSON视图写入权限三元组实现策略配置。
- 权限类型：授权操作对应的读写类型。

# 用户指南

权限	授权项	权限类型 (读/写)	数据库审计 admin策略	数据库审计 系统管理员 策略	数据库审计 审计员策略	数据库审 计安全员 策略	数据库审计 业务管理员 策略
实例安全员角色	dba:ahSecure:access	写	√	×	×	√	×
实例系统管理员角色	dba:ahSystem:access	写	√	√	×	×	×
实例审计员角色	dba:ahAudit:get	读	√	×	√	×	×
获取实例列表	dba:vmList:access	读	√	√	√	√	√
更新实例	dba:vmUpdate:access	写	√	√	×	√	√
更新授权数量	dba:vmAuthAs setUpdate:access	写	√	√	√	√	√
实例启动	dba:vmStart:access	写	√	√	×	√	√
实例关闭	dba:vmShutdown: access	写	√	√	×	√	√
实例删除	dba:vmDelete:access	写	√	√	×	√	√
数据库审计V2 订购	dba:ctydbdba: purchase	写	√	√	√	√	×
数据库审计V2 续订	dba:ctydbdba:renew	写	√	√	√	√	×
数据库审计V2 退订	dba:ctydbdba:refund	写	√	√	√	√	×
数据库审计V2 升配	dba:ctydbdba: upgrade	写	√	√	√	√	×
数据库审计订 购	dba:ctydbDBA VERSION:purchase	写	√	√	√	√	×
数据库审计续 订	dba:ctydbDBA VERSION:renew	写	√	√	√	√	×
数据库审计退 订	dba:ctydbDBA VERSION:refund	写	√	√	√	√	×
数据库审计升 配	dba:ctydbDBA VERSION:upgrade	写	√	√	√	√	×

通过IAM授权使用数据库审计

详细操作请参考：

1. [创建用户组和授权](#)
2. [创建IAM用户和登录](#)
3. [创建企业项目并基于企业项目完成授权](#)

## 云审计服务支持的关键操作

### 操作场景

本服务现已对接天翼云[云审计服务](#)，云审计服务提供对各种云资源操作的记录和查询功能，用于支撑合规审计、安全分析、操作追踪和问题定位等场景，同时提供事件跟踪功能，将操作日志转储至对象存储实现永久保存。

云审计可提供的功能服务具体如下：

- 记录审计日志：支持用户通过管理控制台或API接口发起的操作，以及各服务内部自触发的操作。
- 审计日志查询：支持在管理控制台对7天内操作记录按照事件类型、事件来源、资源类型、筛选类型、操作用户和事件级别等多个维度进行组合查询。
- 审计日志转储：支持将审计日志周期性的转储至对象存储服务（ZOS）下的ZOS桶或日志审计（原生版）服务中。

### 使用限制

- 云审计服务本身免费，包括时间记录以及7天内时间的存储和检索。
  - 若您使用云审计提供的转储至对象存储服务（ZOS）功能，需要开通对象存储服务并支付产生的费用，该费用以对象存储产品的计费为准，参考[计费说明-对象存储](#)。
  - 若您使用云审计提供的转储至日志审计（原生版）功能，需要开通日志审计（原生版）服务并支付产生的费用，该费用以日志审计（原生版）产品的计费为准，参考[计费说明-日志审计（原生版）](#)。
- 用户通过云审计能查询到多久前的操作事件：7天。
- 用户操作后多久可以通过云审计查询到数据：5分钟。
- 其它限制请参考[使用限制-云审计](#)。

### 支持审计的关键操作列表

事件来源	资源类型	操作事件	字段
安全	数据库审计	实例删除	deleteVm
		查询实例列表	queryVoList
		更新实例备注	updateVm
		实例关闭	halt
		实例开启	start
		查询VPC列表	getVpcList
		查询子网列表	getSubnetList
		查询安全组列表	getSecurityList
		查询弹性IP列表	getEipList
		更新实例弹性IP	eipUpdate
		查询可用区列表	getZoneList

# 用户指南

## 查看云审计事件

### 1. 开通云审计服务。

具体操作请参见[开通云审计服务-云审计](#)。

### 2. 在事件列表中，上方时间选择需要筛选的时间段，筛选条件选择事件来源为“安全”，资源类型选择“数据库审计”，单击“查询”即可。

防护事件 [帮助文档](#)

时间选择 **近30分钟** 近一小时 近一天 近七天 自定义时间段 云审计仅记录7天内的操作事件，您需要[创建跟踪任务](#)来保存更长时间的事件！

筛选条件

读写类型  事件级别  操作用户

**事件来源  资源类型**  资源筛选

事件名称

### 3. 在审计事件右侧点击“查看详情”，可以看到更详细的事件信息。

事件级别	事件名称	事件来源	资源类型	资源名称	资源ID	事件时间	操作
> Normal	查询实例列表	安全	数据库审计	--	--	2025-12-10T11:14:01.339	<a href="#">查看详情</a>
> Normal	查询实例列表	安全	数据库审计	--	--	2025-12-10T11:12:00.994	<a href="#">查看详情</a>
> Normal	查询实例列表	安全	数据库审计	--	--	2025-12-10T11:10:01.118	<a href="#">查看详情</a>

详细操作参见[查看审计事件-云审计](#)。更多云审计相关使用说明和常见问题请参考[用户指南](#)、[常见问题](#)。

## 使用云监控服务监控数据库审计实例

### 查看监控数据

为保证数据库审计实例的可靠性、可用性和可观测性，对数据库审计进行监控已经成为一种必要且重要的手段。天翼云控制台提供的数据库审计监控功能，可方便用户更快、更直观的了解数据库审计的运行情况、使用情况及其他性能指标，同时可根据实时监控情况，执行告警通知等操作，帮助客户更好的管理数据库审计实例。

当用户开通数据库审计服务后，即可通过云监控来查看监控指标。

#### 说明

目前仅支持监控“一类节点”区域的实例。数据库审计支持的区域请参见[支持的区域](#)。

#### 实例支持的监控指标

监控指标	指标说明	单位	是否支持告警	监控周期
CPU利用率	该指标用于统计数据库审计实例的CPU利用率。	%	是	5分钟

# 用户指南

监控指标	指标说明	单位	是否支持告警	监控周期
内存总大小	该指标用于统计数据库审计实例的实际内存大小。	GB	是	5分钟
剩余内存大小	该指标用于统计数据库审计实例的空闲的内存大小。	GB	是	5分钟
内存利用率	该指标用于统计数据库审计实例的内存利用率。 内存利用率 = 100% - (剩余内存大小/内存总大小)	%	是	5分钟
系统盘大小	该指标用于统计数据库审计实例的实际系统盘大小。	GB	是	5分钟
剩余系统盘大小	该指标用于统计数据库审计实例的空闲的系统盘大小。	GB	是	5分钟
系统盘利用率	该指标用于统计数据库审计实例的系统盘利用率。 系统盘利用率 = 100% - (剩余系统盘大小/系统盘大小)	%	是	5分钟
数据盘大小	该指标用于统计数据库审计实例的实际数据盘大小。	GB	是	5分钟
剩余数据盘大小	该指标用于统计数据库审计实例的空闲的数据盘大小。	GB	是	5分钟
数据盘利用率	该指标用于统计数据库审计实例的数据盘利用率。 系统盘利用率 = 100% - (剩余数据盘大小/数据盘大小)	%	是	5分钟

## 查看监控图表

1. 登录天翼云控制中心。
2. 在产品服务列表中“管理与部署 > 云监控服务”，进入云监控服务主页面。

# 用户指南

3. 在左侧导航栏，选择“云服务监控”，单击“数据库审计”产品。



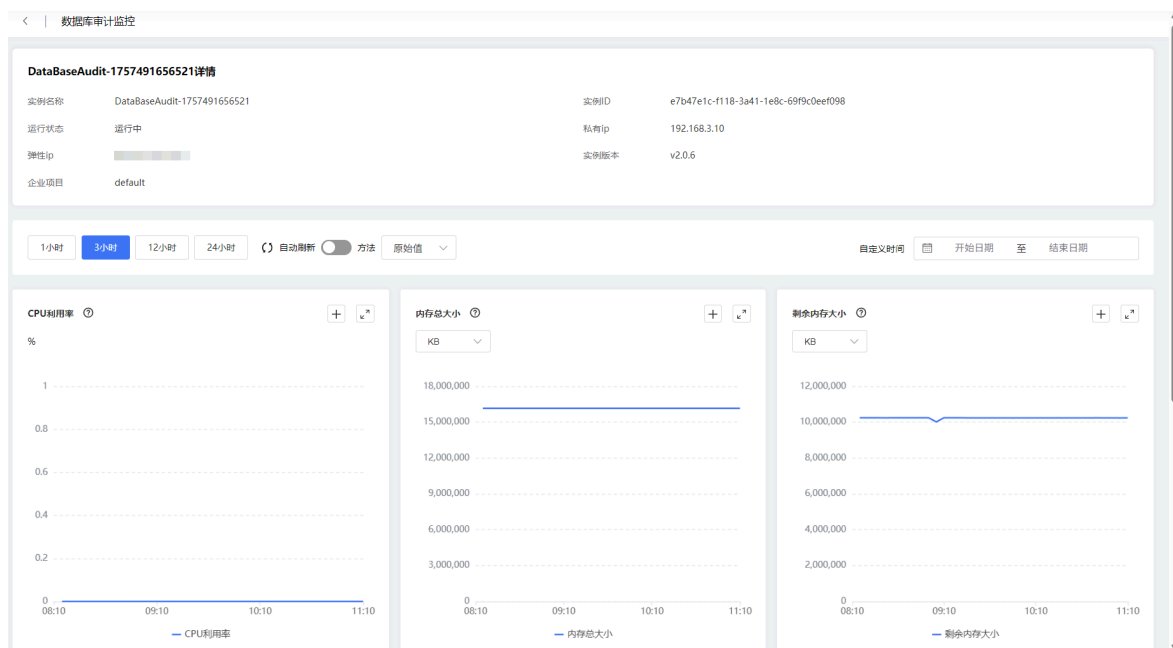
4. 在数据库审计监控列表中选择目标实例，单击操作列的“查看监控图表”，进入监控详情页。



# 用户指南

5. 在监控详情页，可以查看实例详情和监控图表。

切换不同的时间周期，查看不同周期内监控指标的情况。



## 创建告警监控规则

云监控支持灵活的创建告警规则。您既可以根据实际需要为某个监控指标设置自定义告警规则，同时也能够使用告警模板为多个资源或者云服务批量创建告警规则。

### 说明

目前仅支持监控“一类节点”区域的实例。数据库审计支持的区域请参见[支持的区域](#)。

### 操作步骤

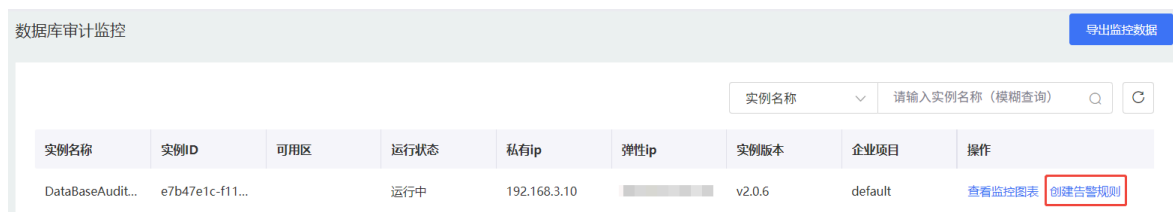
1. 登录天翼云控制中心。
2. 在产品服务列表中“管理与部署 > 云监控服务”，进入云监控服务主页面。

# 用户指南

3. 在左侧导航栏，选择“云服务监控”，单击“数据库审计”产品。



4. 在数据库审计监控列表中选择目标实例，单击操作列的“创建告警规则”。



5. 在“创建告警规则”页面，根据界面提示配置参数。

配置参数及相关含义说明如下：

模块	参数	参数说明	配置示例
选择监控对象	规则类型	选择规则的类型，主要包括指标监控、事件监控、站点监控、自定义监控、自定义事件五种。	指标监控
	服务	配置告警规则监控的云服务资源类型。	数据库审计
	维度	用于指定告警规则对应指标的维度名称。	数据库审计实例
	监控对象类型	具体实例/资源分组/全部资源	具体实例
	监控对象	用来配置该告警规则针对的具体资源，可以是一个或多个。	实例名称

# 用户指南

模块	参数	参数说明	配置示例
定义告警策略	选择类型	支持自定义创建、从模板导入。	自定义创建
	策略	支持选择 <b>满足全部</b> 或 <b>任意策略</b> 。 策略信息包括： <ul style="list-style-type: none"> <li>• 监控指标，支持的监控指标请参见<a href="#">实例支持的监控指标</a>。</li> <li>• 数据类型（原始值）</li> <li>• 判断条件（&gt;、≥、&lt;、≤、=、环比上升、环比下降、环比变化）</li> <li>• 值</li> <li>• 单位</li> <li>• 发生次数</li> <li>• 级别（普通、警示、紧急）</li> </ul> <p>说明 同一告警规则，告警条件最多支持添加20条。</p>	满足全部以下条件：若CPU利用率的原始值≥80%，连续发生1次，普通
	无数据处理	不做处理/视为告警/视为恢复。	不做处理
配置告警通知	发送通知	配置是否发送邮件通知用户，可以选择开启（推荐选择）或者关闭。	开启
	通知方式	仅支持“通知联系人组”。	通知联系人组
	告警联系组	选择发生告警通知时通知的用户组。支持选择联系组或者云账户默认联系人。	-
	触发场景	触发告警邮件的场景，可在出现告警和告警恢复时发送提醒信息。	出现告警
	通知渠道	配置告警通知的通知渠道，支持邮箱、短信、语音（语音需要单独订购）。	邮箱
	重复告警	指告警发生后如果未恢复正常，将重复发送告警通知次数。	不重复
	通知频率	指告警发生后如果未恢复正常，间隔多久重复发送一次告警通知。 若 <b>重复告警</b> 选择“不重复”时，无需配置该参数。	每24小时通知一次
	通知周期	配置告警通知的周期时间。	星期天、星期一、星期二、星期三、星期四、星期五、星期六
	通知时段	配置告警通知的时间段。	00:00:00-23:59:59
	告警回调	配置告警通知webhook地址。	-
通知模板	告警信息默认使用系统模板；也可以选择用户自定义创建的通知模板，自定义模板详细操作请参见 <a href="#">创建自定义告警模板</a> 。	系统模板	

# 用户指南

模块	参数	参数说明	配置示例
规则信息	名称	该告警规则的自定义名称。	evs-alarm-note
	企业项目	选择告警规则适用的企业项目。	default
	描述	添加对该告警规则描述。	-

6. 配置完成后，单击“确定”完成操作。

告警规则添加完成后，当监控指标触发设定的阈值时，云监控会在第一时间通过邮件实时告知您云上资源异常，以免因此造成业务损失。关于云监控的其他操作和更多信息，请参考《云监控服务》。

## 总览

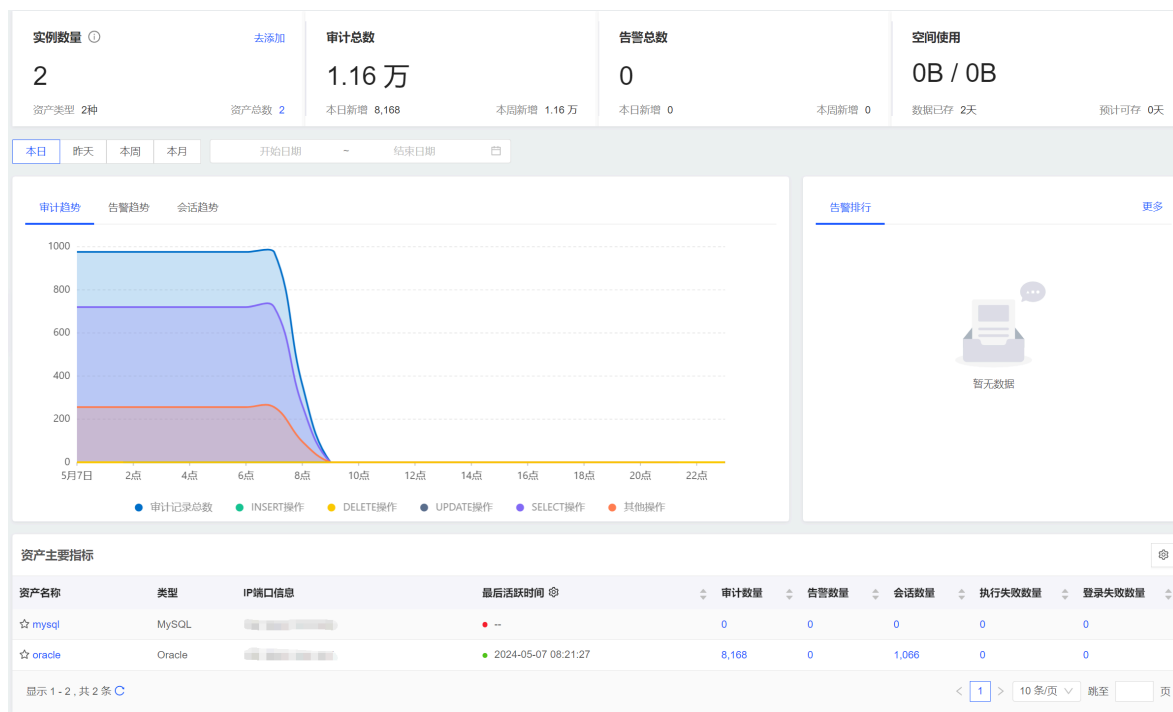
### 仪表盘

在左侧菜单栏选择“总览 > 仪表盘”进入“仪表盘”页面。

“仪表盘”模块提供可视化图表直观展示系统运行状态，主要包括系统资源使用汇总、态势分析、告警排行和资产信息汇总。

用户可在仪表盘查看以下信息，或执行以下操作：

- 查看实例数量、审计总数、告警总数和空间使用等参数。
- 查看指定时间段内的审计趋势、告警趋势、会话趋势和告警统计情况。在告警排行中单击“更多”可在告警分析页面优化告警。



