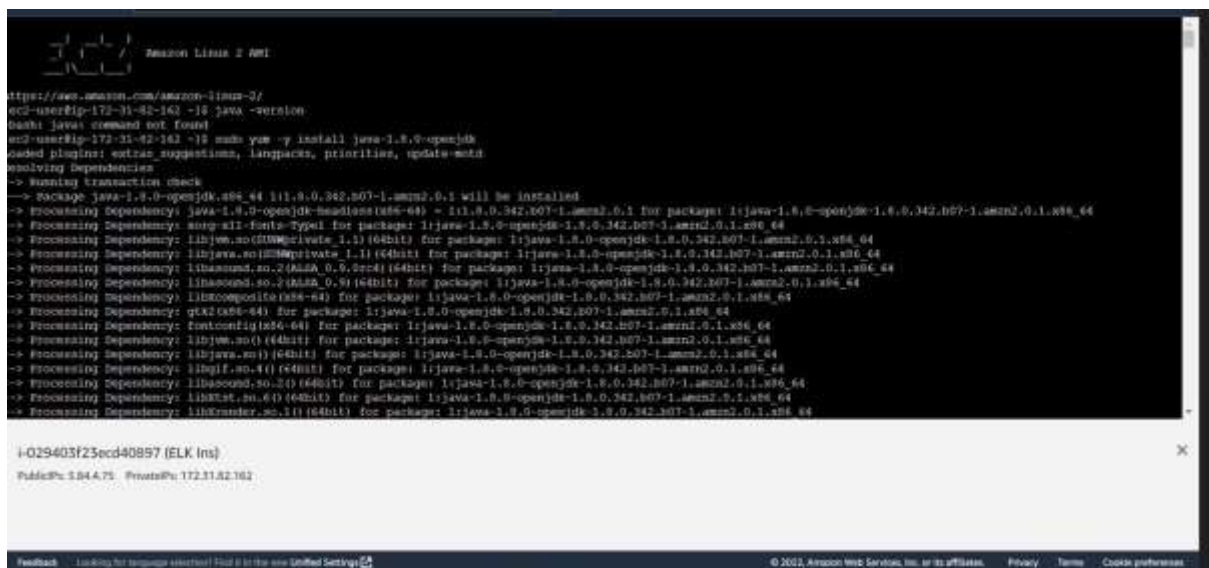


Screenshots:



```
## You can start elasticsearch service by executing
sudo systemctl start elasticsearch.service
Verifying : elasticsearch-1.7.3-1.noarch

Installed:
  elasticsearch.noarch 0:1.7.3-1

Complete!
[root@ip-172-31-82-162 ~]# rm -f elasticsearch-1.7.3.noarch.rpm
[root@ip-172-31-82-162 ~]# service elasticsearch start
Starting elasticsearch (via systemctl): [ OK ]
[root@ip-172-31-82-162 ~]# sudo chkconfig --add elasticsearch
[root@ip-172-31-82-162 ~]# echo "network.host: 0.0.0.0" >> /etc/elasticsearch/elasticsearch.yml
[root@ip-172-31-82-162 ~]# cd /usr/share/elasticsearch/
[root@ip-172-31-82-162 elasticsearch]# ./bin/plugin --install mdeb/elasticsearch-head
+ Installing mdeb/elasticsearch-head...
trying https://github.com/mdeb/elasticsearch-head/archive/master.zip...
Downloading .....DONE
Installed mdeb/elasticsearch-head into /usr/share/elasticsearch/plugins/head
[root@ip-172-31-82-162 elasticsearch]# ./bin/plugin --install lukas-vicsek/bigdesk
+ Installing lukas-vicsek/bigdesk...
trying https://github.com/lukas-vicsek/bigdesk/archive/master.zip...
Downloading .....DONE
Installed lukas-vicsek/bigdesk into /usr/share/elasticsearch/plugins/bigdesk
Identified as a site plugin, moving to site structure ...
[root@ip-172-31-82-162 elasticsearch]# ./bin/plugin --install elasticsearch-cmds-aws/2.3

i-029403f23ecd40b97 (ELK Ins)
```

PublicIP: 3.84.4.75 PrivateIP: 172.31.82.162

Feedback Looking for language selection? Find it in the new Unified Settings.

