Observium - Lab

Contents

1 Introduction

1.1 Goals

- Gain experience with Observium

1.2 Notes

- Commands preceded with "$" imply that you should execute the command as a general user - not as root.
- Commands preceded with "#" imply that you should be working as root.
- Commands with more specific command lines (e.g. "rtrX>" or "mysql>") imply that you are executing commands on remote equipment, or within another program.

2 Observium lab

All components for Observium should already be installed - it will be now up to you to configure the service, add hosts, etc. . .

If this is not the case, a different lab (observium-install.txt) is available. Follow the instructions in this lab to complete the initial Observium installation.

Connect to your virtual machine as the sysadm user, then:

3 1. Access Observium!

A user has already been created for you. This is the user 'admin', and the password is the standard class password:

http://observiumX.ws.nsrc.org/

```
User:      admin
Password:  the class password
```

You should now be logged in to Observium. There should not be any devices configured. Take a look at the interface for a few minutes.

4 2. Edit the configuration file for Observium, to tell it about our network

`$ sudo editor /opt/observium/config.php`

Now make the following changes:

Find the line:

`$config['snmp']['community'] = array("public");`

... and change 'public' to 'NetManage' (NOT "netmanage" or "NETMAN-AGE"), so it looks like this:

`$config['snmp']['community'] = array("NetManage");`

Also, add the following line below:

`$config['autodiscovery']['xdp']          = TRUE;`

Save the file and exit.

5 3. Add a host - your own router

In the web interface (http://observiumX.ws.nsrc.org), navigate to the Device menu, and click on "Add Device"

Hostname: rtrX.ws.nsrc.org SNMP Version: v2c [should already be selected] SNMP Community: you can leave this blank, since we have configured it in the config.php, or you can type it in: NetManage

If all goes well, you should see several messages like these:

```
Adding host rtrX.ws.nsrc.org community NetManage port 161

Trying v2c community NetManage ...

Device added (id = 1)
```

You can navigate to the `devices` view on Observium, and see that the device
has indeed been added:

`http://observiumX.ws.nsrc.org/devices/`

. . . you can explore the web interface for a few minutes - but there is no data
yet, and if you click on the device (rtrX), Observium will complain that the
device hasn't been discovered yet.

We can tell Observium to start collecting data for this host, by running the
following command:

```
$ cd /opt/observium
$ sudo ./poller.php -h all
```

. . . Of course, we don't want to do this manually! We will automate this in the
next steps.

6   4. Tell Observium to run a discovery (scan) of the network, and start collecting data

```
$ cd /opt/observium
$ sudo ./discovery.php -h all
```

Note that a LOT of information will appear!

We'll run a data collection again manually:

```
$ sudo ./poller.php -h all
```

7   5. Go back to the web interface

`http://observiumX.ws.nsrc.org/`

What do you notice ? How do you think Observium found that there were other
devices on the network, and how did it know how to contact them ?

8 6. Enable cron jobs

It's time to make the data collection happen automatically.

A number of automated maintenance tasks need to be added:

Create the file /etc/cron.d/observium:

```
$ sudo editor /etc/cron.d/observium
```

. . . and paste the following lines:

```
33  */6   * * *   root    /opt/observium/discovery.php -h all >> /dev/null 2>&1
*/5 *     * * *   root    /opt/observium/discovery.php -h new >> /dev/null 2>&1
*/5 *     * * *   root    /opt/observium/poller-wrapper.py 1 >> /dev/null 2>&1
```

It will take a little while for data to appear in the graphs.

9 7. While we wait for the traffic to appear, we can navigate the interface

Go to http://observiumX.ws.nsrc.org/

Click on "Devices" in menu at the top. Find the router for your group in the list, and click on its name.

You will land on the Overview page for your device.

You will notice that Observium has automatically detected many, many things about your router!

At the top, under your router's hostname, you will see a list of tabs, all of them presenting information about your device:

```
Overview | Graphs | Health | Ports | Inventory | Logs | Alerts
```

Under "Graphs", you will see all information which can be presented in the form of a graph: Network IO, Disk IO, Memory and CPU usage, etc. . .

You will also see the "Health" tab, which offers various metrics on how the device is doing hardware wise - if this information is available - such as temperature, voltage, fan speed, etc. . . Notice that some of this information is already shown in the overview page for the device (which you get when you click on the name of the device).

Next we'll take a look at the Ports menu tab. Under "Ports" you will find a summary of traffic for all ports, including bits per second and packets per second, port speed, and the type of connection (Ethernet or other).

Note that all elements can be clicked on, including the small graphs, and you will be taken to the corresponding page for the data source.

The Routing tab will present you with an overview of enabled routing protocols. If you have enabled OSPF or BGP on your routers, you will get information about the active sessions, neighbors or peers, and other protocol specific information.

Inventory contains a full list of hardware modules and serial numbers for equipment installed on your router. Note that this will not work on all vendors.

Under Logs you will see a list of events for your router: changes that have taken place in the configuration of the device, or in the state of interfaces, services, etc. . .

Alerts is currently empty for your router - we will see more about this later.

Also, check out the "Map" function, available under "Ports".

