IBM ProjectReport

On

Develop an application to facilitate IPR filing for the grassroots community

Developed By:

Rishabh Patel (19162171034)
Sahil Patel (20162172004)
Smit Patel (19162121031)

Guided By:

Prof. Umesh Lakhtariya (Internal)
Mr. Anoj Dixit (External guide)

Submitted to

Department of Computer Science & Engineering
Institute of Computer Technology

Ganpat University
॥ विद्यया समाजोत्कर्षः ॥
Institute of Computer Technology

Year: 2023

Ganpat University
॥ विद्यया समाजोत्कर्षः ॥
Institute of Computer Technology

CERTIFICATE

This is to certify that the **IBM** Project work entitled "Develop an application to facilitate IPR filing for the grassroots community" by Rishabh Patel (Enrolment No.19162171034), Sahil Patel (Enrolment No.20162172007) and Smit Patel (EnrolmentNo.19162121031) of Ganpat University, towards the partial fulfillment of requirements of the degree of Bachelor of Technology – Computer Science and Engineering, carried out by them in the CSE(CS/BDA) Department at Elegant Microweb Pvt. Ltd. The results/findings contained in this Project have not been submitted in part or full to any other University / Institute for awardof any other Degree.

Name & Signature of Internal Guide

Name & Signature of Head

Place: ICT - GUNI

Date:

ACKNOWLEDGEMENT

IBM Internship project is a golden opportunity for learning and self-development. I considermyself very lucky and honored to have so many wonderful people lead me through in completion of this project. First and foremost, I would like to thank Dr. Hemal Shah, Principal, ICT, and Prof. Dharmesh Darji, Head, ICT who gave us an opportunity to undertake this project. My grateful thanksto Prof. Umesh Lakhtariya & Mr. Anoj Dixit (Internal & External Guides) for their guidance in project work Develop an application to facilitate IPR filing for the grassroots community, who despite being extraordinarily busy with academics, took time out to hear, guide and keep us on the correct path. We do not know where would have been without his/her help. CSE department monitored our progress and arranged all facilities to make life easier. We choose this moment to acknowledge their contribution gratefully.

Rishabh Patel (Enrollment No:19162171034)
Sahil Patel (Enrollment No: 20162172007)
Smit Patel (Enrollment No:19162121031)

ABSTRACT

The development of an application to facilitate IPR filing for the grassroots community aims to address the challenges faced by individuals and small organizations in navigating the complex and often costly process of obtaining intellectual property rights. By providing a user-friendly platform with step-by-step guides, document templates, and the ability to submit applications electronically, the application aims to make the IPR filing process more accessible and efficient for those with limited resources. Additionally, the application would provide information and resources on different types of IPR, such as patents, trademarks, and copyrights, to assist users in understanding the process and making informed decisions. Overall, the application aims to empower the grassroots community to protect their intellectual property and support their growth and development.

INDEX

CHAPTER: 1 INTRODUCTION

CHAPTER 1 INTRODUCTION

An application to facilitate IPR filing for the grassroots community would likely be a software tool or platform that makes it easier for individuals or small organizations with limited resources to file for intellectual property rights. This could include features such as step-by-step guides, document templates, and the ability to submit applications electronically. The application could also provide resources and information on different types of IPR, such as patents, trademarks, and copyrights. The goal of such an application would be to make the IPR filing process more accessible and user-friendly for those who may not have the knowledge or resources to navigate the process on their own.

CHAPTER: 2 PROJECT SCOPE

CHAPTER 2 PROJECT SCOPE

The scope of a project to develop an application to facilitate IPR filing for the grassroots community would include the following:

Research and analysis: This would involve researching the current IPR filing process, identifying the challenges faced by the grassroots community, and determining the features and functionality that would be most useful in addressing these challenges.

Design and development: This would involve creating the user interface and features of the application, such as step-by-step guides, document templates, and the ability to submit applications electronically.

CHAPTER: 3 SOFTWARE AND HARDWARE REQUIREMENTS

Minimum Hardware Requirements

Processor	2.0 GHz
RAM	4GB
HDD	40GB

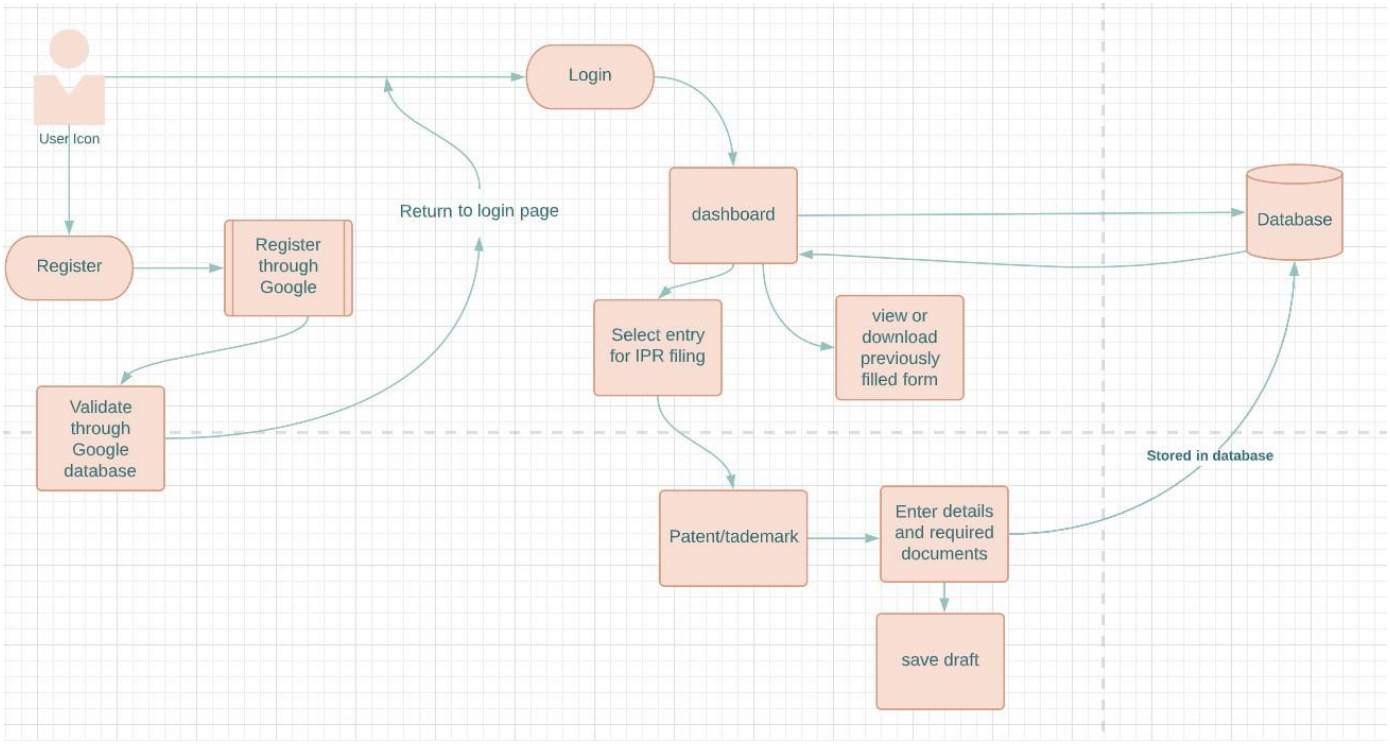
Table 3.1 Minimum Hardware Requirements

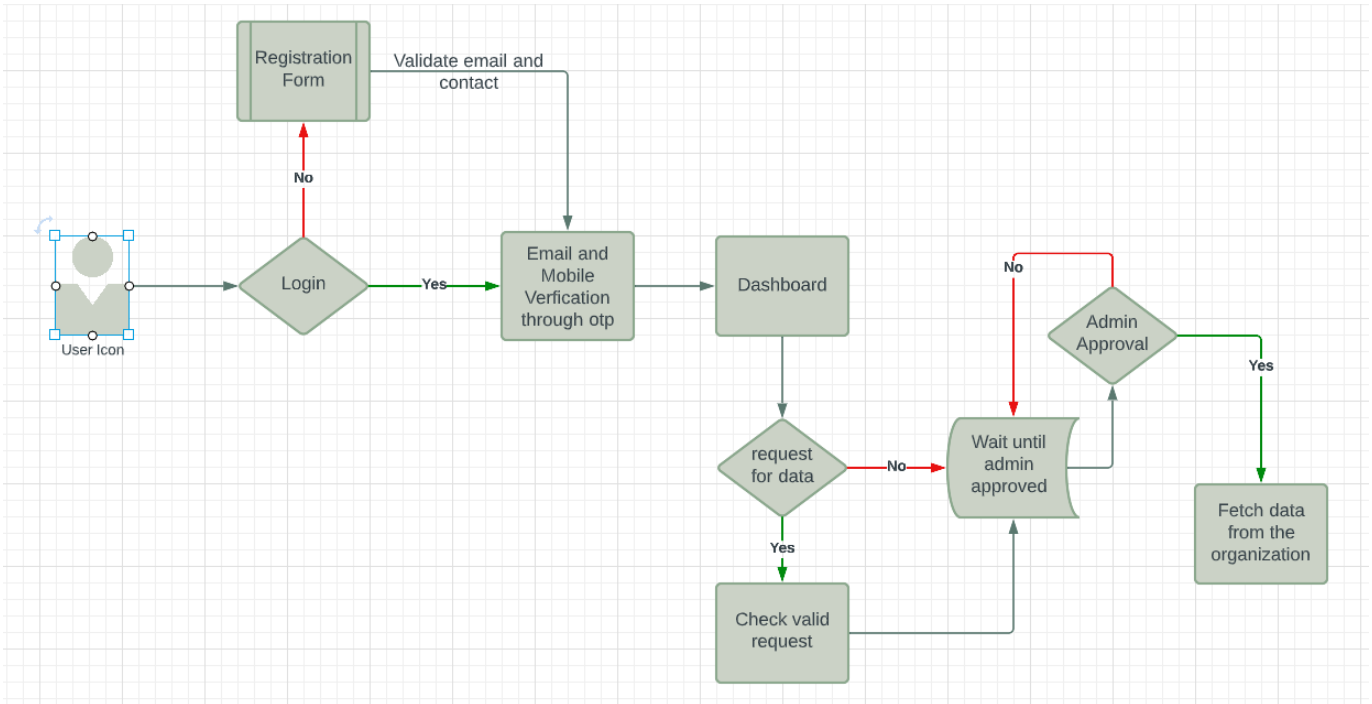
Minimum Software Requirements

Operating System	Any operating system which can support an internet browser.
Programming language	-
Other tools & tech	Internet browser

Table 3.2 Minimum Software Requirements

CHAPTER: 4 PROCESS MODEL


User Icon
Login
Return to login page
dashboard
Database
Register
Register through Google
Select entry for IPR filing
view or download previously filled form
Validate through Google database
Stored in database
Patent/tademark
Enter details and required documents
save draft


Registration Form
Validate email and contact
No
User Icon
Login
Yes
Email and Mobile Verfication through otp
Dashboard
No
Admin Approval
Yes
request for data
No
Wait until admin approved
Fetch data from the organization
Yes
Check valid request

CHAPTER: 5 PROJECT PLAN

CHAPTER 5 PROJECT PLAN

A project plan for developing an application to facilitate IPR filing for the grassroots community could include the following steps:

Kick-off meeting: Hold a meeting with the project team to discuss the project scope, goals, and timelines.

Research and analysis: Conduct research on the current IPR filing process and identify the challenges faced by the grassroots community. Determine the features and functionality that would be most useful in addressing these challenges.

