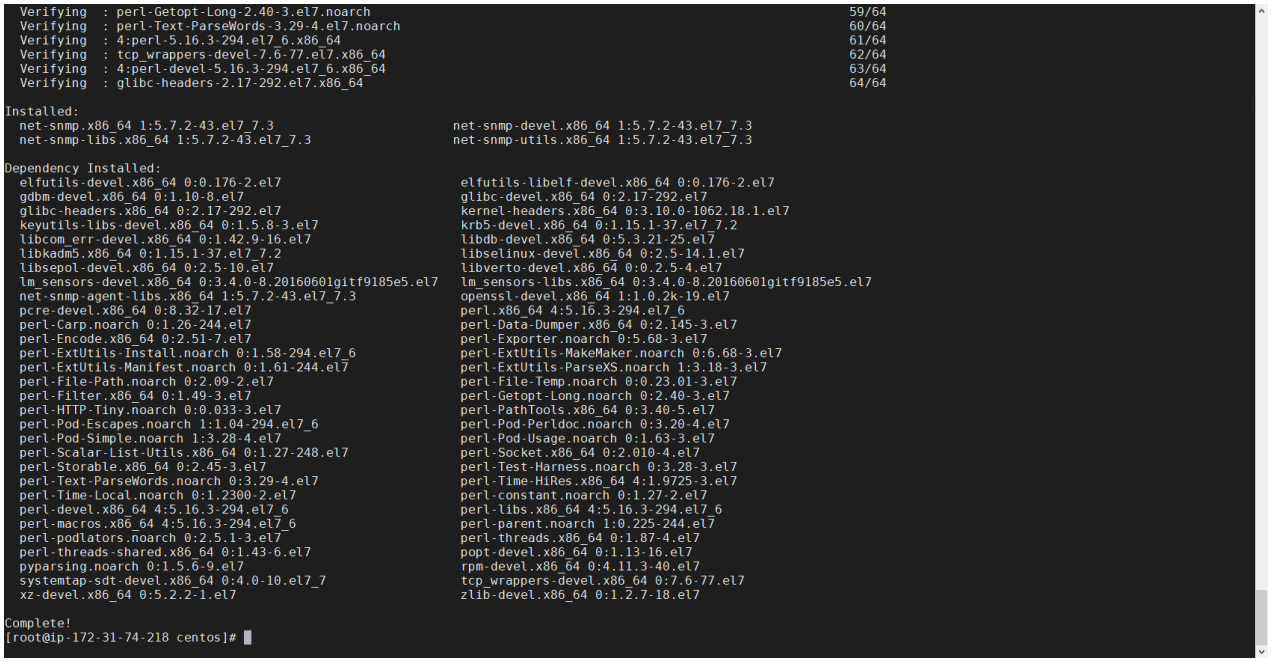
Nome: **Tiago Boeing**

Exercício com o protocolo SNMP

Orientações para a atividade em comandos práticos: Inicie sua máquina Linux, observando a sintaxe dos comandos em maiúsculas e minúsculas como aparecem. Como resposta, abaixo de cada item coloque um pequeno print do resultado do comando.

