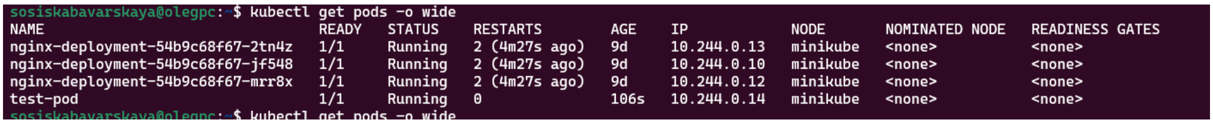
Д37

Применить сетевые политики для деплоймента:

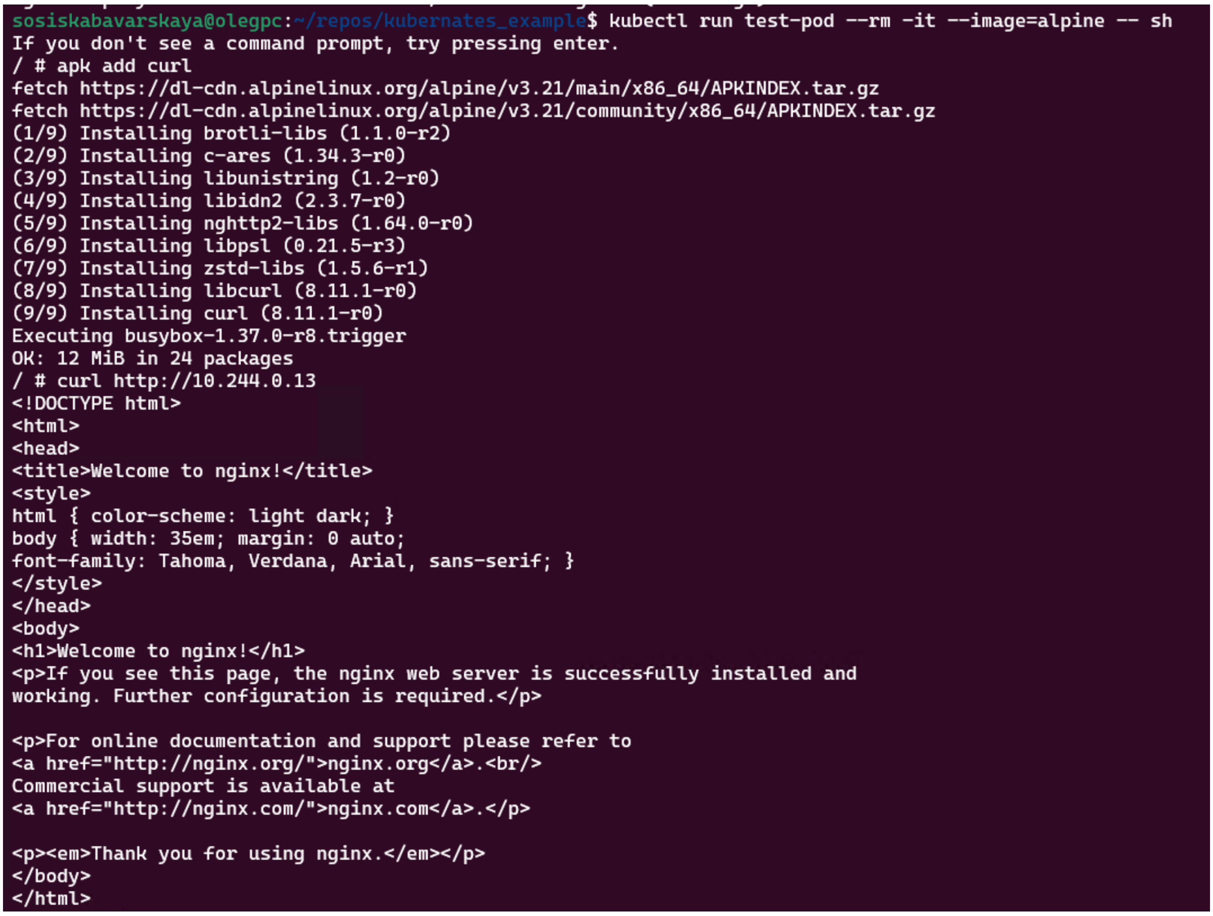
Сначала покажу список айпишников у подов с нгинком и покажу ситуацию до применения моих сетевых политик:



```
sosiskabavarskaya@olegpc:~$ kubectl get pods -o wide
NAME                               READY   STATUS    RESTARTS        AGE    IP            NODE       NOMINATED NODE   READINESS GATES
nginx-deployment-54b9c68f67-2tn4z  1/1     Running   2 (4m27s ago)   9d     10.244.0.13   minikube   <none>           <none>
nginx-deployment-54b9c68f67-jf548  1/1     Running   2 (4m27s ago)   9d     10.244.0.10   minikube   <none>           <none>
nginx-deployment-54b9c68f67-mrr8x  1/1     Running   2 (4m27s ago)   9d     10.244.0.12   minikube   <none>           <none>
test-pod                           1/1     Running   0               106s   10.244.0.14   minikube   <none>           <none>
sosiskabavarskaya@olegpc:~$ kubectl get pods -o wide
```

