tags: kubectl

03. 安装和配置 kubectl

本文档介绍安装和配置 kubernetes 命令行管理工具 kubectl 的步骤。

注意：

1. 如果没有特殊指明，本文档的所有操作均在 **zhangjun-k8s-01** 节点上执行；
2. 本文档只需要部署一次，生成的 kubeconfig 文件是通用的，可以拷贝到需要执行 kubectl 命令的机器的 `~/.kube/config` 位置；

下载和分发 kubectl 二进制文件

```
cd /opt/k8s/work
wget https://dl.k8s.io/v1.16.6/kubernetes-client-linux-amd64.tar.gz # 自行解决翻墙下载问题
tar -xzvf kubernetes-client-linux-amd64.tar.gz
```

分发到所有使用 kubectl 工具的节点：

```
cd /opt/k8s/work
source /opt/k8s/bin/environment.sh
for node_ip in ${NODE_IPS[@]}
  do
    echo ">>> ${node_ip}"
    scp kubernetes/client/bin/kubectl root@${node_ip}:/opt/k8s/bin/
    ssh root@${node_ip} "chmod +x /opt/k8s/bin/*"
  done
```

创建 admin 证书和私钥

kubectl 使用 https 协议与 kube-apiserver 进行安全通信，kube-apiserver 对 kubectl 请求包含的证书进行认证和授权。

kubectl 后续用于集群管理，所以这里创建具有最高权限的 admin 证书。

创建证书签名请求：

```
cd /opt/k8s/work
cat > admin-csr.json <<EOF
{
  "CN": "admin",
  "hosts": [],
  "key": {
    "algo": "rsa",
    "size": 2048
  },
  "names": [
    {
      "C": "CN",
      "ST": "BeiJing",
      "L": "BeiJing",
      "O": "system:masters",
      "OU": "opsnull"
    }
  ]
}
EOF
```

- `O: system:masters`：kube-apiserver 收到使用该证书的客户端请求后，为请求添加组（Group）认证标识 `system:masters`；
- 预定义的 ClusterRoleBinding `cluster-admin` 将 Group `system:masters` 与 Role `cluster-admin` 绑定，该 Role 授予操作集群所需的最高权限；
- 该证书只会被 kubectl 当做 client 证书使用，所以 `hosts` 字段为空；

生成证书和私钥：

```
cd /opt/k8s/work
cfssl gencert -ca=/opt/k8s/work/ca.pem \
  -ca-key=/opt/k8s/work/ca-key.pem \
  -config=/opt/k8s/work/ca-config.json \
  -profile=kubernetes admin-csr.json | cfssljson -bare admin
ls admin*
```

- 忽略警告消息 `[WARNING] This certificate lacks a "hosts" field.`；

创建 kubeconfig 文件

kubectl 使用 kubeconfig 文件访问 apiserver，该文件包含 kube-apiserver 的地址和认证信息（CA 证书和客户端证书）：

```
cd /opt/k8s/work
source /opt/k8s/bin/environment.sh

# 设置集群参数
kubectl config set-cluster kubernetes \
  --certificate-authority=/opt/k8s/work/ca.pem \
  --embed-certs=true \
  --server=https://${NODE_IPS[0]}:6443 \
  --kubeconfig=kubectl.kubeconfig

# 设置客户端认证参数
kubectl config set-credentials admin \
  --client-certificate=/opt/k8s/work/admin.pem \
  --client-key=/opt/k8s/work/admin-key.pem \
  --embed-certs=true \
  --kubeconfig=kubectl.kubeconfig

# 设置上下文参数
kubectl config set-context kubernetes \
  --cluster=kubernetes \
  --user=admin \
  --kubeconfig=kubectl.kubeconfig

# 设置默认上下文
kubectl config use-context kubernetes --kubeconfig=kubectl.kubeconfig
```

- `--certificate-authority`：验证 kube-apiserver 证书的根证书；
- `--client-certificate`、`--client-key`：刚生成的 `admin` 证书和私钥，与 kube-apiserver https 通信时使用；
- `--embed-certs=true`：将 ca.pem 和 admin.pem 证书内容嵌入到生成的 kubectl.kubeconfig 文件中(否则，写入的是证书文件路径，后续拷贝 kubeconfig 到其它机器时，还需要单独拷贝证书文件，不方便。)；
- `--server`：指定 kube-apiserver 的地址，这里指向第一个节点上的服务；

分发 kubeconfig 文件

分发到所有使用 `kubectl` 命令的节点：

```
cd /opt/k8s/work
source /opt/k8s/bin/environment.sh
for node_ip in ${NODE_IPS[@]}
  do
    echo ">>> ${node_ip}"
    ssh root@${node_ip} "mkdir -p ~/.kube"
    scp kubectl.kubeconfig root@${node_ip}:~/.kube/config
  done
```