© 2022 Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

BWS Services Search for services, features, blogs, docs, and more [Alt+F3]

N. Virginia Corestack_Role/govex.mh4x3_rphelo @ srathand-actugalia

EC2 > Instances > Launch an instance

Launch an instance [info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [info](#)

Name: [Add additional tags](#)

Application and OS Images (Amazon Machine Image) [info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or browse for AMIs if you don't see what you are looking for below.

Summary

Number of instances [info](#):

Software (image) [AMI](#): Canonical, Ubuntu, 22.04 LTS, ... [read more](#)
ami-0b4bdc9ed489472

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GB

[Cancel](#) [Launch instance](#)

```
download done
called to extract plugin [/usr/share/elasticsearch/plugins/kgf.zip]: ZipException[zip file is empty]
[root@ip-172-31-82-162 elasticsearch]# yum su
[root@ip-172-31-82-162 elasticsearch]# yum update -y
loaded plugins: extras_suggestions, langpacks, priorities, update-motd
sored2-core
no packages marked for update
[root@ip-172-31-82-162 elasticsearch]# cd /root
[root@ip-172-31-82-162 ~]# wget https://download.elastic.co/kibana/kibana/kibana-4.1.2-linux-x64.tar.gz
--2022-10-10 12:30:24-- https://download.elastic.co/kibana/kibana/kibana-4.1.2-linux-x64.tar.gz
Resolving download.elastic.co (download.elastic.co)... 34.120.127.130, 2401:1901:0110:1
Connecting to download.elastic.co (download.elastic.co [34.120.127.130]:443)... connected.
HTTP request sent, awaiting response... 200 OK
length: 11707239 (11M) [binary/octet-stream]
Saving to: 'kibana-4.1.2-linux-x64.tar.gz'

100%[=====] 11,707,239 25.0MB/s in 0.4s

2022-10-10 12:30:25 (29.1 MB/s) = 'kibana-4.1.2-linux-x64.tar.gz' saved [11707239/11707239]

[root@ip-172-31-82-162 ~]# tar xzf kibana-4.1.2-linux-x64.tar.gz
[root@ip-172-31-82-162 ~]# ls -l kibana-4.1.2-linux-x64.tar.gz
[root@ip-172-31-82-162 ~]# cd kibana-4.1.2-linux-x64
[root@ip-172-31-82-162 kibana-4.1.2-linux-x64]# nano config/kibana.yml
[root@ip-172-31-82-162 kibana-4.1.2-linux-x64]# nohup ./bin/kibana &
[1] 18537
[root@ip-172-31-82-162 kibana-4.1.2-linux-x64]# nohup: ignoring input and appending output to 'nohup.out'
```

i-029403f23ecd40b97 (ELK Ins)

PublicIP: 3.84.4.75 PrivateIP: 172.31.82.162

Feedback Looking for language selection? Find it in the new Unified Settings.

© 2022 Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

```
root@ip-172-31-82-162 elasticsearch# ./bin/plugin --install elasticsearch/elasticsearch-cloud-aws/2.7.1
> Installing elasticsearch/elasticsearch-cloud-aws/2.7.1...
trying http://download.elasticsearch.org/elasticsearch-cloud-aws/elasticsearch-cloud-aws-2.7.1.zip...
downloading 00m
failed to extract plugin [/usr/share/elasticsearch/plugins/cloud-aws.zip]: zipException:zip file is empty!
root@ip-172-31-82-162 elasticsearch# ./bin/plugin --install amazon/elasticsearch-kopf/1.5.7
> Installing amazon/elasticsearch-kopf/1.5.7...
trying http://download.elasticsearch.org/amazon/elasticsearch-kopf/elasticsearch-kopf-1.5.7.zip...
downloading 00m
failed to extract plugin [/usr/share/elasticsearch/plugins/kopf.zip]: zipException:zip file is empty!
root@ip-172-31-82-162 elasticsearch# sudo su
root@ip-172-31-82-162 elasticsearch# yum update -y
loaded plugins: extras_suggestions, langpacks, priorities, update-notif
s2m2-close
No packages marked for update
root@ip-172-31-82-162 elasticsearch# cd /root
root@ip-172-31-82-162 ~# wget https://download.elastic.co/kibana/kibana-4.1.2-linux-x64.tar.gz
--2022-10-10 12:30:24-- https://download.elastic.co/kibana/kibana-4.1.2-linux-x64.tar.gz
Resolving download.elastic.co [download.elastic.co... 34.120.127.170, 2409:1901:0:1d7::]
Connecting to download.elastic.co [download.elastic.co|34.120.127.170|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11787239 (11M) [binary/octet-stream]
Saving to: 'kibana-4.1.2-linux-x64.tar.gz'

20M-----> 11,787,239 25.1MB/s in 0.4s

2022-10-10 12:30:25 (25.1 MB/s) - 'kibana-4.1.2-linux-x64.tar.gz' saved [11787239/11787239]
```

