Assigning Wazuh Static IP Address

Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY

Follow Me: linkedin.com/in/moizuddinrafay

Importance of Assigning a Static IP Address to Your Wazuh Server

In a network infrastructure, ensuring stability and reliability is paramount, especially for critical components like security monitoring servers. Here's why assigning a static IP address to your Wazuh server is crucial:

1. Consistent Configuration: With a static IP, you maintain a consistent configuration. This stability is vital for network services like Wazuh, ensuring uninterrupted monitoring and alerting processes.

2. Ease of Management: A static IP simplifies network management. It ensures that the Wazuh server is always reachable at the same address, streamlining administrative tasks such as remote access, firewall configurations, and DNS mappings.

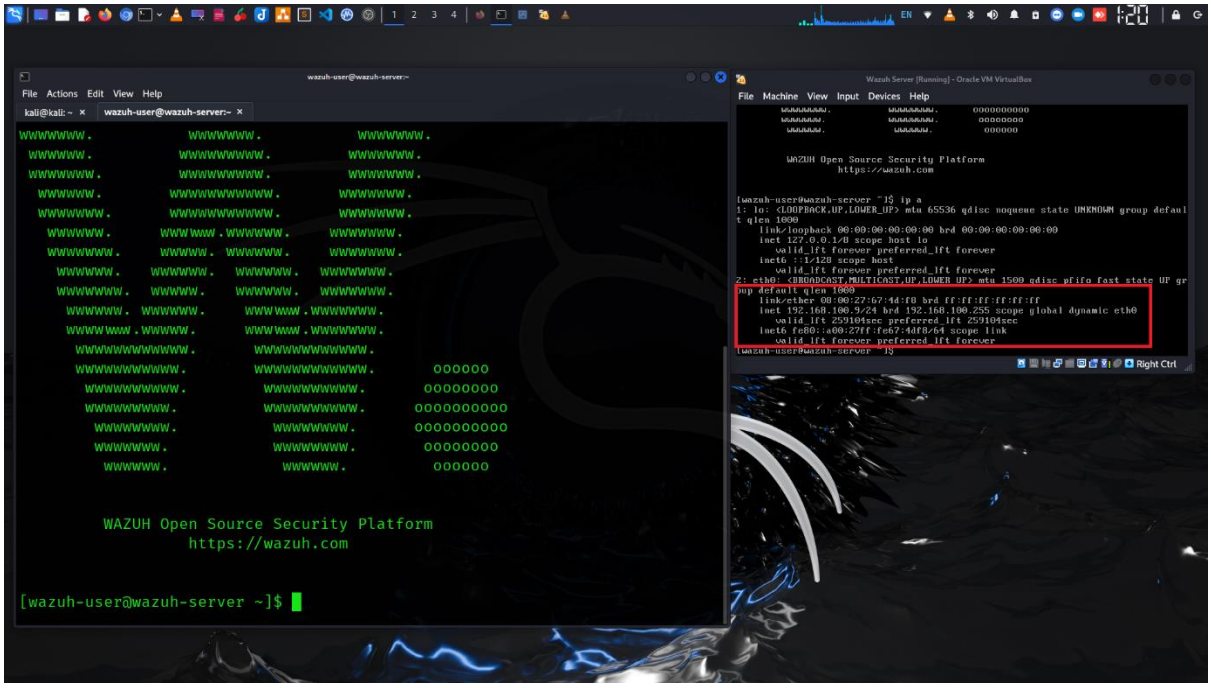
3. Dependency in Distributed Environments: In distributed environments or setups with multiple integrated systems, various services might rely on the Wazuh server's IP address. A static IP prevents disruption to these dependencies caused by dynamic address changes.

4. Enhanced Security: Dynamic IP addresses can potentially introduce security risks, especially if they change frequently. Assigning a static IP to the Wazuh server helps in maintaining consistent firewall rules, access controls, and security policies tailored to its specific address.

