云审计

用户使用指南

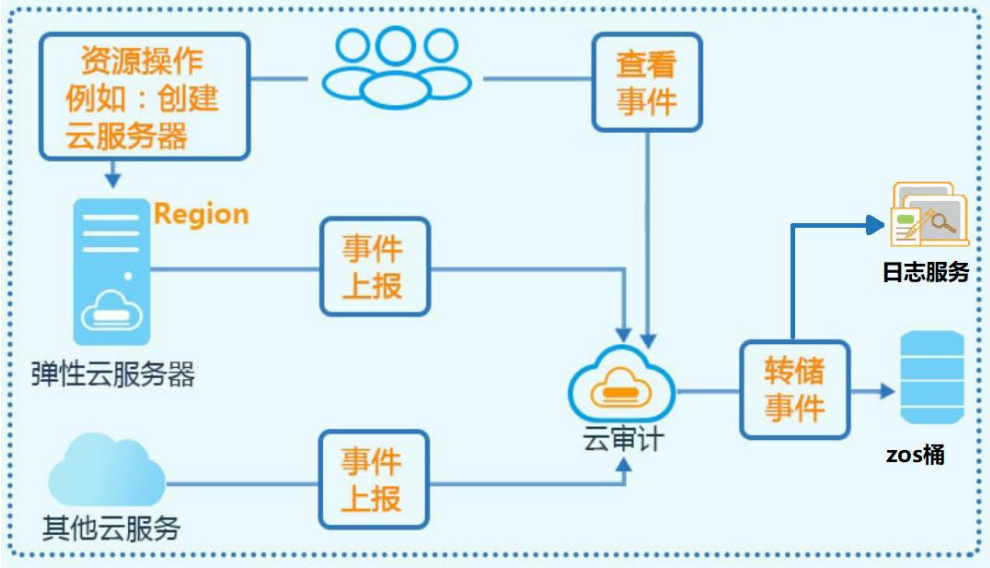
天翼云科技有限公司

目 录

1. 产品简介

1.1. 产品定义

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。



1.2. 产品优势

- 合规性

  审计日志格式统一，所含内容符合常见标准的规定。

- 完整性

  包含所有操作信息，防篡改。

- 实时性

  实时记录、实时检索。

- 低成本

  一键开通，无需维护，支持将操作记录合并，低成本的长久保存。

- 高效率

  提供可视化检索界面，检索维度组合便捷。

1.3. 功能特性

- 记录审计日志

  支持记录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来源、资源类型、事件名称、资源名称/ID、事件级别和时间范围等多个维度进行组合查询。

- 审计日志转储

  支持将审计日志以 gzip 文件的形式周期性的转储至对象存储服务（简称 ZOS）下的存储桶，并以“**目录前缀/日志类型标识符/地域**/年/月/日”逐层设置为目录层级，存放投递的事件。

1.4. 相关术语解释

- 事件：事件是用户通过天翼云控制台、OpenAPI 对云上服务进行操作所产生的记录。事件包含事件来源、操作人员、资源信息、操作时间、操作请求、操作结果等。
- 跟踪：跟踪是云审计的一种配置，可用于将云审计事件投递至对象存储桶、日志服务实现永久存储或日志分析。支持用户选择投递事件类型范围、投递目标等。

1.5. 应用场景

- 合规审计

  助力企业用户业务系统符合监管标准，轻松通过等保、IT 合规设计认证要求。

- 安全分析

  对用户操作进行详细的记录，可用于越权分析、关键资源变更分析等。

- 操作追踪

  当用户的资源出现异常变更时，云审计所记录的操作日志能帮助用户快速溯源，简化运维。

- 问题定位

云资源故障时，可通过事件列表快速检索事发时的可疑操作，极大程度提升问题定位的效率。

1.6. 使用限制

云审计服务中的追踪器数量和关键操作通知有限定的配额，均不支持修改，具体限制如下：

限制事件	限制规格
每个事件跟踪限制的 ZOS 桶数量	1 个
用户操作后多久可以通过云审计查询到数据	• 管理类事件：1 分钟 • 数据类事件：5 分钟
用户通过云审计能查询到多久前的操作事件	7 天

2. 计费说明

2.1. 计费模式

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。

3. 快速入门

3.1. 开通云审计服务

使用云审计服务前需要先开通所在资源池的云审计服务，如果不开通云审计服务，则无法对资源操作进行记录。

前提条件

已注册天翼云账号，并且通过实名认证。

操作步骤

1. 登录天翼云官网，在产品列表中找到云审计。
2. 进入云审计产品详情页，点击“立即开通”。
3. 进入云审计控制台，初次使用会显示欢迎使用页面，点击“立即购买”。

