fase 1, creación y administración de usuarios y grupos

crea tres usuarios con diferentes roles

```
oscar@srv-base-oscarhernandez:~$ id dev_user
uid=1007(dev_user) gid=1007(dev_user) groups=1007(dev_user),100(users),1008(desarrolladores)
oscar@srv-base-oscarhernandez:~$ _
```

sysadmin, administrador con permisos avanzados

```
oscar@srv-base-oscarhernandez:~$ id dev_user
uid=1007(dev_user) gid=1007(dev_user) groups=1007(dev_user),100(users),1008(desarroll
oscar@srv-base-oscarhernandez:~$ sudo adduser sysadmin
info: Adding user `sysadmin' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `sysadmin' (1009) ...
info: Adding new user `sysadmin' (1009) with group `sysadmin (1009)' ...
info: Creating home directory `/home/sysadmin' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for sysadmin
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `sysadmin' to supplemental / extra groups `users' ...
info: Adding user `sysadmin' to group `users' ...
oscar@srv-base-oscarhernandez:~$ sudo usermod -aG sudo sysadmin
oscar@srv-base-oscarhernandez:~$ sudo -u sysadmin sudo whoami
[sudo] password for sysadmin:
root
oscar@srv-base-oscarhernandez:~$
```

inter_user, usuario con permisos limitados. he creado un directorio llamado /datos/inter_user y el usuario tiene acceso pero no al resto de directorios ahora tiene los permisos limitados en el sistema

```
oscar@srv-base-oscarhernandez:~$ sudo adduser intern_user
info: Adding user `intern_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `intern_user' (1010) ...
info: Adding new user `intern_user' (1010) with group `intern_user (1010)' ...
info: Creating home directory `/home/intern_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for intern_user
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `intern_user' to supplemental / extra groups `users' ...
info: Adding user `intern_user' to group `users' ...
oscar@srv-base-oscarhernandez:~$ sudo mkdir /datos/intern_user
mkdir: cannot create directory ‘/datos/intern_user’: No such file or directory
oscar@srv-base-oscarhernandez:~$ sudo mkdir /datos/intern_user
mkdir: cannot create directory ‘/datos/intern_user’: No such file or directory
oscar@srv-base-oscarhernandez:~$ sudo mkdir -p /datos/intern_user
oscar@srv-base-oscarhernandez:~$ sudo chown intern_user:intern_user /datos/intern_us
oscar@srv-base-oscarhernandez:~$ sudo chmod 700 /datos/intern_user
oscar@srv-base-oscarhernandez:~$ _
```

asignar cada usuario a los grupos developers, admins, interns, y configurar acceso a carpetas para cada usuario

```
oscar@srv-base-oscarhernandez:/$ sudo groupadd developers
oscar@srv-base-oscarhernandez:/$ sudo groupadd admins
oscar@srv-base-oscarhernandez:/$ sudo groupadd interns
oscar@srv-base-oscarhernandez:/$ sudo usermod -aG developers dev_user
oscar@srv-base-oscarhernandez:/$ sudo usermod -aG admins sysadmin
oscar@srv-base-oscarhernandez:/$ sudo usermod -aG interns intern_user
oscar@srv-base-oscarhernandez:/$ sudo mkdir -p /proyectos/developers
oscar@srv-base-oscarhernandez:/$ sudo mkdir -p /proyectos/admins
oscar@srv-base-oscarhernandez:/$ sudo mkdir -p /proyectos/interns
oscar@srv-base-oscarhernandez:/$ sudo chown -R :developers /proyectos/developers
oscar@srv-base-oscarhernandez:/$ sudo chown -R :admins /proyectos/admins
oscar@srv-base-oscarhernandez:/$ sudo chown -R :interns /proyectos/interns
oscar@srv-base-oscarhernandez:/$ sudo chown -R 770 /proyectos/developers
oscar@srv-base-oscarhernandez:/$ sudo chown -R 770 /proyectos/admins
oscar@srv-base-oscarhernandez:/$ sudo chown -R 770 /proyectos/interns
oscar@srv-base-oscarhernandez:/$ ls -l /pryectos
ls: cannot access '/pryectos': No such file or directory
oscar@srv-base-oscarhernandez:/$ ls -l /proyectos
total 12
drwxr-xr-x 2 770 admins     4096 jun 22 10:18 admins
drwxr-xr-x 2 770 developers 4096 jun 22 10:18 developers
drwxr-xr-x 2 770 interns    4096 jun 22 10:19 interns
oscar@srv-base-oscarhernandez:/$ _
```

fase 2, configuración de tareas automatizadas.

