Доклад

Система Syslog и журналы событий в Linux

Верниковская Е. А., НПИбд-01-23

21 октября 2024

Российский университет дружбы народов, Москва, Россия

Докладчик

- Верниковская Екатерина Андреевна
- Студентка
- Российский университет дружбы народов
- 1132236136@pfur.ru

Вводная часть

Актуальность темы и проблема: система Syslog и журналы событий в Linux играют ключевую роль в обеспечении безопасности, мониторинга и диагностики систем. В условиях растущей киберугрозы и возрастающей сложности IT-инфраструктур необходимость в эффективном управлении логами становится особенно актуальной. Syslog позволяет централизованно собирать, хранить и анализировать события, что значительно упрощает администрирование и повышает уровень безопасности

Объект и предмет исследования: система Syslog и журналы событий в Linux

Вводная часть

Цель:
цель данного доклада - рассмотреть основные принципы работы системы Syslog и функционирование журналов событий в операционной системе Linux

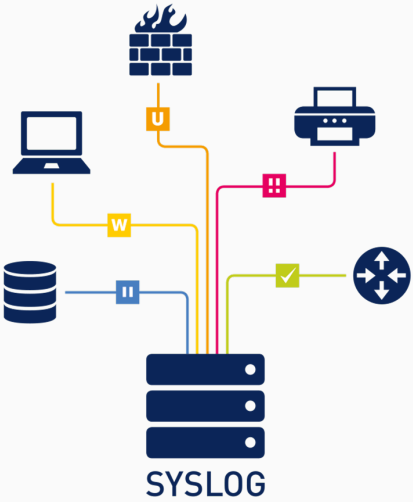
Задачи исследования:
изучить архитектуру системы Syslog и типы журналов событий в Linux

Материалы и методы и инструменты исследования:
интернет-ресурсы, аналитика и практические навыки работы на своей операционной системе Linux (Ubuntu)

Введение

В процессе своей работы система отслеживает и сохраняет важные события в файлы журналов, которые помогают в исправлении ошибок и отладке. Эти файлы могут занимать много места, что иногда связано с ошибками системы или некорректной настройкой. Работа с журналами событий — важная задача системного администратора, от которой зависит качество работы системы и её надежность.

Что такое Syslog и зачем он нужен?



Syslog (от англ. system log — системный журнал) — это стандартная система журналирования в операционных системах, включая Linux, регистрирующая события в системе. Позволяет собирать, сохранять и передавать сообщения, генерируемые программами, службами и ядром операционной системы. Помога- ет администратору отслеживать события, состояния системных служб и выявлять проблемы, возникающие в процессе работы системы.

История и развитие Syslog

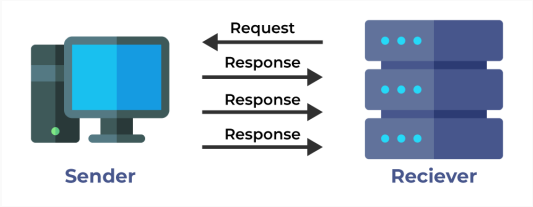
Syslog был разработан в 1980 году Эриком Оллманом (Eric Allman) как часть проекта Sendmail, и использовался первоначально только для Sendmail. Зарекомендовав себя как стабильное и удобное решение, Syslog был использован и в других приложениях, став стандартом ведения журналов в системах UNIX и GNU/Linux. Позднее появились реализации и под другие операционные системы.

Рис. 1: Эрик Оллман

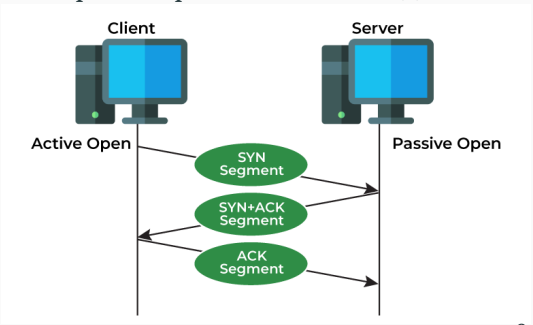
Протоколы Syslog

Протокол syslog определяет стандарт передачи сообщений журнала между клиентами syslog (отправителями) и серверами syslog (получателями).

