数据库审计

用户指南

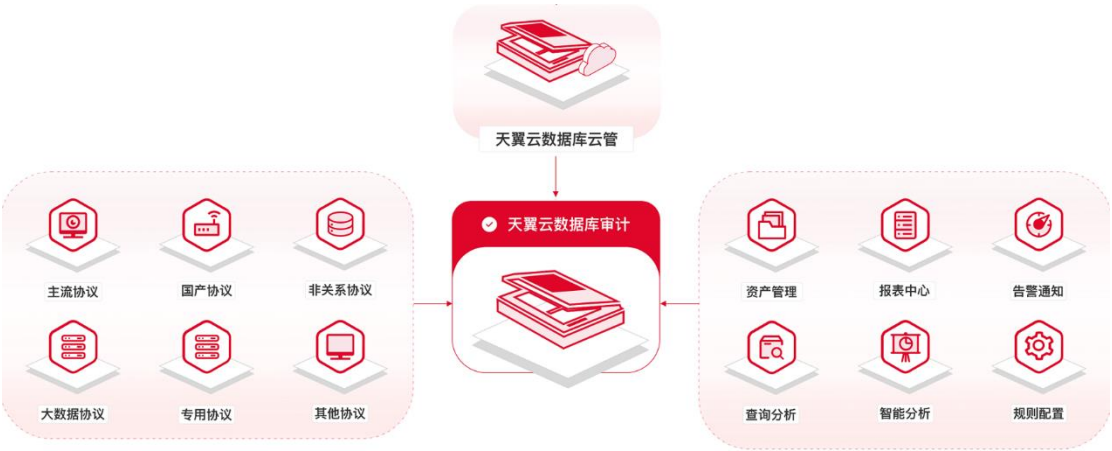
天翼云科技有限公司

目录

1 产品概述

1.1 产品定义

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。



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、

数据库协议	数据库类型
	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。

1.2 产品优势

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

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，包括审传统的数据库系统、大数据系统和 Web 系统等。

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。

1.3 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。

1.4 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。

1.5 部署架构

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。
- 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。

1.6 产品规格

数据库审计提供了基础版、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。

版本	支持的数据库实例个数	资源需求	性能参数
基础版	1 个	CPU：4U 内存：16GB 硬盘：500GB	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	3 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：2TB	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。

1.7 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。

1.8 使用限制

支持的数据库版本

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

数据库类型	支持的版本
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

数据库类型	支持的版本
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

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

Agent 支持的操作系统

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
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

操作系统	操作系统位数	支持版本
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

2 计费说明

2.1 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。

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。

2.2 计费模式

计费模式概述

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

以下计费项支持包年/包月。

计费项	说明
数据库审计版本	购买的数据库审计版本，目前可选基础版、高级版、企业版和旗舰版。
存储扩容	购买存储扩容的内存大小。

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。

2.3 计费项

版本规格

数据库审计提供了基础版、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。

版本	支持的数据库实例个数	资源需求	性能参数
基础版	3 个	CPU：4U 内存：16GB 硬盘：500GB	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。

计费说明

计费项	支持的规格	月计费价格	年计费价格
*数据库审计基础版	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

2.4 续费与退订

到期与欠费

- 包周期资源开通成功后，如果没有按时续费，云平台会提供一定的保留期。
- 保留期 ：指宽限期到期后客户的包年/包月资源仍未续订或按需资源仍未缴清欠款，将进入保留期。保留期内客户不能访问及使用云服务，但对客户存储在云服务中的数据仍予以保留。
- 云服务进入保留期后，天翼云将会通过邮件、短信等方式向您发送提醒，提醒您续订或充值。保留期到期仍未续订或充值，存储在云服务中的数据将被删除、云服务资源将被释放。

- 欠费后，可以查看欠费详情。为防止相关资源不被停止或者释放，请及时进行充值，账号将进入欠费状态，需要在约定时间内支付欠款。

3 快速入门

3.1 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”。

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。
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	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。 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。
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。