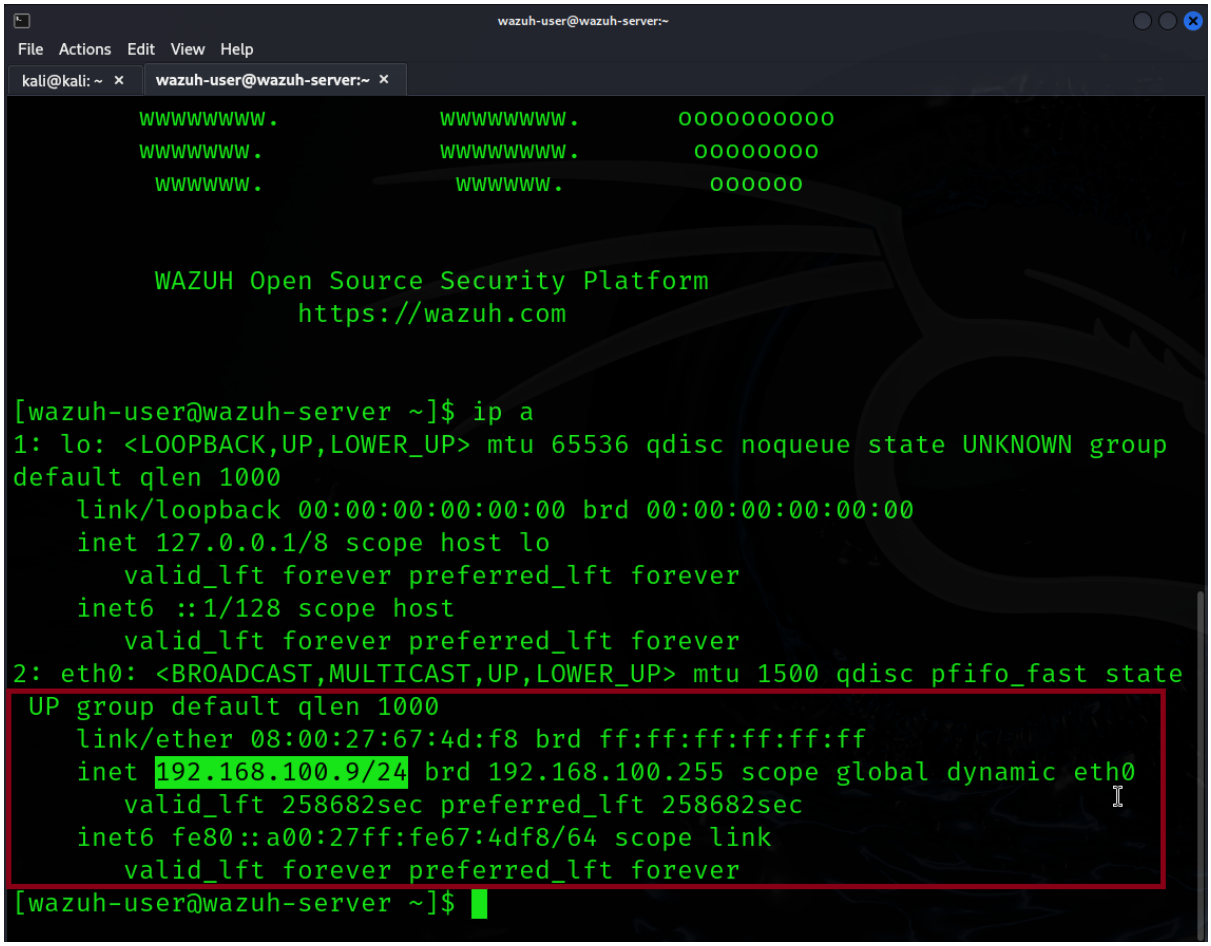
5. Improved Logging and Analysis: Static IP addresses aid in log analysis and correlation by providing a stable identifier for the Wazuh server across different network devices and services. This stability is valuable for forensic investigations and incident response.

Step 01: Check the current IP Address.