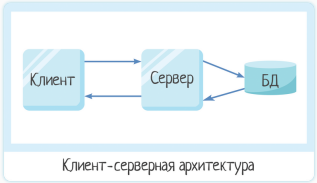
- UDP (User Datagram Protocol) — это протокол без установления соедине- ния

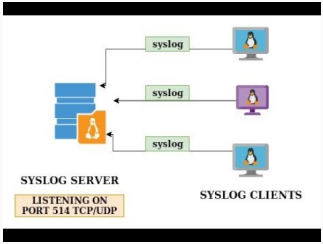


- TCP (Transmission Control Protocol) — это протокол, ориентированный на соединение



Клиенты и серверы Syslog. Принцип работы Syslog





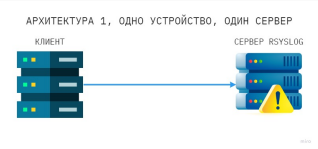
Syslog работает на основе клиент-серверной архитектуры. Клиент syslog отвечает за генерацию сообщений журнала и отправку их на сервер syslog. Сервер syslog получает и сохраняет эти сообщения журнала, делая их доступными для анализа, мониторинга и устранения неполадок.

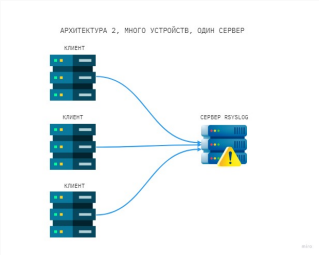
Принцип работы:

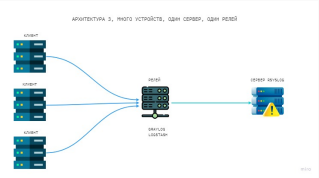
1. Генерация журнала
2. Пересылка журнала
3. Прием журнала
4. Хранение журналов
5. Анализ журнала

Архитектура Syslog

Архитектура Syslog может включать несколько клиентов, которые отправляют логи на центральный сервер (коллектор). Эта базовая конфигурация подходит для небольших инфраструктур. При увеличении числа клиентов или для обеспечения безопасности и отказоустойчивости целесообразно использовать релейную архитектуру. Релей (или релей-агент) выступает промежуточным узлом между клиентами и центральным сервером, куда отправляются логи.

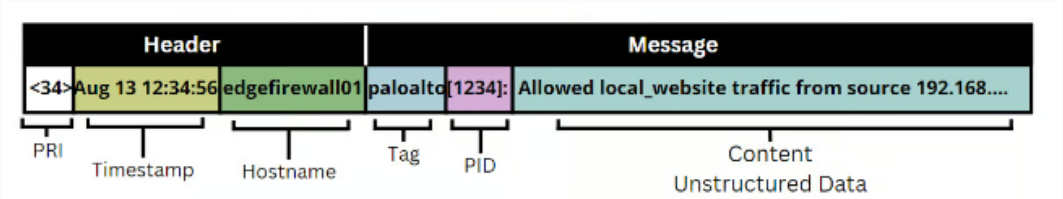






Формат сообщений Syslog

Сообщения syslog следуют определенному формату, который включает несколько компонентов:



Часть PRI: там описываются уровни приоритета сообщения. PRI вычисляется по формуле: **PRI = facility * 8 + severity**

Часть HEADER: состоит из двух полей – TIMESTAMP и HOSTNAME

Часть MSG: содержит информацию о произошедшем событии. Делится на поле TAG и поле CONTENT

Формат сообщений Syslog

Коды объектов (Facility):

- 0 (kern): Сообщения ядра
- 1 (user): Сообщения, сгенерированные в пространстве пользователя
- 2 (mail): Сообщения, связанные с электронной почтой
- 3 (daemon): Сообщения системного демона
- 4 (auth): Сообщения аутентификации и авторизации
- 5 (syslog): Сообщения, генерируемые самим процессом syslog
- 6 (lpr): Сообщения подсистемы строчного принтера
- 7 (news): Сообщения подсистемы сетевых новостей и т.д

Формат сообщений Syslog

Уровни серьёзности (Severity):

- 0 (Emergency): система не пригодна для использования
- 1 (Alert): необходимо немедленно принять меры
- 2 (Critical): критические условия
- 3 (Error): ошибочные состояния
- 4 (Warning): предупреждающие условия
- 5 (Notice): нормальные, но существенные условия
- 6 (Informational): информационные сообщения
- 7 (Debug): сообщения уровня отладки