Далее создам тестовый под и сразу залезу в него и попробую вне деплоймента с нгинксом курлом достучаться до него:

```
kubectl run test-pod --rm -it --image=alpine -- sh
```



```
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ kubectl run test-pod --rm -it --image=alpine -- sh
If you don't see a command prompt, try pressing enter.
/ # apk add curl
fetch https://dl-cdn.alpinelinux.org/alpine/v3.21/main/x86_64/APKINDEX.tar.gz
fetch https://dl-cdn.alpinelinux.org/alpine/v3.21/community/x86_64/APKINDEX.tar.gz
(1/9) Installing brotli-libs (1.1.0-r2)
(2/9) Installing c-ares (1.34.3-r0)
(3/9) Installing libunistring (1.2-r0)
(4/9) Installing libidn2 (2.3.7-r0)
(5/9) Installing nghttp2-libs (1.64.0-r0)
(6/9) Installing libpsl (0.21.5-r3)
(7/9) Installing zstd-libs (1.5.6-r1)
(8/9) Installing libcurl (8.11.1-r0)
(9/9) Installing curl (8.11.1-r0)
Executing busybox-1.37.0-r8.trigger
OK: 12 MiB in 24 packages
/ # curl http://10.244.0.13
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

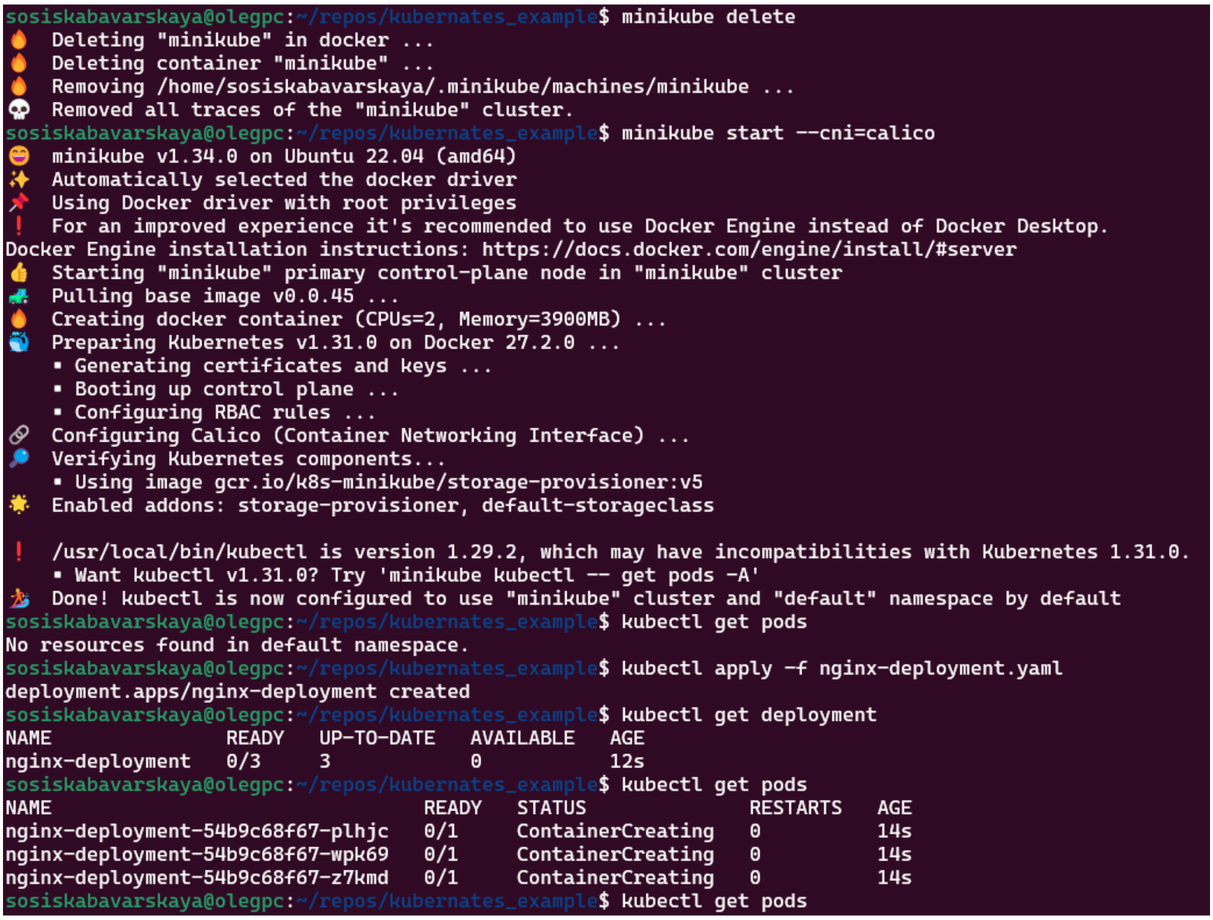
