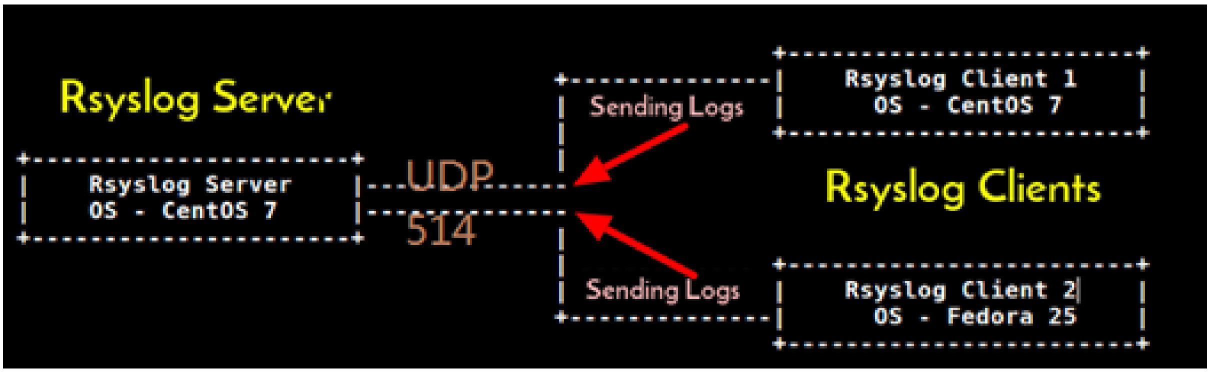
RSYSLOG SERVER

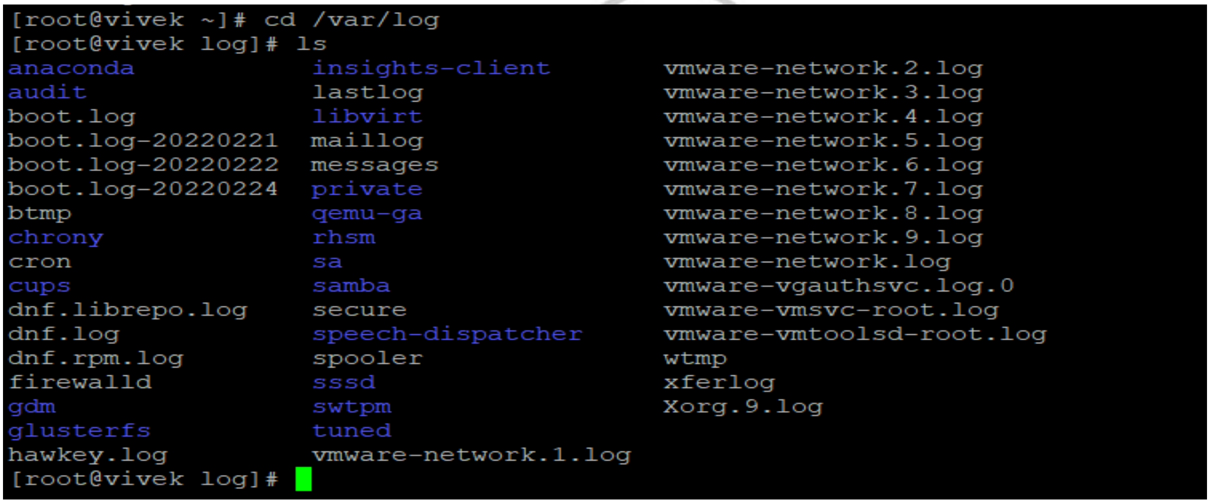
Rsyslog is an open-source software utility used on UNIX and Unix-like computer systems for forwarding log messages in an IP network. ...

