Chrooted SSH Access Setup for loguser

Secure SSH Access using Chroot for loguser

```
1. Create the Chroot Directory Structure
---------------------------------------
sudo mkdir -p /chroot/loguser
sudo chown root:root /chroot/loguser
sudo chmod 755 /chroot/loguser

2. Bind-Mount /logs/rsyslog into the Chroot Jail
-----------------------------------------------
sudo mkdir -p /chroot/loguser/logs/rsyslog
echo "/logs/rsyslog /chroot/loguser/logs/rsyslog none bind 0 0" | sudo tee -a /etc/fstab
sudo mount /chroot/loguser/logs/rsyslog

3. Create the Restricted User
-----------------------------
sudo mkdir -p /chroot/loguser/home/loguser
sudo useradd -d /home/loguser -s /bin/bash -M loguser
sudo passwd loguser
sudo usermod -L loguser

# Copy necessary binaries
sudo cp /bin/bash /chroot/loguser/bin/
ldd /bin/bash
sudo       cp       -v       /lib/x86_64-linux-gnu/{libtinfo.so.6,libdl.so.2,libc.so.6}
/chroot/loguser/lib/
sudo cp -v /lib64/ld-linux-x86-64.so.2 /chroot/loguser/lib64/

4. Configure SSH Daemon
-----------------------
Edit /etc/ssh/sshd_config and add:
Match User loguser
    ChrootDirectory /chroot/loguser
    ForceCommand internal-sftp
    AllowTCPForwarding no
    X11Forwarding no

# Set permissions
sudo chown root:root /chroot/loguser
sudo chmod 755 /chroot/loguser
sudo chown loguser:loguser /chroot/loguser/home/loguser

5. Restart SSH and Test
-----------------------
sudo systemctl restart sshd
ssh loguser@your_server_ip

Expected Result:
User is restricted to /logs/rsyslog and cannot access other parts of the system.
```