We have generated all of the the client certificates our Kubernetes cluster will need, but we also need a server certificate for the Kubernetes API. In this lesson, we will generate one, signed with all of the hostnames and IPs that may be used later in order to access the Kubernetes API. After completing this lesson, you will have a Kubernetes API server certificate in the form of two files called `kubernetes-key.pem` and `kubernetes.pem`.

Here are the commands used in the demo. Be sure to replace all the placeholder values in CERT_HOSTNAME with their real values from your cloud servers:

```
cd ~/kthw

CERT_HOSTNAME=10.32.0.1,<controller node 1 Private IP>,<controller node 1 hostname>,<controller node 2
Private IP>,<controller node 2 hostname>,<API load balancer Private IP>,<API load balancer
hostname>,127.0.0.1,localhost,kubernetes.default

{

cat > kubernetes-csr.json << EOF
{


  "CN": "kubernetes",
  "key": {
    "algo": "rsa",
    "size": 2048
  },
  "names": [
    {
      "C": "US",
      "L": "Portland",
      "O": "Kubernetes",
      "OU": "Kubernetes The Hard Way",
      "ST": "Oregon"
    }
  ]
}
EOF

cfssl gencert \
  -ca=ca.pem \
  -ca-key=ca-key.pem \
  -config=ca-config.json \
  -hostname=${CERT_HOSTNAME} \
  -profile=kubernetes \
  kubernetes-csr.json | cfssljson -bare kubernetes

}
```