# 用户指南

- 查看指定时间段内资产汇总信息和资产活跃时间和状态。可分别根据审计数量、告警数量、会话数量、执行失败数量和登录失败数量进行排序。

资产主要指标

资产名称	类型	IP端口信息	最后活跃时间	审计数量	告警数量	会话数量	执行失败数量	登录失败数量
☆ 正则自动化_192.168...	Oracle	192.168.180.40:1521	2023-05-17 22:31:01	56	14	14	0	0
☆ 正则自动化_192.168...	Oracle	192.168.180.1:1521	2023-05-17 22:30:14	14	7	5	7	0
☆ 正则自动化_192.168...	Oracle	192.168.180.2:1521	2023-05-17 22:30:15	14	7	5	7	0
☆ 正则自动化_192.168...	Oracle	192.168.180.3:1521	2023-05-17 22:30:16	14	7	5	7	0
☆ 正则自动化_192.168...	Oracle	192.168.180.4:1521	2023-05-17 22:30:17	14	7	5	7	0

显示 1 - 10, 共 140 条

- 在实例数量模块中单击“去添加”可添加新的资产。有关资产的详细信息，请参见[资产章节](#)。
- 在告警总数中点击“告警优化”可在告警分析页面优化告警。有关告警优化的详细信息，请参见[告警分析章节](#)。

## 表分析

在左侧菜单栏选择“总览 > 表分析”进入“表分析”页面。

“表分析”模块可从表视角、数据库/SID视角、资产视角查看数据库的使用情况，发现热库、热表，梳理库、表、字段，转为对象组后设置针对性的规则。

## 表视角

从全局视角显示表的使用概况。默认展示分析当天的审计数据，并按照审计数量进行倒叙排列。发现需要关注的表，可单击“表名”列具体的表名进入详情页。

表分析数据每小时更新一次。如无数据请耐心等待。

全部资产 2023-05-18 00:00:00 ~ 2023-05-18 10:59:59 请输入数据库/SID 请输入表名 表过滤管理

资产名称	数据库/SID	表名	审计数量	Select	Insert	Update	Delete	其他
核心业务xxx测试系统	SYSTEM	PAT_VISIT	313251					
核心业务xxx测试系统	SYSTEM	ADT_LOG	296749					
核心业务xxx测试系统	ihd 库的备注信息	Remind 表的备注信息	292465					
核心业务xxx测试系统	ihd 库的备注信息	pat_master_index	274384					
核心业务xxx测试系统	ihd 库的备注信息	REMINO_TYPE_DICT	268300					
核心业务xxx测试系统	ihd 库的备注信息	pats_in_hospital	229842					
核心业务xxx测试系统	ihd 库的备注信息	DEPT_DICT	211662					
核心业务xxx测试系统	SYSTEM	OPERATION_MASTER	189202					
核心业务xxx测试系统	ihd 库的备注信息	pat_visit	161036					
核心业务xxx测试系统	ihd 库的备注信息	d	148174					
核心业务xxx测试系统	ihd 库的备注信息	MR_ON_LINE	128853					
核心业务xxx测试系统	IHD 库的备注信息	AREA_DICT	125902					

共 727 条 < 1 2 3 4 5 ... 37 > 20 条/页 跳至 页

## 表详情

显示该表的基础信息、审计数量、影响行数、访问关系等，可对数据库/SID、表、字段设置备注与对象组信息。各级子菜单信息展示如下：

# 用户指南

- 表结构：显示表所属节点信息，以及对应下级节点的个数、审计数量。
- XX详情（“XX”为具体的表名或数据库/SID名或资产名称，请以实际情况为准）：显示表的基础信息，可对表、数据库/SID设置备注、对象组信息。
- 字段信息：显示选中表中包含的字段信息，可对字段设置字段备注、对象组信息。
- 数据流动趋势：显示各个时间段该表的审计数量与影响行数。
- 访问关系分析：使用图表的方式显示访问该表的客户端IP、数据库账号、操作类型信息，用于梳理访问权限，帮助用户实现权限最小化。

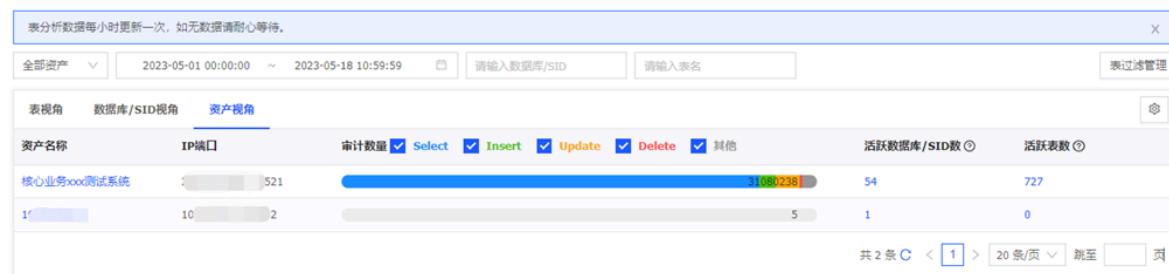
## 数据库/SID视角

从全局视角分析数据库的使用概况，默认展示当天的审计数据，并按照“审计数量”进行倒叙排列。发现需要关注的数据库/SID，可单击“数据库/SID”列具体的数据库/SID名进入详情页。



## 资产视角

从全局视角分析资产的使用概况，可单击对应的资产名称进入详情页。

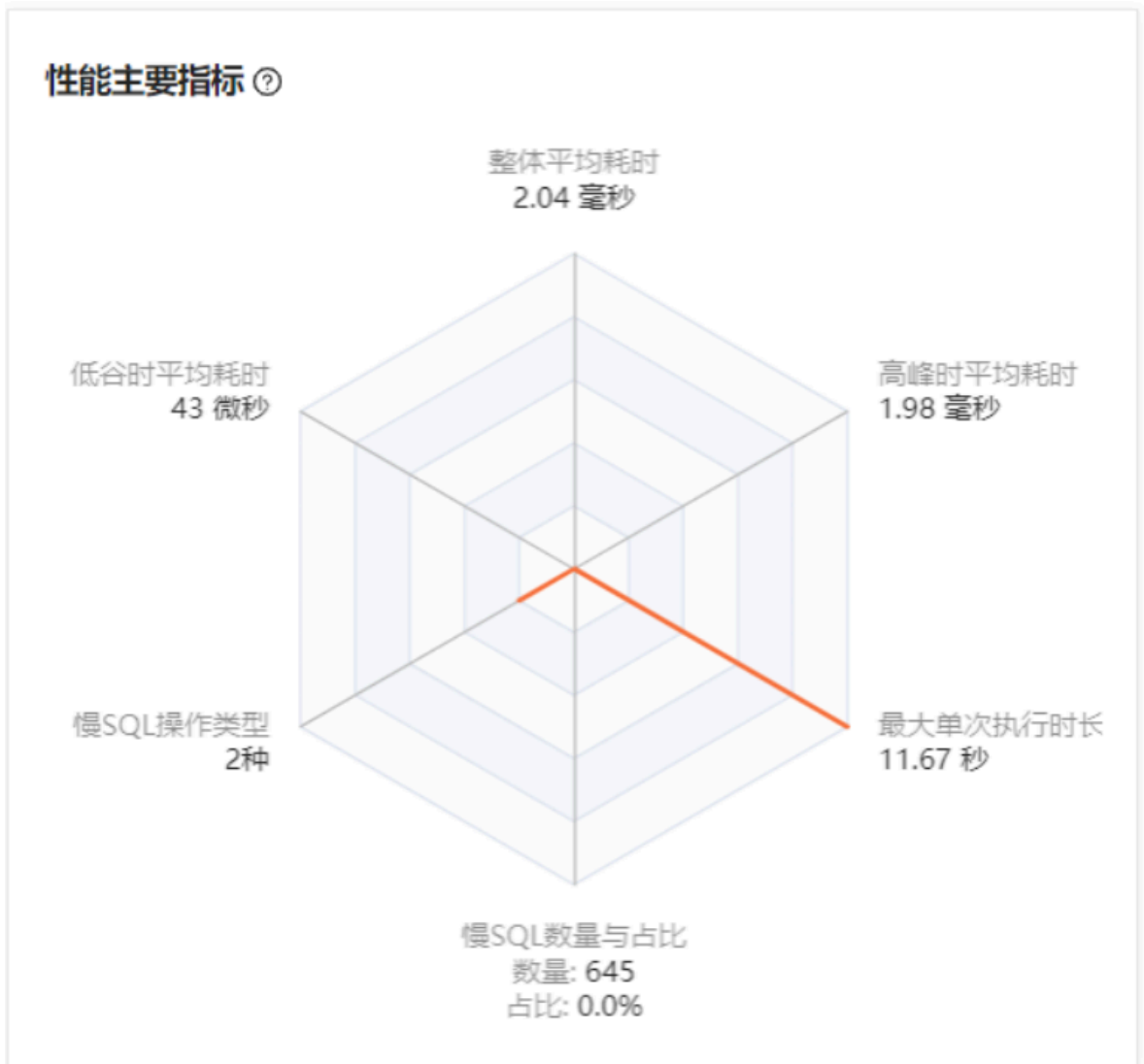


资产详情页显示该资产的基础信息、审计数量、影响行数、访问关系等。资产详情页数据统计维度是根据所选择的资产访问维度进行统计。

## 性能分析

在左侧菜单栏选择“总览 > 性能分析”进入性能分析页面，可查看审计到SQL的性能，包括执行时长和执行次数等信息，为DBA改进数据库性能提供参考数据。

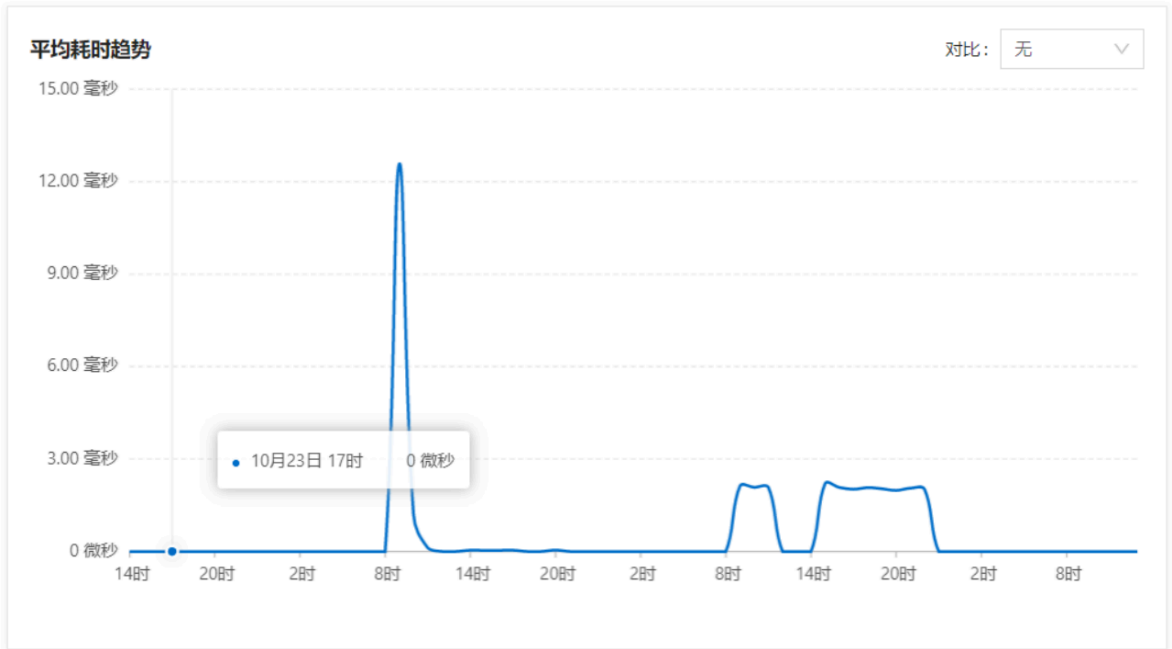
- 查看SQL性能的主要指标。
  - 整体平均耗时：指定时间范围内，SQL总执行时长/执行总数，耗时1s及以上，雷达图满格。
  - 低谷时平均耗时：指定时间范围内有且SQL数量最少的时段，耗时1ms及以上，雷达图满格。
  - 高峰时平均耗时：时间范围内，审计日志数量最多的单位小时内总执行时长/执行总数，耗时1s及以上，雷达图满格。
  - 慢SQL操作类型：时间范围内，执行时长超过1s的语句的操作类型，15种及以上，雷达图满格。
  - 慢SQL数量与占比：时间范围内，执行时长超过1s的语句数量/语句总数，占比100%，雷达图满格。



