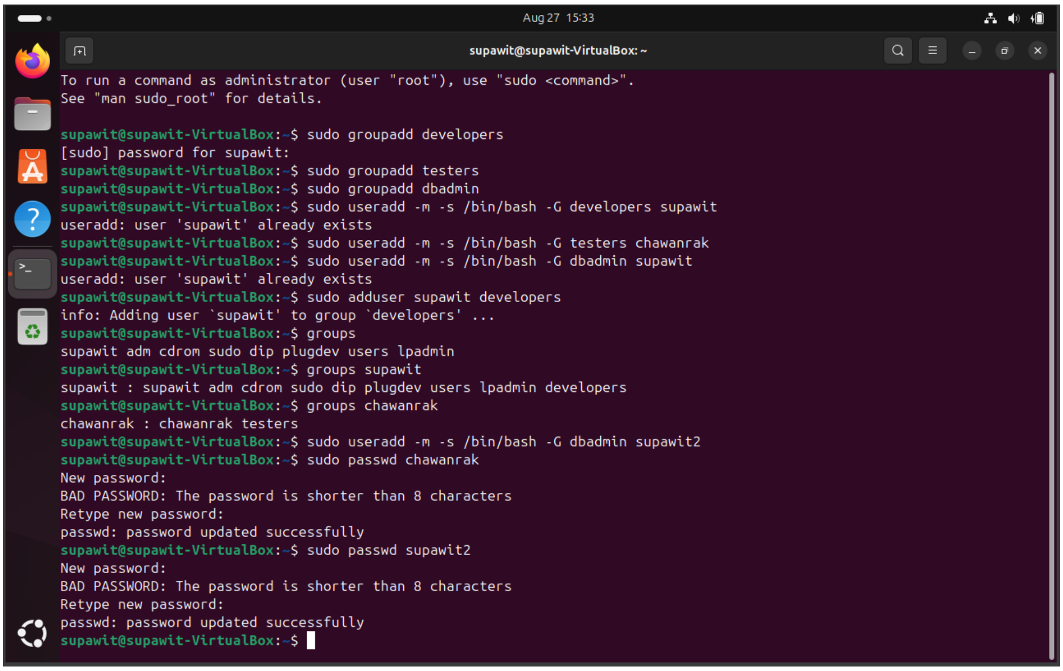
## Task 1: สร้าง User Accounts สำหรับ Team (30นาที)

### 1.1 สร้าง Users และ Groups

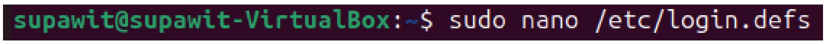
| Groups | Users | password |
|---|---|---|
| Developers | supawit | 1234 |
| Testers | chawanrak | 1234 |
| DBadmin | supawit2 | 1234 |

Screenshots การจัดการ user accounts

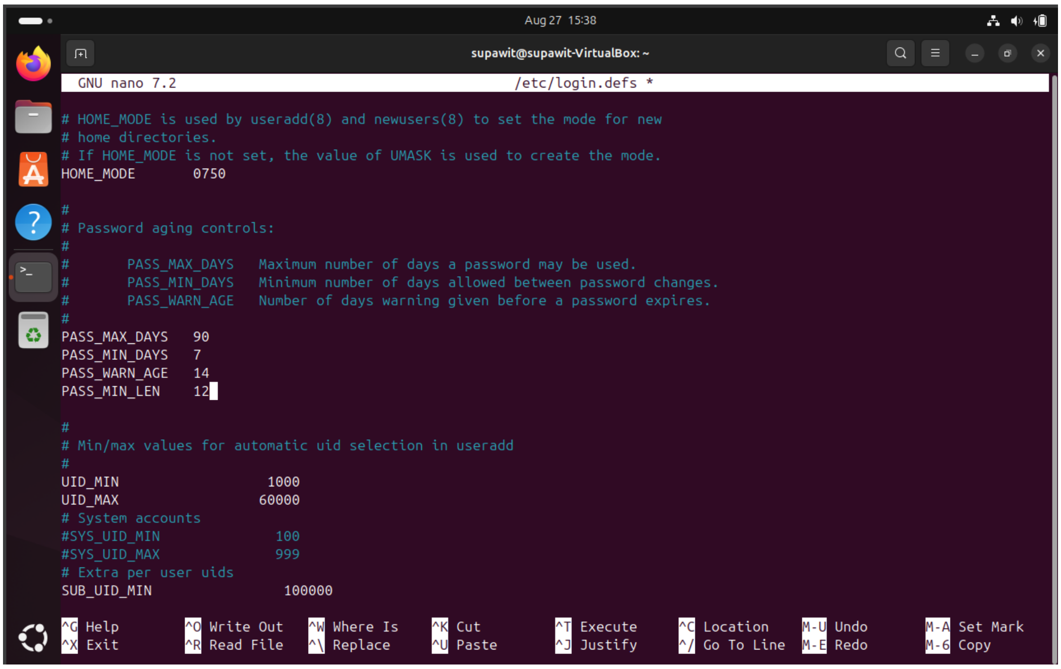


```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

supawit@supawit-VirtualBox:~$ sudo groupadd developers
[sudo] password for supawit:
supawit@supawit-VirtualBox:~$ sudo groupadd testers
supawit@supawit-VirtualBox:~$ sudo groupadd dbadmin
supawit@supawit-VirtualBox:~$ sudo useradd -m -s /bin/bash -G developers supawit
useradd: user 'supawit' already exists
supawit@supawit-VirtualBox:~$ sudo useradd -m -s /bin/bash -G testers chawanrak
supawit@supawit-VirtualBox:~$ sudo useradd -m -s /bin/bash -G dbadmin supawit
useradd: user 'supawit' already exists
supawit@supawit-VirtualBox:~$ sudo adduser supawit developers
info: Adding user `supawit' to group `developers' ...
supawit@supawit-VirtualBox:~$ groups
supawit adm cdrom sudo dip plugdev users lpadmin
supawit@supawit-VirtualBox:~$ groups supawit
supawit : supawit adm cdrom sudo dip plugdev users lpadmin developers
supawit@supawit-VirtualBox:~$ groups chawanrak
chawanrak : chawanrak testers
supawit@supawit-VirtualBox:~$ sudo useradd -m -s /bin/bash -G dbadmin supawit2
supawit@supawit-VirtualBox:~$ sudo passwd chawanrak
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
supawit@supawit-VirtualBox:~$ sudo passwd supawit2
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
supawit@supawit-VirtualBox:~$
```

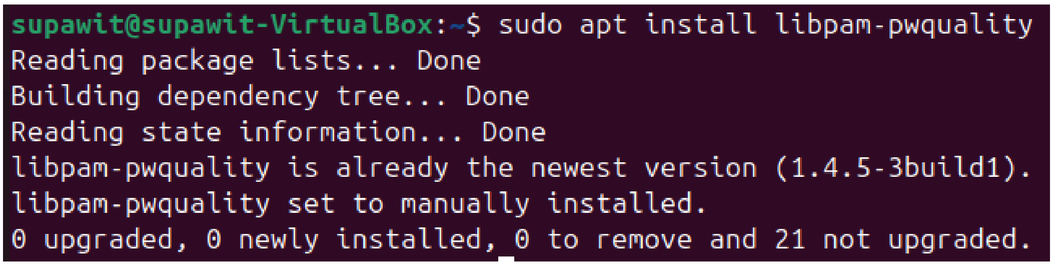
### 1.2 ตั้งค่า password policy



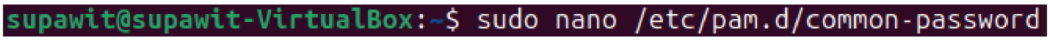
```
supawit@supawit-VirtualBox:~$ sudo nano /etc/login.defs
```



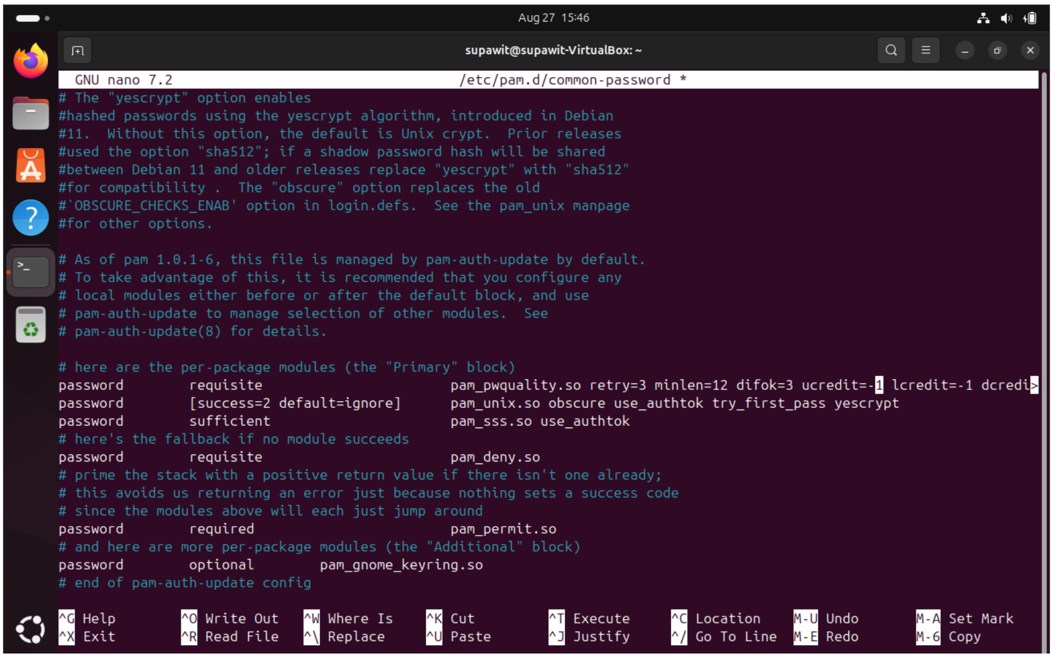
```
  GNU nano 7.2                              /etc/login.defs *

# HOME_MODE is used by useradd(8) and newusers(8) to set the mode for new
# home directories.
# If HOME_MODE is not set, the value of UMASK is used to create the mode.
HOME_MODE       0750

#
# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   90
PASS_MIN_DAYS   7
PASS_WARN_AGE   14
PASS_MIN_LEN    12


#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  1000
UID_MAX                 60000
# System accounts
#SYS_UID_MIN              100
#SYS_UID_MAX              999
# Extra per user uids
SUB_UID_MIN                100000
```



```
supawit@supawit-VirtualBox:~$ sudo apt install libpam-pwquality
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libpam-pwquality is already the newest version (1.4.5-3build1).
libpam-pwquality set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 21 not upgraded.
```

