



云联壹云 Meetup 18

Part 2：负载均衡的应用

云联壹云核心产品融合云 云联壹云 秉承：简单、开放、融合、智能的产品理念，能够帮助企业实现异构IT基础设施的全面云化、统一管理及成本优化，提高运维效率的同时，降低企业运营成本。

2021-05 网络工程师 周有松



扫码进技术交流群



更多资讯关注我

目 录

CONTENTS

01 负载均衡的服务简介

·功能模型 ·业务词汇

02 功能与应用场景

·协议 ·转发策略 ·调度算法 ·会话保持 ...

03 总结

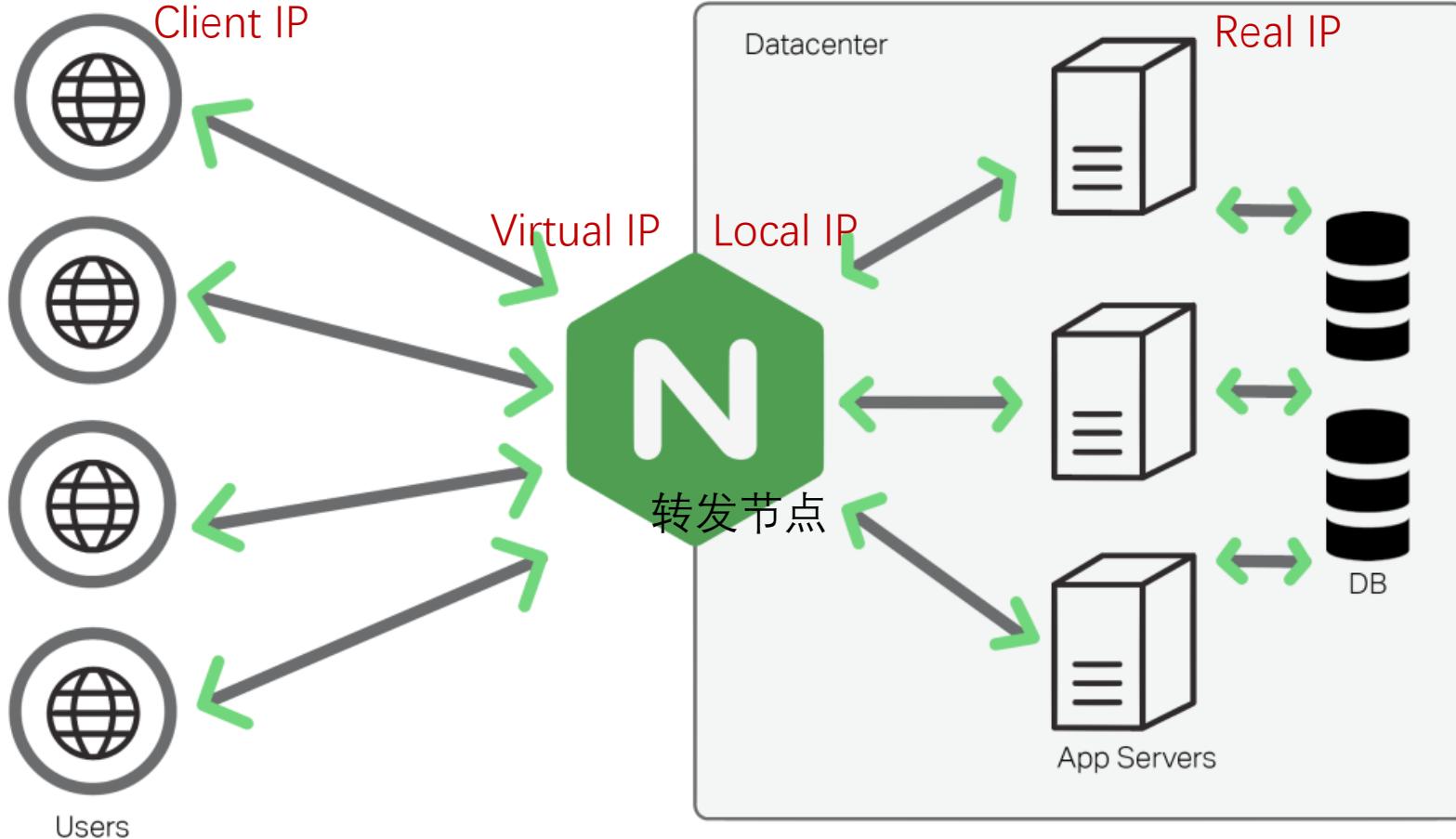


01

负载均衡的服务简介

·功能模型 ·业务词汇

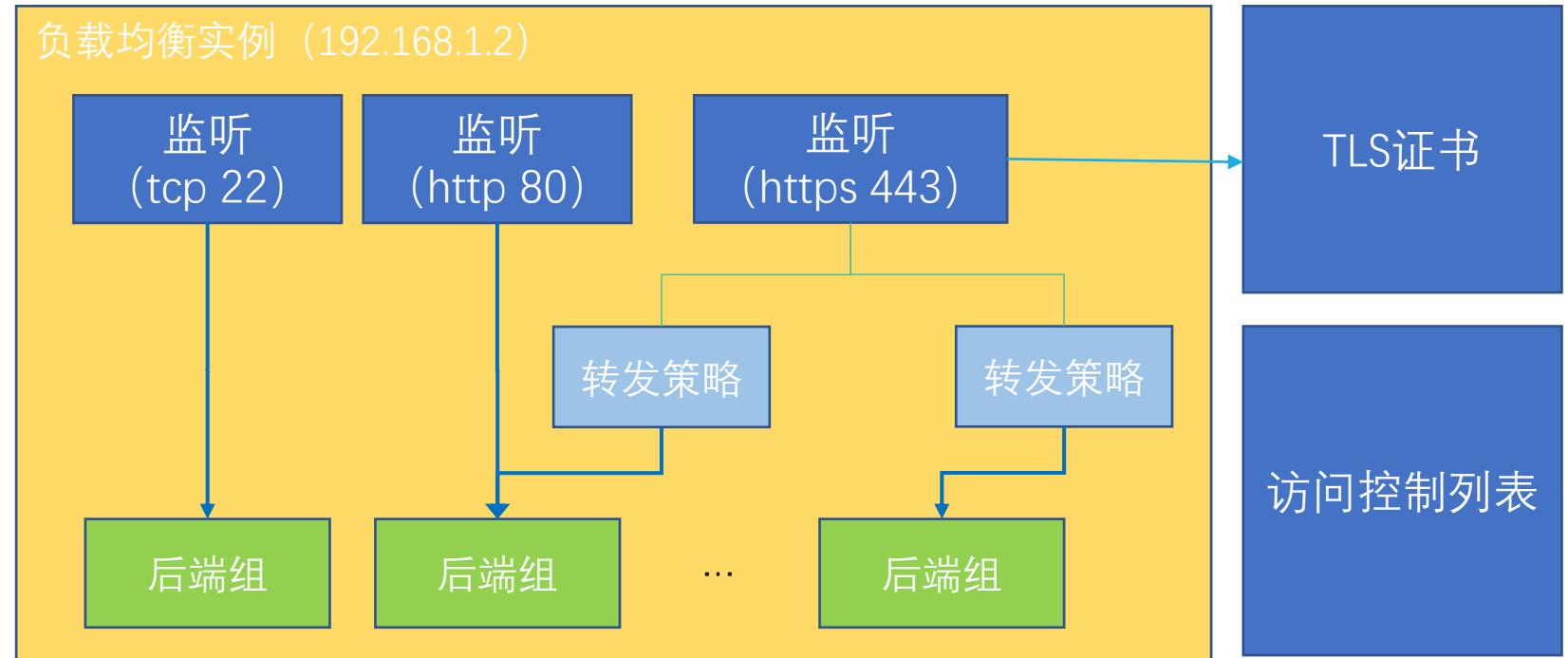
功能模型-Nginx



