

# SteamCloud

```
└─# nmap -sCV -p 22,2380,8443,10250 -A 10.10.11.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 03:28 PDT
Nmap scan report for 10.10.11.133
Host is up (0.23s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 fc:fb:90:ee:7c:73:a1:d4:bf:87:f8:71:e8:44:c6:3c (RSA)
|   256 46:83:2b:1b:01:db:71:64:6a:3e:27:cb:53:6f:81:a1 (ECDSA)
|_  256 1d:8d:d3:41:f3:ff:a4:37:e8:ac:78:08:89:c2:e3:c5 (ED25519)
2380/tcp  open  ssl/etcd-server?
| ssl-cert: Subject: commonName=steamcloud
| Subject Alternative Name: DNS:localhost, DNS:steamcloud, IP Address:10.10.11.133, IP
Address:127.0.0.1, IP Address:0:0:0:0:0:0:0:1
| Not valid before: 2024-06-03T10:26:30
|_ Not valid after:  2025-06-03T10:26:31
| tls-alpn:
|_  h2
|_ ssl-date: TLS randomness does not represent time
8443/tcp  open  ssl/https-alt
| tls-alpn:
|   h2
|_  http/1.1
| ssl-cert: Subject: commonName=minikube/organizationName=system:masters
| Subject Alternative Name: DNS:minikubeCA, DNS:control-plane.minikube.internal,
DNS:kubernetes.default.svc.cluster.local, DNS:kubernetes.default.svc,
DNS:kubernetes.default, DNS:kubernetes, DNS:localhost, IP Address:10.10.11.133, IP
Address:10.96.0.1, IP Address:127.0.0.1, IP Address:10.0.0.1
| Not valid before: 2024-06-02T10:26:29
|_ Not valid after:  2027-06-03T10:26:29
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 403 Forbidden
|     Audit-Id: 6ec7fd63-e0dc-4be9-97bd-639da822b129
|     Cache-Control: no-cache, private
|     Content-Type: application/json
|     X-Content-Type-Options: nosniff
|     X-Kubernetes-Pf-Flowschema-Uid: 7ee25ed4-1110-4366-8b72-26d0d4a5b3c2
```

```
X-Kubernetes-Pf-Prioritylevel-Uid: 04d99ffe-e3c6-42e1-b353-c90e308ba10c
Date: Mon, 03 Jun 2024 10:29:11 GMT
Content-Length: 212
{"kind":"Status","apiVersion":"v1","metadata":
{"status":"Failure","message":"forbidden: User \"system:anonymous\" cannot get path
\"/nice ports,/Trinity.txt.bak\"","reason":"Forbidden","details":{},"code":403}
GetRequest:
HTTP/1.0 403 Forbidden
Audit-Id: 7dbf7e9d-6ae1-45ab-9118-dd02ba34b609
Cache-Control: no-cache, private
Content-Type: application/json
X-Content-Type-Options: nosniff
X-Kubernetes-Pf-Flowschema-Uid: 7ee25ed4-1110-4366-8b72-26d0d4a5b3c2
X-Kubernetes-Pf-Prioritylevel-Uid: 04d99ffe-e3c6-42e1-b353-c90e308ba10c
Date: Mon, 03 Jun 2024 10:29:09 GMT
Content-Length: 185
{"kind":"Status","apiVersion":"v1","metadata":
{"status":"Failure","message":"forbidden: User \"system:anonymous\" cannot get path
\"/\"","reason":"Forbidden","details":{},"code":403}
HTTPOptions:
HTTP/1.0 403 Forbidden
Audit-Id: ecde9564-176e-4641-ba60-fa00a55202d2
Cache-Control: no-cache, private
Content-Type: application/json
X-Content-Type-Options: nosniff
X-Kubernetes-Pf-Flowschema-Uid: 7ee25ed4-1110-4366-8b72-26d0d4a5b3c2
X-Kubernetes-Pf-Prioritylevel-Uid: 04d99ffe-e3c6-42e1-b353-c90e308ba10c
Date: Mon, 03 Jun 2024 10:29:10 GMT
Content-Length: 189
{"kind":"Status","apiVersion":"v1","metadata":
{"status":"Failure","message":"forbidden: User \"system:anonymous\" cannot options
path \"/\"","reason":"Forbidden","details":{},"code":403}
l_ssl-date: TLS randomness does not represent time
l_http-title: Site doesn't have a title (application/json).
10250/tcp open  ssl/http          Golang net/http server (Go-IPFS json-rpc or InfluxDB
API)
l_tls-alpn:
l  h2
l_ http/1.1
l_ssl-date: TLS randomness does not represent time
l ssl-cert: Subject: commonName=steamcloud@1717410393
l Subject Alternative Name: DNS:steamcloud
l Not valid before: 2024-06-03T09:26:33
```

