实验 16：基于 SNMP 实现网络通信监控

一、实验目的

1、掌握 SNMP 的工作原理；
2、掌握 SNMP 监控的搭建配置；

二、实验学时

2 学时

三、实验类型

综合性

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

Windows 7 操作系统，安装 VirtualBox 桌面虚拟化软件。

3、网络

实验室局域网支持，能够访问校园网。

4、工具

无

五、实验理论

1、SNMP、MIB、OID 的基本概念；
2、网络监控系统实现的基本原理；

六、预备知识

1、CentOS 7 操作系统的基本使用方法（安装、网络配置、命令行的使用）；

2、Windows Server 2012 操作系统的基本使用方法（安装、网络配置）；

七、实验任务

本实验在 VirturalBox 虚拟化软件中部署虚拟机，完成整个监控系统的实现。

1、在 VirtualBox 中完成 CentOS 7 和 Windows Server 2012 系统虚拟主机的安装；

2、在 CentOS 7 系统的虚拟主机下配置 SNMP 服务；

3、在 Windows Server201 系统的虚拟主机下配置 SNMP 服务；

4、配置管理机并测试监控信息；

八、实验内容及其步骤

说明：

1. 本实验是在一台实体计算机上，通过 VirtualBox 软件完成；
2. 实体计算机的操作系统为 Windows 7；
3. 本实验基于 Cacti-1.1.30 构建网络监控系统；

任务 1：完成网络规划与设计

任务描述：

利用 VirtualBox 构建局域网，部署网络监控系统的虚拟机。

步骤 1：设计网络拓扑

为简化内容、突出重点，本实验不在 GNS3 中构建虚拟网络环境，而直接在 VirtualBox 中创建虚拟机，并通过“桥接网卡”方式，利用实体机所在的网络实现虚拟机之间的互访以及虚拟机访问互联网，具体设计如下。

1. 实体机可以访问互联网。

注意：此处要求实体机可以访问互联网，是为了实验过程中，Linux 系统安装 SNMP 服务组件时，虚拟机能够在线安装一些软件包。

2. 在 VirtualBox 创建 2 台虚拟机，Computer_1 虚拟机安装 CentOS7 操作系统，用来作为被监控计算机；Computer_2 虚拟机安装 Windows Server 2012 操作系统，用来作为被监控计算机。

3. 在 VirtualBox 中，将所有虚拟机网卡的连接方式设置成“桥接网卡”，使各台虚拟机接入实体机所在的网络，既可实现虚拟机之间的访问，也可以通过实体机访问互联网。

4. 实体机作为“管理机”，用来监控采集代理机的信息。

5. 本实验的拓扑结构如图 16-1 所示。

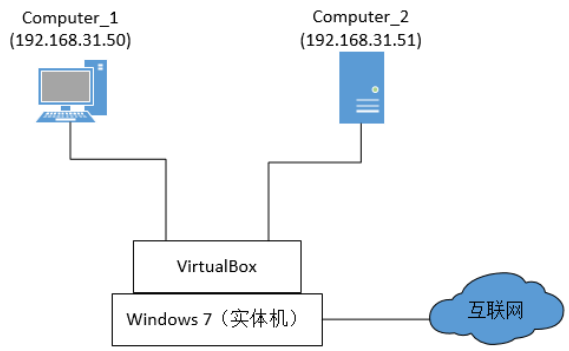

图 16-1 实验拓扑图

步骤 2：规划网络地址方案

根据对网络环境的设计，实验中所用到的网络为实体机所在网络。其网络参数（例如 IP 地址范围、默认网关等）可以从网络管理员处获得（可能是动态获得，也可能是静态设置），具体情况要根据实验环境的实际情况而定。此处各台虚拟机的网络参数设置见表 16-1。

表 16-1　IP 地址规划表

序号	主机名称	IP 地址	网关
1	实体机	192.168.31.100 / 24	192.168.31.1
2	Computer_1	192.168.31.50 / 24	192.168.31.1
3	Computer_2	192.168.31.51 / 24	192.168.31.1

任务 2：创建虚拟机

任务描述：

在 VirtualBox 中创建本实验所需要的 2 台虚拟机。

步骤 1：新建 Computer_1

新建一个名为 Computer_1 的虚拟机，安装 CentOS7 操作系统，作为被监控机使用。

步骤 2： 新建 Computer_2

新建一个名为 Computer_2 的虚拟机，安装 Windows Server 2012 操作系统，作为被监控机使用。

注意：具体操作步骤参见前期实验内容。

任务 3：在被监控主机 Computer_1（安装 CentOS7）上配置 SNMP 服务

任务描述：

被监控主机必须配置好 SNMP 服务，方可被监控到。因此，本任务是在被监控的虚拟机 Computer_1（安装 CentOS7 操作系统）上安装并配置 SNMP 服务。

