

## Elasticsearch Setup on Static IP in Debian/Ubuntu (VMware Lab)

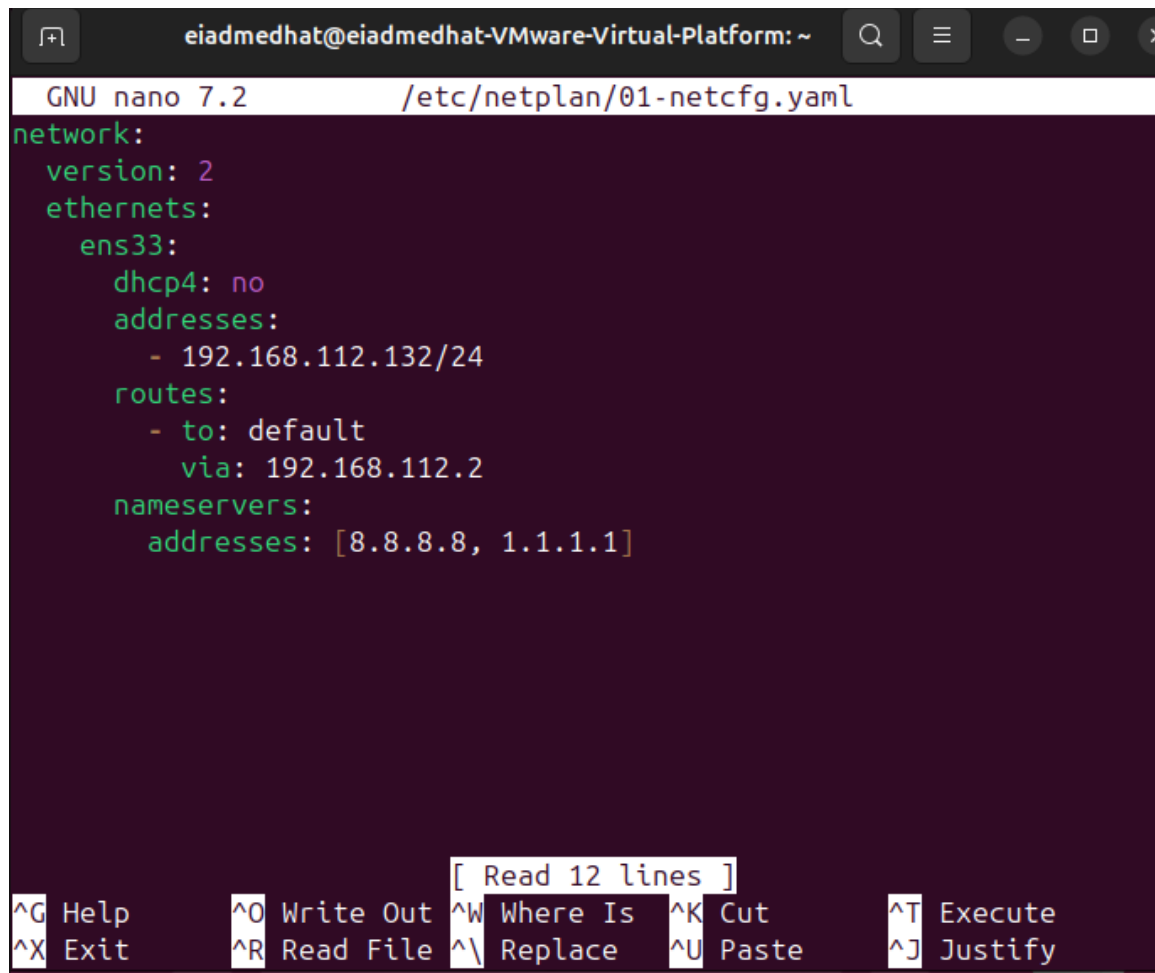
Step 1: Assign a Static IP Address

1. Open the Netplan configuration file:

```
sudo nano /etc/netplan/00-installer-config.yaml
```

2. Edit it to set a static IP, e.g.:

```
network:
  version: 2
  ethernets:
    ens33:
      addresses: [192.168.112.132/24]
      gateway4: 192.168.112.2
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

A screenshot of a terminal window titled 'eiadmedhat@eiadmedhat-VMware-Virtual-Platform: ~'. The terminal shows the nano text editor editing the file '/etc/netplan/01-netcfg.yaml'. The configuration content is as follows:

