Check Config Before Restarting SSH Daemon

Super quick advice today, but one of them pearls of experience that now and then saves your day. Learn how to check and confirm your recent changes to **SSH daemon** config file (**/etc/ssh/sshd_config**) won't break your remote **SSH** access.

Why Double-Checking Configs Is A Good Idea

I should probably start a special section of **Unix Tutorial** someday, just to talk about how and when things can go wrong. These things below would certainly belong to that section.

Why it's a good idea to check that your new config file is error free:

- avoid getting service outage (syntax error means service won't restart)
- prevent service malfunction (if you end up with only partial service functionality)
- don't get yourself locked out of service (or server, in case of broken SSH)

How To Check SSHd Config

I have shown you before how to test new SSHd config on a different port, but there's also a way to check primary config.

Here's how you do it:

```
greys@s2:~ $ sudo sshd -t
```

It will either return nothing, or complain about errors or highlight deprecated options, like this:

```
greys@s2:~ $ sudo sshd -t
/etc/ssh/sshd_config line 56: Deprecated option RSAAuthentication
```

That's all there is to it, enjoy!

See Also

- **SSH reference**
- **Passwordless SSH**
- SSHd on different port
- Basic SSH configuration
- **SSH port**
- **SSH port forwarding**
- Check SSH port status