Command: ip a

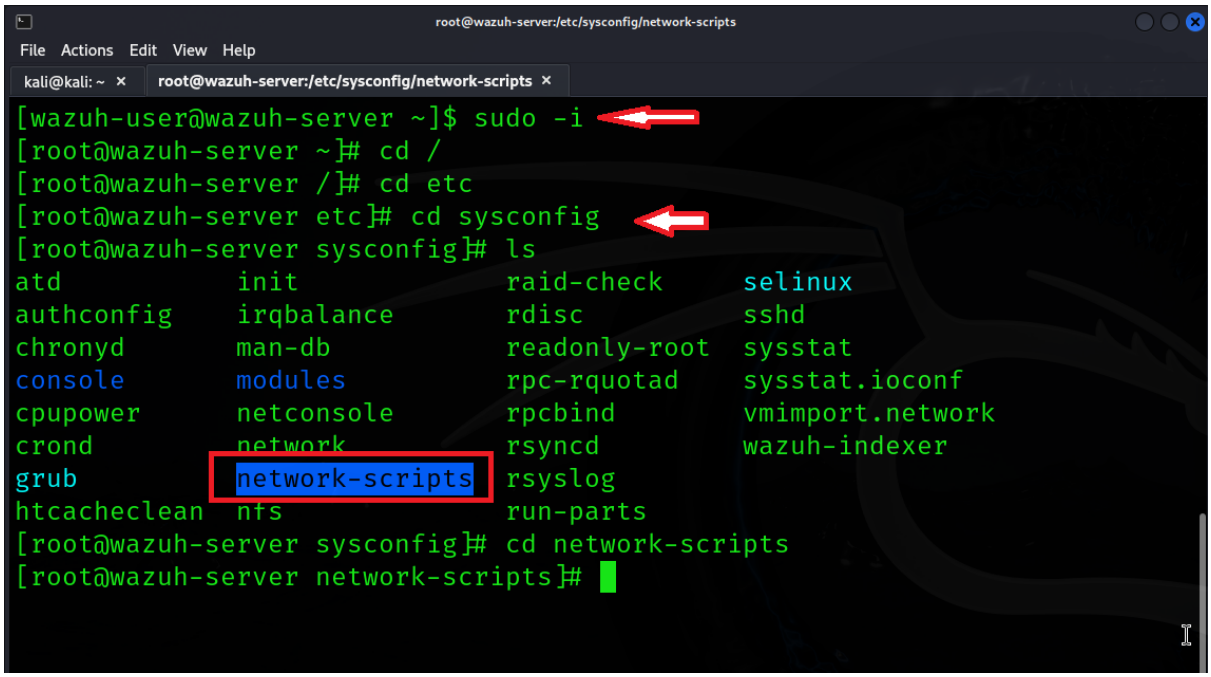


Step 02: Connect Wazuh Server via SSH and find the IP Address again.



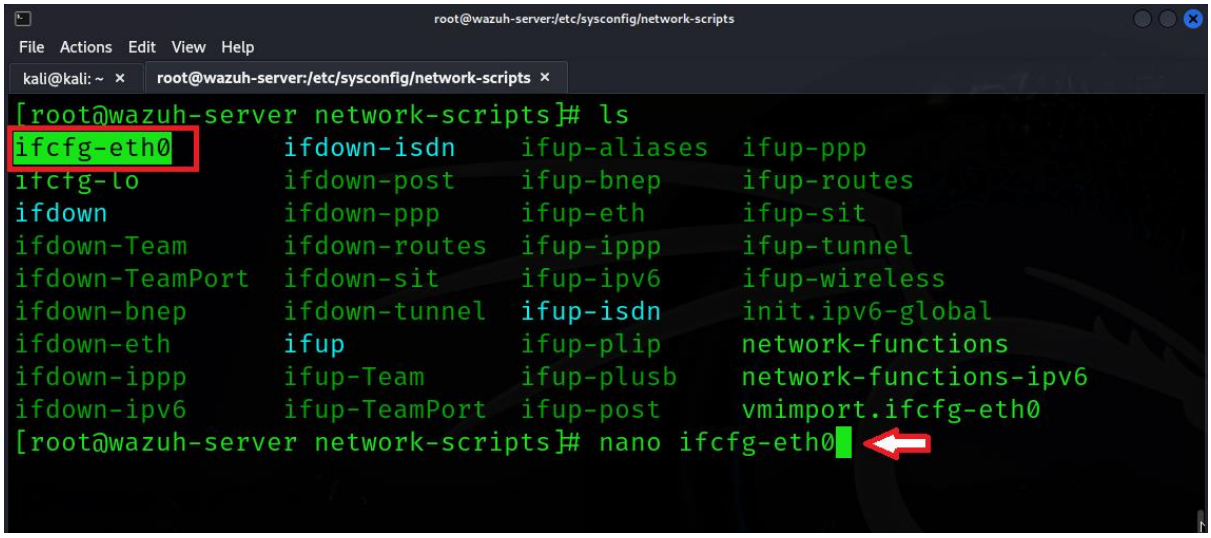
Step 03: Access the configuration file “ifcfg-eth0”

