### **Задание 1: Настройка rsyslog для логирования системных событий**

1. Открыть конфигурационный файл rsyslog

sudo nano /etc/rsyslog.conf

1. Добавить правило для сохранения логов системных событий в отдельный файл

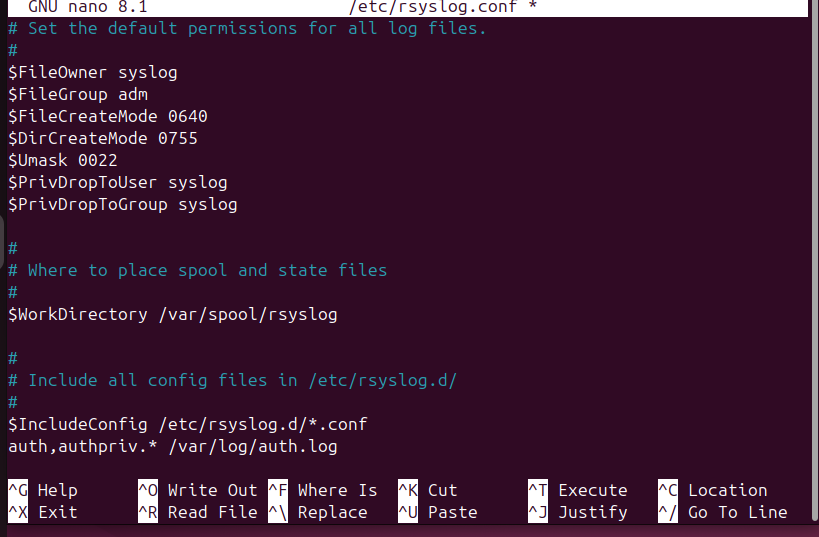
auth,authpriv.\* /var/log/auth.log

1. Перезапустить службу rsyslog

sudo systemctl restart rsyslog

1. Проверить, что логи записываются в указанный файл

tail -f /var/log/auth.log



### **Задание 2: Настройка и использование auditd для аудита безопасности**

1. Установить auditd, если не установлен

sudo apt install auditd

1. Настроить правила аудита в файле конфигурации

echo "-w /etc/passwd -p wa -k passwd\_chechanges" | sudo tee -a /etc/audit/rules.d/audit.rules

1. Перезапустить службу auditd

sudo systemctl restart auditd

1. Использовать ausearch для анализа событий

sudo ausearch -k passwd\_changes

### **Задание 3: Настройка логирования входов и выходов пользователей**

1. Убедиться, что служба rsyslog запущена

sudo systemctl status rsyslog

1. Настроить файл rsyslog.conf для записи логов входов и выходов

sudo sh -c "echo 'auth,authpriv.\* /var/log/auth.log' >> /etc/rsyslog.conf"

1. Перезапустить rsyslog

sudo systemctl restart rsyslog

1. Проверить корректность записи логов

sudo cat /var/log/auth.log

### **Задание 4: Настройка ротации логов с использованием logrotate**

1. Открыть файл конфигурации logrotate

sudo nano /etc/logrotate.conf

1. Добавить правило для ротации логов

sudo sh -c "cat <<EOL >> /etc/logrotate.d/auth-log

/var/log/auth.log {

daily

rotate 7

compress

missingok

notifempty

create 0640 root utmp

}

EOL"

1. Применить изменения и запустить logrotate вручную для проверки

sudo logrotate /etc/logrotate.conf --force

1. Проверить, что логи ротируются и архивируются корректно

ls /var/log/auth.log\*

### **Задание 5: Настройка отправки логов на удаленный сервер**

1. Убедиться, что служба rsyslog запущена на обоих серверах

sudo systemctl status rsyslog

1. Открыть конфигурацию rsyslog на клиенте

sudo nano /etc/rsyslog.conf

1. Добавить правило для отправки логов на удаленный сервер

echo "\*.\* @<remote-server-ip>:514" | sudo tee -a /etc/rsyslog.conf

1. Перезапустить rsyslog на клиенте

sudo systemctl restart rsyslog

1. Настроить сервер для приема удаленных логов

sudo sh -c "echo 'module(load=\"imudp\")\ninput(type=\"imudp\" port=\"514\")\nmodule(load=\"imtcp\")\ninput(type=\"imtcp\" port=\"514\")' >> /etc/rsyslog.conf"