# 用户指南

- 查看平均耗时趋势。

可查看SQL平均耗时趋势图，支持与昨天、上周和上月进行对比。



- 查看审计日志的执行时长的分布情况。

面积越大即代表平均耗时越长，颜色越深即代表SQL数量越多。将光标悬停于对应的区域可以看到具体的信息，包含资产、IP和端口、数据库名、平均耗时和执行次数。

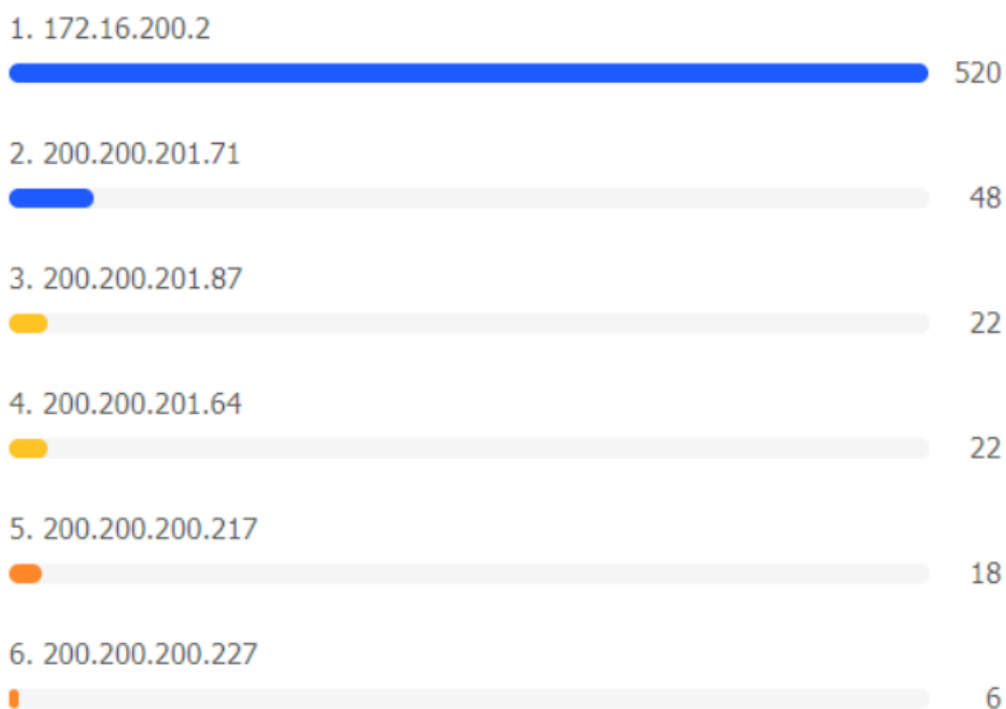


- 查看慢SQL来源。  
支持从客户端IP和数据库账号两个维度统计慢SQL的数量。

## 慢SQL来源

客户端IP

数据库账号



# 用户指南

- 查看SQL语句的性能排行。

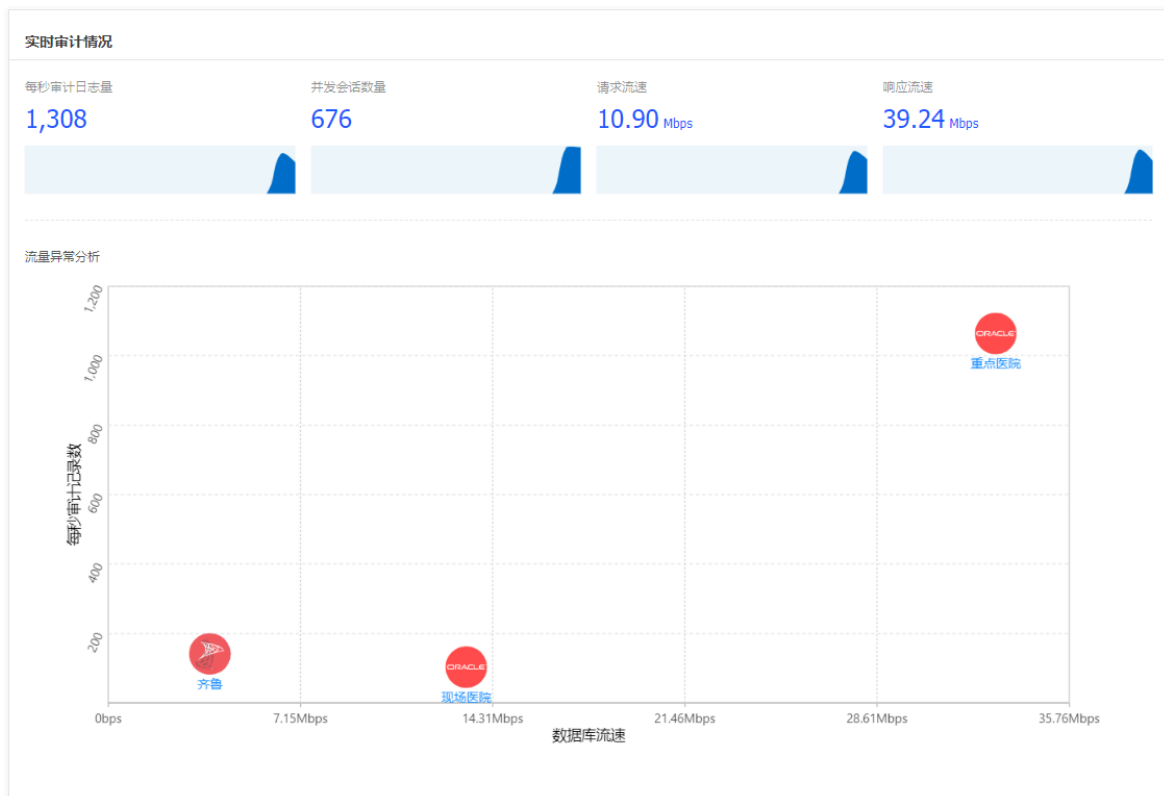
分四个TOP排行，分别是平均执行时长TOP、执行次数TOP、总执行时长TOP和执行时长TOP。其中前三个TOP根据SQL模板进行统计，最后一个执行时长TOP根据审计日志进行统计。点击<更多>可以跳转到TOP SQL页面查看更多的排行信息。

TOP SQL						更多		
平均执行时长TOP						执行次数TOP	总执行时长TOP	执行时长TOP
排行	SQL模板	服务端IP	平均执行时长	执行次数	总执行时长			
1	select A.BED_NO, A.WARD_CODE, A.BED_SEX_TYPE, A.DEPT_CODE, A.BED_LABEL, A.BED_STATUS, A.PATIENT_ID, A.VISIT_ID, A.ADMISSION_DATE_TI	200.200.200.3	146.38 毫秒	31,023	4541.08 秒			
2	SELECT "CLINIC_MASTER"."NAME", "CLINIC_MASTER"."PATIENT_ID", "CLINIC_MASTER"."VISIT_NO", "CLINIC_MASTER"."VISIT_DATE", "CLINIC_MA	200.200.200.3	38.05 毫秒	307	11.68 秒			
3	SELECT "DRUG_PRESC_MASTER_TEMP"."PRESC_NO", "DRUG_PRESC_MASTER_TEMP"."NAME", "DRUG_PRESC_MASTER_TEMP"."NAME_PHONETIC", "DR	200.200.200.3	37.61 毫秒	170	6.39 秒			
4	SELECT "DRUG_PRESC_MASTER_TEMP"."PRESC_NO", "DRUG_PRESC_MASTER_TEMP"."NAME", "DRUG_PRESC_MASTER_TEMP"."NAME_PHONETIC", "I	200.200.200.3	28.82 毫秒	6,845	197.30 秒			
5	select a.PATIENT_ID,a.VISIT_ID,a.NAME,a.SEX,a.STATUS,a.REQUEST_DOCTOR_ID,a.REQUEST_DATE_TIME,a.NAME_PHONETIC,a.DATE_OF_BIRTH,a.DE	200.200.200.3	18.55 毫秒	191,781	3558.14 秒			
6	SELECT "COMM"."AREA_DICT"."AREA_CODE", "COMM"."AREA_DICT"."AREA_NAME" FROM "COMM"."AREA_DICT"	200.200.200.3	15.10 毫秒	42,816	646.53 秒			
7	select A.BED_NO, A.WARD_CODE, A.BED_SEX_TYPE, A.DEPT_CODE, A.BED_LABEL, A.BED_STATUS, A.PATIENT_ID, A.VISIT_ID, A.ADMISSION_DATE_TI	200.200.200.3	10.52 毫秒	20,597	216.76 秒			
8	login :1	200.200.200.3	8.60 毫秒	69,363	596.61 秒			
9	select T1.BED_APPROVED_TYPE,T1.BED_SEX_TYPE,T1.BED_STATUS,T1.BED_NO,T1.BED_CLASS,T1.BED_LABEL,T1.DEPT_CODE,T1.ROOM_NO,T1.WARD.	200.200.200.3	8.42 毫秒	30,291	253.16 秒			
10	SELECT "COMM"."DIAGNOSIS_DICT"."DIAGNOSIS_NAME", "COMM"."DIAGNOSIS_DICT"."DIAGNOSIS_CODE" FROM "COMM"."DIAGNOSIS_DICT"	200.200.200.3	8.36 毫秒	58,804	491.84 秒			

## 实时监控

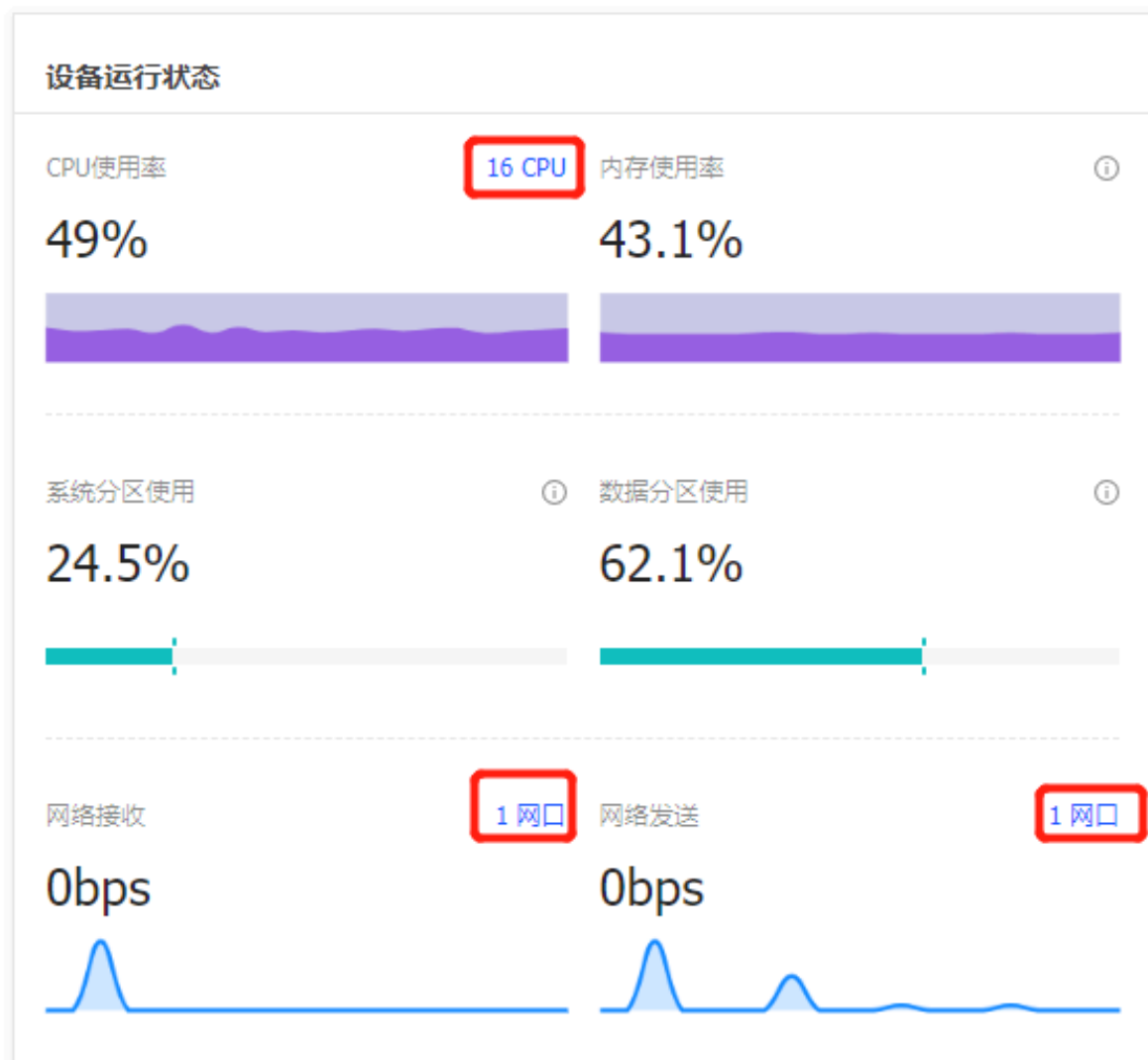
在左侧菜单栏选择“总览 > 实时监控”进入实时监控页面，可实时监控系统状态。

- 查看实时审计情况。



## 用户指南

- 查看设备运行状态。点击<\*CPU>可查看设备所有CPU的使用率；点击<\*网口>可查看设备所有网口的网络速率（“\*”为数字，请以实际情况为准）。



- 查看最新告警信息。

## 最新告警

	 2023-05-17 22:31:35	 orclcdb	 10.11.39.66
	 <b>高风险</b>	MULTILINESTRING报错注入	
	 2023-05-17 22:31:34	 orclcdb	 10.11.39.66
	 <b>高风险</b>	LINESTRING报错注入	
	 2023-05-17 22:31:33	 orclcdb	 10.11.39.66
	 <b>高风险</b>	MULTIPOLYGON报错注入	
	 2023-05-17 22:31:32	 orclcdb	 10.11.39.66
	 <b>高风险</b>	POLYGON报错注入	
	 2023-05-17 22:31:31	 orclcdb	 10.11.39.66
	 <b>高风险</b>	MULTIPOINT报错注入	
	 2023-05-17 22:31:30	 orclcdb	 10.11.39.66
	 <b>中风险</b>	Oracle_使用JAVA_SOURCE调用外部程序2	
	 2023-05-17 22:31:29	 orclcdb	 10.11.39.66
	 <b>中风险</b>	DECODE报错注入	
	 2023-05-17 22:31:28	 orclcdb	 10.11.39.66
	 <b>中风险</b>	布尔盲注特征	

# 用户指南

- 查看资产负载状态。

资产负载状态 <span style="float: right;">实时刷新</span>				
资产名称	并发会话数	请求流速	返回流速	每秒SQL吞吐量
autotestOraclenew	3,412	0bps	0bps	0
autotestMySQLnew	11,241	0bps	0bps	0
autotestSQLServernew	2,375	0bps	0bps	0
autotestDB2new	4,908	0bps	0bps	0
autotestCachenew	1,460	0bps	0bps	0
autotestPostgreSQLnew	46	0bps	0bps	0
autotestMongoDBnew	252	0bps	0bps	0
autotest-mysql	1	0bps	0bps	0
autotest-oracle	3	0bps	0bps	0

显示 1 - 9, 共 9 条 < 1 > 10 条/页 跳至  页

点击并发会话数列的数字可查看资产会话的详细信息。

返回 autotest-oracle的当前会话 <span style="float: right;">实时刷新</span>								
来源	目的	客户端主机名	连接时长	累计SQL数量	请求流速	响应流速	每秒SQL吞吐量	当前是否活跃
10.11.33.177:4613	192.168.21.243:1521	WORKGROUP...	82	24	0B	0B	0	否
10.11.33.177:4204	192.168.21.243:1521	WORKGROUP...	164	37	0B	0B	0	否
10.11.33.177:4197	192.168.21.243:1521		0	3	0B	0B	0	否

显示 1 - 3, 共 3 条 < 1 > 10 条/页 跳至  页

## 数据库审计资产管理

添加资产后，系统可对资产进行安全审计。

### 添加资产

添加资产包括单个添加和批量导入两种方式。

- 在左侧菜单栏选择“资产 > 资产管理”进入“资产管理”页面，选择“资产管理”页签，单击“添加”。

资产管理										
资产管理										
<input type="checkbox"/>	名称	资产组	类型	IP端口	最后活跃时间	编码	操作系统	状态	流量方向	操作
<input type="checkbox"/>	☆ mysql	自发现资产组	MySQL 8.0		--	自动识别	Unix	启用	双向审计	编辑   删除
<input type="checkbox"/>	☆ oracle	自发现资产组	Oracle 21c		2024-05-07 08:31:44	自动识别	Linux	启用	双向审计	编辑   删除

启用全部  禁用全部  共 2 条 < 1 > 20 条/页 跳至  页

# 用户指南

2. 在弹出的“添加资产”窗口编辑相关信息。参数填写规则可参见下表。

参数	参数说明
保存时启用推荐的规则	<ul style="list-style-type: none"><li>勾选此选项，则保存时添加的资产会使用系统推荐的规则。</li><li>不勾选此选项，保存时添加的资产不会使用系统推荐的规则。</li></ul>
类型	设置资产类型，包括关系型、非关系型、大数据、图形、全文、文档、键值、其他、天翼云RDS等。  说明 若添加天翼云RDS资产，还需要在“系统管理 > 日志采集方式”中开启接收天翼云RDS日志。
资产组	设置资产所属的资产组。
名称	填写资产的名称，必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过64字符。
操作系统	设置资产所在主机的操作系统。
IP端口	设置资产所在主机的IP及端口号。

## 说明

- 本地运维行为审计是指通过安装本地Agent捕获本地数据库客户端程序中实际响应的SQL指令，实现对本地运维人员数据库操作行为的审计，支持Oracle、PostgreSQL、MySQL、SQL Server等主流数据库。
- 当使用本地运维行为审计方式时，需要添加回环IP地址127.0.0.1和端口号，端口号需根据数据库类型进行填写。
- 如果使用的IP类型为IPv6，IP地址需填写为“::1”。

3. 如需配置其他更多信息，可点击“更多配置”，选择单向审计或双向审计，设置加密协议审计。参数填写规则可参见下表。

参数	参数说明
流量方向	<ul style="list-style-type: none"><li>单向审计：审计内容包括请求信息、客户端信息、服务端信息，不包括返回结果集。</li><li>双向审计：审计内容包括请求信息、客户端信息、服务端信息、返回结果集。</li></ul>
保持行数	取值范围：0~999，0表示不保存返回结果。最大保存内容为64KB。
最大保存长度	取值范围：1~64KB，确保整行显示。
解密私钥	加密协议导入解密私钥，目前支持MySQL、SQL Server、HTTPS加密解析，证书支持导入和编辑两种方式。
证书密码	安全证书的密码。

4. 配置完成后，单击“保存”即可完成资产添加。

## 说明

资产添加之后，需要确认部署模式。若选择流量代理模式，需要部署Agent程序才能完成数据库审计。

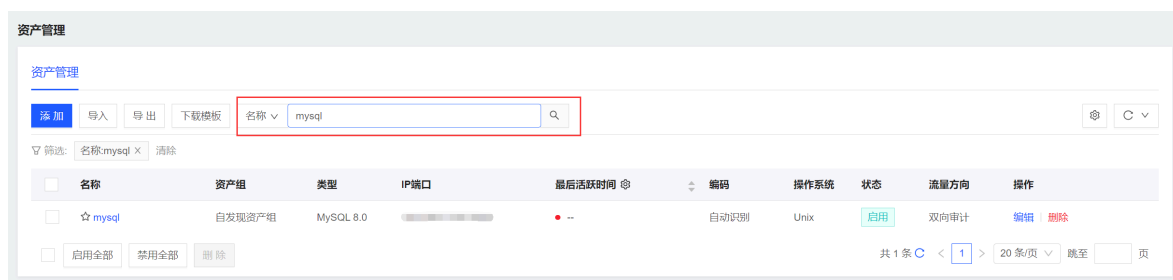
# 用户指南

## 编辑资产

1. 在“资产管理”页面，选择“资产管理”页签，选择待编辑的资产，单击“操作”列的“编辑”按钮。
2. 在编辑“资产页面”可以修改资产的所有配置项。具体字段说明信息请参考[添加资产](#)的配置项和说明。
3. 配置完成后，单击“保存”即可完成资产添加。

