Deploying Nag-Stack with Ubuntu/LXD

What is the Nag-Stack?

Ok, this isn't an official term. The Nag-Stack is what I call the combined suite of Nagios monitoring tools consisting of;

NagiosXI

The base layer! NagiosXI is the foundation on which the enterprise product line of Nagios is built. Second only to LXD, NagiosXI takes center stage in the deployment of Nag-Stack.

Nagios Fusion

"A single pane of glass for monitoring, across the business." ←- Have you heard that requirement/criteria/ask from one of your stakeholders before? This is Nagios Fusion!

No matter the X-Ops mindset your company adopts, Nagios Fusion gives you one location to visualize the triggered events across the business for each deployed NagiosXI Server.

Nagios Log Analyzer (Naglog)

Nagios Log Server greatly simplifies the process of searching your log data. Set up alerts to notify you when potential threats arise, or simply query your log data to quickly audit any system.

Nagios Network Analyzer

Network Analyzer provides an in-depth look at all network traffic sources and potential security threats allowing system admins to quickly gather high-level information regarding the health of the network as well as highly granular data for complete and thorough network analysis.

I love NagiosXI! When it comes to monitoring it's my go too for most anything and everything you can think of. I've got a lot of years in the trenches beginning in 2006. All balls are shiny new at some point, right?

Don't get me wrong, after you've been with something for 14 years, you'll have things to complain about. For me, one of the major drawbacks is the lack of a resilient small footprint deployment method. Let me clarify we're talking containers not the VMware "ova" that is readily available. I have lots of hardware laying around that doesn't meet the requirements for VMware although it can "container" without issues.

Well, there wasn't, would be the correct statement in this case. In this article I'm going to walk you through installing the complete Nag-Stack development environment with a footprint small enough that you can run it on most anything.

I'm installing on a green field, the host is a physical PC.

- HP t620 "Thin Client"
- 4 core AMD 2.2Ghz
- 8g RAM
- 64G SSD
- 1GB NIC
- Ubuntu Server 20.04 LTS installed and updated to current
- SSH Access to the Server
- Internet Access
- I've also downloaded the install packages for all four apps to be installed.

The first thing we need to do is get LXD, our hypervisor, installed on the server.

Install LXD

1. Connect to the server via ssh
2. Type "sudo apt install lxd" and authenticate
3. Go to next step when done

Initialize LXD

1. Type “sudo lxd init: and authenticate
2. This is an interactive process. You answer a couple of questions
3. (you can choose default for most)
4. Deploy Nag-Stack members

OK, that was pretty painless and without much explanation, there’s a reason for that. LXD is dead simple to get up and going. With the hypervisor installed we can move on to deploying our stack member servers.

