

## 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

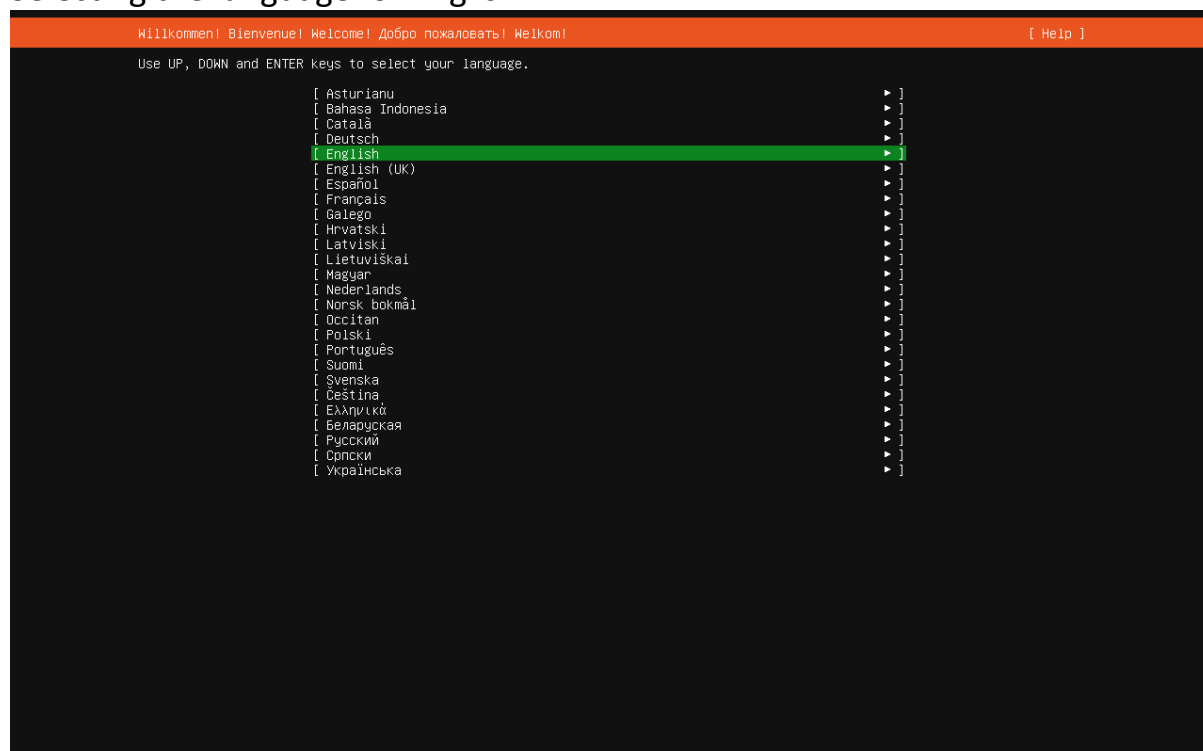


Figure 1

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

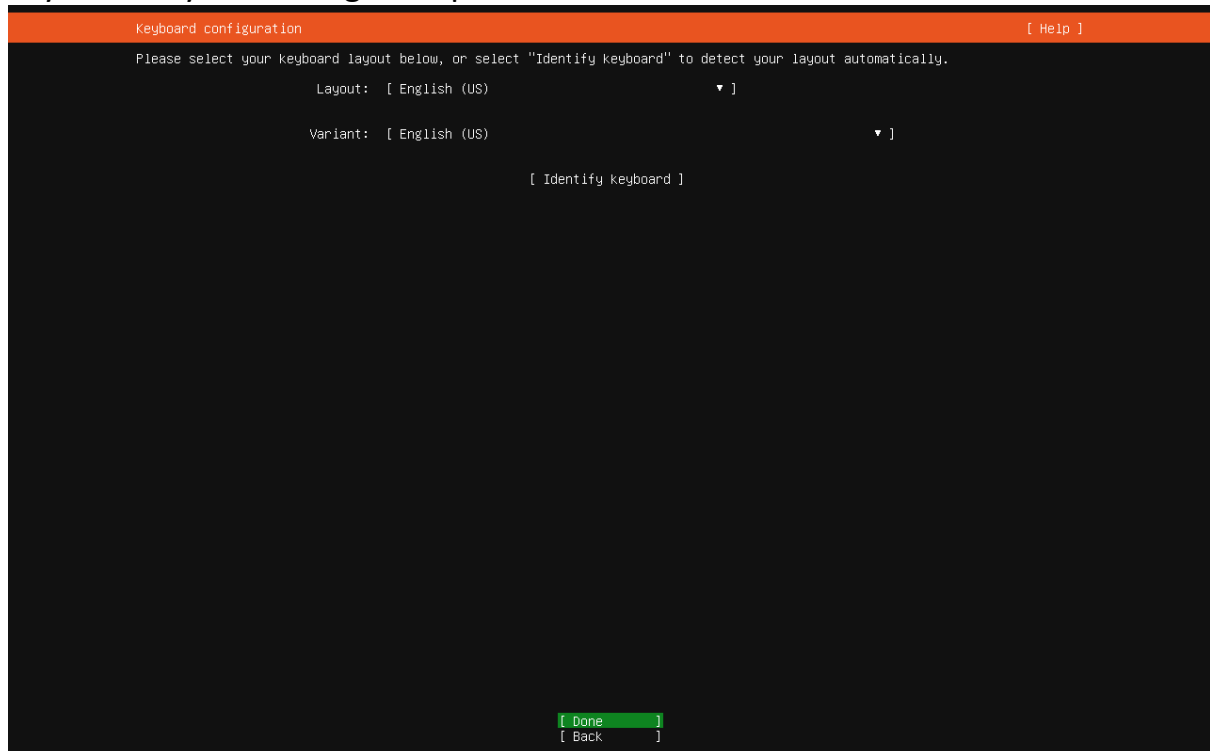


Figure 2

Now press “Done”