i-029403f23ecd40897 (ELK Ins)
PublicIPs: 3.84.4.75 PrivateIPs: 172.31.82.162

Feedback Looking for language selected? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

```
dependencies installed:
alsa-lib.x86_64 0:1.1.4-1-2.amzn2
cairo.x86_64 0:1.15.12-4.amzn2
cjkjavafonts-common.noarch 0:2.33-6.amzn2
fontpackages-filesystem.noarch 0:1.44-0.amzn2
glib.x86_64 0:4.1.6-9.amzn2.0.2
gtk2.x86_64 0:2.24.31-1.amzn2.0.2
javadoc-lib.x86_64 0:1.8.0_9-9.amzn2.0.2
libICE.x86_64 0:1.0.9-9.amzn2.0.2
libX11-common.noarch 0:1.4.7-3.amzn2.0.2
libXcursor.x86_64 0:1.1.15-1.amzn2
libXfixes.x86_64 0:5.0.3-1.amzn2.0.2
libXinerama.x86_64 0:1.1.3-2.1.amzn2.0.2
libXtst.x86_64 0:1.2.3-1.amzn2.0.2
libglvnd.x86_64 1:1.0.1-0.1.git5ba1e5.amzn2.0.1
libthai.x86_64 0:0.1.14-9.amzn2.0.2
libxcb.x86_64 0:1.12-1.amzn2.0.2
libxcp-tool.x86_64 0:1.0.17-2.amzn2.0.2
mesa-libGL.x86_64 0:18.3.4-5.amzn2.0.1
pango.x86_64 0:1.42.4-4.amzn2
python-javapackages.noarch 0:3.4.1-11.amzn2
tclata-java.noarch 0:2022c-1.amzn2
atk.x86_64 0:2.30.0-7.amzn2.0.2
copy-jdk-configs.noarch 0:3.3-10.amzn2
cjkjavafonts-fonts.noarch 0:2.33-6.amzn2
cjklib.x86_64 0:1.0.2-1.amzn2.1
graphite2.x86_64 0:1.3.10-1.amzn2.0.2
harfbuzz.x86_64 0:1.7.5-2.amzn2
java-1.8.0-openjdk-headless.x86_64 1:1.8.0_342-b07-1.amzn2.0.1
libDM.x86_64 0:1.2.2-2.amzn2.0.2
libGL.x86_64 0:1.0.5-2-1.amzn2.0.2
libglvnd.x86_64 0:1.1.4-6-1.amzn2.0.2
libXrandr.x86_64 0:1.5.1-2.amzn2.0.3
libXxf86vm.x86_64 0:1.1.4-1.amzn2.0.2
libglvnd-glx.x86_64 1:1.0.1-0.1.git5ba1e5.amzn2.0.1
libwayland-client.x86_64 0:1.17.0-1.amzn2
libxmf.noarch.x86_64 0:1.2-1.amzn2.0.2
log4j-core-2021-04285-0mputch.noarch 0:1.3-7.amzn2
mesa-libgl.x86_64 0:18.3.4-5.amzn2.0.1
pango-lib.x86_64 0:1.8.0-1.amzn2.0.2
python-lxml.x86_64 0:3.2.2-4.amzn2.0.3
xorg-x11-font-util.x86_64 1:1.5.2-1.amzn2
avahi-libe.x86_64 0:0.6.31-20.amzn2
cups-libe.x86_64 1:1.6.3-51.amzn2
fontconfig.x86_64 0:12.1.0-4.3.amzn2
gtk-pixbuf2.x86_64 0:2.36.12-3.amzn2
gtk-update-icon-cache.x86_64 0:3.22.30-3.amzn2
libcolor-1000-theme.noarch 0:1.12-7.amzn2
javapackages-tools.noarch 0:1.4.1-11.amzn2
libXGL.x86_64 0:1.8.9-5.amzn2.0.2
libXrender.x86_64 0:0.3.10-1.amzn2.0.2
libXtst.x86_64 0:1.1.3-1.amzn2.0.2
libglvnd-glx.x86_64 1:1.0.1-0.1.git5ba1e5.amzn2.0.1
libwayland-server.x86_64 0:1.17.0-1.amzn2
libx11.x86_64 0:1.1.12-6.amzn2
mesa-libGL.x86_64 0:18.3.4-5.amzn2.0.1
mesa-libglapi.x86_64 0:18.3.4-5.amzn2.0.1
plyman.x86_64 0:0.36.0-1.amzn2.0.2
tweakftr.x86_64 0:0.3.0-8-42.amzn2.0.2
xorg-x11-fonts-Type1.noarch 0:1.5.9.amzn2
```

