



wazuh.

Assigning Wazuh Static IP Address

Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY

Follow Me: [linkedin.com/in/moizuddinrafay](https://www.linkedin.com/in/moizuddinrafay)

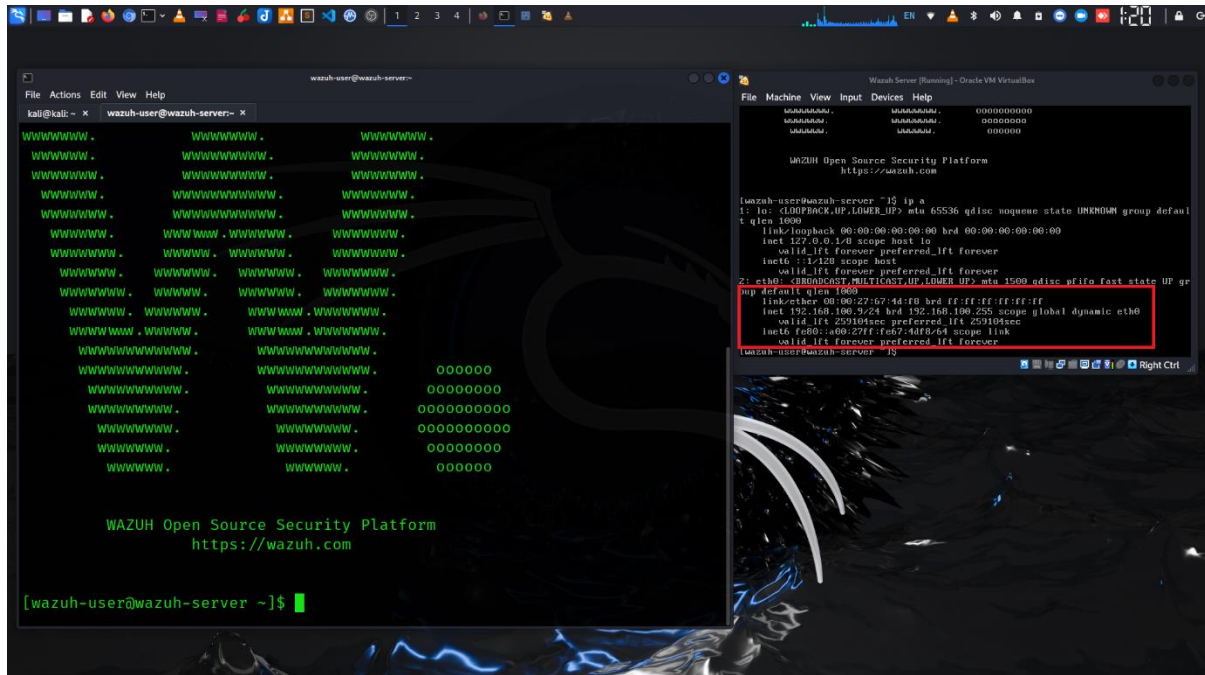
Importance of Assigning a Static IP Address to Your Wazuh Server

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.

