**Linux系统 vsftpd服务加固**

# 1.安装补丁

备份vsftp应用配置，联系操作系统厂商，获取最新版vsftp软件包，升级安装在<http://vsftpd.beasts.org/#download> 下载最新版vsftp源码包，编译安装，或者使用yum update vsftpd 升级更新。

# 2.禁用匿名登录服务

1).添加一个新用户 test，并配置强密码

1. useradd -d /home -s /sbin/nologin test
2. 其中/sbin/nologin 参数表示不能登录Linux shell环境
3. test为举例账号
4. passwd test ---配置强密码，密码建议：8位以上，包括大小写字母、特殊字符、数字混合体，建议不要使用生日、姓名拼音等常见字符串作为密码

2)修改配置文件 vsftpd.conf

1. #vim /etc/vsftpd/vsftpd.conf
2. anonymous\_enable=NO -----配置为NO为禁止匿名登录，必须要创建用户认证后登录

# 3.禁止显示banner信息

修改VSFTP配置文件vsftpd.conf，修改以下语句ftpd\_banner=Welcome重新启动vsftp后，查看Banner

1. >ftp 192.168.10.200
2. Connected to 192.168.10.200.
3. 220 Welcome
4. User (192.168.10.200:(none)):

# 4.限制FTP登录用户

在ftpusers和user\_list文件中列举的用户都是不允许访问FTP服务的用户，例如：root、bin、daemon等，除了需要登录FTP的用户外，其余用户都应该添加到这个拒绝列表中

# 5.限制FTP用户目录

1. 修改vsftp配置文件vsftpd.conf，修改以下行
2. chroot\_list\_enable=YES
3. chroot\_list\_file=/etc/vsftpd/chroot\_list
4. 新建/etc/vsftpd/chroot\_list，添加用户名，如：
5. user1
6. #表示user1登录FTP后，只允许在user1用户的home目录中活动

# 6.修改监听地址和默认端口

1. 修改vsftp配置文件vsftpd.conf，设置监听1.1.1.1地址的8888端口
2. listen\_address=1.1.1.1
3. listen\_port=8888

# 7.启用日志记录

1. 修改vsftp配置文件vsftpd.conf，修改以下行，启用日志记录
2. xferlog\_enable=YES
3. xferlog\_std\_format=YES
4. 如果需要自定义日志存放位置，可以修改以下行
5. xferlog\_file=/var/log/ftplog

# 8.其他安全配置

1. 限制连接数
2. max\_clients=100
3. max\_per\_ip=5
4. 限制传输速度
5. anon\_max\_rate=81920
6. local\_max\_rate=81920

# 9 其他建议

1.如果不需要使用该服务，建议您关停FTP服务

2.强烈建议不要将此类型服务开放在互联网外，您可以使用[VPN](https://market.aliyun.com/products/56820014?spm=5176.doc25475.416540.238.K7pSVM#ymk=%7B%22pageIndex%22:1,%22pageSize%22:10,%22saleMode%22:0,%22categoryId%22:56812015%7D)安全接入手段链接到文件类型的服务器端，同时使用[安全组](https://help.aliyun.com/document_detail/25475.html?spm=5176.doc25470.6.204.SlE11A) 控制访问源IP