SNMP

Trần Hoàng Hải

RFC Các Phiên Bản SNMP

- IETF (Internet Engineering Task Force) đã công bố các phiên bản SNMP sau:
  - SNMP Version 1: được định nghĩa trong RFC 1157. Khả năng bảo mật của SNMPv1 dựa trên nguyên tắc cộng đồng, cho phép bất cứ ứng dụng nào chạy SNMP cũng có thể truy suất thông tin của các thiết bị SNMP khác.
  - SNMP Version 2: tăng cường khả năng bảo mật của SNMPv1 bằng chuỗi community. SNMPv2 được định nghĩa trong RFC 1905, 1906, 1907.
  - SNMP Version 3: tăng cường thêm khả năng chứng thực thông qua các giải thuật chứng thực mạnh. Được định nghĩa trong các RFC 1905, 1906, 1907,2571,2572, 2573, 2574, 2575.

Cấu Hình Agent SNMP Trên Thiết Bị Linux

- Các gói SNMP trong Linux
  - *net-snmp.i386 : A collection of SNMP protocol tools and libraries.*
  - *net-snmp-devel.i386 : The development environment for the NET-SNMP project.*
  - *net-snmp-libs.i386 : The NET-SNMP runtime libraries.*
  - *net-snmp-perl.i386 : The perl NET-SNMP module and the mib2c tool.*
  - *net-snmp-utils.i386 : Network management utilities using SNMP, from the NET-SNMP project.*
  - *openhpi-subagent.i386 : The openhpi snmp subagent*
  - *php-snmp.i386 : A module for PHP applications that query SNMP-managed devices.*

Cấu Hình Agent SNMP Trên Thiết Bị Linux (tt)

- Cài đặt gói agent snmp cho thiết bị linux bằng lệnh sau:

  yum intall net-snmp*

- Kiểm tra hoạt động cài đặt

  service snmpd status

- Kích hoạt daemon snmp

  service snmpd start

- Cấu hình để snmpd tự bật mỗi khi reboot lại máy

  chkconfig –level 2345 snmpd on

- Kiểm tra lại bằng lệnh

  chkconf --list snmpd

Cấu Hình Agent SNMP Trên Thiết Bị Linux (tt)

- Tiếp theo ta cần cấu hình để SNMP agent trên server Linux có thể xử lý các request từ phía Manager bằng cách khai báo trong file cấu hình **/etc/snmp/snmpd.conf**. Ta lần lượt thực hiện các bước sau:
  - Trước khi thực hiện bất kỳ sự thay đổi nào trong file cấu hình ta nên thực hiện backup file snmp.conf.

    cp /etc/snmp/snmpd.conf /etc/snmp/snmp.conf.bak
  - Bước đầu tiên trong cấu hình là ta sẽ map community name với security name tương ứng bằng khai báo như sau trong file **snmpd.conf:**

```
com2sec notConfigUser default public
```

Cấu Hình Agent SNMP Trên Thiết Bị Linux (tt)

- Bước tiếp theo ta sẽ map security name vào một group name bằng cách thêm khai báo như sau trong file **snmpd.conf.**

```
group notConfigGroup v1 notConfigUser
group notConfigGroup v2c notConfigUser
```

- Bươc thứ ba ta sẽ tạo ra các view để chỉ rõ pham vi thông tin có thể truy suất tới snmp agent.

```
view systemview include .1
```

- Tiếp theo ta sẽ chỉ rõ những group vừa khai báo có thể truy suất đến những thông tin nào trên Agent SNMP bằng các view tương ứng.

```
access notConfigGroup "" any noauth exact
systemview none none
```

Cấu Hình Agent SNMP Trên Thiết Bị Linux (tt)

- Thực hiên khai báo thêm thông tin về vị trí của thiết bị và admin quản trị thiết bị thông qua hai option là syslocation và syscontact.

```
syslocation HSU
syscontact admin@hoasen.edu.vn
```

- Khai báo thông tin về Manager sẽ nhận các gói Trap từ phía Agent bằng option trapsink.

```
trapsink    192.168.1.125    public    162
```

- Sau khi khai báo xong ta cần restart lại dịch vụ snmp để những khai báo vừa rồi có tác dụng bằng lệnh:

service snmpd restart

Cấu Hình Agent SNMP Trên Thiết Bị Linux (tt)