Launch and stage LXD Servers for install

NagiosXI

Launch container

1. Type “sudo lxc launch images:centos/8/amd64 lxd-nagios57-centos”

Push the install package to container

1. Type “ lxc push /tmp/xi-current.tar.gz lxd-nagios57-centos/tmp/”

Nagios Log Server

Launch Container

1. Type “lxc launch images:centos/8/amd64 lxd-naglog-centos/tmp/”

Push install package to the container

1. Type “sudo lxd push /tmp/nagioslogserver-2.1.6.tar.gz lxd-naglog-centos/tmp/”

Nagios Fusion

Launch the Container

1. Type “lxc launch images:centos/8/amd64 lxd-nagfusion-centos”

Push the install package to the container

1. Type “ sudo lxc file push /tmp/fusion-4.1.8.tar.gz lxd-nagna-centos/tmp/”

Nagios Network Analyzer

Launch the container

1. Type “ lxc launch images:centos/7/amd64 lxd-nagna-centos”

Push the install package to the container

1. Type “ sudo lxc file push /tmp/nagiosna-2.4.1.tar.gz lxd-nagna-centos/tmp/”

Once complete, run a quick “sudo lxc list” and verify.

```
@svr-ubuntunaglxd:/tmp$ sudo lxc list
+----------------------+---------+---------------------+----------------------------------------------+-----------+-----------+
|         NAME         |  STATE  |        IPV4         |                    IPV6                      |   TYPE    | SNAPSHOTS |
+----------------------+---------+---------------------+----------------------------------------------+-----------+-----------+
| lxd-nagfusion-centos | RUNNING | 10.28.75.73 (eth0)  | fd42:75e8:f4b7:e39:216:3eff:fe2b:448f (eth0) | CONTAINER | 0         |
+----------------------+---------+---------------------+----------------------------------------------+-----------+-----------+
| lxd-nagios57-centos  | RUNNING | 10.28.75.113 (eth0) | fd42:75e8:f4b7:e39:216:3eff:fe18:5140 (eth0) | CONTAINER | 0         |
+----------------------+---------+---------------------+----------------------------------------------+-----------+-----------+
| lxd-naglog-centos    | RUNNING | 10.28.75.109 (eth0) | fd42:75e8:f4b7:e39:216:3eff:fe9b:55d3 (eth0) | CONTAINER | 0         |
+----------------------+---------+---------------------+----------------------------------------------+-----------+-----------+
| lxd-nagna-centos     | RUNNING | 10.28.75.22 (eth0)  | fd42:75e8:f4b7:e39:216:3eff:fe42:843d (eth0) | CONTAINER | 0         |
+----------------------+---------+---------------------+----------------------------------------------+-----------+-----------+
```

OK, pretty quick work! The containers are up and we can start installing stuff. We will start off with XI.

Installing NagiosXI

Get a shell inside the server

1. Type “sudo lxc exec lxd-nagios57-centos /bin/bash”

Install some prerequisites

1. Yum install tar
2. yum install 'dnf-command(config-manager)'

Cd to /tmp/ where we staged our install file

1. Type “tar xvf xi-current.tar.gz”
2. Cd into the directory nagios
3. Execute the “fullinstall” script

This is going to fail at a point due to the nature of what we are doing. Stepping over these failures is pretty quick work.

For checkconfig

1. touch installed.chkconfig in the install directory
2. Rerun the fullinstall command with the “-f” flag
3. The final step will exit with ssh service start failure.
4. This is a non issue due to the fact that ssh is not installed and can be ignored

5. Exit the container shell by typing exit

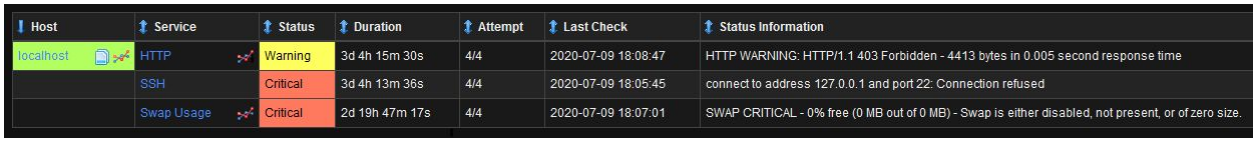
From the lxd host we will add the networking needed to allow us to connect to the Xi interface and finish the install.

1. Type “sudo lxc config device add lxd-nagios57-centos nagiosxi443 proxy listen=tcp:0.0.0.0:443 connect=tcp:127.0.0.1:443”

From a browser on an external device you should now be able to browse to the URL for the XI server and continue the initial configuration as described in the Nagios Documentation.

1. https://<lxdhost/ip>/nagiosxi

NagiosXI is going to immediately start throwing a couple of alerts on the XI Host.



Host	Service	Status	Duration	Attempt	Last Check	Status Information
localhost	HTTP	Warning	3d 4h 15m 30s	4/4	2020-07-09 18:08:47	HTTP WARNING: HTTP/1.1 403 Forbidden - 4413 bytes in 0.005 second response time
	SSH	Critical	3d 4h 13m 36s	4/4	2020-07-09 18:05:45	connect to address 127.0.0.1 and port 22: Connection refused
	Swap Usage	Critical	2d 19h 47m 17s	4/4	2020-07-09 18:07:01	SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.

Update the service checks to correct the issues.

1. SSH is not available (it is a container). Remove from the default config
2. HTTP is not enabled only HTTPS. Remove from default config.
3. The container has no swap partition. Remove from default config.

