

腾讯安全 | 云鼎实验室

锋刃无影 御见未来

腾讯安全沙龙第3期（成都站）



IFS

关于我

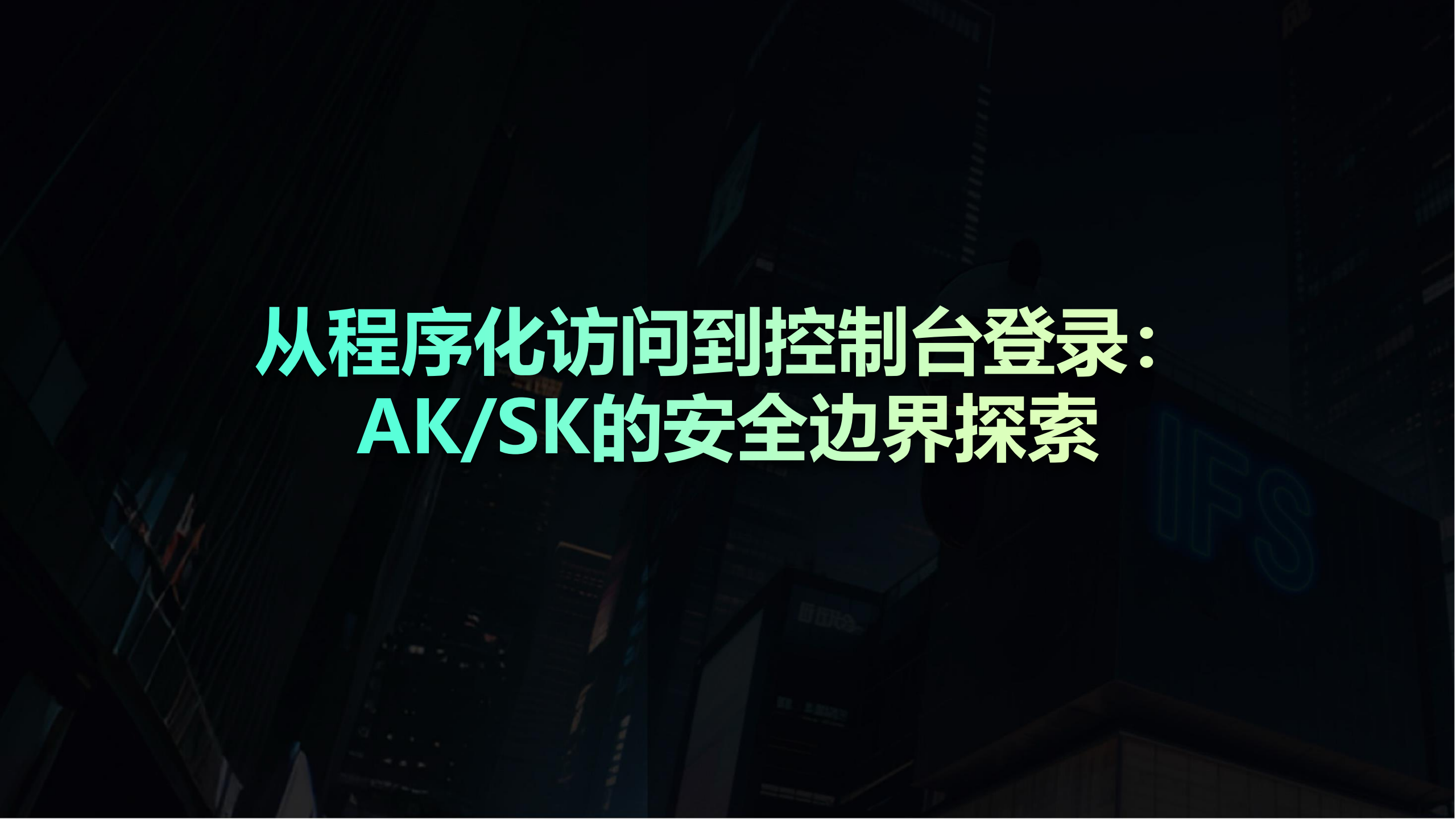
About me

张恒

云鼎实验室（腾讯）

7年云安全搬砖经验





从程序化访问到控制台登录： AK/SK的安全边界探索

引言：泄露AK利用

事件全景：一场持续17分钟的云上攻防战

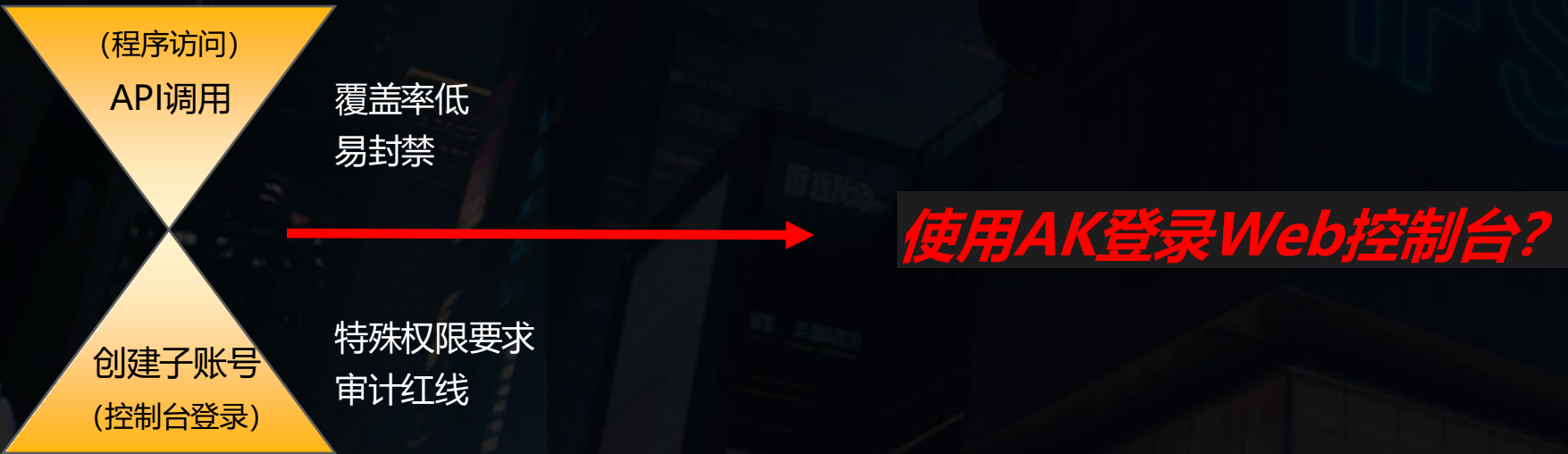
2025年3月9日15:39，阿里云ActionTrail日志突现异常波纹——根账号 `acs:ram::123456789:root`（已脱敏🔍）从立陶宛IP（164.92.91.227）发起高危操作。攻击者利用泄露的AccessKey（AK）在17分钟内完成侦察→提权→持久化攻击链，完整操作序列如下：

```
1  # 攻击者操作序列（脱敏重构）