3.2 安装 Agent

通过远程安装 SSH 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	支持表单格式和文本格式输入。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。支持 IPv4 和 IPv6，最多填写 20 个。

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的 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。

3.3 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：

1.过滤规则；

2.信任规则；

3.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。
- **新增资产和资产账号**

在使用云堡垒机进行运维前，管理员需要将主机资产和主机账号新增到云堡垒机系统中。

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。

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。具体参数请参考安全规则章节。

4 用户指南

4.1 购买数据库审计实例

数据库审计实例规格

数据库审计提供了基础版、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。

版本	支持的数据库实例个数	资源需求	性能参数
基础版	3 个	CPU：4U 内存：16GB 硬盘：500GB	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。

购买步骤

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.单击右上角的“立即购买”，进入数据库审计实例购买页，购买选项参数详见下表。

参数	说明
地域	选择数据库审计实例购买所在的资源池。

参数	说明
数据库审计名称	输入该数据库审计实例的名称。
版本	选择数据库审计的版本，版本说明详见数据库审计规格。
存储扩容	按需选择需要扩容的硬盘大小。
购买时长	选择数据库审计购买的时长。根据业务需求勾选“到期自动续费”选项。

4.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”。

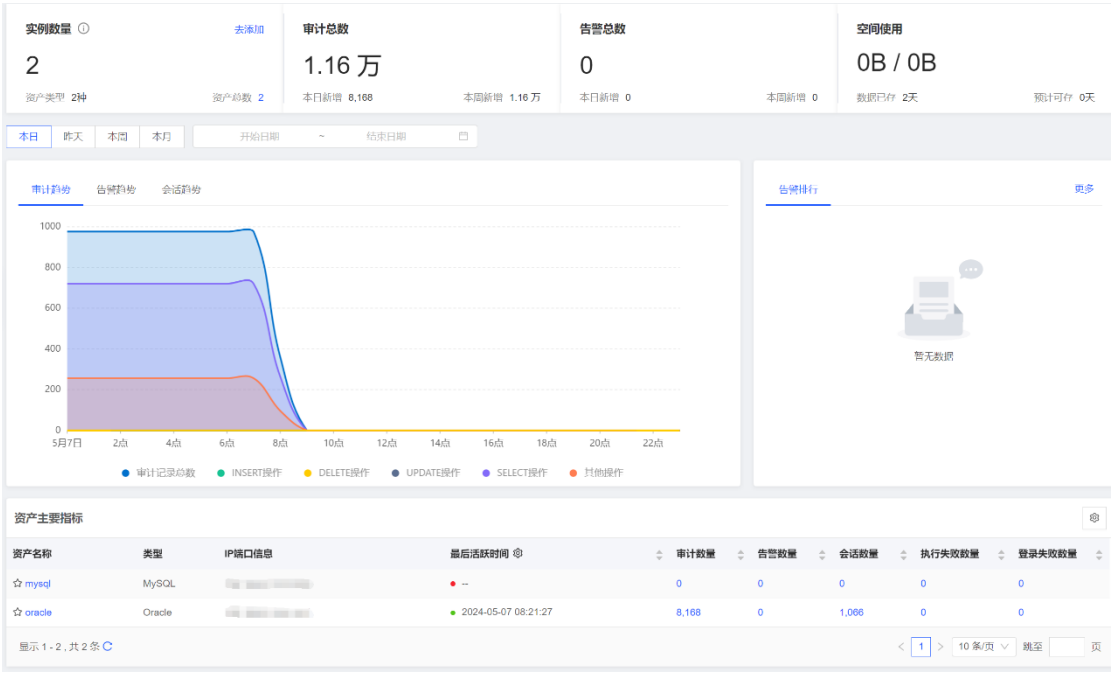
5.在订单详情页确认内容是否正确，确认无误后单击“立即支付”，再后续跳转页中完成支付即成功购买数据库审计服务。

