**Journald**

**Настройка сервера на прием журналов**.

apt-get install systemd-journal-remote -y

cd /etc/systemd/system

cp /lib/systemd/system/systemd-journal-remote.service .

systemd-journal-remote.service

[Service]

ExecStart=/lib/systemd/systemd-journal-remote --listen-http=-3 --output=/var/log/journal/remote/

Меняем https на http

-3 использовать сокет

--output= путь, куда складывать преремещенные логи

systemctl daemon-reload

systemctl start systemd-journal-remote

systemctl status systemd-journal-remote

systemctl enable systemd-journal-remote

ss -atnp | grep journal

LISTEN 0 4096 \*:19532 \*:\* users:(("systemd-journal",pid=14300,fd=3),("systemd",pid=1,fd=46))

**Настройка клиента на отправку журналов.**

apt-get update -y

apt-get install systemd-journal-remote -y

ls /etc/systemd

vim /etc/systemd/journal-upload.conf

[Upload]

URL=http://192.168.51.1:19532

systemctl start systemd-journal-upload.service

**Просмотр собранных журналов на сервере.**

ls /var/log/journal

e4f98b3ca9dba1c6507ae1846514711e remote

где e4f98b3ca9dba1c6507ae1846514711e - UID текущего узла

ls /var/log/journal/remote/

journalctl -D /var/log/journal/remote

journalctl -D /var/log/journal/remote -xe

journalctl --file=/var/log/journal/remote/remote-192.168.51.100.journal -xe

**Rsyslog**

**На сервере:**

apt-get install -y rsyslog-classic

mkdir /var/log/rsyslog

chmod -R 777 /var/log/rsyslog

vim /etc/rsyslog.conf

$ModLoad imtcp

$InputTCPServerRun 514

$template RemoteLogs,"/var/log/rsyslog/%HOSTNAME%/%PROGRAMNAME%.log"

\*.\* ?RemoteLogs

systemctl restart rsyslog

systemctl status rsyslog

**На клиенте:**

apt-get install -y rsyslog-classic

vim /etc/rsyslog.d/log.conf

\*.\* @@192.168.51.1:514

systemctl restart rsyslog

systemctl status rsyslog

**Проверяем переданные логи на сервере:**

ls /var/log/rsyslog

ls /var/log/rsyslog/host-100/

**Использование модулей Rsyslog**

В этом задании мы будем на клиенте отслеживать изменения в файле audit.log и отправлять на сервер события с уровнем warning и выше и категорией local0.

На стороне клиента.

Предварительные требования.

Настройка аудита

vim /etc/audit/rules.d/10-base-config.rules

добавить в конец файла строки:

-w /etc/passwd -p rwa -k passwords-files

-w /etc/shadow -p rwa -k passwords-files

Запустить демон аудита:

systemctl start auditd.service

vim /etc/rsyslog.d/log.conf

Привести файл в следующий вид:

$ModLoad imfile

$InputFileName /var/log/audit/audit.log

$InputFileTag tag\_audit\_log:

$InputFileStateFile audit\_log

$InputFileSeverity warning

$InputFileFacility local0

$InputRunFileMonitor

\*.\* @@192.168.51.1:514

systemctl restart rsyslog

**На стороне сервера**

Настроим файл конфигурации так, чтобы события сохранялись в отдельном файле.

Файл /etc/rsyslog.confбудет иметь следующий вид:

include(file="/etc/rsyslog.d/\*.conf" mode="optional")

$ModLoad imtcp

$InputTCPServerRun 514

#$template RemoteLogs,"/var/log/rsyslog/%HOSTNAME%/%PROGRAMNAME%.log"

#

#\*.\* ?RemoteLogs

$template HostAudit, "/var/log/rsyslog/%HOSTNAME%/audit.log"

Local0.\* ?HostAudit

systemctl restart rsyslog

На клиенте инициируем события аудита командой usermod sa -c ‘Sysadmin’

**Смотрим на сервере результат:**

tail -fn0 /var/log/rsyslog/host-100/audit.log