Login in to root with
Go to location with : “cd /etc/sysconfig/network-scripts”



Step 04: Edit the file “ifcfg-eth0”

Command: nano ifcfg-eth0



Here is the default configuration of file “ifcfg-eth0”

```
root@wazuh-server:/etc/sysconfig/network-scripts
File  Actions  Edit  View  Help
kali@kali: ~ ×   root@wazuh-server:/etc/sysconfig/network-scripts ×
  GNU nano 2.9.8                    ifcfg-eth0

# Automatically generated by the vm import process
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
NM_CONTROLLED=no

                              [ Read 6 lines ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell
```

Step 05: Check routing information

Command: route -n

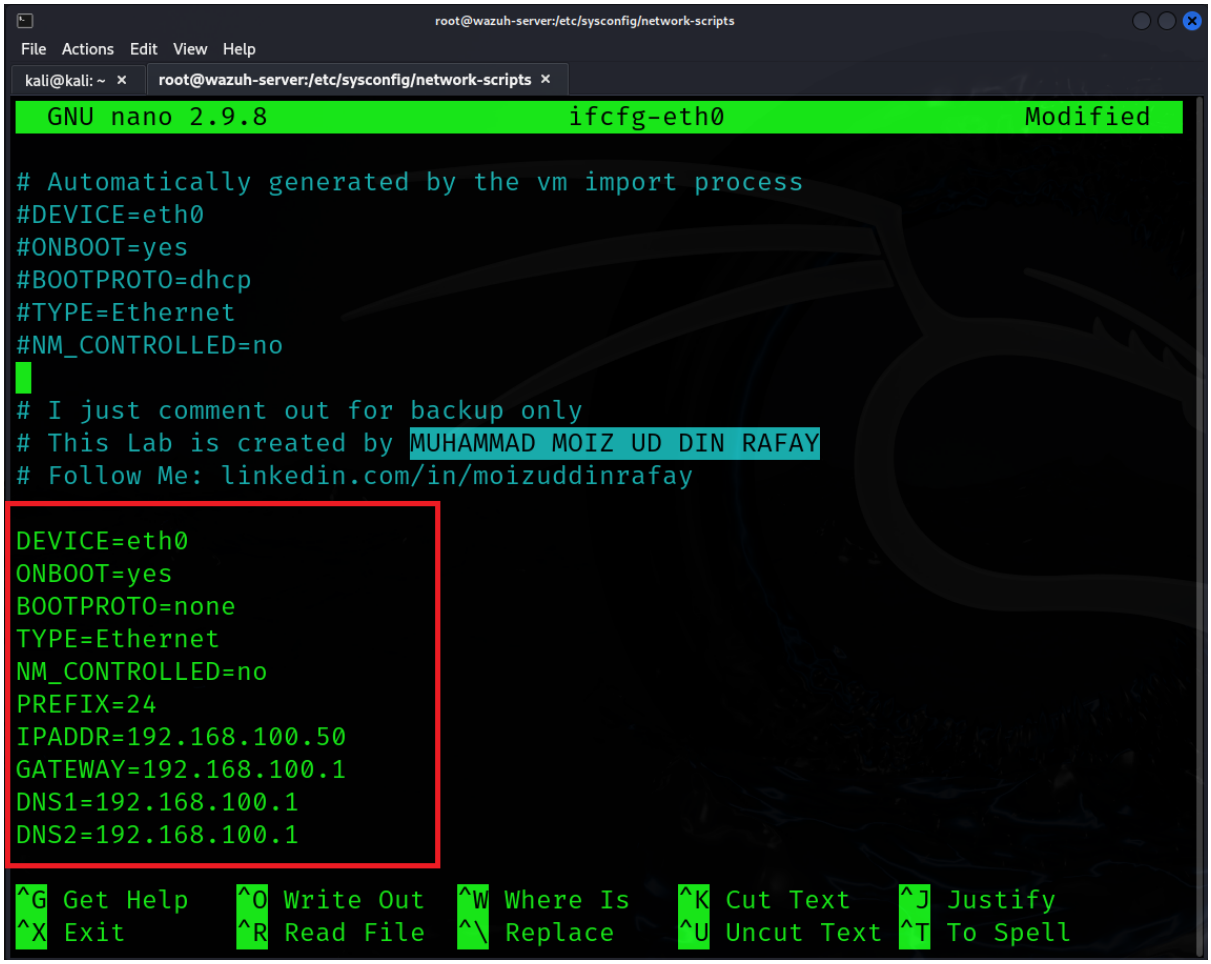
```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.100.1   0.0.0.0         UG    600    0        0 wlan0
192.168.100.0   0.0.0.0         255.255.255.0   U     600    0        0 wlan0
```

Gateway= 192.168.100.1

Subnet Range= 255.255.255.0

DNS= 192.168.100.1

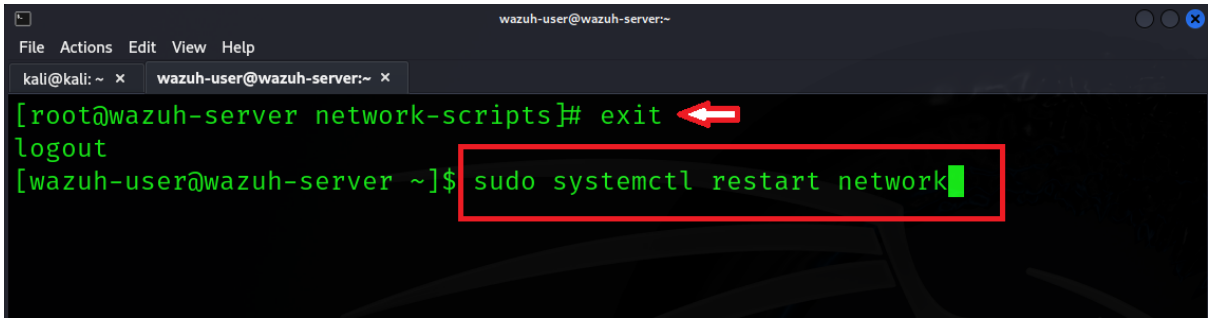
Step 06: Now add new configurations in file “ifcfg-eth0”
Note: before editing make a back of files (recommend)



Configuration:

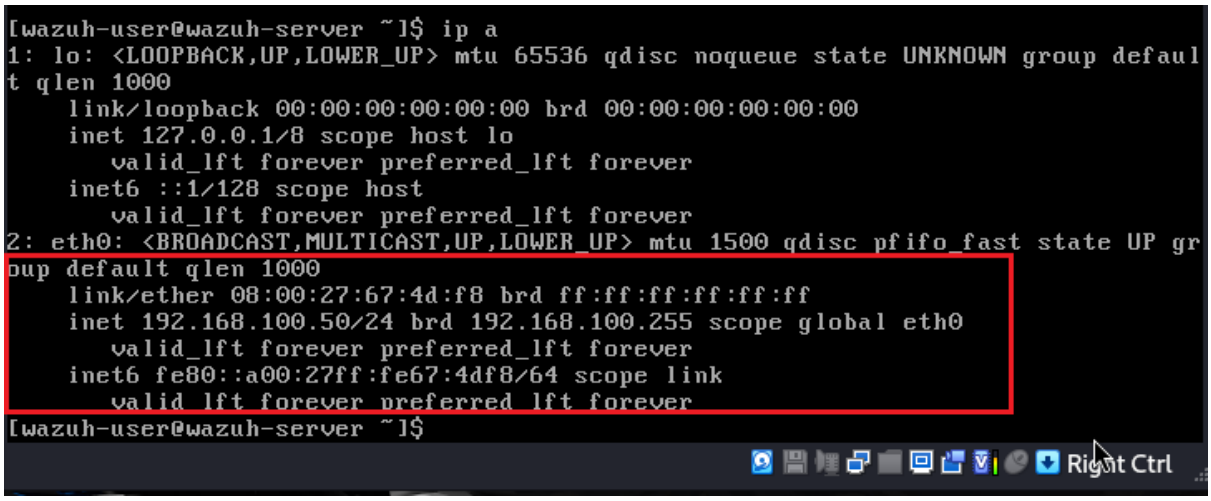
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=none
TYPE=Ethernet
NM_CONTROLLED=no
PREFIX=24
IPADDR=192.168.100.50 “type the IP address you want to add”
GATEWAY=192.168.100.1
DNS1=192.168.100.1
DNS2=192.1688.100.1

Step 07: Now exit form root login and restart network.
Command: sudo systemctl restart network

