Ubuntu server installation for Splunk Enterprise

Installing Windows 10 machines and Windows Server is a very straightforward process. You can find tons of videos about that. I will focus on Splunk server, Splunk, forwarders and Sysmon installation.

To install Kali Linux seamlessly, 7-Zip needs to be installed on the host machine. Once Kali Linux image is downloaded, we need to unzip it with 7-Zip. After unzipping it, the installation of Kali Linux is very straightforward.

In VirtualBox, I created a NAT network and added all virtual machines to that network.

Splunk Server installation

We want to install an Ubuntu server. This server will be the host for Splunk. To get Ubuntu we need to download it from Ubuntu website. Go to Download Ubuntu → Get Ubuntu Server → Download the current version of this server.

Once the server is downloaded, we open it in VirtualBox. I set the memory for 8 GBs and the processor for 2 CPUs, and the hard disk for 100GB. I just skipped the unintended installation. Click on 'Starting machine'. Opening screen appears, then click on Install Ubuntu Server. This installation is quite straightforward.

Selecting the language for English

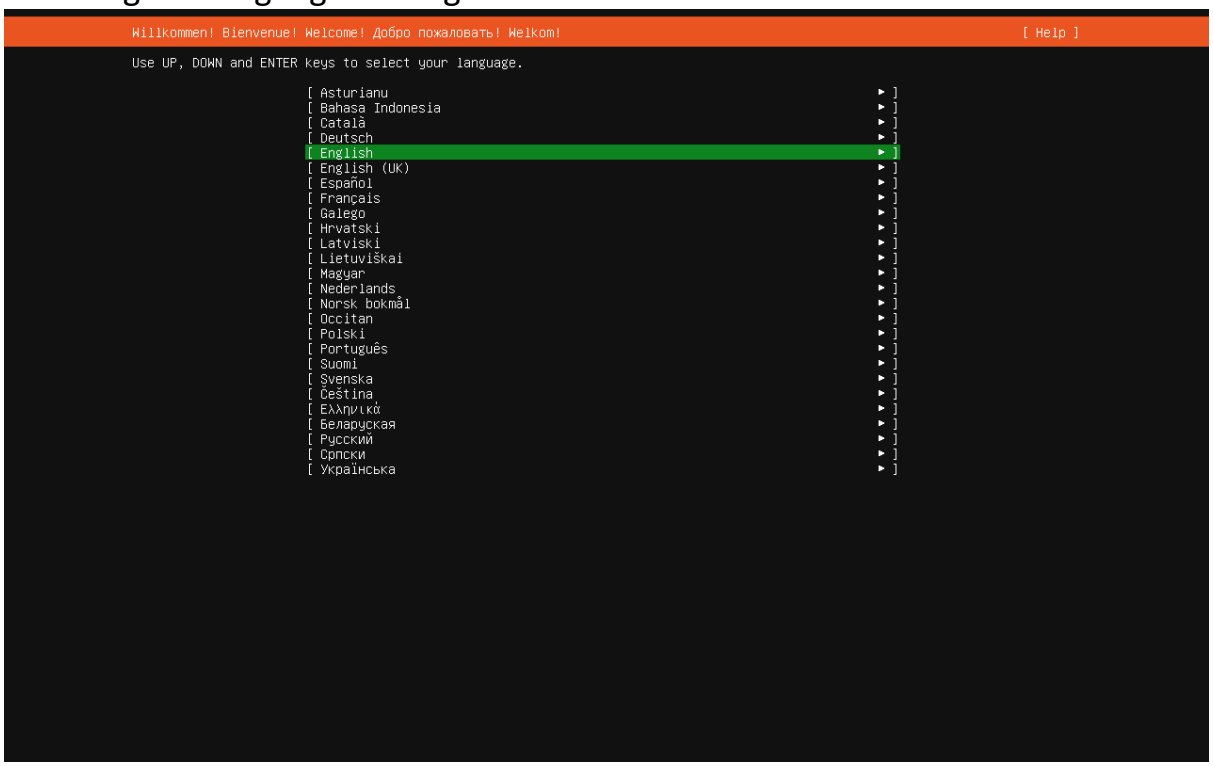

Figure 1

Press continue, and press continue without updating. After this, select keyboard layout settings and press “Done”.

