

## 1 User & Group Management

Create a user `devops_user` and add them to a group `devops_team`.

- To create the user in linux the command used is **`sudo useradd -M devops_user`**
- The users present in the system can be seen in the **`/etc/passwd`** file

```
ubuntu@ip-172-31-11-252:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534:/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:101:/nonexistent:/usr/sbin/nologin
syslog:x:102:102:/nonexistent:/usr/sbin/nologin
systemd-resolve:x:991:991:systemd Resolver:/usr/sbin/nologin
uidd:x:103:103:/run/uidd:/usr/sbin/nologin
tss:x:104:104:TPM software stack,,:/var/lib/tpm:/bin/false
sshd:x:105:65534:/run/sshd:/usr/sbin/nologin
pollinate:x:106:1:/var/cache/pollinate:/bin/false
tcpdump:x:107:108:/nonexistent:/usr/sbin/nologin
landscape:x:108:109:/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:990:990:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
polkitd:x:989:989:User for polkitd:/usr/sbin/nologin
ec2-instance-connect:x:109:65534:/nonexistent:/usr/sbin/nologin
_chrony:x:110:112:Chrony daemon,,:/var/lib/chrony:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
devops_user:x:1001:1001:/home/devops_user:/bin/sh
```

- The list of the groups are present in /etc/group

```

messagebus:x:101:
syslog:x:102:
systemd-resolve:x:991:
uidd:x:103:
tss:x:104:
lxd:x:105:ubuntu
_ssh:x:106:
rdma:x:107:
tcpdump:x:108:
landscape:x:109:
fwupd-refresh:x:990:
polkitd:x:989:
admin:x:110:
netdev:x:111:
_chrony:x:112:
ubuntu:x:1000:
devops_user:x:1001:
devops_team:x:1002:
ubuntu@ip-172-31-11-252:~$

```

- Now we need to add the devops\_user to the group devops\_team
- In order to do this we have a command : **sudo gpasswd -a devops\_user devops\_team**

```

ubuntu@ip-172-31-11-252:~$ sudo gpasswd -a devops_user devops_team
Adding user devops_user to group devops_team
ubuntu@ip-172-31-11-252:~$ cat /etc/group
root:x:0:

```

### Set a password and grant sudo access.

- In order to set the password and grant the user devops\_user sudo access we need to add the user to the sudo group.
- This can be done using the command: **sudo usermod -aG sudo devops\_user**

This shows that the user devops\_user has been granted sudo permission

Restrict SSH login for certain users in `/etc/ssh/sshd_config`.

- To deny the ssh login to the user we need to append `DenyUsers <theusername>` to the file `/etc/ssh/sshd_config`
- Adding the `DenyUser devops_user` command to the file

```
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem        sftp    /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#      X11Forwarding no
#      AllowTcpForwarding no
#      PermitTTY no
#      ForceCommand cvs server
DenyUsers devops_user
```

## 2 File & Directory Permissions

- Create /devops\_workspace and a file project\_notes.txt.
  - To create the directory devops\_workspace : **mkdir devops\_workspace**
  - Change the directory to devops\_workspace: **cd devops\_workspace**
  - Create a file project\_notes.txt : **touch project\_notes.txt**.

```
ubuntu@ip-172-31-11-252:~$ mkdir devops_workspace
ubuntu@ip-172-31-11-252:~$ cd devops_workspace/
ubuntu@ip-172-31-11-252:~/devops_workspace$ touch project_notes.txt
ubuntu@ip-172-31-11-252:~/devops_workspace$ ls -l
total 0
-rw-rw-r-- 1 ubuntu ubuntu 0 Feb  9 14:03 project_notes.txt
ubuntu@ip-172-31-11-252:~/devops_workspace$
```

- Set permissions: Owner can edit, group can read, others have no access. Use **ls -l** to verify permissions.
  - Check the initial permission of the file project\_notes.txt using **ls -l** command. The below screenshot shows that the user and group has read and write access but other users have read only access

```
ubuntu@ip-172-31-11-252:~$ cd devops_workspace/
ubuntu@ip-172-31-11-252:~/devops_workspace$ ls -l
total 0
-rw-rw-r-- 1 ubuntu ubuntu 0 Feb  9 14:03 project_notes.txt
ubuntu@ip-172-31-11-252:~/devops_workspace$
```