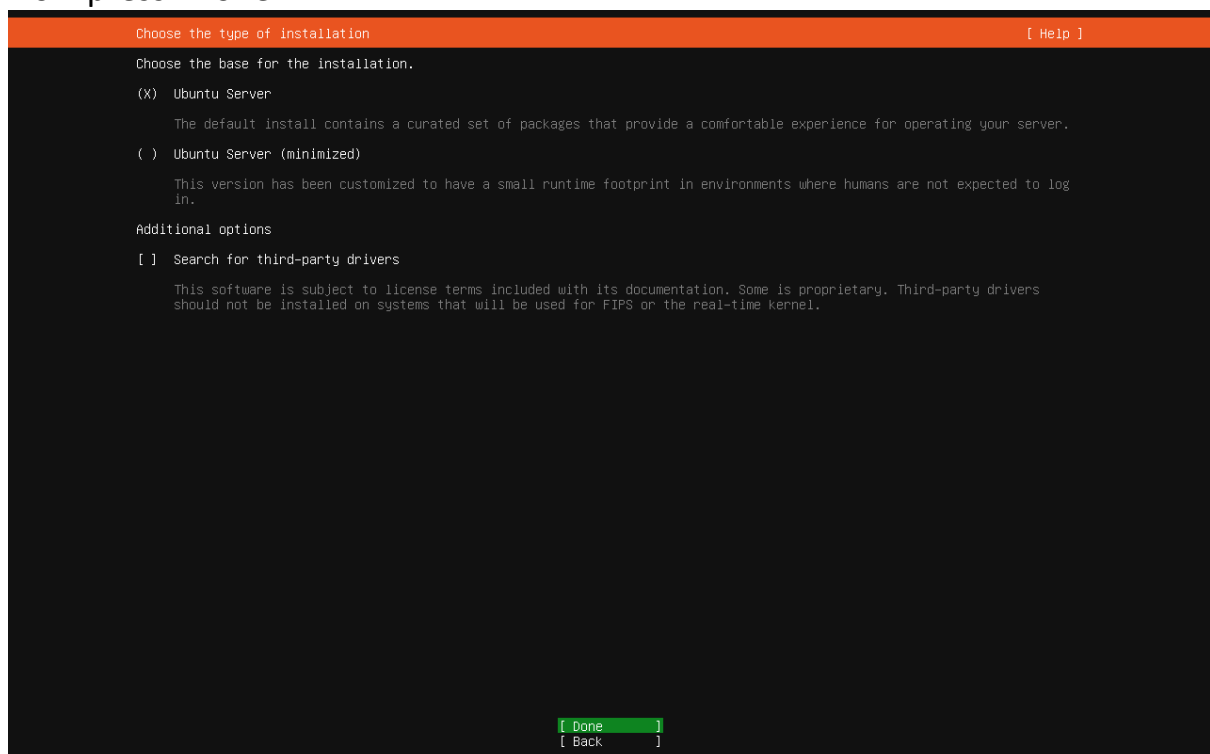


Figure 3

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

