**K8s etcd集群部署**

集群内各节点部署前，需要按照k8s集群部署要求进行检查。

1. 需下载安装初始化工具。

net-tools vim wget lrzsz git cfssl etcdctl etcd

1. 关闭防火墙、selinx。
2. 优化内核。
3. 保证网络正常通讯。
4. 保证网卡、路由配置正确。
5. 保证时区和时间同步正常。
6. 保证操作系统版本符合要求。
7. 保证各个服务器主机文件配置主机名。
8. 保证ssh设置免密互通（k8s集群内所有主机设置免密）。
9. etcd节点选择算法说明。

所采用Raft的保证分布式系统强一致性的算法。由于要做节点选举，所以节点选择单数节点，通常选择3个节点，如果要增加，每次增加两个节点。

1. 服务器的相关节点部署。

|  |  |  |
| --- | --- | --- |
| Ip地址 | 用途 | 备注 |
| 10.129.55.65 | 主节点 | 以65为例，其他节点复制65的生成证书和二进制文件 |
| 10.129.55.61 | 节点 |  |
| 10.129.55.155 | 节点 |  |

1. 主节点10.129.55.65的相关操作步骤。

1.创建文件ca请求文件。

etcd-root-ca-csr.json

{

"key": {

"algo": "rsa",

"size": 4096

},

"names": [

{

"O": "etcd",

"OU": "etcd Security",

"L": "Beijing",

"ST": "Beijing",

"C": "CN"

}

],

"CN": "etcd-root-ca"

}

1. 依据生成证书文件。

1）依据k8s-root-ca-csr.json文件生成证书。

cfssl gencert --initca=true k8s-root-ca-csr.json | cfssljson --bare k8s-root-ca

生成证书名字如下：

etcd-root-ca.csr

etcd-root-ca.pem

etcd-root-ca-key.pem

1. 依据etcd-gencert.json、etcd-csr.json和之前生成的CA证书文件etcd-root-ca.pem、etcd-root-ca-key.pem共同生成etcd的证书。

cfssl gencert --ca /root/k8s/etcd/ssl/etcd-root-ca.pem --ca-key

/root/k8s/etcd/ssl/etcd-root-ca-key.pem --config /root/k8s/etcd/ssl/etcd-gencert.json --profile kubernetes /root/k8s/etcd/ssl/etcd-csr.json | cfssljson --bare etcd

生成证书名字如下：

etcd.csr

etcd.pem

etcd-key.pem

1. 修改etcd启动文件，根据etcd所在的服务器节点不同修改三个服务器的启动文件。

ETCD\_NAME：节点名称，集群中唯一

ETCD\_DATA\_DIR：数据目录

ETCD\_LISTEN\_PEER\_URLS：集群通信监听地址

ETCD\_LISTEN\_CLIENT\_URLS：客户端访问监听地址

ETCD\_INITIAL\_ADVERTISE\_PEER\_URLS：集群通告地址

ETCD\_ADVERTISE\_CLIENT\_URLS：客户端通告地址

ETCD\_INITIAL\_CLUSTER：集群节点地址

ETCD\_INITIAL\_CLUSTER\_TOKEN：集群 Token

ETCD\_INITIAL\_CLUSTER\_STATE：加入集群的当前状态，new 是新集群，existing 表示加入已有集群

例如etcd.conf的样例文件，以服务器10.129.55.61为例：

# [member]

ETCD\_NAME=etcd1

ETCD\_DATA\_DIR="/var/lib/etcd/etcd1.etcd"

ETCD\_WAL\_DIR="/var/lib/etcd/wal"

ETCD\_SNAPSHOT\_COUNT="100"

ETCD\_HEARTBEAT\_INTERVAL="100"

ETCD\_ELECTION\_TIMEOUT="1000"

ETCD\_LISTEN\_PEER\_URLS="https://10.129.55.61:2380"

ETCD\_LISTEN\_CLIENT\_URLS="https://10.129.55.61:2379,http://127.0.0.1:2379"

ETCD\_MAX\_SNAPSHOTS="5"

ETCD\_MAX\_WALS="5"

#ETCD\_CORS=""

# [cluster]

ETCD\_INITIAL\_ADVERTISE\_PEER\_URLS="https://10.129.55.61:2380"