```
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: no
      addresses:
        - 192.168.112.132/24
      routes:
        - to: default
          via: 192.168.112.2
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]
```

The terminal interface includes a status bar at the bottom with various keyboard shortcuts: ^G Help, ^O Write Out, ^W Where Is, ^K Cut, ^T Execute, ^X Exit, ^R Read File, ^\_ Replace, ^U Paste, and ^J Justify. A message '[ Read 12 lines ]' is also visible in the status bar.

3. Apply the configuration:

```
sudo netplan apply
```

## Step 2: Install Elasticsearch

- `wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg`
- `sudo apt-get install apt-transport-https`
- `echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/9.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-9.x.list`
- `sudo apt-get update && sudo apt-get install elasticsearch`

## Step 3: Configure Elasticsearch for Static IP Access

1. Open the config file:

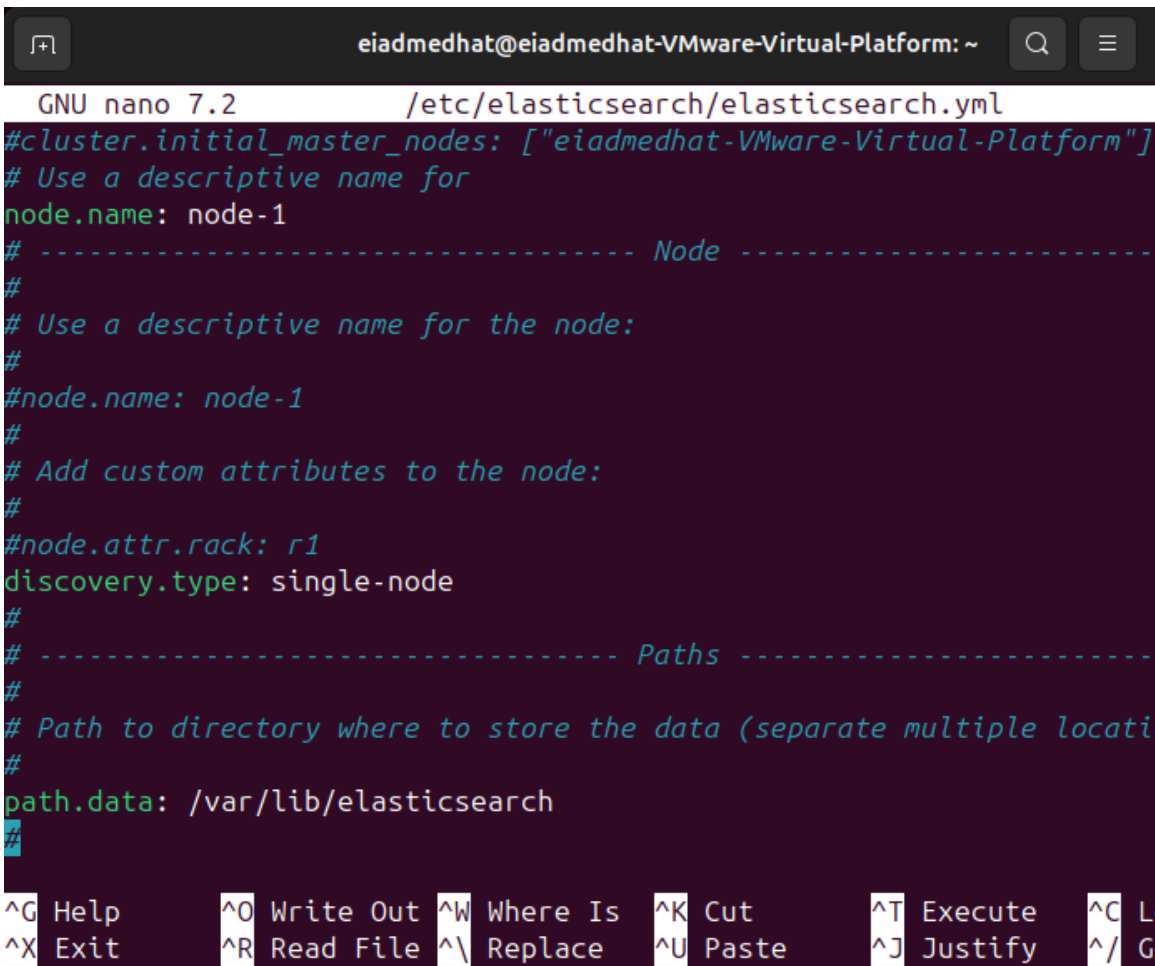
`sudo nano /etc/elasticsearch/elasticsearch.yml`

2. Set the following:

`network.host: 192.168.112.132`

`http.port: 9200`

`cluster.initial_master_nodes: ["node-1"]`