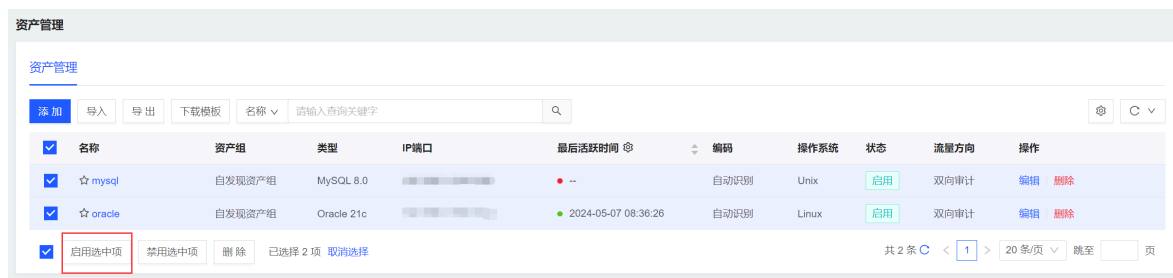
## 查询资产

在“资产管理”页面，选择“资产管理”页签，选择查询条件（包括名称、IP/端口、类型和资产组）填写查询内容即可完成单个条件的查询。



## 启用/禁用资产

1. 在“资产管理”页面，选择“资产管理”页签，选中待启用或禁用的资产，点击列表下方的“启用选中项”或者“禁用选中项”按钮。



2. 在弹出的对话框中，单击“确定”完成资产的启用或禁用。

## 删除资产

1. 在“资产管理”页面，选择“资产管理”页签，选择待删除的资产，单击“操作”列的“删除”按钮。
2. 在弹出的对话框中，单击“确定”完成资产删除。

## 关注资产

关注资产是指当前用户较为关心的资产。

- 点击资产名称左侧的 ☆ 图标即为关注此资产，关注后此资产会置顶。
- 再次点击 ☆ 图标可取消关注，该资产会回到原来的位置。

## Agent管理

审计代理插件（Agent）是安装在数据库系统或者业务系统上的插件，其功能是捕获访问数据库系统的数据包，并将数据包发送至天翼云数据库审计。当数据库系统部署在公有云、私有云或者实际场景下无法进行端口镜像时，可以通过流量代理的方式抓取数据库流量。

### 支持的操作系统

Agent支持的操作系统版本请参考[使用限制](#)。

### Agent工作原理

- Agent在数据库服务器的接口上抓取属于资产下发的IP+Port 的数据库操作的流量。
- Agent 包含两个进程：dbagent.exe 和 dbMonitor.exe。
  - DBAgent与天翼云数据库审计的13002端口建立连接负责流量转发。
  - DBMonitor与天翼云数据库审计的13001端口建立连接负责控制部分，包含接收天翼云数据库审计下发的资产和其他配置。

### 通过SSH远程安装Agent

您可以通过SSH协议将Agent自动安装到需要审计的服务器上，**目前仅支持Linux系统**。

在界面上输入需要审计的服务器IP、SSH端口、root用户名、密码，天翼云数据库审计通过scp协议将agent安装包传输到宿主机上并自动安装。

1. 在菜单栏选择“系统管理 > Agent管理”进入“Agent管理”页面，选择“Agent安装”页签。
2. 单击“开始安装”进入通过SSH远程安装Agent页面，编辑审计服务器IP，并添加安装Agent的服务器，单击“安装”。

填写参数说明请参见下表：

参数	参数说明
审计服务器IP	默认为当前的审计服务器IP，用户可以根据需要修改。
安装Agent的服务器	输入需要安装Agent的服务器IP及该服务器root账户的密码，默认端口为22，用户可以根据实际情况修改。 <ul style="list-style-type: none"><li>• 支持表单格式和文本格式输入。</li><li>• 支持IPv4和IPv6。</li><li>• 最多填写20个。</li></ul>

#### 说明

单击“安装状态”可进入“安装状态”查看页面，可进行以下操作：

- 单击“卸载”可远程卸载已经成功安装了Agent。
- 单击“重新安装”可对未成功安装Agent的服务器重新安装。
- 将光标悬停至“安装失败”后的图标，查看安装失败原因。
- 若您的业务部署在一类节点的资源池上，审计服务器IP需改为数据库审计所在的VPC组的公网IP。（一类节点可参考[支持的区域](#)，如何获取VPC组的公网IP可参考[VPC-查看终端节点](#)章节）

## 手动安装Agent

您可手动下载Agent安装包，并将其手动安装到需要审计的服务器上。目前支持Windows系统和部分Linux系统，支持的操作系统可查看[使用限制](#)。

## 使用Linux系统安装Agent

1. 在左侧菜单栏选择“系统管理 > Agent管理”进入“Agent管理”页面，选择“Agent安装”页签，点击下载对应版本的Agent安装包。

### 注意

- 下载的Agent默认会将流量转发给当前的天翼云数据库审计实例。如需转发到其他天翼云数据库审计实例，请在解压后的Agent路径下agent.ini配置文件中找到serviceIp选项进行地址修改。
- 无论是Linux版本安装包、AIX版本安装包还是Windows版本安装包，文件夹中均有“ReadMe”文档，文档内包含使用说明、文件说明、注意事项、运行环境说明、配置文件说明。在安装前请仔细阅读该文档并严格按照要求进行操作。

2. 安装包下载完之后，将Agent安装包上传到Linux服务器指定目录。

### 说明

- 禁止直接运行二进制文件。
- 解压目录不能出现空格。
- 每次更换运行或解压目录需重新运行安装脚本。
- Linux环境需以root用户运行脚本，指定解释器bash，或不指定解释器直接运行。

```
[root@oracle test_1]# ll
总用量 8276
-rw-r--r-- 1 root root 8472119 6月  2 16:37 dbagent_linux_V2.29.tar.gz
```

3. 使用 `tar -xf dbAgent_V2.28.tar.gz`命令解压Agent安装包，进入Agent安装目录。
4. 在安装目录执行 `./install.sh`命令即可安装Agent程序。

## 使用Windows系统安装Agent

1. 在左侧菜单栏选择“系统管理 > Agent管理”进入“Agent管理”页面，选择“Agent安装”页签，点击下载对应版本的Agent安装包。

### 注意

- 下载的Agent默认会将流量转发给当前的天翼云数据库审计实例。如需转发到其他天翼云数据库审计实例，请在解压后的Agent路径下agent.ini配置文件中找到serviceIp选项进行地址修改。
- 无论是Linux版本安装包、AIX版本安装包还是Windows版本安装包，文件夹中均有“ReadMe”文档，文档内包含使用说明、文件说明、注意事项、运行环境说明、配置文件说明。在安装前请仔细阅读该文档并严格按照要求进行操作。

2. 安装包下载完成之后，将Agent安装包上传到Windows服务器上。

# 用户指南

3. 解压压缩包到指定运行目录。在Agent的安装目录以管理员身份运行“dbAgent-setup.exe”进入安装向导，单击“下一步”。
4. 单击“下一步”之后显示“Install winpcap”和“Install npcap”两个选项，根据实际需求选择完成后单击“下一步”。

## 说明

- 如果没有本地审计的需求请选择“Install winpcap”；
- 如果需要部署本地审计，则选择“Install npcap”。
- 默认推荐使用“Install winpcap”安装方式，对于Windows操作系统的兼容性较好。
- “Data encrypted transmission”仅需要配置agent数据传输加密情况下才需要勾选。

5. 单击“安装”。
6. 点击“I Agree”同意安装协议后，之后按照提示进行操作。

## 说明

由于第四步选择的差异，“Winpcap”和“Npcap”安装操作选项会有些许差别。

- “Winpcap”插件根据默认选择安装即可。
- “Npcap”插件需要选择Legacy loopback support for Nmap 7,80 and older , Not needed for Wireshark. 和 Install Npcap in WinPcap API-compatible Mode. 两个选项。

7. 安装完成后点击“完成”退出安装向导。

## 监控Agent状态

在“Agent管理”页面，在已安装Agent列表的操作列下点击“监控”进入“Agent监控信息”页面，用户可以根据需要设置监控的时段，或者选择不同的监控指标（CPU占用、内存占用、转发速率、丢包数量、磁盘读写）。

## 修改Agent配置

1. 在“Agent管理”页面，选择需要修改配置的Agent，在列表中单击“操作”列中的“配置”。
2. 弹出修改配置对话框，可根据需要修改相关参数，修改完成后单击“确定”。

各配置项参数请参见下表。

配置项	配置项说明
CPU亲和性	启用后，Agent将仅在单颗CPU核心上工作。 CPU亲和性指的是进程在指定的CPU上尽量长时间运行而不被迁移到其他处理器，也称为CPU关联性。在多核运行的机器上，每个CPU会有缓存，缓存着进程使用信息，如果进程被调度到其他CPU上，CPU缓存命中率会降低，导致处理性能降低。 一旦修改配置，Agent会自动重启生效。
CPU使用上限	默认值为100%，取值范围：0%~100%，填0表示不限制。
内存使用上限	Agent缓存数据包所用的内存，默认值200MB，不能超过设备的最大内存。
系统CPU使用阈值	默认值100%，取值范围：0%~100%，填0表示不限制。
系统内存使用阈值	默认值100%，取值范围：0%~100%，填0表示不限制。
系统磁盘读IO阈值	默认值0，表示不限制。不能超过系统磁盘的最大读速率。

# 用户指南

配置项	配置项说明
系统磁盘写IO阈值	默认值0，表示不限制。不能超过系统磁盘的最大写速率。
抓包网口	配置后将只抓取指定网口上的流量，为空时抓取全部网口上的流量，多个网口请用空格分隔。
抓包过滤串	配置后，抓包网口将只抓取匹配该过滤串（通常设置为指定主机的指定端口流量，例如：host 192.168.0.1 and port 3306）的流量。一旦配置，将不再根据配置的资产自动抓包。
按工具过滤	填写后将不再转发指定客户端工具的流量，可填写多个，多个值请用逗号分隔。
按账号过滤	填写后将不再转发指定数据库账号的流量，可填写多个，多个值请用逗号分隔。
本地回环配置	系统支持本地回环审计功能，此功能可以实现不通过TCP/IP连接的本地数据库访问审计。本地回环审计是指Agent为客户端工具注入.so程序，客户端工具与服务端的通信流量客户端工具会复制一份发送给Agent，Agent转发给天翼云数据库审计。 Agent安装成功后，需要在Web界面开启“本地审计”功能。
回环网口	回环网口的名称，为空时会自动识别，不建议配置此项。
回环抓包过滤串	配置后回环网口将只抓取匹配该过滤串的流量。一旦配置，将不再根据配置的资产自动抓包。
回环网口替换IP(v4/v6)	将流量中本地回环的IPv4或IPv6地址改为设置的值，为空则不替换。
远程登录审计	默认关闭。 启用后，本地流量中的IP端口会被远程连接的IP端口所替换。需要在资产界面添加被远程连接的服务器IP地址，若没有远程连接，则不做替换。 一旦开启，性能会明显下降。
本地审计	支持审计非网络形式（进程间通信等）的数据库通信数据，目前仅支持Oracle, PostgreSQL, MySQL, SQL Server, DB2的特定版本。
调试模式	默认关闭。开启后会记录下更详细的调试日志。
数据传输加密	默认关闭。开启后会对Agent转发的数据进行加密。
CPU异常保护阈值	当Agent的CPU使用超过该值时，Agent将自动修复异常。 正常情况下，Agent的CPU使用不会超出所配的上限，该配置可作为兜底保护，防止特殊情况发生。默认值100%，填0表示关闭CPU异常保护功能。
内存异常保护阈值	当Agent的内存使用超过该值时，Agent将自动修复异常。该配置可作为兜底保护，防止特殊情况发生。默认值300M，填0表示关闭内存异常保护功能。

## Agent标签管理

1. 在“Agent管理”页面，点击标签显示列对应区域。
2. 选择标签或者输入新的标签点击阅读即可完成标签添加。
3. 对应已经有标签的Agent，可以点击“X”移除该标签。

## 其他操作

操作	说明
挂起	勾选处于“连接正常”状态的Agent，单击“挂机”可以让正在正常运行中的Agent不再传送数据，但保持连接状态。

# 用户指南

操作	说明
唤醒	勾选处于“挂起”状态的Agent，单击“唤醒”可将该Agent转为正常运行状态。
启动	勾选处于“停止”状态的Agent，单击“启动”可将该Agent转为正常运行状态。 对于V4.0.65之前版本安装的Agent，处于“停止”状态的Agent已经断开链路，不能远程启动，只能登录Agent所在服务器后手动启动。
停止	勾选处于“连接正常”或者“挂起”状态的Agent，点击“停止”可停止Agent。
升级	勾选处于“连接正常”状态的Agent，单击“升级”可将当前Agent版本升级至内置Agent中的最新版本。
回退	勾选处于“连接正常”状态的Agent，单击“回退”可将当前Agent版本退回至升级前的Agent版本。
日志	单击“操作”列中的“更多 > 日志”可下载当前Agent的最近1天日志。
诊断	单击“操作”列中的“更多 > 诊断”，查看当前Agent运行状态。
卸载	勾选处于“连接正常”、“停止”和“挂起”状态的Agent，单击“卸载”可远程卸载该Agent。
删除	勾选处于“异常”状态的Agent，单击“删除”可将当前Agent从Agent列表中删除。

## 审计规则配置

### 过滤规则

#### 过滤规则概述

过滤规则的功能是根据某些特定的条件过滤一些操作，系统对这些操作不审计，从而节省设备的磁盘空间，将有限的资源用来存储更有价值的审计数据。过滤规则的过滤方式有三种：

- 按IP过滤：设置某些IP地址为信任的IP地址，系统对这些IP地址发起的SQL请求不审计。
- 按SQL模板过滤：设置SQL模板为可信任的模板，当访问的SQL语句的模板是设置的过滤模板，则不进行审计。
- 按规则过滤：指按照特定的条件进行审计过滤，规则包括客户端信息、服务端信息、SQL请求和SQL结果等条件。

#### 添加按IP过滤规则

按IP过滤则是将新增的客户端IP认为是白名单，不审计该IP下任何信息。新增按IP过滤规则的操作方法如下：

注意

此处添加的不审计的IP默认使用旁路镜像和Agent日志采集方式的全部资产有效。即添加后，资产中有符合上述不审计IP条件的客户端和服务端均不做任何审计，请谨慎添加。

- 在左侧菜单栏选择“规则配置 > 过滤规则”进入过滤规则页面，选择按“按IP过滤”页签。
- 单击“新增”，进入新增IP过滤页面，编辑名称和不审计的IP。详细配置请参见下表。

配置项	说明
名称	必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过64字符。
不审计的IP	格式为“IP/掩码长度”，可配置多组，用“,”隔开。例如：1.2.3.4/32, 10.0.0.0/8。

# 用户指南

3.填写完成后，单击“保存”，即可完成按IP过滤规则的配置。

## 启用按SQL模板过滤规则

按SQL模板过滤是为用户提供常见的可信任的SQL模板，减少误告警，提高告警准确率。系统内置部分常见数据库的常见非违规SQL语句模板，且默认对全部对应的数据库生效。具体操作步骤如下：