Installing Nagios Log Server

Get a shell inside the server

1. Type “sudo lxc exec lxd-naglog-centos /bin/bash”

Install some prerequisites

1. Yum install tar
2. yum install 'dnf-command(config-manager)'

Cd to /tmp/ where we staged our install file

1. Type “tar xvf nagioslogserver-2.1.6.tar.gz”
2. Cd into the directory /tmp/nagioslogserver
3. Execute the “fullinstall” script
4. Exit the container shell by typing exit

From the host we will add the networking needed to allow us to connect to the Nagios Log Server interface and finish the install.

1. Type “sudo lxc config device add lxd-naglog-centos naglog8080 proxy listen=tcp:0.0.0.0:8080 connect=tcp:127.0.0.1:80”

From a browser on an external device you should now be able to browse to the URL for the Nagios Log Server and continue the initial configuration as described in the Nagios Documentation.

1. https://<lxdhost/ip>:8080/nagioslogserver/

Installing Nagios Fusion

Get a shell inside the server

1. Type “sudo lxc exec lxd-naglog-centos /bin/bash”

Install some prerequisites

1. Yum install tar
2. yum install 'dnf-command(config-manager)'

Cd to /tmp/ where we staged our install file

1. Type “tar xvf fusion-4.1.8.tar.gz”
2. Cd into the directory /tmp/nagiosfusion/
3. Execute the “fullinstall” script
4. The install will fail a couple of times we will step around each failure after the script exits by touching the installed files.

For the subsystem failure

1. Type “touch /tmp/nagiosfusion/setup/installed.subsystem”
2. Execute the “”fullinstall” script with the “-f” flag to continue

For the Security Failure

1. Type “touch /tmp/nagiosfusion/setup/installed.security”
2. Execute the “fulinstall” script with the “-f” flag again to continue
3. Exit the container shell by typing exit

From the host we will add the networking needed to allow us to connect to the Fusion interface and finish the install.

1. Type “sudo lxc config device add lxd-nagfusion-centos nagfusion80 proxy listen=tcp:0.0.0.0:8888 connect=tcp:127.0.0.1:80”

From a browser on an external device you should now be able to browse to the URL for the Nagios Fusion Server and continue the initial configuration as described in the Nagios Documentation.

1. https://<lxdhost/ip>:8888/nagiosfusion/

Installing Nagios Network Analyzer

Get a shell inside the server

1. Type “sudo lxc exec lxd-nagna-centos /bin/bash”

Install some prerequisites

1. Type “Yum install openssl -y”

Cd to /tmp/ where we staged our install file

1. Type “tar xvf nagiosna-2.4.1.tar.gz”
2. Cd into the directory /tmp/nagiosna/
3. Execute the “fullinstall” script
4. Exit the container shell by typing exit

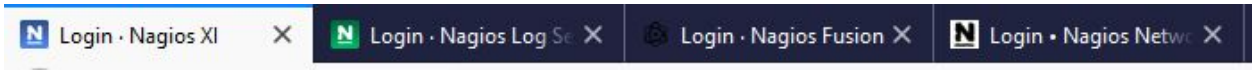
From the host we will add the networking needed to allow us to connect to the *Nagios Network Analyzer* interface and finish the install.

1. Type “sudo lxc config device add lxd-nagna-centos nagna80 proxy listen=tcp:0.0.0.0:8880 connect=tcp:127.0.0.1:80”

From a browser on an external device you should now be able to browse to the URL for the *Nagios Analyzer Server* and continue the initial configuration as described in the Nagios Documentation.

1. https://<lxdhost/ip>:8880/nagiosna/

In pretty short order we've now deployed not one, not two but, all Four of these tools in containers. From here the you now have the full suite of tools available to begin development on your plugins, wizards, integrations or wherever your X-Ops mindset can take you.



Learn more about Nagios Products or LXD from these online resources.

https://www.nagios.org/documentation/

https://www.ubuntu.org.cn/cloud/lxd

https://www.cyberciti.biz/faq/install-lxd-on-ubuntu-20-04-lts-using-apt/