Design and development: Create the user interface and features of the application, such as step-by-step guides, document templates, and the ability to submit applications electronically.

Testing and quality assurance: Test the application to ensure it is user-friendly and functions as intended, and make any necessary adjustments before launch.

Deployment and maintenance: Deploy the application and provide ongoing maintenance and support to ensure it continues to function effectively.

Training: Provide training to end-users on how to use the application and navigate the IPR filing process.

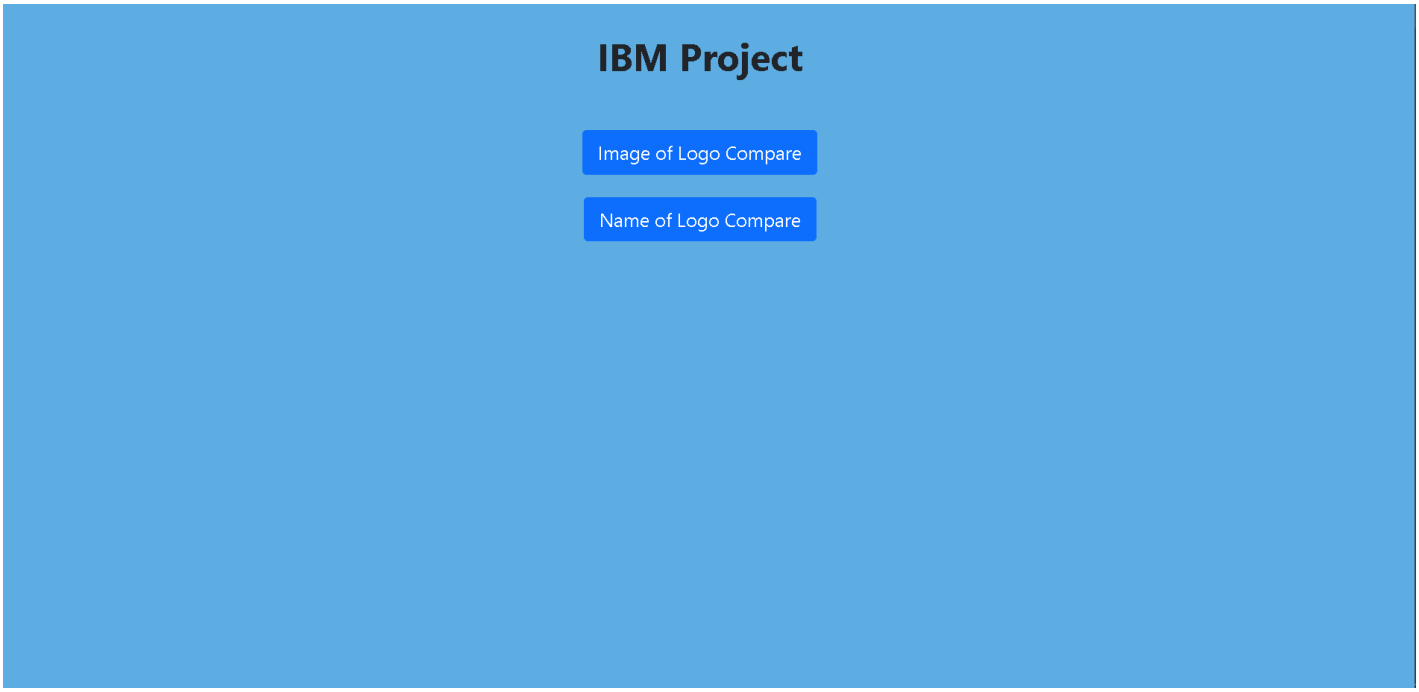
Monitoring and evaluation: Monitor the usage of the application and gather feedback from the end-users to evaluate the effectiveness of the application and identify areas for improvement.

Close project: Close the project and document the lessons learned.

It is important to establish clear milestones and deadlines for each step, and to regularly review the progress of the project to ensure it stays on track. Also, this plan should be flexible enough to accommodate any changes or unforeseen challenges that may arise during the course of the project.

CHAPTER: 6 IMPLEMENTATION DETAILS

CHAPTER 6 IMPLEMENTATION DETAIL



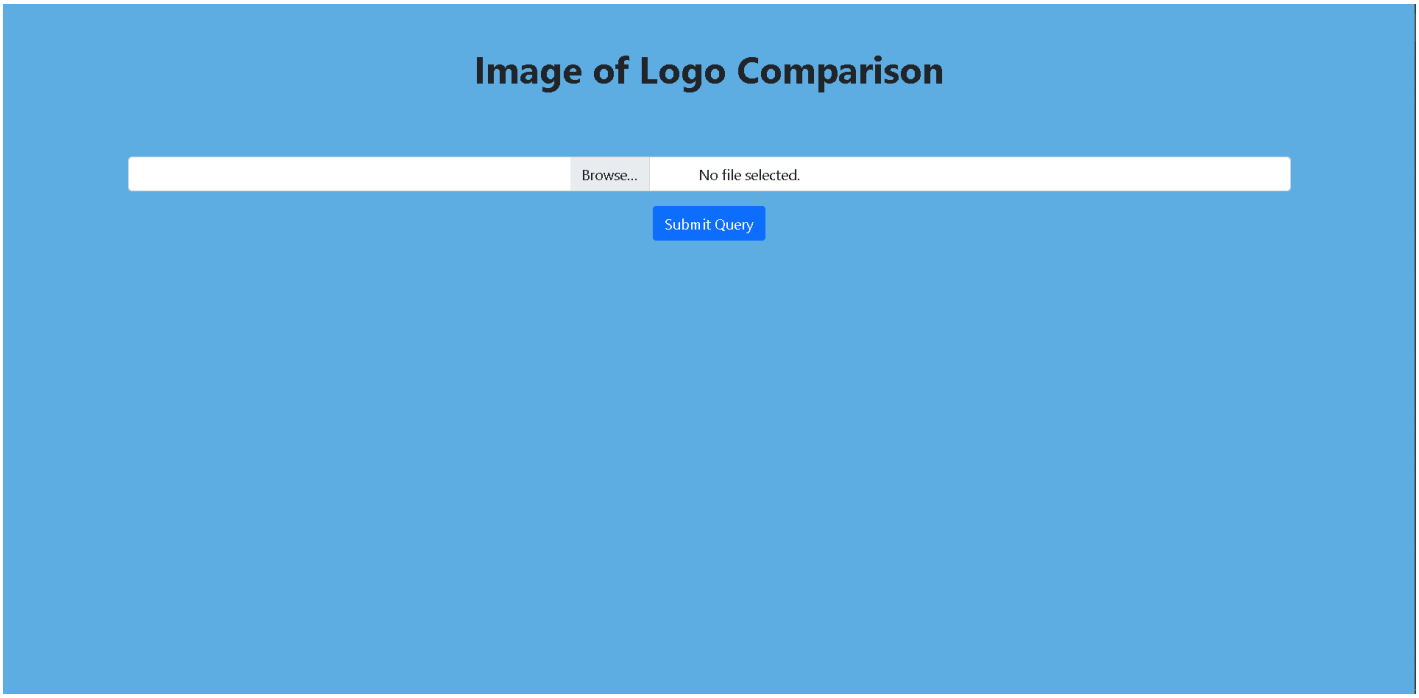
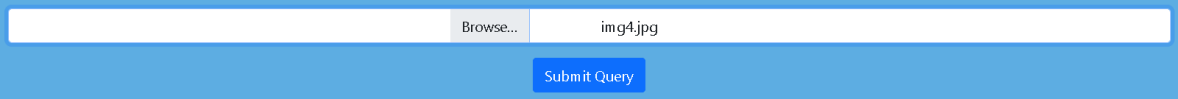


Image of Logo Comparison



Submit Query

Result

This logo Image is already Patent, Please choose another logo!!!


Logo of Name Compare
Enter a Logo Name :
YOUTUBE
Submit Query

Result

This name already Patent : YOUTUBEplease choose another name!!!

Logo of Name Compare

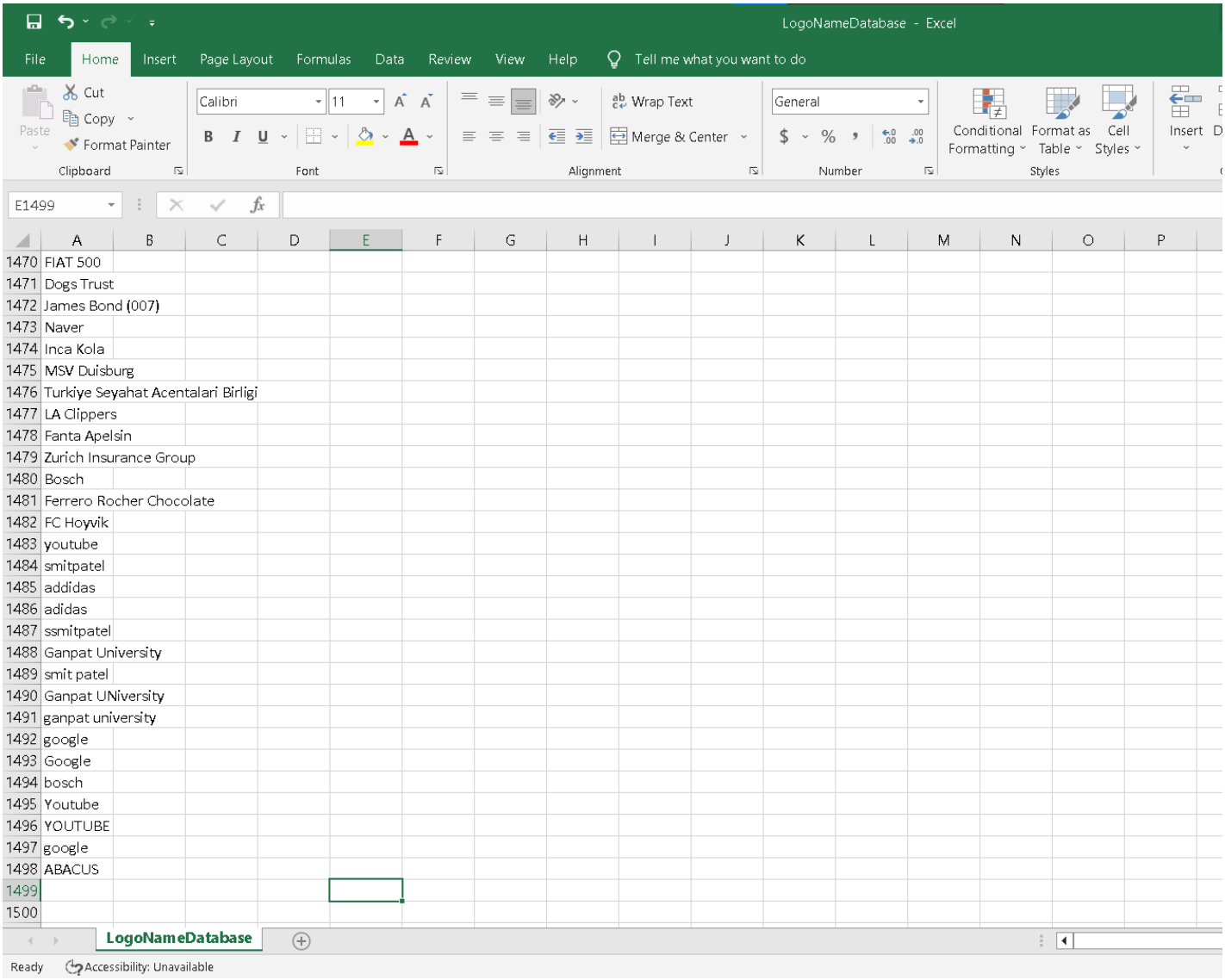
Enter a Logo Name :

