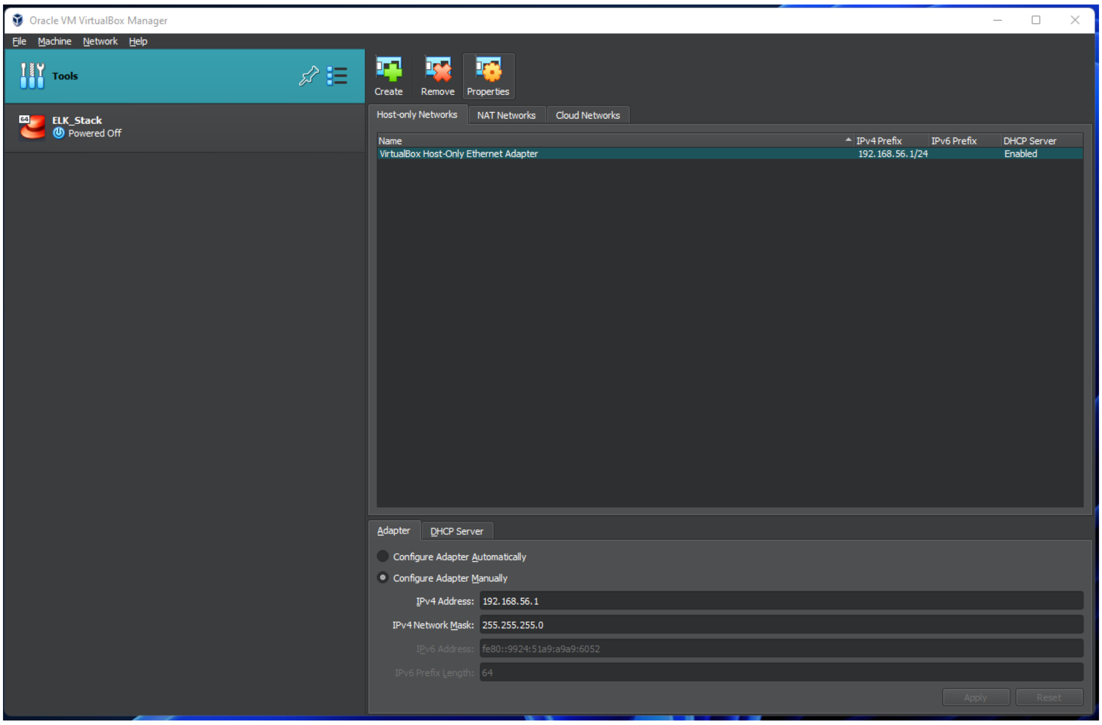


Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
VirtualBox Host-Only Ethernet Adapter	192.168.56.1/24		Enabled

○ Configure Adapter Automatically

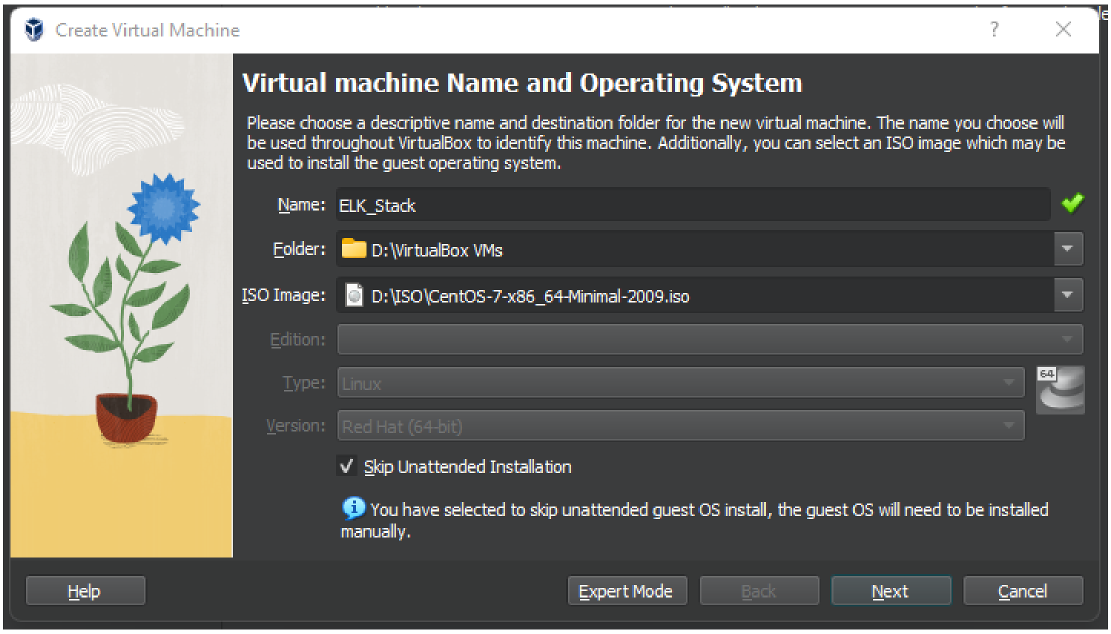
● Configure Adapter Manually

IPv4 Address: 192.168.56.1

IPv4 Network Mask: 255.255.255.0

IPv6 Address: fe80::9924:51a9:a9a9:6052

IPv6 Prefix Length: 64



Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: ELK_Stack

Folder: D:\VirtualBox VMs

ISO Image: D:\ISO\CentOS-7-x86_64-Minimal-2009.iso

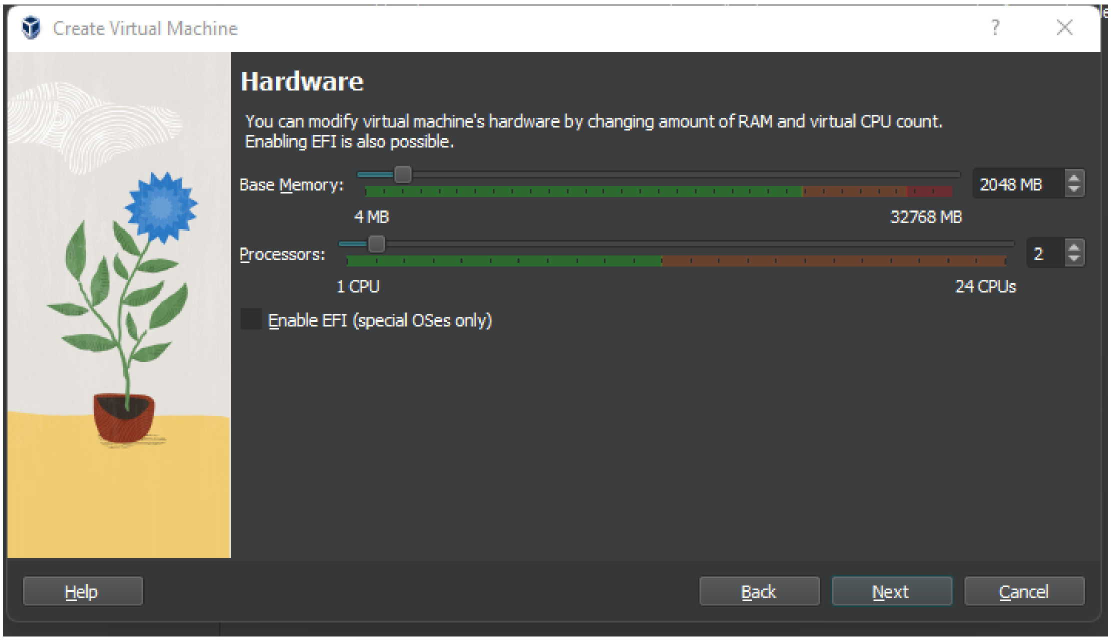
Edition:

Type: Linux

Version: Red Hat (64-bit)

☑ Skip Unattended Installation

You have selected to skip unattended guest OS install, the guest OS will need to be installed manually.



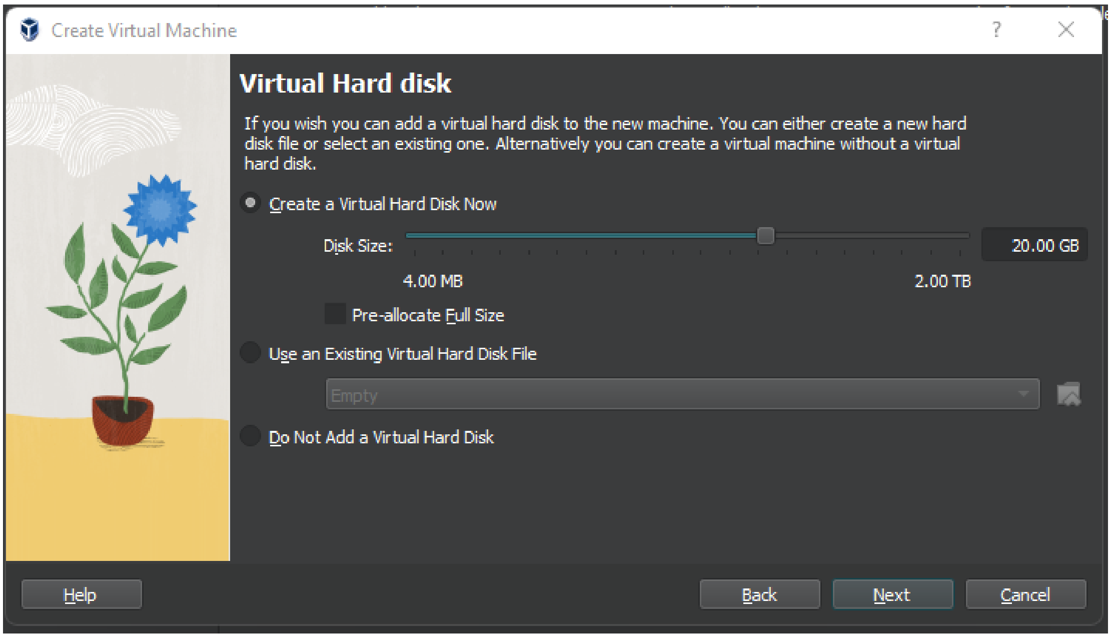
Hardware

You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 2048 MB

Processors: 2

□ Enable EFI (special OSes only)



Create Virtual Machine

Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

● Create a Virtual Hard Disk Now

Disk Size: 20.00 GB

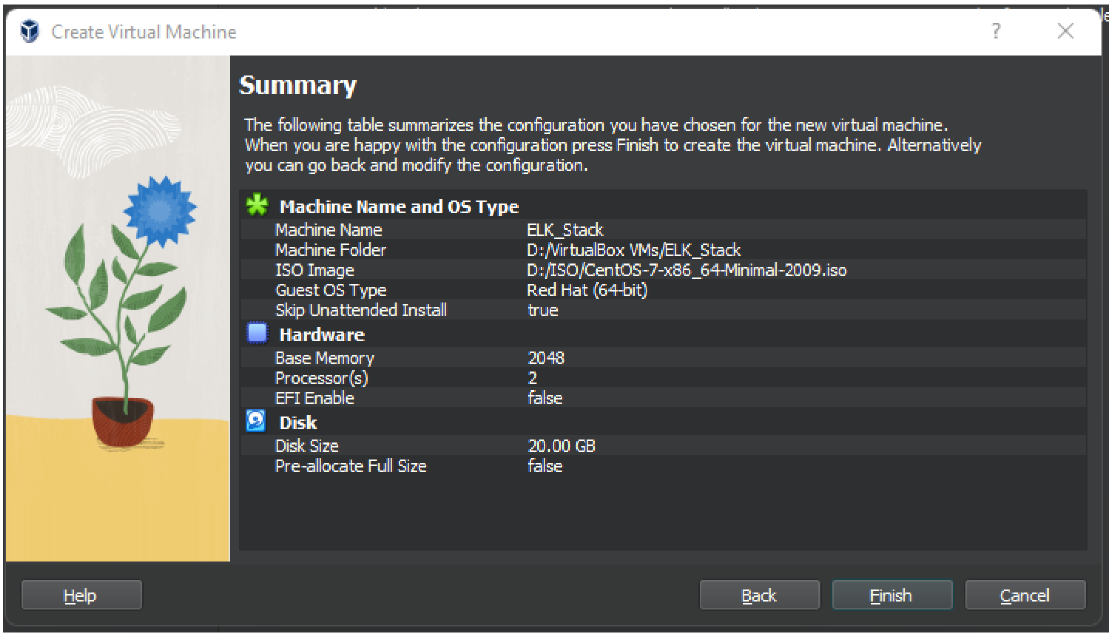
4.00 MB — 2.00 TB

□ Pre-allocate Full Size

○ Use an Existing Virtual Hard Disk File

Empty

○ Do Not Add a Virtual Hard Disk

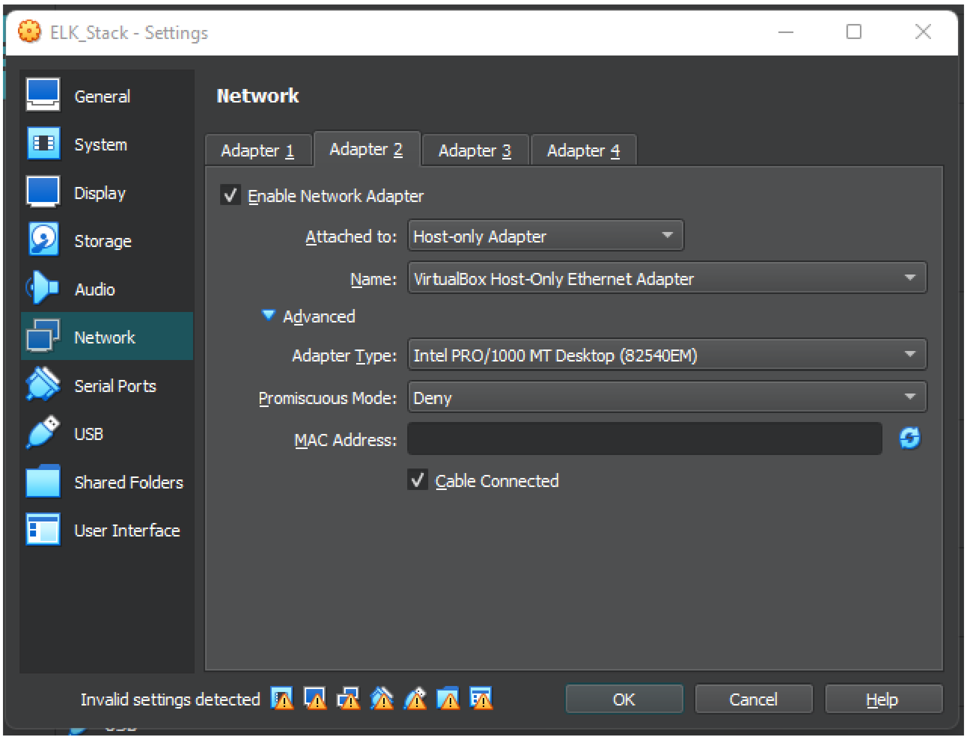


Create Virtual Machine

Summary

The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

Machine Name and OS Type	
Machine Name	ELK_Stack
Machine Folder	D:/VirtualBox VMs/ELK_Stack
ISO Image	D:/ISO/CentOS-7-x86_64-Minimal-2009.iso
Guest OS Type	Red Hat (64-bit)
Skip Unattended Install	true
Hardware	
Base Memory	2048
Processor(s)	2
EFI Enable	false
Disk	
Disk Size	20.00 GB
Pre-allocate Full Size	false



