云审计

产品文档

文档目录

产品简介

产品概述

最近更新时间: 2021-08-25 16:38:58

云审计是一项支持对云平台账号进行监管、合规性检查、操作审核和风险审核的服务。借助云审计，您可以记录日志、持续监控并保留与整个基础设施中操作相关的账号活动。云审计提供云平台账号活动的事件历史记录，这些活动包括通过管理控制台、API 服务、命令行工具和其他服务执行的操作。这一事件历史记录可以简化安全性分析、资源更改跟踪和问题排查工作。

产品优势

最近更新时间: 2021-08-25 16:38:58

为什么选择云平台审计?

优势	为什么选择云平台审计
安全性分析和故障排除	用户获取建行云平台账号后，可通过控制台或 API 登录云平台审计服务，避免用户信息外泄。并且在设置日志内容时，可对内容进行加密处理。借助云审计，您可以通过捕捉特定时段内您的云平台账户所发生更改的全面历史记录，发现并解决安全性和操作性问题。
简化的合规性	借助云审计，您可以自动记录和存储云平台账户中已执行操作的事件日志，从而简化合规性的审核过程，也可以更方便地搜索所有日志数据、识别不合规时间、加快事故调查速度并加快响应审核员请求的速度。
用户与资源活动的可见性	云审计可通过记录云平台相关操作和 API 调用来提高用户和资源活动的可见性。您可以识别调用云平台的用户和账户、发起调用的源 IP 地址及执行调用的时间。

与传统审计工作相比，云审计的优势

优势点	具体描述
高效性	在云审计过程中，用户操作的相关数据存储在云平台中，用户无需再把数据导入自己的办公电脑。通过云服务，将大量原本应由本机进行的计算推送到服务器端，由服务器将计算任务分配到整个云网络的空闲计算机上，迅速得到结果并返还给本地计算机，可以大大节省等待时间。
共享性	收集到用户的各项资料，采集、生成的各种数据，不再分块存储在每位用户手中，而是分类存储在同一个资源平台上；用户通过云审计平台，可以随时查阅云控制平台收集到的各项数据和资料，及时分享审计信息，避免重复劳动。
实时性	用户能够及时了解操作进展情况，并根据实际情况进行查看日志；及时了解自己的操作行为，并将操作过程中遇到的问题及时向管理者反馈：及时地了解相互的工作情况，方便实现线索、方法的共享。

产品功能
操作记录

最近更新时间: 2021-08-25 16:41:57

操作记录功能记录最近365天的云平台 API 或云平台控制台上的所有操作。

- 操作记录列表您可以通过控制台查看操作记录列表，以及对应操作事件时间、用户名、事件名称、资源类型、资源名称等。
- 操作记录详情同时您可以获取单个操作记录详情，包括访问密钥、区域、错误码、事件 ID、事件名称、事件源、事件时间、请求 ID、源 IP 地址、用户名。

应用场景
安全分析

最近更新时间: 2021-08-25 16:41:57

当用户的云账号或资源存在安全问题时，云审计所记录的日志将能帮助用户分析原因。比如，云审计会记录用户的所有账号登录操作，操作时间、源 IP 地址、是否使用多因素认证登录，这些都有详细记录，通过这些记录，用户可以判断账号是否存在安全问题。

资源变更追踪

最近更新时间: 2021-08-25 16:41:57

当用户的资源出现异常变更时，云审计所记录的操作日志将能帮助用户找到原因。比如，当用户发现一台 CVM 实例停机了，用户可以通过云审计找到相应的操作时间、源 IP 地址，以此来分析发起的停机操作。