Видно, что ответ есть, нулевая страница нгинкса.

Попробуем применить сетевые политики, например на доступ к подам нгинкса только для подов с такой же меткой app: nginx

Вот так выглядит файл nginx-network-policy.yaml:

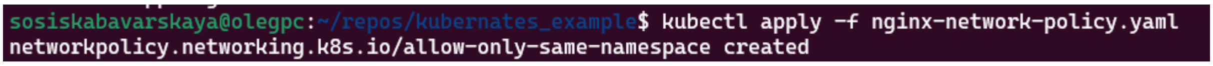
```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-only-same-namespace
  namespace: default
spec:
  podSelector:
    matchLabels:
      app: nginx
  policyTypes:
  - Ingress
  - Egress
  ingress:
  - from:
    - podSelector:
        matchLabels:
          app: nginx
  egress:
  - to:
    - podSelector:
        matchLabels:
          app: nginx
```

Для применения сетевой политики нужно переставить образ миникуба с включенным плагином calcio (CNI плагин). Также придется заново завести деплоймент нгинкса и также сразу применить сетевые политики для этих подов:



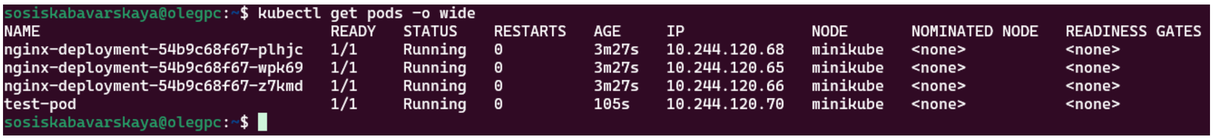
```
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ minikube delete
🔥  Deleting "minikube" in docker ...
