LibreNMS lab

Campus Network Design Workshop

Configuring LibreNMS

Goals

- Learn how to configure the LibreNMS Network Management System

Introduction

In this exercise, we will set up **LibreNMS** as our network monitoring tool. Work together in your campus group, as there is only one instance in each campus.

Connecting to your LibreNMS server

When you are ready to view LibreNMS in your web browser, use the virtual training platform web interface to go to `Campus Y > Web > librenms`, or in the on-site network go to

```
http://librenms.campusY.ws.nsrc.org
```

Login using the admin username and password you created when installing LibreNMS.

Looking at the LibreNMS configuration

LibreNMS is already largely set up on your server. The next few exercises will have you look at the libreNMS configuration (https://docs.librenms.org/Support/Configuration/) to understand some of the basic items that need to be set when you first install the package. Most of these are already set up correctly, but it is good to verify and to know what you would do if you were to install LibreNMS on your own.

The good news is: whilst in old versions of LibreNMS you had to manage a text file called `config.php`, modern versions store all their settings in the database and can be managed via the web interface.

To view them, go to "Settings > Global Settings"

("Settings" is the cog symbol, next to Global Search near the top right-hand corner)

Setting the SNMP community

First, let's change the SNMP community that LibreNMS will try when discovering and adding new devices.

If you scroll down the global settings list, you should find:

```
snmp.community [ "public" ]
```

But that's not what we want.

To change this setting, you need to go back to the top of the page, and instead of the "Global" tab, go to a different tab where the settings can be changed. Unfortunately, it's not always obvious which one.

In this case, you need to go to the "Poller" tab, and at the bottom expand ">SNMP"

Under here you'll find:

```
Communities (priority):     1. public
```

Change "public" to "NetManage"

Next, let's set SNMP v3 authentication credentials. You should see:

```
SNMP v3 Authentication (priority)  1.
                                    No Authentication, No Privacy
```

Change this to "Authentication, No Privacy".

When you do this, new Auth settings pop up. Change them to:

```
Algorithm:      SHA
Username:       admin
Password:       NetManage
```

Finally, we want LibreNMS to try SNMPv3 before SNMPv2c. So above this, look for the section "Version (priority)". Type over fields 1 and 2 so they look like this:

```
1. v3
2. v2c
3. v1
```

That's it. There's no "Save" button to press.

Tell LibreNMS which subnets it is allowed to scan automatically

By default, LibreNMS will ask for the list of "neighbors" that network devices "see" on the network. This is done using the Link Layer Discovery Protocol (LLDP) or Cisco's CDP (Cisco Discovery Protocol).

But to be on the safe side, and not scan networks outside your organization, LibreNMS needs to be told which subnets it's allowed to scan for new devices.

Go to the "Discovery" tab, and open up the "Networks" section.

The "Autodiscovery Networks" field is empty. Enter two new values, and click the "+" button after each one, so that it looks like this:

```
Autodiscovery Neworks    1. 100.68.Y.0/24         (-)
                         2. 172.2Y.0.0/16         (-)
                         [                    ]   (+)
```

Remember, to replace "Y" with your campus number.

There's no need to Save, because the "+" button did this for you.

We're nearly done!

Tell LibreNMS not to add duplicate devices

A situation can happen where two devices have duplicate SNMP *sysName* (that's *hostname* in IOS). They could be two different devices, so it would be a good idea to have LibreNMS automatically add and monitor them.

But it can also happen that the SAME device is seen multiple times by LibreNMS - once using LLDP/CDP, and another time via OSPF (for example), on two different interface IP addresses.

In that case, it ends up added twice. For instance, you may suddenly see two devices called *rtr2-fa0-0.ws.nsrc.org* and *rtr2*, and this is not what we want.

Since "both" devices are in fact the same, their SNMP *sysName* will be identical, and we can tell LibreNMS to **NOT** add devices if one already exists with the same *sysName* - after all, this shouldn't happen in a well configured network! :)

Here's an example of this:

```
2016-07-06 20:16:47 rtr4 discovery Device rtr4 (10.10.0.224)
(port FastEthernet0/0) autodiscovered through CDP on
rtr1.ws.nsrc.org
2016-07-06 20:09:45 rtr4-fa0-0 discovery Device rtr4-fa0-
0.ws.nsrc.org (10.10.0.224) (port ) autodiscovered through OSPF
on rtr1-fa0-0.ws.nsrc.org
```

To handle this, you want the setting `allow_duplicate_sysName` to be `false`.