- 1.在左侧菜单栏选择“规则配置 > 过滤规则”进入过滤规则页面，选择按“按SQL模板过滤”页签。
- 2.勾选需要启用或禁用SQL模板，单击“启用选中项”。

SQL模板	数据库类型	是否内置模板	是否启用	操作
<input checked="" type="checkbox"/> 按文模板				
<input checked="" type="checkbox"/> SELECT PRIVILEGE FROM SYS.SESSION_PRIVS WHERE PRIVILEGE LIKE :1	Oracle	是	启用	查看模板
<input checked="" type="checkbox"/> SELECT LENGTH(CHR(:1 )) L4, LENGTH(CHR(:2 )) L3, LENGTH(CHR(:3 )) L2, :4 C1 FROM DUAL	Oracle	是	启用	查看模板
<input type="checkbox"/> SELECT BANNER FROM V\$VERSION	Oracle	是	启用	查看模板
<input type="checkbox"/> SELECT * FROM V\$VERSION	Oracle	是	启用	查看模板
<input type="checkbox"/> SELECT GRANTEE, NAME FROM SYS.PLSQLDEV_AUTHORIZATION WHERE GRANTEE IN (:1 ) OR GRANTEE IN (SELECT ROLE FROM SYS.S...	Oracle	是	启用	查看模板
<input type="checkbox"/> SELECT STATE AS 'Status', ROUND(SUM(DURATION),:1 ) AS 'Duration', CONCAT(ROUND(SUM(DURATION)/:2 * :3 ,:4 ), :5 ) AS 'Percentage' FR...	MySQL	是	启用	查看模板
<input type="checkbox"/> SELECT QUERY_ID, SUM(DURATION) AS SUM_DURATION FROM INFORMATION_SCHEMA.PROFILING GROUP BY QUERY_ID	MySQL	是	启用	查看模板
<input type="checkbox"/> SELECT TABLE_NAME, CHECK_OPTION, IS_UPDATABLE, SECURITY_TYPE, DEFINER FROM INFORMATION_SCHEMA.VIEWS WHERE TABLE_...	MySQL	是	启用	查看模板
<input type="checkbox"/> SELECT SCHEMA_NAME, DEFAULT_CHARACTER_SET_NAME, DEFAULT_COLLATION_NAME FROM INFORMATION_SCHEMA.SCHEMATA	MySQL	是	启用	查看模板
<input type="checkbox"/> SELECT TABLE_SCHEMA, TABLE_NAME, COLUMN_NAME, COLUMN_TYPE FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_SCHE...	MySQL	是	启用	查看模板
<input type="checkbox"/> SELECT TABLE_SCHEMA, TABLE_NAME, TABLE_TYPE FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA = :1 ORDER BY TABL...	MySQL	是	启用	查看模板
<input type="checkbox"/> SELECT COUNT(*) FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA = :1 UNION SELECT COUNT(*) FROM INFORMATION_SC...	MySQL	是	启用	查看模板
<input type="checkbox"/> SELECT CAST(HAS_DBACCESS(DTB.NAME) AS BIT) AS (ISACCESSIBLE) FROM MASTER.SYS.DATABASES AS DTB WHERE (DTB.NAME= :1 )	SQL Server	是	启用	查看模板
<input type="checkbox"/> SELECT HAS_DBACCESS(:1 )	SQL Server	是	启用	查看模板
<input type="checkbox"/> SELECT CAST(HAS_DBACCESS(DTB.NAME) AS BIT) AS (ISACCESSIBLE) FROM MASTER.SYS.DATABASES AS DTB WHERE (DTB.NAME=MAST...	SQL Server	是	启用	查看模板
<input type="checkbox"/> PING	MySQL	是	启用	查看模板

3.在弹出的对话框中单击“确认”，即可启用SQL模板过滤规则。

## 按规则过滤

按规则过滤是为用户提供自定义的过滤规则，支持用户按照特定的条件设置过滤规则，规则包括客户端信息、服务端信息、SQL请求和SQL结果等条件。在资产上启用了过滤规则后，符合规则的内容则不会被审计。

添加按规则过滤的规则的操作方法与添加安全规则的方法相同，请参见[规则管理](#)。

添加自定义过滤规则后，需要在资产上启用过滤规则后才能生效，具体操作步骤如下：

- 1.在左侧菜单栏选择“规则配置 > 过滤规则”进入过滤规则页面，选择按“按规则过滤”页签。
- 2.勾选需要启用的规则，单击“启用选中项”。
- 3.在弹出的选择资产对话框中勾选资产，单击“确定”。

## 信任规则

当系统匹配信任规则后，不会再匹配安全规则，不产生任何告警信息。

# 用户指南

## 开启步骤

1. 在左侧菜单栏中选择“规则配置 > 信任规则”进入“信任规则”页面。
2. 单击“新增”，在弹出的新增规则对话框中编辑相关信息。

具体参数可参考下表。

项目	参数	参数说明
基本信息	名称	设置规则名称，必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过64字符。
	描述	规则描述。
	等级	必选项，系统默认等级为中风险。等级可选高风险、中风险和低风险。
	所属规则组	必选项，可选择自定义的规则组，也可以选择系统默认规则组。可通过以下步骤对自定义规则组进行管理： 单击所属规则组右边的“规则组管理”，可新增、修改和删除自定义规则组。
	规则类型	当前支持普通规则和统计规则两类。 <ul style="list-style-type: none"><li>• 普通规则：单条审计记录匹配配置普通规则，会触发普通告警（例如一条select语句，可能会触发一条普通告警）。</li><li>• 统计规则：指定时间内多次匹配配置的统计规则，会触发一条统计告警（例如5分钟内10次select失败，可能会触发一条统计告警）。</li></ul>
	行为	当前支持告警和告警并阻断。 <ul style="list-style-type: none"><li>• 告警：操作命中规则后，仍正常执行，无特殊控制。</li><li>• 告警并阻断：操作命中规则后，该操作对应的数据库连接断开。</li></ul>
客户端	客户端来源	访问业务类型的客户端IP或IP组。可填写多个，以逗号“,”分隔。
	客户端工具	可配多个客户端工具，使用逗号“,”分隔，例如：db2bp.exe, java.exe。
	客户端端口	可配置多个值或区间，多个值间以逗号“,”分隔，例如：10-15, 20, 25, 30-40。
	客户端MAC地址	可填多个值，多个值间以逗号“,”分隔。
	操作系统用户	可以选择字符串或者正则表达式，字符串可填多值，多个值间以逗号“,”分隔。
	主机名	可以选择字符串或者正则表达式，字符串可填多值，多个值间以逗号“,”分隔。
	应用IP	指定规则所匹配的应用IP或IP组，对应审计日志中的关联IP，可填多值，多个值间以逗号“,”分隔。
应用用户名	指定规则所匹配的应用用户或用户组，对应审计日志中的关联账号，可填多值，多个值间以逗号“,”分隔。	
服务端	服务端IP	可填多个值，多个值间以逗号“,”分隔。
	服务端端口	可配置多个值或区间，多个值间以逗号“,”分隔，例如：10-15, 20, 25, 30-40。
	数据库账号	指定规则所匹配的数据库登录用户账号或账号组或者使用正则表达式，可填多值，多个值之间以“,”分隔。
	服务端MAC地址	可填多个值，多个值间以逗号“,”分隔。

# 用户指南

项目	参数	参数说明
	数据库名(SID)	可以选择字符串或者正则表达式，Oracle数据库请输入SID，其他数据库输入数据库名，字符串可填多值，多个值间以逗号“，”分隔。
行为	对象	指定规则匹配的对象组。
	操作类型	指定SQL语句的操作类型，例如：select、update、delete等。
	SQL模板ID	可填项，可填多值，多个值间以逗号“，”分隔。
	SQL关键字	SQL关键字：支持以正则表达式匹配报文。 单击“正则验证”输入报文内容，单击“校验”，验证输入内容与执行结果关键字中的正则表达式是否匹配；单击“增加条件”可添加多个条件。 条件运算逻辑表达式：SQL关键字填写后，此项为必填项。条件间的关系，支持与、或、非、括号运算(&：与； ：或；~：非)，条件使用序号表示，即“1”表示条件1，例如：1&2，则代表有2个SQL关键字条件且两个关键字都要满足才能告警。
	SQL长度	指定SQL语句的长度，取值范围：1B~64KB。
	关联表数	SQL操作涉及表的个数大于等于此值时触发本规则，允许输入最大值为255。
	WHERE子句	是否包含WHERE，支持三个选项： <ul style="list-style-type: none"> <li>不判断</li> <li>有WHERE子句</li> <li>没有WHERE子句</li> </ul> 默认为不判断。WHERE子句用于提取满足指定条件的SQL记录，语法如下： SELECT column_name, column_name FROM table_name WHERE column_name operator value;
结果	执行时长	(选填)单位：秒、毫秒、微秒，取值范围：0到半个小时，SQL执行时长属于此范围，则触发规则。
	影响行数	取值范围：0~999,999,999。SQL操作返回的记录数或受影响的行数属于此范围，则触发规则。
	返回结果集	支持以正则表达式匹配结果集。 单击“正则验证”输入报文内容，单击“校验”，验证输入内容与执行结果关键字中的正则表达式是否匹配；单击“增加条件”可添加多个条件。 条件运算逻辑表达式：SQL关键字填写后，此项为必填项。条件间的关系，支持与、或、非、括号运算(&：与； ：或；~：非)，条件使用序号表示，即“1”表示条件1，例如：1&2，则代表有2个SQL关键字条件且两个关键字都要满足才能告警。
	执行状态	可选三类执行状态： <ul style="list-style-type: none"> <li>全部</li> <li>成功</li> <li>失败</li> </ul> 默认为全部。
	执行结果描述	支持以正则表达式方式匹配。

# 用户指南

项目	参数	参数说明
其他	生效时间	可自定义或者选择时间组。
	每日最大告警数	取值范围：0~99,999，输入0表示没有限制。
	结果集存储策略	设置触发该规则的告警日志的返回结果集存储策略，包含使用资产设置、保存和不保存。

3. 配置完成后，单击“保存”即可完成信任规则的配置。

## 安全规则

### 安全规则概述

安全规则库用来保存已发现的不安全SQL语句的特征信息。系统通过将审计到的SQL语句和安全规则进行匹配从而判断SQL语句中是否包含可疑行为。根据不安全SQL的特征，安全规则分成SQL注入攻击规则、漏洞攻击规则、账号安全规则、数据泄露规则和违规操作规则。

- SQL注入攻击是一种将SQL代码插入或添加到应用（用户）的输入参数中的攻击，之后再将这些参数传递给后台的数据库服务器加以解析并执行，SQL注入规则可以有效的发现此类攻击行为并产生告警。
- 漏洞攻击规则是根据已知的SQL漏洞信息而制定的，漏洞安全规则按照不同的漏洞类型可以分成缓冲区溢出和存储过程滥用。
- 账号安全规则是针对对数据库服务器进行暴力破解和登录失败场景下的安全规则。
- 数据泄露规则根据泄露场景分成拖库攻击、数据库外联、大流量返回、非授权访问，系统可以有效地发现这几种泄露场景并及时通知告警。
- 违规操作规则是针对于应用账号违规操作、运维人员的违规操作、数据库探测和异常语句场景。

系统内置900多条安全规则，覆盖了主流的应用场景，并且在不断地丰富。此外，用户可以自定义安全规则。

### 规则管理

内置规则不可更改，默认为推荐规则，您可以通过单击界面右上角的“推荐”按钮切换到全部规则。

#### 说明

内置规则包含特征规则及其他非特征规则，特征规则不可进行克隆和删除操作，非特征规则可进行克隆操作。

您可以管理自定义的规则，新增自定义安全规则的操作方法如下：

- 1.在菜单栏选择“规则配置 > 安全规则”进入“安全规则”页面，选择“规则管理”页签，单击“新增”。
- 2.在弹出的对话框中填写相关参数，填写完成后单击“保存”即可完成安全规则新增任务。

项目	参数	参数说明
基本信息	名称	设置规则名称，必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过64字符。
	描述	规则描述。
	等级	必选项，系统默认等级为中风险。等级可选高风险、中风险和低风险。
	所属规则组	必选项，可选择自定义的规则组，也可以选择系统默认规则组。可通过以下步骤对自定义规则组进行管理： 单击所属规则组右边的“规则组管理”，可新增、修改和删除自定义规则组。

# 用户指南

项目	参数	参数说明
	规则类型	<p>当前支持普通规则和统计规则两类。</p> <ul style="list-style-type: none"> <li>普通规则：单条审计记录匹配配置普通规则，会触发普通告警（例如一条select语句，可能会触发一条普通告警）。</li> <li>统计规则：指定时间内多次匹配配置统计规则，会触发一条统计告警（例如5分钟内10次select失败，可能会触发一条统计告警）。</li> </ul>
	行为	<p>当前支持告警和告警并阻断。</p> <ul style="list-style-type: none"> <li>告警：操作命中规则后，仍正常执行，无特殊控制。</li> <li>告警并阻断：操作命中规则后，该操作对应的数据库连接断开。</li> </ul>
客户端	客户端来源	访问业务类型的客户端IP或IP组。可填写多个，以逗号“,”分隔。
	客户端工具	可配多个客户端工具，使用逗号“,”分隔，例如：db2bp.exe, java.exe。
	客户端端口	可配置多个值或区间，多个值间以逗号“,”分隔，例如：10-15, 20, 25, 30-40。
	客户端MAC地址	可填多个值，多个值间以逗号“,”分隔。
	操作系统用户	可以选择字符串或者正则表达式，字符串可填多值，多个值间以逗号“,”分隔。
	主机名	可以选择字符串或者正则表达式，字符串可填多值，多个值间以逗号“,”分隔。
	应用IP	指定规则所匹配的应用IP或IP组，对应审计日志中的关联IP，可填多值，多个值间以逗号“,”分隔。
	应用用户名	指定规则所匹配的应用用户或用户组，对应审计日志中的关联账号，可填多值，多个值间以逗号“,”分隔。
服务端	服务端IP	可填多个值，多个值间以逗号“,”分隔。
	服务端端口	可配置多个值或区间，多个值间以逗号“,”分隔，例如：10-15, 20, 25, 30-40。
	数据库账号	指定规则所匹配的数据库登录用户账号或账号组或者使用正则表达式，可填多值，多个值之间以“,”分隔。
	服务端MAC地址	可填多个值，多个值间以逗号“,”分隔。
	数据库名(SID)	可以选择字符串或者正则表达式，Oracle数据库请输入SID，其他数据库输入数据库名，字符串可填多值，多个值间以逗号“,”分隔。
行为	对象	指定规则匹配的对象组。
	操作类型	指定SQL语句的操作类型，例如：select、update、delete等。
	SQL模板ID	可填项，可填多值，多个值间以逗号“,”分隔。
	SQL关键字	<p>SQL关键字：支持以正则表达式匹配报文。</p> <p>单击“正则验证”输入报文内容，单击“校验”，验证输入内容与执行结果关键字中的正则表达式是否匹配；单击“增加条件”可添加多个条件。</p> <p>条件运算逻辑表达式：SQL关键字填写后，此项为必填项。条件间的关系，支持与、或、非、括号运算(&amp;：与； ：或；~：非)，条件使用序号表示，即“1”表示条件1，例如：1&amp;2，则代表有2个SQL关键字条件且两个关键字都要满足才能告警。</p>
	SQL长度	指定SQL语句的长度，取值范围：1B~64KB。
	关联表数	SQL操作涉及表的个数大于等于此值时触发本规则，允许输入最大值为255。

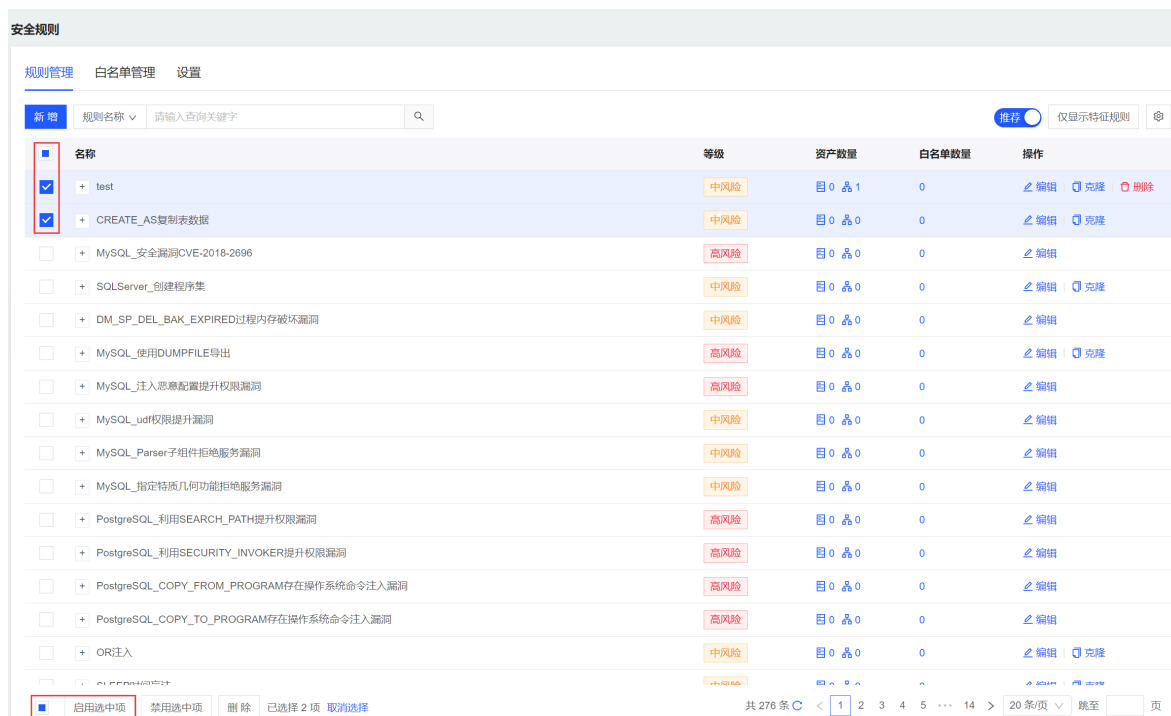
# 用户指南

项目	参数	参数说明
	WHERE子句	<p>是否包含WHERE，支持三个选项：</p> <ul style="list-style-type: none"> <li>• 不判断</li> <li>• 有WHERE子句</li> <li>• 没有WHERE子句</li> </ul> <p>默认为不判断。WHERE子句用于提取满足指定条件的SQL记录，语法如下：            SELECT column_name, column_name            FROM table_name            WHERE column_name operator value;</p>
结果	执行时长	（选填）单位：秒、毫秒、微秒，取值范围：0到半个小时，SQL执行时长属于此范围，则触发规则。
	影响行数	取值范围：0~999,999,999。SQL操作返回的记录数或受影响的行数属于此范围，则触发规则。
	返回结果集	<p>支持以正则表达式匹配结果集。</p> <p>单击“正则验证”输入报文内容，单击“校验”，验证输入内容与执行结果关键字中的正则表达式是否匹配；单击“增加条件”可添加多个条件。</p> <p>条件运算逻辑表达式：SQL关键字填写后，此项为必填项。条件间的关系，支持与、或、非、括号运算(&amp;：与； ：或；~：非)，条件使用序号表示，即“1”表示条件1，例如：1&amp;2，则代表有2个SQL关键字条件且两个关键字都要满足才能告警。</p>
	执行状态	<p>可选三类执行状态：</p> <ul style="list-style-type: none"> <li>• 全部</li> <li>• 成功</li> <li>• 失败</li> </ul> <p>默认为全部。</p>
	执行结果描述	支持以正则表达式方式匹配。
其他	生效时间	可自定义或者选择时间组。
	每日最大告警数	取值范围：0~99,999，输入0表示没有限制。
	结果集存储策略	设置触发该规则的告警日志的返回结果集存储策略，包含使用资产设置、保存和不保存。