- Ta kiểm tra lại hoạt động.

```
[root@rhel51 ~]# snmpget -v 2c -c private 10.10.0.30 UCD-SNMP-MIB::extOutput.3
UCD-SNMP-MIB::extOutput.3 = STRING: Filesystem          Size  Used Avail Use% Mounted on
/dev/sda5             996M  240M  705M  26% /
/dev/sda7             494M   11M  458M   3% /home
/dev/sda3             996M   86M  859M  10% /var
/dev/sda2             3.4G  1.8G  1.4G  57% /usr
/dev/sda1              99M   12M   83M  12% /boot
tmpfs                 506M     0  506M   0% /dev/shm
/dev/md2              296M   11M  271M   4% /root/raid
/dev/hdc              2.9G  2.9G     0 100% /mnt/cdrom
```

Cấu Hình Agent SNMP Trên Thiết Bị Linux (tt)

- Sử dụng SNMP để giám sát dung lượng partition trên thiết bị:
  - Chỉ ra các partitions cần giám sát trong file snmpd.conf

```
disk /
disk /home
disk /var
disk /boot
```

root@rhel51 perl]# snmpwalk -v 2c -c private 10.10.0.30 enterprises.ucdavis.dskTable.dskEntry

1. UCD-SNMP-MIB::dskIndex.1 = INTEGER: 1
2. UCD-SNMP-MIB::dskIndex.2 = INTEGER: 2
3. UCD-SNMP-MIB::dskIndex.3 = INTEGER: 3
4. UCD-SNMP-MIB::dskIndex.4 = INTEGER: 4
5. UCD-SNMP-MIB::dskPath.1 = STRING: /
6. UCD-SNMP-MIB::dskPath.2 = STRING: /home
7. UCD-SNMP-MIB::dskPath.3 = STRING: /var
8. UCD-SNMP-MIB::dskPath.4 = STRING: /boot
9. UCD-SNMP-MIB::dskDevice.1 = STRING: /dev/sda5
10. UCD-SNMP-MIB::dskDevice.2 = STRING: /dev/sda7
11. UCD-SNMP-MIB::dskDevice.3 = STRING: /dev/sda3
12. UCD-SNMP-MIB::dskDevice.4 = STRING: /dev/sda1
13. UCD-SNMP-MIB::dskMinimum.1 = INTEGER: 100000
14. UCD-SNMP-MIB::dskMinimum.2 = INTEGER: 100000
15. UCD-SNMP-MIB::dskMinimum.3 = INTEGER: 100000
16. UCD-SNMP-MIB::dskMinimum.4 = INTEGER: 100000
17. UCD-SNMP-MIB::dskMinPercent.1 = INTEGER: -1
18. UCD-SNMP-MIB::dskMinPercent.2 = INTEGER: -1
19. UCD-SNMP-MIB::dskMinPercent.3 = INTEGER: -1
20. UCD-SNMP-MIB::dskMinPercent.4 = INTEGER: -1
21. UCD-SNMP-MIB::dskTotal.1 = INTEGER: 1019208
22. UCD-SNMP-MIB::dskTotal.2 = INTEGER: 505604
23. UCD-SNMP-MIB::dskTotal.3 = INTEGER: 1019240
24. UCD-SNMP-MIB::dskTotal.4 = INTEGER: 101086
25. UCD-SNMP-MIB::dskAvail.1 = INTEGER: 721400
26. UCD-SNMP-MIB::dskAvail.2 = INTEGER: 468955
27. UCD-SNMP-MIB::dskAvail.3 = INTEGER: 878748
28. UCD-SNMP-MIB::dskAvail.4 = INTEGER: 84567
29. UCD-SNMP-MIB::dskUsed.1 = INTEGER: 245200
30. UCD-SNMP-MIB::dskUsed.2 = INTEGER: 10545
31. UCD-SNMP-MIB::dskUsed.3 = INTEGER: 87880
32. UCD-SNMP-MIB::dskUsed.4 = INTEGER: 11300
33. UCD-SNMP-MIB::dskPercent.1 = INTEGER: 25
34. UCD-SNMP-MIB::dskPercent.2 = INTEGER: 2
35. UCD-SNMP-MIB::dskPercent.3 = INTEGER: 9
36. UCD-SNMP-MIB::dskPercent.4 = INTEGER: 12
37. UCD-SNMP-MIB::dskPercentNode.1 = INTEGER: 2
38. UCD-SNMP-MIB::dskPercentNode.2 = INTEGER: 0
39. UCD-SNMP-MIB::dskPercentNode.3 = INTEGER: 0
40. UCD-SNMP-MIB::dskPercentNode.4 = INTEGER: 0
41. UCD-SNMP-MIB::dskErrorFlag.1 = INTEGER: 0
42. UCD-SNMP-MIB::dskErrorFlag.2 = INTEGER: 0
43. UCD-SNMP-MIB::dskErrorFlag.3 = INTEGER: 0
44. UCD-SNMP-MIB::dskErrorFlag.4 = INTEGER: 1
45. UCD-SNMP-MIB::dskErrorMsg.1 = STRING:
46. UCD-SNMP-MIB::dskErrorMsg.2 = STRING:
47. UCD-SNMP-MIB::dskErrorMsg.3 = STRING:
48. UCD-SNMP-MIB::dskErrorMsg.4 = STRING: /boot: less than 100000 free (= 84567)