4. 勾选“我已阅读，理解并接受《天翼云云审计服务协议》”，点击“立即购买”，即可完成服务开通。

3.2. 查看审计事件

当您已开通云审计服务，系统开始记录云服务资源的操作，并支持查看近 7 天的操作事件。本文为您介绍如何在云审计控制台查看操作审计事件。

前提条件

已开通云审计服务。

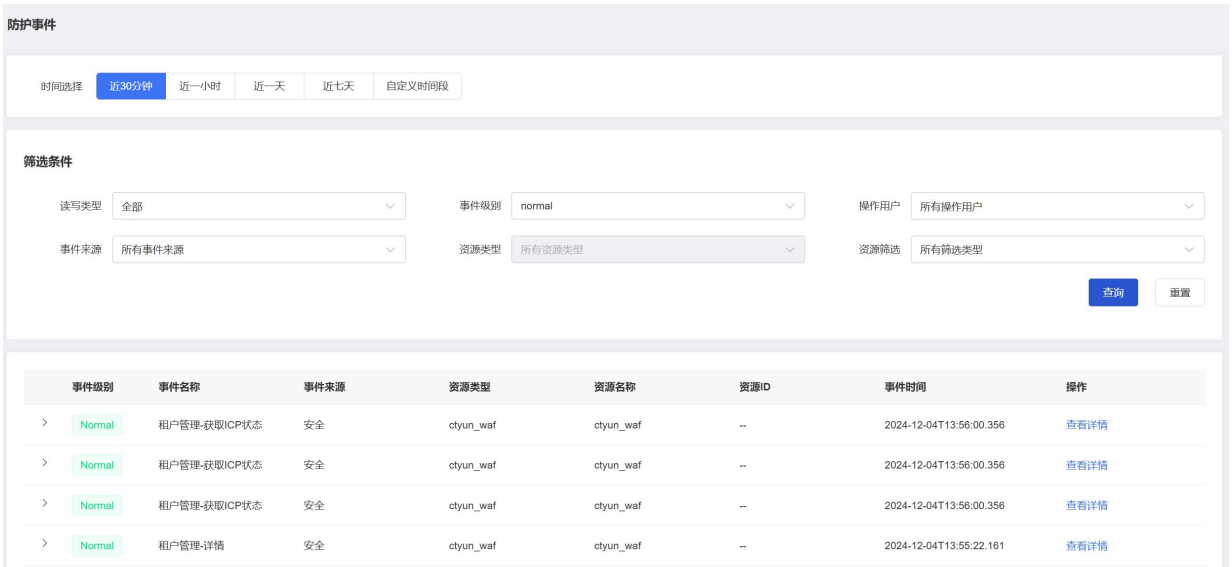
操作步骤

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. 在控制台列表页，选择“云审计”。
4. 进入云审计控制台后，点击侧边栏“事件列表”。
5. 进入事件列表页面，事件列表上方支持通过筛选条件查询。

云审计支持五个维度的组合查询，说明如下：

- 时间筛选：支持快速点选近 30 分钟、近 1 小时、近 1 天、近 7 天的时间范围，也支持自定义时间范围。
- 读写类型：支持根据事件的读写类型进行筛选。
- 事件级别：支持根据事件等级进行筛选，当前事件等级包括 normal（代表本次操作成功）、warning（代 表本次操作失败）。
- 操作用户：支持根据同一租户下的不同主子账号进行筛选。
- 事件来源、资源类型、资源筛选：支持以资源维度进行多层级的筛选，最细粒度支持具体某个资源实例 的筛选。

6. 筛选条件选择完成，点击“查询”，符合条件的事件将以列表显示出来。



4. 用户指南

4.1. 查看审计事件

当您已开通云审计服务，系统开始记录云服务资源的操作，并支持查看近 7 天的操作事件。 本文为您介绍如何在云审计控制台查看操作审计事件。

前提条件

已开通云审计服务。

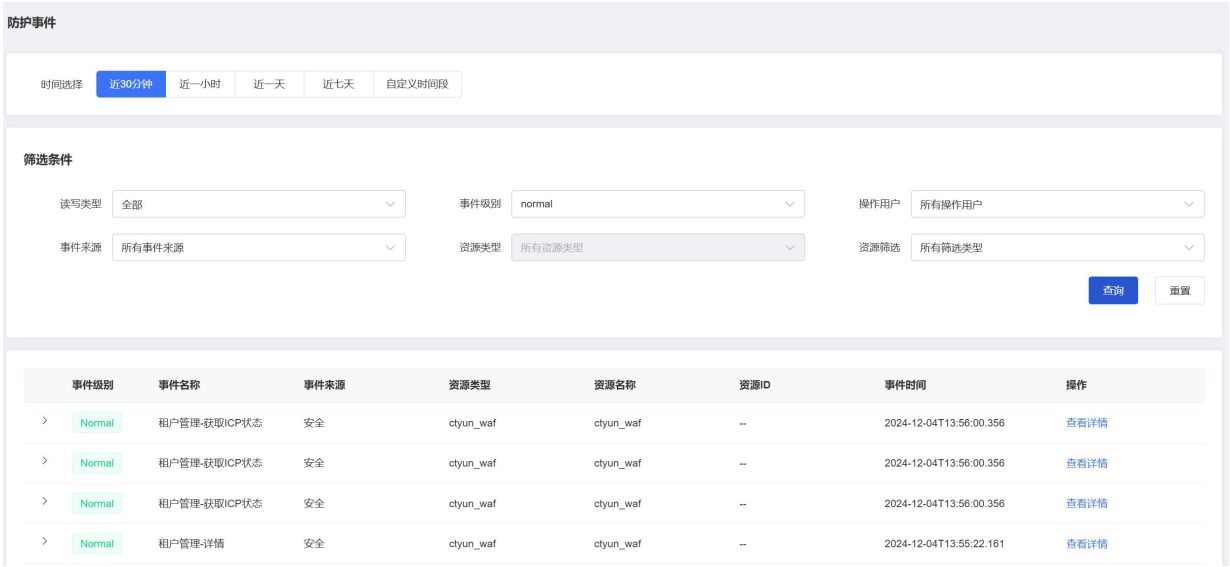
操作步骤

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. 在控制台列表页，选择“云审计”。
4. 进入云审计控制台后，点击侧边栏“事件列表”。
5. 进入事件列表页面，事件列表上方支持通过筛选条件查询。

云审计支持五个维度的组合查询，说明如下：

- 时间筛选：支持快速点选近 30 分钟、近 1 小时、近 1 天、近 7 天的时间范围，也支持自定义时间范围。
- 读写类型：支持根据事件的读写类型进行筛选。
- 事件级别：支持根据事件等级进行筛选，当前事件等级包括 normal（代表本次操作成功）、warning（代 表本次操作失败）。
- 操作用户：支持根据同一租户下的不同主子账号进行筛选。
- 事件来源、资源类型、资源筛选：支持以资源维度进行多层级的筛选，最细粒度支持具体某个资源实例 的筛选。

6. 筛选条件选择完成，点击“查询”，符合条件的事件将以列表显示出来。



4.2. 支持审计的云产品及关键操作列表

4.2.1 计算

弹性云主机

请参见弹性云主机支持的关键操作列表。

弹性伸缩服务

请参见弹性伸缩支持的关键操作列表。

物理机

操作事件	字段
创建物理机	create_bm_server
开机物理机	start_bm_server
关机物理机	stop_bm_server
一键重装物理机	rebuild_bm_server
重启物理机	restart_bm_server
远程登录物理机	get_bm_server_vnc
物理机重置密码	change_bm_server_password
物理机绑定弹性公网 IP	bind_bm_floating
物理机解绑弹性公网 IP	unbind_bm_floating
续订物理机	renew_bm_server

