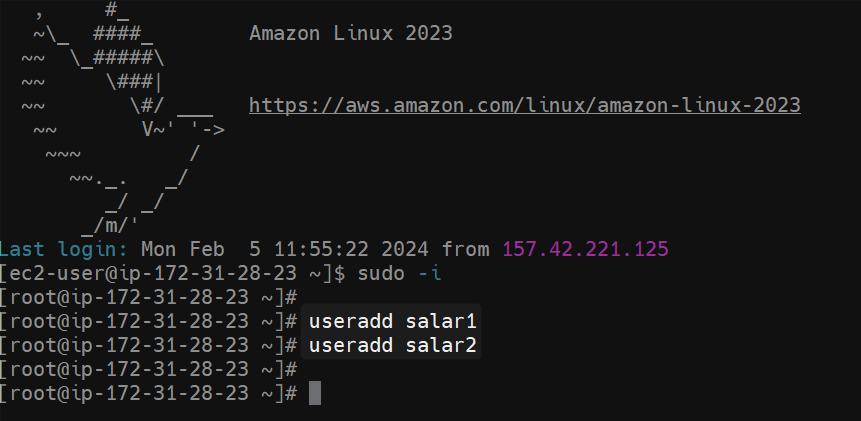
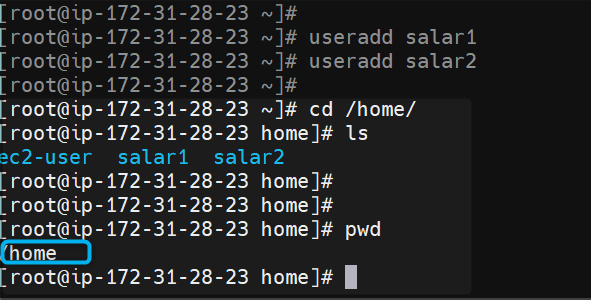
USER MANAGEMENT

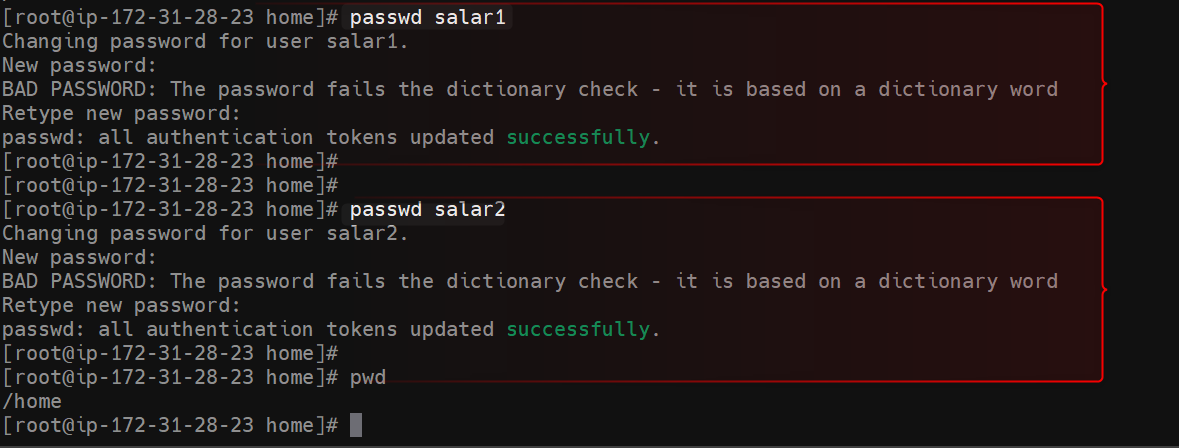
1. (a)Root will create two users named as salar1 and salar2



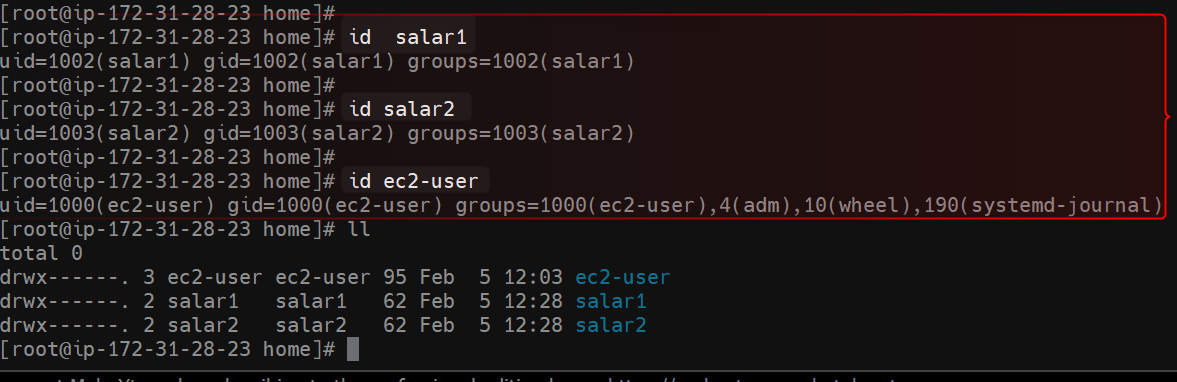
(b) check both users are going to store which path