ELK_Stack - Settings

Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

▾ Advanced

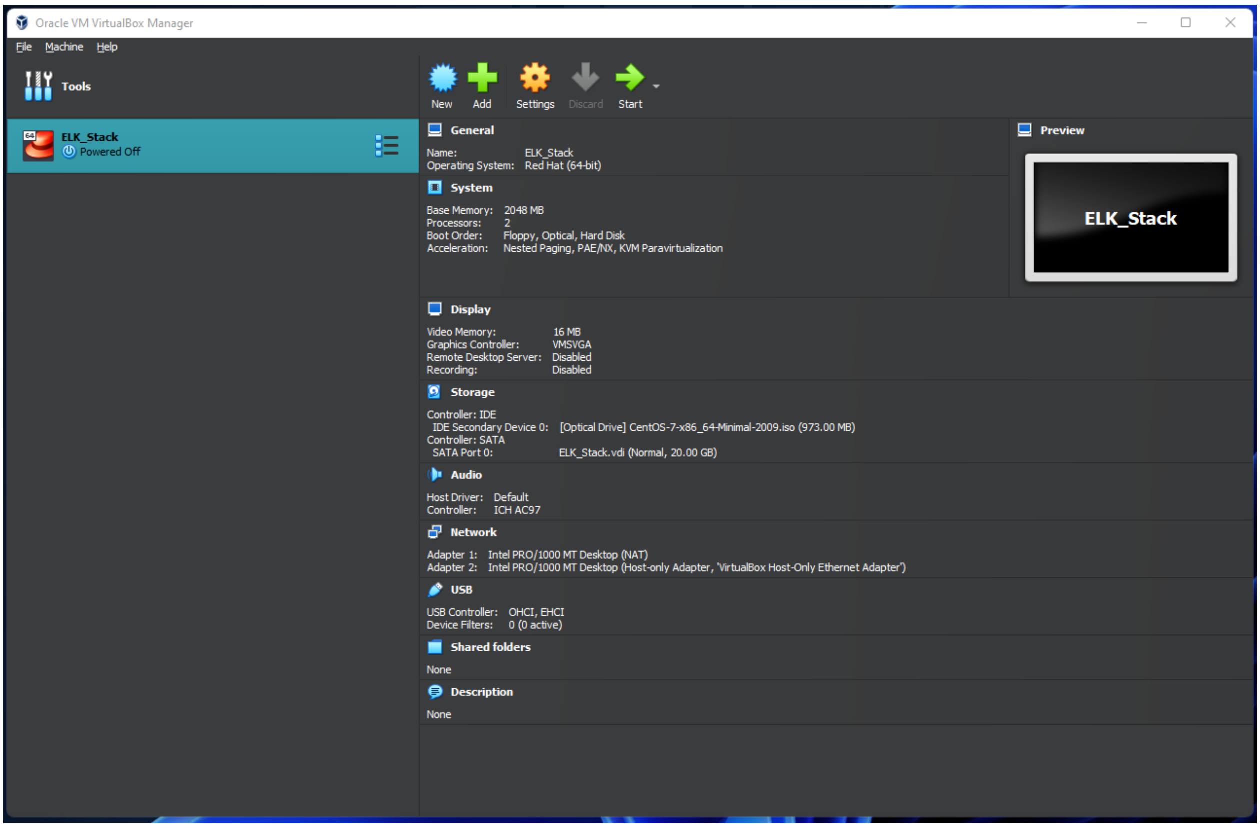
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address:

☑ Cable Connected

Invalid settings detected



General

Name: ELK_Stack
Operating System: Red Hat (64-bit)

System

Base Memory: 2048 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] CentOS-7-x86_64-Minimal-2009.iso (973.00 MB)
Controller: SATA
SATA Port 0: ELK_Stack.vdi (Normal, 20.00 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)
Adapter 2: Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter')

USB

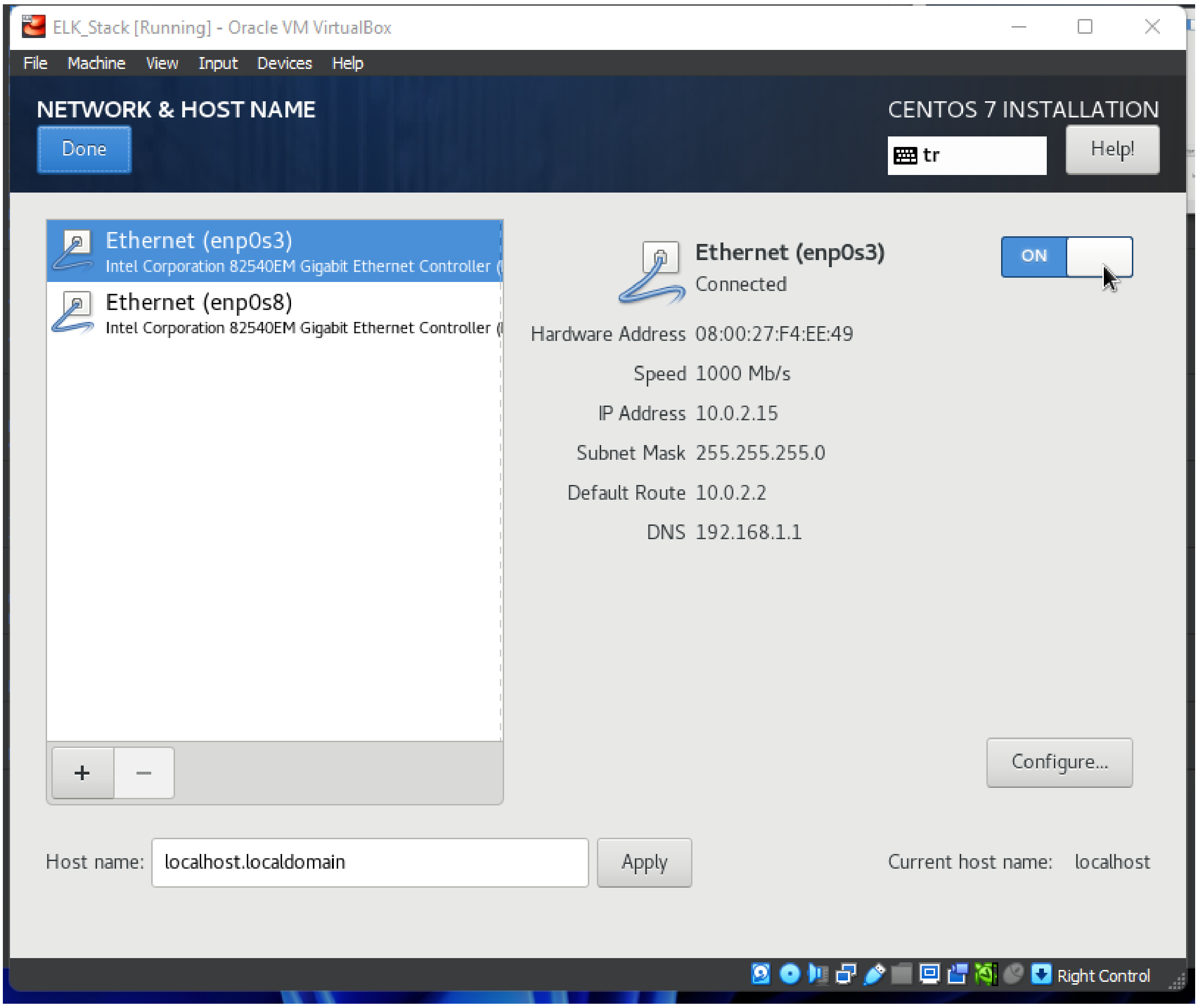
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

None



Ethernet (enp0s3)
Intel Corporation 82540EM Gigabit Ethernet Controller (

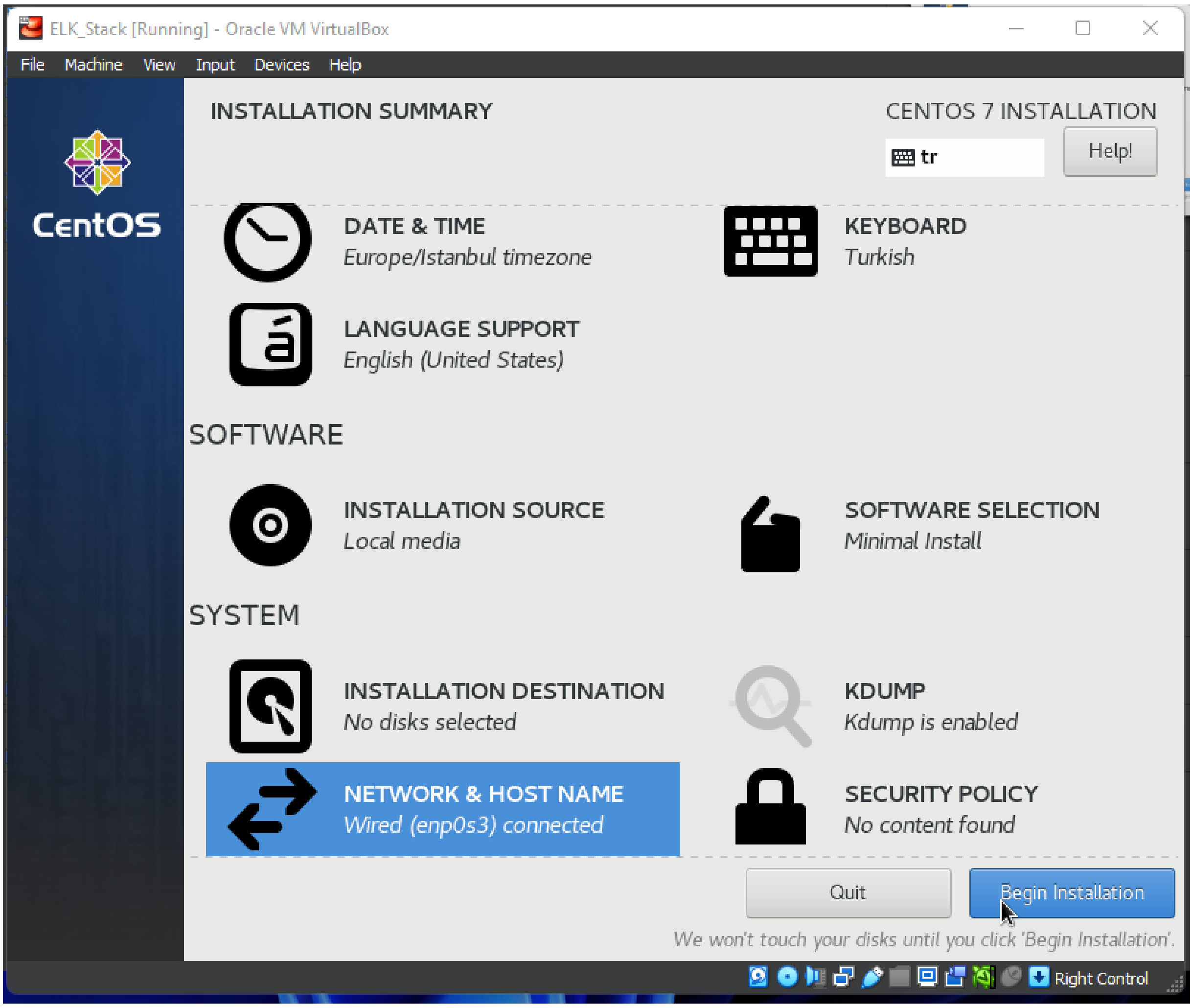
Ethernet (enp0s8)
Intel Corporation 82540EM Gigabit Ethernet Controller (

Ethernet (enp0s3)
Connected

Hardware Address 08:00:27:F4:EE:49
Speed 1000 Mb/s
IP Address 10.0.2.15
Subnet Mask 255.255.255.0
Default Route 10.0.2.2
DNS 192.168.1.1

Host name: localhost.localdomain

Current host name: localhost



ELK_Stack [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
CentOS
tr
Help!
Quit
Begin Installation
Right Control

INSTALLATION SUMMARY

CENTOS 7 INSTALLATION

DATE & TIME
Europe/Istanbul timezone

KEYBOARD
Turkish

LANGUAGE SUPPORT
English (United States)

SOFTWARE

INSTALLATION SOURCE
Local media

SOFTWARE SELECTION
Minimal Install

SYSTEM

INSTALLATION DESTINATION
No disks selected

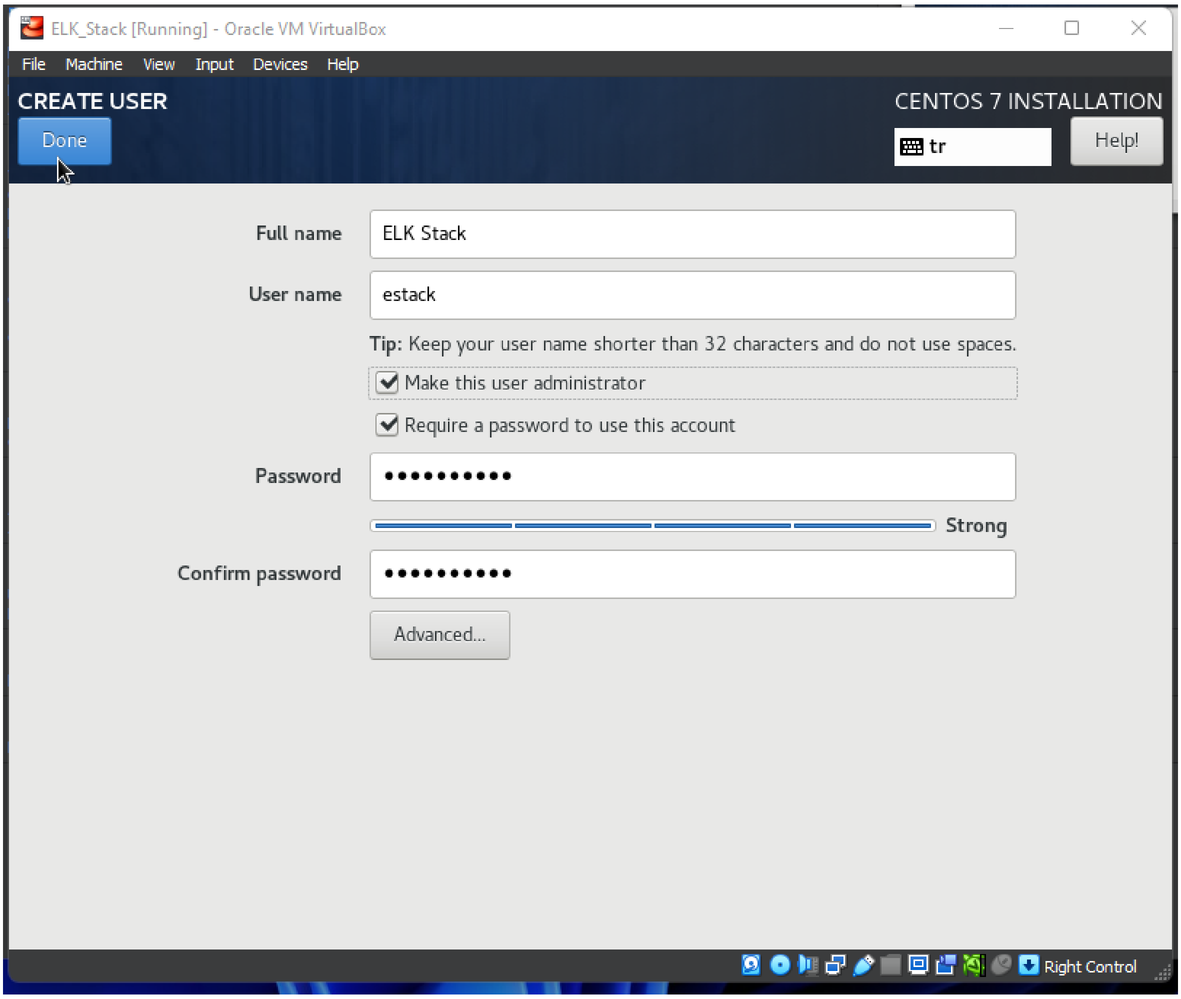
KDUMP
Kdump is enabled

NETWORK & HOST NAME
Wired (enp0s3) connected

SECURITY POLICY
No content found

We won't touch your disks until you click 'Begin Installation'.

Date & Time	: Istanbul timezone
Keyboard	: Turkish
Insatallation Source	: Local Media
Software Selection	: Minimal (Automatic)
Network	: Wired
Root Password	: havelsan06
User Name	: estack (Administrator)
Estack Password	: havelsan57



ELK_Stack [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
CENTOS 7 INSTALLATION
tr
Help!
Done
Advanced...
Right Control

CREATE USER

Full name: ELK Stack

User name: estack

Tip: Keep your user name shorter than 32 characters and do not use spaces.