操作事件	字段
退订物理机	refund_bm_server

镜像服务

操作事件	资源类型	字段名称
创建私有镜像	私有镜像	create_private_image
取消共享镜像	私有镜像	cancel_share_image
接受共享镜像	私有镜像	accept_share_image
共享私有镜像	私有镜像	share_image
删除私有镜像	私有镜像	delete_private_image
拒绝共享镜像	私有镜像	reject_share_image
更新私有镜像（更新镜像描述信息、名称等）	私有镜像	update_private_image

4.2.2 存储

分类	云产品	支持审计的关键操作列表
存储	云硬盘	云硬盘支持的关键操作列表
	对象存储	对象存储支持的关键操作列表
	海量文件服务 OceanFS	海量文件服务 OceanFS 支持的关键操作列表

4.2.3 网络

VPN 连接

请参见 VPN 连接支持的关键操作列表。

云间高速（标准版）

请参见云间高速（标准版）支持的关键操作列表。

云专线

请参见云专线支持的关键操作列表。

弹性负载均衡

资源类型	动作
负载均衡器	查看负载均衡器列表
	查看负载均衡器详情

资源类型	动作
	创建负载均衡器
	修改负载均衡器
	删除负载均衡器
	经典型负载均衡升级性能保障型
	续订
	规格变配
监听器	查看监听器列表
	查看监听器详情
	创建监听器
	修改监听器
	删除监听器
转发策略	查看转发策略列表
	查看转发策略详情
	创建转发策略
	修改转发策略
	删除转发策略
后端主机组	查看后端主机组列表
	查看后端主机组详情
	创建后端主机组
	删除后端主机组
	修改后端主机组
健康检查	查看健康检查类别
	查看健康检查详情
	创建健康检查
	删除健康检查
	修改健康检查
后端主机	查看后端主机列表
	查看后端主机详情
	创建后端主机
	删除后端主机
	修改后端主机
证书	查看证书列表
	查看证书详情
	创建证书

资源类型	动作
	修改证书
	删除证书
访问策略组	查看访问策略组列表
	查看访问策略组详情
	创建访问策略组
	修改访问策略组
	删除访问策略组
	绑定弹性 IP
	解绑弹性 IP
	修改弹性 IP 带宽
	绑定 IPv6 带宽
	解绑 IPv6 带宽
	添加标签
	删除标签
	查看标签

弹性公网 IP

操作事件	字段名称
绑定 EIP	bind_ip
开通 ipv6 带宽	create_ipv6
绑定 ipv6 带宽	bind_ipv6
续订 ipv6 带宽	renew_ipv6
变配弹性 ip	resize_ip
退订弹性 ip	refund_ip
退订 ipv6 带宽	refund_ipv6
解绑 EIP	unbind_ip
续订 EIP	renew_ip
变配 ipv6 带宽	resize_ipv6
开通 EIP	create_ip
解绑 ipv6 带宽	unbind_ipv6

NAT 网关

事件名称	事件的读写类型	srcProdName、srcRes Id
查询私网 NAT 网关列表	读	私网 NAT 网关，无

事件名称	事件的读写类型	srcProdName、srcRes Id
查询私网 NAT 网关详情	读	私网 NAT 网关，私网 NAT 网关 ID
创建私网 NAT 网关	写	私网 NAT 网关，无
退订私网 NAT 网关	写	私网 NAT 网关，私网 NAT 网关 ID
删除私网 NAT 网关	写	私网 NAT 网关，私网 NAT 网关 ID
获取私网 NAT 网关绑定的标签	读	私网 NAT 网关，私网 NAT 网关 ID
私网 NAT 网关绑定标签	写	私网 NAT 网关，私网 NAT 网关 ID
私网 NAT 网关解绑标签	写	私网 NAT 网关，私网 NAT 网关 ID
获取私网 NAT 网关绑定的标签	读	私网 NAT 网关，私网 NAT 网关 ID
创建 SNAT 规则	写	私网 NAT 网关，无
查看 SNAT 规则列表	读	私网 NAT 网关，无
查看 SNAT 规则	读	私网 NAT 网关，SNAT 规则 ID
修改 SNAT 规则	写	私网 NAT 网关，SNAT 规则 ID
删除 SNAT 规则	写	私网 NAT 网关，SNAT 规则 ID
创建 DNAT 规则	写	私网 NAT 网关，无
查看 DNAT 规则列表	读	私网 NAT 网关，无
查看 DNAT 规则	读	私网 NAT 网关，DNAT 规则 ID
修改 DNAT 规则	写	私网 NAT 网关，DNAT 规则 ID
删除 DNAT 规则	写	私网 NAT 网关，DNAT 规则 ID
创建中转 IP	写	私网 NAT 网关，私网 NAT 网关 ID
查看中转 IP	读	私网 NAT 网关，私网 NAT 网关 ID
查询公网 NAT 网关列表	读	公网 NAT 网关，无
查询公网 NAT 网关详情	读	公网 NAT 网关，公网 NAT 网关 ID
创建公网 NAT 网关	写	公网 NAT 网关，无
退订公网 NAT 网关	写	公网 NAT 网关，公网 NAT 网关 ID
删除公网 NAT 网关	写	公网 NAT 网关，公网 NAT 网关 ID
获取公网 NAT 网关绑定的标签	读	公网 NAT 网关，公网 NAT 网关 ID
公网 NAT 网关绑定标签	写	公网 NAT 网关，公网 NAT 网关 ID
公网 NAT 网关解绑标签	写	公网 NAT 网关，公网 NAT 网关 ID
获取公网 NAT 网关绑定的标签	读	公网 NAT 网关，公网 NAT 网关 ID
创建 SNAT 规则	写	公网 NAT 网关，无
查看 SNAT 规则列表	读	公网 NAT 网关，无
查看 SNAT 规则	读	公网 NAT 网关，SNAT 规则 ID
修改 SNAT 规则	写	公网 NAT 网关，SNAT 规则 ID
删除 SNAT 规则	写	公网 NAT 网关，SNAT 规则 ID

