Настройка rsyslog для хранения логов на удаленном сервере

Оглавление

[Подготовка сервера 2](#_Toc164119105)

[Время 2](#_Toc164119106)

[Брандмауэр 2](#_Toc164119107)

[SELinux 3](#_Toc164119108)

[Установка и запуск rsyslog 3](#_Toc164119109)

[Настройка сервера 3](#_Toc164119110)

[Настройка клиента 4](#_Toc164119111)

[Все логи 4](#_Toc164119112)

[Для определенных категорий 5](#_Toc164119113)

[Возможные категории для логов (facility): 5](#_Toc164119114)

[Для определенного уровня 6](#_Toc164119115)

[Аудит определенного лог-файла 7](#_Toc164119116)

[Настройка клиента 7](#_Toc164119117)

[Настройка сервера (фильтрация сообщений) 7](#_Toc164119118)

[Лог определенного приложения 8](#_Toc164119119)

[Чтение логов на сервере 9](#_Toc164119120)

Rsyslog позволяет настроить отправку логов для определенного приложения на централизованный сервер. Это может значительно упростить процесс контроля за событиями на компьютерах в сети. Его настройка на различных системах на базе Linux, практически, не отличается. В данной инструкции мы рассмотрим процесс установки и настройки на примере CentOS и Ubuntu.

# Подготовка сервера

На сервере нужно, предварительно, выполнить следующие настройки.

## Время

Для правильной фиксации момента события в логе, необходимо настроить синхронизацию времени.

Сначала задаем правильный часовой пояс:

cp /usr/share/zoneinfo/Europe/Moscow /etc/localtime

\* в данном примере мы использовали московское время.

Затем устанавливаем и запускаем chrony.

на системе Ubuntu / Debian:

apt-get install chrony

systemctl enable chrony

systemctl start chrony

## Брандмауэр

Если используется брандмауэр, необходимо открыть порты TCP/UDP 514.

1. с помощью firewalld:

firewall-cmd --permanent --add-port=514/{tcp,udp}

firewall-cmd –reload

1. с помощью iptables:

iptables -A INPUT -p tcp --dport 514 -j ACCEPT

iptables -A INPUT -p udp --dport 514 -j ACCEPT

1. с помощью ufw:

ufw allow 514/tcp

ufw allow 514/udp

ufw reload

## SELinux

Проверяем, работает ли в нашей системе SELinux:

Getenforce

Если мы получаем в ответ:

Enforcing

Тогда необходимо либо настроить SELinux:

semanage port -m -t syslogd\_port\_t -p tcp 514

semanage port -m -t syslogd\_port\_t -p udp 514

либо отключить его командами:

setenforce 0

sed -i 's/^SELINUX=.\*/SELINUX=disabled/g' /etc/selinux/config

## Установка и запуск rsyslog

Установить rsyslog необходимо как на сервер, так и клиентские компьютеры.

Для систем на базе deb (Debian / Ubuntu):

apt-get install rsyslog

После установки разрешаем автозапуск службы и запускаем ее:

systemctl enable rsyslog

systemctl start rsyslog

## Настройка сервера

Открываем конфигурационный файл:

nano /etc/rsyslog.conf

Снимаем комментарии со следующих строк:

$ModLoad imudp

$UDPServerRun 514

$ModLoad imtcp

$InputTCPServerRun 514

\* в данном примере мы разрешили запуск сервера для соединений **TCP** и **UDP** на портах **514**. На самом деле, можно оставить только один протокол, например, более безопасный и медленный TCP.

После добавляем в конфигурационный файл строки:

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

\*.\* ?RemoteLogs

& ~

\* в данном примере мы создаем шаблон с названием **RemoteLogs**, который принимает логи всех категорий, любого уровня (про категории и уровни читайте ниже); логи, полученный по данному шаблону будут сохраняться в каталоге по маске **/var/log/rsyslog/<имя компьютера, откуда пришел лог>/<приложение, чей лог пришел>.log**; конструкция **& ~** говорит о том, что после получения лога, необходимо остановить дальнейшую его обработку.

Перезапускаем службу логов:

systemctl restart rsyslog

# Настройка клиента

Устанавливаем и запускаем rsyslog по инструкции, описанной выше. После приступаем к настройке клиента.

## Все логи

Для начала можно настроить отправку всех логов на сервер. Создаем конфигурационный файл для rsyslog:

nano /etc/rsyslog.d/all.conf

Добавляем:

\*.\* @@192.168.0.15:514

\* где **192.168.0.15** — IP-адрес сервера логов. \*.\* — перенаправлять любой лог.