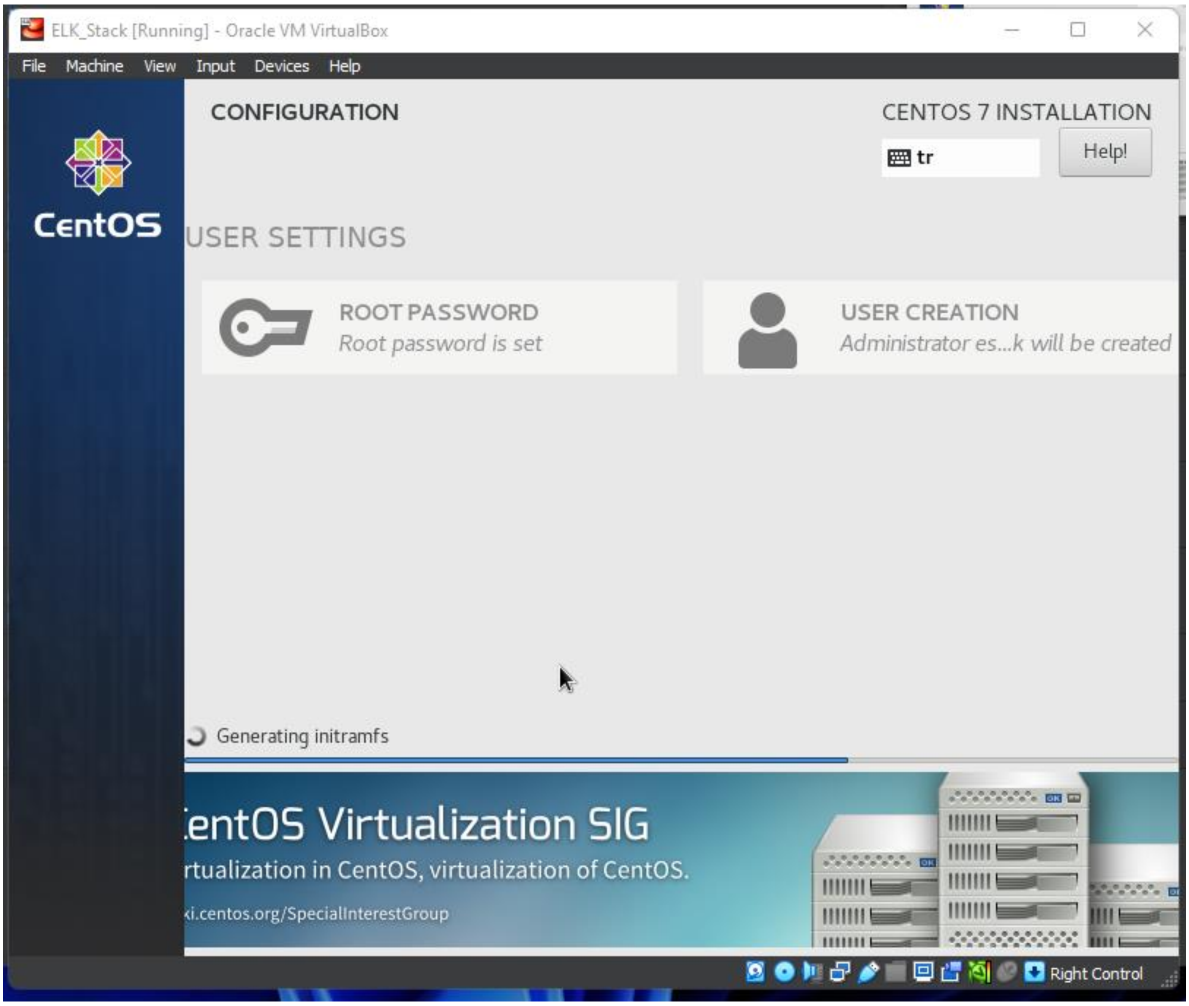
☑ Make this user administrator

☑ Require a password to use this account

Password: ••••••••••

Strong

Confirm password: ••••••••••



ELK_Stack [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
CentOS
CENTOS 7 INSTALLATION
tr
Help!
entOS Virtualization SIG
rtualization in CentOS, virtualization of CentOS.
i.centos.org/SpecialInterestGroup
Right Control

CONFIGURATION

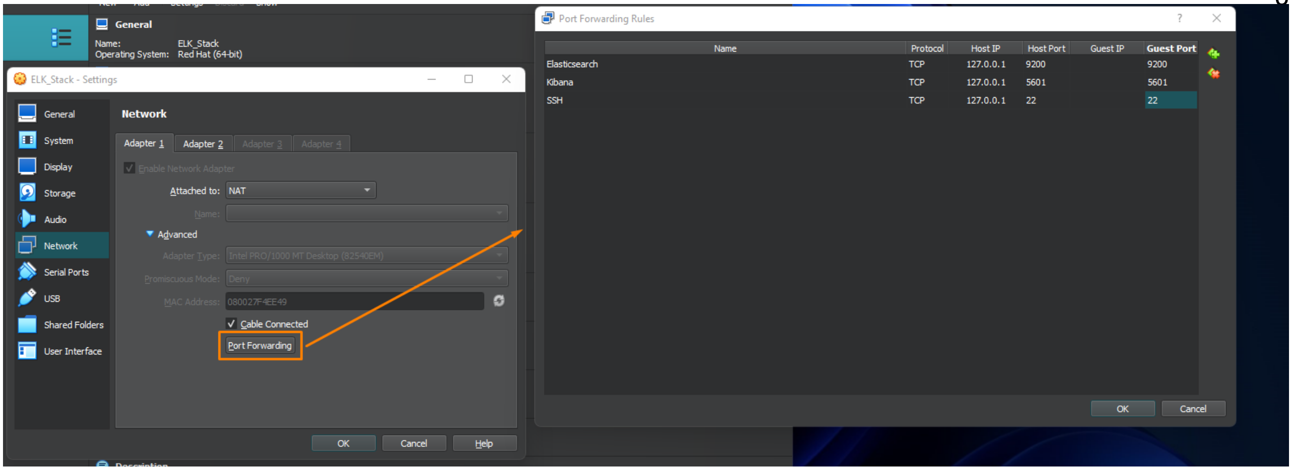
USER SETTINGS

ROOT PASSWORD
Root password is set

USER CREATION
Administrator es...k will be created

Generating initramfs

Port Forwarding

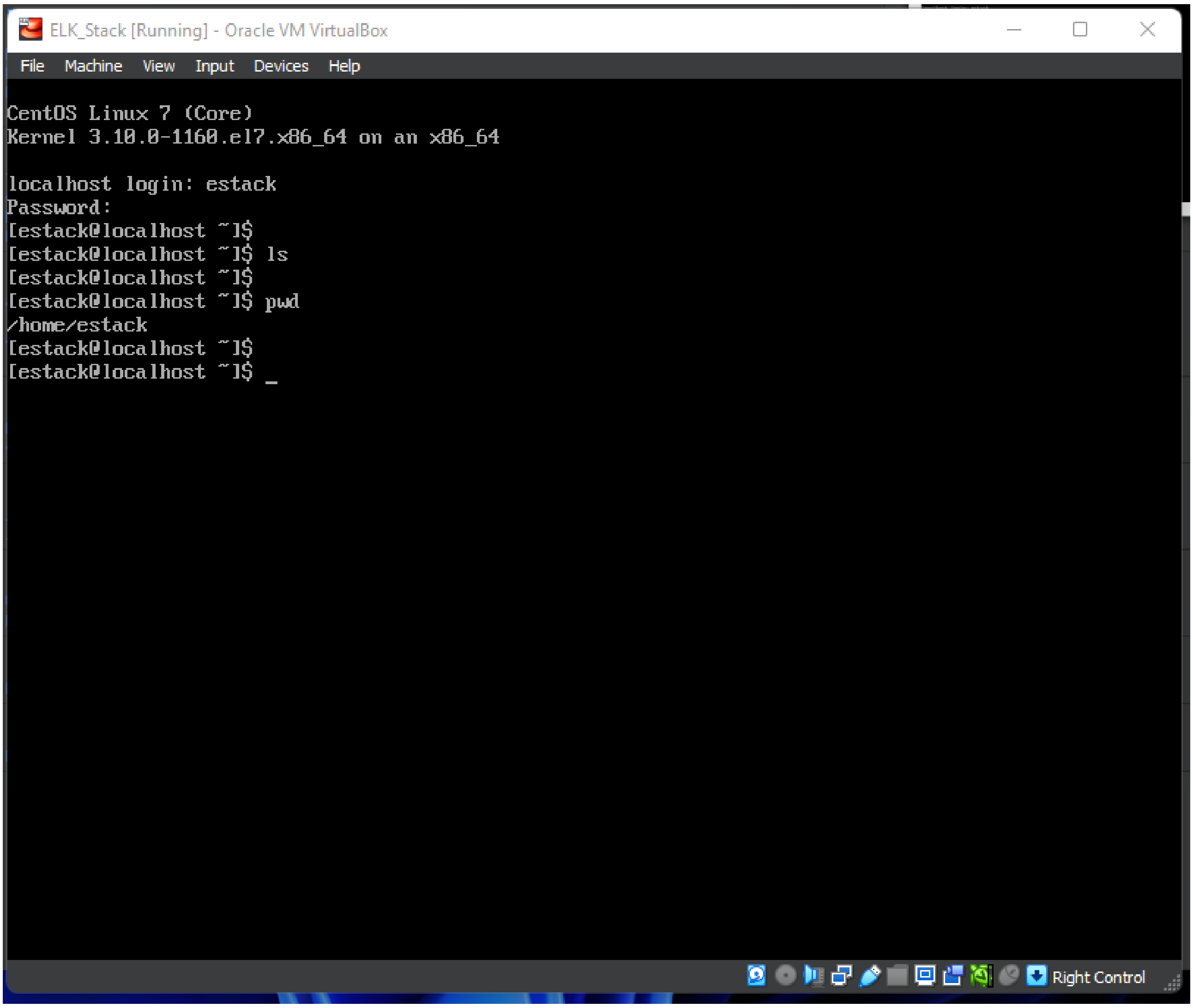


Name: ELK_Stack
Operating System: Red Hat (64-bit)

☑ Enable Network Adapter
Attached to: NAT
Name:
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
MAC Address: 080027F4EE49
☑ Cable Connected

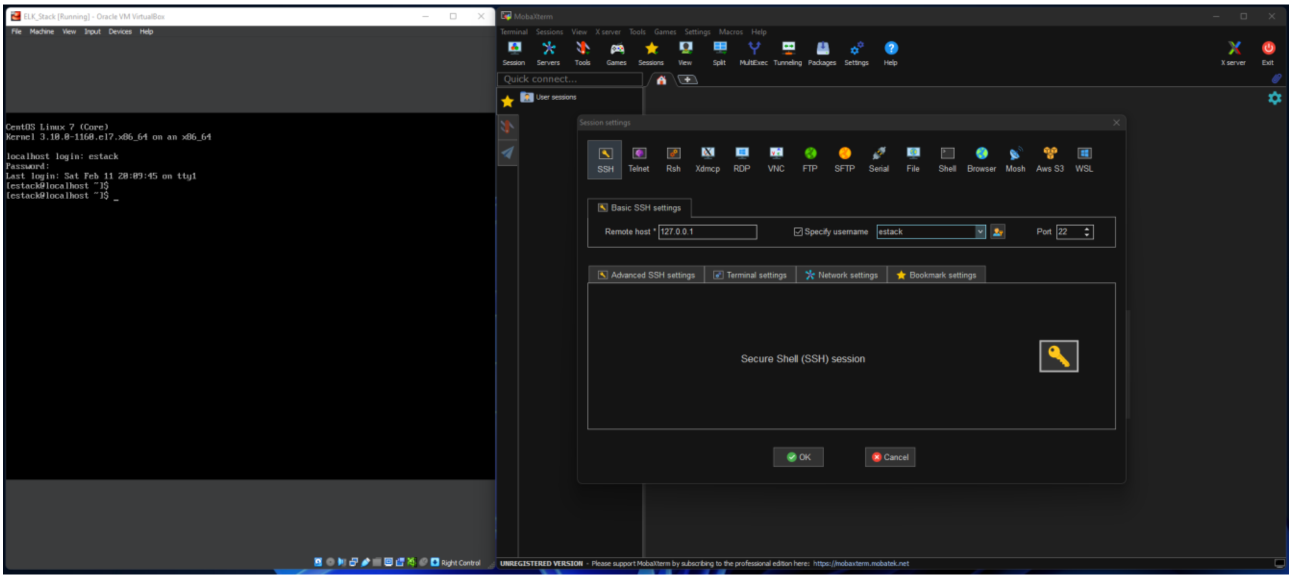
Name	Protocol	Host IP	Host Port	Guest IP	Guest Port
Elasticsearch	TCP	127.0.0.1	9200		9200
Kibana	TCP	127.0.0.1	5601		5601
SSH	TCP	127.0.0.1	22		22

Start Machine



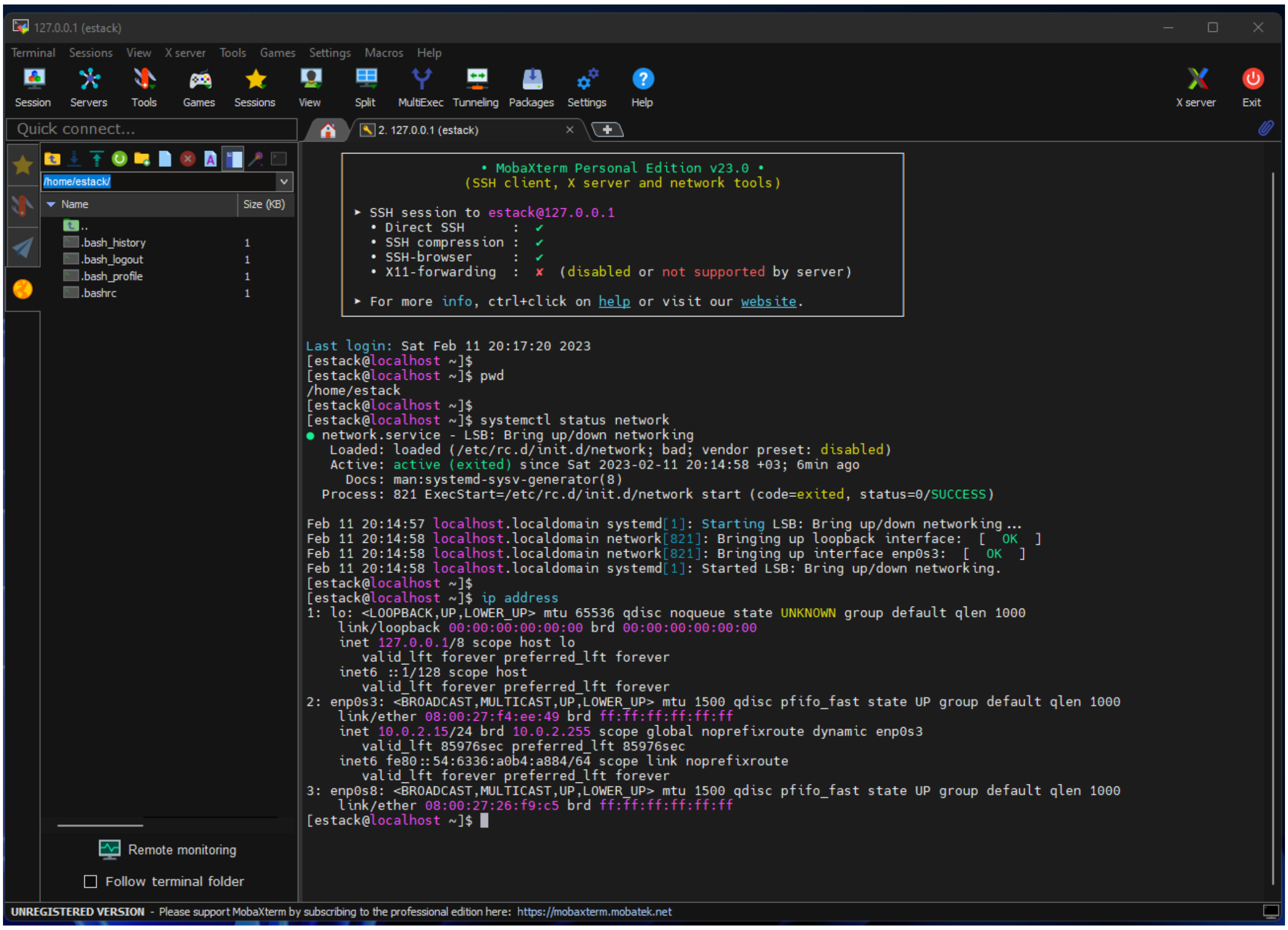
```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.el7.x86_64 on an x86_64

localhost login: estack
Password:
[estack@localhost ~]$
[estack@localhost ~]$ ls
[estack@localhost ~]$
[estack@localhost ~]$ pwd
/home/estack
[estack@localhost ~]$
[estack@localhost ~]$ _
```