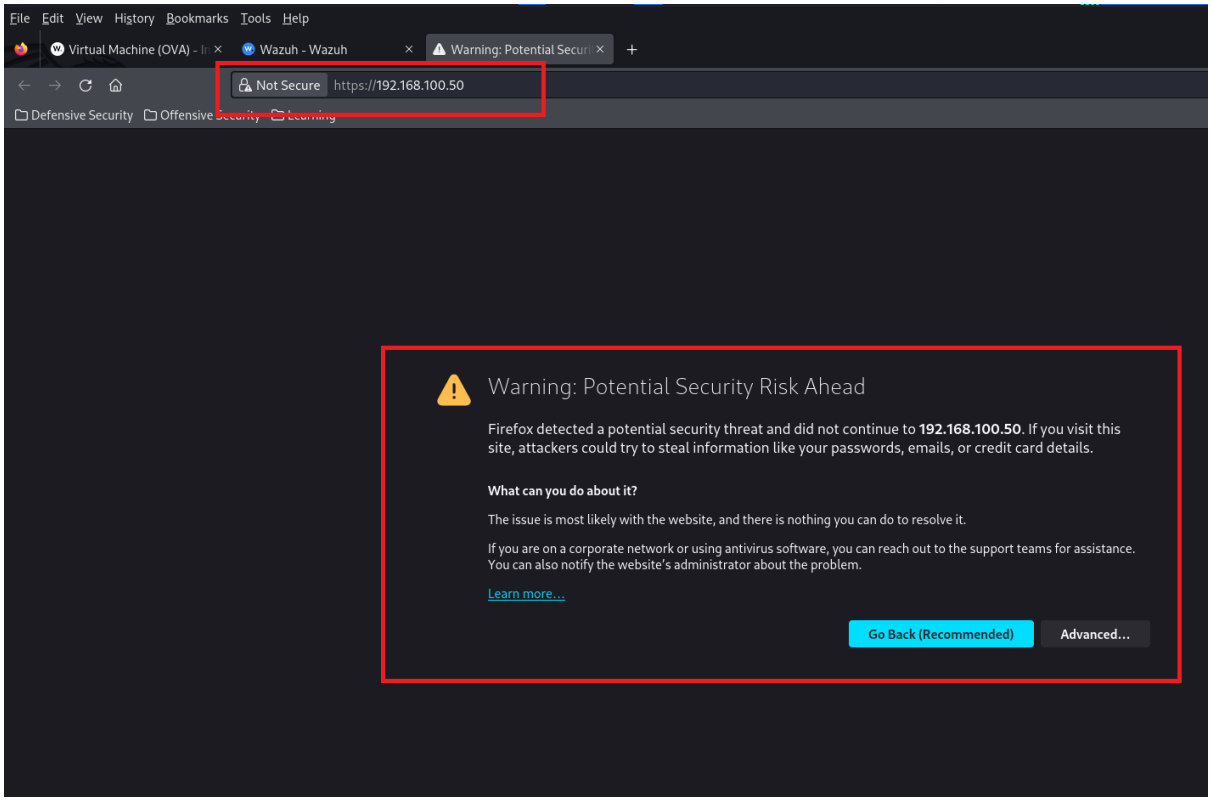


Network is restarting.

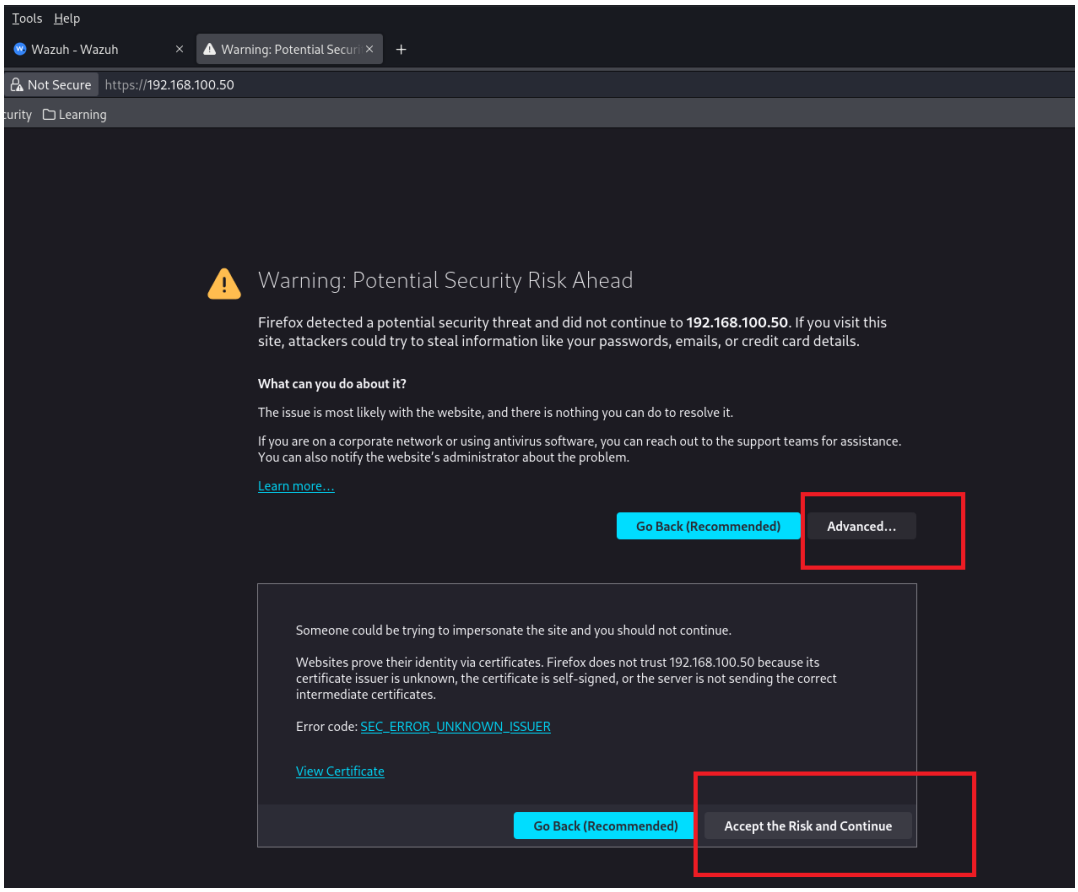
Here is New Static IP Address.



