

# 云审计

# 目录

## 产品介绍

产品定义.....	2
产品优势.....	2
功能特性.....	3
相关术语解释.....	3
应用场景.....	3
使用限制.....	3

## 计费说明

计费模式.....	5
-----------	---

## 快速入门

开通云审计服务.....	6
查看审计事件.....	7

## 用户指南

查看审计事件.....	9
支持审计的云产品及关键操作列表.....	10
支持审计的关键操作.....	21
审计服务事件参考.....	23
配置事件追踪器.....	24
IAM权限管理.....	28

## 最佳实践

查看云产品的操作记录.....	30
-----------------	----

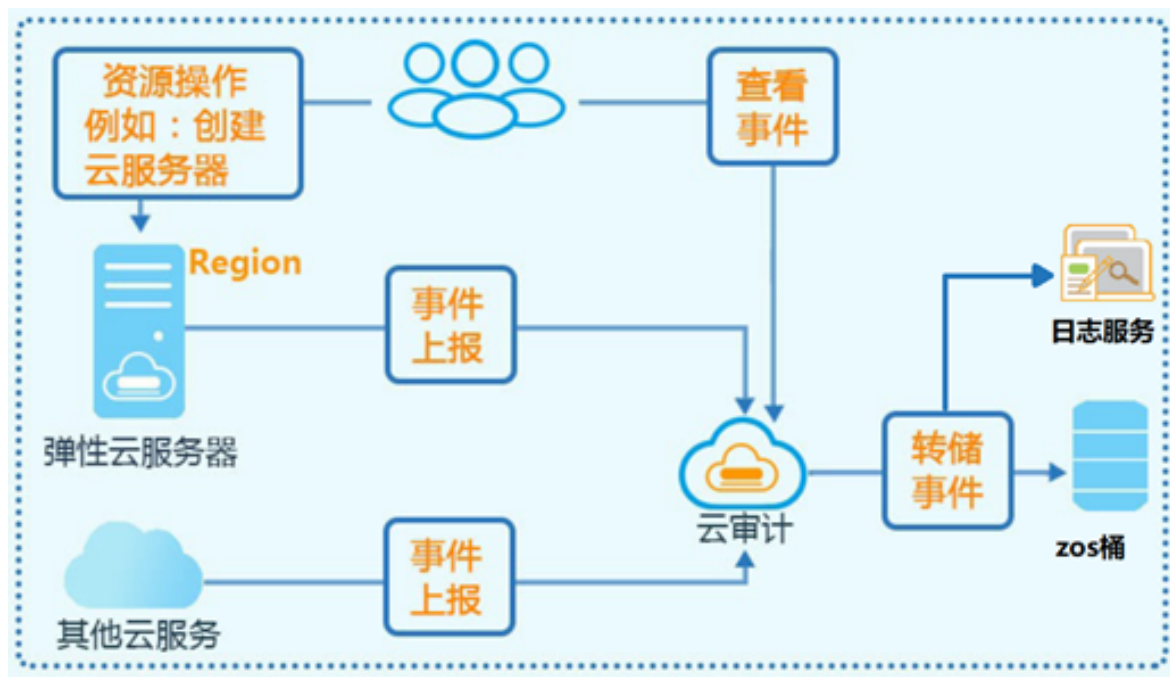
## 常见问题

常见问题.....	32
-----------	----

# 产品介绍

## 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。



## 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。

# 产品介绍

## 功能特性

### 记录审计日志

支持记录用户通过管理控制台发起的操作，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。

## 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实现180天以上存储。支持用户选择投递事件类型范围、投递目标等。

## 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。

## 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

# 产品介绍

限制事件	限制规格
用户操作后多久可以通过云审计查询到数据	<ul style="list-style-type: none"><li>• 管理类事件：1分钟</li><li>• 数据类事件：5分钟</li></ul>
用户通过云审计能查询到多久前的操作事件	7天

## 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。

## 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，并且完成实名认证。

### 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”。



## 快速入门

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。

### 开通云审计服务



产品名称： 云审计服务

计费类型： 云审计服务免费使用

我已阅读，理解并接受 [《天翼云云审计服务协议》](#)

取消

立即购买

## 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”。

# 快速入门

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。

### 防护事件

时间选择 近30分钟 近一小时 近一天 近七天 自定义时间段

**筛选条件**

读写类型	<input type="text" value="请选择"/>	事件级别	<input type="text" value="请选择"/>	操作用户	<input type="text" value="请选择"/>
事件来源	<input type="text" value="所有事件来源"/>	资源类型	<input type="text" value="所有资源类型"/>	资源筛选	<input type="text" value="所有筛选类型"/>