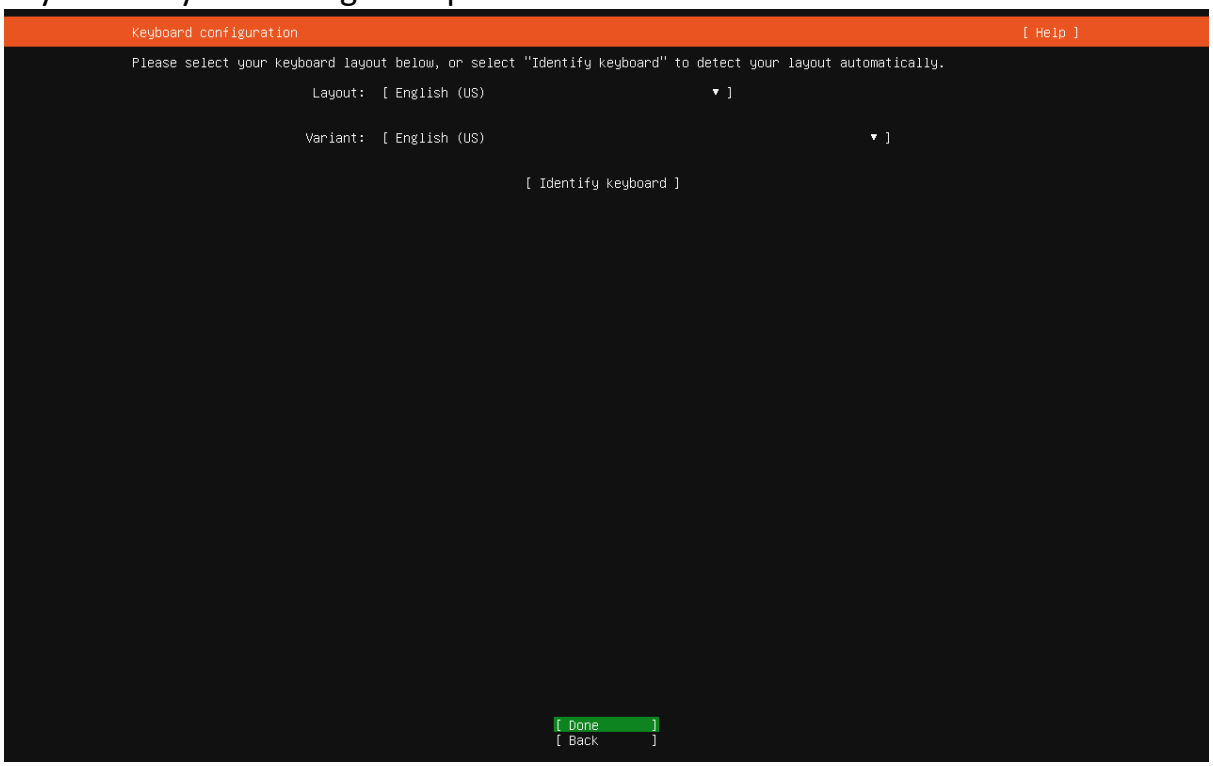

Figure 2

Now press “Done”

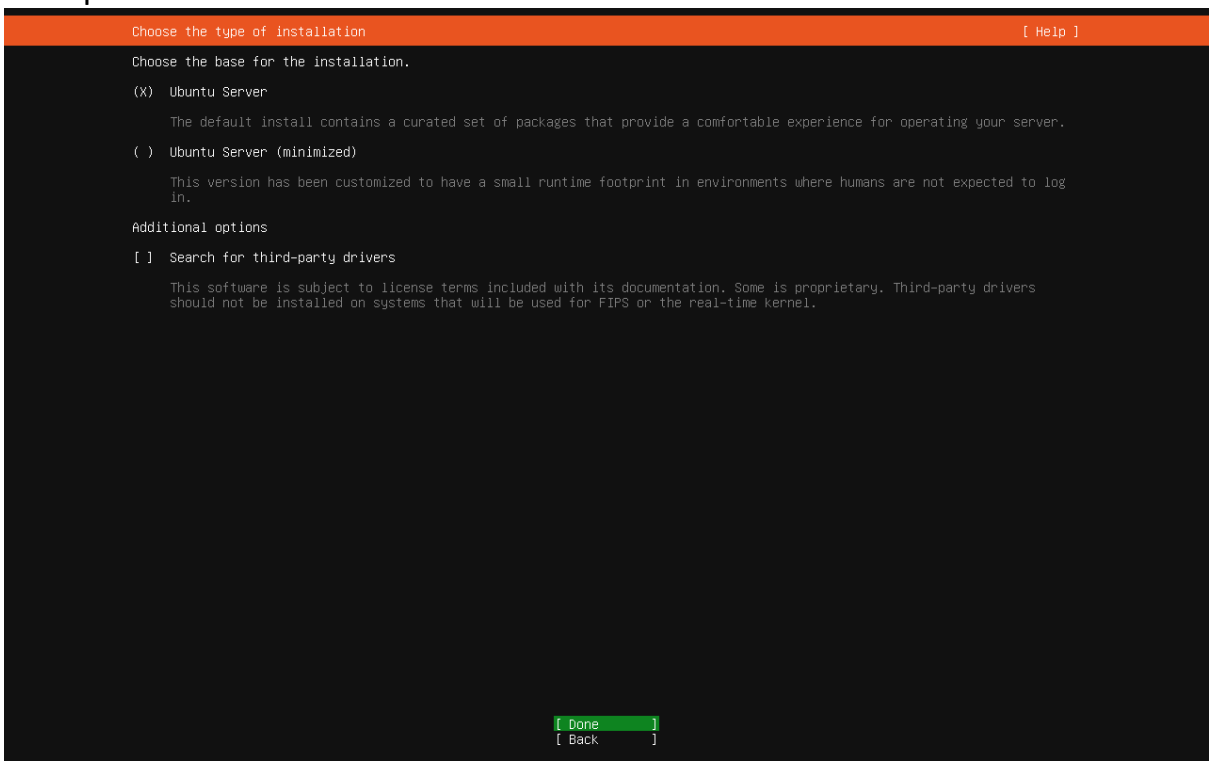

Figure 3

The next one is Network configuration. Simply press “Done”.