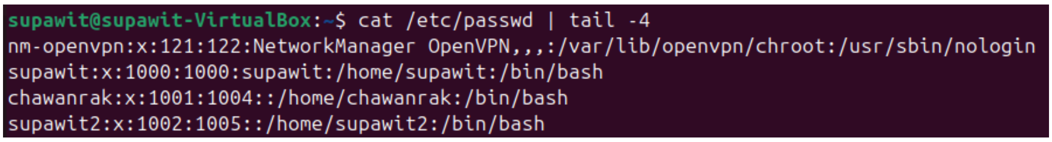


```
supawit@supawit-VirtualBox:~$ sudo nano /etc/pam.d/common-password
```

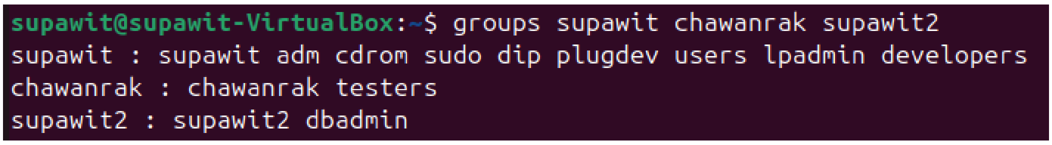


```
  GNU nano 7.2                               /etc/pam.d/common-password *
# The "yescrypt" option enables
#hashed passwords using the yescrypt algorithm, introduced in Debian
#11.  Without this option, the default is Unix crypt.  Prior releases
#used the option "sha512"; if a shadow password hash will be shared
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility .  The "obscure" option replaces the old
#`OBSCURE_CHECKS_ENAB' option in login.defs.  See the pam_unix manpage
#for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password        requisite                       pam_pwquality.so retry=3 minlen=12 difok=3 ucredit=-1 lcredit=-1 dcredi>
password        [success=2 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yescrypt
password        sufficient                      pam_sss.so use_authtok
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
# end of pam-auth-update config

^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location   M-U Undo     M-A Set Mark
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line M-E Redo     M-6 Copy
```

1.3 ใช้คำสั่งทดสอบ



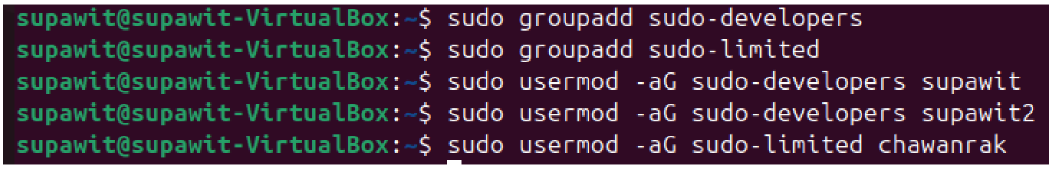
```
supawit@supawit-VirtualBox:~$ cat /etc/passwd | tail -4
nm-openvpn:x:121:122:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
supawit:x:1000:1000:supawit:/home/supawit:/bin/bash
chawanrak:x:1001:1004::/home/chawanrak:/bin/bash
supawit2:x:1002:1005::/home/supawit2:/bin/bash
```



```
supawit@supawit-VirtualBox:~$ groups supawit chawanrak supawit2
supawit : supawit adm cdrom sudo dip plugdev users lpadmin developers
chawanrak : chawanrak testers
supawit2 : supawit2 dbadmin
```

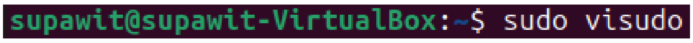
## Task 2: ตั้งค่า Sudo permission (45นาที)

### 2.1 สร้าง Sudo Groups

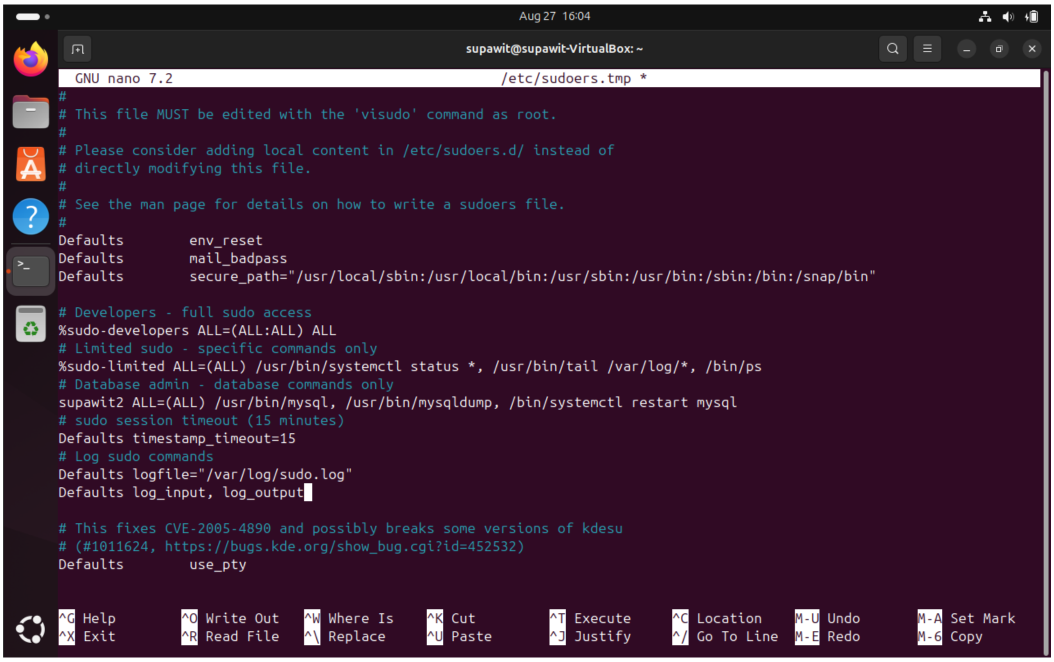


```
supawit@supawit-VirtualBox:~$ sudo groupadd sudo-developers
supawit@supawit-VirtualBox:~$ sudo groupadd sudo-limited
supawit@supawit-VirtualBox:~$ sudo usermod -aG sudo-developers supawit
supawit@supawit-VirtualBox:~$ sudo usermod -aG sudo-developers supawit2
supawit@supawit-VirtualBox:~$ sudo usermod -aG sudo-limited chawanrak
```

### 2.2 Configure sudoers

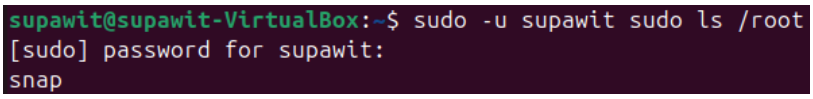


```
supawit@supawit-VirtualBox:~$ sudo visudo
```

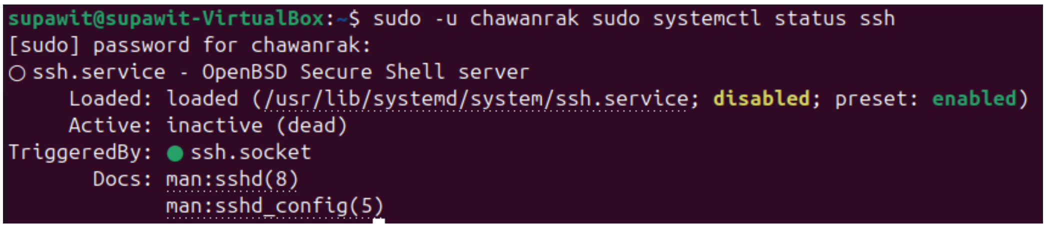


```
  GNU nano 7.2                                  /etc/sudoers.tmp *
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Developers - full sudo access
%sudo-developers ALL=(ALL:ALL) ALL
# Limited sudo - specific commands only
%sudo-limited ALL=(ALL) /usr/bin/systemctl status *, /usr/bin/tail /var/log/*, /bin/ps
# Database admin - database commands only
supawit2 ALL=(ALL) /usr/bin/mysql, /usr/bin/mysqldump, /bin/systemctl restart mysql
# sudo session timeout (15 minutes)
Defaults timestamp_timeout=15
# Log sudo commands
Defaults logfile="/var/log/sudo.log"
Defaults log_input, log_output

# This fixes CVE-2005-4890 and possibly breaks some versions of kdesu
# (#1011624, https://bugs.kde.org/show_bug.cgi?id=452532)
Defaults        use_pty

^G Help      ^O Write Out  ^W Where Is  ^K Cut     ^T Execute  ^C Location   M-U Undo   M-A Set Mark
^X Exit      ^R Read File  ^\ Replace   ^U Paste   ^J Justify  ^/ Go To Line M-E Redo   M-6 Copy
```

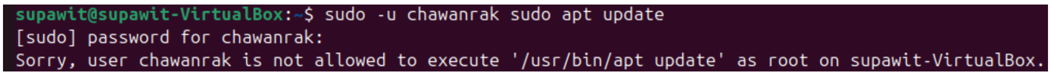
### 2.3 ทดสอบ sudo permissions



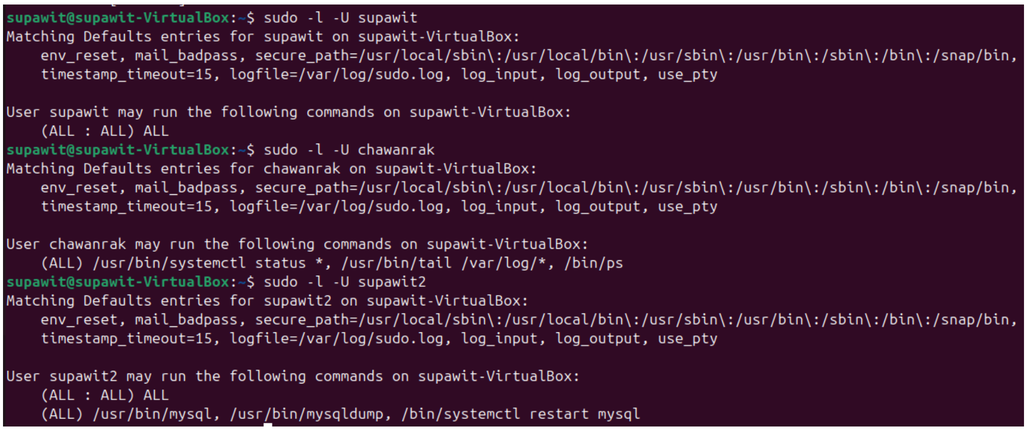
```
supawit@supawit-VirtualBox:~$ sudo -u supawit sudo ls /root
[sudo] password for supawit:
snap
```



