如何使用 SNPM 来监控 Linux 服务器

作 者: icefired (icefired@netexpert.cn)

2005-9-16

[Keywords] SNMP, Linux, Orion NPM, MRTG, Net-SNMP

[Ojects] Using SNMP to monitor a Linux server

[准 备]

1. Net-SNMP 5.1.2 或 UCD-SNMP 4.2.3
   下载：http://www.net-snmp.org/download.html
2. A Linux Server: Redhat Linux 7/8/9,RHEL 3/4 或其他 Linux 发行版。
3. SNMP Tool: Solarwinds toolset V8.2 或 Orion Network Performance Monitor V7.8, 其他支持 SNMP 监控的工具如 HP OpenView, IBM NetView, SNMPC V7 均可以。

[步 骤]

1. 安装 Net-SNMP 或 UCD-SNMP. (三种方法)

1.1 安装 Linux 系统时自动安装

安装 Linux 系统的时候选择 UCD-SNMP 和 SNMP-Utility 两个安装包就可以了。

1.2 使用 RPM 包来安装,这里以 Redhat 9 为例来说明。

先检查有无安装旧的版本: rpm -q ucd-snmp
全新安装:

```
#rpm -ivh net-snmp-5.1.2-1.rh9.i386.rpm
#rpm -ivh net-snmp-devel-5.1.2-1.rh9.i386.rpm
```

1.3 使用原代码来安装

```
#wget http://mesh.dl.sourceforge.net/sourceforge/net-snmp/net-snmp-5.1.3.1.tar.gz
#tar -xzvf net-snmp-5.1.3.1.tar.gz
#cd net-snmp-5.1.3.1
#./configure
# make & make install
```