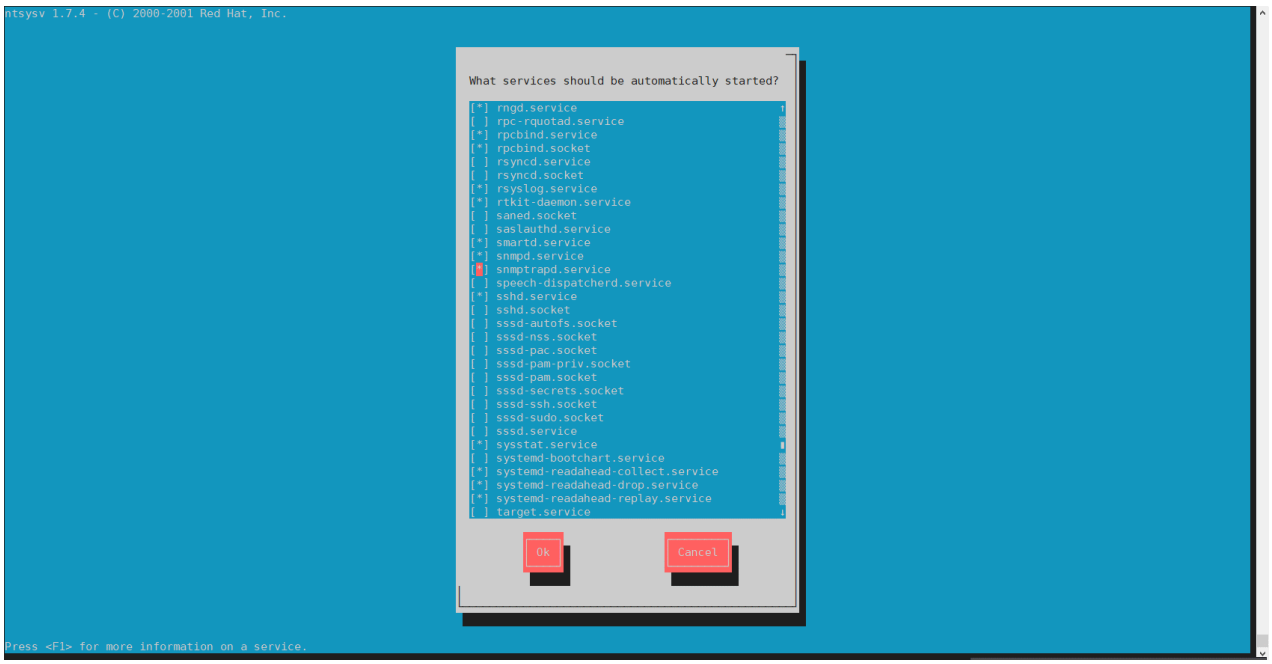
1. Utilizando a máquina Linux instalada no Virtualbox (CentoOS), instalar e habilitar o serviço de SNMP no Linux. Caso esteja utilizando outra distribuição confirme o comando para instalação dos pacotes.

yum -y install net-snmp net-snmp-devel net-snmp-utils net-snmp-libs



ntsysv

Selecione as opções “**snmpd**” e “**snmpdtrapd**” e clique em “**OK**” para iniciar o serviço automaticamente.



2. Utilizando boas práticas para Adminsitração de Serviços, utilize o comando cp para backup do arquivo original de configuração

cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.original

```
[root@ip-172-31-74-218 centos]# ntsysv
[root@ip-172-31-74-218 centos]# cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.original
[root@ip-172-31-74-218 centos]#
```

3. Para que um servidor responda às solicitações do protocolo SNMP v1 e v2c, configure os direitos da comunidade, que pode ter direito de leitura, escrita ou ambas. Utilizando editor:

/etc/snmp/snmpd.conf v1/v2c básico (snmpd.conf.01)
rocommunity public
rwcommunity private
^C

```
 GNU nano 2.3.1                    File: /etc/snmp/snmpd.conf                    Modified

# 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"
rocommunity public
rwcommunity private

#       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

####

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

Com a alteração do arquivo, reiniciar o serviço:

service snmpd restart

```
[root@ip-172-31-74-218 centos]# service snmpd restart
Redirecting to /bin/systemctl restart snmpd.service
```

4. Verifique o status do serviço por meio do comando:

service snmpdstatus

```
Redirecting to /bin/systemctl status snmpd.service
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/usr/lib/systemd/system/snmpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2020-04-14 00:15:15 UTC; 15s ago
 Main PID: 6063 (snmpd)
    Tasks: 1
   CGroup: /system.slice/snmpd.service
           └─6063 /usr/sbin/snmpd -LS0-6d -f