🔥  Deleting container "minikube" ...
🔥  Removing /home/sosiskabavarskaya/.minikube/machines/minikube ...
💀  Removed all traces of the "minikube" cluster.
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ minikube start --cni=calico
😄  minikube v1.34.0 on Ubuntu 22.04 (amd64)
✨  Automatically selected the docker driver
📌  Using Docker driver with root privileges
❗  For an improved experience it's recommended to use Docker Engine instead of Docker Desktop.
Docker Engine installation instructions: https://docs.docker.com/engine/install/#server
👍  Starting "minikube" primary control-plane node in "minikube" cluster
🚜  Pulling base image v0.0.45 ...
🔥  Creating docker container (CPUs=2, Memory=3900MB) ...
🐳  Preparing Kubernetes v1.31.0 on Docker 27.2.0 ...
    ▪ Generating certificates and keys ...
    ▪ Booting up control plane ...
    ▪ Configuring RBAC rules ...
🔗  Configuring Calico (Container Networking Interface) ...
🔎  Verifying Kubernetes components...
    ▪ Using image gcr.io/k8s-minikube/storage-provisioner:v5
🌟  Enabled addons: storage-provisioner, default-storageclass

❗  /usr/local/bin/kubectl is version 1.29.2, which may have incompatibilities with Kubernetes 1.31.0.
    ▪ Want kubectl v1.31.0? Try 'minikube kubectl -- get pods -A'
🏄  Done! kubectl is now configured to use "minikube" cluster and "default" namespace by default
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ kubectl get pods
No resources found in default namespace.
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ kubectl apply -f nginx-deployment.yaml
deployment.apps/nginx-deployment created
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ kubectl get deployment
NAME               READY   UP-TO-DATE   AVAILABLE   AGE
