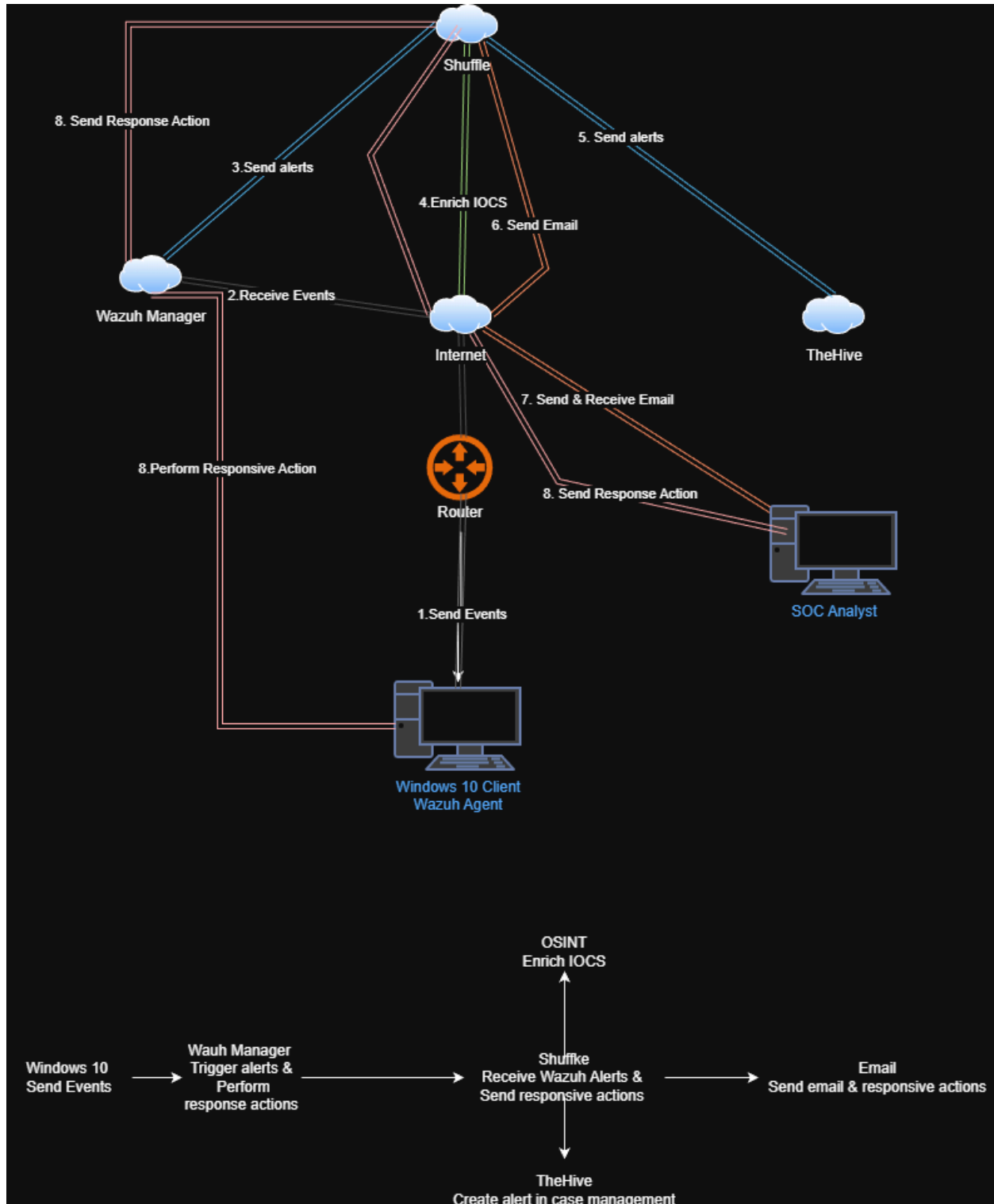


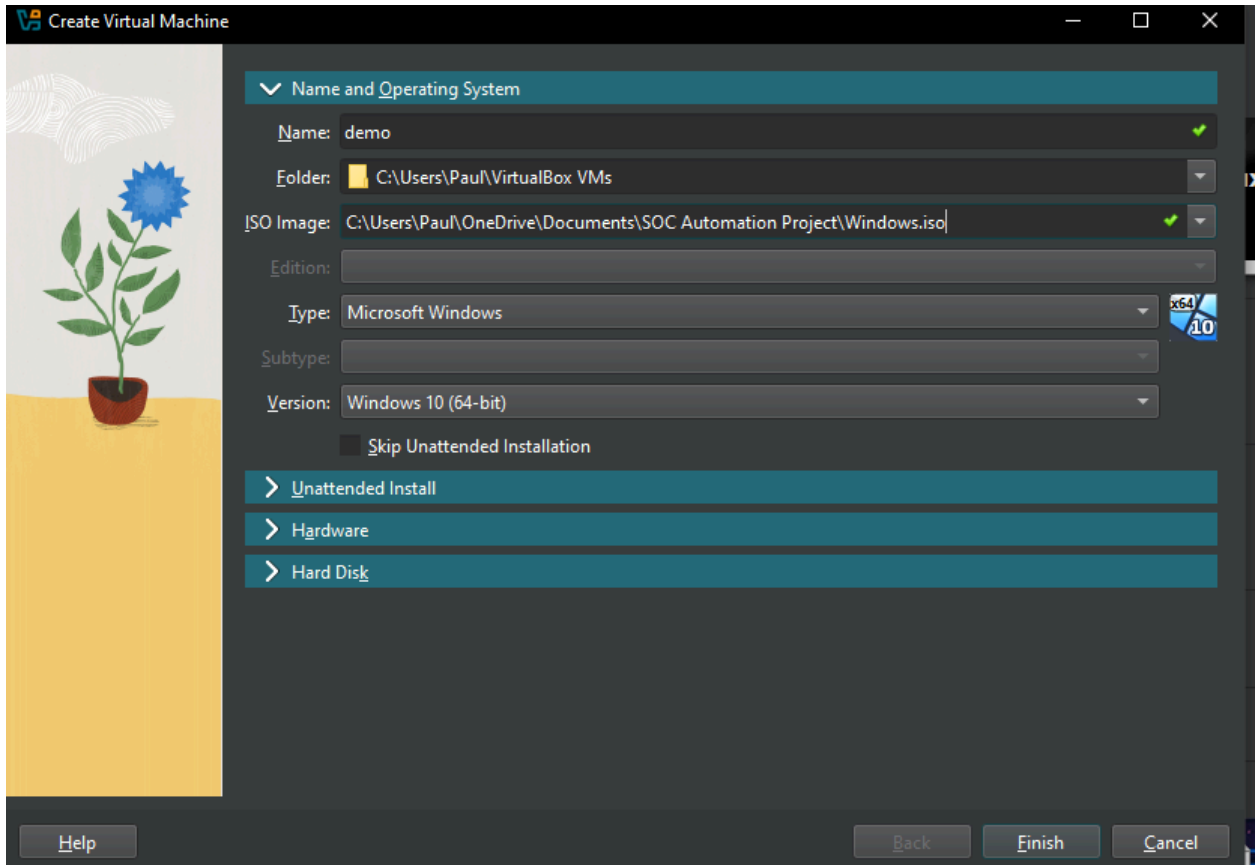