4.2 总览

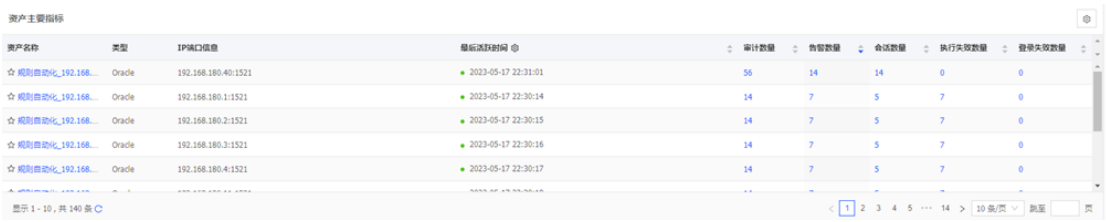
仪表盘

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



- 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。



- 在实例数量模块中单击“去添加”可添加新的资产。
- 在告警总数中点击“告警优化”可在告警分析页面优化告警。

表分析

在左侧菜单栏选择“总览 > 标分析”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：

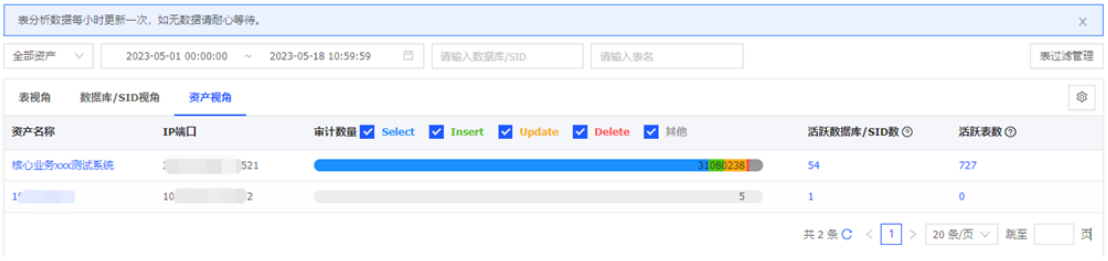
- 表结构：显示表所属节点信息，以及对应下级节点的个数、审计数量。
- XX 详情（“XX”为具体的表名或数据库/SID 名或资产名称，请以实际情况为准）：显示表的基础信息，可对表、数据库/SID 设置备注、对象组信息。
- 字段信息：显示选中表中包含的字段信息，可对字段设置字段备注、对象组信息。
- 数据流动趋势：显示各个时间段该表的审计数量与影响行数。
- 访问关系分析：使用图表的方式显示访问该表的客户端 IP、数据库账号、操作类型信息，用于梳理访问权限，帮助用户实现权限最小化。

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。

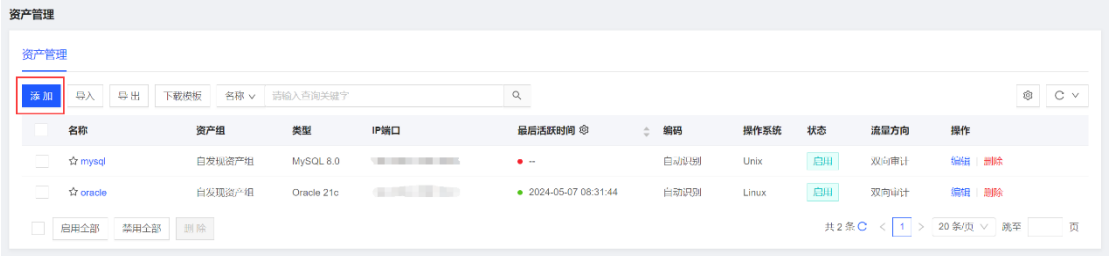
4.3 数据库审计资产管理

添加资产后，系统可对资产进行安全审计。添加资产的方法包括手动添加和资产自发现两种方式。

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”。



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。
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	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。 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。
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。