The Map function is an automatically generated diagram of the topology of your network, as seen from the point of view of your router. This will only function for CDP/LLDP enabled devices (Cisco, IOS, . . .)

```
You can enable CDP/LLDP on your Linux devices by installing 'ladvd'
(sudo apt-get install ladvd). Try adding your Linux devices this way.
```

It will only be available if you have enabled 'autodiscovery' 'xdp' as detailed in step 4.

10   8. Add a location and contact for your router

If you navigate back to the Overview page for your router (Go to Devices, click on your router's name), you will see that Observium has picked up the Hardware platform, the Operating System and the Uptime for your device.

Now, log into your router with SSH and add the following information to your SNMP configuration:

Set the location (make it a City, Country format, so that your host will appear on the geo map overview page)

Set the contact (email address or name)

To do this:

```
rtr8> enable
Password:
rtr8# conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rtr8(config)# snmp-server contact user@email.address
rtr8(config)# snmp-server location City, Country
rtr8(config)# exit
rtr8# write memory
```

You want to replace "City, Country" with the city and country (or state) we are currently in. For example:

```
Bloomington, Indiana
Thimphu, Bhutan
```

etc...

If you wait a few minutes (maximum 5), you should see this information appear automatically on the Overview tab for your router in Observium.

For fun, talk to your colleagues in the classroom, and ask them to pick a different City and Country for each of the routers! Then wait until Observium has re-scanned the devices, and look at the World map view on the main Observium page (http://observiumX.ws.nsrc.org/)

11   9. Adding an interface description

While you are still logged in to your router, add a pseudo interface to your router, to see if Observium will pick it up:

```
rtr8(config)# interface loopback123
rtr8(config-if)# description A useless interface
rtr8(config-if)# exit
rtr8(config)# exit
rtr8# write memory
```

This should also show up in Observium after a while - try and find the description under "Ports"

12   10. IP address lookup

From Observium's main page, you will find, under the Overview menu at the TOP of the page), a submenu "Search" with 5 options:

- IPv4 search -> http://observiumX.ws.nsrc.org/search/search=ipv4/
- IPv6 search -> http://observiumX.ws.nsrc.org/search/search=ipv6/
- MAC search -> http://observiumX.ws.nsrc.org/search/search=mac/
- ARP/NDP tables -> http://observiumX.ws.nsrc.org/search/search=arp/
- FDB tables -> http://observiumX.ws.nsrc.org/search/search=fdb/

Using the IPv4 and ARP table searches, try and search IPs of equipment in the class:

- IP of the GW (10.10.0.254)
- IPs of the routers (10.10.X.254)
- IPs of the PCs (10.10.1.1, 10.10.5.17, etc. . .)

Try and search IPs for your OWN laptop! Find the IP of you own laptop, and see if you can search it in Observium. Can you ? Why ?

13 11. Add the switch

From the TOP menu "Devices", choose "Add device". Fill out the fields:

```
Hostname: sw.ws.nsrc.org
Community: NetManage
```

Click on "Add Host". After a few seconds, it should have added the switch. After a few minutes, data should appear in Observium for the switch.

Notice the "Ports" line at the TOP right of the Observium interface.

Does it say that ports are down ? Which ones ?

Try and click on the 'X down' ports message to see which ports are down on which devices.

14 12. Let's disable ports that are unused!

Find the Overview page for "sw.ws.nsrc.org".

From there, you can configure the device (the "key" icon on the top right). You are then presented with a configuration page for the device.

Click on Ports, then you will get an overview of the Port status on the switch. Look at the ones that are "down".

For those that are "down", check the "Ignore" box, then "Save" under "Index".

If you call back the main Observium page:

```
http://observiumX.ws.nsrc.org/
```

... Observium should no longer complain about these ports!

15   15. Have you tried adding your PC yet? Other PCs in the class?

More fun things:

- From the top menu, choose Devices -> All devices

- Find your router, and click on it on the list.

- Below the graph summary, you'll see a list of the interfaces on your router:

  ```
  Fa0/0, Fa0/1, Null0
  ```

- Click on Fa0/0

- Click on "Real Time"

16   16. Region settings for the map

Optionally, you can change the part of the world the map will show when you log into observium.

Look at the parameters for this listed at

http://www.observium.org/wiki/Configuration_Options#Map_overview_settings

In particular, $config['frontpage']['map']['region'] can be set to a particular country or region. There is more information at https://developers.google.com/chart/interactive/docs/gallery/geochar

In reference to the configuration settings in step 4.

The parameter $config['frontpage']['map']['region'] can take multiple values. From:

https://developers.google.com/chart/interactive/docs/gallery/geochart

```
region: The area to display on the map. (Surrounding areas will be displayed
        as well.) Can be one of the following:

    * 'world' - A map of the entire world.
    * A continent or a sub-continent, specified by its 3-digit
```

```
       code, e.g., '011' for Western Africa.
     * A country, specified by its ISO 3166-1 alpha-2 code, e.g.,
       'AU' for Australia.
     * A state in the United States, specified by its ISO 3166-2:US
       code, e.g., 'US-AL' for Alabama. Note that the resolution
       option must be set to either 'provinces' or 'metros'.
```

You can test these options by changing the parameter and reloading the overview page of Observium.