Мониторинг в ОС FreeBSD 2

Первое с чего начну, это всем известная утилита **top**. Она показывает общие сведения о процессоре, памяти и процессах, если возникают вопросы по производительности, я её запускаю первой, чтобы выявить аномалии в системе. У утилиты **top** есть параметры, которые облегают жизнь, их мы набираем в top’е когда он запущен:

S – показать системные процессы, по умолчанию они не показываются
u – и имя пользователя, например u mysql покажет процессы запущенные от пользователя mysql
o – используем для сортировки, возможные параметры – pri, size, res, cpu, time, threads
m – переключение между режимами отображения нагрузки и ввода-вывода
k – завершить процесс, ввод pid процесса
r – изменить приоритет процесса, вводим pid процесса
n – отображать статистику по определённому процессу
a – показывает абсолютные запущенных процессов

top -n 3 – показывает самые ресурсоёмкие приложения в данный момент

gstat – *показывает использование дисков*.
gstat -a – используется для вывода только активных устройств

vmstat – *показывает состояние виртуальной памяти и буфера*.
vmstat 5 – отображает статистику раз в пять секунд
vmstat -z – показывает состояние буфера
vmstat -i – показывает состояние прерываний

iostat – *выводит статистику по I/O устройств*
iostat -d -w5 – показывать информацию по дискам, с периодичностью в пять секунд безостановочно
iostat -dx -w5 – показывает расширенную статистику

systat – *отображает различные параметры системы*.
systat -vmstat 1 – отображает суммарную системную статистику
systat -netstat 1 – показывает активные сетевые соединения
systat -ifstat 1 – отображает нагрузку сетевых интерфейсов

systat -tcp 1 – отображает статистику tcp-соединения, возможен просмотр по icmp, ip, icmp6, ip6
systat -iostat 1 – отображает нагрузку на процессов, дисковую подсистему
systat -swap 1 – показывает загрузку файла подкачки

netstat – *показывает активные сетевые соединения*.
netstat -w 1 – количество пакетов в настоящее время
netstat -ibt – вывод сетевых интерфейсов с разбивкой по IP адресам, отображает объём трафика, количество ошибок, коллизий.
netstat -rn – отображает таблицу маршрутизации
netsat -na -f inet – чтобы увидеть открытые сетевые соединения,
можно использовать команду netstat(8) с ключом **-a**. Ключ **-n** сообщает команде **netstat(8)**,
что она не должна выполнять преобразование IP-адресов в имена хостов, –
такое преобразование не только замедляет вывод информации, но и может породить
неоднозначность полученных результатов. Наконец, параметр **-f inet** требует от **netstat(8)**
беспокоиться только о сетевых соединениях.

Колонки **Recv-Q** и **Send-Q** показывают, сколько байт в том или ином соединении ожидают обслуживания. Если в колонке **Recv-Q** *ненулевые* значения присутствуют *постоянно*, значит, система *не может* обрабатывать входные данные достаточно быстро. Точно так же постоянно присутствующие значения в **Send-Q** говорят о том, что либо сеть, либо другая сторона соединения не могут принять данные с той скоростью, с какой они посылаются. Случайные пакеты, ожидающие своей очереди, – это нормально. Колонка **Foreign Address** (внешний адрес) показывает удаленный адрес (remote address) и номер порта для каждого соединения. Наконец, колонка **(state)** показывает состояние рукопожатия TCP. В данный момент не требуется знать все возможные состояния TCP-соединения; достаточно понять, какие из них являются нормальными. Состояние **ESTABLISHED** означает, что соединение установлено и данные, по всей видимости, передаются. Состояния LAST_ACK, FIN_WAIT_1 и FIN_WAIT_2

означают, что соединение закрывается. Состояния SYN_RCVD, ACK и SYN+ACK – это этапы нормального создания соединения. Состояние **LISTEN** говорит, что порт готов принимать входящие соединения. Если вас не интересуют сведения о *сокетах*, ожидающих входящие соединения, а интерес представляют только *активные соединения*, можно вместо ключа **-a** использовать ключ **-b**. Например, команда **netstat -nb -f inet** отобразит только *установленные соединения* с удаленными системами.

ifconfig - *используется для конфигурирования сетевых интерфейсов*
ifconfig -a - список всех сетевых интерфейсов
ifconfig -u - список поднятых сетевых интерфейсов
ifconfig -d - список выключенных сетевых интерфейсов
ifconfig rl0 down - отключить сетевой интерфейс
ifconfig rl0 up - поднять интерфейс
ifconfig eth0 192.168.2.2 - назначить IP адрес 192.168.2.2 на интерфейс eth0
ifconfig eth0 netmask 255.255.255.0 - изменить сетевую маску на интерфейсе eth0
ifconfig eth0 broadcast 192.168.2.255 - изменить бродкаст адрес для интерфейса eth0
ifconfig eth0 192.168.2.2 netmask 255.255.255.0 broadcast 192.168.2.255 - назначить IP адрес, маску и бродкаст одной командой
ifconfig eth0 mtu XX - для изменения Maximum transmission unit (MTU) на значение XX
ifconfig eth0 promisc - команда переводи интерфейс в *promiscuous mode*
ifconfig eth0 -promisc - команда перевести интерфейс в нормальный режим

*По умолчанию когда сетевая карта получает пакет, она проверяет адрес получателя. В случае если этот адрес отличен от назначенных ей адресов, пакет отбрасывается. В **promiscuous mode**, карта не отбрасывает данные пакеты. Вместо этого она принимает все пакеты, приходящие через интрефейс. Для установки данного режима требуются привелегии суперпользователя. Большинство сетевых мониторов и анализаторов используют данный режим для захвата пакетов и*

анализа сетевого трафика.

diskinfo -t ad0 – *показывает информацию по диску*, и делает тест на дисковую производительность.

sysctl – *позволяет посмотреть параметры в системы и внести изменения, такие как стек tcp/ip, вирутальной памяти*.
sysctl -a – показывает все параметры
sysctl kern.ipc.numopensockets – показывает количество открытых сокетов
sysctl kern.openfiles – показывает количество открытых файлов

df – *утилита, которая показывает свободное место на дисках*.
df -h – отображает слайсы, и свободное\занятое место.
df -i – показывает количество занятых инодов.

fstat – *показывает список открытых файлов*.
fstat |grep http| wc -l – показывает список открытых файлов по процессу http

sockstat – *отображает информацию о сокетах, сетевых и файловых*.
sockstat -l – список портов открытых на прослушивание
sockstat -c список установленных соединений
sockstat -4, -6 – по протоколу ipv4 или ipv6

lsof – *показывает информацию от откртых сокетах, файлах и сетевых соединениях*.
lsof -i -n – показывает открытые интернет-соединения
lsof -i -n |grep ESTABLISHED – показывает открытые, и установленные сетевые соединения

ps auxww|grep имя\pid\от_кого_запущено – *позволяет получить информацию по интересующему процессу*.

mount – *показывает смонтированные разделы*.
swapinfo – *показывает информацию о файле подкачки*.

Также можно установить **iftop**, которая показывает статистику по сетевым интерфейсам, к при меру:

iftop -i em0

tunefs -p /tmp – *показывает информацию о файловой системе*.

pciconf -lv - *информация об устройствах* (в т.ч. сетевых картах)

uname -a – показывает информацию о системе, ядре.
date – выводит текущую дату и время.
w – показывает кто, откуда, во сколько зашёл в систему.
last – показывает историю входов в систему, и последнюю перезагрузку.
uptime – показывает сколько система работает с момента последней перезагрузки.