如果没什么问题则顺利完成安装，Linux 的安装和命令使用不在本文讨论范围，请大家查询相关手册。

2. 配置 SNMP

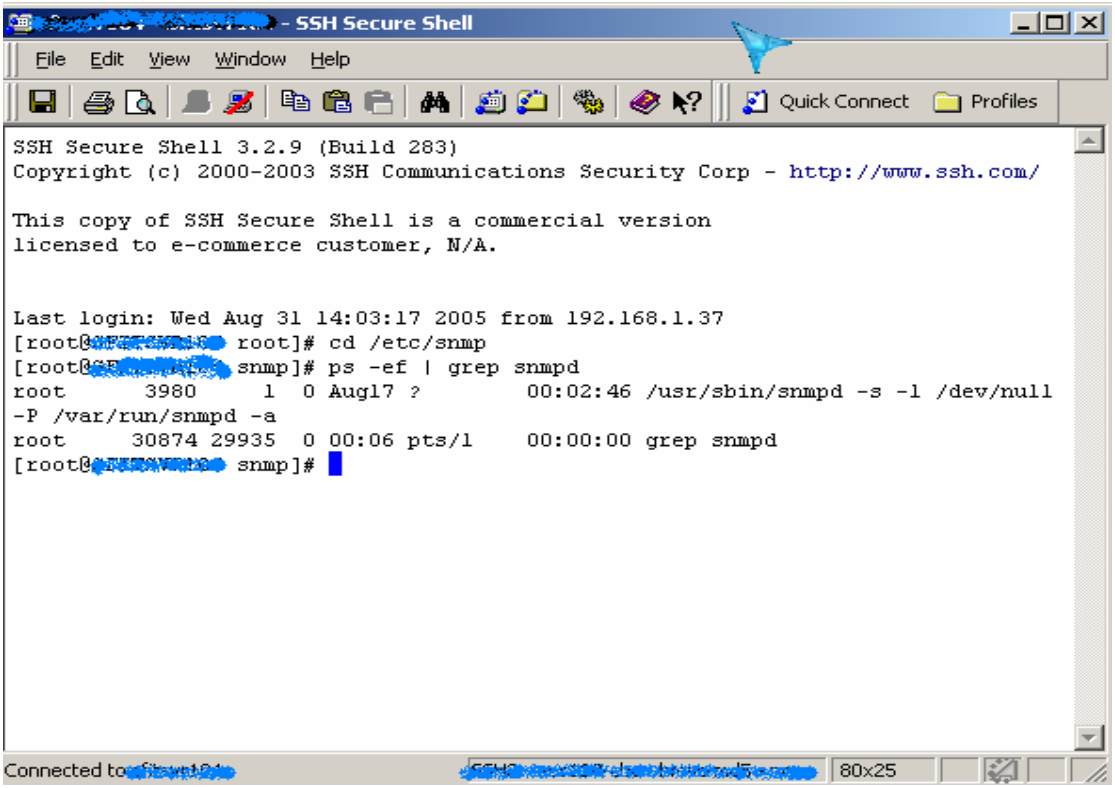
2.1 设置 SNMPD 服务自动启动

setup 然后勾选上 services -> snmpd
启动 snmpd 进程

#service snmpd start

2.2 检查一下 snmpd 进程是否运行正常

 # ps -ef | grep snmpd



2.3 配置/etc/snmp/snmpd.conf

好了，按照前面的步骤我们已经顺利的安装好 SNMP 服务了，如果使用默认的 snmpd.conf 文件，我们将只能够看到系统信息，而不能对系统资源进行监测。

下面是一份 net-snmp 自带的 snmpd.conf 文件：

```
####################---Begin---###################################
#####################
# snmpd.conf:
#   An example configuration file for configuring the ucd-snmp snmpd agent.
#
############################################################
#
# This file is intended to only be as a starting point.  Many more
# configuration directives exist than are mentioned in this file.  For
# full details, see the snmpd.conf(5) manual page.
#
# All lines beginning with a '#' are comments and are intended for you
# to read.  All other lines are configuration commands for the agent.
```

```
###########################################################
# Access Control
###########################################################
# As shipped, the snmpd demon will only respond to queries on the
# system mib group until this file is replaced or modified for
# security purposes.  Examples are shown below about how to increase the
# level of access.

# By far, the most common question I get about the agent is "why won't
# it work?", when really it should be "how do I configure the agent to
# allow me to access it?"
#
# By default, the agent responds to the "public" community for read
# only access, if run out of the box without any configuration file in
# place.  The following examples show you other ways of configuring
# the agent so that you can change the community names, and give
# yourself write access to the mib tree as well.
#
# For more information, read the FAQ as well as the snmpd.conf(5)
# manual page.

####
# First, map the community name "public" into a "security name"

#         sec.name  source          community
com2sec notConfigUser  default       public

####
# Second, map the security name into a group name:

#         groupName      securityModel securityName
group   notConfigGroup v1           notConfigUser
group   notConfigGroup v2c           notConfigUser

####
# Third, create a view for us to let the group have rights to:

# Make at least  snmpwalk -v 1 localhost -c public system fast again.
#         name           incl/excl     subtree         mask(optional)
view    systemview    included   .1.3.6.1.2.1.1
view    systemview    included   .1.3.6.1.2.1.25.1.1

####
```

```
# Finally, grant the group read-only access to the systemview view.

#           group                context sec.model sec.level prefix read     write    notif
access    notConfigGroup ""          any           noauth       exact    systemview none none

# ----------------------------------------------------------------------

# Here is a commented out example configuration that allows less
# restrictive access.

# YOU SHOULD CHANGE THE "COMMUNITY" TOKEN BELOW TO A NEW KEYWORD ONLY
# KNOWN AT YOUR SITE.   YOU *MUST* CHANGE THE NETWORK TOKEN BELOW TO
# SOMETHING REFLECTING YOUR LOCAL NETWORK ADDRESS SPACE.

##           sec.name    source               community
#com2sec local        localhost          COMMUNITY
#com2sec mynetwork NETWORK/24          COMMUNITY

##        group.name sec.model    sec.name
#group MyRWGroup    any             local
#group MyROGroup    any             mynetwork
#
#group MyRWGroup    any             otherv3user
#...

##                incl/excl subtree                                mask
#view all       included   .1                                    80

## -or just the mib2 tree-

#view mib2     included    .iso.org.dod.internet.mgmt.mib-2 fc


##                        context sec.model sec.level prefix read     write    notif
#access MyROGroup ""          any           noauth       0          all       none     none
#access MyRWGroup ""          any           noauth       0          all       all       all

############################################################
# System contact information
#

# It is also possible to set the sysContact and sysLocation system
# variables through the snmpd.conf file:
```

```
syslocation Unknown (edit /etc/snmp/snmpd.conf)
syscontact Root <root@localhost> (configure /etc/snmp/snmp.local.conf)

# Example output of snmpwalk:
#     % snmpwalk -v 1 localhost -c public system
#     system.sysDescr.0 = "SunOS name sun4c"
#     system.sysObjectID.0 = OID: enterprises.ucdavis.ucdSnmpAgent.sunos4
#     system.sysUpTime.0 = Timeticks: (595637548) 68 days, 22:32:55
#     system.sysContact.0 = "Me <me@somewhere.org>"
#     system.sysName.0 = "name"
#     system.sysLocation.0 = "Right here, right now."
#     system.sysServices.0 = 72


# -----------------------------------------------------------------------------


###########################################################
# Process checks.
#
#   The following are examples of how to use the agent to check for
#   processes running on the host.    The syntax looks something like:
#
#   proc NAME [MAX=0] [MIN=0]
#
#   NAME:    the name of the process to check for.    It must match
#            exactly (ie, http will not find httpd processes).
#   MAX:     the maximum number allowed to be running.    Defaults to 0.
#   MIN:     the minimum number to be running.    Defaults to 0.

#
#   Examples (commented out by default):
#

#   Make sure mountd is running
#proc mountd

#   Make sure there are no more than 4 ntalkds running, but 0 is ok too.
#proc ntalkd 4

#   Make sure at least one sendmail, but less than or equal to 10 are running.
#proc sendmail 10 1

#   A snmpwalk of the process mib tree would look something like this:
```

```
#
# % snmpwalk -v 1 localhost -c public .1.3.6.1.4.1.2021.2
# enterprises.ucdavis.procTable.prEntry.prIndex.1 = 1
# enterprises.ucdavis.procTable.prEntry.prIndex.2 = 2
# enterprises.ucdavis.procTable.prEntry.prIndex.3 = 3
# enterprises.ucdavis.procTable.prEntry.prNames.1 = "mountd"
# enterprises.ucdavis.procTable.prEntry.prNames.2 = "ntalkd"
# enterprises.ucdavis.procTable.prEntry.prNames.3 = "sendmail"
# enterprises.ucdavis.procTable.prEntry.prMin.1 = 0
# enterprises.ucdavis.procTable.prEntry.prMin.2 = 0
# enterprises.ucdavis.procTable.prEntry.prMin.3 = 1
# enterprises.ucdavis.procTable.prEntry.prMax.1 = 0
# enterprises.ucdavis.procTable.prEntry.prMax.2 = 4
# enterprises.ucdavis.procTable.prEntry.prMax.3 = 10
# enterprises.ucdavis.procTable.prEntry.prCount.1 = 0
# enterprises.ucdavis.procTable.prEntry.prCount.2 = 0
# enterprises.ucdavis.procTable.prEntry.prCount.3 = 1
# enterprises.ucdavis.procTable.prEntry.prErrorFlag.1 = 1
# enterprises.ucdavis.procTable.prEntry.prErrorFlag.2 = 0
# enterprises.ucdavis.procTable.prEntry.prErrorFlag.3 = 0
# enterprises.ucdavis.procTable.prEntry.prErrMessage.1 = "No mountd process running."
# enterprises.ucdavis.procTable.prEntry.prErrMessage.2 = ""
# enterprises.ucdavis.procTable.prEntry.prErrMessage.3 = ""
# enterprises.ucdavis.procTable.prEntry.prErrFix.1 = 0
# enterprises.ucdavis.procTable.prEntry.prErrFix.2 = 0
# enterprises.ucdavis.procTable.prEntry.prErrFix.3 = 0
#
#   Note that the errorFlag for mountd is set to 1 because one is not
#   running (in this case an rpc.mountd is, but thats not good enough),
#   and the ErrMessage tells you what's wrong.   The configuration
#   imposed in the snmpd.conf file is also shown.
#
#   Special Case:   When the min and max numbers are both 0, it assumes
#   you want a max of infinity and a min of 1.
#


# ---------------------------------------------------------------------
##########################################################