```
GNU nano 7.2 /etc/elasticsearch/elasticsearch.yml
#cluster.initial_master_nodes: ["eiadmedhat-VMware-Virtual-Platform"]
# Use a descriptive name for
node.name: node-1
# ----- Node -----
#
# Use a descriptive name for the node:
#
#node.name: node-1
#
# Add custom attributes to the node:
#
#node.attr.rack: r1
discovery.type: single-node
#
# ----- Paths -----
#
# Path to directory where to store the data (separate multiple locati
#
path.data: /var/lib/elasticsearch
#
```

Terminal window showing the configuration of `elasticsearch.yml` in nano editor. The configuration includes setting `node.name` to `node-1`, `discovery.type` to `single-node`, and `path.data` to `/var/lib/elasticsearch`. The terminal window title is `eiadmedhat@eiadmedhat-VMware-Virtual-Platform: ~`.

```

eiadmedhat@eiadmedhat-VMware-Virtual-Platform: ~
GNU nano 7.2 /etc/elasticsearch/elasticsearch.yml
# address here to expose this node on the network:
#
network.host: 192.168.112.132
#
# By default Elasticsearch listens for HTTP traffic on the first free
# 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 i
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
#discovery.seed_hosts: ["host1", "host2"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes
#

```

```

eiadmedhat@eiadmedhat-VMware-Virtual-Platform: ~
GNU nano 7.2 /etc/elasticsearch/elasticsearch.yml
xpack.security.enrollment.enabled: true

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

# Enable encryption and mutual authentication between cluster nodes
xpack.security.transport.ssl:
  enabled: true
  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: ["eiadmedhat-VMware-Virtual-Platform"]

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

^G Help      ^O Write Out ^W Where Is  ^K Cut      ^T Execute  ^C L
^X Exit      ^R Read File ^\ Replace  ^U Paste    ^J Justify  ^/ G

```

```

eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo systemctl status elasticsearch
arch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; pr>
   Active: active (running) since Mon 2025-08-11 23:36:05 EEST; 8min ago
     Docs: https://www.elastic.co
  Main PID: 6987 (java)
    Tasks: 108 (limit: 3840)
   Memory: 2.0G (peak: 2.0G swap: 36.0M swap peak: 36.2M)
      CPU: 44.346s
   CGroup: /system.slice/elasticsearch.service
           └─6987 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+U>
             7053 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.c>
             7075 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x>

Aug 11 23:35:48 eiadmedhat-VMware-Virtual-Platform systemd[1]: Starting elastic>
Aug 11 23:36:05 eiadmedhat-VMware-Virtual-Platform systemd[1]: Started elastics>
lines 1-15/15 (END)

```

3. Save and exit.

Step 4: Enable Security (Built-in User Authentication)

1. In `/etc/elasticsearch/elasticsearch.yml`, add:

```

xpack.security.enabled: true
xpack.security.http.ssl.enabled: false

```

2. Save and restart Elasticsearch:

```

sudo systemctl restart elasticsearch

```

Step 5: Enable and Start Elasticsearch Service

```

sudo systemctl enable elasticsearch
sudo systemctl start elasticsearch

```

Step 6: Set Password for elastic User