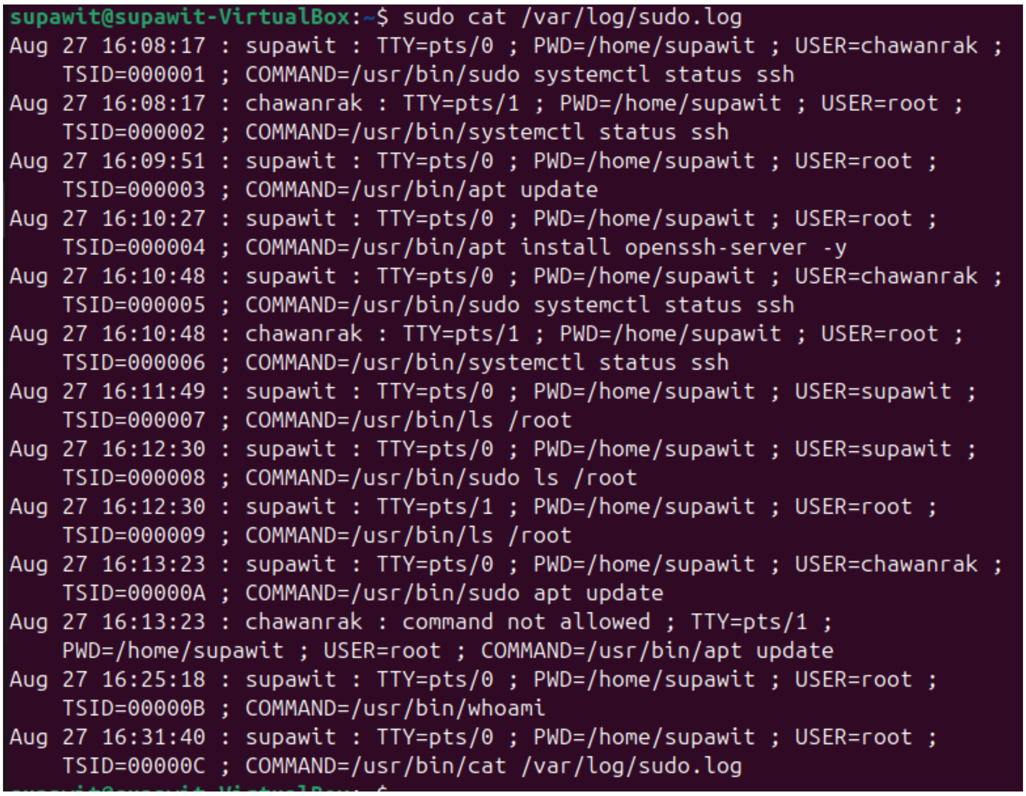
```
supawit@supawit-VirtualBox:~$ sudo -u chawanrak sudo systemctl status ssh
[sudo] password for chawanrak:
○ ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
     Active: inactive (dead)
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
```



```
supawit@supawit-VirtualBox:~$ sudo -u chawanrak sudo apt update
[sudo] password for chawanrak:
Sorry, user chawanrak is not allowed to execute '/usr/bin/apt update' as root on supawit-VirtualBox.
```



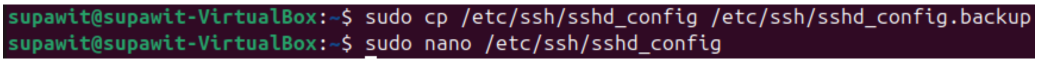
```
supawit@supawit-VirtualBox:~$ sudo -l -U supawit
Matching Defaults entries for supawit on supawit-VirtualBox:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    timestamp_timeout=15, logfile=/var/log/sudo.log, log_input, log_output, use_pty

User supawit may run the following commands on supawit-VirtualBox:
    (ALL : ALL) ALL
supawit@supawit-VirtualBox:~$ sudo -l -U chawanrak
Matching Defaults entries for chawanrak on supawit-VirtualBox:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    timestamp_timeout=15, logfile=/var/log/sudo.log, log_input, log_output, use_pty

User chawanrak may run the following commands on supawit-VirtualBox:
    (ALL) /usr/bin/systemctl status *, /usr/bin/tail /var/log/*, /bin/ps
supawit@supawit-VirtualBox:~$ sudo -l -U supawit2
Matching Defaults entries for supawit2 on supawit-VirtualBox:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    timestamp_timeout=15, logfile=/var/log/sudo.log, log_input, log_output, use_pty

User supawit2 may run the following commands on supawit-VirtualBox:
    (ALL : ALL) ALL
    (ALL) /usr/bin/mysql, /usr/bin/mysqldump, /bin/systemctl restart mysql
```



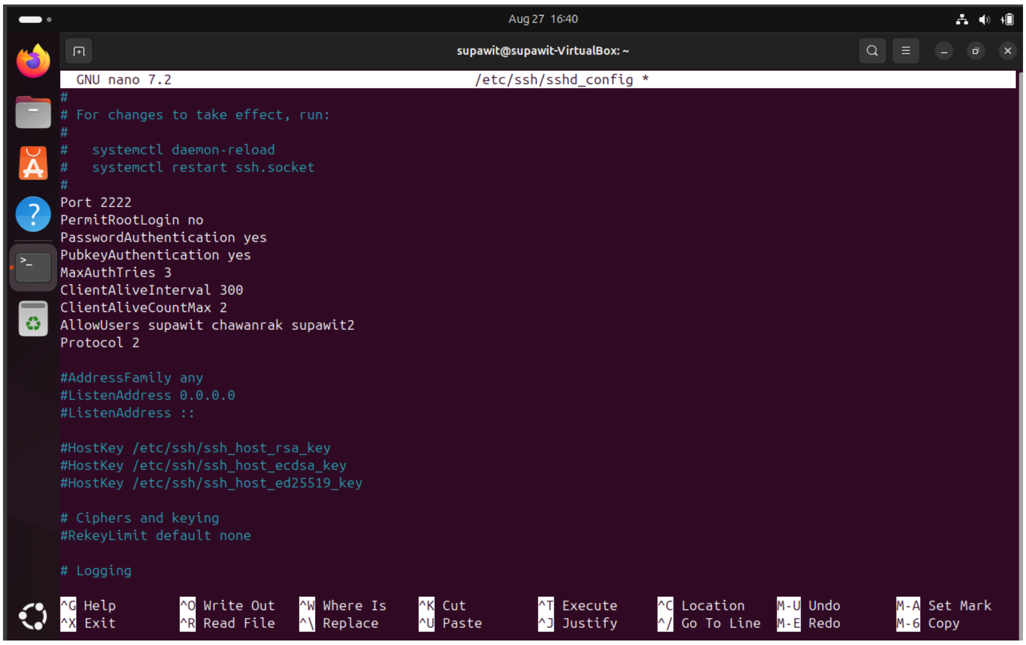
```
supawit@supawit-VirtualBox:~$ sudo cat /var/log/sudo.log
Aug 27 16:08:17 : supawit : TTY=pts/0 ; PWD=/home/supawit ; USER=chawanrak ;
    TSID=000001 ; COMMAND=/usr/bin/sudo systemctl status ssh
Aug 27 16:08:17 : chawanrak : TTY=pts/1 ; PWD=/home/supawit ; USER=root ;
    TSID=000002 ; COMMAND=/usr/bin/systemctl status ssh
Aug 27 16:09:51 : supawit : TTY=pts/0 ; PWD=/home/supawit ; USER=root ;
    TSID=000003 ; COMMAND=/usr/bin/apt update
Aug 27 16:10:27 : supawit : TTY=pts/0 ; PWD=/home/supawit ; USER=root ;
    TSID=000004 ; COMMAND=/usr/bin/apt install openssh-server -y
Aug 27 16:10:48 : supawit : TTY=pts/0 ; PWD=/home/supawit ; USER=chawanrak ;
    TSID=000005 ; COMMAND=/usr/bin/sudo systemctl status ssh
Aug 27 16:10:48 : chawanrak : TTY=pts/1 ; PWD=/home/supawit ; USER=root ;
    TSID=000006 ; COMMAND=/usr/bin/systemctl status ssh
Aug 27 16:11:49 : supawit : TTY=pts/0 ; PWD=/home/supawit ; USER=supawit ;
    TSID=000007 ; COMMAND=/usr/bin/ls /root
Aug 27 16:12:30 : supawit : TTY=pts/0 ; PWD=/home/supawit ; USER=supawit ;
    TSID=000008 ; COMMAND=/usr/bin/sudo ls /root
Aug 27 16:12:30 : supawit : TTY=pts/1 ; PWD=/home/supawit ; USER=root ;
    TSID=000009 ; COMMAND=/usr/bin/ls /root
Aug 27 16:13:23 : supawit : TTY=pts/0 ; PWD=/home/supawit ; USER=chawanrak ;
    TSID=00000A ; COMMAND=/usr/bin/sudo apt update
Aug 27 16:13:23 : chawanrak : command not allowed ; TTY=pts/1 ;
    PWD=/home/supawit ; USER=root ; COMMAND=/usr/bin/apt update
Aug 27 16:25:18 : supawit : TTY=pts/0 ; PWD=/home/supawit ; USER=root ;
    TSID=00000B ; COMMAND=/usr/bin/whoami
Aug 27 16:31:40 : supawit : TTY=pts/0 ; PWD=/home/supawit ; USER=root ;
    TSID=00000C ; COMMAND=/usr/bin/cat /var/log/sudo.log
```

## Task 3: Configure ssh Security (45 นาที)

### 3.1 Backup และแก้ไข SSH Config

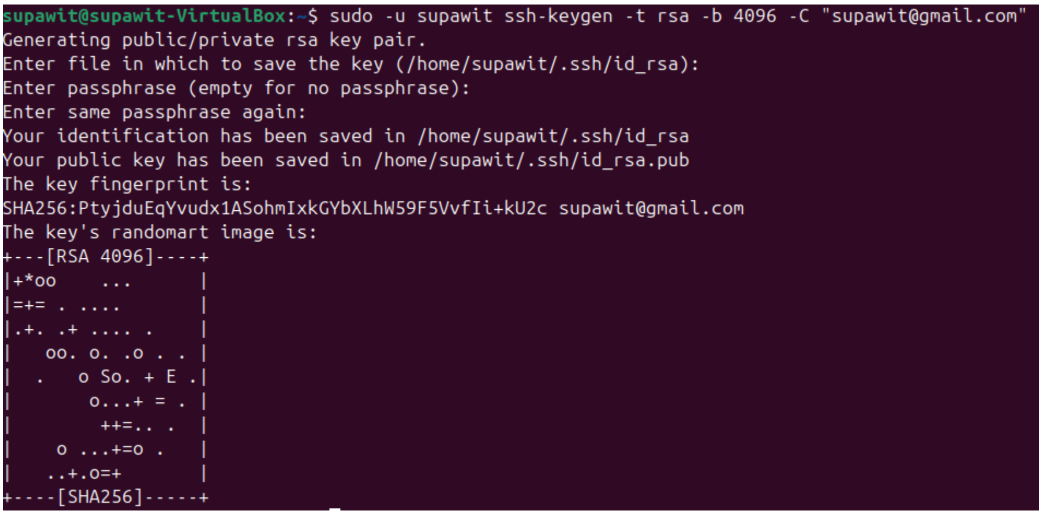


```
supawit@supawit-VirtualBox:~$ sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.backup
supawit@supawit-VirtualBox:~$ sudo nano /etc/ssh/sshd_config
```