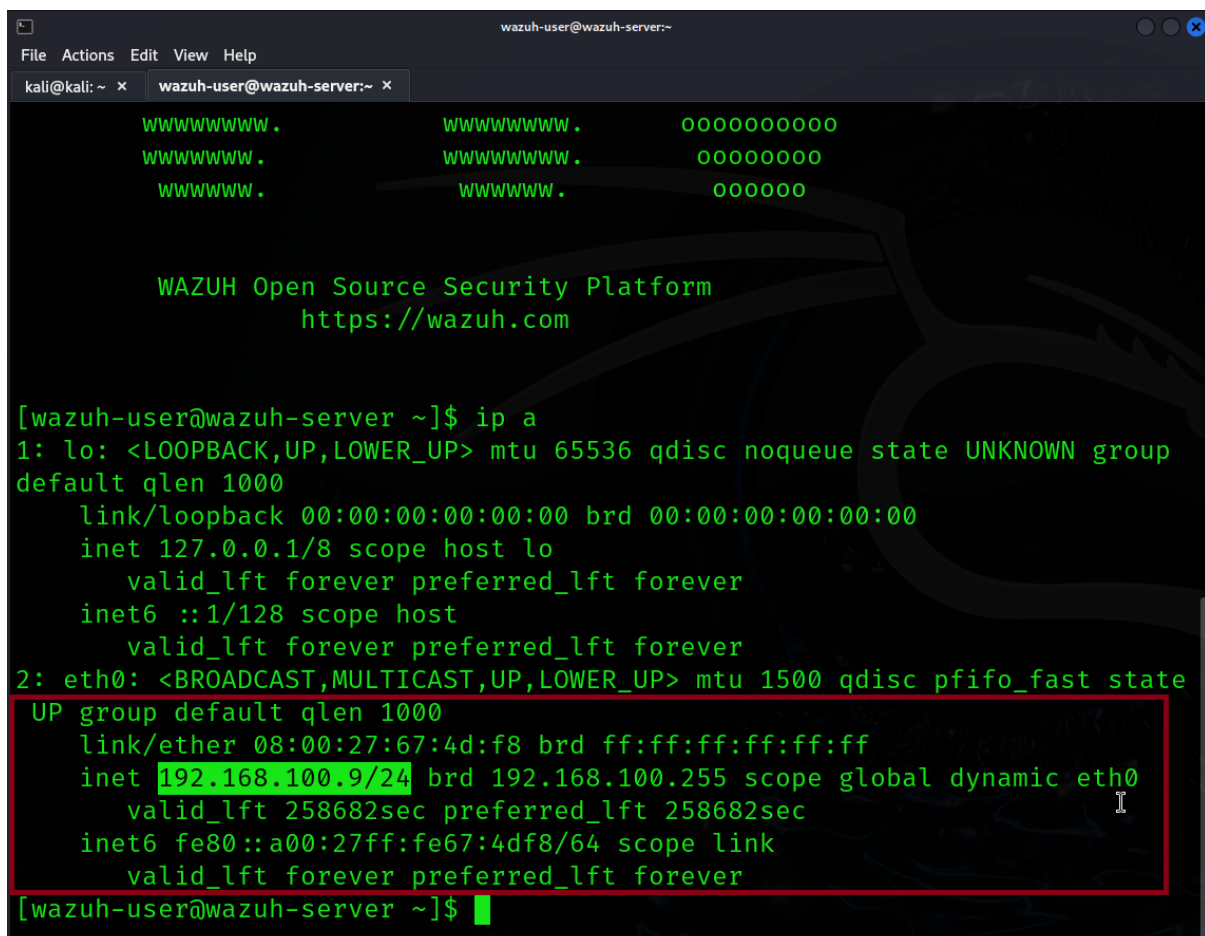
Step 01: Check the current IP Address.

Command: ip a



```
wazuh-user@wazuh-server ~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:67:4d:f8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.9/24 brd 192.168.100.255 scope global dynamic eth0
        valid_lft 258682sec preferred_lft 258682sec
    inet6 fe80::a00:27ff:fe67:4df8/64 scope link
        valid_lft forever preferred_lft forever
```

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

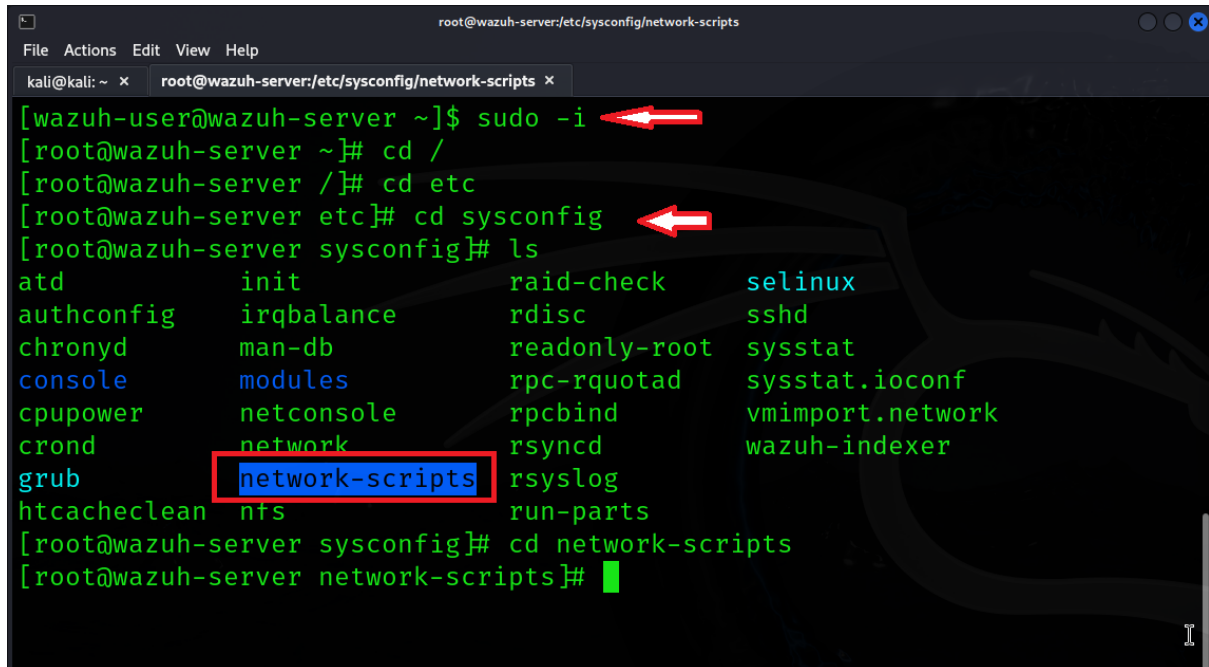


```
wazuh-user@wazuh-server ~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:67:4d:f8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.9/24 brd 192.168.100.255 scope global dynamic eth0
        valid_lft 258682sec preferred_lft 258682sec
    inet6 fe80::a00:27ff:fe67:4df8/64 scope link
        valid_lft forever preferred_lft forever
```

