

Lab: Network Management

In this lab, we are going to configure SNMP services on fw01, web01 and ad01. We are going to configure a network monitoring system called nmon01, where we will query our systems for SNMP properties.

Prerequisites

- Set up web01: 10.0.5.200/24, web01-Name, does not join AD, everything else
- AD is happy, & DNS Names are resolving

Configure fw01's SNMP Service

- Figure out how to **enable** SNMP services on pfSense. Fill out the SNMP Daemon settings, and pay attention to the community string. Make sure to Bind SNMP to the LAN interface. Use your name for the System Contact.

SNMP Daemon

Enable ☒ Enable the SNMP Daemon and its controls

SNMP Daemon Settings

Polling Port

161

Enter the port to accept polling events on (default 161).

System Location

Lakeside

System Contact

Hermione Granger

Read Community String

SYS265

The community string is like a password, restricting access to querying & protect from unauthorized information disclosure.

SNMP Traps Enable

Enable ☐ Enable the SNMP Trap and its controls

SNMP Modules

SNMP modules

☒ MibII

☒ Netgraph

☒ PF

☒ Host Resources

☒ UCD

☒ Regex

Interface Binding

Bind Interfaces

All

WAN

LAN

Localhost

- Figure out how to restart the SNMP service

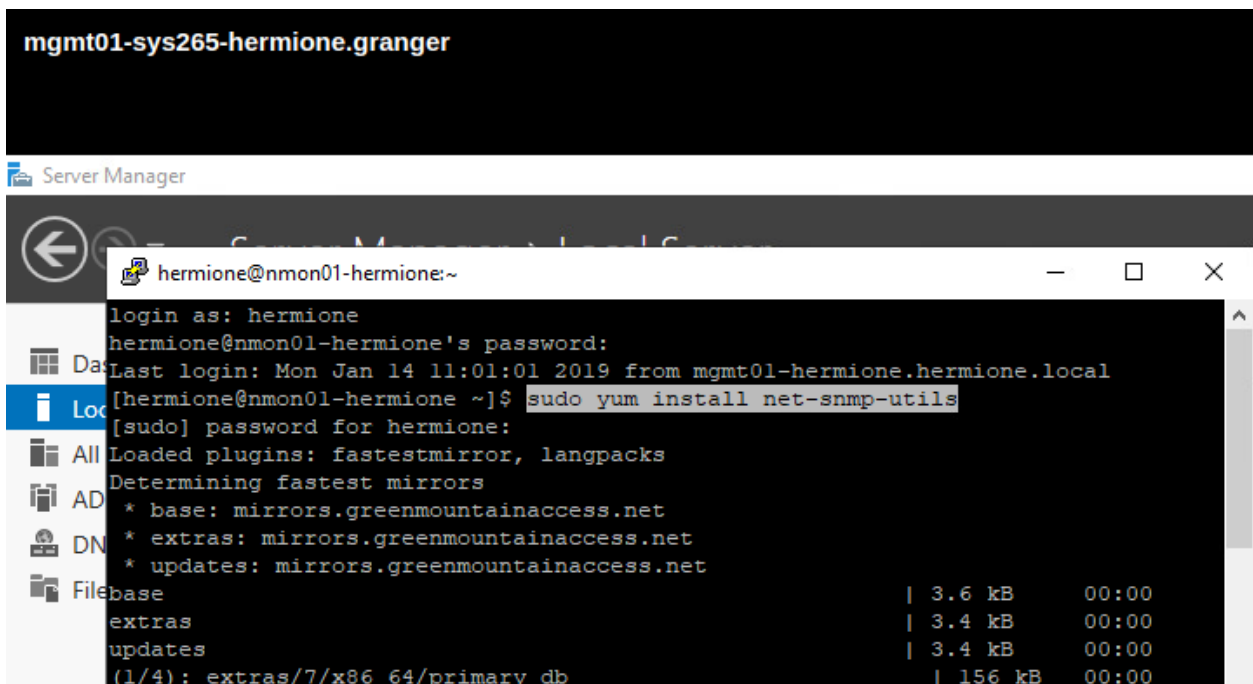
Configure nmon01

You should have a newly provisioned CentOS7 Linux server called nmon01

 nmon1-sys265-hermione.granger

- 10.0.5.11/24, DNS's IP, add domain to the search suffix in network, hostnamed, nmon01-yourname, records, sudo named user, disable root SSH, and manage with your sudo account via PuTTY or Powershell/SSH from mgmt01 (FYI: last reminder)