```

sudo /usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic

```

```

eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo /usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic
This tool will reset the password of the [elastic] user to an autogenerated value.
The password will be printed in the console.
Please confirm that you would like to continue [y/N]y

Password for the [elastic] user successfully reset.
New value: ZqCQt2tNVOGyPB3vHd6Z

```

I Changed The Pass After That Because I forgot it the new pass =" g5E5JsuKDY4jSYh\_h8\_

" and it will be changed in winlogbeat configuration

## Step 7: Test the Connection

curl -u elastic:< ZqCQt2tNVOGyPB3vHd6Z > <http://192.168.112.132:9200>

```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ curl -u elastic:ZqCQt2tNVOGyPB3vHd6Z http://192.168.112.132:9200
{
  "name" : "node-1",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "uhyGLtXBSRWIwiGq781qIw",
  "version" : {
    "number" : "9.1.1",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "5e94055934defa56e454868b7783b2a3b683785e",
    "build_date" : "2025-08-05T01:07:31.959947279Z",
    "build_snapshot" : false,
    "lucene_version" : "10.2.2",
    "minimum_wire_compatibility_version" : "8.19.0",
    "minimum_index_compatibility_version" : "8.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Then

### Kibana Installation and Configuration

- wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
- sudo apt-get install apt-transport-https
- echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/9.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-9.x.list
- sudo apt-get update && sudo apt-get install kibana

Then

### Configure Kibana

sudo nano /etc/kibana/kibana.yml

```
GNU nano 7.2 /etc/kibana/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
# The default is 'localhost', which usually means remote machines will not be able
# To allow connections from remote users, set this parameter to a non-loopback
server.host: "0.0.0.0"
```

```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform: ~  
GNU nano 7.2 /etc/kibana/kibana.yml *  
  
# ===== System: Elasticsearch =====  
# The URLs of the Elasticsearch instances to use for all your queries.  
elasticsearch.hosts: ["http://192.168.112.132:9200"]  
  
# If your Elasticsearch is protected with basic authentication, these settings  
# the username and password that the Kibana server uses to perform maintenance  
# index at startup. Your Kibana users still need to authenticate with Elasticse  
# is proxied through the Kibana server.  
elasticsearch.username: "kibana_system"  
elasticsearch.password: "WpYGH3QcLsYkvEFgCDwZ"  
  
# Kibana can also authenticate to Elasticsearch via "service account tokens".  
# Service account tokens are Bearer style tokens that replace the traditional u  
# Use this token instead of a username/password.  
# elasticsearch.serviceAccountToken: "my_token"  
  
# Time in milliseconds to wait for Elasticsearch to respond to pings. Defaults  
# the elasticsearch.requestTimeout setting.  
# elasticsearch.pingTimeout: 1500  
  
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

```
will not be shown, you would have to be root to see it all.)  
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo ss -tulnp | grep 5601  
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo systemctl restart kibana  
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo netstat -tulnp | grep 560  
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo systemctl restart kibana  
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo systemctl status kibana  
  
● kibana.service - Kibana  
   Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled>  
   Active: active (running) since Mon 2025-08-11 23:56:53 EEST; 8s>  
     Docs: https://www.elastic.co  
  Main PID: 10580 (node)  
    Tasks: 11 (limit: 3840)  
   Memory: 321.0M (peak: 321.1M)  
      CPU: 9.419s  
   CGroup: /system.slice/kibana.service  
           └─10580 /usr/share/kibana/bin/../node/glibc-217/bin/nod>  
  
Aug 11 23:56:53 eiadmedhat-VMware-Virtual-Platform systemd[1]: Start>  
Aug 11 23:56:53 eiadmedhat-VMware-Virtual-Platform kibana[10580]: {">  
Aug 11 23:56:54 eiadmedhat-VMware-Virtual-Platform kibana[10580]: Na>
```

## Winlogbeat Configuration:

Open C:\Program Files\Winlogbeat\winlogbeat.yml in a text editor

```
# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["192.168.112.132:9200"]