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。

### 防护事件

时间选择 近30分钟 近一小时 近一天 近七天 自定义时间段

**筛选条件**

读写类型	<input type="text" value="全部"/>	事件级别	<input type="text" value="normal"/>	操作用户	<input type="text" value="所有操作用户"/>
事件来源	<input type="text" value="所有事件来源"/>	资源类型	<input type="text" value="所有资源类型"/>	资源筛选	<input type="text" value="所有筛选类型"/>

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	租户管理-获取ICP状态	安全	ctyun_waf	ctyun_waf	--	2024-12-04T13:56:00.356	<a href="#">查看详情</a>
> Normal	租户管理-获取ICP状态	安全	ctyun_waf	ctyun_waf	--	2024-12-04T13:56:00.356	<a href="#">查看详情</a>
> Normal	租户管理-获取ICP状态	安全	ctyun_waf	ctyun_waf	--	2024-12-04T13:56:00.356	<a href="#">查看详情</a>
> Normal	租户管理-详情	安全	ctyun_waf	ctyun_waf	--	2024-12-04T13:55:22.161	<a href="#">查看详情</a>

## 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。

The screenshot shows the '防护事件' (Protection Events) section of the Cloud Audit console. At the top, there is a '时间选择' (Time Selection) area with buttons for '近30分钟' (Near 30 minutes), '近一小时' (Near 1 hour), '近一天' (Near 1 day), '近七天' (Near 7 days), and '自定义时间段' (Custom time range). Below this is the '筛选条件' (Filter Conditions) section, which includes six dropdown menus: '读写类型' (Read/Write Type) set to '请选择' (Please select), '事件级别' (Event Level) set to '请选择' (Please select), '操作用户' (Operation User) set to '请选择' (Please select), '事件来源' (Event Source) set to '所有事件来源' (All event sources), '资源类型' (Resource Type) set to '所有资源类型' (All resource types), and '资源筛选' (Resource Filter) set to '所有筛选类型' (All filter types). At the bottom right of the filter section are two buttons: '查询' (Query) and '重置' (Reset).

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。

# 用户指南

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。

防护事件

时间选择 近30分钟 近一小时 近一天 近七天 自定义时间段

筛选条件

读写类型 全部 事件级别 normal 操作用户 所有操作用户

事件来源 所有事件来源 资源类型 所有资源类型 资源筛选 所有筛选类型

查询 重置

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	租户管理-获取ICP状态	安全	ctyun_waf	ctyun_waf	--	2024-12-04T13:56:00.356	<a href="#">查看详情</a>
> Normal	租户管理-获取ICP状态	安全	ctyun_waf	ctyun_waf	--	2024-12-04T13:56:00.356	<a href="#">查看详情</a>
> Normal	租户管理-获取ICP状态	安全	ctyun_waf	ctyun_waf	--	2024-12-04T13:56:00.356	<a href="#">查看详情</a>
> Normal	租户管理-详情	安全	ctyun_waf	ctyun_waf	--	2024-12-04T13:55:22.161	<a href="#">查看详情</a>

## 支持审计的云产品及关键操作列表

### 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

# 用户指南

操作事件	字段
续订物理机	renew_bm_server
退订物理机	refund_bm_server

## 镜像服务

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

## 存储

分类	云产品	支持审计的关键操作列表
存储	云硬盘	<a href="#">云硬盘支持的关键操作列表</a>
	云硬盘备份	<a href="#">云硬盘备份支持的关键操作列表</a>
	对象存储	<a href="#">对象存储支持的关键操作列表</a>
	海量文件服务OceanFS	<a href="#">海量文件服务OceanFS支持的关键操作列表</a>
	云主机备份	<a href="#">云主机备份支持的关键操作列表</a>
	并行文件服务 HPFS	<a href="#">并行文件服务 HPFS支持的关键操作列表</a>

## 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	操作事件
负载均衡器	查看负载均衡器列表
	查看负载均衡器详情
	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

# 用户指南

资源类型	操作事件
证书	修改后端主机
	查看证书列表
	查看证书详情
	创建证书
	修改证书
访问策略组	删除证书
	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

# 用户指南

操作事件	字段名称
解绑ipv6带宽	unbind_ipv6

## NAT网关

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

# 用户指南

事件名称	事件的读写类型	srcProdName、srcResId
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
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