# if you use different ETCD\_NAME (e.g. test), set ETCD\_INITIAL\_CLUSTER value for this name, i.e. "test=http://..."

ETCD\_INITIAL\_CLUSTER="etcd1=https://10.129.55.61:2380,etcd2=https://10.129.55.65:2380,etcd3=https://10.129.55.155:2380"

ETCD\_INITIAL\_CLUSTER\_STATE="new"

ETCD\_INITIAL\_CLUSTER\_TOKEN="etcd-cluster"

ETCD\_ADVERTISE\_CLIENT\_URLS="https://10.129.55.61:2379"

#ETCD\_DISCOVERY=""

#ETCD\_DISCOVERY\_SRV=""

#ETCD\_DISCOVERY\_FALLBACK="proxy"

#ETCD\_DISCOVERY\_PROXY=""

#ETCD\_STRICT\_RECONFIG\_CHECK="false"

#ETCD\_AUTO\_COMPACTION\_RETENTION="0"

# [proxy]

#ETCD\_PROXY="off"

#ETCD\_PROXY\_FAILURE\_WAIT="5000"

#ETCD\_PROXY\_REFRESH\_INTERVAL="30000"

#ETCD\_PROXY\_DIAL\_TIMEOUT="1000"

#ETCD\_PROXY\_WRITE\_TIMEOUT="5000"

#ETCD\_PROXY\_READ\_TIMEOUT="0"

# [security]

ETCD\_CERT\_FILE="/etc/etcd/ssl/etcd.pem"

ETCD\_KEY\_FILE="/etc/etcd/ssl/etcd-key.pem"

ETCD\_CLIENT\_CERT\_AUTH="true"

ETCD\_TRUSTED\_CA\_FILE="/etc/etcd/ssl/etcd-root-ca.pem"

ETCD\_AUTO\_TLS="true"

ETCD\_PEER\_CERT\_FILE="/etc/etcd/ssl/etcd.pem"

ETCD\_PEER\_KEY\_FILE="/etc/etcd/ssl/etcd-key.pem"

ETCD\_PEER\_CLIENT\_CERT\_AUTH="true"

ETCD\_PEER\_TRUSTED\_CA\_FILE="/etc/etcd/ssl/etcd-root-ca.pem"

ETCD\_PEER\_AUTO\_TLS="true"

# [logging]

#ETCD\_DEBUG="false"

# examples for -log-package-levels etcdserver=WARNING,security=DEBUG

#ETCD\_LOG\_PACKAGE\_LEVELS=""

服务器10.129.55.65类似：

# [member]

ETCD\_NAME=etcd2

ETCD\_DATA\_DIR="/var/lib/etcd/etcd2.etcd"

ETCD\_WAL\_DIR="/var/lib/etcd/wal"

ETCD\_SNAPSHOT\_COUNT="100"

ETCD\_HEARTBEAT\_INTERVAL="100"

ETCD\_ELECTION\_TIMEOUT="1000"

ETCD\_LISTEN\_PEER\_URLS="https://10.129.55.65:2380"

ETCD\_LISTEN\_CLIENT\_URLS="https://10.129.55.65:2379,http://127.0.0.1:2379"

ETCD\_MAX\_SNAPSHOTS="5"

ETCD\_MAX\_WALS="5"

#ETCD\_CORS=""

# [cluster]

ETCD\_INITIAL\_ADVERTISE\_PEER\_URLS="https://10.129.55.65:2380"

# if you use different ETCD\_NAME (e.g. test), set ETCD\_INITIAL\_CLUSTER value for this name, i.e. "test=http://..."

ETCD\_INITIAL\_CLUSTER="etcd1=https://10.129.55.61:2380,etcd2=https://10.129.55.65:2380,etcd3=https://10.129.55.155:2380"

ETCD\_INITIAL\_CLUSTER\_STATE="new"

ETCD\_INITIAL\_CLUSTER\_TOKEN="etcd-cluster"

ETCD\_ADVERTISE\_CLIENT\_URLS="https://10.129.55.65:2379"

#ETCD\_DISCOVERY=""

#ETCD\_DISCOVERY\_SRV=""

#ETCD\_DISCOVERY\_FALLBACK="proxy"

#ETCD\_DISCOVERY\_PROXY=""

#ETCD\_STRICT\_RECONFIG\_CHECK="false"

#ETCD\_AUTO\_COMPACTION\_RETENTION="0"

# [proxy]

#ETCD\_PROXY="off"

