

3. ?????????????? ??

??????????????

????????????????

??????????????

Для встановлення балансувальника навантаження на відповідній віртуальній машині необхідно виконати наступні кроки:

1. Закрити доступ до сторонніх репозиторіїв за допомогою виконання наступної команди:

```
sudo sed -i 's/^[A-Za-z0-9]#&/' /etc/apt/sources.list
```

2. Додати у операційну систему репозиторій з пакетами системи «Трембіта»:

```
echo 'deb https://project-repo.trembita.gov.ua:8081/repository/ss-1.12.6/ bionic main' | sudo tee -a /etc/apt/sources.list
```

Перевірити результат виконання команд можна за допомогою текстового редактора nano, відкривши файл на редагування за допомогою виконання наступної команди:

```
nano /etc/apt/sources.list
```

3. Додати GPG ключ репозиторію за допомогою виконання наступної команди:

```
sudo wget -O - https://project-repo.trembita.gov.ua:8081//public-keys/public.key.txt | sudo apt-key add -
```

Якщо команду виконано успішно, буде виведено повідомлення «ОК».

4. Оновити списки пакетів, та встановити Nginx за допомогою за допомогою послідовного виконання наступних команд:

```
sudo apt update  
sudo apt install -y nginx
```

5. Створити файл `/etc/nginx/conf.d/upstream.conf` та відкрити його на редагування за допомогою виконання наступної команди:

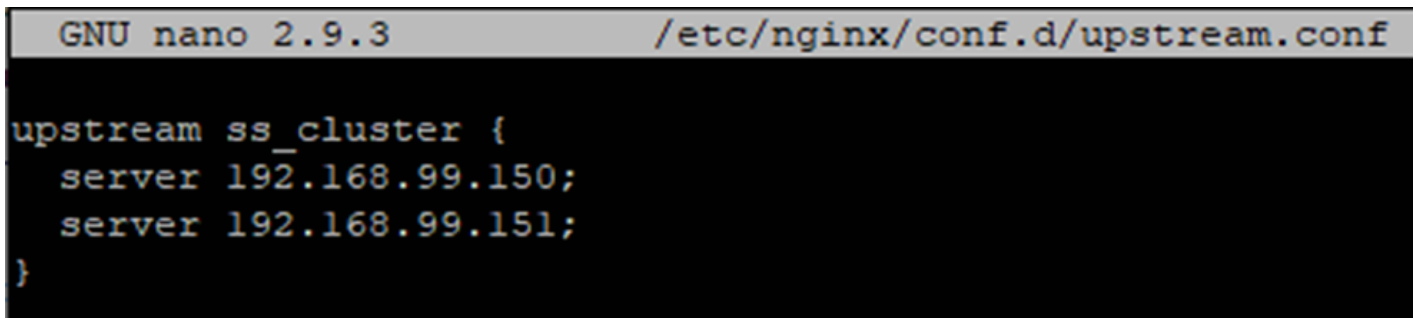
```
sudo nano /etc/nginx/conf.d/upstream.conf
```

6. Додати наступні рядки до новоствореного файлу:

```
upstream ss_cluster {  
    server <Your-security-server-1-IP>;  
    server <Your-security-server-2-IP>;  
}
```

де `<Your-security-server-1-IP>` — внутрішня (локальна) IP-адреса першого шлюзу безпечного обміну, який буде працювати в кластері,

`<Your-security-server-2-IP>` — внутрішня (локальна) IP-адреса другого шлюзу безпечного обміну, який буде працювати в кластері.



```
GNU nano 2.9.3 /etc/nginx/conf.d/upstream.conf  
upstream ss_cluster {  
    server 192.168.99.150;  
    server 192.168.99.151;  
}
```

7. Створити файл `/etc/nginx/conf.d/upstream_log_def.conf` та відкрити його на редагування за допомогою виконання наступної команди:

```
sudo nano /etc/nginx/conf.d/upstream_log_def.conf
```

8. Додати наступні рядки до новоствореного файлу:

```
log_format upstreamlog '[${time_local}] $remote_addr - $remote_user - $server_name $host to:  
$upstream_addr: $request $status upstream_response_time $upstream_response_time msec $msec  
request_time $request_time';
```