事件名称	事件的读写类型	srcProdName、srcRes Id
创建 DNAT 规则	写	公网 NAT 网关，无
查看 DNAT 规则列表	读	公网 NAT 网关，无
查看 DNAT 规则	读	公网 NAT 网关，DNAT 规则 ID
修改 DNAT 规则	写	公网 NAT 网关，DNAT 规则 ID
删除 DNAT 规则	写	公网 NAT 网关，DNAT 规则 ID

共享带宽

事件来源	资源类型	事件名称
弹性网络	共享带宽	创建共享带宽
弹性网络	共享带宽	删除共享带宽
弹性网络	共享带宽	查询共享带宽详情
弹性网络	共享带宽	查询共享带宽列表
弹性网络	共享带宽	共享带宽绑定 eip
弹性网络	共享带宽	共享带宽绑定 ipv6
弹性网络	共享带宽	共享带宽解绑 eip
弹性网络	共享带宽	共享带宽解绑 ipv6
弹性网络	共享带宽	共享带宽修改带宽

虚拟私有云

事件来源	资源类型	事件名称
弹性网络	虚拟私有云	创建专有网络
弹性网络	虚拟私有云	修改专有网络属性
弹性网络	虚拟私有云	删除专有网络属性
弹性网络	虚拟私有云	查询用户专有网络
弹性网络	虚拟私有云	VPC解绑扩展网段
弹性网络	虚拟私有云	查询用户专有网络列表
弹性网络	虚拟私有云	修改专有网络的 IPv6状态
弹性网络	虚拟私有云	VPC绑定扩展网段
弹性网络	虚拟私有云	查看某个子网已使用 IP
弹性网络	虚拟私有云	查询用户专有网络下子网列表
弹性网络	虚拟私有云	修改子网的 IPv6状态
弹性网络	虚拟私有云	创建子网
弹性网络	虚拟私有云	子网解绑路由表
弹性网络	虚拟私有云	子网替换 ACL

事件来源	资源类型	事件名称
弹性网络	虚拟私有云	子网开启 IPv6
弹性网络	虚拟私有云	查询用户专有网络 VPC 下子网详情
弹性网络	虚拟私有云	修改子网属性
弹性网络	虚拟私有云	子网更换路由表
弹性网络	虚拟私有云	子网解绑 ACL
弹性网络	虚拟私有云	删除子网
弹性网络	虚拟私有云	创建高可用虚 IP
弹性网络	虚拟私有云	将 HaVip 绑定到 ECS 实例上
弹性网络	虚拟私有云	查询高可用虚 IP 列表
弹性网络	虚拟私有云	删除高可用虚 IP
弹性网络	虚拟私有云	将 HaVip 从ECS 实例上解绑
弹性网络	虚拟私有云	查看高可用虚 IP 详情
弹性网络	虚拟私有云	创建 prefixlist
弹性网络	虚拟私有云	修改 prefixlist
弹性网络	虚拟私有云	查看 prefixlist 详情
弹性网络	虚拟私有云	删除 prefixlist
弹性网络	虚拟私有云	克隆 prefixlist
弹性网络	虚拟私有云	查看 prefixlist 列表
弹性网络	虚拟私有云	查看 prefixlist 绑定资源
弹性网络	虚拟私有云	修改 prefixlist_rule
弹性网络	虚拟私有云	创建 prefixlist_rule
弹性网络	虚拟私有云	删除 prefixlist_rule
弹性网络	虚拟私有云	修改路由表规则
弹性网络	虚拟私有云	删除路由表规则
弹性网络	虚拟私有云	查询路由表列表
弹性网络	虚拟私有云	查询路由表规则列表
弹性网络	虚拟私有云	修改单条路由表规则
弹性网络	虚拟私有云	查询路由表详情
弹性网络	虚拟私有云	创建网关路由表
弹性网络	虚拟私有云	创建路由表
弹性网络	虚拟私有云	创建单条路由规则
弹性网络	虚拟私有云	修改路由表属性
弹性网络	虚拟私有云	创建路由表规则
弹性网络	虚拟私有云	删除路由表

事件来源	资源类型	事件名称
弹性网络	虚拟私有云	弹性网卡列表
弹性网络	虚拟私有云	删除弹性网卡
弹性网络	虚拟私有云	多个网卡解绑 IPv6 地址（批量时使用）
弹性网络	虚拟私有云	网卡绑定物理机
弹性网络	虚拟私有云	查询网卡信息
弹性网络	虚拟私有云	网卡绑定实例
弹性网络	虚拟私有云	创建弹性网卡
弹性网络	虚拟私有云	网卡解绑物理机
弹性网络	虚拟私有云	修改网卡属性
弹性网络	虚拟私有云	多个网卡关联 IPv6（批量时使用）
弹性网络	虚拟私有云	网卡关联辅助私网 IP
弹性网络	虚拟私有云	单个网卡关联多个 IPv6 地址
弹性网络	虚拟私有云	更换 VPC
弹性网络	虚拟私有云	修改内网 IP
弹性网络	虚拟私有云	网卡解绑辅助私网 IP
弹性网络	虚拟私有云	单个网卡解绑多个 IPv6地址
弹性网络	虚拟私有云	网卡解绑实例
弹性网络	虚拟私有云	获取资源绑定的标签
弹性网络	虚拟私有云	资源绑定标签
弹性网络	虚拟私有云	资源解绑标签
弹性网络	虚拟私有云	获取绑定标签的资源列表
弹性网络	虚拟私有云	创建安全组
弹性网络	虚拟私有云	查询用户安全组详情
弹性网络	虚拟私有云	创建安全组入向规则
弹性网络	虚拟私有云	删除一条入方向安全组规则
弹性网络	虚拟私有云	查询用户安全组列表
弹性网络	虚拟私有云	获取安全组绑定网卡
弹性网络	虚拟私有云	删除一条出方向安全组规则
弹性网络	虚拟私有云	安全组批量解绑网卡
弹性网络	虚拟私有云	删除安全组
弹性网络	虚拟私有云	获取安全组绑定机器列表
弹性网络	虚拟私有云	创建安全组出向规则
弹性网络	虚拟私有云	解绑安全组
弹性网络	虚拟私有云	批量删除安全组规则