nginx-deployment   0/3     3            0           12s
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ kubectl get pods
NAME                                READY   STATUS              RESTARTS   AGE
nginx-deployment-54b9c68f67-plhjc   0/1     ContainerCreating   0          14s
nginx-deployment-54b9c68f67-wpk69   0/1     ContainerCreating   0          14s
nginx-deployment-54b9c68f67-z7kmd   0/1     ContainerCreating   0          14s
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ kubectl get pods
```



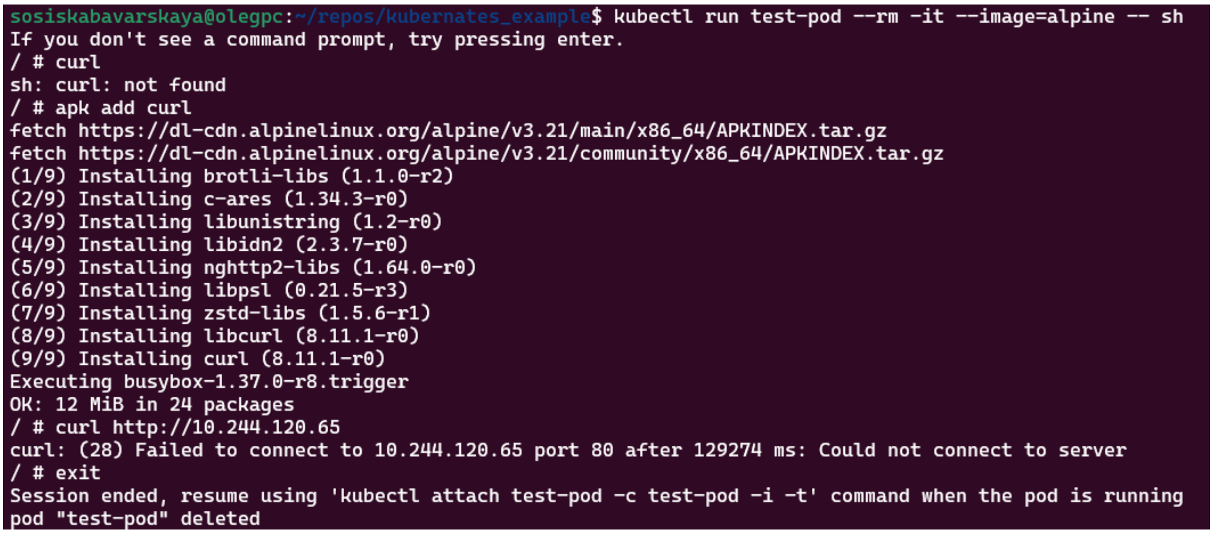
```
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ kubectl apply -f nginx-network-policy.yaml
networkpolicy.networking.k8s.io/allow-only-same-namespace created
```

Также получим новые айпишники подов



```
sosiskabavarskaya@olegpc:~$ kubectl get pods -o wide
NAME                                READY   STATUS    RESTARTS   AGE     IP              NODE       NOMINATED NODE   READINESS GATES
nginx-deployment-54b9c68f67-plhjc   1/1     Running   0          3m27s   10.244.120.68   minikube   <none>           <none>
nginx-deployment-54b9c68f67-wpk69   1/1     Running   0          3m27s   10.244.120.65   minikube   <none>           <none>
nginx-deployment-54b9c68f67-z7kmd   1/1     Running   0          3m27s   10.244.120.66   minikube   <none>           <none>
test-pod                            1/1     Running   0          105s    10.244.120.70   minikube   <none>           <none>
sosiskabavarskaya@olegpc:~$ 
```

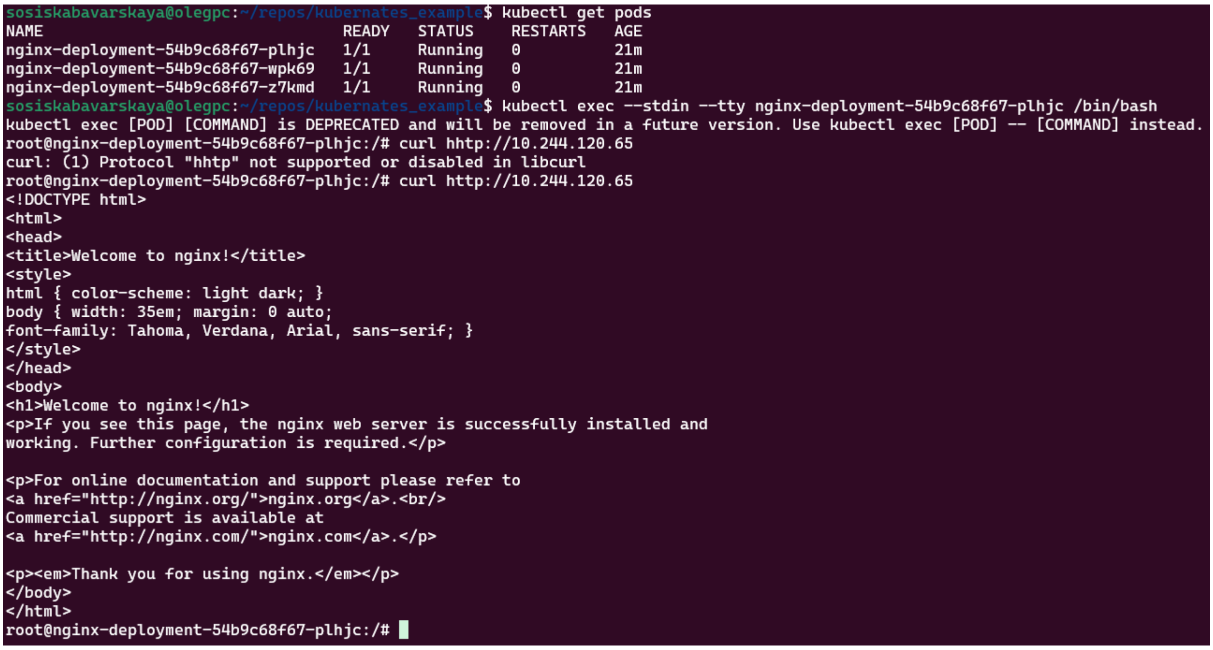
Попробуем пробиться через курл к подам нгинкса через тестовый под:



```
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ kubectl run test-pod --rm -it --image=alpine -- sh
If you don't see a command prompt, try pressing enter.