Setup Link: https://mobaxterm.mobatek.net/download-home-edition.html


ELK_Stack [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
MobaXterm
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
User sessions
Session settings
SSH Telnet Rsh Xdmcp RDP VNC FTP SFTP Serial File Shell Browser Mosh Aws S3 WSL
Basic SSH settings
Advanced SSH settings
Terminal settings
Network settings
Bookmark settings
Secure Shell (SSH) session
OK
Cancel
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.el7.x86_64 on an x86_64

localhost login: estack
Password:
Last login: Sat Feb 11 20:09:45 on tty1
[estack@localhost ~]$
[estack@localhost ~]$ _
```

Remote host * 127.0.0.1 ☑ Specify username estack Port 22


127.0.0.1 (estack)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. 127.0.0.1 (estack)
/home/estack/
Name
Size (KB)
..
.bash_history 1
.bash_logout 1
.bash_profile 1
.bashrc 1
Remote monitoring
□ Follow terminal folder
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```
              • MobaXterm Personal Edition v23.0 •
            (SSH client, X server and network tools)

 ▸ SSH session to estack@127.0.0.1
   • Direct SSH      :  ✓
   • SSH compression :  ✓
   • SSH-browser     :  ✓
   • X11-forwarding  :  ✘  (disabled or not supported by server)

 ▸ For more info, ctrl+click on help or visit our website.

Last login: Sat Feb 11 20:17:20 2023
[estack@localhost ~]$
[estack@localhost ~]$ pwd
/home/estack
[estack@localhost ~]$
[estack@localhost ~]$ systemctl status network
● network.service - LSB: Bring up/down networking
   Loaded: loaded (/etc/rc.d/init.d/network; bad; vendor preset: disabled)
   Active: active (exited) since Sat 2023-02-11 20:14:58 +03; 6min ago
     Docs: man:systemd-sysv-generator(8)
  Process: 821 ExecStart=/etc/rc.d/init.d/network start (code=exited, status=0/SUCCESS)

Feb 11 20:14:57 localhost.localdomain systemd[1]: Starting LSB: Bring up/down networking...
Feb 11 20:14:58 localhost.localdomain network[821]: Bringing up loopback interface:  [  OK  ]
Feb 11 20:14:58 localhost.localdomain network[821]: Bringing up interface enp0s3:  [  OK  ]
Feb 11 20:14:58 localhost.localdomain systemd[1]: Started LSB: Bring up/down networking.
[estack@localhost ~]$
[estack@localhost ~]$ ip address
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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:f4:ee:49 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global noprefixroute dynamic enp0s3
       valid_lft 85976sec preferred_lft 85976sec
    inet6 fe80::54:6336:a0b4:a884/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:26:f9:c5 brd ff:ff:ff:ff:ff:ff
[estack@localhost ~]$
```

[estack@localhost ~]$ ip address

[estack@localhost ~]$ systemctl status network

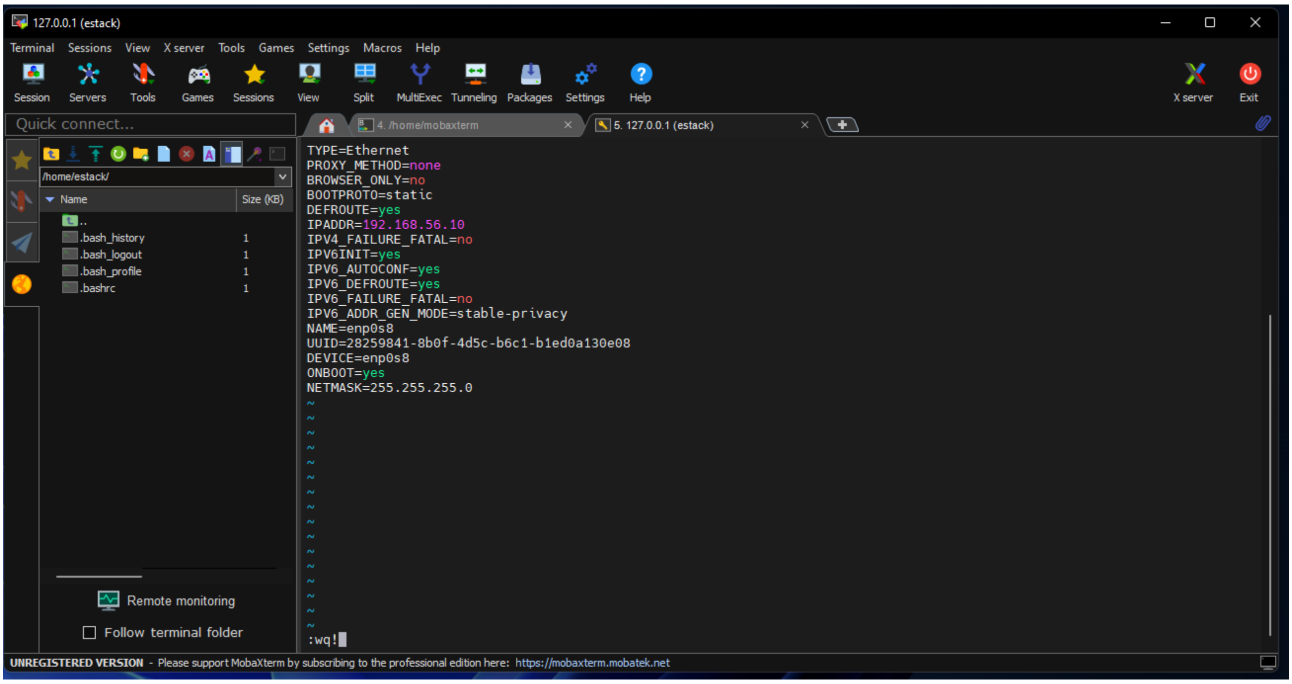
[estack@localhost ~]$ ip address

[estack@localhost ~]$ sudo vi /etc/sysconfig/network-scripts/ifcfg-enp0s8

```
DEVICE=enp0s8
BOOTPROTO=static
ONBOOT=yes
IPADDR=192.168.56.10
NETMASK=255.255.255.0
```

vi Editor Kullanımı

Dosya içerisindeki değişikleri kaydetmek : ESC - :wq! – ENTER
Dosya içerisindeki değişikleri kaydetmeden çıkmak : ESC - :q! – ENTER



```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=yes
IPADDR=192.168.56.10
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=enp0s8
UUID=28259841-8b0f-4d5c-b6c1-b1ed0a130e08
DEVICE=enp0s8
ONBOOT=yes
NETMASK=255.255.255.0
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:wq!
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

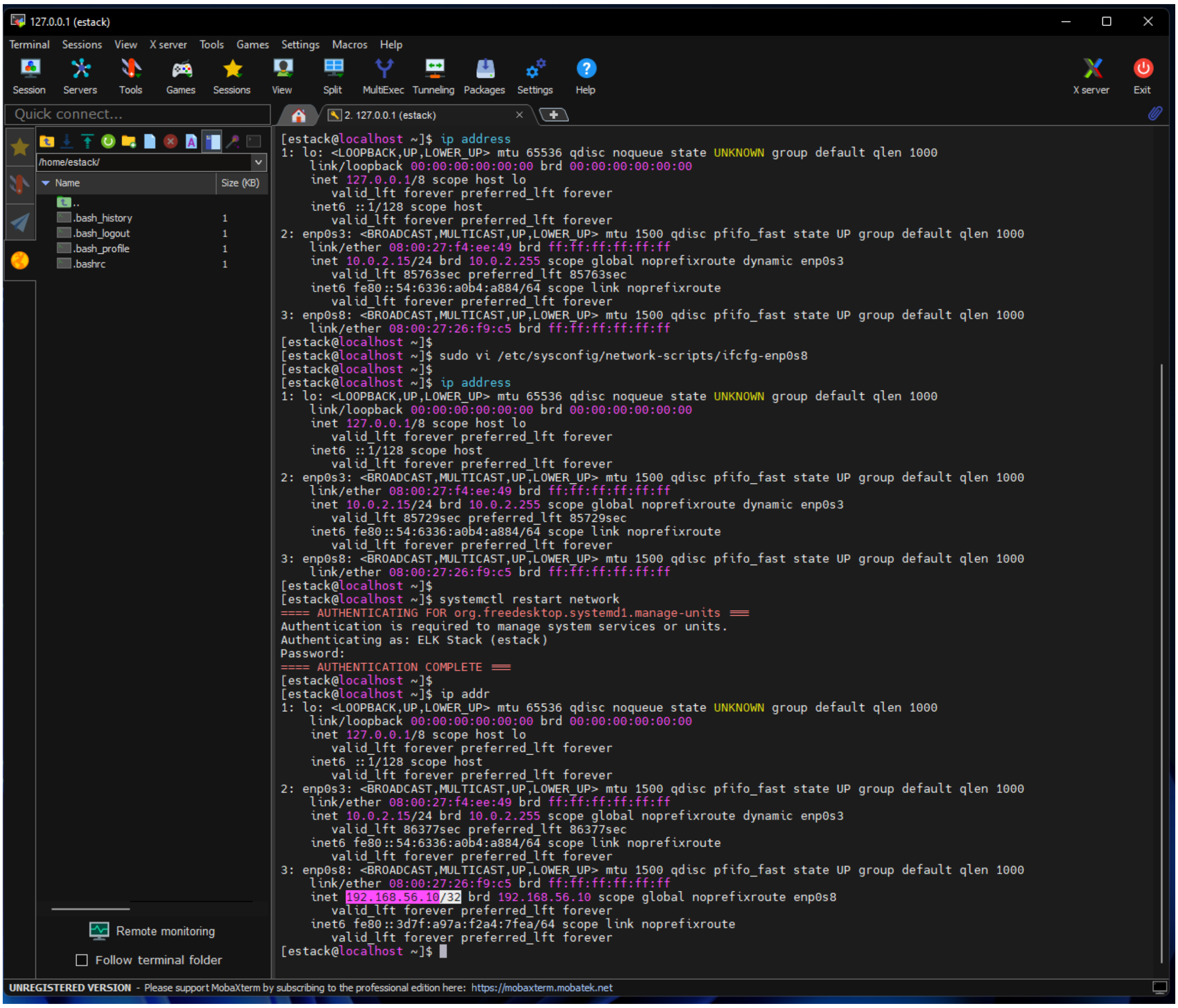
[estack@localhost ~]$ systemctl restart network

[estack@localhost ~]$ systemctl status network

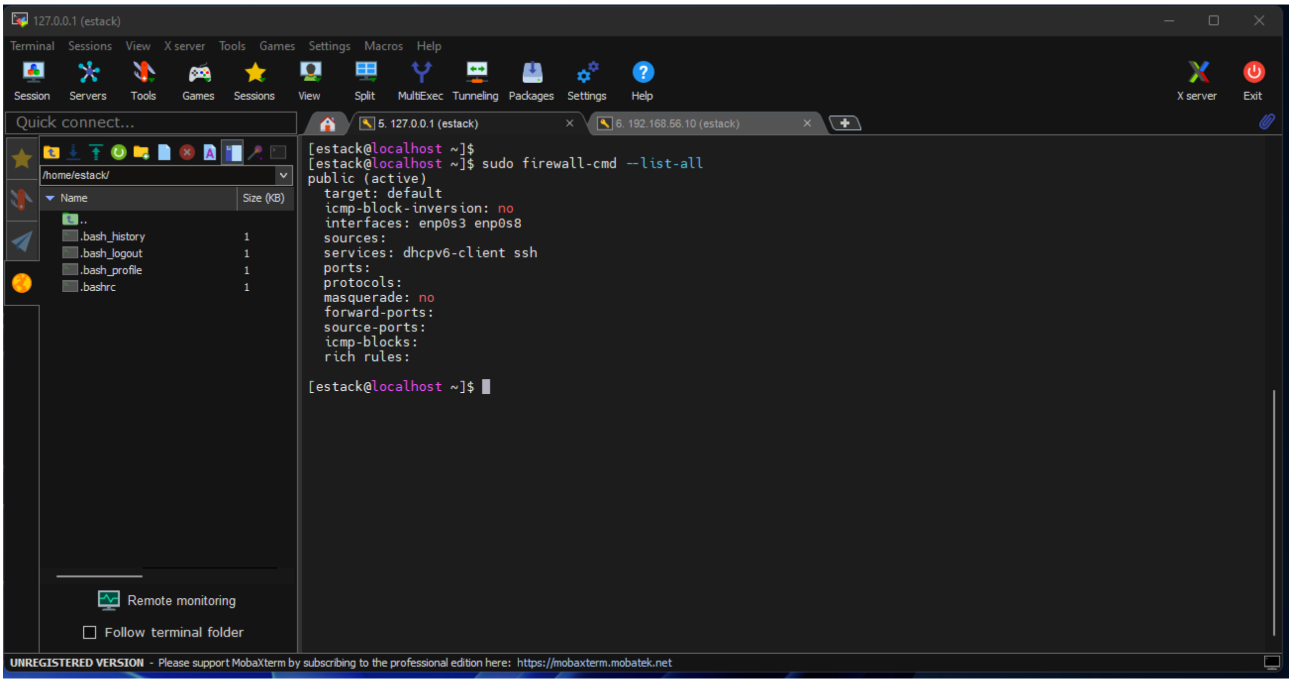
[estack@localhost ~]$ ip address

[estack@localhost ~]$ sudo systemctl stop firewalld.service && systemctl disable firewalld.service

- sudo nano /etc/sysconfig/selinux [Disable]
- reboot


127.0.0.1 (estack)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. 127.0.0.1 (estack)
/home/estack/
Name
Size (KB)
..
.bash_history 1
.bash_logout 1
.bash_profile 1
.bashrc 1
Remote monitoring
☐ Follow terminal folder
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```
[estack@localhost ~]$ ip address
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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:f4:ee:49 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global noprefixroute dynamic enp0s3
       valid_lft 85763sec preferred_lft 85763sec
    inet6 fe80::54:6336:a0b4:a884/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:26:f9:c5 brd ff:ff:ff:ff:ff:ff
[estack@localhost ~]$
[estack@localhost ~]$ sudo vi /etc/sysconfig/network-scripts/ifcfg-enp0s8
[estack@localhost ~]$
[estack@localhost ~]$ ip address
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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:f4:ee:49 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global noprefixroute dynamic enp0s3
       valid_lft 85729sec preferred_lft 85729sec
    inet6 fe80::54:6336:a0b4:a884/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:26:f9:c5 brd ff:ff:ff:ff:ff:ff
[estack@localhost ~]$
[estack@localhost ~]$ systemctl restart network
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to manage system services or units.
Authenticating as: ELK Stack (estack)
Password:
==== AUTHENTICATION COMPLETE ===
[estack@localhost ~]$
[estack@localhost ~]$ ip addr
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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:f4:ee:49 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global noprefixroute dynamic enp0s3
       valid_lft 86377sec preferred_lft 86377sec
    inet6 fe80::54:6336:a0b4:a884/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:26:f9:c5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.10/32 brd 192.168.56.10 scope global noprefixroute enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::3d7f:a97a:f2a4:7fea/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[estack@localhost ~]$
```


127.0.0.1 (estack)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
5. 127.0.0.1 (estack)
6. 192.168.56.10 (estack)
/home/estack/
Name
Size (KB)
..
.bash_history 1
.bash_logout 1
.bash_profile 1
.bashrc 1
Remote monitoring
☐ Follow terminal folder
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```
[estack@localhost ~]$
[estack@localhost ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3 enp0s8
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

