CAPACITYBAY

INSTLLATION AND CONFIGURATION OF ELASTICSEARCH AND KIBANA ON CENTOS

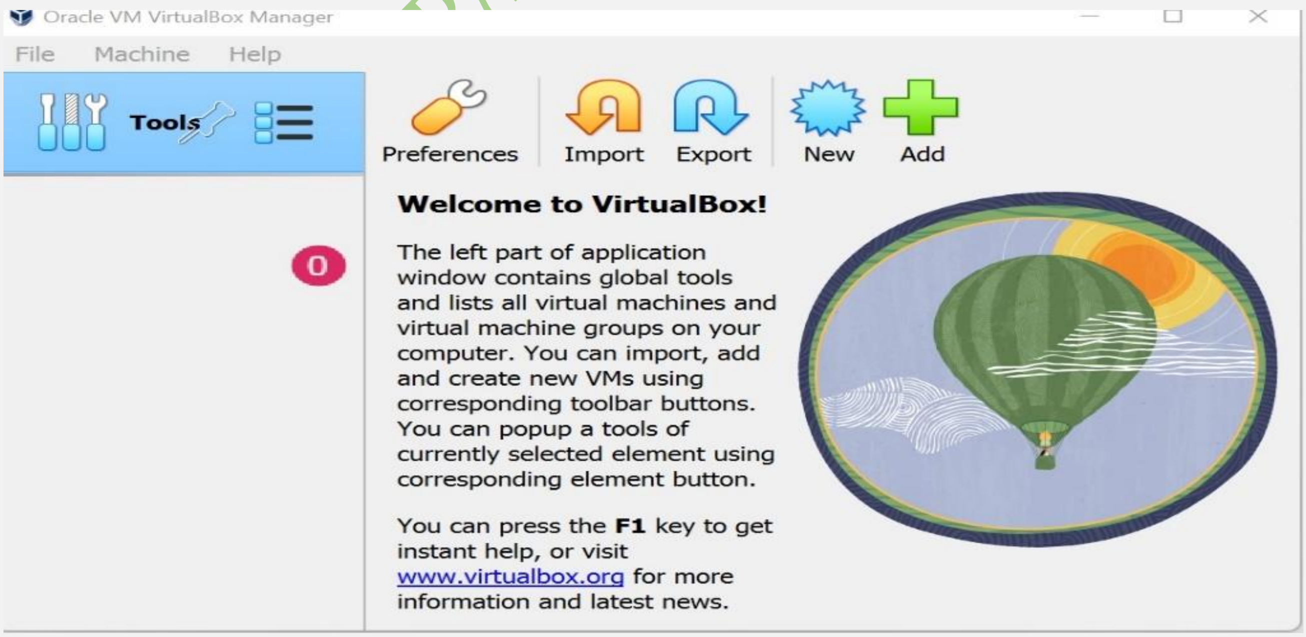
PREREQUISITE:

- Download and install virtual box
- Link: https://www.virtualbox.org/wiki/Downloads
- Download centos. Link: https://www.centos.org/download/
- Download mobaxterm Link https://mobaxterm.mobatek.net/download.html

SYSTEM REQUIREMENTS:

- RAM: minimum of 8gb
- PROCESSOR: core i3 and above
- Virtualization enable computer

Step 1: Lunch virtual box and click on the add icon

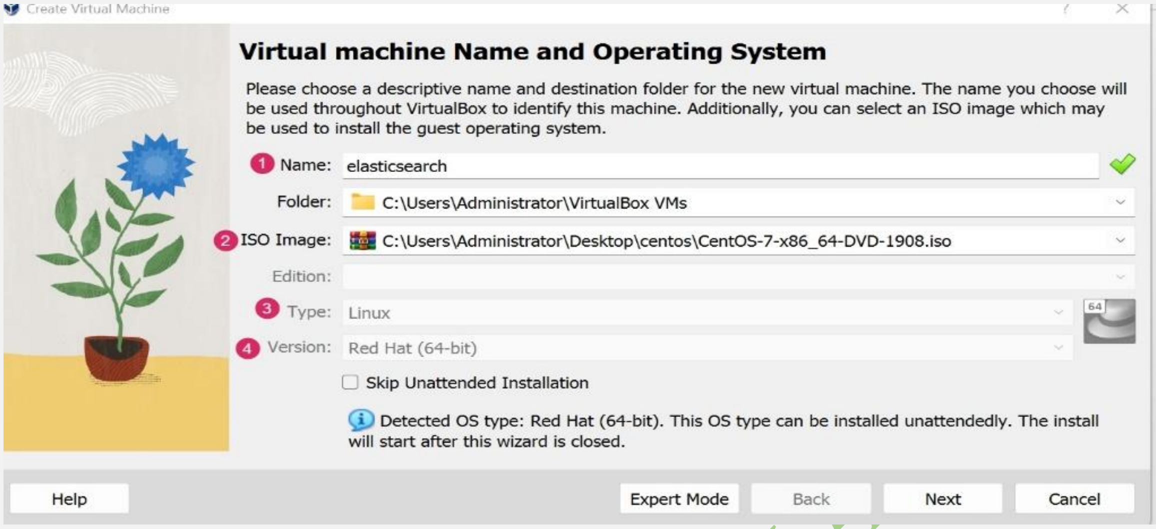


Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

Step 2: Centos server Setup


Create Virtual Machine

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.

1 Name: elasticsearch

Folder: C:\Users\Administrator\VirtualBox VMs

2 ISO Image: C:\Users\Administrator\Desktop\centos\CentOS-7-x86_64-DVD-1908.iso

Edition:

3 Type: Linux

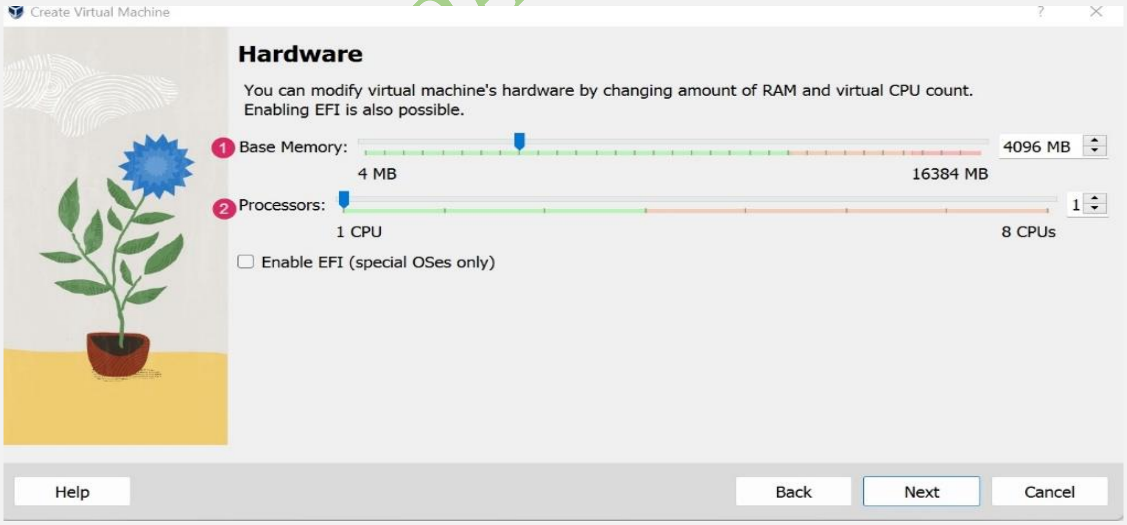
4 Version: Red Hat (64-bit)

□ Skip Unattended Installation

Detected OS type: Red Hat (64-bit). This OS type can be installed unattendedly. The install will start after this wizard is closed.

1. Input your Elasticsearch server name
2. Select Centos ISO file
3. Select operating system type
4. Select RedHat (choose OS architecture type)
5. Click on next to proceed

Step 3: RAM and CPU configuration


Create Virtual Machine

Hardware

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

1 Base Memory: 4096 MB (4 MB – 16384 MB)

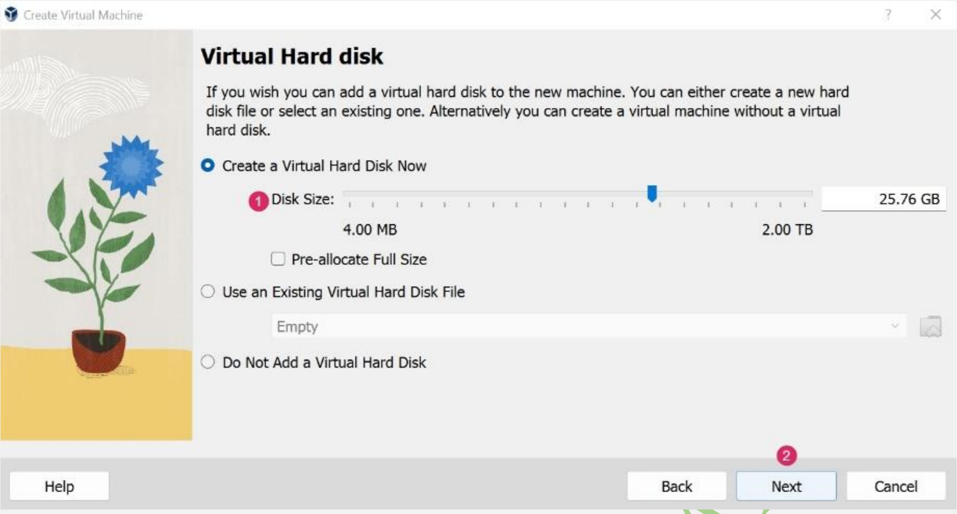
2 Processors: 1 (1 CPU – 8 CPUs)

□ Enable EFI (special OSes only)

1. Select virtual RAM size

2. Choose number of virtual CPUs
3. Click on next

Step 4: Virtual disk configuration



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

1 Disk Size: 25.76 GB (4.00 MB – 2.00 TB)

□ Pre-allocate Full Size

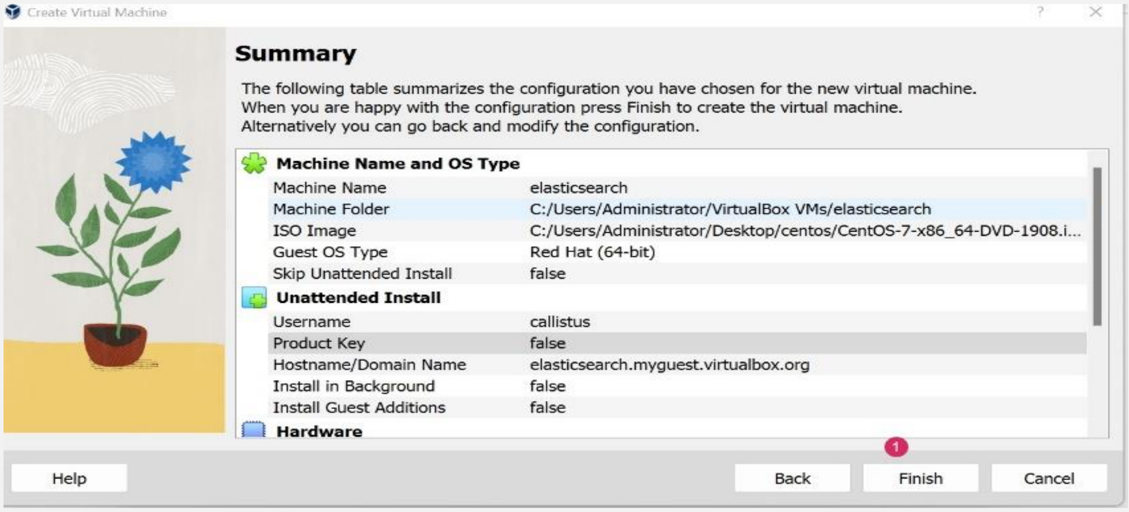
○ Use an Existing Virtual Hard Disk File

Empty

○ Do Not Add a Virtual Hard Disk

1. Select virtual disk capacity
2. Click on next

Step 5: Review configuration Settings

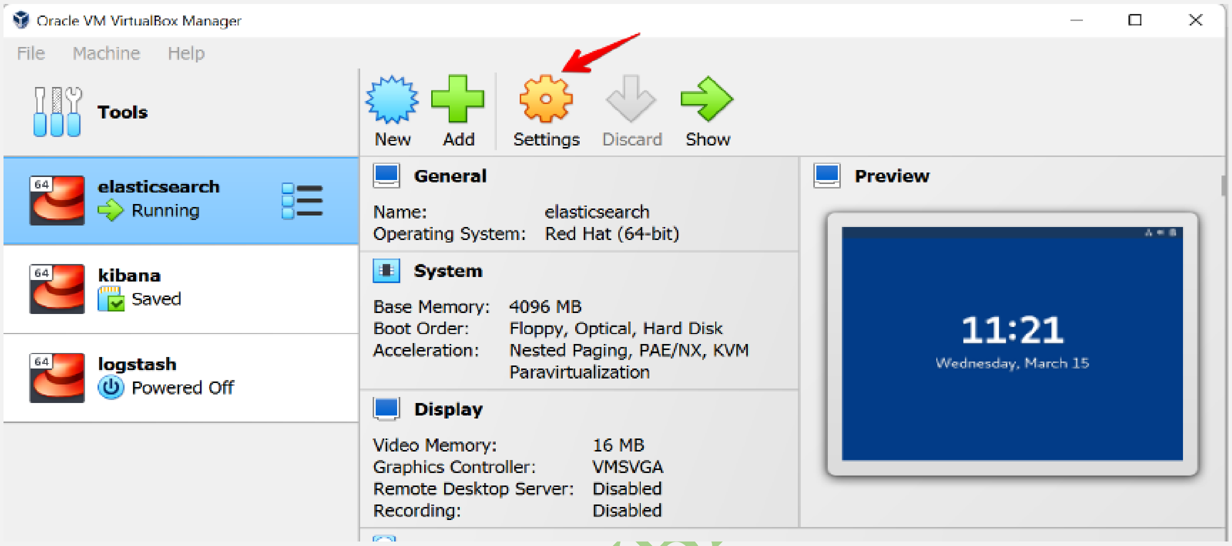


Summary

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	elasticsearch
Machine Folder	C:/Users/Administrator/VirtualBox VMs/elasticsearch
ISO Image	C:/Users/Administrator/Desktop/centos/CentOS-7-x86_64-DVD-1908.i...
Guest OS Type	Red Hat (64-bit)
Skip Unattended Install	false
Unattended Install	
Username	callistus
Product Key	false
Hostname/Domain Name	elasticsearch.myguest.virtualbox.org
Install in Background	false
Install Guest Additions	false
Hardware	

