# 集群架构改造文档

针对痛点：

* 生产环境固定周期漏洞扫描，会对集群所有端口“一网打尽”，含开发，测试，演示等，且每次扫描结果都可能不一样
* Kubesphere七层访问问题，https支持因k8s版本问题存在问题

实施步骤：

1. 修改集群默认的NodePort监听方式，默认全集群监控，现改为除10.10.48.31外，其他所有用户类NodePort监听在除48.31外的所有机器上
2. 10.10.48.31部署nginx, 以docker-compose形式部署，因牵扯生产，所有配置文件代码化管理，约定更新配置以代码形式提交记录，其中nginx.conf为全局配置，conf.d目录下为各个项目的配置文件，名称为项目标准名称，每个项目为一个独立server，具体内容见代码。



仓库地址： [**http://git.software.dimpt.com/devops/nginx-gateway.git**](http://git.software.dimpt.com/devops/nginx-gateway.git)

1. 4层备选方案：使用iptables 做网络层地址转发，详细内容见链接文档。

[**http://git.software.dimpt.com/devops/nginx-gateway/-/blob/main/iptables/iptables**](http://git.software.dimpt.com/devops/nginx-gateway/-/blob/main/iptables/iptables)

1. 开发验证改造效果。

异常问题回滚方案：

1，恢复10.10.48.31的NodePort监听，生产环境等恢复到改造前。