ABACUS

Submit Query

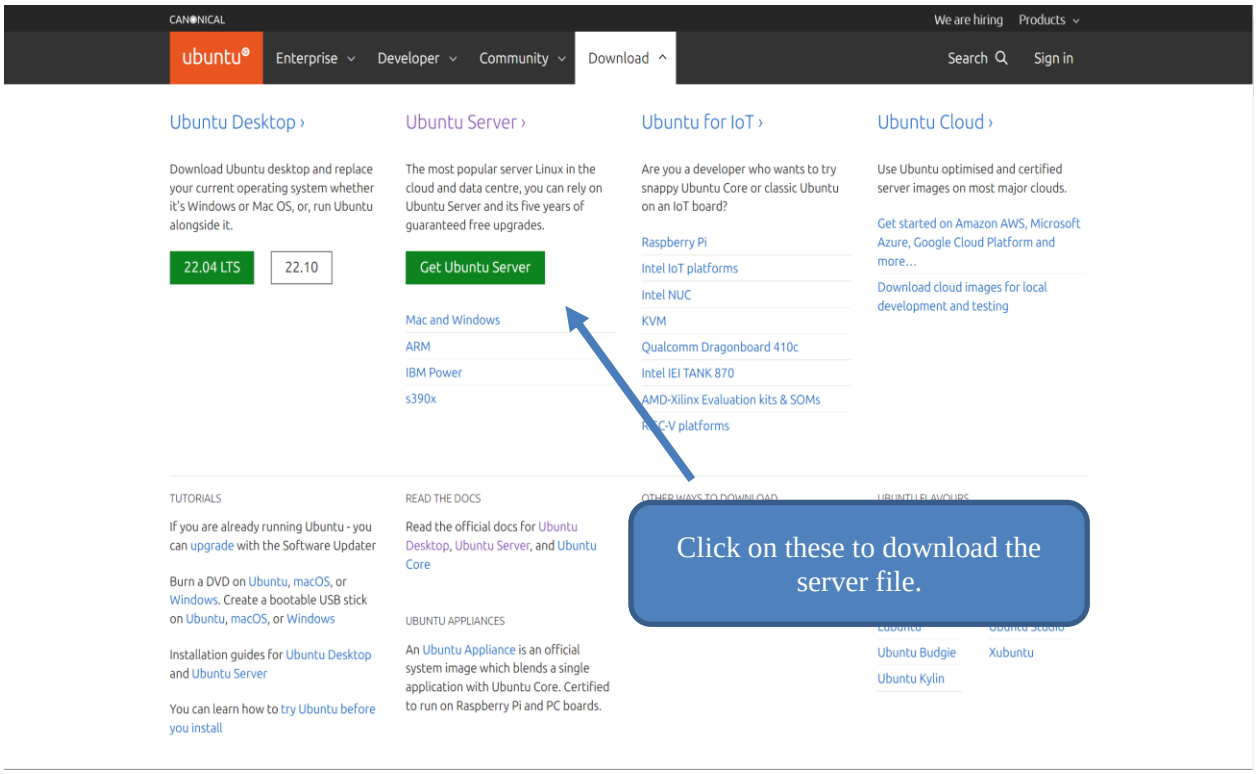
Result

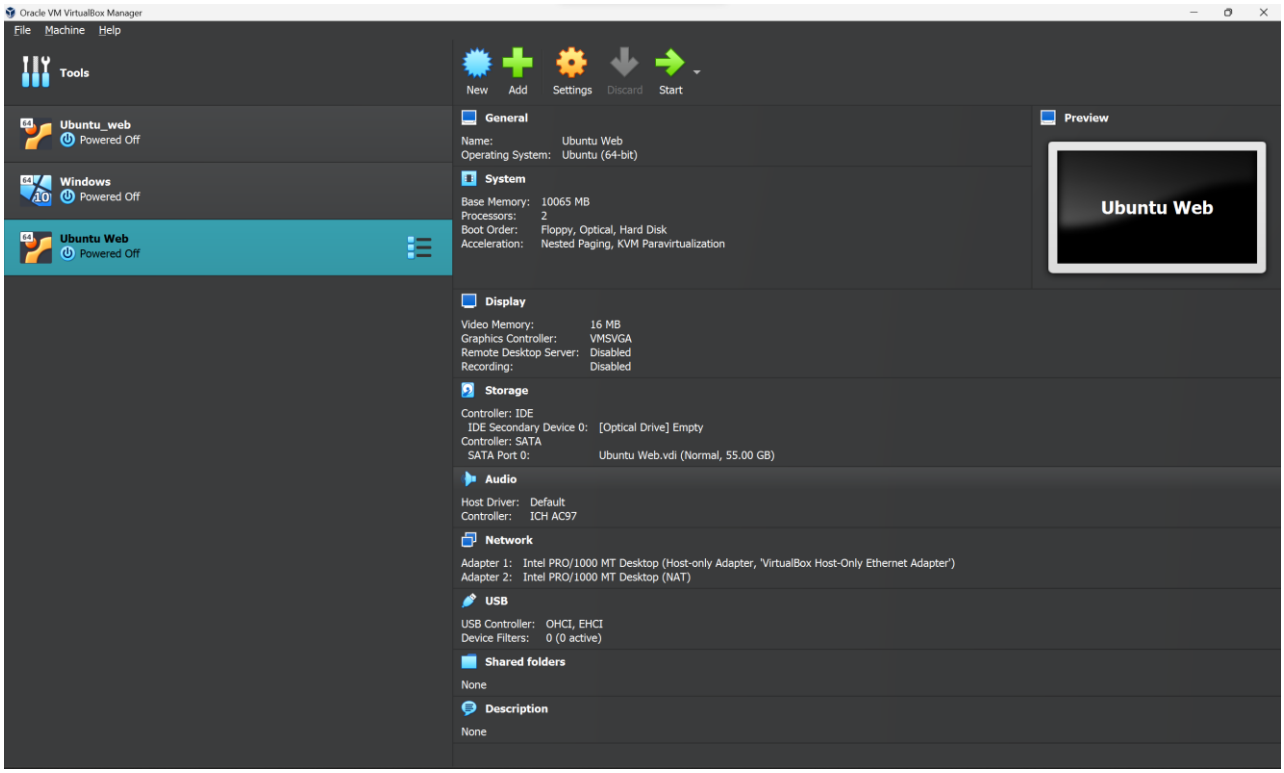
This name is unique : ABACUSnow saved in our database.

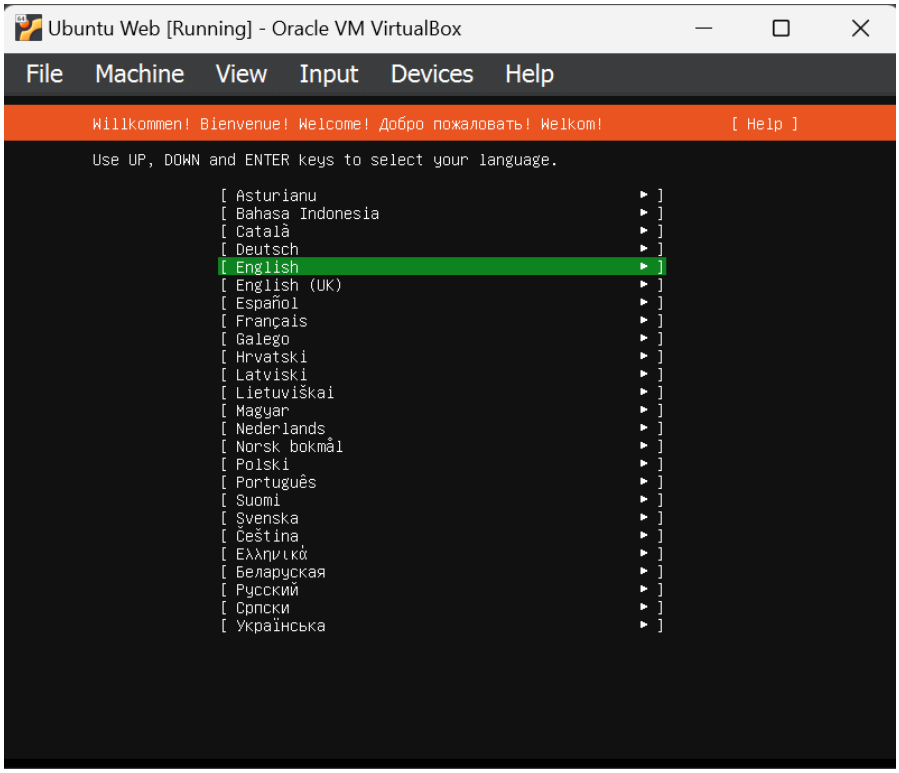


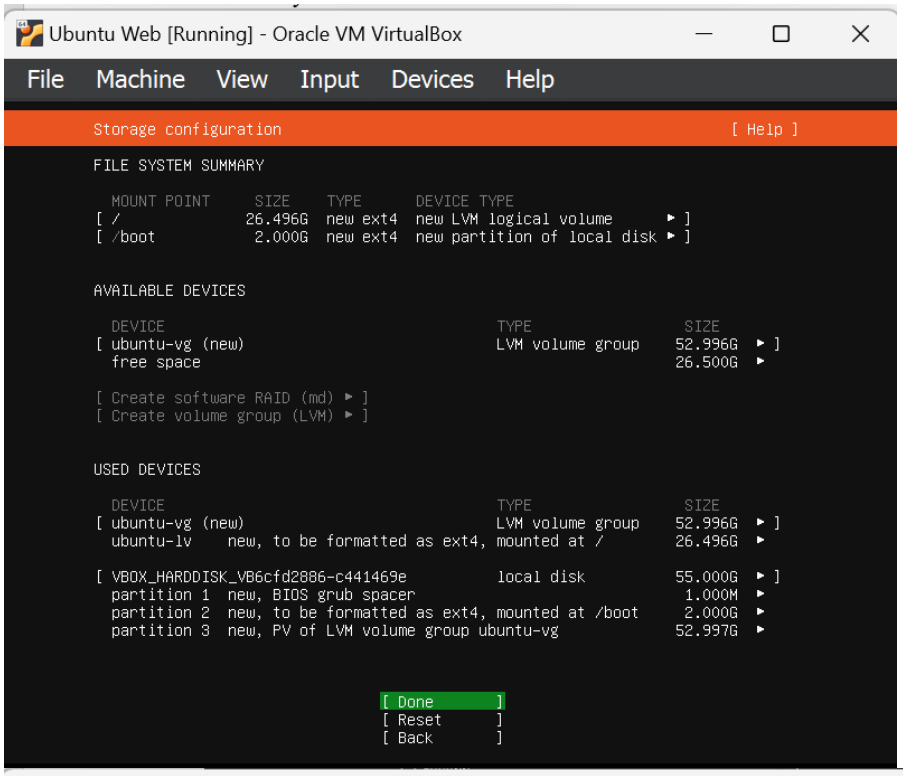
4.1. Ubuntu server installation.