Step 6: Network Configuration



elasticsearch Running

kibana Saved

logstash Powered Off

General

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

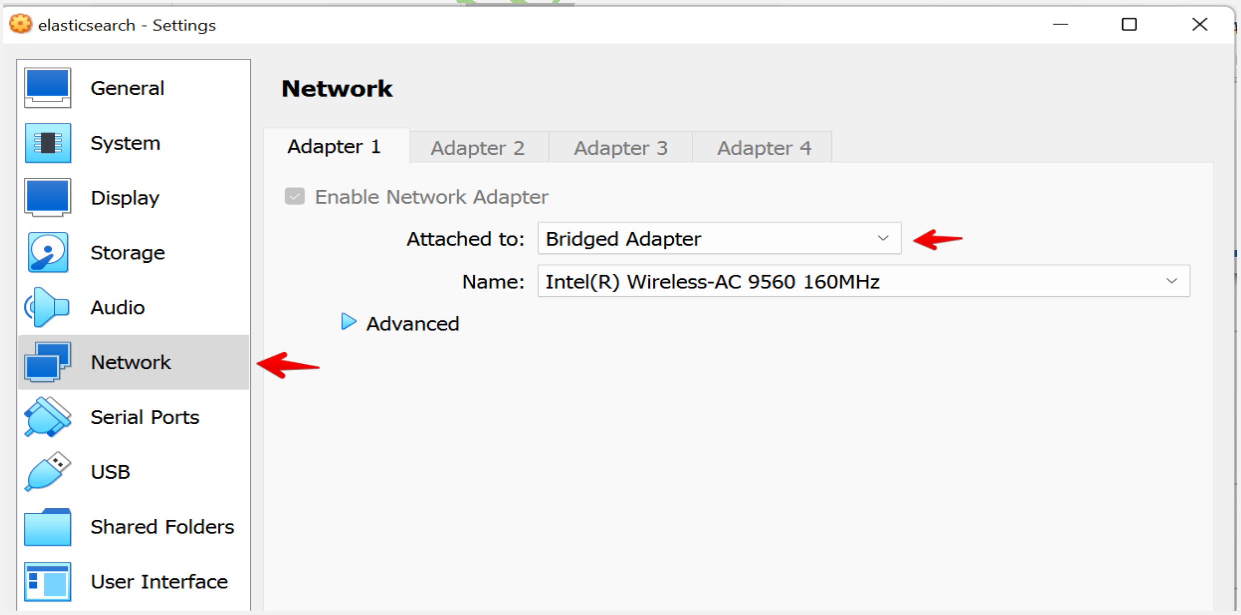
System

Base Memory: 4096 MB
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

Preview



Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

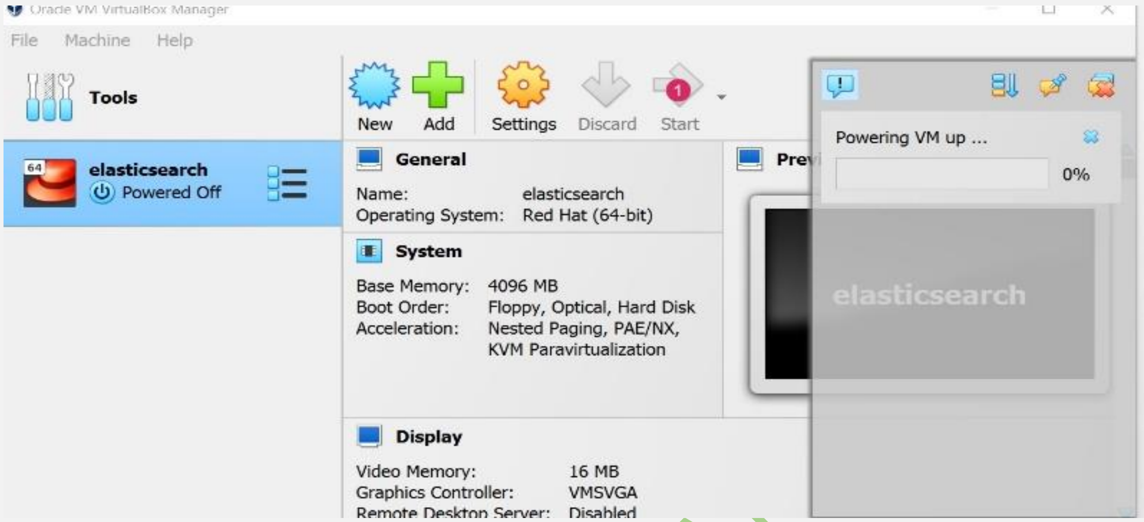
Attached to: Bridged Adapter

Name: Intel(R) Wireless-AC 9560 160MHz

▷ Advanced

1. Click on network option
2. Select bridged adapter
3. Click ok

Step 7: Lunch Centos server



elasticsearch
Powered Off

General

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

System

Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

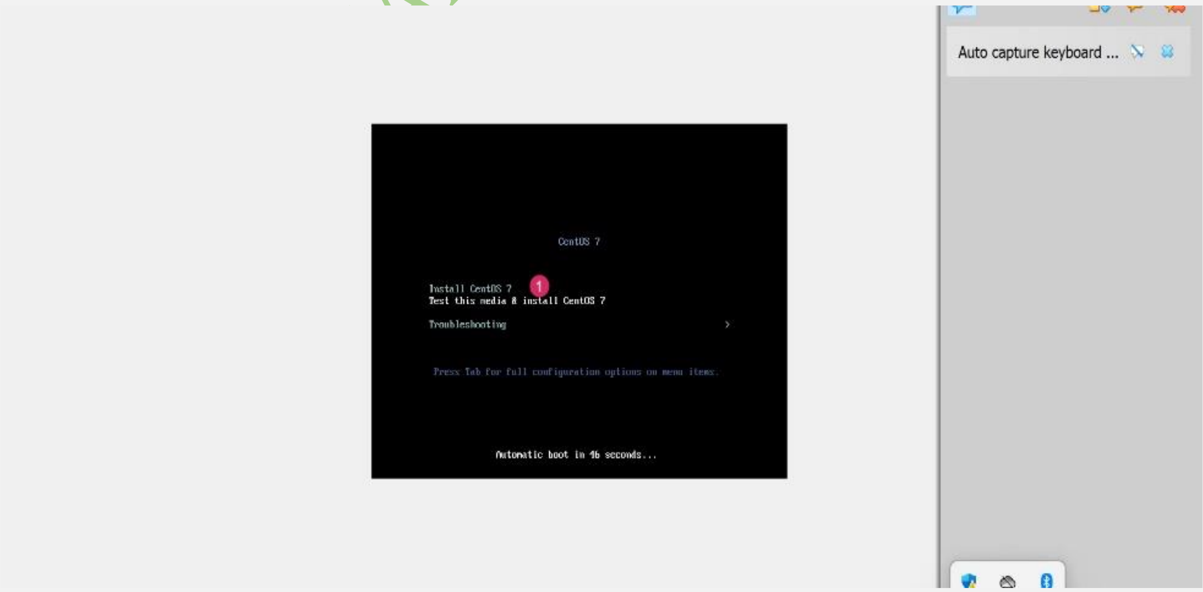
Display

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

Powering VM up ...
0%

1. Click on start

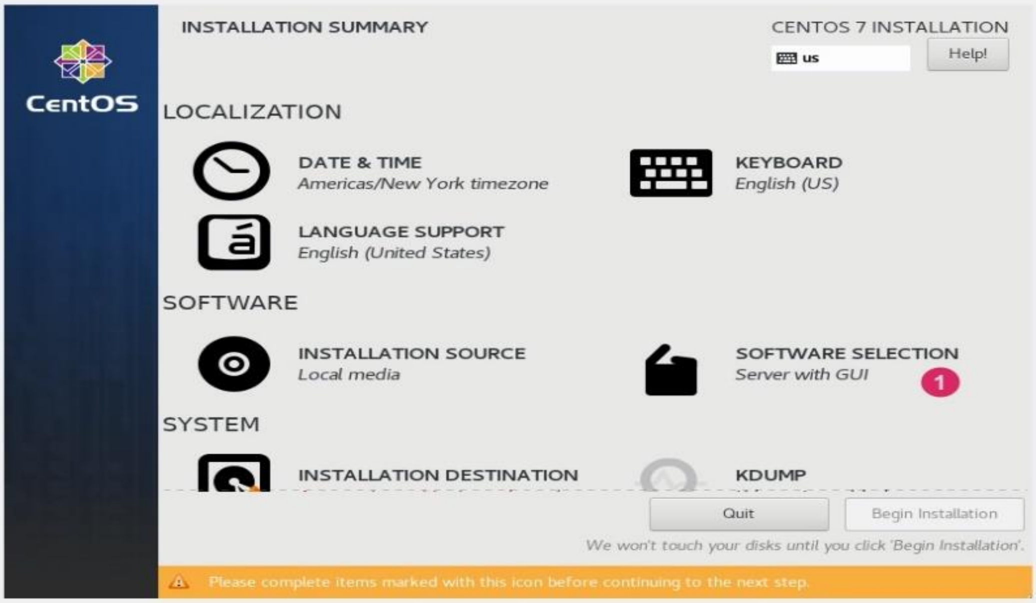
Step 8: Select install centos



Auto capture keyboard ...

```
CentOS 7

Install CentOS 7
Test this media & install CentOS 7

Troubleshooting                                        >

Press Tab for full configuration options on menu items.

Automatic boot in 46 seconds...
```

Step 9: Centos Server configuration



INSTALLATION SUMMARY

CENTOS 7 INSTALLATION

LOCALIZATION

DATE & TIME
Americas/New York timezone

KEYBOARD
English (US)

LANGUAGE SUPPORT
English (United States)

SOFTWARE

INSTALLATION SOURCE
Local media

SOFTWARE SELECTION
Server with GUI

SYSTEM

INSTALLATION DESTINATION

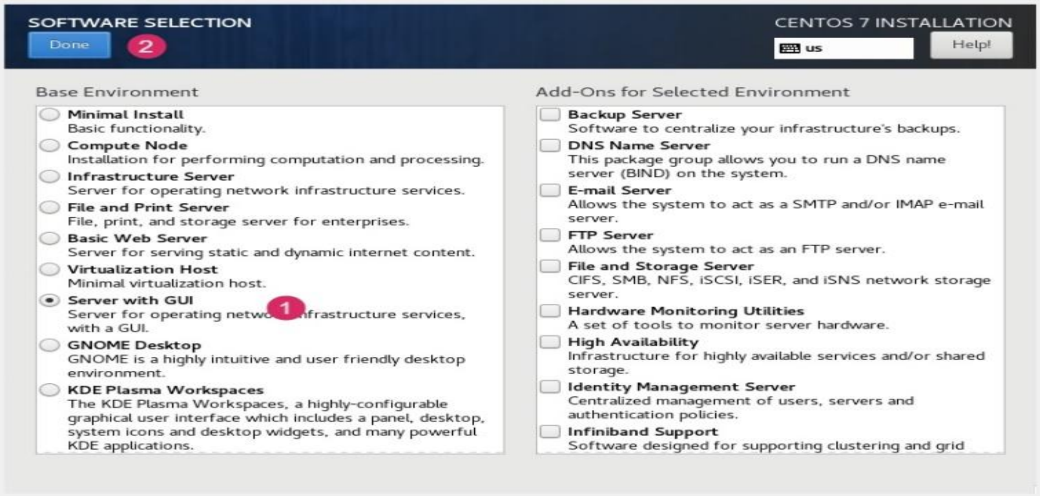
KDUMP

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

Please complete items marked with this icon before continuing to the next step.

1. Click on software section

Step 10: Choose server enviroment



Base Environment

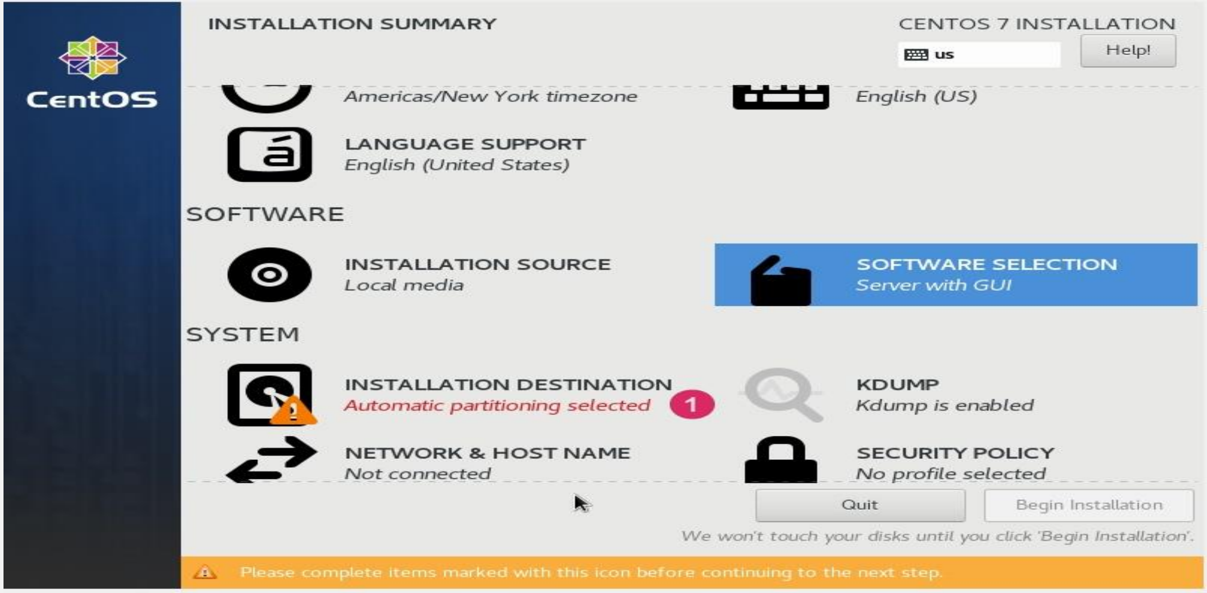
○ **Minimal Install**
Basic functionality.
○ **Compute Node**
Installation for performing computation and processing.
○ **Infrastructure Server**
Server for operating network infrastructure services.
○ **File and Print Server**
File, print, and storage server for enterprises.
○ **Basic Web Server**
Server for serving static and dynamic internet content.
○ **Virtualization Host**
Minimal virtualization host.
● **Server with GUI**
Server for operating network infrastructure services, with a GUI.
○ **GNOME Desktop**
GNOME is a highly intuitive and user friendly desktop environment.
○ **KDE Plasma Workspaces**
The KDE Plasma Workspaces, a highly-configurable graphical user interface which includes a panel, desktop, system icons and desktop widgets, and many powerful KDE applications.

Add-Ons for Selected Environment

□ **Backup Server**
Software to centralize your infrastructure's backups.
□ **DNS Name Server**
This package group allows you to run a DNS name server (BIND) on the system.
□ **E-mail Server**
Allows the system to act as a SMTP and/or IMAP e-mail server.
□ **FTP Server**
Allows the system to act as an FTP server.
□ **File and Storage Server**
CIFS, SMB, NFS, iSCSI, iSER, and iSNS network storage server.
□ **Hardware Monitoring Utilities**
A set of tools to monitor server hardware.
□ **High Availability**
Infrastructure for highly available services and/or shared storage.
□ **Identity Management Server**
Centralized management of users, servers and authentication policies.
□ **Infiniband Support**
Software designed for supporting clustering and grid

1. Choose server with GUI or any other option of your choice

Step 10: Configure Installation destination(disk partition configuration)



Americas/New York timezone
English (US)

LANGUAGE SUPPORT
English (United States)

SOFTWARE

INSTALLATION SOURCE
Local media

SOFTWARE SELECTION
Server with GUI

SYSTEM

INSTALLATION DESTINATION
Automatic partitioning selected

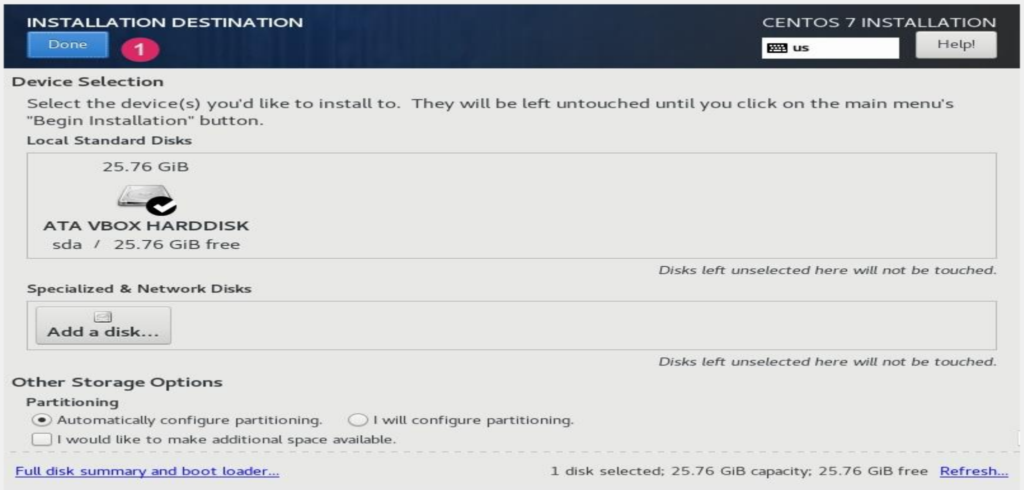
KDUMP
Kdump is enabled

NETWORK & HOST NAME
Not connected

SECURITY POLICY
No profile selected

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

Please complete items marked with this icon before continuing to the next step.