步骤 1：设置 CentOS 系统的时间

本实验中，我们要通过 Cacti 系统定时采集被监控设备的信息，因此此处要查看一下被监控主机的时间，若不正确，需要修改过来。查看和修改 CentOS 时间的命令如下

```
#date                                          //显示系统时间
#hwclock                                       //显示硬件时间
#hwclock --set --date '2018-1-21 13:24:00'     //设置成正确的时间
#hwclock --hctosys                             //设置硬件时间与系统时间同步。
#hwclock -w                                    //保存时间
```

注意：在服务器上，时间的精确是非常重要的，通常情况下，使用时间修改命令 date -s ‘2015-8-31 13:15:00’ 即可立即生效，但这只是暂时的修改时间，机器重启之后系统时间依旧没有改变，原因是在 CentOS 中，时间分为系统时间和硬件时间，更改其一无法奏效的，必须两者都修改。

步骤 2：对虚拟主机进行网络配置，使其能够访问互联网

虚拟机 Computer_1 安装的是 CentOS7 操作系统，配置 SNMP 服务时，需要在线安装 SNMP 组件，因此首先必须保证该虚拟机能够连通互联网，并且可以实现虚拟机与实体机之间的互访。

（1）设置虚拟主机的网络连接方式

图 16-2 设置虚拟机

图 16-3 将虚拟机网络连接方式为“桥接网卡”

在 VirtualBox 界面左侧的虚拟机列表中，选中 Computer_1，单击【设置】按钮，见图 16-2。将虚拟机 Computer_1 的网络连接方式设置为【桥接网卡】，见图 16-3。其他选项为默认选项，点击【确认】保存配置。

（2）配置虚拟机的 IP 地址参数

启动虚拟机，根据任务 1 中的网络规划设计，修改 CentOS7 系统的网卡配置文件 ifcfg-enp0s3，将其 IP 地址设置为 192.168.31.50/24，默认网关 192.168.31.1。命令及配置如下：

```
# vi /etc/sysconfig/network-scripts/ifcfg-enp0s3
……
BOOTPROTO=static       //此处将 IP 地址的获得方式改为静态 static
……

DEVICE=enp0s3
IPADDR=192.168.31.50        //增加该语句，用“IPADDR=”来配置静态 IP 地址
NETMASK=255.255.255.0       //增加该语句，用“NETMASK”来配置子网掩码
GATEWAY=192.168.31.1        //增加该语句，用“GATEWAY=”来配置本机的默认网关
ONBOOT=yes                  //此处“yes”表示将上述配置修改为开机启动
```

配置好网络参数后，重启网络服务，使刚才的配置生效。

```
#systemctl restart network
```

（3）配置虚拟机的 DNS 参数

由于本实验中的虚拟机，配置是静态 IP，因此，必须配置 DNS 参数，否则 yum 命令无法正常工作。Linux 的 DNS 配置信息是在/etc/resolv.conf 文件中。

```
#vi /etc/resolv.conf

# Generated by NetworkManager
```

```
# No nameservers found; try putting DNS servers into your
# ifcfg files in /etc/sysconfig/network-scripts like so:
nameserver 114.114.114.114          // 此处添加 DNS 信息
nameserver 8.8.8.8                  //也可添加第 2 台 DNS 服务器信息
```

（4）测试网络连接效果

```
#ip add     //查看本机 IP 地址
```

可以看到本机 IP 地址已经修改为 192.168.31.50/24，见图 16-4

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
qlen 1000
    link/ether 08:00:27:c6:ef:df brd ff:ff:ff:ff:ff:ff
    inet 192.168.31.50/24 brd 192.168.31.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fec6:efdf/64 scope link
       valid_lft forever preferred_lft forever
[root@MiWiFi-R2D-srv ~]# _
```

图 16-4 查看虚拟机的 IP 地址

通过 Ping 命令的方式进行访问，若可以访问本地实体主机和互联网，则说明配置的地址起效，见图 16-5。