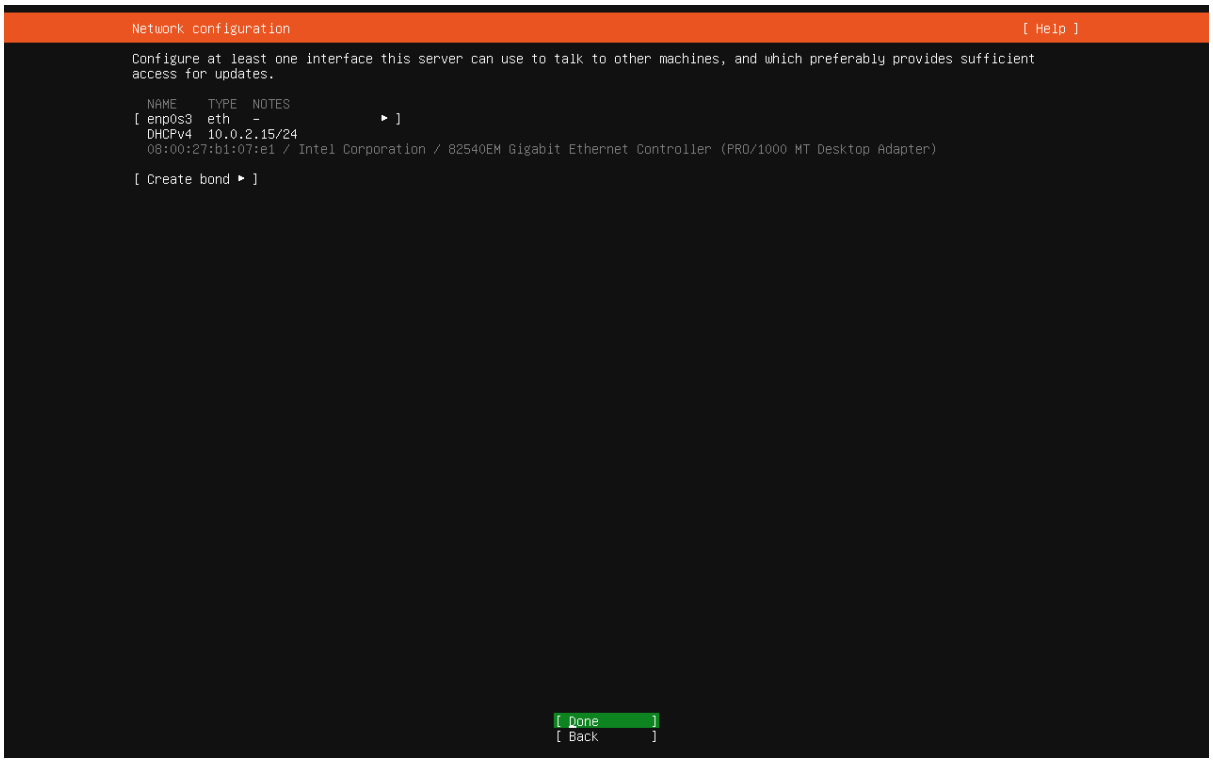

Figure 4

Configure proxy. Press “Done” again.
The next one is the Profile configuration.
You need to enter your name, server name, username and password.
After that press “Done”.