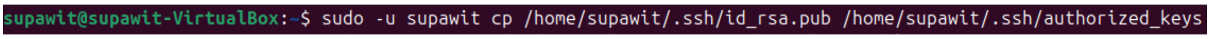


```
  GNU nano 7.2                          /etc/ssh/sshd_config *
#
# For changes to take effect, run:
#
#   systemctl daemon-reload
#   systemctl restart ssh.socket
#
Port 2222
PermitRootLogin no
PasswordAuthentication yes
PubkeyAuthentication yes
MaxAuthTries 3
ClientAliveInterval 300
ClientAliveCountMax 2
AllowUsers supawit chawanrak supawit2
Protocol 2

#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
```

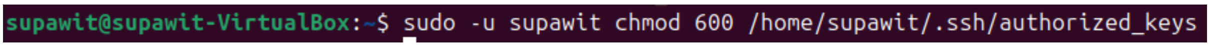
3.2 สร้าง SSH keys



```
supawit@supawit-VirtualBox:~$ sudo -u supawit ssh-keygen -t rsa -b 4096 -C "supawit@gmail.com"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/supawit/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/supawit/.ssh/id_rsa
Your public key has been saved in /home/supawit/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:PtyjduEqYvudx1ASohmIxkGYbXLhW59F5VvfIi+kU2c supawit@gmail.com
The key's randomart image is:
+---[RSA 4096]----+
|+*oo    ...      |
|=+= . ....       |
|.+. .+ .... .    |
|   oo. o. .o . . |
|  .   o So. + E .|
|       o...+ = . |
|        ++=.. .  |
|    o ...+=o .   |
|   ..+.o=+       |
+----[SHA256]-----+
```

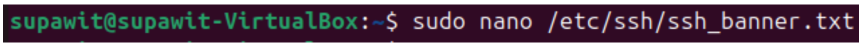


```
supawit@supawit-VirtualBox:~$ sudo -u supawit cp /home/supawit/.ssh/id_rsa.pub /home/supawit/.ssh/authorized_keys
```

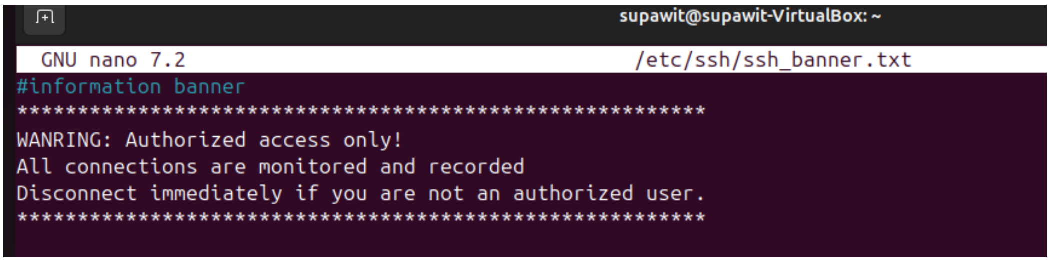


```
supawit@supawit-VirtualBox:~$ sudo -u supawit chmod 600 /home/supawit/.ssh/authorized_keys
```

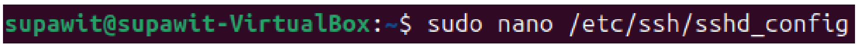
3.3 configure SSH Banner



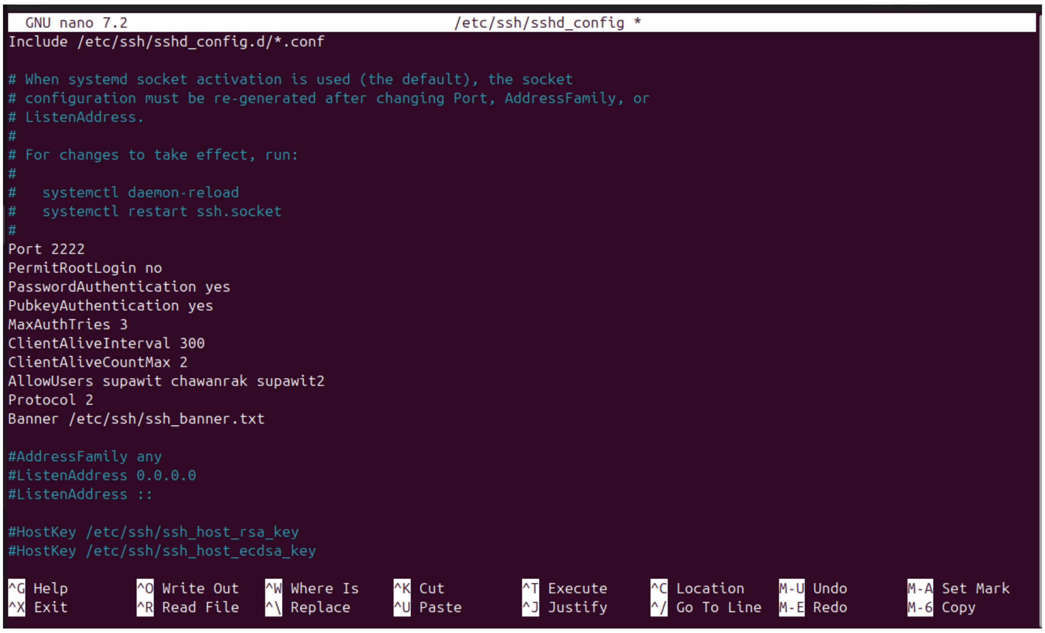
```
supawit@supawit-VirtualBox:~$ sudo nano /etc/ssh/ssh_banner.txt
```



```
  GNU nano 7.2                               /etc/ssh/ssh_banner.txt
#information banner
****************************************************************
WANRING: Authorized access only!
All connections are monitored and recorded
Disconnect immediately if you are not an authorized user.
****************************************************************
```

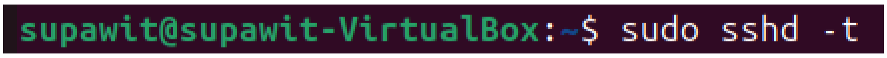


```
supawit@supawit-VirtualBox:~$ sudo nano /etc/ssh/sshd_config
```

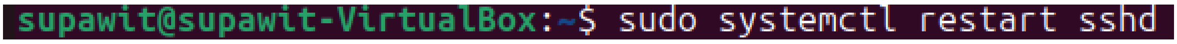


```
  GNU nano 7.2                               /etc/ssh/sshd_config *
Include /etc/ssh/sshd_config.d/*.conf

# When systemd socket activation is used (the default), the socket
# configuration must be re-generated after changing Port, AddressFamily, or
# ListenAddress.
#
# For changes to take effect, run:
#
#   systemctl daemon-reload
#   systemctl restart ssh.socket
#
Port 2222
PermitRootLogin no
PasswordAuthentication yes
PubkeyAuthentication yes
MaxAuthTries 3
ClientAliveInterval 300
ClientAliveCountMax 2
AllowUsers supawit chawanrak supawit2
Protocol 2
Banner /etc/ssh/ssh_banner.txt

#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
```

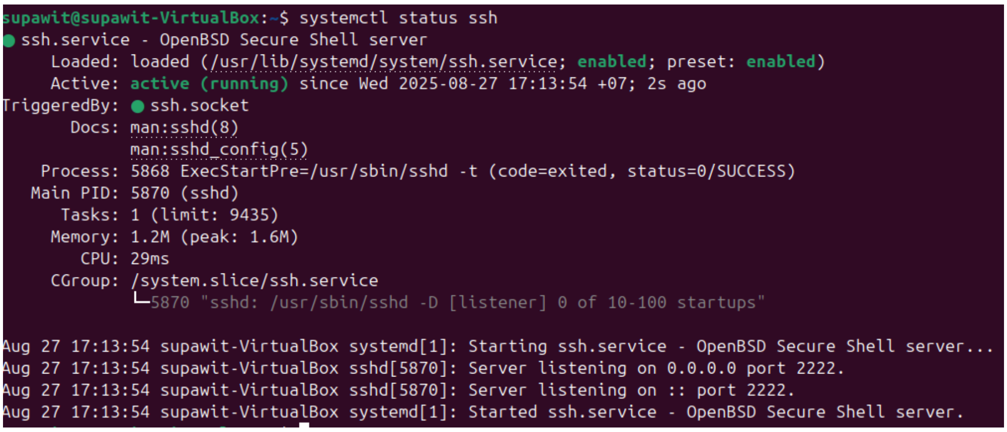
### 3.4 Restart SSH และ ทดสอบ



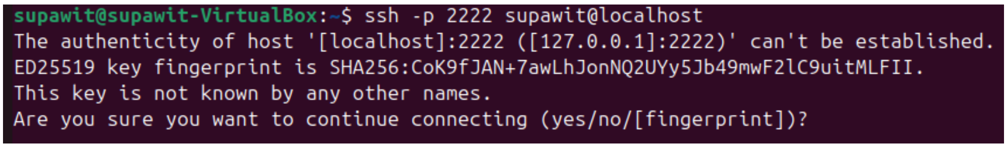
```
supawit@supawit-VirtualBox:~$ sudo sshd -t
```