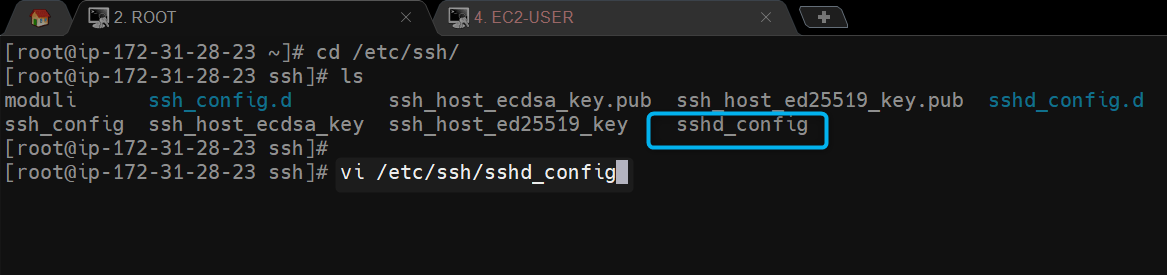
1. (A). Create root password to both user 1 and user 2

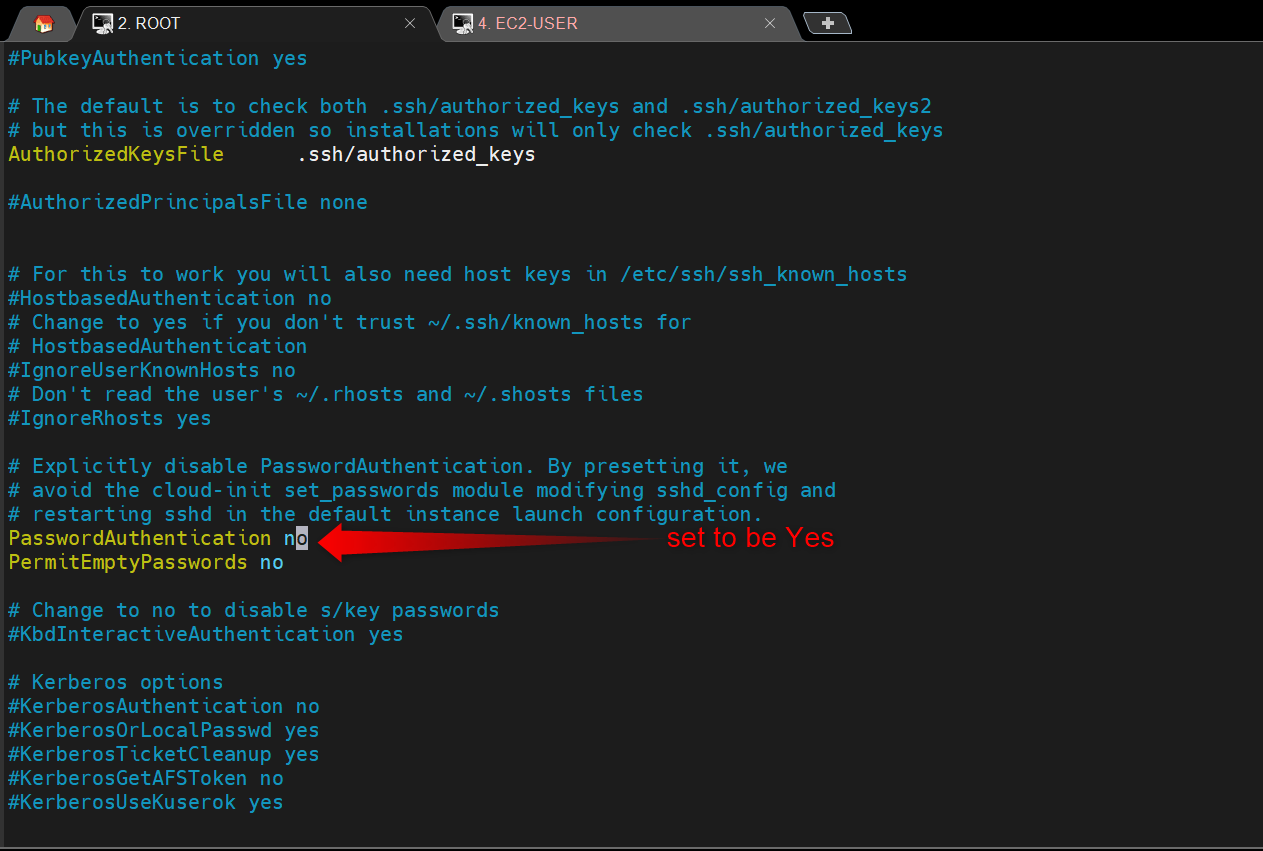


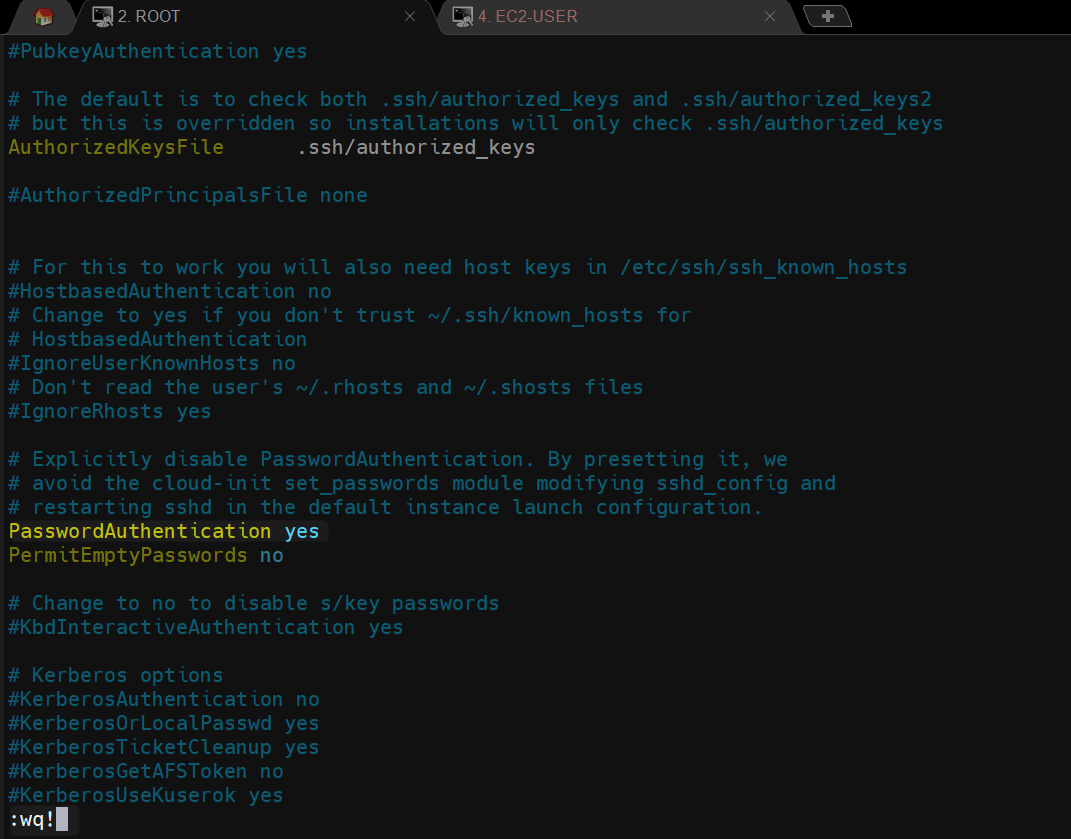
(B.) Check group details for both users