```
[root@localhost etc]# ping www.baidu.com
PING www.a.shifen.com (115.239.210.27) 56(84) bytes of data.
64 bytes from 115.239.210.27: icmp_seq=1 ttl=53 time=41.1 ms
64 bytes from 115.239.210.27: icmp_seq=2 ttl=53 time=41.0 ms
64 bytes from 115.239.210.27: icmp_seq=3 ttl=53 time=40.4 ms
64 bytes from 115.239.210.27: icmp_seq=4 ttl=53 time=41.3 ms
```

图 16-5 用 ping 命令测试网络连通性

步骤 3：安装 SNMP 服务组件

使用 SNMP 服务时，需要先安装 SNMP 服务的相关组件。

CentOS 及其它 RedHat 系列产品提供了 net-snmp 的二进制包。我们可以直接从源里安装。需要安装的组件除了 net-snmp 之外，还有 net-snmp-utils，net-snmp-libs 等。命令如下：

```
# yum –y install net-snmp-libs net-snmp net-snmp-utils net-snmp-devel net-snmp-perl
```

注意：

1. net-snmp-devel 是为了使用 net-snmp-config，net-snmp-utils 是为了使用 snmpwalk。
2. 在 yum 安装过程中，系统会提出某些组件是否安装，让你回答“y”或“n”，加上 -y 参数 指的是对所有问题都默认回答 yes，省去安装时的交互。

输入上述的命令后，可看到安装加载过程，见图 16-6，安装完成后可看到“Complete”字符。

```
[root@localhost etc]# yum -y install net-snmp net-snmp-libs net-snmp-utils net-snmp-dev
el net-snmp-perl
已加载插件: fastestmirror
base                                                     | 3.6 kB  00:00:00
extras                                                   | 3.4 kB  00:00:00
updates                                                  | 3.4 kB  00:00:00
```

图 16-6 安装 SNMP 服务组件

步骤 4：配置被监控机的 SNMP 配置文件

SNMP 服务的配置信息存放在/etc/snmp/snmpd.conf 文件中，我们需要对此文件进行修改，包括设置共同体名称，添加可访问信息的节点等操作。

（1）编辑打开 snmpd.conf 文件

```
# vi /etc/snmp/snmpd.conf
```

（2）配置 SNMP 服务的共同体名称

在配置文件中找到图 16-7 中的内容。

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

#        sec.name  source          community
com2sec notConfigUser  default       public
```

图 16-7 安装 SNMP 服务组件

说明：Linux vi 中查找字符内容的方法

使用 vi 编辑器编辑长文件时，常常是头昏眼花，也找不到需要更改的内容。这时，使用查找功能尤为重要。方法如下：

1、命令模式下输入“/字符串”，例如/community 表示查找“community”。

2、如果查找下一个，按“n”即可。

“community”字段名即表示 SNMP 共同体，其下为字段值，默认值是“public”，表示本机的 SNMP 共同体名称是 public。

“source”表示采集数据请求的来源，即允许谁从本机采集监控数据，其默认值是“default”，表示允许任何主机进行数据采集。

本实验中，将共同体名改为“My_Cacti”，将“source”的值由“default”改为 Cacti 监控主机的 IP 地址，即 192.168.31.100。见图 16-8.

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

#        sec.name  source          community
com2sec notConfigUser  192.168.31.100    My_Cacti
```

图 16-8 修改共同体名称

注意：

1. 在 SNMP v1 版本中，引入了共同体的概念。在进行监控数据采集时，必须知道被监控设备的共同体名称，因此，将共同体名称修改为你自己才知道的字符串，是一种安全措施；
2. 修改“source”的值，只允许指定的设备进行监控数据的采集，也是一种安全措施。
3. SNMP v2 版本使用共同体名称。v1 没有安全措施，v3 使用认证和加密的机制实现安全。

（3）添加可访问信息的节点

继续在 snmpd.conf 文件中找到图 16-9 所示内容，其下添加“.1”的访问节点，表示可访问到 OID 值为.1.*的对应信息，从而增加可访问信息的节点。

完成上述配置后，点击【Esc】键退出编辑状态，然后在配置文件中输入“：wq”，点击回车，保存配置文件并退出。

```
# 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
view     systemview     included    .1     // 添加此行
```

图 16-9 添加可访问信息的节点

注意：SNMP 中，MIB（管理信息库）是树形目录，此处的“subtree”字段值，用来定义可以访问到（即监控到）的设备信息节点，例如定义为.1.3.6，就表示只能够访问 1.3.6.*的 OID 对应的信息。

步骤 5：安装配置防火墙

SNMP 的访问是使用 UDP 协议，并通过 161 端口，CentOS 7 系统中默认安装的防火墙为 Firewall 防火墙，默认情况下，防火墙禁止 SNMP 的访问。因此，要想实现 SNMP 的访问，需要在防火墙上设置允许规则。

由于 firewall 防火墙操作复杂，因此，本实验中使用 IPTables 防火墙，其具体操作步骤如下。

（1）禁用 Firewall 防火墙。

由于在 CentOS 7 系统中默认安装的防火墙为 Firewall 防火墙，为避免防火墙冲突，需要禁止系统自带防火墙，主要的命令如下。