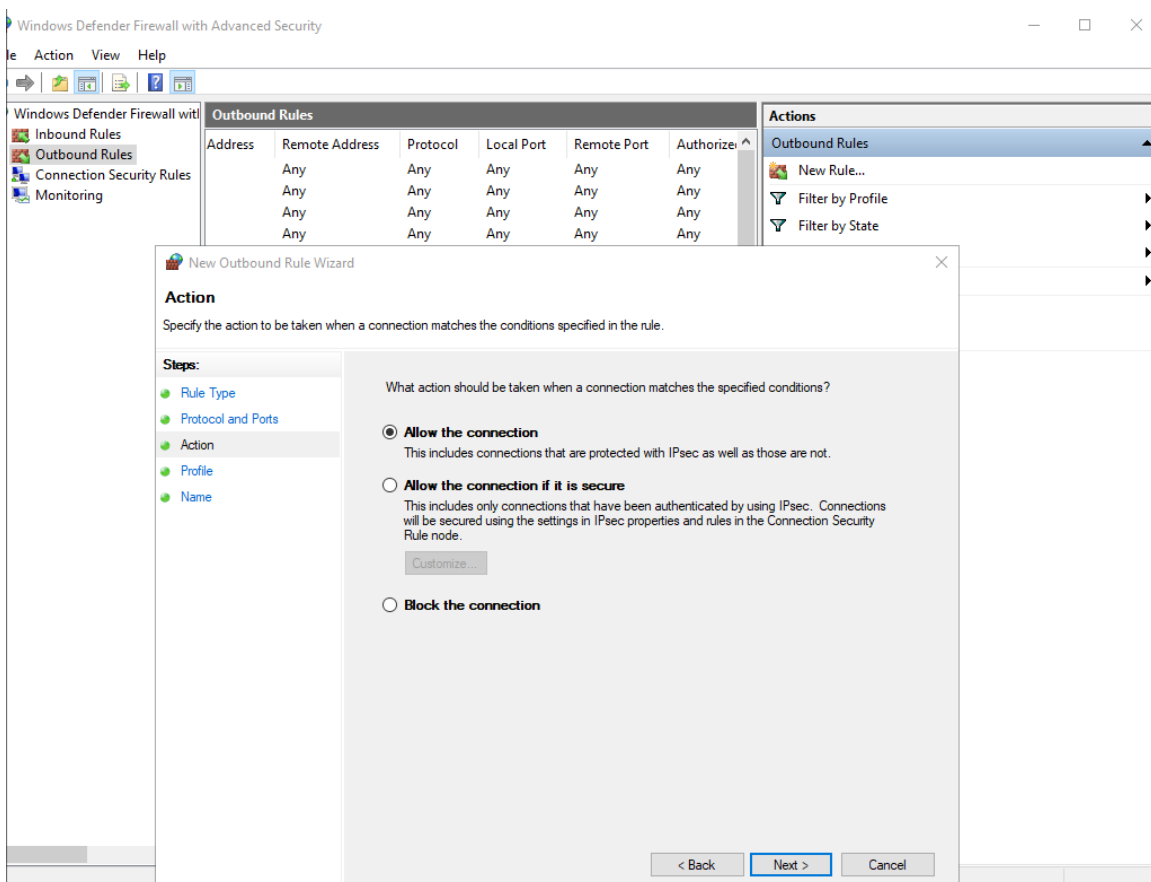
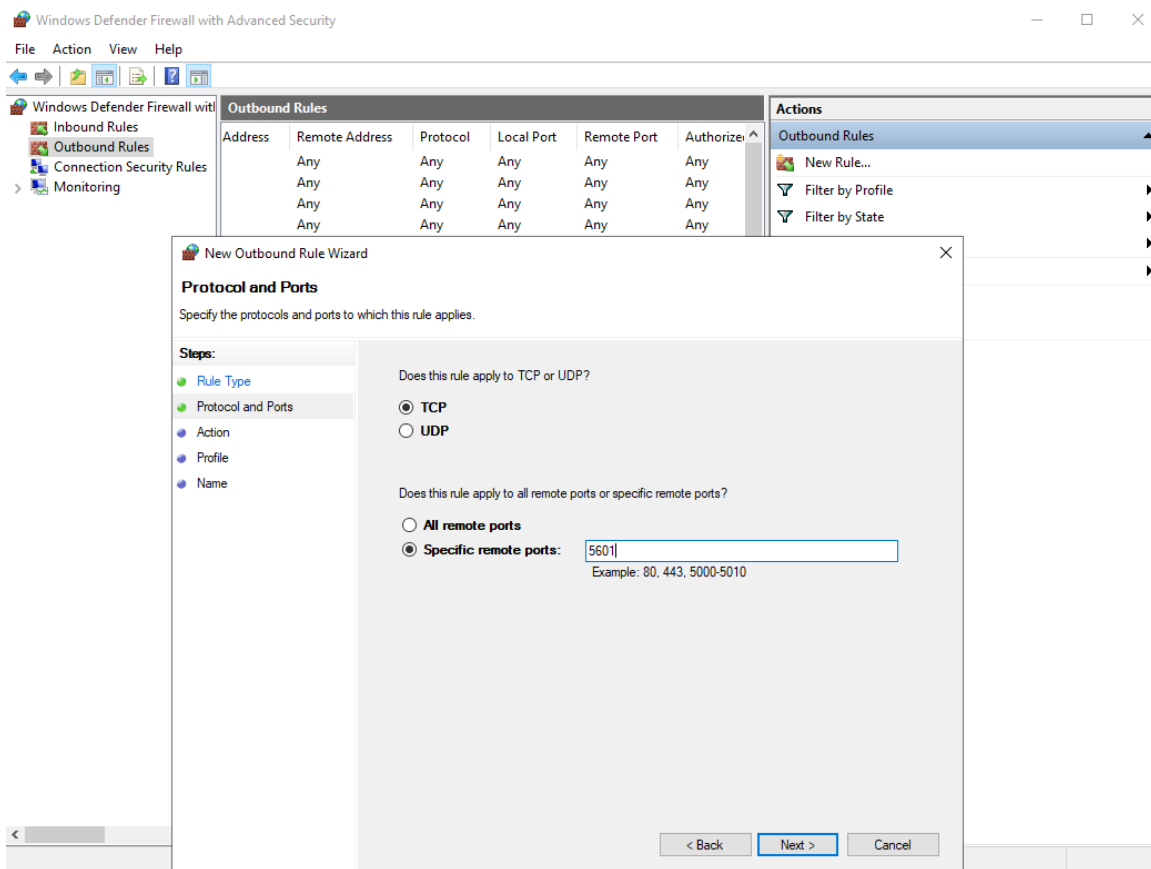
  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "g5E5JsuKDYY4jSYh_h8_"