Журналы событий в Linux

Все файлы журналов, можно отнести к одной из следующих категорий:

- приложения
- события
- службы
- системный

В Linux существует несколько основных типов журналов событий:

- /var/log/messages или /var/log/syslog
- /var/log/dmesg или /var/log/kern.log
- /var/log/secure
- /var/log/boot.log
- /var/log/maillog
- /var/log/samba
- /var/log/sssd
- /var/log/cups
- /var/log/httpd/
- /var/log/faillog

Настройка и использование Syslog

Для настройки Syslog используется файл конфигурации /etc/rsyslog.conf или /etc/syslogd.conf

Основные параметры настройки:

- Уровни важности (emerg, alert, crit, err, warning, notice, info, debug)
- Типы сообщений (auth, cron, daemon, mail, user, kern)

Можно настроить локальное и удалённое логирование, а также фильтры и маршрутизацию.

- Фильтрация по уровню сообщений
- Фильтрация по программе
- Маршрутизация на основе тегов

Инструменты для работы с журналами. Rsyslog и Syslog-ng

В настоящее время для эффективного управления и анализа журналов используются различные инструменты. Два наиболее популярных решения — Rsyslog и Syslog-ng. Они обеспечивают сбор, обработку и отправку системных сообщений, но имеют некоторые ключевые отличия в функциональности и возможностях настройки.

Команды для анализа журналов

Для анализа и управления журналами в Linux можно использовать несколько команд:

- tail: Используется для просмотра последних строк файла журнала.
- grep: Позволяет искать строки, содержащие определенные слова или шаб- лоны.
- less: Удобный просмотрщик файлов, позволяющий прокручивать и искать текст.
- cat: Отображает содержимое файла целиком.
- awk и sed: Мощные инструменты для обработки текстовых данных.

Настройка Syslog на серверах (Linux)

Установим Rsyslog (на большинстве дистрибутивов Linux Rsyslog установлен по умолчанию)

```
root@ubuntu-katerok:~# sudo apt install rsyslog
Чтение списков пакетов… Готово
Построение дерева зависимостей… Готово
Чтение информации о состоянии… Готово
```

Рис. 2: Установка rsyslog

```
root@ubuntu-katerok:~# systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-10-14 15:46:00 MSK; 34s ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 11359 (rsyslogd)
      Tasks: 4 (limit: 18904)
     Memory: 1.0M
        CPU: 8ms
     CGroup: /system.slice/rsyslog.service
             └─11359 /usr/sbin/rsyslogd -n -iNONE

окт 14 15:46:00 ubuntu-katerok systemd[1]: Starting System Logging Service...
окт 14 15:46:00 ubuntu-katerok rsyslogd[11359]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3)
окт 14 15:46:00 ubuntu-katerok rsyslogd[11359]: rsyslogd's groupid changed to 111
окт 14 15:46:00 ubuntu-katerok systemd[1]: Started System Logging Service.
окт 14 15:46:00 ubuntu-katerok rsyslogd[11359]: rsyslogd's userid changed to 104
окт 14 15:46:00 ubuntu-katerok rsyslogd[11359]: [origin software="rsyslogd" swVersion="8.2112.0" x-pid="11359" x-in
lines 1-20/20 (END)
```

Рис. 3: Проверка статуса rsyslog после установки

Настройка Syslog на серверах (Linux)

Проверим, существуют ли какие-то файлы куда записываются логи. Мы видим, что таких файлов не существует.

```
root@ubuntu-katerok:~# cat /var/log/error.log
cat: /var/log/error.log: Нет такого файла или каталога
root@ubuntu-katerok:~# cat /var/log/sshd.log
cat: /var/log/sshd.log: Нет такого файла или каталога
root@ubuntu-katerok:~# cat /var/log/mail.log
cat: /var/log/mail.log: Нет такого файла или каталога
root@ubuntu-katerok:~# cat /var/log/auth.log
cat: /var/log/auth.log: Нет такого файла или каталога
root@ubuntu-katerok:~# cat /var/log/messages
cat: /var/log/messages: Нет такого файла или каталога
root@ubuntu-katerok:~#
```