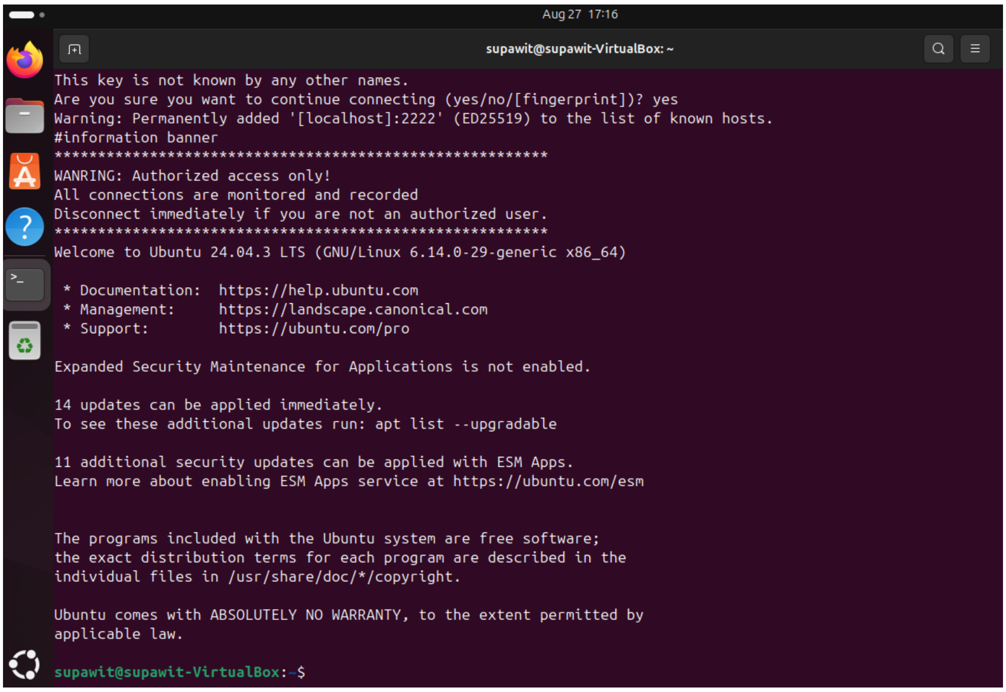
```
supawit@supawit-VirtualBox:~$ sudo systemctl restart sshd
```



```
supawit@supawit-VirtualBox:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-08-27 17:13:54 +07; 2s ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 5868 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 5870 (sshd)
      Tasks: 1 (limit: 9435)
     Memory: 1.2M (peak: 1.6M)
        CPU: 29ms
     CGroup: /system.slice/ssh.service
             └─5870 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 27 17:13:54 supawit-VirtualBox systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Aug 27 17:13:54 supawit-VirtualBox sshd[5870]: Server listening on 0.0.0.0 port 2222.
Aug 27 17:13:54 supawit-VirtualBox sshd[5870]: Server listening on :: port 2222.
Aug 27 17:13:54 supawit-VirtualBox systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```



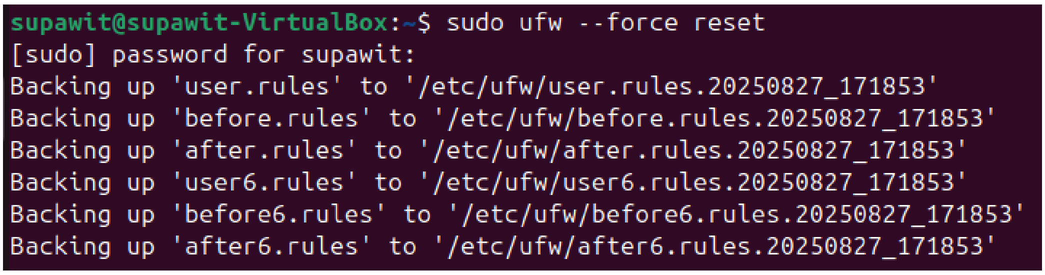
```
supawit@supawit-VirtualBox:~$ ssh -p 2222 supawit@localhost
The authenticity of host '[localhost]:2222 ([127.0.0.1]:2222)' can't be established.
ED25519 key fingerprint is SHA256:CoK9fJAN+7awLhJonNQ2UYy5Jb49mwF2lC9uitMLFII.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```



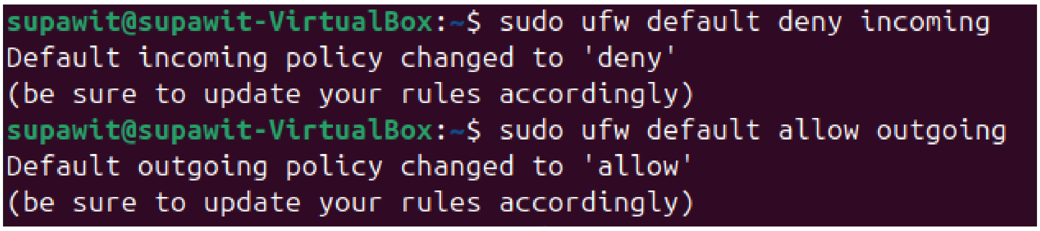
```
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:2222' (ED25519) to the list of known hosts.
#information banner
**********************************************************
WANRING: Authorized access only!
All connections are monitored and recorded
Disconnect immediately if you are not an authorized user.
**********************************************************
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-29-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

14 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

11 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

supawit@supawit-VirtualBox:~$
```

## Task 4: Set up Firewall Rules (30 นาที)

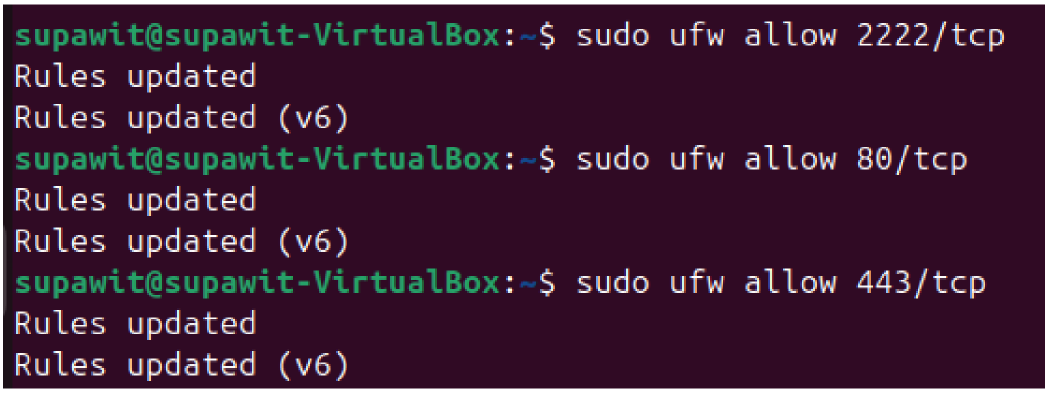
4.1 Configure UFW



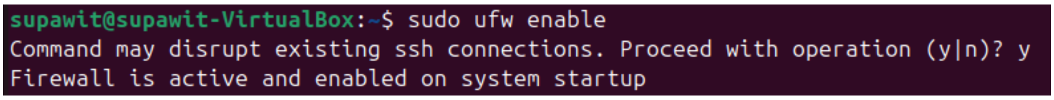
```
supawit@supawit-VirtualBox:~$ sudo ufw --force reset
[sudo] password for supawit:
Backing up 'user.rules' to '/etc/ufw/user.rules.20250827_171853'
Backing up 'before.rules' to '/etc/ufw/before.rules.20250827_171853'
Backing up 'after.rules' to '/etc/ufw/after.rules.20250827_171853'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20250827_171853'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20250827_171853'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20250827_171853'
```



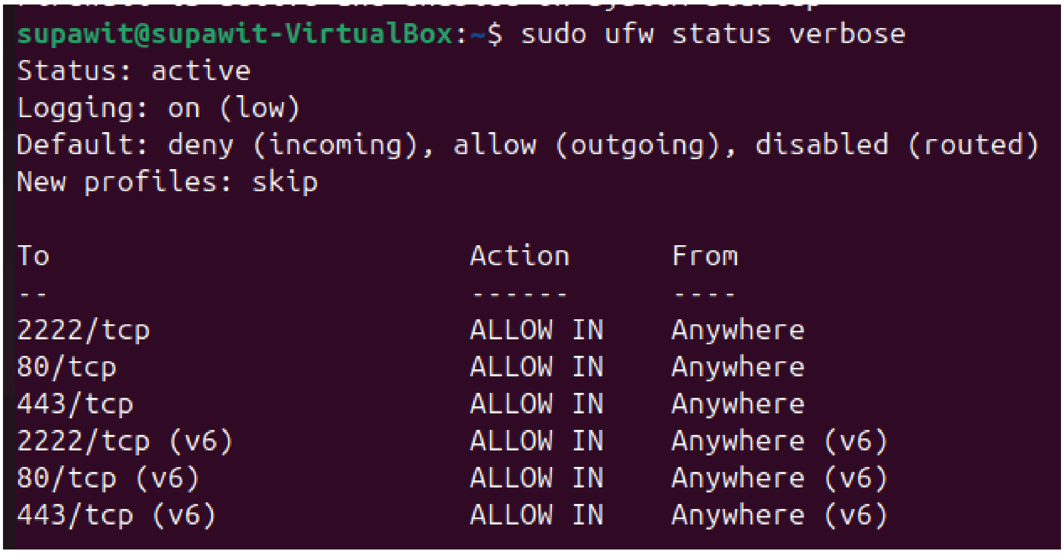
```
supawit@supawit-VirtualBox:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
supawit@supawit-VirtualBox:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
```



```
supawit@supawit-VirtualBox:~$ sudo ufw allow 2222/tcp
Rules updated
Rules updated (v6)
supawit@supawit-VirtualBox:~$ sudo ufw allow 80/tcp
Rules updated
Rules updated (v6)
supawit@supawit-VirtualBox:~$ sudo ufw allow 443/tcp
Rules updated
Rules updated (v6)
```