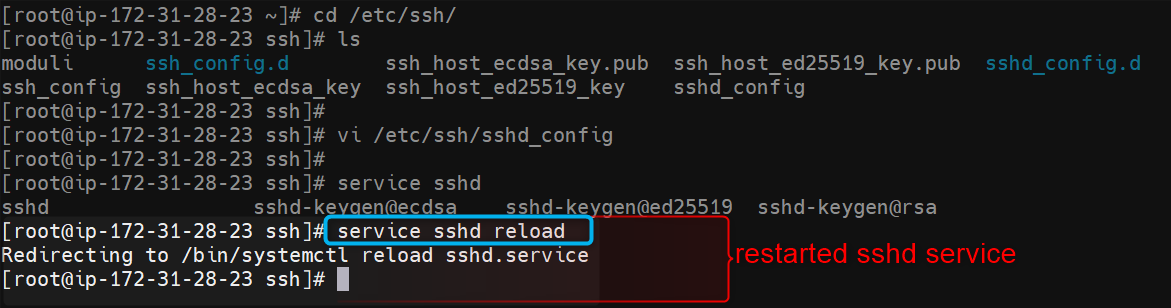
1. (A). Enable password authentication in config file

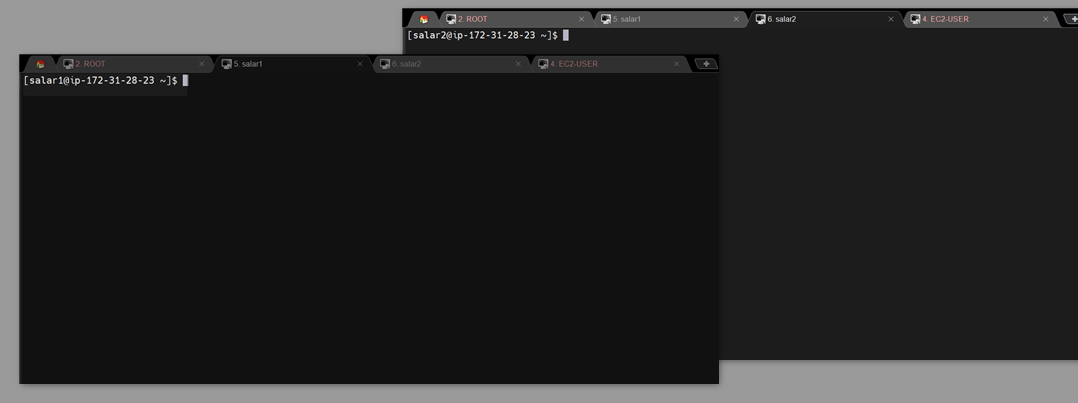






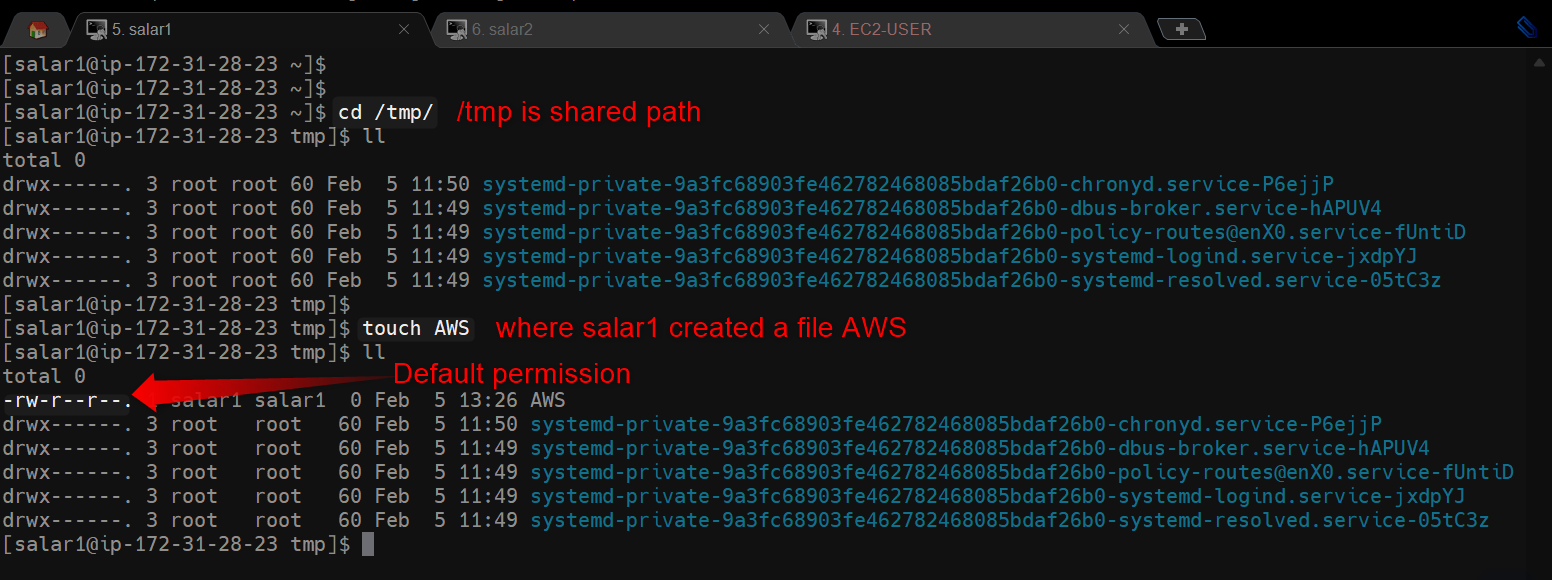
(B). Restart sshd service & connect user1 and user2 in mobaxtreme.