l\_Not valid after: 2025-06-03T09:26:33

l\_http-title: Site doesn't have a title (text/plain; charset=utf-8).

l service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

SF-Port8443-TCP:V=7.94SVN%T=SSL%I=7%D=6/3%Time=665D9AF5%P=aarch64-unknown-SF:linux-gnu%r(GetRequest,22F,"HTTP/1.0\x20403\x20Forbidden\r\nAudit-Id:\r\nCache-Control:\x20no-cache,\r\nContent-Type:\x20application/json\r\nX-Content-Type-Options:\x20nosniff\r\nX-Kubernetes-Pf-Flowschema-Uid:\x207ee25ed4-1110-4366-8b72-26d0d4a5b3c2\r\nX-Kubernetes-Pf-Prioritylevel-Uid:\x2004d99ffe-e3c6-42e1-b353-c90e308ba10c\r\nDate:\x20Mon,\x2003\x20Jun\x202024\x2010:29:09\x20GMT\r\nContent-Length:\x20185\r\n\r\n{"kind":"Status","apiVersion":"v1","metadata":{"status":"Failure","message":"Forbidden: \x20User \x20""\x20cannot \x20get \x20path \x20""\x20""\x20""\x20","reason":"Forbidden","details":{"code":403}}\n")%r(HTTPOptions,233,"HTTP/1.0\x20403\x20Forbidden\r\nAudit-Id:\x20ecde9564-176e-4641-ba60-fa00a55202d2\r\nCache-Control:\x20no-cache,\x20private\r\nContent-Type:\x20application/json\r\nX-Content-Type-Options:\x20nosniff\r\nX-Kubernetes-Pf-Flowschema-Uid:\x207ee25ed4-1110-4366-8b72-26d0d4a5b3c2\r\nX-Kubernetes-Pf-Prioritylevel-Uid:\x2004d99ffe-e3c6-42e1-b353-c90e308ba10c\r\nDate:\x20Mon,\x2003\x20Jun\x202024\x2010:29:10\x20GMT\r\nContent-Length:\x20189\r\n\r\n{"kind":"Status","apiVersion":"v1","metadata":{"status":"Failure","message":"forbidden: \x20User \x20""\x20cannot \x20options \x20path \x20""\x20""\x20""\x20","reason":"Forbidden","details":{"code":403}}\n")%r(FourOhFourRequest,24A,"HTTP/1.0\x20403\x20Forbidden\r\nAudit-Id:\x206ec7fd63-e0dc-4be9-97bd-639da822b129\r\nCache-Control:\x20no-cache,\x20private\r\nContent-Type:\x20application/json\r\nX-Content-Type-Options:\x20nosniff\r\nX-Kubernetes-Pf-Flowschema-Uid:\x207ee25ed4-1110-4366-8b72-26d0d4a5b3c2\r\nX-Kubernetes-Pf-Prioritylevel-Uid:\x2004d99ffe-e3c6-42e1-b353-c90e308ba10c\r\nDate:\x20Mon,\x2003\x20Jun\x202024\x2010:29:11\x20GMT\r\nContent-Length:\x20212\r\n\r\n{"kind":"Status","apiVersion":"v1","metadata":{"status":"Failure","message":"forbidden: \x20User \x20""\x20cannot \x20get \x20path \x20""\x20""\x20""\x20/nice\x20ports,/Trinity.txt.bak""\x20""\x20","reason":"Forbidden","details":{"code":403}}\n");

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Linux 5.0 (96%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE (using port 22/tcp)

HOP	RTT	ADDRESS
-----	-----	---------

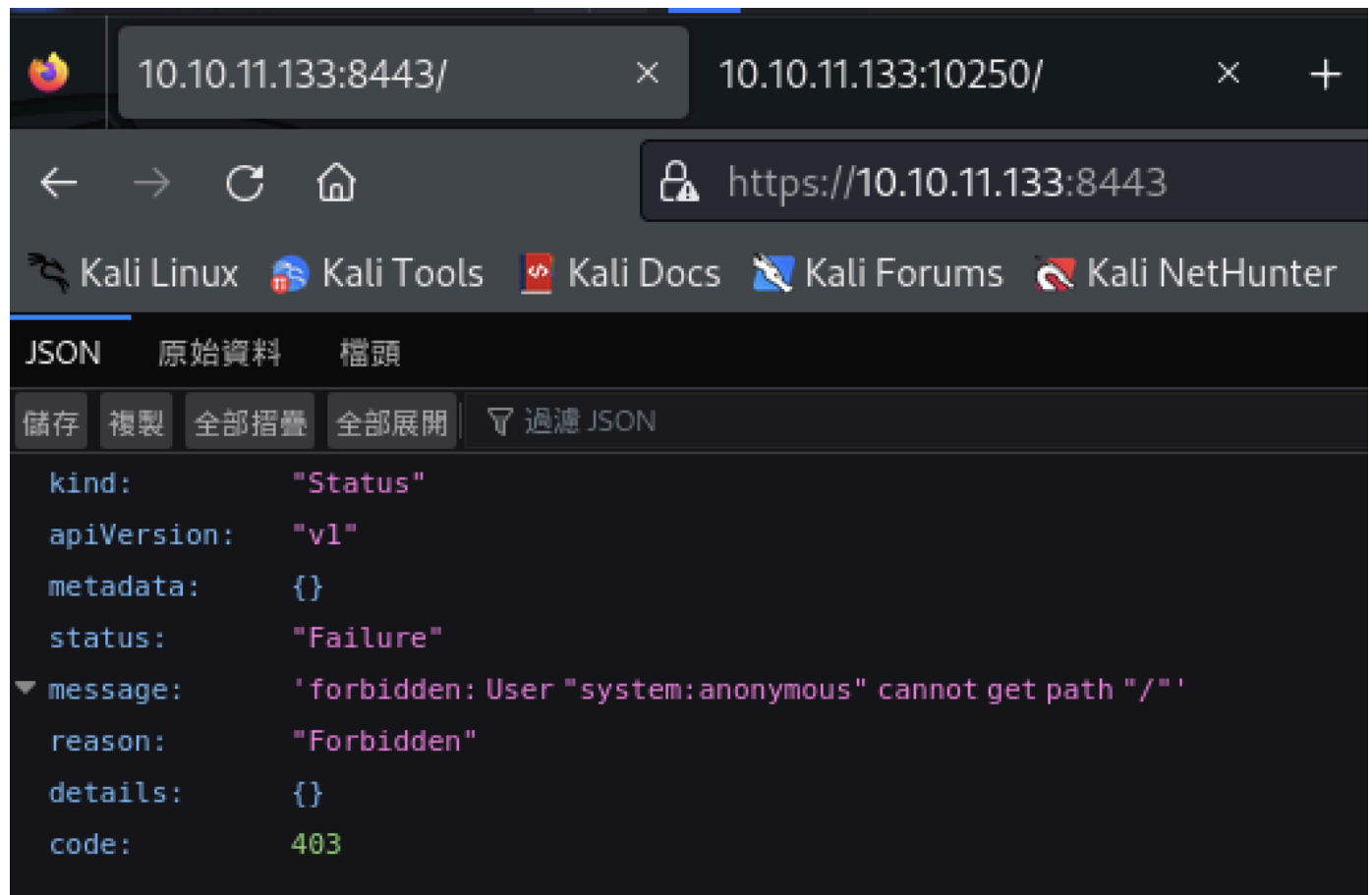
1	282.12 ms	10.10.14.1
---	-----------	------------

