OneCloud负载均衡

模型和私有云实现

周有松 @yousong

2020-02-22

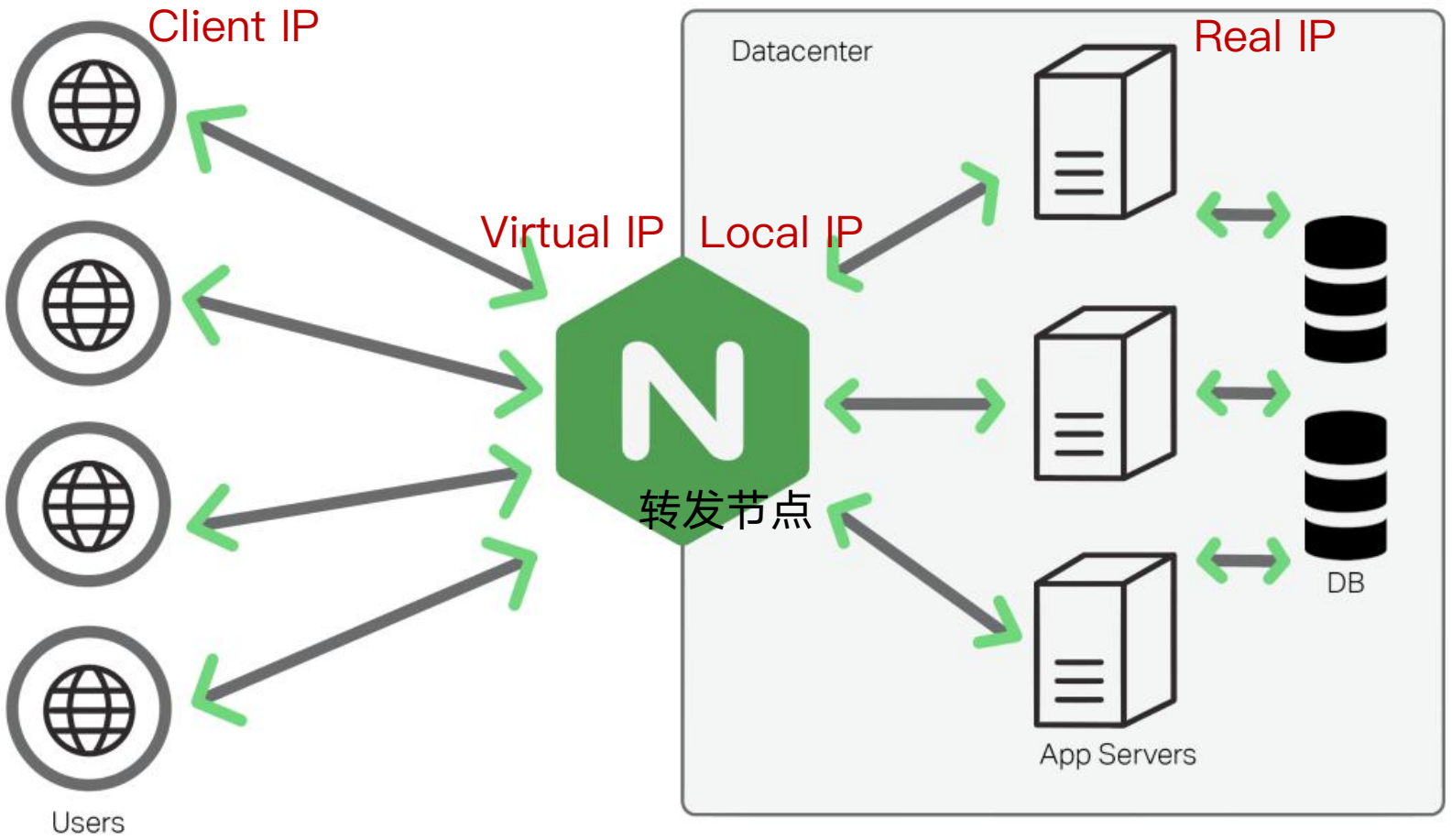
内容提要

- 负载均衡服务简介
  - 功能模型
  - 业务词汇
- 功能与应用场景
  - 协议
  - 转发策略
  - 调度算法
  - 会话保持
  - …
- 转发集群管理