```
# systemctl stop firewalld
  //禁止 Firewall 防火墙
# systemctl disable firewalld.service
  //禁止开机启动 Firewall 防火墙
# systemctl status firewalld
  //查看 Firewall 防火墙状态
```

可通过查看防火墙的状态，判断该防火墙是否被禁用，如图 16-10 所示。

```
[root@localhost ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since 日 2018-01-21 16:15:23 CST; 4s ago
  Process: 602 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS (code=exited, status=
CESS)
 Main PID: 602 (code=exited, status=0/SUCCESS)

1月 21 16:14:02 localhost.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon...
1月 21 16:14:05 localhost.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.
1月 21 16:15:23 localhost.localdomain systemd[1]: Stopping firewalld - dynamic firewall daemon...
1月 21 16:15:23 localhost.localdomain systemd[1]: Stopped firewalld - dynamic firewall daemon.
[root@localhost ~]#
```

图 16-10 查看 Firewall 防火墙状态

（2）安装 IPTables 防火墙

下载并安装 IPTables 防火墙及防火墙服务，主要命令如下。

```
# yum install   iptables iptables-services
  //下载并安装 IPTables 防火墙及服务
```

安装成功后，系统会给出提示，见图 16-11。

```
Running transaction
  Updating   : iptables-1.4.21-18.2.el7_4.x86_64                          1/3
  Installing : iptables-services-1.4.21-18.2.el7_4.x86_64                 2/3
  Cleanup    : iptables-1.4.21-13.el7.x86_64                              3/3
  Verifying  : iptables-1.4.21-18.2.el7_4.x86_64                          1/3
  Verifying  : iptables-services-1.4.21-18.2.el7_4.x86_64                 2/3
  Verifying  : iptables-1.4.21-13.el7.x86_64                              3/3

Installed:
  iptables-services.x86_64 0:1.4.21-18.2.el7_4

Updated:
  iptables.x86_64 0:1.4.21-18.2.el7_4

Complete!
[root@localhost sysconfig]#
```

图 16-11 成功安装 iptables 防火墙

（3）配置防火墙，添加防火墙规则

安装成功 iptables 后，在 /etc/sysconfig 目录中会生成 iptables 文件，编辑该文件，设置 iptables 防火墙规则。主要配置如下所示。

```
# vi /etc/sysconfig/iptables
  //打开 IPTables 防火墙的配置文件
-A INPUT –p udp -m state --state NEW –m udp --dport 161 –j ACCEPT
  //添加 161 端口通过防火墙的规则
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
  //添加允许 80 端口通过防火墙的规则
```

修改的配置文件结果如图 16-12 所示。添加规则完成后，在配置文件中输入“：wq”，点击回车，保存规则并退出。

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 161 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

图 16-12 在 iptables 防火墙配置文件中添加规则

注意：防火墙规则的顺序，顺序不对，规则不起作用。

步骤 6：重启相关服务

经过上述的配置之后，需要重启相关服务，使 SNMP 客户端的配置生效，具体命令如下。