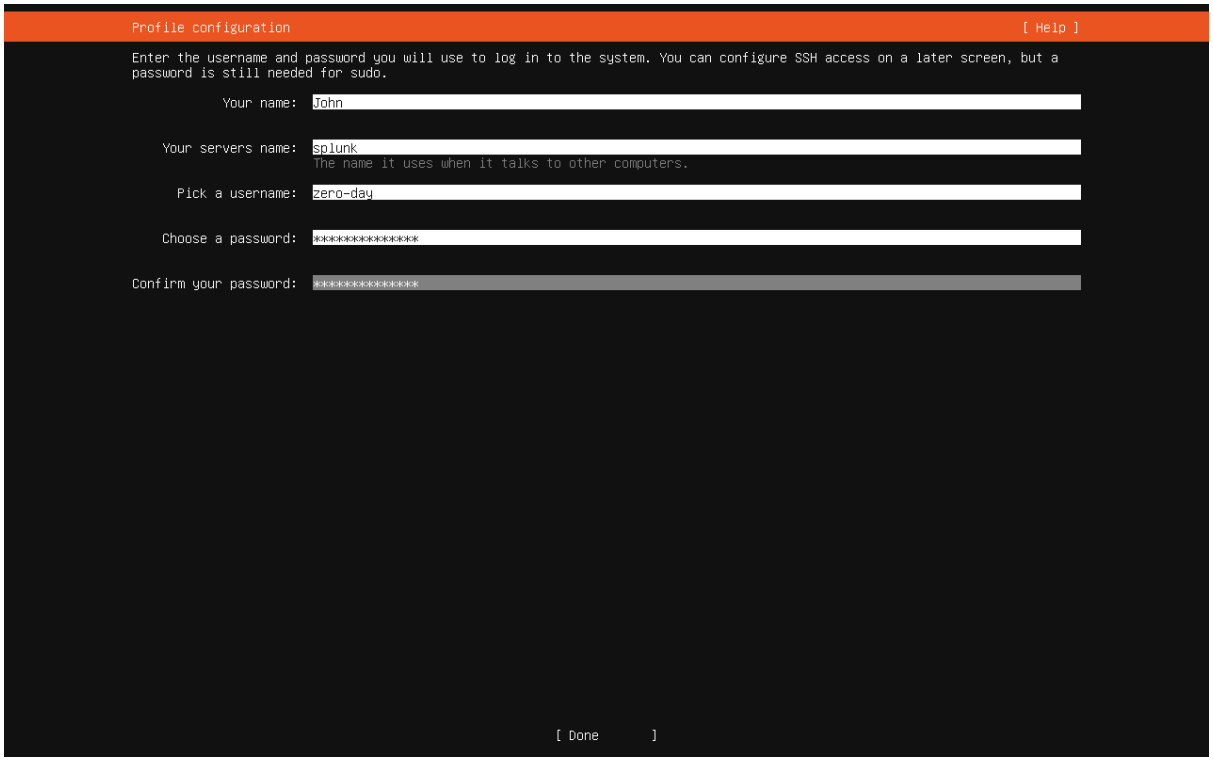

Figure 5

The next one is an upgrade Ubntu, use the down arrow and skip for now, then press “Continue”.

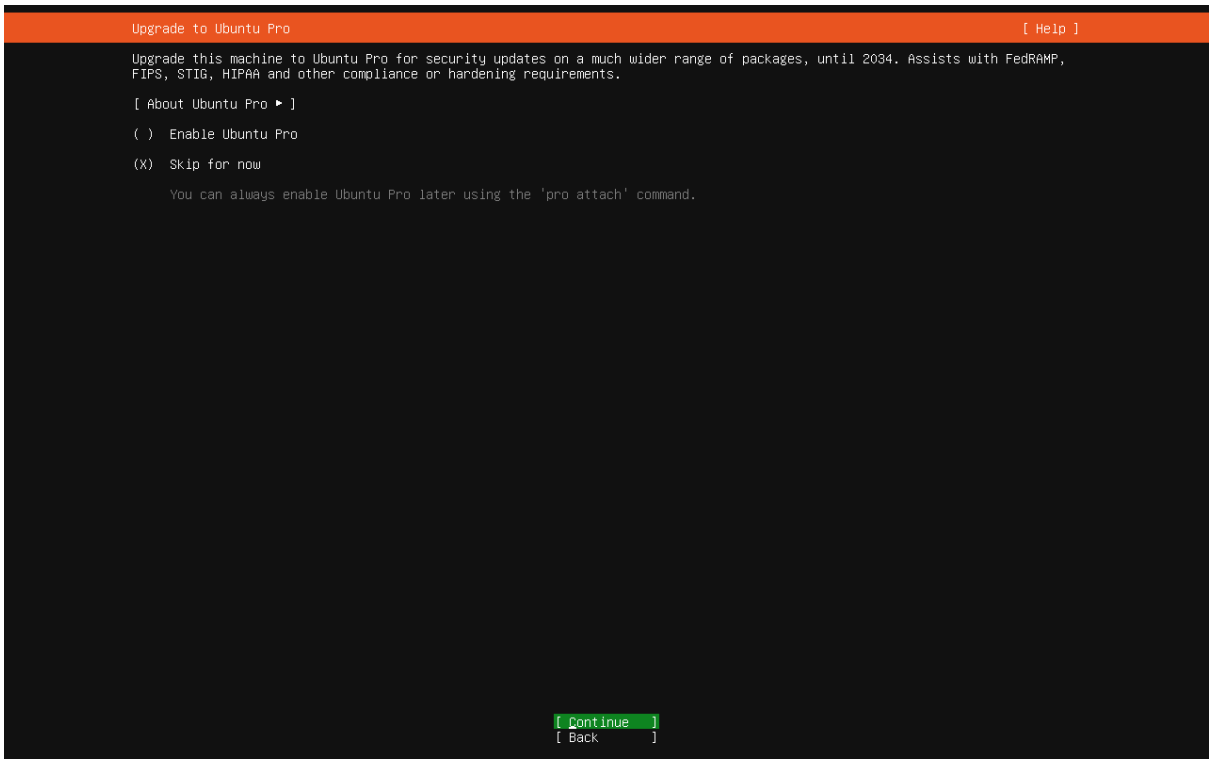

Figure 6

The next one is Opens SSH configuration. If you want it, go ahead and install it, otherwise, press “Done”.