2  15:39:06 ecs:DescribeInstances --region cn-hangzhou # 侦察：获取ECS元数据
3  15:39:33 ram:CreateUser --UserName attack_bot      # 横向移动：创建持久化账号
```

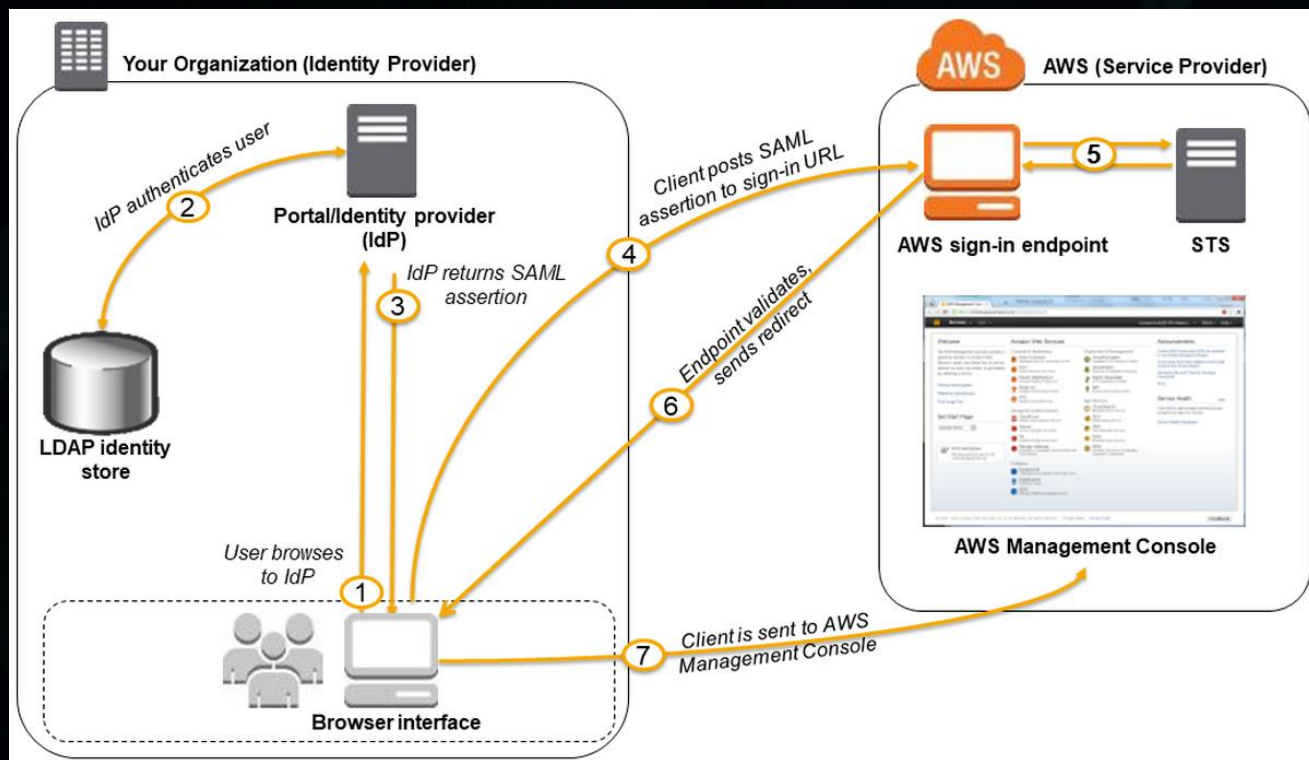
引言：泄露AK利用

获取AK后，枚举账号资源是攻击链的关键环节

方式	优势	劣势	云API审计风险等级
云API调用（编程&工具）	自动化程度高	<ul style="list-style-type: none">异常调用易触发告警云API覆盖开发成本高	⚠ 中等
创建子账号登录控制台	直观获取完整资源视图	<ul style="list-style-type: none">需高权限操作留痕明显易被审计	● 高危



AWS身份提供商 (Identity providers, IdP)



SAML提交至AWS的登录端点 (Sign-in Endpoint)