```
# systemctl restart snmpd.service          //重启 SNMP 服务
# systemctl enable snmpd.service           //配置 SNMP 服务开机启动
# systemctl restart iptables.service       //重启 IPTables 防火墙
# systemctl enable iptables.service        //配置 IPTables 防火墙开机启动
```

经过上述的步骤，完成对 CentOS 7 系统虚拟主机的 SNMP 服务配置。

步骤 7：测试 SNMP 服务配置效果

我们可以先测试一下被监控主机 Computer_1 的 SNMP 服务的配置效果，看一看是否能够通过网络监控到相关数据，从而也保证了后面实验过程的顺利进行。

我们可以在本地实体主机上（安装 Windows 7 操作系统）安装 NET-SNMP 软件，通过该软件进行 SNMP 数据采集，具体操作步骤如下。

（1）下载并安装 Net-SNMP

可通过 Net-SNMP 官方网站 http://www.net-snmp.org（见图 16-13）下载获得安装软件 net-snmp-5.6.1.1-1.x86。

图 16-13 从 net-snmp 官网上下载软件

根据提示，在本地实体机上完成安装 Net-SNMP 软件，见图 16-14、19-15。

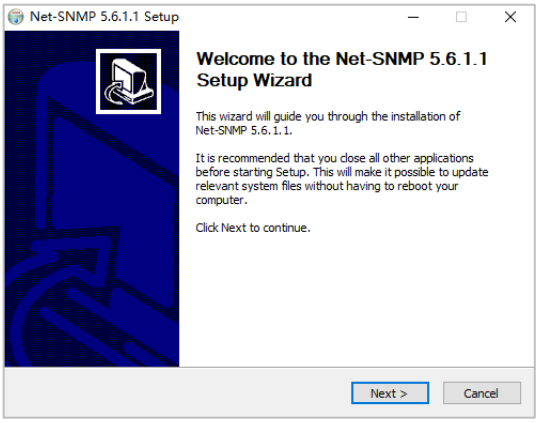

图 16-14 开始安装 net-snmp

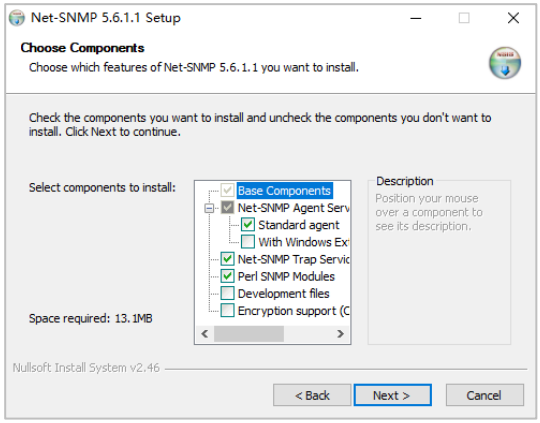

图 16-15 选择 net-snmp 组件

（2）使用 Net-SNMP 软件进行数据采集

通过 Windows 的命令行方式，对 CentOS 7 系统进行数据采集，具体操作步骤如下。

第一步：打开本地实体主机的【运行】程序，输入“cmd”，回车运行，打开本地主机的命令行界面。

第二步：在命令行中输入如下命令

snmpwalk -v 2c -c My_Cacti 192.168.31.50 .1.3.6.1.4.1.2021.4

此命令是通过 Net-SNMP 工具向被监控主机发送了一个 SNMP 请求，其中，snmpwalk 为命令动词，-v 2c 表示使用 SNMP v2，My_Cacti 是被监控主机的共同体名称，192.168.31.50 是被监控主机的 IP 地址，.1.3.6.1.4.1.2021.4 是 MIB 的值（即 OID 值，此处表示获取内存相关信息）。其结果见图 16-16。说明被监控主机 Computer_1 的 SNMP 配置是正确的。

```
C:\Users>snmpwalk -v 2c -c My_Cacti 192.168.31.50 .1.3.6.1.4.1.2021.4
UCD-SNMP-MIB::memIndex.0 = INTEGER: 0
UCD-SNMP-MIB::memErrorName.0 = STRING: swap
UCD-SNMP-MIB::memTotalSwap.0 = INTEGER: 839676 kB
UCD-SNMP-MIB::memAvailSwap.0 = INTEGER: 839676 kB
UCD-SNMP-MIB::memTotalReal.0 = INTEGER: 501080 kB
UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 241792 kB
UCD-SNMP-MIB::memTotalFree.0 = INTEGER: 1081468 kB
UCD-SNMP-MIB::memMinimumSwap.0 = INTEGER: 16000 kB
UCD-SNMP-MIB::memShared.0 = INTEGER: 4464 kB
UCD-SNMP-MIB::memBuffer.0 = INTEGER: 764 kB
UCD-SNMP-MIB::memCached.0 = INTEGER: 167456 kB
UCD-SNMP-MIB::memSwapError.0 = INTEGER: noError(0)
UCD-SNMP-MIB::memSwapErrorMsg.0 = STRING:
```

图 16-16 通过 net-snmp 获取被监控主机的内存相关信息

还可以使用 snmpget 命令获取指定的信息，例如获取内存总大小，见图 16-17。

```
C:\Users>snmpget -v 2c -c My_Cacti 192.168.31.50 .1.3.6.1.4.1.2021.4.5.0
UCD-SNMP-MIB::memTotalReal.0 = INTEGER: 501080 kB
```

图 16-17 通过 net-snmp 获取被监控主机的内存大小

注意：

1. 命令中的 OID 值可以互联网上查询；
2. Windows 操作系统和 Linux 操作系统针对相同对象的 OID 值通常并不相同，查询时要注意；
3. snmpwalk 是对 OID 值的遍历，例如某个 OID 值下面有 N 个节点，则依次遍历出这 N 个节点的值；snmpget 是取具体的 OID 的值，适用于 OID 值是一个叶子节点的情况。例如，将图 16-16 中的命令动词换成 snmpget，则结果出现错误，见图 16-18。