编辑资产

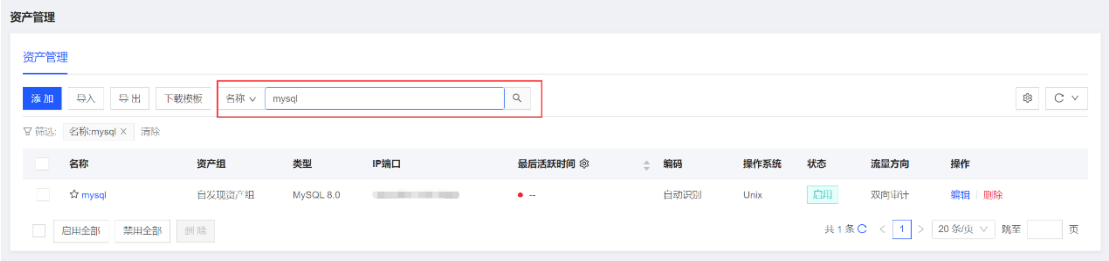
1.在“资产管理”页面，选择“资产管理”页签，选择待编辑的资产，单击“操作”列的“编辑”按钮。

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。



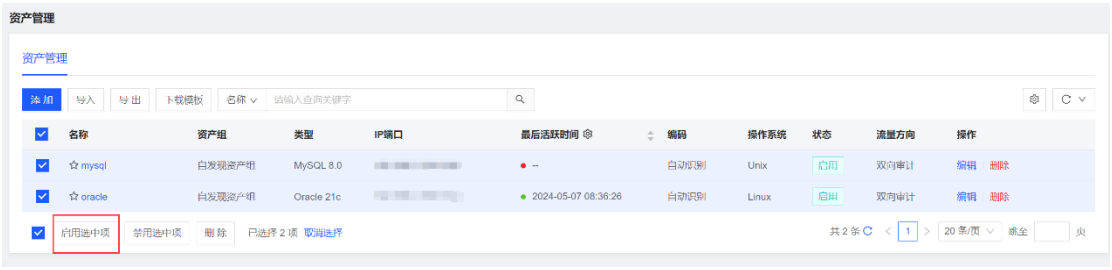
删除资产

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。

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。

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。

4.4 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。

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	支持表单格式和文本格式输入。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。支持 IPv4 和 IPv6，最多填写 20 个。

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的 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。

手动安装 Agent

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章节。

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。

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。

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，“Wincap”和“Npcap”安装操作选项会有些许差别：

- “Wincap”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。

6.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。

配置项	配置项说明
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。
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。

配置项	配置项说明
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。

配置项	配置项说明
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。
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。