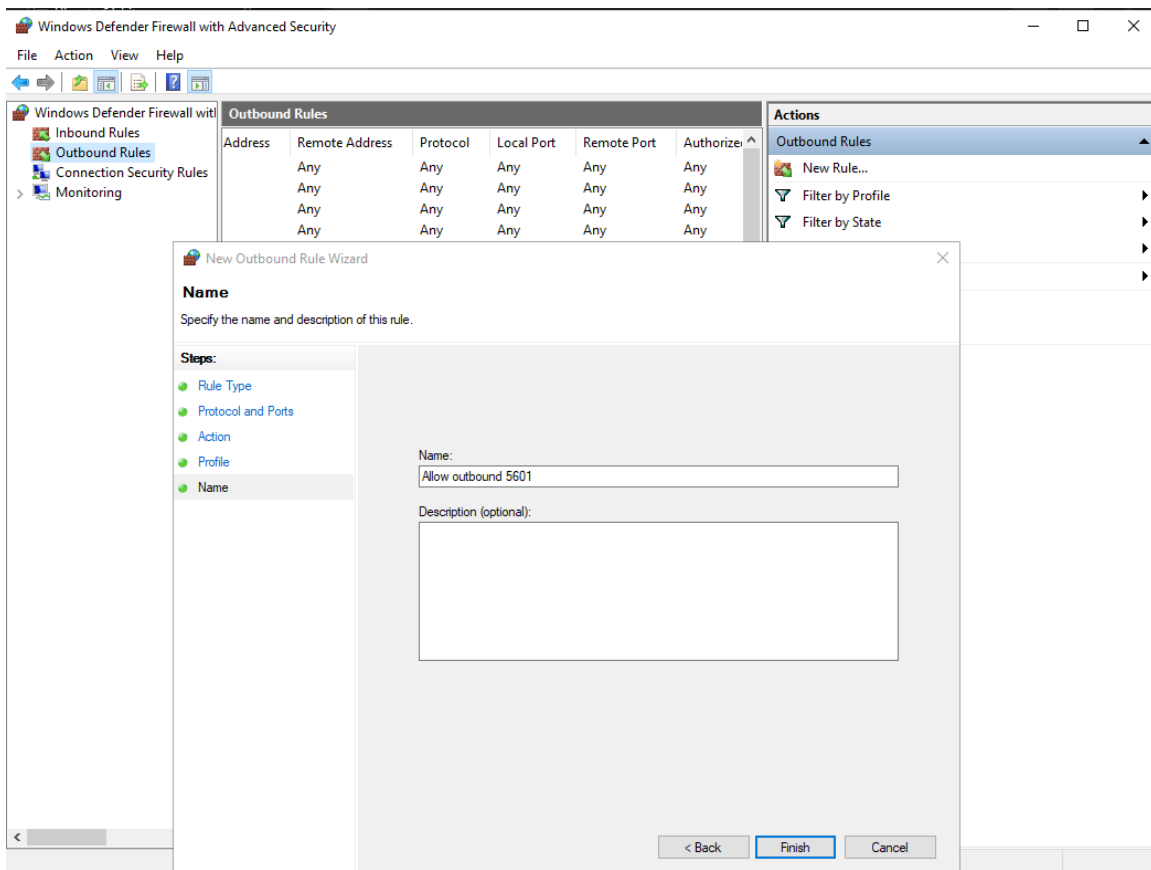
  # Pipeline to route events to security, sysmon, or powershell pipelines.
  pipeline: "winlogbeat-%{[agent.version]}-routing"
```