Рис. 4: Файлы с логами

Отредактиркем файл /etc/rsyslog.conf для определения того, какие логи и куда направлять.

```
#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
```

Рис. 5: Файл /etc/rsyslog.conf

Настройка Syslog на серверах (Linux)

1. Удалённое логирование

- На сервере-получателе: Добавляем строки, чтобы настроить rsyslog принимать удалённые логи

```
#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

Рис. 6: Настройка rsyslog принимать удалённые логи

- На сервере-отправителе: Добавляем строки для настройки отправки логов на удалённый сервер логи

```
# Send logs to remote Syslog server
*.* @172.16.82.68:514     # Используйте @ для UDP
#*.* @@172.16.82.68:514   # Используйте @@ для TCP
```

Рис. 7: Настройка отправки логов на удалённый сервер

Настройка Syslog на серверах (Linux)

2. Фильтрация по программе: Добавим правило, которое перенаправляет все логи, полученные от процесса sshd (сервер SSH) в отдельный файл /var/log/ssh.log:

```
# Filter SSHD logs to a separate file
if $programname == 'sshd' then /var/log/sshd.log
if $programname == 'sshd' then ~  # Не записывать эти сообщения больше никуда
```

Рис. 8: Фильтрация по программе

3. Маршрутизация на основе тегов: Настроим фильтр для сортировки логов и их записи в соответствующие файлы. Например, пусть все сообщения с уровнем серьёзности “error” будут записываться в отдельный файл /var/log/error.log. Для этого добавим строки:

```
# Filter error messages to a separate file
if $syslogseverity-text == 'error' then /var/log/error.log
```

Рис. 9: Маршрутизация на основе тегов

4. Фильтрация по уровню сообщений:

И наконец добавим правила, которые перенаправляют логи разных системных служб в отдельные файлы:

```
# Log various facilities to specific files
authpriv.* /var/log/auth.log       # Все сообщения авторизации
mail.* /var/log/mail.log           # Все сообщения, связанные с почтой
*.info;mail.none;authpriv.none;cron.none /var/log/messages  # Остальные сообщения
```

Рис. 10: Фильтрация по уровню сообщений

Настройка Syslog на серверах (Linux)

После внесения изменений файла /etc/rsyslog.conf обязательно надо перезапустить службу rsyslog

```
root@ubuntu-katerok:~# sudo systemctl restart rsyslog
root@ubuntu-katerok:~#
```

Рис. 11: Перезапуск rsyslog

```
root@ubuntu-katerok:~# systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-10-14 15:59:15 MSK; 14s ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 12900 (rsyslogd)
      Tasks: 10 (limit: 18904)
     Memory: 1.5M
        CPU: 12ms
     CGroup: /system.slice/rsyslog.service
             └─12900 /usr/sbin/rsyslogd -n -iNONE

окт 14 15:59:15 ubuntu-katerok systemd[1]: Starting System Logging Service...
окт 14 15:59:15 ubuntu-katerok rsyslogd[12900]: warning: ~ action is deprecated, consider using the 'stop' statemen>
окт 14 15:59:15 ubuntu-katerok rsyslogd[12900]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3)>
окт 14 15:59:15 ubuntu-katerok systemd[1]: Started System Logging Service.
окт 14 15:59:15 ubuntu-katerok rsyslogd[12900]: rsyslogd's groupid changed to 111
окт 14 15:59:15 ubuntu-katerok rsyslogd[12900]: rsyslogd's userid changed to 104
окт 14 15:59:15 ubuntu-katerok rsyslogd[12900]: [origin software="rsyslogd" swVersion="8.2112.0" x-pid="12900" x-in>
lines 1-21/21 (END)
```

Рис. 12: Проверка статуса rsyslog после редактирования файла

Проверка настроек Syslog

Проверим, работают ли настройки Syslog. Для этого сначала создадим тестовое сообщение об ошибке с помощью logger. Теперь мы видим, что создался файл /var/log/error.log куда записываются все сообщения с уровнем серьёзности “error”