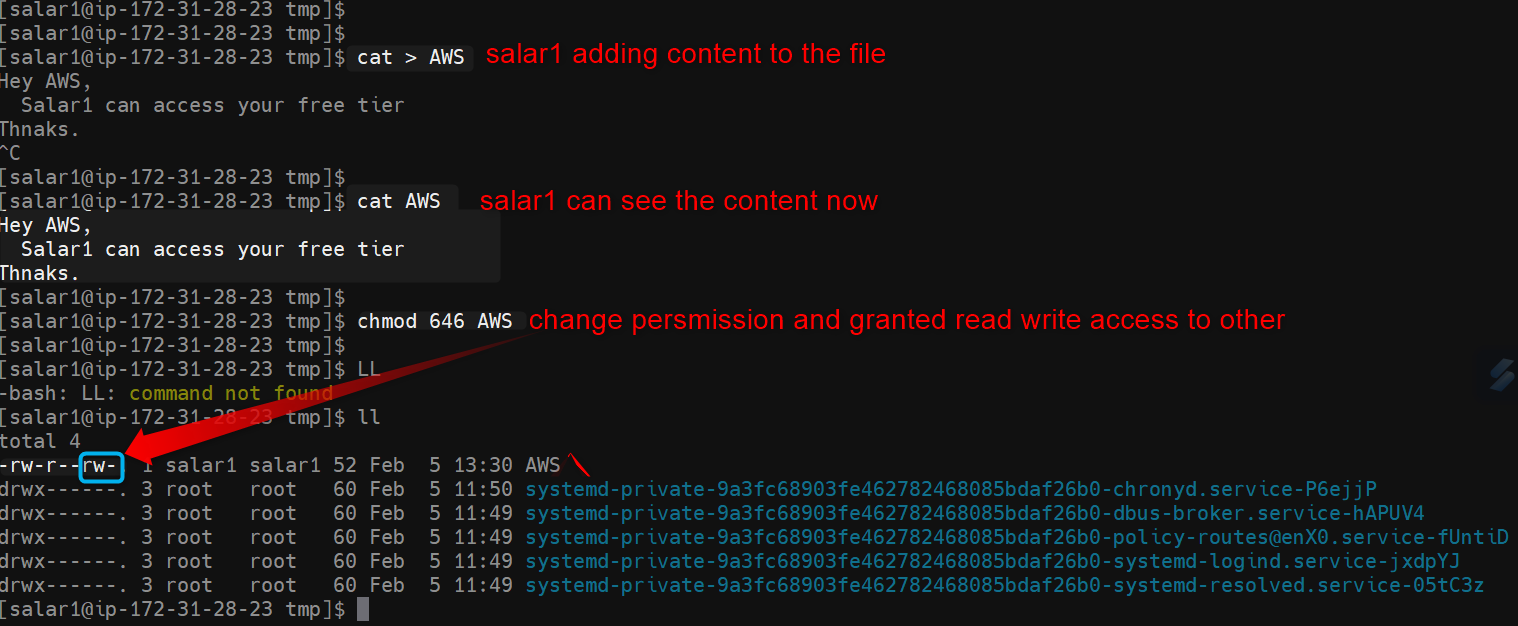


------- Other user level ------------------

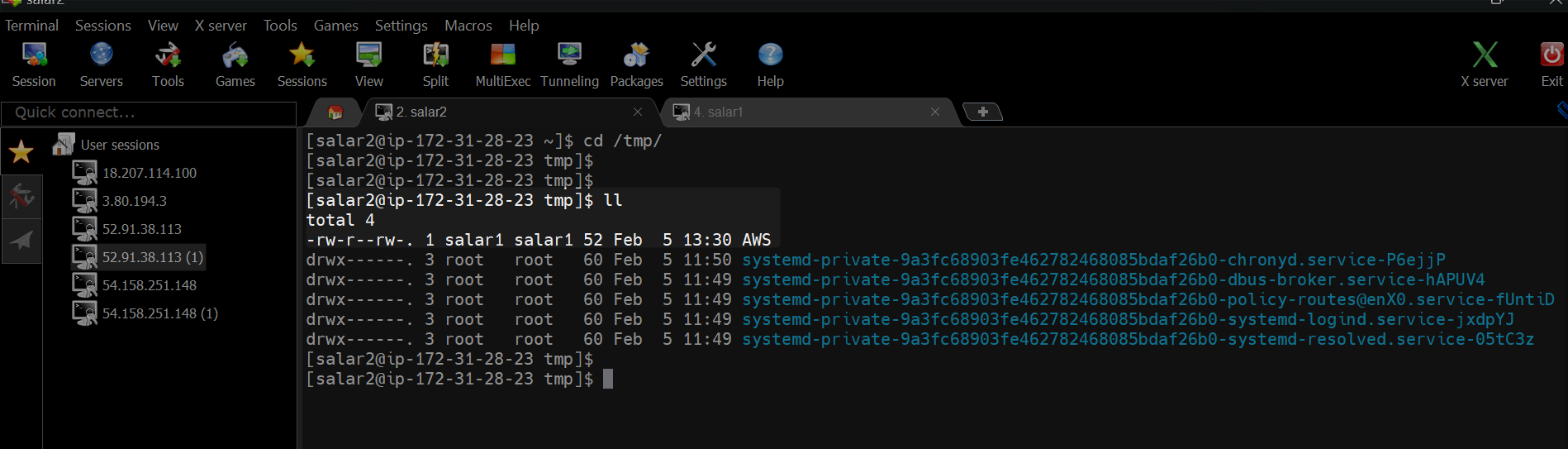
1. (a)our user salar1 create one file named as (AWS) in share directory.



(b)salar1 will add some content and user1 will