Apr 14 00:15:14 ip-172-31-74-218.ec2.internal systemd[1]: Starting Simple Network Management Protocol (SNMP) Daemon....
Apr 14 00:15:15 ip-172-31-74-218.ec2.internal snmpd[6063]: NET-SNMP version 5.7.2
Apr 14 00:15:15 ip-172-31-74-218.ec2.internal systemd[1]: Started Simple Network Management Protocol (SNMP) Daemon..
```

5. Utilizando o comando smnpget, realize a leitura do host: (usando as duas versões do protocolo SMNP)

snmpget -v 1 -c public localhost sysContact.0

```
[root@ip-172-31-74-218 centos]# snmpget -v 1 -c public localhost sysContact.0
SNMPv2-MIB::sysContact.0 = STRING: Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
```

snmpget -v 2c -c public localhost sysContact.0

```
[root@ip-172-31-74-218 centos]# snmpget -v 2c -c public localhost sysContact.0
SNMPv2-MIB::sysContact.0 = STRING: Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
```

6. Verifique a descrição das interfaces de rede:

snmpget -v 2c -c public localhost ifDescr.1

```
[root@ip-172-31-74-218 centos]# snmpget -v 2c -c public localhost ifDescr.1
IF-MIB::ifDescr.1 = STRING: lo
[root@ip-172-31-74-218 centos]#
```

snmpget -v 2c -c public localhost ifDescr.2

```
[root@ip-172-31-74-218 centos]# snmpget -v 2c -c public localhost ifDescr.2
IF-MIB::ifDescr.2 = STRING: ens5
```

7. Gravar o nome Aluno em sysContact

snmpset -v 2c -c private localhost sysContact.0 s Aluno

Tive problemas nesta etapa.

```
[root@ip-172-31-74-218 centos]# snmpset -v 2c -c private localhost sysContact.0 s Aluno
Error in packet.
Reason: notWritable (That object does not support modification)
Failed object: SNMPv2-MIB::sysContact.0

[root@ip-172-31-74-218 centos]# su snmpset -v 2c -c private localhost sysContact.0 s Aluno
su: invalid option -- 'v'

Usage:
 su [options] [-] [USER [arg]...]

Change the effective user id and group id to that of USER.
A mere - implies -l.   If USER not given, assume root.

Options:
 -m, -p, --preserve-environment  do not reset environment variables
 -g, --group <group>             specify the primary group
 -G, --supp-group <group>        specify a supplemental group

 -, -l, --login                  make the shell a login shell
 -c, --command <command>         pass a single command to the shell with -c
 --session-command <command>     pass a single command to the shell with -c
                                 and do not create a new session
 -f, --fast                      pass -f to the shell (for csh or tcsh)
 -s, --shell <shell>             run shell if /etc/shells allows it

 -h, --help     display this help and exit
 -V, --version  output version information and exit

For more details see su(1).
[root@ip-172-31-74-218 centos]#
```

8. Solicitando a próxima informação

snmpgetnext -v 2c -c public localhost sysContact.0

```
[root@ip-172-31-74-218 centos]# snmpgetnext -v 2c -c public localhost sysContact.0
SNMPv2-MIB::sysName.0 = STRING: ip-172-31-74-218.ec2.internal
```

9. Utilize o comando snmpwalk para percorrer toda a árvore, no galho system, lendo todas as informações do host:

snmpwalk -v 2c -c public localhost