RSYSLOG configuration log → /etc/rsyslog.conf

Port no → 514

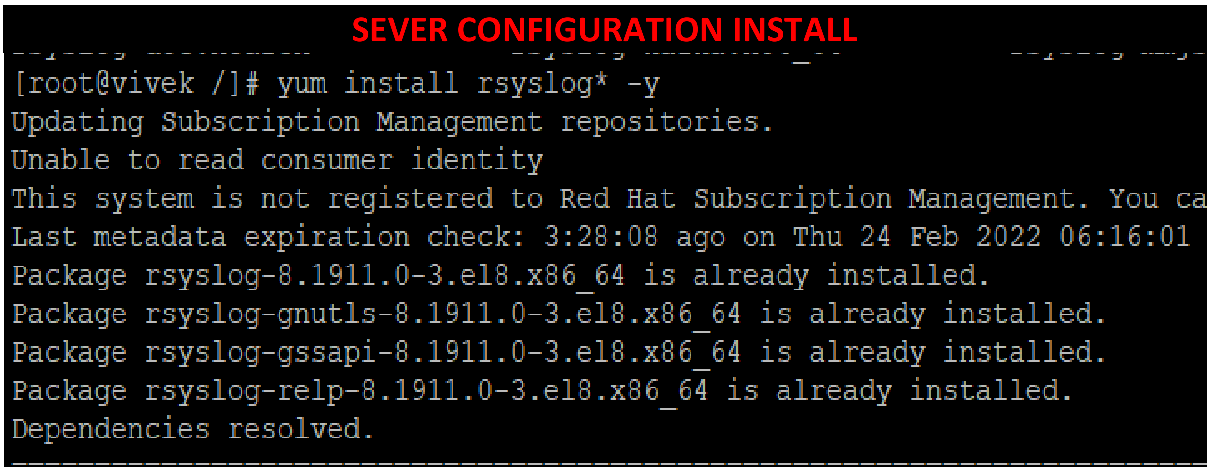


SSH TELNET: - /var/log/secure
Crontab: - /var/log/cron
Mail server: - /var/log/maillog



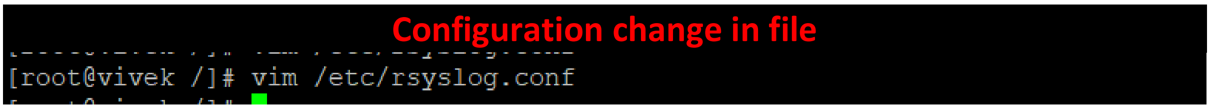
```
[root@vivek ~]# cd /var/log
[root@vivek log]# ls
anaconda             insights-client        vmware-network.2.log
audit                lastlog                vmware-network.3.log
boot.log             libvirt                vmware-network.4.log
boot.log-20220221    maillog                vmware-network.5.log
boot.log-20220222    messages               vmware-network.6.log
boot.log-20220224    private                vmware-network.7.log
btmp                 qemu-ga                vmware-network.8.log
chrony               rhsm                   vmware-network.9.log
cron                 sa                     vmware-network.log
cups                 samba                  vmware-vgauthsvc.log.0
dnf.librepo.log      secure                 vmware-vmsvc-root.log
dnf.log              speech-dispatcher      vmware-vmtoolsd-root.log
dnf.rpm.log          spooler                wtmp
firewalld            sssd                   xferlog
gdm                  swtpm                  Xorg.9.log
glusterfs            tuned
hawkey.log           vmware-network.1.log
[root@vivek log]#
```