/ # curl
sh: curl: not found
/ # apk add curl
fetch https://dl-cdn.alpinelinux.org/alpine/v3.21/main/x86_64/APKINDEX.tar.gz
fetch https://dl-cdn.alpinelinux.org/alpine/v3.21/community/x86_64/APKINDEX.tar.gz
(1/9) Installing brotli-libs (1.1.0-r2)
(2/9) Installing c-ares (1.34.3-r0)
(3/9) Installing libunistring (1.2-r0)
(4/9) Installing libidn2 (2.3.7-r0)
(5/9) Installing nghttp2-libs (1.64.0-r0)
(6/9) Installing libpsl (0.21.5-r3)
(7/9) Installing zstd-libs (1.5.6-r1)
(8/9) Installing libcurl (8.11.1-r0)
(9/9) Installing curl (8.11.1-r0)
Executing busybox-1.37.0-r8.trigger
OK: 12 MiB in 24 packages
/ # curl http://10.244.120.65
curl: (28) Failed to connect to 10.244.120.65 port 80 after 129274 ms: Could not connect to server
/ # exit
Session ended, resume using 'kubectl attach test-pod -c test-pod -i -t' command when the pod is running
pod "test-pod" deleted
```

Теперь получить доступ по адресу пода нельзя

Попробуем получить доступ к поду нгинкс из соседнего в деплойменте:



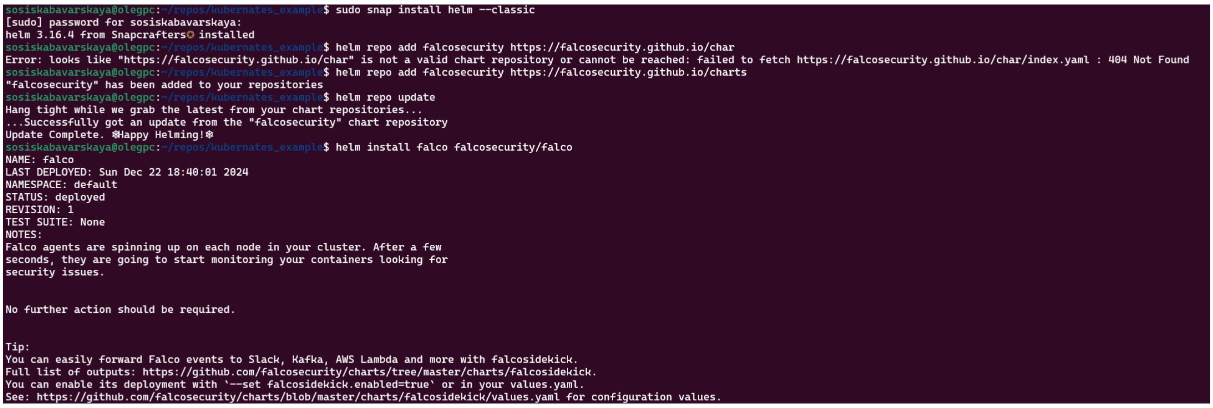
```
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ kubectl get pods
NAME                                READY   STATUS    RESTARTS   AGE
nginx-deployment-54b9c68f67-plhjc   1/1     Running   0          21m
nginx-deployment-54b9c68f67-wpk69   1/1     Running   0          21m
nginx-deployment-54b9c68f67-z7kmd   1/1     Running   0          21m
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ kubectl exec --stdin --tty nginx-deployment-54b9c68f67-plhjc /bin/bash
kubectl exec [POD] [COMMAND] is DEPRECATED and will be removed in a future version. Use kubectl exec [POD] -- [COMMAND] instead.