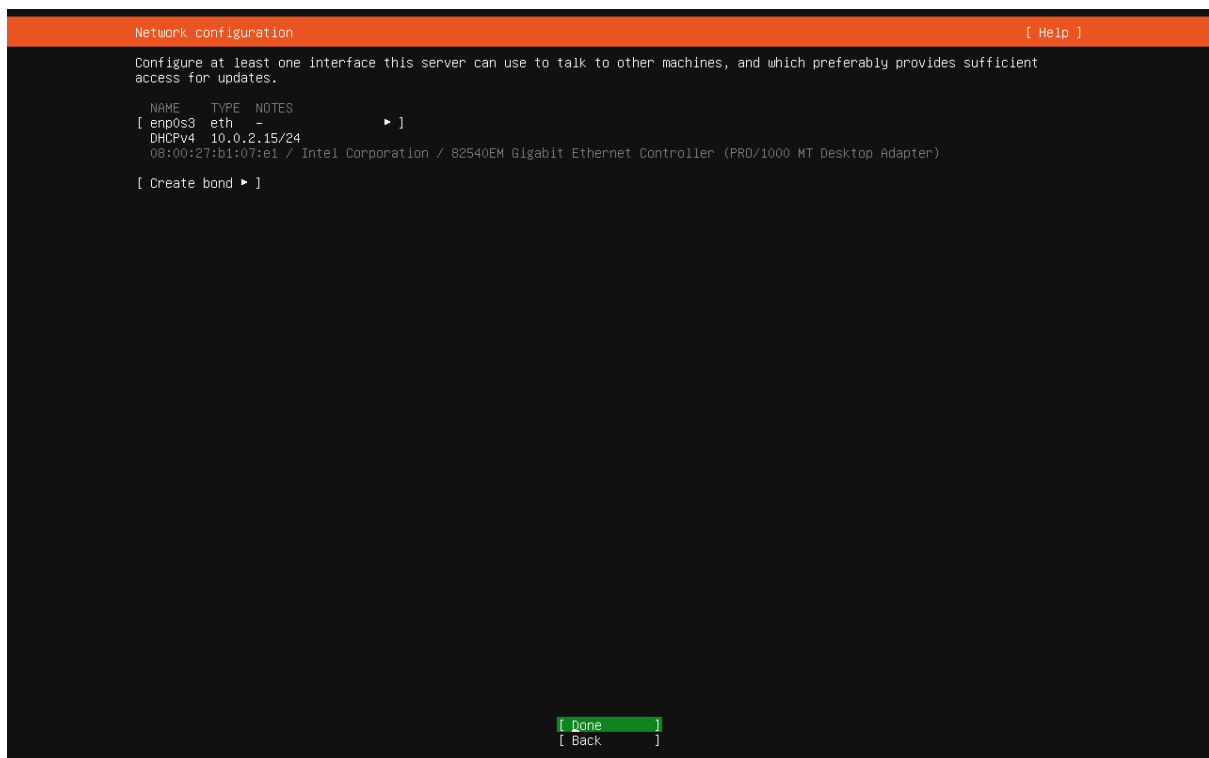


Figure 4

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”.