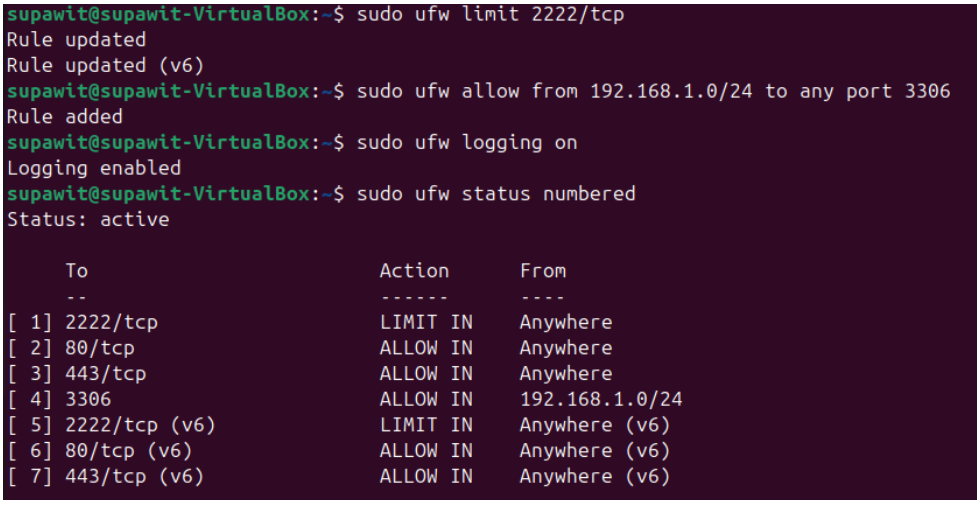


```
supawit@supawit-VirtualBox:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

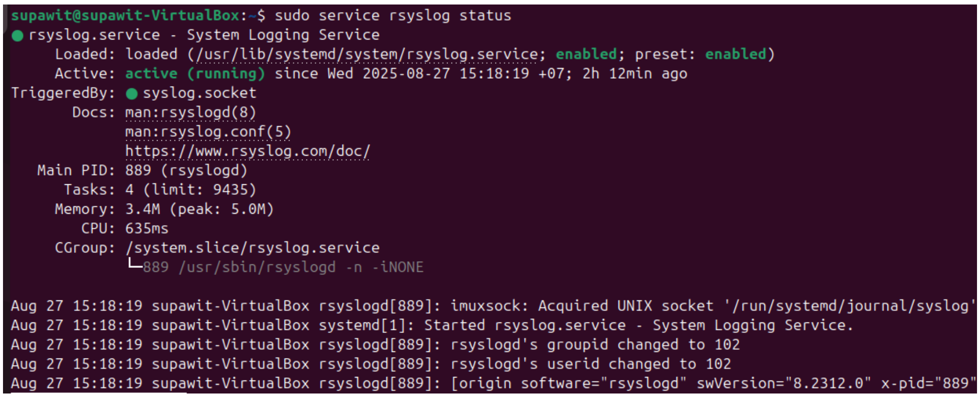


```
supawit@supawit-VirtualBox:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
2222/tcp                   ALLOW IN    Anywhere
80/tcp                     ALLOW IN    Anywhere
443/tcp                    ALLOW IN    Anywhere
2222/tcp (v6)              ALLOW IN    Anywhere (v6)
80/tcp (v6)                ALLOW IN    Anywhere (v6)
443/tcp (v6)               ALLOW IN    Anywhere (v6)
```

### 4.2 Advance UFW Rules



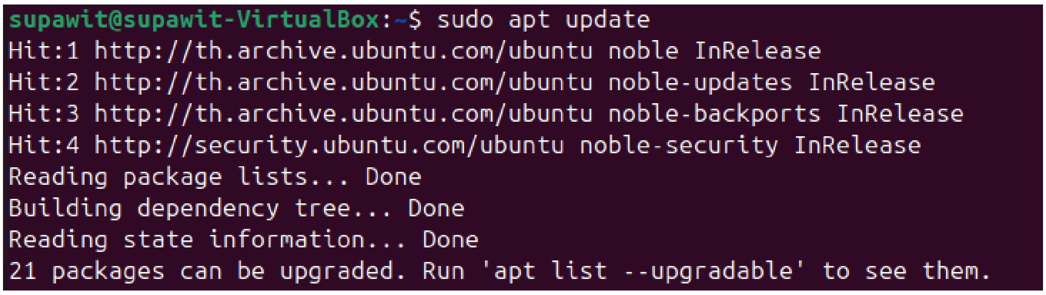
```
supawit@supawit-VirtualBox:~$ sudo ufw limit 2222/tcp
Rule updated
Rule updated (v6)
supawit@supawit-VirtualBox:~$ sudo ufw allow from 192.168.1.0/24 to any port 3306
Rule added
supawit@supawit-VirtualBox:~$ sudo ufw logging on
Logging enabled
supawit@supawit-VirtualBox:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 2222/tcp                   LIMIT IN    Anywhere
[ 2] 80/tcp                     ALLOW IN    Anywhere
[ 3] 443/tcp                    ALLOW IN    Anywhere
[ 4] 3306                       ALLOW IN    192.168.1.0/24
[ 5] 2222/tcp (v6)              LIMIT IN    Anywhere (v6)
[ 6] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 7] 443/tcp (v6)               ALLOW IN    Anywhere (v6)
```



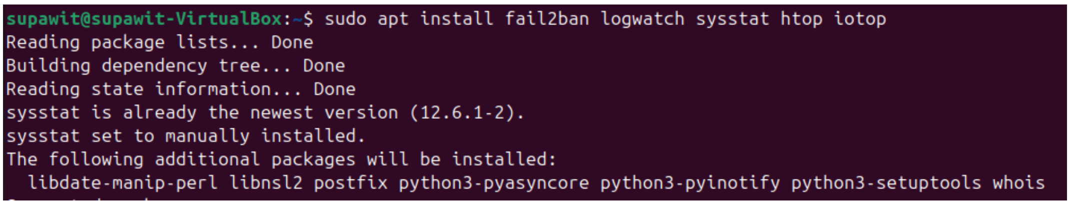
```
supawit@supawit-VirtualBox:~$ sudo service rsyslog status
● rsyslog.service - System Logging Service
     Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-08-27 15:18:19 +07; 2h 12min ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 889 (rsyslogd)
      Tasks: 4 (limit: 9435)
     Memory: 3.4M (peak: 5.0M)
        CPU: 635ms
     CGroup: /system.slice/rsyslog.service
             └─889 /usr/sbin/rsyslogd -n -iNONE

Aug 27 15:18:19 supawit-VirtualBox rsyslogd[889]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog'
Aug 27 15:18:19 supawit-VirtualBox systemd[1]: Started rsyslog.service - System Logging Service.
Aug 27 15:18:19 supawit-VirtualBox rsyslogd[889]: rsyslogd's groupid changed to 102
Aug 27 15:18:19 supawit-VirtualBox rsyslogd[889]: rsyslogd's userid changed to 102
Aug 27 15:18:19 supawit-VirtualBox rsyslogd[889]: [origin software="rsyslogd" swVersion="8.2312.0" x-pid="889"
```

## Task 5: Enable System Monitoring (60 นาที)

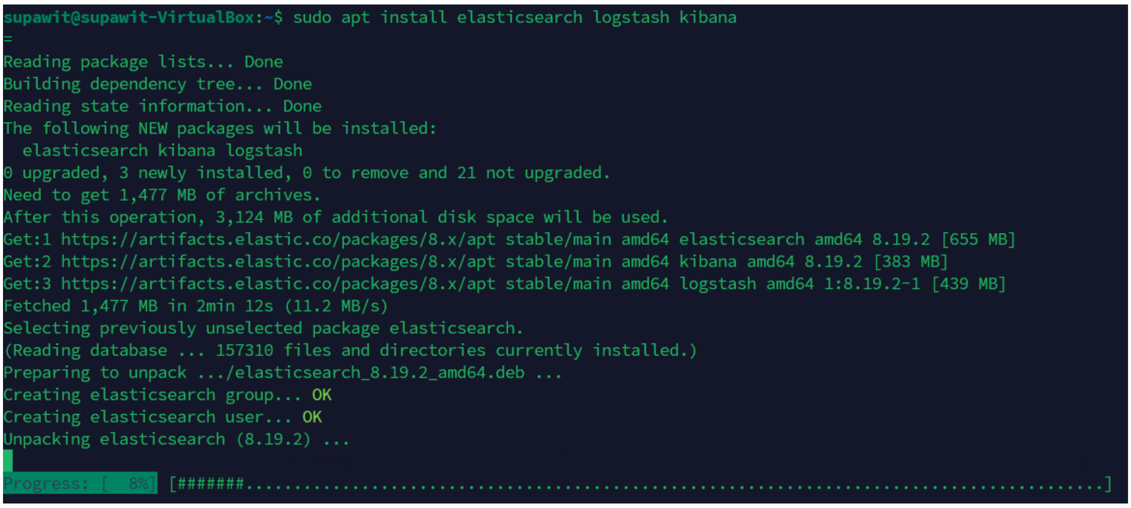
### 5.1 Install Monitoring Tools



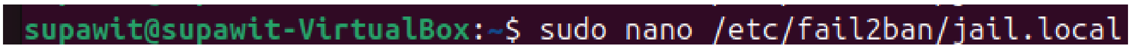
```
supawit@supawit-VirtualBox:~$ sudo apt update
Hit:1 http://th.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://th.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://th.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
21 packages can be upgraded. Run 'apt list --upgradable' to see them.
```



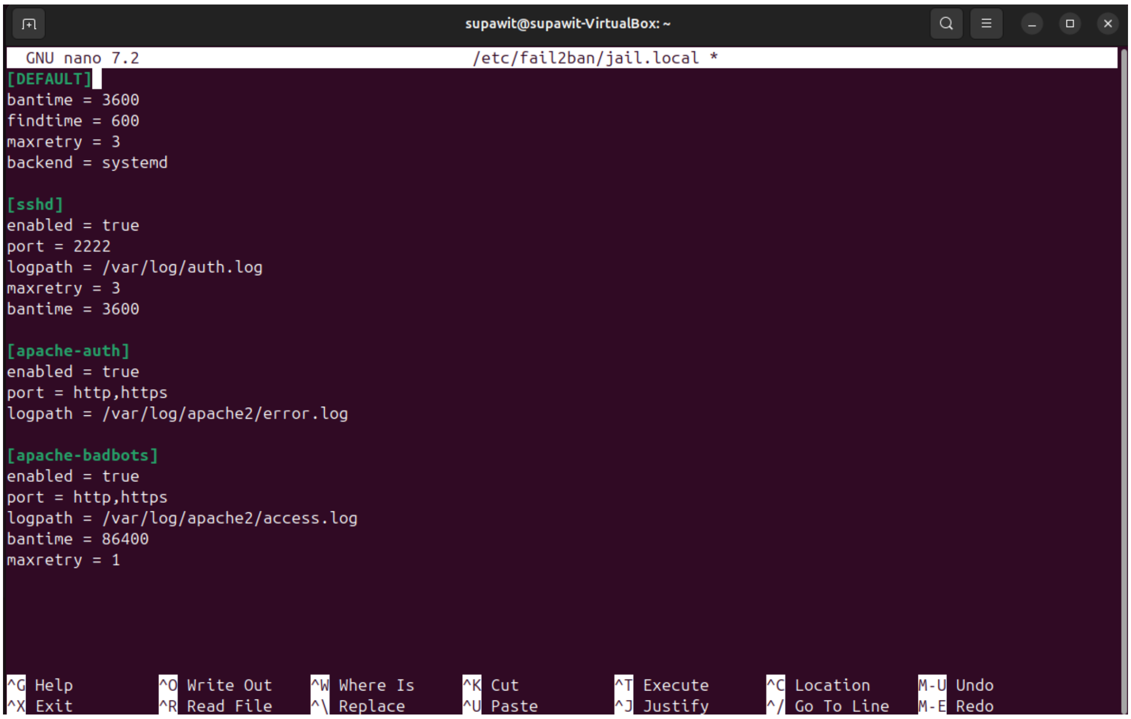
```
supawit@supawit-VirtualBox:~$ sudo apt install fail2ban logwatch sysstat htop iotop
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
sysstat is already the newest version (12.6.1-2).
sysstat set to manually installed.
The following additional packages will be installed:
  libdate-manip-perl libnsl2 postfix python3-pyasyncore python3-pyinotify python3-setuptools whois
```



