**Implemented Linux user management and security hardening on Ubuntu 24.04**

What actually do here:

* SSH key-only access
* disabled root SSH
* UFW firewall
* Fail2Ban
* PAM password policy(14 day expiration policy)
* auditd logging
* automated security updates

NB: The quick automation script will be found in the last page of this documents

Here the step by step process to do the following things

**Step01: System update + install tools**

sudo apt update && sudo apt upgrade -y

sudo apt install -y ufw fail2ban auditd audispd-plugins unattended-upgrades logwatch libpam-pwquality

**Step02: Create non-root admin user(s) with SSH key auth**

**# create user (interactive - set a password)**

sudo adduser opsuser

**# add to sudo group**

sudo usermod -aG sudo opsuser



**# create .ssh and authorized\_keys (paste your public key)**

sudo mkdir -p /home/opsuser/.ssh

sudo tee /home/opsuser/.ssh/authorized\_keys > /dev/null <<'KEY'

ssh-rsa AAAA...your\_public\_key\_here... user@host

KEY

**# set correct permissions**

sudo chmod 700 /home/opsuser/.ssh

sudo chmod 600 /home/opsuser/.ssh/authorized\_keys

sudo chown -R opsuser:opsuser /home/opsuser/.ssh

**Note: Do not** **remove your original key from ubuntu user until opsuser SSH test succeeds.**

**Step03: Backup and harden SSH configuration**

sudo cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.bak

SSH changes — open in editor OR apply safely with sed (I prefer manual edit to avoid mistakes):

sudo vi /etc/ssh/sshd\_config

ensure these lines (uncomment/modify accordingly):

Port 22 # keep 22 unless you plan to change — if change, update AWS SG

PermitRootLogin no

PasswordAuthentication no # ONLY after confirming key login works

ChallengeResponseAuthentication no

UsePAM yes

PermitEmptyPasswords no

# Optionally restrict login users:

# AllowUsers opsuser ubuntu

Then test config and reload:

sudo sshd -t # syntax check

sudo systemctl reload sshd

**Important:** Keep your current session open; from another terminal try **ssh -i key opsuser@<PUBLIC\_IP>** to confirm.

If you change Port to custom (e.g., 2222), update AWS Security Group inbound rule to allow that port and run:

sudo ufw allow 2222/tcp

**Step04: Enable and configure UFW (firewall)**

Allow OpenSSH first (to avoid lockout), then HTTP/HTTPS as needed, then enable:

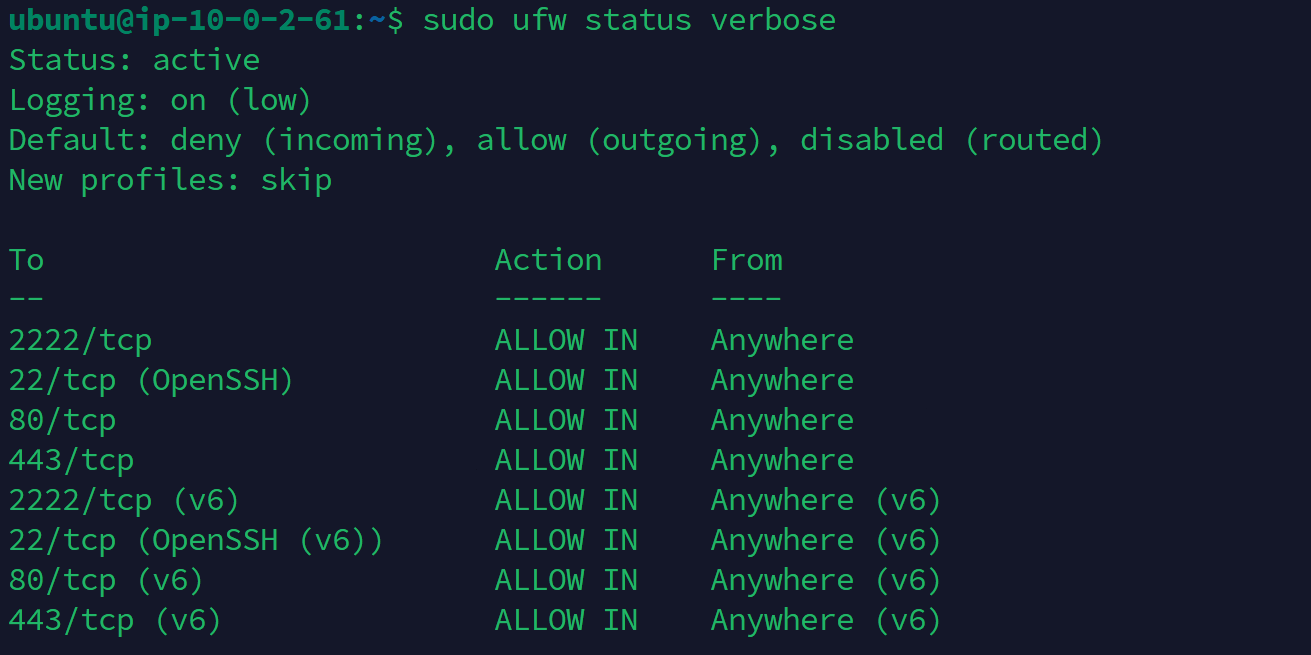
sudo ufw allow OpenSSH

sudo ufw allow 80/tcp # if web server

sudo ufw allow 443/tcp # if planning HTTPS

sudo ufw enable

sudo ufw status verbose



**Step05: Install & enable Fail2Ban (protect SSH)**

sudo apt install -y fail2ban

**# Create a local jail (safe to edit)**

sudo tee /etc/fail2ban/jail.d/local.conf > /dev/null <<'EOF'

[sshd]