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

Login in to root with

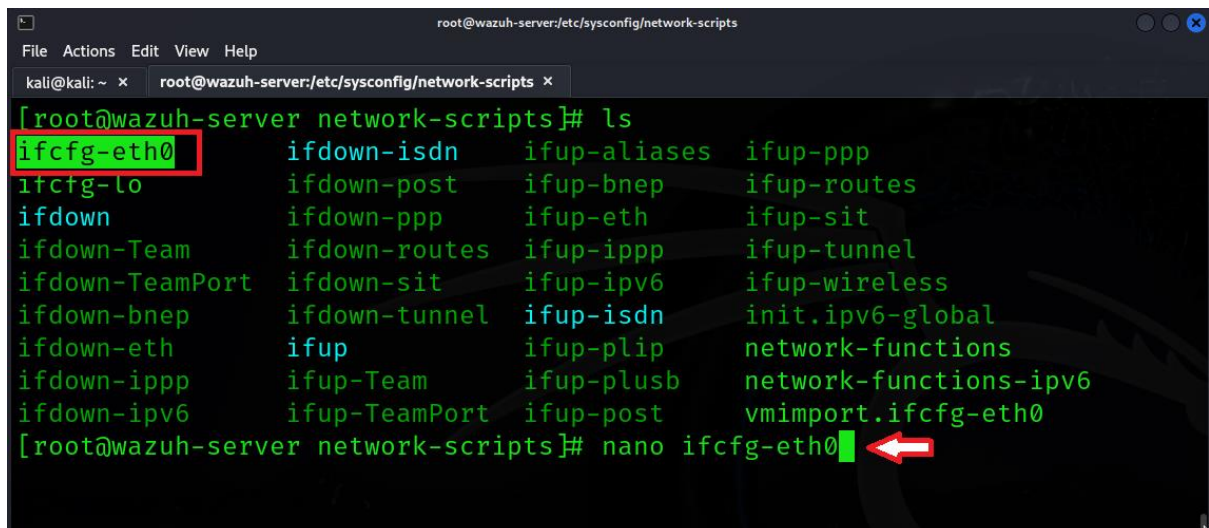
Go to location with : “cd /etc/sysconfig/network-scripts”



```
root@wazuh-server/etc/sysconfig/network-scripts
File Actions Edit View Help
kali@kali: ~ x root@wazuh-server/etc/sysconfig/network-scripts x
[wazuh-user@wazuh-server ~]$ sudo -i
[root@wazuh-server ~]# cd /
[root@wazuh-server /]# cd etc
[root@wazuh-server etc]# cd sysconfig
[root@wazuh-server sysconfig]# ls
atd          init          raid-check    selinux
authconfig   irqbalance    rdisc         sshd
chronyd       man-db        readonly-root sysstat
console      modules       rpc-rquotad   sysstat.ioconf
cpupower     netconsole    rpcbind       vmimport.network
crond         network       rsyncd        wazuh-indexer
grub          network-scripts rsyslog
htcacheclean nfs            run-parts
[root@wazuh-server sysconfig]# cd network-scripts
[root@wazuh-server network-scripts]#
```