INSTALLATION DESTINATION

CENTOS 7 INSTALLATION

Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

25.76 GiB
ATA VBOX HARDDISK
sda / 25.76 GiB free

Disks left unselected here will not be touched.

Specialized & Network Disks

Disks left unselected here will not be touched.

Other Storage Options

Partitioning

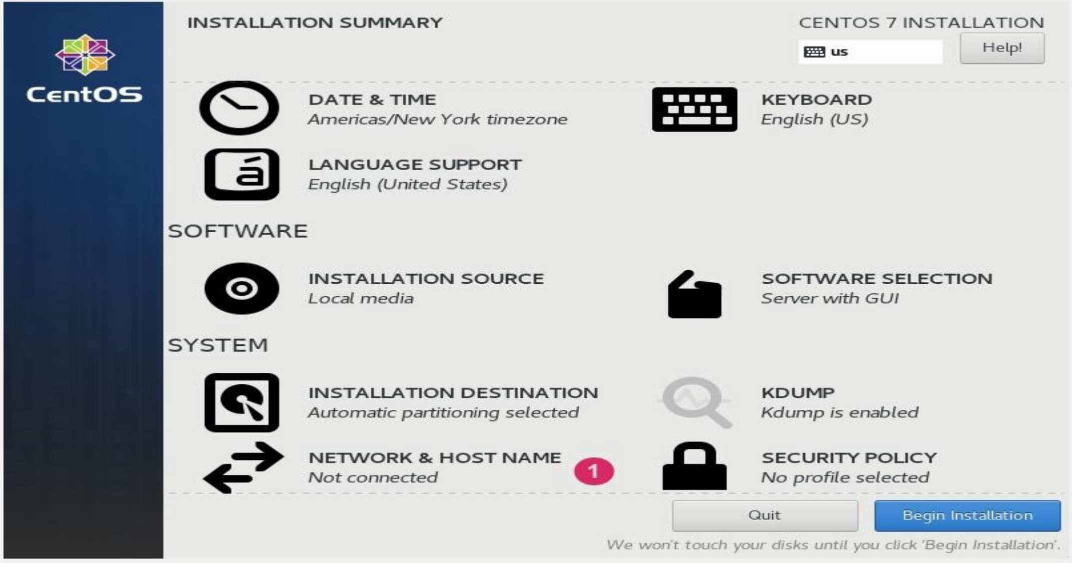
● Automatically configure partitioning. ○ I will configure partitioning.

□ I would like to make additional space available.

Full disk summary and boot loader... 1 disk selected; 25.76 GiB capacity; 25.76 GiB free Refresh...

1. Click done or add custom disk configuration

Step 11: Configure Network



INSTALLATION SUMMARY

CENTOS 7 INSTALLATION

DATE & TIME
Americas/New York timezone

KEYBOARD
English (US)

LANGUAGE SUPPORT
English (United States)

SOFTWARE

INSTALLATION SOURCE
Local media

SOFTWARE SELECTION
Server with GUI

SYSTEM

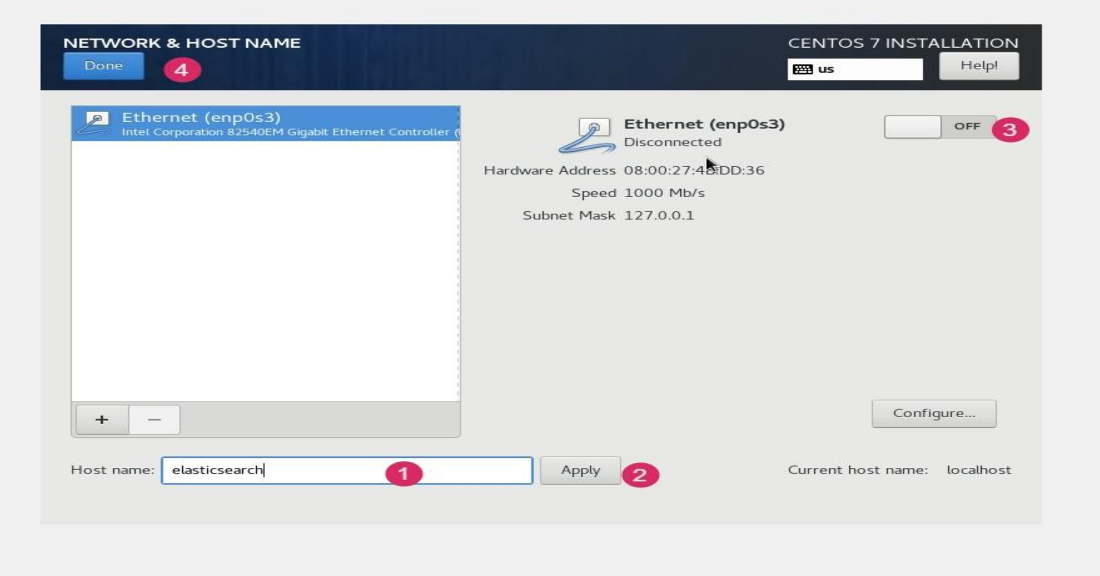
INSTALLATION DESTINATION
Automatic partitioning selected

KDUMP
Kdump is enabled

NETWORK & HOST NAME
Not connected

SECURITY POLICY
No profile selected

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



NETWORK & HOST NAME

CENTOS 7 INSTALLATION

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

Ethernet (enp0s3)
Disconnected

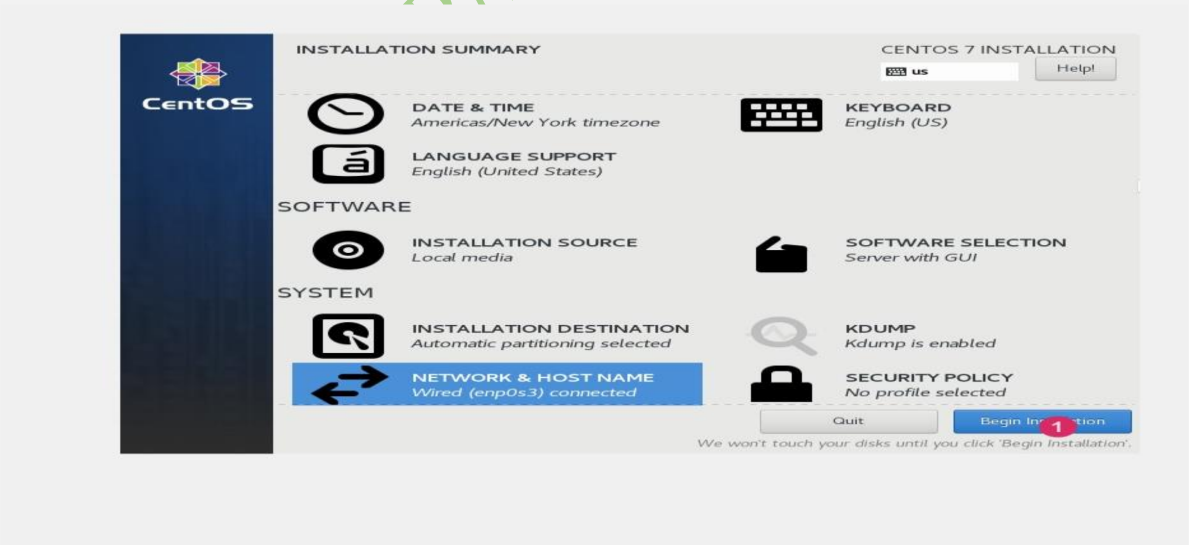
Hardware Address 08:00:27:4B:DD:36
Speed 1000 Mb/s
Subnet Mask 127.0.0.1

Host name: elasticsearch

Current host name: localhost

1. Enter Elasticsearch hostname
2. Click on apply
3. Connect network
4. Click on done button.

Step 12: Begin Installation



INSTALLATION SUMMARY

CENTOS 7 INSTALLATION

DATE & TIME
Americas/New York timezone

KEYBOARD
English (US)

LANGUAGE SUPPORT
English (United States)

SOFTWARE

INSTALLATION SOURCE
Local media

SOFTWARE SELECTION
Server with GUI

SYSTEM

INSTALLATION DESTINATION
Automatic partitioning selected

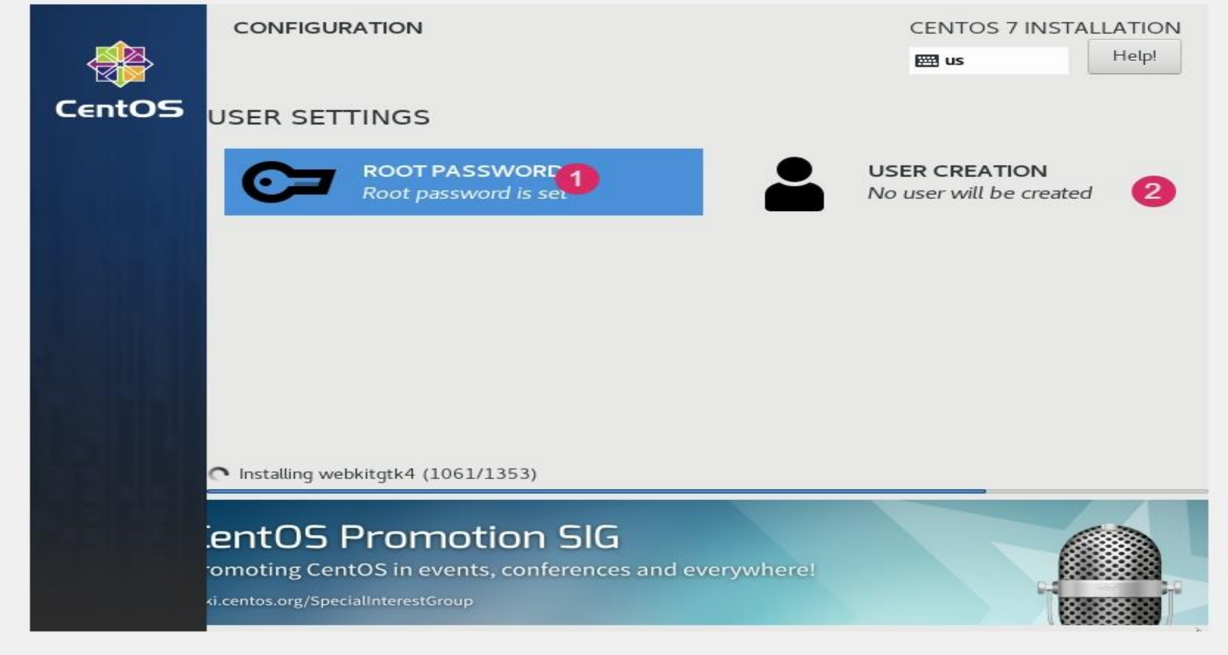
KDUMP
Kdump is enabled

NETWORK & HOST NAME
Wired (enp0s3) connected

SECURITY POLICY
No profile selected

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

Step 13: Account setup (Setup Root account and user account)



Root password is set

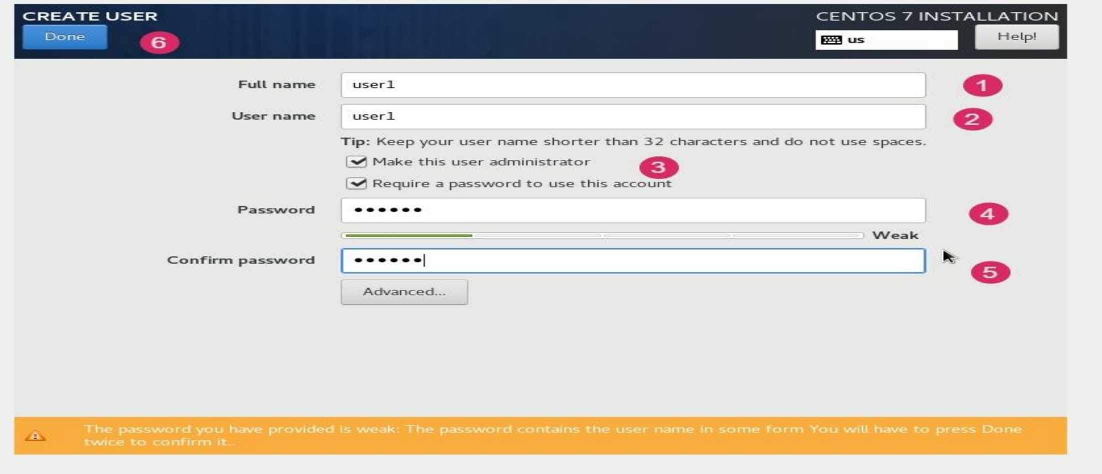
No user will be created

Installing webkitgtk4 (1061/1353)

entOS Promotion SIG
romoting CentOS in events, conferences and everywhere!
ki.centos.org/SpecialInterestGroup

1. Root account setup
2. User account setup

Step 14: User account setup



Full name: user1

User name: user1

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

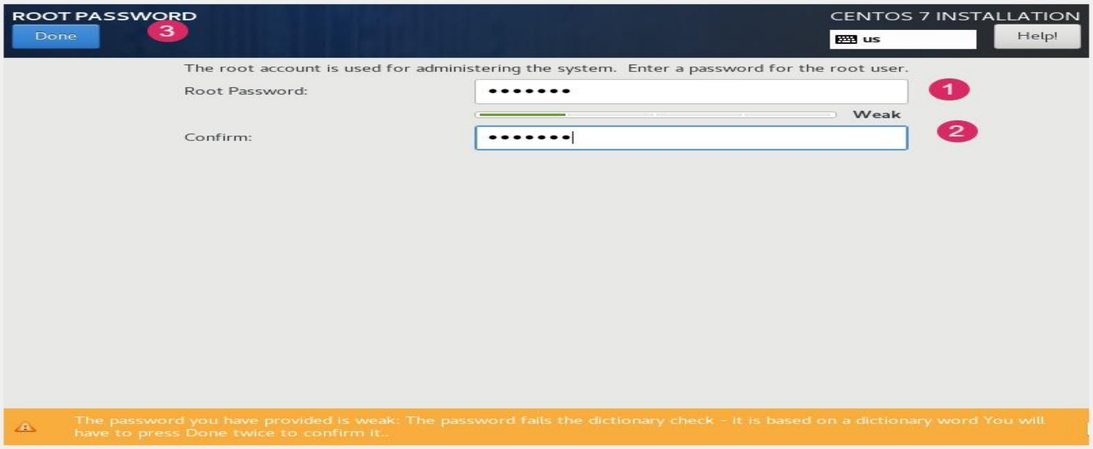
Password: ••••••

Confirm password: ••••••

The password you have provided is weak: The password contains the user name in some form You will have to press Done twice to confirm it.