enabled = true

port = ssh

maxretry = 5

bantime = 3600

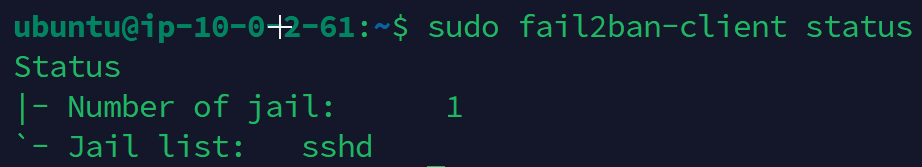
findtime = 600

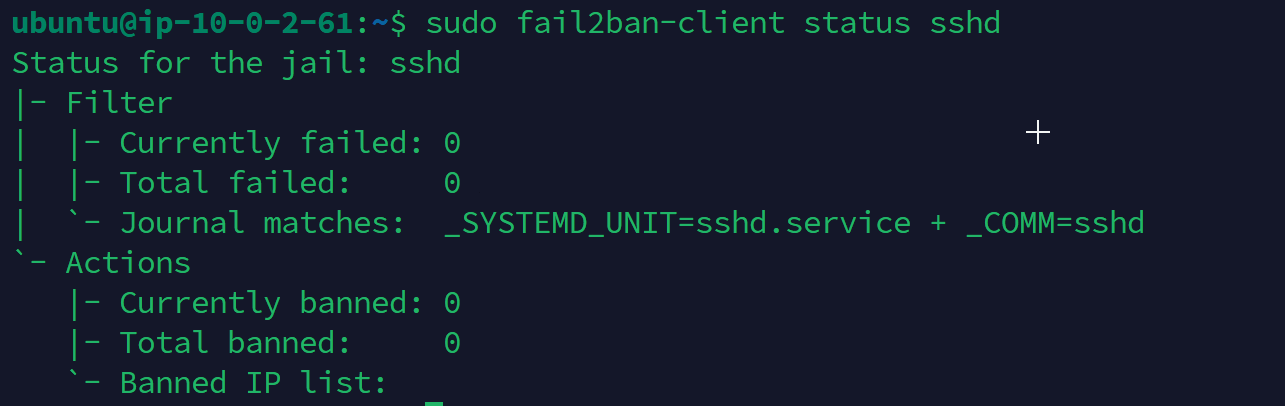
EOF

sudo systemctl restart fail2ban

**# check status**

sudo fail2ban-client status sshd





**Step06: Enforce password policy (PAM / pwquality)**

**Backup then edit:**

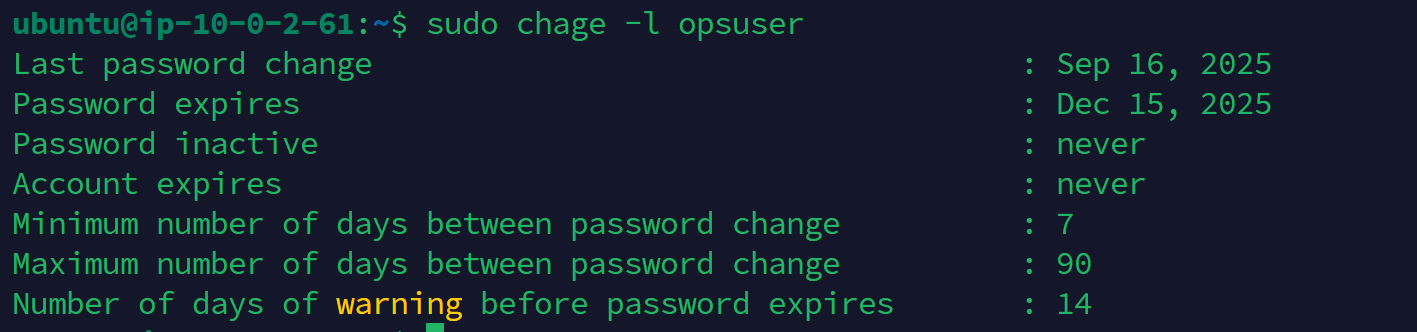
sudo cp /etc/pam.d/common-password /etc/pam.d/common-password.bak

sudo sed -i 's/^password\s\+requisite\s\+pam\_pwquality.so.\*/password requisite pam\_pwquality.so retry=3 minlen=12 difok=3/' /etc/pam.d/common-password || true

**Set password expiration policy:**

**# set max 90 days, min 7 days, warn 14 days**

sudo chage -M 90 -m 7 -W 14 opsuser



**Step07: File & webroot permissions (for hosting web)**

**Set secure permissions for /var/www:**

sudo chown -R www-data:www-data /var/www

sudo find /var/www -type d -exec chmod 755 {} \;

sudo find /var/www -type f -exec chmod 644 {} \;

**Step08: Disable unused services**

**List enabled services:**

systemctl list-unit-files --type=service | grep enabled

**Disable anything unnecessary :**

sudo systemctl disable --now avahi-daemon || true

**Caution:** Don’t disable cloud-init or sshd. Only stop services you understand.

**Step09: Install & configure auditd (important)**

sudo apt install -y auditd audispd-plugins

**# Add basic watch rules (create a file)**

sudo tee /etc/audit/rules.d/hardening.rules > /dev/null <<'AUDP'

-w /etc/passwd -p wa -k identity

-w /etc/shadow -p wa -k identity

-w /etc/group -p wa -k identity

-w /etc/sudoers -p wa -k scope

-w /var/log/auth.log -p wa -k authlog

AUDP

sudo augenrules --load

sudo systemctl restart auditd

**# check status**

sudo auditctl -l

**Step10: Enable automatic security updates**

sudo apt install -y unattended-upgrades

sudo dpkg-reconfigure -plow unattended-upgrades

**# quick verify file:**

cat /etc/apt/apt.conf.d/20auto-upgrades

**Step11: AppArmor hardening (Ubuntu)**

**Check status & enable profile for services (Apache):**

sudo aa-status

**# Enforce apache profile (example)**

sudo aa-enforce /etc/apparmor.d/usr.sbin.apache2 || true

**Step12: Centralized logging / rotate config**

Ensure logrotate and logwatch installed (we installed logwatch earlier). Configure mail alerts or export logs to external host/S3 (advanced).

**Step13: Enforce UMASK and secure cron**

Set default umask in /etc/profile or systemd service overrides. Audit cron jobs and restrict by permissions.