root@nginx-deployment-54b9c68f67-plhjc:/# curl hhtp://10.244.120.65
curl: (1) Protocol "hhtp" not supported or disabled in libcurl
root@nginx-deployment-54b9c68f67-plhjc:/# curl http://10.244.120.65
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
root@nginx-deployment-54b9c68f67-plhjc:/# █
```

Все прекрасно работает, сетевые политики настроены, но не ясно, зачем это было сделано для нгинкса.

Установка фалко:



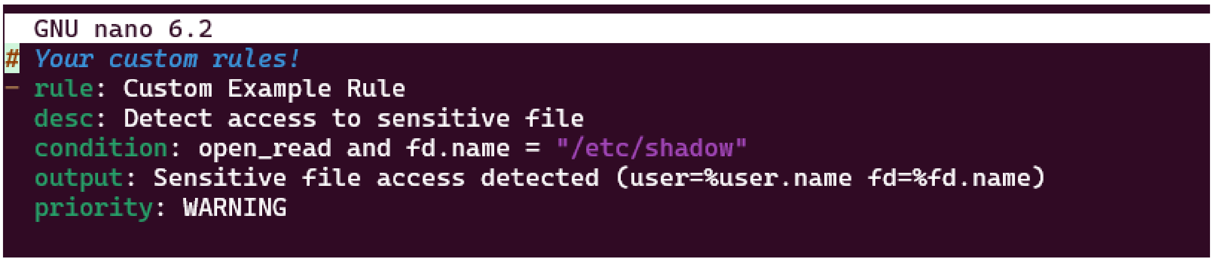
```
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ sudo snap install helm --classic
[sudo] password for sosiskabavarskaya:
helm 3.16.4 from Snapcrafters✪ installed
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ helm repo add falcosecurity https://falcosecurity.github.io/char
Error: looks like "https://falcosecurity.github.io/char" is not a valid chart repository or cannot be reached: failed to fetch https://falcosecurity.github.io/char/index.yaml : 404 Not Found
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ helm repo add falcosecurity https://falcosecurity.github.io/charts
"falcosecurity" has been added to your repositories
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ helm repo update
Hang tight while we grab the latest from your chart repositories...
...Successfully got an update from the "falcosecurity" chart repository
Update Complete. ⎈Happy Helming!⎈
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ helm install falco falcosecurity/falco
NAME: falco
LAST DEPLOYED: Sun Dec 22 18:40:01 2024
NAMESPACE: default
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
Falco agents are spinning up on each node in your cluster. After a few
seconds, they are going to start monitoring your containers looking for
security issues.


No further action should be required.


Tip:
You can easily forward Falco events to Slack, Kafka, AWS Lambda and more with falcosidekick.
Full list of outputs: https://github.com/falcosecurity/charts/tree/master/charts/falcosidekick.
You can enable its deployment with `--set falcosidekick.enabled=true` or in your values.yaml.
See: https://github.com/falcosecurity/charts/blob/master/charts/falcosidekick/values.yaml for configuration values.
```

Настройка фалко:

кастомное правило для фалко, далее рестарт фалко (удалением подов, оно само перезапустит)



```
  GNU nano 6.2
# Your custom rules!
- rule: Custom Example Rule
  desc: Detect access to sensitive file
  condition: open_read and fd.name = "/etc/shadow"
  output: Sensitive file access detected (user=%user.name fd=%fd.name)
  priority: WARNING
```