```
C:\Users>snmpget -v 2c -c My_Cacti 192.168.31.50 .1.3.6.1.4.1.2021.4
UCD-SNMP-MIB::memory = No Such Object available on this agent at this OID
```

图 16-18 使用 snmpget 命令访问非叶子节点的结果

表 19-2 OID 值举例

OID 值	描述	适用操作系统
.1.3.6.1.2.1.1.1.0	获取系统基本信息	Linux / Windows
.1.3.6.1.2.1.1.3.0	监控时间	Linux / Windows
.1.3.6.1.2.1.2.1.0	网络接口的数目	Linux / Windows
.1.3.6.1.2.1.2.2.1.3	网络接口类型	Linux / Windows
.1.3.6.1.2.1.2.2.1.6	接口的物理地址	Linux / Windows
.1.3.6.1.2.1.2.2.1.10	接口收到的字节数	Linux / Windows
.1.3.6.1.2.1.25.2.3.1.4	硬盘簇的大小	Linux / Windows
.1.3.6.1.2.1.25.2.3.1.5	硬盘簇的的数目	Linux / Windows
.1.3.6.1.2.1.25.2.3.1.6	使用多少，跟总容量相除就是占用率	Linux / Windows
. 1.3.6.1.4.1.2021.11.10.0	系统 CPU 百分比	Linux

. 1.3.6.1.4.1.2021.11.11.0	空闲 CPU 百分比	Linux

任务 4：在被监控主机 Computer_2（Windows Server2012）上配置 SNMP 服务

任务描述：

被监控主机必须配置好 SNMP 服务，方可被监控到。因此，本任务是在被监控的虚拟机 Computer_1（安装 Windows Server2012）上安装并配置 SNMP 服务。

步骤 1：测试 Computer_2 的网络连通性

（1）配置 IP 地址

根据任务 1 中的规划，给本虚拟机配置 IP 地址 192.168.31.51/24 。

（2）测试网络连通性

通过 Ping 命令的方式进行访问，若可以访问本地实体主机和互联网，则说明配置的地址起效。

步骤 2：在 Windows Server 2012 上安装 SNMP

（1）在虚拟主机中，依次点击打开【控制面板】→【程序】→【启用或关闭 Windows 功能】，如图 16-19 所示。