## 启用规则

1.在左侧菜单栏选择“规则配置 > 安全规则”进入“安全规则”页面，选择“规则管理”页签，在规则列表中勾选目标规则，单击“启用选中项”。

# 用户指南



2.在弹出对话框中勾选需要启用相关规则资产，单击“确定”，则可将已启用的规则直接应用到选择的资产上。

## 禁用规则

1.在左侧菜单栏选择“规则配置 > 安全规则”进入“安全规则”页面，选择“规则管理”页签，在规则列表中勾选目标规则，单击“禁用选中项”。

2.在弹出对话框中勾选需要禁用相关规则资产，单击“确定”，则可将已禁用的规则直接应用到选择的资产上。

## 白名单管理

已经匹配到安全规则的审计日志如果符合白名单的条件就不会触发告警。条件包含客户端、服务端、基本信息、结果、行为等。

新增白名单并启用的操作方法如下：

- 1.在左侧菜单栏选择“规则配置 > 安全规则”进入“安全规则”页面，选择“白名单管理”页签。
- 2.单击“新增”，进入“新增白名单”页面，编辑相关配置项（配置方法与新增自定义规则的参数配置方法相同，请参考规则管理）。
- 3.配置完成后，单击“保存”即可完成白名单的新增。

## 说明

添加白名单后，需在对应的规则上启用该白名单才会生效。

4.在左侧菜单栏选择“规则配置 > 安全规则”进入“安全规则”页面，选择“规则管理”页签。

5.单击“白名单数量”列的数字。

# 用户指南

名称	等级	资产数量	白名单数量	操作
test	中风险	0 1	0	编辑 克隆 删除
CREATE_AS复制表数据	中风险	0 0	0	编辑 克隆
MySQL_安全漏洞CVE-2018-2696	高风险	0 0	0	编辑

6.在弹出的对话框中，将“状态”列的状态改为“启用”即可启用白名单。

## 说明

如您需要删除白名单规则，则需要将白名单上启用的所有安全规则禁用后才能删除该白名单。

## 设置

此功能可设置规则的优先级状态，启用优先级可自定义规则匹配顺序，匹配上某条规则后，优先级更低的规则就不再匹配。关闭规则的优先级后，每个数据库操作行为可以触发的所有满足条件的安全规则。

## 规则维护

### 规则维护概述

规则维护包括升级内置安全规则和导入/导出自定义安全规则。

### 操作步骤

- 1.在菜单栏选择“规则设置 > 规则维护”进入规则维护页面。
- 2.单击“导入规则”，选择自定义规则文件，即可导入自定义规则；单击“导出规则”即可导出自定义规则至本地。

## 查询审计内容

### 查询审计日志

#### 审计日志概述


天翼云数据库审计通过对双向数据包进行解析、识别以及还原，不仅可以对数据库操作请求进行实时审计，还可对数据库系统返回结果进行完整的还原和审计。包括SQL报文、数据库命令执行时长、执行的结果集、客户端工具、客户端IP地址、服务端端口、数据库账号、对象、执行状态、数据库类型以及报文长度等内容。

#### 搜索审计日志

- 1.在菜单栏选择“查询分析 > 审计日志”进入“审计日志”页面。
- 2.选择“审计日志”页签，设置查询条件（时间范围、报文、资产、数据库账号、客户端IP、服务端IP、操作类型、执行状态等），单击“搜索”即可查询相关审计日志。

## 后续操作

### 导出审计日志

单击界面右上角的  图标，即可将查询结果导出至本地。

### 查看审计日志详情

在查询结果列表中，在“操作”列下单击“详情”，可查看审计日志的详细信息。

## 查询告警日志

### 告警日志概述

当系统根据安全规则捕捉到异常访问时，会根据匹配的安全规则的级别产生相应级别的告警信息。系统支持在告警日志页面查看的所有产生告警的SQL语句的信息和告警等级等相关内容，并可以根据时间、字段和告警等级、规则名称等条件进行筛选。

### 查询告警日志

- 1.在菜单栏选择“查询分析 > 告警日志”进入“告警日志”页面，选择“告警日志”页签，设置查询条件（如时间范围、报文、资产等），单击“搜索”即可查询相关告警日志。
- 2.在告警日志列表中，单击右侧“操作”列中的“详情”可以查看该告警记录的详细信息，包括告警记录基本信息、客户端信息、服务端信息、请求详情、响应详情。
- 3.在告警日志详细页面，单击“统计数据”，可查看客户端、数据库账号等信息。

### 告警分析

- 1.在左侧菜单栏选择“查询分析 > 告警日志”进入“告警日志”页面，选择“告警分析”页签，可设置过滤条件（时间范围、规则名称、资产、数据库账号、客户端IP），查询符合过滤条件的告警信息。
- 2.单击“操作”列下的“详情”，可查看告警统计详情，包含规则详情、告警资产、各资产下的告警趋势、告警来源（维度包含客户端IP和数据库账号）和触发告警的SQL模板。
- 3.在“规则详情”区域单击资产数量链接可编辑已启用该规则的资产，单击白名单数量链接可以编辑该规则上启用的白名单。
- 4.在“告警资产”区域单击“规则启用状态”开关可以变更规则在某资产上的启用状态。
- 5.在“告警来源”区域，单击“操作”列下的“不再告警”。
- 6.在弹出的不再告警对话框中编辑相关信息，单击“确定”。将满足条件的客户端IP添加到信任规则和添加到规则白名单。对于普通规则产生的告警：
  - 选择“添加到白名单”，再单击“确定”。添加为白名单后，系统对于此规则符合选中项的条件的相关操作不再产生告警。
  - 选择“添加到信任规则”，再单击“确定”。添加为信任规则后，对于资产符合信任规则可选属性的将不再发生告警。
- 7.在触发告警的“SQL模板”区域，单击“操作”列下的“不再告警”。
- 8.在弹出的不再告警对话框中编辑相关信息，单击“确定”。将满足条件的SQL模板添加到信任规则和添加到规则白名单。对于普通规则产生的告警：

# 用户指南

- 选择“添加到白名单”，再单击“确定”。添加为白名单后，系统对于此规则符合选中项的条件的相关操作不再产生告警。
- 选择“添加到信任规则”，再单击“确定”。添加为信任规则后，对于资产符合信任规则可选属性的将不再发生告警。

## 查询会话日志

### 会话日志概述

会话（Session）是客户端与数据库服务器之间的不中断的SQL请求和响应序列。一个会话中可能包含一个或多个SQL请求和响应。可以根据会话的状态将其分成在线会话和历史会话。

- 在线会话指的是会话还没有结束，仍然有后续的请求或响应。
- 历史会话指的是已经结束的会话，会话双方已经断开了本次会话的连接。

会话的基本四元素是指客户端IP、客户端端口、服务端IP和服务端端口。

会话的四元素可以定位在同时刻的唯一会话信息。系统支持查看历史会话和在线会话，并支持通过会话信息查看一次会话过程中产生的所有请求或响应日志。

### 查询历史会话

- 1.在菜单栏选择“查询分析 > 会话日志”进入“会话日志”页面，选择“历史会话”页签，设置查询条件（如时间范围、资产等），单击“搜索”即可查询相关历史会话。
- 2.单击“操作”列的“详情”可查看会话详情。

## 查询SQL模板

### SQL模板概述

SQL模板（SQL Template）是去参数化的SQL语句。系统支持将访问数据库系统的SQL语句使用的模板信息提取并存储到磁盘中，用户可以通过Web页面查看SQL模板集合。通常认为应用在访问数据库时使用的模板是固定的，如果出现了新的SQL模板，可以怀疑是否存在异常访问行为。

### 查询SQL模板

- 1.在左侧菜单栏选择“查询分析 > SQL模板”进入“SQL模板”页面，设置查询条件（如时间范围、SQL模板等），单击“搜索”即可查询相关SQL模板。
- 2.在SQL模板列表中单击“详细”可以查看该SQL模板记录的详细信息，包括基本信息、模板、首次发生报文、不审计匹配的报文和数据库信息。其中请求详情中可以查看报文，返回详情可以查看SQL语句的返回信息。

## 报表中心

### 报表预览

在左侧菜单栏选择“报表中心 > 报表预览”进入“报表预览”页面，选择希望查阅的报表类型、资产或者资产组、报表时间范围，即可生成所需的报表文件。

可以直接阅读已生成的报表，也可以单击右上角的“导出”，选择导出格式（HTML、PDF、PNG、WORD、EXCEL和CSV）即可将报表按指定文件格式导出至本地。

# 用户指南

数据库审计内置的报表类型可参照下表

报表类型	报表说明
塞班斯报表	从计划与组织、确保和控制、评估风险、综合情况四个方面，全面分析数据库安全状况。
综合分析报告	从SQL语句执行情况分析、会话连接分析、风险事件分析和SQL性能分析四个角度对数据库态势进行综合分析。
性能分析报表	从性能变化趋势、性能最差的数据库/SID、耗时最久的SQL、性能最差的SQL、执行最多的SQL五个方面对数据库的性能做出分析。
等保参考分析报表	紧密切合当前信息安全技术网络安全等级保护评测要求GB/T 28448-2019（以下简称“等级保护2.0”）的大趋势，针对等级保护2.0里关注的安全审计中的入侵防范、恶意代码监测、安全审计监控等进行针对性的分析和展示。
语句分析类报表	从SQL语句分析、失败语句分析、SQL语句变化趋势、审计趋势分析和执行次数最多SQL模板分析5个维度分析和展示当前语句的信息。
会话分析类报表	包含会话数量变化趋势分析、新增会话分析、并发会话分析和失败会话分析4张报表。
告警分析类报表	从告警变化趋势分析、告警来源分析、告警对象分析、规则命中分析4个维度分析当前告警的情况。
其他报表	主要分为：表分析、客户端工具分析、数据库账号分析、数据库/SID分析、数据库访问来源IP分析、数据库/实例名访问分析6张报表。
自定义报表	用户自定义创建的报表，有关自定义报表的详细信息请参考 <a href="#">自定义报表</a> 。

## 报表订阅

- 1.在左侧菜单栏选择“报表中心 > 报表预览”进入“报表预览”页面，单击右上角的“订阅”。
- 2.在弹出的对话框中，编辑相关信息后，单击“保存”。配置项说明请参见下表。

配置项	说明
任务名称	设置任务名称。必须为中文字符、字母、数字、下划线“_”、点“.”或短横线“-”，长度不超过64字符。
收件人邮箱	报表发送的接收人邮箱，可以设置多个。
报表类型	指定要发送报表类型，可选择内置报表和自定义报表。
报表格式	指定报表发送格式，支持HTML、PDF、PNG和WORD四种格式，默认为“PDF”。
资产	指定要发送报表的资产，默认全部资产。
任务周期	选择任务周期（日报，周报，月报，年报），默认为“每天(日报)”。

# 用户指南

配置项	说明
发送时间	指定报表发送的时间，可选1~23整点。
时间范围	指定报表统计的时间范围，支持选择外送某一时间段的报表数据。（仅在任务周期选择“每天（日报）”时显示，只能选择连续的时间）。

## 说明

您也可以在左侧在菜单栏选择“报表中心 > 报表订阅”进入订阅任务页面，单击“添加”。进行报表订阅

## 查看订阅记录

左侧在菜单栏选择“报表中心 > 报表订阅”进入订阅任务页面，选择“订阅记录”页签查看历史订阅记录。订阅记录是对订阅任务中将报表发送到指定邮箱的记录，主要记录报表的发送时间、收件人、发送结果等。

发送时间	任务名称	报表类型	报表统计时间范围	收件人	报表格式	发送结果	操作
2024-05-08 01:00:31	报表订阅	综合分析报告	2024-05-07 00:00:00 ~ 2024-05-07 23:59:59	[REDACTED]	pdf	成功	下载 重发
2024-05-07 01:00:09	报表订阅	综合分析报告	2024-05-06 00:00:00 ~ 2024-05-06 23:59:59	[REDACTED]	pdf	成功	下载 重发

## 自定义报表

自定义报表，即用户可以自定义报表内容（包括文档架构以及报表数据）。

自定义报表您需要先设置“报表数据”，然后再自定义报表。

## 报表数据管理

报表数据是自定义报表中展示的实际内容，是对审计日志、告警日志、会话日志从不同维度（例如客户端IP、主机名等）进行统计分析。

## 添加报表数据操作步骤

- 1.在左侧菜单栏选择“报表中心 > 自定义报表”进入自定义报表页面，选择“报表数据管理”页签，再单击“添加”。
- 2.进入“添加数据报表”页面，编辑相关信息。
- 3.编辑名称（必须为中文字符、字母、数字、下划线“\_”、点“.”或短横“-”，长度不超过64字符）。
- 4.选择统计维度和统计指标。
- 5.设置筛选条件，单击“添加”。
- 6.在弹出的“添加筛选条件”对话框中设置名称（必须为中文字符、字母、数字、下划线“\_”、点“.”或短横“-”，长度不超过64字符）和条件，单击“保存”。
- 7.在筛选条件文本框中点击∨图标，选择筛选条件。
- 8.配置完成后，单击保存。

# 用户指南

## 添加自定义报表

1. 在左侧菜单栏选择“报表中心 > 自定义报表”进入自定义报表页面，单击“添加”。



2. 进入添加“自定义报表”页面，编辑名称和描述。

配置项	说明
名称	用来标识自定义报表，必须为中文字符、字母、数字、下划线“_”或短横“-”，长度不超过48字符。
描述	自定义报表的描述信息，任意字符类型，长度不超过64字符。

3. 单击“一级标题”，在页面右侧编辑一级标题（必须为中文字符、字母、数字、下划线“\_”或短横“-”，长度不超过48字符）。

4. 单击“二级标题”，在页面右侧编辑二级标题（必须为中文字符、字母、数字、下划线“\_”或短横“-”，长度不超过48字符）。

5. 单击“正文”，在页面右侧输入正文内容（任意字符类型，长度不超过1000字符，系统提供了格式编辑工具，可使用格式编辑工具丰富正文格式）。

6. 单击“分析对象与范围”，在页面右侧选择显示内容，当前可选：全部、仅显示对象或仅显示范围。

7. 单击“图标”，在页面右侧选择“报表数据”、“图表类型”和“图标标题”，并且设置“显示指标”或“显示维度”。

8. 单击“保存”完成自定义报表的设置。

## 设置告警通知

### 邮件方式通知告警

1. 在菜单栏选择“通知外送 > 告警通知”进入“告警通知”页面，选择“邮件”页签。

2. 单击“编辑”，在弹出的“邮箱配置”对话框中编辑相关信息。具体参数说明可参考下表。

配置项	说明
SMTP服务器	SMTP服务器的IP或域名。
SMTP服务器端口	SMTP服务器所用端口。
发件人	发件人的邮箱。
SMTP验证	邮箱是否开启SMTP验证。