In the Global Settings, Global tab, scan down the list for `allow_duplicate_sysName`. This should already be set to `false`, which is what we want.

If you needed to change it, then you'd need to find what individual tab the setting is under. In this case, it's the "Discovery" tab, and under that open "General Discovery Settings", where you should see:

```
    Discovery on Reboot:      (O...)
    Allow Duplicate sysName: (O...)
    Primary Domain:          [              ]
```

Since "Allow Duplicate sysName" is off, this will prevent LibreNMS from adding the device if it exists already with the same *sysName*. You will be able to see if there are duplicate devices detected in the *Event Log* (Overview -> Event Log).

All our configuration is now done!

> *For more information, this video (https://www.youtube.com/watch?v=QPzgjJfKgUo) talks about LibreNMS configuration in detail.*

Add a host

Let's add your border router.

At the very top menu bar, select Devices > Add Device.

Enter the details:

```
Hostname or IP        bdr1.campusY.ws.nsrc.org
SNMP                  ON
SNMP Version          v3              [port blank]     udp
Port Assoc Mode       ifIndex


SNMPv3 Configuration


Auth Level            authNoPriv
Auth User Name        admin
Auth Password         NetManage
Auth Algorithm        SHA
Crypto Password       [leave empty]
Crypto Algorithm      AES
Force add             [   ]OFF
```

(remember to change campusY accordingly)

You should see:

```
Added SNMPv3 host: bdr1.campusY.ws.nsrc.org port: 161
Device added bdr1.campusY.ws.nsrc.org (1)
```

If not, try again and check all your parameters carefully - and check that SNMP is configured properly on your bdr1 router.

Final Configuration

Discover and Poll newly added hosts

LibreNMS needs to "discover" each host that has been added. This means that it methodically examines each host you added, learns what type of device it is and what it has, and figures out what it should monitor.

This should take place automatically within a few seconds of adding a host.

(Note that in LibreNMS terminology, "discover" does *not* mean scanning your network to find new devices - that's called "autodiscovery")

Refresh your page by clicking the "LibreNMS" logo at the top left corner of the screen. Then click the Devices menu again, and select "All Devices > Network".

You should find that your bdr1 device has been added, and that it has worked out what type of device it is - it has been discovered.

You may also see other devices in your network have been added. That means autodiscovery is working as well!

To start with, you may see graphs are empty or broken. This is because LibreNMS now needs to "poll" the hosts. In other words, LibreNMS now knows what it wishes to monitor for each host, but it has yet to populate its database with initial values for each item.

The poller is run automatically every 5 minutes, so you just need to wait for data to start to appear.

Install complete

That's it! You now should be able to log in to http://librenms.campusY.ws.nsrc.org/ (http://librenms.campusY.ws.nsrc.org/) and begin to explore the information being collected for your monitored devices.

See the existing devices under Devices > All Devices.

You can add some additional devices via the LibreNMS web interface. If you don't already have these, then add them:

- core1.campusY.ws.nsrc.org
- dist1-b1.campusY.ws.nsrc.org
- dist1-b2.campusY.ws.nsrc.org

What about your other hosts? host[1..6].campusY.ws.nsrc.org, srv1.campusY.ws.nsrc.org? These aren't autodiscovered as LLDP or CDP neighbors, so you will most likely have to add them by hand.

Using the class snmp community. See if you can figure out how to do this on your own.

NOTE: If SNMP is not configured on a device, then LibreNMS will not be able to add that device.

NOTE: When you first add a device it may end up in the "Generic" devices group. This is because LibreNMS needs to run it's cron job to discover it, obtain more specific device information and then

classify the device in the proper group. This could take 5 to 10 minutes from the time you add the device.

PLEASE NOTE: We have not covered HTTPS setup in this example, so your LibreNMS install is not secure by default. Please do not expose it to the public Internet unless you have configured HTTPS and taken appropriate web server hardening steps.

