Sudo ss –tulnpa

Sudo systemctl status ssh

Sudo ps –el | grep ssh

Sudo apt install openssh-server

managing and inspecting the **OpenSSH server** and its related services. Here's when and why you might use each command:

**1. sudo ss –tulnpa**

* **Purpose**: To display detailed information about network sockets (listening ports).
* **When to Use**:
  + To check if the SSH server (or any service) is listening on a specific port (usually port 22 for SSH).
  + Troubleshooting when SSH connections fail and you suspect the service isn't active or the port is blocked.
* **Output Highlights**:
  + t - TCP sockets.
  + u - UDP sockets.
  + l - Listening sockets.
  + n - Show numeric addresses (skip DNS resolution for speed).
  + p - Show processes using the sockets.
  + a - Show all listening and non-listening sockets.

**2. sudo systemctl status ssh**

* **Purpose**: Check the status of the SSH service managed by systemd.
* **When to Use**:
  + To see if the SSH service is **active**, **inactive**, or **failed**.
  + Useful for managing and troubleshooting SSH server operation.
* **Output Highlights**:
  + Service status (active, inactive, or failed).
  + Any logs related to the last service start or failure.

**3. sudo ps –el | grep ssh**

* **Purpose**: Look for SSH-related processes in the system.
* **When to Use**:
  + To confirm if the sshd process (SSH server) or other SSH-related processes are running.
  + Useful for diagnosing issues like multiple SSH processes or server crashes.
* **Output Highlights**:
  + Process ID (PID).
  + CPU and memory usage details.

**4. sudo apt install openssh-server**

* **Purpose**: Install the OpenSSH server package.
* **When to Use**:
  + When SSH is not yet installed on your system.
  + To set up an SSH server on a new system or after a minimal OS installation.

**General Workflow for SSH Management**

1. **Check if the SSH server is installed**:
   * Run sudo apt list --installed | grep openssh or directly sudo systemctl status ssh.
2. **Install the SSH server**:
   * If not installed, run sudo apt install openssh-server.
3. **Verify if SSH is running**:
   * Use sudo systemctl status ssh to check its status.
   * Use sudo ss –tulnpa to confirm the SSH port (22 by default) is listening.
4. **Inspect running processes**:
   * Use sudo ps –el | grep ssh to debug and ensure SSH-related processes are active.

This systematic approach ensures you can effectively install, verify, and troubleshoot the SSH service.