[estack@localhost ~]$
```

Elasticsearch Installation (Centos 7.9)

Link: https://www.elastic.co/guide/en/elasticsearch/reference/current/rpm.html

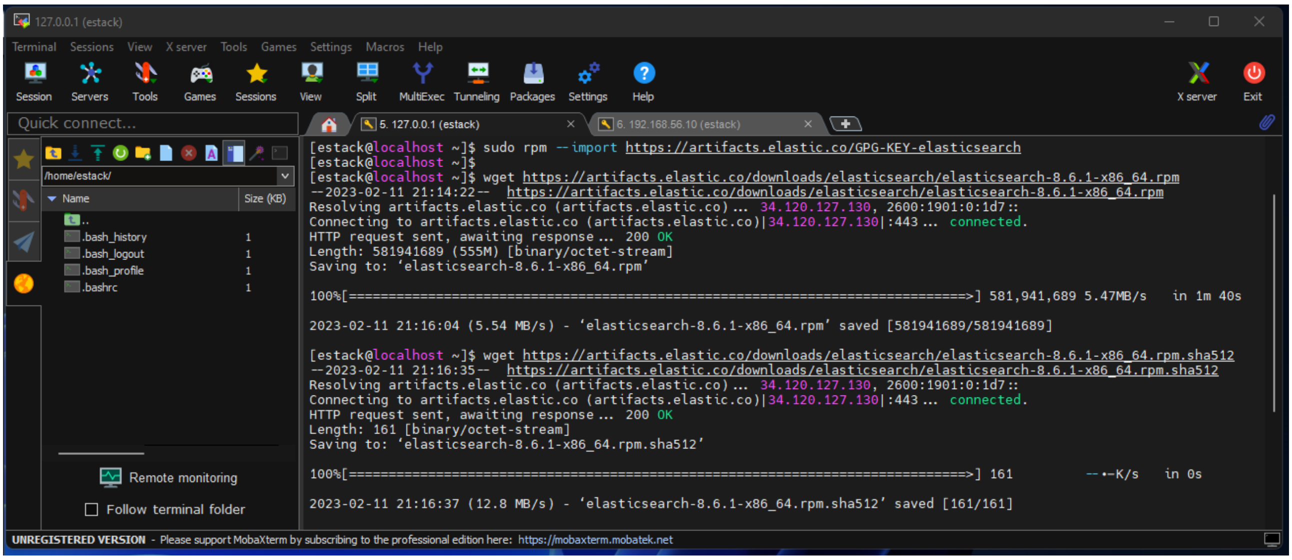
Before elasticsearch installation, requirements: java | wget | nano | perl-Digest-SHA

[estack@localhost ~]$ sudo yum update -y

- sudo yum install wget nano perl-Digest-SHA

- sudo yum install java-1.8.0-openjdk.x86_64
- java -version

- sudo rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch



```
[estack@localhost ~]$ sudo rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
[estack@localhost ~]$
[estack@localhost ~]$ wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.6.1-x86_64.rpm
--2023-02-11 21:14:22--  https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.6.1-x86_64.rpm
Resolving artifacts.elastic.co (artifacts.elastic.co)... 34.120.127.130, 2600:1901:0:1d7::
Connecting to artifacts.elastic.co (artifacts.elastic.co)|34.120.127.130|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 581941689 (555M) [binary/octet-stream]
Saving to: ‘elasticsearch-8.6.1-x86_64.rpm’

100%[===========================================================================>] 581,941,689 5.47MB/s   in 1m 40s

2023-02-11 21:16:04 (5.54 MB/s) - ‘elasticsearch-8.6.1-x86_64.rpm’ saved [581941689/581941689]

[estack@localhost ~]$ wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.6.1-x86_64.rpm.sha512
--2023-02-11 21:16:35--  https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.6.1-x86_64.rpm.sha512
Resolving artifacts.elastic.co (artifacts.elastic.co)... 34.120.127.130, 2600:1901:0:1d7::
Connecting to artifacts.elastic.co (artifacts.elastic.co)|34.120.127.130|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 161 [binary/octet-stream]
Saving to: ‘elasticsearch-8.6.1-x86_64.rpm.sha512’

100%[===========================================================================>] 161         --.-K/s   in 0s

2023-02-11 21:16:37 (12.8 MB/s) - ‘elasticsearch-8.6.1-x86_64.rpm.sha512’ saved [161/161]
```

Download and install the RPM manually

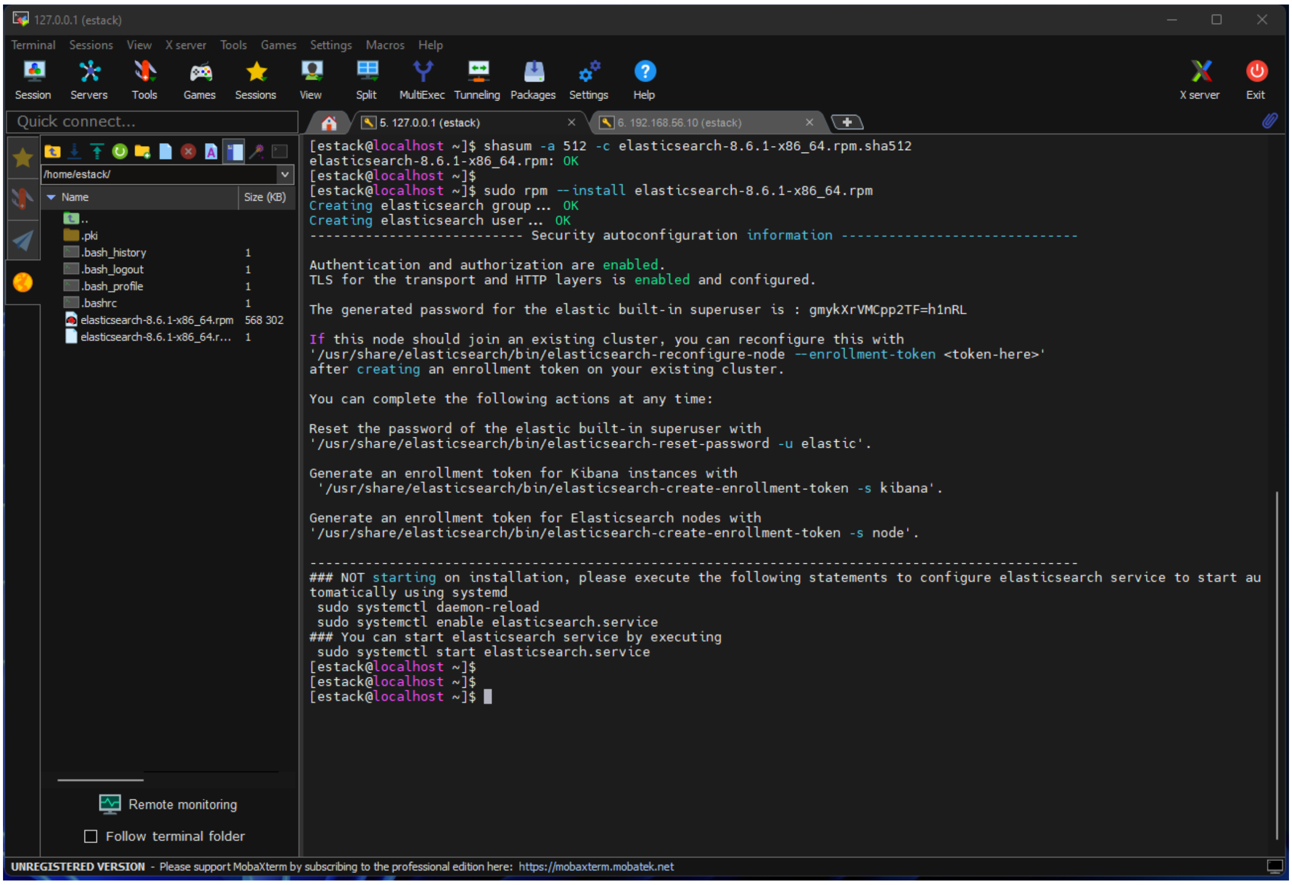
[estack@localhost ~]$

- wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.6.1-x86_64.rpm
- wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.6.1-x86_64.rpm.sha512

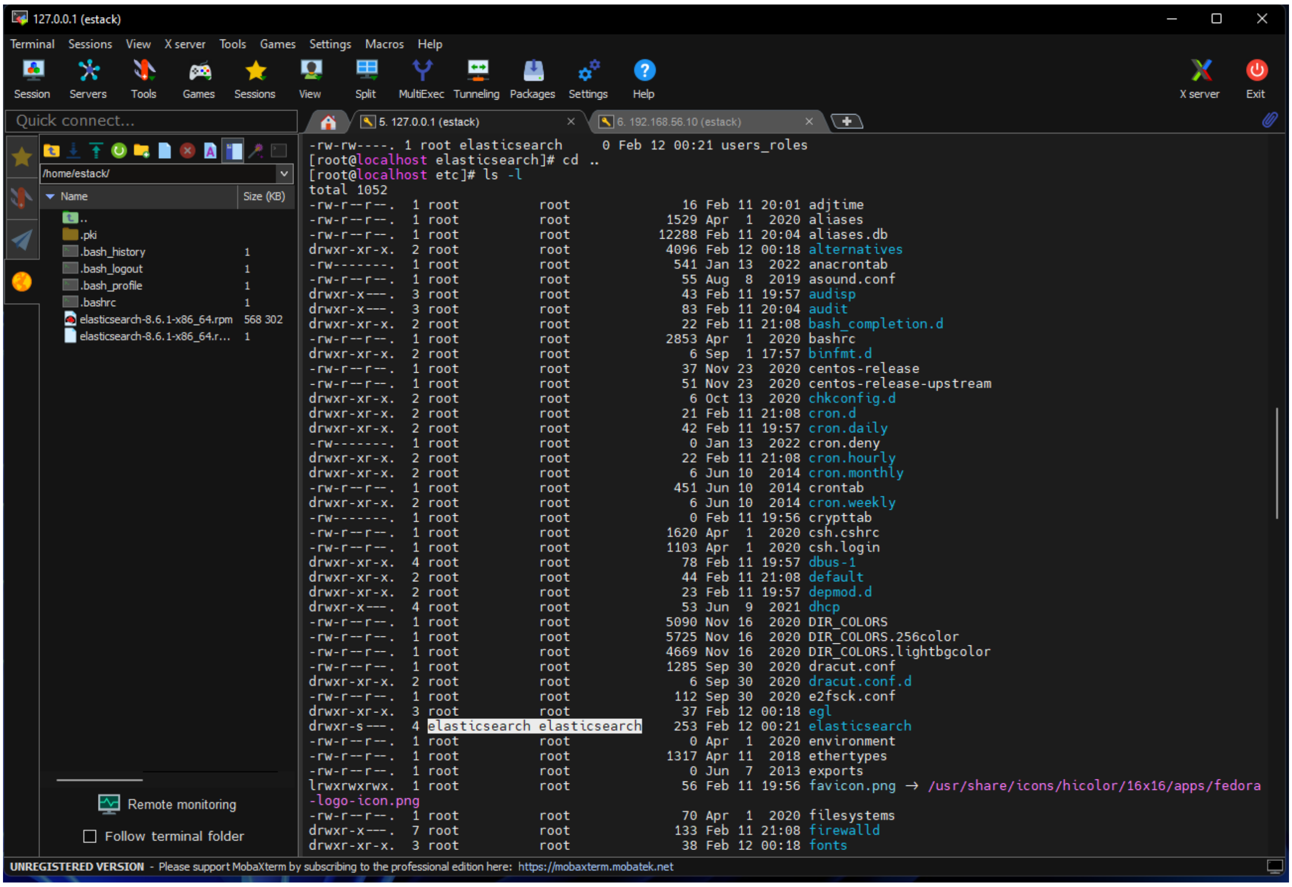
- shasum -a 512 -c elasticsearch-8.6.1-x86_64.rpm.sha512
- sudo rpm --ivh elasticsearch-8.6.1-x86_64.rpm

- sudo /bin/systemctl daemon-reload

- sudo systemctl enable elasticsearch.service


127.0.0.1 (estack)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit
Quick connect...
5. 127.0.0.1 (estack)
6. 192.168.56.10 (estack)
/home/estack/
Name Size (KB)
..
.pki
.bash_history 1
.bash_logout 1
.bash_profile 1
.bashrc 1
elasticsearch-8.6.1-x86_64.rpm 568 302
elasticsearch-8.6.1-x86_64.r... 1
Remote monitoring
□ Follow terminal folder
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```
[estack@localhost ~]$ shasum -a 512 -c elasticsearch-8.6.1-x86_64.rpm.sha512
elasticsearch-8.6.1-x86_64.rpm: OK
[estack@localhost ~]$
[estack@localhost ~]$ sudo rpm --install elasticsearch-8.6.1-x86_64.rpm
Creating elasticsearch group... OK
Creating elasticsearch user... OK
--------------------------- Security autoconfiguration information ------------------------------

Authentication and authorization are enabled.
TLS for the transport and HTTP layers is enabled and configured.

The generated password for the elastic built-in superuser is : gmykXrVMCpp2TF=h1nRL

If this node should join an existing cluster, you can reconfigure this with
'/usr/share/elasticsearch/bin/elasticsearch-reconfigure-node --enrollment-token <token-here>'
after creating an enrollment token on your existing cluster.

You can complete the following actions at any time:

Reset the password of the elastic built-in superuser with
'/usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic'.

Generate an enrollment token for Kibana instances with
 '/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana'.

Generate an enrollment token for Elasticsearch nodes with
'/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s node'.

-------------------------------------------------------------------------------------------------
### NOT starting on installation, please execute the following statements to configure elasticsearch service to start au
tomatically using systemd
 sudo systemctl daemon-reload
 sudo systemctl enable elasticsearch.service
### You can start elasticsearch service by executing
 sudo systemctl start elasticsearch.service
[estack@localhost ~]$
[estack@localhost ~]$
[estack@localhost ~]$
```