check the permission and provide read and write permission to OTHER for file (AWS)

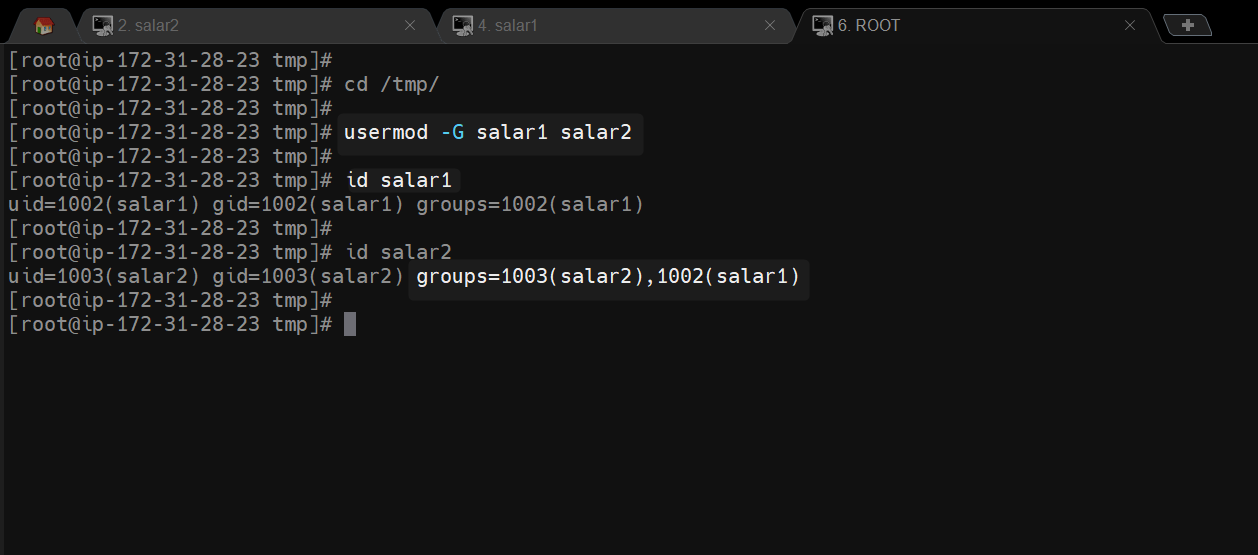


(c)Go to user 2 & in share directory and check whether user 2 is able read and write/overwrite the same content or not.