AWS安全令牌服务 (STS) 签发临时AWS访问凭证

用户凭STS下发的令牌成功登录，浏览器被定向至AWS管理控制台界面

AWS身份提供商 (Identity providers, IdP)

1. STS服务获取临时凭据: AssumeRole*, GetFederationToken

```
{"sessionId": "*** temporary access key ID ***",  
"sessionKey": "*** temporary secret access key ***",  
"sessionToken": "*** session token ***"}
```

2. 请求登录端点 <https://signin.aws.amazon.com/federation>, 获取SigninToken

```
Action = getSigninToken  
SessionDuration = time in seconds  
Session = *** the URL encoded JSON string
```

3. 生成控制台登录URL <https://signin.aws.amazon.com/federation>

```
?Action = login  
&Issuer = *** the form-urlencoded URL for your internal sign-in page ***  
&Destination = *** the form-urlencoded URL to the desired AWS console page ***  
&SigninToken = *** the value of SigninToken received in the previous step ***
```

AWS身份提供商 (Identity providers, IdP)

<https://signin.aws.amazon.com/federation>

?Action=login

&Issuer=https%3A%2F%2Fsignin.aws.amazon.com%2Ffederation

&Destination=https%3A%2F%2Fconsole.aws.amazon.com%2F

&SigninToken=VCQgs5qZZt3Q6fn8Tr5EXAMPLEmLnwB7JjUc-SHwnUWabcRdnWsi4DBn-dvC

CZ85wrD0nmldUcZEXAMPLE-vXYH4Q_mleuF_W2BE5HYexbe9y4Of-kje53SsjNNecATfjlzpW1

WibbnH6YcYRiBoffZBGExbEXAMPLE5aiKX4THWjQKC6gg6alHu6JFrnOJoK3dtP6I9a6hi6yPgm

iOkPZMmNGmhsVvXetKzr8mx3pxhHbMEXAMPLETv1pij0rok3IyCR2YVcljqwfWv32HU2Xlj471u

3fU6uOfUComeKiqTGX974xzJOZbdmX_t_lLrhEXAMPLEDDlisSnyHGw2xaZZqudm4mo2uTDk9Pv

9I5K0ZCqIgEXAMPLEcA6tgLPykEWGUyH6BdSC6166n4M4JkXIQgac7_7821YqixsNxZ6rsrpzwf

nQoS14O7R0eJCCJ684EXAMPLEZRdBNnuLbUYpz2Iw3vIN0tQgOujwnwydPscM9F7foaEK3jwMkg

Apeb1-6L_OB12MZhuFxx55555EXAMPLEhyETEd4ZulKPdXHkgI6T9ZkIIHz2Uy1RUTUhhUxNtSQ

nWc5xkbBoEcXqpoSleK7yhje9Vzhd61AEXAMPLEIbWeouACEMG6-Vd3dAgFYd6i5FYoyFrZLWvm

0LSG7RyYKeYN5VlZUk3YWQpyjP0RiT5KUrSUi-NEXAMPLExMOMdoODBEgKQsk-iu2ozh6r8bxwC

RNhujg

<https://signin.aws.amazon.com/federation>



永久凭据
AK/SK

STS:

AssumeRole

AssumeRoleWithSAML

AssumeRoleWithWebIdentity

GetFederationToken

临时凭据

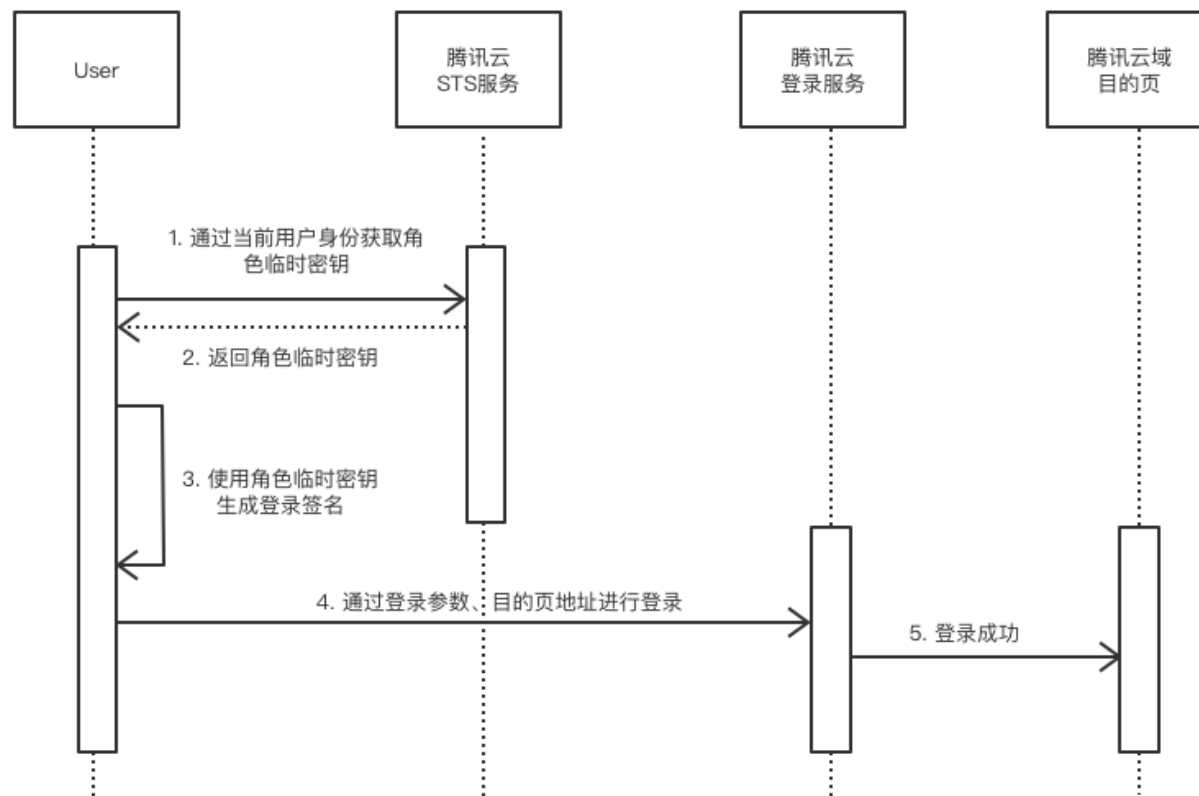
AccessKeyId

SecretAccessKey

SessionToken

腾讯云角色免密登录控制台

角色免密登录腾讯云流程



腾讯云角色免密登录控制台

<https://cloud.tencent.com/login/roleAccessCallback>

?algorithm= <签名时加密算法, 目前只支持sha1和sha256, 不填默认sha1>

&secretId= <签名时secretId>

&token= <临时密钥token>

&nonce= <签名时nonce>

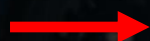
×tamp= <签名时timestamp>

&signature= <签名串>

&s_url= <登录后目的URL>



永久凭据
AK/SK



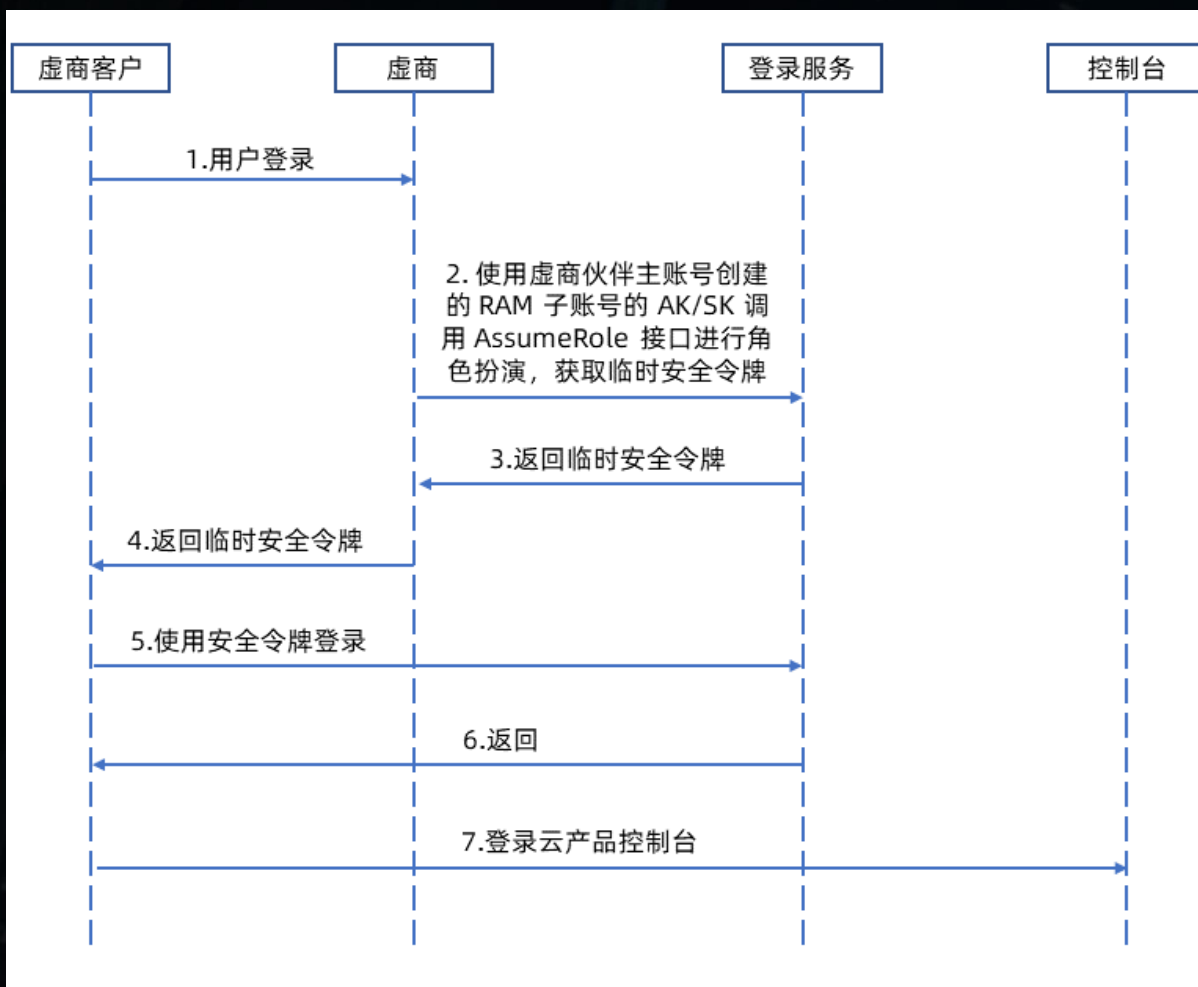
STS: AssumeRole
AssumeRoleWithSAML
AssumeRoleWithWebIdentity