1. Enter full name
2. Enter a user name
3. Make user an admin by checking the box
4. Enter and (5) confirm password

Setup 15: Root account setup



The root account is used for administering the system. Enter a password for the root user.

Root Password: ••••••••

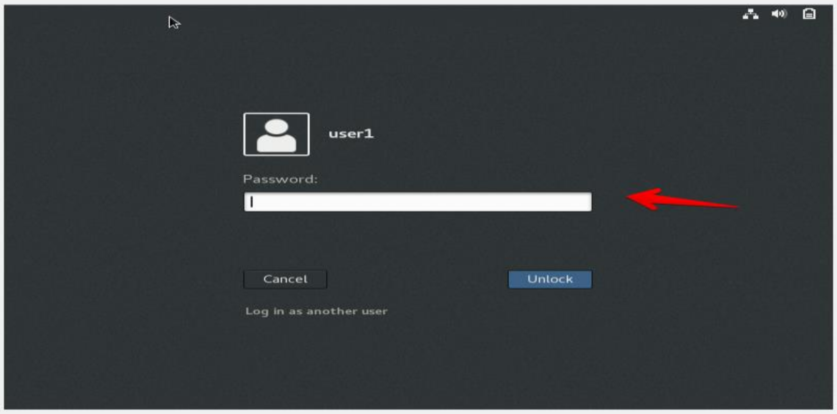
Confirm: ••••••••

The password you have provided is weak: The password fails the dictionary check - it is based on a dictionary word You will have to press Done twice to confirm it..

1. Enter root password
2. Confirm root password
3. Click on done

NB: Once installation completes, click on reboot to restart the server.

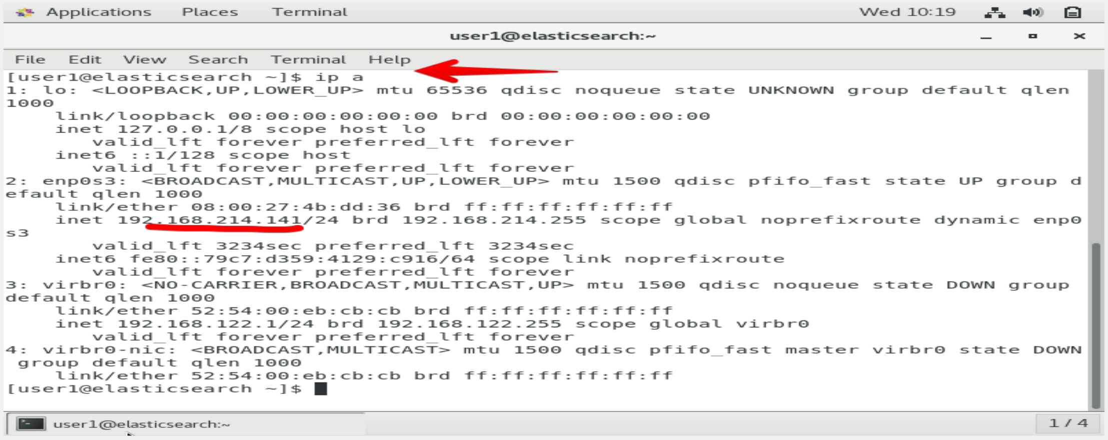
Step 16: Account login



Password:

Step 17: Get server IP

Note: After logging in, you can access the server terminal by right-clicking on the desktop and selecting the terminal option.

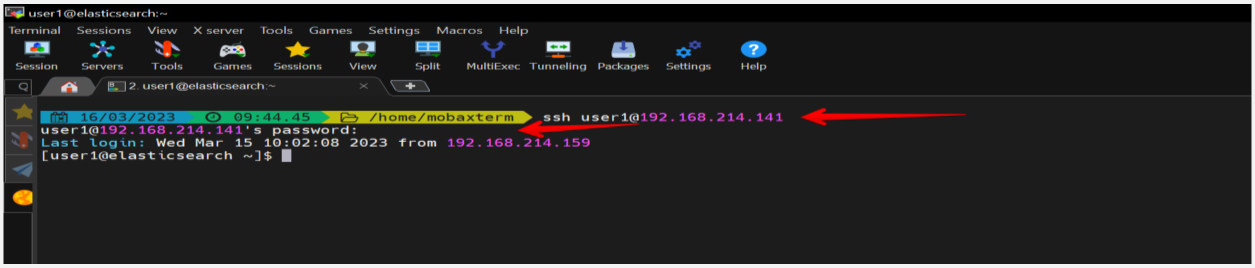


```
[user1@elasticsearch ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group d
efault qlen 1000
    link/ether 08:00:27:4b:dd:36 brd ff:ff:ff:ff:ff:ff
    inet 192.168.214.141/24 brd 192.168.214.255 scope global noprefixroute dynamic enp0
s3
       valid_lft 3234sec preferred_lft 3234sec
    inet6 fe80::79c7:d359:4129:c916/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group
default qlen 1000
    link/ether 52:54:00:eb:cb:cb brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
4: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master virbr0 state DOWN
 group default qlen 1000
    link/ether 52:54:00:eb:cb:cb brd ff:ff:ff:ff:ff:ff
[user1@elasticsearch ~]$
```

1. Get ip address by typing “ip a” on the terminal

2. Copy IP address

Step 18: Access your Elasticsearch server by logging in via Mobaxterm or any other SSH client that you prefer.



```
 16/03/2023  09:44.45  /home/mobaxterm  ssh user1@192.168.214.141
user1@192.168.214.141's password:
Last login: Wed Mar 15 10:02:08 2023 from 192.168.214.159
[user1@elasticsearch ~]$
```

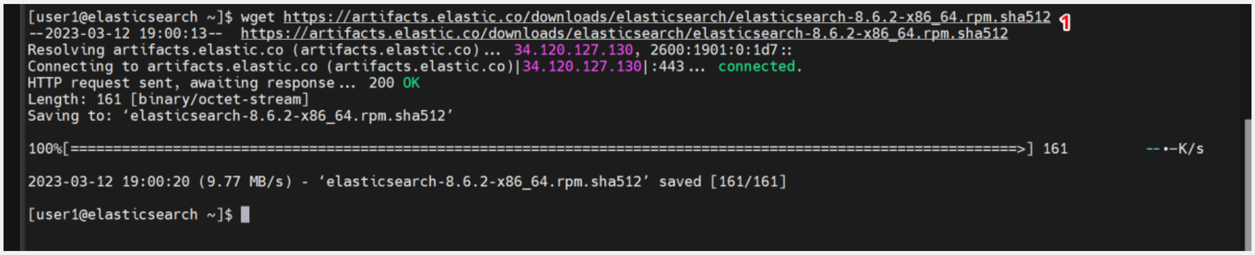
1. Login using server user and IP address
2. Enter your server password

ELASTICSEARCH VERSION 8 INSTALLATION AND CONFIGURATION

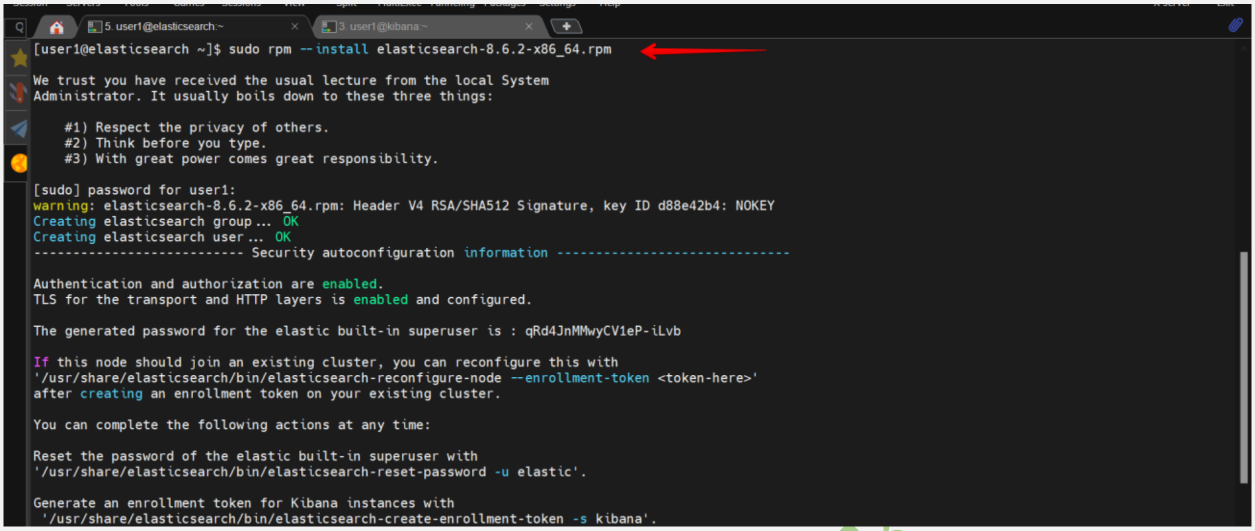
Step 1: Execute the following commands sequentially.

Note: you can get the latest version from: https://www.elastic.co/guide/en/elasticsearch/reference/current/rpm.html#install-rpm

1. wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.6.2-x86_64.rpm
2. wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.6.2-x86_64.rpm.sha512
3. shasum -a 512 -c elasticsearch-8.6.2-x86_64.rpm.sha512
4. sudo rpm --install elasticsearch-8.6.2-x86_64.rpm

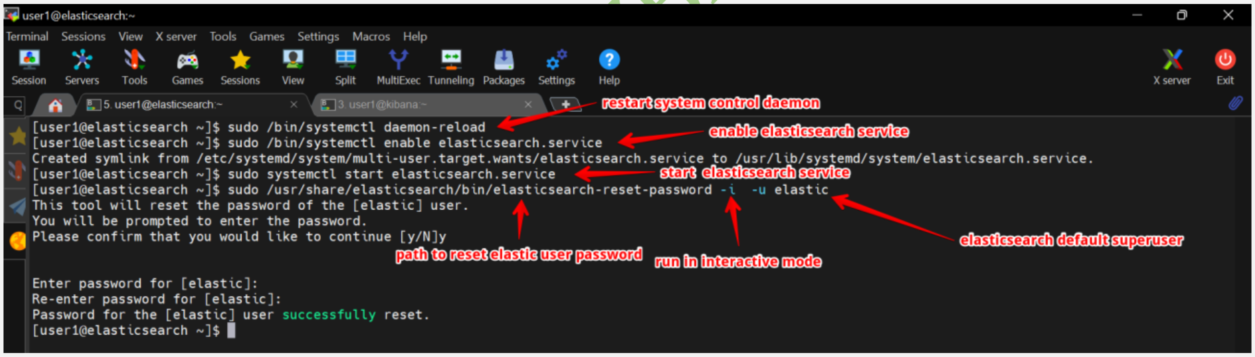


```
[user1@elasticsearch ~]$ wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.6.2-x86_64.rpm.sha512
--2023-03-12 19:00:13--  https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.6.2-x86_64.rpm.sha512
Resolving artifacts.elastic.co (artifacts.elastic.co)... 34.120.127.130, 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-8.6.2-x86_64.rpm.sha512’

100%[===========================================================================================>] 161         --•-K/s

2023-03-12 19:00:20 (9.77 MB/s) - ‘elasticsearch-8.6.2-x86_64.rpm.sha512’ saved [161/161]

[user1@elasticsearch ~]$ █
```



```
[user1@elasticsearch ~]$ sudo rpm --install elasticsearch-8.6.2-x86_64.rpm

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for user1:
warning: elasticsearch-8.6.2-x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID d88e42b4: NOKEY
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 : qRd4JnMMwyCV1eP-iLvb

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'.
```

Step 2: Running Elasticsearch



```
[user1@elasticsearch ~]$ sudo /bin/systemctl daemon-reload
[user1@elasticsearch ~]$ sudo /bin/systemctl enable elasticsearch.service
Created symlink from /etc/systemd/system/multi-user.target.wants/elasticsearch.service to /usr/lib/systemd/system/elasticsearch.service.
[user1@elasticsearch ~]$ sudo systemctl start elasticsearch.service
[user1@elasticsearch ~]$ sudo /usr/share/elasticsearch/bin/elasticsearch-reset-password -i  -u elastic
This tool will reset the password of the [elastic] user.
You will be prompted to enter the password.
Please confirm that you would like to continue [y/N]y


Enter password for [elastic]:
Re-enter password for [elastic]:
Password for the [elastic] user successfully reset.
[user1@elasticsearch ~]$ 
```

restart system control daemon

enable elasticsearch service

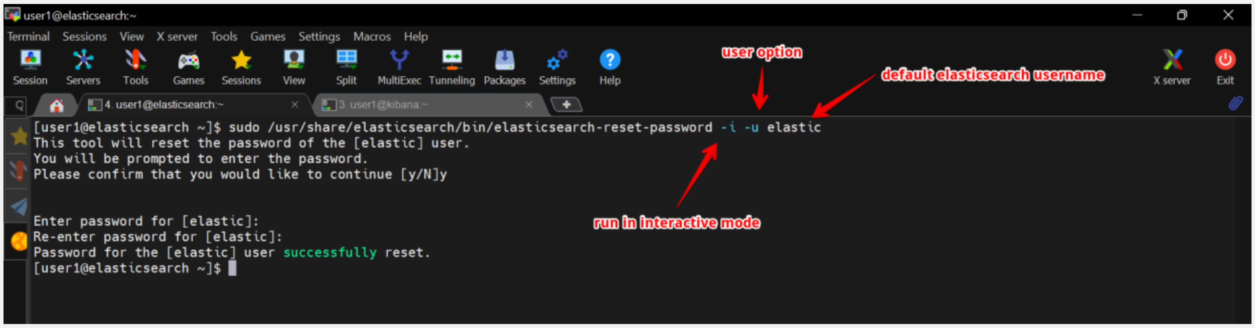
start elasticsearch service

path to reset elastic user password

run in interactive mode

elasticsearch default superuser

Step 3: Reset Elasticsearch default user password



user option

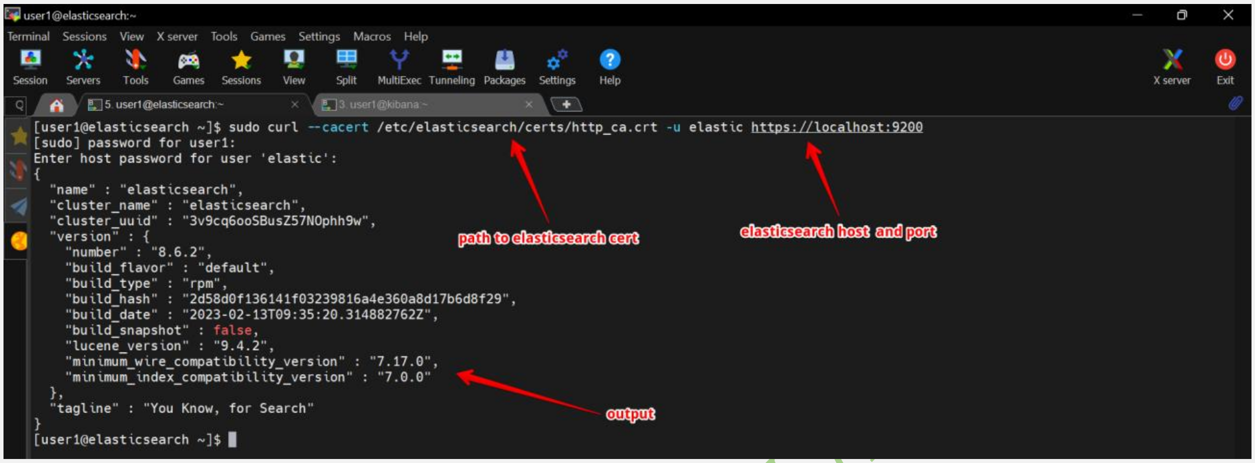
default elasticsearch username

```
[user1@elasticsearch ~]$ sudo /usr/share/elasticsearch/bin/elasticsearch-reset-password -i -u elastic
This tool will reset the password of the [elastic] user.
You will be prompted to enter the password.
Please confirm that you would like to continue [y/N]y


Enter password for [elastic]:
Re-enter password for [elastic]:
Password for the [elastic] user successfully reset.
[user1@elasticsearch ~]$ 
```

