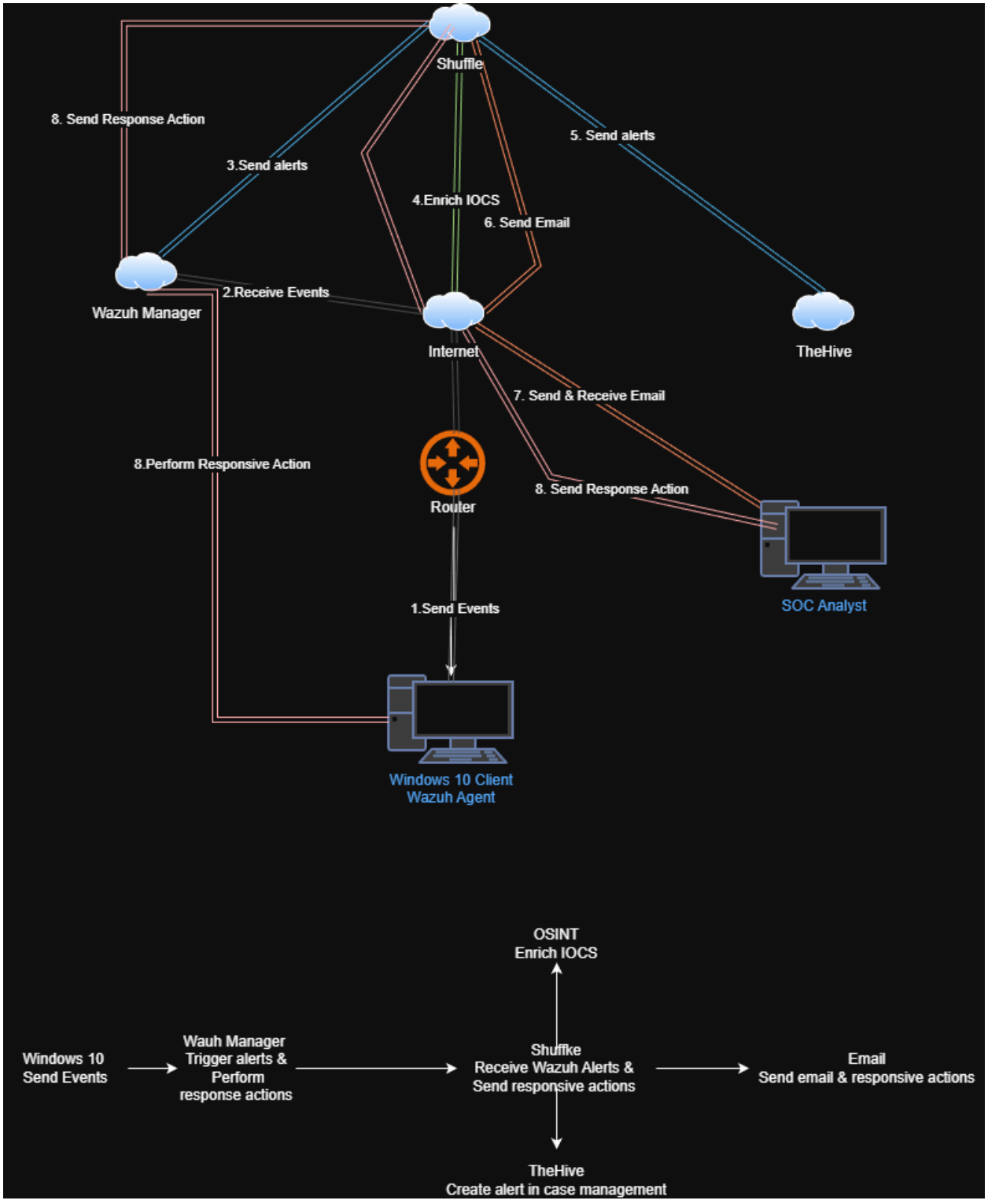
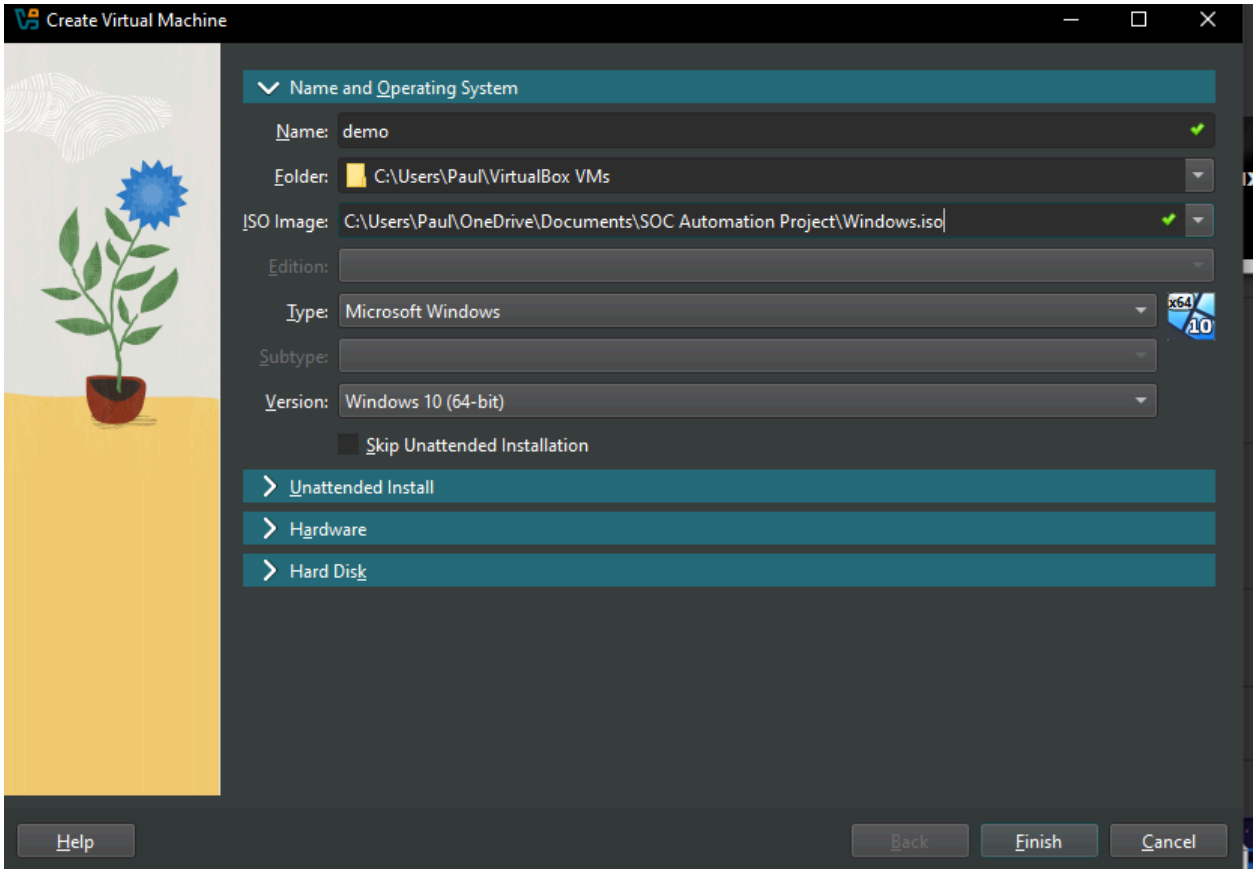
Initial Lab Design