# 用户指南

配置项	说明
用户名	邮箱的用户名。
密码	与邮箱用户名对应的用户密码。
是否加密	邮箱是否进行加密。
编码	服务器支持的编码方式，主要为：UTF-8、GBK。以上SMTP服务器相关配置与服务器端设置保持一致即可。
实时告警模板	发送实时告警信息的模板，可修改默认模板，具体字段请依据界面中的“填写说明”编辑。
聚合告警模板	发送聚合告警信息的模板，可修改默认模板，具体字段请依据界面中的“填写说明”编辑。
统计告警模板	发送统计告警信息的模板，可修改默认模板，具体字段请依据界面中的“填写说明”编辑。
系统告警模板	发送系统告警信息的模板，可修改默认模板，具体字段请依据界面中的“填写说明”编辑。

3. 配置邮件发送接口后，可对需要通过邮件发送接口发送通知的资产配置发送方式。单击“添加”。



4. 在弹出的对话框中编辑相关信息，编辑完成后单击“保存”。具体参数说明可参考下表。

配置项	说明
资产	选择要发送告警信息的资产，可选择多项。
接收者	接收告警信息的邮箱，可设置多个邮箱。
告警等级	选择要发送的告警信息的告警等级。
通知周期	同一个规则在通知周期内多次触发告警时只通知第一次触发的告警。 取值范围：0~86400，单位为秒。 0表示发送全部告警。如果设置为0，聚合通知功能将无法开启。
聚合通知	开启聚合通知功能后，系统会在通知周期结束后发送一条聚合告警信息。 聚合消息示例：在过去*秒，总计触发*条告警（“*”为具体数值）。
告警统计	选择是否开启发送告警统计信息的功能。
发送时间	每天在设定的时间点发送前一天的告警统计信息。

## 短信方式通知告警

1. 在菜单栏选择“通知外送 > 告警通知”进入“告警通知”页面，选择“短信”页签。
2. 单击“添加”，在弹出的“新增告警通知接收配置”对话框中编辑相关信息。具体参数说明可参考下表。

配置项	说明
资产	选择需要对外发送信息的资产。
接受者	选择需要接受信息的相关人员。
告警等级	可选：低风险、中风险、高风险。
通知周期	同一个规则在通知周期内多次触发时只通知第一次触发的告警。 取值范围：0~86400，单位为秒。设为0时发送全部告警。
告警统计	选择是否打开告警统计。
发送时间	选择发送告警的时间。

## 其他操作

### 用户管理

用户管理主要是指对用户权限及用户认证等进行管理。包括用户管理、远程认证配置、角色管理、用户安全配置以及授权数据库。

### 角色管理

角色可以看作是具有相同权限的用户的集合。系统将权限分配给角色，然后为用户指定角色。配置用户时通过设定用户所属角色，限制用户的操作权限范围。用户的操作权限包括菜单显示和功能权限。只有赋予操作权限，用户才能进行相应的操作。

### 创建角色操作步骤

- 1.在菜单栏选择“系统管理 > 用户管理”，选择“角色管理”页签，进入“角色管理”页面。
- 2.单击“添加”进入“新增角色”页面，编辑名称（必须为中文字符、字母、数字、下划线“\_”、点“.”或短横“-”，长度不超过64字符），选择权限后，单击“保存”。

### 用户管理

添加角色后即可增加该角色的用户。系统内置了以下四个默认用户：

说明

admin初始密码请联系天翼云技术支持获取。

- admin：超级管理员，具备系统所有权限。系统只有一个超级管理员。
- security：具备安全管理员权限，可配置数据库与规则、查看各类告警报告、管理安全员。
- system：具备系统管理员权限，进行系统权限的配置和维护。
- audit：具备审计管理员权限，查看其他用户的操作日志、管理审计员。

### 添加用户操作步骤

- 1.在左侧菜单栏选择“系统管理 > 用户管理”进入“用户管理”页面，单击“添加用户”。

# 用户指南

2.进入添加用户页面，编辑相关信息，完成后单击“保存”。

配置项	说明
用户名	必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，最大长度64字符。
启用	单击“启用”后的开关，设置添加用户后是否立即启用用户。
角色	指定用户角色，包括内置角色和用户自定义角色，必填。
密码/确认密码	创建并确认新建用户的登录密码。密码长度6~64位，当启用强密码功能后需符合密码强度要求。修改密码时新旧密码不能相同。
手机号	设置用户的手机号。
邮箱	设置用户的邮件地址。
认证方式	用户登录系统时的认证方式。
登录IP/MAC限制	对用户登录系统时使用的IP/MAC进行限制。包括不限制、黑名单和白名单三种模式。
登录时间限制	限制用户登录系统的时间。

## 辅助功能

### IP别名

为方便对网络进行识别，可对网段或IP地址设置别名。

操作步骤如下：

- 1.在左侧菜单栏选择“系统管理 > 辅助功能”进入“辅助功能”页面，选择“IP别名”页签，单击“新增”。
- 2.弹出“新增IP别名”对话框，编辑相关信息，单击“保存”。

配置项	说明
名称	必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过64字符。
IP/网络	格式1：输入多个IP地址，用英文逗号分隔。格式2：IP范围，仅支持IPv4格式，例如：10.1.1.10-10.1.1.20。

### 数据脱敏

数据脱敏可以将银行卡号、手机号码、身份证号码等敏感数据进行脱敏处理。

操作步骤如下：

- 1.在左侧菜单栏选择“系统管理 > 辅助功能”进入“辅助功能”页面，选择“数据脱敏”页签，单击“新增”。
- 2.弹出“数据脱敏”对话框，编辑相关信息，单击“保存”。

# 用户指南

参数	说明
名称	必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过64字符。
状态	启用或禁用该规则。
正则表达式	正则表达式用于检索、替换符合特定模式（规则）的文本，例如： <code>([^d]</code>
开始位置	开始替换的字符位置。
截取长度	数据串中被替换的字符长度。

## 系统告警

天翼云数据库审计支持系统自检功能，当出现系统资源使用率过高、长时间没有审计日志等情况时，会自动产生一条告警信息，方便用户快速定位问题。

### 修改告警系统配置

- 1.在左侧菜单栏选择“系统管理 > 系统告警”进入“系统告警”页面，选择“告警查询”页签，单击“修改”。
- 2.在弹出“修改告警系统配置”对话框中，编辑相关信息，单击“确定”。

参数	参数说明
日志保留天数	设置日志保留天数，取值范围：7~365天。
CPU阈值	设置CPU告警阈值，取值范围：1~100%。
内存阈值	设置内存告警阈值，取值范围：1~100%。
磁盘阈值	设置磁盘告警阈值，取值范围：1~100%。
网口流量阈值	设置网口流量阈值，取值范围：1~100%。
无日志告警	默认关闭。开启后可配置无日志告警阈值。
无日志阈值	设置无日志告警阈值，取值范围：6~360天。

### 查询告警日志


设置时间范围、告警类型、告警级别，单击“搜索”即可查询相关告警日志信息。



## 操作日志

系统可记录所有用户的操作。审计员或超级管理员可以通过查看操作日志来审计其他用户的操作。

### 查询审计日志

在左侧菜单栏选择“系统管理 > 操作日志”进入操作日志页面，可根据时间范围、用户、来源IP、操作名称、操作类型、操作内容和操作结果来搜索相应操作日志。点击  图标可导出操作日志。

### 日志外送

操作日志外送通知是指将操作日志发送至指定的接收者，支持SYSLOG和KAFKA两种方式。

添加操作日志外送任务的操作方法如下：

- 1.在左侧菜单栏选择“系统管理 > 操作日志”进入“操作”页面，选择“日志查询”页签，单击“添加”。
- 2.在弹出添加操作日志外送任务对话框，编辑相关信息，单击“保存”。

### 添加操作日志外送任务

×

操作类型： 获取信息  状态变更

外送方式： SYSLOG  KAFKA

外送接口：

如没有所需外送SYSLOG接口，[前往配置](#)

保存

取消

## 日志外发

数据库审计使用Syslog外发日志，主要是为了集中管理多源日志、利用通用协议兼容异构系统，并实时传输加密日志至独立平台，确保安全存储、防篡改，同时支持快速告警和深度分析，满足合规与溯源需求。

### 创建Syslog日志外送任务

- 1.登录数据库审计实例
- 2.在左侧导航栏选择“通知发送 > 日志外送”，进入“日志外送”页面。
- 3.在日志接口管理下单击“新增”按钮，在右侧滑出的对话框中填写日志外送接口的相关配置。

## 新增日志外送接口



\* 名称:

\* 服务器地址:

\* 端口:

\* 发送协议:

\* 是否tls加密:  加密  不加密

\* 是否发送消息头:

\* 内容协议格式:

报文默认主机名:

报文默认应用名:

程序模块编码:

严重等级:

审计日志模板: 

```
{ "logType": "${logType}", "startTime": "${dateTimeFmt}", "assetName": "${assetName}", "sqlLen": "${sqlLen}", "clientUserName": "${clientUser}", "srcHostName": "${hostName}", "dvcAction": "${dvcAction}", "destMacAddress": "${dmacFmt}"
```

[填写说明](#)

告警日志模板: 

```
{ "alarmId": "${alarmId}", "assetName": "${assetName}", "logType": "${logType}", "startTime": "${dateTimeFmt}", "sqlLen": "${sqlLen}", "clientUserName": "${clientUser}", "srcHostName": "${hostName}", "destMacAddress": "${dmacFmt}", "dvcAction": "${dvcAction}"
```

[填写说明](#)

会话日志模板: 

```
{ "logType": "${logType}", "assetName": "${assetName}", "clientUserName": "${clientUser}", "encodeType": "${encode}", "srcHostName": "${hostName}", "destMacAddress": "${dmacFmt}", "databaseName": "${dbName}", "srcMacAddress": "${smacFmt}"
```

[填写说明](#)

4.填写完成后，单击保存。

5.在日志外送任务管理下单击“新增”按钮，在弹出的窗口中配置需要外发的资产和外发接口。

新增日志外送任务

X

\* 资产: 请选择资产

\* 日志类型: 审计日志(原始) X

\* 外送接口: 请选择外送接口

外送选项:  过滤不完整的日志 [?](#)

取消

确定

6.单击“确定”即可完成日志外送任务配置。

## 审计云上自建数据库

### 背景

为保护数据库的数据安全，防范各种攻击事件，满足国家等保合规要求，您都需要对您的数据库进行保护。

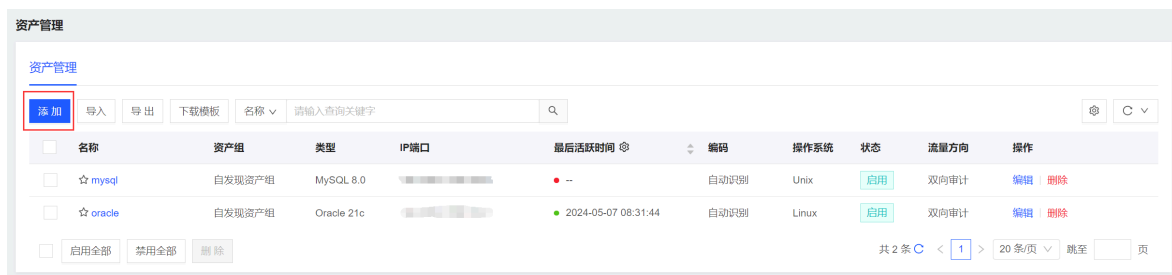
天翼云数据库审计，提供旁路模式数据库安全审计服务功能，通过实时记录用户访问数据库行为，形成细粒度的审计报告，对风险行为和攻击行为进行实时告警。同时，数据库安全审计可以生成满足数据安全标准（例如Sarbanes-Oxley）的合规报告，对数据库的内部违规和不正当操作进行定位追责，保障数据资产安全。

### 步骤一：购买数据库审计实例

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

### 步骤二：添加数据库资产

1.在左侧菜单栏选择“资产 > 资产管理”进入“资产管理”页面，选择“资产管理”页签，单击“添加”。



2.在弹出的“添加资产”窗口编辑相关信息。参数填写规则可参见下表。

参数	参数说明
保存时启用推荐的规则	勾选此选项，则保存时添加的资产会使用系统推荐的规则；不勾选此选项，保存时添加的资产不会使用系统推荐的规则。
类型	选择“关系型”数据库，此处以MySQL 5.7版本举例。
资产组	设置资产所属的资产组。
名称	填写资产的名称，必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过64字符。
操作系统	此处以“Linux”系统举例。
IP端口	设置资产所在主机的IP及端口号。

3.添加完成后，单击“保存”即可将数据库纳入资产中。

### 步骤三：添加Agent

1.在左侧菜单栏选择“系统管理 > Agent管理”进入“Agent管理”页面，选择“Agent安装”页签，点击下载对应版本的Agent安装包。

## 注意

- 下载的Agent默认会将流量转发给当前的天翼云数据库审计实例。如需转发到其他天翼云数据库审计实例，请在解压后的Agent路径下agent.ini配置文件中找到serviceIp选项进行地址修改。
- 无论是Linux版本安装包、AIX版本安装包还是Windows版本安装包，文件夹中均有“ReadMe”文档，文档内包含使用说明、文件说明、注意事项、运行环境说明、配置文件说明。在安装前请仔细阅读该文档并严格按照要求进行操作。

2.安装包下载完之后，将Agent安装包上传到Linux服务器指定目录。

## 说明

- 禁止直接运行二进制文件。
- 解压目录不能出现空格。
- 每次更换运行或解压目录需重新运行安装脚本。
- Linux环境需以root用户运行脚本，指定解释器bash，或不指定解释器直接运行。

```
[root@oracle test_1]# ll
总用量 8276
-rw-r--r-- 1 root root 8472119 6月  2 16:37 dbagent_linux_V2.29.tar.gz
```

3.使用 `tar -xf dbAgent_V2.28.tar.gz`命令解压Agent安装包，进入Agent安装目录。

4.在安装目录执行 `./install.sh`命令即可安装Agent程序。

## 审计云数据库

### 背景说明

在云计算环境中，部分云上的关系型数据库服务（RDS）所依托的宿主机基于一系列安全策略与架构设计的考量，不允许数据库审计相关的产品部署Agent程序。

天翼云关系数据库MySQL版支持通过免Agent安装的方式进行数据库审计。

其他不支持免Agent安装的云上数据库，您可以通过在使用云上数据库的应用端云主机安装数据库审计Agent的方式来获取数据库流量，以便您对数据库进行审计。

### 通过免Agent的方式审计天翼云关系数据库MySQL版

#### 注意

通过免Agent方式审计RDS数据库之前，首先需要开启SQL审计日志功能，具体操作请参考：[关系型数据库MySQL版-开启SQL审计日志](#)。（II类资源池中仅支持一类节点的资源池）

- 1.登录数据库审计实例。
- 2.在左侧导航栏选择“系统管理 > 系统配置 > 日志采集方式”，确认是否已开始天翼云RDS日志采集。

## 许可证 日志采集方式

**日志采集方式** 建议关闭不必要的日志采集方式，可减少资源的浪费

接收镜像流量：启用

接收Agent流量：启用

天翼云RDS日志：启用

修改

3.确认完成后，需要在“资产 > 资产管理”下添加对应的RDS数据库资产，类型需选择“天翼云RDS > Teledb-MySQL > 所有版本”，实例ID请参考关系数据库MySQL版控制台“实例名称/实例ID”。

注意

实例ID项只能填实例ID，切勿填写自定义的RDS实例名称。

\* 类型：天翼云RDS / Teledb-MySQL / 所有版本

\* 实例ID：

资产组：请选择资产所属的资产组

管理

\* 名称：请输入资产名称

\* IP端口：

3306

更多配置

## 最佳实践

4. 剩余配置项完成后，单击“保存”即可纳管RDS数据库并审计，需要配置审计规则请参考：[审计规则配置](#)章节。

### 通过Agent方式审计云上数据库

1. 登录数据库审计实例。
2. 在左侧导航栏选择“系统管理 > Agent管理 > Agent安装”，进入“Agent安装”页面。
3. 选择SSH远程安装Agent，在弹出的对话框中的填写RDS数据库所在应用端服务器的IP。

#### 说明

若您有多个应用端服务器对接至同一数据库，则使用“增加”功能添加多个应用端服务器IP。

此处对接Agent的应用端服务器IP数量没有限制。

### SSH远程安装Agent ×

审计服务器IP:

安装Agent的服务器:  表单填写

服务器公网IP  root密码  👁

+ 增加

4. 填写完成后安装Agent服务，后续操作可参考：[Agent安装](#)章节。

5. 在您安装完后，需要在“资产 > 资产管理”下添加对应的RDS数据库资产，IP和端口为云上数据库的IP和数据库实际使用的端口。具体操作请参见：[添加资产](#)章节。