事件来源	资源类型	事件名称
弹性网络	虚拟私有云	更新安全组
弹性网络	虚拟私有云	批量绑定安全组
弹性网络	虚拟私有云	修改安全组入方向规则描述
弹性网络	虚拟私有云	安全组规则详情
弹性网络	虚拟私有云	安全组批量绑定网卡
弹性网络	虚拟私有云	绑定安全组
弹性网络	虚拟私有云	修改安全组出方向规则描述
弹性网络	虚拟私有云	添加 IPv6s 至共享带宽
弹性网络	虚拟私有云	查询 IPv6 网关列表
弹性网络	虚拟私有云	删除 IPv6 网关
弹性网络	虚拟私有云	查询 IPv6 网关详情
弹性网络	虚拟私有云	查询 IPv6 列表
弹性网络	虚拟私有云	查询 IPv6 详情
弹性网络	虚拟私有云	ipv4gw 移除路由表绑定
弹性网络	虚拟私有云	查看 ipv4gw 列表
弹性网络	虚拟私有云	查看 ipv4gw 详情
弹性网络	虚拟私有云	ipv4gw 绑定路由表
弹性网络	虚拟私有云	获取 igw 列表
弹性网络	虚拟私有云	更新 dhcpoptionsets
弹性网络	虚拟私有云	获取绑定的 vpc 列表
弹性网络	虚拟私有云	获取未绑定 dhcp 的 vpc 列表
弹性网络	虚拟私有云	dhcpoptionsets 关联 vpc
弹性网络	虚拟私有云	dhcpoptionsets 取消关联 vpc
弹性网络	虚拟私有云	删除 dhcpoptionsets
弹性网络	虚拟私有云	查询 dhcpoptionsets 详情
弹性网络	虚拟私有云	创建 dhcpoptionsets
弹性网络	虚拟私有云	查询 dhcpoptionsets
弹性网络	虚拟私有云	vpc 替换 dhcpoptionset
弹性网络	虚拟私有云	修改 Acl
弹性网络	虚拟私有云	查看 Acl 列表
弹性网络	虚拟私有云	删除 Acl
弹性网络	虚拟私有云	克隆 Acl
弹性网络	虚拟私有云	创建 Acl
弹性网络	虚拟私有云	查看 Acl 详情

事件来源	资源类型	事件名称
弹性网络	虚拟私有云	创建 Acl规则
弹性网络	虚拟私有云	删除 Acl规则列表
弹性网络	虚拟私有云	修改 Acl规则列表属性
弹性网络	虚拟私有云	查看 Acl规则列表

4.2.4 容器与中间件

分类	云产品	支持审计的关键操作列表
容器与中间件	云容器引擎	云容器引擎支持的关键操作列表
	容器镜像服务	容器镜像服务支持的关键操作列表
	分布式消息服务 Kafka	分布式消息服务 Kafka 支持的关键操作列表

4.2.5 数据库

分类	云产品	支持审计的关键操作列表
数据库	关系型数据库 MySQL 版	关系型数据库 MySQL 版服务支持的关键操作列表
	关系型数据库 PostgreSQL 版服务	关系型数据库 PostgreSQL 版服务支持的关键操作列表
	关系型数据库 SQLServer 版	关系型数据库 SQL Server 版服务支持的关键操作列表
	分布式关系型数据库	分布式关系型数据库支持的关键操作列表
	文档数据库服务	文档数据库服务支持的关键操作列表
	分布式缓存服务 Redis 版	分布式缓存服务 Redis 版支持的关键操作列表

4.2.6 大数据

分类	云产品	支持审计的关键操作列表
大数据	翼 MapReduce	翼 MapReduce 服务支持的关键操作列表
	云搜索服务	云搜索服务支持的关键操作列表

4.2.7 安全及管理

分类	云产品	支持审计的关键操作列表
安全及管理	Web 应用防火墙（原生版）	Web 应用防火墙（原生版）支持的关键操作列表
	密钥管理	密钥管理服务支持的关键操作列表
	数据库审计	数据库审计支持的关键操作列表

分类	云产品	支持审计的关键操作列表
	云审计	云审计服务支持审计的关键操作列表
	云安全中心	云安全中心支持的关键操作列表
	云等保专区	云等保专区支持的关键操作列表

4.2.8 迁移与管理

分类	云产品	支持审计的关键操作列表
迁移与管理	云监控服务	云监控服务支持的关键操作列表

4.2.9 专属云

分类	云产品	支持审计的关键操作列表
专属云	专属云（计算独享型）	专属云（计算独享型）支持审计的关键操作列表

4.2.10 管理工具

统一身份认证（一类节点）

操作事件	资源类型	字段名称
编辑子用户	user	ctiam:user:update
删除子用户	user	ctiam:user:invalid
创建 AccessKey	credential	ctiam:credential:create
从回收站中彻底删除 AccessKey	credential	ctiam:credential:delete
用户-添加到用户组	user	ctiam:userGroup:addUserToGroup
创建子用户	user	ctiam:user:create
删除用户组	userGroup	ctiam:userGroup:invalid
用户组管理	userGroup	ctiam:userGroup:addUserToGroup
编辑用户组	userGroup	ctiam:user:updateGroup
授权管理-删除授权	privilege	ctiam:permission:invalidGroupPolicy
删除自定义策略	delegate	ctiam:policy:delete
委托-解除 IAM 授权	delegate	ctiam:permission:invalidD elegateRolePolicy
删除委托	delegate	ctiam:delegateRole:delete
用户登录设置-设置密码	user	ctiam:user:settingPassword
企业项目为用户组设置策略	enterpriseProject	ctiam:project:setEpGroupPolicy
用户组授权	privilege	ctiam:permission:attachGroupPolicy
为单个用户授权策略	privilege	ctiam:permission:attachPolicyToUser