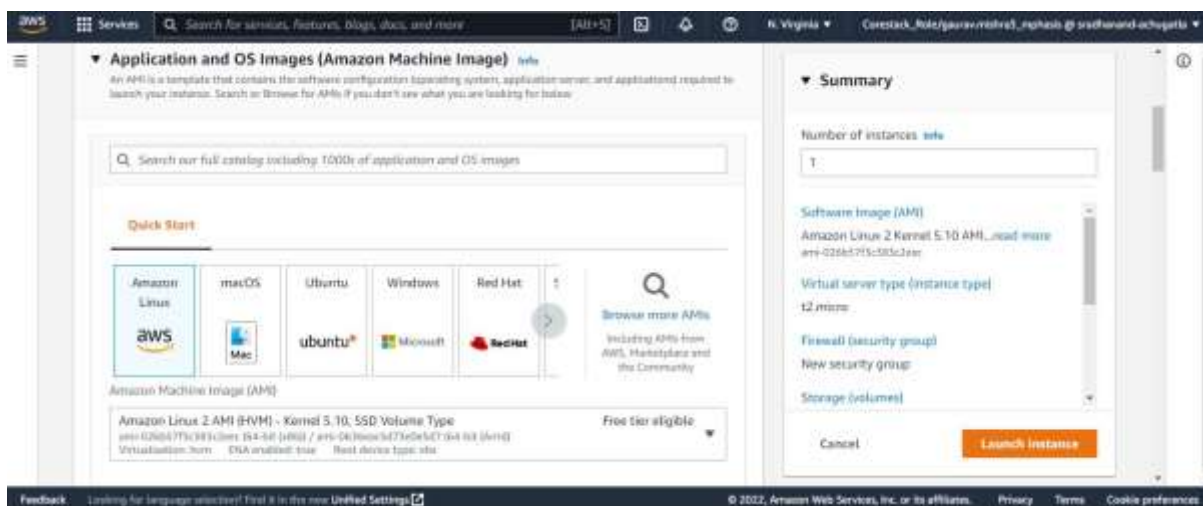
complete!

ec2-user@ip-172-31-82-162 ~\$ java -version
openjdk version "1.8.0_342"
OpenJDK Runtime Environment (build 1.8.0_342-b07)
OpenJDK 64-Bit Server VM (build 25.342-b07, mixed mode)

i-029403f23ecd40897 (ELK Ins)
PublicIPs: 3.84.4.75 PrivateIPs: 172.31.82.162

Feedback Looking for language selected? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



Services

Search for services, features, blogs, docs, and more

[Alt+S]

N. Virginia

Corestack_Role/gaurav.mishra5_mphosis @ srathanand-achugatta

Instance type [info](#)

t2.micro [Free tier eligible](#)

Family: t2 1 vCPU 1 GB Memory
 On-Demand Linux pricing: 0.0116 USD per hour
 On-Demand Windows pricing: 0.0162 USD per hour

Compare instance types

Key pair (login) [info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

ELK-Ins

Create new key pair

Network settings [info](#)

Summary

Number of instances [info](#)
 1

Software image (AMI)
 Amazon Linux 2 Kernel 5.10 AMI...[read more](#)
 ami-026b57f3c385c2ee...