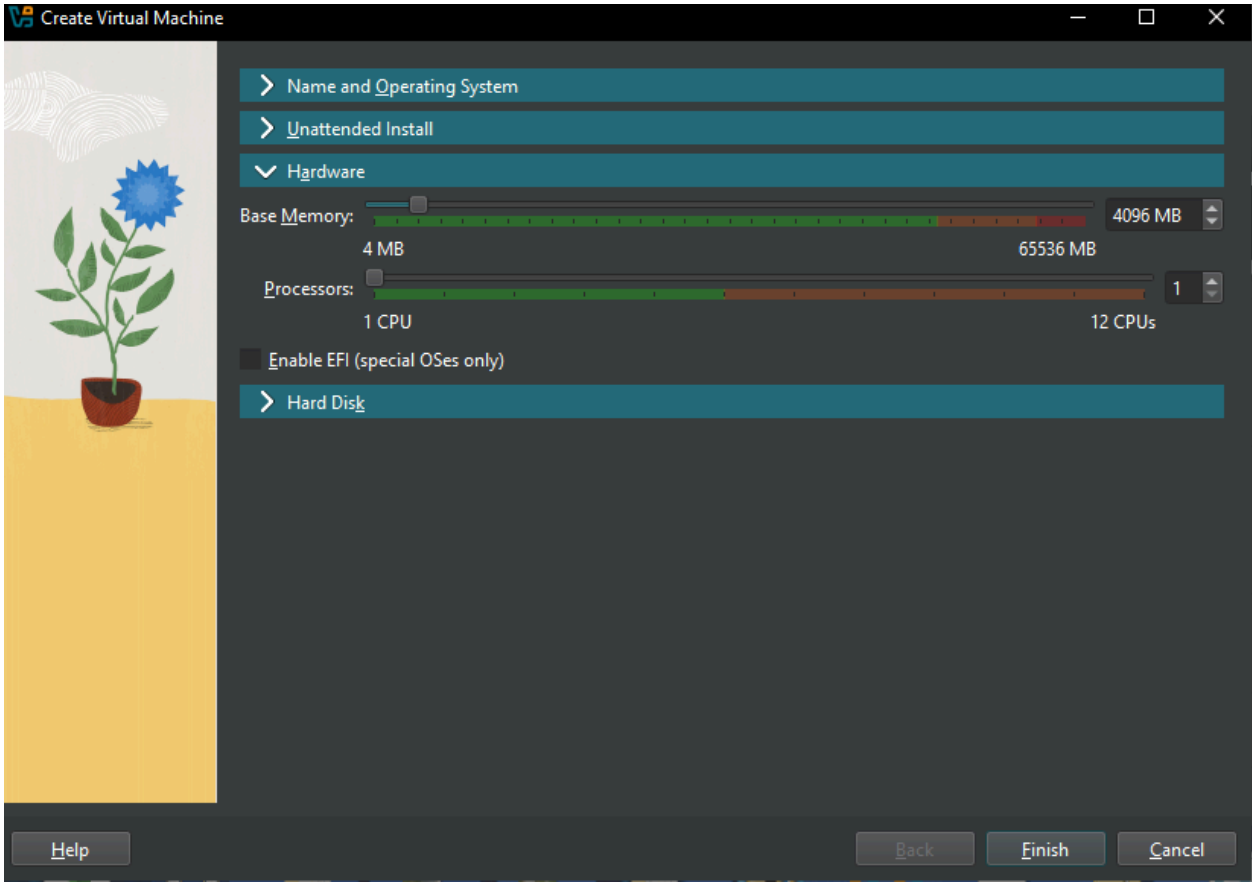


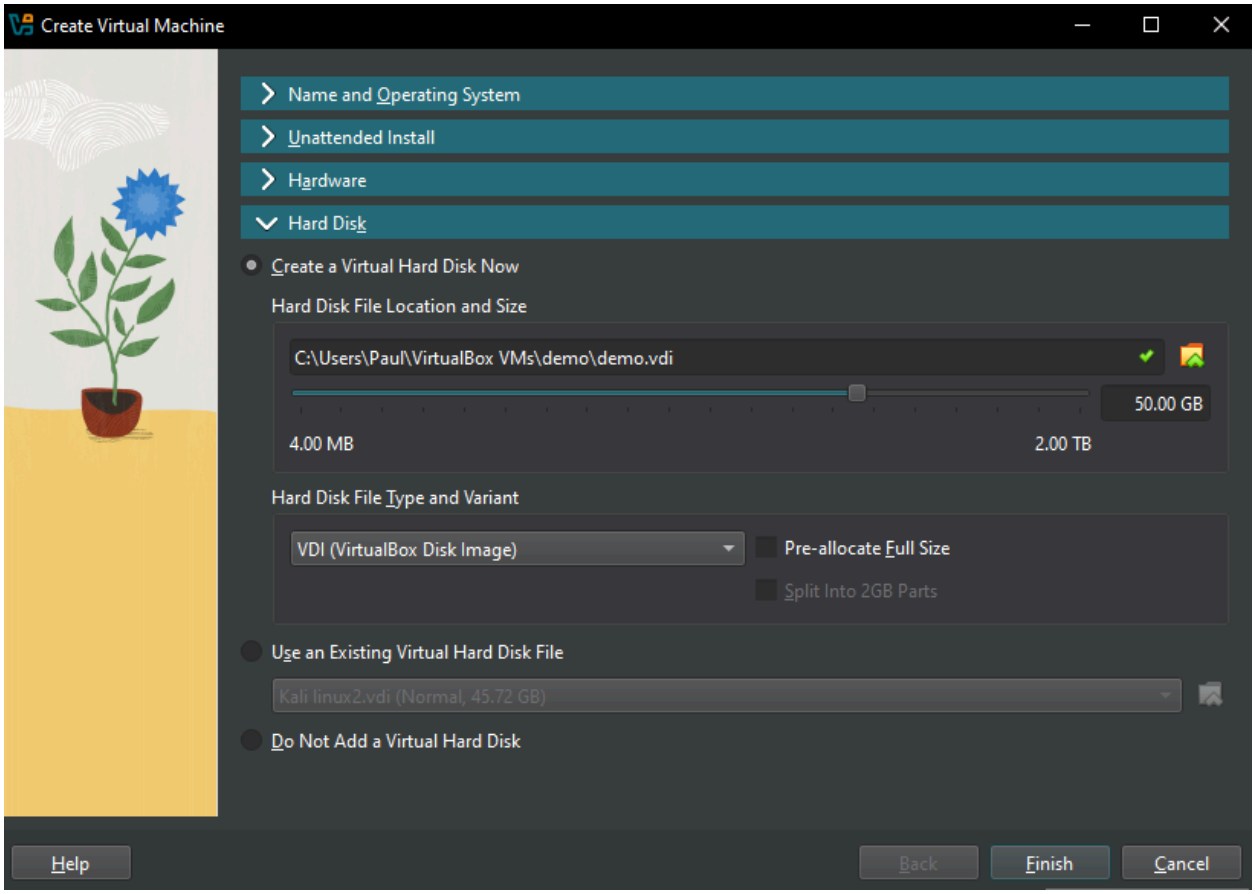
Setting Up Infrustructure

Windows 10 Client Setup

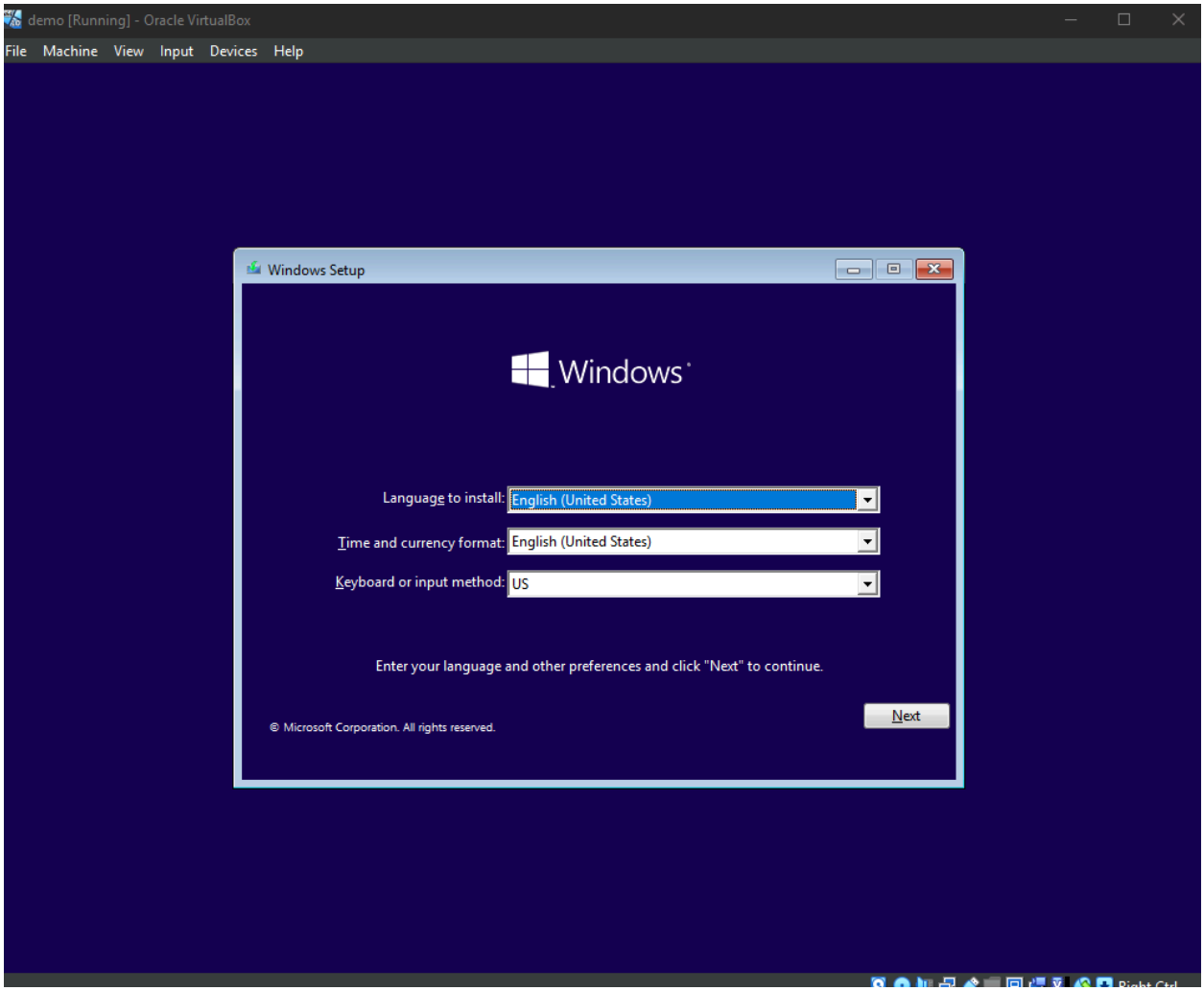
1. Install Windows 10 on VirtualBox



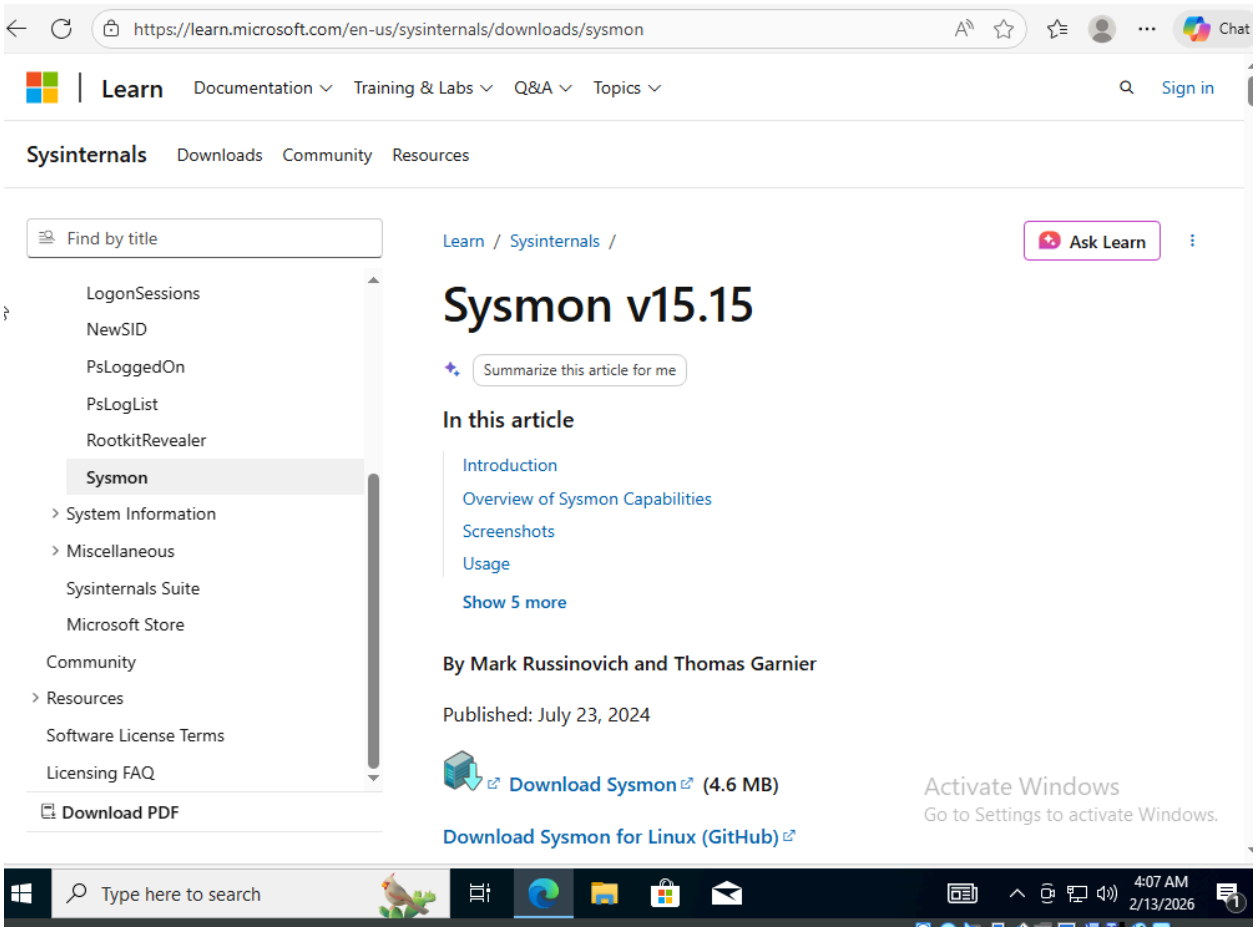

Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Base Memory:
4096 MB
4 MB
65536 MB
Processors:
1
1 CPU
12 CPUs
Enable EFI (special OSes only)
Hard Disk
Help
Back
Finish
Cancel


Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Hard Disk