Перезапускаем rsyslog:

systemctl restart rsyslog

## Для определенных категорий

Если необходимо отправлять только определенные категории логов, создаем конфигурационный файл для соответствующей, например:

nano /etc/rsyslog.d/kern.conf

Добавим строку:

kern.\* @@192.168.0.15:514

Перезапускаем сервис логов:

systemctl restart rsyslog

## Возможные категории для логов (facility):

Таблица

|  |  |  |
| --- | --- | --- |
| **№** | **Категория** | **Описание** |
| 0 | kern | Сообщения, отправляемые ядром |
| 1 | user | Пользовательские программы |
| 2 | mail | Почта |
| 3 | daemon | Сервисы (демоны) |
| 4 | auth | Безопасность/вход в систему/аутентификация |
| 5 | syslog | Сообщения от syslog |
| 6 | lpr | Логи печати |
| 7 | news | Новостные группы (usenet) |
| 8 | uucp | Unix-to-Unix CoPy (копирование файлов между компьютерами) |
| 9 | cron | Планировщик заданий |
| 10 | authpriv | Безопасность/вход в систему/аутентификация - защищенный режим |
| 11 | ftp | Логи при передаче данных по FTP |
| 12 | ntp | Лог службы синхронизации времени (существует не везде) |
| 13 | security, log audit | Журнал аудита (существует не везде) |
| 14 | console, log alert | Сообщения, отправляемые в консоль (существует не везде) |
| 15 | solaris-cron, clock daemon | Cron в solaris (существует не везде) |
| 16-23 | local0 - local7 | Зарезервированы для локального использования. Уровень серьезности определяется числом от 0 до 7. |

## Для определенного уровня

Если мы хотим передавать только сообщения об ошибках, добавляем строку в файл конфигурации rsyslog:

nano /etc/rsyslog.d/erors.conf

*\*.err @@192.168.0.15:514*

Перезапускаем сервис логов:

systemctl restart rsyslog

Возможные категории для логов (severity):

Таблица

|  |  |  |
| --- | --- | --- |
| № | Уровень | Расшифровка |
| 0 | emerg | Система не работает (PANIC) |
| 1 | alert | Серьезная проблема, требующая внимания |
| 2 | crit | Критическая ошибка |
| 3 | err | Ошибка (ERROR) |
| 4 | warning | Предупреждение (WARN) |
| 5 | notice | Важное информационное сообщение |
| 6 | info | Информационное сообщение |
| 7 | debug | Отладочная информация |

## Аудит определенного лог-файла

Мы можем настроить слежение за изменением определенного лога и передавать их на сервер. Для этого нужно настроить и сервер, и клиента.

### Настройка клиента

Создаем новый конфигурационный файл:

nano /etc/rsyslog.d/audit.conf

Наполняем следующим содержимым:

$ModLoad imfile

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

$InputFileTag tag\_audit\_log:

$InputFileStateFile audit\_log

$InputFileSeverity info

$InputFileFacility local6

$InputRunFileMonitor

\*.\* @@192.168.0.15:514

\* в данном примере мы будем отслеживать изменения лог-файла **/var/log/audit/audit.log**; нас интересуют события от уровня **info** и выше; все события будет отмечены категорией **local6** и переданы на сервер **192.168.0.15**.

Перезапускаем сервис на клиенте:

systemctl restart rsyslog

### Настройка сервера (фильтрация сообщений)

На сервере нам нужно фильтровать все сообщения категории local6 (такую категорию мы выбрали, когда настроили клиента) и перенаправлять их в нужных нам файл. Открываем на редактирование конфигурационный файл rsyslog:

nano /etc/rsyslog.conf

Создаем новый шаблон для захвата логов:

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

local6.\* ?HostAudit

\* в данном примере мы создаем шаблон **HostAudit**; **rsyslog** будет принимать логи категории **local6** и сохранять в файле **/var/log/rsyslog/<имя компьютера, откуда пришел лог>/audit.log**.

Перезапускаем сервер:

systemctl restart rsyslog

## Лог определенного приложения

Некоторые приложения умеют отправлять лог напрямую на syslog. Например, nginx (начиная с версии 1.7.1). Для этого открываем конфигурационной файл (основной или конфиг виртуального домена):

nano /etc/nginx/nginx.conf

Добавляем или редактируем соответствующие настройки для логов:

...

access\_log syslog:server=192.168.0.15:514 info;

error\_log syslog:server=192.168.0.15:514 warn;

error\_log /var/log/nginx/error.log warn;

...

\* в данном примере мы настроили хранение логов для nginx на сервере **192.168.0.15**. Для ошибок также сохраняется локальный лог в файле **/var/log/nginx/error.log**.

Проверяем корректность конфигурационного файла nginx:

nginx -t

Перезапускаем сервис:

systemctl restart nginx

# Чтение логов на сервере

В нашем примере сервер настроен на хранение логов по маске /var/log/rsyslog/%HOSTNAME%/%PROGRAMNAME%.log. Это значит, что в каталоге /var/log/rsyslog должны появляться папки с именами компьютеров, которые отправляют на сервер свои логи. Посмотреть список данных папок можно командой:

ls /var/log/rsyslog

Чтение логов выполняется обычной командой cat или tail, например:

tail /var/log/rsyslog/comp1/CROND.log

\* здесь мы прочитаем лог для **cron** на компьютере **comp1**.