- Sử dụng SNMP giám sát các processes trong hệ thống.
  - Chỉ ra các processes cần giám sát (ví dụ: httpd, sshd) bằng cách thêm vào các khai báo sau trong file snmpd.conf

    proc sshd 1 1

    proc httpd 5 1

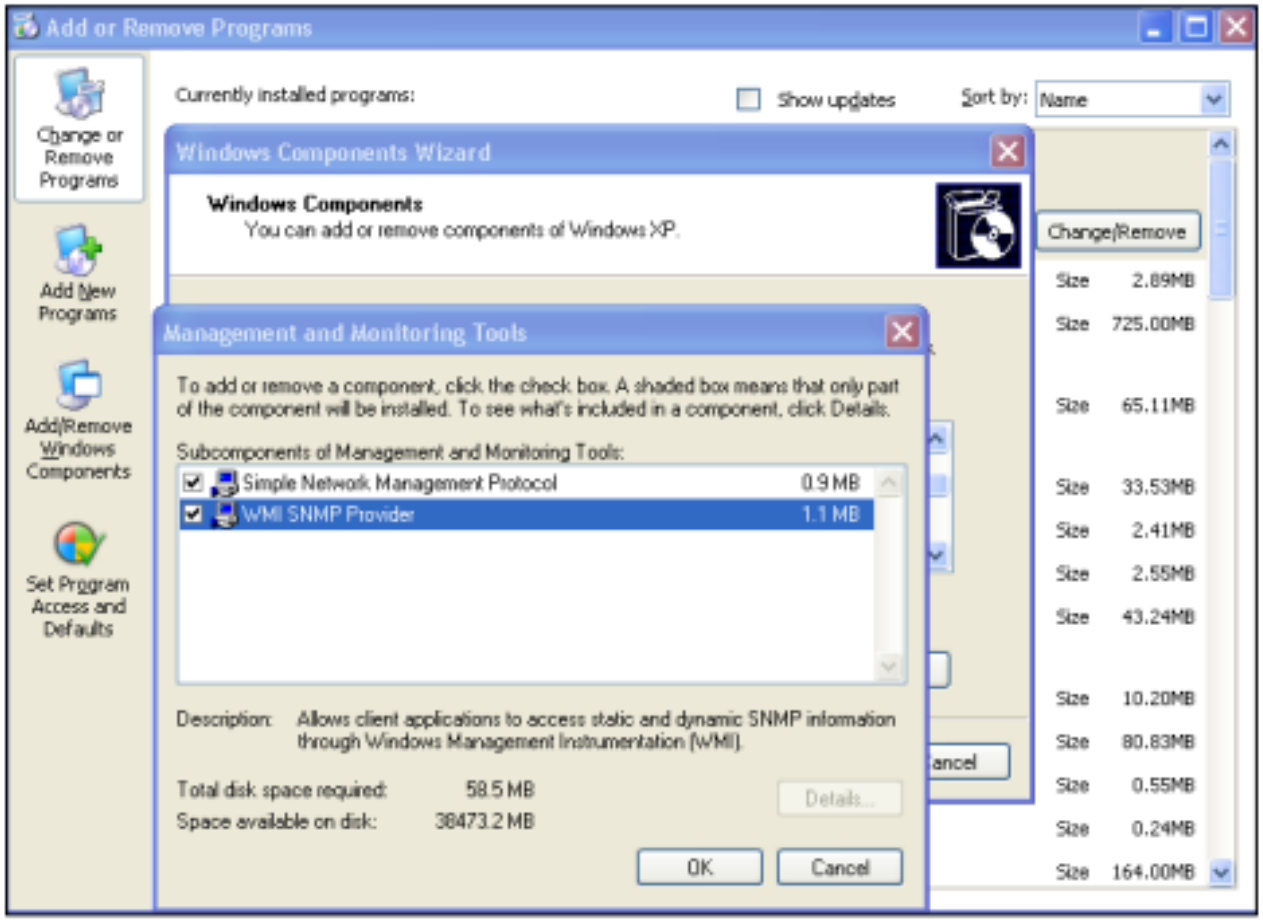
[root@rhel51 perl]# snmpwalk -v 2c -c private 10.10.0.30 enterprises.ucdavis.prTable