临时凭据
AccessKeyId
SecretAccessKey
SessionToken

阿里云角色免密登录控制台

阿里云集成转售-虚商伙伴使用角色登录阿里云官网，同样适合普通账号。

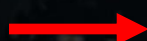


阿里云角色免密登录控制台

```
https://signin.aliyun.com/federation  
?Action=Login  
&LoginUrl=<登录URL>  
&Destination=<登录后目的URL>  
&SigninToken=<登录Token>
```



永久凭据
AK/SK

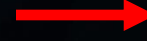


STS:

AssumeRole

AssumeRoleWithSAML

AssumeRoleWithOIDC



临时凭据

AccessKeyId

SecretAccessKey

SessionToken

角色免密登录云控制台

云平台名称	AWS	腾讯云	阿里云
云API权限	AssumeRole AssumeRoleWithSAML AssumeRoleWithWebIdentity GetFederationToken	AssumeRole AssumeRoleWithSAML AssumeRoleWithWebId entity	AssumeRole AssumeRoleWithSAML AssumeRoleWithOIDC
登录端点	https://signin.aws.amazon.com/federation	https://cloud.tencent.com/login/roleAccessCallback	https://signin.aliyun.com/federation
凭证签发服务	STS服务	STS服务	STS服务
典型应用场景	企业员工访问AWS控制台	子账号通过角色切换访问	页面集成
限制	控制台访问资源的权限，取决于角色/策略的权限		
差异性	通过控制台可访问未开放的云API		

开源: cloud-console

```
→ cloud-console git:(master) ✕ ./cloudconsole
A CLI application for managing cloud services.
```

```
Usage:
  cloudconsole [command]
```

```
cli Commands:
  alibaba    生成阿里云角色登录 URL
  aws        生成AWS角色登录 URL
  tencent    生成腾讯云角色登录 URL
```

```
server Commands:
  server      启动 RPC 服务器和 HTTP 网关
```

```
Additional Commands:
  completion  Generate the autocompletion script for the specified shell
  help        Help about any command
```

```
Flags:
  -h, --help  help for cloudconsole
```

```
Use "cloudconsole [command] --help" for more information about a command.
```

云控制台助手

一键登录各大云服务商控制台

输入云账号凭据，快速获取临时访问链接

快速配置

请选择云服务商并填写相关凭据信息

云服务商

腾讯云

SecretId

AKIDoOOi WCbnmU

SecretKey

.....

Token (与 RoleArn 二选一)

输入 Token

RoleArn (与 Token 二选一)

qcs::cam::uin/10****:roleName/te le

高级选项

控制台访问链接已生成

```
https://cloud.tencent.com/login/roleAccessCallback?
signature=35HSGTwu70vlfKDscmCFXMBE7uI%3D&s_url=http
s%3A%2F%2Fconsole.cloud.tencent.com&algorithm=sha1&
secretId=AKIDME0vqo0-IKos592H3BjGcwXcFHShtVTvpqqHE
QG-Suv50_B3x5b10Ajw-6sd4P4&token=UwRfcTcX8e5eDk3jrb
RiBI1hMU2yj4ia7528b24257f4c26b1d108a8fceb9c13YS7VB
8FGTRAVQGqjgm_RYTZhqoZsNy-y_jl2eiKUq6Xm9G1bZNTvjnoJ
IpeybRsV_RsDPkDCUtQ4xuYouGIgxFk1WoxM4-cDLWqjTCZoCF
iMOWmzRk0UnUfVjHzdI2haHHGgo3oPn4d9D4PbHUzF01bej0M_
KAX0aZ5qcbwjfpNQW2c50sv-z1RAgyfDqd0Wys8-SzRLPW0ETtr
rjv0VXrHdmXrZBMH0zJ85AGFEAy0c18Pr0jWC7ZiFfhJ3HZTDL3
xyw66NQ8p5x2mReqAF_CH1ER342S2Q6fgw2mu_fTnRJ5aNZvcMx
e-Jsy1w63o0aYwGTTrTjmo9ecB6ZTkqP-TdtV8XmDfV9N49w9GC_
fALqJoLaSowS4nQCRqgLBP&nonce=384653&timestamp=17453
10510
```

复制链接

立即访问

链接生成后会自动更新此区域

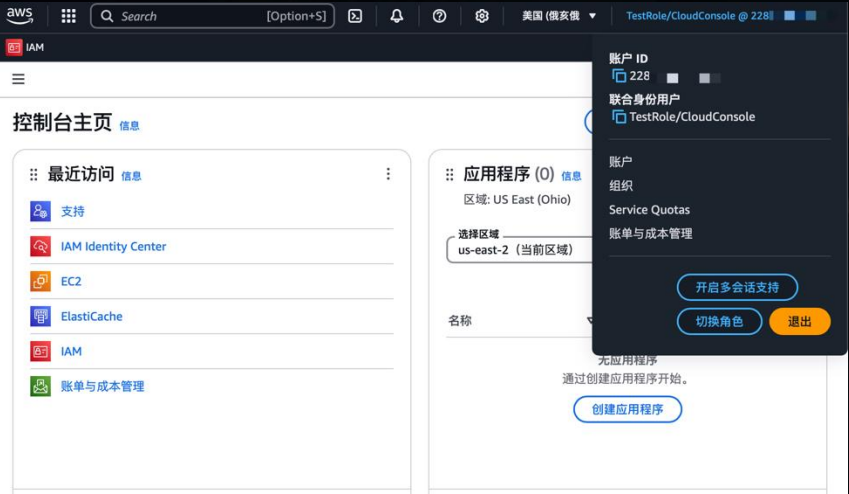
- <https://github.com/sg4i/cloud-console>