1. Перезапустить rsyslog на сервере

sudo systemctl restart rsyslog

1. Проверить, что логи передаются и записываются на удаленном сервере

sudo tail -f /var/log/syslog

вывод:  
**На клиенте (где настроен отправитель):** Логи будут перенаправляться на удаленный сервер, поэтому локально ничего нового в стандартных логах не появится, кроме подтверждения работы rsyslog:  
plaintext  
Копировать код  
rsyslogd: [origin software="rsyslogd"] rsyslogd was started

**На сервере (где принимаются логи):** При успешной настройке на сервере появятся логи, отправленные с клиента. Например, если клиент отправил системные сообщения:  
plaintext  
Копировать код  
Jan 06 12:34:56 client-hostname systemd[1]: Starting Session 1234...

Jan 06 12:34:57 client-hostname sshd[9876]: Accepted publickey for user

### **Задание 6: Настройка логирования действий администратора**

1. Убедиться, что служба rsyslog запущена

sudo systemctl status rsyslog

1. Настроить файл rsyslog.conf для записи логов действий администратора

sudo sh -c "echo 'authpriv.\* /var/log/sudo.log' >> /etc/rsyslog.conf"

1. Перезапустить rsyslog

sudo systemctl restart rsyslog

1. Настроить файл sudoers для логирования команд sudo

sudo sh -c "echo 'Defaults logfile=\"/var/log/sudo.log\"' >> /etc/sudoers"

1. Проверить, что логи записываются корректно

sudo cat /var/log/sudo.log

вывод:  
Jan 06 12:45:00 hostname sudo: user : TTY=pts/0 ; PWD=/home/user ; COMMAND=/bin/ls

Если администратор вводил неправильный пароль или отменил выполнение команды, также будет запись:

plaintext

Копировать код

Jan 06 12:46:10 hostname sudo: PAM authentication failure for user

### **Задание 7: Настройка мониторинга и оповещений с использованием auditd и auditd-plugins**

1. Установить auditd и необходимые плагины

sudo apt install auditd audispd-plugins

вывод:  
time->Mon Jan 06 12:50:00 2025 type=PATH msg=audit(1673022600.123:456): item=0 name="/etc/passwd" inode=123456 dev=00:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap\_fp=0 cap\_fi=0 cap\_fe=0 cap\_fver=0 type=PROCTITLE msg=audit(1673022600.123:456): proctitle="nano" type=SYSCALL msg=audit(1673022600.123:456): arch=c000003e syscall=2 success=yes exit=0 a0=7ffcf5671234 a1=0 a2=7ffcf5675678 items=1 ppid=1234 pid=5678 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=1 comm="nano" exe="/usr/bin/nano" key="passwd\_changes"

1. Настроить файл конфигурации audit.rules для мониторинга важных файлов

echo "-w /etc/passwd -p wa -k passwd\_changes" | sudo tee -a /etc/audit/rules.d/audit.rules

echo "-w /var/log/auth.log -p wa -k auth\_log\_changes" | sudo tee -a /etc/audit/rules.d/audit.rules

вывод:  
time->Mon Jan 06 12:55:00 2025

type=PATH msg=audit(1673022900.123:789): item=0 name="/var/log/auth.log" inode=789012 dev=00:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap\_fp=0 cap\_fi=0 cap\_fe=0 cap\_fver=0

type=SYSCALL msg=audit(1673022900.123:789): arch=c000003e syscall=2 success=yes exit=0 a0=7ffcf5671234 a1=0 a2=7ffcf5675678 items=1 ppid=5678 pid=9101 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=1 comm="echo" exe="/bin/echo" key="auth\_log\_changes"

1. Настроить плагин audispd-plugins для отправки уведомлений

sudo nano /etc/audisp/plugins.d/syslog.conf

# Добавить:

# active = yes

# direction = out

# path = builtin\_syslog

# type = builtin

# args = LOG\_INFO

# format = string

1. Перезапустить auditd и rsyslog

sudo systemctl restart auditd

sudo systemctl restart rsyslog

1. Проверить, что оповещения работают

sudo ausearch -k passwd\_changes

вывод:  
Jan 06 12:56:00 hostname audispd: Suspicious modification detected: passwd\_changes