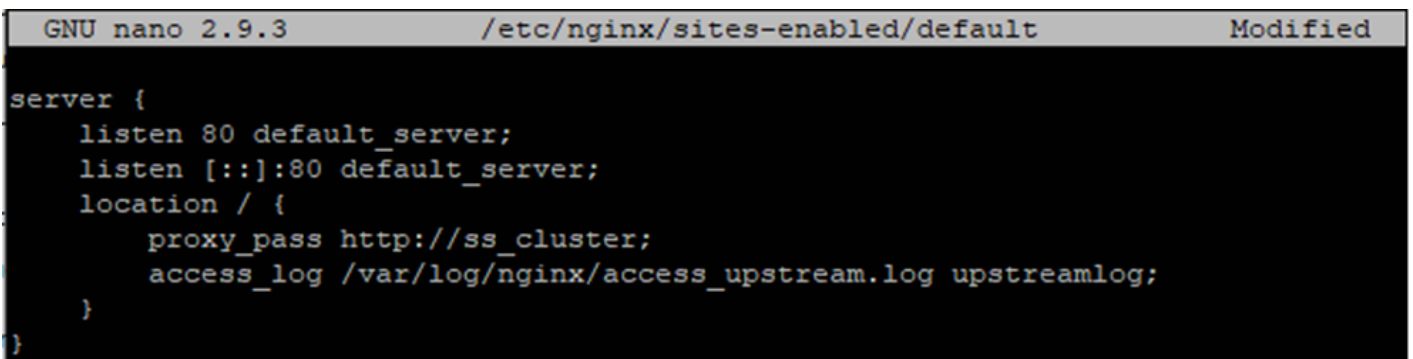
```
GNU nano 6.2 /etc/nginx/conf.d/upstream_log_def.conf  
log_format upstreamlog '[${time_local}] $remote_addr - $remote_user - $server_name $host to: $upstream_addr: $request $status upstream_response_time $upstream_response_time msec $msec request_time $request_time';
```

9. Створити файл `/etc/nginx/sites-enabled/default` та відкрити його на редагування за допомогою виконання наступної команди:

```
sudo nano /etc/nginx/sites-enabled/default
```

10. Додати наступні рядки до новоствореного файлу (замінити вміст файлу, якщо даний файл не порожній):

```
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    location / {
        proxy_pass http://ss_cluster;
        access_log /var/log/nginx/access_upstream.log upstreamlog;
    }
}
```

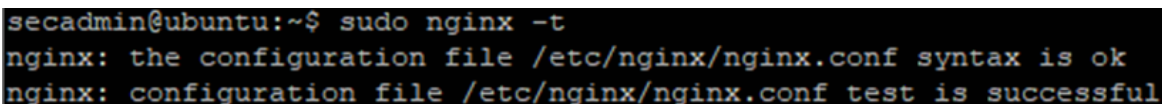


```
GNU nano 2.9.3 /etc/nginx/sites-enabled/default Modified
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    location / {
        proxy_pass http://ss_cluster;
        access_log /var/log/nginx/access_upstream.log upstreamlog;
    }
}
```

11. Перевірити конфігурацію за допомогою виконання наступної команди:

```
sudo nginx -t
```

Якщо перевірку конфігурації пройдено успішно, буде виведено повідомлення «test is successful»:



```
secadmin@ubuntu:~$ sudo nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

12. Перезавантажити сервіс NGINX за допомогою виконання наступної команди:

```
sudo service nginx reload
```

Після закінчення налаштування балансувальника навантаження необхідно переналаштувати вебклієнт таким чином, щоб запити надсилались на мережеву адресу балансувальника навантаження (замість IP-адреси шлюзу безпечного обміну необхідно вказати IP-адресу балансувальника навантаження, інші параметри запиту залишити без зміни), який буде автоматично розподіляти запити між шлюзами безпечного обміну порівну. Шлях URL в запиті буде повністю переадресовуватися на шлюзи безпечного обміну

Приклад запиту до REST-сервісу через балансувальник навантаження буде виглядати наступним чином:

http://<Load-Balancer-IP_address>/restapi

де <Load-Balancer-IP_address> — локальна IP-адреса балансувальника навантаження.

Версія #5

Admin створив 2024-06-25 09:29:32 UTC

Admin оновив 2024-09-22 23:12:31 UTC