- <https://github.com/sg4i/CloudConsoleFE>

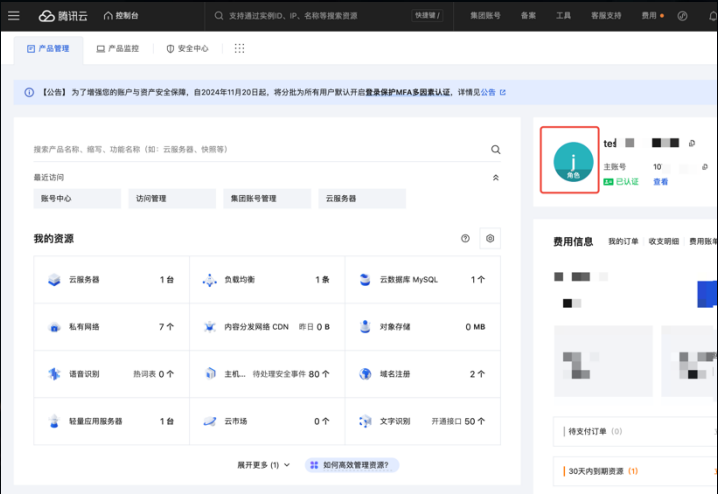
- <http://cloud.beesfun.com/>

角色登录控制台

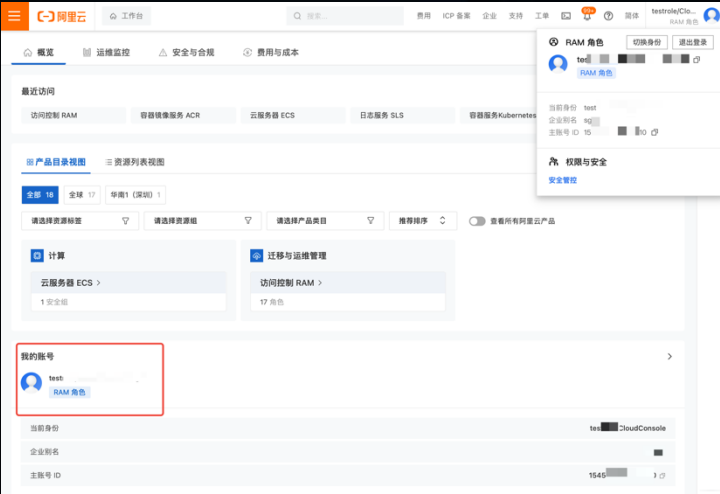
AWS



腾讯云



阿里云



事前加固

攻击链路：AK调用 STS:AssumeRole 获取临时凭据，角色免密登录云控制台

1

AK权限

AssumeRole - 扮演角色
ListRole - 角色列表
GetRole - 角色详情
ModifyAssumeRolePolicy - 修改角色信任策略

最小化AK权限：

- 按需授予AK所需权限（推荐）
- 禁止为AK授予sts:AssumeRole权限
- 限制IAM服务相关权限

2

角色信任策略

收敛角色信任策略：

- 限制sts:AssumeRole的调用主体
- 禁止为角色设置"Effect": "Allow"且"Principal": "*"

3

角色权限

GetRolePolicies - 角色绑定权限策略详情
AttachRolePolicy - 绑定权限策略到角色
CreateRole - 创建角色

ModifyAssumeRolePolicy - 修改角色信任策略

- 最小化角色权限：
- 按需授予角色所需权限（推荐）
 - 限制IAM服务相关权限

事前加固

AWS

sts:assume-role
iam:list-roles
iam:list-role-policies
iam:get-role
iam:get-role-policy
iam:update-role
iam:create-role
iam:attach-role-policy
iam:put-role-policy

腾讯

sts:AssumeRole
cam:DescribeRoleList
cam:GetRole
cam:UpdateAssumeRolePolicy
cam:CreateRole
cam:AttachRolePolicy
cam:UpdateRoleConsoleLogin
cam:UpdateRoleSessionDuration

阿里

sts:AssumeRole
ram:ListRoles
ram:GetRole
ram:UpdateRole
ram:CreateRole
ram:AttachPolicyToRole
ram:ListPoliciesForRole

事中/事后审计

AWS

角色登录后访问行为

eventName

eventType

eventCategory

userIdentity.type

userIdentity.sessionContext.sessionIssuer.type

userIdentity.sessionContext.sessionIssuer.userName

事件记录 信息

JSON 视图

```
1 {
2   "eventVersion": "1.10",
3   "userIdentity": {
4     "type": "AssumedRole",
5     "principalId": "AROAI47:CloudConsole",
6     "arn": "arn:aws:sts::2286:assumed-role/TestRole/CloudConsole",
7     "accountId": "2286",
8     "accessKeyId": "ASIA",
9     "sessionContext": {
10      "sessionIssuer": {
11        "type": "Role",
12        "principalId": "AROAI47",
13        "arn": "arn:aws:iam::2286:role/TestRole",
14        "accountId": "2286",
15        "userName": "TestRole",
16      },
17      "attributes": {
18        "creationDate": "2025-04-22T10:56:43Z",
19        "mfaAuthenticated": "false"
20      }
21    }
22  },
23  "eventTime": "2025-04-22T10:57:05Z",
24  "eventSource": "ec2.amazonaws.com",
25  "eventName": "DescribeRegions",
26  "awsRegion": "us-east-2",
27  "sourceIPAddress": "127.0.0.75",
28  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/6",
29  "requestParameters": {
30    "regionSet": {},
31    "allRegions": true
32  },
33  "responseElements": null,
34  "requestID": "8d5b41e7-8c2c-4750-a85d-117346bc4c96",
35  "eventID": "ba4b93a5-d976-4524-b61e-02d0da9003ae",
36  "readOnly": true,
37  "eventType": "AwsApiCall",
38  "managementEvent": true,
39  "recipientAccountId": "228688117607",
40  "eventCategory": "Management",
```