SEVER CONFIGURATION INSTALL

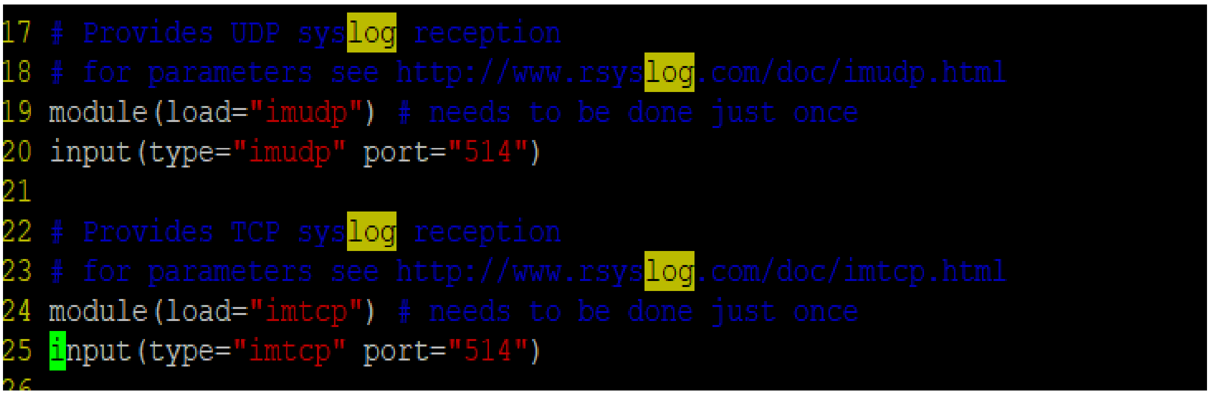


```
[root@vivek /]# yum install rsyslog* -y
Updating Subscription Management repositories.
Unable to read consumer identity
This system is not registered to Red Hat Subscription Management. You ca
Last metadata expiration check: 3:28:08 ago on Thu 24 Feb 2022 06:16:01
Package rsyslog-8.1911.0-3.el8.x86_64 is already installed.
Package rsyslog-gnutls-8.1911.0-3.el8.x86_64 is already installed.
Package rsyslog-gssapi-8.1911.0-3.el8.x86_64 is already installed.
Package rsyslog-relp-8.1911.0-3.el8.x86_64 is already installed.
Dependencies resolved.
```

Configuration change in file

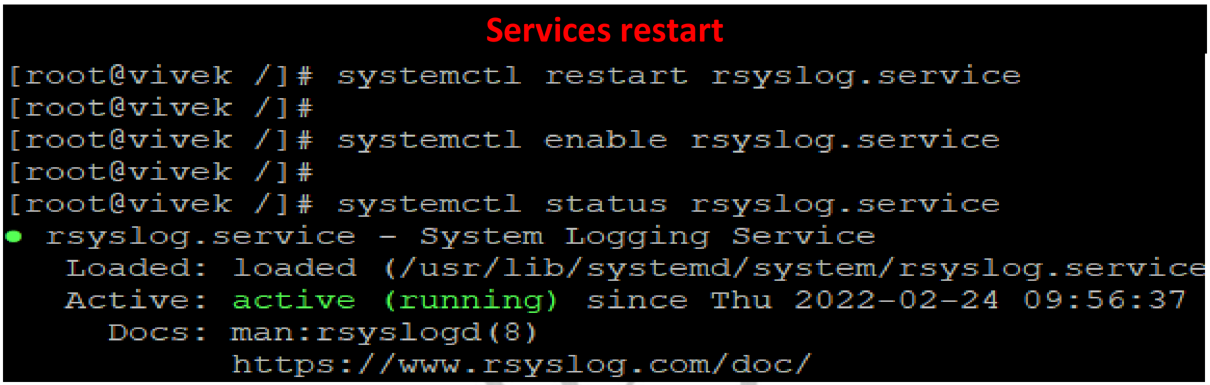


```
[root@vivek /]# vim /etc/rsyslog.conf
```



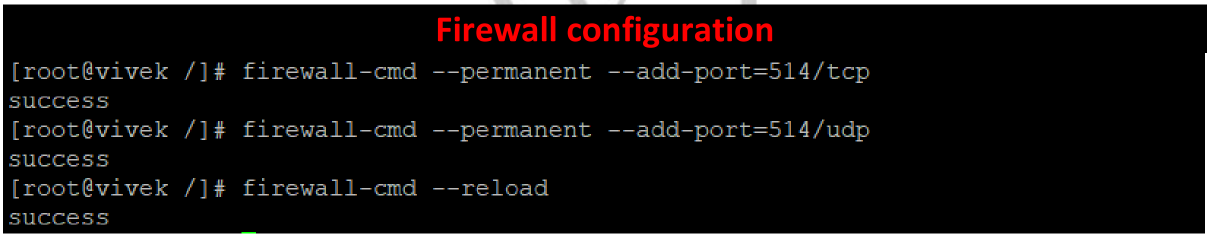
```
# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")

# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")
```