Install and test SNMP Client on nmon01



The screenshot shows a terminal window titled "hermione@nmon01-hermione:~". The user "hermione" is logged in. The terminal output shows the command `sudo yum install net-snmp-utils` being executed. The output includes the password prompt, the list of loaded plugins (fastestmirror, langpacks), the determination of the fastest mirrors, and the installation progress for the base, extras, and updates repositories. The progress bar shows the installation of net-snmp-utils (1/4) with a size of 156 kB and a time of 00:00.

```
login as: hermione
hermione@nmon01-hermione's password:
Last login: Mon Jan 14 11:01:01 2019 from mgmt01-hermione.hermione.local
[hermione@nmon01-hermione ~]$ sudo yum install net-snmp-utils
[sudo] password for hermione:
Loaded plugins: fastestmirror, langpacks
Determining fastest mirrors
 * base: mirrors.greenmountainaccess.net
 * extras: mirrors.greenmountainaccess.net
 * updates: mirrors.greenmountainaccess.net
base | 3.6 kB | 00:00
extras | 3.4 kB | 00:00
updates | 3.4 kB | 00:00
(1/4): extras/7/x86_64/primary db | 156 kB | 00:00
```

Deliverable 1. Take a screenshot of the output that shows some of the SNMP values from fw01 (note the nslookup to make sure of the hostname). The output should look similar to this:

```
hermione@nmon01-hermione:~  
[hermione@nmon01-hermione ~]$ nslookup 10.0.5.2  
Server:          10.0.5.5  
Address:         10.0.5.5#53  
  
2.5.0.10.in-addr.arpa    name = fw01-hermione.hermione.local.  
  
[hermione@nmon01-hermione ~]$ snmpwalk -Os -c SYS265 -v2c fw01-hermione system  
sysDescr.0 = STRING: pfSense 2.4.4-RELEASE pfSense FreeBSD 11.2-RELEASE-p4 amd64  
sysObjectID.0 = OID: enterprises.12325.1.1.2.1.1  
sysUpTimeInstance = Timeticks: (116704) 0:19:27.04  
sysContact.0 = STRING: Hermione Granger  
sysName.0 = STRING: fw01-hermione.hermione.local  
sysLocation.0 = STRING: Lakeside  
sysServices.0 = INTEGER: 76  
sysORLastChange.0 = Timeticks: (22) 0:00:00.22  
sysORID.1 = OID: enterprises.12325.1.1.1.10.2  
sysORID.2 = OID: enterprises.12325.1.1.1.10.3
```

Install SNMPD (a SNMP Server) on web01

By now you should be remotely managing your Linux systems from MGMT01 via PuTTY or Powershell/SSH and a named sudo account.

```
hermione@web01-hermione:~  
login as: hermione  
hermione@web01-hermione's password:  
Last login: Mon Jan 14 10:32:30 2019  
[hermione@web01-hermione ~]$ sudo yum install net-snmp-utils net-snmp  
[sudo] password for hermione:  
Loaded plugins: fastestmirror, langpacks  
Determining fastest mirrors  
 * base: linux.cc.lehigh.edu  
 * extras: centos.mirror.constant.com  
 * updates: mirrors.greenmountainaccess.net  
base | 3.6 kB | 00:00  
extras | 3.4 kB | 00:00  
updates | 3.4 kB | 00:00  
(1/4): extras/7/x86_64/primary_db | 156 kB | 00:00  
(2/4): base/7/x86_64/group_gz | 166 kB | 00:00  
(3/4): base/7/x86_64/primary_db | 6.0 MB | 00:00
```

The default snmp configuration does not suit our purpose. Make a backup copy of /etc/snmp/snmpd.conf and create a new/blank version.