# Executables/scripts
#

#
#   You can also have programs run by the agent that return a single
```

```
#    line of output and an exit code.   Here are two examples.
#
#    exec NAME PROGRAM [ARGS ...]
#
#    NAME:        A generic name.
#    PROGRAM:   The program to run.   Include the path!
#    ARGS:        optional arguments to be passed to the program

# a simple hello world

#exec echotest /bin/echo hello world

# Run a shell script containing:
#
# #!/bin/sh
# echo hello world
# echo hi there
# exit 35
#
# Note:   this has been specifically commented out to prevent
# accidental security holes due to someone else on your system writing
# a /tmp/shtest before you do.   Uncomment to use it.
#
#exec shelltest /bin/sh /tmp/shtest

# Then,
# % snmpwalk -v 1 localhost -c public .1.3.6.1.4.1.2021.8
# enterprises.ucdavis.extTable.extEntry.extIndex.1 = 1
# enterprises.ucdavis.extTable.extEntry.extIndex.2 = 2
# enterprises.ucdavis.extTable.extEntry.extNames.1 = "echotest"
# enterprises.ucdavis.extTable.extEntry.extNames.2 = "shelltest"
# enterprises.ucdavis.extTable.extEntry.extCommand.1 = "/bin/echo hello world"
# enterprises.ucdavis.extTable.extEntry.extCommand.2 = "/bin/sh /tmp/shtest"
# enterprises.ucdavis.extTable.extEntry.extResult.1 = 0
# enterprises.ucdavis.extTable.extEntry.extResult.2 = 35
# enterprises.ucdavis.extTable.extEntry.extOutput.1 = "hello world."
# enterprises.ucdavis.extTable.extEntry.extOutput.2 = "hello world."
# enterprises.ucdavis.extTable.extEntry.extErrFix.1 = 0
# enterprises.ucdavis.extTable.extEntry.extErrFix.2 = 0

# Note that the second line of the /tmp/shtest shell script is cut
# off.   Also note that the exit status of 35 was returned.

# ---------------------------------------------------------------------------
```

```
##############################################################
# disk checks
#

# The agent can check the amount of available disk space, and make
# sure it is above a set limit.

# disk PATH [MIN=100000]
#
# PATH:   mount path to the disk in question.
# MIN:    Disks with space below this value will have the Mib's errorFlag set.
#         Default value = 100000.

# Check the / partition and make sure it contains at least 10 megs.

#disk / 10000

# % snmpwalk -v 1 localhost -c public .1.3.6.1.4.1.2021.9
# enterprises.ucdavis.diskTable.dskEntry.diskIndex.1 = 0
# enterprises.ucdavis.diskTable.dskEntry.diskPath.1 = "/" Hex: 2F
# enterprises.ucdavis.diskTable.dskEntry.diskDevice.1 = "/dev/dsk/c201d6s0"
# enterprises.ucdavis.diskTable.dskEntry.diskMinimum.1 = 10000
# enterprises.ucdavis.diskTable.dskEntry.diskTotal.1 = 837130
# enterprises.ucdavis.diskTable.dskEntry.diskAvail.1 = 316325
# enterprises.ucdavis.diskTable.dskEntry.diskUsed.1 = 437092
# enterprises.ucdavis.diskTable.dskEntry.diskPercent.1 = 58
# enterprises.ucdavis.diskTable.dskEntry.diskErrorFlag.1 = 0
# enterprises.ucdavis.diskTable.dskEntry.diskErrorMsg.1 = ""

# ------------------------------------------------------------------------


##############################################################
# load average checks
#

# load [1MAX=12.0] [5MAX=12.0] [15MAX=12.0]
#
# 1MAX:    If the 1 minute load average is above this limit at query
#          time, the errorFlag will be set.
# 5MAX:    Similar, but for 5 min average.
# 15MAX:   Similar, but for 15 min average.

# Check for loads:
```

```
#load 12 14 14

# % snmpwalk -v 1 localhost -c public .1.3.6.1.4.1.2021.10
# enterprises.ucdavis.loadTable.laEntry.loadaveIndex.1 = 1
# enterprises.ucdavis.loadTable.laEntry.loadaveIndex.2 = 2
# enterprises.ucdavis.loadTable.laEntry.loadaveIndex.3 = 3
# enterprises.ucdavis.loadTable.laEntry.loadaveNames.1 = "Load-1"
# enterprises.ucdavis.loadTable.laEntry.loadaveNames.2 = "Load-5"
# enterprises.ucdavis.loadTable.laEntry.loadaveNames.3 = "Load-15"
# enterprises.ucdavis.loadTable.laEntry.loadaveLoad.1 = "0.49" Hex: 30 2E 34 39
# enterprises.ucdavis.loadTable.laEntry.loadaveLoad.2 = "0.31" Hex: 30 2E 33 31
# enterprises.ucdavis.loadTable.laEntry.loadaveLoad.3 = "0.26" Hex: 30 2E 32 36
# enterprises.ucdavis.loadTable.laEntry.loadaveConfig.1 = "12.00"
# enterprises.ucdavis.loadTable.laEntry.loadaveConfig.2 = "14.00"
# enterprises.ucdavis.loadTable.laEntry.loadaveConfig.3 = "14.00"
# enterprises.ucdavis.loadTable.laEntry.loadaveErrorFlag.1 = 0
# enterprises.ucdavis.loadTable.laEntry.loadaveErrorFlag.2 = 0
# enterprises.ucdavis.loadTable.laEntry.loadaveErrorFlag.3 = 0
# enterprises.ucdavis.loadTable.laEntry.loadaveErrMessage.1 = ""
# enterprises.ucdavis.loadTable.laEntry.loadaveErrMessage.2 = ""
# enterprises.ucdavis.loadTable.laEntry.loadaveErrMessage.3 = ""

# ---------------------------------------------------------

###########################################################
# Extensible sections.
#

# This alleviates the multiple line output problem found in the
# previous executable mib by placing each mib in its own mib table:

# Run a shell script containing:
#
# #!/bin/sh
# echo hello world
# echo hi there
# exit 35
#
# Note:    this has been specifically commented out to prevent
# accidental security holes due to someone else on your system writing
# a /tmp/shtest before you do.    Uncomment to use it.
#
# exec .1.3.6.1.4.1.2021.50 shelltest /bin/sh /tmp/shtest
```

```
# % snmpwalk -v 1 localhost -c public .1.3.6.1.4.1.2021.50
# enterprises.ucdavis.50.1.1 = 1
# enterprises.ucdavis.50.2.1 = "shelltest"
# enterprises.ucdavis.50.3.1 = "/bin/sh /tmp/shtest"
# enterprises.ucdavis.50.100.1 = 35
# enterprises.ucdavis.50.101.1 = "hello world."
# enterprises.ucdavis.50.101.2 = "hi there."
# enterprises.ucdavis.50.102.1 = 0

# Now the Output has grown to two lines, and we can see the 'hi
# there.' output as the second line from our shell script.
#
# Note that you must alter the mib.txt file to be correct if you want
# the .50.* outputs above to change to reasonable text descriptions.

# Other ideas:
#
# exec .1.3.6.1.4.1.2021.51 ps /bin/ps
# exec .1.3.6.1.4.1.2021.52 top /usr/local/bin/top
# exec .1.3.6.1.4.1.2021.53 mailq /usr/bin/mailq

# ----------------------------------------------------------

###########################################################
# Pass through control.
#

# Usage:
#     pass MIBOID EXEC-COMMAND
#
# This will pass total control of the mib underneath the MIBOID
# portion of the mib to the EXEC-COMMAND.
#
# Note:    You'll have to change the path of the passtest script to your
# source directory or install it in the given location.
#
# Example:    (see the script for details)
#                 (commented out here since it requires that you place the
#                 script in the right location. (its not installed by default))

# pass .1.3.6.1.4.1.2021.255 /bin/sh /usr/local/local/passtest

# % snmpwalk -v 1 localhost -c public .1.3.6.1.4.1.2021.255
# enterprises.ucdavis.255.1 = "life the universe and everything"
```

```
# enterprises.ucdavis.255.2.1 = 42
# enterprises.ucdavis.255.2.2 = OID: 42.42.42
# enterprises.ucdavis.255.3 = Timeticks: (363136200) 42 days, 0:42:42
# enterprises.ucdavis.255.4 = IpAddress: 127.0.0.1
# enterprises.ucdavis.255.5 = 42
# enterprises.ucdavis.255.6 = Gauge: 42
#
# % snmpget -v 1 localhost public .1.3.6.1.4.1.2021.255.5
# enterprises.ucdavis.255.5 = 42
#
# % snmpset -v 1 localhost public .1.3.6.1.4.1.2021.255.1 s "New string"
# enterprises.ucdavis.255.1 = "New string"
#

# For specific usage information, see the man/snmpd.conf.5 manual page
# as well as the local/passtest script used in the above example.

# Added for support of bcm5820 cards.
pass .1.3.6.1.4.1.4413.4.1 /usr/bin/ucd5820stat

############################################################
# Further Information
#
#   See the snmpd.conf manual page, and the output of "snmpd -H".

############################--END-----##############################
```