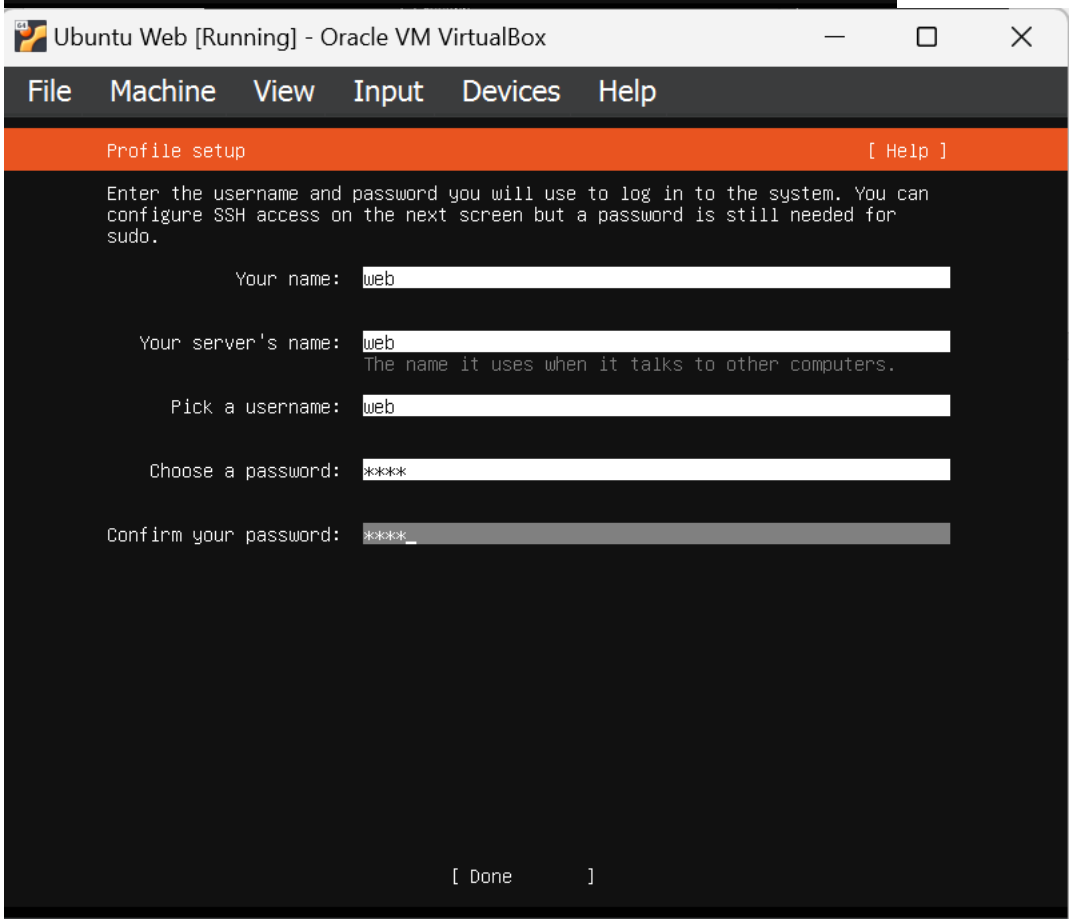
Move to Ubuntu official web side and download the server file form the download tab.

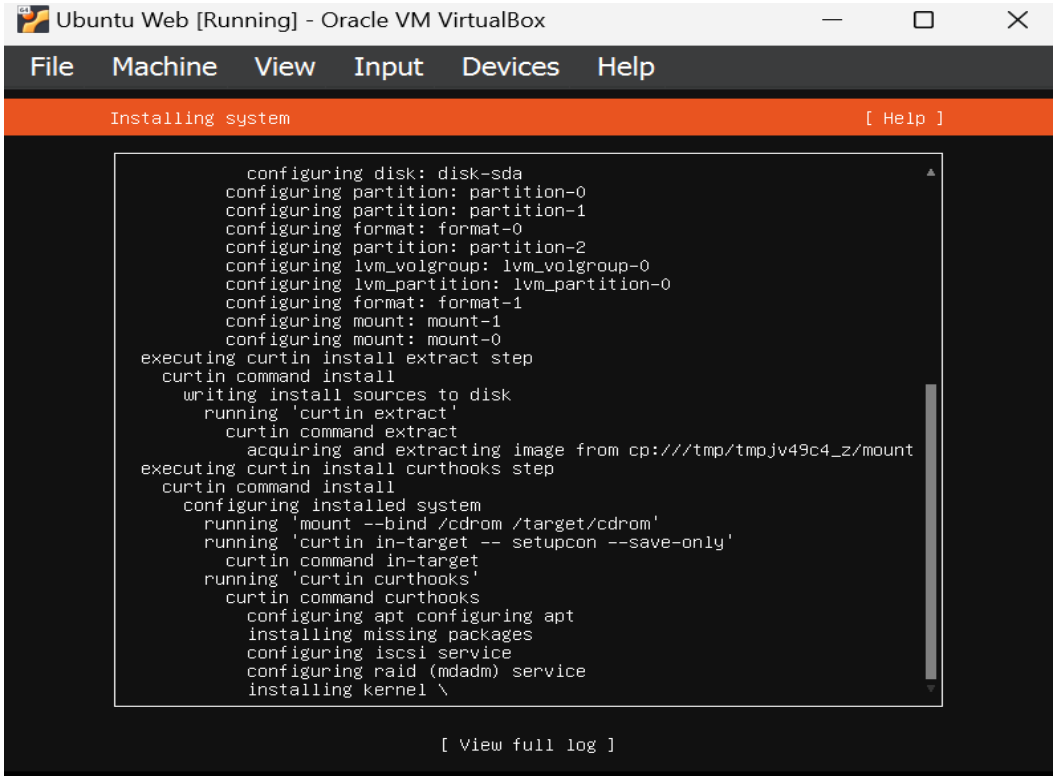

CANONICAL
We are hiring
Products
ubuntu
Enterprise
Developer
Community
Download
Search
Sign in
Ubuntu Desktop ›
Download Ubuntu desktop and replace your current operating system whether it's Windows or Mac OS, or, run Ubuntu alongside it.
22.04 LTS
22.10
Ubuntu Server ›
The most popular server Linux in the cloud and data centre, you can rely on Ubuntu Server and its five years of guaranteed free upgrades.
Get Ubuntu Server
Mac and Windows
ARM
IBM Power
s390x
Ubuntu for IoT ›
Are you a developer who wants to try snappy Ubuntu Core or classic Ubuntu on an IoT board?
Raspberry Pi
Intel IoT platforms
Intel NUC
KVM
Qualcomm Dragonboard 410c
Intel IEI TANK 870
AMD-Xilinx Evaluation kits & SOMs
Ubuntu Cloud ›
Use Ubuntu optimised and certified server images on most major clouds.
Get started on Amazon AWS, Microsoft Azure, Google Cloud Platform and more…
Download cloud images for local development and testing
TUTORIALS
If you are already running Ubuntu - you can upgrade with the Software Updater
Burn a DVD on Ubuntu, macOS, or Windows. Create a bootable USB stick on Ubuntu, macOS, or Windows
Installation guides for Ubuntu Desktop and Ubuntu Server
You can learn how to try Ubuntu before you install
READ THE DOCS
Read the official docs for Ubuntu Desktop, Ubuntu Server, and Ubuntu Core
UBUNTU APPLIANCES
An Ubuntu Appliance is an official system image which blends a single application with Ubuntu Core. Certified to run on Raspberry Pi and PC boards.
Ubuntu Budgie
Xubuntu
Ubuntu Kylin
Click on these to download the server file.


Oracle VM VirtualBox Manager
File Machine Help
Tools
Ubuntu_web
Powered Off
Windows
Powered Off
Ubuntu Web
Powered Off
New Add Settings Discard Start
General
Name: Ubuntu Web
Operating System: Ubuntu (64-bit)
System
Base Memory: 10065 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization
Preview
Ubuntu Web
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Ubuntu Web.vdi (Normal, 55.00 GB)
Audio
Host Driver: Default
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter')
Adapter 2: Intel PRO/1000 MT Desktop (NAT)
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)
Shared folders
None
Description
None


Ubuntu Web [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Willkommen! Bienvenue! Welcome! Добро пожаловать! Welkom! [Help]
Use UP, DOWN and ENTER keys to select your language.
[Asturianu]
[Bahasa Indonesia]
[Català]
[Deutsch]
[English]
[English (UK)]
[Español]
[Français]
[Galego]
[Hrvatski]
[Latviski]
[Lietuviškai]
[Magyar]
[Nederlands]
[Norsk bokmål]
[Polski]
[Português]
[Suomi]
[Svenska]
[Čeština]
[Ελληνικά]
[Беларуская]
[Русский]
[Српски]
[Українська]

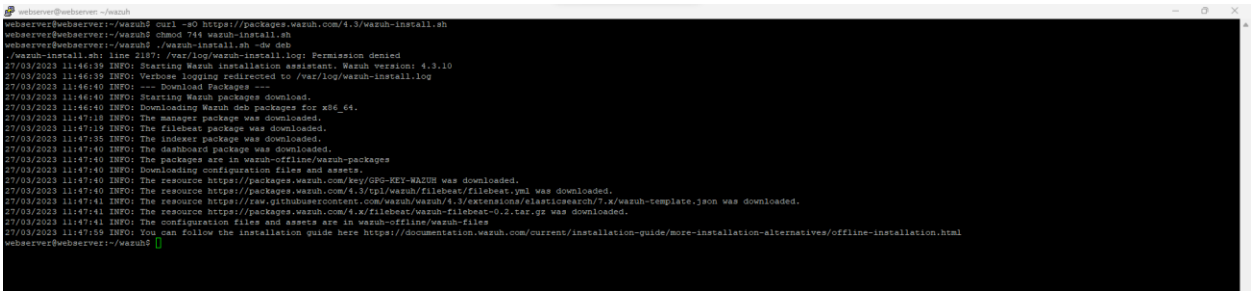

Ubuntu Web [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Storage configuration [Help]
FILE SYSTEM SUMMARY
MOUNT POINT SIZE TYPE DEVICE TYPE
[/ 26.496G new ext4 new LVM logical volume ▸]
[/boot 2.000G new ext4 new partition of local disk ▸]
AVAILABLE DEVICES
DEVICE TYPE SIZE
[ubuntu-vg (new) LVM volume group 52.996G ▸]
free space 26.500G ▸
[Create software RAID (md) ▸]
[Create volume group (LVM) ▸]
USED DEVICES
DEVICE TYPE SIZE
[ubuntu-vg (new) LVM volume group 52.996G ▸]
ubuntu-lv new, to be formatted as ext4, mounted at / 26.496G ▸
[VBOX_HARDDISK_VB6cfd2886-c441469e local disk 55.000G ▸]
partition 1 new, BIOS grub spacer 1.000M ▸
partition 2 new, to be formatted as ext4, mounted at /boot 2.000G ▸
partition 3 new, PV of LVM volume group ubuntu-vg 52.997G ▸
[Done]
[Reset]
[Back]


Ubuntu Web [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Profile setup [Help]
Enter the username and password you will use to log in to the system. You can configure SSH access on the next screen but a password is still needed for sudo.
Your name: web
Your server's name: web
The name it uses when it talks to other computers.
Pick a username: web
Choose a password: ****
Confirm your password: ****
[Done]

