

# في Kubernetes عداهش ةي حالص ءاهتنا رود ةومجملل عساوولا لاصتالافقوت

## تاوت حملال

[ةمدقملا](#)

[ةلكشمللا](#)

[لحللا](#)

## ةمدقملا

ماظن مهيدل نوكي امدنع ءالمعال اههجاوي دق ةلمتحم عاطقنا ةلكشم دنتسمللا اذه فصوي تاوطخلاب رمي هنإف، كلذىل ءوالع. اموي 365 نم رثكال هتيبثت مت Kubernetes لىل ءاق ستيانربوك ءءاق لىل ءاقلا ماطنلا نم ةيطايحتا ءسن لمعو فوقوملا حالصال ءمزاللا.

## ةلكشمللا

ةي حالص يهتنت، Kubernetes cluster ماطن لىل تبثمللا يضارتفالا تقولا نم ءنس رورم دعب نم مغللا لىل. Cisco CloudCentre (CCS) ءومجمللا لوصوللا نم نكمتت نل. لىل ءاداهش رطس ءهجاو لىل تلقنتنا اذا. لوخدلا لىل جست نم نكمتت نل، ءشاشلا لىل رهظت لظتس اهنأ وءءاهشلا ءي حالص تهتنا: x509: مءاخلاب لاصتالافقوت، أطلالا اذه لىل رتس، Kubectll رماو أءعب ءحلل اص دعت مل.

مهءاداهش ءي حالص ءاهتنا ءي رتلا لىل ساساللا لىل صنلا ءمانربلا اذه لىل ءشنت كنكمي:

```
for crt in /etc/kubernetes/pki/*.crt; do
    printf '%s: %s\n' \
        "$(date --date="$(openssl x509 -enddate -noout -in "$crt"|cut -d= -f 2)" --iso-8601)" \
        "$crt"
done | sort
```

ةبقارمب موقيس لىل Action Orchestrator ل OpenSource لمع ريس لىل روثعلا اضيا كنكمي. تاللكشمللاب مههبيبتو ايموي اذه.

[https://github.com/cisco-cx-workflows/cx-ao-shared-workflows/tree/master/CCSCheckKubernetesExpiration\\_definition\\_workflow\\_01E01VIRWZDE24mWlsHrqCGB9xUix0f9ZxG](https://github.com/cisco-cx-workflows/cx-ao-shared-workflows/tree/master/CCSCheckKubernetesExpiration_definition_workflow_01E01VIRWZDE24mWlsHrqCGB9xUix0f9ZxG)

## لحللا

مض ءءاعا بءي مثنمو، ءومجمللا ماطن ربك Kubeadm ربك ءءءاللا ءاداهشلا رادصا ءءاعا بءي تاللساسالا لىل لمال دق.

1. ءيسئر ءءق لىل لوخدلا لىل جستب مق.
2. IP نىوانع ضرع ربك هب صاخاللا IP ناوانع لىل لصحا.

```
[root@cx-ccs-prod-master-d7f34f25-f524-4f90-9037-7286202ed13a3 kubernetes]# ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 8920 qdisc pfifo_fast state UP group default
qlen 1000
link/ether fa:16:3e:19:63:a2 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.20/24 brd 192.168.1.255 scope global dynamic eth0
valid_lft 37806sec preferred_lft 37806sec
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group
default
link/ether 02:42:d0:29:ce:5e brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 scope global docker0
valid_lft forever preferred_lft forever
13: tunl0@NONE: <NOARP,UP,LOWER_UP> mtu 1430 qdisc noqueue state UNKNOWN group default qlen
1000
link/ipip 0.0.0.0 brd 0.0.0.0
inet 172.16.176.128/32 brd 172.16.176.128 scope global tunl0
valid_lft forever preferred_lft forever
14: cali65453a0219d@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1430 qdisc noqueue state UP
group default
link/ether ee:ee:ee:ee:ee:ee brd ff:ff:ff:ff:ff:ff link-netnsid 4
```