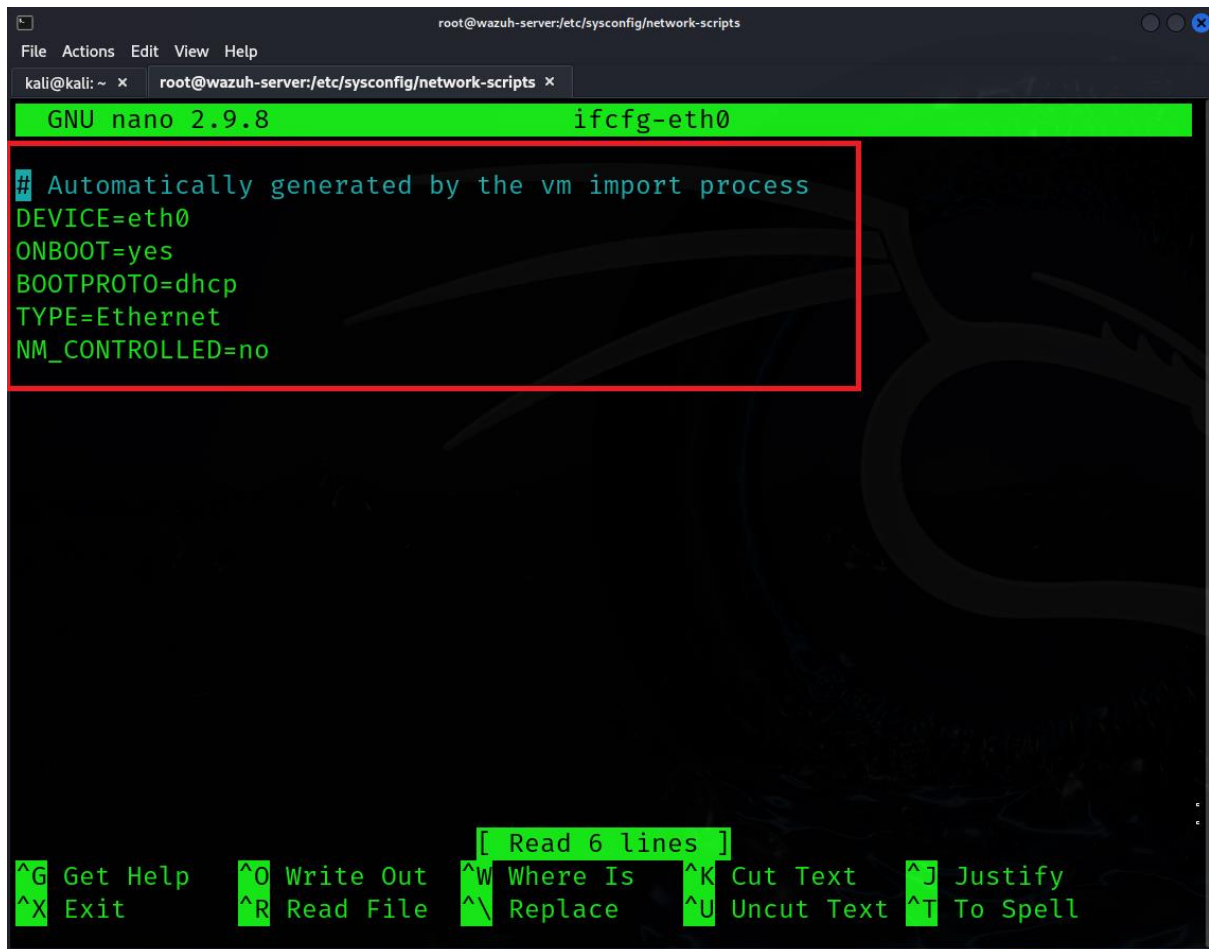
Step 04: Edit the file “ifcfg-eth0”

Command: nano ifcfg-eth0



```
root@wazuh-server/etc/sysconfig/network-scripts
File Actions Edit View Help
kali@kali: ~ x root@wazuh-server/etc/sysconfig/network-scripts x
[root@wazuh-server network-scripts]# ls
ifcfg-eth0    ifdown-isdn    ifup-aliases  ifup-ppp
ifcfg-lo      ifdown-post    ifup-bnep     ifup-routes
ifdown        ifdown-ppp     ifup-eth      ifup-sit
ifdown-Team   ifdown-routes  ifup-ipppp    ifup-tunnel
ifdown-TeamPort ifdown-sit     ifup-ipv6     ifup-wireless
ifdown-bnep   ifdown-tunnel  ifup-isdn     init.ipv6-global
ifdown-eth    ifup           ifup-plip     network-functions
ifdown-ipppp  ifup-Team      ifup-plusb    network-functions-ipv6
ifdown-ipv6   ifup-TeamPort  ifup-post     vmimport.ifcfg-eth0
[root@wazuh-server network-scripts]# nano ifcfg-eth0
```

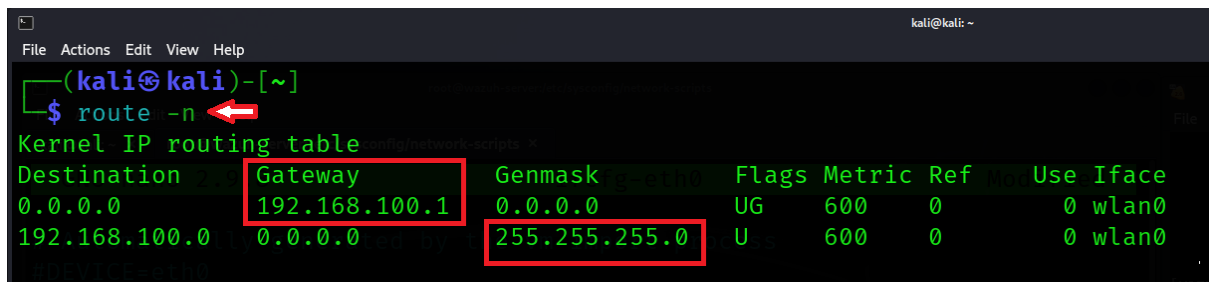
Here is the default configuration of file “ifcfg-eth0”



```
root@wazuh-server:/etc/sysconfig/network-scripts
File Actions Edit View Help
kali@kali: ~ x root@wazuh-server:/etc/sysconfig/network-scripts x
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
```

