

PySNMP实验手册

1 PySNMP简介

PySNMP是Python的第三方模块，实现了SNMP v1/v2c/v3的所有功能，最新版本为v4.4.12。使用者可以使用Python语言，利用该模块实现SNMP的所有操作。

PIP国内源安装PySNMP并降级安装pyasn1的0.4.8版本：

```
pip install pysnmp pyasn1==0.4.8 -i http://mirrors.aliyun.com/pypi/simple/ --trusted-host mirrors.aliyun.com
```

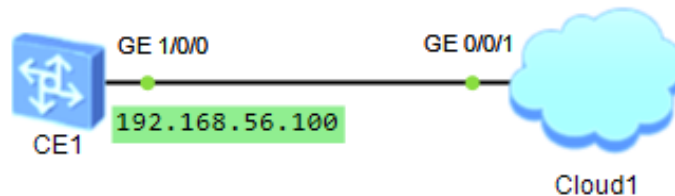
```
C:\Users\Administrator>pip install pysnmp -i http://mirrors.aliyun.com/pypi/simple/ --trusted-host mirrors.aliyun.com
Collecting pysnmp
  Downloading pysnmp-4.4.12-py2.py3-none-any.whl (296 kB)
    |████████████████████████████████████████| 296 kB 409 kB/s
Collecting pysmi
  Downloading pysmi-0.3.4-py2.py3-none-any.whl (80 kB)
    |████████████████████████████████████████| 80 kB 838 kB/s
Collecting pycryptodomex
  Downloading pycryptodomex-3.10.1-cp35-abi3-win_amd64.whl (1.6 MB)
    |████████████████████████████████████████| 1.6 MB 159 kB/s
Collecting pyasn1>=0.2.3
  Downloading pyasn1-0.4.8-py2.py3-none-any.whl (77 kB)
    |████████████████████████████████████████| 77 kB 211 kB/s
Collecting ply
  Downloading ply-3.11-py2.py3-none-any.whl (49 kB)
    |████████████████████████████████████████| 49 kB 147 kB/s
Installing collected packages: ply, pysmi, pycryptodomex, pyasn1, pysnmp
Successfully installed ply-3.11 pyasn1-0.4.8 pycryptodomex-3.10.1 pysmi-0.3.4 pysnmp-4.4.12
WARNING: You are using pip version 20.2.2; however, version 21.0.1 is available.
You should consider upgrading via the 'd:\python3_7_6\python.exe -m pip install --upgrade pip' command.
```

检查 pysnmp 的版本

```
C:\Users\Administrator>python
Python 3.7.6 (tags/v3.7.6:43364a7ae0, Dec 19 2019, 00:42:30) [MSC v.1916 64 bit (AMD64)]
on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import pysnmp
>>> pysnmp.__version__
'4.4.12'
>>>
```

2 网络拓扑

某公司现有一台CE12800设备，管理IP地址为192.168.56.100/24，可以SSH远程登陆。现有SNMP配置脚本snmp.txt文件。需要编写自动化脚本，首先进行设备SNMP配置，然后收集设备SNMP信息。



文件snmp.txt的内容

```
snmp-agent usm-user v3 admin group dc-admin
snmp-agent usm v3 admin auth sha
Huawei@123
Huawei@123
snmp-agent usm-user v3 admin privacy aes128
Huawei@123
Huawei@123
snmp-agent trap source GE1/0/0
snmp-agent mib-view included nt iso
snmp-agent mib-view included rd iso
snmp-agent mib-view included wt iso
snmp-agent mib-view included iso-view iso
snmp-agent group v3 dc-admin privacy read-view rd write-view wt notify-view nt
```