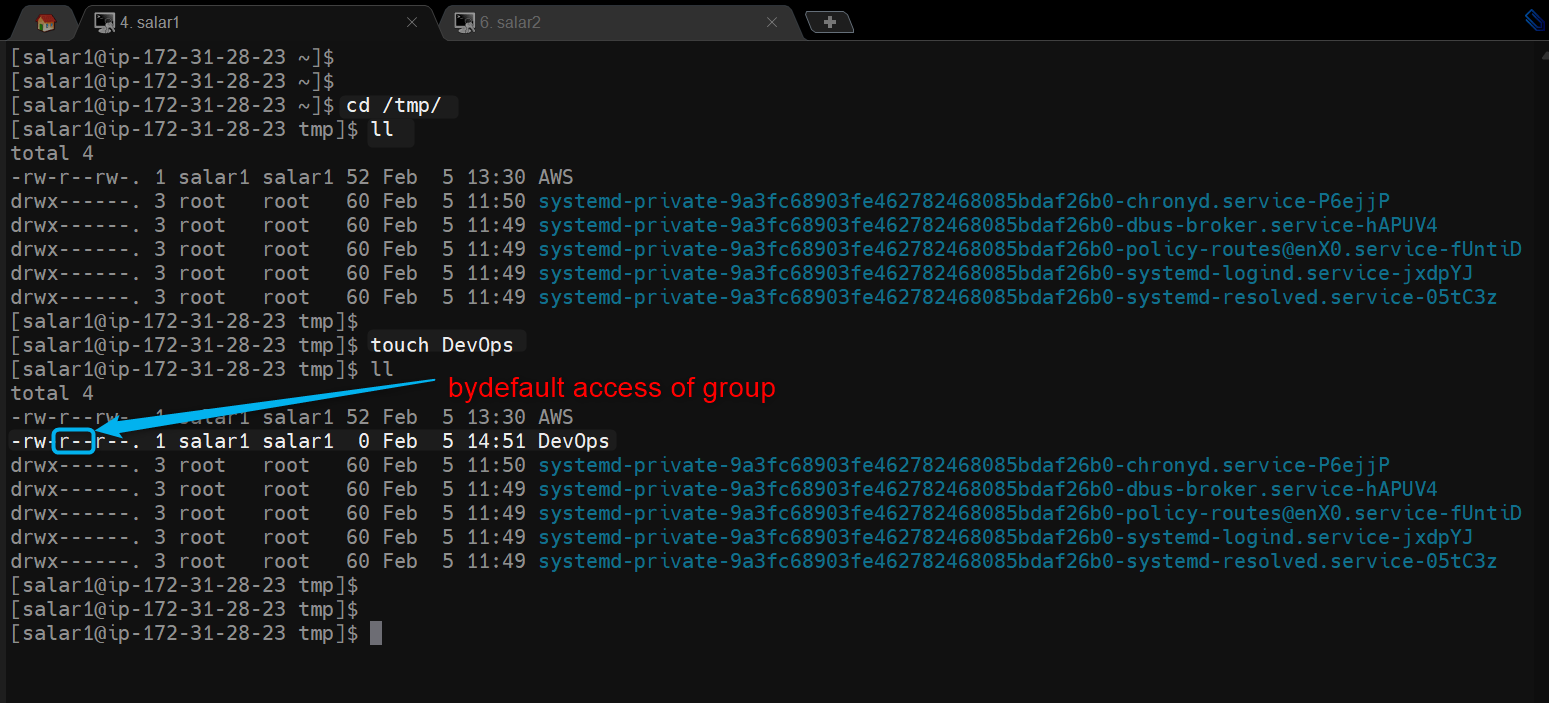


--------------group level --------------------------

1. (a)Root will add user1 and user2 on same group and check group details for both users.

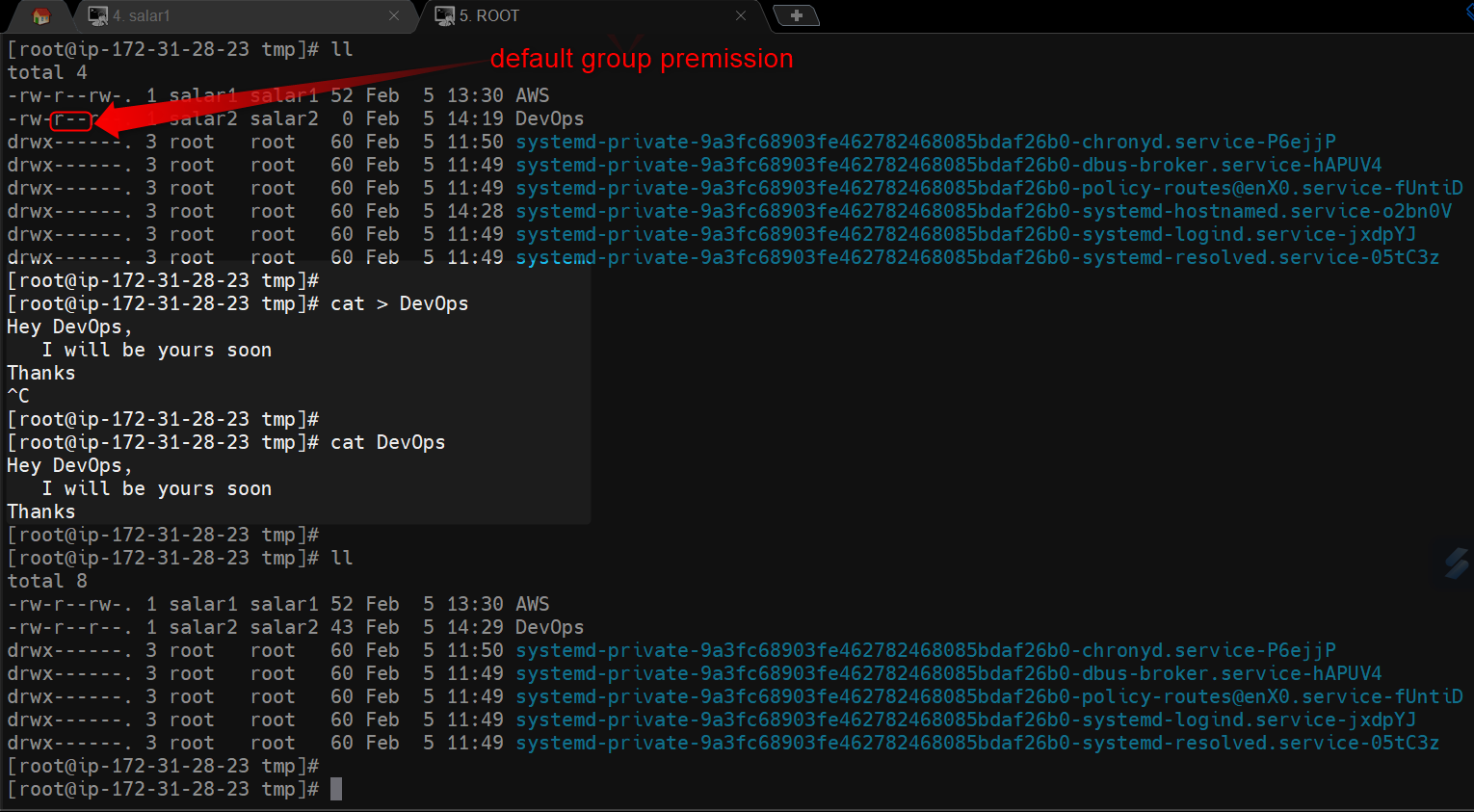


(b)salar1 create another file named as (DevOps) in share directory.