合规性审计

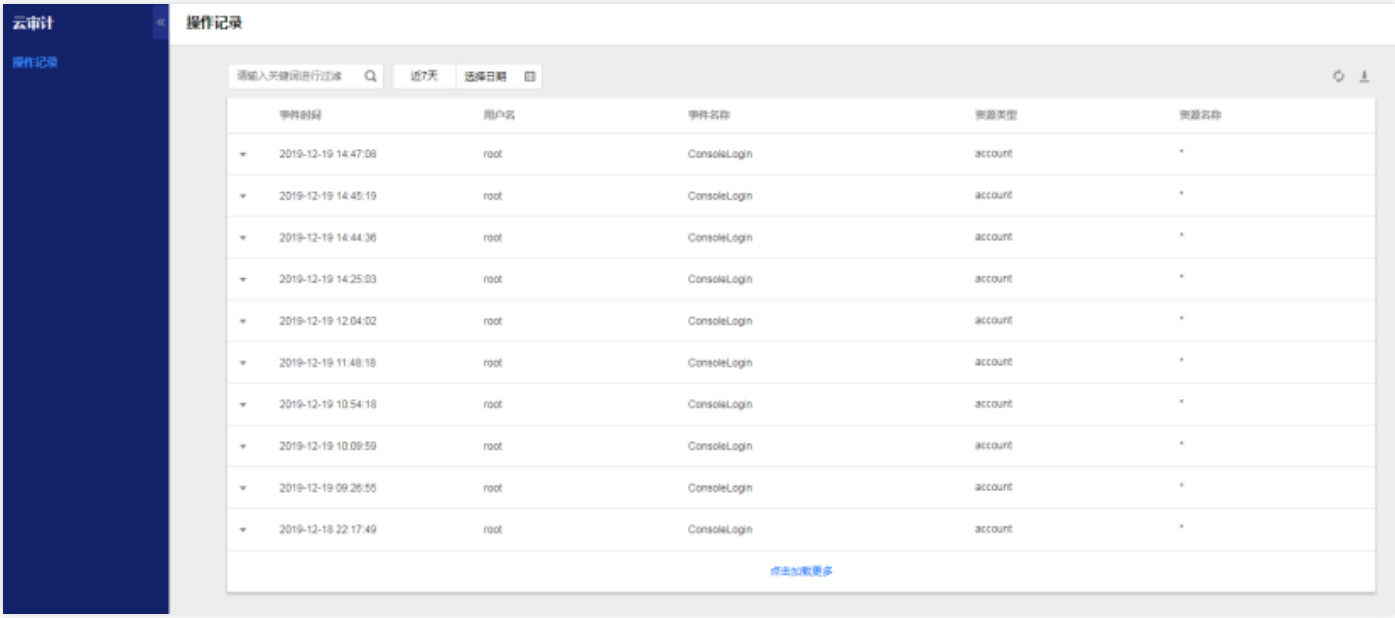
最近更新时间: 2021-08-25 16:41:57

如果用户的组织有多个成员，而且用户已经使用云平台的访问管理-CAM 服务来管理这些成员的身份，那么为了满足用户所在组织的合规新审计需要，用户需要获取每个成员的详细操作记录。云审计所记录的操作事件将能满足这种合规性审计需求。