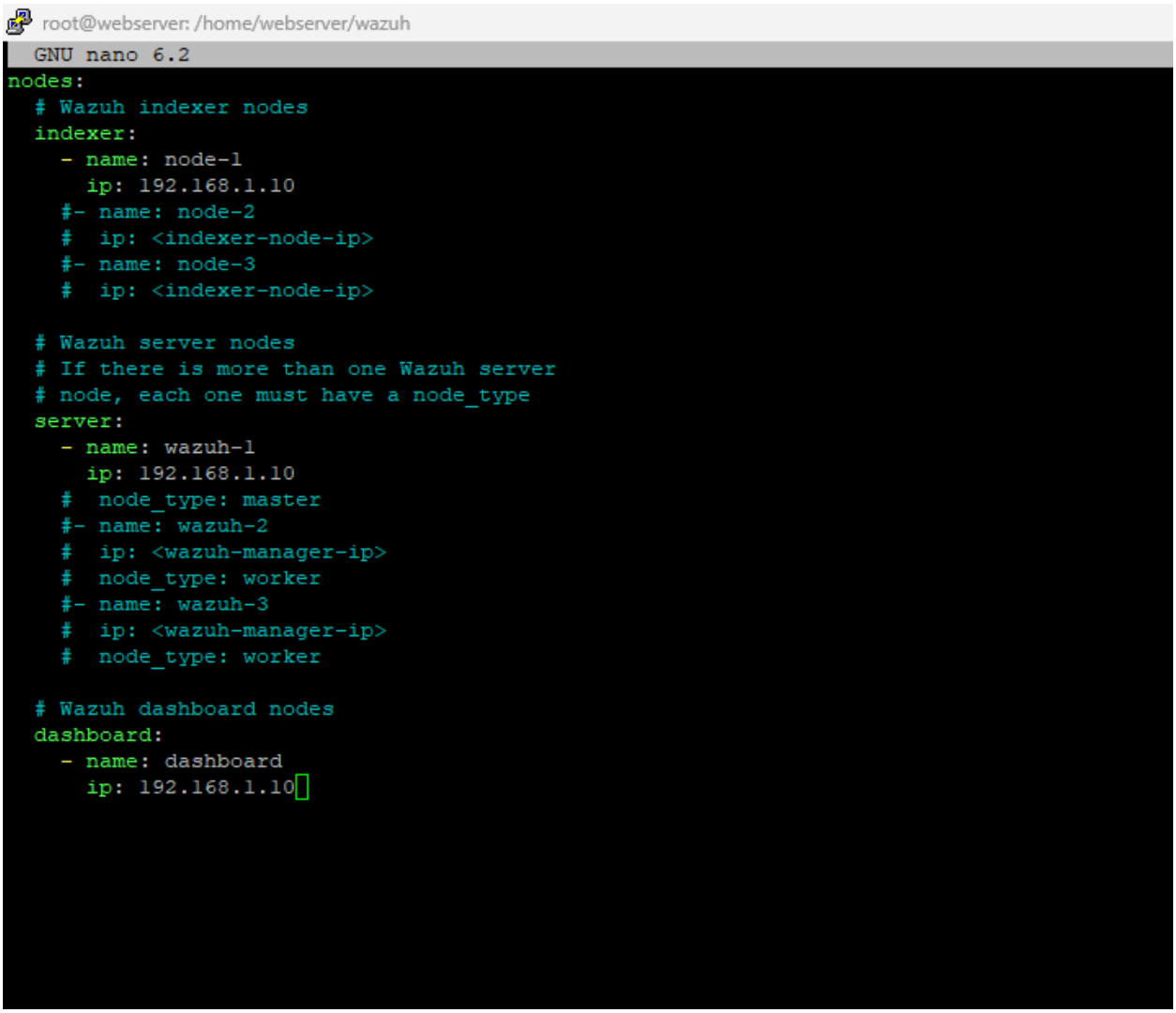



```
webserver@webserver:~$ mkdir wazuh
webserver@webserver:~$ mkdir backup
```

```
webserver@webserver:~/wazuh$ curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh
webserver@webserver:~/wazuh$
```




```
webserver@webserver:~/wazuh$ curl -sO https://packages.wazuh.com/4.3/config.yml
webserver@webserver:~/wazuh$ ls
config.yml  wazuh-install.sh  wazuh-offline.tar.gz
webserver@webserver:~/wazuh$
```


root@webserver: /home/webserver/wazuh
GNU nano 6.2
nodes:
Wazuh indexer nodes
indexer:
- name: node-1
ip: 192.168.1.10
#- name: node-2
ip: <indexer-node-ip>
#- name: node-3
ip: <indexer-node-ip>
Wazuh server nodes
If there is more than one Wazuh server
node, each one must have a node_type
server:
- name: wazuh-1
ip: 192.168.1.10
node_type: master
#- name: wazuh-2
ip: <wazuh-manager-ip>
node_type: worker
#- name: wazuh-3
ip: <wazuh-manager-ip>
node_type: worker
Wazuh dashboard nodes
dashboard:
- name: dashboard
ip: 192.168.1.10

```
root@webserver:/home/webserver/wazuh# cat config.yml
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: 192.168.1.10
    #- name: node-2
    #  ip: <indexer-node-ip>
    #- name: node-3
    #  ip: <indexer-node-ip>

  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh-1
      ip: 192.168.1.10
    #  node_type: master
    #- name: wazuh-2
    #  ip: <wazuh-manager-ip>
    #  node_type: worker
    #- name: wazuh-3
    #  ip: <wazuh-manager-ip>
    #  node_type: worker

  # Wazuh dashboard nodes
  dashboard:
    - name: dashboard
      ip: 192.168.1.10
```

```
root@webserver:/home/webserver/wazuh# ls
config.yml  wazuh-certificates  wazuh-certs-tool.sh  wazuh-install.sh  wazuh-offline.tar.gz
root@webserver:/home/webserver/wazuh#
```

```
root@webserver:/home/webserver/wazuh# scp -r wazuh-offline.tar.gz webserver@192.168.1.10:/home/webserver/
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be established.
ED25519 key fingerprint is SHA256:owokQm7byYnDOetXTkw81OoKZcLkoLP+RNNtjoqMYyS.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.10' (ED25519) to the list of known hosts.
webserver@192.168.1.10's password:
wazuh-offline.tar.gz                                                                                    100%  599MB 384.7MB/s   00:01
root@webserver:/home/webserver/wazuh# scp -r wazuh-certificates webserver@192.168.1.10:/home/webserver/
webserver@192.168.1.10's password:
root-ca.pem                                                                                             100% 1204     1.3MB/s   00:00
wazuh-1.pem                                                                                             100% 1277     1.4MB/s   00:00
dashboard-key.pem                                                                                       100% 1704     1.5MB/s   00:00
node-1-key.pem                                                                                          100% 1700     1.8MB/s   00:00
admin-key.pem                                                                                           100% 1704     2.5MB/s   00:00
root-ca.key                                                                                             100% 1704     2.3MB/s   00:00
wazuh-1-key.pem                                                                                         100% 1704     1.5MB/s   00:00
node-1.pem                                                                                              100% 1277     1.8MB/s   00:00
admin.pem                                                                                               100% 1119   764.6KB/s   00:00
dashboard.pem                                                                                           100% 1281     1.9MB/s   00:00
root@webserver:/home/webserver/wazuh#
```

```
webserver@webserver:~$ ls
backup  wazuh  wazuh-certificates  wazuh-offline.tar.gz
webserver@webserver:~$ sudo su
[sudo] password for webserver:
root@webserver:/home/webserver# mv wazuh-certificates /home/webserver/backup/
root@webserver:/home/webserver# ls
backup  wazuh  wazuh-offline.tar.gz
root@webserver:/home/webserver# mv wazuh-offline.tar.gz /home/webserver/backup/
root@webserver:/home/webserver# ls
backup  wazuh
root@webserver:/home/webserver# _
```

```
root@webserver:/home/webserver# cd backup/
root@webserver:/home/webserver/backup# ls
wazuh-certificates  wazuh-offline.tar.gz
root@webserver:/home/webserver/backup# ls -l
total 613844
drwxr--r-- 2 webserver webserver      4096 Mar 27 12:00 wazuh-certificates
-rw------- 1 webserver webserver 628567785 Mar 27 11:59 wazuh-offline.tar.gz
root@webserver:/home/webserver/backup#
```

```
root@webserver:/home/webserver/wazuh# tar xf wazuh-offline.tar.gz
root@webserver:/home/webserver/wazuh#
```

root@webserver: /home/webserver/wazuh

```
root@webserver:/home/webserver/wazuh# dpkg -i ./wazuh-offline/wazuh-packages/wazuh-indexer*.deb
Selecting previously unselected package wazuh-indexer.
(Reading database ... 73929 files and directories currently installed.)
Preparing to unpack .../wazuh-indexer_4.3.10-1_amd64.deb ...
Creating wazuh-indexer group... OK
Creating wazuh-indexer user... OK
Unpacking wazuh-indexer (4.3.10-1) ...
Setting up wazuh-indexer (4.3.10-1) ...
Created opensearch keystore in /etc/wazuh-indexer/opensearch.keystore
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
root@webserver:/home/webserver/wazuh#
```

```
root@webserver:/home/webserver/wazuh# systemctl daemon-reload
root@webserver:/home/webserver/wazuh# systemctl enable wazuh-indexer
Synchronizing state of wazuh-indexer.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable wazuh-indexer
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-indexer.service → /lib/systemd/system/wazuh-indexer.service.
root@webserver:/home/webserver/wazuh# systemctl start wazuh-indexer
root@webserver:/home/webserver/wazuh#
```

root@webserver: /home/webserver/wazuh

```
root@webserver:/home/webserver/wazuh# systemctl daemon-reload
root@webserver:/home/webserver/wazuh# systemctl enable wazuh-manager
Synchronizing state of wazuh-manager.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable wazuh-manager
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-manager.service → /lib/systemd/system/wazuh-manager.service.
root@webserver:/home/webserver/wazuh# systemctl start wazuh-manager
root@webserver:/home/webserver/wazuh#
```

```
root@webserver:/home/webserver/wazuh# systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2023-03-27 12:18:49 UTC; 23s ago
    Process: 40542 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 133 (limit: 20362)
     Memory: 580.2M
        CPU: 20.715s
     CGroup: /system.slice/wazuh-manager.service
             ├─40595 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─40634 /var/ossec/bin/wazuh-authd
             ├─40650 /var/ossec/bin/wazuh-db
             ├─40664 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─40667 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─40679 /var/ossec/bin/wazuh-execd
             ├─40693 /var/ossec/bin/wazuh-analysisd
             ├─40754 /var/ossec/bin/wazuh-syscheckd
             ├─40773 /var/ossec/bin/wazuh-remoted
             ├─40805 /var/ossec/bin/wazuh-logcollector
             ├─40827 /var/ossec/bin/wazuh-monitord
             └─40849 /var/ossec/bin/wazuh-modulesd

Mar 27 12:18:40 webserver env[40542]: Started wazuh-db...
Mar 27 12:18:41 webserver env[40542]: Started wazuh-execd...
Mar 27 12:18:42 webserver env[40542]: Started wazuh-analysisd...
Mar 27 12:18:43 webserver env[40542]: Started wazuh-syscheckd...
Mar 27 12:18:44 webserver env[40542]: Started wazuh-remoted...
Mar 27 12:18:46 webserver env[40542]: Started wazuh-logcollector...
Mar 27 12:18:47 webserver env[40542]: Started wazuh-monitord...
Mar 27 12:18:47 webserver env[40542]: Started wazuh-modulesd...
Mar 27 12:18:49 webserver env[40542]: Completed.
Mar 27 12:18:49 webserver systemd[1]: Started Wazuh manager.
root@webserver:/home/webserver/wazuh#
```

```
root@webserver:/home/webserver/wazuh# dpkg -i ./wazuh-offline/wazuh-packages/filebeat*.deb
Selecting previously unselected package filebeat.
(Reading database ... 93565 files and directories currently installed.)
Preparing to unpack .../filebeat-oss-7.10.2-amd64.deb ...
Unpacking filebeat (7.10.2) ...
Setting up filebeat (7.10.2) ...
root@webserver:/home/webserver/wazuh#
```

