云审计

用户使用指南

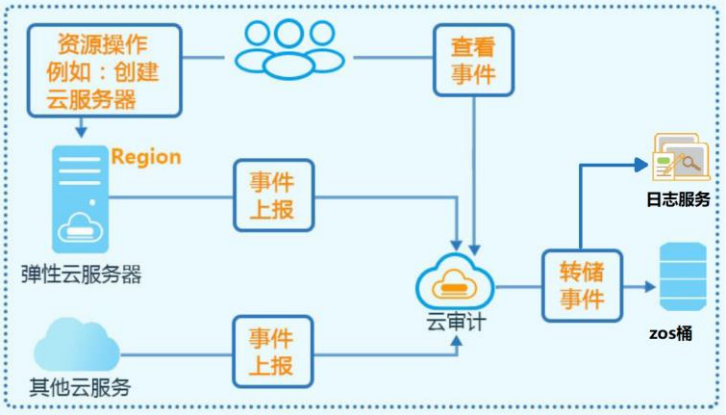
天翼云科技有限公司

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，关键操作可邮件、短信通知。

- 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。

2. 快速入门

2.1. 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“进入控制台”；

3. 进入云审计控制台，初次使用会显示欢迎使用页面，点击“立即开通”；

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

2.2. 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. 单机管理控制台右上方的 南京3 ，选择地域；
3. 在控制台列表页，选择“云审计”；
4. 进入日志服务控制台后，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。

3. 用户指南

3.1. 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. 单机管理控制台右上方的 南京3 ，选择地域；
3. 在控制台列表页，选择“云审计”；
4. 进入日志服务控制台后，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。

3.2. 支持审计的云产品及关键操作列表

云审计支持记录的云产品包括： 云主机、云硬盘、镜像服务、物理机、弹性伸缩、弹性公网 IP、弹性负载均衡、NAT 网关、虚拟私有云、云监控。

- 弹性云主机的关键操作列表

```
vm_op_list = ['restart_all_server', 'remove_nic', 'bind_ip',
'rebuild_server','restart_server', 'detach_volume', 'start_server', 'refund_server',
'stop_server','create_server', 'add_nic', 'import_keypair', 'start_all_server',
'change_firewall','unbind_ip', 'remove_firewall', 'renew_server',
'create_gpu_server','change_server_password', 'delete_keypair', 'create_keypair',
'attach_volume','get_server_vnc','delete_server', 'resize_server', 'stop_all_server']
```

- 云主机组的关键操作列表

```
OS_ASYNC_LIST = ["create_server", "delete_server", "resize_server", "start_server",
"stop_server", "reboot_server","rebuild_server", "change_server_password",
"create_server_interface", "delete_port","get_server_vnc", "create_keypair",
"delete_keypair","upload_volume_image", "delete_image","create_volume", "delete_volume",
"attach_volume_to_server", "detach_volume_from_server","extend_volume", "create_backup",
"delete_backup", "backup_restore","create_ip", "delete_ip", "add_floating_ip_to_server",
"remove_floating_ip_from_server","update_ip","create_network", "delete_network",
"update_network","create_subnet", "delete_subnet", "update_subnet","create_security_group",
"delete_security_group","create_security_group_rule",
"delete_security_group_rule","create_load_balancer", "create_listener","create_instances",
"create_floating_ip_port_forwarding","create_firewall_group", "create_floating_ip_snat",
"add_ip_pool_address","delete_ip_pool_address",]
```

- 弹性伸缩的关键操作列表

```
instance_protect_op_list = ['enable_instance_protect', 'disable_instance_protect']
```

```
scaling_rule_op_list = ['create_scaling_rule', 'disable_scaling_rule',
'execute_scaling_rule','update_scaling_rule', 'delete_scaling_rule', 'enable_scaling_rule']
scaling_group_op_list = ['create_scaling_group', 'update_scaling_group',
'disable_scaling_group','delete_scaling_group', 'enable_scaling_group', 'move_out_group',
'move_in_group','move_out_group_release']
scaling_op_list = instance_protect_op_list + scaling_rule_op_list + scaling_group_op_list
```

- 物理机服务的关键操作列表

```
bm_op_list = ['get_bm_server_vnc', 'stop_bm_server', 'refund_bm_server','create_bm_server',
'restart_bm_server','start_bm_server', 'rebuild_bm_server', 'change_bm_server_password',
'renew_bm_server','bind_bm_floating', 'unbind_bm_floating']
```

- 镜像服务的关键操作列表

```
image_op_list = ['create_private_image', 'cancel_share_image', 'accept_share_image',
'share_image','delete_private_image', 'reject_share_image', 'update_private_image']
```

- 云硬盘的关键操作列表

```
volume_op_list = ['detach_volume', 'refund_volume', 'renew_volume', 'attach_volume',
'create_volume','delete_volume', 'resize_volume']
```