1. UCD-SNMP-MIB::prIndex.1 = INTEGER: 1
2. UCD-SNMP-MIB::prIndex.2 = INTEGER: 2
3. UCD-SNMP-MIB::prNames.1 = STRING: sshd
4. UCD-SNMP-MIB::prNames.2 = STRING: httpd
5. UCD-SNMP-MIB::prMin.1 = INTEGER: 1
6. UCD-SNMP-MIB::prMin.2 = INTEGER: 0
7. UCD-SNMP-MIB::prMax.1 = INTEGER: 1
8. UCD-SNMP-MIB::prMax.2 = INTEGER: 0
9. **UCD-SNMP-MIB::prCount.1 = INTEGER: 3**
10. UCD-SNMP-MIB::prCount.2 = INTEGER: 9
11. UCD-SNMP-MIB::prErrorFlag.1 = INTEGER: 1
12. UCD-SNMP-MIB::prErrorFlag.2 = INTEGER: 0
13. UCD-SNMP-MIB::prErrMessage.1 = STRING: **Too many sshd running (# = 3)**
14. UCD-SNMP-MIB::prErrMessage.2 = STRING:
15. UCD-SNMP-MIB::prErrFix.1 = INTEGER: 0
16. UCD-SNMP-MIB::prErrFix.2 = INTEGER: 0
17. UCD-SNMP-MIB::prErrFixCmd.1 = STRING:
18. UCD-SNMP-MIB::prErrFixCmd.2 = STRING:

Cấu Hình Agent SNMP Trên Thiết Bị Windows

- Các thiết bị sử dụng hệ điều hành Windows hỗ trợ giám sát qua hai phương thức là: WMI và SNMP. Tuy nhiên theo mặc định thì tính năng này không được kích hoạt. Ta cần phải thực các bước sau để kích hoạt tính năng này:
  - Mở cửa sổ **Control Panel.**
  - Chọn **Add/ Remove Windows Components.**
  - Click vào ô **Management and Monitoring Tools** và chọn **Details.**
  - Chọn phương thức hỗ trợ giám sát: **SNMP** hoặc **WMI** hoặc cả hai phương thức.
  - Save lại những thay đổi để tiến hành cài đặt **Windows Components.**