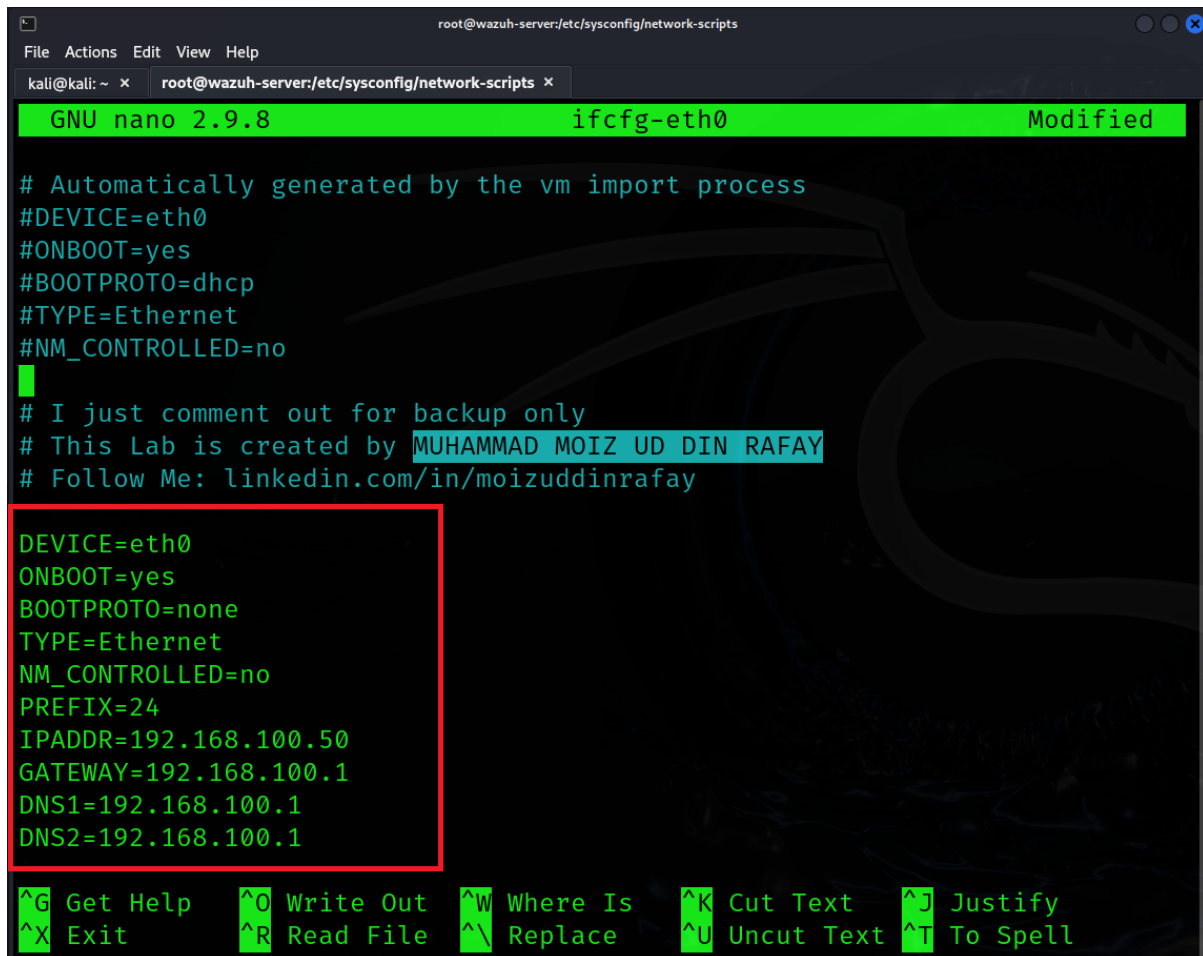
Gateway= 192.168.100.1

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)



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

# Automatically generated by the vm import process
#DEVICE=eth0
#ONBOOT=yes
#BOOTPROTO=dhcp
#TYPE=Ethernet
#NM_CONTROLLED=no
#
# I just comment out for backup only
# This Lab is created by MUHAMMAD MOIZ UD DIN RAFAY
# Follow Me: linkedin.com/in/moizuddinrafay

DEVICE=eth0
ONBOOT=yes
BOOTPROTO=none
TYPE=Ethernet
NM_CONTROLLED=no
PREFIX=24
IPADDR=192.168.100.50
GATEWAY=192.168.100.1
DNS1=192.168.100.1
DNS2=192.168.100.1