操作事件	资源类型	字段名称
为委托授权策略	delegate	ctiam:permission:attachDelegateRolePolicy
为委托解除授权	delegate	ctiam:permission:invalidDelegateRolePolicy
为委托设置企业项目权限	delegate	ctiam:permission:attachDelegateRolePolicy
为委托取消企业项目权限	delegate	ctiam:permission:invalidDelegateRolePolicy

4.2.11 用户服务

天翼云用户及 SSO 用户

事件来源	资源类型	事件名称
天翼云官网	用户	登录
	用户	登出
	云 SSO 用户	创建云 SSO 用户
	云 SSO 用户	编辑云 SSO 用户
	云 SSO 用户	删除云 SSO 用户
	云 SSO 用户	禁用云 SSO 用户
	云 SSO 用户	启用云 SSO 用户
	云 SSO 用户组	创建云 SSO 用户组
	云 SSO 用户组	编辑云 SSO 用户组
	云 SSO 用户组	删除云 SSO 用户组
	云 SSO 用户组	添加云 SSO 用户组用户
	云 SSO 用户组	删除云 SSO 用户组用户

4.3. 云审计服务支持审计的关键操作列表

云审计服务支持记录云审计自身服务相关的操作事件，便于日后的查询、审计和回溯。

云审计服务支持的自身服务操作列表

事件名称	读写类型
开通云审计	写类型
新建跟踪任务	写类型
修改跟踪任务	写类型
删除跟踪任务	写类型
保存授权凭据	写类型

事件名称	读写类型
查询事件列表	读类型
查询筛选事件的条件列表	读类型
查询跟踪任务列表	读类型
查询跟踪任务详情	读类型

查看云审计自身服务事件

1. 开通云审计服务。

   参见开通云审计服务。

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“管理与部署”，资源类型选 择“云审计”，点击“查询”即可。

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。

4. 4. 审计服务事件参考

事件结构

领域	字段名称	类型	是否必须	字段描述
事件	eventId	String	是	事件 id
	eventName	String	是	事件名称（接口名称），中文名称
	eventTime	Long	是	事件发生时间（触发时间），13 位时 间戳

领域	字段名称	类型	是否必须	字段描述
	eventLevel	Integer	否	事件级别，操作事件等级，分为三级： 0：normal 1：warning 2：incident
	eventType	Integer	是	发生的事件类型。取值： 0：API 调用事件（ApiCall） 1：部分控制台或售卖页的管控事件（ConsoleOperation） 2：用户登录登出 3：其他(待定)
	eventActType	Integer	是	事件的读写类型。取值： 0：读类型（read） 1：写类型（write）
事件来源	srcRegion	String	是	资源池 id,不区分传入 all
	srcServiceType	String	是	事件来源服务名称（计算、存储、网络、安全）
	srcIp	String	否	事件来源 ip,发起请求的地址
	srcProdTypeName	String	是	事件来源资源的类型名称
	srcProdName	String	是	事件来源资源的名称（产品名称）
	srcResId	String	否	事件操作资源的 id（页面展示的 id）
用户	userId	String	是	用户唯一标识
	accountId	String	是	主账号 id
操作数据	reqId	String	是	操作请求 id
	reqData	String	是	请求数据，格式为 json 字符串，get 请求传请求链接就行
	respData	String	否	操作响应数据，格式为 json 字符串。
	apiVersion	String	否	API 调用事件对应的 api 版本

事件样例


```
{
"eventId": "66523425",
"eventName": "云主机远程登录",
"eventTime": 1677547897000,
"eventLevel": 0,
"eventType": 1,
"eventActType": 0,
"srcRegion": "aaf589124d5d11eaa04d0242ac110002",
"srcServiceType": "计算",
"srcIp": "",
```

```
"srcProdTypeName": "云主机",
"srcProdName": "ecm-ff0d",
"srcResId": "f7f71805-2ce2-454b-82a1-33de9b92fc01",
"userId": "010cdad75c8e452a866b2cae6534c3d2",
"accountId": "d581e41449ed428c8107ee3e35827e18",
"reqId": "66523425",
"reqData": "{\"resource_name\": \"ecm-ff0d\", \"resource_uuid\": \"f7f71805-2ce2-454b-82a1-33de9b92fc01\"}",
"respData": "0",
"apiVersion": "v1"
}
```