图 16-19 启用或关闭 Windows 功能

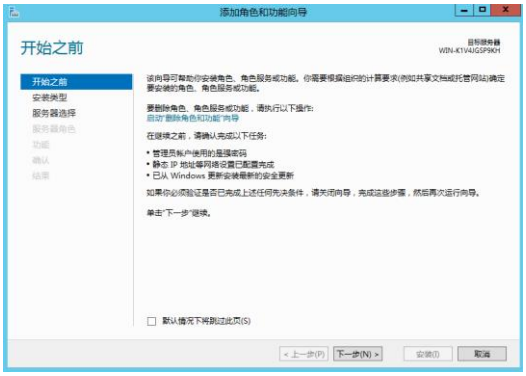

图 16-20 添加角色和功能向导界面

（2）点击【启用或关闭 Windows 功能】按钮，系统将弹出【添加角色和功能向导】的界面，在【开始之前】选项界面中，点击【下一步（N）】按钮开始添加角色和功能。见图 16-21。

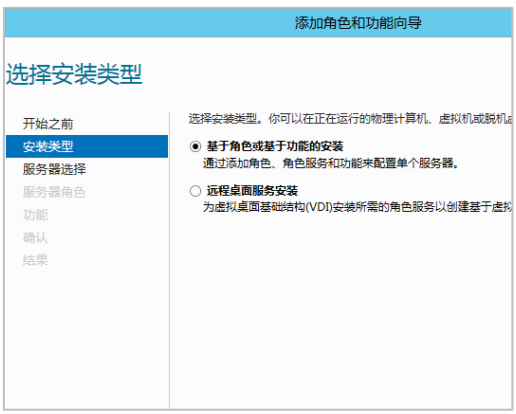

图 16-21 选择安装类型

图 16-22 选择服务器

（3）在接下来的【安装类型】界面中，选择右侧管理界面中的【基于角色或基于功能的安装】选项，点击【下一步（N）】按钮继续安装，见图 16-21

（4）在【服务器选择】界面中，选择点击【从服务器池中选择服务器】选项，在界面下的【服务器池】中选择服务器，本实验选择虚拟主机 192.168.31.51，点击【下一步（N）】按钮继续，如图 16-22。

图 16-23 选择服务器角色

图 16-24 添加 SNMP 服务功能

（5）在【服务器角色】选项的右侧管理界面中，选择添加角色。本实验不安装服务器角色，所以本处不进行配置，点击【下一步（N）】按钮，如图 16-23 所示。

（6）在【功能】选项的右侧管理窗体中，选择要安装的功能，选择【SNMP 服务】中【SNMP WMI 提供程序】选项，如图 16-24 所示。选择之后，系统将选择是否安装工具来管理此功能，点击【添加功能】按钮进行安装，如图 16-25 所示。添加工具完成后，在【功能】选项界面中，点击【下一步（N）】，完成对功能的添加。

图 16-25 为服务添加工具

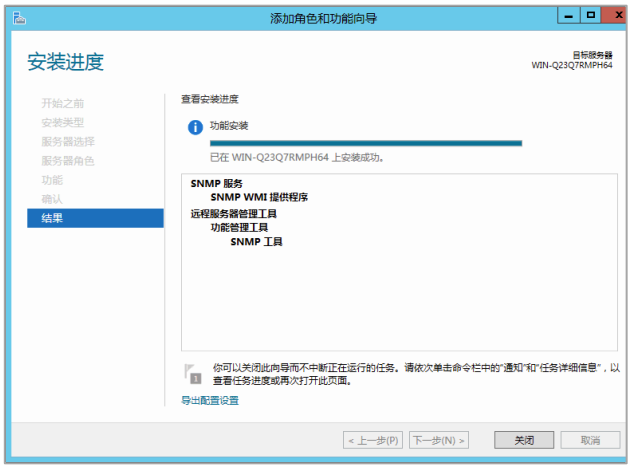

图 16-26 添加功能安装完成

（7）在【结果】选项界面中，可查看功能安装的进度。当安装完成后，点击【关闭】按钮完成安装，如图 16-26 所示。

步骤 3：配置 SNMP 服务

当完成 SNMP 安装之后，需对被监控主机的 SNMP 服务进行配置，具体操作步骤如下。

（1）打开“服务”选项

打开虚拟主机的【控制面板】，找到【系统和安全】→【管理工具】→【服务】，见图 16-27，双击打开【服务】，或者在【运行】中输入“services.msc”回车（见图 16-28），打开本地服务管理界面，见图 16-28。

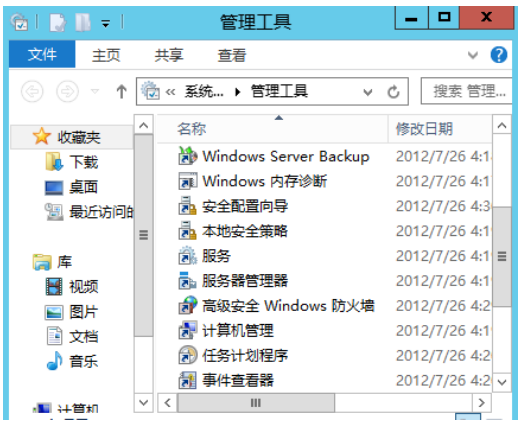

图 16-27 找到控制面板→管理工具→【服务】