^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
```

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”

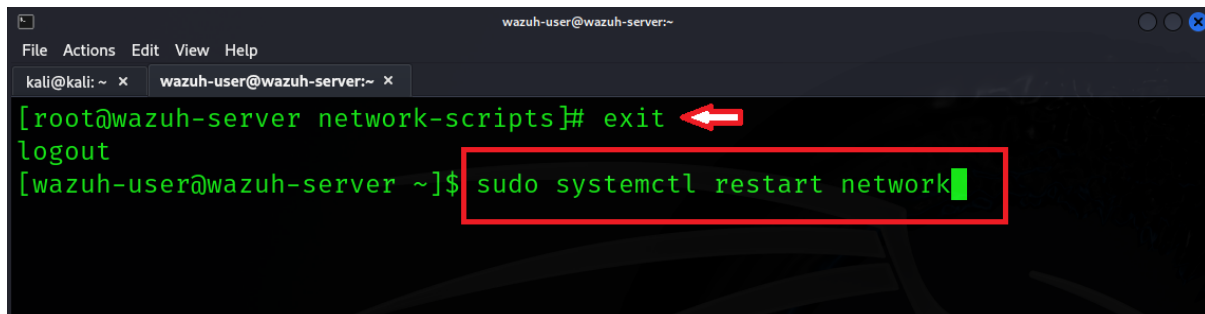
GATEWAY=192.168.100.1

DNS1=192.168.100.1

DNS2=192.168.100.1

Step 07: Now exit from root login and restart network.

Command: `sudo systemctl restart network`



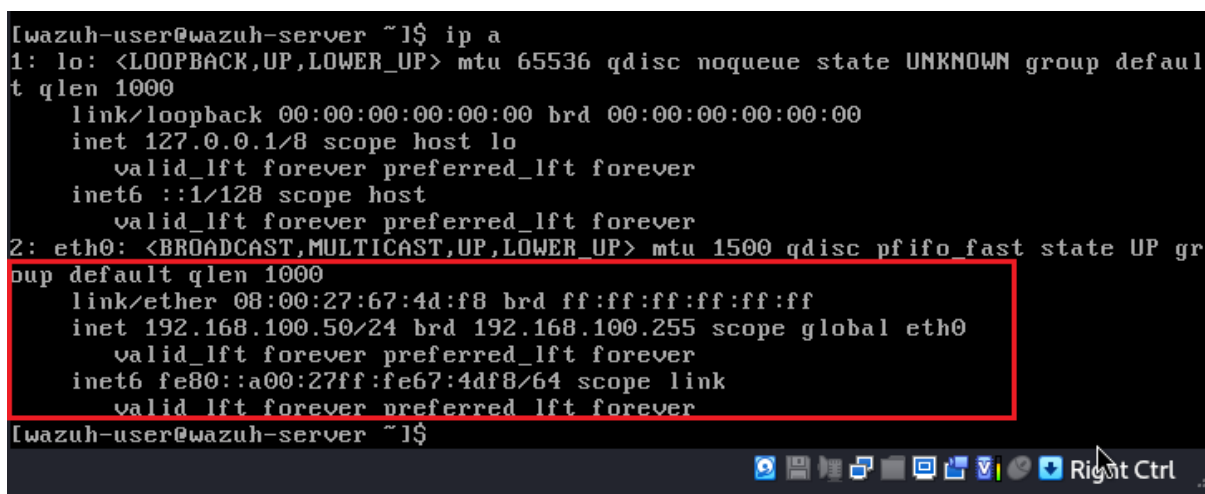
```
wazuh-user@wazuh-server:~  
File Actions Edit View Help  
kali@kali: ~ x wazuh-user@wazuh-server: ~ x  
[root@wazuh-server network-scripts]# exit  