```
root@ubuntu-katerok:~# logger -p user.error "Это тестирует сообщение об ошибке."
root@ubuntu-katerok:~# cat /var/log/error.log
Oct 14 16:00:21 ubuntu-katerok root: Это тестирует сообщение об ошибке.
root@ubuntu-katerok:~#
```

Рис. 13: Файл /var/log/error.log

Проверка настроек Syslog

Проверим файл /var/log/sshd.log. Для этого выполним событие, которое будет записано в логи sshd

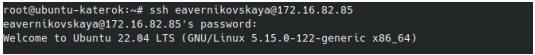


Рис. 14: Вход на сервер с помощью SSH

После мы видим, что создался файл /var/log/sshd.log, в который записываются все логи, полученные от процесса sshd (сервер SSH)

Рис. 15: Файл /var/log/sshd.log

Проверка настроек Syslog

Далее проверяем всё остальное

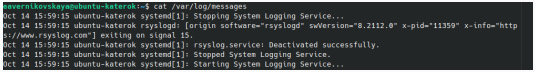


Рис. 16: Файл /var/log/messages.log

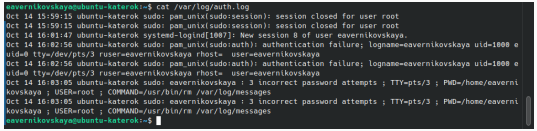


Рис. 17: Файл /var/log/auth.log

Проверка настроек Syslog

```
eavernikovskaya@ubuntu-katerok:~$ cat /var/log/mail.log
Oct 14 16:06:17 ubuntu-katerok eavernikovskaya: Тестовое сообщение для почты
Oct 14 16:06:17 ubuntu-katerok eavernikovskaya: Тестовое сообщение для почты
eavernikovskaya@ubuntu-katerok:~$
```

Рис. 18: Файл /var/log/mail.log

Практические примеры поиска ошибок и предупреждений

После настройки Syslog, важно уметь анализировать журналы для нахождения ошибок и предупреждений. Найдём с помощью grep ошибки и предупреждения

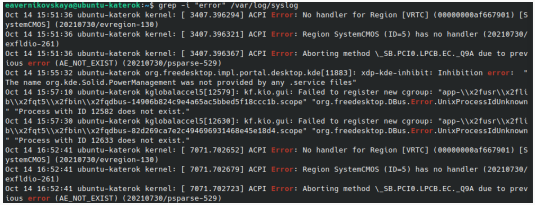


Рис. 19: Поиск ошибок

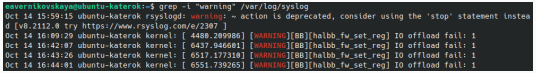
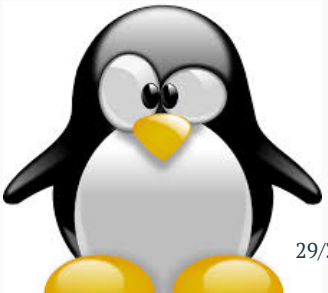


Рис. 20: Поиск предупреждений

Вывод

Syslog — ключевой инструмент для централизованного сбора и анализа системных событий в Linux и других ОС. Его гибкая архитектура поддерживает как локальное, так и удаленное логирование, что упрощает мониторинг в распределенных системах. Использование таких инструментов, как rsyslog и syslog-ng, позволяет настраивать фильтрацию и маршрутизацию логов. Правильная конфигурация Syslog важна для обеспечения безопасности и производительности, что помогает администраторам отслеживать события, выявлять угрозы и устранять сбои.



Список литературы

1. Система Syslog и журналы логов в Linux. ИТ Проффи, 2023. [Электронный ресурс] URL: https://itproffi.ru/sistema-syslog-i-zhurnaly-logov-v-linux/
2. synergix. Контора пишет - syslog. unix.uz, 2010. [Электронный ресурс] URL: https://unix.uz/articles/tuning/131-kontora-pishet-syslog.html
3. Differences between TCP and UDP. GeeksforGeeks, 2024. [Электронный ресурс] URL: https://www.geeksforgeeks.org/differences-between-tcp-and-udp/
4. What is syslog? sumo logic. [Электронный ресурс] URL: https://www.sumologic.com/syslog/
5. cryptoparty. Syslog : Полное руководство. 2022. [Электронный ресурс] URL: https://itsecforu.ru/
6. Syslog. sematext. [Электронный ресурс] URL: https://sematext.com/glossary/syslog/
7. Просмотр и настройка логов Linux на Ubuntu, Debian и CentOS. beget.