Linux系统中提高VSFTP服务器的安全性Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/619/2021_2022_Linux_E7_B3_BB_E7_BB_c103_619592.htm FTP是互联网应用中的一个元老级人物了，其方便企业用户文件的共享。但是，安全问题也一直伴随在FTP左右。如何防止攻击者通过非法手段窃取FTP服务器中的重要信息；如何防止攻击者利用FTP服务器来传播木马与病毒等等。这些都是系统管理员所需要关注的问题。这次我就已Linux操作系统平台上使用的最广泛的VSFTP为例，谈谈如何来提高FTP服务器的安全性。 一、禁止系统级别用户来登录FTP服务器。 为了提高FTP服务器的安全，系统管理员最好能够为员工设置单独的FTP帐号，而不要把系统级别的用户给普通用户来使用，这会带来很大的安全隐患。在 VSFTP服务器中，可以通过配置文件vsftpd.ftpusers来管理登陆帐户。不过这个帐户是一个黑名单，列入这个帐户的人员将无法利用其帐户来登录FTP服务器。部署好VSFTP服务器后，我们可以利用vi命令来查看这个配置文件，发现其已经有了许多默认的帐户。其中，系统的超级用户root也在其中。可见出于安全的考虑，VSFTP服务器默认情况下就是禁止root帐户登陆FTP服务器的。如果系统管理员想让root等系统帐户登陆到FTP服务器，则知需要在这个配置文件中将root等相关的用户名删除即可。不过允许系统帐户登录FTP服务器，会对其安全造成负面的影响，为此我不建议系统管理员这么做。对于这个文件中相关的系统帐户管理员最好一个都不要改，保留这些帐号的设置。 如果出于其他的原因，需要把另外一些帐户也禁用掉，则可以把帐户名字加入到这个文

件中即可。如在服务器上可能同时部署了FTP服务器与数据库服务器。那么为了安全起见，把数据库管理员的帐户列入到这个黑名单，是一个不错的做法。 二、加强对匿名用户的控制。 匿名用户是指那些在FTP服务器中没有定义相关的帐户，而FTP系统管理员为了便于管理，仍然需要他们进行登陆。但是他们毕竟没有取得服务器的授权，为了提高服务器的安全性，必须要对他们的权限进行限制。在VSFTP服务器上也有很多参数可以用来控制匿名用户的权限。系统管理员需要根据FTP服务器的安全级别，来做好相关的配置工作。需要说明的是，匿名用户的权限控制的越严格，FTP服务器的安全性越高，但是同时用户访问的便利性也会降低。故最终系统管理员还是需要在服务器安全性与便利性上取得一个均衡。 下面是我推荐的几个针对匿名用户的配置，大家若不清楚该如何配置的话，可以参考这些配置。这些配置兼顾了服务器的安全与用户的使用便利。 一是参数anon_world_readable_only.这个参数主要用来控制匿名用户是否可以从FTP服务器上下载可阅读的文件。如果FTP服务器部署在企业内部，主要供企业内部员工使用的话，则最好把这个参数设置为YES.然后把一些企业常用表格等等可以公开的文件放置在上面，让员工在匿名的情况下也可以下载这些文件。这即不会影响到FTP服务器的安全，而且也有利于其他员工操作的便利性上。 二是参数anon_upload_enable.这个参数表示匿名用户能否在匿名访问的情况下向FTP服务器上传文件。通常情况下，应该把这个参数设置为 No.即在匿名访问时不允许用户上传文件。否则的话，随便哪个人都可以上传文件的话，那对方若上传一个病毒文件，那企业不是要