- Edit your new snmpd.conf to reflect the following contents (these should be the only four lines in the file)

```
root@web01-hermione:/etc/snmp
GNU nano 2.3.1 File: /etc/snmp/snmpd.conf
com2sec myNetwork 10.0.5.0/24 SYS265
group myROGroup v2c myNetwork
view all included .1 80
access myROGroup "" any noauth exact all none none
```

- enable and start the snmpd service
- check the status of the snmpd service and debug any errors
- allow port 161/udp or the snmp service through the firewall permanently
- From nmon01, query web01

Deliverable 2. Provide the output from the following command run on nmon01.

```
hermione@nmon01-hermione:~
[hermione@nmon01-hermione ~]$ nslookup 10.0.5.200
Server:          10.0.5.5
Address:         10.0.5.5#53

200.5.0.10.in-addr.arpa name = web01-hermione.hermione.local.

[hermione@nmon01-hermione ~]$ snmpwalk -Os -c SYS265 -v2c web01-hermione system
sysDescr.0 = STRING: Linux web01-hermione 3.10.0-957.1.3.el7.x86_64 #1 SMP Thu N
ov 29 14:49:43 UTC 2018 x86_64
sysObjectID.0 = OID: netSnmpAgentOIDs.10
sysUpTimeInstance = Timeticks: (34855) 0:05:48.55
sysContact.0 = STRING: root@localhost
sysName.0 = STRING: web01-hermione
sysLocation.0 = STRING: Unknown
```

Install SNMP Service on AD01

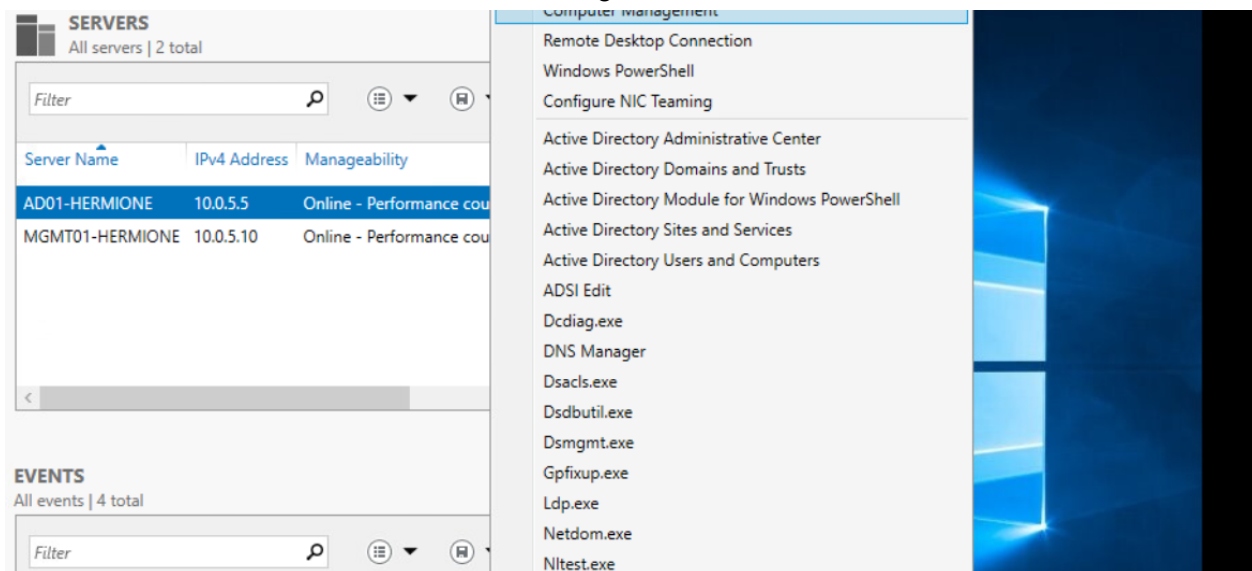
Figure out how to install the SNMP Service Feature on AD01 using Server Manager on MGMT

Install SNMP Tools on MGMT01

Figure out how to install the SNMP-Tools Remote Administration Feature on MGM01

Enable Remote Management on AD01

Remote Computer Management does not work immediately for our remote AD01 Server due to firewall restrictions as seen in the error message.



