Steps For Changing SSH Port For Linux VMs

Please follow the steps below to safely update your SSH port:

Step 1:

Edit the SSH daemon configuration file:
sudo vim /etc/ssh/sshd_config

Step 2:

Locate the Port directive.
You will see **#Port 22**
Uncomment it by removing the **#** (if commented) and change it from **22** to your preferred new port.
Ensure you are editing /etc/ssh/sshd_config (not /etc/ssh/ssh_config).

Step 3:

Reload systemd daemon:
sudo systemctl daemon-reload

Step 4:

Restart SSH services:
sudo systemctl restart ssh

Step 5:

Verify the new port is listening:
sudo ss -tlnp | grep ssh

You should see SSH listening on the new port.

Then, test the new connection from your local machine using:
ssh ubuntu@102.164.38.21 -p <new_port>

CentOS/Fedora VMs

Step-by-Step Instructions

The following steps walk through changing the SSH port from the default **22** to a custom port, e.g., **2222**. Substitute your desired port number throughout.

Step 1: Choose a New Port Number

Select a port that is:

I. In the range 1024–4096 for a non-privileged port, or higher
II. Not already in use by another service
III. Allowed by your network/cloud security group

To check currently listening ports, run:

$ ss -tlnp

or

$ netstat -tlnp

Step 2: Edit the SSH Daemon Configuration

Open the SSH daemon configuration file using your preferred text editor:

$ sudo vi /etc/ssh/sshd_config

or

$ sudo nano /etc/ssh/sshd_config

Locate the following line (it may be commented out with a **#**):

#Port 22

Uncomment it and change the port number:

Port 2222

Save and close the file.

Step 3: Configure SELinux to Allow the New Port

CentOS/Fedora uses SELinux by default. You must inform SELinux that the new port is permitted for the SSH service, otherwise the daemon will fail to start.

Check the current SELinux status:

$ sestatus

Add the new port to the SELinux policy:

$ sudo semanage port -a -t ssh_port_t -p tcp 2222

Note: The 2222 above should be replaced by the new port number you created.

Verify the change was applied:

$ sudo semanage port -l | grep ssh

Expected output:

ssh_port_t tcp 2222, 22

Note: The 2222 above should be replaced by the new port number you created.

Step 4: Update Firewall Rules (firewalld)

By default, CentOS/Fedora uses **firewalld** to manage firewall rules. You must open the new port before restarting SSH.

Add the new port to the firewall:

$ sudo firewall-cmd --permanent --add-port=2222/tcp

Then, remove the old SSH port from firewalld (do this only after confirming the new port works):

$ sudo firewall-cmd --permanent --remove-service=ssh

$ sudo firewall-cmd --permanent --remove-port=22/tcp

Reload firewalld to apply changes:

$ sudo firewall-cmd --reload

Verify the port is now open:

$ sudo firewall-cmd --list-ports

Expected output:

2222/tcp

Note: The 2222 above should be replaced by the new port number you created.

Step 5: Restart the SSH Daemon

Restart the sshd service to apply the new port configuration:

$ sudo systemctl restart sshd

Confirm the service is running:

$ sudo systemctl status sshd

Check the service is now listening on the new port:

$ ss -tlnp | grep sshd

Expected output (example):

LISTEN 0 128 0.0.0.0:2222 0.0.0.0:* users:(("sshd",...,...))

Step 6: Test the New Port

Open a new terminal window or session and connect using the new port. Do NOT close your current session yet.

$ ssh -p 2222 your_user@your_server_ip

Additional **Success Criteria**

You can log in successfully via the new port in the new session.

Your existing session remains active.

Running ss -tlnp | grep sshd shows port 2222 (or your chosen port) listening.

Change RDP Port On Windows VMs

Step 1:

Press Windows + R to open the Run box.

Step 2:

Type 'regedit' and click OK.

Step 3:

Navigate through folders:

HKEY_LOCAL_MACHINE → System → CurrentControlSet → Control → Terminal Server → WinStations → RDP-Tcp

Step 4:

Double-click 'PortNumber', select Decimal, and enter a new port (e.g., 3390).

Step 5:

Open Windows Defender Firewall → Advanced settings.

Step 6:

Create a new inbound rule for your port (TCP).

Step 7:

Restart Remote Desktop service:

net stop termservice

net start termservice

Step 8:

Connect using IP:PORT

Eg. 192.168.1.10:3390

Verification Commands:

reg query "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v PortNumber

sc query termservice

netstat -an | findstr :3390

Test-NetConnection -ComputerName localhost -Port 3390

If TcpTestSucceeded : True → Success