事中/事后审计

腾讯云

角色登录时

eventName: ConsoleLogin

eventType

userIdentity.sessionContext.loginType

角色登录后访问行为

eventName

eventType

userIdentity.type

userIdentity.roleName

```
事件记录 查看事件字段说明
1 {
2   "userIdentity": {
3     "principalId": "461-0000-0000-0000-0000-0000-0000-0000-0000-0000",
4     "accountId": "10000000000000000000",
5     "secretId": "",
6     "sessionContext": {
7       "aid": "",
8       "assumerOwnerAppId": "12000000000000000000",
9       "assumerOwnerUin": "10000000000000000000",
10      "assumerUin": "10000000000000000000",
11      "clientType": "pcweb",
12      "clientUA": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/
13      605.1.15 (KHTML, like Gecko) Version/17.6 Safari/605.1.15",
14      "loginTo": "https://cloud.tencent.com",
15      "loginType": "role",
16      "platform": "qcloud",
17      "roleName": "testRole",
18      "roleOwnerUin": "10000000000000000000",
19      "roleSessionName": "CloudConsole",
20      "roleType": 1,
21      "trafficParams": "***;timestamp=1744024575490;from_type=server;
22      track=0505e207-4364-4128-a9e2-9515c44e922c;***"
23    },
24    "type": "AssumedRole",
25    "userName": "testRole",
26    "roleName": "testRole",
27    "roleSessionName": ""
28  },
29  "eventRegion": "ap-guangzhou",
30  "eventVersion": 2,
31  "errorCode": "0",
32  "errorMessage": "",
33  "requestID": "1745310527",
34  "apiVersion": "2.0",
35  "eventType": "ConsoleCall",
36  "actionType": "Write",
37  "httpMethod": "POST",
38  "apiErrorCode": 0,
39  "apiErrorMessage": "",
40  "userAgent": "",
41  "eventTime": 1745310527,
42  "sensitiveAction": "0",
43  "sourceIPAddress": "121.35.103.75",
44  "resourceType": "account",
45  "eventName": "ConsoleLogin",
46  "eventSource": "account.tencentcloudapi.com",
47  "resourceSet": [],
48  "requestParameters": "{}",
49  "responseElements": "{}",
50  "resources": [{"qcs::account:gz:uin/10000000000000000000:account/10000000000000000000"}],
51  "resourceName": "account/10000000000000000000",
52  "tags": []
53 }
```

登录类型

事件类型

事件名称

```
1 {
2   "userIdentity": {
3     "principalId": "461-0000-0000-0000-0000-0000-0000-0000-0000-0000",
4     "accountId": "10000000000000000000",
5     "secretId": "",
6     "sessionContext": {},
7     "type": "AssumedRole",
8     "userName": "testRole",
9     "roleName": "testRole",
10    "roleSessionName": ""
11  },
12  "eventRegion": "ap-guangzhou",
13  "eventVersion": 2,
14  "errorCode": "0",
15  "errorMessage": "ok",
16  "requestID": "61419b42-0240-49d4-8891-5f91cf33f2ea",
17  "apiVersion": "3.0",
18  "eventType": "ApiCall",
19  "actionType": "Read",
20  "httpMethod": "POST",
21  "apiErrorCode": 0,
22  "apiErrorMessage": "",
23  "userAgent": "",
24  "eventTime": 1745310532,
25  "sensitiveAction": "0",
26  "sourceIPAddress": "121.35.103.75",
27  "resourceType": "cvm",
28  "eventName": "DescribeInstances",
29  "eventSource": "cvm.tencentcloudapi.com",
30  "resourceSet": [],
31  "requestParameters": "{}",
32  "responseElements": "{}",
33  "resources": [{"qcs::cvm:gz:uin/10000000000000000000:instance/*"}],
34  "resourceName": "instance/*",
35  "tags": []
36 }
37
38 }
```

用户身份类型

角色名称

事件类型

事件名称

事中/事后审计

阿里云

角色登录时

eventName: ConsoleSignin

eventType

userIdentity.type

角色登录后访问行为

eventName

eventType

userIdentity.type

userIdentity.userName

关联资源

事件记录

```
{ 15 items
  "eventId" : "56868440a45540d6a91ddb3c16a1597e_3617c_1745314560815_137.43"
  "eventVersion" : 1
  "eventSource" : "signin.aliyun.com"
  "sourceIpAddress" : "121.13.75"
  "userAgent" : "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.1 Safari/605.1.15"
  "eventRW" : "Write"
  "eventType" : "ConsoleSignin"
  "userIdentity" : { 5 items
    "sessionContext" : { 1 item
      "attributes" : { 1 item
        "mfaAuthenticated" : "false"
      }
    }
    "accountId" : "15410"
    "principalId" : "30087:CloudConsole"
    "type" : "assumed-role"
    "userName" : "testrole"
  }
  "serviceName" : "AasSub"
  "additionalEventData" : { 3 items
    "CallerBid" : "26842"
    "callbackUrl" : "https://home.console.aliyun.com"
    "mfaChecked" : "false"
  }
  "requestId" : "56868440a45540d6a91ddb3c16a1597e_3617c_1745314560815_137.43"
  "eventTime" : "2025-04-22T09:36:01Z"
  "isGlobal" : true
  "acsRegion" : "cn-hangzhou"
  "eventName" : "ConsoleSignin"
```