Services restart



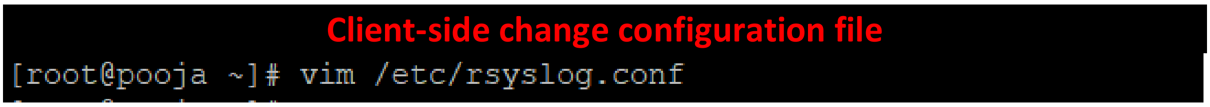
```
[root@vivek /]# systemctl restart rsyslog.service
[root@vivek /]#
[root@vivek /]# systemctl enable rsyslog.service
[root@vivek /]#
[root@vivek /]# systemctl status rsyslog.service
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service
   Active: active (running) since Thu 2022-02-24 09:56:37
     Docs: man:rsyslogd(8)
           https://www.rsyslog.com/doc/
```

Firewall configuration

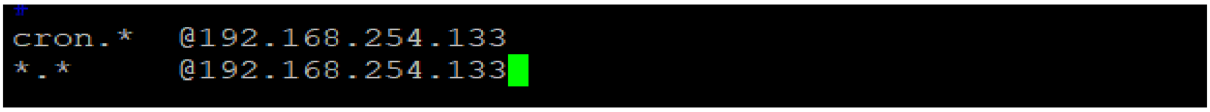


```
[root@vivek /]# firewall-cmd --permanent --add-port=514/tcp
success
[root@vivek /]# firewall-cmd --permanent --add-port=514/udp
success
[root@vivek /]# firewall-cmd --reload
success
```

Client-side change configuration file

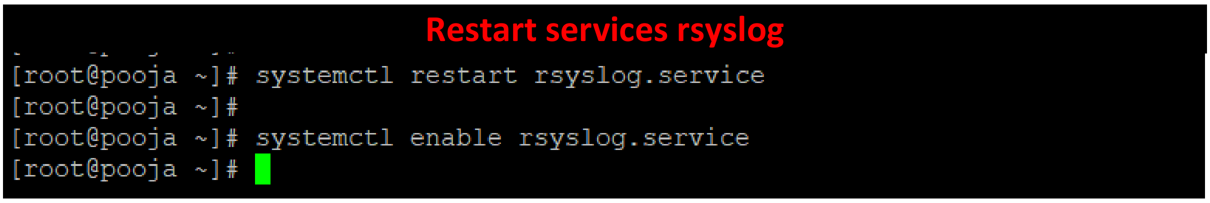


```
[root@pooja ~]# vim /etc/rsyslog.conf
```



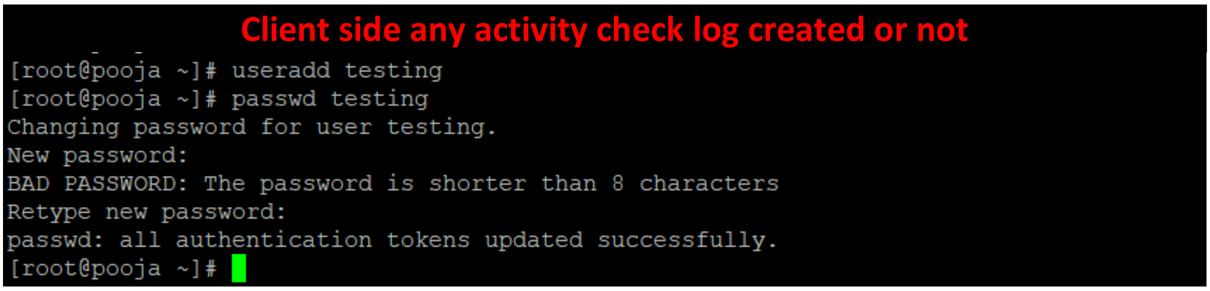
```
cron.*   @192.168.254.133
*.*      @192.168.254.133
```