3. **طوغض الما صرق ل ربح Kubernetes ليلد لى ل لقتنا .**

4. **ربح kubeadmCERT.yaml ربح vi kubeadmCERT.yaml.**

5. **يلى امك فللما ودبي نأ بحجى:**

```
apiVersion: kubeadm.k8s.io/v1alpha1
kind: MasterConfiguration
api:
  advertiseAddress: <IP ADDRESS FROM STEP 2>
kubernetesVersion: v1.11.6
#NOTE: If the customer is running a load balancer VM then you must add these lines after...
#apiServerCertSANS:
#- <load balancer IP>
```

6. **ىصوي نكلو بولطم ريغ اذهو .ةمي دقل احيات افلملاو تاداهش لل يطايتح ا خسن عارجاب مق .هه لى ل ا تافلملا هذو خسنو يطايتح ا خسن لى ل د عاشنا .ه**

```
#Files
#apiserver.crt
#apiserver.key
#apiserver-kubelet-client.crt
#apiserver-kubelet-client.key
#front-proxy-client.crt
#front-proxy-client.key

#ie
cd /etc/kubernetes/pki
mkdir backup
mv apiserver.key backup/apiserver.key.bak
```

7. **لثم rm رمأ ربع ةق باسلا تافلملا فذح طقف كنكمي .، 6 ةوطخال ي طختب تمق اذا .**  
**apiserver.crt.**

8. ةديج ليحرت ةداهش عاشنإب مق `kubeadmCERT.yaml` فلم دجوي شح فلخال لىل لقتنا رب `Kubeadm —config kubeadmCERT.yaml alpha phase apiserver`.

```
[root@cx-ccs-prod-master-d7f34f25-f524-4f90-9037-7286202ed13a3 kubernetes]# kubeadm --
config kubeadmCERT.yaml alpha phase certs apiserver
[certificates] Generated apiserver certificate and key.
[certificates] apiserver serving cert is signed for DNS names [cx-ccs-prod-master-d7f34f25-
f524-4f90-9037-7286202ed13a3 kubernetes kubernetes.default kubernetes.default.svc
kubernetes.default.svc.cluster.local] and IPs [10.96.0.1 192.168.1.20]
```

9. ربع ةديج تانايب ةدعاق ةداهش عاشنإب مق `kubeadm —config kubeadmCERT.yaml alpha phase apiserver-kubelet-client`.

10. ربع ةديج يمامألليكووليمع ةداهش عاشنإب مق `kubeadm —config kubeadmCERT.yaml proxy-client` لىل لقتنا افأل.

11. هب صوم نكلو بولطم ريغ. دربم `.conf`. ةيطايحتإ ةخسن، `/etc/kubernetes/` دلجم يي `kubelet.conf`، `controller-manager.conf`، `scheduler.conf`، امبرو `admin.conf` اي طايحتإ اهخسن يي بغيرت مل اذا اهفدح كنكمي.

12. ربع ةديج نيوكت تافلما عاشنإب مق `kubeadm —config kubeadmCERT.yaml alpha phase kubeconfig all`.

```
[root@cx-ccs-prod-master-d7f34f25-f524-4f90-9037-7286202ed13a3 kubernetes]# kubeadm --
config kubeadmCERT.yaml alpha phase kubeconfig all
[kubeconfig] Wrote KubeConfig file to disk: "/etc/kubernetes/admin.conf"
[kubeconfig] Wrote KubeConfig file to disk: "/etc/kubernetes/kubelet.conf"
[kubeconfig] Wrote KubeConfig file to disk: "/etc/kubernetes/controller-manager.conf"
[kubeconfig] Wrote KubeConfig file to disk: "/etc/kubernetes/scheduler.conf"
```

13. فيضمال لىل ديجال `admin.conf` فلم ريصدت.

```
cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
chown $(id -u):$(id -g) $HOME/.kube/config
chmod 777 $HOME/.kube/config
export KUBECONFIG=.kube/config
```

14. نأل `-r` ليغشتلا فاق يي ربع ةيسيسيئرلا ةدقعال ديهمت دعأ.

15. ةلاح `Kubelet` لالخنم لمعي `Kubelet` ناك اذا امم ققحت، ريذملل ييطايحتال خسنال درجمب `Kubelet` ماطنلا.