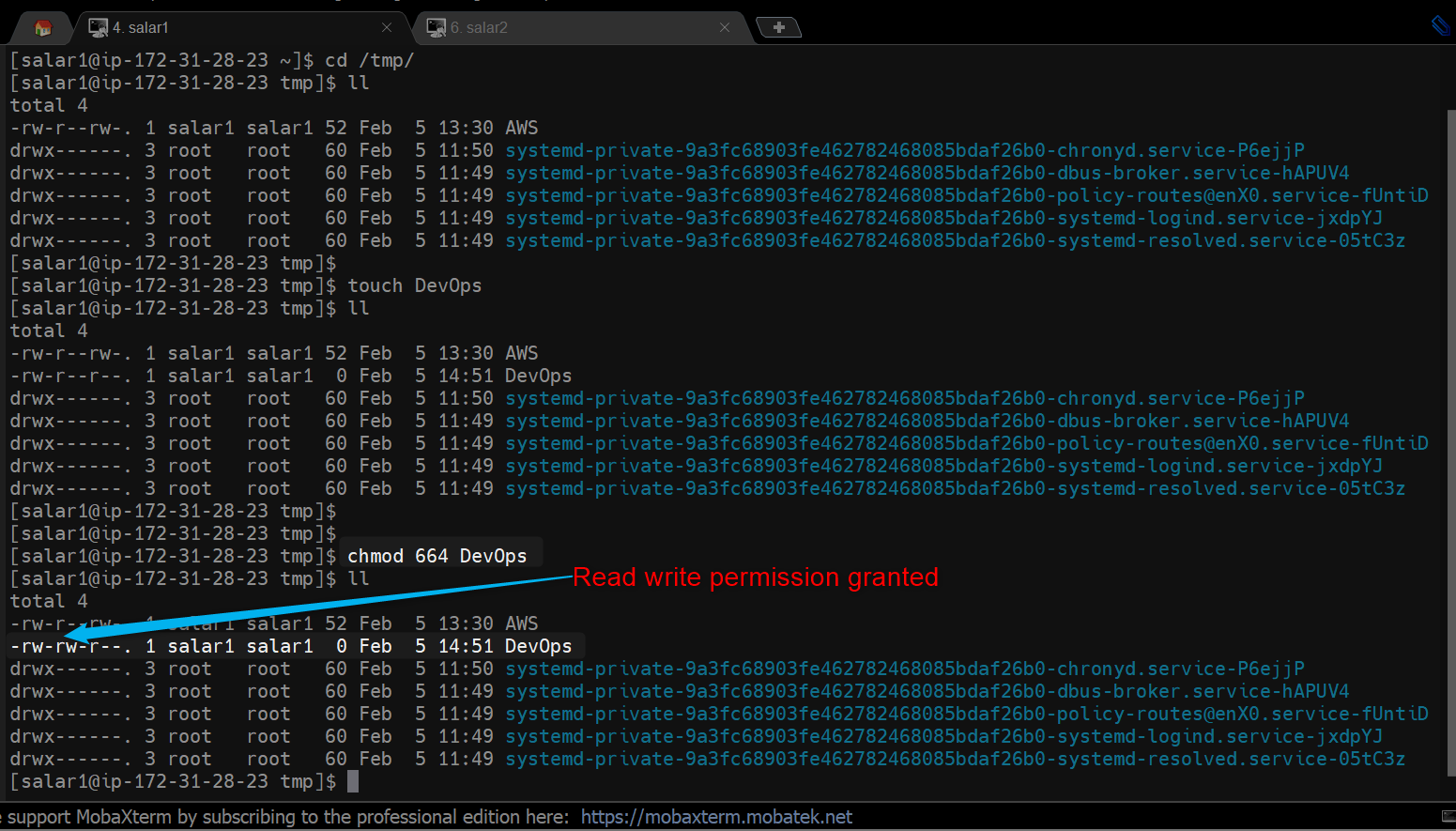


ROOT can able to read and write by default as root is super user by default he granted with full access.