Restart services rsyslog



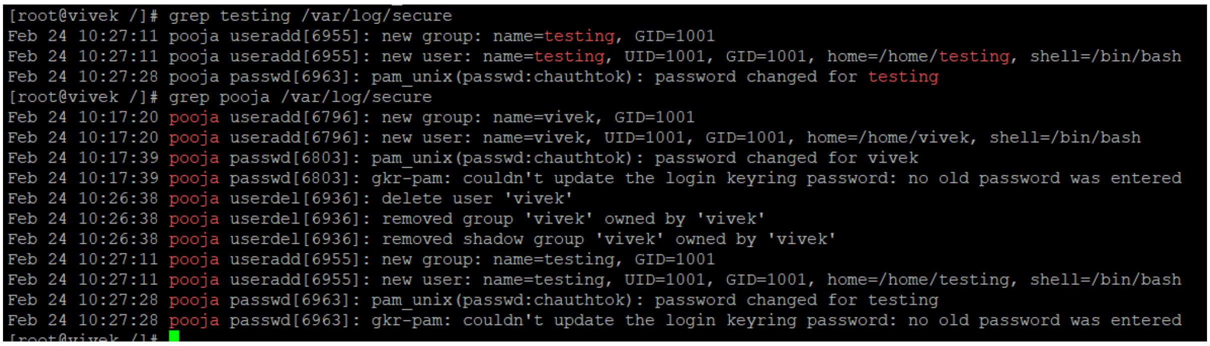
```
[root@pooja ~]# systemctl restart rsyslog.service
[root@pooja ~]#
[root@pooja ~]# systemctl enable rsyslog.service
[root@pooja ~]#
```

Client side any activity check log created or not



```
[root@pooja ~]# useradd testing
[root@pooja ~]# passwd testing
Changing password for user testing.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@pooja ~]#
```

Check server side



```
[root@vivek /]# grep testing /var/log/secure
Feb 24 10:27:11 pooja useradd[6955]: new group: name=testing, GID=1001
Feb 24 10:27:11 pooja useradd[6955]: new user: name=testing, UID=1001, GID=1001, home=/home/testing, shell=/bin/bash
Feb 24 10:27:28 pooja passwd[6963]: pam_unix(passwd:chauthtok): password changed for testing
[root@vivek /]# grep pooja /var/log/secure
Feb 24 10:17:20 pooja useradd[6796]: new group: name=vivek, GID=1001
Feb 24 10:17:20 pooja useradd[6796]: new user: name=vivek, UID=1001, GID=1001, home=/home/vivek, shell=/bin/bash
Feb 24 10:17:39 pooja passwd[6803]: pam_unix(passwd:chauthtok): password changed for vivek
Feb 24 10:17:39 pooja passwd[6803]: gkr-pam: couldn't update the login keyring password: no old password was entered
Feb 24 10:26:38 pooja userdel[6936]: delete user 'vivek'
Feb 24 10:26:38 pooja userdel[6936]: removed group 'vivek' owned by 'vivek'
Feb 24 10:26:38 pooja userdel[6936]: removed shadow group 'vivek' owned by 'vivek'
Feb 24 10:27:11 pooja useradd[6955]: new group: name=testing, GID=1001
Feb 24 10:27:11 pooja useradd[6955]: new user: name=testing, UID=1001, GID=1001, home=/home/testing, shell=/bin/bash
Feb 24 10:27:28 pooja passwd[6963]: pam_unix(passwd:chauthtok): password changed for testing
Feb 24 10:27:28 pooja passwd[6963]: gkr-pam: couldn't update the login keyring password: no old password was entered
[root@vivek /]#
```