

PERFORMANCE CHECKLIST

In this lab you will set a default local password policy, create a supplementary group for three users, allow that group to use sudo to run commands as root, and modify the password policy for one user.

OUTCOMES

BEFORE YOU BEGIN

You should be able to:

- Set a default password aging policy of the local user's password.
- Create a group and use the group as a supplementary group for new users.
- Create three new users with the new group as their supplementary group.
- Configure the group members of the supplementary group to run any command as any user using sudo.
- Set a user-specific password aging policy

PRACTICE SET :

1. On serverb, ensure that newly created users have passwords that must be changed every 30 days.
2. Create the new group consultants with a GID of 40000.
3. Configure administrative rights for all members of consultants to be able to execute any command as any user.
4. Create the consultant1, consultant2, and consultant3 users with consultants as their supplementary group.
5. Set the consultant1, consultant2, and consultant3 accounts to expire in 90 days from the current day.
6. Change the password policy for the consultant2 account to require a new password every 15 days.
7. Additionally, force the consultant1, consultant2, and consultant3 users to change their passwords on the first login.

Finish