# 用户指南

事件来源	资源类型	事件名称
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
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

# 用户指南

事件来源	资源类型	事件名称
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
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

# 用户指南

事件来源	资源类型	事件名称
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
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

# 用户指南

事件来源	资源类型	事件名称
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
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

## 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	<a href="#">云容器引擎支持的关键操作列表</a>
	容器镜像服务	<a href="#">容器镜像服务支持的关键操作列表</a>
	分布式消息服务Kafka	<a href="#">分布式消息服务Kafka支持的关键操作列表</a>
	弹性容器实例	<a href="#">弹性容器实例服务支持的关键操作列表</a>

## 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	<a href="#">关系型数据库MySQL版服务支持的关键操作列表</a>
	关系型数据库PostgreSQL版服务	<a href="#">关系型数据库PostgreSQL版服务支持的关键操作列表</a>
	关系型数据库SQL Server版	<a href="#">关系型数据库SQL Server版服务支持的关键操作列表</a>
	分布式关系型数据库	<a href="#">分布式关系型数据库支持的关键操作列表</a>
	文档数据库服务	<a href="#">文档数据库服务支持的关键操作列表</a>
	分布式缓存服务Redis版	<a href="#">分布式缓存服务Redis版支持的关键操作列表</a>
	数据传输服务DTS	<a href="#">数据传输服务DTS支持的关键操作列表</a>

# 用户指南

## 大数据

分类	云产品	支持审计的关键操作列表
大数据	翼MapReduce	<a href="#">翼MapReduce服务支持的关键操作列表</a>
	云搜索服务	<a href="#">云搜索服务支持的关键操作列表</a>

## 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）	<a href="#">Web应用防火墙（原生版）支持的关键操作列表</a>
	密钥管理	<a href="#">密钥管理服务支持的关键操作列表</a>
	数据库审计	<a href="#">数据库审计支持的关键操作列表</a>
	云审计	<a href="#">云审计服务支持审计的关键操作列表</a>
	云安全中心	<a href="#">云安全中心支持的关键操作列表</a>
	云等保专区	<a href="#">云等保专区支持的关键操作列表</a>
	服务器安全卫士（原生版）	<a href="#">服务器安全卫士（原生版）支持的关键操作列表</a>

## 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	<a href="#">云监控服务支持的关键操作列表</a>

## 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）	<a href="#">专属云（计算独享型）支持审计的关键操作列表</a>

## 管理工具

### 统一身份认证（一类节点）

事件来源	资源类型	事件名称
安全	统一身份认证（一类节点）	编辑子用户
		删除子用户
		创建AccessKey
		从回收站中彻底删除AccessKey
		用户-添加到用户组
		创建子用户
		删除用户组
		用户组管理
		编辑用户组

# 用户指南

事件来源	资源类型	事件名称
		授权管理-删除授权
		删除自定义策略
		委托-解除IAM授权
		删除委托
		用户登录设置-设置密码
		企业项目为用户组设置策略
		用户组授权
		为单个用户授权策略
		为委托授权策略
		为委托解除授权
		为委托设置企业项目权限
		为委托取消企业项目权限

## 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

## 支持审计的关键操作

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。

# 用户指南

## 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
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。

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: 请选择 | 事件级别: 请选择 | 操作用户: 请选择

**事件来源: 管理与部署** | **资源类型: 云审计** | 资源筛选: 所有筛选类型

事件名称: 请选择

[查询](#) [重置](#)

#### 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	查询筛选事件的条件...	管理与部署	云审计	云审计控制台	--	2025-09-12T14:29:09.210	<a href="#">查看详情</a>
> Normal	查询筛选事件的条件...	管理与部署	云审计	云审计控制台	--	2025-09-12T14:29:06.001	<a href="#">查看详情</a>
> Normal	查询事件列表	管理与部署	云审计	云审计控制台	--	2025-09-12T14:29:02.988	<a href="#">查看详情</a>
> Normal	查询筛选事件的条件...	管理与部署	云审计	云审计控制台	--	2025-09-12T14:29:02.350	<a href="#">查看详情</a>