Initial Lab Design



Setting Up Infrastructure

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

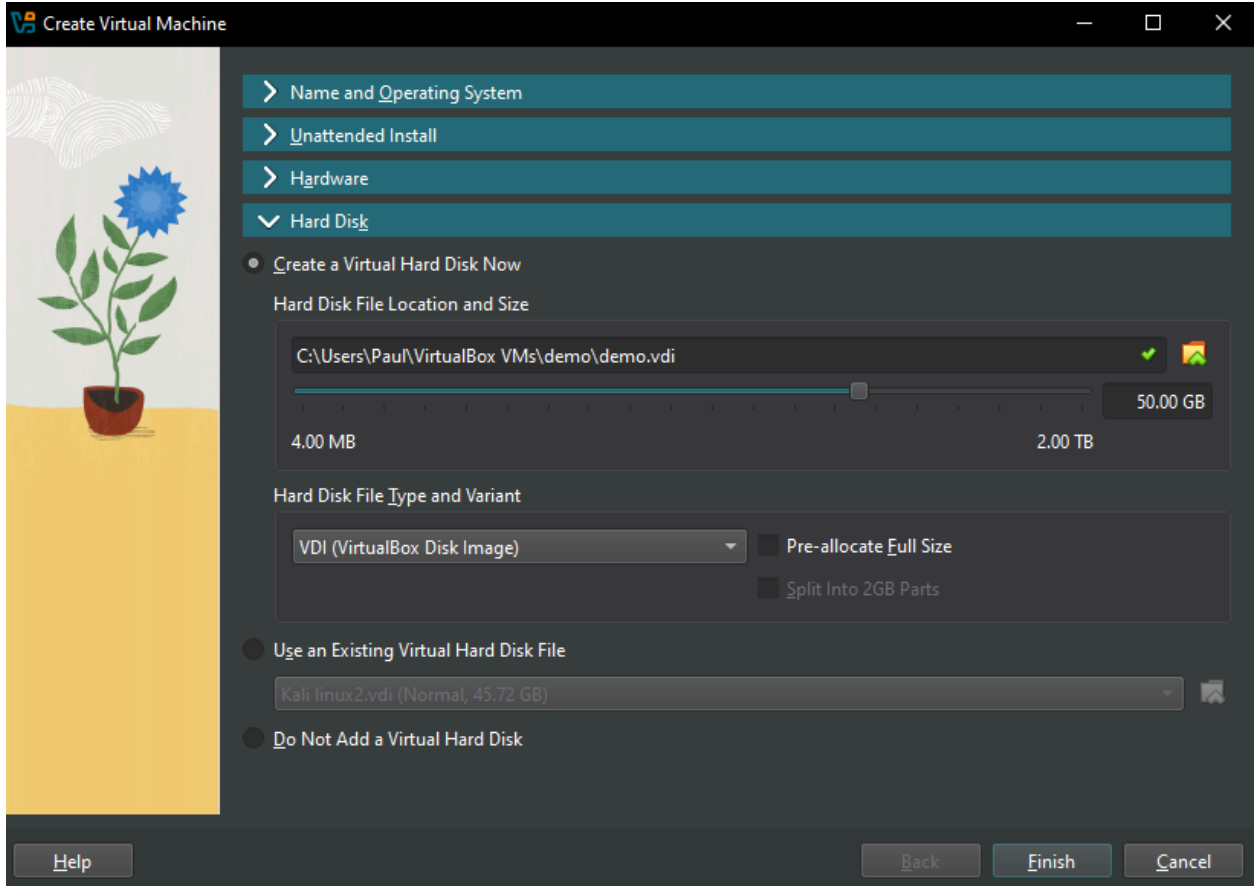
1 CPU 12 CPUs

Enable EFI (special OSes only)