```
supawit@supawit-VirtualBox:~$ sudo apt install elasticsearch logstash kibana
=
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  elasticsearch kibana logstash
0 upgraded, 3 newly installed, 0 to remove and 21 not upgraded.
Need to get 1,477 MB of archives.
After this operation, 3,124 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 elasticsearch amd64 8.19.2 [655 MB]
Get:2 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 kibana amd64 8.19.2 [383 MB]
Get:3 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 logstash amd64 1:8.19.2-1 [439 MB]
Fetched 1,477 MB in 2min 12s (11.2 MB/s)
Selecting previously unselected package elasticsearch.
(Reading database ... 157310 files and directories currently installed.)
Preparing to unpack .../elasticsearch_8.19.2_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (8.19.2) ...

Progress: [  8%] [#######.............................................................................]
```

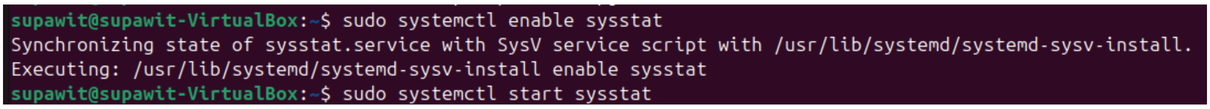


```
supawit@supawit-VirtualBox:~$ sudo nano /etc/fail2ban/jail.local
```

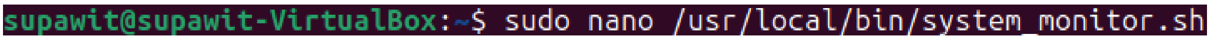


```
[DEFAULT]
bantime = 3600
findtime = 600
maxretry = 3
backend = systemd

[sshd]
enabled = true
port = 2222
logpath = /var/log/auth.log
maxretry = 3
bantime = 3600

[apache-auth]
enabled = true
port = http,https
logpath = /var/log/apache2/error.log

[apache-badbots]
enabled = true
port = http,https
logpath = /var/log/apache2/access.log
bantime = 86400
maxretry = 1
```

## 5.3 Configure System Monitoring

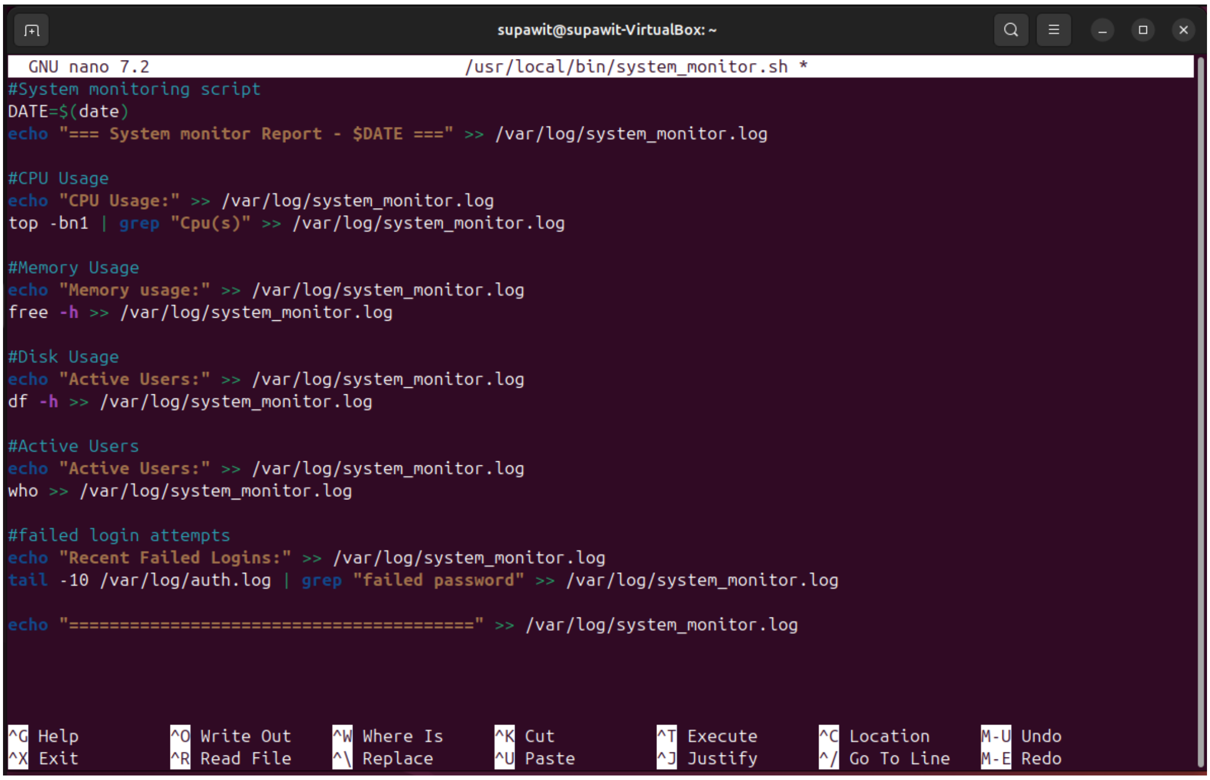


```
supawit@supawit-VirtualBox:~$ sudo systemctl enable sysstat
Synchronizing state of sysstat.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable sysstat
supawit@supawit-VirtualBox:~$ sudo systemctl start sysstat
```

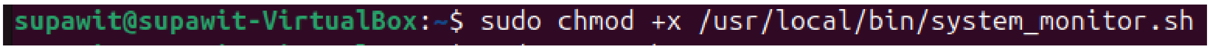


```
supawit@supawit-VirtualBox:~$ sudo nano /usr/local/bin/system_monitor.sh
```

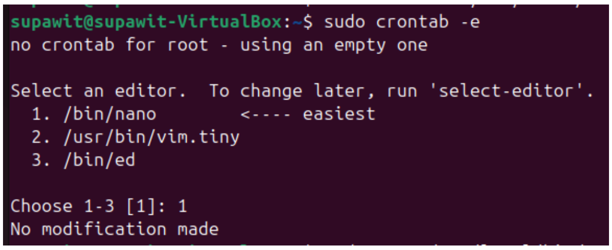
กลุ่ม 5 นายศุภวิชญ์ แก่นนาค และ นางสาวชวัลลักษณ์ ไพบูลย์ชมพู



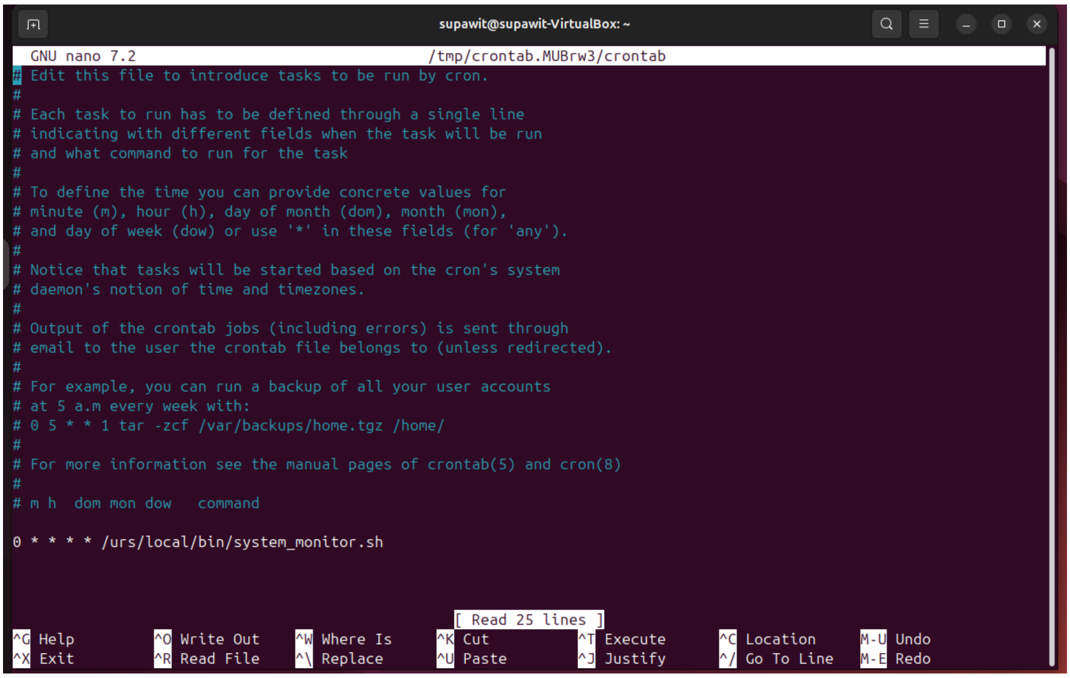
```
  GNU nano 7.2                    /usr/local/bin/system_monitor.sh *
#System monitoring script
DATE=$(date)
echo "=== System monitor Report - $DATE ===" >> /var/log/system_monitor.log

#CPU Usage
echo "CPU Usage:" >> /var/log/system_monitor.log
top -bn1 | grep "Cpu(s)" >> /var/log/system_monitor.log

#Memory Usage
echo "Memory usage:" >> /var/log/system_monitor.log
free -h >> /var/log/system_monitor.log

#Disk Usage
echo "Active Users:" >> /var/log/system_monitor.log
df -h >> /var/log/system_monitor.log

#Active Users
echo "Active Users:" >> /var/log/system_monitor.log
who >> /var/log/system_monitor.log

#failed login attempts
echo "Recent Failed Logins:" >> /var/log/system_monitor.log
tail -10 /var/log/auth.log | grep "failed password" >> /var/log/system_monitor.log

echo "========================================" >> /var/log/system_monitor.log



^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^/ Go To Line   M-E Redo
```