run in interactive mode

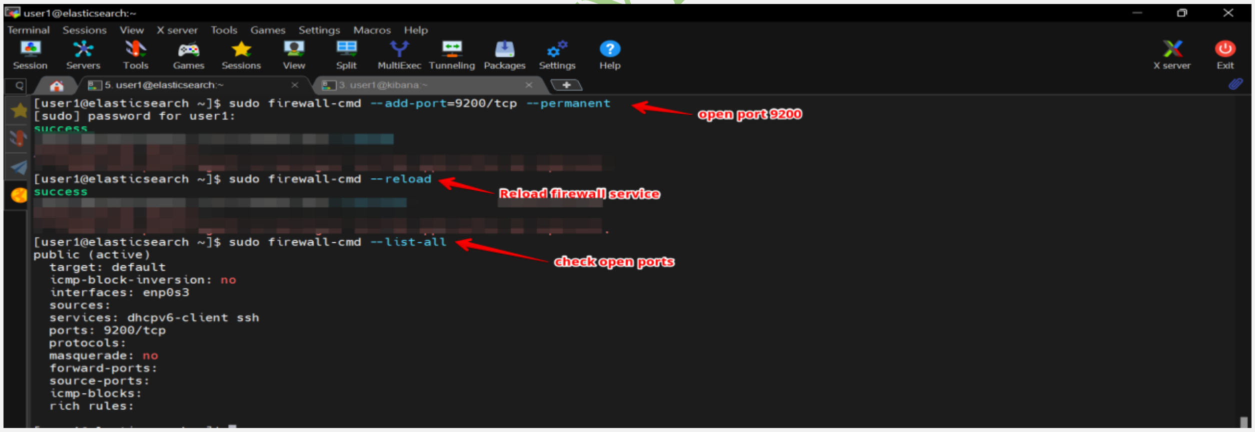
Step 4: Verify if Elasticsearch is up and running with this command

Cmd: sudo curl –cacert /etc/elasticsearch/http_ca.crt –u https://localhost:9200



```
[user1@elasticsearch ~]$ sudo curl --cacert /etc/elasticsearch/certs/http_ca.crt -u elastic https://localhost:9200
[sudo] password for user1:
Enter host password for user 'elastic':
{
  "name" : "elasticsearch",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "3v9cq6ooSBusZ57NOphh9w",
  "version" : {
    "number" : "8.6.2",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "2d58d0f136141f03239816a4e360a8d17b6d8f29",
    "build_date" : "2023-02-13T09:35:20.314882762Z",
    "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"
}
[user1@elasticsearch ~]$
```

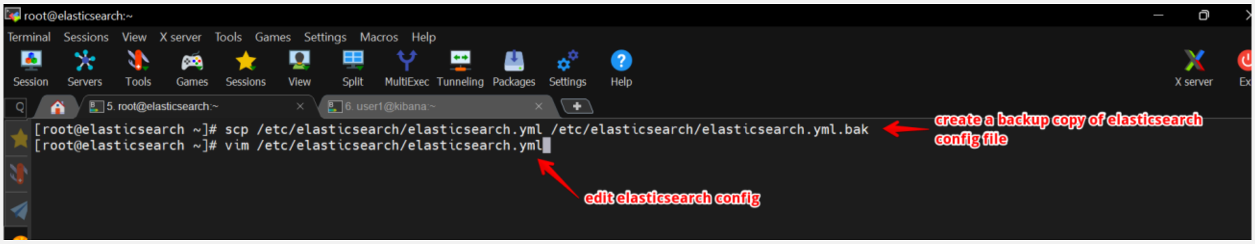
Step 5: To enable Elasticsearch to listen on port 9200 through the firewall, you can use the firewall-cmd command. Here's how:



```
[user1@elasticsearch ~]$ sudo firewall-cmd --add-port=9200/tcp --permanent
[sudo] password for user1:
success
[redacted]
[user1@elasticsearch ~]$ sudo firewall-cmd --reload
success
[redacted]
[user1@elasticsearch ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpv6-client ssh
  ports: 9200/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Step 6: Edit Elasticsearch configuration file

Note: Make a backup of the configuration file before editing

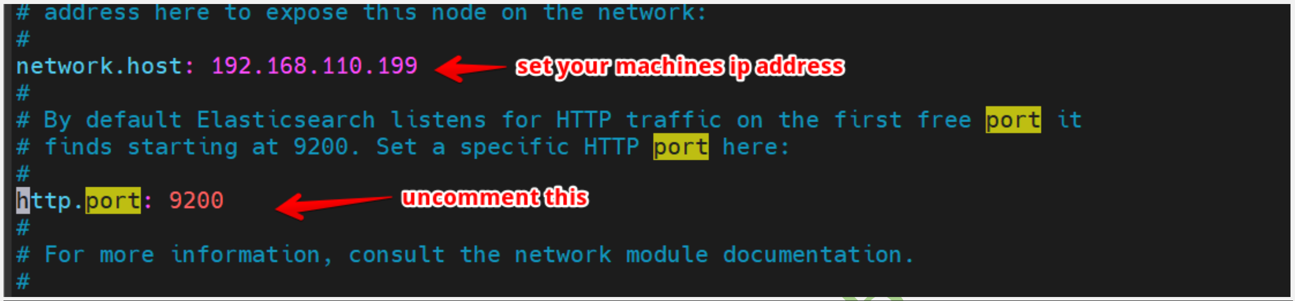

root@elasticsearch:~
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Ex
5. root@elasticsearch:~
6. user1@kibana:~

```
[root@elasticsearch ~]# scp /etc/elasticsearch/elasticsearch.yml /etc/elasticsearch/elasticsearch.yml.bak
[root@elasticsearch ~]# vim /etc/elasticsearch/elasticsearch.yml
```

create a backup copy of elasticsearch config file

edit elasticsearch config

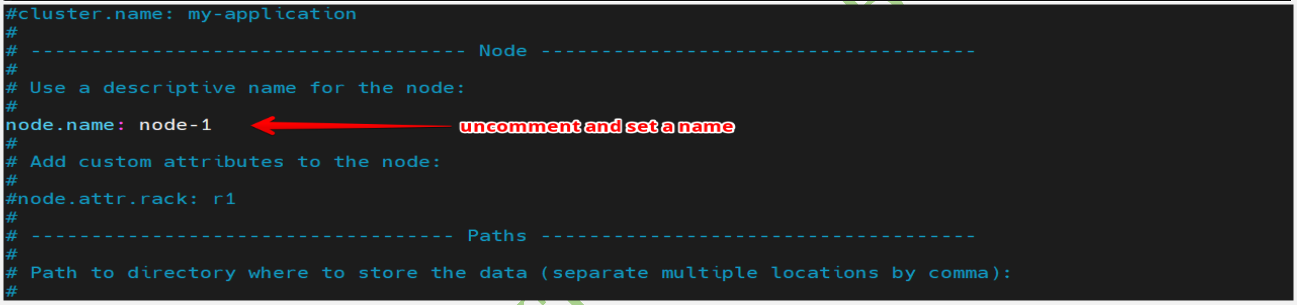
- set Node name, network host and port