因为配置文件较长，为了方便大家查看，同时也可以偷懒，注释文件也没有删除。下面简单地介绍一下配置文件，主要针对我们要使用的。

（1）配置 community string, 默认的是 public,我们可以改成自己想要的字符串。

```
37  ####
38  # First, map the community name "public" into a "security name"
39
40  #       sec.name  source          community
41  com2sec notConfigUser  default       public
42
```

(2) 影射 security name 到 group

```
43  ####
44  # Second, map the security name into a group name:
45
46  #       groupName      securityModel securityName
47  group   notConfigGroup v1            notConfigUser
48  group   notConfigGroup v2c           notConfigUser
49
```

（3）分组授权

```
50 ####
51 # Third, create a view for us to let the group have rights to:
52
53 # Make at least  snmpwalk -v 1 localhost -c public system fast again.
54 #       name           incl/excl     subtree         mask(optional)
55 view    systemview    included   .1.3.6.1.2.1.1
56 view    systemview    included   .1.3.6.1.2.1.25.1.1
57
```

```
58 ####
59 # Finally, grant the group read-only access to the systemview view.
60
61 #       group          context sec.model sec.level prefix read   write  notif
62 access  notConfigGroup ""      any       noauth    exact  systemview none none
63
```

默认的只能看到系统信息，而我们想对系统的资源进行全面的监控，所以要做修改。注意，为了安全起见，请把 write 对应的改为 none,如果要修改系统设定，一般还是使用 ssh 远程连接要方便一些。

```
52 ####
53 # Third, create a view for us to let the group have rights to:
54
55 # Make at least  snmpwalk -v 1 localhost -c public system fast again.
56 #       name           incl/excl     subtree         mask(optional)
57 view    systemview    included   .1.3.6.1.2.1.1
58 view    systemview    included   .1.3.6.1.2.1.25.1.1
59
60 ####
61 # Finally, grant the group read-only access to the systemview view.
62
63 #       group          context sec.model sec.level prefix read   write  notif
64 access  notConfigGroup ""      any       noauth    exact  all none none
65
```

（4） 修改要监控的项目

```
121 # Third, create a view for us to let the group have rights to:
122 # Open up the whole tree for ro, make the RFC 1213 required ones rw.
123 #       name           incl/excl       subtree mask(optional)
124 view    roview         included        .1
125 view    rwview         included        system.sysContact
126 view    rwview         included        system.sysName
127 view    rwview         included        system.sysLocation
128 view    rwview         included        interfaces.ifTable.ifEntry.ifAdminStatus
129 view    rwview         included        at.atTable.atEntry.atPhysAddress
130 view    rwview         included        at.atTable.atEntry.atNetAddress
131 view    rwview         included        ip.ipForwarding
132 view    rwview         included        ip.ipDefaultTTL
133 view    rwview         included        ip.ipRouteTable.ipRouteEntry.ipRouteDest
134 view    rwview         included        ip.ipRouteTable.ipRouteEntry.ipRouteIfIndex
135 view    rwview         included        ip.ipRouteTable.ipRouteEntry.ipRouteMetric1
136 view    rwview         included        ip.ipRouteTable.ipRouteEntry.ipRouteMetric2
137 view    rwview         included        ip.ipRouteTable.ipRouteEntry.ipRouteMetric3
138 view    rwview         included        ip.ipRouteTable.ipRouteEntry.ipRouteMetric4
139 view    rwview         included        ip.ipRouteTable.ipRouteEntry.ipRouteType
140 view    rwview         included        ip.ipRouteTable.ipRouteEntry.ipRouteAge
141 view    rwview         included        ip.ipRouteTable.ipRouteEntry.ipRouteMask
142 view    rwview         included        ip.ipRouteTable.ipRouteEntry.ipRouteMetric5
143 view    rwview         included        ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaIfIndex
144 view    rwview         included        ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaPhysAddress
145 view    rwview         included        ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaNetAddress
146 view    rwview         included        ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType
147 view    rwview         included        tcp.tcpConnTable.tcpConnEntry.tcpConnState
148 view    rwview         included        egp.egpNeighTable.egpNeighEntry.egpNeighEventTrigger
149 view    rwview         included        snmp.snmpEnableAuthenTraps
150
```

（5）修改系统信息

```
157 ###############################################################################
158 # System contact information
159 #
160
161 # It is also possible to set the sysContact and sysLocation system
162 # variables through the snmpd.conf file:
163
164 syslocation A2 Server Room
165 syscontact SysMaster <icefired@netexpert.cn>
166
167 # Example output of snmpwalk:
168 #   % snmpwalk -v 1 localhost -c public system
169 #   system.sysDescr.0 = "SunOS name sun4c"
170 #   system.sysObjectID.0 = OID: enterprises.ucdavis.ucdSnmpAgent.sunos4
171 #   system.sysUpTime.0 = Timeticks: (595637548) 68 days, 22:32:55
172 #   system.sysContact.0 = "Me <me@somewhere.org>"
173 #   system.sysName.0 = "name"
174 #   system.sysLocation.0 = "Right here, right now."
175 #   system.sysServices.0 = 72
176
177
178 # -------------------------------------------------------------------------------
```

其实 SNMP 还可以做很多我们意想不到的事情，比如进程监测，执行 command/scripts,磁盘检查，检查负载，自定义 OID 等。配置文件中已经有例子可以供我们参考，有兴趣的朋友可以尝试一下。

为了方便大家，下面我附上一份已经配置好的 snmpd.conf 文档，大家可以直接的 copy 下来替换即可。**如果你对 snmpd.conf 做了任何改动，请重启一下 snmpd 进程，命令为：**