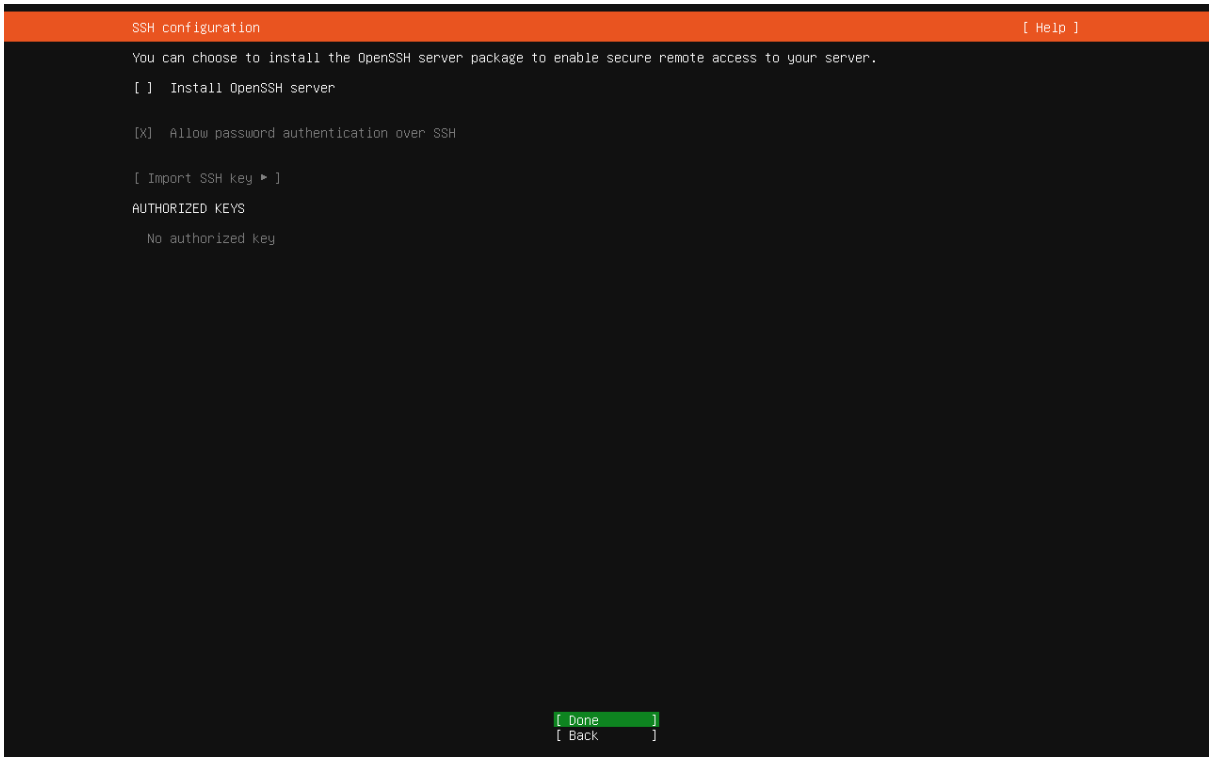

Figure 7

Featured server snaps, scroll down and press “Done”.