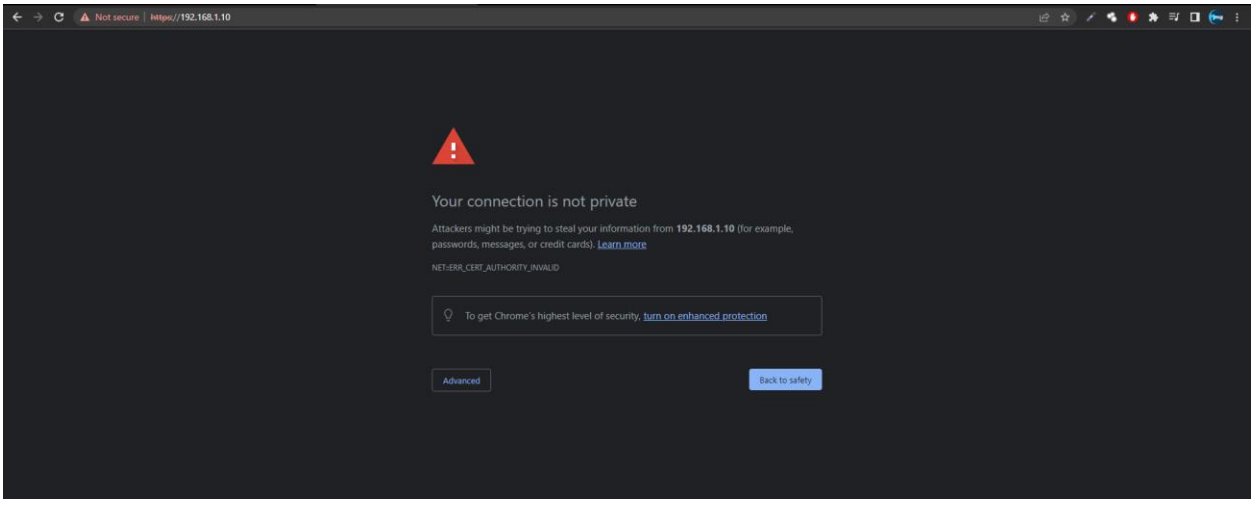
```
root@webserver:/home/webserver/wazuh# cp ./wazuh-offline/wazuh-files/filebeat.yml /etc/filebeat/ &&\
cp ./wazuh-offline/wazuh-files/wazuh-template.json /etc/filebeat/ &&\
chmod go+r /etc/filebeat/wazuh-template.json
root@webserver:/home/webserver/wazuh#
root@webserver:/home/webserver/wazuh# dpkg -i ./wazuh-offline/wazuh-packages/wazuh-dashboard*.deb
Selecting previously unselected package wazuh-dashboard.
(Reading database ... 93884 files and directories currently installed.)
Preparing to unpack .../wazuh-dashboard_4.3.10-1_amd64.deb ...
Creating wazuh-dashboard group... OK
Creating wazuh-dashboard user... OK
Unpacking wazuh-dashboard (4.3.10-1) ...
Setting up wazuh-dashboard (4.3.10-1) ...
root@webserver:/home/webserver/wazuh#
```

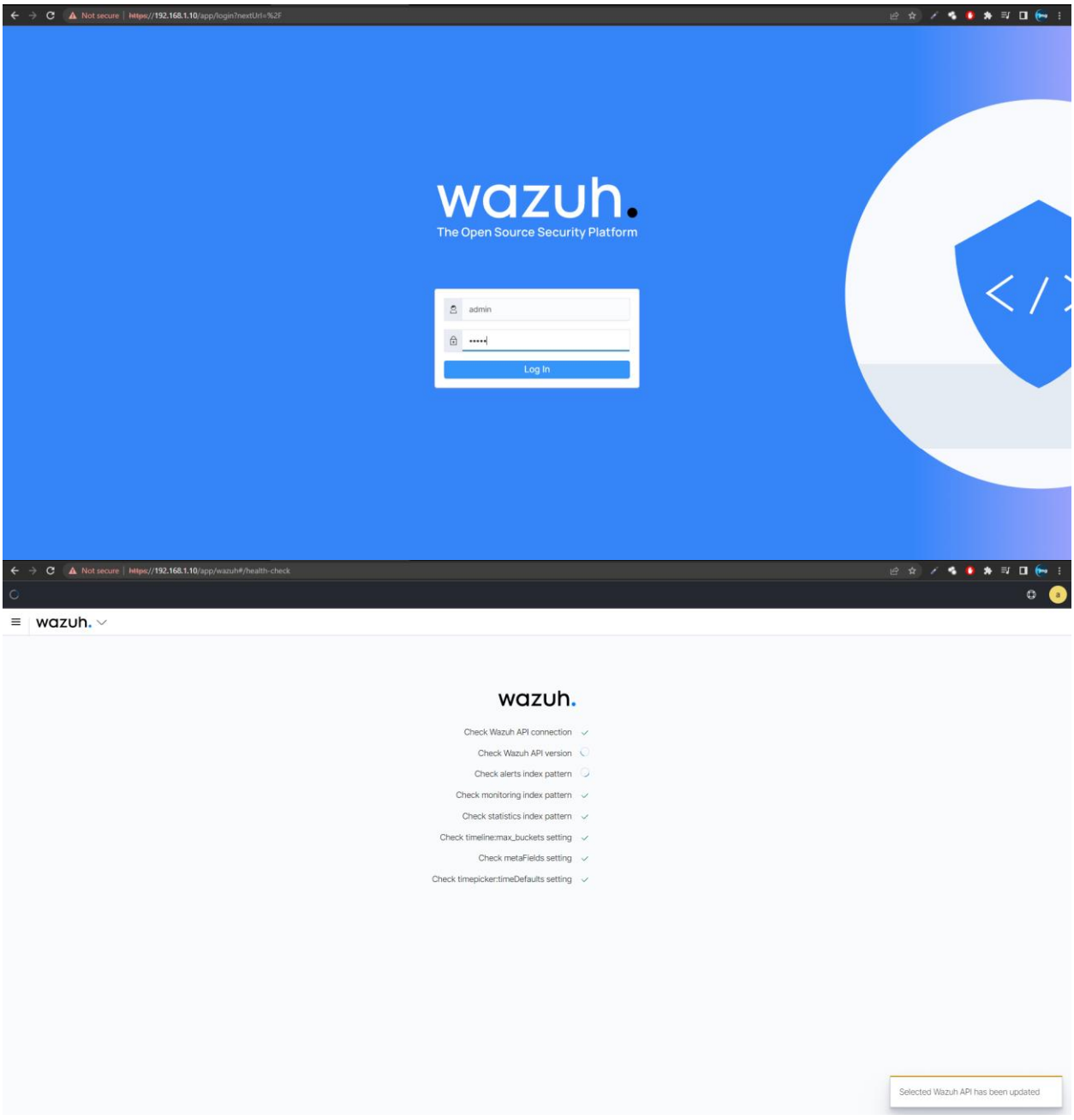
```
root@webserver:/home/webserver/wazuh# NODE_NAME=dashboard
root@webserver:/home/webserver/wazuh# mkdir /etc/wazuh-dashboard/certs
root@webserver:/home/webserver/wazuh# mv -n wazuh-certificates/$NODE_NAME.pem /etc/wazuh-dashboard/certs/dashboard.pem
root@webserver:/home/webserver/wazuh# mv -n wazuh-certificates/$NODE_NAME-key.pem /etc/wazuh-dashboard/certs/dashboard-key.pem
root@webserver:/home/webserver/wazuh# cp wazuh-certificates/root-ca.pem /etc/wazuh-dashboard/certs/
root@webserver:/home/webserver/wazuh# chmod 500 /etc/wazuh-dashboard/certs
root@webserver:/home/webserver/wazuh# chmod 400 /etc/wazuh-dashboard/certs/*
root@webserver:/home/webserver/wazuh# chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs
root@webserver:/home/webserver/wazuh#
```

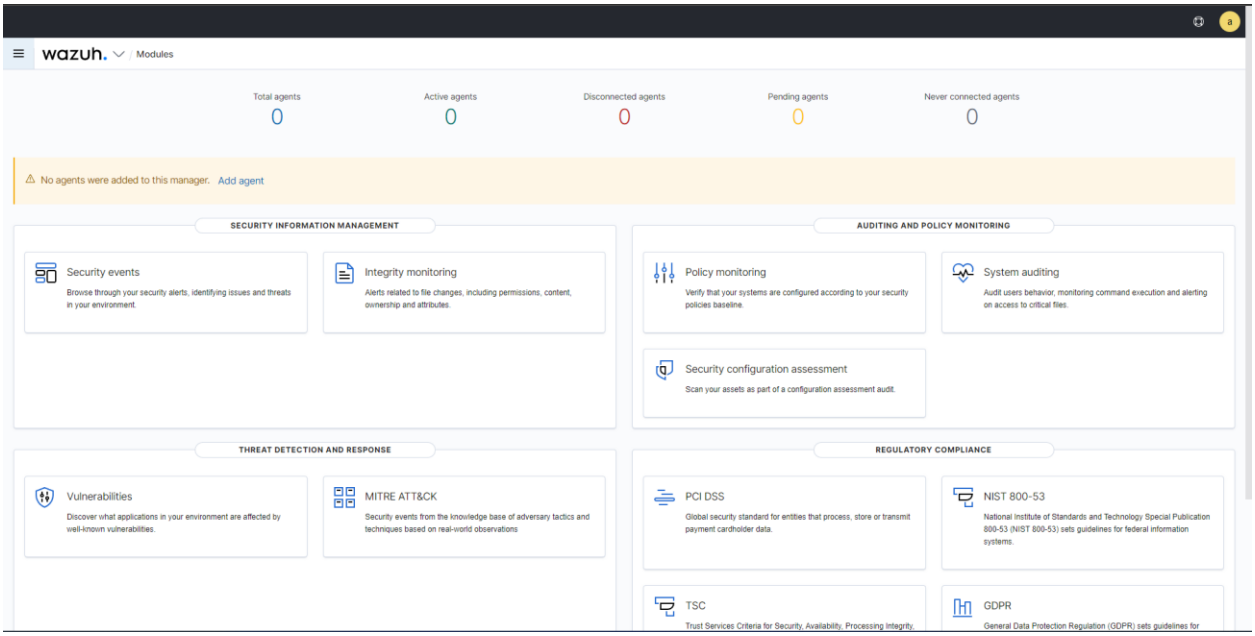
root@webserver: /home/webserver/wazuh

```
  GNU nano 6.2
server.host: 0.0.0.0
server.port: 443
opensearch.hosts: https://192.168.1.10:9200
opensearch.ssl.verificationMode: certificate
#opensearch.username:
#opensearch.password:
opensearch.requestHeadersWhitelist: ["securitytenant","Authorization"]
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ["kibana_read_only"]
server.ssl.enabled: true
server.ssl.key: "/etc/wazuh-dashboard/certs/dashboard-key.pem"
server.ssl.certificate: "/etc/wazuh-dashboard/certs/dashboard.pem"
opensearch.ssl.certificateAuthorities: ["/etc/wazuh-dashboard/certs/root-ca.pem"]
uiSettings.overrides.defaultRoute: /app/wazuh
```