#service snmpd restart

```
############ -- A well-configured snmpd.conf file-- ########
############ -- Begin -- ########
##########################################################
#
# snmpd.conf:
#     An example configuration file for configuring the ucd-snmp snmpd agent.
#
##########################################################
#
# This file is intended to only be as a starting point.   Many more
# configuration directives exist than are mentioned in this file.   For
# full details, see the snmpd.conf(5) manual page.
#
# All lines beginning with a '#' are comments and are intended for you
# to read.   All other lines are configuration commands for the agent.

##########################################################
# Access Control
```

```
##############################################################

# As shipped, the snmpd demon will only respond to queries on the
# system mib group until this file is replaced or modified for
# security purposes.  Examples are shown below about how to increase the
# level of access.

# By far, the most common question I get about the agent is "why won't
# it work?", when really it should be "how do I configure the agent to
# allow me to access it?"
#
# By default, the agent responds to the "public" community for read
# only access, if run out of the box without any configuration file in
# place.  The following examples show you other ways of configuring
# the agent so that you can change the community names, and give
# yourself write access to the mib tree as well.
#
# For more information, read the FAQ as well as the snmpd.conf(5)
# manual page.

### First Edited By ICE 2005/08/10 ####################

####
# First, map the community name "public" into a "security name"

#          sec.name  source          community
com2sec notConfigUser  default       public

####
# Second, map the security name into a group name:

#          groupName      securityModel securityName
group   notConfigGroup v1           notConfigUser
group   notConfigGroup v2c           notConfigUser

####
# Third, create a view for us to let the group have rights to:

# Make at least  snmpwalk -v 1 localhost -c public system fast again.
#          name           incl/excl     subtree         mask(optional)
view    systemview    included   .1.3.6.1.2.1.1
view    systemview    included   .1.3.6.1.2.1.25.1.1

####
```

```
# Finally, grant the group read-only access to the systemview view.

#           group                context sec.model sec.level prefix read     write    notif
access    notConfigGroup ""          any           noauth       exact    all none none

# ----------------------------------------------------------------------------

# Here is a commented out example configuration that allows less
# restrictive access.

# YOU SHOULD CHANGE THE "COMMUNITY" TOKEN BELOW TO A NEW KEYWORD ONLY
# KNOWN AT YOUR SITE.   YOU *MUST* CHANGE THE NETWORK TOKEN BELOW TO
# SOMETHING REFLECTING YOUR LOCAL NETWORK ADDRESS SPACE.

##           sec.name    source               community
#com2sec local        localhost          COMMUNITY
#com2sec mynetwork NETWORK/24          COMMUNITY

##        group.name sec.model    sec.name
#group MyRWGroup    any             local
#group MyROGroup    any             mynetwork
#
#group MyRWGroup    any             otherv3user
#...

##                incl/excl subtree                                mask
view all       included    .1                                      80

## -or just the mib2 tree-

view mib2      included    .iso.org.dod.internet.mgmt.mib-2 fc


##                        context sec.model sec.level prefix read     write    notif
#access MyROGroup ""          any           noauth       0          all       none      none
#access MyRWGroup ""          any           noauth       0          all       all       all


############################################################
# Sample configuration to make net-snmpd RFC 1213.
# Unfortunately v1 and v2c don't allow any user based authentification, so
# opening up the default config is not an option from a security point.
#
# WARNING: If you uncomment the following lines you allow write access to your
```

```
# snmpd daemon from any source! To avoid this use different names for your
# community or split out the write access to a different community and
# restrict it to your local network.
# Also remember to comment the syslocation and syscontact parameters later as
# otherwise they are still read only (see FAQ for net-snmp).
#

# First, map the community name "public" into a "security name"
#           sec.name            source              community
#com2sec notConfigUser     default             public

# Second, map the security name into a group name:
#           groupName           securityModel     securityName
#group     notConfigGroup    v1                  notConfigUser
#group     notConfigGroup    v2c                 notConfigUser

# Third, create a view for us to let the group have rights to:
# Open up the whole tree for ro, make the RFC 1213 required ones rw.
#           name                incl/excl         subtree mask(optional)
view      roview              included          .1
view      rwview              included          system.sysContact
view      rwview              included          system.sysName
view      rwview              included          system.sysLocation
view      rwview              included          interfaces.ifTable.ifEntry.ifAdminStatus
view      rwview              included          at.atTable.atEntry.atPhysAddress
view      rwview              included          at.atTable.atEntry.atNetAddress
view      rwview              included          ip.ipForwarding
view      rwview              included          ip.ipDefaultTTL
view      rwview              included          ip.ipRouteTable.ipRouteEntry.ipRouteDest
view      rwview              included          ip.ipRouteTable.ipRouteEntry.ipRouteIfIndex
view      rwview              included          ip.ipRouteTable.ipRouteEntry.ipRouteMetric1
view      rwview              included          ip.ipRouteTable.ipRouteEntry.ipRouteMetric2
view      rwview              included          ip.ipRouteTable.ipRouteEntry.ipRouteMetric3
view      rwview              included          ip.ipRouteTable.ipRouteEntry.ipRouteMetric4
view      rwview              included          ip.ipRouteTable.ipRouteEntry.ipRouteType
view      rwview              included          ip.ipRouteTable.ipRouteEntry.ipRouteAge
view      rwview              included          ip.ipRouteTable.ipRouteEntry.ipRouteMask
view      rwview              included          ip.ipRouteTable.ipRouteEntry.ipRouteMetric5
view                          rwview                                        included
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaIfIndex
view                          rwview                                        included
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaPhysAddress
view                          rwview                                        included
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaNetAddress
```

```
view                    rwview                                          included
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType
view    rwview          included        tcp.tcpConnTable.tcpConnEntry.tcpConnState
view                    rwview                                          included
egp.egpNeighTable.egpNeighEntry.egpNeighEventTrigger
view    rwview          included        snmp.snmpEnableAuthenTraps

# Finally, grant the group read-only access to the systemview view.
#          group          context sec.model sec.level prefix read     write    notif
access   notConfigGroup ""          any          noauth       exact    roview rwview none



############################################################
# System contact information
#

# It is also possible to set the sysContact and sysLocation system
# variables through the snmpd.conf file:

syslocation XX Server Room
syscontact SysMaster <icefired@netexpert.cn>

# Example output of snmpwalk:
#     % snmpwalk -v 1 localhost -c public system
#     system.sysDescr.0 = "SunOS name sun4c"
#     system.sysObjectID.0 = OID: enterprises.ucdavis.ucdSnmpAgent.sunos4
#     system.sysUpTime.0 = Timeticks: (595637548) 68 days, 22:32:55
#     system.sysContact.0 = "Me <me@somewhere.org>"
#     system.sysName.0 = "name"
#     system.sysLocation.0 = "Right here, right now."
#     system.sysServices.0 = 72


# ---------------------------------------------------------------------------


############################################################
# Process checks.
#
#   The following are examples of how to use the agent to check for
#   processes running on the host.    The syntax looks something like:
#
#   proc NAME [MAX=0] [MIN=0]
```

```
#
#   NAME:   the name of the process to check for.   It must match
#           exactly (ie, http will not find httpd processes).
#   MAX:    the maximum number allowed to be running.   Defaults to 0.
#   MIN:    the minimum number to be running.   Defaults to 0.

#
#   Examples (commented out by default):
#

#   Make sure mountd is running
proc mountd

#   Make sure there are no more than 4 ntalkds running, but 0 is ok too.
proc ntalkd 4

#   Make sure at least one sendmail, but less than or equal to 10 are running.
#proc sendmail 10 1