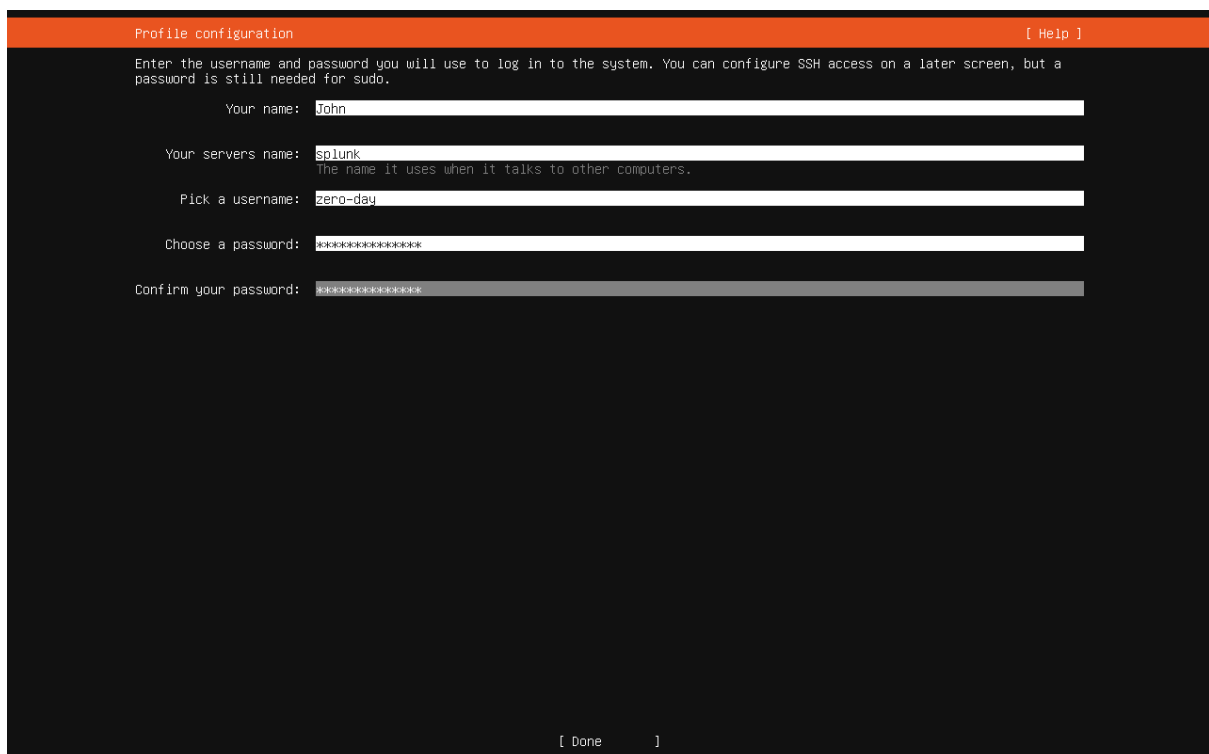


Figure 5

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

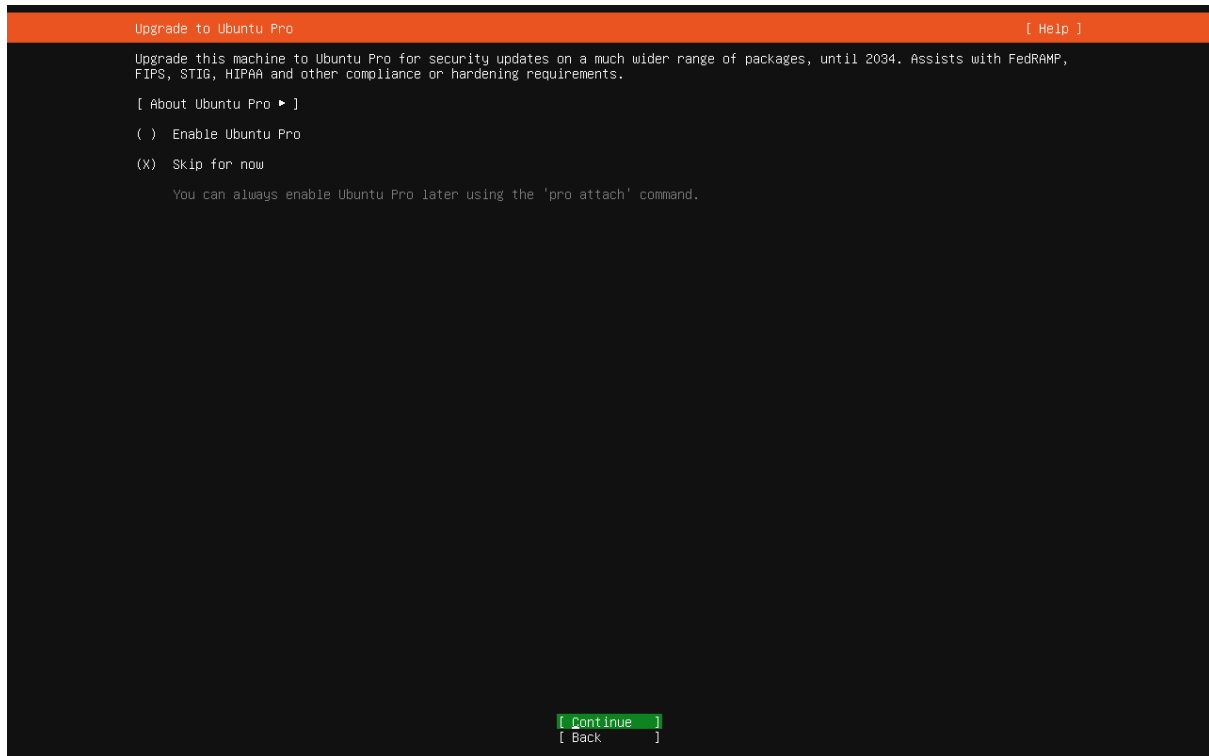


Figure 6

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

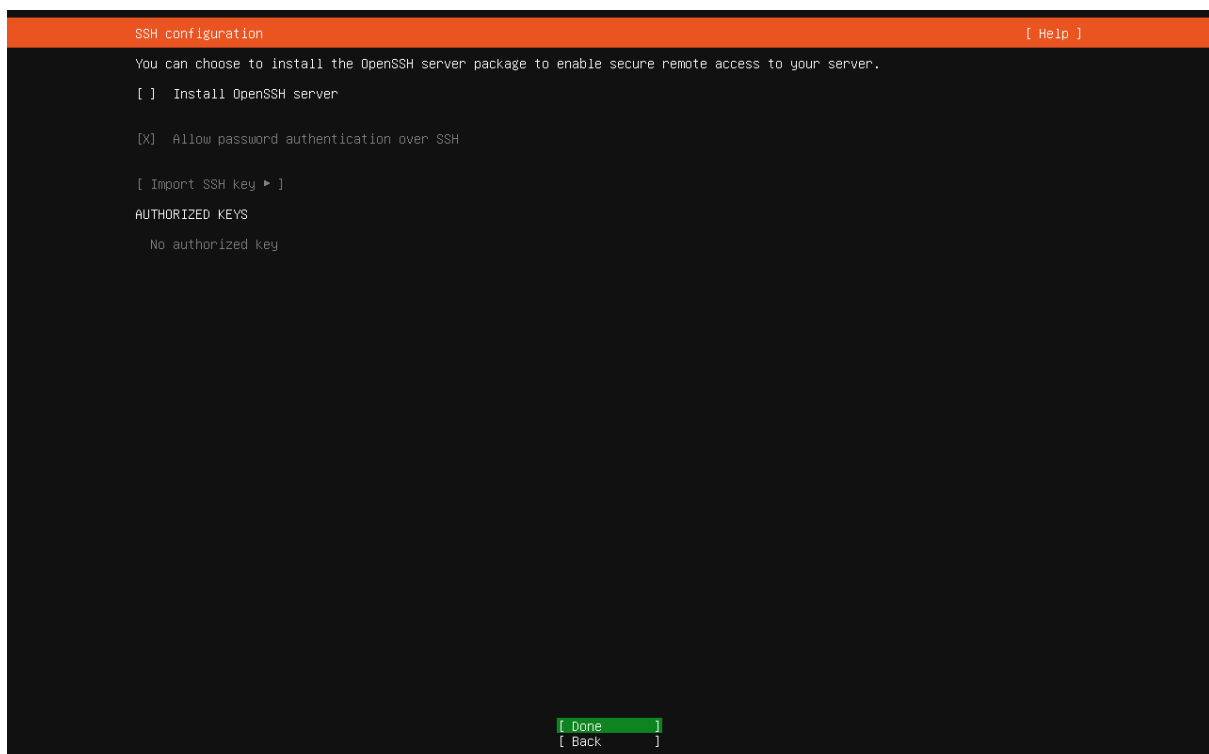


Figure 7

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

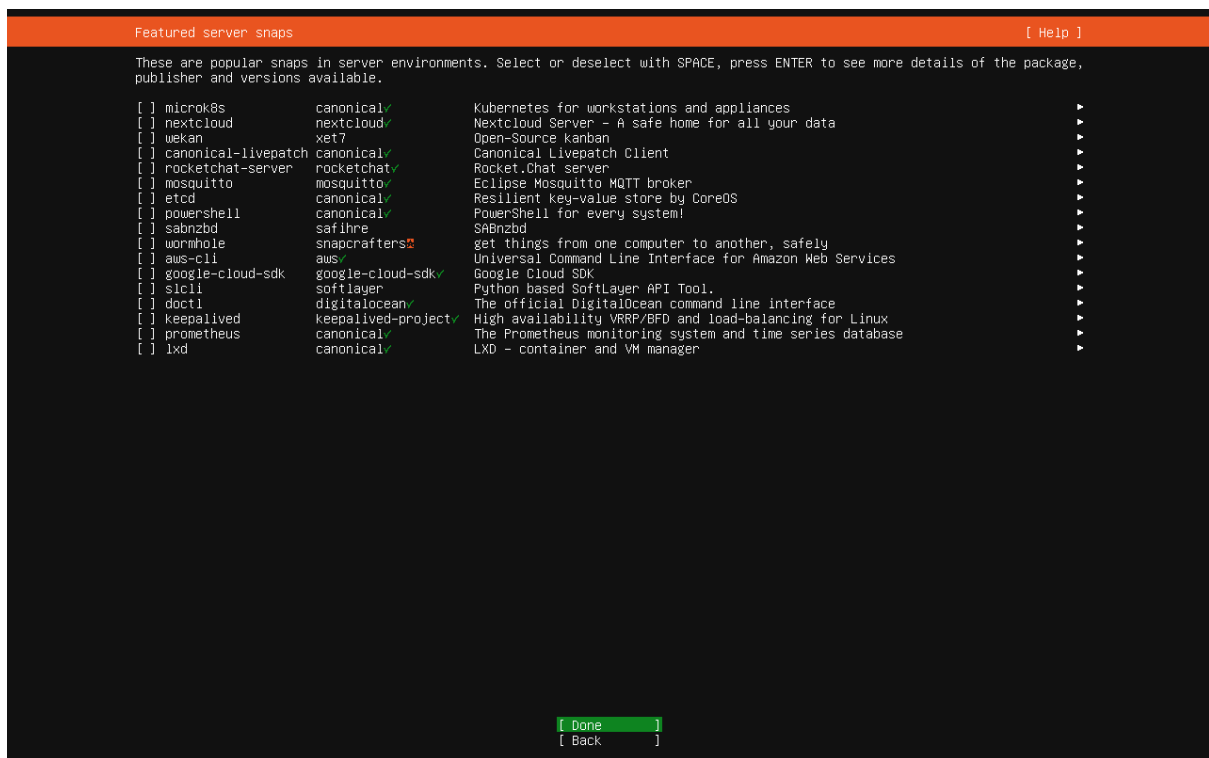


Figure 8

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

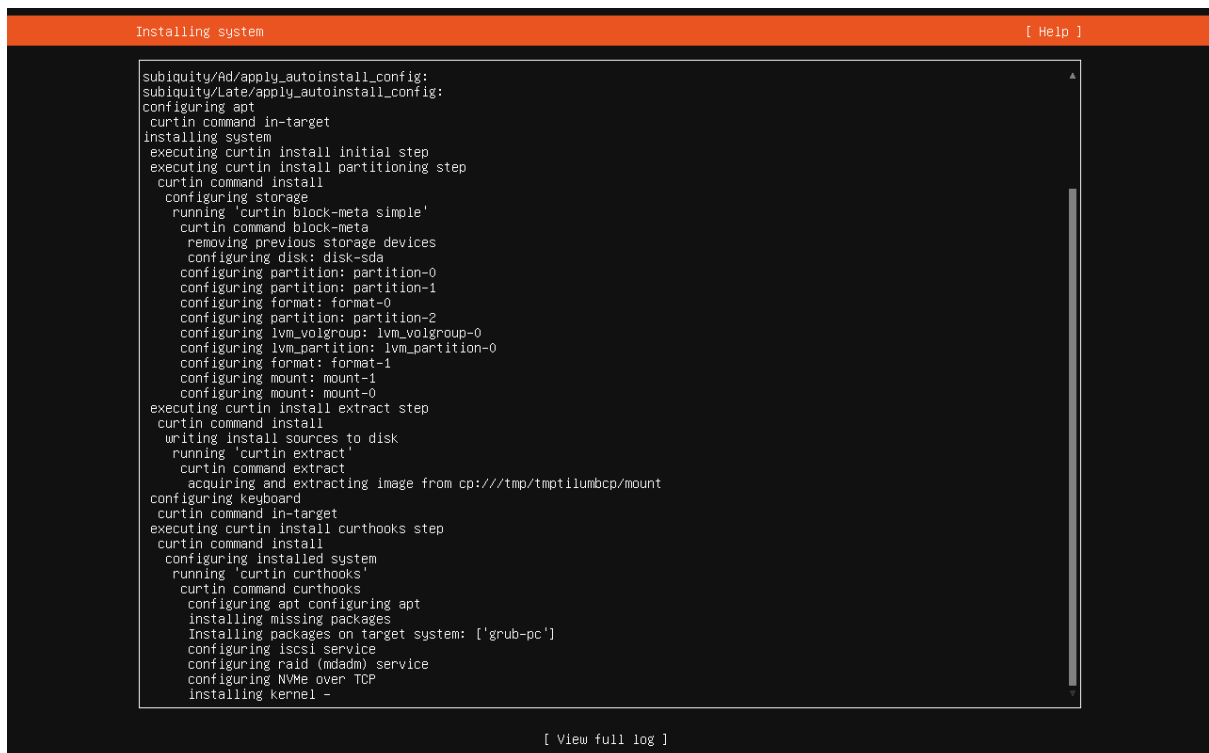


Figure 9

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

```
Installation complete! [ Help ]

configuring format: format-1
configuring mount: mount-1
configuring mount: mount-0
executing curtin install extract step
curtin command install
writing install sources to disk
running 'curtin extract'
curtin command extract