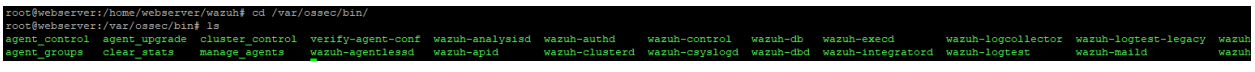
```
root@webserver:/home/webserver/wazuh# systemctl daemon-reload
root@webserver:/home/webserver/wazuh# systemctl enable wazuh-dashboard
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-dashboard.service → /etc/systemd/system/wazuh-dashboard.service.
root@webserver:/home/webserver/wazuh# systemctl start wazuh-dashboard
root@webserver:/home/webserver/wazuh#
```



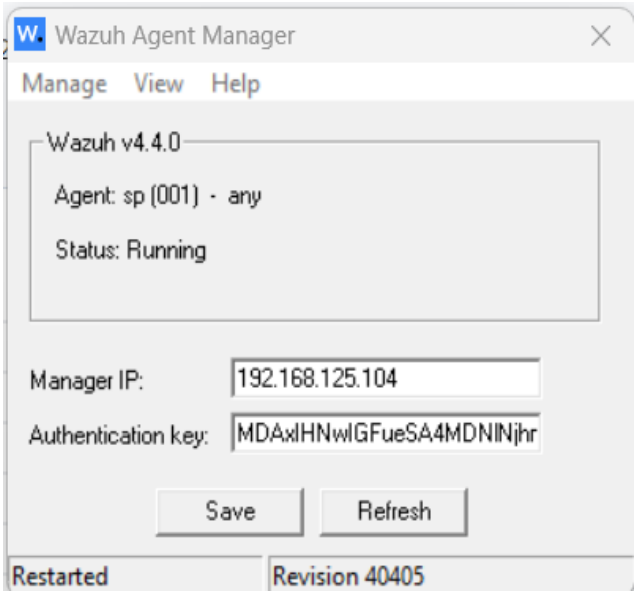

Not secure | https://192.168.1.10/app/login?nextUrl=%2F
wazuh.
The Open Source Security Platform
admin
Log In
Not secure | https://192.168.1.10/app/wazuh#/health-check
wazuh.
wazuh.
Check Wazuh API connection
Check Wazuh API version
Check alerts index pattern
Check monitoring index pattern
Check statistics index pattern
Check timeline:max_buckets setting
Check metaFields setting
Check timepicker:timeDefaults setting
Selected Wazuh API has been updated

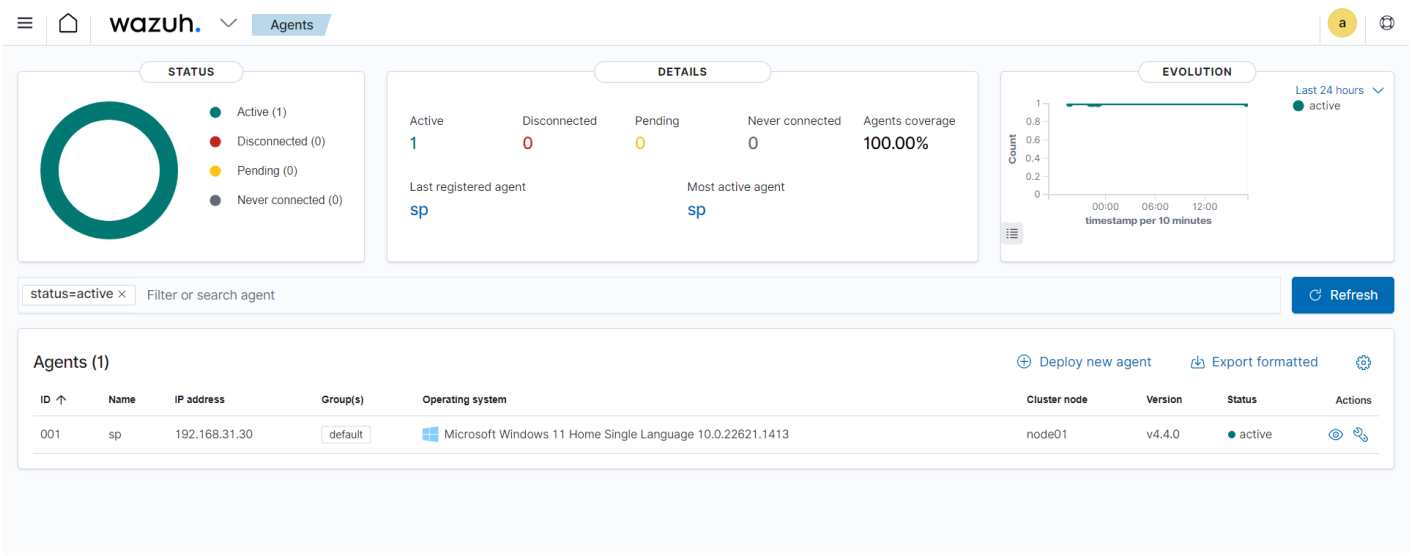

wazuh.
Modules
Total agents
0
Active agents
0
Disconnected agents
0
Pending agents
0
Never connected agents
0
No agents were added to this manager.
Add agent
SECURITY INFORMATION MANAGEMENT
Security events
Browse through your security alerts, identifying issues and threats in your environment.
Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.
AUDITING AND POLICY MONITORING
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.
Security configuration assessment
Scan your assets as part of a configuration assessment audit.
THREAT DETECTION AND RESPONSE
Vulnerabilities
Discover what applications in your environment are affected by well-known vulnerabilities.
MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on real-world observations
REGULATORY COMPLIANCE
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,
GDPR
General Data Protection Regulation (GDPR) sets guidelines for

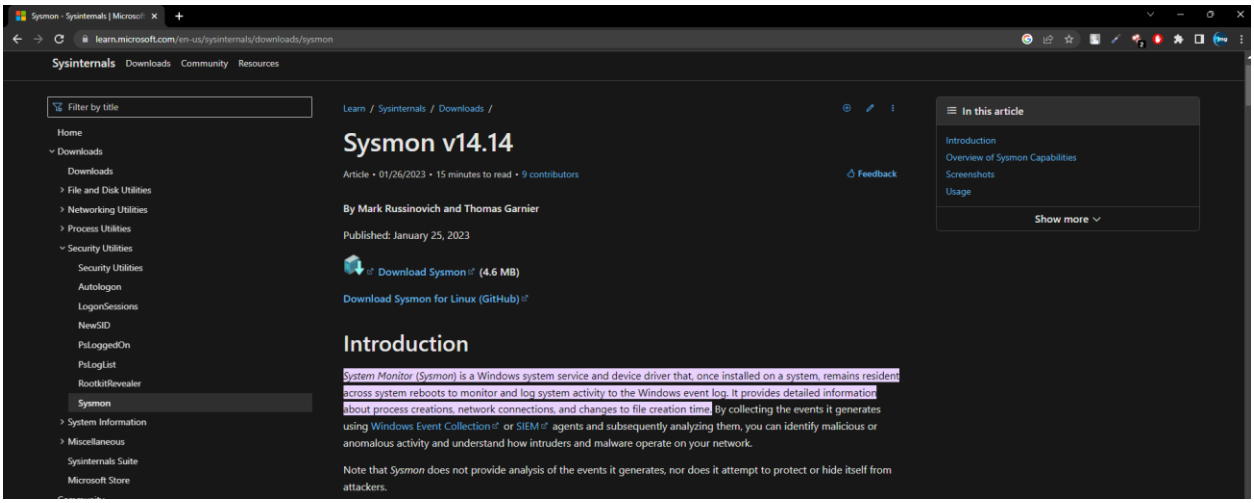

wazuh.
Platform
Cloud
Services
Partners
Blog
Company
Search
Getting started
Quickstart
Installation guide
Wazuh indexer
Wazuh server
Wazuh dashboard
Wazuh agent
Linux
Installation guide / Wazuh agent / Installing Wazuh agents on Windows endpoints
Installing Wazuh agents on Windows endpoints
The agent runs on the endpoint you want to monitor and communicates with the Wazuh server, sending data in near real-time through an encrypted and authenticated channel. Monitor your Windows systems with Wazuh, from Windows XP to the latest available versions including Windows 11 and Windows Server 2022.
Note To perform the installation, administrator privileges are required.
1. To start the installation process, download the Windows installer.
2. Select the installation method you want to follow: command line interface (CLI) or graphical user interface (GUI).

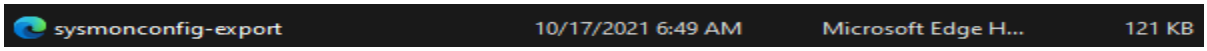

root@webserver:/home/webserver/wazuh# cd /var/ossec/bin/
root@webserver:/var/ossec/bin# ls
agent_control agent_upgrade cluster_control verify-agent-conf wazuh-analysisd wazuh-authd wazuh-control wazuh-db wazuh-execd wazuh-logcollector wazuh-logtest-legacy wazuh
agent_groups clear_stats manage_agents wazuh-agentlessd wazuh-apid wazuh-clusterd wazuh-csyslogd wazuh-dbd wazuh-integratord wazuh-logtest wazuh-maild wazuh

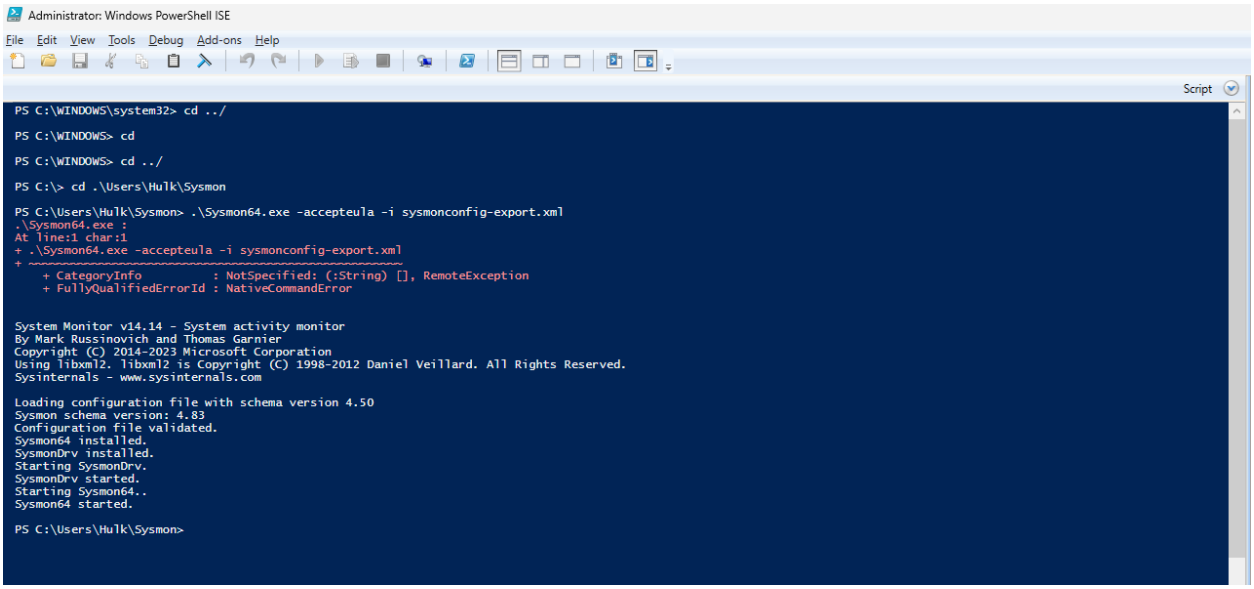
```
   (Q)uit.
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: sahil
   * The IP Address of the new agent: any
Confirm adding it?(y/n): y
2023/04/06 14:00:56 manage_agents: WARNING: 9008: Duplicate name


****************************************
* Wazuh v4.4.0 Agent manager.          *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
```

