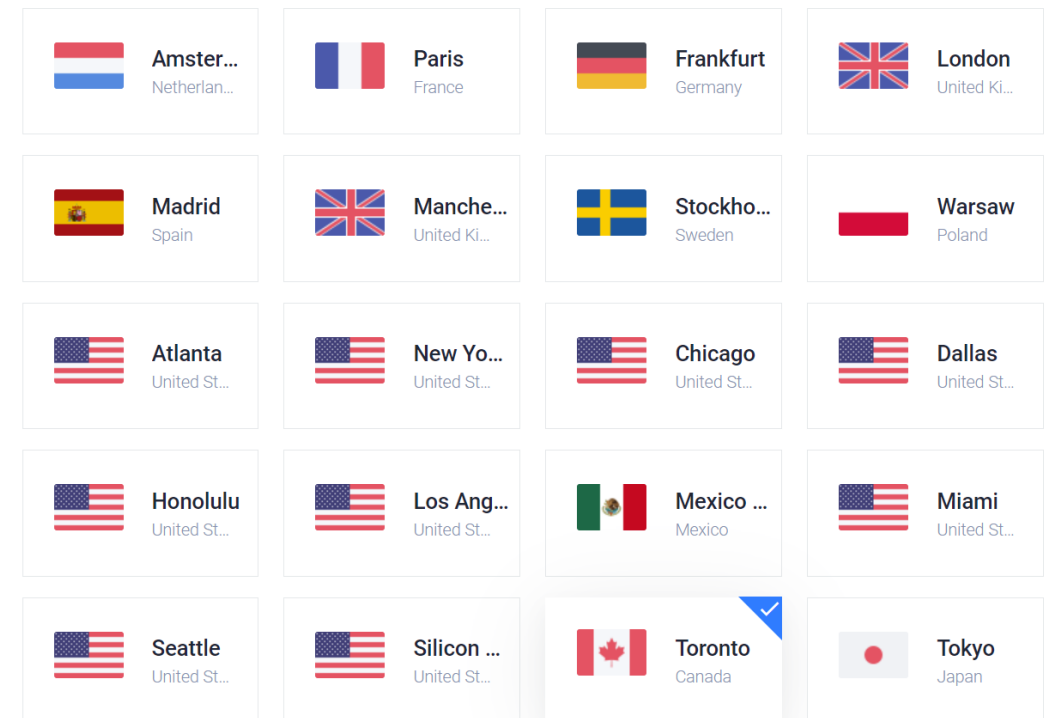
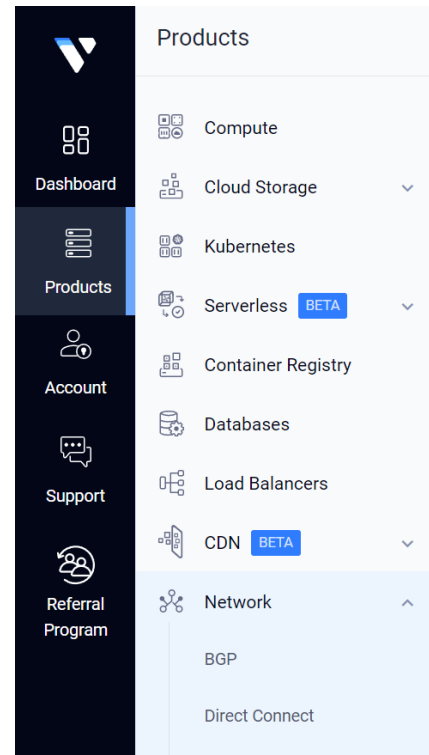


# Day 3 – Elasticsearch Setup

# Elasticsearch setup

Per creare l'infrastruttura così come l'abbiamo progettata nel Day 1, ci serviremo del Cloud Provider **Vultr**.  
Prima di procedere col setup di **Elasticsearch** creiamo una **VPC** (Virtual Private Cloud network), assicurandoci che le macchine virtuali che creerò siano nella stessa location della VPC creata.



# Elasticsearch setup

Qui impostiamo il range di Ip di cui ci serviremo con relativa maschera di rete e daremo un nome a tale rete.