操作	说明
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。

4.5 审计规则配置

4.5.1 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。

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 IP 过滤”页签。

2.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。

配置项	说明
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。

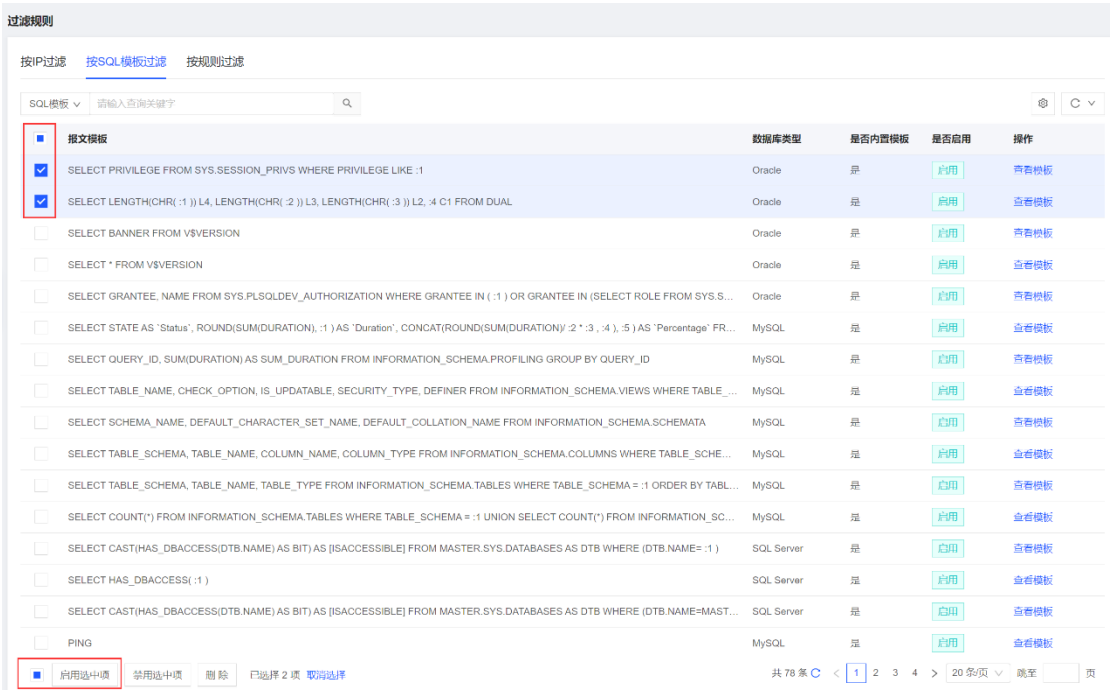
3.填写完成后，单击“保存”，即可完成按 IP 过滤规则的配置。

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”。



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。

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”。

4.5.2 信任规则

信任规则概述

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。

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：

项目	参数	参数说明
		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。 • 普通规则：单条审计记录匹配配置的普通规则，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）。 • 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）。
	行为	当前支持告警和告警并阻断。 • 告警：操作命中规则后，仍正常执行，无特殊控制。 • 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。
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。

项目	参数	参数说明
	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。

项目	参数	参数说明
	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	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。

项目	参数	参数说明
		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 字句	是否包含 WHERE，支持三个选项： • 不判断 • 有 WHERE 子句 • 没有 WHERE 子句 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;

项目	参数	参数说明
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： • 全部 • 成功 • 失败

项目	参数	参数说明
		默认为全部。
	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。

3.配置完成后，单击“保存”即可完成信任规则的配置。

4.5.3 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。
	规则类型	当前支持普通规则和统计规则两类。

项目	参数	参数说明
		• 普通规则：单条审计记录匹配配置的普通规则，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）。 • 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）。
	行为	当前支持告警和告警并阻断。 • 告警：操作命中规则后，仍正常执行，无特殊控制。 • 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。
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。

项目	参数	参数说明
	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。

项目	参数	参数说明
	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	SQL 关键字：支持以正则表达式匹配报文。

项目	参数	参数说明
		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 字句	是否包含 WHERE，支持三个选项： • 不判断 • 有 WHERE 子句 • 没有 WHERE 子句