操作指南
查看操作记录

最近更新时间: 2021-08-25 17:02:02

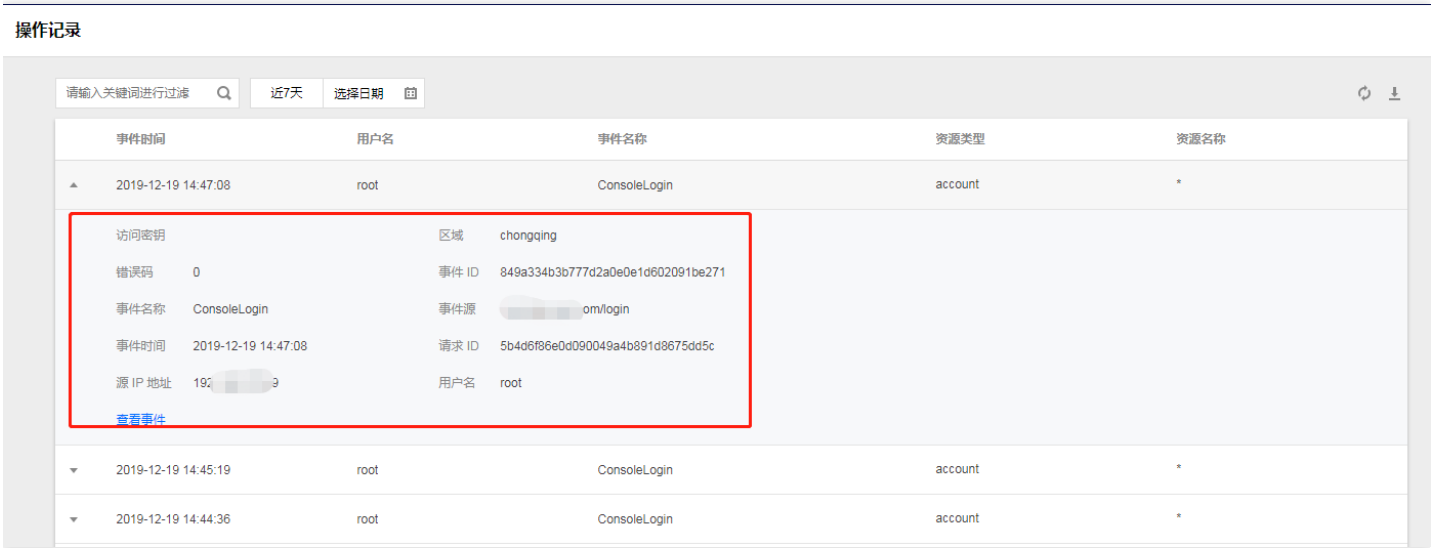
1. 登录云平台，点击【云产品】>【管理与审计】>【云审计】，进入“云审计”界面。
2. 在操作记录页面中，您可以根据用户名、资源类型、资源名称、事件源、事件 ID 、关键词或对应操作事件时间，获取相关的操作记录信息。您可以查询365天以内的操作记录，需要查询的操作记录将会以列表的形式展示出来，需要了解更多的记录可单击【点击加载更多】。可以通过右上角的下载按钮，下载操作记录。