Create a Virtual Hard Disk Now
Hard Disk File Location and Size
C:\Users\Paul\VirtualBox VMs\demo\demo.vdi
50.00 GB
4.00 MB
2.00 TB
Hard Disk File Type and Variant
VDI (VirtualBox Disk Image)
Pre-allocate Full Size
Split Into 2GB Parts
Use an Existing Virtual Hard Disk File
Kali linux2.vdi (Normal, 45.72 GB)
Do Not Add a Virtual Hard Disk
Help
Back
Finish
Cancel

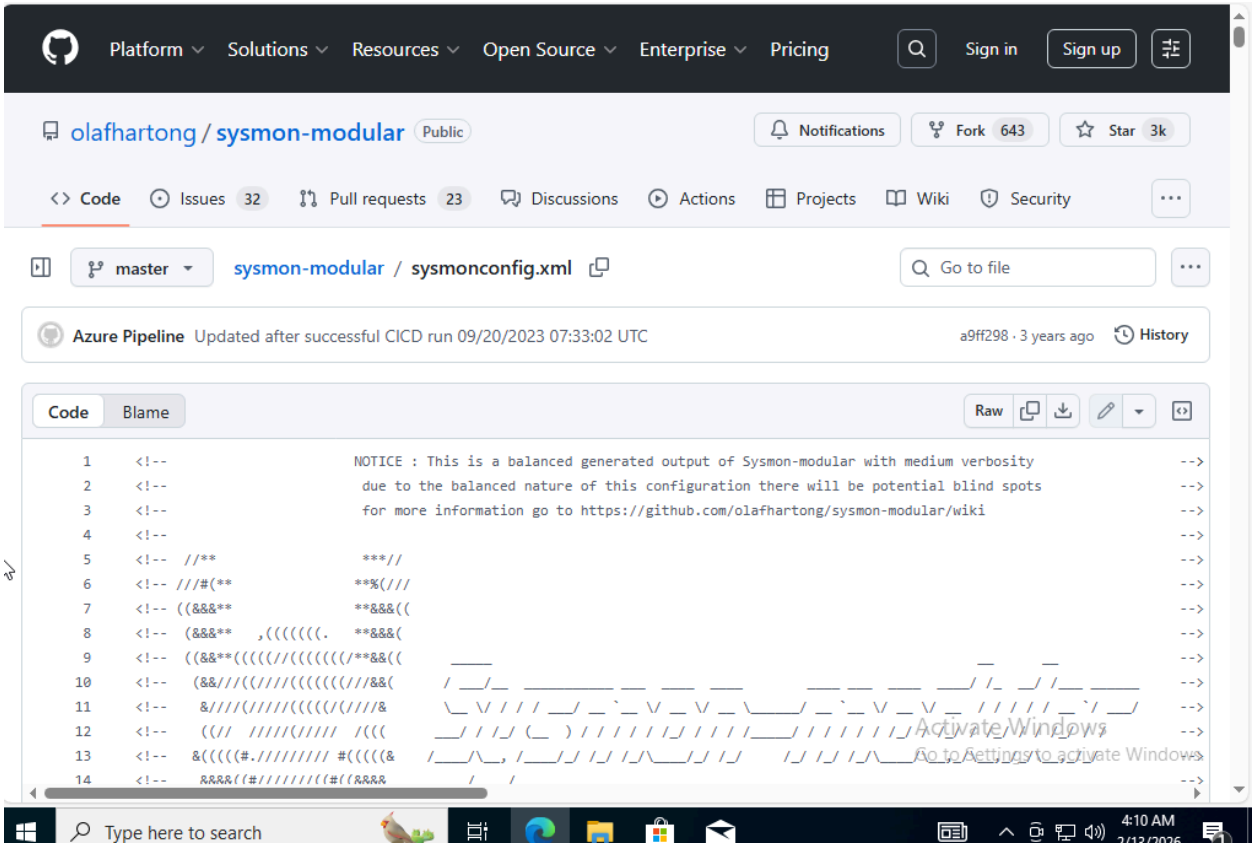
2. Click through installation



Installing Sysmon

1. 