Customize your Installation

When you first log in to LibreNMS your default screen is empty. This is because you are allowed to edit your default screen using the Dashboard editing tool to make it look as you prefer. To do this do:

- Click on the Edit Dashboard icon that looks like a Pencil next to a Red icon of a garbage can.
- Name your Dashboard or leave it as "Default"
- If you select Private then your dashboard is only available to your user.
- If you make it Shared (Read) then you control the look, but others can use it.
- If you make it just Shared, then anyone can update the look and feel of the dashboard.
- Click on Add Widgets and select items you would like to see by default when you log in. A good one to start with is "Top Interfaces".
- Place the selected widget on the screen where you want it.
- You can click on the red "X" to close the placeholder notice about editing dashboards so that it does not appear next time you log in.
- If you want specific graphs you can select the "Graph" widget and customize this. (e.g. Graph Type "Port bits" will show traffic on a specific interface). Try adding a graph for the bdr1 interface towards the NREN (Gi0/0).
- Many people use the "Top devices" and "Top interfaces" widgets.
  - For Top interfaces note you can set the details on this widget, by clicking the pencil. When done, press the "Save" button.

Remember, you can resize the widgets as you like.

When you are done press the "Update" button. Note that the top-devices and top-interfaces widgets may take some time before they populate with interesting information, so they will appear as largely blank for a while.

If you create multiple Dashboards you can switch between your default login Dashboard by going to the person icon, selecting "My Settings" and going down to "Default Dashboard".

View a Real-Time Graph on an Interface

Now we're going to look at the interface traffic in real time. Pick a device or VM that you want to monitor (say srv1, or bdr1)

In the LibreNMS interface do:

- Select Devices ==> All Devices ==> Server or Network
- Select a server from the resulting screen (click on its name)
- Click on the "Ports" item near the top.
- Click on a network interface, e.g. "ens3" or "GigabitEthernet0/0"
- Next to the Graphs item select "Real time"

The default polling interval is 2 seconds, after which the graph should start filling from the left-hand side.

If you do not see any traffic, go to that host and do something… Like,

```
$ ping hostX.campusY.ws.nsrc.org
```

Or some other device or machine, or run an apt update, etc…

A few other items

Creating an Alert

LibreNMS has a number of built-in alerts that you can add easily. By default you will set up a Default contact for your install. This is the contact that will receive all alerts.

We are going to set up an alert that will trigger if a device goes down and when a device comes back up. You can, also, set up an alert that triggers only when a device goes down - as well as many, many other alerts.

To get started we need to set up our LibreNMS install to work with alerts.

In your LibreNMS interface do the following:

- Click on the settings icon next to the "Global Search" box
- Select Select "Global Settings"
- Click on the Alerting tab
- Expand the "General alert settings" tab
- In the Default contact box add in your sysadm user on the srv1 host:
    - sysadm@srv1.campusY.ws.nsrc.org
- Now click on the "Email Options" tab and you are going to set the following:

```
Enable email alerting:          Yes
From name:                      LibreNMS
From email address:
librenms@librenms.campusY.ws.nsrc.org
Use HTML emails:                No
Attach graph images:            Yes
How to deliver mail:            SMTP
SMTP Server:                    srv1.campusY.ws.nsrc.org
SMTP Port setting:              25
SMTP Timeout setting:           10
Encryption:                     Disabled
Auto TLS Support:               No
SMTP Authentication:            No
```

Next, click on "Alerts" on the top menu bar, and select "Alert Transports". Click the button "Create alert transport"

```
Transport name:        sysadm
Transport type:        mail
Default alert:         On
Email:                 sysadm@srv1.campusY.ws.nsrc.org
Include Graphs:        On
```

Click Save Transport. If you get "Failed to process alert transport", and you're sure that you're using the fully qualified domain name, then you may be running and old version of LibreNMS and need to update.

You can test that your email is working on srv1.campusY.ws.nsrc.org by clicking on the orange tick button next to the transport. It should respond "Test to mail OK".

ssh into to your campus' srv1 machine (srv1.campusY.ws.nsrc.org) as the "sysadm" user, then type:

```
$ mutt
```

and see if email has arrived from LibreNMS. It should have a subject of "Testing transport from LibreNMS". Hit Enter to view the message. You can exit from Mutt by press the "q" key twice.

Now we are ready to add an alert to our LibreNMS install.

- At the top of your LibreNMS browser window look for the Alerts menu, it has a green icon with the "!" in a circle.
- Click on this and select the menu item "Alert Rules".
- Click on the button labeled, "Create new alert rule"
- Enter "Devices up/down" as the rule name
- There is an initial empty rule. Underneath AND/OR, click on the drop-down which initially shows "———"
- From the long list of entities (https://docs.librenms.org/Alerting/Entities/) , select "devices.status"

Now we need to fill in some reasonable choices. The devices.status Entity will alert whenever a device goes down, or comes back up. This means an email will be sent to sysadm@srv1.campusY.ws.nsrc.org from librenms@librenms.campusY.ws.nsrc.org.