logout  
[wazuh-user@wazuh-server ~]$ sudo systemctl restart network
```

Network is restarting.



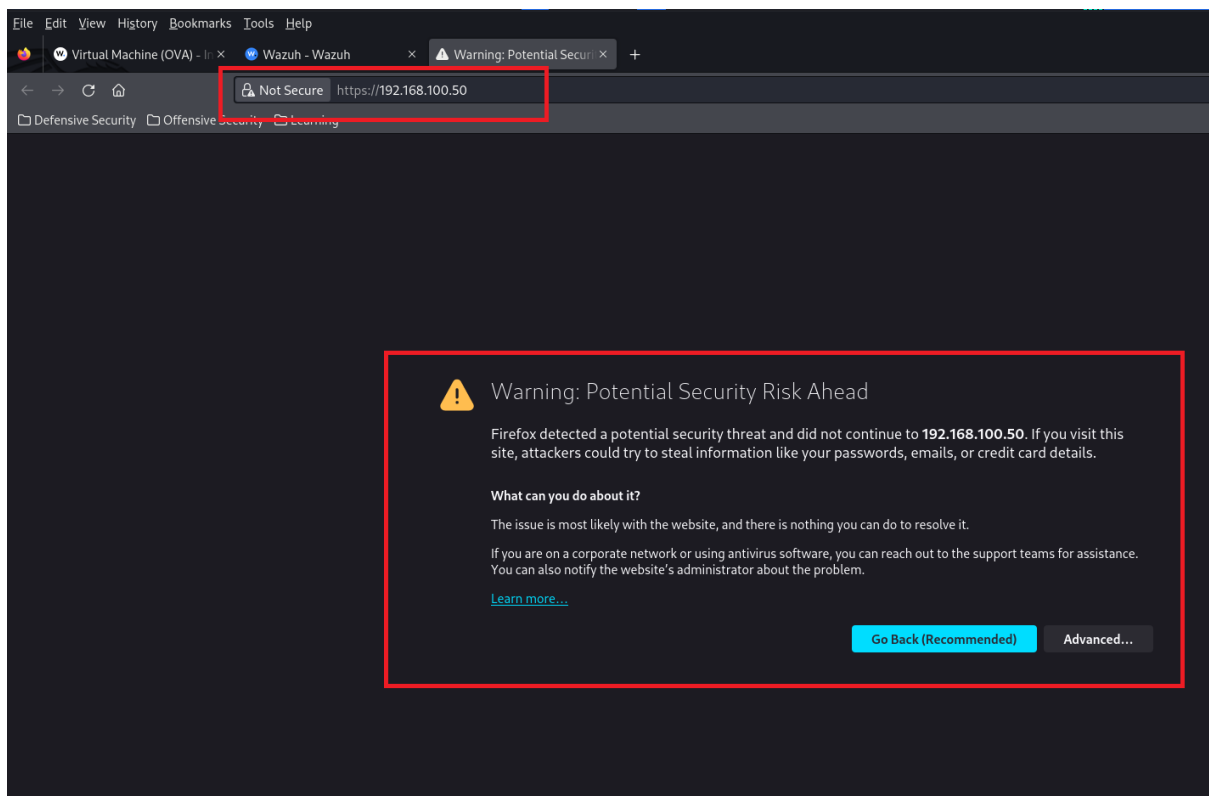
```
[wazuh-user@wazuh-server ~]$ [ 1378.499032] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready  
[ 1380.524428] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX  
[ 1380.530628] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready  
[wazuh-user@wazuh-server ~]$
```

Here is New Static IP Address.

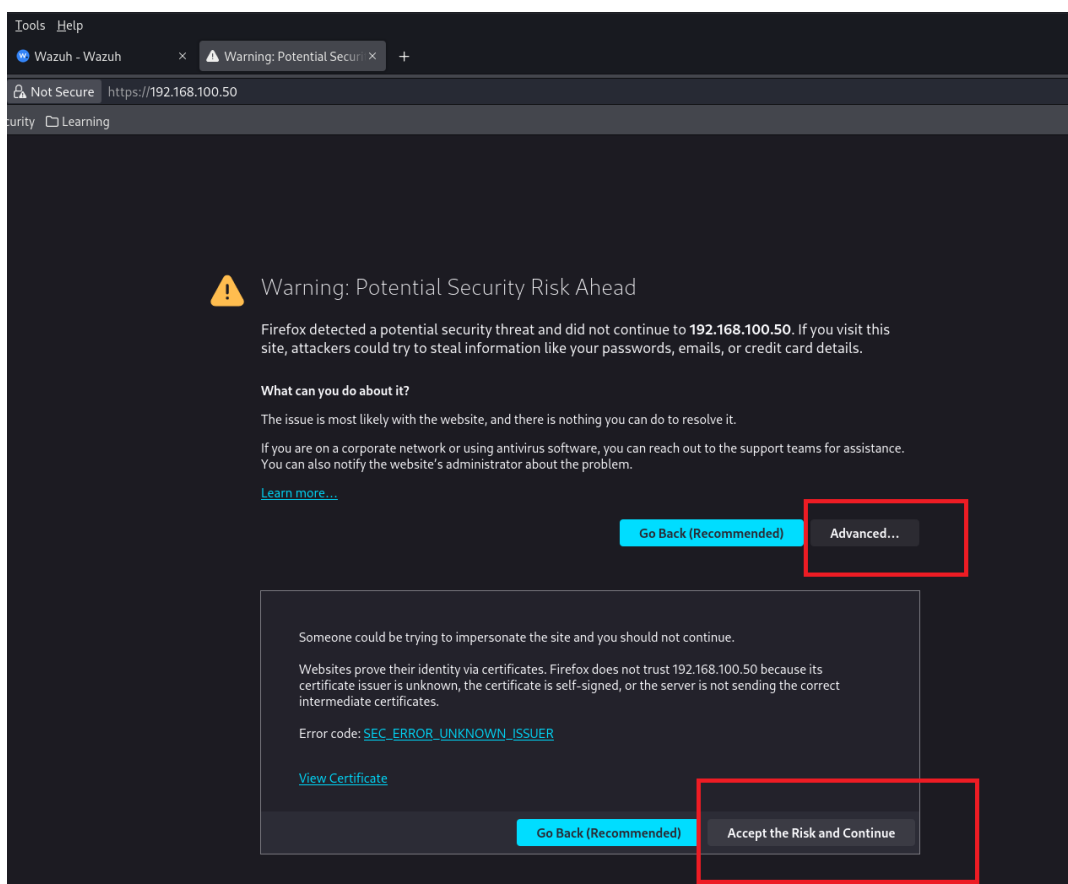