- Permission is set using the **chmod** command, where the owner can edit, group can read and others have no access

**Command: chmod 640 project\_notes.txt**

```
ubuntu@ip-172-31-11-252:~/devops_workspace$ chmod 640 project_notes.txt
ubuntu@ip-172-31-11-252:~/devops_workspace$ ls -l
total 0
-rw-r----- 1 ubuntu ubuntu 0 Feb  9 14:03 project_notes.txt
ubuntu@ip-172-31-11-252:~/devops_workspace$
```

### ③ Log File Analysis with AWK, Grep & Sed

- Download the log file from the repository Linux\_2k.log
- Command : curl -O [https://github.com/logpai/loghub/blob/master/Linux/Linux\\_2k.log](https://github.com/logpai/loghub/blob/master/Linux/Linux_2k.log)

```
ubuntu@ip-172-31-11-252:~/devops_workspace$ curl -O https://github.com/logpai/loghub/blob/master/Linux/Linux_2k.log
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 876k    0 876k    0    0 1177k    0 --:--:-- --:--:-- --:--:-- 1177k
ubuntu@ip-172-31-11-252:~/devops_workspace$
```

- Extract insights using commands:
- Use grep to find all occurrences of the word "error".

```
ubuntu@ip-172-31-11-252:~/devops_workspace$ grep error Linux_2k.log
  <script type="application/json" id="client-env">{"locale":"en", "featureFlags":["bypass_copilot_indexing_quota", "copilot_immersive_file_preview", "copilot_new_references_ui", "copilot_attach_folder_reference", "copilot_chat_repo_custom_instructions_preview", "copilot_chat_retry_on_error", "copilot_chat_persist_submitted_input", "copilot_conversational_ux_history_refs", "copilot_chat_shared_topic_indicator", "copilot_chat_shared_repo_sso_banner", "copilot_editor_upsells", "copilot_dotcom_chat_reduce_telemetry", "copilot_free_limited_user", "copilot_implicit_context", "copilot_no_floating_button", "copilot_smell_icebreaker_ux", "copilot_new_markdown_renderer", "experimentation_azure_variant_endpoint", "failbot_handle_non_errors", "geojson_azure_maps", "ghost_pilot_confidence_truncation_25", "ghost_pilot_confidence_truncation_40", "github_models_o3_mini_streaming", "github_models_per_chunk_timeout", "hovercard_accessibility", "issues_react_remove_placeholders", "issues_react_blur_item_picker_on_close", "issues_react_include_bots_in_pickers", "marketing_pages_search_explore_provider", "remove_child_patch", "sample_network_conn_type", "swp_enterprise_contact_form", "site_copilot_acc", "site_copilot_vscode_link_update", "site_proxima_australia_update", "issues_react_create_milestone", "issues_react_cache_fix_workaround", "lifecycle_label_name_updates"]}</script>
  <script crossorigin="anonymous" defer="defer" type="application/javascript" src="https://github.githubassets.com/assets/app_assets_modules_github_behaviors_ajax-error_ts-app_assets_modules_github_behaviors_include-87a4ae-0a6bb0ce2586.js"></script>
  <meta name="browser-errors-url" content="https://api.github.com/_private/browser/errors">
  <template id="copilot-error-icon">
    <svg aria-hidden="true" height="16" viewBox="0 0 16 16" version="1.1" width="16" data-view-component="true" class="octicon octicon-copilot-error">
      .hlzFvi:where([data-validation='error']){border-color:var(--borderColor-danger-emphasis,var(--color-danger-emphasis,#cf222e));}/*!sc*/
      .hlzFvi:where([data-validation='error']):where([data-trailing-action][data-focused]),.hlzFvi:where([data-validation='error']):where(:not([data-trailing-action])):focus-within{border-color:var(--fgColor-accent,var(--color-accent-fg,#0969da));outline:2px solid var(--fgColor-accent,var(--color-accent-fg,#0969da));outline-offset:-1px;}/*!sc*/
    <div id="ajax-error-message" class="ajax-error-message flash flash-error" hidden>
```