2	282.37 ms	10.10.11.133
---	-----------	--------------

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 135.91 seconds

web8443



8443Port憑證(端口掃描的)

ssl-cert: Subject:

commonName=minikube/organizationName=system:masters

Subject Alternative Name:

DNS:minikubeCA,

DNS:control-plane.minikube.internal,

DNS:kubernetes.default.svc.cluster.local,

DNS:kubernetes.default.svc,

DNS:kubernetes.default,

IP Address: 10.0.0.1

工具：<https://github.com/cyberark/kubeletctl>

```
Kali Linux 2023
一次模式

root@kali: ~  

檔案 動作 編輯 檢視 幫助  

root@kali: ~ x root@kali: ~ x root@kali: ~ x  

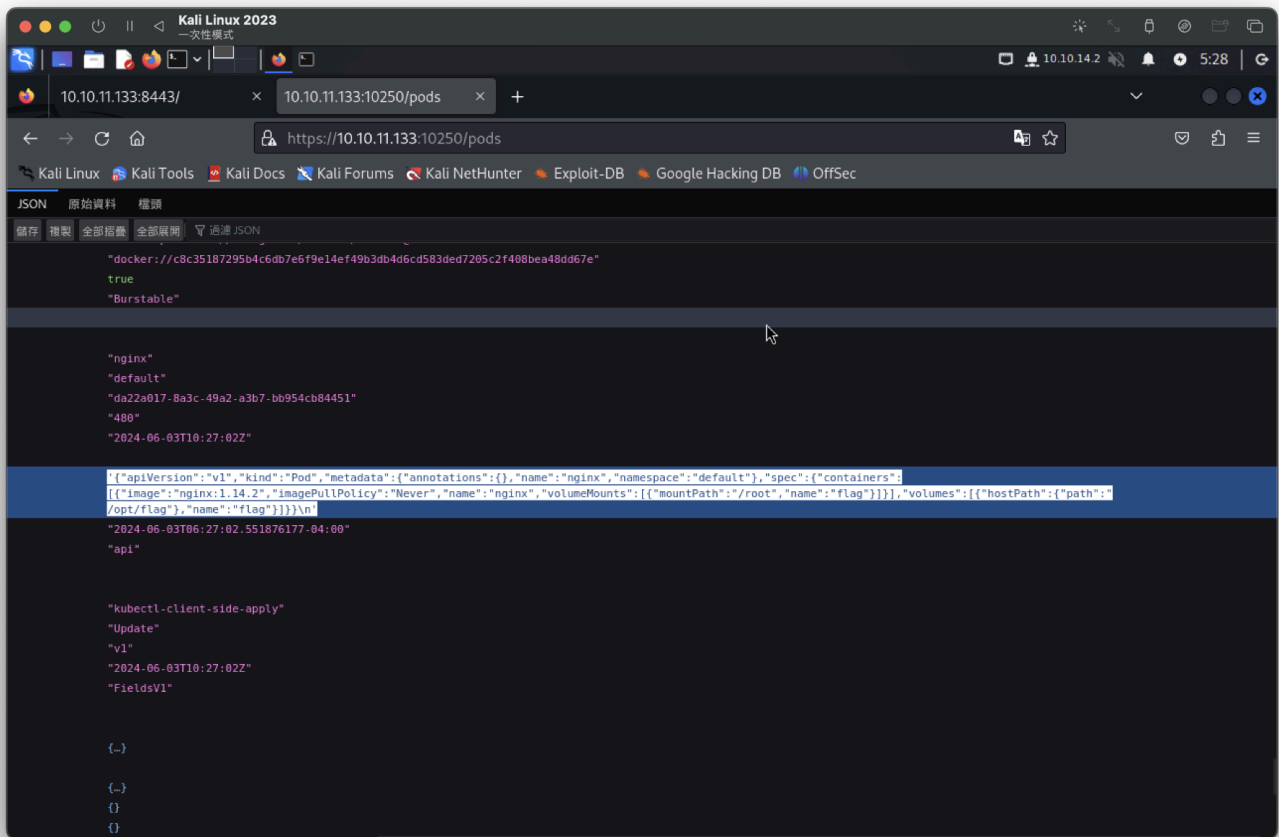
[~]  

curl -k https://10.10.11.133:10250/pods  

{"kind": "PodList", "apiVersion": "v1", "metadata": {}, "items": [{"metadata": {"name": "kube-apivserver-steamcloud", "namespace": "kube-system", "selflink": "/api/v1/namespaces/kube-system/pods/kube-apivserver-steamcloud", "uid": "c1926d0465cd9de10197b95a2c359105", "creationTimestamp": null, "labels": {"component": "kube-apivserver", "tier": "control-plane"}, "annotations": {"kubernetes.io/kube-apivserver.advertise-address.endpoint": "10.10.11.133:8443", "kubernetes.io/config.hash": "c1926d0465cd9de10197b95a2c359105", "kubernetes.io/config.seen": "2024-06-03T06:26:49.142961385-04:00", "kubernetes.io/config.source": "file", "spec": {"volumes": [{"name": "ca-certs", "hostPath": {"path": "/etc/ssl/certs", "type": "DirectoryOrCreate"}, {"name": "etc-ca-certificates", "hostPath": {"path": "/etc/ca-certificates", "type": "DirectoryOrCreate"}, {"name": "k8s-certs", "hostPath": {"path": "/var/lib/minikube/certs", "type": "DirectoryOrCreate"}, {"name": "usr-share-ca-certificates", "hostPath": {"path": "/usr-local/share/ca-certificates", "type": "DirectoryOrCreate"}, {"name": "usr-local-share-ca-certificates", "hostPath": {"path": "/usr/share/ca-certificates", "type": "DirectoryOrCreate"}]}, "containers": [{"name": "kube-apivserver", "image": "k8s.gcr.io/kube-apivserver:v1.22.3", "command": ["kube-apivserver", "-advertise-address=10.10.11.133"], "--allow-privileged=true", "--authorization-mode=Node,RBAC", "--client-ca-file=/var/lib/minikube/certs/ca.crt", "--enable-admission-plugins=NamespaceLifecycle,LimitRanger,ServiceAccount,DefaultStorageClass,DefaultTolerationSeconds,NodeRestriction,MutatingAdmissionWebhook,ValidatingAdmissionWebhook,ResourceQuota", "--enable-bootstrap-token-auth=true", "--etcd-cafile=/var/lib/minikube/certs/etcd/ca.crt", "--etcd-certfile=/var/lib/minikube/certs/apivserver-etcd-client.crt", "--etcd-keyfile=/var/lib/minikube/certs/apivserver-etcd-client.key", "--etcd-servers=https://127.0.0.1:2379", "--kubelabel-preferred-address-types=InternalIP,ExternalIP,Hostname", "--proxy-client-cert-file=/var/lib/minikube/certs/front-proxy-client.crt", "--proxy-client-key=/var/lib/minikube/certs/front-proxy-client.key", "--requestheader-allowed-names=front-proxy-client", "--requestheader-client-ca-file=/var/lib/minikube/certs/front-proxy-ca.crt", "--requestheader-extra-headers-prefix=X-Remote-Extra", "--requestheader-group-headers=X-Remote-Group", "--requestheader-username-headers=X-Remote-User", "--secure-port=8443", "--service-account-issuer=https://kubernetes.default.svc.cluster.local", "--service-account-key-file=/var/lib/minikube/certs/ca.pub", "--service-account-signing-key-file=/var/lib/minikube/certs/sa.key", "--service-cluster-ip-range=10.0.0.0/24", "--tls-cert-file=/var/lib/minikube/certs/apivserver.crt", "--tls-private-key-file=/var/lib/minikube/certs/apivserver.key", "--resources":{"requests":{"cpu":"250m"},"volumeMounts":[{"name": "ca-certs", "readOnly": true, "mountPath": "/etc/ssl/certs"}, {"name": "etc-ca-certificates", "readOnly": true, "mountPath": "/etc/ca-certificates"}, {"name": "k8s-certs", "readOnly": true, "mountPath": "/var/lib/minikube/certs"}, {"name": "usr-local-share-ca-certificates", "readOnly": true, "mountPath": "/usr/local/share/ca-certificates"}, {"name": "usr-share-ca-certificates", "readOnly": true, "mountPath": "/usr/share/ca-certificates"}, {"name": "livenessProbe": {"httpGet": {"path": "/livez", "port": 8443}, "host": "10.10.11.133", "scheme": "HTTPS"}, "initialDelaySeconds": 10, "periodSeconds": 10, "successThreshold": 1, "failureThreshold": 3}, {"name": "readinessProbe": {"httpGet": {"path": "/readyz", "port": 8443}, "host": "10.10.11.133", "scheme": "HTTPS"}, "timeoutSeconds": 15, "periodSeconds": 15, "successThreshold": 1, "failureThreshold": 3}, {"startUpProbe": {"httpGet": {"path": "/livez", "port": 8443}, "host": "10.10.11.133", "scheme": "HTTPS"}, "initialDelaySeconds": 