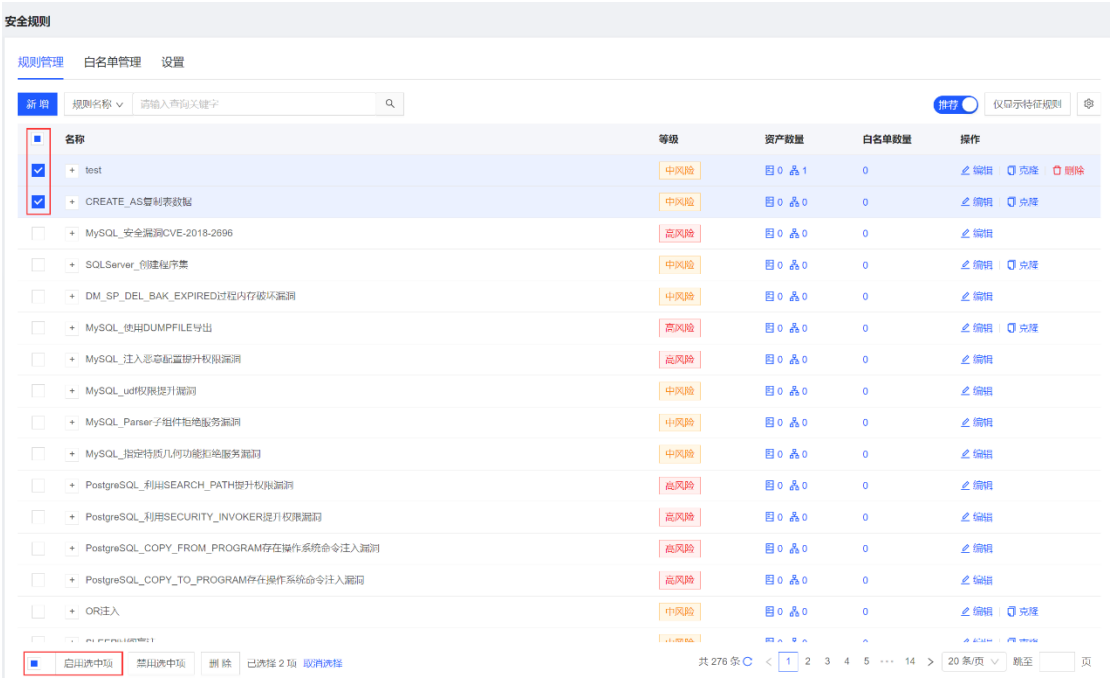
项目	参数	参数说明
		默认为不判断。WHERE 子句用于提取满足指定条件的 SQL 记录，语法如下： SELECT column_name,column_name FROM table_name WHERE column_name operator value;
结果	执行时长	（选填）单位：秒、毫秒、微秒，取值范围：0 到半个小时，SQL 执行时长属于此范围，则触发规则。
	影响行数	取值范围：0~999,999,999。SQL 操作返回的记录数或受影响的行数属于此范围，则触发规则。
	返回结果集	支持以正则表达式匹配结果集。 单击“正则验证”输入报文内容，单击“校验”，验证输入内容与执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：

项目	参数	参数说明
		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： • 全部 • 成功 • 失败 默认为全部。
	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。

项目	参数	参数说明
	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”。



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）。

3.配置完成后，单击“保存”即可完成白名单的新增。

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。

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。

4.5.4 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。

4.6 查询审计内容

4.6.1 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。

4.6.2 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：

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。

4.6.3 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。

4.6.4 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，可以怀疑是否是存在异常访问行为。

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。

4.7 报表中心

4.7.1 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。

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	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

报表类型	报表说明
析类报表	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。

4.7.2 报表订阅

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)”。
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）。

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。

4.7.3 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。

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。

4.8 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。

配置项	说明
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上的“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上的“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上的“填写说明”编辑。

配置项	说明
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上的“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。

配置项	说明
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：0~8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“编辑”，在弹出的“短信配置”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
发送方式	选择短信发送方式，支持 Web 接口和数据库接口。

配置项	说明
发送方法（Web 接口）	请求方法，支持 GET、POST 请求。
URL（Web 接口）	短信网关的接入 URL。
头信息（Web 接口）	请求头。可添加多个请求头信息。
Post 参数（Web 接口 Post 方法）	请求 Post 参数内容，如果使用 Json 方式，该值填写 Json 内容。
数据库类型	选择数据库的类型，支持 MySQL、Oracle、DB2 和 SQL Server。
数据库名称/SID（数据库接口）	短信通知接口数据库名称。
用户名/密码（数据库接口）	短信通知接口数据库的用户名和密码。
域名或者 IP（数据库接口）	短信通知接口数据库的 IP 或域名。
端口（数据库接口）	短信通知接口数据库的端口。

配置项	说明
参数顺序（数据库接口）	支持“先手机号码，后短信内容”和“先短信内容，后手机号码”。
插入 SQL 模板（数据库接口）	使用两个参数（1.手机号码，2.短信内容），用“?”表示，顺序可在“参数顺序”中设置。例如：insert into MSG(count,phonenum,content,priority) values(1,?,?,1)。 注意 语句最后不用加分号“;”。
调用方式（数据库接口）	可选择 INSERT 语句或者存储过程。
编码方式	服务器支持的编码方式，主要为：UTF-8、GBK。以上配置与短信服务器端保持一致即可。
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上的“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上的“填写说明”编辑。

