



ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование

Проверить, идет ли запись!





Меня хорошо видно && слышно?

Ставьте  , если все хорошо
Напишите в чат, если есть проблемы

Анализ логов веб-сервера



Вяземский Семён Валерьевич

QA Automation Lead

Beeline

svvyazemsky@gmail.com

Правила вебинара



Активно участвуем



Задаем вопрос в чат или голосом



Off-topic обсуждаем в Slack #канал группы или #general



Вопросы вижу в чате, могу ответить не сразу

Маршрут вебинара

Потоки ввода / вывода



Логи



Утилиты для работы с текстом



Рефлексия

Цели вебинара | После занятия вы сможете

1 Различать stderr, stdin, stdout

2 Научиться находить логи

3 Использовать утилиты командной строки и питон для работы с текстом

Смысл | Зачем вам это уметь

1 Эффективно работать с текстом

2 Проводить диагностику приложения

The image features a high-angle, blue-tinted aerial photograph of a dense urban skyline, likely New York City, with numerous skyscrapers and buildings. A semi-transparent blue band with a white geometric network pattern of dots and lines runs horizontally across the center of the image. The word "Начнем" is written in white, bold, sans-serif font within this band.

Начнем

Ввод / вывод

- stdin стандартный поток ввода
- stdout стандартный поток вывода
- stderr стандартный поток вывода ошибок

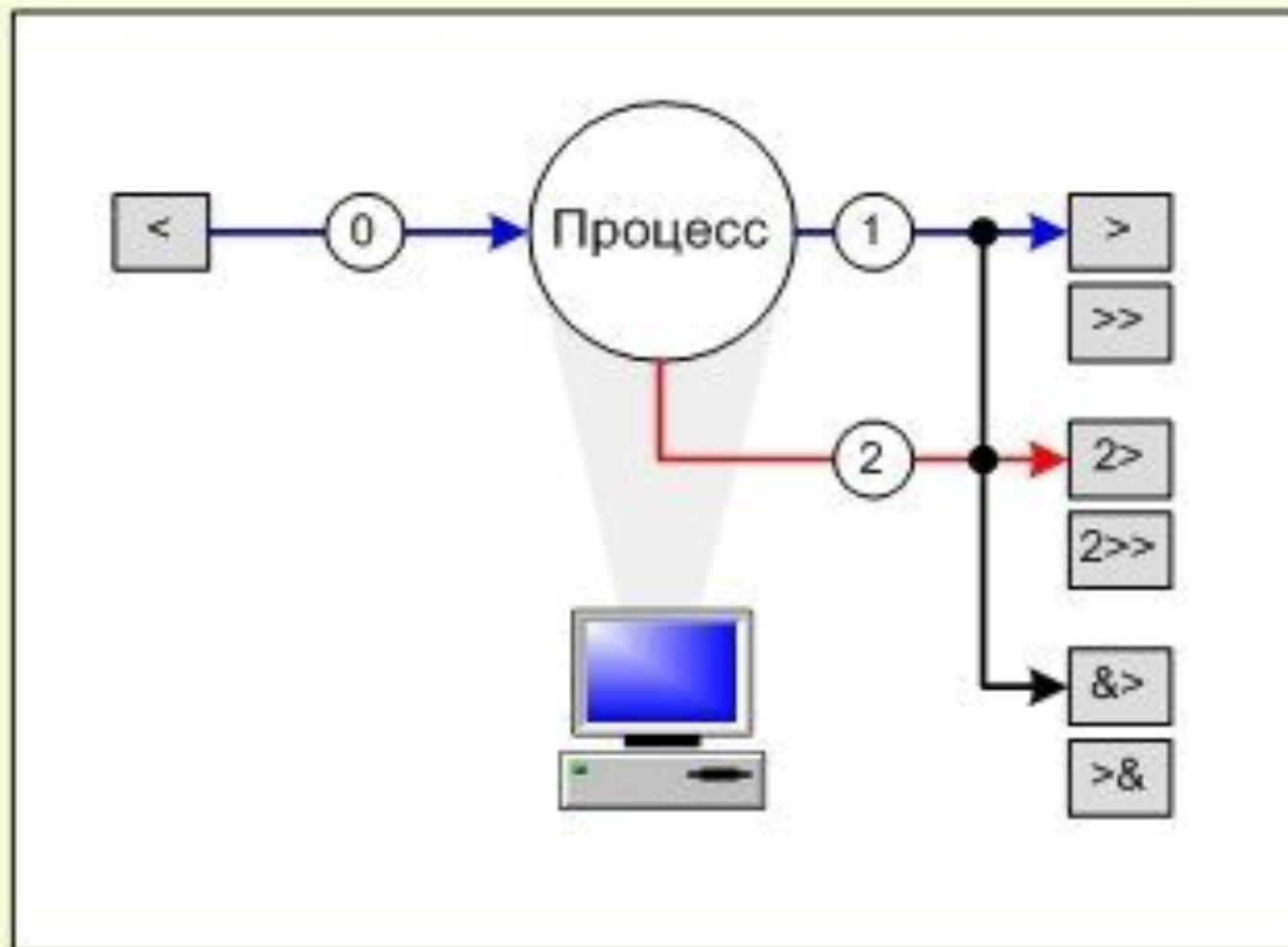
http://xgu.ru/wiki/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%BD%D1%8B%D0%B5_%D0%BF%D0%BE%D1%82%D0%BE%D0%BA%D0%B8_%D0%B2%D0%B2%D0%BE%D0%B4%D0%B0/%D0%B2%D1%8B%D0%B2%D0%BE%D0%B4%D0%B0