## Virtual Private Clouds 2.0

Products

- Dashboard
- Products
- Account
- Support
- Referral Program

Products

- Compute
- Cloud Storage
- Kubernetes
- Serverless **BETA**
- Container Registry
- Databases
- Load Balancers
- CDN **BETA**
- Network **^**
  - BGP
  - Direct Connect

multiple VPCs with overlapping IP blocks, the network connectivity on that node will not work correctly.

Auto-Assi...  
Automatic...

Configure...  
Manual - ...

### Set IP Range

[IPv4 Subnet Calculator](#) ?

Network Address  
172.31.0.0

Network Prefix  
24


### VPC 2.0 Network Description

Give the network a name.

Name  
MYDFIR-SOC-Challenge

Add Network

+ Add VPC 2.0 Network

| ID                                   | Description          | Location  | Subnet        |
|--------------------------------------|----------------------|---|---------------|
| 3f1ca0fa-e8a4-46b2-a005-9a96a2772719 | MYDFIR-SOC-Challenge |  Toronto | 172.31.0.0/24 |

Scegliamo la configurazione e le caratteristiche del server che ospiterà **Elasticsearch** e **Kibana**. Inoltre verrà assegnato anche un IP privato a tale macchina all'interno della nostra **VPC** (evidenziato in basso a destra).

**Optimized Cloud Compute - Dedicated CPU**

Virtual machines for more demanding business apps, e.g. production websites, CI/CD, video transcoding, or larger databases.

**Ubuntu**

22.04 LTS x64

**Toronto** Canada

Choose Plan

General Purpose CPU Optimized Memory Optimized Storage Optimized

| Name       | Cores   | Memory | Storage    | Bandwidth | Price                       |
|------------|---------|--------|------------|-----------|-----------------------------|
| 30 GB NVMe | 1 vCPU  | 4 GB   | 30 GB NVMe | 4 TB      | \$30/month<br>\$0.045/hour  |
| 50 GB NVMe | 2 vCPUs | 8 GB   | 50 GB NVMe | 5 TB      | \$60/month<br>\$0.089/hour  |
| 80 GB NVMe | 4 vCPUs | 16 GB  | 80 GB NVMe | 6 TB      | \$120/month<br>\$0.179/hour |

Additional Features

**Auto Backups** \$24.00/mo

Highly recommend for mission-critical systems. Backups enable easy recovery from a disaster by spinning up a new instance from a saved image.

[Learn More](#)

**IPv6** Free

If checked, an IPv6 address will be assigned to the instance.

**DDoS Protection** \$10/mo

Add a layer of protection to ensure consistent performance and uninterrupted system access, even when targeted by Distributed Denial of Service attacks.

[Learn more](#)

**Virtual Private Cloud** Free

If you have VPCs in this region, you can select one below. Otherwise a default VPC will be created. An IP is provided, but you may set a different IP if desired.

[Learn more](#)

**Virtual Private Cloud 2.0** Free

If you have VPCs in this region, you can select one below. Otherwise a default VPC will be created. An IP is provided, but you may set a different IP if desired.

[Learn more](#)

**Limited User Login** Free

If checked, credentials for a limited user (linuxuser) will be configured instead of the root user. The linuxuser account will have sudo access.

VPC 2.0 Manage

Be careful if you have VPCs with overlapping IP blocks. If you attach a

**MYDFIR-SOC-Challenge**

IP Address  
172.31.0.3

# Elasticsearch setup

Diamo un nome al server:

## Server Settings

SSH Keys

Manage

Choose SSH Key



## Server Hostname & Label

Server Hostname

Enter server hostname (3/63)  
ELK

Server Label

Enter server label  
ELK

# Elasticsearch setup

Scelta la configurazione procediamo con il deploy della macchina virtuale con la versione di Ubuntu selezionata, come da immagine sotto risulta avviata.





Server added successfully!