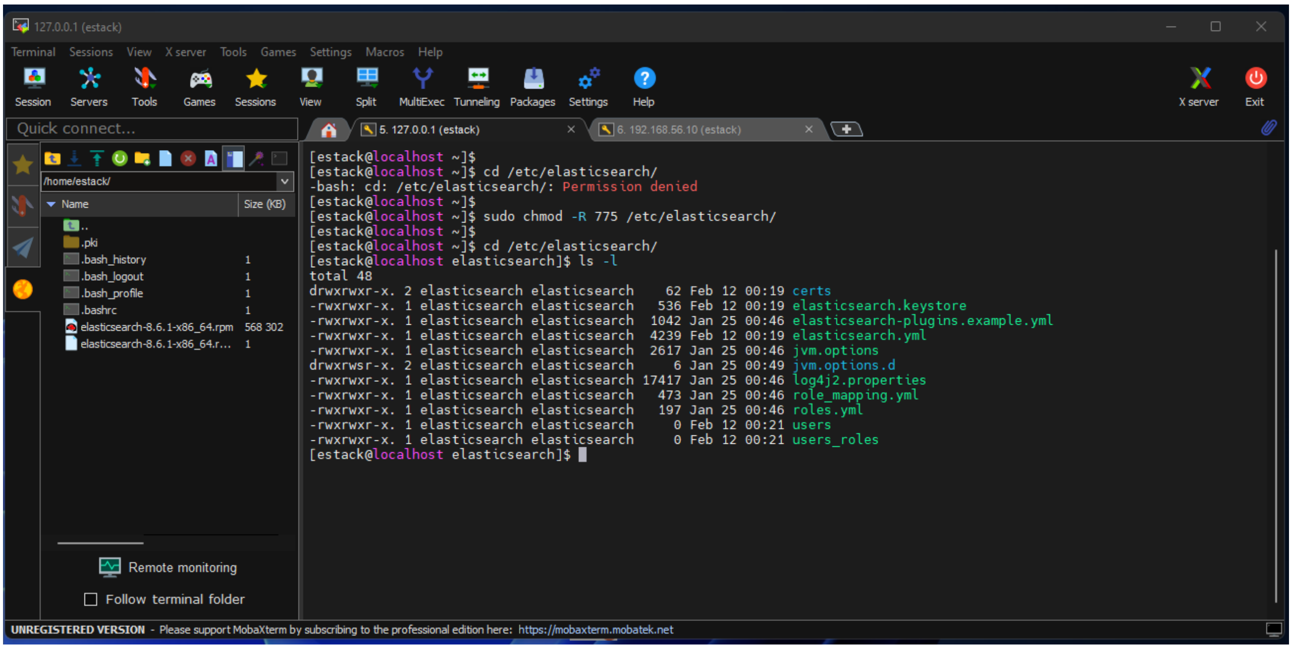

127.0.0.1 (estack)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit
Quick connect...
5. 127.0.0.1 (estack)
6. 192.168.56.10 (estack)
/home/estack/
Name Size (KB)
..
.pki
.bash_history 1
.bash_logout 1
.bash_profile 1
.bashrc 1
elasticsearch-8.6.1-x86_64.rpm 568 302
elasticsearch-8.6.1-x86_64.r... 1
Remote monitoring
□ Follow terminal folder
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```
-rw-rw----. 1 root elasticsearch     0 Feb 12 00:21 users_roles
[root@localhost elasticsearch]# cd ..
[root@localhost etc]# ls -l
total 1052
-rw-r--r--.  1 root          root             16 Feb 11 20:01 adjtime
-rw-r--r--.  1 root          root           1529 Apr  1  2020 aliases
-rw-r--r--.  1 root          root          12288 Feb 11 20:04 aliases.db
drwxr-xr-x.  2 root          root           4096 Feb 12 00:18 alternatives
-rw-------.  1 root          root            541 Jan 13  2022 anacrontab
-rw-r--r--.  1 root          root             55 Aug  8  2019 asound.conf
drwxr-x---.  3 root          root             43 Feb 11 19:57 audisp
drwxr-x---.  3 root          root             83 Feb 11 20:04 audit
drwxr-xr-x.  2 root          root             22 Feb 11 21:08 bash_completion.d
-rw-r--r--.  1 root          root           2853 Apr  1  2020 bashrc
drwxr-xr-x.  2 root          root              6 Sep  1 17:57 binfmt.d
-rw-r--r--.  1 root          root             37 Nov 23  2020 centos-release
-rw-r--r--.  1 root          root             51 Nov 23  2020 centos-release-upstream
drwxr-xr-x.  2 root          root              6 Oct 13  2020 chkconfig.d
drwxr-xr-x.  2 root          root             21 Feb 11 21:08 cron.d
drwxr-xr-x.  2 root          root             42 Feb 11 19:57 cron.daily
-rw-------.  1 root          root              0 Jan 13  2022 cron.deny
drwxr-xr-x.  2 root          root             22 Feb 11 21:08 cron.hourly
drwxr-xr-x.  2 root          root              6 Jun 10  2014 cron.monthly
-rw-r--r--.  1 root          root            451 Jun 10  2014 crontab
drwxr-xr-x.  2 root          root              6 Jun 10  2014 cron.weekly
-rw-------.  1 root          root              0 Feb 11 19:56 crypttab
-rw-r--r--.  1 root          root           1620 Apr  1  2020 csh.cshrc
-rw-r--r--.  1 root          root           1103 Apr  1  2020 csh.login
drwxr-xr-x.  4 root          root             78 Feb 11 19:57 dbus-1
drwxr-xr-x.  2 root          root             44 Feb 11 21:08 default
drwxr-xr-x.  2 root          root             23 Feb 11 19:57 depmod.d
drwxr-x---.  4 root          root             53 Jun  9  2021 dhcp
-rw-r--r--.  1 root          root           5090 Nov 16  2020 DIR_COLORS
-rw-r--r--.  1 root          root           5725 Nov 16  2020 DIR_COLORS.256color
-rw-r--r--.  1 root          root           4669 Nov 16  2020 DIR_COLORS.lightbgcolor
-rw-r--r--.  1 root          root           1285 Sep 30  2020 dracut.conf
drwxr-xr-x.  2 root          root              6 Sep 30  2020 dracut.conf.d
-rw-r--r--.  1 root          root            112 Sep 30  2020 e2fsck.conf
drwxr-xr-x.  3 root          root             37 Feb 12 00:18 egl
drwxr-s---.  4 elasticsearch elasticsearch   253 Feb 12 00:21 elasticsearch
-rw-r--r--.  1 root          root              0 Apr  1  2020 environment
-rw-r--r--.  1 root          root           1317 Apr 11  2018 ethertypes
-rw-r--r--.  1 root          root              0 Jun  7  2013 exports
lrwxrwxrwx.  1 root          root             56 Feb 11 19:56 favicon.png → /usr/share/icons/hicolor/16x16/apps/fedora
-logo-icon.png
-rw-r--r--.  1 root          root             70 Apr  1  2020 filesystems
drwxr-x---.  7 root          root            133 Feb 11 21:08 firewalld
drwxr-xr-x.  3 root          root             38 Feb 12 00:18 fonts
```

```
[root@localhost elasticsearch]# sudo chown -R elasticsearch:elasticsearch /etc/elasticsearch/
[root@localhost elasticsearch]# ls -l
total 48
drwxr-x---. 2 elasticsearch elasticsearch    62 Feb 12 00:19 certs
-rw-rw----. 1 elasticsearch elasticsearch   536 Feb 12 00:19 elasticsearch.keystore
-rw-rw----. 1 elasticsearch elasticsearch  1042 Jan 25 00:46 elasticsearch-plugins.example.yml
-rw-rw----. 1 elasticsearch elasticsearch  4239 Feb 12 00:19 elasticsearch.yml
-rw-rw----. 1 elasticsearch elasticsearch  2617 Jan 25 00:46 jvm.options
drwxr-s---. 2 elasticsearch elasticsearch     6 Jan 25 00:49 jvm.options.d
-rw-rw----. 1 elasticsearch elasticsearch 17417 Jan 25 00:46 log4j2.properties
-rw-rw----. 1 elasticsearch elasticsearch   473 Jan 25 00:46 role_mapping.yml
-rw-rw----. 1 elasticsearch elasticsearch   197 Jan 25 00:46 roles.yml
-rw-rw----. 1 elasticsearch elasticsearch     0 Feb 12 00:21 users
-rw-rw----. 1 elasticsearch elasticsearch     0 Feb 12 00:21 users_roles
```

Grant for /etc/elasticsearch

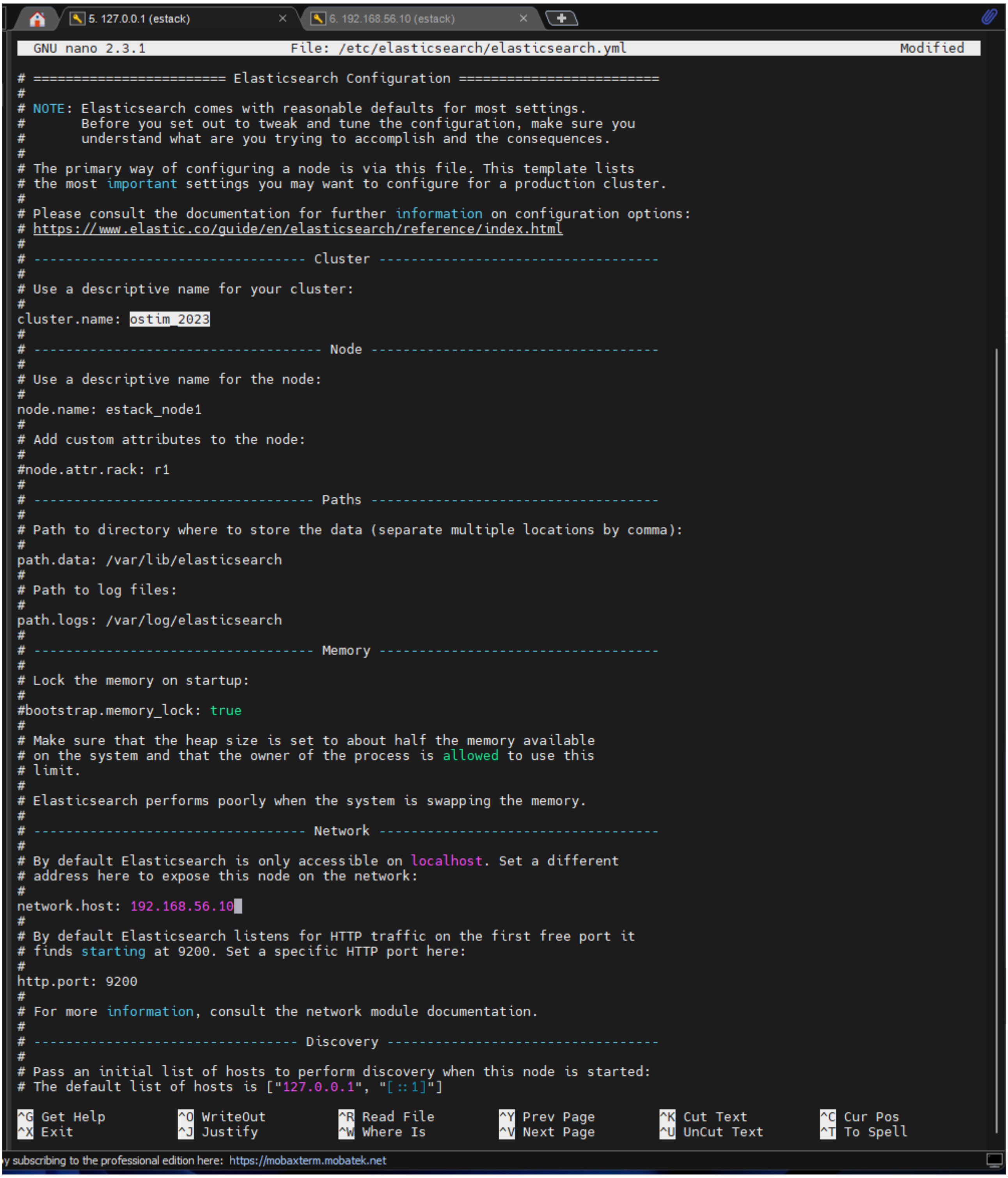
```
[estack@localhost elasticsearch]$ sudo chmod -R 775 /etc/elasticsearch/
```



127.0.0.1 (estack)
Terminal Sessions View X server Tools Games Settings Macros Help
Session
Servers
Tools
Games
Sessions
View
Split
MultiExec
Tunneling
Packages
Settings
Help
X server
Exit
Quick connect...
5. 127.0.0.1 (estack)
6. 192.168.56.10 (estack)
/home/estack/
Name
Size (KB)
..
.pki
.bash_history 1
.bash_logout 1
.bash_profile 1
.bashrc 1
elasticsearch-8.6.1-x86_64.rpm 568 302
elasticsearch-8.6.1-x86_64.r... 1
Remote monitoring
☐ Follow terminal folder
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

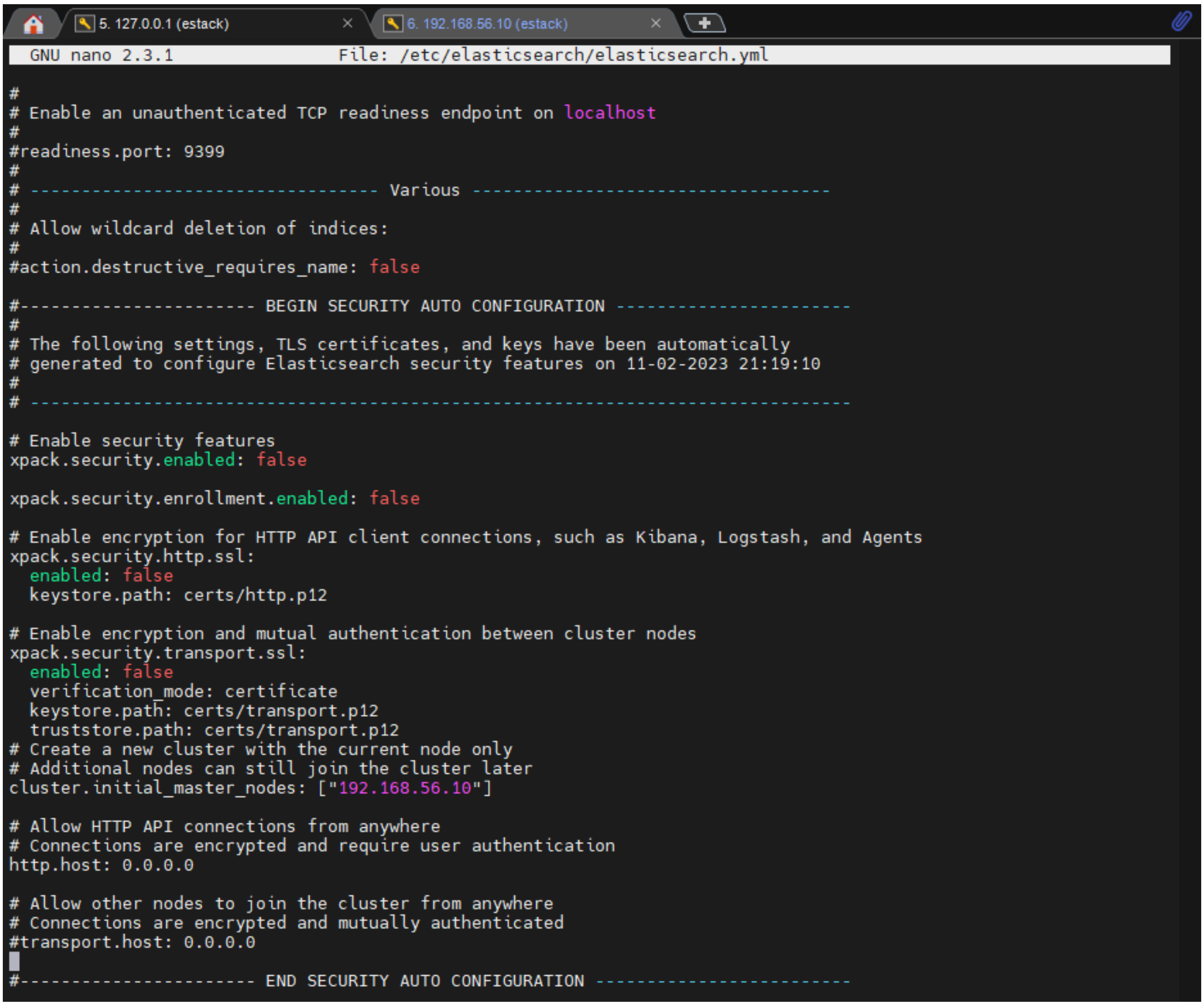
```
[estack@localhost ~]$
[estack@localhost ~]$ cd /etc/elasticsearch/
-bash: cd: /etc/elasticsearch/: Permission denied
[estack@localhost ~]$
[estack@localhost ~]$ sudo chmod -R 775 /etc/elasticsearch/
[estack@localhost ~]$
[estack@localhost ~]$ cd /etc/elasticsearch/
[estack@localhost elasticsearch]$ ls -l
total 48
drwxrwxr-x. 2 elasticsearch elasticsearch    62 Feb 12 00:19 certs
-rwxrwxr-x. 1 elasticsearch elasticsearch   536 Feb 12 00:19 elasticsearch.keystore
-rwxrwxr-x. 1 elasticsearch elasticsearch  1042 Jan 25 00:46 elasticsearch-plugins.example.yml
-rwxrwxr-x. 1 elasticsearch elasticsearch  4239 Feb 12 00:19 elasticsearch.yml
-rwxrwxr-x. 1 elasticsearch elasticsearch  2617 Jan 25 00:46 jvm.options
drwxrwsr-x. 2 elasticsearch elasticsearch     6 Jan 25 00:49 jvm.options.d
-rwxrwxr-x. 1 elasticsearch elasticsearch 17417 Jan 25 00:46 log4j2.properties
-rwxrwxr-x. 1 elasticsearch elasticsearch   473 Jan 25 00:46 role_mapping.yml
-rwxrwxr-x. 1 elasticsearch elasticsearch   197 Jan 25 00:46 roles.yml
-rwxrwxr-x. 1 elasticsearch elasticsearch     0 Feb 12 00:21 users
-rwxrwxr-x. 1 elasticsearch elasticsearch     0 Feb 12 00:21 users_roles
[estack@localhost elasticsearch]$
```