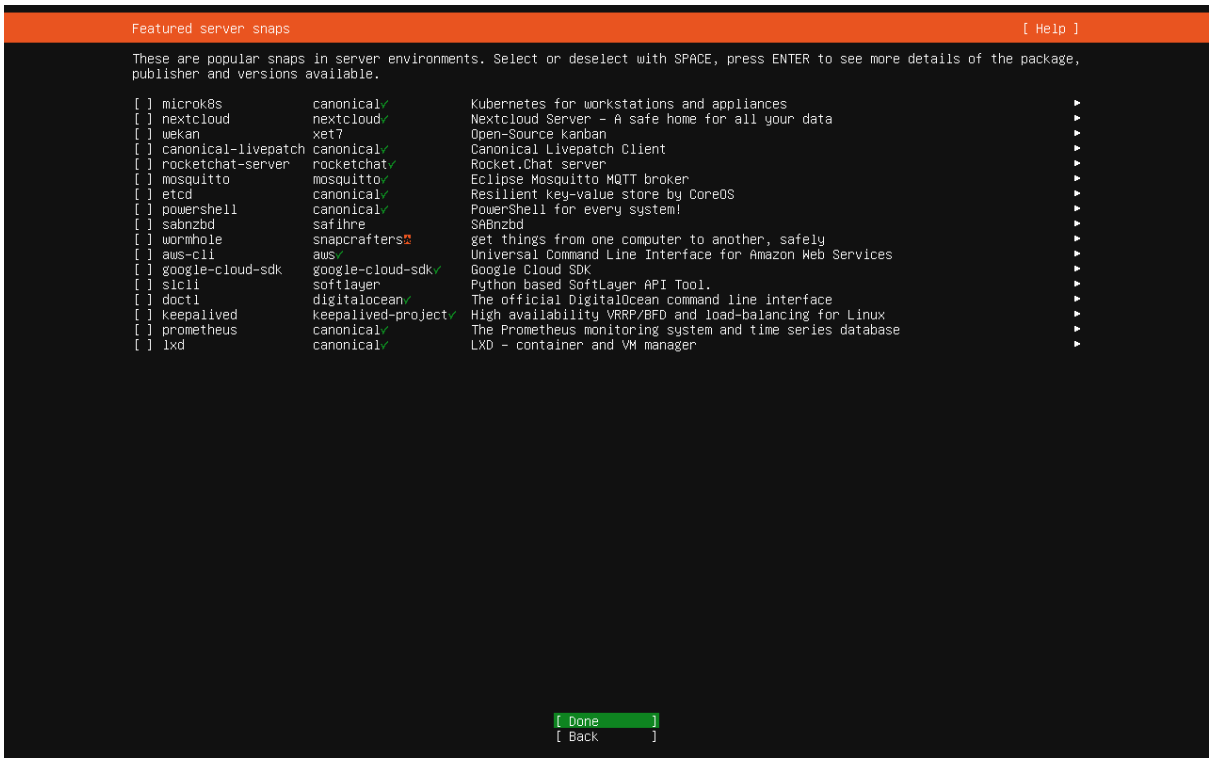

Figure 8

The next one is “Installing system”. The Ubuntu server will be installed on our virtual machine.

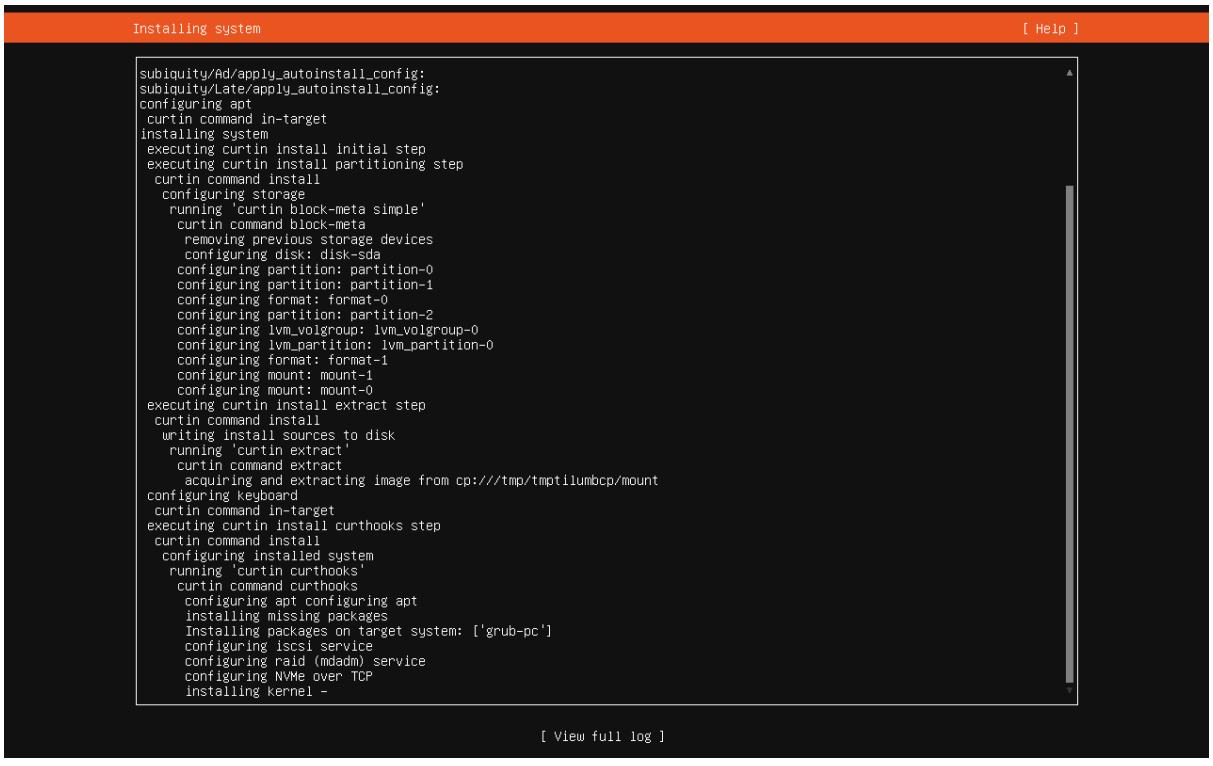

Figure 9

When the installation is completed, you will see a “Reboot now”. Select it and press Enter.