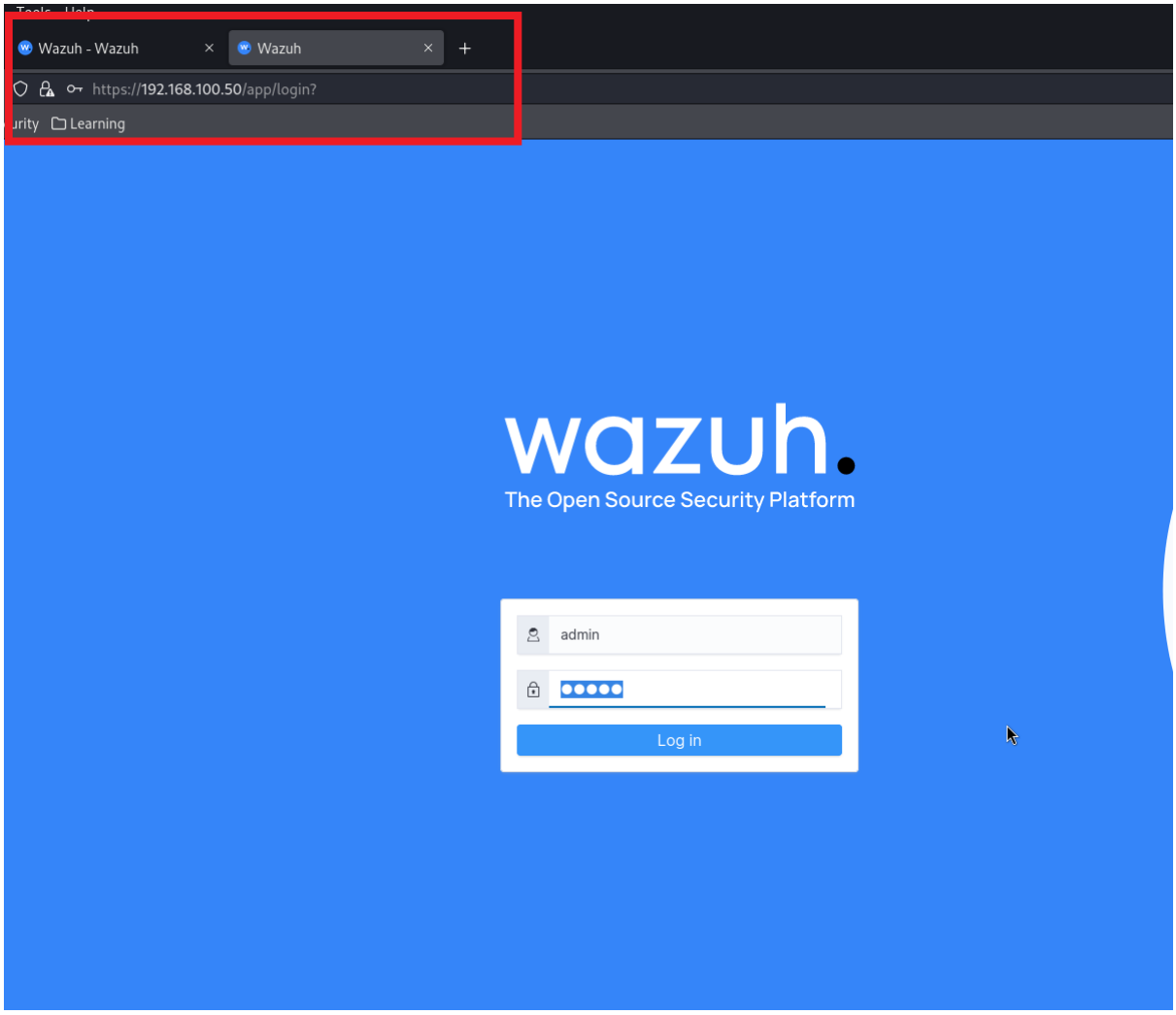
Step 08: Now access with browser by typing IP Address in URL bar.



Accept the security risk.



Here is Wazuh is running on Static IP Address



SUMMARY

In summary, assigning a static IP address to your Wazuh server is essential for maintaining network stability, simplifying management tasks, ensuring seamless integration with other services, enhancing security measures, and facilitating effective log analysis and monitoring.