## Cloud Compute

☰ Location ▼

🔍 Search

+ Deploy

| <input type="checkbox"/> | Name   | OS  | Location  | Charges | Status  |     |
|--------------------------|--|---|---|---------|---|-----|
| <input type="checkbox"/> | <b>ELK</b><br>16384.00 MB Optimized Cloud - 155  |  |  Toronto | \$0.18  |  Running | ... |

# Elasticsearch setup

Dal mio PC, mi collego in **SSH** alla macchina virtuale utilizzando il suo IP pubblico. Questo IP pubblico è assegnato dal cloud provider e funge da ponte verso l'IP privato della macchina all'interno della VPC (Virtual Private Cloud). Attraverso il meccanismo di NAT (Network Address Translation), il traffico proveniente dal mio PC tramite internet viene instradato dall'IP pubblico all'IP privato della macchina, consentendo così l'accesso sicuro e remoto alle risorse all'interno della VPC.

Location:  Toronto

IP Address: 155.  

Username: root

Password: .....  

```
PS C:\Windows\system32> ssh root@[redacted]
root@[redacted]:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Fri Sep 13 05:30:39 PM UTC 2024

System load:  0.0          Processes:            145
Usage of /:   16.0% of 74.45GB Users logged in:        0
Memory usage: 1%          IPv4 address for enp1s0: [redacted]
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

# Elasticsearch setup

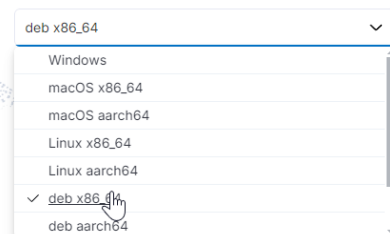
Ora che sono all'interno della macchina virtuale (che chiameremo semplicemente **ELK**, aggiorniamo i repository del sistema operativo:

```
root@ELK: ~  
root@ELK:~# apt-get update && apt-get upgrade -y
```

Scarichiamo **Elasticsearch** copiando il link dal sito ufficiale e lanciandolo sulla console:

## 1 Download and unzip Elasticsearch

Choose platform:



```
root@ELK: ~  
root@ELK:~# wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.15.1-amd64.deb
```



# Elasticsearch setup

Verifico se il file è stato scaricato e procedo con l'installazione:

```
root@ELK:~# ls
elasticsearch-8.15.1-amd64.deb  snap
root@ELK:~# dpkg -i elasticsearch-8.15.1-amd64.deb
Selecting previously unselected package elasticsearch.
(Reading database ... 85487 files and directories currently installed.)
Preparing to unpack elasticsearch-8.15.1-amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (8.15.1) ...
```

# Elasticsearch setup

Una volta completata l'installazione, è importante prestare attenzione a questa sezione, poiché contiene la password generata per il superuser e le istruzioni su come effettuare il reset della stessa.

```
----- 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 : XXXXXXXXXX  
  
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'.  
-----
```

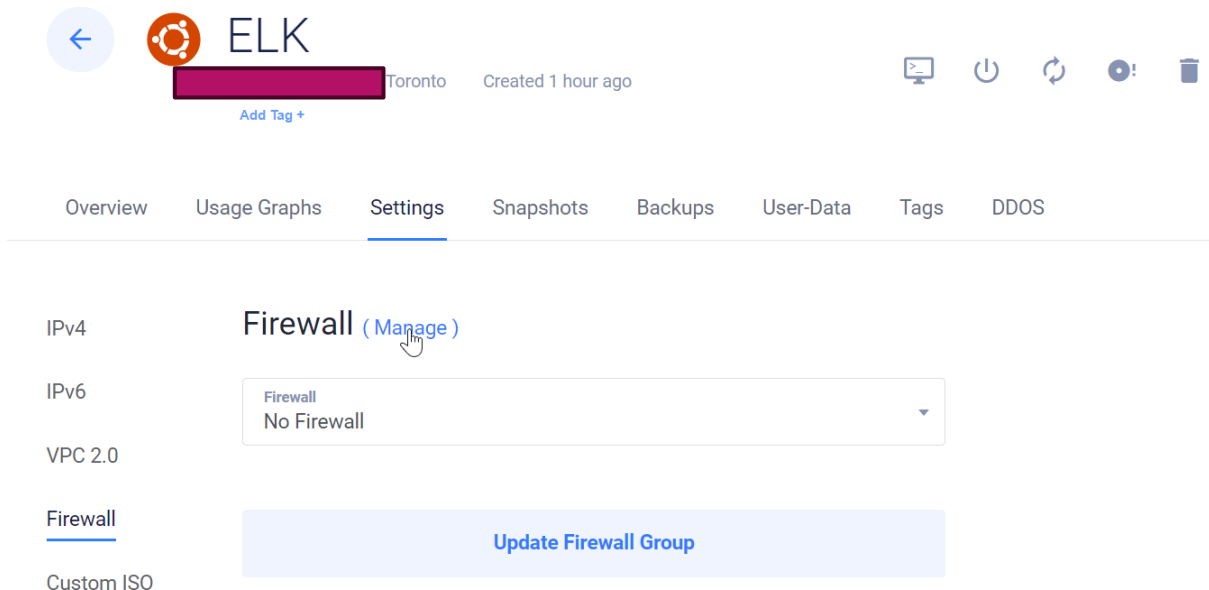
# Elasticsearch setup

Configuriamo **Elasticsearch** modificando il file `elasticsearch.yml`. Aggiorno la sezione «Network» per consentire le connessioni remote al servizio:

```
# ----- Network -----  
#  
# By default Elasticsearch is only accessible on localhost. Set a different  
# address here to expose this node on the network:  
#  
network.host: 155.██████████  
#  
# 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.  
#
```

# Elasticsearch setup

Per rafforzare i controlli e migliorare la sicurezza, configuriamo un **gruppo firewall** nella sezione dedicata di Vultr, definendo regole che limitano e controllano il traffico in entrata e in uscita verso la macchina virtuale.



The screenshot shows the Vultr dashboard for an instance named 'ELK'. The instance is located in 'Toronto' and was created '1 hour ago'. The 'Settings' tab is selected in the top navigation bar. On the left sidebar, the 'Firewall' section is highlighted. The main content area shows the 'Firewall' settings for the selected instance, with a dropdown menu currently set to 'No Firewall'. A blue button labeled 'Update Firewall Group' is visible at the bottom of the settings panel.

← ELK Toronto Created 1 hour ago

Add Tag +

Overview Usage Graphs **Settings** Snapshots Backups User-Data Tags DDOS

IPv4 Firewall (Manage)

IPv6 Firewall No Firewall

VPC 2.0

Firewall Update Firewall Group

Custom ISO

## ← Add Firewall Group

### Add Firewall Group

SOC Analyst

**Add Firewall Group**

# Elasticsearch setup

Per impostazione predefinita, chiunque su Internet può accedere alla macchina virtuale che abbiamo configurato. Per limitare l'accesso solo a me, seleziono 'myip' per fare in modo che solo il mio IP pubblico possa connettersi.

Manage Firewall Group

4-09-13 17:56:21

Updated: 2024-09-13 17:56:21

Description

SOC Analyst

Group Rules

0/50

Linked Instances

0

IPv4 Rules

IPv6 Rules

Linked Instances

Inbound IPv4 Rules

This firewall ruleset will not be active until at 1

MyIP

Custom

Anywhere

Cloudflare

Load Balancer

| Action | Protocol | Port (or range) ? | Source         | Notes    | Action |
|--------|----------|-------------------|----------------|----------|--------|
| accept | SSH      | 22                | A... 0.0.0.0/0 | Add note | +      |

IPv4 Rules

IPv6 Rules

Linked Instances

## Inbound IPv4 Rules

| Action | Protocol | Port (or range) ? | Source    | Notes     | Action     |
|--------|----------|-------------------|-----------|-----------|------------|
| accept | SSH      | 22                | Anywhere  | 0.0.0.0/0 | Add note + |
| accept | SSH      | 22                |           |           |            |
| drop   | any      | 0 - 65535         | 0.0.0.0/0 |           | (default)  |

# Elasticsearch setup

Poi vado su «Compute» a sinistra, seleziono la macchina virtuale **ELK** e, nella sezione firewall, attribuisco il firewall group appena creato. Infine, clicco su 'Update Firewall Group' per applicare le regole del firewall alla macchina virtuale.

The screenshot shows the Oracle Cloud console interface for a virtual machine named 'ELK'. The top navigation bar includes a back arrow, the VM icon, the name 'ELK', its IP address '155. [redacted]', location 'Toronto', and creation time 'Created 1 hour ago'. Below this is a row of tabs: Overview, Usage Graphs, Settings (selected), Snapshots, Backups, User-Data, Tags, and DDOS. The main content area is titled 'Firewall (Manage)' and shows a list of firewall groups. The 'No Firewall' option is currently selected. A search bar is visible above the list. The list contains two items: 'No Firewall' and 'c4233d71-70e4-440e-73-ddbbe854ce6b: SOC Analyst'. A mouse cursor is hovering over the 'SOC Analyst' option, which is highlighted in blue. On the left side of the console, a sidebar menu shows 'IPv4', 'IPv6', 'VPC 2.0', 'Firewall' (selected), and 'Custom ISO'.

Firewall group updated. It may take up to 120 seconds for these changes to apply.

# Elasticsearch setup

1. **daemon-reload**: Applica le modifiche ai file di configurazione ricaricando le configurazioni.
2. **enable**: Configura il servizio per avviarsi automaticamente al prossimo riavvio del sistema.
3. **start**: Avvia immediatamente il servizio.