#   A snmpwalk of the process mib tree would look something like this:
#
# % snmpwalk -v 1 localhost -c public .1.3.6.1.4.1.2021.2
# enterprises.ucdavis.procTable.prEntry.prIndex.1 = 1
# enterprises.ucdavis.procTable.prEntry.prIndex.2 = 2
# enterprises.ucdavis.procTable.prEntry.prIndex.3 = 3
# enterprises.ucdavis.procTable.prEntry.prNames.1 = "mountd"
# enterprises.ucdavis.procTable.prEntry.prNames.2 = "ntalkd"
# enterprises.ucdavis.procTable.prEntry.prNames.3 = "sendmail"
# enterprises.ucdavis.procTable.prEntry.prMin.1 = 0
# enterprises.ucdavis.procTable.prEntry.prMin.2 = 0
# enterprises.ucdavis.procTable.prEntry.prMin.3 = 1
# enterprises.ucdavis.procTable.prEntry.prMax.1 = 0
# enterprises.ucdavis.procTable.prEntry.prMax.2 = 4
# enterprises.ucdavis.procTable.prEntry.prMax.3 = 10
# enterprises.ucdavis.procTable.prEntry.prCount.1 = 0
# enterprises.ucdavis.procTable.prEntry.prCount.2 = 0
# enterprises.ucdavis.procTable.prEntry.prCount.3 = 1
# enterprises.ucdavis.procTable.prEntry.prErrorFlag.1 = 1
# enterprises.ucdavis.procTable.prEntry.prErrorFlag.2 = 0
# enterprises.ucdavis.procTable.prEntry.prErrorFlag.3 = 0
# enterprises.ucdavis.procTable.prEntry.prErrMessage.1 = "No mountd process running."
# enterprises.ucdavis.procTable.prEntry.prErrMessage.2 = ""
# enterprises.ucdavis.procTable.prEntry.prErrMessage.3 = ""
# enterprises.ucdavis.procTable.prEntry.prErrFix.1 = 0
```

```
# enterprises.ucdavis.procTable.prEntry.prErrFix.2 = 0
# enterprises.ucdavis.procTable.prEntry.prErrFix.3 = 0
#
#   Note that the errorFlag for mountd is set to 1 because one is not
#   running (in this case an rpc.mountd is, but thats not good enough),
#   and the ErrMessage tells you what's wrong.   The configuration
#   imposed in the snmpd.conf file is also shown.
#
#   Special Case:   When the min and max numbers are both 0, it assumes
#   you want a max of infinity and a min of 1.
#


# ---------------------------------------------------------------------------


##########################################################
# Executables/scripts
#

#
#   You can also have programs run by the agent that return a single
#   line of output and an exit code.   Here are two examples.
#
#   exec NAME PROGRAM [ARGS ...]
#
#   NAME:       A generic name.
#   PROGRAM:    The program to run.   Include the path!
#   ARGS:       optional arguments to be passed to the program

# a simple hello world

#exec echotest /bin/echo hello world

# Run a shell script containing:
#
# #!/bin/sh
# echo hello world
# echo hi there
# exit 35
#
# Note:   this has been specifically commented out to prevent
# accidental security holes due to someone else on your system writing
# a /tmp/shtest before you do.   Uncomment to use it.
```

```
#
#exec shelltest /bin/sh /tmp/shtest

# Then,
# % snmpwalk -v 1 localhost -c public .1.3.6.1.4.1.2021.8
# enterprises.ucdavis.extTable.extEntry.extIndex.1 = 1
# enterprises.ucdavis.extTable.extEntry.extIndex.2 = 2
# enterprises.ucdavis.extTable.extEntry.extNames.1 = "echotest"
# enterprises.ucdavis.extTable.extEntry.extNames.2 = "shelltest"
# enterprises.ucdavis.extTable.extEntry.extCommand.1 = "/bin/echo hello world"
# enterprises.ucdavis.extTable.extEntry.extCommand.2 = "/bin/sh /tmp/shtest"
# enterprises.ucdavis.extTable.extEntry.extResult.1 = 0
# enterprises.ucdavis.extTable.extEntry.extResult.2 = 35
# enterprises.ucdavis.extTable.extEntry.extOutput.1 = "hello world."
# enterprises.ucdavis.extTable.extEntry.extOutput.2 = "hello world."
# enterprises.ucdavis.extTable.extEntry.extErrFix.1 = 0
# enterprises.ucdavis.extTable.extEntry.extErrFix.2 = 0

# Note that the second line of the /tmp/shtest shell script is cut
# off.   Also note that the exit status of 35 was returned.

# ---------------------------------------------------------------------------


###########################################################
# disk checks
#

# The agent can check the amount of available disk space, and make
# sure it is above a set limit.

# disk PATH [MIN=100000]
#
# PATH:   mount path to the disk in question.
# MIN:    Disks with space below this value will have the Mib's errorFlag set.
#           Default value = 100000.

# Check the / partition and make sure it contains at least 10 megs.

#disk / 10000

# % snmpwalk -v 1 localhost -c public .1.3.6.1.4.1.2021.9
# enterprises.ucdavis.diskTable.dskEntry.diskIndex.1 = 0
# enterprises.ucdavis.diskTable.dskEntry.diskPath.1 = "/" Hex: 2F
```

```
# enterprises.ucdavis.diskTable.dskEntry.diskDevice.1 = "/dev/dsk/c201d6s0"
# enterprises.ucdavis.diskTable.dskEntry.diskMinimum.1 = 10000
# enterprises.ucdavis.diskTable.dskEntry.diskTotal.1 = 837130
# enterprises.ucdavis.diskTable.dskEntry.diskAvail.1 = 316325
# enterprises.ucdavis.diskTable.dskEntry.diskUsed.1 = 437092
# enterprises.ucdavis.diskTable.dskEntry.diskPercent.1 = 58
# enterprises.ucdavis.diskTable.dskEntry.diskErrorFlag.1 = 0
# enterprises.ucdavis.diskTable.dskEntry.diskErrorMsg.1 = ""

# ---------------------------------------------------------------------------


############################################################
# load average checks
#

# load [1MAX=12.0] [5MAX=12.0] [15MAX=12.0]
#
# 1MAX:     If the 1 minute load average is above this limit at query
#           time, the errorFlag will be set.
# 5MAX:     Similar, but for 5 min average.
# 15MAX:    Similar, but for 15 min average.

# Check for loads:
#load 12 14 14

# % snmpwalk -v 1 localhost -c public .1.3.6.1.4.1.2021.10
# enterprises.ucdavis.loadTable.laEntry.loadaveIndex.1 = 1
# enterprises.ucdavis.loadTable.laEntry.loadaveIndex.2 = 2
# enterprises.ucdavis.loadTable.laEntry.loadaveIndex.3 = 3
# enterprises.ucdavis.loadTable.laEntry.loadaveNames.1 = "Load-1"
# enterprises.ucdavis.loadTable.laEntry.loadaveNames.2 = "Load-5"
# enterprises.ucdavis.loadTable.laEntry.loadaveNames.3 = "Load-15"
# enterprises.ucdavis.loadTable.laEntry.loadaveLoad.1 = "0.49" Hex: 30 2E 34 39
# enterprises.ucdavis.loadTable.laEntry.loadaveLoad.2 = "0.31" Hex: 30 2E 33 31
# enterprises.ucdavis.loadTable.laEntry.loadaveLoad.3 = "0.26" Hex: 30 2E 32 36
# enterprises.ucdavis.loadTable.laEntry.loadaveConfig.1 = "12.00"
# enterprises.ucdavis.loadTable.laEntry.loadaveConfig.2 = "14.00"
# enterprises.ucdavis.loadTable.laEntry.loadaveConfig.3 = "14.00"
# enterprises.ucdavis.loadTable.laEntry.loadaveErrorFlag.1 = 0
# enterprises.ucdavis.loadTable.laEntry.loadaveErrorFlag.2 = 0
# enterprises.ucdavis.loadTable.laEntry.loadaveErrorFlag.3 = 0
# enterprises.ucdavis.loadTable.laEntry.loadaveErrMessage.1 = ""
# enterprises.ucdavis.loadTable.laEntry.loadaveErrMessage.2 = ""
```

```
# enterprises.ucdavis.loadTable.laEntry.loadaveErrMessage.3 = ""

# --------------------------------------------------------------------


##########################################################
# Extensible sections.
#

# This alleviates the multiple line output problem found in the
# previous executable mib by placing each mib in its own mib table:

# Run a shell script containing:
#
# #!/bin/sh
# echo hello world
# echo hi there
# exit 35
#
# Note:    this has been specifically commented out to prevent
# accidental security holes due to someone else on your system writing
# a /tmp/shtest before you do.    Uncomment to use it.
#
# exec .1.3.6.1.4.1.2021.50 shelltest /bin/sh /tmp/shtest

# % snmpwalk -v 1 localhost -c public .1.3.6.1.4.1.2021.50
# enterprises.ucdavis.50.1.1 = 1
# enterprises.ucdavis.50.2.1 = "shelltest"
# enterprises.ucdavis.50.3.1 = "/bin/sh /tmp/shtest"
# enterprises.ucdavis.50.100.1 = 35
# enterprises.ucdavis.50.101.1 = "hello world."
# enterprises.ucdavis.50.101.2 = "hi there."
# enterprises.ucdavis.50.102.1 = 0

# Now the Output has grown to two lines, and we can see the 'hi
# there.' output as the second line from our shell script.
#
# Note that you must alter the mib.txt file to be correct if you want
# the .50.* outputs above to change to reasonable text descriptions.

# Other ideas:
#
# exec .1.3.6.1.4.1.2021.51 ps /bin/ps
# exec .1.3.6.1.4.1.2021.52 top /usr/local/bin/top
```

```
# exec .1.3.6.1.4.1.2021.53 mailq /usr/bin/mailq

# ---------------------------------------------------------------------------


##########################################################
# Pass through control.
#

# Usage:
#     pass MIBOID EXEC-COMMAND
#
# This will pass total control of the mib underneath the MIBOID
# portion of the mib to the EXEC-COMMAND.
#
# Note:    You'll have to change the path of the passtest script to your
# source directory or install it in the given location.
#
# Example:    (see the script for details)
#                 (commented out here since it requires that you place the
#                 script in the right location. (its not installed by default))

# pass .1.3.6.1.4.1.2021.255 /bin/sh /usr/local/local/passtest

# % snmpwalk -v 1 localhost -c public .1.3.6.1.4.1.2021.255
# enterprises.ucdavis.255.1 = "life the universe and everything"
# enterprises.ucdavis.255.2.1 = 42
# enterprises.ucdavis.255.2.2 = OID: 42.42.42
# enterprises.ucdavis.255.3 = Timeticks: (363136200) 42 days, 0:42:42
# enterprises.ucdavis.255.4 = IpAddress: 127.0.0.1
# enterprises.ucdavis.255.5 = 42
# enterprises.ucdavis.255.6 = Gauge: 42
#
# % snmpget -v 1 localhost public .1.3.6.1.4.1.2021.255.5
# enterprises.ucdavis.255.5 = 42
#
# % snmpset -v 1 localhost public .1.3.6.1.4.1.2021.255.1 s "New string"
# enterprises.ucdavis.255.1 = "New string"
#

# For specific usage information, see the man/snmpd.conf.5 manual page
# as well as the local/passtest script used in the above example.

# Added for support of bcm5820 cards.
```

```
pass .1.3.6.1.4.1.4413.4.1 /usr/bin/ucd5820stat

###########################################################
# Further Information
#
#   See the snmpd.conf manual page, and the output of "snmpd -H".
############ -- End -- ########
```