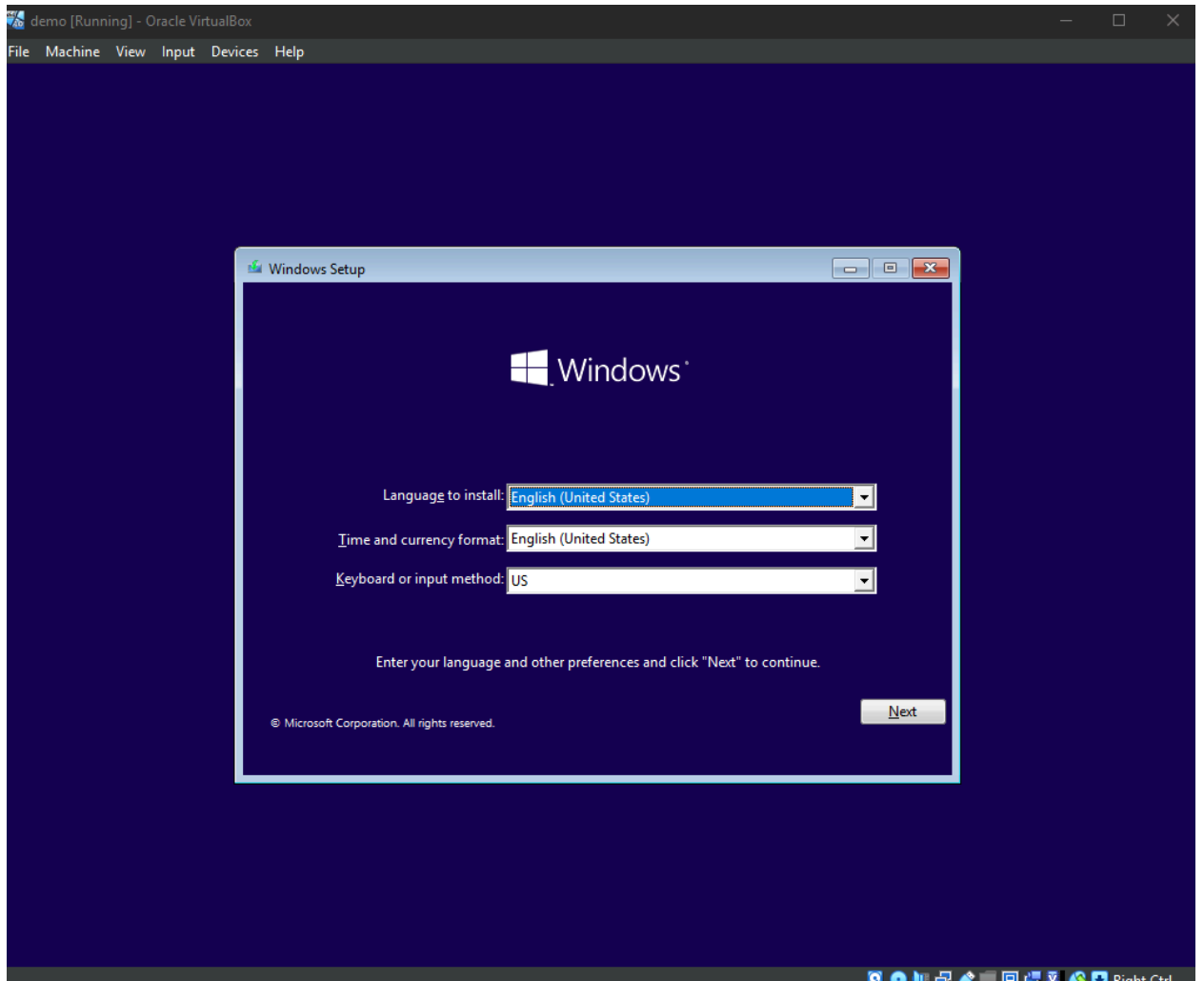
> Hard Disk

Help Back Finish Cancel





2. Click through installation



Installing Sysmon

1. <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>

Learn | Documentation | Training & Labs | Q&A | Topics | Sign in

Sysinternals | Downloads | Community | Resources

Find by title

- LogonSessions
- NewSID
- PsLoggedOn
- PsLogList
- RootkitRevealer
- Sysmon**
- > System Information
- > Miscellaneous
- Sysinternals Suite
- Microsoft Store
- Community
- > Resources
- Software License Terms
- Licensing FAQ

Download PDF

Learn / Sysinternals /

Sysmon v15.15

Summarize this article for me

In this article

- Introduction
- Overview of Sysmon Capabilities
- Screenshots
- Usage
- Show 5 more

By Mark Russinovich and Thomas Garnier

Published: July 23, 2024

[Download Sysmon \(4.6 MB\)](#)

[Download Sysmon for Linux \(GitHub\)](#)

Activate Windows
Go to Settings to activate Windows.

Type here to search | 4:07 AM 2/13/2026

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 Wazuh Server on Digital Ocean

Search by resource name or public IP (Ctrl+B) Create ? 🔔 🗨️ My Team Free Trial Active MT +

Create Droplets

Droplets are virtual machines that anyone can setup in seconds. You can use droplets, either standalone or as part of a Kubernetes cluster.