```
[wazuh-user@wazuh-server ~]$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
    link/ether 08:00:27:67:4d:f8 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.100.50/24 brd 192.168.100.255 scope global eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::a00:27ff:fe67:4df8/64 scope link  
        valid_lft forever preferred_lft forever  
[wazuh-user@wazuh-server ~]$
```

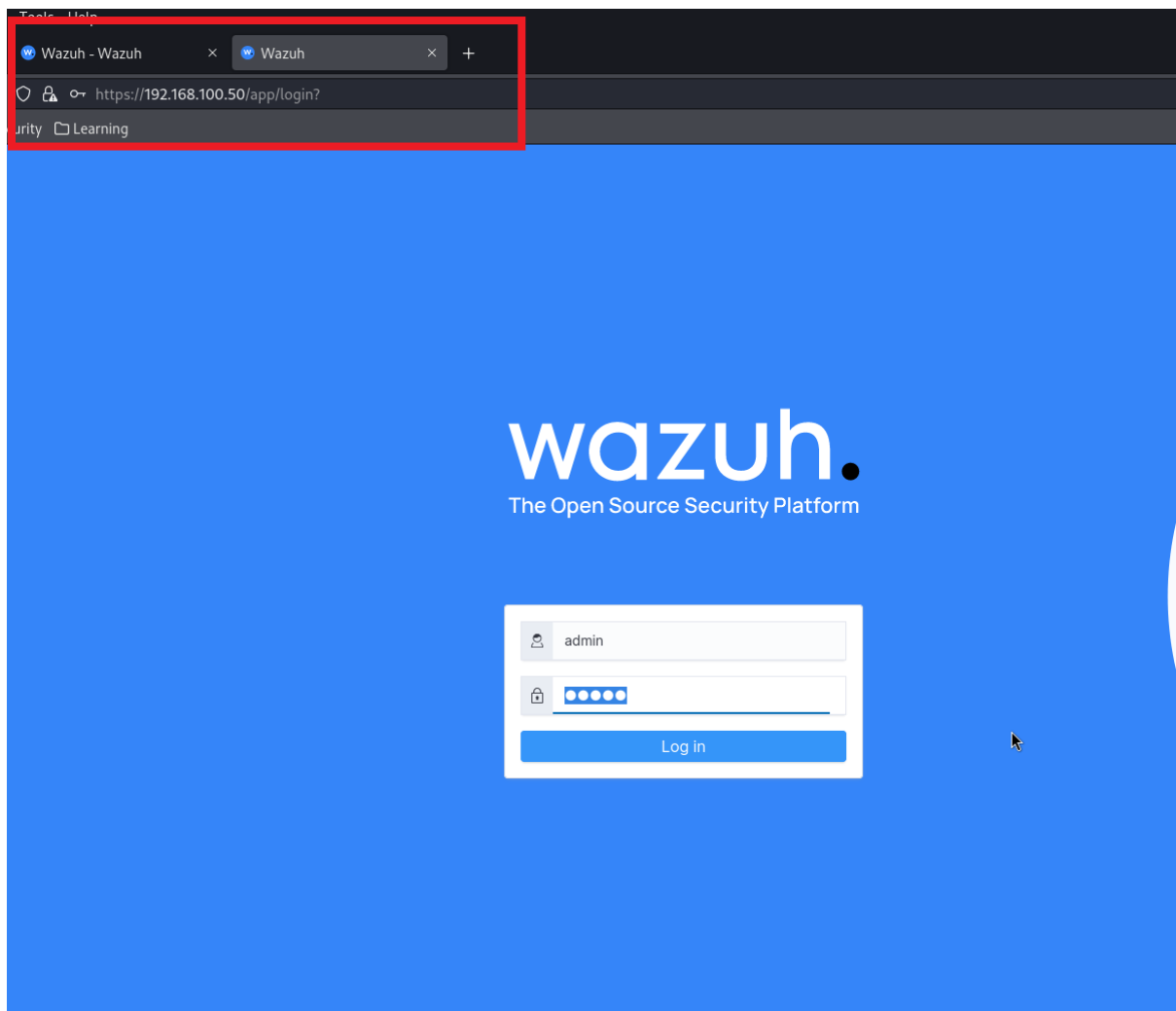
Step 08: Now access with browser by typing IP Address in URL bar.



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.