01

产 品 简 介

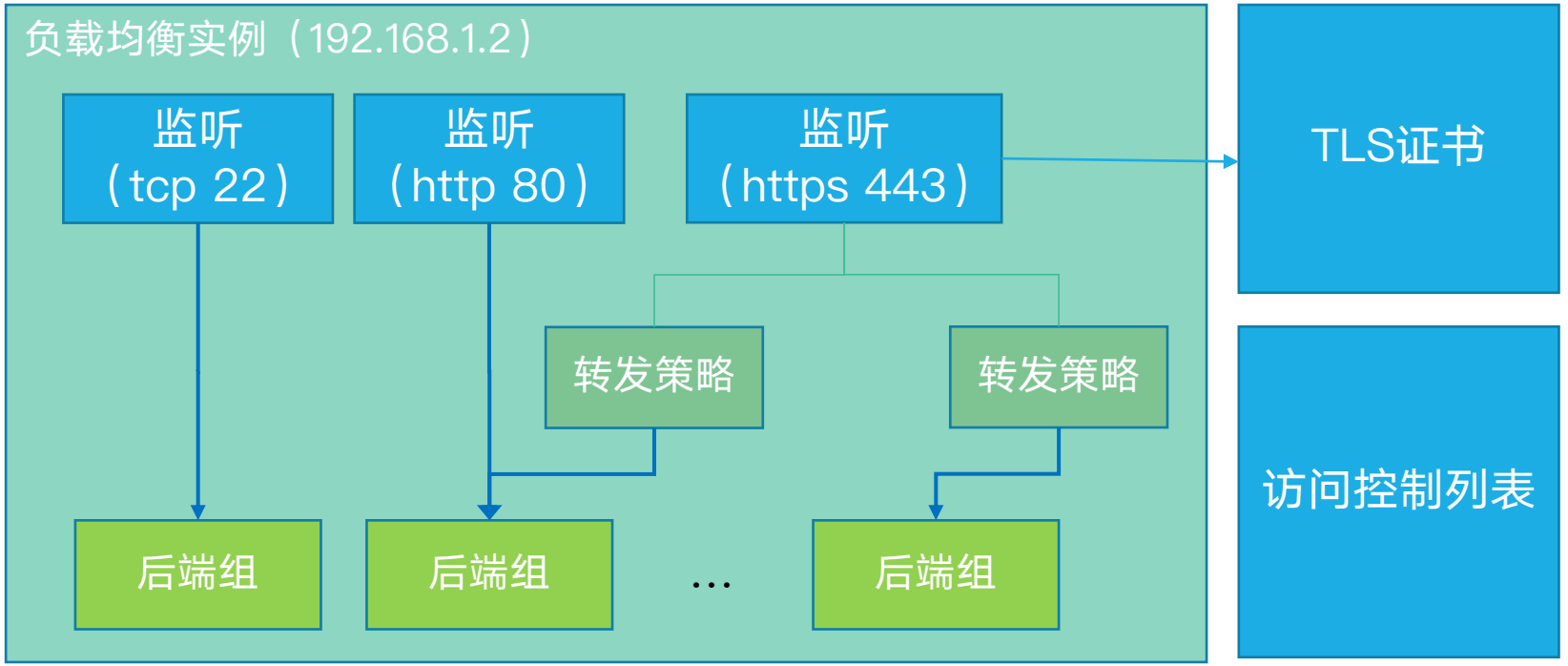
功能模型



- NGINX做什么
- 流量路径
- 解决的问题
- 适用的场景

业务词汇

- 实例：virtual ip
- 监听：virtual port
  - 协议、端口
  - 调度算法
  - 健康检查
  - 转发策略
- 后端服务器组
  - 后端服务器：real ip + real port
- TLS证书
- 访问控制列表