Event Viewer



Computer 'AD01-HERMIONE.HERMIONE.LOCAL' cannot be connected. Verify that the network path is correct, the computer is available on the network, and that the appropriate Windows Firewall rules are enabled on the target computer.

To enable the appropriate Windows Firewall rules on the remote computer, open the Windows Firewall with Advanced Security snap-in and enable the following inbound rules:

COM+ Network Access (DCOM-In)
All rules in the Remote Event Log Management group

You can also enable these rules by using Group Policy settings for Windows Firewall with Advanced Security. For servers that are running the Server Core installation option, run the Netsh AdvFirewall command, or the Windows PowerShell NetSecurity module.

OK

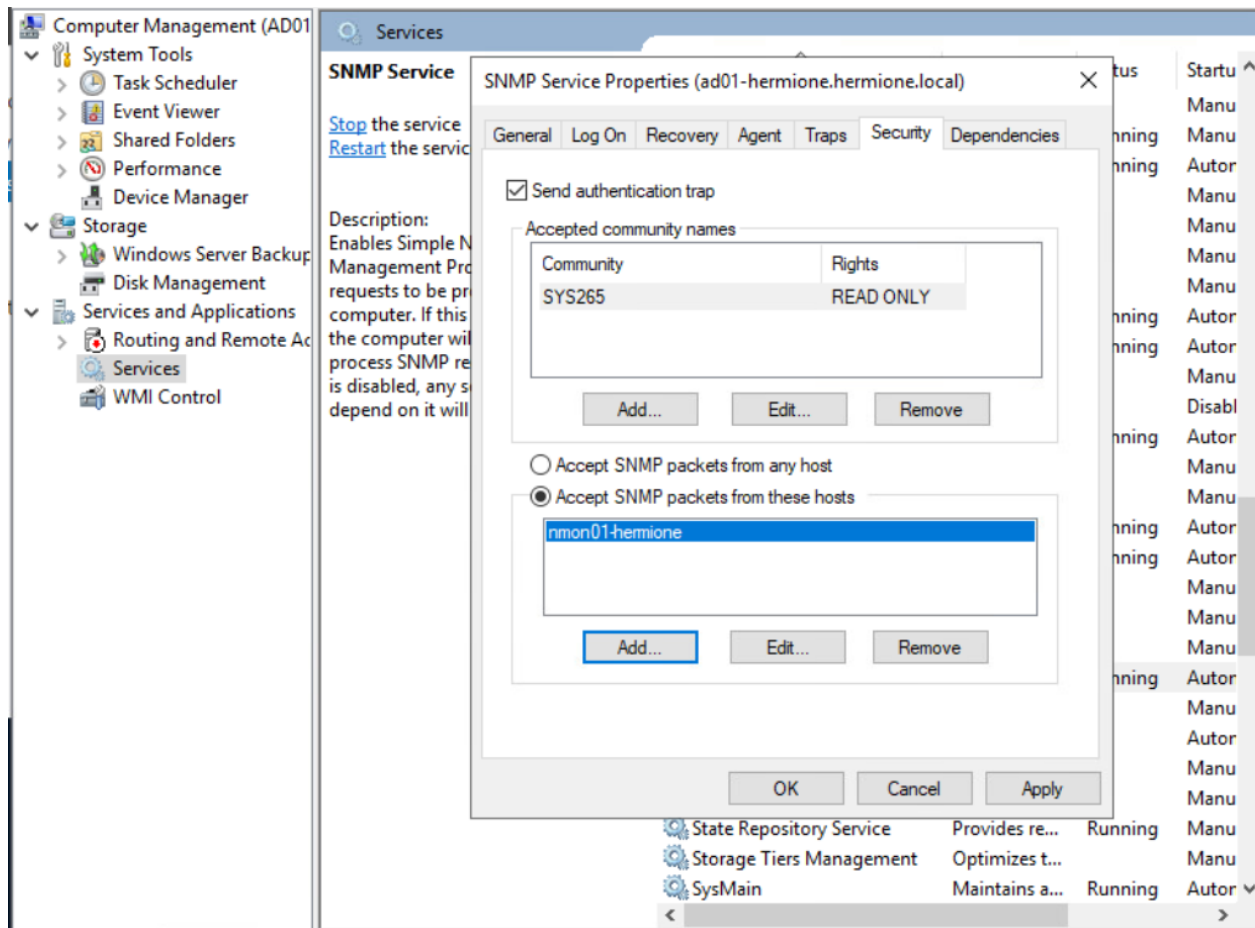
We will fix this by invoking a remote PowerShell session with AD01 from mgmt01. Figure out how to do that.