2. Download config file

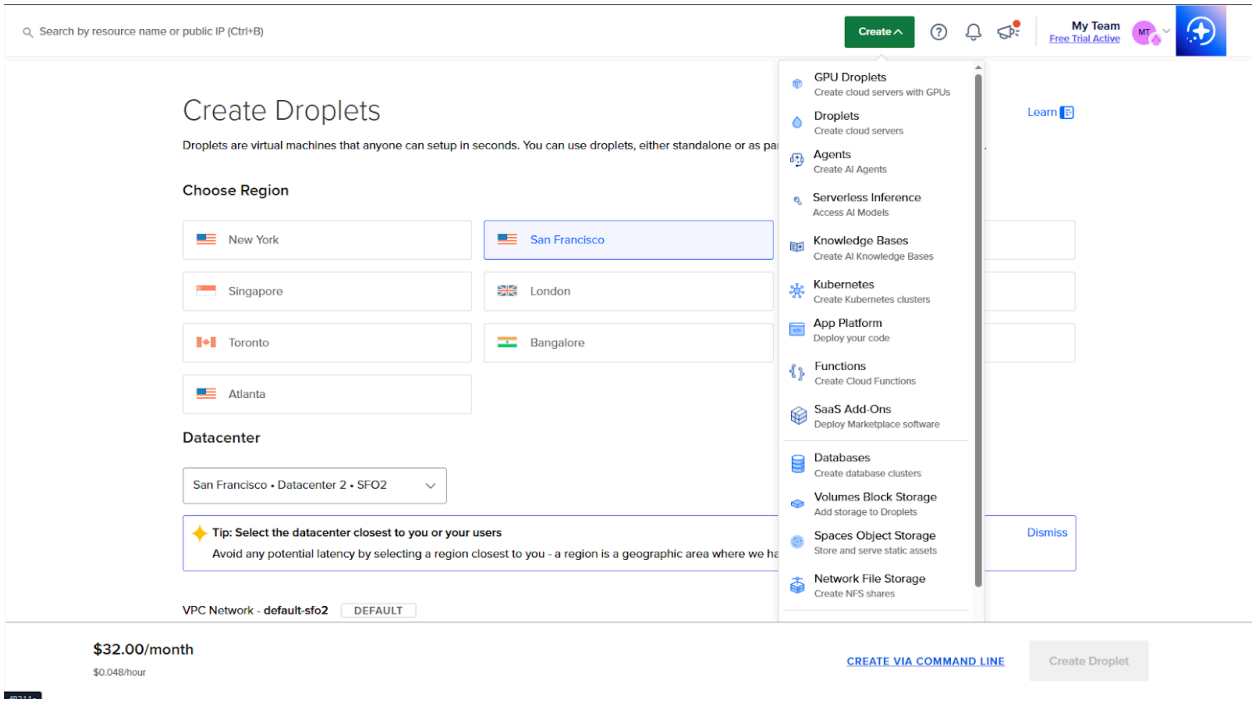


3. Configure Sysmon with PowerShell, ensure all files are in the working directory

```
PS C:\Windows\system32> cd C:\Users\SOCAu\Downloads\Sysmon
PS C:\Users\SOCAu\Downloads\Sysmon> ls


    Directory: C:\Users\SOCAu\Downloads\Sysmon


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/13/2026   4:11 AM           7490 Eula.txt
-a----         2/13/2026   4:11 AM        8480560 Sysmon.exe
-a----         2/13/2026   4:11 AM        4563248 Sysmon64.exe
-a----         2/13/2026   4:11 AM        4993440 Sysmon64a.exe


PS C:\Users\SOCAu\Downloads\Sysmon> ls


    Directory: C:\Users\SOCAu\Downloads\Sysmon


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/13/2026   4:11 AM           7490 Eula.txt
-a----         2/13/2026   4:11 AM        8480560 Sysmon.exe
-a----         2/13/2026   4:11 AM        4563248 Sysmon64.exe
-a----         2/13/2026   4:11 AM        4993440 Sysmon64a.exe
-a----         2/13/2026   4:11 AM         253169 sysmonconfig.xml
```

```
PS C:\Users\SOCAu\Downloads\Sysmon> .\Sysmon64.exe -i sysmonconfig.xml


System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Users\SOCAu\Downloads\Sysmon>
```

Build Wazauh Server on Digital Ocean

1. 

Choose an image

OS | Marketplace (249) | Custom images

Ubuntu | Fedora | Debian | CentOS | AlmaLinux | Rocky Linux

Version

22.04 (LTS) x64

Choose Size

Need help picking a plan? Help me choose

Droplet Type

SHARED CPU	DEDICATED CPU			
Basic (Plan selected)	General Purpose	CPU-Optimized	Memory-Optimized	Storage-Optimized

Basic virtual machines with a mix of memory and compute resources. Best for small projects that can handle variable levels of CPU performance, like blogs, web apps and dev/test environments.