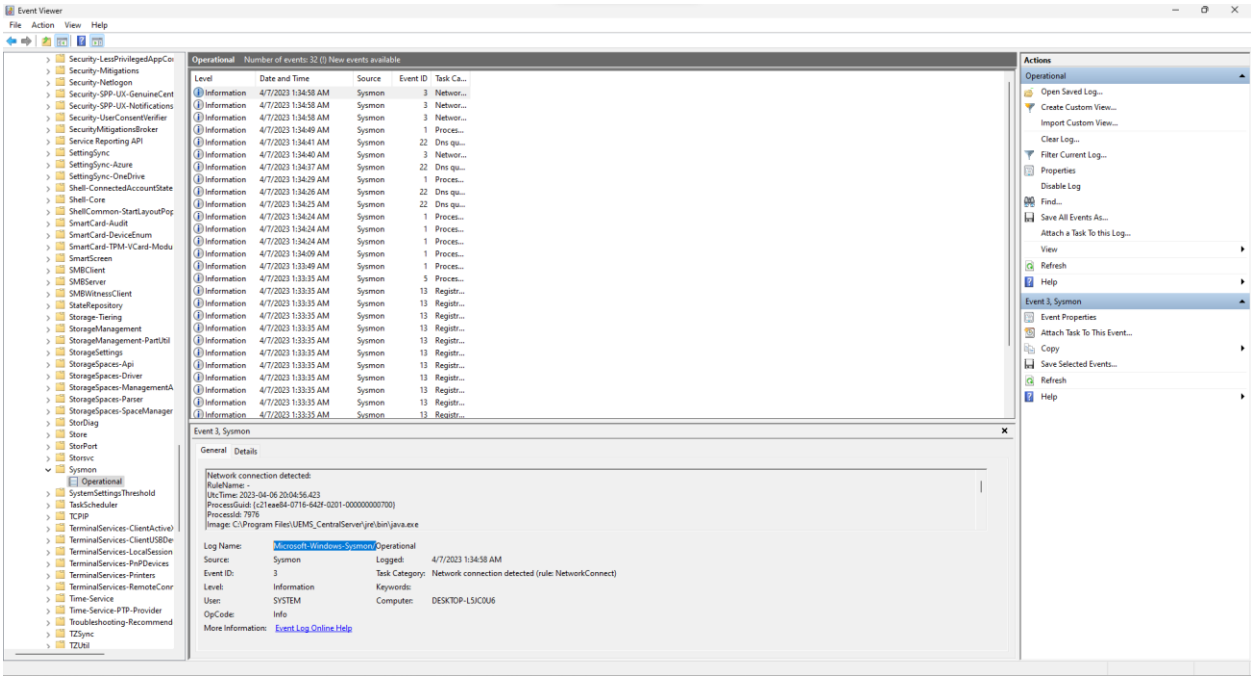


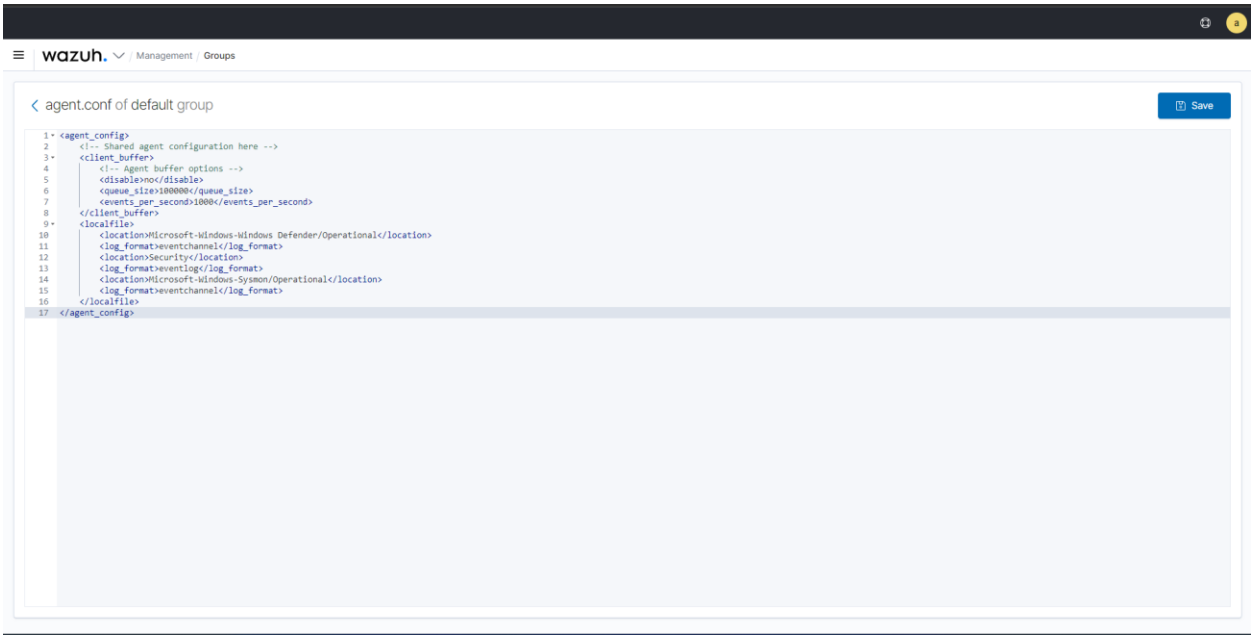

wazuh.
Agents
a
STATUS
Active (1)
Disconnected (0)
Pending (0)
Never connected (0)
DETAILS
Active
1
Disconnected
0
Pending
0
Never connected
0
Agents coverage
100.00%
Last registered agent
sp
Most active agent
sp
EVOLUTION
Last 24 hours
active
Count
1
0.8
0.6
0.4
0.2
0
00:00
06:00
12:00
timestamp per 10 minutes
status=active
Filter or search agent
Refresh
Agents (1)
Deploy new agent
Export formatted
ID
Name
IP address
Group(s)
Operating system
Cluster node
Version
Status
Actions
001
sp
192.168.31.30
default
Microsoft Windows 11 Home Single Language 10.0.22621.1413
node01
v4.4.0
active


Sysmon - Sysinternals | Microsoft
learn.microsoft.com/en-us/sysinternals/downloads/sysmon
Sysinternals Downloads Community Resources
Filter by title
Home
Downloads
Downloads
File and Disk Utilities
Networking Utilities
Process Utilities
Security Utilities
Security Utilities
Autologon
LogonSessions
NewSID
PsLoggedOn
PsLogList
RootkitRevealer
Sysmon
System Information
Miscellaneous
Sysinternals Suite
Microsoft Store
Learn / Sysinternals / Downloads /
Sysmon v14.14
Article • 01/26/2023 • 15 minutes to read • 9 contributors
Feedback
By Mark Russinovich and Thomas Garnier
Published: January 25, 2023
Download Sysmon (4.6 MB)
Download Sysmon for Linux (GitHub)
Introduction
System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.
Note that Sysmon does not provide analysis of the events it generates, nor does it attempt to protect or hide itself from attackers.
In this article
Introduction
Overview of Sysmon Capabilities
Screenshots
Usage
Show more


sysmonconfig-export
10/17/2021 6:49 AM
Microsoft Edge H...
121 KB


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script
PS C:\WINDOWS\system32> cd ../
PS C:\WINDOWS> cd
PS C:\WINDOWS> cd ../
PS C:\> cd .\Users\Hulk\Sysmon
PS C:\Users\Hulk\Sysmon> .\Sysmon64.exe -accepteula -i sysmonconfig-export.xml
.\Sysmon64.exe :
At line:1 char:1
+ .\Sysmon64.exe -accepteula -i sysmonconfig-export.xml
+ ~~~~~~
+ CategoryInfo : NotSpecified: (:String) [], RemoteException
+ FullyQualifiedErrorId : NativeCommandError
System Monitor v14.14 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2023 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 4.50
Sysmon schema version: 4.83
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Users\Hulk\Sysmon>


Event Viewer
File Action View Help
Operational Number of events: 32 (!) New events available
Level Date and Time Source Event ID Task Ca...
Information 4/7/2023 1:34:58 AM Sysmon 3 Networ...
Information 4/7/2023 1:34:58 AM Sysmon 3 Networ...
Information 4/7/2023 1:34:58 AM Sysmon 3 Networ...
Information 4/7/2023 1:34:49 AM Sysmon 1 Proces...
Information 4/7/2023 1:34:41 AM Sysmon 22 Dns qu...
Information 4/7/2023 1:34:40 AM Sysmon 3 Networ...
Information 4/7/2023 1:34:37 AM Sysmon 22 Dns qu...
Information 4/7/2023 1:34:29 AM Sysmon 1 Proces...
Information 4/7/2023 1:34:26 AM Sysmon 22 Dns qu...
Information 4/7/2023 1:34:25 AM Sysmon 22 Dns qu...
Information 4/7/2023 1:34:24 AM Sysmon 1 Proces...
Information 4/7/2023 1:34:24 AM Sysmon 1 Proces...
Information 4/7/2023 1:34:24 AM Sysmon 1 Proces...
Information 4/7/2023 1:34:09 AM Sysmon 1 Proces...
Information 4/7/2023 1:33:49 AM Sysmon 1 Proces...
Information 4/7/2023 1:33:35 AM Sysmon 5 Proces...
Information 4/7/2023 1:33:35 AM Sysmon 13 Registr...
Information 4/7/2023 1:33:35 AM Sysmon 13 Registr...
Information 4/7/2023 1:33:35 AM Sysmon 13 Registr...
Information 4/7/2023 1:33:35 AM Sysmon 13 Registr...
Information 4/7/2023 1:33:35 AM Sysmon 13 Registr...
Information 4/7/2023 1:33:35 AM Sysmon 13 Registr...
Information 4/7/2023 1:33:35 AM Sysmon 13 Registr...
Information 4/7/2023 1:33:35 AM Sysmon 13 Registr...
Information 4/7/2023 1:33:35 AM Sysmon 13 Registr...
Event 3, Sysmon
General Details
Network connection detected:
RuleName: -
UtcTime: 2023-04-06 20:04:56.423
ProcessGuid: {c21eae84-0716-642f-0201-000000000700}
ProcessId: 7976
Image: C:\Program Files\UEMS_CentralServer\jre\bin\java.exe
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 4/7/2023 1:34:58 AM
Event ID: 3
Task Category: Network connection detected (rule: NetworkConnect)
Level: Information
Keywords:
User: SYSTEM
Computer: DESKTOP-L5JC0U6
OpCode: Info
More Information: Event Log Online Help
Actions
Operational
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Disable Log
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 3, Sysmon
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help


wazuh.
Management
Groups
agent.conf of default group
Save
<agent_config>
<!-- Shared agent configuration here -->
<client_buffer>
<!-- Agent buffer options -->
<disable>no</disable>
<queue_size>100000</queue_size>
<events_per_second>1000</events_per_second>
</client_buffer>
<localfile>
<location>Microsoft-Windows-Windows Defender/Operational</location>
<log_format>eventchannel</log_format>
<location>Security</location>
<log_format>eventlog</log_format>
<location>Microsoft-Windows-Sysmon/Operational</location>
<log_format>eventchannel</log_format>
</localfile>
</agent_config>

CHAPTER: 8 REFERENCES

CHAPTER 8 REFERENCES

- https://www.ipindia.gov.in/
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3217699/
- https://www.ies.gov.in/pdfs/why-India-needs-to-urgently-invest-in-its-IPR-ecosystem-16th-Aug-2022.pdf
- http://www.sric.iitkgp.ac.in/docss/iitkgpipguide.pdf