- 弹性公网 IP 的关键操作列表

```
floating_op_list = ['bind_ip', 'create_ipv6', 'bind_ipv6', 'renew_ipv6', 'resize_ip',
'refund_ip', 'refund_ipv6','unbind_ip', 'renew_ip', 'resize_ipv6', 'create_ip',
'unbind_ipv6']
```

- 弹性负载均衡的关键操作列表

```
lb_op_list = ['lb_assign_server', 'delete_vm_pool', 'delete_listener', 'lb_remove_server',
'create_listener','delete_lb', 'create_lb', 'update_listener', 'update_vm_pool',
'lb_bind_ip', 'lb_unbind_ip','lb_bind_ipv6', 'lb_unbind_ipv6']
```

- NAT 网关的关键操作列表

```
nat_op_list = ['refund_nat', 'renew_nat', 'delete_dnat', 'delete_snat', 'create_nat',
'create_snat', 'create_dnat','update_nat']
```

- 虚拟私有云的关键操作列表

```
vpc_op_list = ['bind_vip', 'update_subnet', 'disable_acl_rule', 'update_vpc',
'create_ingress_acl_rule','update_firewall', 'create_egress_acl_rule',
'create_firewall_rule', 'delete_ingress_acl_rule','delete_vpc', 'delete_egress_acl_rule',
'delete_firewall_rule', 'change_egress_acl_rule','unbind_vip', 'delete_acl',
'create_acl_rule', 'create_vpc', 'delete_subnet', 'create_firewall','create_vip',
'create_subnet', 'enable_acl_rule', 'delete_firewall',
'change_ingress_acl_rule','delete_vip', 'create_acl', 'update_security_group',
'create_security_group','delete_security_group', "create_firewall_group", "delete_acl",
"enable_acl", "disable_acl"]
```

- 云监控的关键操作列表

```
alarm_rule_op_list = ['enable_alarm_rule', 'delete_alarm_rule', 'create_alarm_rule',
'disable_alarm_rule','update_alarm_rule']
contacts_group_op_list = ['create_contacts_group', 'delete_contacts_group',
'update_contacts_group']
contacts_op_list = ['create_contacts', 'delete_contacts', 'update_contacts']
template_op_list = ['create_template', 'update_template', 'delete_template']
collect_board_op_list = ['create_collect_board', 'delete_collect_board']
```

3.3. 审计服务事件参考

事件结构

字段名	含义
id	事件 ID
eventId	请求 ID
eventName	操作事件名称
eventTime	事件发生时间（触发时间）
eventLevel	事件级别，操作事件等级，分为二级： 0：normal，代表本次操作成果 1：warning，代表本次操作失败

eventType	发生的事件类型，当前云审计仅记录部分控制台或售卖页的管控事件（ConsoleOperation）
eventActType	事件的读写类型。取值： 0：读类型（read） 1：写类型（write）
srcRegion	操作事件发生所在的资源池 ID
srcServiceType	事件来源服务名称，如计算、存储、网络、安全等
srcIp	事件来源 ip,发起请求的地址
srcProdTypeName	事件来源资源对应的产品名称
srcProdName	事件来源对应的资源名称
srcResId	事件来源对应的资源 ID
accountId	租户 ID，租户的唯一标识
reqId	操作请求 ID
reqData	操作请求数据，格式为 json 字符串
respData	操作响应数据，格式为 json 字符串
apiVersion	操作事件对应的 api 版本
createTime	操作审计事件创建时间
updateTime	操作审计事件更新时间

事件样例


```
{
    "id": "6b231dfb9f684d65a9bf5f53a3d7f828",
    "eventId": "58160545",
    "eventName": "create_volume",
    "eventTime": "2022-12-17 14:52:55",
    "eventLevel": {
        "code": "0",
        "value": "normal"
```

```
        },
        "eventType": {
            "code": "1",
            "value": "部分控制台或售卖页的管控事件（ConsoleOperation）"
        },
        "eventActType": {
            "code": "1",
            "value": "写类型"
        },
        "srcRegion": "d8d23b1e44ad11e9accd0242ac110002",
        "srcServiceType": "存储",
        "srcIp": "",
        "srcProdTypeName": "云硬盘",
        "srcProdName": "evs-d55c",
        "srcResId": "f9028cd6-5b42-4227-bc67-1e6f8d9fa982",
        "accountId": "532a108316474db4a03e5b3fcc089757",
        "reqId": "58160545",
        "reqData": "{\"resource_name\": \"evs-d55c\", \"resource_uuid\": \"f9028cd6-5b42-
4227-bc67-1e6f8d9fa982\"}",
        "respData": "0",
        "apiVersion": "v1",
        "createTime": "2022-12-17 15:00:04",
        "updateTime": "2022-12-17 15:00:04"
}
```

4. 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 OBS 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。