## 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
	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 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"
}
```

## 配置事件追踪器

### 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。

# 用户指南

参数	填写说明
发送端口	日志审计待发送的端口。 <b>注意</b> 默认值为6514，需要与 <a href="#">日志审计配置</a> 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。

## 新增跟踪任务

\* 跟踪任务名称

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

\* 事件范围

## 投递目标

投递类型

\* 日志审计实例

\* 发送端口

\* 证书

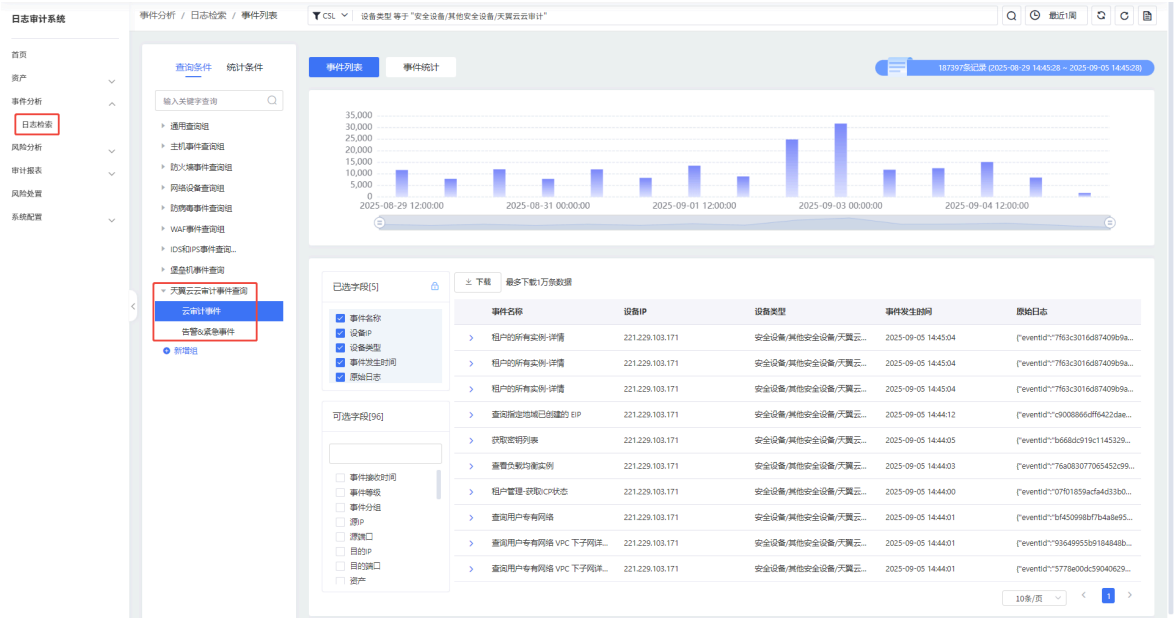
支持扩展名: .p12

4. 配置完成后单击“确定”，完成事件跟踪配置。

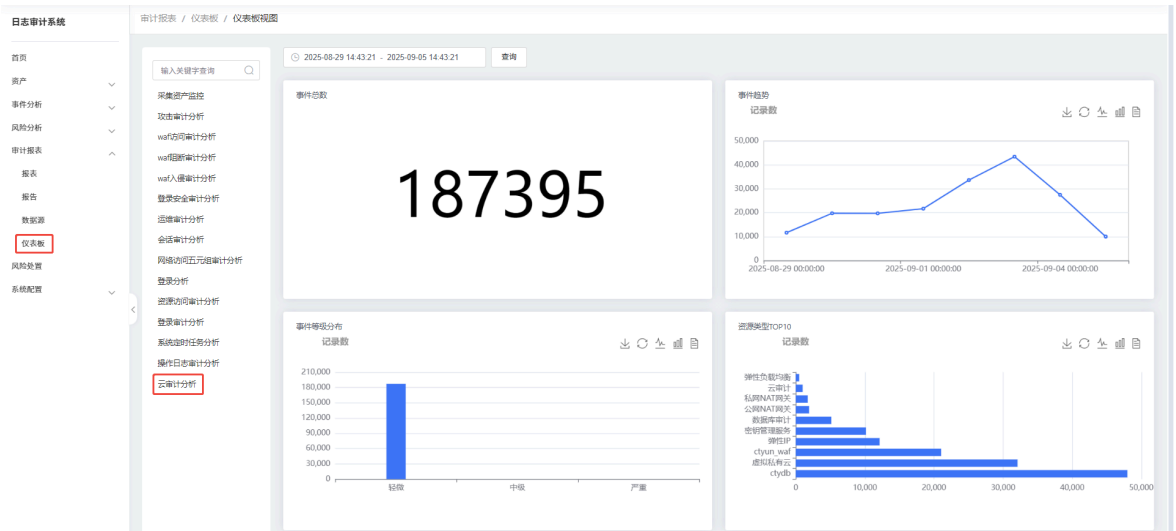
# 用户指南

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）](#)。



- 查看仪表盘：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。



# 用户指南

## 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

### 新增跟踪任务

\* 跟踪任务名称

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

\* 事件范围

### 投递目标

投递类型

\* ZOS存储桶

\* 目录前缀

### 系统授权

启用状态

创建投递任务前，须进行ZOS桶写入角色授权。 [去授权](#)，授权成功后自动刷新

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。

## IAM权限管理

本文为您介绍云审计的权限管理能力，支持通过IAM实现对云审计的访问控制、权限分配。

云审计通过IAM（统一身份认证服务，Identity and Access Management）对用户权限进行管理，IAM可以帮助用户安全地控制云审计服务的访问及操作权限。

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。

## 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。

## 云审计IAM策略说明

天翼云为云审计提供如下**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
cloudaudit-admin	云审计管理员策略。	系统策略	全局
cloudaudit-viewer	云审计查看策略。	系统策略	全局
cloudaudit-auditor	云审计审计员策略。	系统策略	全局

## 云审计权限及授权项

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。

# 用户指南

- 权限类型：授权操作对应的读写类型。

权限	授权项	权限类型 (读/写)	cloudaudit- admin	cloudaudit- viewer	cloudaudit-auditor
服务开通	cloudaudit:user:create	写	✓	×	×
服务开通状态 查询	cloudaudit:user:enable	读	✓	✓	✓
查询事件列表	cloudaudit:eventList:select	读	✓	✓	✓
查询事件条件 列表	cloudaudit:eventSelection:select	读	✓	✓	✓
新建跟踪任务	cloudaudit:trackTask:create	写	✓	×	×
删除跟踪任务	cloudaudit:trackTask:delete	写	✓	×	×
查询跟踪任务	cloudaudit:trackTask:select	读	✓	✓	✓