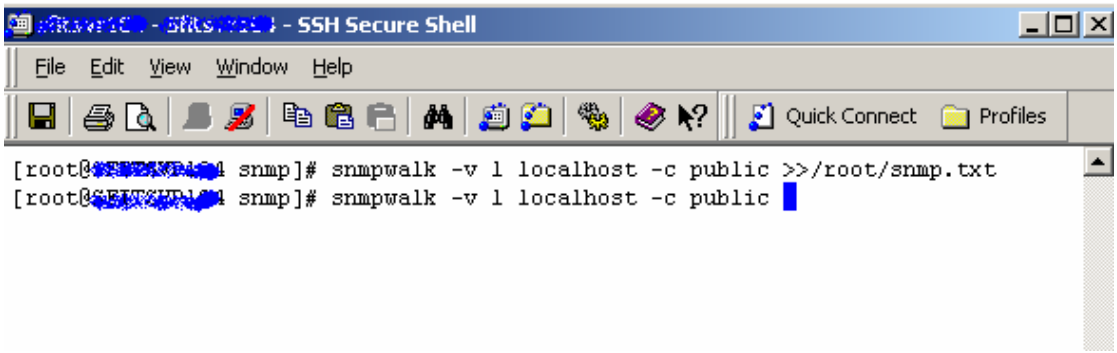
2.2 添加并监控 SNMP 设备

好了，经过前期努力，已经离成功不远了。朋友，如果你有耐心读到这里，我已经很佩服你了，也要恭喜你了！不要被前面长长的配置文件吓倒，因为我会准备好一份给你的，如果你需要的话，也可以 email 给我。

在使用 snmp 工具之前，我建议先用 Net-SNMP 自带的工具测试一下。再次提醒修改了 snmpd.conf 以后要重启一下 snmpd 进程。

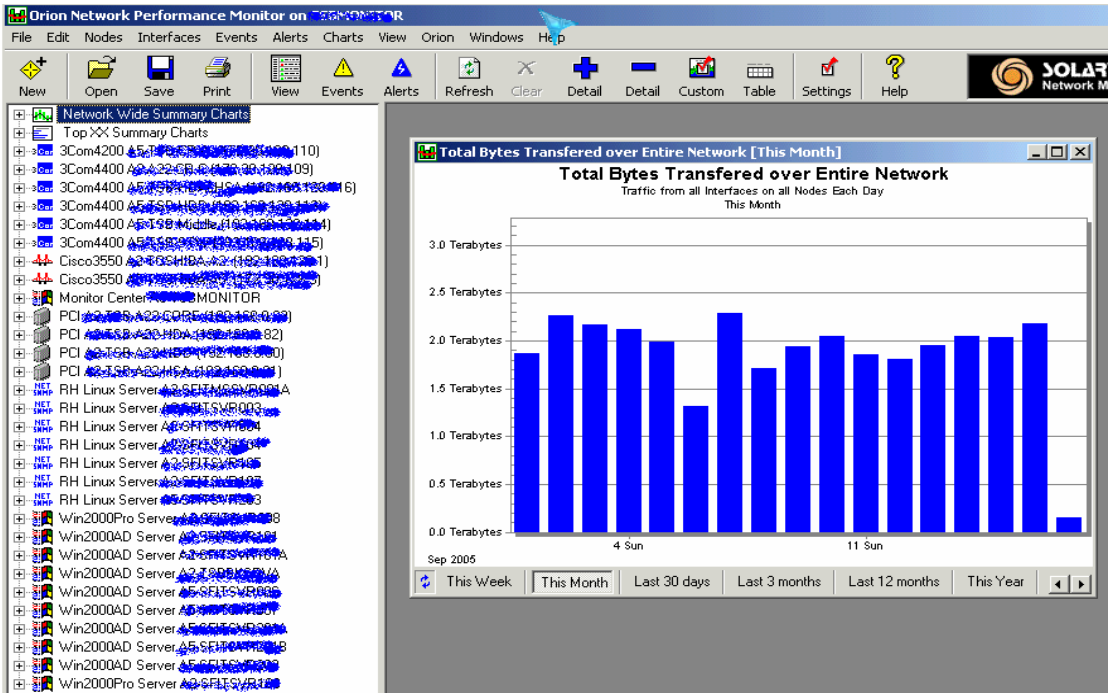
```
[root@[redacted] snmp]# service snmpd restart
Stopping snmpd:                                            [  OK  ]
Starting snmpd:                                            [  OK  ]
You have new mail in /var/spool/mail/root
```

使用 snmpwalk 来检查 snmp 是否配置正确：

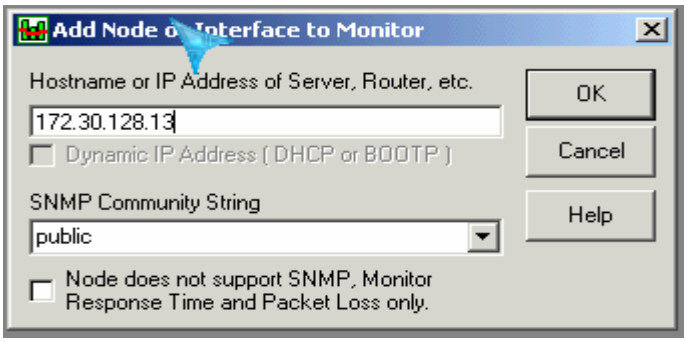


整个命令的输出大概有 3000~5000 行，可见 Net-SNMP 还是提供了非常丰富的信息，我们可以把他保存到一个文本仔细看看他到底提供了那些监控内容，也可以用来查看 OID.

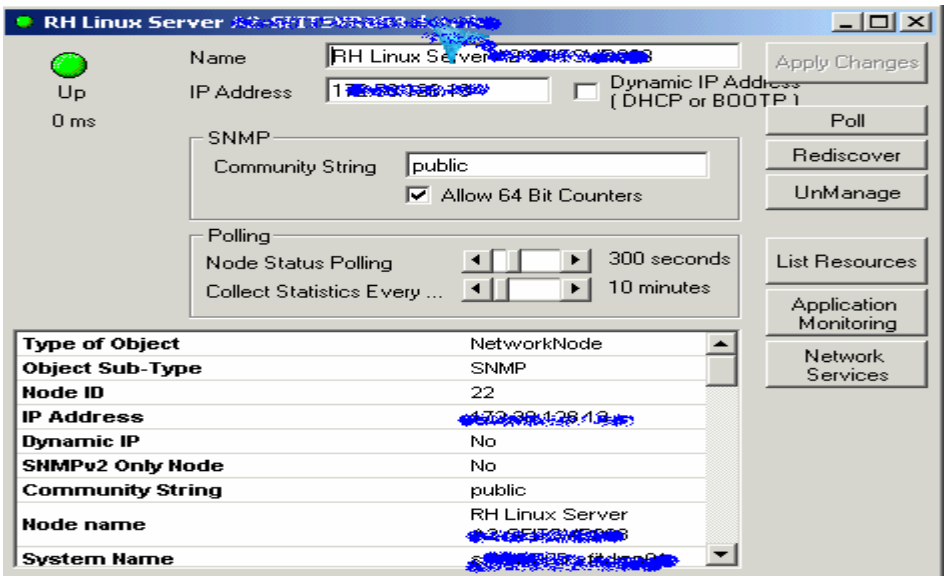
书归正转，我们拿 Solarwinds 出品的 Orion NPM 来监控此 Linux Server.



