linux认证:Xined服务客户端与服务器的中介Linux认证考试

https://www.100test.com/kao_ti2020/583/2021_2022_linux_E8_AE_A4_E8_AF_c103_583317.htm Linux等操作系统在企业中承担客户端的角色其实还不多，大部分是利用Linux来做企业的应用服务器。不过这种现象正在逐渐转变。或许不久的将来，Linux操作系统会成为主流的客户端之一。但是在短时间内其还是主要作为Linux服务器的角色。为此Linux操作系统管理员平时的工作就离不开网络了。而在Linux操作系统中，Xined服务是其网络平台的一个守门神，其直接决定了 Linux操作系统的各种网络管理功能。xinetd服务负责接收客户端的网络服务请求，并且将客户端的请求发送到正确的服务程序。 一、Linux应用服务器配置要实现的需求。 Linux服务器之所以能够在服务器市场上跟微软相抗衡，除了其免费之外，主要还是因为其稳定与安全性上面跟微软有过之而不及。在这方面Linux操作系统的优点是数不胜数，笔者就不罗嗦了。笔者现在就结合网络管理这块内容，来谈谈Xined服务。 1、连接成功与失败的管理。为了安全的考虑，网络管理员一般要求在服务器上能够记录客户端连接的相关信息。如客户端连接应用服务器的时候，是否连接成功.如果连接成功的话，用户访问了哪些文件，以及进行了哪些操作等等。这些信息对于Linux系统管理员来说非常的重要。巧妇难为无米之炊，如果没有这些信息的话，Linux系统管理员的很多工作将无法展开。所以让应用服务器在提供相关网络服务的同时，记录这些信息是非常必要的。 2、相关服务的连接限制。在Windows操作系统中，相关应用服务都会有一些连接的限制。如

在Windows操作系统中，如果部署邮箱服务器的话，最多可以连接多少客户端等等。之所以要设置这个限制，主要是出于两方面的原因。一是操作系统厂家赚钱的一种工具，可以根据客户端的点数来进行收费.二也是出于服务性能的考虑。可以针对企业的不同需求，而推出可以运行不同客户端点数的操作系统。在保障企业需求的同时，也不影响服务的性能。在Linux服务器中也有类似的需求。 3、另外随着信息化应用越来越复杂，若光靠单台服务器有时候往往不能够完成一些复杂的任务。如现在网络部署中，最常见的一种情况就是把身分认证与应用服务器隔离开来。如上图所示，客户端向服务器请求某种应用服务的时候，服务器要求客户端先进行身份验证。只有通过了身份验证之后，才可以跟自己进行连接。这一方面身份的合法性认证有独立的第三方来负责，可以提高权威性.另一方面这身份认证与应用服务分开，可以提高应用服务的性能，让其能够全心全意提供应用服务层面的内容。 以上这些都是Linux服务器配置管理中的一些基本需求。这些需求在Windows服务器操作系统中是可以实现的。那么在Linux操作系统中是否可以实现呢?答案是肯定的。Xinetd服务就可以帮助系统管理员来实现这些需求。 二、Xinetd服务配置与管理要点。 根据笔者的经验，Xinetd服务的配置与管理要点主要有三个方面的内容。这四个方面的内容即是Linux服务器的管理核心，也是我们管理的重点。 一是日志管理相关的内容。这块内容主要包括两个方面，一是需要把日志存放在哪个地方.二是需要记录哪些内容。如果Linux服务器是企业的关键应用服务器，而且其保存的内容比较机密，那么把相关的日志放置在本机不是很好的方法。因为如果攻

击事件发生的话，则攻击者在退出应用服务器的时候，可以轻松修改事务日志的内容，把自己入侵过的痕迹清除掉。而且若服务器硬盘发生损坏，则系统管理员因为无法查询事务日志，也很难追踪问题的原因。为此把事务日志保存在本地并不是很合理的方法。通常情况下，笔者建议大家，如果应用服务器比较重要，那么最好能够把日志保存在独立的日志服务器中。在Linux服务器操作系统中可以实现这方面的需求。这主要是有Linux系统中的Xinetd服务来完成。这个服务中有一个log_type参数，可以重定向日志记录文件，将日志文件保存在系统管理员指定的主机上。如可以把这个参数设置为SYSLOG，则表示通过网络中独立的SYSLOG服务器来记录相关的日志。 日志文件的保存位置确定了，接下去就可以来考虑到底需要记录哪些必要的信息。在考虑这方面内容之前，系统管理员需要确定一件事情，即日志文件需要耗费服务器一定数量的资源，也就是说日志文件并不是越多越好，只要足够就行。所以如果简单的说，把所有信息都记录下来就好了，这往往不是明智的做法。作为系统管理员需要根据服务器的用途来判断，要在日志文件中记录哪些信息。如笔者认为，对于普通的服务器，只需要记录连接失败的信息即可。如通过设置 xinetd服务中的log_on_failure参数，可以让Linux操作系统将用户访问服务器失败的信息记录在相关的日志中。而对于服务器安全要求比较高的话，那么可以设置log_on_success参数，这可以让Linux操作系统即使在访问成功的时候也会记录客户端的主机与程序信息。笔者再次强调一下，在考虑日志中需要捕获哪些信息的时候，需要根据服务器的安全级别来进行考虑，决不是越多越好。 二是需要设

置单一服务在同一时间内提供客户端连接请求的最高上限。注意，这里指的是单一服务、同一时间。如在服务器中提供了邮箱与文件服务器两种不同的服务，则需要分别为他们设置客户端连接请求的最高上限。而不是他们的累计上限。这跟微软操作系统中的客户端最大连接数有一定的差异。在Windows操作系统中是一个总合的概念，而在Linux操作系统中则是单一服务的独立统计。不过有些Linux操作系统版本跟微软操作系统一样，也是累计计算的。在 Linux操作系统中可以通过Xinetd服务的instances参数来设置单一服务在同一时间内提供客户端连接请求的最高上限。这除了面所说的可以用来进行版权控制之外，还可以用来防止一些恶意的攻击。如拒绝服务式攻击是黑客常用的一种攻击程序，可以消耗目标计算机的资源，让其无法继续服务。虽然拒绝服务式攻击并不会损坏被攻击计算机内部的文件信息，但是会让服务器瘫痪。而他们就可以利用其他的服务器来充当这台被攻击瘫痪的服务器，以达到不可告人的目的。而通过设置这个单一服务在同一时间内提供客户端连接请求的最高上限，在可以避免这种攻击。如可以把instances参数设置为80，那么最多只有 80个客户端可以向这台服务器发送ping命令。如果超过这个客户端的数量，则Linux服务器会忽略其他的ping命令。而光凭80个客户端的ping 命令，是不会让Linux服务器崩溃的。为此如果系统管理员有版权控制或者防止DOS攻击的需要，则可以通过设置这个参数来实现。 三是必要时要限制外部到内部网络的连接速度。有时候系统管理员可能会把Linux服务器当作企业网络的一个安全网关来使用，或者当作NAT服务器来使用。此时Linux网络管理人员就需要配置xinetd服务

的cps参数。这个参数主要用来限制外部网络到内部网络的连接速度。如我们可以如下设置cps 50 30。这第一个参数是指每秒钟可以连接的速度(这里设置为50)。如果连接到内部网络的速度超过这个值的话(如达到80)，则这个服务就会暂时停止。第2 个参数30是指这个服务暂时停止后，系统等待重新启动服务的秒数。上面这个命令的含义，就是当连接速度超过50的话，Linxu服务器就会暂时停止这个服务。等到30秒以后再重新启动服务。这跟上面设置的客户端连接请求的最高上限一样，可以用来提高服务器的安全性，可以防止因为某个服务请求过多而造成服务器的瘫痪。不过参数在设置的时候比较难把握。系统管理员在部署Linux服务器的时候，需要在一段时间内进行观测，以确定这个参数合理的配置值。通常情况下，需要经过几次测试之后才能够取得一个合理的值。 另外百考试题最后需要强调的一点就是，虽然Linux操作系统中还有其他的方法可以实现类似的需求，如在应用服务器中实现。但是笔者还是建议大家通过Xinetd服务来实现。因为这个应用服务只是起到监听、转发的功能，而并没有运行特定的服务。为此采用这种管理机制，可以优化应用服务的性能。因为应用服务有xinetd服务来帮助监听客户端的连接请求，所以不需要在每次启动的时候就加载大量的程序，可以提高服务器资源的利用率。现在不少在Linux 操作系统上开发的应用服务，就会直接引用xinetd服务来提高其自身的性能。