```
DISMAN-EVENT-MIB::mteEventNotificationObjectsOwner."_snmpd"."_mteTriggerFalling' = STRING: _snmpd
DISMAN-EVENT-MIB::mteEventNotificationObjectsOwner."_snmpd"."_mteTriggerFired' = STRING: _snmpd
DISMAN-EVENT-MIB::mteEventNotificationObjectsOwner."_snmpd"."_mteTriggerRising' = STRING: _snmpd
DISMAN-EVENT-MIB::mteEventNotificationObjects."_snmpd"."_linkDown' = STRING: _linkUpDown
DISMAN-EVENT-MIB::mteEventNotificationObjects."_snmpd"."_linkUp' = STRING: _linkUpDown
DISMAN-EVENT-MIB::mteEventNotificationObjects."_snmpd"."_mteTriggerFailure' = STRING: _triggerFail
DISMAN-EVENT-MIB::mteEventNotificationObjects."_snmpd"."_mteTriggerFalling' = STRING: _triggerFire
DISMAN-EVENT-MIB::mteEventNotificationObjects."_snmpd"."_mteTriggerFired' = STRING: _triggerFire
DISMAN-EVENT-MIB::mteEventNotificationObjects."_snmpd"."_mteTriggerRising' = STRING: _triggerFire
NOTIFICATION-LOG-MIB::nlmConfigGlobalEntryLimit.0 = Gauge32: 1000
NOTIFICATION-LOG-MIB::nlmConfigGlobalAgeOut.0 = Gauge32: 1440 minutes
NOTIFICATION-LOG-MIB::nlmStatsGlobalNotificationsLogged.0 = Counter32: 0 notifications
NOTIFICATION-LOG-MIB::nlmStatsGlobalNotificationsBumped.0 = Counter32: 0 notifications
SCTP-MIB::sctpCurrEstab.0 = Gauge32: 0
SCTP-MIB::sctpActiveEstabs.0 = Counter32: 0
SCTP-MIB::sctpPassiveEstabs.0 = Counter32: 0
SCTP-MIB::sctpAborteds.0 = Counter32: 0
SCTP-MIB::sctpShutdowns.0 = Counter32: 0
SCTP-MIB::sctpOutOfBlues.0 = Counter32: 0
SCTP-MIB::sctpChecksumErrors.0 = Counter32: 0
SCTP-MIB::sctpOutCtrlChunks.0 = Counter64: 0
SCTP-MIB::sctpOutOrderChunks.0 = Counter64: 0
SCTP-MIB::sctpOutUnorderChunks.0 = Counter64: 0
SCTP-MIB::sctpInCtrlChunks.0 = Counter64: 0
SCTP-MIB::sctpInOrderChunks.0 = Counter64: 0
SCTP-MIB::sctpInUnorderChunks.0 = Counter64: 0
SCTP-MIB::sctpFragUsrMsgs.0 = Counter64: 0
SCTP-MIB::sctpReasmUsrMsgs.0 = Counter64: 0
SCTP-MIB::sctpOutSCTPPacks.0 = Counter64: 0
SCTP-MIB::sctpInSCTPPacks.0 = Counter64: 0
SCTP-MIB::sctpDiscontinuityTime.0 = Timeticks: (0) 0:00:00.00
SCTP-MIB::sctpRtoAlgorithm.0 = INTEGER: 0
SCTP-MIB::sctpRtoMin.0 = Gauge32: 0 milliseconds
SCTP-MIB::sctpRtoMax.0 = Gauge32: 0 milliseconds
SCTP-MIB::sctpRtoInitial.0 = Gauge32: 0 milliseconds
SCTP-MIB::sctpMaxAssocs.0 = INTEGER: 0
SCTP-MIB::sctpValCookieLife.0 = Gauge32: 0 milliseconds
SCTP-MIB::sctpMaxInitRetr.0 = Gauge32: 0
[root@ip-172-31-74-218 centos]#
```

10. Na versão 2c do protocolo SNMP foram incluídas algumas funções como bulkwalk, que traz um bloco de informações da tabela de forma mais rápida:

#snmpbulkget -v 2c -c public localhost sysLocation

```
[root@ip-172-31-74-218 centos]# snmpbulkget    -v  2c -c public localhost sysLocation
SNMPv2-MIB::sysLocation.0 = STRING: Unknown (edit /etc/snmp/snmpd.conf)
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (8) 0:00:00.08
SNMPv2-MIB::sysORID.1 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.6 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
```