<https://stackoverflow.com/questions/3385201/confused-about-stdin-stdout-and-stderr>

Ввод / вывод. Перенаправления

- **< файл** -- Из файла в stdin.
- **> файл** -- Из stdout в файл (с перезаписью).
- **2> файл** -- stderr в файл (с перезапи).
- **>>файл** или **2>>файл** -- перенаправление с дозаписью
- **&>файл** или **>&файл** или **>файл 2>&1** -- stdout и stderr в файл.
- **|** для перенаправления между процессами

Ввод / вывод



< файл файл в поток ввода

> файл поток вывода в новый файл

>> файл поток вывода в конец файла

2> файл поток ошибок в новый файл

2>> файл поток ошибок в конец файла

&> файл потоки вывода и ошибок в
>& файл новый файл

2> &1 потоки ошибок туда, куда
 направлен поток вывода

1> &2 потоки вывода туда, куда
 направлен поток ошибок

The image features a high-angle, blue-tinted aerial photograph of a dense urban skyline, likely New York City, with numerous skyscrapers and buildings. A semi-transparent blue band with a white geometric network pattern of dots and lines stretches horizontally across the middle of the image. The word "Демо" is centered within this band in a large, white, sans-serif font.

Демо

Логи

Логи -- текстовые файлы содержащие информацию о работе системы или приложения

- `/var/log/syslog` или `/var/log/messages` глобальный системный журнал
- `/var/log/auth.log` или `/var/log/secure` — информация об авторизации пользователей
- `/var/log/dmesg` — драйвера устройств
- `/var/log/audit` — записи, созданные службой аудита `auditd`.
- `/var/log/boot.log` — информация о загрузке системы
- `/var/log/cron` — отчет службы `cron`
- `/var/log/cups` — принтеры

<https://habr.com/ru/post/332502/>

Логи. Где искать?

1. /var/log
2. Рядом с приложением
3. В специальной системе (ELK)
4. Использовать find / locate поискать самостоятельно
5. Спросить у людей, которые настраивали логирование

Логи. На что смотреть

- Самые долгие запросы
- Серверные ошибки (5xx)
- Клиентские ошибки (4xx)
- Количество запросов с одинаковым IP / UA
- Для логов приложения обычные ошибки

The image features a blue-tinted aerial view of a dense city skyline, likely New York City, with numerous skyscrapers. A semi-transparent blue band with a white network pattern of dots and lines runs horizontally across the center. The word "Вопросы?" is written in white, bold, sans-serif font within this band.