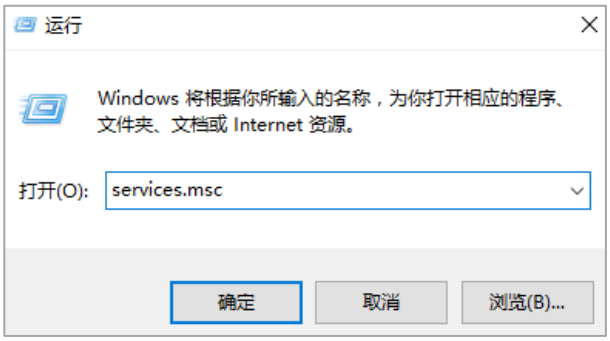

图 16-28 在【运行】中启动“服务”程序

在“服务”界面中，找到“SNMP Service”，见图 16-29。

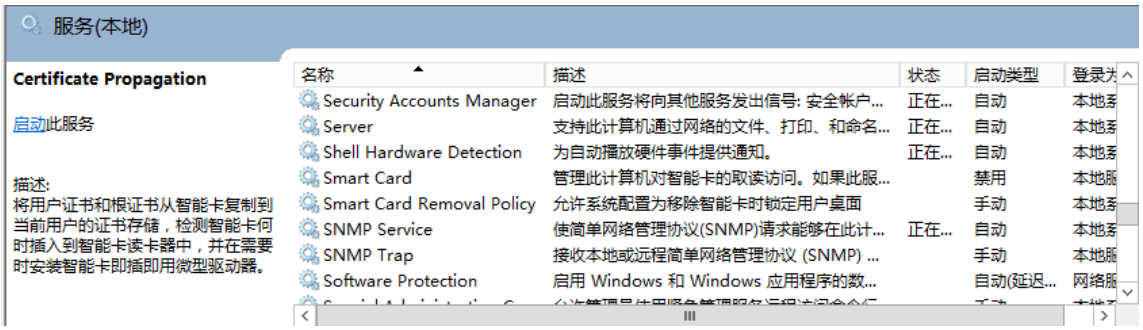

图 16-29 在【服务】中找到“SNMP Service”

（2）配置“SNMP Service”选项

① 双击打开“SNMP Service”选项，并配置 SNMP 服务，见图 16-30。

图 16-30 SNMP Service 选项

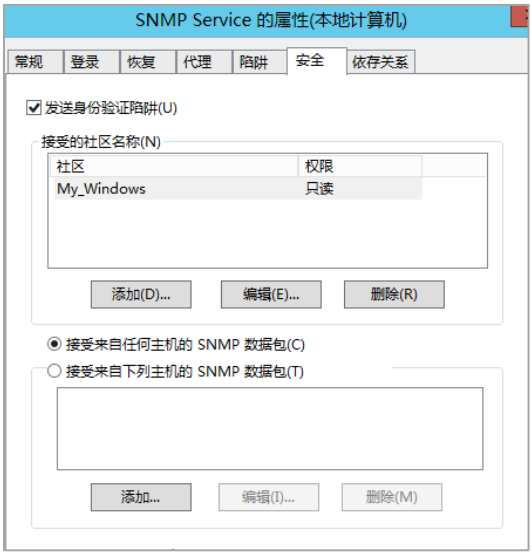

图 16-31 配置共同体名称

②在 SNMP Service 服务界面中，点击【安全】→【接受的社区名称（N）】→【添加

（D）...】,添加共同体名称。将本虚拟机的共同体（社区）名称设置为 My_Windows，权限设置为“只读”，并选择【接受来自任何主机的 SNMP 数据包（C）】，见图 16-31。

③选择【应用】和【确定】按钮，完成对 SNMP 服务的配置。

④在【服务】管理界面中，选择“SNMP Service”服务，点击【重启动此服务】，对 SNMP 服务进行重新启动，使得配置生效。如图 16-32 所示。

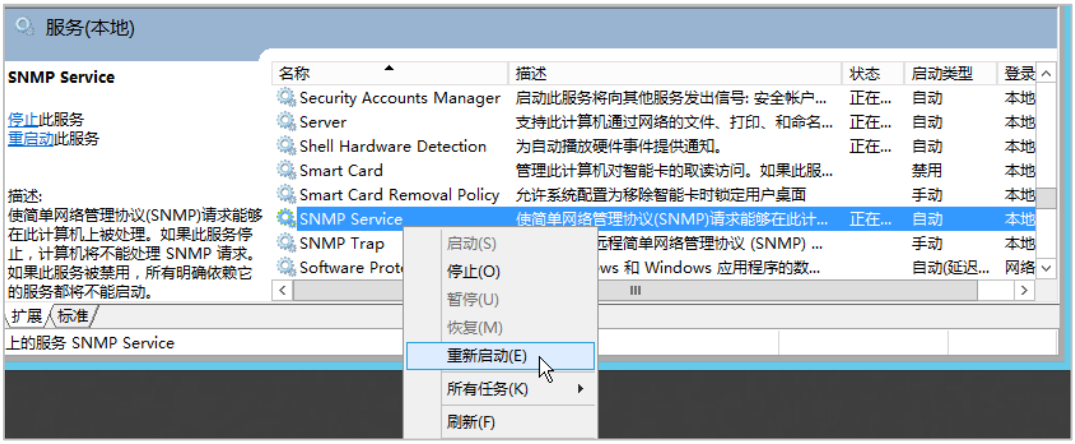

图 16-32 重新启动 SNMP Service 服务

通过上述的配置，Windows Server 2012 操作系统的虚拟主机可以通过共同体名称（My_Windows）响应任何能够访问本主机的 SNMP 请求。

步骤 4：测试 SNMP 服务配置效果

在本地实体主机上，使用以下命令测试虚拟机 Computer_2（安装 Windows Server 2012）的 SNMP 安装结果。

```
C:\Users>snmpget -v 2c -c My_Windows 192.168.31.51 .1.3.6.1.2.1.1.1.0
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: Intel64 Family 6 Model 78
Stepping 3 AT/AT COMPATIBLE - Software: Windows Version 6.2 (Build 9200
Multiprocessor Free)
```

九、实验分析

1、和 SNMP v1、v2 相比，SNMP v3 在提高安全性方面，做了哪些改进？