```
[estack@localhost elasticsearch]$  sudo nano /etc/elasticsearch/elasticsearch.yml
        ....
        cluster.name: ostim_2023
        node.name: estack_node1
        network.host: 192.168.56.10
        xpack.security.enabled: false
        xpack.security.enrollment.enabled: false
        xpack.security.http.ssl:
          enabled: false
        xpack.security.transport.ssl:
          enabled: false
        cluster.initial_master_nodes: ["192.168.56.10"]
        .....
[estack@localhost elasticsearch]$  sudo nano /etc/elasticsearch/jvm.options
        .....
        -Xms1g
        -Xmx1g
        .....
```

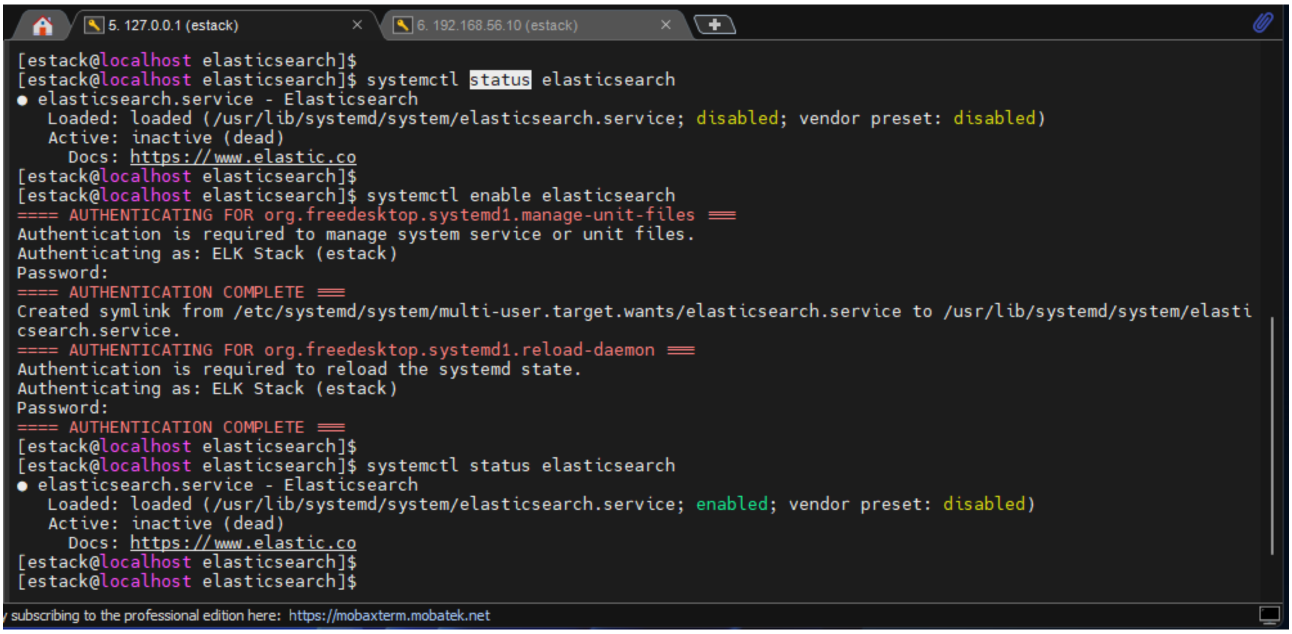


```
  GNU nano 2.3.1                File: /etc/elasticsearch/elasticsearch.yml                     Modified

# ======================== Elasticsearch Configuration =========================
#
# NOTE: Elasticsearch comes with reasonable defaults for most settings.
#       Before you set out to tweak and tune the configuration, make sure you
#       understand what are you trying to accomplish and the consequences.
#
# The primary way of configuring a node is via this file. This template lists
# the most important settings you may want to configure for a production cluster.
#
# Please consult the documentation for further information on configuration options:
# https://www.elastic.co/guide/en/elasticsearch/reference/index.html
#
# ---------------------------------- Cluster -----------------------------------
#
# Use a descriptive name for your cluster:
#
cluster.name: ostim_2023
#
# ------------------------------------ Node ------------------------------------
#
# Use a descriptive name for the node:
#
node.name: estack_node1
#
# Add custom attributes to the node:
#
#node.attr.rack: r1
#
# ----------------------------------- Paths ------------------------------------
#
# Path to directory where to store the data (separate multiple locations by comma):
#
path.data: /var/lib/elasticsearch
#
# Path to log files:
#
path.logs: /var/log/elasticsearch
#
# ----------------------------------- Memory -----------------------------------
#
# Lock the memory on startup:
#
#bootstrap.memory_lock: true
#
# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowed to use this
# limit.
#
# Elasticsearch performs poorly when the system is swapping the memory.
#
# ---------------------------------- Network -----------------------------------
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: 192.168.56.10
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
# --------------------------------- Discovery ----------------------------------
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]

^G Get Help    ^O WriteOut    ^R Read File   ^Y Prev Page   ^K Cut Text    ^C Cur Pos
^X Exit        ^J Justify     ^W Where Is    ^V Next Page   ^U UnCut Text  ^T To Spell
```

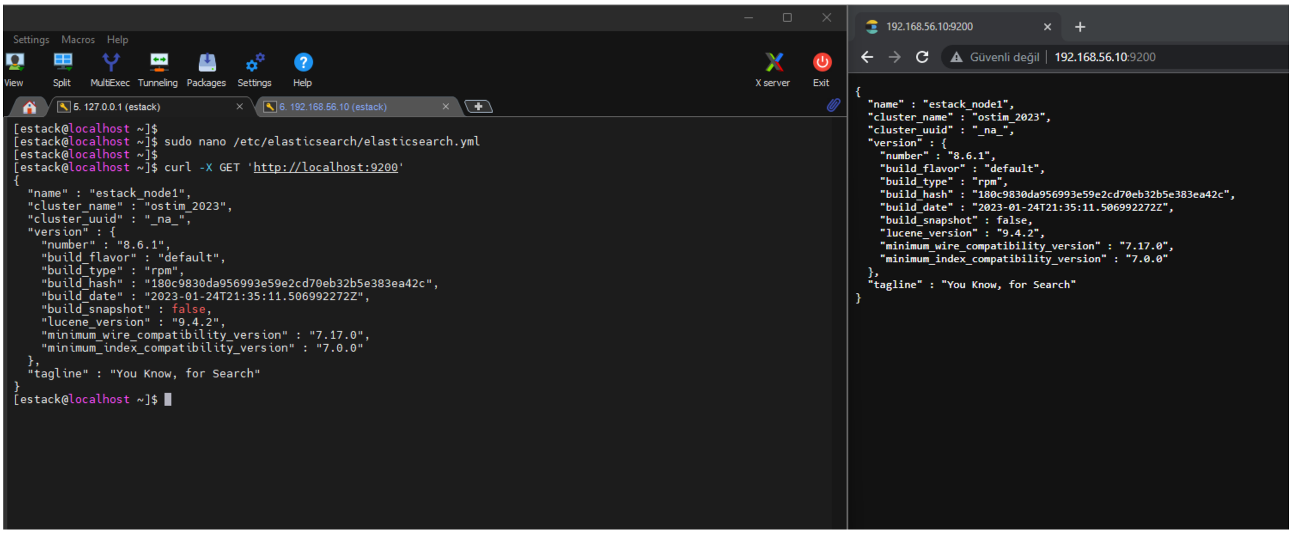
y subscribing to the professional edition here: https://mobaxterm.mobatek.net



```
  GNU nano 2.3.1             File: /etc/elasticsearch/elasticsearch.yml

#
# Enable an unauthenticated TCP readiness endpoint on localhost
#
#readiness.port: 9399
#
# ---------------------------------- Various -----------------------------------
#
# Allow wildcard deletion of indices:
#
#action.destructive_requires_name: false

#----------------------- BEGIN SECURITY AUTO CONFIGURATION -----------------------
#
# The following settings, TLS certificates, and keys have been automatically
# generated to configure Elasticsearch security features on 11-02-2023 21:19:10
#
# --------------------------------------------------------------------------------

# Enable security features
xpack.security.enabled: false

xpack.security.enrollment.enabled: false

# Enable encryption for HTTP API client connections, such as Kibana, Logstash, and Agents
xpack.security.http.ssl:
  enabled: false
  keystore.path: certs/http.p12

# Enable encryption and mutual authentication between cluster nodes
xpack.security.transport.ssl:
  enabled: false
  verification_mode: certificate
  keystore.path: certs/transport.p12
  truststore.path: certs/transport.p12
# Create a new cluster with the current node only
# Additional nodes can still join the cluster later
cluster.initial_master_nodes: ["192.168.56.10"]

# Allow HTTP API connections from anywhere
# Connections are encrypted and require user authentication
http.host: 0.0.0.0

# Allow other nodes to join the cluster from anywhere
# Connections are encrypted and mutually authenticated
#transport.host: 0.0.0.0

#----------------------- END SECURITY AUTO CONFIGURATION ------------------------
```


5. 127.0.0.1 (estack)
6. 192.168.56.10 (estack)
y subscribing to the professional edition here: https://mobaxterm.mobatek.net

```
[estack@localhost elasticsearch]$
[estack@localhost elasticsearch]$ systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: https://www.elastic.co
[estack@localhost elasticsearch]$
[estack@localhost elasticsearch]$ systemctl enable elasticsearch
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-unit-files ===
Authentication is required to manage system service or unit files.
Authenticating as: ELK Stack (estack)
Password:
==== AUTHENTICATION COMPLETE ===
Created symlink from /etc/systemd/system/multi-user.target.wants/elasticsearch.service to /usr/lib/systemd/system/elasti
csearch.service.
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ===
Authentication is required to reload the systemd state.
Authenticating as: ELK Stack (estack)
Password:
==== AUTHENTICATION COMPLETE ===
[estack@localhost elasticsearch]$
[estack@localhost elasticsearch]$ systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: https://www.elastic.co
[estack@localhost elasticsearch]$
[estack@localhost elasticsearch]$
```



```
[estack@localhost ~]$
[estack@localhost ~]$ sudo nano /etc/elasticsearch/elasticsearch.yml
[estack@localhost ~]$
[estack@localhost ~]$ curl -X GET 'http://localhost:9200'
{
  "name" : "estack_node1",
  "cluster_name" : "ostim_2023",
  "cluster_uuid" : "_na_",
  "version" : {
    "number" : "8.6.1",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "180c9830da956993e59e2cd70eb32b5e383ea42c",
    "build_date" : "2023-01-24T21:35:11.506992272Z",
    "build_snapshot" : false,
    "lucene_version" : "9.4.2",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
[estack@localhost ~]$
```

```
{
  "name" : "estack_node1",
  "cluster_name" : "ostim_2023",
  "cluster_uuid" : "_na_",
  "version" : {
    "number" : "8.6.1",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "180c9830da956993e59e2cd70eb32b5e383ea42c",
    "build_date" : "2023-01-24T21:35:11.506992272Z",
    "build_snapshot" : false,
    "lucene_version" : "9.4.2",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

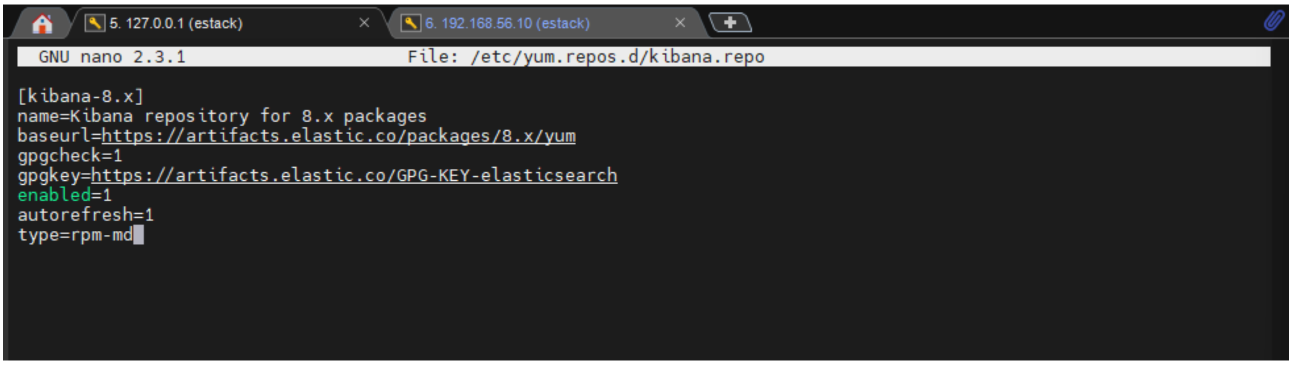
Kibana Installation

Link: https://www.elastic.co/guide/en/kibana/current/rpm.html

Installing from the RMP repository

Adding Repo: `/etc/yum.repos.d/  kibana.repo`

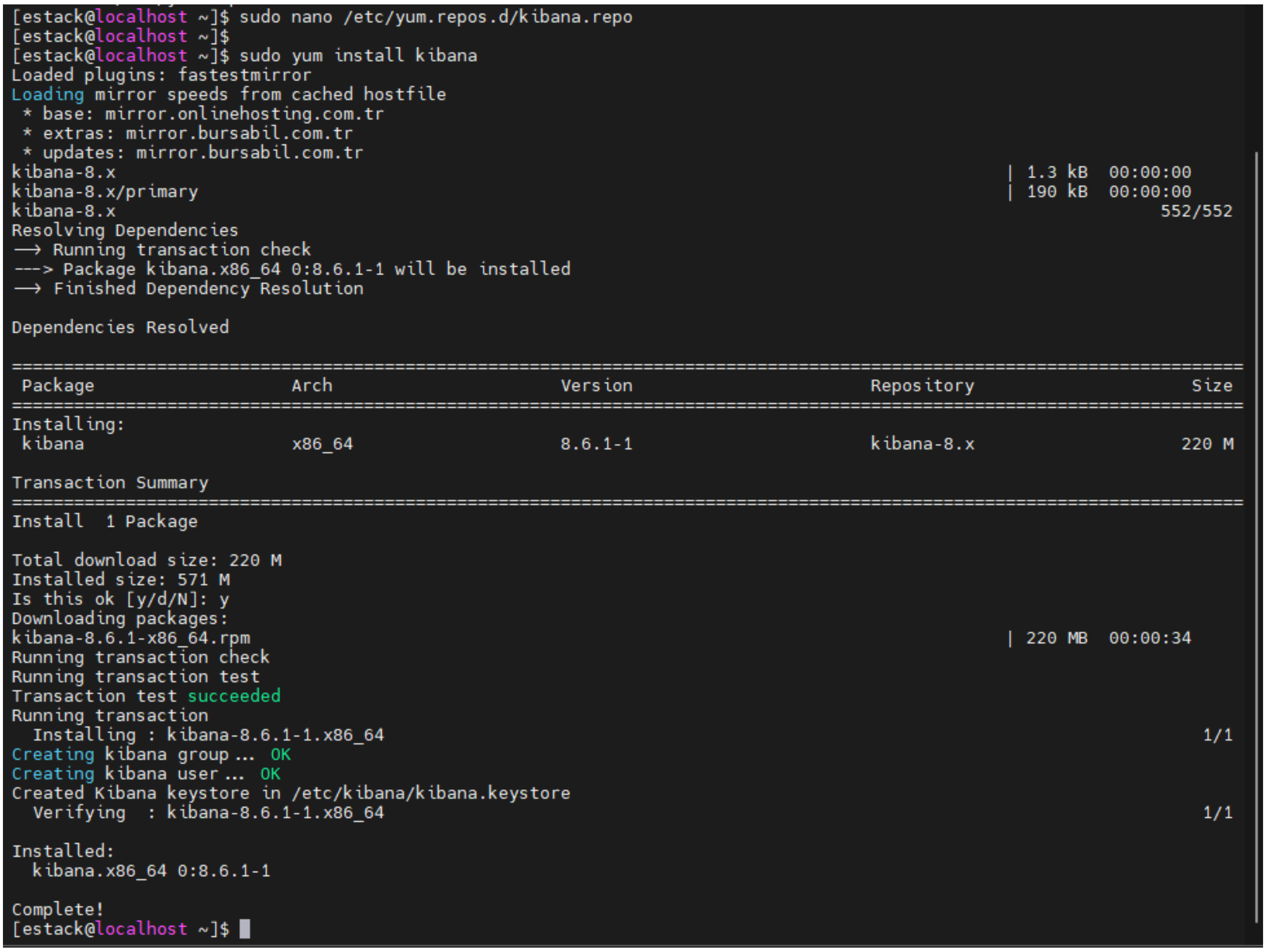
```
[kibana-8.x]
name=Kibana repository for 8.x packages
baseurl=https://artifacts.elastic.co/packages/8.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```



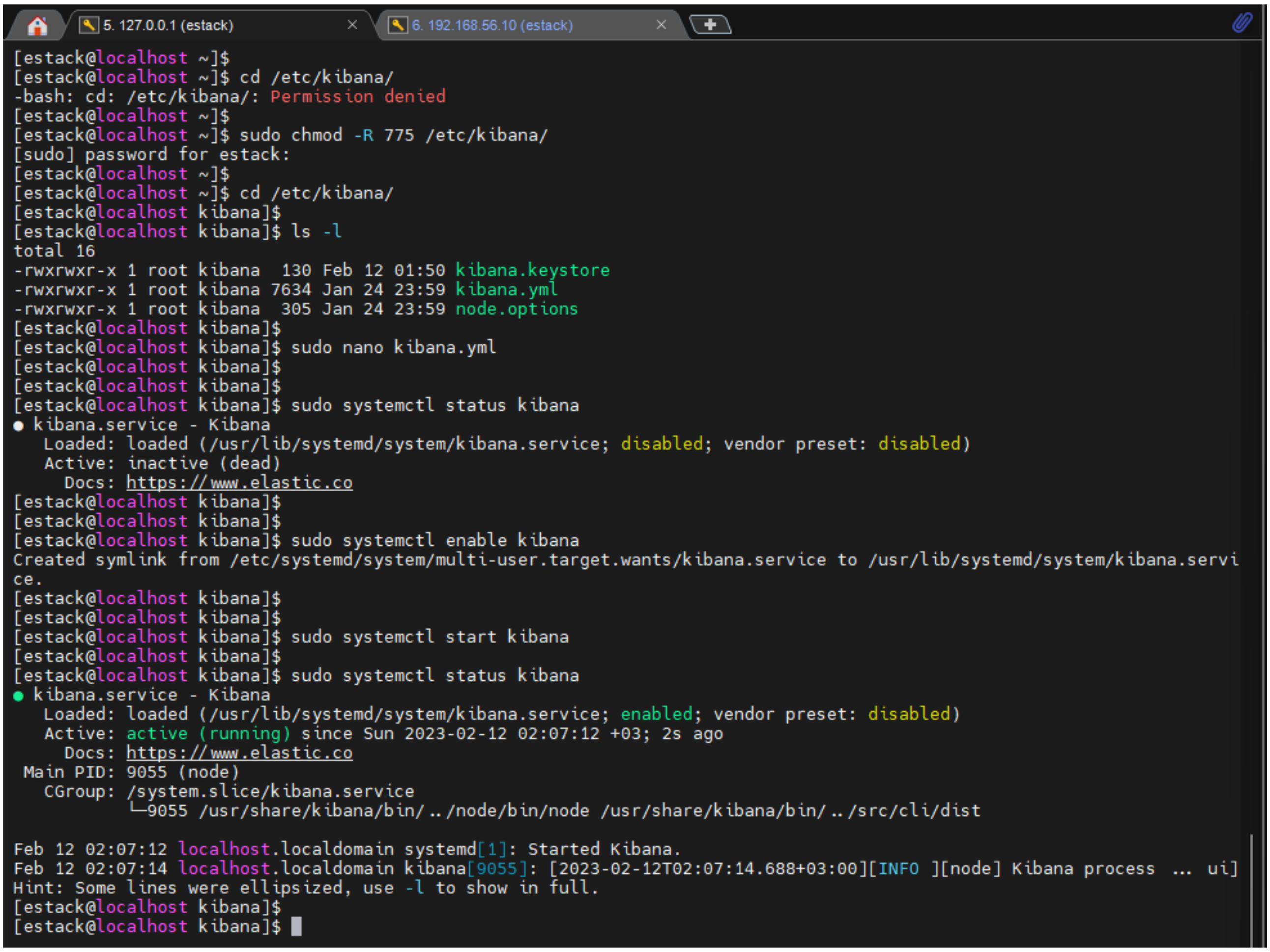
```
  GNU nano 2.3.1                File: /etc/yum.repos.d/kibana.repo