Вопросы?

The background of the slide features an aerial view of a dense city skyline, likely New York City, with numerous skyscrapers. The image is overlaid with a semi-transparent blue layer that contains a white network pattern of interconnected dots and lines, suggesting a digital or technological theme. The word "Дисклеймер" is centered in the middle of the slide in a large, white, sans-serif font.

Дисклеймер

Утилиты для работы с текстом. tail

tail -- по умолчанию утилита выводит десять последних строк из файла

Использование: tail опции файл[файл]

- с - выводить указанное количество байт с конца файла;
- f - обновлять информацию по мере появления новых строк в файле;
- n - выводить указанное количество строк из конца файла;
- pid - используется с опцией -f, позволяет завершить работу утилиты, когда завершится указанный процесс;
- q - не выводить имена файлов;
- retry - повторять попытки открыть файл, если он недоступен;
- v - выводить подробную информацию о файле;

<https://losst.ru/komanda-tail-linux>

Утилиты для работы с текстом. cat

cat -- прочитать файлы и напечатать результат

Использование: cat опции файл[файл]

- b - нумеровать только непустые строки;
- E - показывать символ \$ в конце каждой строки;
- n - нумеровать все строки;
- s - удалять пустые повторяющиеся строки;
- T - отображать табуляции в виде ^I;

<https://losst.ru/komanda-cat-linux>

Утилиты для работы с текстом. head

head -- печатает первые N строк из файла (по умолчанию 10)

Использование: head опции файл

-с напечатать N байтов

-n напечатать N строк

Утилиты для работы с текстом. less

less -- открывает файл для просмотра

Использование: less файл

Перемещение по файлу j/k или стрелочками

/pattern поиск вперед

?pattern поиск назад

n повторить последний поиск

N повторить последний поиск в обратном направлении

/& Отображать только найденные строки (может зависнуть на большом файле)

pattern -- регулярное выражение

<http://rus-linux.net/MyLDP/consol/hdrguide/rusman/more.htm>

Утилиты для работы с текстом. less, more, most

more -- открываем файл, позволяет прокручивать его сверху вниз.

less -- открывает файл, умеет искать по тексту, и скроллить вверх и вниз.

most -- открывает файл, умеет открывать несколько файлов, сплитить экран, редактировать текст.

<https://andreyex.ru/operacionnaya-sistema-linux/otliche-mezhdu-komandami-more-less-i-most/>

Утилиты для работы с текстом. grep

grep -- поиск в файлах/файлов по паттерну

Использование: `grep [опции] шаблон [имя файла...]`

- m - остановить после m вхождений;
- c - подсчитать количество вхождений шаблона;
- i - не учитывать регистр;
- l - отобразить только имена файлов, в которых найден шаблон;
- n - показывать номер строки в файле;
- v - инвертировать поиск, выдавать все строки кроме тех, что содержат шаблон;
- e - использовать регулярные выражения при поиске;
- An - показать вхождение и n строк до него;
- Bn - показать вхождение и n строк после него;
- Cn - показать n строк до и после вхождения;

`tail -f file | grep -e "regexp"` -- отслеживание файла по регулярному выражению

The image features a blue-tinted aerial view of a dense city skyline, likely New York City, with numerous skyscrapers. A semi-transparent blue band with a white network pattern of dots and lines runs horizontally across the middle of the image. The word "Вопросы?" is centered in this band in a large, white, sans-serif font.

Вопросы?

Утилиты для работы с текстом. sed

sed -- потоковый текстовый редактор

Использование: sed options file

В чем отличие от vim/nano/most?