4.5. 配置事件追踪器

约束限制

事件跟踪器仅支持在“合肥 2”、“华北 2”、“杭州 7”区域支持配置。

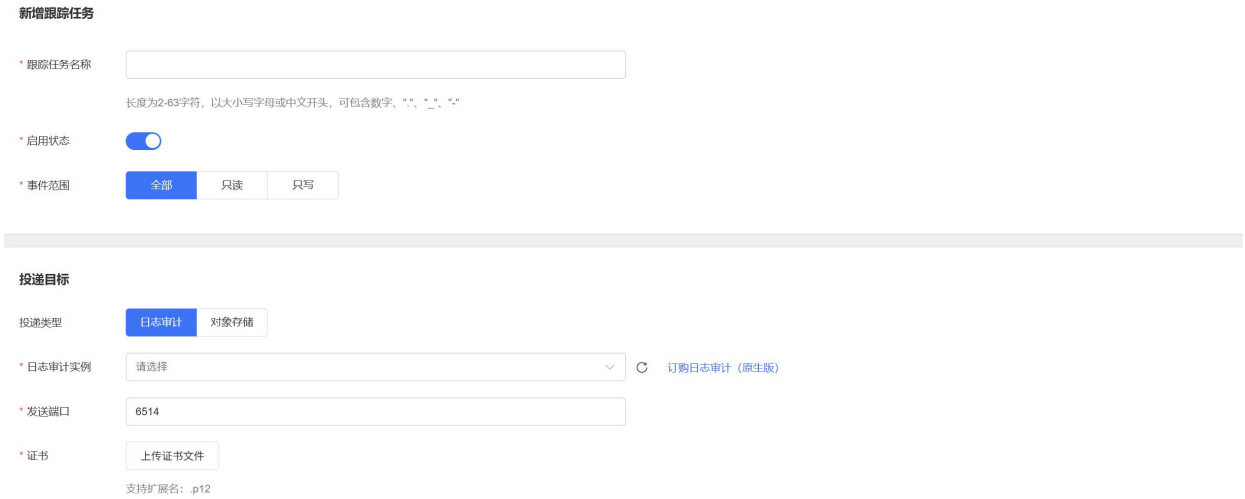
创建事件跟踪并投递至日志审计服务

说明：

云审计目前仅支持投递至 v3.0.1 版本的日志审计服务中，若您的版本低于 v3.0.1 可提交工单升级。

1. 进入云审计服务控制台。
2. 在左侧导航栏选择“事件跟踪”，进入“事件跟踪”页面。
3. 单击左上角的“创建跟踪任务”，进入“新建事件跟踪”页面并填写相关参数。

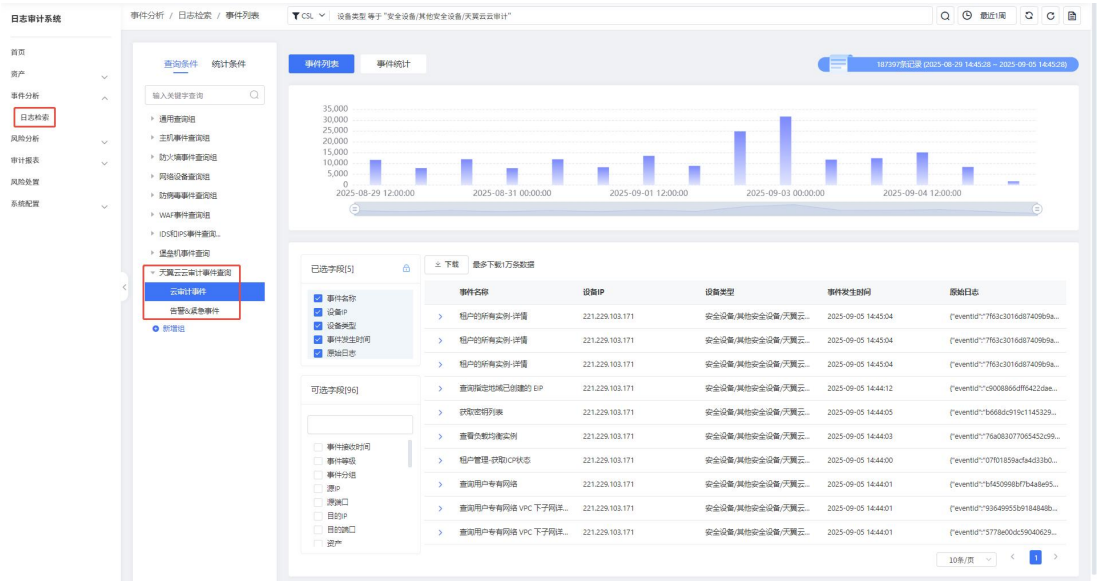
参数	填写说明
跟踪任务名称	填写跟踪任务的相关名称。长度为 2-63 字符，以大小写 字母或中文开头，可包含数字、"."、"_"、"-"。
启用状态	选择跟踪任务的启用状态。
事件范围	跟踪任务记录的事件范围，可选“全部”、“只 读”和“可选”。
投递类型	选择投“日志审计”。
日志审计实例	选择需要投放日志审计实例。
发送端口	日志审计待发送的端口。 注意： 默认值为 6514，需要与日志审计配置中保持一致。
证书	上传在日志审计中下载的证书，仅支持.p12 格式。



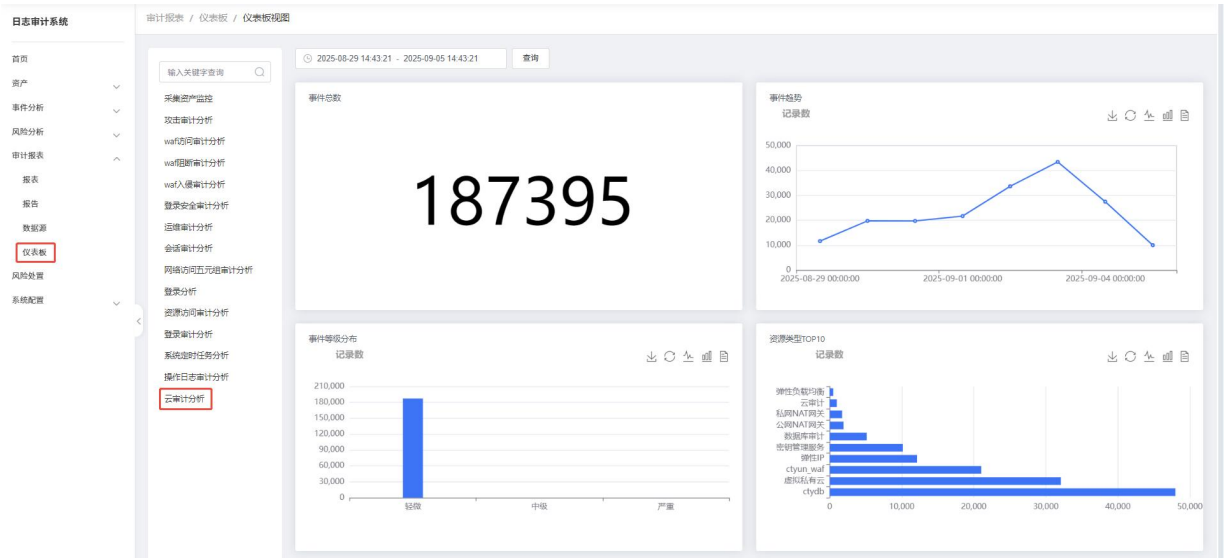
4. 配置完成后单击“确定”，完成事件跟踪配置。

5. 配置完成后，即可在日志审计（原生版）控制台查看云审计事件。

   - 查询日志：在“事件分析 > 日志检索”页面，支持通过列表和统计图的方式查看日志数据。详细操作请 参见日志检索-日志审计（原生版）。



   - 查看仪表板：在“审计报表 > 仪表版”页面，可以查看所选时间范围内的全景视图，通过可视化方式展 示统计数据，包括事件总数、事件趋势、事件等级分布、资源类型 TOP10 信息。