Choose Region

New York San Francisco

Singapore London

Toronto Bangalore

Atlanta

Datacenter

San Francisco - Datacenter 2 - SFO2

Tip: Select the datacenter closest to you or your users
Avoid any potential latency by selecting a region closest to you - a region is a geographic area where we have datacenters.

VPC Network - default-sfo2 DEFAULT

\$32.00/month
\$0.048/hour

[CREATE VIA COMMAND LINE](#) Create Droplet

- GPU Droplets
Create cloud servers with GPUs
- Droplets
Create cloud servers
- Agents
Create AI Agents
- Serverless Inference
Access AI Models
- Knowledge Bases
Create AI Knowledge Bases
- Kubernetes
Create Kubernetes clusters
- App Platform
Deploy your code
- Functions
Create Cloud Functions
- SaaS Add-Ons
Deploy Marketplace software
- Databases
Create database clusters
- Volumes Block Storage
Add storage to Droplets
- Spaces Object Storage
Store and serve static assets
- Network File Storage
Create NFS shares

1.

Choose an image

OS Marketplace (249) Custom images



Version

22.04 (LTS) x64

Choose Size

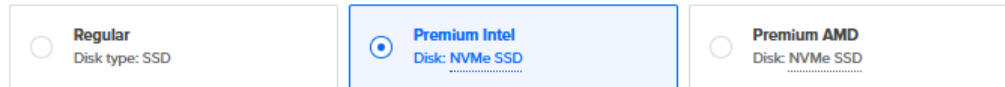
Need help picking a plan? [Help me choose](#)

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



\$8/mo \$0.012/hour	\$16/mo \$0.024/hour	\$24/mo \$0.036/hour	\$32/mo \$0.048/hour	\$48/mo \$0.071/hour	\$64/mo \$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

Create Firewall

Name

Name
Firewall

Inbound Rules

Set the Firewall rules for incoming traffic. Only the specified ports will accept inbound connections. All of

Type	Protocol	Port Range	Sources
All TCP	TCP	All ports	All IPv4 All IPv6
All UDP	UDP	All ports	All IPv4 All IPv6
New rule			

Outbound Rules

Set the Firewall rules for outbound traffic. Outbound traffic will only be allowed to the specified ports. All

Type	Protocol	Port Range	Destinations
ICMP	ICMP		All IPv4 All IPv6
All TCP	TCP	All ports	All IPv4 All IPv6

1.

← Back to Firewalls

Firewall updated successfully.

Firewall
5 Rules / 1 Droplet

Rules **Droplets** Destroy

Learn

Add Droplets

Name	IP Address	State	Added	
Wazuh 8 GB / 2 Intel vCPUs / 160 GB / NYC3	68.183.159.227	Updating...	Just now	More

2.