```
supawit@supawit-VirtualBox:~$ sudo chmod +x /usr/local/bin/system_monitor.sh
```

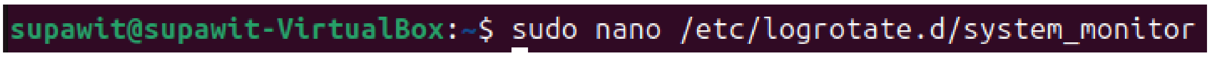


```
supawit@supawit-VirtualBox:~$ sudo crontab -e
no crontab for root - using an empty one

Select an editor.  To change later, run 'select-editor'.
  1. /bin/nano        <---- easiest
  2. /usr/bin/vim.tiny
  3. /bin/ed

Choose 1-3 [1]: 1
No modification made
```

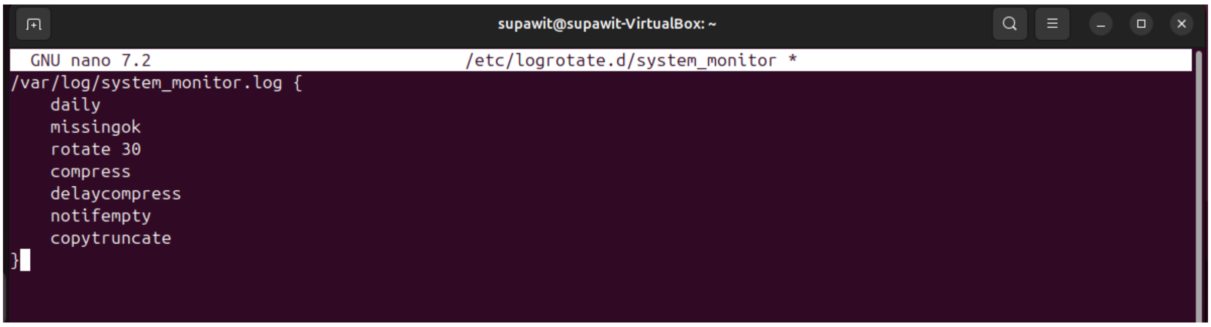


```
  GNU nano 7.2                          /tmp/crontab.MUBrw3/crontab
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define 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 * * * * /urs/local/bin/system_monitor.sh


                                      [ Read 25 lines ]
^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^/ Go To Line   M-E Redo
```

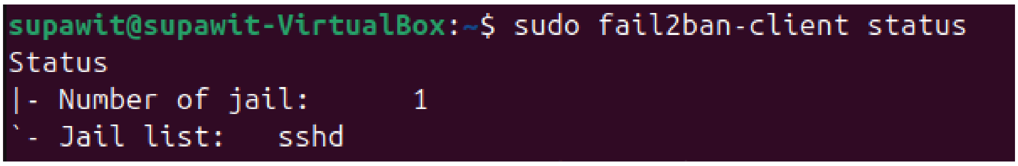
5.4 Configure Log Rotation



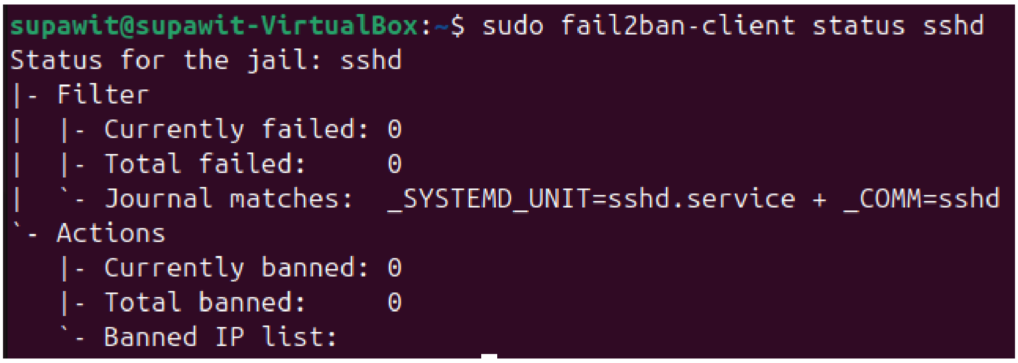
```
supawit@supawit-VirtualBox:~$ sudo nano /etc/logrotate.d/system_monitor
```



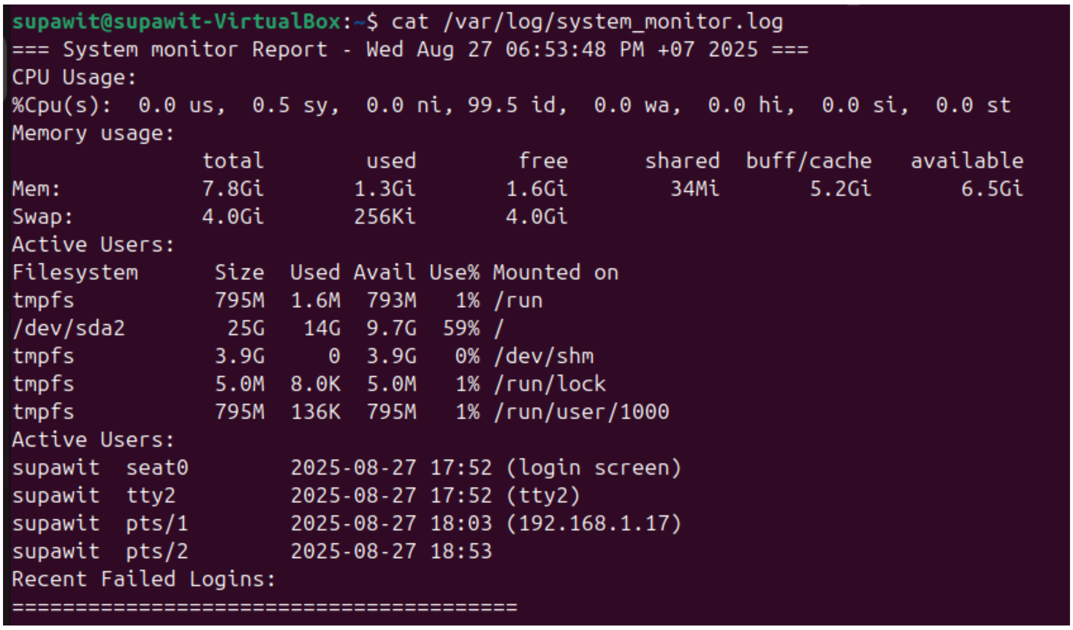
```
  GNU nano 7.2                          /etc/logrotate.d/system_monitor *
/var/log/system_monitor.log {
    daily
    missingok
    rotate 30
    compress
    delaycompress
    notifempty
    copytruncate
}
```



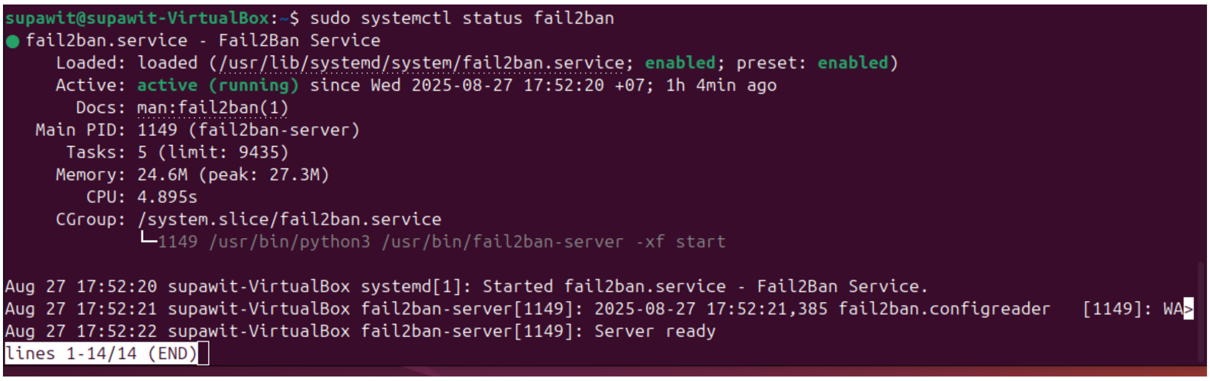
```
supawit@supawit-VirtualBox:~$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
```



```
supawit@supawit-VirtualBox:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
```



```
supawit@supawit-VirtualBox:~$ cat /var/log/system_monitor.log
=== System monitor Report - Wed Aug 27 06:53:48 PM +07 2025 ===
CPU Usage:
%Cpu(s):  0.0 us,  0.5 sy,  0.0 ni, 99.5 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
Memory usage:
               total        used        free      shared  buff/cache   available
Mem:           7.8Gi       1.3Gi       1.6Gi        34Mi       5.2Gi       6.5Gi
Swap:          4.0Gi       256Ki       4.0Gi
Active Users:
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           795M  1.6M  793M   1% /run
/dev/sda2        25G   14G  9.7G  59% /
tmpfs           3.9G     0  3.9G   0% /dev/shm
tmpfs           5.0M  8.0K  5.0M   1% /run/lock
tmpfs           795M  136K  795M   1% /run/user/1000
Active Users:
supawit  seat0        2025-08-27 17:52 (login screen)
supawit  tty2         2025-08-27 17:52 (tty2)
supawit  pts/1        2025-08-27 18:03 (192.168.1.17)
supawit  pts/2        2025-08-27 18:53
Recent Failed Logins:
========================================
```



```
supawit@supawit-VirtualBox:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-08-27 17:52:20 +07; 1h 4min ago
       Docs: man:fail2ban(1)
   Main PID: 1149 (fail2ban-server)
      Tasks: 5 (limit: 9435)
     Memory: 24.6M (peak: 27.3M)
        CPU: 4.895s
     CGroup: /system.slice/fail2ban.service
             └─1149 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Aug 27 17:52:20 supawit-VirtualBox systemd[1]: Started fail2ban.service - Fail2Ban Service.
Aug 27 17:52:21 supawit-VirtualBox fail2ban-server[1149]: 2025-08-27 17:52:21,385 fail2ban.configreader   [1149]: WA>
Aug 27 17:52:22 supawit-VirtualBox fail2ban-server[1149]: Server ready
lines 1-14/14 (END)
```

**ปัญหาที่พบและวิธีแก้ไข**

1.มี tools บางตัวไม่ได้ติดตั้ง และพอติดตั้งแล้ว error หาไม่เจอ วิธีแก้ไขดูตามใน stack overflow และ reddit 9 ตอนนี้สามารถแก้ไขได้แล้วและใช้งานได้ปกติ