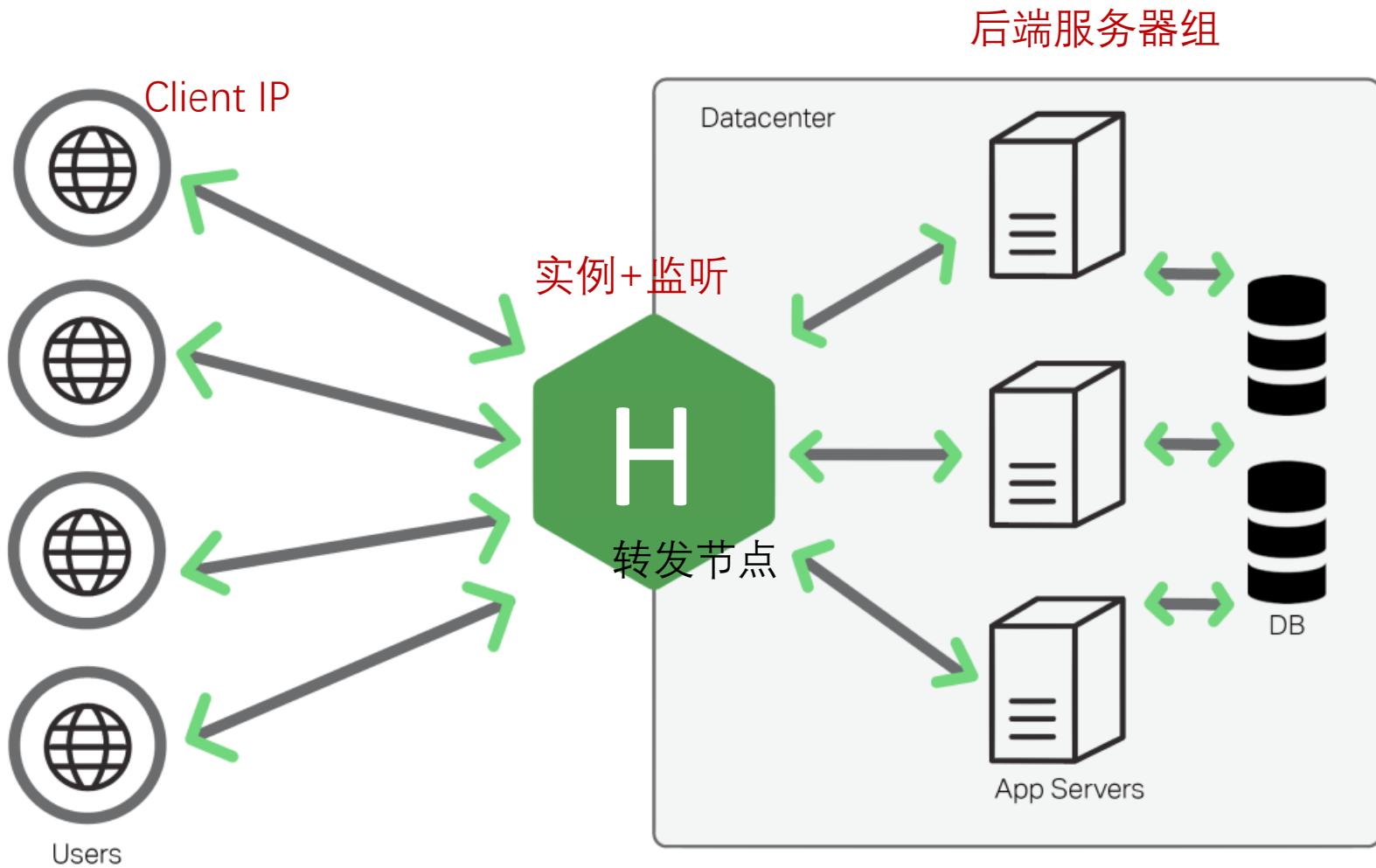
- NGINX做什么
- 流量路径
- 解决的问题
- 适用的场景

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



功能模型 - HAProxy



02

功能与应用场景

· 协议 · 转发策略 · 调度算法 · 会话保持 ...