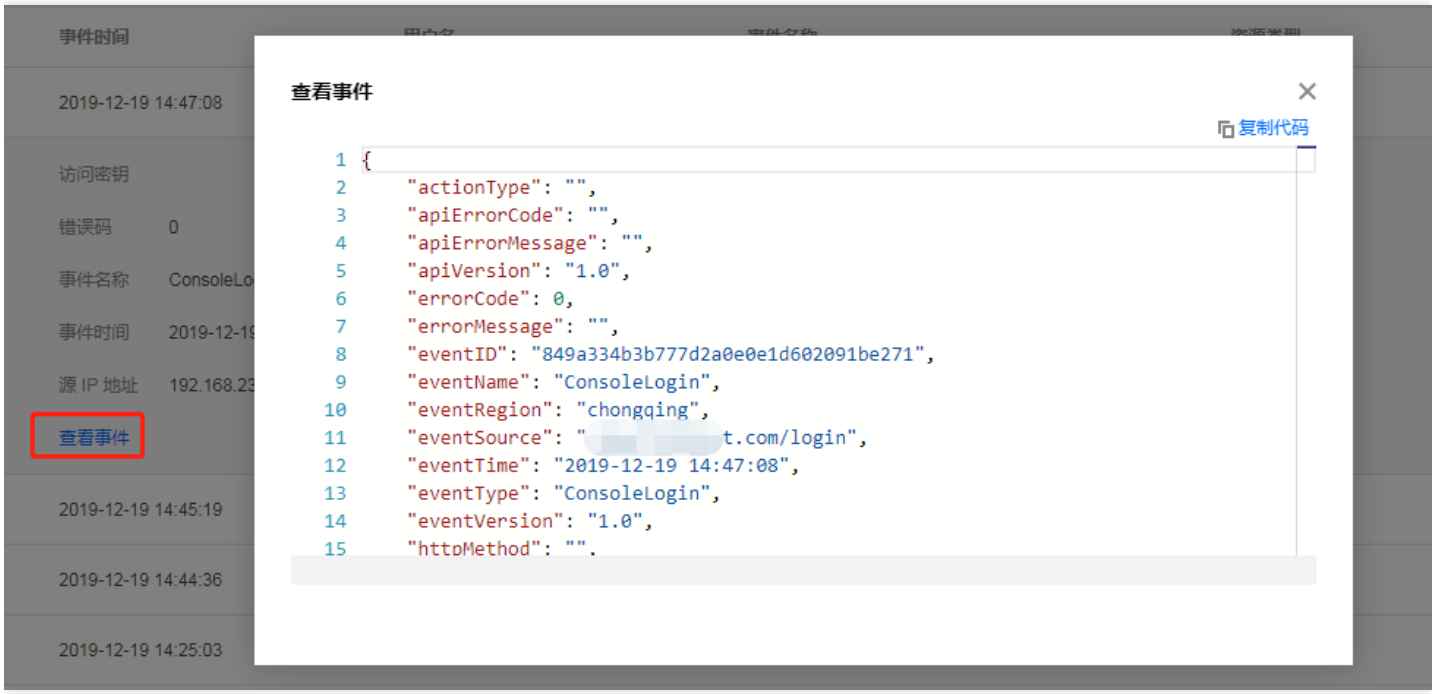
查看详情

最近更新时间: 2021-08-25 17:02:02

1. 您在获取到相关的操作记录列表后，如果想更进一步了解单个操作记录，可以单击该操作记录左侧的【▼】，您就会得到此操作记录的详情，包括访问密钥、区域、错误码、事件 ID 、事件名称、事件源、事件时间、请求 ID 、源 IP 地址、用户名。同时，可以单击【查看事件】，进行了解事件的相关信息。



2. 点击“查看事件”，可以得到相关代码信息。


事件时间
2019-12-19 14:47:08
访问密钥
错误码 0
事件名称 ConsoleLo
事件时间 2019-12-19
源 IP 地址 192.168.23
查看事件
2019-12-19 14:45:19
2019-12-19 14:44:36
2019-12-19 14:25:03
查看事件
复制代码
{
"actionType": "",
"apiErrorCode": "",
"apiErrorMessage": "",
"apiVersion": "1.0",
"errorCode": 0,
"errorMessage": "",
"eventID": "849a334b3b777d2a0e0e1d602091be271",
"eventName": "ConsoleLogin",
"eventRegion": "chongqing",
"eventSource": "t.com/login",
"eventTime": "2019-12-19 14:47:08",
"eventType": "ConsoleLogin",
"eventVersion": "1.0",
"httpMethod": "",

常见问题
一般性问题

最近更新时间: 2021-08-25 16:44:48

什么是云审计?

云审计是一种 Web 服务，可记录在您账号上进行的活动，并将日志文件传送至Elasticsearch系统。

云审计有哪些优势?

云审计可通过记录账号上执行的操作来提供用户活动的可见性。云审计可记录每个操作的重要信息，包括操作事件时间、用户名、事件名称、资源类型、资源名称等。 这些信息能够帮助您跟踪TCE资源的变更情况，帮助您解决操作性问题。

我可以使用哪些搜索筛选条件来查看账号活动?

您可以根据用户名、资源类型、资源名称、事件源、事件 ID 、关键词或对应操作事件时间，获取相关的账号活动。

云审计支持哪些服务?

云审计可支持以下服务：云服务器 CVM ，访问管理 CAM 和账号 Account。

一个操作记录中包含了哪些信息?

一个操作记录包括访问密钥、区域、错误码、事件 ID 、事件名称、事件源、事件时间、请求 ID 、源 IP 地址、用户名。

云审计传送一个 API 调用事件需要多长时间?

一般情况下，云审计会在 API 调用后2 – 5分钟传送操作记录事件到Elasticsearch系统，并可在租户端云审计页面查看到。