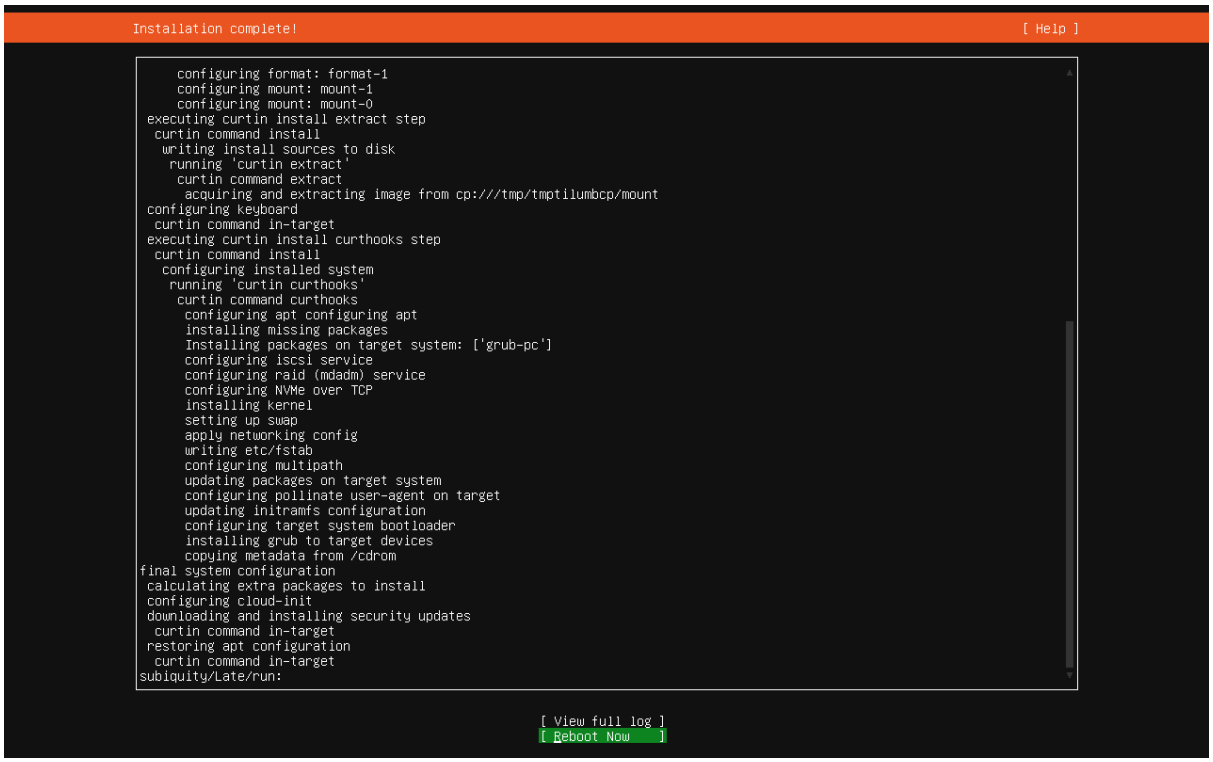

Figure 10

Once the system has been rebooted, a log-on screen will appear.

