**K8S组件端口**

**(红色字体表示对外开放端口)**

**黑色字体表示监听在本机的端口不用对外开放**

**Master Node**

|  |  |  |
| --- | --- | --- |
| Service | Port | Protocol |
| kube-apiserver | 6443/TCP 8443/TCP |  |
| kube-controller-manager | 10252/TCP 10257/TCP |  |
| kube-scheduler | 10251/TCP 10259/TCP |  |
| keepalived |  | VRRP |
| kubelet | 10248/TCP 10250/TCP 10255/TCP |  |
| kube-proxy | 10249/TCP 10256/TCP 3000-32767/TCP |  |
| etcd | 2379/TCP 2379/TCP |  |
| CoreDNS | 53/TCP 53/UDP 9053/TCP |  |
| Calico | 179/TCP | BGP |
| Flannel | 8285/UDP 8472/UDP |  |
| ceph-csi | 8680/TCP |  |

**Worker Node**

|  |  |  |
| --- | --- | --- |
| kubelet | 10248/TCP 10250/TCP 10255/TCP |  |
| kube-proxy | 10249/TCP 10256/TCP 3000-32767/TCP |  |
| CoreDNS | 53/TCP 53/UDP 9053/TCP |  |
| Ingress-controller | 8443/TCP |  |
| Calico | 179/TCP | BGP |
| Flannel | 8285/UDP 8472/UDP |  |
| ceph-csi | 8680/TCP |  |

**一：对外开放服务和端口**

1. 为 K8S 创建默认的的 Firewalld Zone，名字叫做 k8s
2. 该 Zone 的默认防火墙策略是 DROP 所有的数据包
3. 开放 DHCP 服务（k8s 节点可以通过 DHCP 获去IP地址）
4. 开放 ICMP 协议（其他主机就可以 ping 来探测 k8s 节点）
5. 开发 VRRP 协议（避免和局域网内其他的 Keepalived 冲突）
6. 开放 SSH 服务给指定的IP地址（22/tcp）
   1. 堡垒机，比如IP地址为 10.240.0.10
   2. 特定IP 地址，比如只允许 IP 地址为 10.240.0.100、10.240.0.101 的IP 地址可以通过 ssh 登录到 k8s 节点。所有当某管理员想要登录登录 k8s 时，需要将IP地址设置为 10.240.0.100或者10.240.0.101 才可以放登录 SSH登录。或者通过堡垒机来管理 k8s 节点服务器。
7. 开放 http 服务（80/tcp）
8. 开放 https 服务（ 443/tcp）
9. 开放 NodePort 端口（30000-32767）
10. 开放K8S 的 kube-apiserver 或者 kube-apiserver LB给指定的IP地址（6443/tcp）。

**二：K8S 节点之间开放的端口**

1. K8S Zone 开启 masquerade
2. K8S 所有节点都允许 Docker bridge network cidr 网段的流量
3. K8S所有节点都允许 Pod network cidr 网段的流量
4. K8S 所有节点都允许 Service network cidr网段的流量
5. K8S所有节点的 kubelet 监听端口（10250/tcp）允许所有 K8S 节点访问
6. K8S 所有节点的 CoreDNS 监听端口（53/TCP、51/UDP、9053/TCP）允许所有 K8S 节点访问
7. K8S master 节点的 kube-apiserver 监听端口（6443/tcp）允许所有 K8S 节点访问
8. K8S master 节点的 kube-apiserver 监听端口（6443/tcp）允许 kube-apiserver LB 访问
9. K8S master 节点的 etcd 监听端口（2379/tcp、2380/tcp）允许所有 K8S master 节点访问
10. K8S 所有节点的 Calico 监听端口（179/TCP）允许所有 K8S 节点访问（如果安装了 Calico）
11. K8S 所有节点的 Flannel 监听端口（8285/UDP 8472/UDP）允许所有K8S 节点访问（如果安装了Flannel）
12. K8S 所有节点的 Ingress 监听端口（8443/TCP）允许所有K8S 节点访问（如果安装了 Ingress）

参考资料

<https://github.com/coreos/coreos-kubernetes/blob/master/Documentation/kubernetes-networking.md>

<https://docs.projectcalico.org/getting-started/kubernetes/requirements>

<https://docs.projectcalico.org/security/protect-hosts>

<https://rancher.com/docs/rancher/v2.x/en/installation/resources/advanced/firewall/>

<https://medium.com/platformer-blog/kubernetes-on-centos-7-with-firewalld-e7b53c1316af>

<https://github.com/kubernetes-retired/contrib/blob/master/ansible/roles/node/tasks/firewalld.yml>

<https://github.com/wrightrocket/k8s-firewalld>

<https://serverfault.com/questions/607808/linux-firewalld-zones-logic-and-priority> (理解 firewalld 匹配规则)

<https://www.linuxjournal.com/content/understanding-firewalld-multi-zone-configurations> (理解 firewalld 匹配规则)