#ETCD\_PROXY\_FAILURE\_WAIT="5000"

#ETCD\_PROXY\_REFRESH\_INTERVAL="30000"

#ETCD\_PROXY\_DIAL\_TIMEOUT="1000"

#ETCD\_PROXY\_WRITE\_TIMEOUT="5000"

#ETCD\_PROXY\_READ\_TIMEOUT="0"

# [security]

ETCD\_CERT\_FILE="/etc/etcd/ssl/etcd.pem"

ETCD\_KEY\_FILE="/etc/etcd/ssl/etcd-key.pem"

ETCD\_CLIENT\_CERT\_AUTH="true"

ETCD\_TRUSTED\_CA\_FILE="/etc/etcd/ssl/etcd-root-ca.pem"

ETCD\_AUTO\_TLS="true"

ETCD\_PEER\_CERT\_FILE="/etc/etcd/ssl/etcd.pem"

ETCD\_PEER\_KEY\_FILE="/etc/etcd/ssl/etcd-key.pem"

ETCD\_PEER\_CLIENT\_CERT\_AUTH="true"

ETCD\_PEER\_TRUSTED\_CA\_FILE="/etc/etcd/ssl/etcd-root-ca.pem"

ETCD\_PEER\_AUTO\_TLS="true"

# [logging]

#ETCD\_DEBUG="false"

# examples for -log-package-levels etcdserver=WARNING,security=DEBUG

#ETCD\_LOG\_PACKAGE\_LEVELS=""

服务器：10.129.55.155类似：

# [member]

ETCD\_NAME=etcd3

ETCD\_DATA\_DIR="/var/lib/etcd/etcd3.etcd"

ETCD\_WAL\_DIR="/var/lib/etcd/wal"

ETCD\_SNAPSHOT\_COUNT="100"

ETCD\_HEARTBEAT\_INTERVAL="100"

ETCD\_ELECTION\_TIMEOUT="1000"

ETCD\_LISTEN\_PEER\_URLS="https://10.129.55.155:2380"

ETCD\_LISTEN\_CLIENT\_URLS="https://10.129.55.155:2379,http://127.0.0.1:2379"

ETCD\_MAX\_SNAPSHOTS="5"

ETCD\_MAX\_WALS="5"

#ETCD\_CORS=""

# [cluster]

ETCD\_INITIAL\_ADVERTISE\_PEER\_URLS="https://10.129.55.155:2380"

# if you use different ETCD\_NAME (e.g. test), set ETCD\_INITIAL\_CLUSTER value for this name, i.e. "test=http://..."

ETCD\_INITIAL\_CLUSTER="etcd1=https://10.129.55.61:2380,etcd2=https://10.129.55.65:2380,etcd3=https://10.129.55.155:2380"

ETCD\_INITIAL\_CLUSTER\_STATE="new"

ETCD\_INITIAL\_CLUSTER\_TOKEN="etcd-cluster"

ETCD\_ADVERTISE\_CLIENT\_URLS="https://10.129.55.155:2379"

#ETCD\_DISCOVERY=""

#ETCD\_DISCOVERY\_SRV=""

#ETCD\_DISCOVERY\_FALLBACK="proxy"

#ETCD\_DISCOVERY\_PROXY=""

#ETCD\_STRICT\_RECONFIG\_CHECK="false"

#ETCD\_AUTO\_COMPACTION\_RETENTION="0"

# [proxy]

#ETCD\_PROXY="off"

#ETCD\_PROXY\_FAILURE\_WAIT="5000"

#ETCD\_PROXY\_REFRESH\_INTERVAL="30000"

#ETCD\_PROXY\_DIAL\_TIMEOUT="1000"

#ETCD\_PROXY\_WRITE\_TIMEOUT="5000"

#ETCD\_PROXY\_READ\_TIMEOUT="0"

# [security]

ETCD\_CERT\_FILE="/etc/etcd/ssl/etcd.pem"

ETCD\_KEY\_FILE="/etc/etcd/ssl/etcd-key.pem"

ETCD\_CLIENT\_CERT\_AUTH="true"

ETCD\_TRUSTED\_CA\_FILE="/etc/etcd/ssl/etcd-root-ca.pem"

ETCD\_AUTO\_TLS="true"

ETCD\_PEER\_CERT\_FILE="/etc/etcd/ssl/etcd.pem"

ETCD\_PEER\_KEY\_FILE="/etc/etcd/ssl/etcd-key.pem"

