**动手实验CLI CloudTrail**

**实验目的**

使用CLI查看CloudTrail事件

**实验要求**

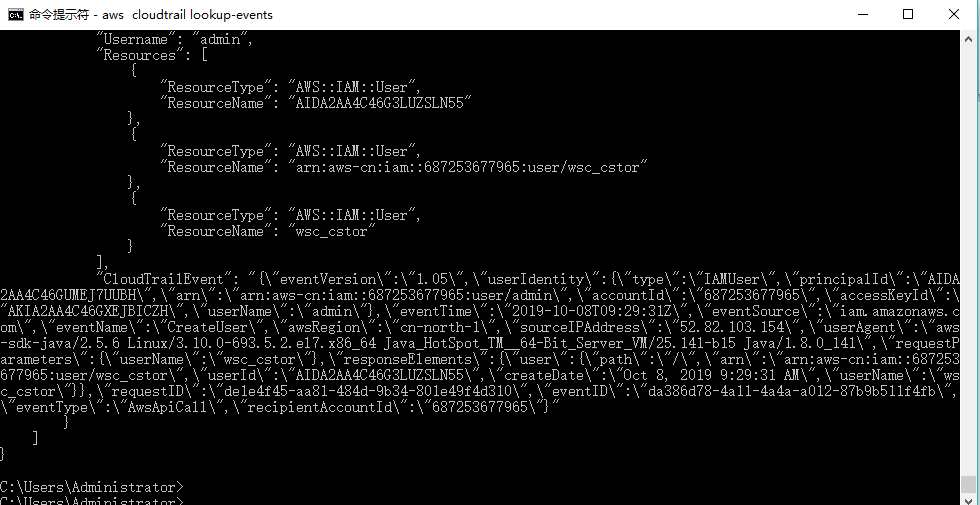
已安装CLI  
了解CloudTrail文档

**实验原理**

AWS CloudTrail是一项AWS服务，可帮助您启用AWS账户的治理，合规性以及运营和风险审计。用户，角色或AWS服务执行的操作在CloudTrail中记录为事件。事件包括在AWS管理控制台，AWS命令行界面以及AWS开发工具包和API中采取的操作。

**实验步骤**

1.点击【开始菜单】，在搜索栏输入【cmd】，然后显示“命令提示符”，我们点击“命令提示符”如下：  


2.首先我们在“命令提示符”中，使用【aws cloudtrail lookup-events】命令查看是个最新事件；如下：  


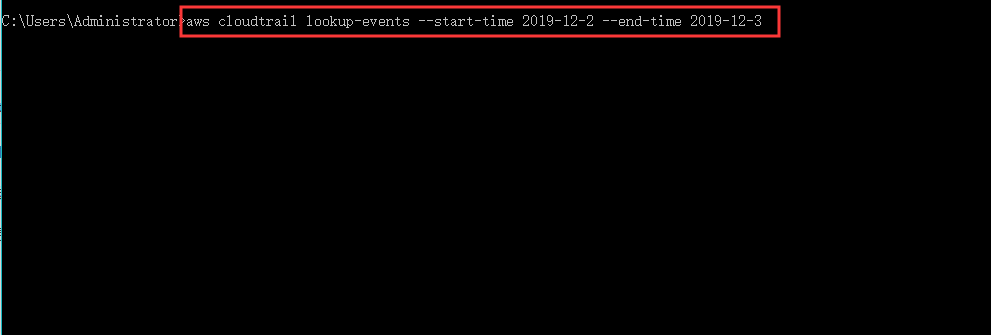
1. 要指定要返回的事件数，使用 【aws cloudtrail lookup-events --max-results 】命令，默认值为10，可能的值为1到50，下面的实例返回一个结果；如图：

aws cloudtrail lookup-events --max-results 1



4．按时间范围查找事件，可以查询过去90天的事件，要指定时间范围，使用【aws cloudtrail lookup-events --start-time --end-time 】命令；如图：

aws cloudtrail lookup-events --start-time 2019-12-2 --end-time 2019-12-3



1. 以下是有效格式的示例。日期，月份和年份的值可以用连字符或正斜杠分隔。如果存在空格，则必须使用双引号。

1422317782

1422317782.0

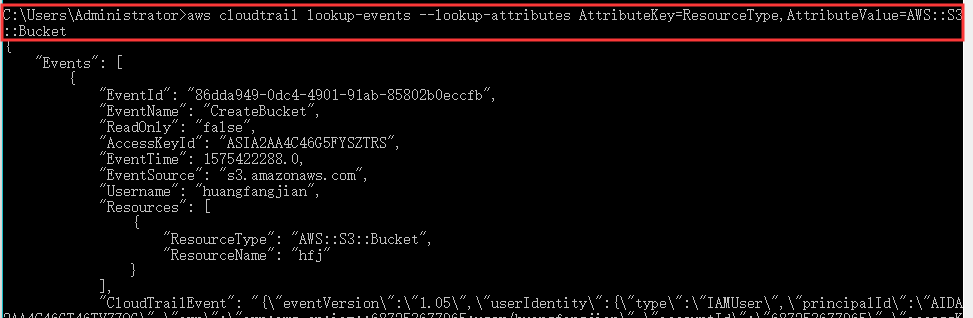
01-27-2015

01-27-2015,01:16PM

"01-27-2015, 01:16 PM"

6.属性进行筛选，使用【aws cloudtrail lookup-events --lookup-attributes AttributeKey=,AttributeValue=】命令；下面的示例命令返回事件，其中的值 ResourceType是AWS::S3::Bucket的事件；如下：

aws cloudtrail lookup-events --lookup-attributes AttributeKey=ResourceType,AttributeValue=AWS::S3::Bucket



**实验结果**

可以使用 aws cloudtrail lookup-events 命令查找过去 90 天的 CloudTrail 事件。lookup-events 具有以下选项：  
﹒–max-results  
﹒–start-time  
﹒–lookup-attributes