对submariner的调研

20210719

submariner最早由rancher公司开源（rancher公司也是一个非常厉害的公司，CEO是华裔，该公司开源了k3s），因为一些不愉快的事情，现在主要由redhat公司维护（两个公司在该项目上出现了一些分歧）

在将多个集群注册到一个非统一的控制面板后，对于高可用（high available, HA）和分布式应用程序调度情况，需要在多个集群之间实现pod的相互访问，submariner方案目前是一种非常好的备选方案，

(1)能够覆盖相当广泛的使用场景，

(独立集群，托管集群)

(kubernetes 老版本，新版本)

(网络插件flannel，calico)

(云厂商AWS，GKE，AKS，GKE，CCE)

(有没有公网ip，没有就用NAT)

(网络CIDR是否冲突，global-net CIDR)。

(2)几乎不依赖并与已注册的集群部署，拓扑更好地保持一致。对集群的入侵性小，submariner官网有详细的安装和卸载步骤，安装的话不必多说，卸载主要是删除对应的namespace，删除CRD(Custom Resource Definition，自定义资源，Kubernetes API的一个拓展)，删除iptables中的相关策略

(3)技术实现简单，易于维护(也有人认为技术过于久远，缺乏创新)

主要功能：

与现有集群的兼容性和连接性：用户可以将 Submariner 部署到已有的 Kubernetes 集群中，并在位于不同集群的节点之间添加三层网络连接。

安全路径： 使用 IPSec 隧道实现加密的网络连接。

集中式代理 ：用户可以注册和维护一组健康的网关节点。通过 Gateway 组件实现

全局私有网络：使用全局虚拟网络解决多集群网络 overlapping CIDRs 的问题。通过 Globalnet 组件实现

服务发现： Submariner 提供跨多个 Kubernetes 集群的服务发现, 通过 Lighthouse 组件实现。

CNI 兼容性： 适用于流行的 CNI 驱动程序。

多集群之间 pod 与 pod 互通

多集群之间 pod 与 service 的连接

适配不同云厂商

适配常见的网络 CNI 插件

允许通过云原生的方式部署，创建自定义资源 CR 就可以快速在多集群之间部署

主要组件的功能简述

broker 经纪人，代理

operator组件 部署submariner

lighthouse组件 服务发现

gateway组件 pod跨集群访问

竞争方案，cilium mash、 istio和GKE Anthos

GKE Anthos参考链接https://cloud.google.com/anthos/docs/concepts/overview

GKE Anthos主要的优势在于有Google专业的团队维护，质量有保证

主要原理是将指定的service暴露到公网，然后采用Google Cloud VPN访问，还有一些关于Fleet的原理，这个比较复杂

IPSec 隧道，就是在公网打一个隧道，参考链接<http://www.h3c.com/cn/d_201005/675214_97665_0.htm> 例如，允许外出员工访问公司网络

Google Cloud VPN就是采用的该方案