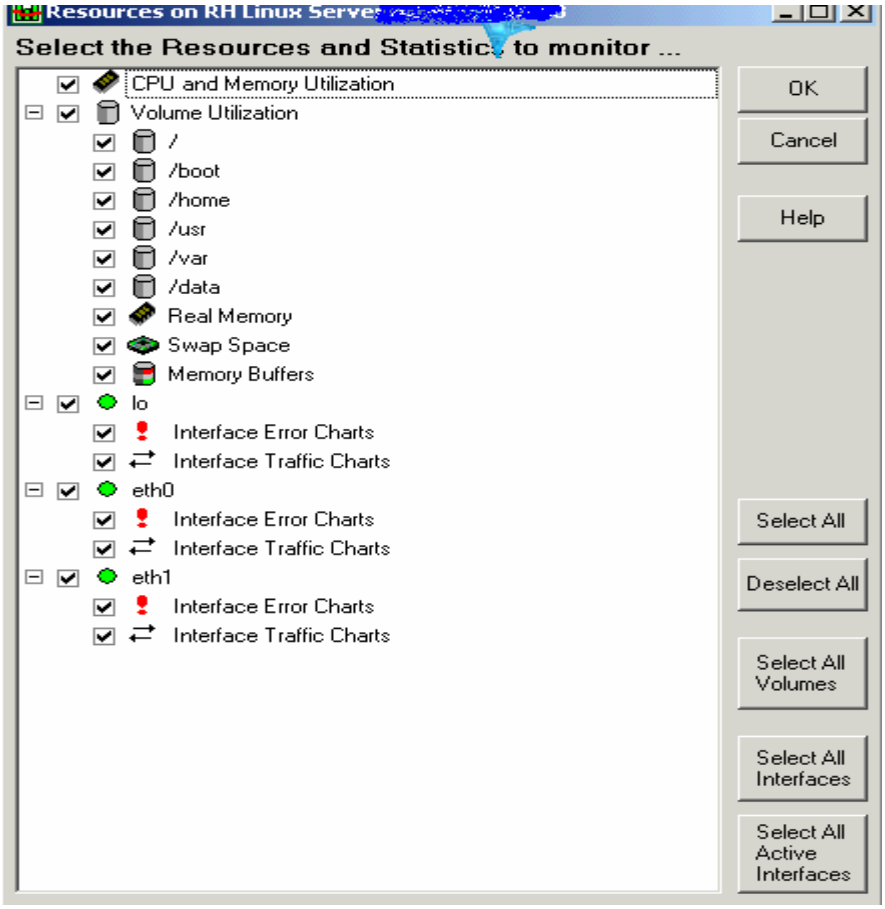
Nodes -> Add



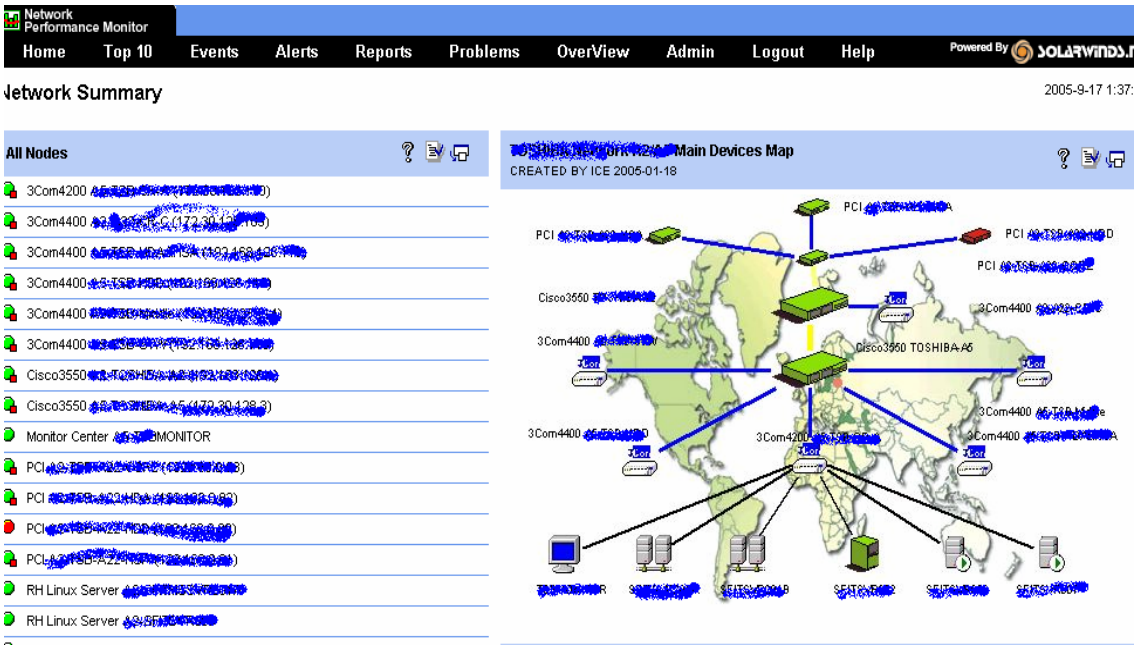
Nodes Detail

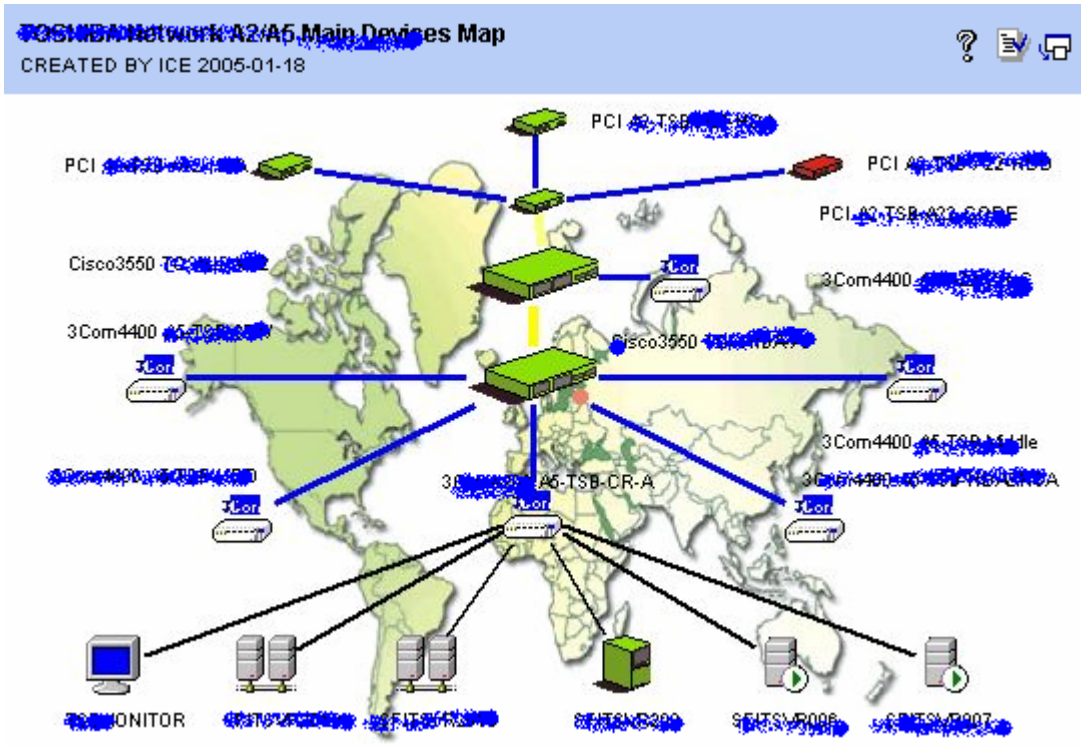


List Resources



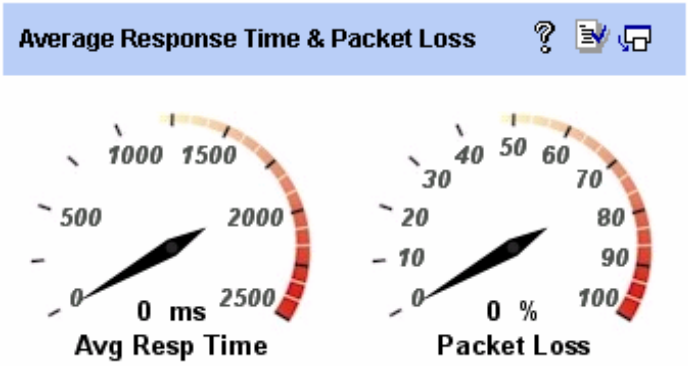
完成了！打开 web 看看？

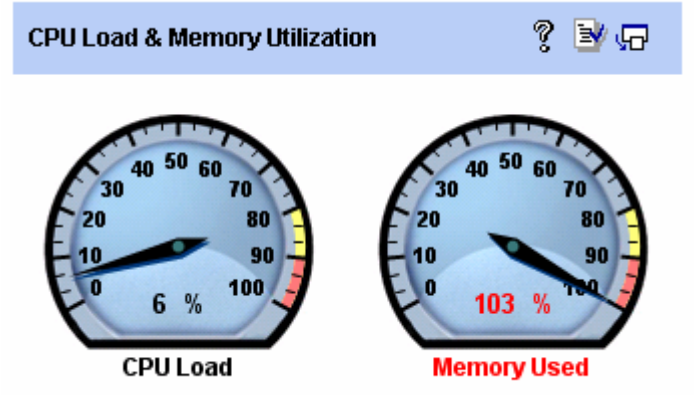




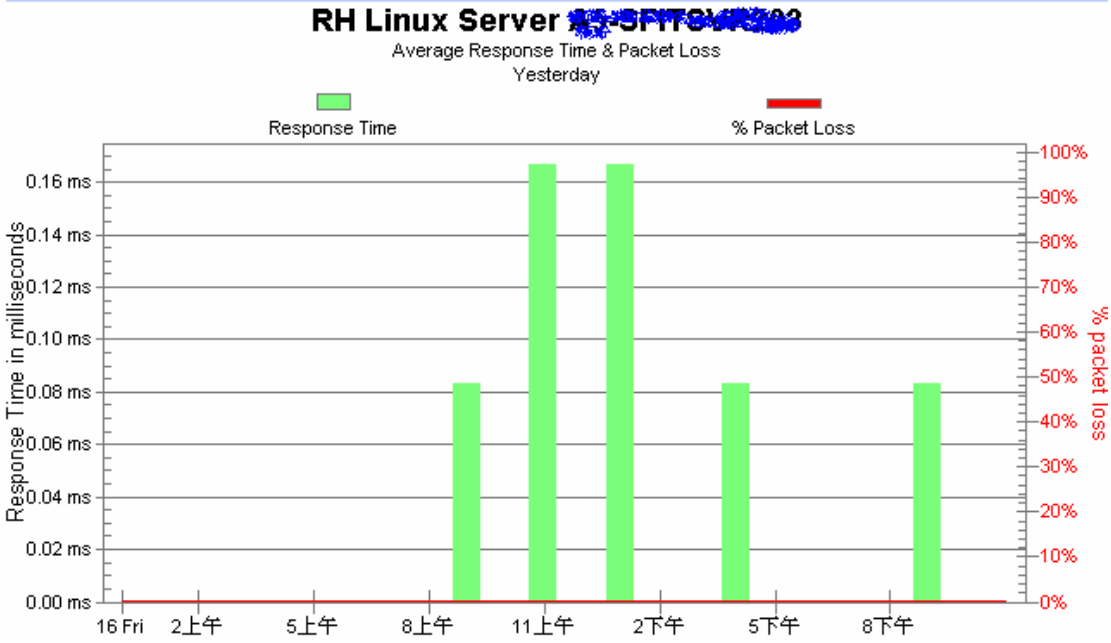
找到 Linux Server

Response Time & Packt Loss





Average Response Time & Packet Loss
YESTERDAY

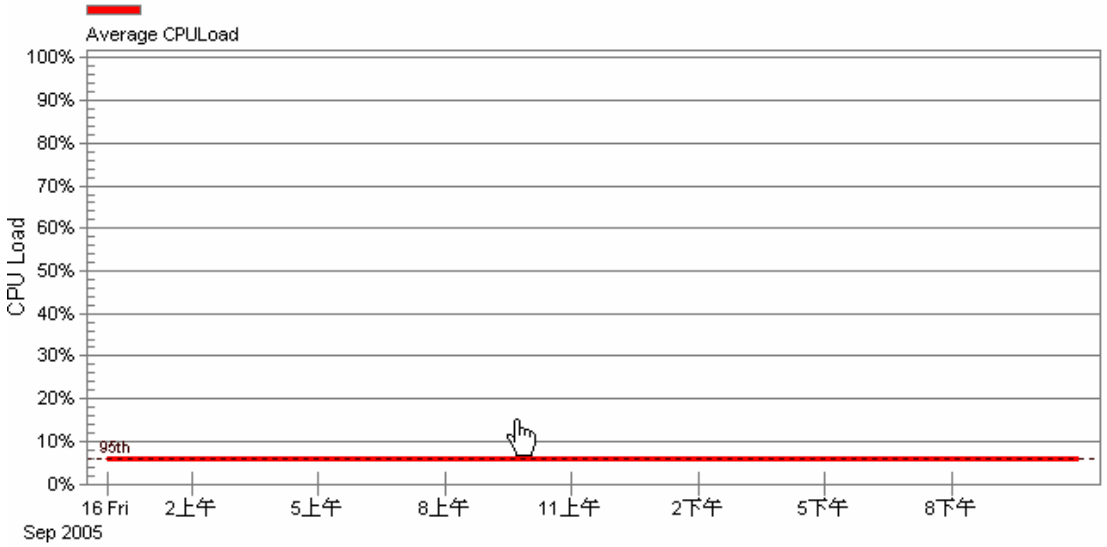


Node Details

Node Status		Node status is Up.
IP Address		
Dynamic IP		No
Machine Type	NET SNMP	net-snmp
DNS		
System Name		
Description		Linux 2.4.20-20.8smp #1 SMP Mon Aug 18 14:39:22 EDT 2003 i686
Location		
Contact		Admin
Last Boot		2005年8月10日 13:40
Operating System		
IOS Image		

Min/Max Average CPU Load
YESTERDAY

RH Linux Server [redacted]
Min/Max Average CPU Load
Yesterday



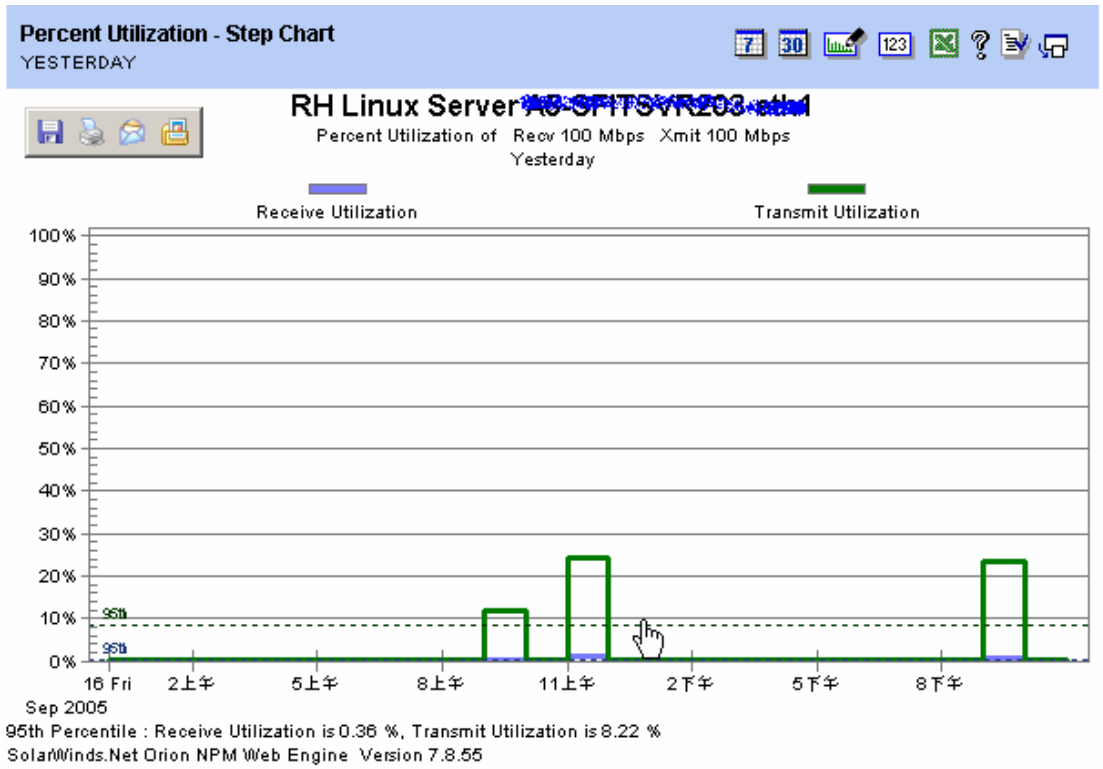
95th Percentile : Average CPULoad is 6.00 %
SolarWinds.Net Orion NPM Web Engine Version 7.8.55

Current Percent Utilization of each Interface

STATUS		INTERFACE	TRANSMIT	RECEIVE
Up		lo	0 %	0 %
Shutdown		eth0		
Up		eth1	0 %	0 %

Disk Volumes

VOLUME	SIZE	SPACE USED		
/	65.3 GB	7.5 GB	11 %	
/boot	99 MB	17 MB	17 %	
/data	134.6 GB	32.9 GB	24 %	
Memory Buffers	0 B	0 B		
Real Memory	2.0 GB	2.0 GB	100 %	
Swap Space	1.9 GB	97 MB	4 %	



不用文字说明，大家都能看懂了，呵呵，不过图片放的太多，有显摆和关税的嫌疑，希望大家不要见外。

[小 结]

以前看到论坛的文章里面说，只要是监控 Linux 的资源都要写脚本，或者要调用第三方软件，经过实践，我发现最简单的办法就是使用 Net-SNMP/UCD-SNMP, 设置简单，上手容易，对系统资源占用较少。

如果要用 mrtg 来监控 Linux ,只需找到相应的 OID 即可。
如：Linux RAM 对应的 OID 为：
.iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageRam
或： .1.3.6.1.2.1.25.2.1.2

Linux Swap Space 对应的 OID 为：
.iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageVirtualMemory
或：.1.3.6.1.2.1.25.2.1.3
至于如何使用MRTG,请参考 www.netexpert.cn上面的专题。

好长啊，到此为止吧，如果有什么不对之处请大家尽情拍砖，有什么好的建议和经验，请到论坛和我们一起分享！