#### 说明

此处对接的IP端口个数受您的数据库审计版本影响：

标准版：支持3个数据库实例（即最多添加3个IP+端口组合）

高级版：支持6个数据库实例（即最多添加6个IP+端口组合）

企业版：支持12个数据库实例（即最多添加12个IP+端口组合）

旗舰版：支持30个数据库实例（即最多添加30个IP+端口组合）

## 最佳实践

\* 类型: 关系型 / Oracle / 21c

资产组: 请选择资产所属的资产组 管理

\* 名称: 请输入资产名称

\* 操作系统: Linux

\* IP端口:  1521

+ 增加IP与端口

更多配置



6.上述操作完成后,就完成了对云上数据库的数据获取,后续可参考[规则配置](#)章节完成后续配置进行审计。

## 产品咨询

### 数据库审计是什么？

数据库审计产品是专业的数据库应用安全防护产品，帮助用户应对网站运营中的安全风险，为数据库应用提供全方位的防护，提供覆盖数据库使用全生命周期的安全审计解决方案。

### 数据库审计日志能否满足等保合规需求？

数据库审计系统提供日志留存180天，满足等保合规要求。

### 数据库审计支持哪些数据库？

数据库类型	支持的版本
Oracle	21c、19c、18c、12c、11g、10g、9i、8i
MySQL	8.0、5.7、5.6、5.5、5.1、5.0、4.1、4.0
SQL Server	2019、2017、2016、2014、2012、2008、2005、2000
SyBase ASE	12.5、11.9
DB2	v11.5、v11.1、v10.5、v9.7、v9.5、v8.2、v8.1、v8.0
infomix	IDS9
Oscar	5.7、5.5
达梦数据库（DM）	DM8、DM7
Cache	2021、2016、2010
Postgre SQL	14、13、12、11、10、9
Teradata	所有版本
人大金仓（Kingbase）	V8、V7、V6
Gbase（南大通用）	8.8s、8.5a
mariaDB	10.3、10.2、10.1、10.0、5.5、5.3、5.2、5.1
Hana	2.0、1.0
GaussDB	300、200、100
librA	6
K-DB	11
SyBase IQ	15.4
TiDB	4.X、5.X
Vertica	11、10、9、8、7
Ocean Base	4.X、3.X、2.X
PolarDB	兼容oracle语法版本、PostgreSQL版本、MySQL版本

## 常见问题

数据库类型	支持的版本
PolarDB-X	2.0/MySQL5.7、1.0/MySQL5、1.0/MySQL8
AnalyticDB	PostgreSQL版本、MySQL版本
TBase	v2
HighGo (瀚高)	6.0
TDSQL-C MySQL	8.0、5.7
TDSQL-C PostgreSQL	14、10
Percona-MySQL	8.0、5.7、5.6
Vastbase	2.X
Clickhouse-MySQL	所有版本
teleDB-MySQL	所有版本
teleDB-PostgreSQL	所有版本
MongoDB	5.X、4.X、3.X、2.X
Hbase (Protobuf)	所有版本
Hbase (Thrift)	Thrift1、Thrift2
Hive	3.X、2.X、1.X
Redis	所有版本
Elasticsearch	所有版本
Cassandra	3.X
HDFS	所有版本
Impala	3.X
GraphBase	6
Greenplum	5、6
Spark SQL(Thrift)	2.X、1.X
Spark SQL(RESTful)	2.X、1.X
SSDB	所有版本
ArangoDB	3.4.9
Neo4j	4.2.0
OrientDB	3.1.6
Percona-MongoDB	5.X、4.X
Hbase (Protobuf)	所有版本
Hbase (Thrift)	Thrift1、Thrift2
Hive	3.X、2.X、1.X

## 常见问题

### 数据库审计有哪些版本？

版本	支持的数据库实例个数	资源需求	性能参数
标准版	3个	CPU: 4U内存: 16GB硬盘: 512GB	吞吐量峰值: 3,000条/秒 入库速率值: 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。
高级版	6个	CPU: 8U内存: 32GB硬盘: 1TB	吞吐量峰值: 6,000条/秒 入库速率值: 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。
企业版	12个	CPU: 16U内存: 64GB硬盘: 2TB	吞吐量峰值: 12,000条/秒 入库速率值: 1440万条/小时 10亿条在线SQL语句存储。 200亿条归档SQL语句存储。
旗舰版	30个	CPU: 16U内存: 64GB硬盘: 5TB	吞吐量峰值: 35,000条/秒 入库速率值: 1440万条/小时 16亿条在线SQL语句存储。 200亿条归档SQL语句存储。

数据库审计可以对天翼云上的哪些数据库提供保护？

数据库审计支持纳管天翼云的云上数据库：Teledb-MySQL和Teledb-PostgreSQL。

为什么购买数据库审计实例后，不能第一时间在控制台看见创建中的实例？

购买数据库审计实例时，由于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。购买数据库安全服务实例后，建议您刷新页面后，再查看创建中的实例。

数据库审计上传日志是通过公网的带宽还是内网的带宽？

数据库审计上传日志是通过内网的带宽，不占用公网资源。

数据库审计到期后不续费会影响业务吗？

购买的数据库审计到期后，如果未续费，您将不能使用数据库审计，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审计。

## 购买问题

### 每个资源池最多支持购买几个数据库审计实例？

根据你购买的数据库审计版本而决定。

- 标准版: 3个
- 高级版: 6个
- 企业版: 12个
- 旗舰版: 30个

## 常见问题

### 如何为数据库审计实例续费？

在数据库审计实例到期前，用户可以通过续费操作继续使用数据库审计。

#### 续费步骤

1. 登录天翼云控制台。
2. 选择“安全 > 数据库审计”，进入数据库审计实例管理页面。
3. 在待续费的数据库审计实例的“操作”列，选择“更多 > 续订”。
4. 在续费页选择续订时长。
5. 确认订单无误并阅读《天翼云数据库审计产品服务协议》后，勾选“我已阅读并同意《天翼云数据库审计产品服务协议》”，单击“提交订单”。
6. 在后续操作中完成支付即可正常续费数据库审计。

### 如何退订数据库审计实例？

1. 登录天翼云控制台。
2. 选择“安全 > 数据库审计”，进入数据库审计实例管理页面。
3. 在待退订的数据库审计实例的“操作”列，选择“更多 > 退订”。
4. 在弹出的对话框中单击“确定”。
5. 在“退订申请”页面中选择退订原因和确认后，单击“退订”，即完成数据库审计实例的退订。

## 功能类问题

### 数据库审计会影响业务的使用吗？

不影响。数据库审计是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。

### 数据库审计支持多账号一起使用吗？

数据库审计不支持多个账号共享使用。

### 数据库审计可以应用于哪些场景？

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

### 数据库审计支持哪些数据库类型？

数据库类型	支持的版本
Oracle	21c、19c、18c、12c、11g、10g、9i、8i
MySQL	8.0、5.7、5.6、5.5、5.1、5.0、4.1、4.0

## 常见问题

数据库类型	支持的版本
SQL Server	2019、2017、2016、2014、2012、2008、2005、2000
SyBase ASE	12.5、11.9
DB2	v11.5、v11.1、v10.5、v9.7、v9.5、v8.2、v8.1、v8.0
infomix	IDS9
Oscar	5.7、5.5
达梦数据库 (DM)	DM8、DM7
Cache	2021、2016、2010
Postgre SQL	14、13、12、11、10、9
Teradata	所有版本
人大金仓 (Kingbase)	V8、V7、V6
Gbase (南大通用)	8.8s、8.5a
mariaDB	10.3、10.2、10.1、10.0、5.5、5.3、5.2、5.1
Hana	2.0、1.0
GaussDB	300、200、100
librA	6
K-DB	11
SyBase IQ	15.4
TiDB	4.X、5.X
Vertica	11、10、9、8、7
Ocean Base	4.X、3.X、2.X
PolarDB	兼容oracle语法版本、PostgreSQL版本、MySQL版本
PolarDB-X	2.0/MySQL5.7、1.0/MySQL5、1.0/MySQL8
AnalyticDB	PostgreSQL版本、MySQL版本
TBase	v2
HighGo (瀚高)	6.0
TDSQL-C MySQL	8.0、5.7
TDSQL-C PostgreSQL	14、10
Percona-MySQL	8.0、5.7、5.6
Vastbase	2.X
Clickhouse-MySQL	所有版本
teleDB-MySQL	所有版本
teleDB-PostgreSQL	所有版本
MongoDB	5.X、4.X、3.X、2.X

## 常见问题

数据库类型	支持的版本
Hbase (Protobuf)	所有版本
Hbase (Thrift)	Thrift1、Thrift2
Hive	3.X、2.X、1.X
Redis	所有版本
Elasticsearch	所有版本
Cassandra	3.X
HDFS	所有版本
Impala	3.X
GraphBase	6
Greenplum	5、6
Spark SQL(Thrift)	2.X、1.X
Spark SQL(RESTful)	2.X、1.X
SSDB	所有版本
ArangoDB	3.4.9
Neo4j	4.2.0
OrientDB	3.1.6
Percona-MongoDB	5.X、4.X
Hbase (Protobuf)	所有版本
Hbase (Thrift)	Thrift1、Thrift2
Hive	3.X、2.X、1.X

数据库审计的Agent支持部署在哪些操作系统上？

操作系统	操作系统位数	支持版本
Ubuntu	X64	14.04、16.04、18.04
Debian	X64	7.6、8.7、9.5、10.11、11.2
CentOS	X64	5.11、6.0、7.4、7.6、8
RedHat	X64	6.5、7.0、7.5
SUSE	X64	11SP4、12SP4
Solaris X86	X86	5.10、5.11
Solaris Sparc	X64	5.10
AIX	-	5.3、6.1、7.1
Windows	X64	Windows7、Windows10
Windows	X86	Windows7

## 常见问题

操作系统	操作系统位数	支持版本
Windows Server	X64	2003、2008、2012、2016、2022
EulerOS（欧拉）	x64	EulerOS 2.0 SP9
银河麒麟	aarch64	v10服务器版
兆芯cpu+银河麒麟系统	x64	v10服务器版
兆芯cpu+中标麒麟系统	x64	7
兆芯cpu+统信UOS	x86	v20
海光cpu+统信UOS	x64	v20
鲲鹏cpu+统信UOS	aarch64	v20

数据库审计支持双向审计吗？

数据库审计支持双向审计。双向审计是对数据库的请求和响应都进行审计。

数据库审计默认使用双向审计。

数据库审计支持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。

数据库审计的审计数据可以保存多久？

数据库审计支持将在线和归档的审计数据至少保存180天的功能。根据实际的磁盘大小，会优先删除存储日期较早的审计数据。

若您需要更多的磁盘空间，可选择买更高级的数据库审计实例规格或者购买磁盘存储容量。

数据库审计发生异常，多长时间用户可以收到告警通知？

在数据库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。

在业务侧使用中间件会影响数据库审计功能吗？

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。

数据库审计能否对第三方工具执行的SQL语句进行捕捉？

可以。数据库审计审计的数据是Agent接入的全量日志和流量数据，与工具无关。

数据库审计是否支持云下部署？

不支持。数据库审计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。

## Agent问题

### 数据库审计的Agent提供哪些功能？

数据库审计的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

### 数据库审计的Agent可以安装在哪些Windows操作系统上？

操作系统	操作系统位数	支持版本
Windows	X64	Windows7、Windows10
Windows	X86	Windows7
Windows Server	X64	2003、2008、2012、2016、2022

### 数据库审计的Agent可以安装在哪些Linux操作系统上？

操作系统	操作系统位数	支持版本
Ubuntu	X64	14.04、16.04、18.04、20.04
Debian	X64	7.6、8.7、9.5、10.11、11.2
CentOS	X64	5.11、6.0、7.4、7.6、8
RedHat	X64	6.5、7.0、7.5
SUSE	X64	11SP4、12SP4
Solaris X86	X86	5.10、5.11
Solaris Sparc	X64	5.10
AIX	-	5.3、6.1、7.1
EulerOS（欧拉）	x64	EulerOS 2.0 SP9
银河麒麟	aarch64	v10服务器版
兆芯cpu+银河麒麟系统	x64	v10服务器版
兆芯cpu+中标麒麟系统	x64	7
兆芯cpu+统信UOS	x86	v20
海光cpu+统信UOS	x64	v20
鲲鹏cpu+统信UOS	aarch64	v20

#### （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
```

## 使用类问题

### 如何配置数据库审计？

步骤顺序	操作说明
步骤一：添加资产	添加系统需要审计的数据库，详情请参见 <a href="#">资产</a> 。
步骤二：安装Agent	安装Agent进行数据库审计，详情请参见 <a href="#">Agent管理</a> 。
步骤三：配置规则	配置数据库的安全规则和过滤规则，详情请参见 <a href="#">规则配置</a> 。
步骤四：订阅报表的设置告警通知	便于管理员及时了解数据库的运行状态及安全告警信息，详情请参见 <a href="#">报表订阅</a> 和 <a href="#">告警通知</a> 。

### 如何关闭数据库SSL？

以MySQL数据库自带的客户端为例说明，操作步骤如下：

1. 使用MySQL数据库自带的客户端，以root用户登录MySQL数据库。
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:Notinuse
```

- 如果界面回显类似以下信息，说明MySQL数据库已开启SSL，请执行第3步。

```
SSL:CipherinuseisXXX-XXX-XXXXXX-XXX
```

3. 以SSL模式登录MySQL数据库。

- a. 执行以下命令，退出MySQL数据库。

```
exit
```

- b. 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。

- c. 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:Notinuse
```

## 常见问题

### 数据库审计如何对日志进行快速检索？

日志查询分析菜单 > 日志检索功能，提供根据时间范围、资产、类型等条件对审计日志进行检索，同时支持关键词搜索和高级（自定义过滤逻辑条件）查询，并保存常用历史查询信息，便于后续对所需日志进行快速检索。

### 数据库审计如何配置告警规则？

规则配置菜单 > 安全规则，通过启用产品内置的规则或用户自定义新增规则，配置告警的触发条件（敏感库表字段、行为等）和风险等级，根据相应的条件触发告警日志。可以不断优化告警配置，提升告警准确性。

### 数据库审计如何进行查看报表分析？

报表中心模块 > 报表预览，选择对应的报表及资产、时间范围进行报表生成。

### 数据库审计采集日志需要做哪些操作？

进入数据库审计后，您需要先配置审计资产，在应用/数据库服务器上部署agent产生审计日志，以及启用告警规则，对可疑行为进行风险告警。可在平台中检索审计到的审计日志和告警日志。

## 故障类

### 数据库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。关闭数据库SSL操作请参考：[关闭数据库SSL](#)。
- 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。

### 数据库审计告警邮件异常

故障现象：

- 数据库审计实例功能正常，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：

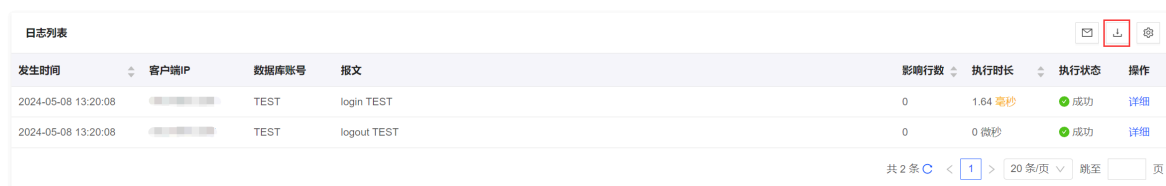
- 新增数据库审计实例，分担当前数据审计流量或者更改审计规则，优化缩小审计范围。
- 制定自动小时备份任务，避免数据量存储磁盘达到85%触发日志清理机制。

## 日志类问题

### 备份的数据库审计日志可以下载到本地吗？

可以。

您可在对应的日志页面，在“日志列表”的上方单击下载按钮下载日志。



发生时间	客户端IP	数据库账号	报文	影响行数	执行时长	执行状态	操作
2024-05-08 13:20:08		TEST	login TEST	0	1.64 毫秒	成功	详细
2024-05-08 13:20:08		TEST	logout TEST	0	0 毫秒	成功	详细

### 数据库审计的操作日志是否可以迁移？

不支持。数据审计当前不支持迁移数据库操作日志。

### 数据库审计日志可以保存多久？

数据库审计支持将在线和归档的审计日志至少保存180天的功能。根据实际的磁盘大小，会优先删除存储日期较早的审计日志。

若您需要更多的磁盘空间，可选择买更高级的数据库审计实例规格或者购买磁盘存储容量。

### 如何查看数据库审计的用户操作日志？

- 1.在菜单栏选择“查询分析 > 审计日志”进入“审计日志”页面。
- 2.选择“审计日志”页签，设置查询条件（时间范围、报文、资产、数据库账号、客户端IP、服务端IP、操作类型、执行状态等），单击“搜索”即可查询审计日志。

### 数据库审计的日志处理机制是什么？

数据库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。

### 数据库报表查询字段大小写是否敏感？

SQL语句关键字、数据库用户名称、规则名称对大小写敏感，其余例如：操作类型对大小写不敏感。请您在输入的时候注意区分大小写。