16. دقعال لىل لصحا `Kubectl` ربع `Kubernetes` نم ققحت.

```
[root@cx-ccs-prod-master-d7f34f25-f524-4f90-9037-7286202ed13a3 ~]# kubectl get nodes
NAME                                     STATUS    ROLES    AGE
VERSION
cx-ccs-prod-master-d7f34f25-f524-4f90-9037-7286202ed13a1 Ready     master   1y
v1.11.6
cx-ccs-prod-master-d7f34f25-f524-4f90-9037-7286202ed13a2 Ready     master   1y
v1.11.6
cx-ccs-prod-master-d7f34f25-f524-4f90-9037-7286202ed13a3 Ready     master   1y
v1.11.6
```

|   |          |        |    |
|---|----------|--------|----|
| cx-ccs-prod-worker-d7f34f25-f524-4f90-9037-7286202ed13a1<br>v1.11.6 | NotReady | <none> | 1y |
| cx-ccs-prod-worker-d7f34f25-f524-4f90-9037-7286202ed13a2<br>v1.11.6 | NotReady | <none> | 1y |
| cx-ccs-prod-worker-d7f34f25-f524-4f90-9037-7286202ed13a3<br>v1.11.6 | NotReady | <none> | 1y |
| cx-ccs-prod-worker-d7f34f25-f524-4f90-9037-7286202ed13a4<br>v1.11.6 | NotReady | <none> | 1y |
| cx-ccs-prod-worker-d7f34f25-f524-4f90-9037-7286202ed13a5<br>v1.11.6 | NotReady | <none> | 1y |
| cx-ccs-prod-worker-d7f34f25-f524-4f90-9037-7286202ed13a6<br>v1.11.6 | NotReady | <none> | 1y |

17. ةيساسأ ةدقع لك ل 16 لى 1 نم تاوطخلال ررك .

18. ل زيمم زمر ءاشن لال خ نم مامضنلال دي دج زيمم زمر ءاشن اب مق ، دحاو يساسأ لى ع .  
Kubeadm — join-ةعاب ط رما اذخ ال مادختس الال رمالا اذخ سنا .

```
[root@cx-ccs-prod-master-d7f34f25-f524-4f90-9037-7286202ed13a1 k8s-mgmt]# kubeadm token
create
--print-join-command kubeadm join 192.168.1.14:6443 --token mlynvj.f4n3et3poki88ry4
--discovery-token-ca-cert-hash
sha256:4d0c569985c1d460ef74dc01c85740285e4af2c2369ff833eed1ba86e1167575
```

19. - دقعل لى ع لصلحاو Kubectl لال خ نم لك يدل ني لماع اب ةصاخ ال IP ني وانع لى ع لصلحا .  
ةضيرع ةحاسم لى ع .

20. ي رذجل لوصول لى ع لى ح فصت و user@192.168.1.17 ssh -i /home/cloud-user/keys/gen3-ao-prod.key cloud-  
user@192.168.1.17 لى ح فصت ب مق .

21. SystemCtl stop kubelet. ربع Kubelet ةمدخ فاقى اب مق .

22. bootstrap-kubelet.conf، و kubelet.conf، و ca.crt نمضتت يتلاو ، ةم يدق لال ني وك تلاتا فلم ةلازاب مق .  
kubelet.conf.

```
rm /etc/kubernetes/pki/ca.crt
rm /etc/kubernetes/kubelet.conf
rm /etc/kubernetes/bootstrap-kubelet.conf
```

23. 19 ةوطخلال نم ةدقعلال مسا لى ع لوصولال .

24. 18 نم رمالا مدختسأ . ةومجم لال ماطن لى ع لى مامضنلالا ةداع لى لماع لى رمالا رادص اب مق .  
node-name <name of node>—فصأ ةياهنلال لى ع لى لى .

```
[root@cx-ccs-prod-worker-d7f34f25-f524-4f90-9037-7286202ed13a1 kubernetes]# kubeadm join
192.168.1.14:6443 --token mlynvj.f4n3et3poki88ry4 --discovery-token-ca-cert-hash
sha256:4d0c569985c1d460ef74dc01c85740285e4af2c2369ff833eed1ba86e1167575 --node-name cx-
ccs-prod-worker-d7f34f25-f524-4f90-9037-7286202ed13a1
[preflight] running pre-flight checks
[WARNING RequiredIPVSKernelModulesAvailable]: the IPVS proxier will not be used,
because the following required kernel modules are not loaded: [ip_vs_rr ip_vs_wrr
ip_vs_sh] or no builtin kernel ipvs support: map[ip_vs:{}] ip_vs_rr:{}] ip_vs_wrr:{}]
ip_vs_sh:{}] nf_conntrack_ipv4:{}]
```

you can solve this problem with following methods:

1. Run 'modprobe -- ' to load missing kernel modules;
2. Provide the missing builtin kernel ipvs support

```
I0226 17:59:52.644282 19170 kernel_validator.go:81] Validating kernel version
I0226 17:59:52.644421 19170 kernel_validator.go:96] Validating kernel config
[discovery] Trying to connect to API Server "192.168.1.14:6443"
[discovery] Created cluster-info discovery client, requesting info from
"https://192.168.1.14:6443"
[discovery] Requesting info from "https://192.168.1.14:6443" again to validate TLS against
the pinned public key
[discovery] Cluster info signature and contents are valid and TLS certificate validates
against pinned roots, will use API Server "192.168.1.14:6443"
[discovery] Successfully established connection with API Server "192.168.1.14:6443"
[kubelet] Downloading configuration for the kubelet from the "kubelet-config-1.11"
ConfigMap in the kube-system namespace
[kubelet] Writing kubelet configuration to file "/var/lib/kubelet/config.yaml"
[kubelet] Writing kubelet environment file with flags to file "/var/lib/kubelet/kubeadm-
flags.env"
[preflight] Activating the kubelet service
[tlsbootstrap] Waiting for the kubelet to perform the TLS Bootstrap...
[patchnode] Uploading the CRI Socket information "/var/run/dockershim.sock" to the Node
API object "cx-ccs-prod-worker-d7f34f25-f524-4f90-9037-7286202ed13a1" as an annotation
```

This node has joined the cluster:

- \* Certificate signing request was sent to master and a response was received.
- \* The Kubelet was informed of the new secure connection details.

Run 'kubectl get nodes' on the master to see this node join the cluster.

25. دقعلال دلل لوصحلل Kubectl ربع ريدم دلل ةلحال نم ققحتو لماعال نم جورخلاب مق .  
"زهاج" ةلاح يف نوكي نأ بجي .

26. لماع لكل 25. دلل 20 نم تاوطخلال ررك .

27. دلل مضمنت مث ، تنرتنإلا دلل دوعت مث ، "زهاج" ةلاح يف ةريخألا دقعلال رهظت نأ بجي .  
ةوعومجمال ماظن .

```
[root@cx-ccs-prod-master-d7f34f25-f524-4f90-9037-7286202ed13a1 ~]# kubectl get nodes
NAME                                     STATUS    ROLES    AGE
VERSION
cx-ccs-prod-master-d7f34f25-f524-4f90-9037-7286202ed13a1  Ready    master   1y
v1.11.6
cx-ccs-prod-master-d7f34f25-f524-4f90-9037-7286202ed13a2  Ready    master   1y
v1.11.6
cx-ccs-prod-master-d7f34f25-f524-4f90-9037-7286202ed13a3  Ready    master   1y
v1.11.6
cx-ccs-prod-worker-d7f34f25-f524-4f90-9037-7286202ed13a1  Ready    <none>   1y
v1.11.6
cx-ccs-prod-worker-d7f34f25-f524-4f90-9037-7286202ed13a2  Ready    <none>   1y
v1.11.6
cx-ccs-prod-worker-d7f34f25-f524-4f90-9037-7286202ed13a3  Ready    <none>   1y
v1.11.6
cx-ccs-prod-worker-d7f34f25-f524-4f90-9037-7286202ed13a4  Ready    <none>   1y
v1.11.6
cx-ccs-prod-worker-d7f34f25-f524-4f90-9037-7286202ed13a5  Ready    <none>   1y
v1.11.6
cx-ccs-prod-worker-d7f34f25-f524-4f90-9037-7286202ed13a6  Ready    <none>   1y
v1.11.6
```

v1.11.6

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل