F5负载均衡综合实例详解

转载

网络负载均衡（load balance），就是将负载（工作任务）进行平衡、分摊到多个操作单元上进行执行，例如web服务器、FTP服务器、企业关键应用服务器关键任务服务器等，从而共同完成工作任务。实际上就是，负载均衡会对外部展现一个虚拟的服务器地址，当用户试图连接时，它会将连接通过双向网络地址（NAT）转到最适合的真实服务器上，以完成用户的请求。下面我们就了解一下F5负载均衡。F5 BIG-IP LTM 的官方名称叫做本地流量管理器,可以做4-7层负载均衡,具有负载均衡、应用交换、会话交换、状态监控、智能网络地址转换、通用持续性、响应错误处理、IPv6网关、高级路由、智能端口镜像、SSL加速、智能HTTP压缩化、第7层速率整形、内容缓冲、内容转换、连接加速、高速缓存、Cookie加密、选择性内容加密、应用攻击过滤、拒绝服务(DoS)攻击和SYN Flood保护、防火墙—包消毒等功能。

F5负载均衡产品时我们常用的网络负载控制的产品之一，那么在此我们对它的功能和特点进行一个全面的介绍。通过对这个产品的认识，我们也能发现络管理中我们需要注意哪些方面的问题。那么更多的内容，还是从下文中了解吧。

配置F5交换机的问题在于，与平时所学的交换机、路由器思路完全不同，拿到设备后，完全不知如何下手。

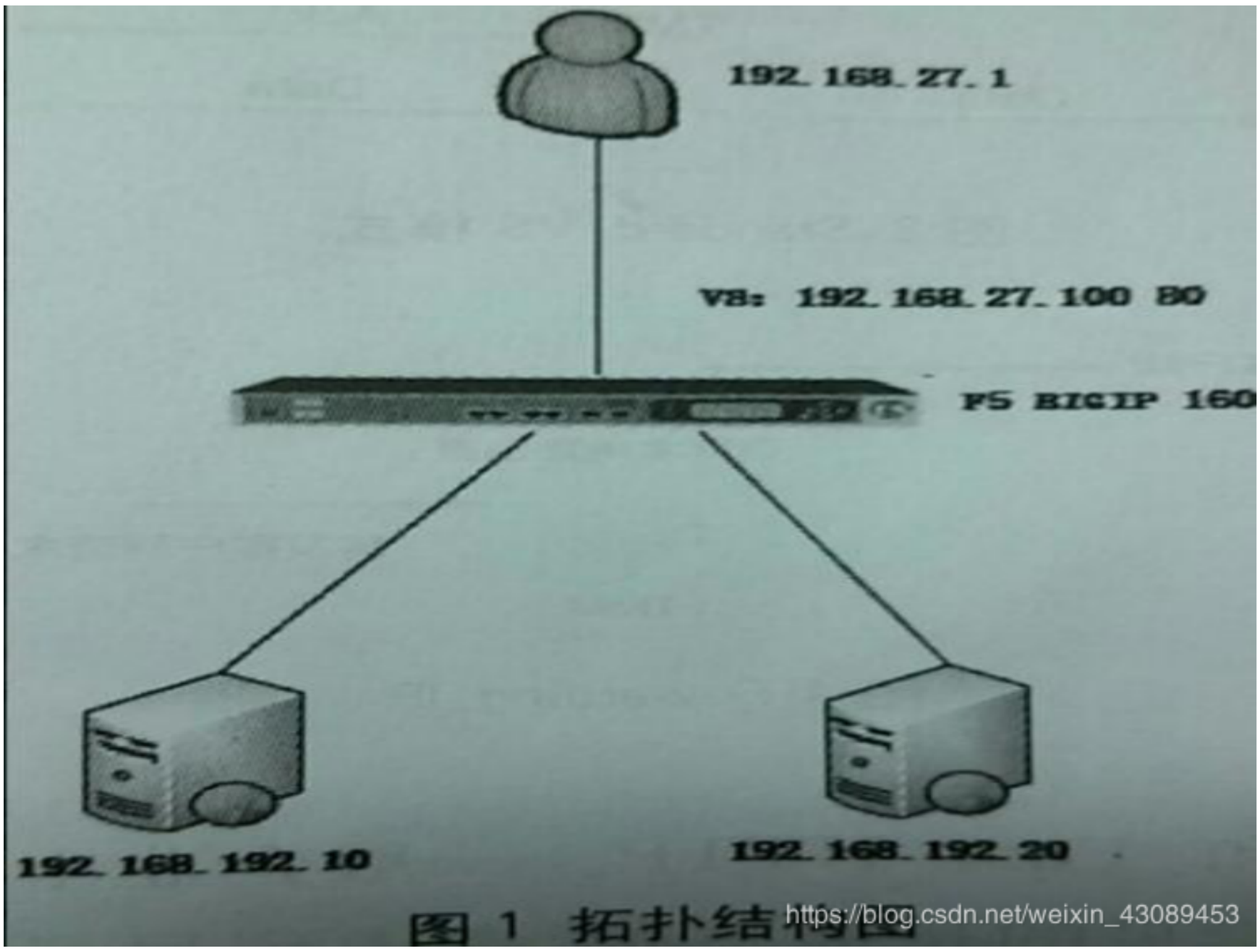


图 1 拓扑结构图

网络拓扑图如下：

两台web服务器对外提供服务，Ip地址为：192.168.192.10-20/24,外网地址192.168.27.100的80端口进行负载均衡的访问。

F5配置最简单负载均衡，需要配置的参数有Node（节点）、Pool（资源池）、和Virtual Server（虚拟服务器），它们的关系式，先配置Node，然后配置Pool，再配置Virtual Server，Node是最基本的定义，如每个服务器就是一个Node，负载均衡Pool是一组Node接收和处理流量的一组设备，如web服务器集群。BIGIP系统将客户机流量请求到Pool成员中的任一服务器上（Node），然后将Pool与BIGIP系统中的Virtual server相关联，最后，BIGIP系统将进入Virtual Server中流量传输到Pool成员，再传达给Node。

F5负载均衡功能1.多链路的负载均衡和冗余

与互联网络相关的关键业务都需要安排和配置多条ISP接入链路以保证网络服务的质量,消除单点故障,减少停机时间，多条ISP接入的方案并不是简单的多条ISP接入,而是要解决多条ISP接入的广域网络的路由问题,因为不同的ISP有不同自治域,所以必须考虑到两种情况下如何实现多条链路的负载均衡:内部的应用系统和网络工作站在访问互联网络和网站时如何能够在多条不同的链路中动态分配和负载均衡,这也被称为OUTBOUND流量的负载均衡，互联网络的外部用户如何在外部访问内部的网站和应用系统,也能够动态的在多条链路上平衡分配,并在一条链路中断的时候能够智能地自动切换到另外一条链路到达服务器和应用系统,这也被称作为INBOUND流量的负载均衡，

F5 的BIG-IP LC可以智能的解决以上两个问题:对于OUTBOUND流量,BIG-IP LC接收到流量以后,可以智能的将OUTBOUND流量分配到不同的INTERNET链路,并做源地址的NAT,可以指定某一合法IP地址进行源地址的 NAT,也可以用BIG-IP LC的接口地址自动映射,保证数据包返回时能够正确接收，对于INBOUND流量,BIG-IP LC分别绑定两个ISP 服务商的公网地址,解析来自两个ISP服务商的DNS解析请求，BIG-IP LC不仅可以根据服务器的健康状况和响应速度回应LDNS相应的请求,还可以通过两条链路分别与LDNS建立连接,根据RTT时间判断链路的好坏,并且综合以上两个参数回应LDNS相应的IP地址，

F5负载均衡功能2.防火墙负载均衡

考虑到绝大多数的防火墙只能达到线速的30%吞吐能力,故要使系统达到设计要求的线速处理能力,必须添加多台防火墙,以满足系统要求，然而,防火墙必须保证数据同进同出,否则连接将被拒绝，如何解决防火墙的负载均衡问题,是关系到整个系统的稳定性的关键问题，F5的防火墙负载均衡方案,能够为用户提供异构防火墙的负载均衡与故障自动排除能力，典型的提高防火墙处理能力的方法是采用“防火墙三明治"的方法,以实现透明设备的持续性，这可满足某些要求客户为成功完成交易必须通过同一防火墙的应用程序的要求,也能够维护原来的网络安全隔离的要求，

F5负载均衡功能3.服务器负载均衡

对于所有的对外提供服务的服务器,均可以在BIG-IP上配置Virtual Server实现负载均衡,同时BIG-IP可持续检查服务器的健康状态,一旦发现故障服务器,则将其从负载均衡组中摘除，BIG-IP利用虚拟IP地址(VIP由IP地址和TCP/UDP应用的端口组成,它是一个地址)来为用户的一个或多个目标服务器(称为节点:目标服务器由IP地址和TCP/UDP应用的端口组成,它可以是internet的私网地址)提供服务，因此,它能够为大量的基于TCP/IP的网络应用提供服务器负载均衡服务，根据服务类型分别定义服务器群组,可以根据不同服务端口将流量导向到相应的服务器，BIG-IP连续地对目标服务器进行L4到L7合理性检查,当用户通过VIP请求目标服务器服务时,BIG-IP根椐目标服务器之间性能和网络健康情况,选择性能最佳的服务器响应用户的请求，如果能够充分利用所有的服务器资源,将所有流量均衡的分配到各个服务器,我们就可以有效地避免“不平衡"现象的发生，利用UIE+iRules可以将TCP/UDP数据包打开,并搜索其中的特征数据,之后根据搜索到的特征数据作相应的规则处理,因此可以根据用户访问内容的不同将流量导向到相应的服务器,例如:根据用户访问请求的URL将流量导向到相应的服务器，

F5负载均衡功能4.系统高可用性

系统高可用性主要可以从以下几个方面考虑:

4.1.设备自身的高可用性:F5 BIG-IP专门优化的体系结构和卓越的处理能力保证99.999%的正常运行时间,在双机冗余模式下工作时可以实现毫秒级切换,保证稳定运行,另外还有冗余电源模块可选，在采用双机备份方式时,备机切换时间最快会在200ms之内进行切换，BIG-IP 产品是业界唯一的可以达到毫秒级切换的产品,而且设计极为合理,所有会话通过Active 的BIG-IP 的同时,会把会话信息通过同步数据线同步到Backup的BIG-IP,保证在Backup BIG-IP内也有所有的用户访问会话信息;另外每台设备中的watchdog芯片通过心跳线监控对方设备的电频,当Active BIG-IP故障时,watchdog会首先发现,并通知Backup BIG-IP接管Shared IP,VIP等,完成切换过程,因为Backup BIG-IP中有事先同步好的会话信息,所以可以保证访问的畅通无阻，

4.2.链路冗余:BIG-IP可以检测每条链路的运行状态和可用性,做到链路和ISP故障的实时检测，一旦出现故障,流量将被透明动态的引导至其它可用链路，控和管理出入数据中心的双向流量,内部和外部用户均可保持网络的全时连接，

4.3.服务器冗余,多台服务器同时提供服务,当某一台服务器故障不能提供服务时,用户的访问不会中断，BIG-IP可以在OSI七层模型中的不同层面上对服务健康检查,实时监测服务器健康状况,如果某台服务器出现故障,BIG-IP确定它无法提供服务后,就会将其在服务队列中清除,保证用户正常的访问应用,确保回应内确性，

F5负载均衡功能5.高度的安全性

BIG-IP采用防火墙的设计原理,是缺省拒绝设备,它可以为任何站点增加额外的安全保护,防御普通网络攻击，可以通过支持命令行的SSH或支持浏览器管理方便，安全的进行远程管理,提高设备自身的安全性;能够拆除空闲连接防止拒绝服务攻击;能够执行源路由跟踪防止IP欺骗;拒绝没有ACK缓冲确认的SYN防止击;拒绝teartop和land攻击;保护自己和服务器免受ICMP攻击;不运行SMTP，FTP，TELNET或其它易受攻击的后台程序，

BIG-IP的Dynamic Reaping特性可以高效删除各类网络DoS攻击中的空闲连接,这可以保护BIG-IP不会因流量过多而瘫痪，BIG-IP可以随着攻击量的增加连接切断速率,从而提供一种具有极强适应能力，能够防御最大攻击量的解决方案，BIG-IP的Delay Binding技术可以为部署在BIG-IP后面的服务器提供全面地Flood保护，此时,BIG-IP设备作为安全代理来有效保护整个网络，BIG-IP可以和其它安全设备配合,构建动态安全防御体系，BIG-IP可以根据用户单位时间内数生成控制访问列表,将该列表加载到其它安全设备上,有效控制攻击流量，F5负载均衡功能6.SSL加速,在每台BIG-IP上,都具有SSL硬件加速芯片,并且自带10的License,用户可以不通过单独付费,就可以拥有100个TPS的SSL 加速功能,节约了用户的投资，在将来系统扩展时,可以简单的通过License升级的方式,获得SSL加速性能，

F5负载均衡功能7.系统管理

BIG-IP提供HTTPS，SSH，Telnet，SNMP等多种管理方式,用户客户端只需操作系统自带的浏览器软件即可,不需安装其它软件，可以通过支持命令行的支持浏览器管理的SSL方便，安全的进行远程管理，直观易用的Web图形用户界面大服务降低了多归属基础设施的实施成本和日常维护费用，BIG-IP包含详报告和历史纪录报告,可供评测站点流量，相关ISP性能和预计带宽计费周期，管理员可以通过全面地报告功能充分掌握带宽资源的利用状况，另外,通过F5 的Control 开发包,目前国内已有基于i-Control开发的网管软件x-control, 可以定制针对系统服务特点的监控系统,比如服务的流量情况，各种服务连接数，访问情点的健康状况等等,进行可视化显示，告警方式可以提供syslog，snmp trap，mail等方式，

F5负载均衡功能8.其它

内存扩充能力:F5 BIG-IP 1000以上设备单机最大可扩充到2G内存,此时可支持400万并发回话，升级能力:F5 所有设备均可通过软件方式升级,在服务有效级软件包由F5公司提供，F5 NETWORKS已经发布其系统的最新版本BIG-IP V9.0,主要有以下特性:虚拟 IPV4 / IPV6 应用，加速Web应用高达3倍，减少66%多的基础架构成本，确保高优先级应用的性能，确保更高级别的可用性，大幅提高网络和应用安全性，强大的性能,简单的管理方式，无以匹敌的自适应能力能力和突破的性能表现力，其强大的HTTP压缩功能可以将用户下载时间缩短50%,节省80%的带宽，IP地址过滤和带宽控制:BIG-IP可以根据访问控制列表对进行过滤,并且针对某一关键应用进行带宽控制,确保关键应用的稳定运行，配置管理及系统报告:F5 BIG-IP提供WEB 界面配置方式和命令行方式进行配置管其中提供了丰富的系统报告,更可通过i-Control自行开发复杂的配置及报告生成

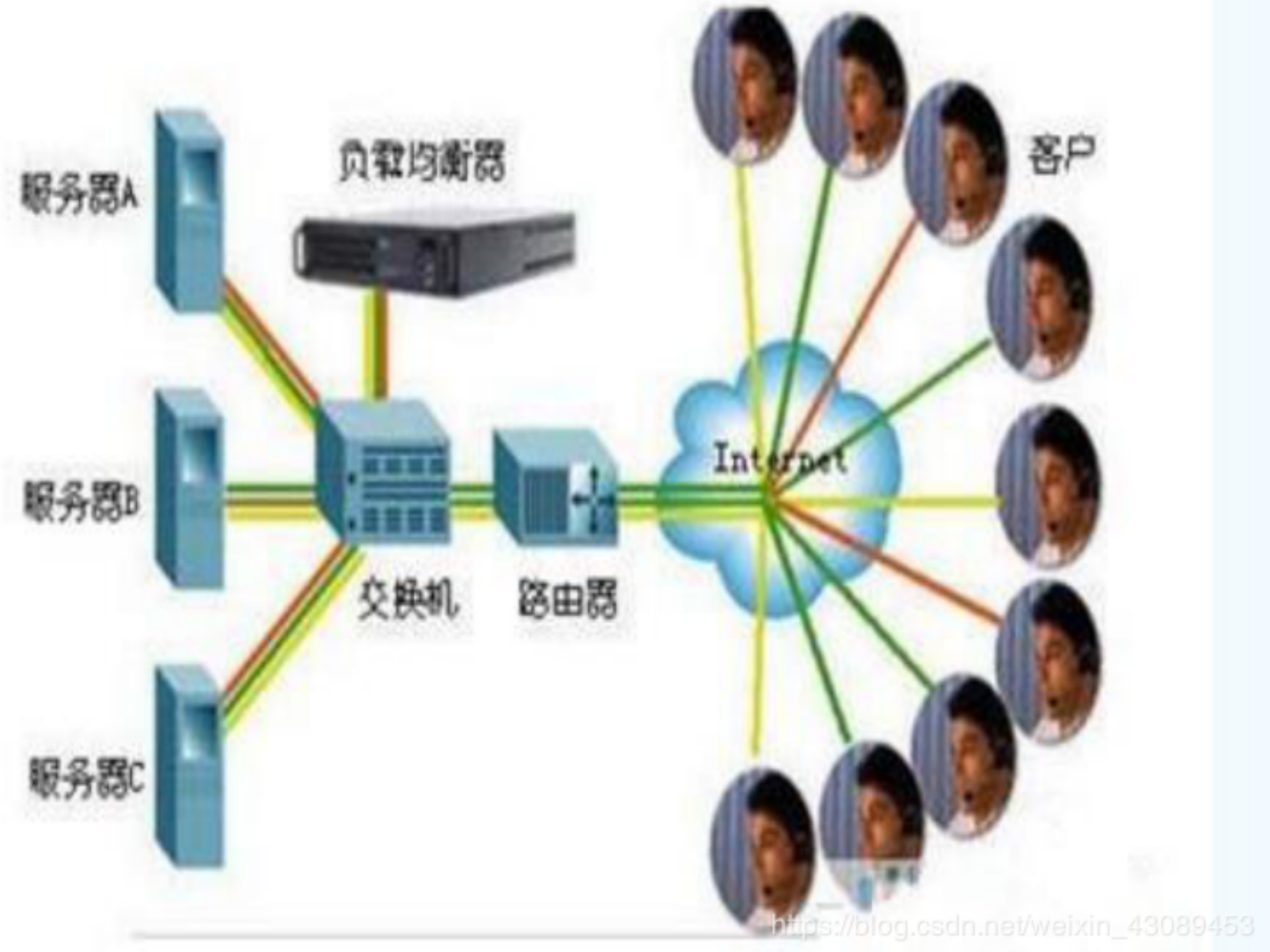
对我们管理系统应用环境来说，由于负载均衡器本身不需要对数据进行处理，性能瓶颈更多的是在于后台服务器，通常采用软负载均衡器已非常够用且好的软件源码授权使得我们可以非常灵活的设计，无逢的和我们管理系统平台相结合。

Virtual Server重要参数

F5的核心就是Virtual Server。

1、VS Type

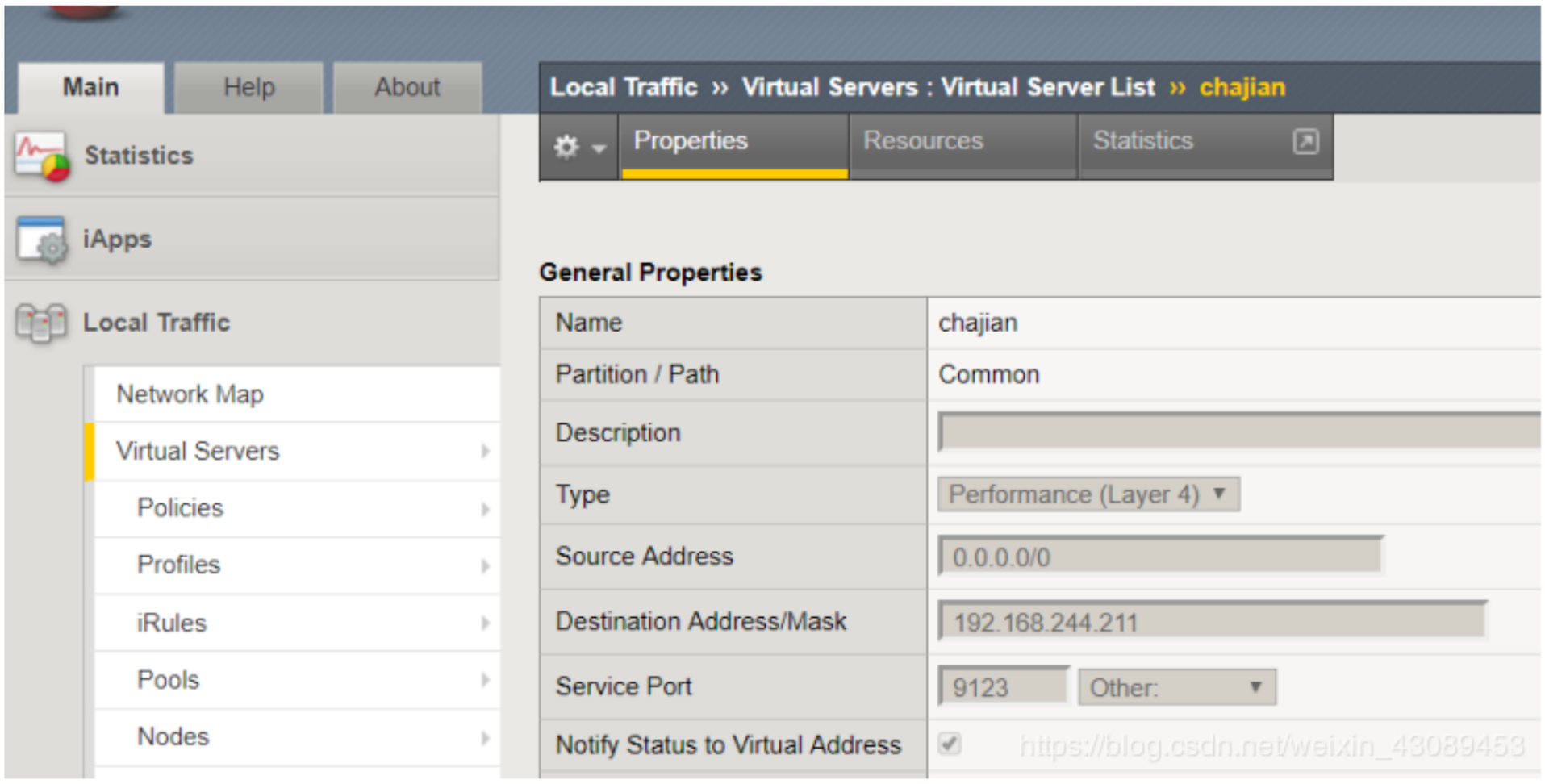
在配置VS时，VS的Type有Performance L4、Standard VS、Forwarding IP 和 Fast Http。一般企业中常见的是前三种，考虑到尽量减少F5负载均衡引入系统的影响，在可能的情况下，建议优先选用Performance L4类型的Virtual Server。在一些必须使用Standard的情况下，必然需要在F5设备上启用7层功能，Cookie会话保持、Session ID会话保持、Header会话保持、基于交易的长连接拆分等应用场景。另外，在应用系统需要使用F5实现Syn攻击防护时，可以采Standard Virtual Server。在明确后台应用基于HTTP协议时，建议在Standard的基础上关联BIGIP内置的标准HTTP Profile。对于非HTTP协议的应用，需要关联的其他Profile或者iRules根据实际的业务需求进行确定。



下面对每个VS的类型进行深入的说明：

第一种： Performance L4 模式（4层数据的转发）

Performance L4模式如图2所示，其中TMM只是负责客户端连接的分配和转发，不改变TCP连接中的任何参数，即客户端连接与服务器拦截是1：1的关系，一般企业中常是这种模式，因为转发速率快。但在一些7层数据包的情况下，如HTTP，建议使用Standard VS模式。



第二种 Standard VS模式

在这种模式下，客户端与服务器端的TCP连接完全独立，同时F5默认情况下以客户端源IP和后台建立连接，在打开SNAT的情况下用SNAT地址和后台建立连接。Standard VS的端口永远对外开放，无论后台是否有服务器在工作。也就是说，如果VS开放的端口是80，在Node A和Node B都down的情况下，虚IP的80还是可以telnet通的，只不过网页访问不了了。

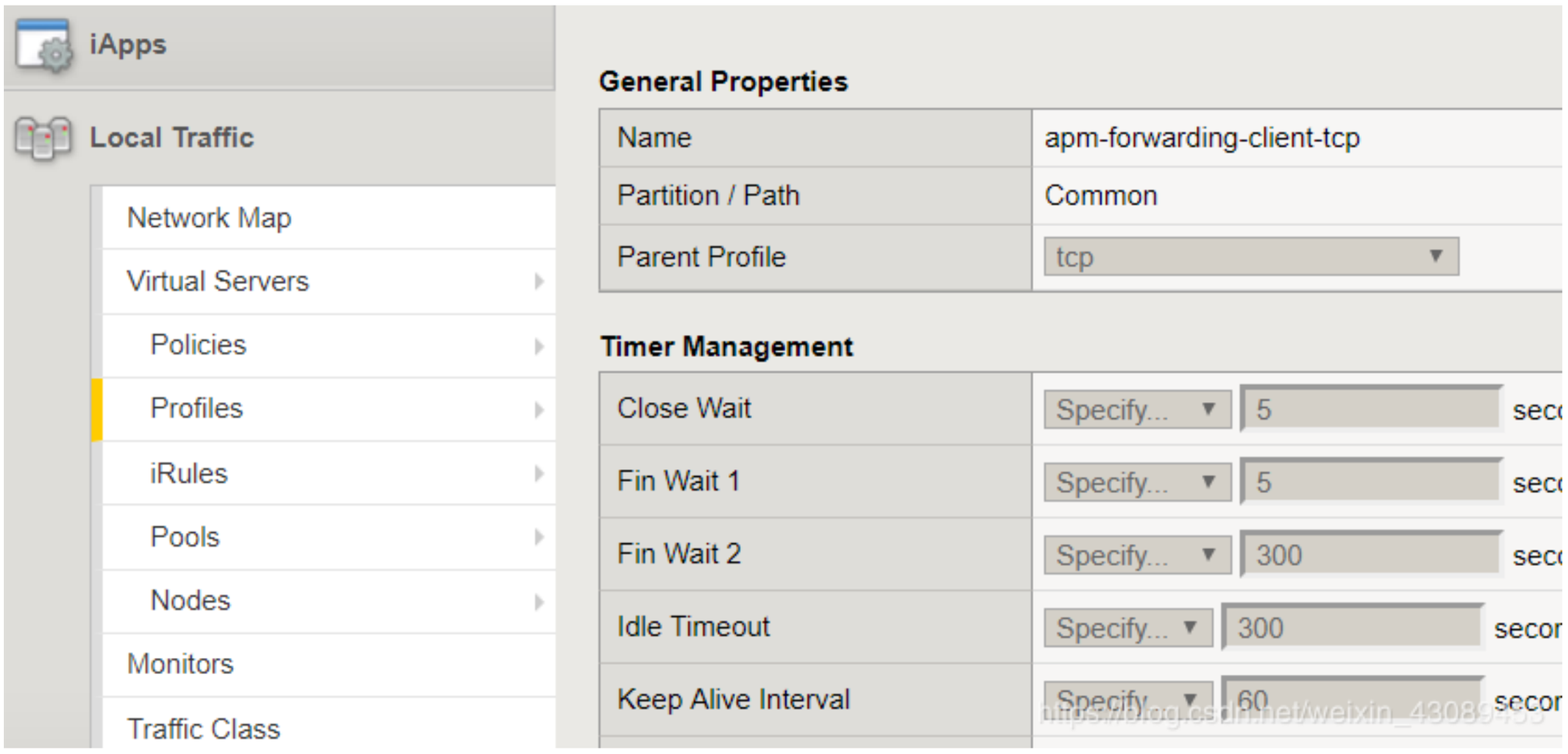
第三种： Forwarding IP

一般用于内外网连接，没有Pool Member，转发完全取决于本地路由。默认情况下，F5没有路由功能，需要建立一个全0的VS去开启F5的路由功能，其实如果想控制只有内网可以访问外网，而外网不能访问内网，可以通过调整“VLAN and Tunnel Traffic”参数来实现。

2. VS Profile

VS Profile 是依赖于VS的存在，是对于VS的流量进行格式化处理。如果VS上配置了TCP Profile，那么对于UDP的连接，F5是不会接受的。

tcp参数中Idel Timeout值（多长时间连接里面没有数据流量时就删除连接表）必须要与服务器相配合，否则会出现错误。如果F5上此值为150s，而IIs服



300s，就会产生大量错误。

3、 VS里面的Address Translation 和 Port Translation ，默认情况下都是 enabled。

Address Translation的含义是如果外面访问的主机和VS IP不一样，就需要开启此参数，比如VS IP地址是192.168.27.100，真实机器为192.168.27.10，要开启Address Translation，而企业应用中，这参数一般是开启的，除非特殊的上面介绍的Fowarding IP模式不需要开启。

Port Translation 参数的意思是VS地址是192.168.27.100的8080端口对应真实地址的80端口，那么需要开启Port Translation

4、SNAT Pool？？？

内网需要访问公网进行NAT转换。当配置SNAT AutoMap的时候，表示请求从哪个VLAN发出去，则SNAT的源地址为VLAN上的SelfIp，比如外网用户（192.168.27.1）访问内网服务器（192.168.192.10），在开启SNAT AutoMap的情况下，访问的源IP将转变为F5的内网SelfIP（192.168.192.2）去访问。当vlan上有多个SelfIP存在的时候，SNAT的源地址是在多个SelfIP之间轮询。

5、会话保持

在大多数电子商务的应用系统或者需要进行用户身份认证的在线系统中，一个客户与服务器经常经过多次的交互过程才能完成一笔交易或者是一个请求的由于这几次交互过程是密切相关的，服务器在进行这些交互过程的某一个交互步骤时，往往需要了解上一次交互过程的处理结果，服务器进行下一步操作时需要求所有这些相关的交互过程都由一台服务器完成，而不能被负载均衡器分散到不同的服务器上。

经验总结：

1、拿到F5首先就是要激活，通过向导可以很简单的进行激活，但是记住一定要能上网，最好在上架前完成激活工作。

2、打开浏览器使用https://192.168.1.245 设备管理ip可以登录到F5设备。默认用户名和密码均为admin。

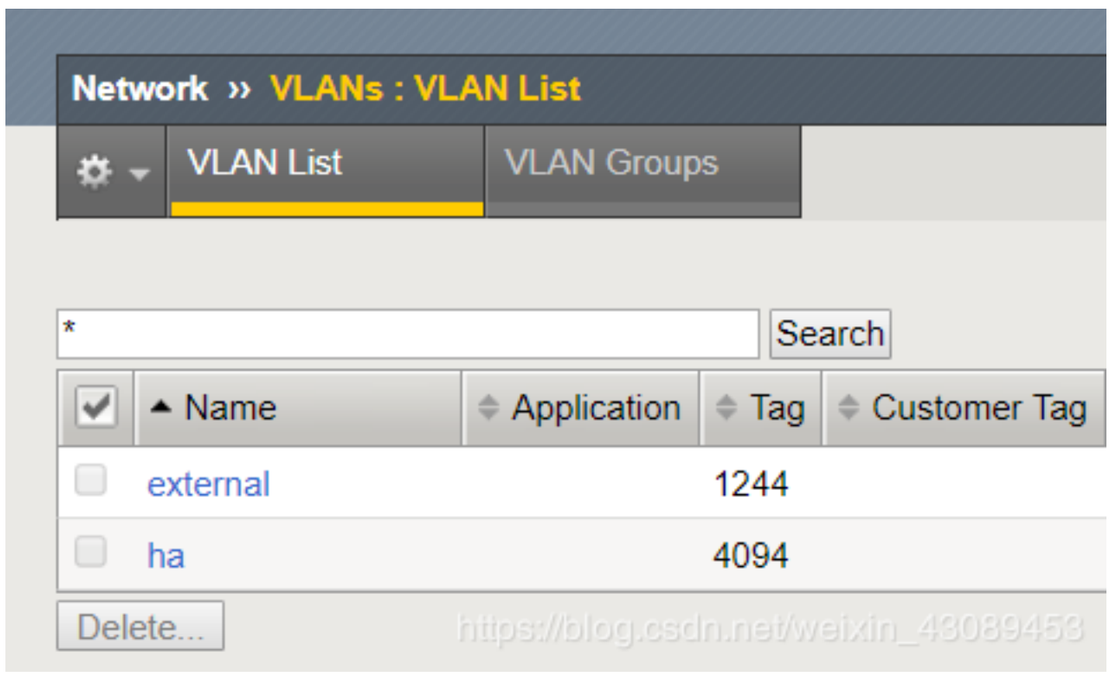
3、创建相应的VLAN，并将接口加入相应的VLAN，Network -> VLANS 。

Name： 设置这个VLAN的名字；

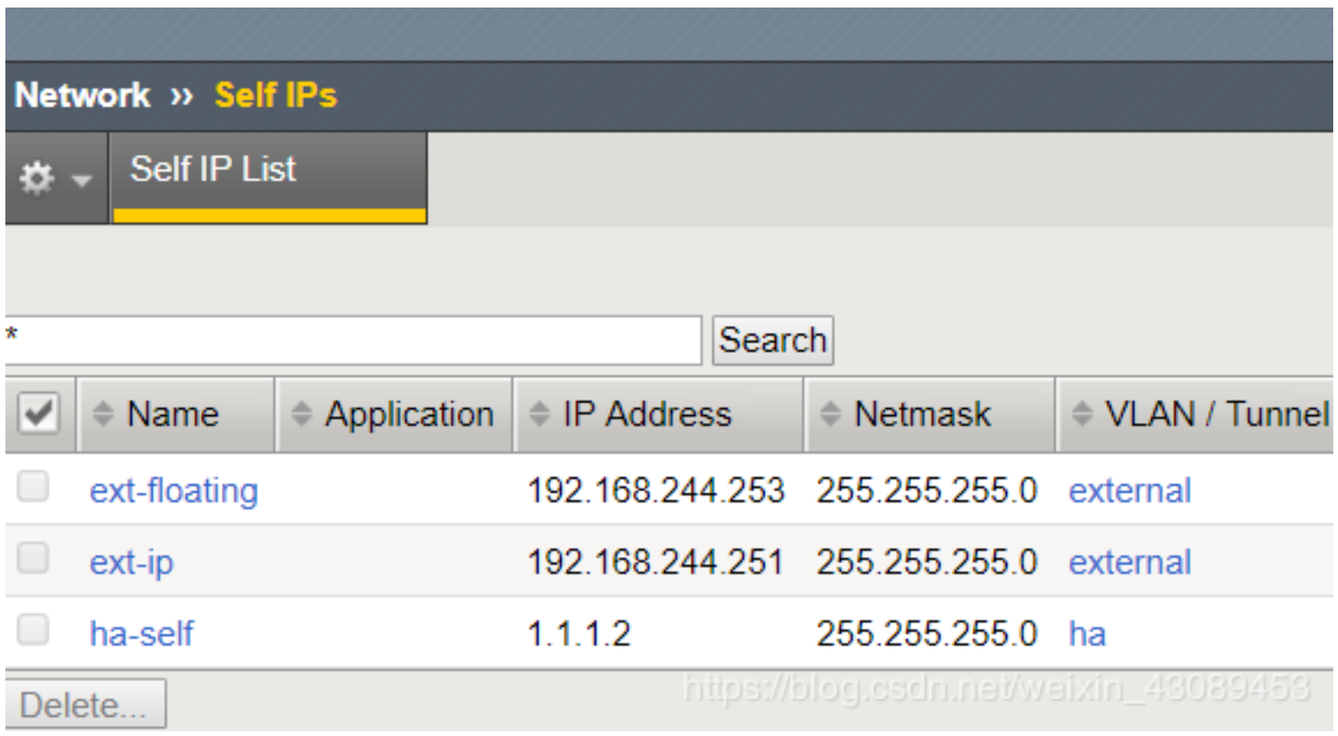
Tag: 保留为空；

Interface：定义Avalilable 中显示的端口有选择性的划分到这个vlan中，指定端口后，单击<< 选人 Untagged 栏即可。

点击 Finished 完成。



4、在划分完VLAN后，即可对每个VLAN进行IP地址的定义，方法如下：点击左侧导航条中的 Networks -> Self IPS。



5、配置路由，点击左侧导航条中的 Networks -> Routes .

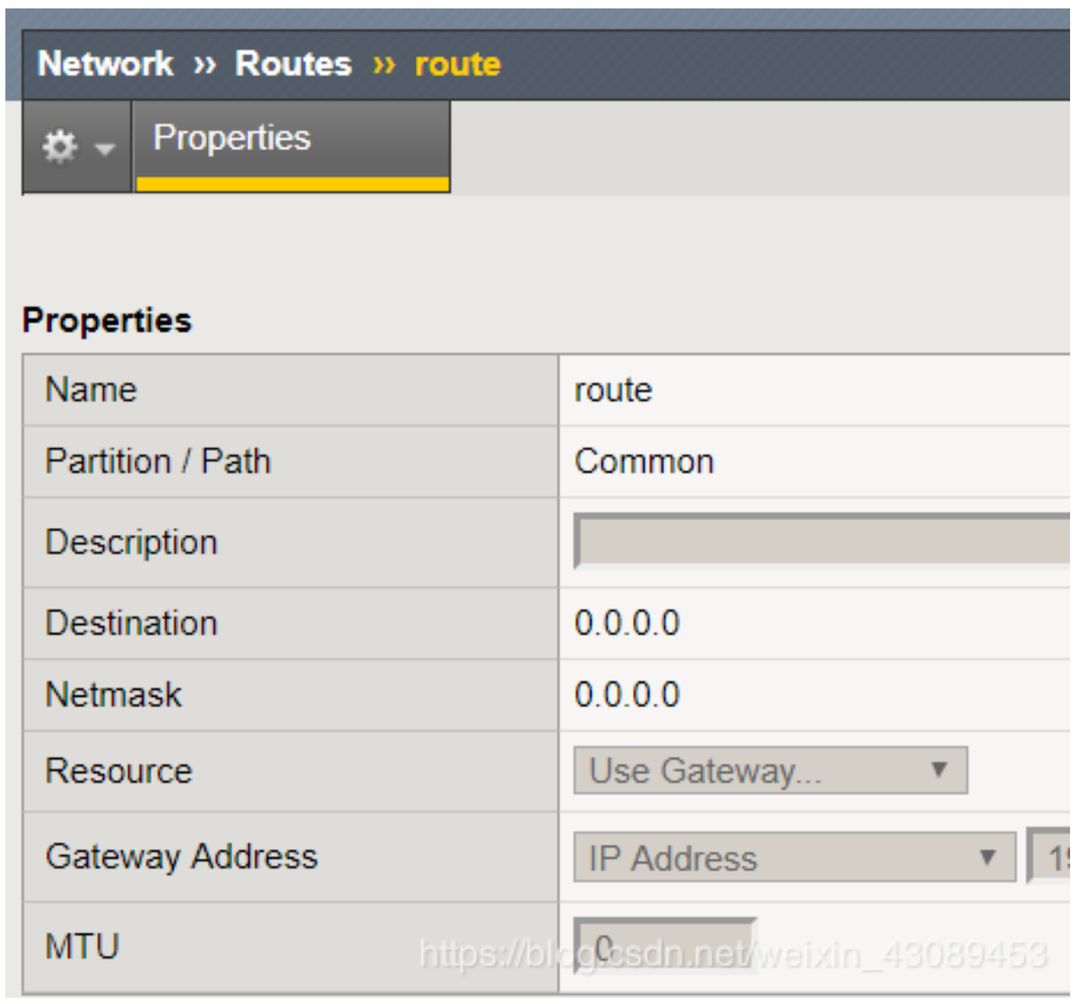
Type： 定义配置的是默认网关还是静态路由。

Destination: 定义目标网段。

Netmask : 定义目标网段的掩码;

Resource： 定义网关地址。

点击 Finished 完成。



6、Pool 配置：点击左侧导航条中的Local Traffic -> Virtual Servers -> Pools;

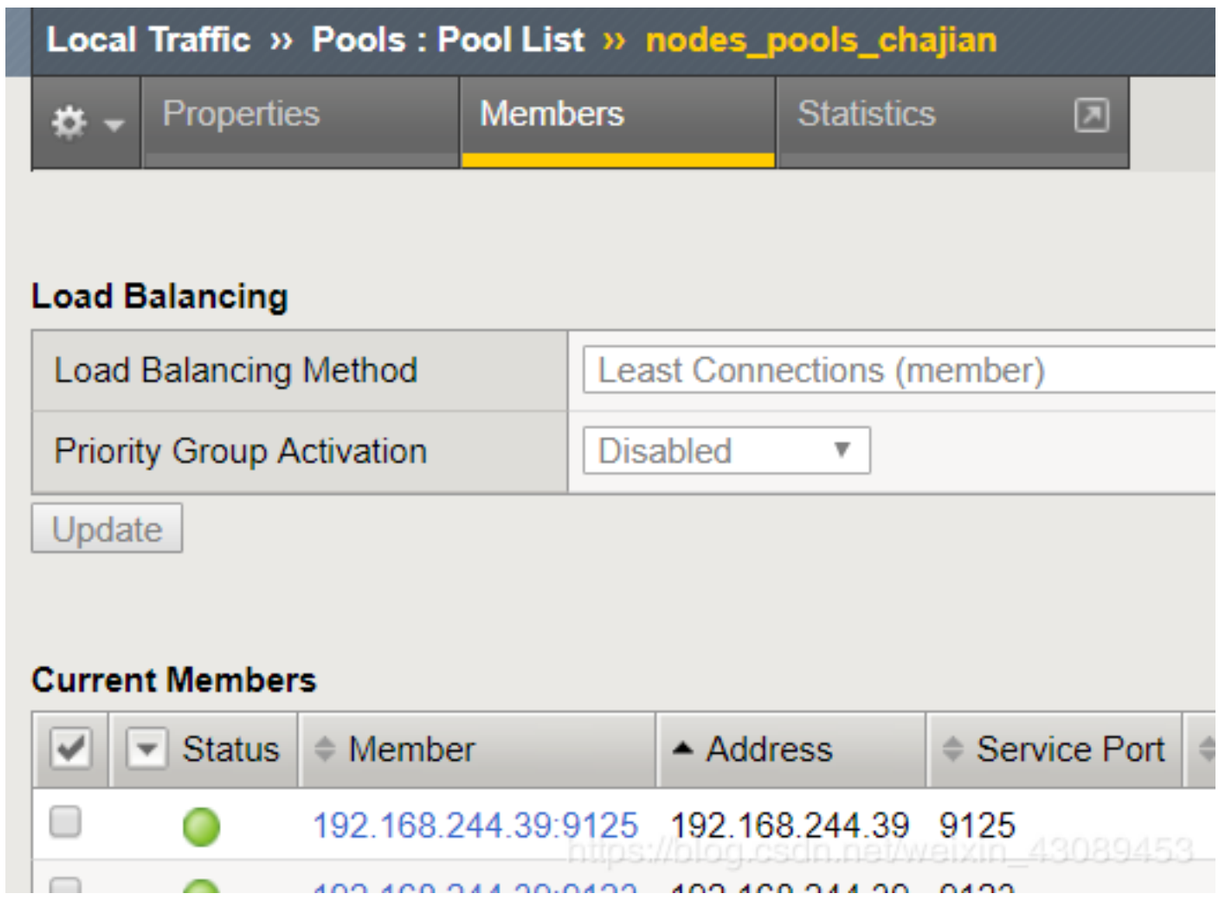
Name 定义创建的Pool的名字。

Health Monitors 定义该Pool使用的健康检查机制，此处为TCP。

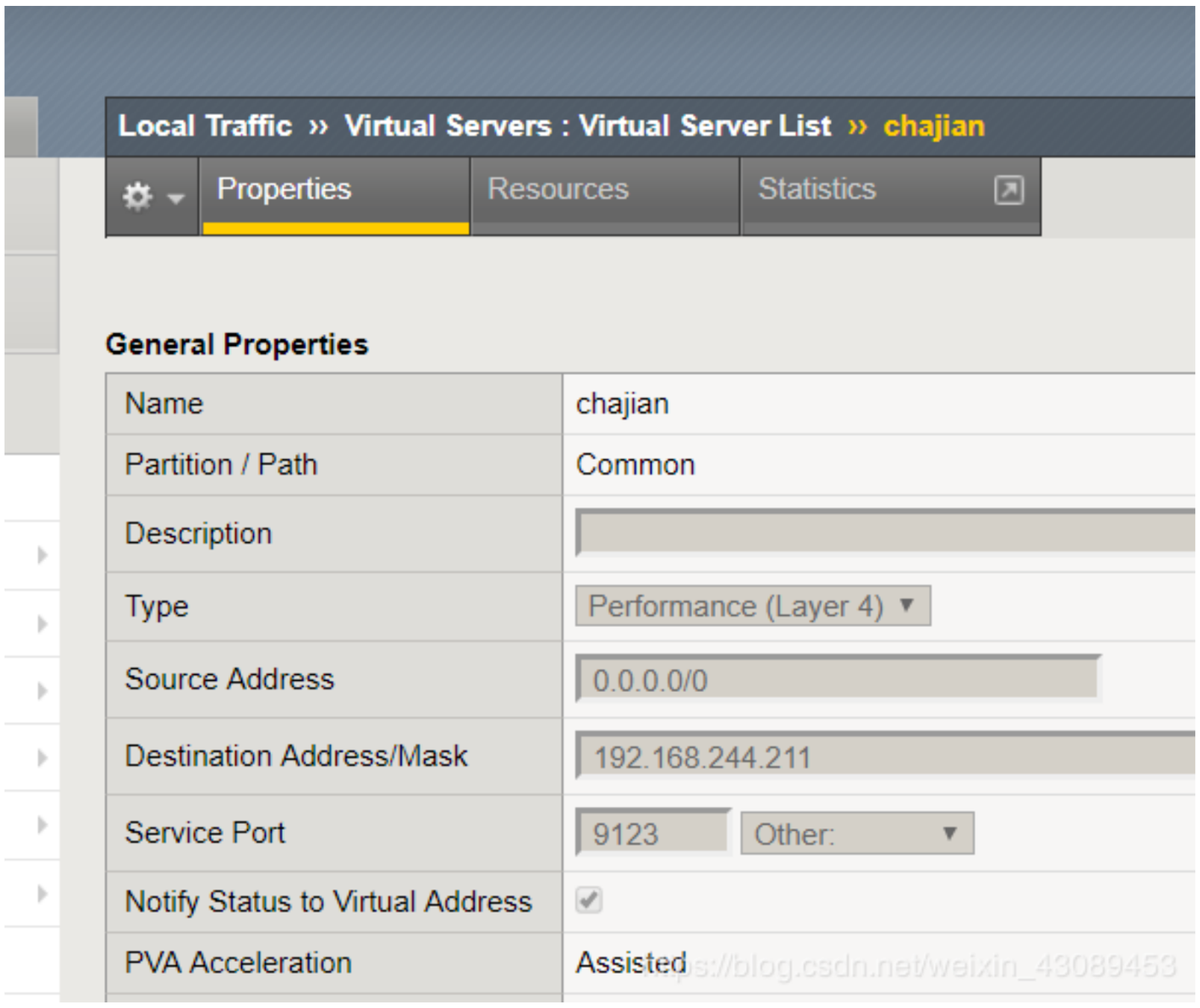
Load Balacing Method定义该Pool使用哪种负载均衡算法 --我们选用 observed-member（观察法）。

New Members 定义该pool下真实的服务器的IP和Port。

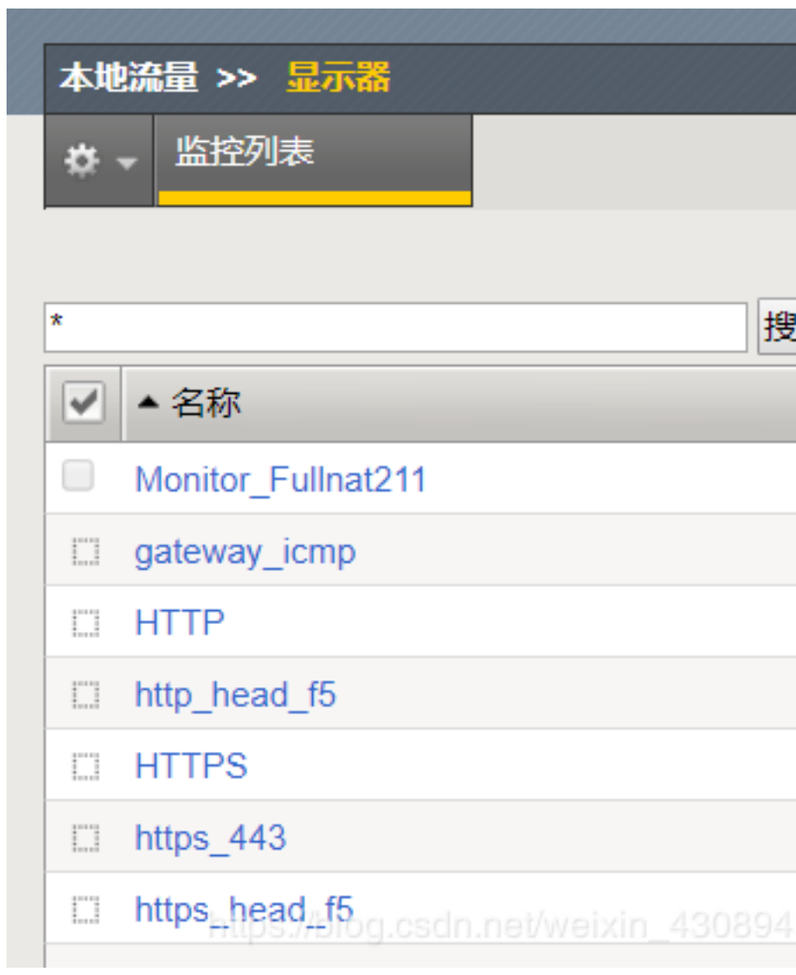
点击 Finished 完成。



7、Virtual Server 配置，Local Traffic -> Virtual Servers，这里面的参数可以参见之前介绍的进行填写，并将管理相应的Pool。并配置相应的F5轮询方式



的是轮询（RoundRobin）。



8、配置Monitor 的作用是检查服务器的健康状态，然后关联的相应的Pool，Local Traffic -> Monitors。

9、配置Redundant,这在前面已介绍。

近几年来，四到七层网络负载均衡首先在电信、移动、银行、大型网站等单位进行了应用，因为其网络流量瓶颈的现象最突出。目前在多家企业，随着