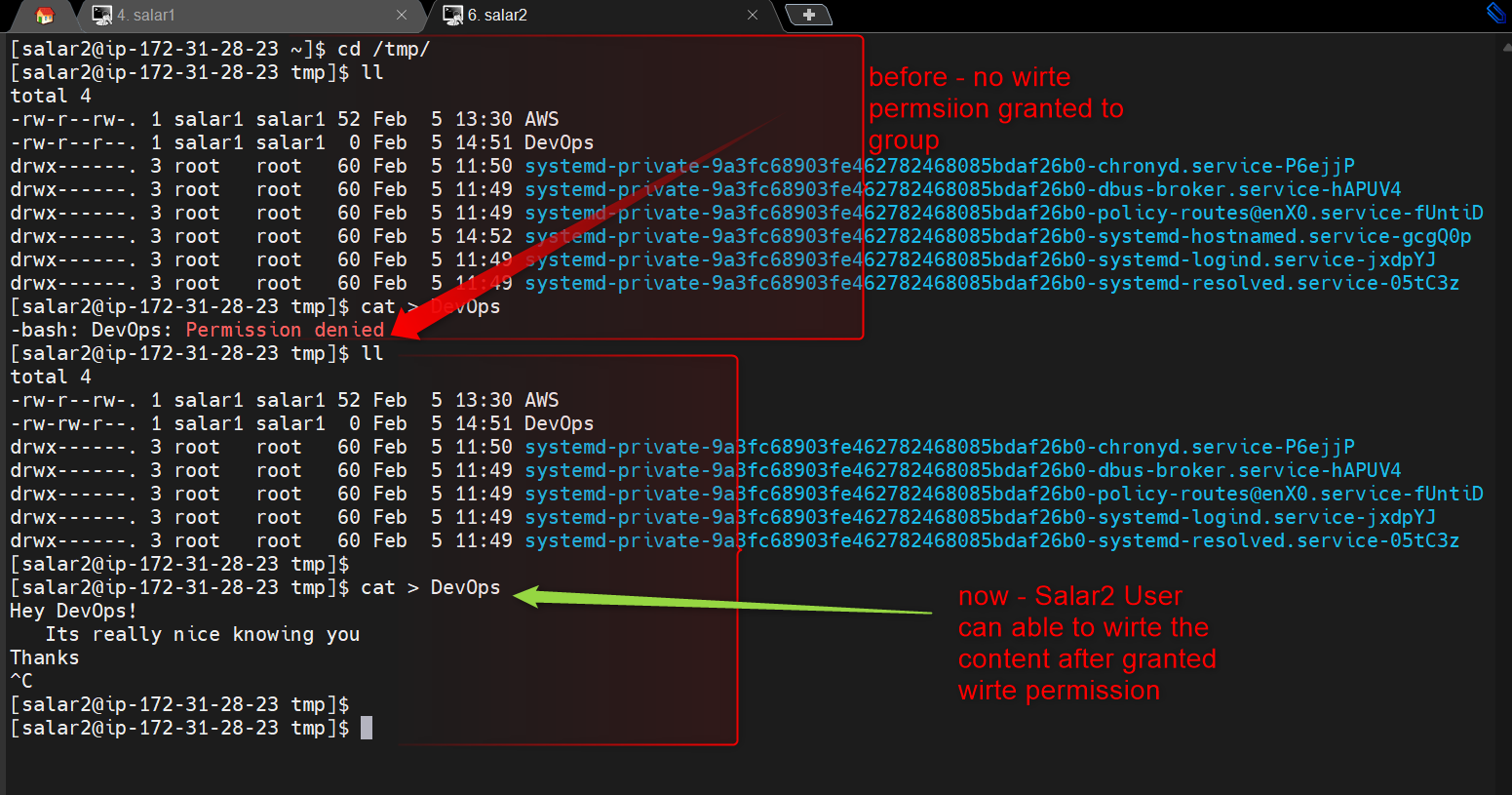
Root

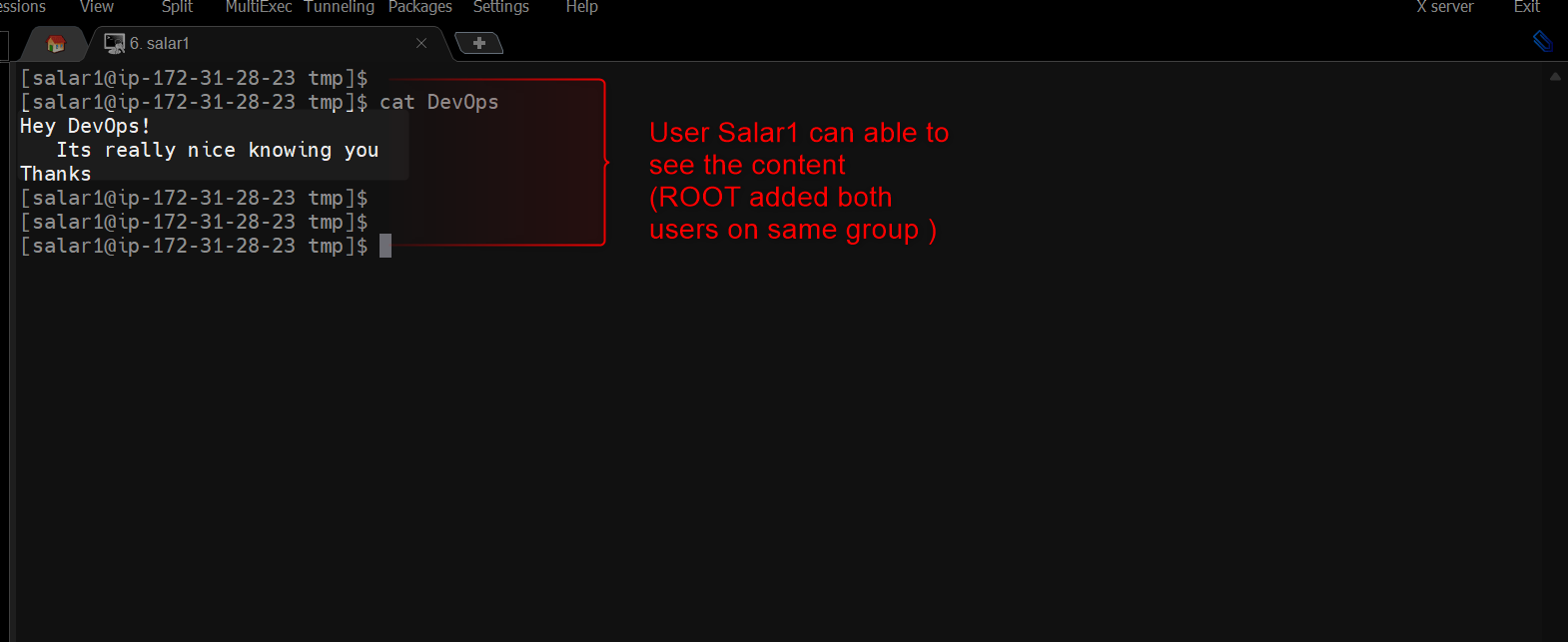


(c)salar1 will add some content and salar1 will check the permission and provide read write permission to GROUP for file (DevOps).



(d)Go to salar2 & in share directory and check whether salar2 is able read only and no write/overwrite permission the same content or not.





(e)As here salar2 is only part of salar1 group we can consider ec-2 as OTHER. Check EC2-user (who is other) can only able to read the content not write.

