

Linux Automation Documentation

Section 1: Introduction to Linux Automation

Objective:

The goal is to set up a system that tracks when `sudo` commands are used and sends email alerts when needed. This includes creating a test user, installing email tools, configuring email with Gmail, and checking that everything works.

Workflow:

1. **Create a Low-Privileged User:** Set up a new user in the Linux system for testing purposes.
2. **Install mailutils:** Install the necessary package to enable email sending from the terminal.
3. **Configure Postfix and Gmail:** Set up Postfix and create an app password in Gmail for secure email sending.
4. **Test Email Notifications:** Verify that the email configuration works by sending a test email from the terminal

Knowledge gained:.

1. **Automating Tasks:** Learned to use Linux commands for automating monitoring tasks.
2. **Email Setup:** Gained experience in configuring and sending emails from the terminal.
3. **Testing:** Developed skills in testing email systems to ensure they work correctly.

Screenshots-Executing commands in terminal

```
pms@LAPTOP-RNATB7H7:~$ sudo adduser sne
[sudo] password for pms:
Adding user `sne' ...
Adding new group `sne' (1001) ...
Adding new user `sne' (1001) with group `sne' ...
Creating home directory `/home/sne' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for sne
Enter the new value, or press ENTER for the default
    Full Name []: Hello
    Room Number []: 1234
    Work Phone []: 1234567890
    Home Phone []: 9876543210
    Other []: 9999999999
Is the information correct? [Y/n] Y
pms@LAPTOP-RNATB7H7:~$
```

```
pms@LAPTOP-RNATB7H7:~$ pwd
/home/pms
pms@LAPTOP-RNATB7H7:~$ cd ../
pms@LAPTOP-RNATB7H7:/home$ pwd
/home
pms@LAPTOP-RNATB7H7:/home$ ls
pms  sne
pms@LAPTOP-RNATB7H7:/home$ cd bob/
-bash: cd: bob/: No such file or directory
pms@LAPTOP-RNATB7H7:/home$ whoami
pms
pms@LAPTOP-RNATB7H7:/home$ su sne
Password:
sne@LAPTOP-RNATB7H7:/home$ whoami
sne
sne@LAPTOP-RNATB7H7:/home$ pwd
/home
sne@LAPTOP-RNATB7H7:/home$
```

```
pms@LAPTOP-RNATB7H7:/$ sudo apt install mailutils -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  gsasl-common guile-3.0-libs libgc1 libgsasl7 libidn12 libltdl7
  libmailutils8 libmysqlclient21 libntlm0 libpq5 mailutils-common
  mysql-common postfix ssl-cert
Suggested packages:
  mailutils-mh mailutils-doc procmail postfix-mysql postfix-pgsql
  postfix-ldap postfix-pcre postfix-lmdb postfix-sqlite sasl2-bin
  | dovecot-common resolvconf postfix-cdb postfix-mta-sts-resolver
  postfix-doc
The following NEW packages will be installed:
  gsasl-common guile-3.0-libs libgc1 libgsasl7 libidn12 libltdl7
  libmailutils8 libmysqlclient21 libntlm0 libpq5 mailutils mailutils-common
  mysql-common postfix ssl-cert
0 upgraded, 15 newly installed, 0 to remove and 2 not upgraded.
Need to get 11.7 MB of archives.
```

```
pms@LAPTOP-RNATB7H7:/$ mail --version
mail (GNU Mailutils) 3.14
Copyright (C) 2007-2022 Free Software Foundation, inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

pms@LAPTOP-RNATB7H7:/$
```

```
root@LAPTOP-RNATB7H7: /etc/postfix
# See /usr/share/postfix/main.cf.dist for a commented, more complete version

# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTPE $mail_name (Ubuntu)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

readme_directory = no

# See http://www.postfix.org/COMPATIBILITY_README.html -- default to 3.6 on
# fresh installs.
compatibility_level = 3.6

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtp_tls_CApath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = LAPTOP-RNATB7H7.
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, LAPTOP-RNATB7H7., localhost., , localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
smtp_sasl_password_maps=hash:/etc/postfix/sasl/sasl_passwd
smtp_sasl_auth_enable=yes
smtp_tls_security_level=encrypt
smtp_sasl_security_options=noanonymous,
-- INSERT --
```