```
# address here to expose this node on the network:
#
network.host: 192.168.110.199
#
# 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.
#
```

set your machines ip address

uncomment this



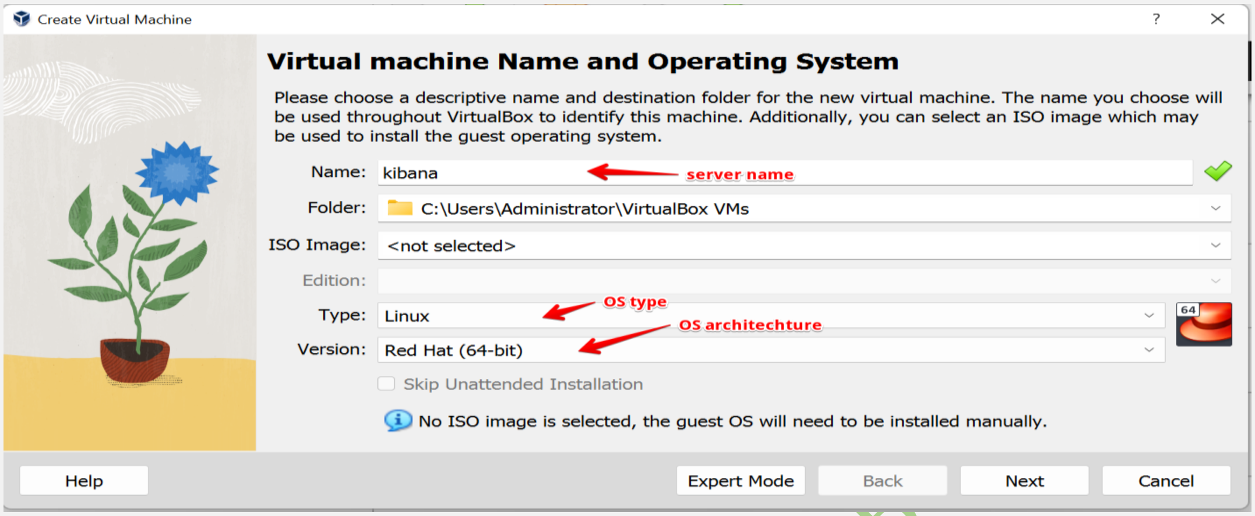
```
#cluster.name: my-application
#
# ------------------------------------ Node ------------------------------------
#
# Use a descriptive name for the node:
#
node.name: node-1
#
# Add custom attributes to the node:
#
#node.attr.rack: r1
#
# ----------------------------------- Paths ------------------------------------
#
# Path to directory where to store the data (separate multiple locations by comma):
#
```

uncomment and set a name

KIBANA INSTALLATION AND SETUP

Step 1: Create a new virtual machine

NOTE: Please utilize the same virtual machine setup guide that was used for setting up the Elasticsearch server.



Create Virtual Machine

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: kibana

Folder: C:\Users\Administrator\VirtualBox VMs

ISO Image: <not selected>

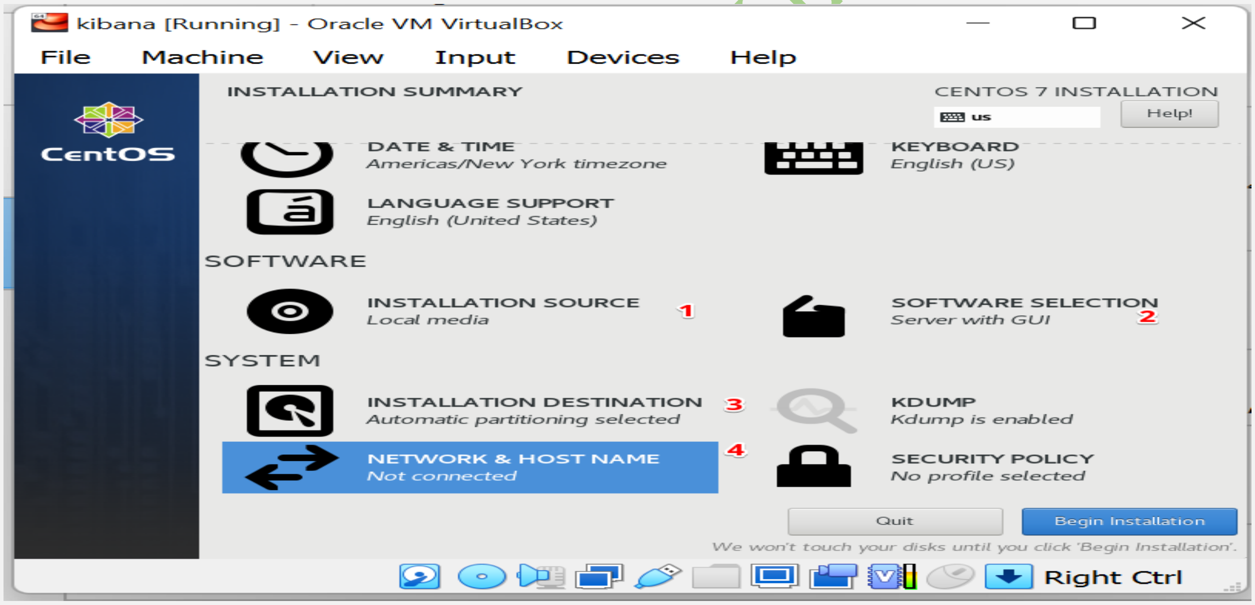
Edition:

Type: Linux

Version: Red Hat (64-bit)

☐ Skip Unattended Installation

No ISO image is selected, the guest OS will need to be installed manually.



kibana [Running] - Oracle VM VirtualBox

INSTALLATION SUMMARY

CENTOS 7 INSTALLATION

DATE & TIME
Americas/New York timezone

KEYBOARD
English (US)

LANGUAGE SUPPORT
English (United States)

SOFTWARE

INSTALLATION SOURCE
Local media

SOFTWARE SELECTION
Server with GUI

SYSTEM

INSTALLATION DESTINATION
Automatic partitioning selected

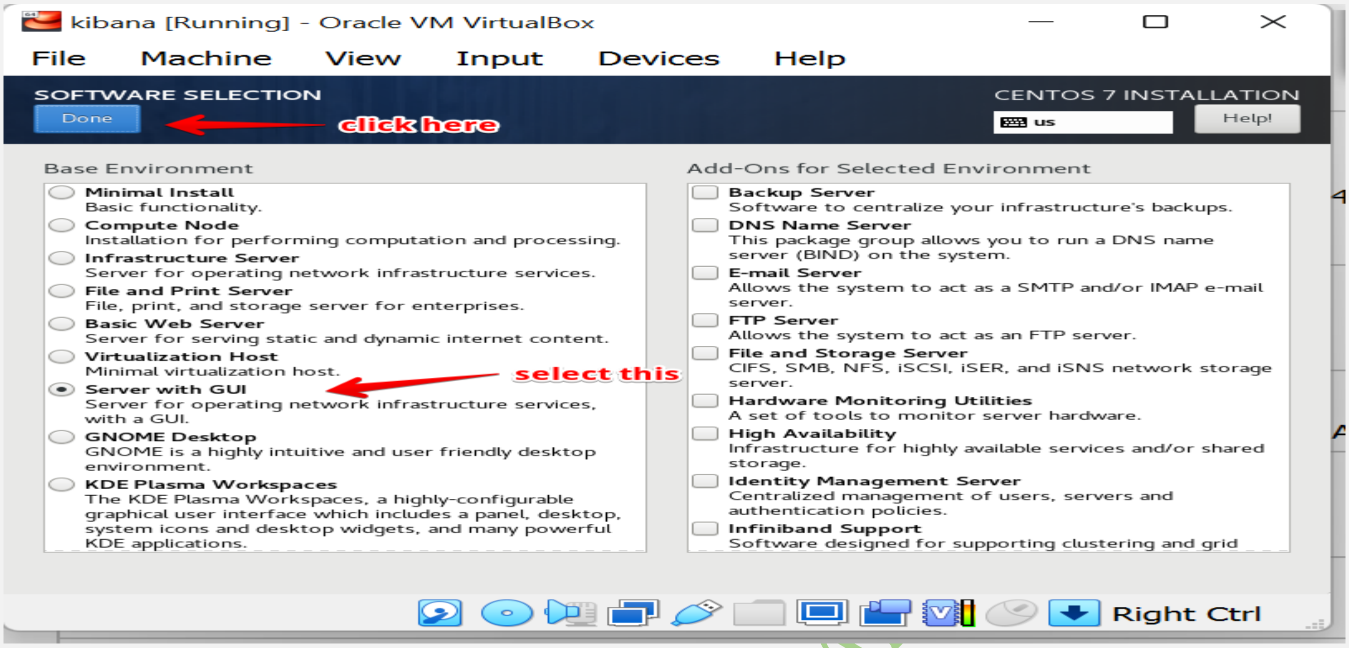
KDUMP
Kdump is enabled

NETWORK & HOST NAME
Not connected

SECURITY POLICY
No profile selected

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

a. Setup partition manager



SOFTWARE SELECTION

CENTOS 7 INSTALLATION

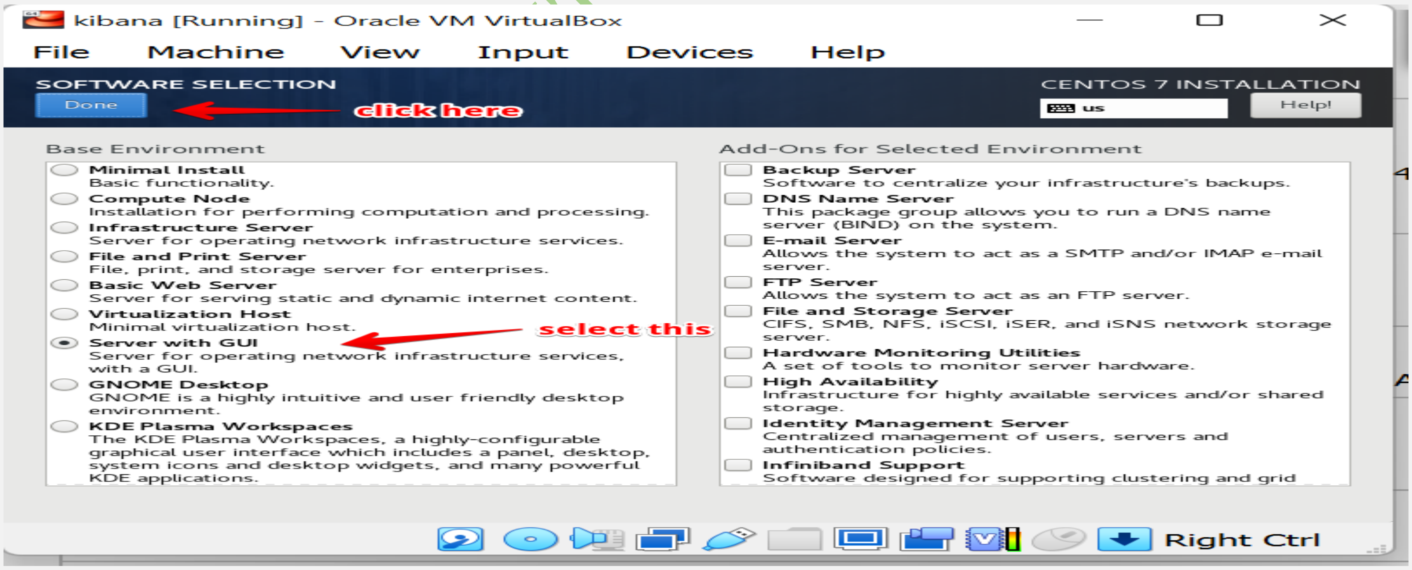
Base Environment

○ **Minimal Install**
Basic functionality.
○ **Compute Node**
Installation for performing computation and processing.
○ **Infrastructure Server**
Server for operating network infrastructure services.
○ **File and Print Server**
File, print, and storage server for enterprises.
○ **Basic Web Server**
Server for serving static and dynamic internet content.
○ **Virtualization Host**
Minimal virtualization host.
● **Server with GUI**
Server for operating network infrastructure services, with a GUI.
○ **GNOME Desktop**
GNOME is a highly intuitive and user friendly desktop environment.
○ **KDE Plasma Workspaces**
The KDE Plasma Workspaces, a highly-configurable graphical user interface which includes a panel, desktop, system icons and desktop widgets, and many powerful KDE applications.

Add-Ons for Selected Environment

□ **Backup Server**
Software to centralize your infrastructure's backups.
□ **DNS Name Server**
This package group allows you to run a DNS name server (BIND) on the system.
□ **E-mail Server**
Allows the system to act as a SMTP and/or IMAP e-mail server.
□ **FTP Server**
Allows the system to act as an FTP server.
□ **File and Storage Server**
CIFS, SMB, NFS, iSCSI, iSER, and iSNS network storage server.
□ **Hardware Monitoring Utilities**
A set of tools to monitor server hardware.
□ **High Availability**
Infrastructure for highly available services and/or shared storage.
□ **Identity Management Server**
Centralized management of users, servers and authentication policies.
□ **Infiniband Support**
Software designed for supporting clustering and grid

b. Setup Installation type


SOFTWARE SELECTION

CENTOS 7 INSTALLATION

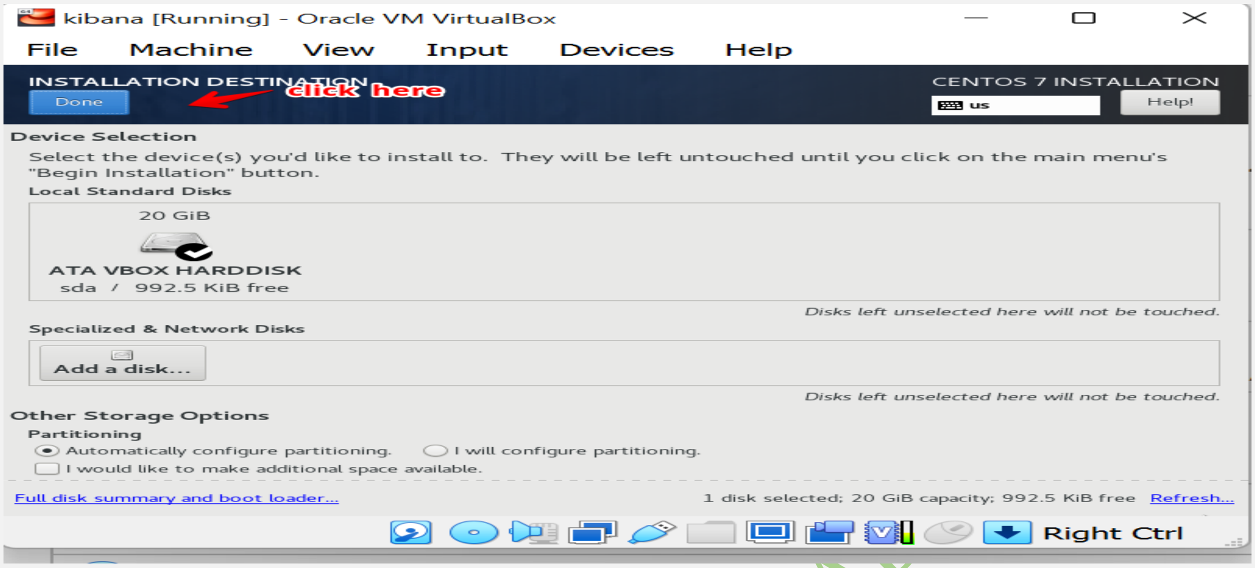
Base Environment

○ **Minimal Install**
Basic functionality.
○ **Compute Node**
Installation for performing computation and processing.
○ **Infrastructure Server**
Server for operating network infrastructure services.
○ **File and Print Server**
File, print, and storage server for enterprises.
○ **Basic Web Server**
Server for serving static and dynamic internet content.
○ **Virtualization Host**
Minimal virtualization host.
● **Server with GUI**
Server for operating network infrastructure services, with a GUI.
○ **GNOME Desktop**
GNOME is a highly intuitive and user friendly desktop environment.
○ **KDE Plasma Workspaces**
The KDE Plasma Workspaces, a highly-configurable graphical user interface which includes a panel, desktop, system icons and desktop widgets, and many powerful KDE applications.

Add-Ons for Selected Environment

□ **Backup Server**
Software to centralize your infrastructure's backups.
□ **DNS Name Server**
This package group allows you to run a DNS name server (BIND) on the system.
□ **E-mail Server**
Allows the system to act as a SMTP and/or IMAP e-mail server.
□ **FTP Server**
Allows the system to act as an FTP server.
□ **File and Storage Server**
CIFS, SMB, NFS, iSCSI, iSER, and iSNS network storage server.
□ **Hardware Monitoring Utilities**
A set of tools to monitor server hardware.
□ **High Availability**
Infrastructure for highly available services and/or shared storage.
□ **Identity Management Server**
Centralized management of users, servers and authentication policies.
□ **Infiniband Support**
Software designed for supporting clustering and grid

c. Server Partition Setup



kibana [Running] - Oracle VM VirtualBox

Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

20 GiB

ATA VBOX HARDDISK

sda / 992.5 KiB free

Disks left unselected here will not be touched.

Specialized & Network Disks

Add a disk...

Disks left unselected here will not be touched.

Other Storage Options

Partitioning

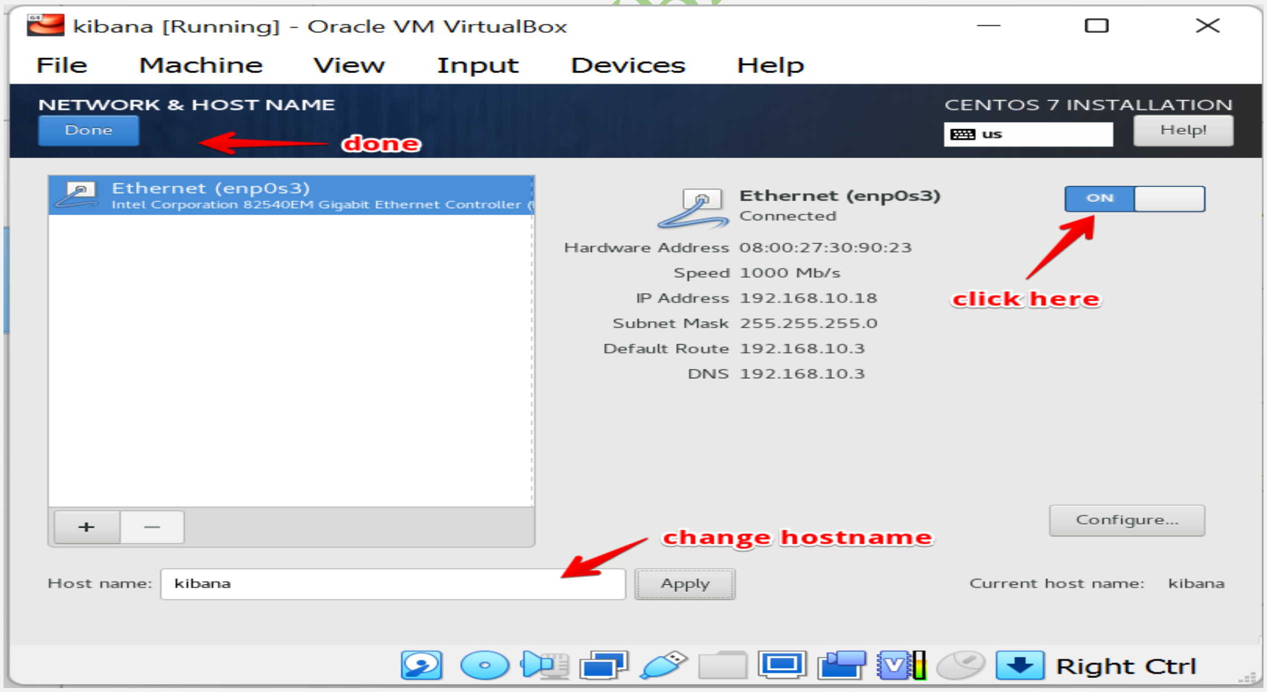
● Automatically configure partitioning. ○ I will configure partitioning.

□ I would like to make additional space available.

Full disk summary and boot loader...

1 disk selected; 20 GiB capacity; 992.5 KiB free Refresh...

d. Server Network setup



kibana [Running] - Oracle VM VirtualBox

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

Ethernet (enp0s3)
Connected

ON

Hardware Address 08:00:27:30:90:23

Speed 1000 Mb/s

IP Address 192.168.10.18

Subnet Mask 255.255.255.0

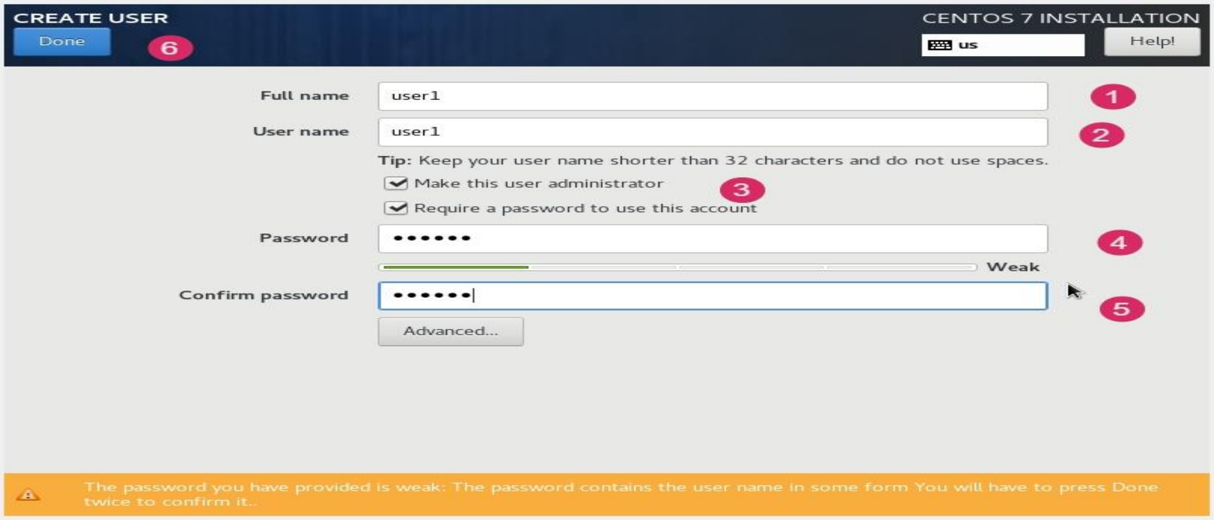
Default Route 192.168.10.3

DNS 192.168.10.3

Host name: kibana Apply

Current host name: kibana

Step 2: User Account Setup


CREATE USER

Full name: user1

User name: user1

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: ••••••

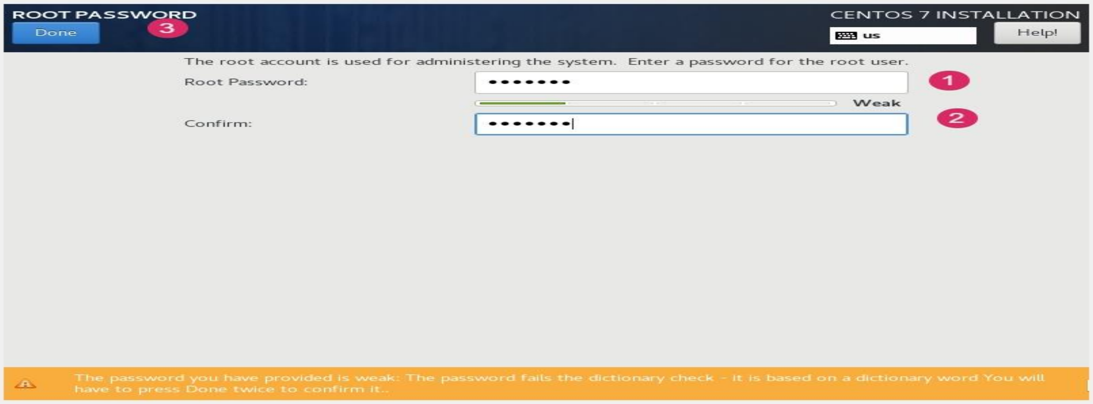
Weak

Confirm password: ••••••

The password you have provided is weak: The password contains the user name in some form You will have to press Done twice to confirm it..

1. Enter full name
2. Enter a user name
3. Make user an admin by checking the box
4. Create password
5. Confirm password

Step 3: Root account setup


ROOT PASSWORD

The root account is used for administering the system. Enter a password for the root user.

Root Password: •••••••

Weak

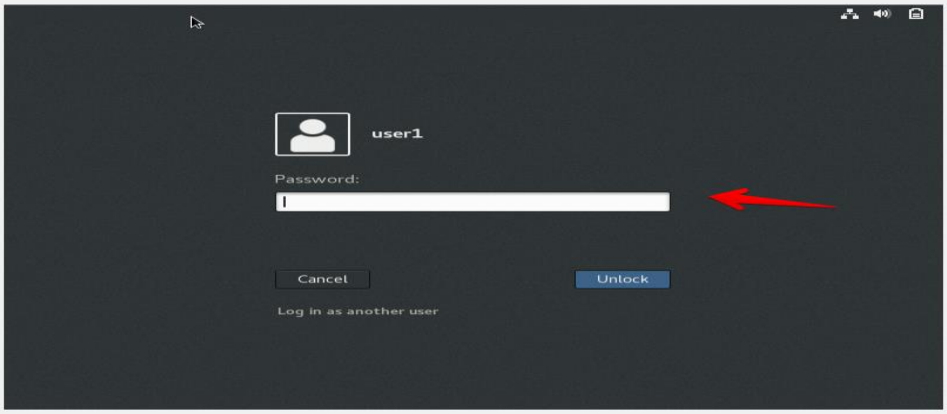
Confirm: •••••••

The password you have provided is weak: The password fails the dictionary check - it is based on a dictionary word You will have to press Done twice to confirm it..

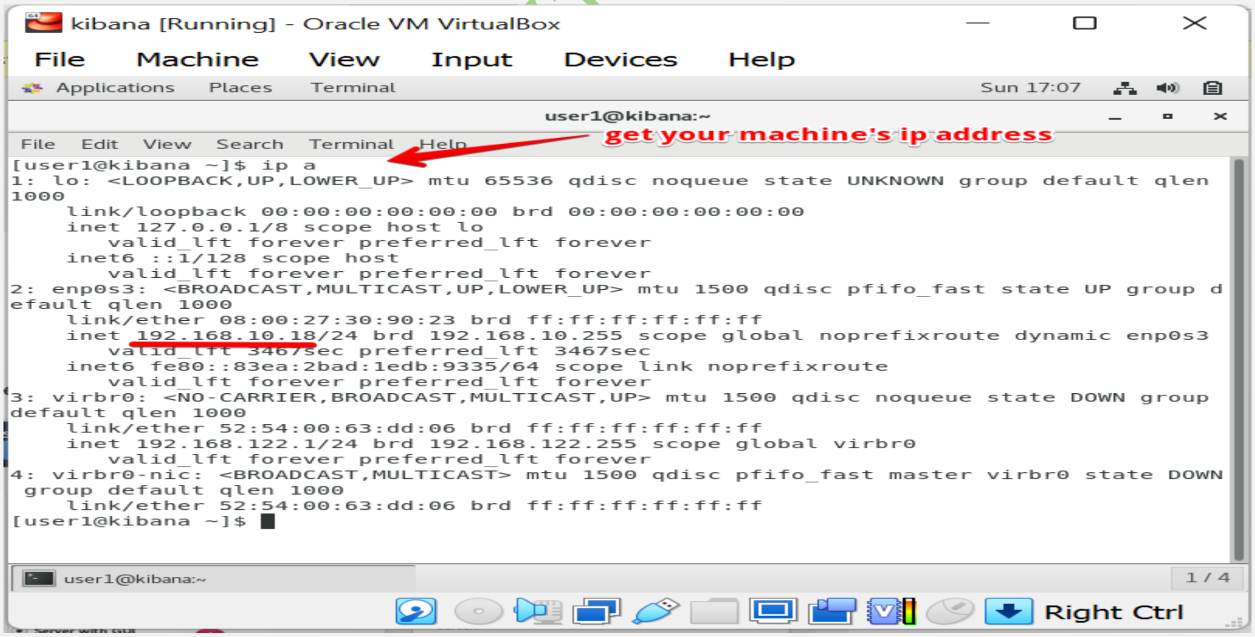
1. Enter root password
2. Confirm root password
3. Click on done

NOTE: Once the installation completes, click on reboot to restart the server

Step 4: Account Login



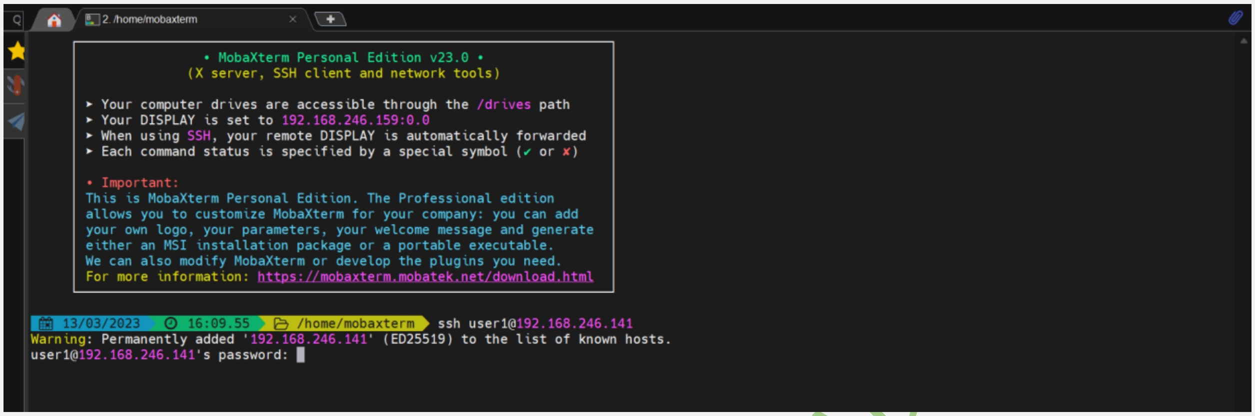
Step 5: Get server IP



get your machine's ip address