配置项	说明
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上的“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上的“填写说明”编辑。

3.配置短信通知接口页面的相关信息后，可以给需要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，可选择多个。
接受者	接收告警信息的手机号，可设置多个手机号。
告警模板	选择要发送的告警信息的告警等级。

配置项	说明
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：0~86,400，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。聚合消息示例如下：在过去*秒，总计触发*条告警。
告警统计	开启或关闭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。

4.9 其他操作

4.9.1 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：

- 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”。

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。

配置项	说明
登录时间限制	限制用户登录系统的时间。

4.9.2 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”。

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：([^d]
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。

4.9.3 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。
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。

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。

4.9.4 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”。

5 最佳实践

5.1 审计 RDS 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

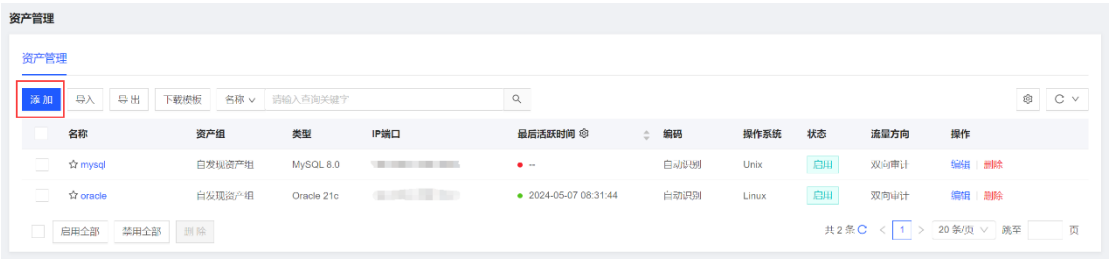
全审计可以生成满足数据安全标准（例如 Sarbanes-Oxley）的合规报告，对数据库的内部违规和不正当操作进行定位追责，保障数据资产安全。

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。

参数	参数说明
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。

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。

6 常见问题

6.1 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

数据库类型	支持的版本
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

数据库类型	支持的版本
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

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

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

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
基础版	3 个	CPU：4U 内存：16GB 硬盘：500GB	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。

版本	支持的数据库实例个数	资源需求	性能参数
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?

数据库审计暂不支持纳管天翼云的云上数据库。

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。

6.2 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。

基础版：3 个

高级版：6 个

企业版：12 个

旗舰版：30 个

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。

6.3 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
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

数据库类型	支持的版本
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

数据库类型	支持的版本
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

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

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

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

操作系统	操作系统位数	支持版本
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

操作系统	操作系统位数	支持版本
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。

6.4 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
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

操作系统	操作系统位数	支持版本
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

6.5 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，详情请参见资产。
步骤二：安装 Agent	安装 Agent 进行数据库审计，详情请参见 Agent 管理。
步骤三：配置规则	配置数据库的安全规则和过滤规则，详情请参见规则配置。
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，详情请参见报表订阅和告警通知。

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：

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

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

以 SSL 模式登录 MySQL 数据库。

执行以下命令，退出 MySQL 数据库。

exit

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。

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

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，对可以行为进行风险告警。可在平台中检索审计到的审计日志和告警日志。

6.6 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。

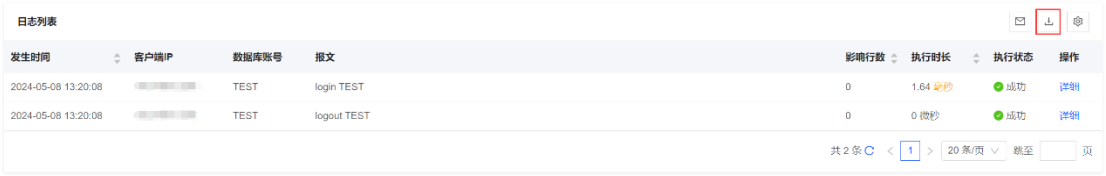
制定自动小时备份任务，避免数据量存储磁盘达到 85%触发日志清理机制。

6.7 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。



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。