```
# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:
  host: "http://192.168.112.132:5601"
  username: "elastic"
  password: "WpYGH3QcLsYkvEFgCDwZ"

# Kibana Host
```







## 2.3 Install and Start Winlogbeat Service

1. Open PowerShell as Administrator.
2. Navigate to Winlogbeat folder:
3. Install Winlogbeat as a service:
4. Start the service:

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Administrator> cd "C:\Program Files\Winlogbeat"
>> .\winlogbeat.exe setup --dashboards
>>
Loading dashboards (Kibana must be running and reachable)
Exiting: error connecting to Kibana: fail to get the Kibana version: fail to parse kibana version (): passed version is
not semver:
PS C:\Program Files\Winlogbeat> curl.exe http://192.168.112.132:5601
>>
PS C:\Program Files\Winlogbeat> curl.exe http://192.168.112.132:5601
>>
PS C:\Program Files\Winlogbeat> Test-NetConnection -ComputerName 192.168.112.132 -Port 5601
>>

ComputerName      : 192.168.112.132
RemoteAddress     : 192.168.112.132
RemotePort        : 5601
InterfaceAlias    : VMware Network Adapter VMnet8
SourceAddress     : 192.168.112.1
TcpTestSucceeded  : True
```

```

PS C:\Program Files\Winlogbeat> curl.exe -u elastic:WpYGH3QcLsYkvEFgCDwZ http://192.168.112.132:5601/api/status | Conver
tFrom-Json | Format-List *
>>
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
             Dload  Upload    Total   Spent    Left   Speed
100    44    100    44      0      0    462      0  --:--:-- --:--:-- --:--:--    463

status : @{overall=}

PS C:\Program Files\Winlogbeat> ping 192.168.112.132
>>

Pinging 192.168.112.132 with 32 bytes of data:
Reply from 192.168.112.132: bytes=32 time<1ms TTL=64
Reply from 192.168.112.132: bytes=32 time<1ms TTL=64
Reply from 192.168.112.132: bytes=32 time<1ms TTL=64
Reply from 192.168.112.132: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.112.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Program Files\Winlogbeat> Test-NetConnection -ComputerName 192.168.112.132 -Port 5601
>>

ComputerName      : 192.168.112.132
RemoteAddress     : 192.168.112.132
RemotePort        : 5601
InterfaceAlias    : VMware Network Adapter VMnet8
SourceAddress     : 192.168.112.1
TcpTestSucceeded  : True

PS C:\Program Files\Winlogbeat> Start-Service winlogbeat
>>
PS C:\Program Files\Winlogbeat> curl.exe -u elastic:g5E5JsuKDY4jSYh_h8_ http://192.168.112.132:9200/_cat/indices?v
health status index                                uuid                                pri rep docs.cou
nt docs.deleted store.size pri.store.size dataset.size
green open      .internal.alerts-transform.health.alerts-default-000001 euBBg82fR26DJj8h2Lcb2Q 1 0
0 0 249b 249b 249b
green open      .internal.alerts-observability.logs.alerts-default-000001 q-zXv3kxR10iWok7U1fn8A 1 0
0 0 249b 249b 249b

PS C:\Program Files\Winlogbeat> curl.exe -u elastic:g5E5JsuKDY4jSYh_h8_ http://192.168.112.132:9200/_cat/indices?v
health status index                                uuid                                pri rep docs.cou
nt docs.deleted store.size pri.store.size dataset.size
green open      .internal.alerts-transform.health.alerts-default-000001 euBBg82fR26DJj8h2Lcb2Q 1 0
0 0 249b 249b 249b
green open      .internal.alerts-observability.logs.alerts-default-000001 q-zXv3kxR10iWok7U1fn8A 1 0
0 0 249b 249b 249b
green open      .internal.alerts-observability.uptime.alerts-default-000001 Yb6906CETHqTe4UpjiVt-g 1 0
0 0 249b 249b 249b
green open      .internal.alerts-ml.anomaly-detection.alerts-default-000001 URw1f-9uTKywCO_JeeJcsg 1 0
0 0 249b 249b 249b
green open      .internal.alerts-observability.slo.alerts-default-000001 pi-DMgcPSxuNpjMRaDi67g 1 0
0 0 249b 249b 249b
green open      .internal.alerts-default.alerts-default-000001 soJciXNFQD201QUP18ikIQ 1 0
0 0 249b 249b 249b
green open      .internal.alerts-streams.alerts-default-000001 1yETNaosSF6jc1kQk3pow 1 0
0 0 249b 249b 249b
green open      .internal.alerts-observability.apm.alerts-default-000001 XgNlo64QRv6UC_X88FE5DA 1 0
0 0 249b 249b 249b
green open      .internal.alerts-security.attack.discovery.alerts-default-000001 n5fIM60xTny1BxwVNSEksg 1 0
0 0 249b 249b 249b
green open      .internal.alerts-observability.metrics.alerts-default-000001 a1ZY4q18RIKFSSS_dLcDyw 1 0
0 0 249b 249b 249b
yellow open     .ds-winlogbeat-9.1.1-2025.08.11-000001 hZ3HU4CKQ1iChT2y9wizDg 1 1 272
48 0 25.9mb 25.9mb 25.9mb
green open      .internal.alerts-ml.anomaly-detection-health.alerts-default-000001 F1q3UDIXtnmt08Xbjppu4w 1 0
0 0 249b 249b 249b
green open      .internal.alerts-observability.threshold.alerts-default-000001 YNVHtxbuQtWLXfID9G2vQg 1 0
0 0 249b 249b 249b
green open      .internal.alerts-security.alerts-default-000001 z103Y5EbTR-1Nk-dT0zLug 1 0
0 0 249b 249b 249b
green open      .internal.alerts-dataset.quality.alerts-default-000001 jziKgGvYrTsyTZ2bYHj8r2g 1 0
0 0 249b 249b 249b
green open      .internal.alerts-stack.alerts-default-000001 M8ZvAUb3S9yn1GRY3MH3Kg 1 0
0 0 249b 249b 249b

```



# Welcome to Elastic

You have logged out of Elastic.

Username

elastic

Password

g5E5JsuKDYY4jSYh\_h8\_

Log in