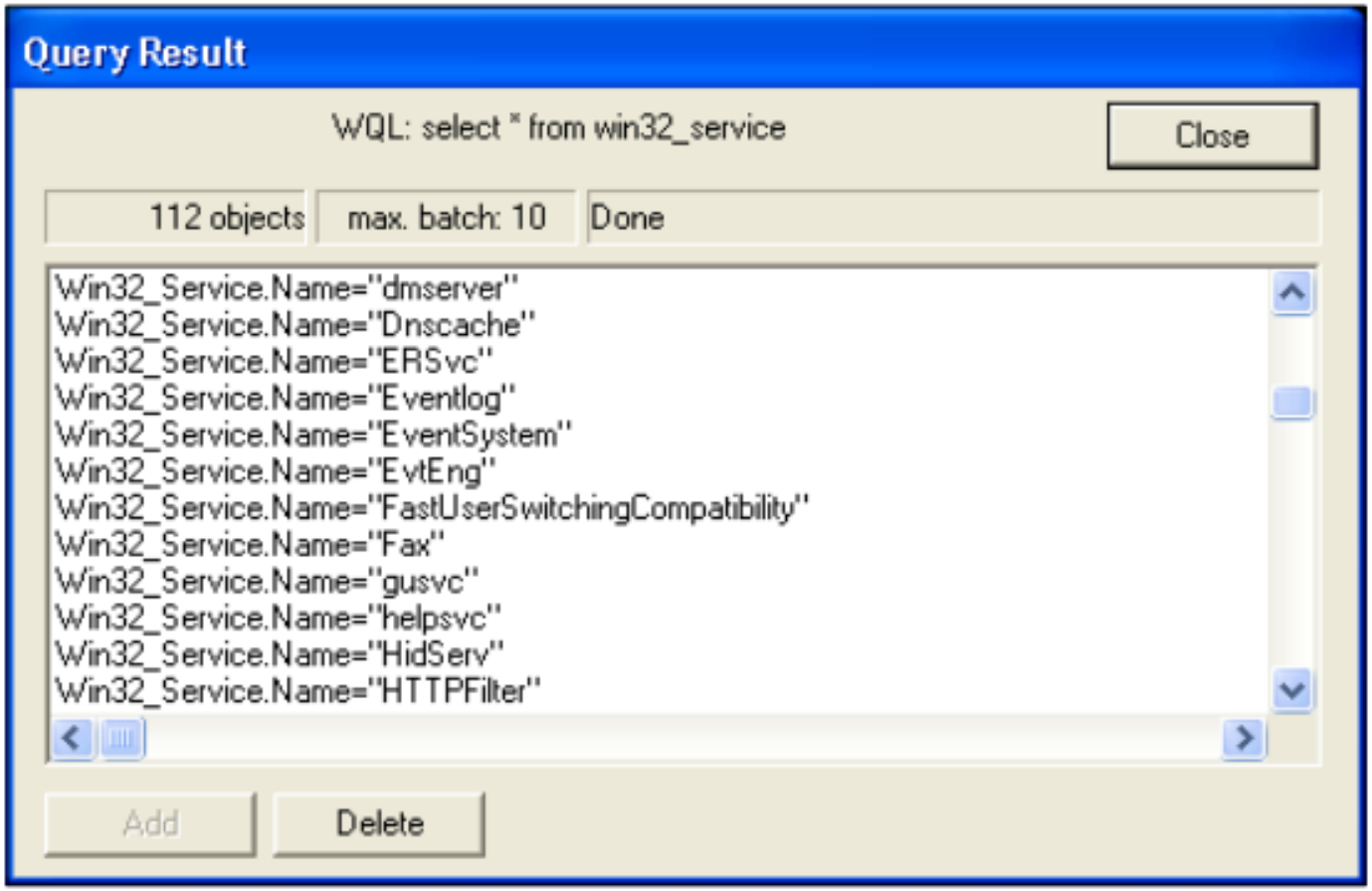
Cấu Hình Agent SNMP Trên Thiết Bị Windows (tt)



Cấu Hình Agent SNMP Trên Thiết Bị Windows (tt)

- Nếu chúng ta cài đặt thêm giao thức quản trị WMI trên Windows thì chúng ta có thể thực hiện các thao tác sau để kiểm tra hoạt động của WMI.
  - Từ menu **Start** chọn **Run.**
  - Trên thanh **Run** gõ command: wbemtest.
  - Click vào nút **Connect** trên cửa sổ Windows Management Instrumentation Tester.
  - Tại filed **Namespace** ta đổi thành \\HOST\root\cimv2**.**
  - Nhập username và password của người quản trị.
  - Click vào nút **Query.**
  - Trên box search, ta gõ select * from win32_service để liệt kê các services.

Cấu Hình Agent SNMP Trên Thiết Bị Windows (tt)



Cấu Hình Agent SNMP Trên Thiết Bị Cisco

- **Với SNMP polling**

  R(config)#snmp community public rw 2

  R(config)#access-lists 2 permit 10.10.0.4

- **Với SNMP Trap (Alert)**

  R(config)#snmp-server enable traps

  R(config)#snmp-server host 192.168.1.21 public **config bgp tty**

  R(config)#snmp contact Admin

  R(config)#snmp location HSU