SSH Into Wazuh to Update and Upgrade

1.

```
root@Wazuh:~# apt-get update && apt-get upgrade
```
2.

```
root@Wazuh:~# curl -s0 https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```
3. Login into wazuh via webbrowser

Not secure https://68.183.159.227/app/login?

wazuh.
The Open Source Security Platform

admin

Log in

4.

The screenshot shows the Wazuh dashboard interface. At the top, there are statistics for agents: Total agents (0), Active agents (0), Disconnected agents (0), Pending agents (0), and Never connected agents (0). Below this is a yellow notification bar stating "No agents were added to this manager. Add agent". The main dashboard is divided into four quadrants:

- SECURITY INFORMATION MANAGEMENT:** Includes Security events (Browse through your security alerts, identifying issues and threats in your environment) and Integrity monitoring (Alerts related to file changes, including permissions, content ownership and attributes).
- AUDITING AND POLICY MONITORING:** Includes Policy monitoring (Verify that your systems are configured according to your security policies baseline), System auditing (Audit users behavior, monitoring command execution and alerting on access to critical files), and Security configuration assessment (Scan your assets as part of a configuration assessment audit).
- THREAT DETECTION AND RESPONSE:** Includes Vulnerabilities (Discover what applications in your environment are affected by well-known vulnerabilities) and MITRE ATT&CK (Security events from the knowledge base of adversary tactics and techniques based on real-world observations).
- REGULATORY COMPLIANCE:** Includes PCI DSS (Global security standard for entities that process, store or transmit payment cardholder data), NIST 800-53 (National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems), TSC (Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy), and GDPR (General Data Protection Regulation (GDPR) sets guidelines for processing of personal data).

Install TheHive

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

The screenshot shows the DigitalOcean Firewall console. The Firewall is named "Firewall" and has 5 Rules and 2 Droplets. The Droplets tab is selected, showing a table of droplets:

Name	IP Address	State	Added
Wazuh 8 GB / 2 Intel vCPUs / 160 GB / NYC3	68.183.159.227	Up-to-date	25 minutes ago
TheHive 8 GB / 2 Intel vCPUs / 160 GB / NYC3	138.197.101.50	Up-to-date	Just now

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/corretto.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 gpg
--dearmor -o /usr/share/keyrings/cassandra-archive.gpg
echo "deb [signed-by=/usr/share/keyrings/cassandra-archive.gpg] https://debian.cassandra.apache.org 40x main" | sudo tee -a /etc/apt/sources.list.d/cassandra.sources.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://artifacts.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 | sudo 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/strangebee.list
sudo apt-get update
sudo apt-get install -y thehive

```

Configuring Machines to Work Together

Configure TheHive

```

root@TheHive:~# nano /etc/cassandra/cassandra.yaml

```

1.

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

```

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:~#

```

2.

Next, we configure Elastic Search

```
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:~# █
```

1.

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

The screenshot shows the 'Organisation List' page in TheHive. The top navigation bar includes the TheHive logo, a search icon, the text 'Organisation List', a document icon, the language 'ENGLISH (UK)', and the user 'DEFAULT ADMIN USER'. Below the navigation bar, there are buttons for '+', 'default', and 'Export list', along with a toggle switch. The main content area is a table with the following data:

<input type="checkbox"/>	NAME	CREATED BY	CREATED DATE
<input type="checkbox"/>	<div style="display: flex; align-items: center;"> <div style="margin-right: 5px;">Active</div> <div style="display: flex; align-items: center;"> <div style="border: 1px solid gray; border-radius: 50%; width: 20px; height: 20px; display: flex; align-items: center; justify-content: center; margin-right: 5px;">A</div> <div> <p>admin</p> <p>Linked organisations: None</p> </div> </div> </div>	TheHive system user	13/02/2026 06:32

At the bottom of the page, there is a pagination bar with the following elements: '< Previous', '0 - 1 of 1', 'Next >', 'Show', and a dropdown menu set to '30'.

Wazuh Configuration

Click on Add agent

The screenshot displays the Wazuh dashboard interface. At the top, there are five statistics: Total agents (0), Active agents (0), Disconnected agents (0), Pending agents (0), and Never connected agents (0). Below this is a yellow banner with a warning icon and the text "No agents were added to this manager. Add agent". The main content is divided into four sections: SECURITY INFORMATION MANAGEMENT, AUDITING AND POLICY MONITORING, THREAT DETECTION AND RESPONSE, and REGULATORY COMPLIANCE. The SECURITY INFORMATION MANAGEMENT section includes Security events and Integrity monitoring. The AUDITING AND POLICY MONITORING section includes Policy monitoring and System auditing. The THREAT DETECTION AND RESPONSE section is currently empty. The REGULATORY COMPLIANCE section includes Security configuration assessment.

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

```
PS C:\Users\SOCAD> cd ..
PS C:\Users> cd ..
PS C:\> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -OutFile ${env:tmp}\wazuh-agent; msixec.exe /i ${env:tmp}\wazuh-agent /q WAZUH_MANAGER='68.183.159.227' WAZUH_AGENT_NAME='mydfir' WAZUH_REGISTRATION_SERVER='68.183.159.227'
PS C:\>
```