[kibana-8.x]
name=Kibana repository for 8.x packages
baseurl=https://artifacts.elastic.co/packages/8.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

Grant for /etc/kibana

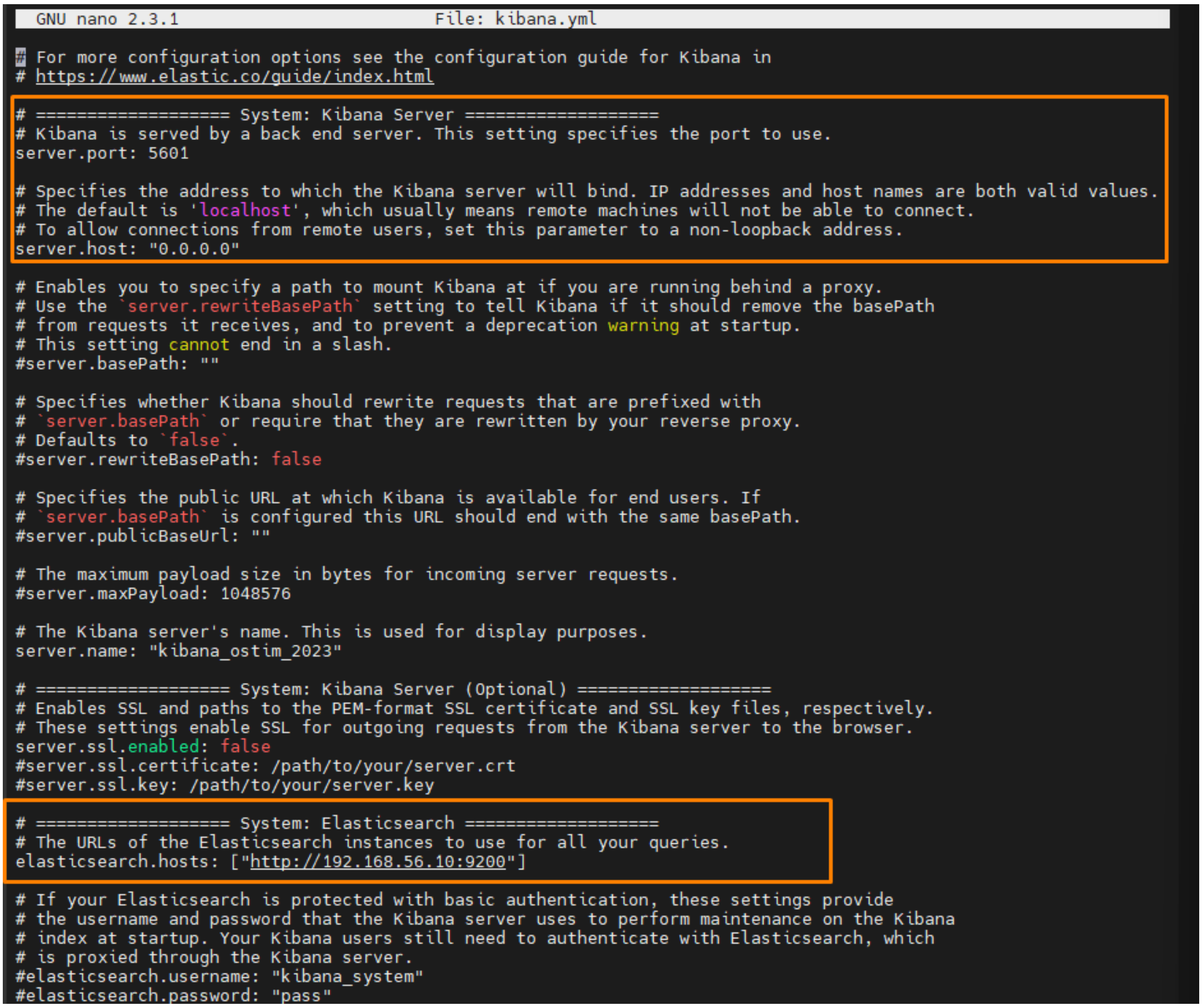
[estack@localhost]$ sudo chmod -R 775 /etc/kibana/



```
[estack@localhost ~]$ sudo nano /etc/yum.repos.d/kibana.repo
[estack@localhost ~]$
[estack@localhost ~]$ sudo yum install kibana
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.onlinehosting.com.tr
 * extras: mirror.bursabil.com.tr
 * updates: mirror.bursabil.com.tr
kibana-8.x                                                                                  | 1.3 kB  00:00:00
kibana-8.x/primary                                                                          | 190 kB  00:00:00
kibana-8.x                                                                                                552/552
Resolving Dependencies
--> Running transaction check
---> Package kibana.x86_64 0:8.6.1-1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=======================================================================================================================
 Package                     Arch                       Version                       Repository                  Size
=======================================================================================================================
Installing:
 kibana                      x86_64                     8.6.1-1                       kibana-8.x                 220 M

Transaction Summary
=======================================================================================================================
Install  1 Package

Total download size: 220 M
Installed size: 571 M
Is this ok [y/d/N]: y
Downloading packages:
kibana-8.6.1-x86_64.rpm                                                                     | 220 MB  00:00:34
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : kibana-8.6.1-1.x86_64                                                                          1/1
Creating kibana group... OK
Creating kibana user... OK
Created Kibana keystore in /etc/kibana/kibana.keystore
  Verifying  : kibana-8.6.1-1.x86_64                                                                          1/1

Installed:
  kibana.x86_64 0:8.6.1-1

Complete!
[estack@localhost ~]$
```



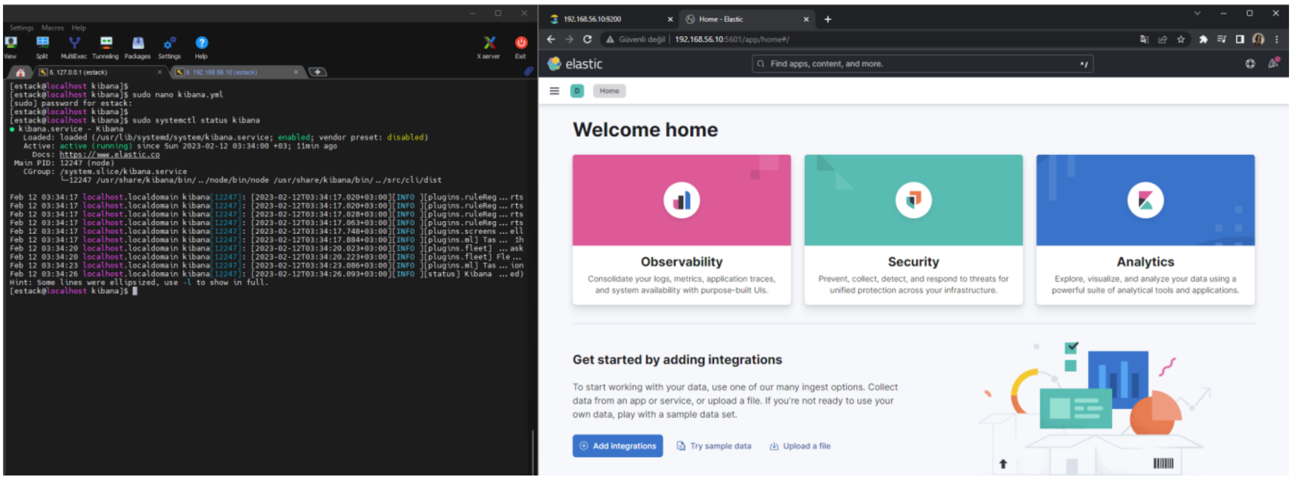
```
[estack@localhost ~]$
[estack@localhost ~]$ cd /etc/kibana/
-bash: cd: /etc/kibana/: Permission denied
[estack@localhost ~]$
[estack@localhost ~]$ sudo chmod -R 775 /etc/kibana/
[sudo] password for estack:
[estack@localhost ~]$
[estack@localhost ~]$ cd /etc/kibana/
[estack@localhost kibana]$
[estack@localhost kibana]$ ls -l
total 16
-rwxrwxr-x 1 root kibana  130 Feb 12 01:50 kibana.keystore
-rwxrwxr-x 1 root kibana 7634 Jan 24 23:59 kibana.yml
-rwxrwxr-x 1 root kibana  305 Jan 24 23:59 node.options
[estack@localhost kibana]$
[estack@localhost kibana]$ sudo nano kibana.yml
[estack@localhost kibana]$
[estack@localhost kibana]$
[estack@localhost kibana]$ sudo systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/usr/lib/systemd/system/kibana.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: https://www.elastic.co
[estack@localhost kibana]$
[estack@localhost kibana]$
[estack@localhost kibana]$ sudo systemctl enable kibana
Created symlink from /etc/systemd/system/multi-user.target.wants/kibana.service to /usr/lib/systemd/system/kibana.servi
ce.
[estack@localhost kibana]$
[estack@localhost kibana]$
[estack@localhost kibana]$ sudo systemctl start kibana
[estack@localhost kibana]$
[estack@localhost kibana]$ sudo systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2023-02-12 02:07:12 +03; 2s ago
     Docs: https://www.elastic.co
 Main PID: 9055 (node)
   CGroup: /system.slice/kibana.service
           └─9055 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist

Feb 12 02:07:12 localhost.localdomain systemd[1]: Started Kibana.
Feb 12 02:07:14 localhost.localdomain kibana[9055]: [2023-02-12T02:07:14.688+03:00][INFO ][node] Kibana process ... ui]
Hint: Some lines were ellipsized, use -l to show in full.
[estack@localhost kibana]$
[estack@localhost kibana]$
```



```
GNU nano 2.3.1                          File: kibana.yml

# For more configuration options see the configuration guide for Kibana in
# https://www.elastic.co/guide/index.html

# =================== System: Kibana Server ===================
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "0.0.0.0"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.
# Defaults to `false`.
#server.rewriteBasePath: false

# Specifies the public URL at which Kibana is available for end users. If
# `server.basePath` is configured this URL should end with the same basePath.
#server.publicBaseUrl: ""

# The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576

# The Kibana server's name. This is used for display purposes.
server.name: "kibana_ostim_2023"

# =================== System: Kibana Server (Optional) ===================
# Enables SSL and paths to the PEM-format SSL certificate and SSL key files, respectively.
# These settings enable SSL for outgoing requests from the Kibana server to the browser.
server.ssl.enabled: false
#server.ssl.certificate: /path/to/your/server.crt
#server.ssl.key: /path/to/your/server.key

# =================== System: Elasticsearch ===================
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://192.168.56.10:9200"]

# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the Kibana
# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which
# is proxied through the Kibana server.
#elasticsearch.username: "kibana_system"
#elasticsearch.password: "pass"
```

/etc/kibana/kibana.yml

```
# =================== System: Kibana Server ===================
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "0.0.0.0"

# The Kibana server's name. This is used for display purposes.
server.name: "kibana_ostim_2023"

# =================== System: Kibana Server (Optional) ===================
# Enables SSL and paths to the PEM-format SSL certificate and SSL key files, respectively.
# These settings enable SSL for outgoing requests from the Kibana server to the browser.
server.ssl.enabled: false
#server.ssl.certificate: /path/to/your/server.crt
#server.ssl.key: /path/to/your/server.key

# =================== System: Elasticsearch ===================
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://192.168.56.10:9200"]
.......
<End of the File (EOF)>
```



```
[estack@localhost kibana]$
[estack@localhost kibana]$ sudo nano kibana.yml
[sudo] password for estack:
[estack@localhost kibana]$
[estack@localhost kibana]$ sudo systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2023-02-12 03:34:00 +03; 11min ago
     Docs: https://www.elastic.co
 Main PID: 12247 (node)
   CGroup: /system.slice/kibana.service
           └─12247 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist

Feb 12 03:34:17 localhost.localdomain kibana[12247]: [2023-02-12T03:34:17.020+03:00][INFO ][plugins.ruleReg ... rts
Feb 12 03:34:17 localhost.localdomain kibana[12247]: [2023-02-12T03:34:17.020+03:00][INFO ][plugins.ruleReg ... rts
Feb 12 03:34:17 localhost.localdomain kibana[12247]: [2023-02-12T03:34:17.028+03:00][INFO ][plugins.ruleReg ... rts
Feb 12 03:34:17 localhost.localdomain kibana[12247]: [2023-02-12T03:34:17.063+03:00][INFO ][plugins.ruleReg ... rts
Feb 12 03:34:17 localhost.localdomain kibana[12247]: [2023-02-12T03:34:17.748+03:00][INFO ][plugins.screens ... ell
Feb 12 03:34:17 localhost.localdomain kibana[12247]: [2023-02-12T03:34:17.884+03:00][INFO ][plugins.ml] Tas ...  1h
Feb 12 03:34:20 localhost.localdomain kibana[12247]: [2023-02-12T03:34:20.023+03:00][INFO ][plugins.fleet] ... ask
Feb 12 03:34:20 localhost.localdomain kibana[12247]: [2023-02-12T03:34:20.223+03:00][INFO ][plugins.fleet] Fle ...
Feb 12 03:34:23 localhost.localdomain kibana[12247]: [2023-02-12T03:34:23.086+03:00][INFO ][plugins.ml] Tas ... ion
Feb 12 03:34:26 localhost.localdomain kibana[12247]: [2023-02-12T03:34:26.093+03:00][INFO ][status] Kibana  ... ed)
Hint: Some lines were ellipsized, use -l to show in full.
[estack@localhost kibana]$
```

Welcome home

Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Analytics

Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, play with a sample data set.