You can enter in the following to the Alert Rules box:

```
Entity:                devices.status (already selected)
Condition:             Not Equal
Value:                 1
```

And beneath this:

```
Severity:              Critical
Max alerts:            1
Delay:                 1m
Interval:              5m
```

```
Mute alerts:              OFF
Invert rule match:        OFF
Recovery alerts:          ON
Match devices etc         <leave blank>
Tranports:                select "Mail: sysadm" from the list
Procedure URL:            <blank>
```

Now press "Save Rule".

To verify that your new alert is working you need to bring down a host that you are monitoring in LibreNMS. Select one of the hosts in your campus that is visible in LibreNMS and halt that host. To do this log in on the host (hostX.campusY.ws.nsrc.org) and type:

```
$ sudo halt -p
```

Now go back to the srv1.campusY.ws.nsrc.org command line and type:

```
$ id        # make sure you're running as the "sysadm" user
$ mutt
```

and wait for a few minutes. (You can also monitor the web interface under Alerts > Notifications)

Eventually you should get an email with a subject like:

```
Alert for device hostX.campusY.ws.nsrc.org - Devices up/down
```

You can read the alert and it will say something like:

```
Date: Tue, 20 Feb 2018 10:29:01 +0000
From: librenms@librenms.campusY.ws.nsrc.org
To: NOC <sysadm@srv1.campusY.ws.nsrc.org>
Subject: Alert for device hostX.campusY.ws.nsrc.org - Devices
up/down
X-Mailer: LibreNMS

Alert for device hostX.campusY.ws.nsrc.org - Devices up/down
Severity: critical
Timestamp: 2018-02-20 10:25:28
Unique-ID: 371
Rule: Devices up/down
Faults:
  #1: sysObjectID => enterprises.8072.3.2.10; sysDescr => Linux
hostX.campusY.ws.nsrc.org 4.4.0-96-generic #119-Ubuntu SMP Tue
Sep 12
```

```
14:59:54 UTC 2017 x86_64;
Alert sent to: NOC <sysadm@srv1.campusY.ws.nsrc.org>
```

Notice the `sysObjectID` and the `SysDescr` items. These are values for OIDs that are contained within the SNMP MIB on the LibreNMS server.

Now you can exit from Mutt (press "q" twice) and return to the shell prompt.

Note that when we bring your host back up you will receive another alert with a subject like:

```
Device hostX.campusY.ws.nsrc.org recovered from Devices up/down
```

Note: You should ask an instructor to restart the host that you brought down at this time.

There are more examples of alerting rules in the documentation (https://docs.librenms.org/Alerting/Rules/#examples) .

Global Frontpage Map

It is possible to create a world map of all your entries that is displayed by LibreNMS. Use the "Globe Map" widget on the dashboard. See also

- https://docs.librenms.org/Extensions/World-Map/ (https://docs.librenms.org/Extensions/World-Map/)
- https://docs.librenms.org/Support/SNMP-Configuration-Examples/ (https://docs.librenms.org/Support/SNMP-Configuration-Examples/)

You must use the sysLocation snmp variable on your hosts and network devices providing latitude and longitude information for each item for this to work: these must be provided inside square brackets, for example:

```
snmp-server location Buckingham Palace, London
[51.501364,-0.144084]
```

After changing this, you will need to re-run discovery on the host to pick up the change. Navigate to the device in the web interface, click on the settings cog, and you should see a Device Settings tab with a "Rediscover device" button.

Wait a few seconds, click on the "Overview" tab for the device, and check that it shows:

```
Location        Buckingham Palace, London
Lat / Lng       51.501364, -0.144084
```

About Daily Updates

LibreNMS performs daily updates by default. At 00:15 system time every day, a *git pull –no-edit – quiet* is performed. If you don't want this, you can disable it under Settings > System > Updates.

Unfortunately, there is a risk that this will fail. For example, the old LibreNMS VM image is built using Ubuntu 20.04 with PHP 7.4, but recent version of LibreNMS require at least PHP 8.1. This means you may have to upgrade the entire OS to continue using LibreNMS.