Утилиты для работы с текстом. sed

- Меняет данные “на лету”
- По умолчанию не изменяет файл
- По умолчанию заменяет только первое вхождение
- Печатает изменения на экран частями, не дожидаясь всех изменений

Утилиты для работы с текстом. sed substitute

`sed s/pattern1/pattern2/ -- s (substitute) команда замены`

`echo 'foo' | sed 's/foo/bar/' -- с получением вывода из другой команды`

`sed 's/foo/bar' ./foo.txt -- из файла`

`sed -e "s/foo/bar/; s/bar/zoo/" ./foo.txt`

Утилиты для работы с текстом. sed команды из файла

Содержимое файла с командами (commands):

```
s/foo/bar/  
s/baz/qux/
```

Вызов sed:

```
sed -f commands foo.txt
```

Утилиты для работы с текстом. sed флаги

Использование: s/pattern/replacement/flags

- g -- заменять все вхождения
- число -- укажет номер вхождения для замены
- p -- выводить содержимое исходной строки (если были изменения, часто используется вместе с -n)
- w -- сохранит вывод в файл

Утилиты для работы с текстом. sed флаги примеры

- `sed 's/foo/bar/g'` -- замена всех foo на bar
- `sed 's/foo/bar/2'` -- замена второго foo в строке на bar
- `sed -n 's/foo/bar/p'` -- напечатать **только** строку в которой заменили foo на bar
- `sed 's/foo/bar/w out'` -- сохранить вывод в out (будет создан если не существует)

Утилиты для работы с текстом. sed разделители

Разделитель первый символ после s.

```
sed 's/foo/bar' foo.txt -- разделитель /  
sed 's!foo!bar' foo.txt -- разделитель !
```

Утилиты для работы с текстом. sed диапазоны

sed '2s/foo/bar' foo.txt -- заменять только во 2-ой строке

sed '2,5s/foo/bar' foo.txt -- заменять в строках с 2-ой по 5-ую

sed '2,\$s/foo/bar' foo.txt -- заменять в строках с 2-ой и до конца

Утилиты для работы с текстом. sed фильтры

`sed 'baz/s/foo/bar' foo.txt` -- заменять foo на bar только в строке содержащей baz

Утилиты для работы с текстом. sed удаление

sed "3d" foo.txt -- удалить 3-ю строку

sed "2,3d" foo.txt -- удалить 2-ую и 3-ю строки

sed "2,\$d" foo.txt -- удалить с 2-ой строки до конца

Утилиты для работы с текстом. sed другие команды

```
echo "foo" | sed 'i\bar ' -- добавить bar перед foo  
echo "foo" | sed 'a\bar ' -- добавить foo перед bar  
sed '3c\bar.' foo.txt -- заменить 3-ю строку целиком
```


Утилиты для работы с текстом. sed

<https://habr.com/ru/company/ruvds/blog/327530/>

Утилиты для работы с текстом. awk

awk -- DSL для обработки текста.

Возможности:

- Создавать переменные
- Арифметические и строковые операторы
- Ветвления и циклы

<https://github.com/TheMozg/awk-raycaster> -- 3D игра на awk.

Утилиты для работы с текстом. awk примеры

```
awk '{print "hello world"}' -- hello world
```

```
awk '{print $1}' foo.txt -- напечатать первое слово
```

```
awk '  
BEGIN{  
foo="bar"
```

```
print foo
```

```
}' -- создание переменной
```

Утилиты для работы с текстом. awk

<https://habr.com/ru/company/ruvds/blog/327754/>

Поиск файлов. find

find -- утилита для поиска файлов

find [папка] [параметры] критерий шаблон [действие]

Поиск файлов. find аргументы

- maxdepth - максимальная глубина поиска по подкаталогам (1 для поиска только в текущем каталоге)
- print - выводить полные имена файлов
- type f - искать только файлы
- type d - искать только папки