```
[user1@kibana ~]$ 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group d
efault qlen 1000
    link/ether 08:00:27:30:90:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.18/24 brd 192.168.10.255 scope global noprefixroute dynamic enp0s3
       valid_lft 3467sec preferred_lft 3467sec
    inet6 fe80::83ea:2bad:1edb:9335/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group
default qlen 1000
    link/ether 52:54:00:63:dd:06 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
4: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master virbr0 state DOWN
 group default qlen 1000
    link/ether 52:54:00:63:dd:06 brd ff:ff:ff:ff:ff:ff
[user1@kibana ~]$ █
```

Step 6: Server Login, from Mobaxterm

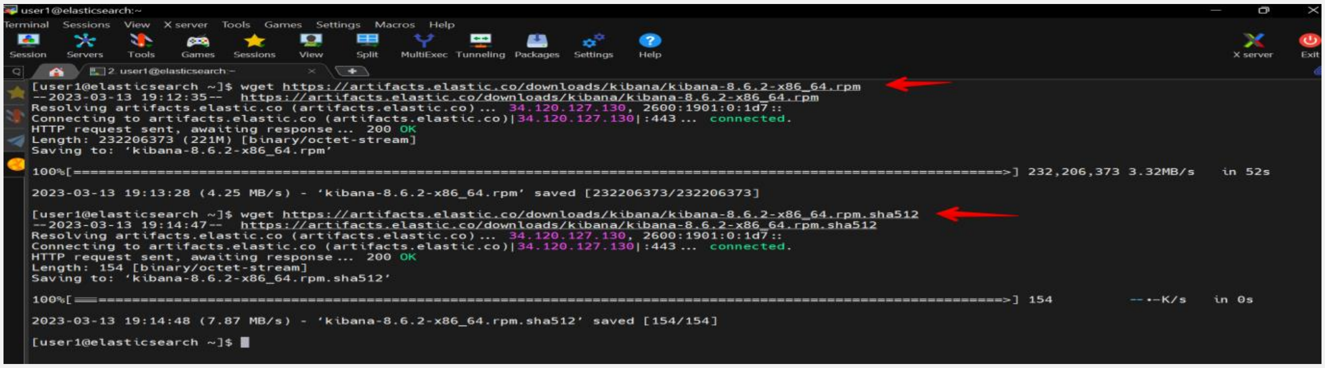


```
        • MobaXterm Personal Edition v23.0 •
      (X server, SSH client and network tools)

 ➤ Your computer drives are accessible through the /drives path
 ➤ Your DISPLAY is set to 192.168.246.159:0.0
 ➤ When using SSH, your remote DISPLAY is automatically forwarded
 ➤ Each command status is specified by a special symbol (✓ or ✗)

 • Important:
 This is MobaXterm Personal Edition. The Professional edition
 allows you to customize MobaXterm for your company: you can add
 your own logo, your parameters, your welcome message and generate
 either an MSI installation package or a portable executable.
 We can also modify MobaXterm or develop the plugins you need.
 For more information: https://mobaxterm.mobatek.net/download.html

 13/03/2023  16:09.55  /home/mobaxterm  ssh user1@192.168.246.141
Warning: Permanently added '192.168.246.141' (ED25519) to the list of known hosts.
user1@192.168.246.141's password: █
```

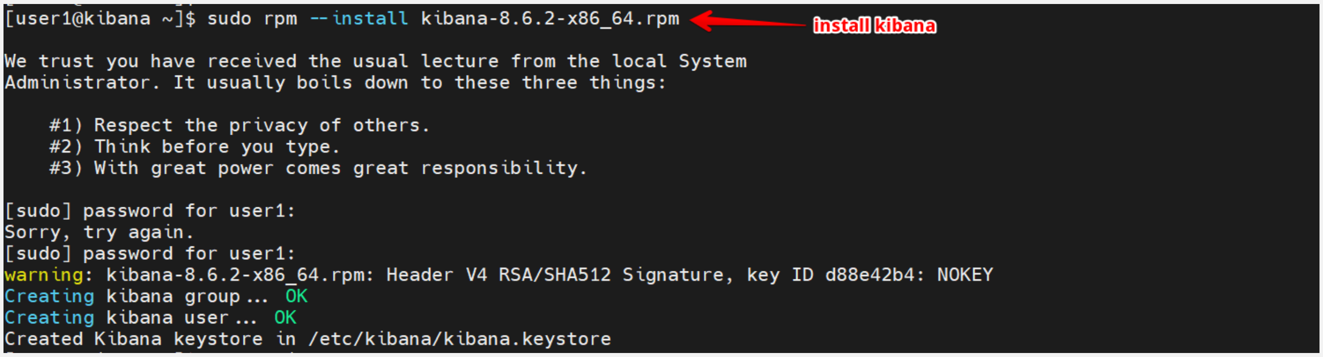
Step 8: Kibana Download and Installation

Run the following commands sequentially

1. wget https://artifacts.elastic.co/downloads/kibana/kibana-8.6.2-x86_64.rpm
2. wget https://artifacts.elastic.co/downloads/kibana/kibana-8.6.2-x86_64.rpm.sha512
3. shasum -a 512 -c kibana-8.6.2-x86_64.rpm
4. sudo rpm --install kibana-8.6.2-x86_64.rpm

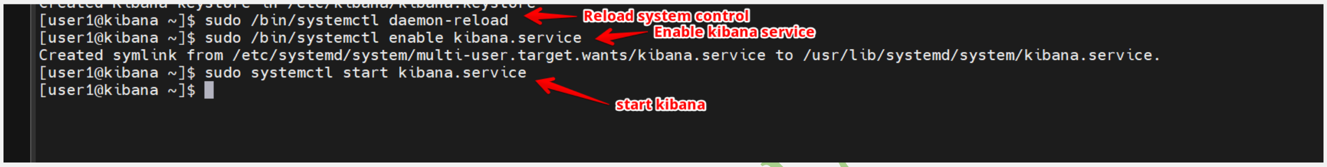


```
[user1@elasticsearch ~]$ wget https://artifacts.elastic.co/downloads/kibana/kibana-8.6.2-x86_64.rpm
--2023-03-13 19:12:35--  https://artifacts.elastic.co/downloads/kibana/kibana-8.6.2-x86_64.rpm
Resolving artifacts.elastic.co (artifacts.elastic.co)... 34.120.127.130, 2600:1901:0:1d7::
Connecting to artifacts.elastic.co (artifacts.elastic.co)|34.120.127.130|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 232206373 (221M) [binary/octet-stream]
Saving to: 'kibana-8.6.2-x86_64.rpm'

100%[=================================================================================================>] 232,206,373 3.32MB/s   in 52s

2023-03-13 19:13:28 (4.25 MB/s) - 'kibana-8.6.2-x86_64.rpm' saved [232206373/232206373]

[user1@elasticsearch ~]$ wget https://artifacts.elastic.co/downloads/kibana/kibana-8.6.2-x86_64.rpm.sha512
--2023-03-13 19:14:47--  https://artifacts.elastic.co/downloads/kibana/kibana-8.6.2-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: 154 [binary/octet-stream]
Saving to: 'kibana-8.6.2-x86_64.rpm.sha512'

100%[=================================================================================================>] 154          --.-K/s   in 0s

2023-03-13 19:14:48 (7.87 MB/s) - 'kibana-8.6.2-x86_64.rpm.sha512' saved [154/154]

[user1@elasticsearch ~]$ █
```



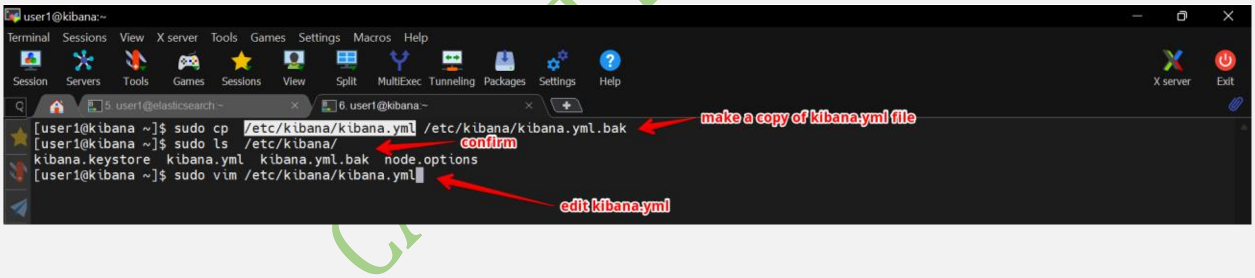
```
[user1@kibana ~]$ sudo rpm --install kibana-8.6.2-x86_64.rpm

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for user1:
Sorry, try again.
[sudo] password for user1:
warning: kibana-8.6.2-x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID d88e42b4: NOKEY
Creating kibana group... OK
Creating kibana user... OK
Created Kibana keystore in /etc/kibana/kibana.keystore
```

Step 9: Enable and run Kibana



```
[user1@kibana ~]$ sudo /bin/systemctl daemon-reload
[user1@kibana ~]$ sudo /bin/systemctl enable kibana.service
Created symlink from /etc/systemd/system/multi-user.target.wants/kibana.service to /usr/lib/systemd/system/kibana.service.
[user1@kibana ~]$ sudo systemctl start kibana.service
[user1@kibana ~]$ 
```

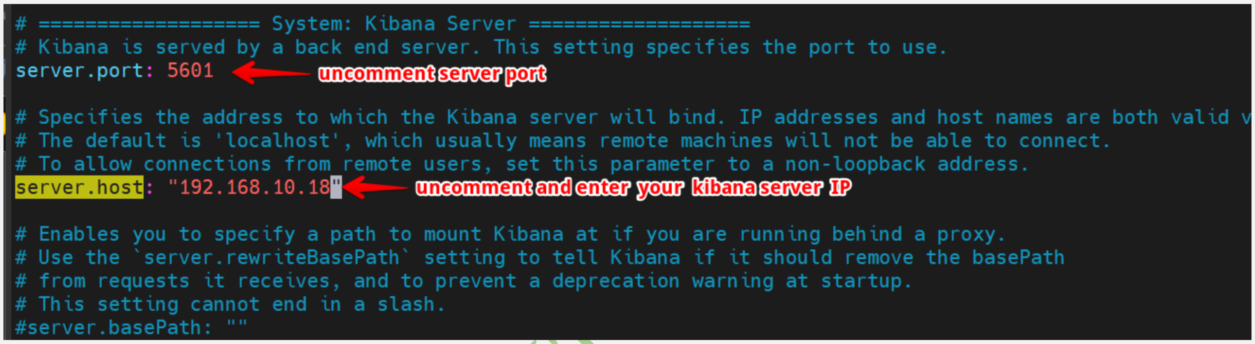
Step 10: Create a duplicate of the Kibana configuration file, and modify the primary Kibana configuration file.