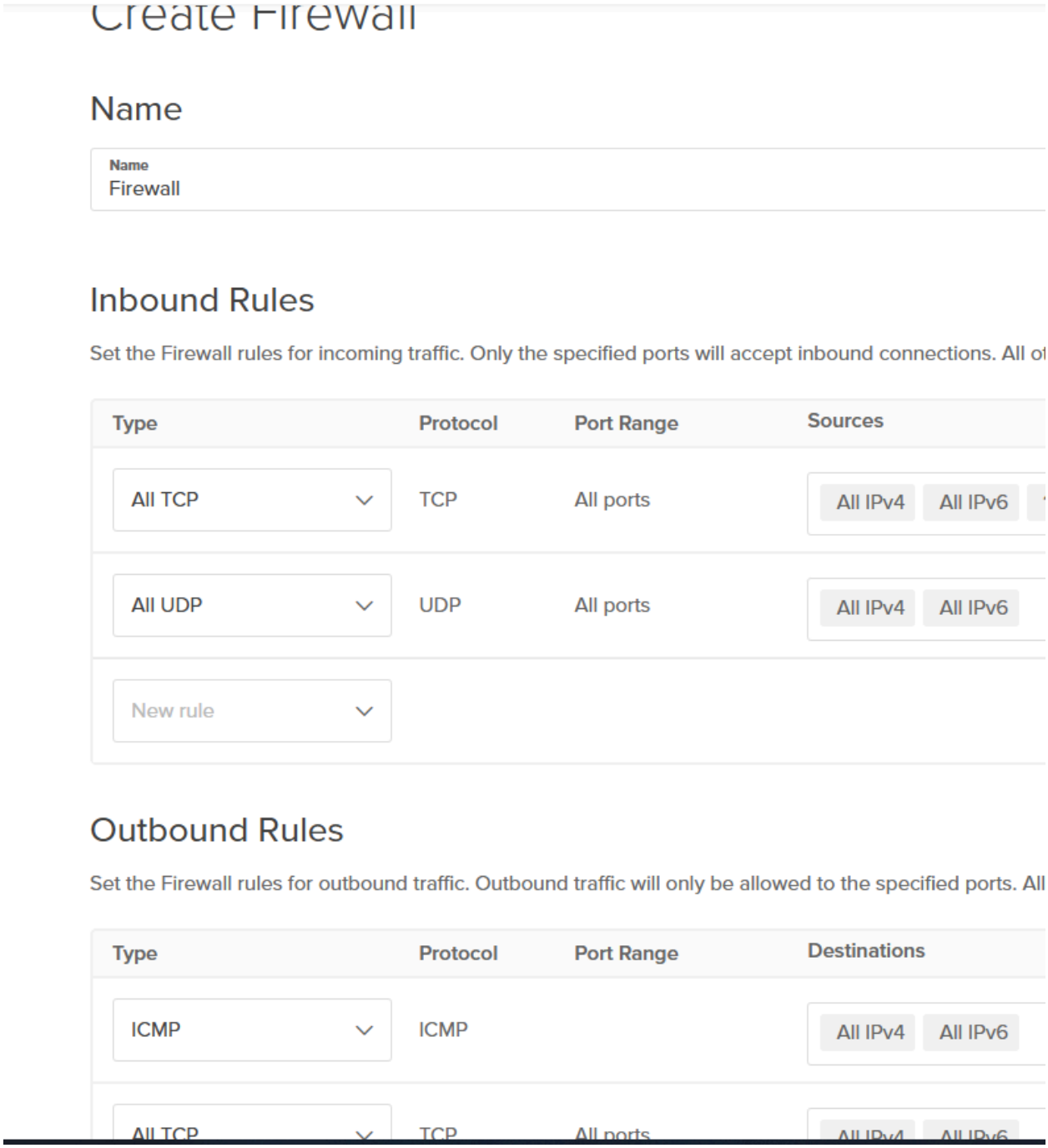
CPU options

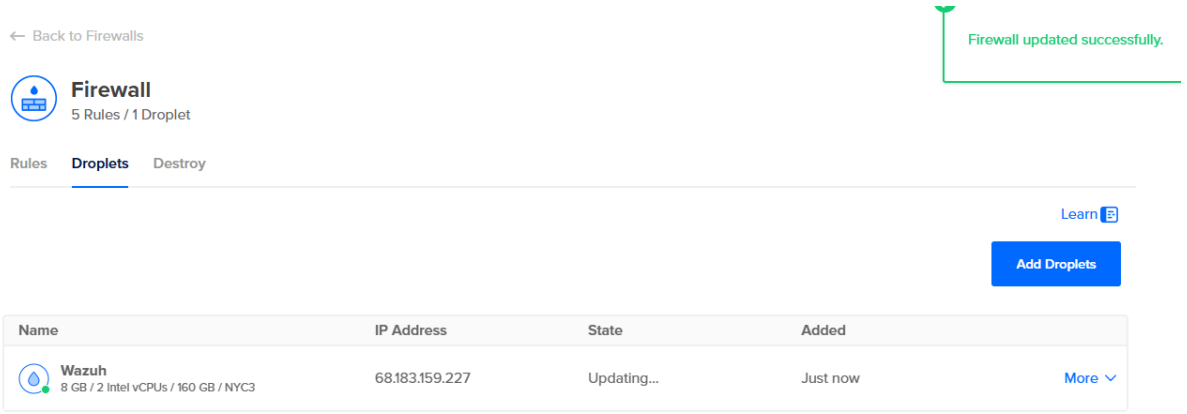
Regular	Premium Intel	Premium AMD
Disk type: SSD	Disk: NVMe SSD	Disk: NVMe SSD

$8/mo	$16/mo	$24/mo	$32/mo	$48/mo	$64/mo
$0.012/hour	$0.024/hour	$0.036/hour	$0.048/hour	$0.071/hour	$0.095/hour
1 GB / 1 Intel CPU 35 GB NVMe SSDs 1000 GB transfer	2 GB / 1 Intel CPU 70 GB NVMe SSDs 2 TB transfer	2 GB / 2 Intel CPUs 90 GB