Поиск файлов. find аргументы

- name - поиск файлов по имени
- perm - поиск файлов по режиму доступа
- user - поиск файлов по владельцу
- group - поиск по группе
- mtime - поиск по времени модификации файла
- atime - поиск файлов по дате последнего чтения
- nogroup - поиск файлов, не принадлежащих ни одной группе
- nouser - поиск файлов без владельцев
- newer - найти файлы новее чем указанный
- size - поиск файлов в Linux по их размеру

Поиск файлов. find примеры

`find foo.txt --` файл `foo.txt` в текущей папке

`find . --` все файлы в текущей папке

`find . -name *.log --` все файлы оканчивающиеся на `.log`

`find ~/ -name *.log --` все файлы оканчивающиеся на `.log` в домашней директории

`find . -exec ls {} \;` -- найти все файлы в текущей папке и применить к ним `ls`

Поиск файлов. locate

locate -- утилита для быстрого поиска файлов

locate [имя-файла] -- поиск файла с именем
updatedb -- обновление базы данных

Регулярные выражения

`\d`

Соответствует любой цифре; эквивалент класса `[0-9]`.

`\D`

Соответствует любому нечисловому символу; эквивалент класса `[^0-9]`.

`\s`

Соответствует любому символу whitespace; эквивалент `[\t\n\r\f\v]`.

`\S`

Соответствует любому не-whitespace символу; эквивалент `[^\t\n\r\f\v]`.

`\w`

Соответствует любой букве или цифре; эквивалент `[a-zA-Z0-9_]`.

`\W`

Наоборот; эквивалент `[^a-zA-Z0-9_]`.

? - один опциональный символ, + - больше одного символа, * - любое количество, или отсутствие

The background of the slide features an aerial view of a dense city skyline, likely New York City, with numerous skyscrapers. The image is overlaid with a semi-transparent blue layer that contains a white network pattern of interconnected dots and lines, resembling a digital or data network. The text "Подготовка к ДЗ" is centered in the middle of the slide in a large, white, sans-serif font.

Подготовка к ДЗ

Рефлексия



Отметьте 3 пункта, которые вам запомнились с вебинара



Что вы будете применять в работе из сегодняшнего вебинара?

Слайд с тезисами

- 1 Три основных потока ввода / вывода, stderr, stdin, stdout
- 2 Логи -- текстовые файлы, которые могут быть где угодно
- 3 С текстом можно сделать что угодно используя tail, cat, less, grep, awk, sed
- 4 Регулярные выражения очень полезная штука




Слайд с домашним заданием

- 1 Написать скрипт для анализа access.log

Список материалов для изучения

- Про потоки
- <https://stackoverflow.com/questions/3385201/confused-about-stdin-stdout-and-stderr> про потоки 2
- <https://habr.com/ru/post/332502/> про логи в линуксе
- <https://losst.ru/komanda-tail-linux> про tail
- <https://losst.ru/komanda-cat-linux> про cat
- <https://debian.pro/573> про less
- <https://losst.ru/gerp-poisk-vnutri-fajlov-v-linux> про grep
- <https://linux.die.net/man/1/head> про head
- <https://habr.com/ru/company/ruvds/blog/327530/> про sed
- <https://habr.com/ru/company/ruvds/blog/327754/> про awk
- <https://losst.ru/komanda-find-v-linux> про find
- <https://www.howtoforge.com/linux-locate-command/> про locate
- <https://regexone.com> тренажер регэкспов
- <https://regex101.com> тестилка для регэкспов

The background of the image is an aerial photograph of a dense city skyline, likely New York City, with numerous skyscrapers. The image is overlaid with a semi-transparent blue layer that features a white network pattern of interconnected dots and lines. The text is centered within this blue layer.

Заполните, пожалуйста,
опрос о занятии по ссылке в ЛК
<https://otus.ru/polls/10237/>

Всем спасибо! Ждём на следующих занятиях



Вяземский Семён Валерьевич

QA Automation Lead

Beeline

svvyazemsky@gmail.com