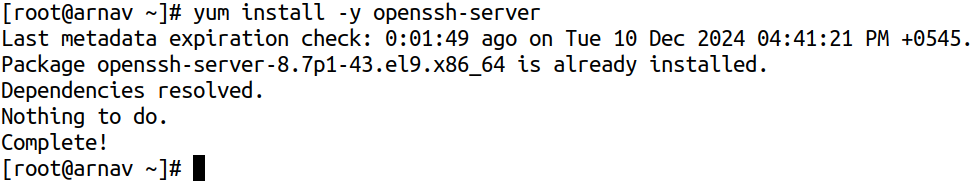
**Task 5**

**Configuring SSH Server to allow/deny root login and allow/deny users login**

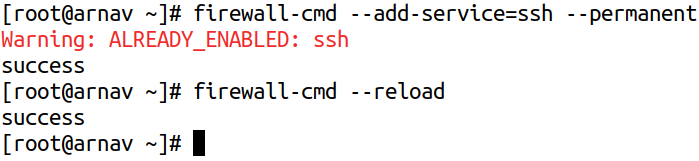
1. Install required package for OpenSSH server

To install any package in Alma Linux, simple command ‘yum install <package\_name>’ is used. For OpenSSH Server, we simply install the package named ‘openssh-server’.



1. Allow ssh packets to enter through the firewall

To add anything to the firewall, we use the ‘firewall-cmd’ command interface. To allow ssh packets to enter through the firewall, we can simply use the command, ‘firewall-cmd --permanent --add-service=ssh’, and then by reloading the firewall



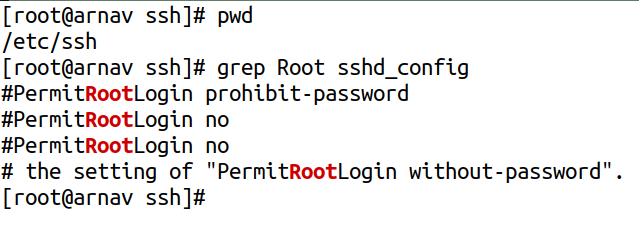
1. Start and enable ssh service

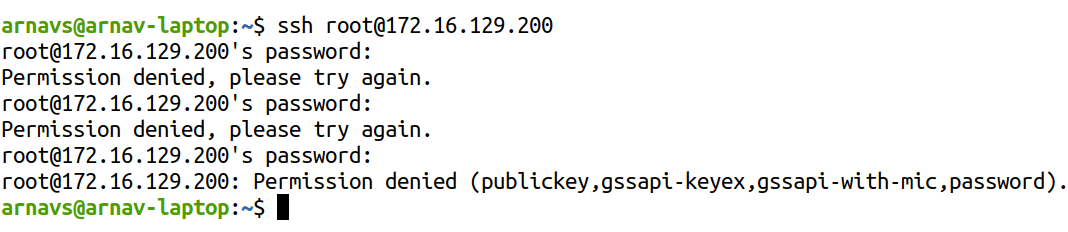
OpenSSH Server works as a service named ‘sshd’, whose status can be viewed by using the command ‘systemctl status sshd’. To enable it, we can simply use the command as ‘systemctl enable sshd --now’, which starts the sshd service at the same time as well as creates a symlink such that the sshd service starts on every boot.



1. Configure OpenSSH server to deny direct root login

To configure OpenSSH server to deny direct root login, on Alma Linux 9, we can go to the path /etc/ssh/ and then modify the file present there named sshd\_config, and set the flag named ‘PermitRootLogin’ to ‘no’ so we can deny direct root login.





1. Configure OpenSSH Server to block login from users named ram and sita.

To deny logins from specific user into the server, we can again modify the same ‘sshd\_config’ file to add a block of ‘DenyUsers’ as follows:

