centos7系统配置记录SFTP操作日志

1、修改ssh配置

[root@elk-node2 ~]# vim /etc/ssh/sshd_config
大概132行把下面这个句注释掉

#Subsystem	sftp	/usr/libexec/openssh/sftp-server
添加以下内容

Subsystem sftp /usr/libexec/openssh/sftp-server -l INFO -f local5

LogLevel INFO

2、修改rsyslog配置

[root@elk-node2 ~]# vim /etc/rsyslog.conf
添加以下内容

auth,authpriv.*,local5.* /var/log/sftp.log

3、重启服务

[root@elk-node2 ~]# systemctl restart sshd
[root@elk-node2 ~]# systemctl restart rsyslog

4、用FTP工具连接查看日志

[root@elk-node2 ~]# tail /var/log/sftp.log
Aug 5 23:01:49 elk-node2 sshd[1341]: pam_unix(sshd:session): session opened for user root by (uid=0)
Aug 5 23:01:49 elk-node2 sftp-server[1343]: session opened for local user root from [192.168.247.1]
Aug 5 23:01:49 elk-node2 sftp-server[1343]: opendir "/root"
Aug 5 23:01:49 elk-node2 sftp-server[1343]: closedir "/root"
Aug 5 23:01:56 elk-node2 sftp-server[1343]: remove name "/root/135.txt"
Aug 5 23:01:56 elk-node2 sftp-server[1343]: opendir "/root"
Aug 5 23:01:56 elk-node2 sftp-server[1343]: closedir "/root"
Aug 5 23:01:59 elk-node2 sftp-server[1343]: session closed for local user root from [192.168.247.1]
Aug 5 23:01:59 elk-node2 sshd[1341]: pam_unix(sshd:session): session closed for user root
Aug 5 23:01:59 elk-node2 systemd-logind: Removed session 7.