acquiring and extracting image from cp:///tmp/tmptilumbcp/mount
configuring keyboard
curtin command in-target
executing curtin install curthooks step
curtin command install
configuring installed system
running 'curtin curthooks'
curtin command curthooks
configuring apt configuring apt
installing missing packages
Installing packages on target system: ['grub-pc']
configuring iscsi service
configuring raid (mdadm) service
configuring NVMe over TCP
installing kernel
setting up swap
apply networking config
writing etc/fstab
configuring multipath
updating packages on target system
configuring pollinate user-agent on target
updating initramfs configuration
configuring target system bootloader
installing grub to target devices
copying metadata from /cdrom
final system configuration
calculating extra packages to install
configuring cloud-init
downloading and installing security updates
curtin command in-target
restoring apt configuration
curtin command in-target
subiquity/Late/run:

[ View full log ]
[ Reboot Now ]
```

Figure 10

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

```
Ubuntu 24.04.3 LTS splunk tty1
splunk login: zero-day
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-88-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Mon Dec  1 07:09:31 PM UTC 2025

System load:          0.29
Usage of /:           13.5% of 47.93GB
Memory usage:         2%
Swap usage:           0%
Processes:            109
Users logged in:      0
IPv4 address for enp0s3: 10.0.2.15
IPv6 address for enp0s3: fd17:625c:f037:2:a00:27ff:feb1:7e1

Expanded Security Maintenance for Applications is not enabled.

34 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See 'man sudo_root' for details.

zero-day@splunk:~$ _
```

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".

```
Ubuntu 24.04.3 LTS splunk tty1
splunk login: zero-day
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-88-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Mon Dec  1 07:09:31 PM UTC 2025

System load:          0.29
Usage of /:           13.5% of 47.9GB
Memory usage:         2%
Swap usage:           0%
Processes:            109
Users logged in:      0
IPv4 address for enp0s3: 10.0.2.15
IPv6 address for enp0s3: fd17:625c:f037:2:a00:27ff:feb1:7e1

Expanded Security Maintenance for Applications is not enabled.

34 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

zero-day@splunk:~$ 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.