



链滴

使用 python 基于 boto3 定时更新 aws ec2 安全组入站规则

作者: [LesterHoly](#)

原文链接: <https://ld246.com/article/1578381073790>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

更新aws ec2安全组入站规则

在使用AWS上的ec2服务时，需要ssh到服务器才能进行进一步的操作，由于设置了安全组（security group），需要将家里的ip填加到安全组的入站规则中，由于家里没有固定ip，需要定时获取ip同安全组中的ip进行校验，以下是一个简单的脚本来更新安全组的入站ip，方便自己维护查看。

```
# -*- coding:utf-8 -*-
import requests
import boto3
import re
import pendulum

def get_internet_ip():
    # get local ip address
    ip = ""
    res = requests.get('http://www.3322.org/dyndns/getip')
    if res.status_code == 200:
        ip = re.sub(r'\s+', "", res.text)
    else:
        res = requests.get('http://myip.ipip.net')
        ip_ = re.findall(r'\d+\.\d+\.\d+\.\d+', res.text)
        if ip_:
            ip = ip_[0]
    return ip + "/32"

def revoke_ip_rule(ec2, group_id, security_ip, security_port):
    # revoke security group ingress
    res_revoke = ec2.revoke_security_group_ingress(
        CidrIp=security_ip,
        FromPort=security_port,
        GroupId=group_id,
        IpProtocol='tcp',
        ToPort=security_port
    )
    print('revoke success')

def set_ip_rule(ec2, group_id, security_port, home_ip):
    # set security group ingress
    res_set = ec2.authorize_security_group_ingress(
        GroupId=group_id,
        IpPermissions=[{
            'IpProtocol': 'tcp',
            'FromPort': security_port,
            'ToPort': security_port,
            'IpRanges': [{'CidrIp': home_ip, 'Description': now}]
        }]
    )
    print('set success')
```

```

def get_ec2_security_group(home_ip):
    ec2 = boto3.client('ec2')
    security_group = ec2.describe_security_groups(GroupIds=[my_group_id])
    ips = security_group['SecurityGroups'][0]['IpPermissions']
    if ips:
        ip = ips[0]['IpRanges'][0]['CidrIp']
        if home_ip not in ip:
            revoke_ip_rule(ec2, my_group_id, ip, port)
            set_ip_rule(ec2, my_group_id, port, home_ip)
        else:
            print('ip is the same with aws config')
    else:
        set_ip_rule(ec2, my_group_id, port, home_ip)
return True

```

```

def main():
    home_ip = get_internet_ip()
    get_ec2_security_group(home_ip)

if __name__ == '__main__':
    """
    python3 -m scripts.auto_dynamic_security_group_for_ec2
    """
    my_group_id = 'sg-01af5580433805f59'
    port = 22
    now = pendulum.now().to_datetime_string()
    main()

```

在ubuntu中设置crontab定时运行脚本，以下是我的脚本设置

crontab设置 **crontab -e**

```

@reboot bash /home/lester/auto_open.sh # 开机自启脚本
*/5 * * * * bash /home/lester/auto_open.sh # 每5min运行一次

```

auto_open.sh

```

#!/bin/bash
source /home/lester/my_env/tf/bin/activate
cd /home/lester/my_github/my_airflow
python3 -m scripts.auto_dynamic_security_group_for_ec2

```