事件类型

用户身份类型

事件名称

关联资源

事件记录

```
{ 17 items
  "eventId" : "2A358981-241B-5BF5-86E2-31EA76B440AE"
  "eventVersion" : 1
  "eventSource" : "ecs-cn-hangzhou-share.aliyuncs.com"
  "requestParameters" : { 8 items
    "ByShare" : false
    "SourceRegionId" : "cn-hangzhou"
    "AcsProduct" : "Ecs"
    "ClientPort" : 2214
    "AcceptLanguage" : "zh-CN"
    "X-Acs-Client-Tls-Version" : "TLSv1.3"
    "stsTokenPlayerUid" : 1545276417870210
    "X-Acs-Client-Tls-Cipher-Suite" : "TLS_AES_256_GCM_SHA384"
  }
  "sourceIpAddress" : "121.13.75"
  "userAgent" : "ecs.console.aliyun.com"
  "eventRW" : "Read"
  "eventType" : "ConsoleOperation"
  "userIdentity" : { 6 items
    "accessKeyId" : "STS.9iSPT5u5F48755c"
    "sessionContext" : { 1 item
      "attributes" : { 2 items
        "mfaAuthenticated" : "false"
        "creationDate" : "2025-04-22T09:36:03Z"
      }
    }
    "accountId" : "1545210"
    "principalId" : "30087:CloudConsole"
    "type" : "assumed-role"
    "userName" : "testrole"
  }
  "serviceName" : "Ecs"
  "additionalEventData" : { 1 item
    "CallerBid" : "26842"
  }
  "apiVersion" : "2014-05-26"
  "requestId" : "2A358981-241B-5BF5-86E2-31EA76B440AE"
  "eventTime" : "2025-04-22T09:36:03Z"
  "isGlobal" : false
  "acsRegion" : "cn-hangzhou"
  "eventName" : "DescribeRegions"
```

访问源 IP

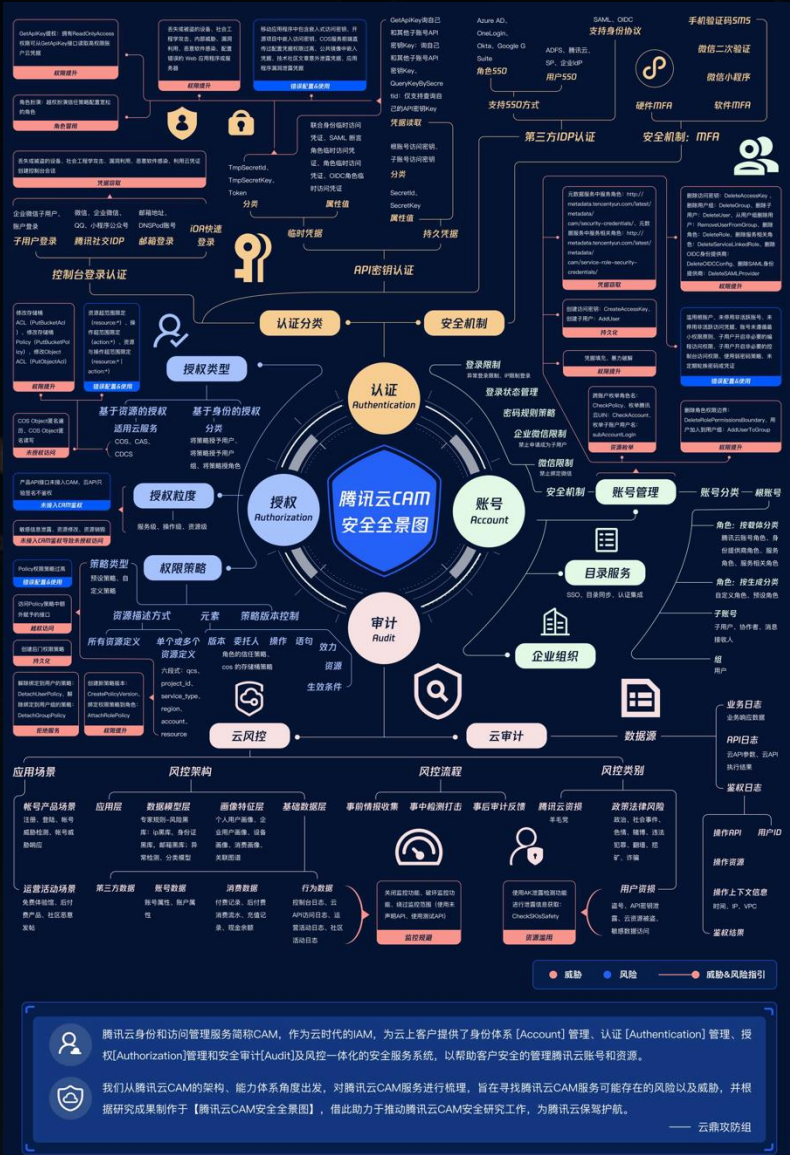
事件类型

用户身份类型

用户名称

事件名称

腾讯云CAM安全全景图



附录

- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_enable-console-custom-url.html
- <https://docs.aws.amazon.com/general/latest/gr/signin-service.html>
- <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/sts/get-federation-token.html>
- <https://awscli.amazonaws.com/v2/documentation/api/2.13.0/reference/sts/assume-role-with-web-identity.html>
- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_sts-comparison.html
- <https://cloud.tencent.com/document/product/598/45529>
- https://help.aliyun.com/document_detail/91911.html

谢谢