Change the firewall rules by enabling the "Remote Event Log Management" Firewall group.

```
Select Administrator: Windows PowerShell
[ad01-hermione.hermione.local]: PS C:\Users\hermione.granger-admin\Documents> Set-NetFirewallRule -DisplayGroup "Remote Event Log Management" -Enabled True
[ad01-hermione.hermione.local]: PS C:\Users\hermione.granger-admin\Documents>
```

Try your Remote Computer Management session again and the error should go away.

SNMP Service Security Properties on AD01



- Adjust the SNMP service properties on AD01 to add the SYS265 community string and limit queries to those from nmon01.
- Restart the SNMP Service on ad01

Query AD01 from nmon01

From nmon01, find out how much snmp information is available. In this case, 11843 lines were returned from the SNMP query to ad01.

```
hermione@nmon01-hermione:~  
[hermione@nmon01-hermione ~]$ snmpwalk -Os -c SYS265 -v2c ad01-hermione | wc -l  
11843  
[hermione@nmon01-hermione ~]$
```

Deliverable 3. Provide the output of the SNMP system values on ad01 with the following command

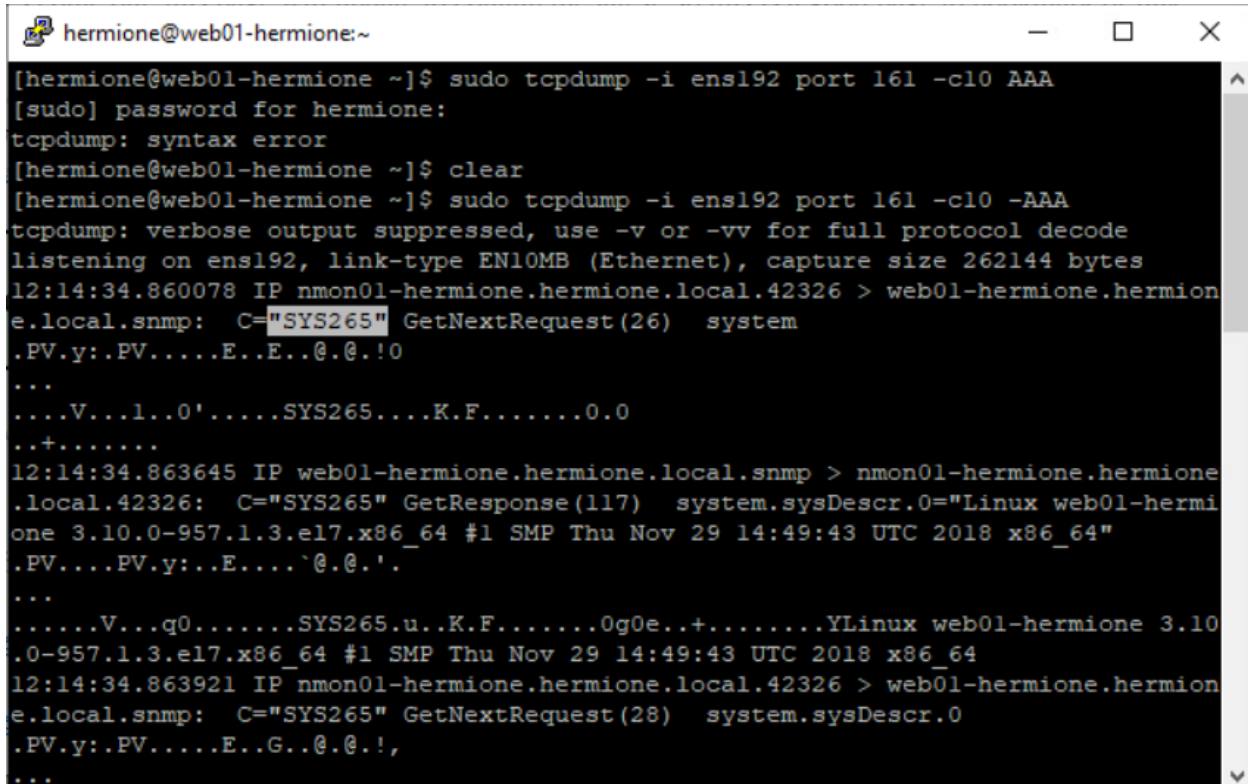
```
hermione@nmon01-hermione:~  
[hermione@nmon01-hermione ~]$ snmpwalk -Os -c SYS265 -v2c ad01-hermione system  
sysDescr.0 = STRING: Hardware: Intel64 Family 6 Model 47 Stepping 2 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 17763 Multiprocessor Free)  
sysObjectID.0 = OID: enterprises.311.1.1.3.1.3  
sysUpTimeInstance = Timeticks: (14423) 0:02:24.23  
sysContact.0 = STRING:  
sysName.0 = STRING: ad01-hermione.hermione.local  
sysLocation.0 = STRING:  
sysServices.0 = INTEGER: 76  
[hermione@nmon01-hermione ~]$
```