02

功能与应用场景

监听 - 协议

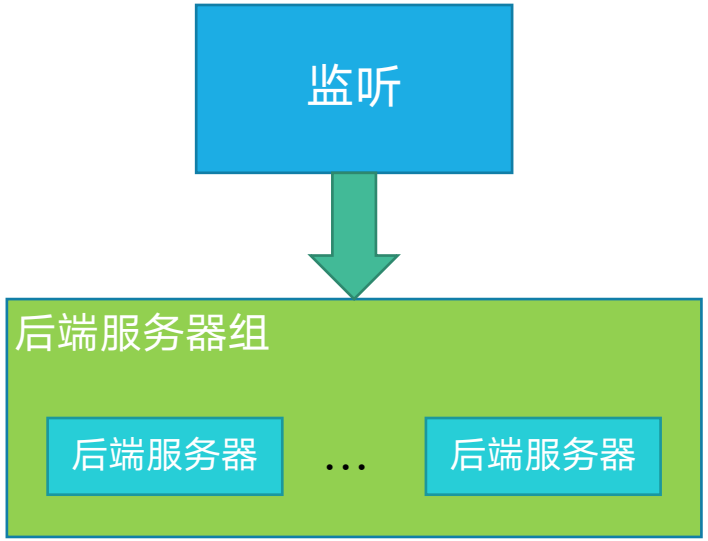
云联万维 YUNION

- 协议：HTTP, HTTPS, TCP, UDP, WS, WSS, HTTP2
- TCP, UDP的端口空间是独立的
- 举例：同一负载均衡实例下
  - TCP/53, UDP/53可以共存
  - TCP/80, HTTP/80不可以同时存在
- 计算量：HTTPS > HTTP > TCP > UDP
- HTTPS
  - 关联证书
  - 启用HTTP2