3 配置CE1的SSH服务并添加用户

```
<HUAWEI>system-view immediately
Enter system view, return user view with return command.
[HUAWEI]sysname CE1
[CE1]interface Vlanif 1
```

```

[CE1-Vlanif1]ip add 192.168.56.100 24
[CE1-Vlanif1]quit
[CE1]

[CE1]interface GE1/0/0
[CE1-GE1/0/0]undo shutdown
[CE1-GE1/0/0]quit
[CE1]

[CE1]stelnet server enable
[CE1]user-interface vty 0 4
[CE1-ui-vty0-4]authentication-mode aaa
[CE1-ui-vty0-4]protocol inbound ssh
[CE1-ui-vty0-4]user privilege level 3
[CE1-ui-vty0-4]quit
[CE1]

[CE1]aaa
[CE1-aaa]local-user python password irreversible-cipher Huawei12#$
[CE1-aaa]local-user python user-group manage-ug
[CE1-aaa]local-user python service-type ssh
[CE1-aaa]quit
[CE1]

[CE1]ssh user python
[CE1]ssh user python authentication-type password
[CE1]ssh user python service-type stelnet

```

4 PySNMP代码

```

# 1、导入模块
import paramiko
import time
from pynmp.hlapi import *

# 2、定义交换机信息
ip = '192.168.56.100'
username='python'
password='Huawei12#$'

# 3、SSH登陆设备
ssh = paramiko.client.SSHClient()
ssh.set_missing_host_key_policy(paramiko.client.AutoAddPolicy())
ssh.connect(hostname=ip,port=22,username=username,password=password)
print(ip+' login succesfully')

# 4、打开一个channel, 输入配置
cli = ssh.invoke_shell()
cli.send('N\n')
time.sleep(0.5)
cli.send('screen-length 0 temporary\n')

```

```

time.sleep(0.5)

# 5、进入系统视图
cli.send('system-view immediately\n')
time.sleep(0.5)

# 6、逐行读取本地同一个文件夹里的snmp.txt，写入SSH通道
f = open('snmp.txt', 'r')
snmp_config_list = f.readlines()
for i in snmp_config_list:
    cli.send(i)
    time.sleep(0.5)

# 7、建立SNMP的通道
UdpTransportTarget((ip, 161))

# 8、通过pySNMP获取设备的主机名
g = getCmd(
    SnmpEngine(),
    UsmUserData(
        'admin',
        'Huawei@123',
        'Huawei@123',
        authProtocol=usmHMACSHAAuthProtocol,
        privProtocol=usmAesCfb128Protocol
    ),
    UdpTransportTarget((ip, 161)),
    ContextData(),
    ObjectType(ObjectIdentity('SNMPv2-MIB', 'sysName', 0))
)

errorIndication, errorStatus, errorIndex, varBinds = next(g)

for i in varBinds:
    print(i)
    print(str(i).split('=')[1].strip())

# 9、最大限度接收返回信息
dis_this = cli.recv(999999).decode()
print(dis_this)

#关闭会话
ssh.close()

```

执行以上代码，可以得到如下输出

```

192.168.56.100 login successfully
SNMPv2-MIB::sysName.0 = CE1
CE1

Warning: The initial password poses security risks.
The password needs to be changed. Change now? [Y/N]:N

```

```
Info: The max number of VTY users is 5, the number of current VTY users online is 1, and
total number of terminal users online is 2.
    The current login time is 2021-08-14 15:28:55.
    First login successfully.
<CE1>screen-length 0 temporary
Info: The configuration takes effect on the current user terminal interface only.
<CE1>system-view immediately
Enter system view, return user view with return command.
[CE1]snmp-agent usm-user v3 admin group dc-admin
Warning: Adding the user to a privacy group is recommended, because the bound group has
insecure properties (with authentication or noauthentication configured).
[CE1]snmp-agent usm v3 admin au sha
Please configure the authentication password (8-255)
Enter Password:
Confirm Password:
[CE1]snmp-agent usm-user v3 admin pr aes128
Please configure the privacy password (8-255)
Enter Password:
Confirm Password:
Warning: The privacy and authentication passwords are the same, which is insecure. It is
recommended that the privacy and authentication passwords be different.
[CE1]snmp-agent trap source G1/0/0
Warning: Please configure an IP address to the interface.
[CE1]snmp-agent mib-view included nt iso
[CE1]snmp-agent mib-view included rd iso
[CE1]snmp-agent mib-view included wt iso
[CE1]snmp-agent mib-view included iso-view iso
[CE1]snmp-agent group v3 dc-admin privacy read-view rd write-view wt notify-view nt
[CE1]
```

思考：如何通过Netmiko实现以上代码？