Virtual server type (instance type)
 t2.micro

Firewall (security group)
 New security group

Storage (volumes)

Cancel

Launch instance

Looking for language selection? Find it in the new Unified Settings
 © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Services

Search for services, features, blogs, docs, and more

[Alt+S]

N. Virginia

Corestack_Role/gaurav.mishra5_mphosis @ srathanand-achugatta

Security group rule 1 (TCP, 22, 0.0.0.0/0)

Remove

Type [info](#)

Protocol [info](#)

Port range [info](#)

ssh

TCP

22

Source type [info](#)

Source [info](#)

Description - optional [info](#)

Custom

Add CIDR, prefix list or security group
 0.0.0.0/0

e.g. SSH for admin desktop

Security group rule 2 (TCP, 0, 106.195.60.16/32)

Remove

Type [info](#)

Protocol [info](#)

Port range [info](#)

Custom TCP

TCP

0

Source type [info](#)

Source [info](#)

Description - optional [info](#)

My IP

Add CIDR, prefix list or security group
 106.195.60.16/32

e.g. SSH for admin desktop

Summary

Number of instances [info](#)
 1

Software image (AMI)
 Amazon Linux 2 Kernel 5.10 AMI...[read more](#)
 ami-026b57f3c385c2ee...

Virtual server type (instance type)
 t2.micro

Firewall (security group)
 New security group

Storage (volumes)

Cancel

Launch instance

Looking for language selection? Find it in the new Unified Settings
 © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Services

Search for services, features, blogs, docs, and more

[Alt+S]

N. Virginia

Corestack_Role/gaurav.mishra5_mphosis @ srathanand-achugatta

security group rules to allow access from known IP addresses only.

Add security group rule

Configure storage [info](#)

Advanced

1 x 17 GiB gp2

Root volume (Not encrypted)

Add new volume

0 x File systems

Edit

Advanced details [info](#)

Summary

Number of instances [info](#)
 1

Software image (AMI)
 Amazon Linux 2 Kernel 5.10 AMI...[read more](#)
 ami-026b57f3c385c2ee...

Virtual server type (instance type)
 t2.micro

Firewall (security group)
 New security group

Storage (volumes)

Cancel

Launch instance

Looking for language selection? Find it in the new Unified Settings
 © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia Corestack_Role/gaurav.mishra1_ryhask @ srathanand-achugatto

EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance [i-096c5d10b58b42685](#)

[Launch log](#)

Next Steps

Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
[Create billing alerts](#)

Connect to your instance
Once your instance is running, log into it from your local computer.
[Connect to instance](#)
[Learn more](#)

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
[Connect an RDS database](#)
[Create a new RDS database](#) [Learn more](#)

[back](#) Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

EC2 > Instances > [i-029403f23ecd40897](#) > Connect to instance

Connect to instance [Info](#)

Connect to your instance [i-029403f23ecd40897](#) (ELK Ins) using any of these options

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID
[i-029403f23ecd40897](#) (ELK Ins)

Public IP address
[3.84.4.75](#)

User name

Connect using a custom user name, or use the default user name `ec2-user` for the AMI used to launch the instance.

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

[Cancel](#) [Connect](#)

```
← ↻ ⚠ Not secure | 3.84.475.9200
{
  "status": 200,
  "name": "Harry Leland",
  "cluster_name": "elasticsearch",
  "version": {
    "number": "1.7.3",
    "build_hash": "443670b1385b81250647f593f7202acbd810e8ec",
    "build_timestamp": "2015-09-14T09:40:53Z",
    "build_snapshot": false,
    "lucene_version": "4.10.4"
  },
  "tagline": "You Know, for Search"
}
```

← ↻ ⚠ Not secure | 3.84.475.9200/plugins/head/

Elasticsearch <http://3.84.4.75:9200/> Connect **elasticsearch** Cluster Health: green (6 of 6)

Overview | Indices | Browser | Structured Query [+] | Any Request [+]

Cluster Overview [Split Cluster](#) [Split Indices](#) [View Aliases](#) [Index Files](#)

★ **Harry Leland** [Info](#) [Actions](#)

Not secure | 244.75.5350/plugin/aggregates/node/

ES node REST endpoint: <http://34.4.79.9290> Refresh every: 2 sec Keep: 5 min History Disconnect

[nodes](#) [cluster](#)