ETCD\_PEER\_CLIENT\_CERT\_AUTH="true"

ETCD\_PEER\_TRUSTED\_CA\_FILE="/etc/etcd/ssl/etcd-root-ca.pem"

ETCD\_PEER\_AUTO\_TLS="true"

# [logging]

#ETCD\_DEBUG="false"

# examples for -log-package-levels etcdserver=WARNING,security=DEBUG

#ETCD\_LOG\_PACKAGE\_LEVELS=""

1. 创建etcd.service

[Unit]

Description=Etcd Server

After=network.target

After=network-online.target

Wants=network-online.target

[Service]

Type=notify

WorkingDirectory=/var/lib/etcd/

EnvironmentFile=-/etc/etcd/etcd.conf

#User=etcd

# set GOMAXPROCS to number of processors

ExecStart=/bin/bash -c "GOMAXPROCS=$(nproc) /usr/local/bin/etcd --name=\"${ETCD\_NAME}\" --data-dir=\"${ETCD\_DATA\_DIR}\" --listen-client-urls=\"${ETCD\_LISTEN\_CLIENT\_URLS}\""

Restart=on-failure

LimitNOFILE=65536

[Install]

WantedBy=multi-user.target

1. 主节点创建etcd目录。

mkdir -p /var/lib/etcd/ /etc/etcd/ssl/

说明：10.129.55.65相关操作都需要在其他节点执行一次。拷贝10.129.55.65相关的二进制文件etcd、etcdctl和/etc/etcd目录下的所有证书文件到各个etcd服务器节点。

（1）拷贝二进制文件到各个节点的操作命令：

scp -rp /k8sInstall/etcdClusterInstall/software/{etcd,etcdctl} root@"10.129.55.155":/usr/local/bin/

scp -rp /k8sInstall/etcdClusterInstall/software/{etcd,etcdctl} root@"10.129.55.61":/usr/local/bin/

（2）拷贝/etc/etcd下证书文件命令：

Scp -rp /k8sInstall/etcdClusterInstall/config/ssl root@10.129.55.155:/k8sInstall/etcdClusterInstall/config/ssl

Scp -rp /k8sInstall/etcdClusterInstall/config/ssl root@10.129.55.61:/k8sInstall/etcdClusterInstall/config/ssl

1. 拷贝etcd.service文件到集群各个节点的/usr/lib/systemd/system/目录下。

scp -rp /etcdClusterInstall/config root@10.129.55.61:/usr/lib/systemd/system/etcd.servic

scp -rp /etcdClusterInstall/config root@10.129.55.155:/usr/lib/systemd/system/etcd.servic

1. 启动所有节点上的etcd服务（各个节点都要保证安装完毕）。

systemctl start etcd.service

1. etcd集群健康状态检查，可在任意节点执行下面命令。

etcdctl --ca-file=/etc/etcd/ssl/etcd-root-ca.pem --cert-file=/etc/etcd/ssl/etcd.pem \

> --key-file=/etc/etcd/ssl/etcd-key.pem --endpoints="https://10.129.55.61:2379,https://10.129.55.65:2379,https://10.129.55.155:2379" cluster-health

member f758a80efdf4be01 is healthy: got healthy result from https://10.129.55.61:2379

member fc0dd343c5856818 is healthy: got healthy result from https://10.129.55.65:2379

member f758a80efdf4be01 is healthy: got healthy result from https://10.129.55.155:2379

Etcd集群健康状态保证检查状态如上是healthy就能提供正常访问，集群安装到此完毕。

etcd常见报错举例。

1. 启动文件配置错误，etcd如果报错大部分是启动文件第3条中配置文件修改错误。

注：另外两台需要修改配置文件中的ETCD\_NAME、ETCD\_DATA\_DIR及相关IP地址，否则将无法启动，具体报错如下：

Oct 18 17:56:47 etcd2 etcd[3117]: recognized environment variable ETCD\_NAME, but unused: shadowed by corresponding flag

Oct 18 17:56:47 etcd2 etcd[3117]: recognized environment variable ETCD\_DATA\_DIR, but unused: shadowed by corresponding flag

Oct 18 17:56:47 etcd2 systemd[1]: etcd.service: main process exited, code=exited, status=1/FAILURE

Oct 18 17:56:47 etcd2 systemd[1]: Failed to start Etcd Server.