NVMe SSDs 3 TB transfer	4 GB / 2 Intel CPUs 120 GB NVMe SSDs 4 TB transfer	8 GB / 2 Intel CPUs 160 GB NVMe SSDs 5 TB transfer	8 GB / 4 Intel CPUs 240 GB NVMe SSDs 6 TB transfer

2.

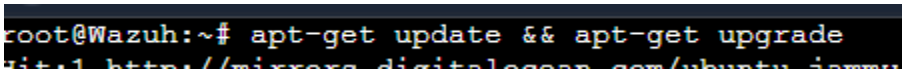
Create a Firewall

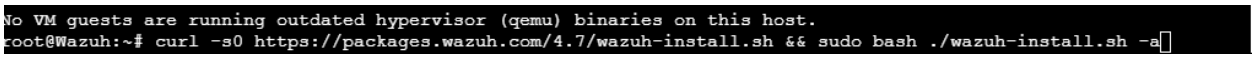
1. 



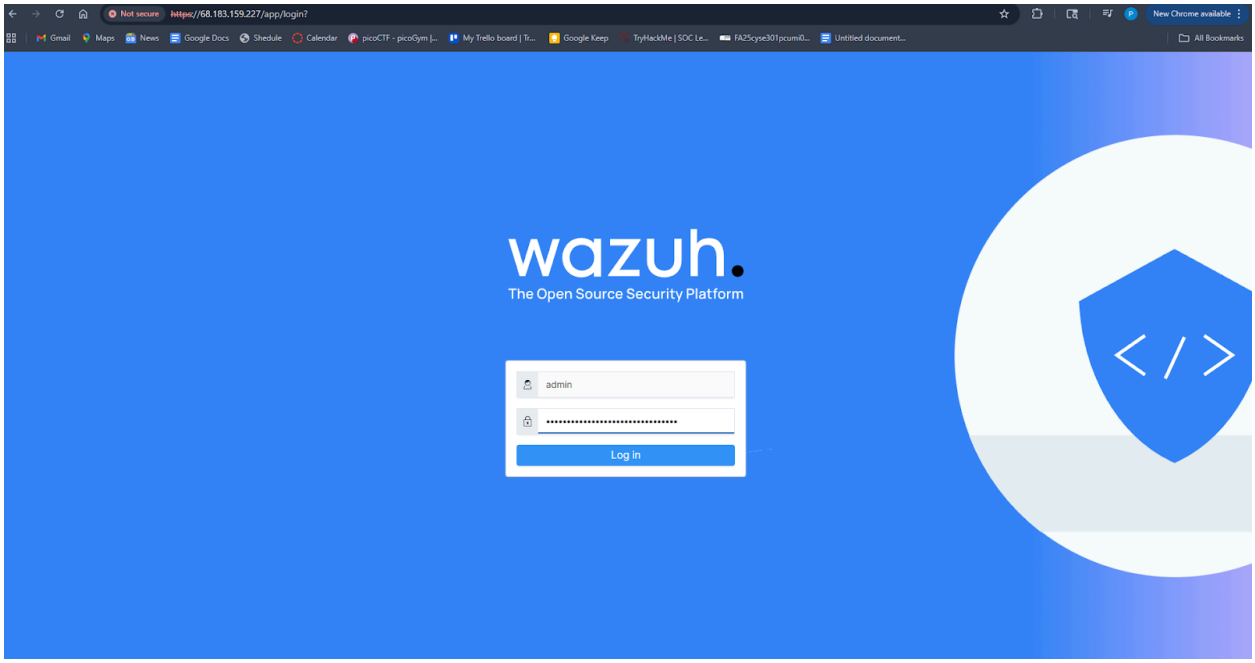
2.

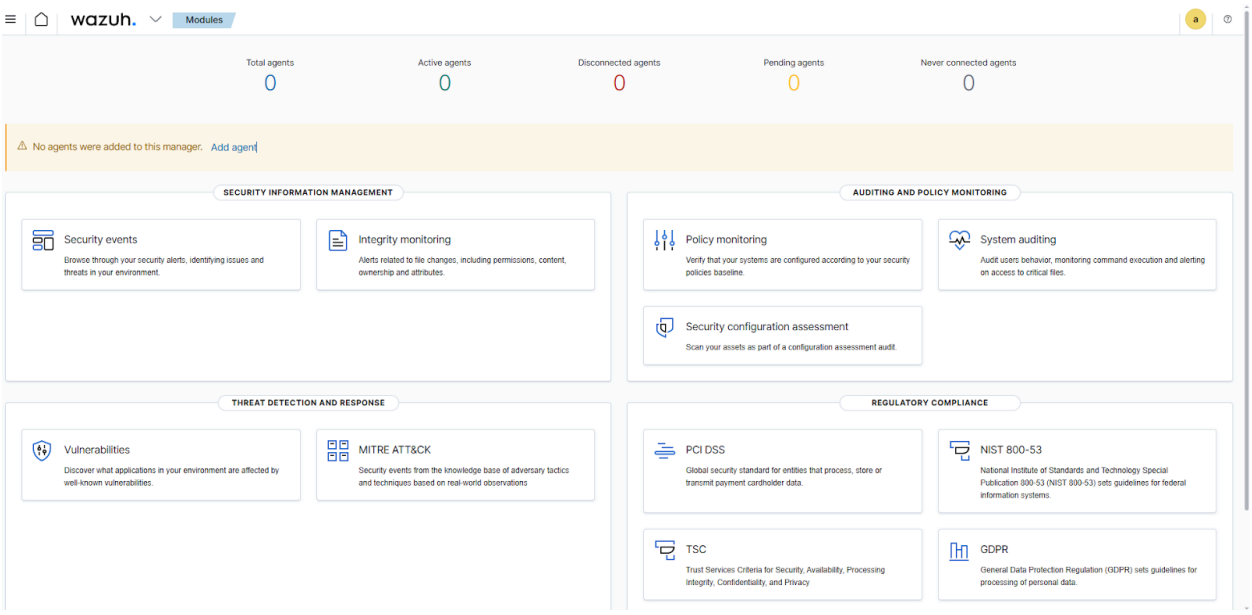
SSH Into Wazuh to Update and Upgrade

1. 