修改跟踪任务	cloudaudit:trackTask:update	写	✓	×	×
查询任务列表	cloudaudit:trackTaskList:select	读	✓	✓	✓
获取用户授权 信息	cloudaudit:userAuthority:select	读	✓	✓	✓
保存授权凭据	cloudaudit:userArn:create	写	✓	×	×

## 通过IAM授权使用云审计

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](#)

## 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。

The screenshot shows the '防护事件' (Protection Events) section of the Cloud Audit console. At the top, there is a '时间选择' (Time Selection) area with buttons for '近30分钟' (Near 30 minutes), '近一小时' (Near 1 hour), '近一天' (Near 1 day), '近七天' (Near 7 days), and '自定义时间段' (Custom time range). Below this is the '筛选条件' (Filtering Conditions) section, which includes six dropdown menus: '读写类型' (Read/Write Type), '事件级别' (Event Level), '操作用户' (Operation User), '事件来源' (Event Source), '资源类型' (Resource Type), and '资源筛选' (Resource Selection). The '读写类型' dropdown is currently set to '请选择' (Please select). The '事件级别' dropdown is also set to '请选择'. The '操作用户' dropdown is set to '请选择'. The '事件来源' dropdown is set to '所有事件来源' (All event sources). The '资源类型' dropdown is set to '所有资源类型' (All resource types). The '资源筛选' dropdown is set to '所有筛选类型' (All selection types). At the bottom right of the filtering section, there are two buttons: '查询' (Query) and '重置' (Reset).

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。

# 最佳实践

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。

防护事件

时间选择 **近30分钟** 近一小时 近一天 近七天 自定义时间段

筛选条件

读写类型 全部 事件级别 normal 操作用户 所有操作用户

事件来源 所有事件来源 资源类型 所有资源类型 资源筛选 所有筛选类型

[查询](#) [重置](#)

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	租户管理-获取ICP状态	安全	ctyun_waf	ctyun_waf	--	2024-12-04T13:56:00.356	<a href="#">查看详情</a>
> Normal	租户管理-获取ICP状态	安全	ctyun_waf	ctyun_waf	--	2024-12-04T13:56:00.356	<a href="#">查看详情</a>
> Normal	租户管理-获取ICP状态	安全	ctyun_waf	ctyun_waf	--	2024-12-04T13:56:00.356	<a href="#">查看详情</a>
> Normal	租户管理-详情	安全	ctyun_waf	ctyun_waf	--	2024-12-04T13:55:22.161	<a href="#">查看详情</a>

## 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。