```
[user1@kibana ~]$ sudo cp /etc/kibana/kibana.yml /etc/kibana/kibana.yml.bak
[user1@kibana ~]$ sudo ls /etc/kibana/
kibana.keystore  kibana.yml  kibana.yml.bak  node.options
[user1@kibana ~]$ sudo vim /etc/kibana/kibana.yml
```

Step 10: Update the configuration file

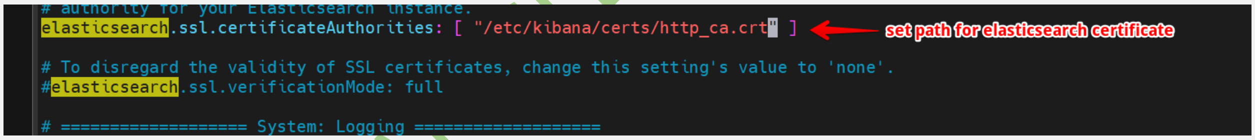
- Go to the server port and remove the commenting to enable it.
- Configure the server.host property with the IP address of the Kibana server.
- Set the elasticsearch.host field to the IP address of the Elasticsearch server.
- Configure the Elasticsearch credentials that Kibana will use for authentication.
- Enable SSL certificate authorities for Kibana. Provide the path where Kibana will locate the Elasticsearch SSL certificate



```
# =================== 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 v
# 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: "192.168.10.18"

# 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: ""
```

uncomment server port

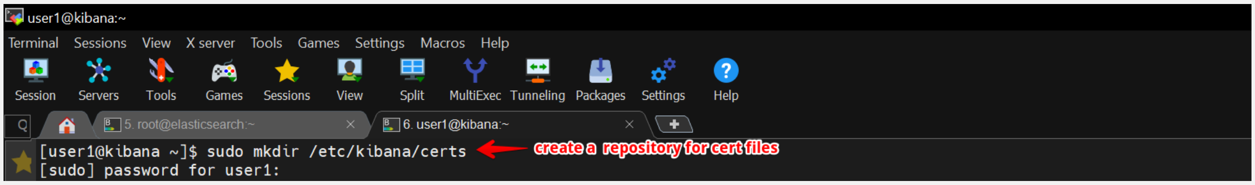
uncomment and enter your kibana server IP



```
  # authority for your Elasticsearch instance.
  elasticsearch.ssl.certificateAuthorities: [ "/etc/kibana/certs/http_ca.crt" ]

  # To disregard the validity of SSL certificates, change this setting's value to 'none'.
  #elasticsearch.ssl.verificationMode: full

  # ================== System: Logging ==================
```

set path for elasticsearch certificate

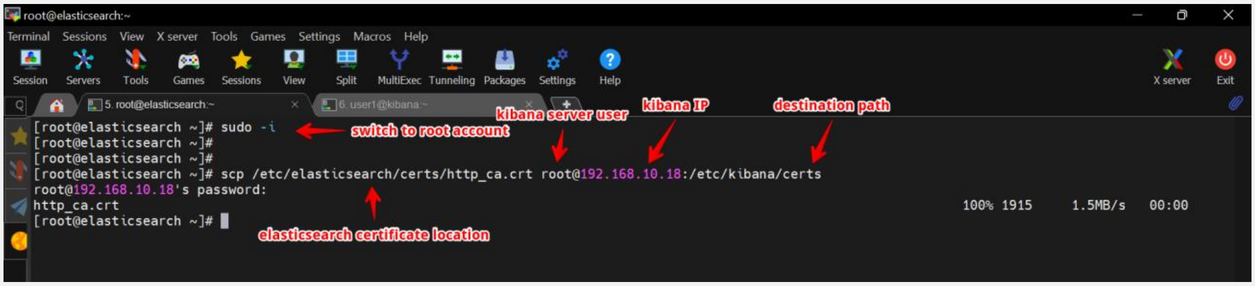
Step 11: Create a directory named "certs" within the "/etc/kibana/" path to store the Elasticsearch SSL certificate.



```
[user1@kibana ~]$ sudo mkdir /etc/kibana/certs
[sudo] password for user1:
```

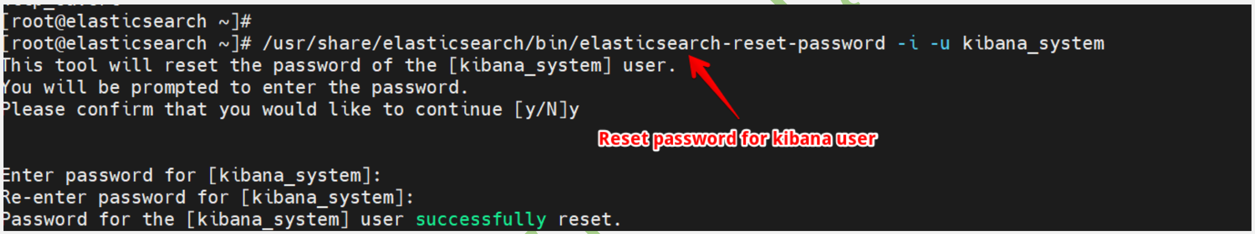
create a repository for cert files

Step 12: Login to Elasticsearch server and transfer the SSL certificate to kibana server



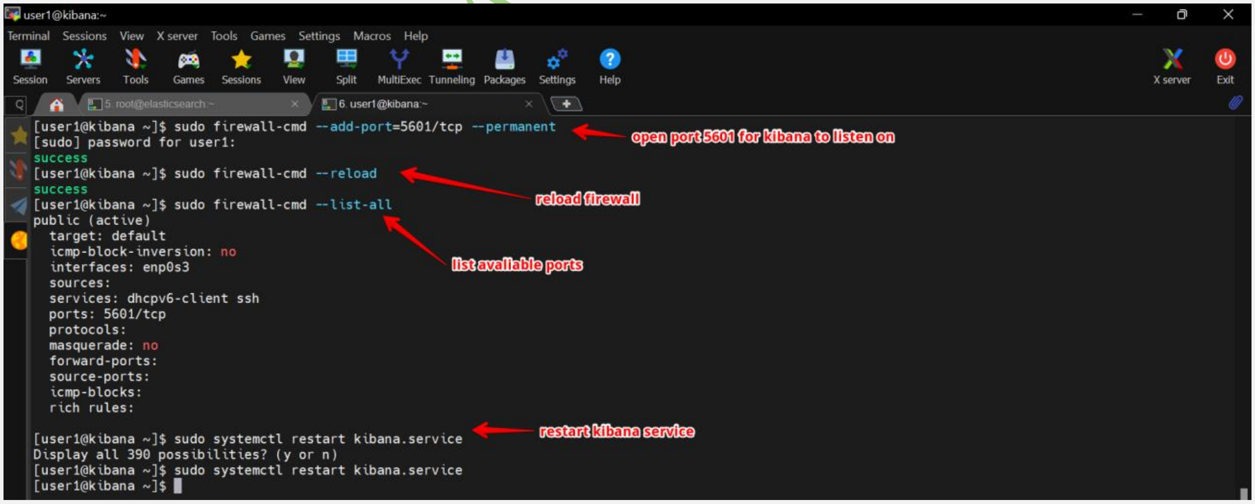
```
[root@elasticsearch ~]# sudo -i
[root@elasticsearch ~]#
[root@elasticsearch ~]#
[root@elasticsearch ~]# scp /etc/elasticsearch/certs/http_ca.crt root@192.168.10.18:/etc/kibana/certs
root@192.168.10.18's password:
http_ca.crt                                                                   100% 1915     1.5MB/s   00:00
[root@elasticsearch ~]#
```

Step 13: Still on Elasticsearch server,reset password for Kibana default system user



```
[root@elasticsearch ~]#
[root@elasticsearch ~]# /usr/share/elasticsearch/bin/elasticsearch-reset-password -i -u kibana_system
This tool will reset the password of the [kibana_system] user.
You will be prompted to enter the password.
Please confirm that you would like to continue [y/N]y


Enter password for [kibana_system]:
Re-enter password for [kibana_system]:
Password for the [kibana_system] user successfully reset.
```

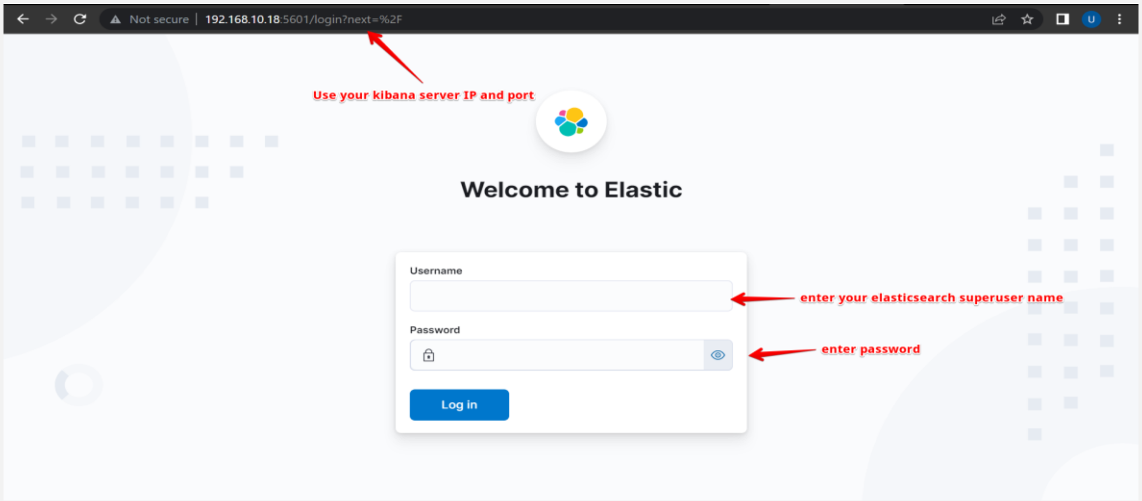
Step 14: Allow Kibana to listen on port 5601



```
[user1@kibana ~]$ sudo firewall-cmd --add-port=5601/tcp --permanent
[sudo] password for user1:
success
[user1@kibana ~]$ sudo firewall-cmd --reload
success
[user1@kibana ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpv6-client ssh
  ports: 5601/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

[user1@kibana ~]$ sudo systemctl restart kibana.service
Display all 390 possibilities? (y or n)
[user1@kibana ~]$ sudo systemctl restart kibana.service
[user1@kibana ~]$
```

Step 15: Proceed to your web browser and enter your Kibana address.

Syntax: http://<your kibana server IP>:5601

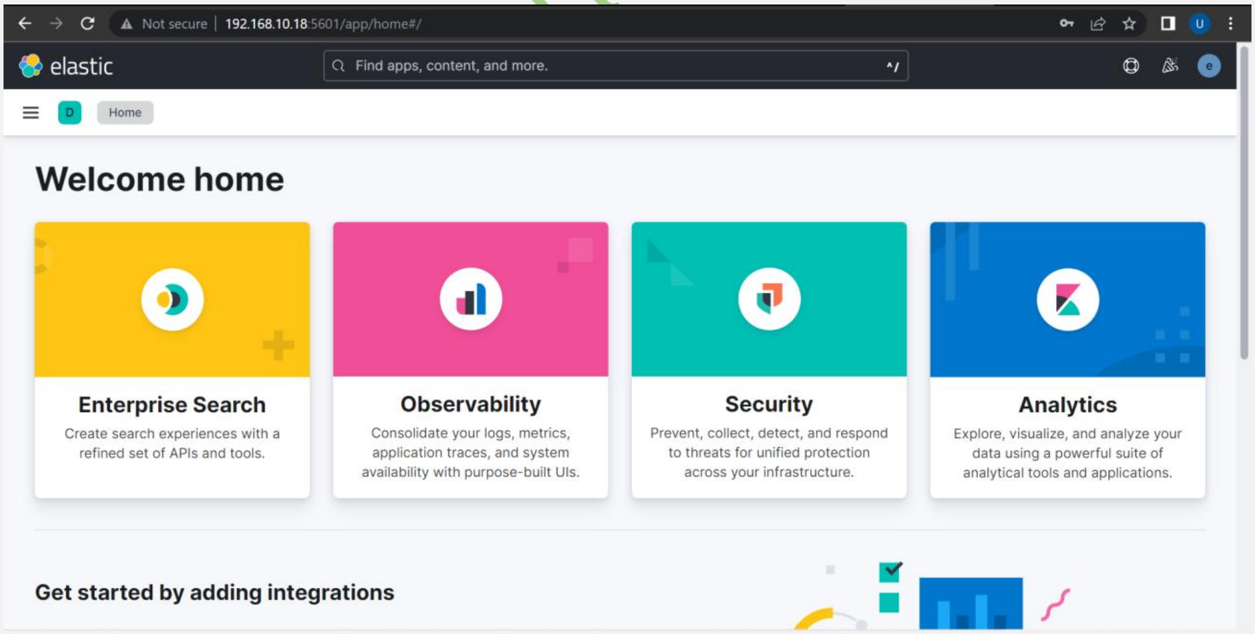


Use your kibana server IP and port

enter your elasticsearch superuser name

enter password

Kbana Home Screen


Not secure | 192.168.10.18:5601/app/home#/
elastic
Find apps, content, and more.
D
Home

Welcome home

Enterprise Search
Create search experiences with a refined set of APIs and tools.

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

END