2. 

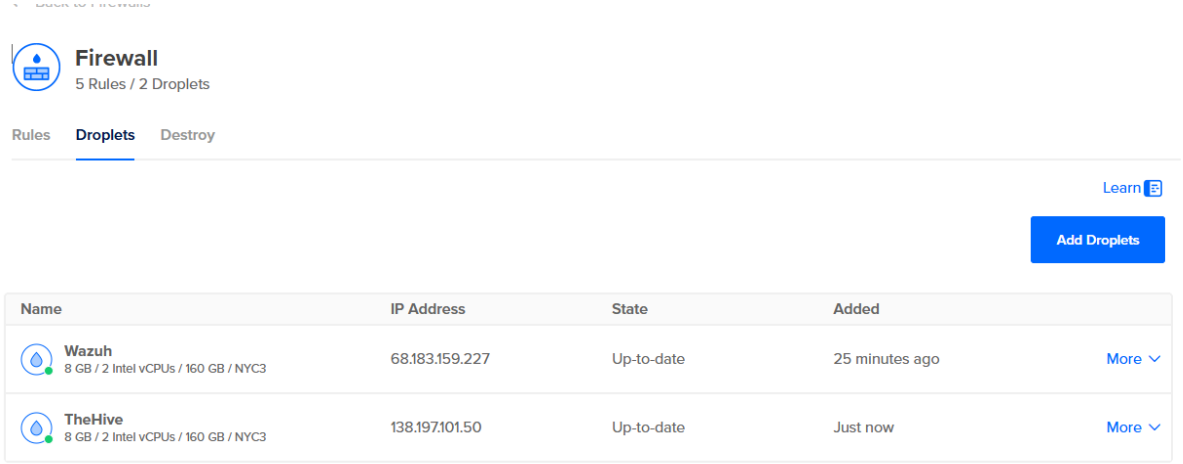
3. Login into wazzah via webbrowser



4. 

Install TheHive

1. Create a droplet similar to Wazuh and add the TheHive droplet to Firewall



2. Install java, Cassandra, Elastic Search, and TheHive on the server!

```
root@TheHive:~# wget -qO- https://apt.corretto.aws/corretto.key | sudo gpg --dearmor  -o /usr/share/keyrings/corr
etto.gpg
echo "deb [signed-by=/usr/share/keyrings/corretto.gpg] https://apt.corretto.aws stable main" |  sudo tee -a /etc/
apt/sources.list.d/corretto.sources.list
sudo apt update
sudo apt install java-common java-11-amazon-corretto-jdk
echo JAVA_HOME="/usr/lib/jvm/java-11-amazon-corretto" | sudo tee -a /etc/environment
export JAVA_HOME="/usr/lib/jvm/java-11-amazon-corretto"
```

```
root@TheHive:~# wget -qO -  https://downloads.apache.org/cassandra/KEYS | sudo gp
g --dearmor  -o /usr/share/keyrings/cassandra-archive.gpg
echo "deb [signed-by=/usr/share/keyrings/cassandra-archive.gpg] https://debian.ca
ssandra.apache.org 40x main" |  sudo tee -a /etc/apt/sources.list.d/cassandra.sou
rces.list
sudo apt update
sudo apt install cassandra
```

```
root@TheHive:~# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch |
sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
sudo apt-get install apt-transport-https
echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artif
acts.elastic.co/packages/7.x/apt stable main" |  sudo tee /etc/apt/sources.list.d
/elastic-7.x.list
sudo apt update
sudo apt install elasticsearch
```

```
root@TheHive:~# wget -O- https://archives.strangebee.com/keys/strangebee.gpg | su
do gpg --dearmor -o /usr/share/keyrings/strangebee-archive-keyring.gpg
echo 'deb [signed-by=/usr/share/keyrings/strangebee-archive-keyring.gpg] https://
deb.strangebee.com thehive-5.2 main' | sudo tee -a /etc/apt/sources.list.d/strang
ebee.list
sudo apt-get update
sudo apt-get install -y thehive
```