10, "timeoutSeconds": 15, "periodSeconds": 10, "successThreshold": 1, "failureThreshold": 24}, "terminationMessagePath": "/dev/termination-log", "terminationMessagePolicy": "File", "imagePullPolicy": "IfNotPresent"}, "restartPolicy": "Always", "terminationGracePeriodSeconds": 30, "dnsPolicy": "ClusterFirst", "nodeName": "steamcloud", "hostNetwork": true, "securityContext": {"seccompProfile": {"type": "RuntimeDefault"}, "schedulerName": "default-scheduler", "tolerations": [{"operator": "Exists", "effect": "NoExecute", "priorityClassName": "system-node-critical", "enableServiceLinks": true}], "status": {"phase": "Running", "conditions": [{"type": "Initialized", "status": "True", "lastProbeTime": null, "lastTransitionTime": "2024-06-03T10:26:46Z"}, {"type": "Ready", "status": "True", "lastProbeTime": null, "lastTransitionTime": "2024-06-03T10:26:54Z"}, {"type": "ContainersReady", "status": "True", "lastProbeTime": null, "lastTransitionTime": "2024-06-03T10:26:54Z"}, {"type": "PodsScheduled", "status": "True", "lastProbeTime": null, "lastTransitionTime": "2024-06-03T10:26:46Z"}, {"type": "HostIP": "10.10.11.133", "podIP": "10.10.11.133", "podIPs": [{"ip": "10.10.11.133"}, {"start": "2024-06-03T10:26:46Z", "containerStatuses": [{"name": "kube-apivserver", "state": "running", "startedAt": "2024-06-03T10:26:35Z", "lastState": {"type": "Ready", "reason": "RestartContainer", "message": "K8s.gcr.io/kube-apivserver:v1.22.3", "imageID": "docker-pullable://k8s.gcr.io/kube-apivserver:sha256:6eefc59ec1f570e7958e267a699388ea2248beb70dd9de7afb21e862e9d", "containerID": "docker://61dc5c37a1cb9406a437059ec83ee5fb061fd8694a5c1bd467aab03766c65", "started": true}], qosClass": "Burstable"}], "metadata": {"name": "kube-controller-manager-steamcloud", "namespace": "kube-system", "selflink": "/api/v1/namespaces/kube-system/pods/kube-controller-manager-steamcloud", "uid": "be2478237d1af44b62acbf157f9c4", "creationTimestamp": null, "labels": {"component": "kube-controller-manager", "tier": "control-plane"}, "annotations": {"kubernetes.io/config.hash": "be2478237d1af44b62acbf157f9c4", "kubernetes.io/config.seen": "2024-06-03T06:26:49.142962638-04:00", "kubernetes.io/c
```

太亂了，工具也要弄一堆東西放棄，

用web手動查找，找到有關root字眼



name : `nginx`

但需要工具才能反彈。。。。

工具弄不好