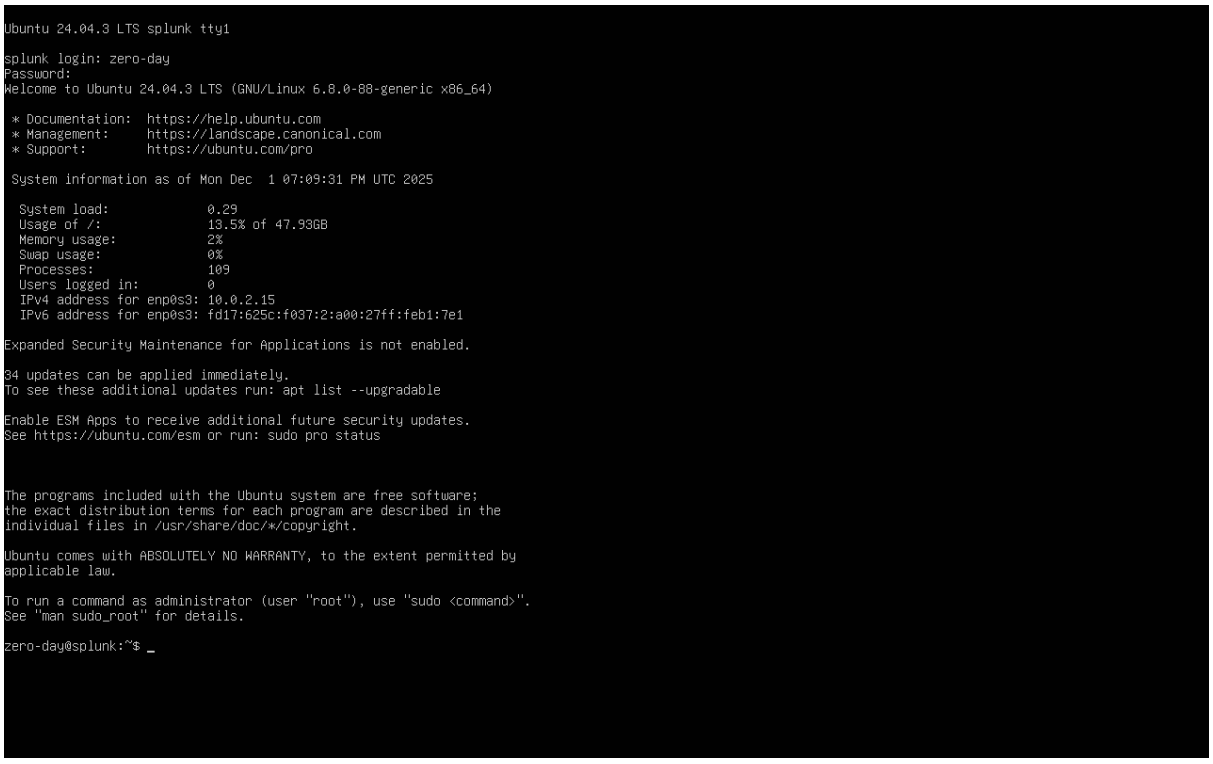

Figure 11

Now log on with the account we created earlier. The password is not shown for security purposes. Once we logged in let’s run an upgrade and update. To do that, type in “sudo apt-get update && sudo apt-get upgrade -y”.

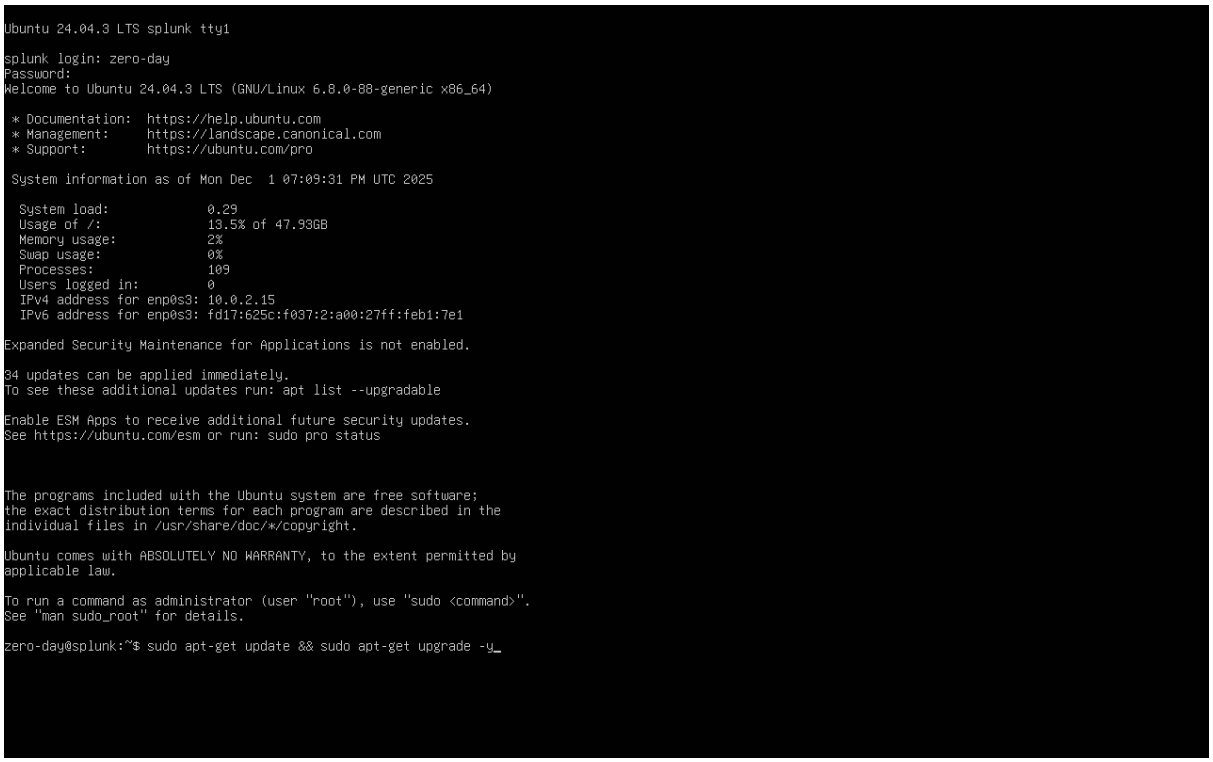

Figure 12

After you hit enter, it will update and upgrade the entire repository. Now, the server is ready.

In the next chapter, we will install Splunk and its forwarders and Sysmon.