Configuring Machines to Work Together

Configure TheHive

1.
```
root@TheHive:~# nano /etc/cassandra/cassandra.yml
```

   Change rpc_address, listen_address and seed address to Hive's public IP

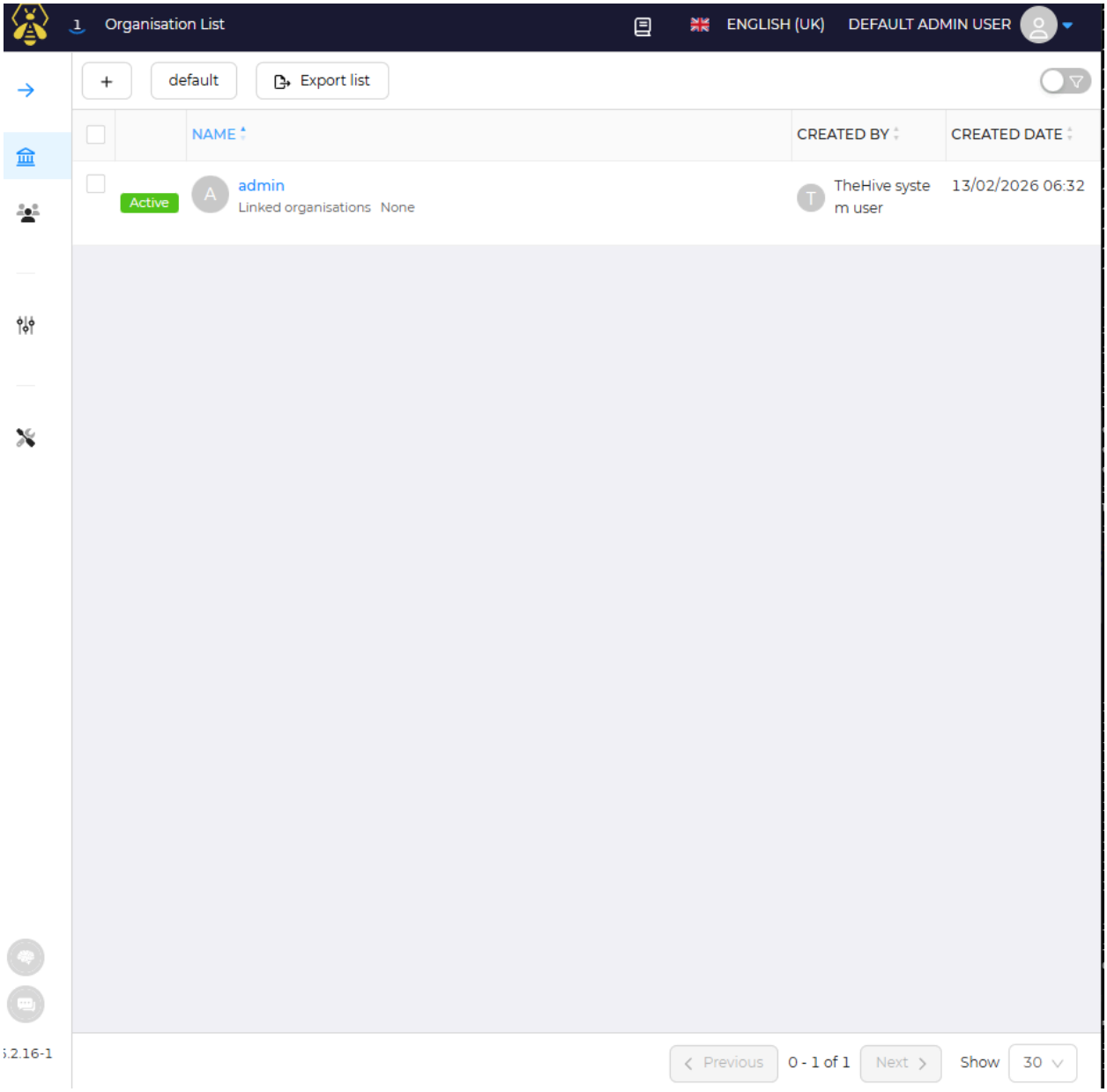
2.
```
root@TheHive:~# vim /etc/cassandra/cassandra.yaml
root@TheHive:~# systemctl stop cassandra.service
root@TheHive:~# rm -rf /var/lib/cassandra/*
root@TheHive:~# systemctl start cassandra.service
root@TheHive:~# systemctl status cassandra.service
● cassandra.service - LSB: distributed storage system for structured data
     Loaded: loaded (/etc/init.d/cassandra; generated)
     Active: active (exited) since Fri 2026-02-13 10:53:35 UTC; 14s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 23383 ExecStart=/etc/init.d/cassandra start (code=exited, status=0/SUCCESS)
        CPU: 10.458s

Feb 13 10:53:35 TheHive systemd[1]: Starting LSB: distributed storage system for structured data...
Feb 13 10:53:35 TheHive systemd[1]: Started LSB: distributed storage system for structured data.
root@TheHive:~#
```

Next, we configure Elastic Search

1.

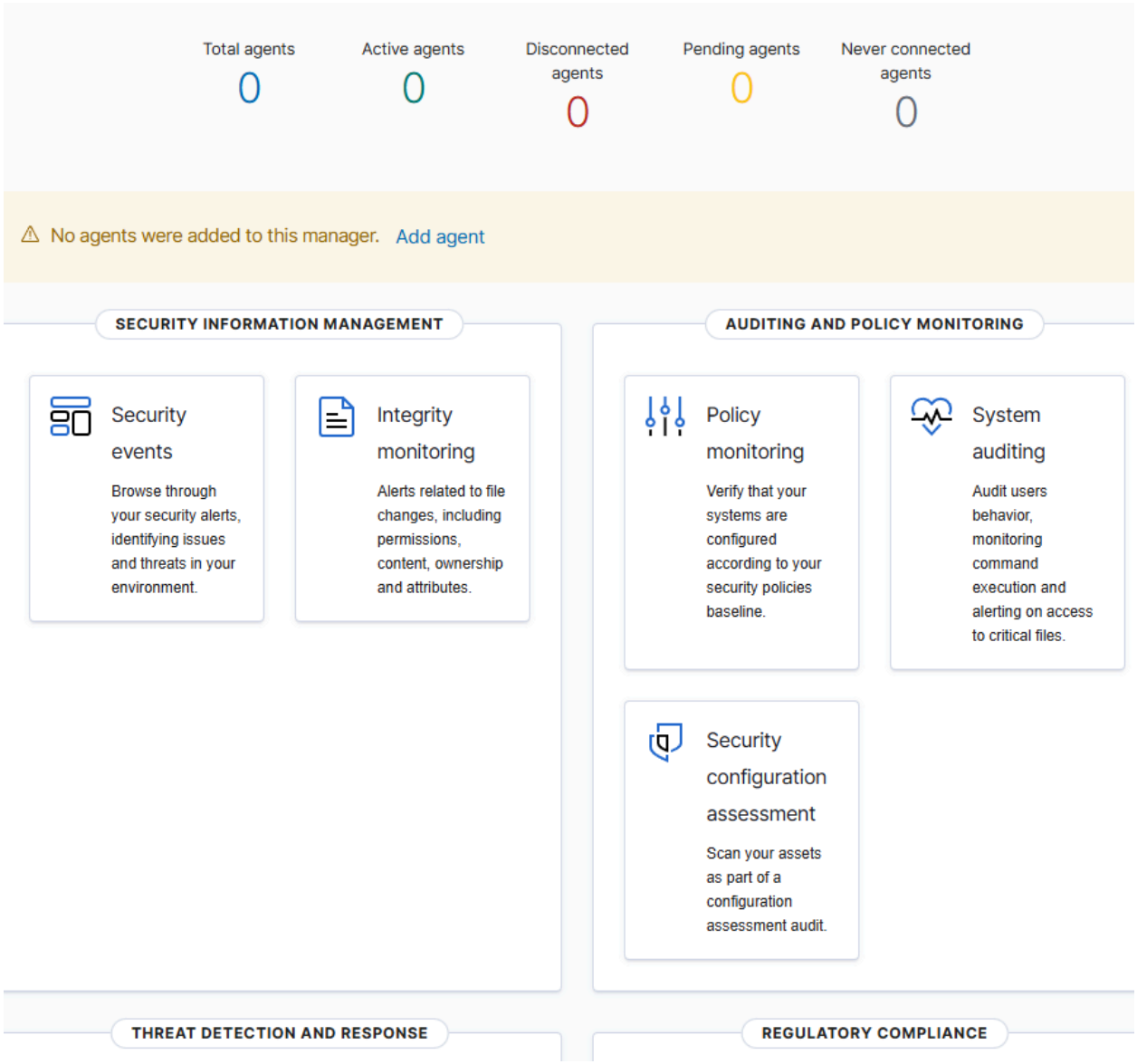
```
root@TheHive:~# vim /etc/elasticsearch/elasticsearch.yml
root@TheHive:~# systemctl start elasticsearch
root@TheHive:~# systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-ins
tall.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/
elasticsearch.service.
root@TheHive:~#
```

Lastly, we configure the Hive application.conf file and are finally able to loginto the hive via the web



Wazuh Configuration

Click on Add agent



Run through the creation window using Wazuh's public ip.
Copy the command provided and run it on the Windows VM.