创建事件跟踪并投递至对象存储服务

说明：

云审计日志转存至对象存储服务仅支持在“合肥 2”、“华北 2”、“杭州 7”区域支持配置，转存日志涵盖所有 一类资源池的数据。

1. 进入云审计服务控制台。
2. 在左侧导航栏选择“事件跟踪”，进入“事件跟踪”页面。
3. 单击左上角的“创建跟踪任务”，进入“新建事件跟踪”页面并填写相关参数。

参数	填写说明
跟踪任务名称	填写跟踪任务的相关名称。长度为 2-63 字符，以大小写 字母或中文开头，可包含数字、"."、"_"、"-"。
启用状态	选择跟踪任务的启用状态。
事件范围	跟踪任务记录的事件范围，可选“全部”、“只 读”和“可选”。
投递类型	选择投“对象存储”。
ZOS 存储桶	选择需要投放的 ZOS 桶。
目录前缀	投递 ZOS 桶的目录下，目录前缀已非“/”开头

4. 配置完成后单击“确定”，完成事件跟踪配置。

编辑事件跟踪

1. 进入云审计服务控制台。
2. 在左侧导航栏选择“事件跟踪”，进入“事件跟踪”页面。
3. 找到待编辑的事件，选择“操作”列的“编辑”。
4. 在编辑页面修改相关内容后，单击“确定”完成修改。

删除事件跟踪

1. 进入云审计服务控制台。
2. 在左侧导航栏选择“事件跟踪”，进入“事件跟踪”页面。
3. 找到待删除的事件，选择“操作”列的“删除”。
4. 在弹出的对话框中，单击“确认”完成事件删除。

5. 最佳实践

5.1. 查看云产品的操作记录

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。本文为您介绍如何通过云审计查看云资源的操作记录。

前提条件

已开通云审计服务。

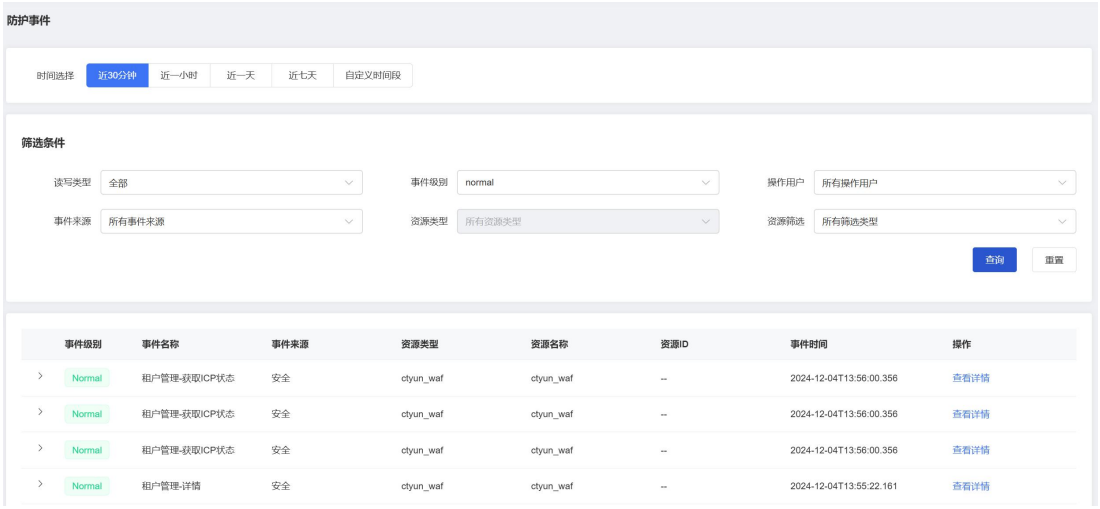
操作步骤

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. 在控制台列表页，选择“云审计”。
4. 进入云审计控制台后，点击侧边栏“事件列表”。
5. 进入事件列表页面，事件列表上方支持通过筛选条件查询。

云审计支持五个维度的组合查询，说明如下：

- 时间筛选：支持快速点选近 30 分钟、近 1 小时、近 1 天、近 7 天的时间范围，也支持自定义时间范围。
- 读写类型：支持根据事件的读写类型进行筛选。
- 事件级别：支持根据事件等级进行筛选，当前事件等级包括 normal（代表本次操作成功）、warning（代 表本次操作失败）。
- 操作用户：支持根据同一租户下的不同主子账号进行筛选。
- 事件来源、资源类型、资源筛选：支持以资源维度进行多层级的筛选，最细粒度支持具体某个资源实例 的筛选。

6. 筛选条件选择完成，点击“查询”，符合条件的事件将以列表显示出来。



6. 常见问题

云审计服务如何收费？

云审计服务支持免费使用。

云审计服务如何开通？

云审计为 region 级服务，您需要分别在云资源所在的资源池开通云审计服务，才能使用云审计服务。

事件列表用于记录哪些信息？

事件列表记录了云账户中对云服务资源新建、修改、删除等操作的详细信息。

事件列表中的信息可以删除吗？

不可以，根据 SAC/TC 及国际信息、数据安全管理部门发布的规范，审计日志必须保持客观全面、准确，因此不提供删除或修改功能。

事件文件可以存储多长时间？

默认情况下，云审计服务管理控制台可存储最近 7 天内的事件文件，而对于已保存至 ZOS 桶的历史操作记录，您可以无限期存储这些事件文件。

启用云审计服务是否会影响其他云服务资源的性能？

不会。启用云审计服务不会影响其他云服务资源的性能。