Cluster: elasticsearch
Number of nodes: 1
Status: green

Harry Leland

Not secure | 244.75.5350/plugin/aggregates/node/xxw2w2GAv0y1D3XmU3Q

ES node REST endpoint: <http://34.4.79.9290> Refresh every: 2 sec Keep: 5 min History Disconnect

[nodes](#) [cluster](#)

Cluster: elasticsearch
Number of nodes: 1
Status: green

Harry Leland

Selected node:
Name: Harry Leland
ID: xxw2w2GAv0y1D3XmU3Q
Hostname: ip-172-31-52-162.ec2.internal
Elasticsearch version: 1.7.2

JVM

VM name: OpenJDK 64-Bit Server VM
VM vendor: Red Hat, Inc.
VM version: 25.342-b07

Uptime: 41.3m
Java version: 1.8.0_342
PID: 3728

Heap Mem

Committed: 247.8mb
Used: 83.1mb

Non-Heap Mem

Committed: 43.8mb
Used: 44.8mb

Threads

Peak: 26
Count: 26

GC (1)

Total time (G1): 52ms / 112ms
Total count (G1): 1 / 2

Thread Pools

Search	Index	Bulk	Refresh

The figure displays four empty charts, each representing a different Elasticsearch operation: Search, Index, Bulk, and Refresh. Each chart has a legend with three items: Queue (blue circle), Peak (orange square), and Count (green triangle). Below each chart, the status for Queue, Peak, and Count is shown as 0.

Operation	Queue	Peak	Count
Search	0	0	0
Index	0	0	0
Bulk	0	0	0
Refresh	0	0	0

CPU vendor: Intel
CPU model: Xeon (2399 MHz)
CPU total logical cores: 1
CPU cache: 30kb

Uptime: 2.9s
Refresh interval: 1ams
Total mem: 965.7mb (1012988368 B)
Total swap: 0b (0 B)

CPU (%)

Total: 100%
User: 1%
Sys: 1%

Mem

Free: 561.6mb
Used: 404mb

Swap

Free: 0b
Used: 0b

Load Average

2.0
1.01
0.02

The screenshot displays the Netstat application window with the following sections:

- Process:**
 - File Descriptors:** A line graph showing the number of open and closed file descriptors over time. The y-axis ranges from 0 to 600. The 'Open' series is consistently near zero, while the 'Close' series shows periodic spikes reaching up to 600.
 - Mem:** A bar chart showing memory usage for 'Total virtual', 'Resident', and 'Shared' memory. The y-axis ranges from 0 to 80. 'Total virtual' is the highest, followed by 'Resident', and 'Shared' is the lowest.
 - CPU time (s):** A line graph showing CPU time usage for 'Total', 'User', and 'Sys' over time. The y-axis ranges from 0 to 20. The 'Total' series shows significant spikes, while 'User' and 'Sys' are lower.
 - CPU (%)**: A bar chart showing CPU usage for 'Total', 'User', and 'Sys' over time. The y-axis ranges from 0 to 100. 'Total' usage is consistently high, near 100%.
- HTTP & Transport:**
 - HTTP address:** A line graph showing the number of HTTP connections over time. The y-axis ranges from 0 to 100. The 'Open' series shows periodic spikes reaching up to 100.
 - Transport address:** A line graph showing the number of transport connections over time. The y-axis ranges from 0 to 10. The 'Open' series shows periodic spikes reaching up to 10.
- Indices:**
 - Docs count:** A line graph showing the number of documents over time. The y-axis ranges from 0 to 100. The 'Open' series shows periodic spikes reaching up to 100.
 - Search requests per second (s):** A line graph showing the number of search requests per second over time. The y-axis ranges from 0 to 10. The 'Open' series shows periodic spikes reaching up to 10.
 - Search time per second (s):** A line graph showing the search time per second over time. The y-axis ranges from 0 to 10. The 'Open' series shows periodic spikes reaching up to 10.
 - Get requests per second (s):** A line graph showing the number of get requests per second over time. The y-axis ranges from 0 to 10. The 'Open' series shows periodic spikes reaching up to 10.
 - Get time per second (s):** A line graph showing the get time per second over time. The y-axis ranges from 0 to 10. The 'Open' series shows periodic spikes reaching up to 10.