遭殃了。故应该禁止匿名用户上传文件。但是这也有例外。如有些企业通过FTP协议来备份文件。此时如果企业网络的安全性有所保障的话，可以把这个参数设置为YES，即允许操作系统调用FTP命令往FTP服务器上备份文件。在这种情况下，为了简化备份程序的部署，往往采用匿名访问。故需要在FTP服务器上允许匿名用户上传文件。 三是参数anon_other_write_enable与参数anon_mkdir_write_enable.这两个参数主要涉及到匿名用户的一些比较高级的权限。如第一个参数表示匿名用户具有上传和建立子目录之外的权限，如可以更改FTP服务器上文件的名字等等。而第二个参数则表示匿名用户可以在特定的情况下建立子目录。这些功能都会影响到FTP服务器的安全与文件的安全。为此除非有特别需要的原因，否则的话都应该把这些权限禁用掉。即把这些参数的值设置为NO.我认为，除非FTP服务器是系统管理员拿来玩玩的，可以开启这些参数。否则的话，还是把这些参数设置为NO为好，以提高FTP服务器的安全。 总的来说，对于匿名用户的控制要遵循权限最小原则。因为匿名用户是FTP服务器没有授权的用户，故无法进行深级别的权限访问控制。为此只有通过这些基本参数来实现对其的控制。 三、做好目录的控制。 通常情况下，系统管理员需要为每个不同的用户设置不同的根目录。而为安全起见，不让不同用户之间进行相互的干扰，则系统管理员需要设置不让用户可以访问其他用户的根目录。如有些企业为每个部门设置了一个FTP帐户，以利于他们交流文件。那么销售部门Sales有一个根目录sales；仓库部门有一个根目录 Ware.作为销售员工来说，他们可以访问自己根目录下的任何子目录，但是无法访问仓库用户的

根目录Ware.如此的话，销售部门员工也就无法访问仓库用户的文件了。可见，通过限制用户访问根目录以外的目录，可以防止不同用户之间相互干扰，以提高FTP服务器上文件的安全。为了实现这个目的，可以把参数 chroot_local_user设置为NO.如此设置后，所有在本地登陆的用户都不可以进入根目录之外的其他目录。不过在进行这个控制的时候，最好能够设置一个大家都可以访问的目录，以存放一些公共的文件。我们既要保障服务器的安全，也不能够因此影响到文件的正常共享交流。 四、进行传输速率的限制。 有时候为了保障FTP服务器的稳定运行，需要对其文件上传下载的速率进行限制。如在同一台服务器上，分别部署了FTP服务器、邮件服务器等等。为了这些应用服务能够和平共处，就需要对其的最大传输速率进行控制。因为同一台服务器的带宽是有最大限制的。若某个应用服务占用比较大的带宽时，就会对其他应用服务产生不利的影响，甚至为导致其他应用服务无法正常相应用户的需求。再如有时候FTP用途的不同，也需要设置最大速率的限制。如FTP同时作为文件备份与文件上传下载等用途，那么为了提高文件备份的效率，缩短备份时间就需要对文件上传下载的速率进行最大值的限制。 为了实现传输速率的限制，系统管理员可以设置local_max_rate参数。默认情况下，这个参数是不启用的，即没有最大速率的限制。不过基于以上这些原因，我还是建议各位系统管理员在把FTP服务器投入生产运营之前能够先对这个参数进行设置。防止因为上传下载耗用了过多的带宽而对其他应用服务产生负面的影响。系统管理员需要在各个应用服务之间取得一个均衡，合理的分配带宽。至少要保证各个应用服务能够正

常响应客户的请求。另外在有可能的情况下，需要执行错峰运行。如在一台主机上同时部署有邮件服务器与FTP服务器。而FTP服务器主要用来进行文件备份。那么为了防止文件备份对邮件收发产生不利影响（因为文件备份需要比较大的带宽会在很大程度上降低邮件收发的速度），最好能够把文件备份与邮件收发的高峰时期分开来。如一般情况下早上上班时是邮件收发的高峰时期，那就不要利用FTP服务来进行文件备份。而中午休息的时候一般收发邮件就比较少了。此时就可以利用FTP来进行文件备份。所以把FTP服务器与其他应用服务错峰运行，那么就可以把这个速率设置的大一点，以提高FTP服务的运行效率。当然，这对系统管理员提出了比较高的要求。因为系统管理员需要分析各种应用，然后再结合服务器的部署，来进行综合. 