监听 - 调度算法

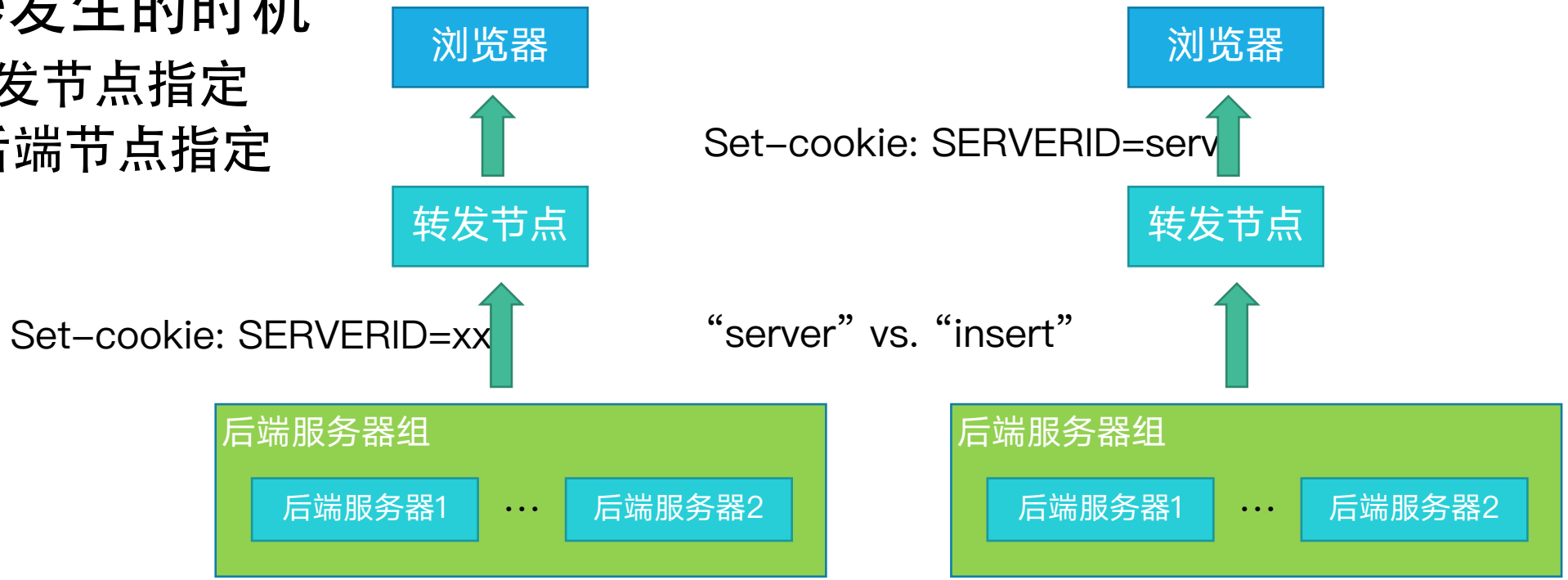
云联万维
YUNION

- 监听收到请求后，向后端服务器组转发：如何选择
- 轮询，round robin
  - 适用于短连接业务，如网页浏览
- 最小连接数，least connected
  - 适用于长连接，如文件上传下载
- 源一致性哈希
  - 适用于需要维护会话状态的业务
  - HTTP可以用会话保持（cookie）



监听 - 会话保持

- 仅适用监听协议为HTTP：cookie
- 在cookie中告诉转发节点，将请求转发到指定后端
- Set-Cookie发生的时机
  - Insert：转发节点指定
  - Server：后端节点指定



监听 - 健康检查

云联万维 YUNION

- TCP检查
  - 连接建立是否成功
- UDP检查
  - 指定请求报文内容
  - 是否收到指定响应
- HTTP检查
  - 构造HEAD /path HTTP/1.0请求
  - 检查响应的状态码，2xx |3xx |4xx |5xx
- 所有后端不可用时，503 Service Unavailable
- 检查结果描述：超时，连接错误，响应错误…

HTTP转发策略

云联万维 YUNION

- 转发节点解析HTTP请求
- 根据Host, Path转发到不同的后端组
- 意义
  - 复用IP、端口
  - 共用ACL规则
  - 共享带宽
  - 配置简单

```
GET / HTTP/1.1
Host: oh-my-lb0
User-Agent: curl/7.46.0
Accept: */*
```

其他

云联万维 YUNION

- 跳转：HTTP跳转HTTPS，选移
- 基于网段的访问控制
- 后端获得客户端真实IP（Local IP vs. Client IP）
  - X-Forwarded-For
  - PROXY protocol
- HTTP请求速率控制
  - 每个监听、转发策略的速率控制
  - 每个源IP的速率控制
- ECDSA, RSA证书支持

03

转发集群管理

多转发集群

云联万维 YUNION

- 使用场景
  - 不同的部署环境：测试环境、线上环境
  - 转发能力水平扩展

hey –c 256 –n 10000 –disable–keepalive

协议	Keepalive	RPS
TCP	on	1,8000
HTTP	on	1,5000
HTTPS	on	1,200
TCP	off	7,800
HTTP	off	7,000
HTTPS	off	1,200

转发节点

云联万维 YUNION

- 组件：LBAgent, Keepalived, HAProxy, Gobetween
- 单个集群内：节点间主备高可用
- 宕机恢复：根据配置决定是否切换回原状
- 部署环境要求
  - 节点能够访问OneCloud API服务
  - 客户端能够访问到绑定于此的Virtual IP
  - 节点能够访问Real IP
  - 节点间能够维持Keepalived会话

OneCloud技术交流群

该二维码7天内(2月25日前)有效，重新进入将更新