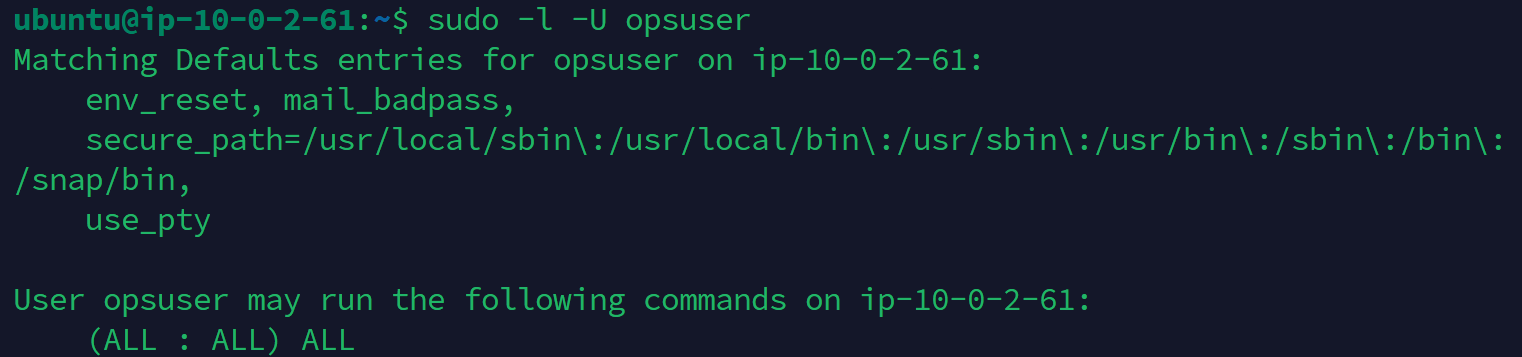
**Step14: SSH banner and session timeout**

**Add to /etc/ssh/sshd\_config:**

ClientAliveInterval 300

ClientAliveCountMax 2

And add Banner /etc/issue.net with custom message as needed.



**Quick Automation Script(Change where you need before running)**

#!/bin/bash

set -euo pipefail

# Variables: change as needed

USER="opsuser"

SSH\_PUBKEY="ssh-rsa AAAA...your\_public\_key\_here"

# update

apt update && apt upgrade -y

# install tools

apt install -y ufw fail2ban auditd audispd-plugins unattended-upgrades logwatch libpam-pwquality

# create user

if ! id -u "$USER" >/dev/null 2>&1; then

adduser --disabled-password --gecos "" "$USER"

usermod -aG sudo "$USER"

fi

mkdir -p /home/$USER/.ssh

echo "$SSH\_PUBKEY" > /home/$USER/.ssh/authorized\_keys

chmod 700 /home/$USER/.ssh

chmod 600 /home/$USER/.ssh/authorized\_keys

chown -R $USER:$USER /home/$USER/.ssh

# ufw

ufw allow OpenSSH

ufw allow 80/tcp

ufw allow 443/tcp

ufw --force enable

# fail2ban simple jail

cat > /etc/fail2ban/jail.d/default.local <<'EOF'

[sshd]

enabled = true

port = ssh

maxretry = 5

bantime = 3600

findtime = 600

EOF

systemctl restart fail2ban

# pam pwquality - append if not exists

grep -q "pam\_pwquality.so" /etc/pam.d/common-password || echo "password requisite pam\_pwquality.so retry=3 minlen=12 difok=3" >> /etc/pam.d/common-password

# audit rules

cat > /etc/audit/rules.d/hardening.rules <<'AUDP'

-w /etc/passwd -p wa -k identity

-w /etc/shadow -p wa -k identity

-w /etc/group -p wa -k identity

-w /etc/sudoers -p wa -k scope

-w /var/log/auth.log -p wa -k authlog

AUDP

augenrules --load || true

systemctl restart auditd || true

# enable unattended upgrades

dpkg-reconfigure -plow unattended-upgrades || true

echo "HARDENING DONE. Please verify settings and test SSH key login before closing current session."