| 协议

- 协议 : HTTP, HTTPS, TCP, UDP
- 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
- 开销 : HTTPS > HTTP > TCP > UDP
- 其它协议 :
 - WebSocket: WS, WSS
 - HTTP2: HTTPS
 - QUIC: HAProxy 2.5

协议 (续)

新建负载均衡监听

1 协议&监听 2 后端服务器组

基础配置

* 名称: lb0ls0

* 监听端口: 443

协议: TCP UDP HTTP **HTTPS**

* 证书: expire-0804
没有想要的? 可以前往[新建证书](#)

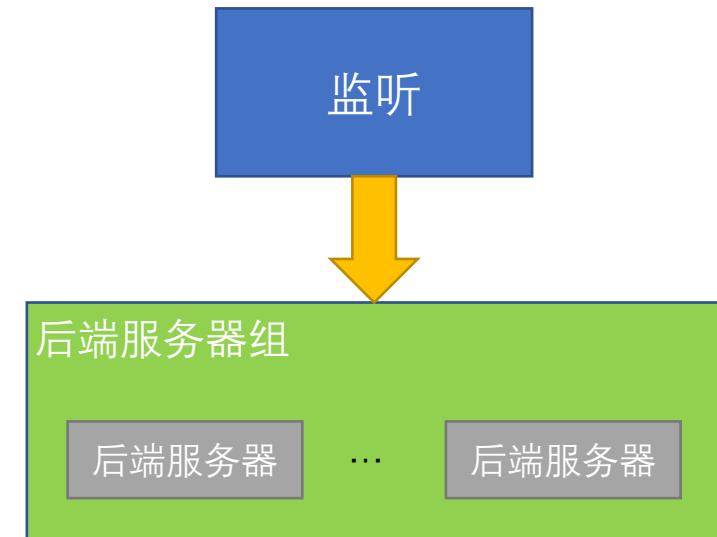
重定向:



- 所有协议 : 端口
- HTTPS : 证书
- WS, WSS, HTTP2

调度算法

- 监听到收到请求后，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）



调度算法 (续)

实例
Yunion-FE 启用 禁用 更多 ▾

详情 监听 **后端服务器组** 操作日志

新建 删除

添加筛选项

| <input type="checkbox"/> 名称 | 状态 | 前端协议:端口 | 调度算法 | 后端服务器组 |
|-----------------------------|----|-----------|------------|----------------|
| https-redirect | 启用 | http:80 | - | - |
| Git-SSH | 启用 | tcp:22 | 加权最小连接数 | Yunion-Git-SSH |
| https | 启用 | https:443 | 基于源IP一致性哈希 | https |

| 健康检查

- 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…

健康检查（续）

基础配置

开启健康检查：

高级配置

健康检查协议： TCP HTTP

* 健康检查路径：

健康检查域名：

* 正常状态码： http_2xx http_3xx http_4xx http_5xx

健康检查间隔时间： 秒

健康检查健康阈值： 次

健康检查不健康阈值： 次

HTTP转发策略

- 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: */*
```

HTTP转发策略 (续)

监听
https 修改 删除 更多 ▾

详情 **转发策略** 监控 后端服务器 操作日志

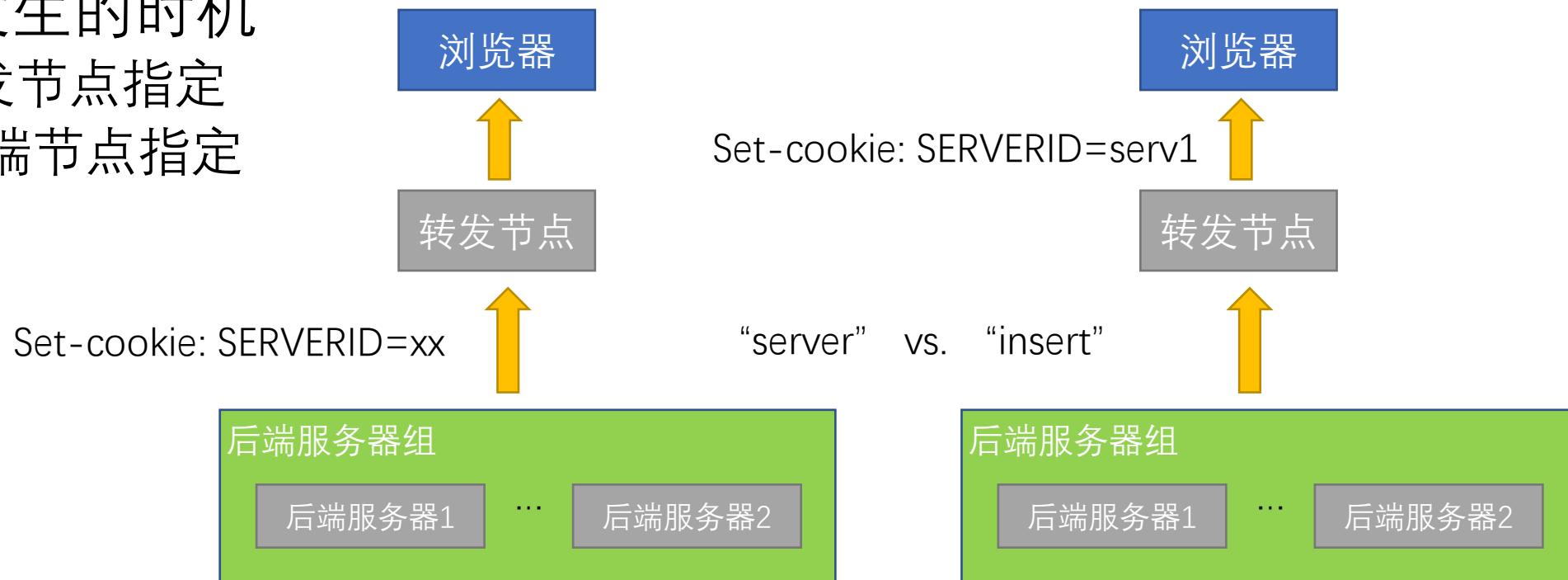
新建

添加筛选选项

| <input type="checkbox"/> 名称 | 状态 | 所属域 | URL | 后端服务器组 |
|-----------------------------|------|---------|-----|------------|
| Yunion-N9e | ● 启用 | Default | - | - |
| Yunion-Ops | ● 启用 | Default | - | Yunion-Ops |
| ESXi | ● 启用 | Default | - | ESXi |
| vCenter | ● 启用 | Default | - | vCenter |
| OpenStack | ● 启用 | Default | - | OpenStack |
| Harbor | - | - | - | - |

| 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



跳转

协议:

TCP UDP **HTTP** HTTPS

重定向:



重定向方式:

永久重定向 (301) 临时重定向 (302) 临时重定向 (307)

重定向至:

HTTP 请输入域名或IP地址 (端口号) 请输入URL路径

HTTP 地址不能与重定向之前相同

HTTPS

> 高级配置

- HTTP跳转HTTPS

- 站点迁移

- 应用升级

其他 – 访问控制

新建访问控制

* 策略组名称:

* 批量添加地址①:
每个条目一行, 以回车分隔
每个条目的地址/地址段和备注以|分隔, 如“192.168.1.0/24|备注”
地址例如: 192.168.1.1|备注
地址段例如: 192.168.1.1/24|备注
备注为可选, 限制16个字符以内

启用访问控制:

访问控制方式:

* 访问控制策略组:
 白名单: 允许特定IP访问负载均衡
 白名单: 允许特定IP访问负载均衡
 黑名单: 禁止特定IP访问负载均衡
[请选择切换策略](#)

- 向合作伙伴开放接口
- 限定应用服务区域

| 其他 – 获取客户端真实IP

- 后端获得客户端真实IP (Local IP vs. Client IP)
- 通过HTTP头部传递 : X-Forwarded-For
- PROXY规范: AWS LB, NGINX, Stunnel等



| 其他 – 请求速率控制

- 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
- 保护后端应用

限定接收请求速率：

0

次/秒

0为默认，表示不限速

限定同源IP发送请求速率：

0

次/秒

限制同一源地址对监听发送请求的速率，0为默认值，表示不限速

| 其他 - TLS证书

- 算法 : RSA, EC
- 文件格式 : PEM
- 私钥格式标准 :

-----BEGIN RSA PRIVATE KEY-----

PKCS#1

-----BEGIN EC PRIVATE KEY-----

?

-----BEGIN PRIVATE KEY-----

PKCS#8

其他 - TLS证书 (续)

网络

基础网络

VPC

二层网络

IP子网

网络服务

弹性公网IP

NAT网关

DNS解析

负载均衡

实例

访问控制

证书

证书

新建

删除

添加筛选选项

证书名称

证书域名

过期时间

关联扩展域名

项目

操作

主要信息

| 证书名称 | 证书域名 | 过期时间 | 关联扩展域名 | 项目 | 操作 |
|-------------|-----------|----------------------|--|----------------|----|
| expire-0804 | yunion.io | 2021年08月04日 23:48:37 | *.yunion.cn *.yunion.com *.yunion.io *.yunionyun.com yunion.cn yunion.com yunion.io yunion.com | system Default | 删除 |
| expire-0530 | yunion.io | 2021年05月30日 23:48:12 | *.yunion.cn *.yunion.com *.yunion.io *.yunionyun.com yunion.cn yunion.com yunion.io yunion.com | system Default | 删除 |

菜单位置

TLS证书 – 批量更新

证书
expire-0804 [删除](#)

详情 监听 [缓存列表](#) 操作日志

[更换证书](#)

添加筛选项

| 名称 | 状态 | 前端协议:端口 |
|---------------|------|-----------|
| Jumpserver... | ● 启用 | https:443 |
| https | ● 启用 | https:443 |

你所选的 2个负载均衡监听 将执行 调整访问控制 操作, 你是否确认操作?

| 名称 | 状态 | 前端协议:端口 |
|----------------|------|-----------|
| Jumpserver-Web | ● 启用 | https:443 |
| https | ● 启用 | https:443 |

* 新证书:

没有想要的? 可以前往[新建证书](#)

[确定](#) [取消](#)

A large blue right-angled triangle is positioned on the left side of the slide. Its hypotenuse runs from the bottom-left towards the top-right, and its vertical leg is aligned with the center of the slide.

03

总结

| 总结

- 与自建NGINX服务相比
- 模块化封装的产品
 - 高可用部署
 - 监控、告警
 - 权限管理
 - 操作过程可审计
- 信息呈现直观，一目了然
- 变更操作简便，更可预期
- 开放API：可编程控制

Q&A

2021

THANK YOU

云联壹云核心产品融合云 云联壹云 秉承：简单、开放、融合、智能的产品理念，能够帮助企业实现异构IT基础设施的全面云化、统一管理及成本优化，提高运维效率的同时，降低企业运营成本。

高现起&周有松 2021-05



扫码进技术交流群



更多资讯关注我