```
root@ELK: /etc/elasticsearch
```

```
root@ELK:/etc/elasticsearch# systemctl daemon-reload
root@ELK:/etc/elasticsearch# systemctl enable elasticsearch.service
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.
root@ELK:/etc/elasticsearch# systemctl start elasticsearch.service
root@ELK:/etc/elasticsearch#
```

# Elasticsearch setup

```
root@ELK:/etc/elasticsearch# systemctl status elasticsearch.service
```

```
● elasticsearch.service - Elasticsearch  
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)  
   Active: active (running) since Fri 2024-09-13 18:06:12 UTC; 47s ago  
     Docs: https://www.elastic.co  
    Main PID: 14858 (java)  
      Tasks: 95 (limit: 19042)  
    Memory: 8.4G  
       CPU: 43.927s  
    CGroup: /  
            └─┬─ java  
               │   ├── elasticsearch.bootstrap  
               │   ├── elasticsearch.configserver  
               │   ├── elasticsearch.datastream  
               │   ├── elasticsearch.indexing  
               │   ├── elasticsearch.logstash  
               │   ├── elasticsearch.migration  
               │   ├── elasticsearch.monitor  
               │   ├── elasticsearch.pluginmgr  
               │   ├── elasticsearch.reindex  
               │   ├── elasticsearch.snapshotrestore  
               │   ├── elasticsearch.taskscheduler  
               │   └── elasticsearch.transporter  
             └─┴─ java  
                  └─ jdk.jvmti
```

```
Sep 13 18:05:5 root@elk: ~$ journalctl --no-pager -f -n 100 -e -t "Elasticsearch startup"
```

```
Sep 13 18:06:00 root@elk: ~$ journalctl --no-pager -f -n 100 -e -t "Elasticsearch startup"
```

```
Sep 13 18:06:00 root@elk: ~$ journalctl --no-pager -f -n 100 -e -t "Elasticsearch startup"
```

```
Sep 13 18:06:12 root@elk: ~$ journalctl --no-pager -f -n 100 -e -t "Elasticsearch startup"
```

```
lines 1-17/17 (END)
```

```
root@ELK:/etc/elasticsearch# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2024-09-13 18:06:12 UTC; 47s ago
     Docs: https://www.elastic.co
   Main PID: 14858 (java)
     Tasks: 95 (limit: 19042)
    Memory: 8.4G
       CPU: 43.927s
   CGroup: /
           └─┬─ java
               │
               └─┬─ java
                   │
                   └─ java

Sep 13 18:05:5
Sep 13 18:06:0
Sep 13 18:06:0
Sep 13 18:06:1
lines 1-17/17 (END)
```