Capturing snmp packets nmon01->web01

On web01, run [tcpdump](#) listening to your primary interface, port 161 (udp/tcp), capturing 10 packets and dumping the packets in [ASCII](#) format.

On nmon=01, run your previous system query against web01.

Deliverable 4. Provide a screenshot from the tcpdump session on web01 that shows the clear text community string. Remember, anyone in a position to grab packets between nmon01 and the target can see this string.



```
hermione@web01-hermione:~  
[hermione@web01-hermione ~]$ sudo tcpdump -i ens192 port 161 -c10 AAA  
[sudo] password for hermione:  
tcpdump: syntax error  
[hermione@web01-hermione ~]$ clear  
[hermione@web01-hermione ~]$ sudo tcpdump -i ens192 port 161 -c10 -AAA  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on ens192, link-type EN10MB (Ethernet), capture size 262144 bytes  
12:14:34.860078 IP nmon01-hermione.hermione.local.42326 > web01-hermione.hermione.local.snmp: C="SYS265" GetNextRequest(26) system  
.PV.y:.PV.....E..E..@.!.0  
...  
....V...1..0'.....SYS265....K.F.....0.0  
..+.....  
12:14:34.863645 IP web01-hermione.hermione.local.snmp > nmon01-hermione.hermione.local.42326: C="SYS265" GetResponse(117) system.sysDescr.0="Linux web01-hermione 3.10.0-957.1.3.el7.x86_64 #1 SMP Thu Nov 29 14:49:43 UTC 2018 x86_64"  
.PV....PV.y:..E....`@.@.!.  
...  
.....V...q0.....SYS265.u..K.F.....0g0e..+.....YLinux web01-hermione 3.10.0-957.1.3.el7.x86_64 #1 SMP Thu Nov 29 14:49:43 UTC 2018 x86_64  
12:14:34.863921 IP nmon01-hermione.hermione.local.42326 > web01-hermione.hermione.local.snmp: C="SYS265" GetNextRequest(28) system.sysDescr.0  
.PV.y:.PV.....E..G..@.@.!,  
...
```

Deliverable 5: Tech Journal entry - This week's journal should include notes re: SNMP (in far more detail than [the example](#)). Make sure you include at least 3 topics/articles from the lecture or lab that you were unfamiliar with and your research results. Be sure to add your instructor's GitHub account as a collaborator if your wiki is not public.

Deliverable 6. Your deliverable meets the submission [guidelines](#).