programar una tarea en cron para respaldar un directorio, respaldar el directorio proyectos.

```
  GNU nano 7.2                                                    /tmp/crontab.Ji
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
0 2 * * * tar -czf /backup/directorio_$(date +\%y-\%m-\%d).tar.gz /proyectos
```

```
crontab: installing new crontab
oscar@srv-base-oscarhernandez:/$ contrab -l
contrab: command not found
oscar@srv-base-oscarhernandez:/$ crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
0 2 * * * tar -czf /backup/directorio_$(date +\%y-\%m-\%d).tar.gz /proyectos
oscar@srv-base-oscarhernandez:/$
```

establecer un scrip que envíe notificaciones de actividad al servidor, para ello instaló mailutils despues creamos el scrip

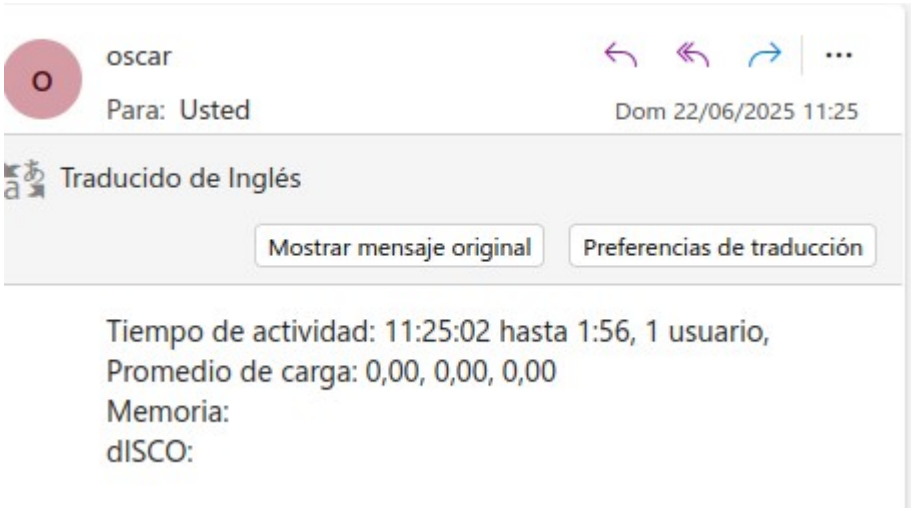
```
#!/bin/bash

#configura el destinatario y el asunto
DESTINATARIO="oscar_cdm@hotmail.com"
ASUNTO="notificacion de actividad del servidro"

# obtine la informacion del servidor
UPTIME=$(uptime)
MEMORIA=$(free -m)
DISCO=$(df -h)

# envia el correo electronico
echo "uptime: $UPTIME
Memoria: $memoria
dISCO: $disco" | mail -s "$ASUNTO" $destinatario_
```

comprobamos ejecutando el scrip manualmente y viendo si recibimos el correo



fase 3, monitorización y optimización del servidor.

identificar procesos en ejecución y priorizarlos si es necesario

```
    972    0 apache2
    973    0 apache2
   1171    0 systemd
   1172    0 (sd-pam)
   1181    0 bash
   1322    0 fwupd
   1331    0 upowerd
   1596  -20 kworker/R-tls-s
   1943    0 kworker/u5:2-events_power_efficient
   2201    0 kworker/u5:0-flush-252:0
   2822    - psimon
   3140    0 master
   3141    0 pickup
   3142    0 qmgr
   3169    0 rsyslogd
   3324    0 kworker/0:0-events
   3331    0 kworker/u6:0-events_power_efficient
   3386    0 kworker/u5:3-events_freezable_power_
   3436    0 tlsmgr
   3442    0 kworker/u6:1-events_power_efficient
   3452    0 kworker/0:3-cgroup_destroy
   3502    0 kworker/u6:3-events_unbound
   3509    0 kworker/1:1-cgroup_destroy
   3533    0 kworker/0:1
   3544    0 ps
```

configurar logs de auditoria para registrar accesos y acciones de usuarios

primero instalamos el paquete auditd

```
## This file is automatically generated from /etc/audit/rules.d
-D
-b 8192
-f 1
--backlog_wait_time 60000
```

despues utilizar la auditoria de linux para registrar los accesos y acciones del usuario dev_user añadiendo la regla

```
## This file is automatically generated from /etc/audit/rules.d
-D
-b 8192
-f 1
--backlog_wait_time 60000
-a exit,always -F uid=$(id -u dev_user) -S all
```

después comprobamos una sin haber iniciado con el usuario y otra después de haber iniciado

```
oscar@srv-base-oscarhernandez:/$ sudo ausearch -ua dev_user
<no matches>
oscar@srv-base-oscarhernandez:/$
```

```
----
time->Sun Jun 22 11:54:45 2025
type=USER_START msg=audit(1750586085.898:210): pid=1507 uid=1007 auid=1007 ses=1 subj=unconfined msg='op=PAM:session_open grantors=pam_env,pam_env,pam_m
limits,pam_permit,pam_umask,pam_unix,pam_systemd acct="oscar" exe="/usr/bin/su" hostname=srv-base-oscarhernandez addr=? terminal=/dev/tty1 res=success'
----
```