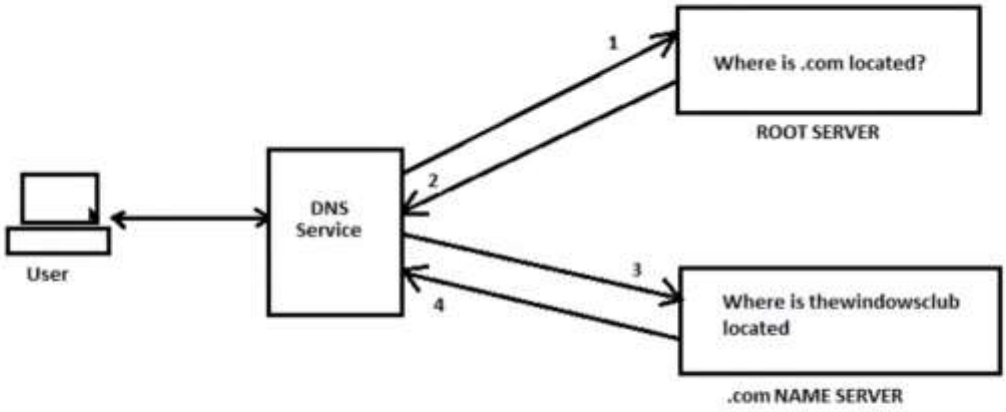
DNS

Все коннекты, передача пакетов происходит по ip адресу. DNS – сервер преобразования имен(в ip адреса).



Understanding How DNS Lookup Works

Пользователь пишет запрос, комп по 53 upd порту отсылает запрос на свой DNS сервер.

2 сервера: master и его репликация(slave), на случай если мастер упал. В них находится таблица соответствия хостов и ip адресов.

13-15 главных DNS серверов, которые вшиты в os, обращение к ним по дефолту. Эти сервера расположены по всему миру.

host –t ns ru.

sudo vim /etc/hosts – тут можно править «локальный днс», т.е сначала система будет смотреть в этот файл и брать ip из соответствия.

DNS записи

Это соответствие хоста и определенной информации. Например A – запись это соответствие имени к ip адресу(ipv4).

Запись AAAA показывает ipv6 адрес.

ipv6 придуман, т.к закончились ipv4 адреса, там есть изменения типа другого dhcp и тд.

Запись MX – когда отправляем письмо на почту админа сайта, почтовый клиент посмотрит запись mx и будет знать на какой хост послать это письмо. У этих записей есть приоритет. Чем меньше – приоритет больше.

Запись CAA – если тут указаны какие-либо записи с указанием определенных провайдеров ssl сертификатов, то только они смогут выписать сертификат на этот домен.

Запись CNAME – соответствие одного домену другому, например перенаправлять vk.net на vk.com

Запись TXT – техническая информация, можно использовать для подтверждение владения доменом.

Запись SRV – информация о сервисе, например название веб-сервера, порт.

Запись PTR – по ip адресу ищет имя сайта.

Логи в Linux

Все логи по умолчанию лежат в /var/log

Структура этой директории:

alternatives.log – тут разные символьные ссылки

apt – логи команды apt

less apt/term.log – что происходило при установке

logrotate – политика чистки логов, архивация логов

auth.log – все коннекты по ssh тут хранятся

bootstrap.log – файл, который создается при первом запуске системы

btmp – информация о логинах/ip адресах при ssh подключениях.

cloud-init-output.log – система, которая позволяет настраивать и запускать виртуалку нужным образом.

dist-updrage – логи обновления пакетов в системе.

dmesg – кольцевой буфер ядра, эти сообщения генерирует ядро. Тут информация с последнего запуска система.

dmesg.0 – за все время.

dpkg – логи установки dpkg

faillog – неудачные коннекты к серверу.

installer – все что происходило при установке операционной системы писалось в этот лог.

journal – служба, как и syslog отслеживает stdout приложений, но пишет бинарно, данные лежат более компактно.

kern.log – сообщения ядра.

landscape – система управления больших кол-вом debian подобных систем.

lastlog – используется в команде last

nginx – логи nginx, тут например будет mysql

syslog – здесь все сообщения, которые не попали под фильтр в утилите syslog.

unattended-upgrades – логи принудительных апгрейдов

wtmp – команда last читает этот файл.

oom killer

Когда в системе кончается ОЗУ, комп начинает тупить, программы не могут нормально функционировать. Для всех действий нужна оперативная память. Когда кончится ОЗУ система упадет, kernel panic. Чтобы такого не было есть механизм oom killer. Ядро само контролирует каждый процесс, и проставляет им баллы, например это приложение есть много ОЗУ. И когда нужно запустить приложение, а памяти уже не осталось и при этом весь кеш уже очистился, то система ищет кого пристрелить(приложение с самым большим количеством очков).

kill – посыл сигнала приложению.

dmesg – T | grep –i oom – смотрим вызовы киллера в системе.

mtr – это как traceroute, только в динамике.

mtr --tcp facebook.com –P 443

tcpdump

tcpdump –vvnnelpi any arp – можно увидеть запрос на широковещательный адрес «who-has ip»

arp – a – таблица соответствий ip адресов и mac.

strace

Используется для отслеживания системных вызовов.

strace ls –la

Как узнать путь к конфигам процесса?

strace –s 1000 –tTyfp 4966 (4966-pid)

strace –e openat –s 1000 –tTyfp 4966 (4966-pid) ищем в выводе строки с openat

lsof – все открытые файлы в системе.

lsof –p pid – открытые файлы процессом с pid

ltrace – отображает вызовы функций в шареной библиотеке.

ldd /user/bin/nginx – какие библиотеки использует бинарь

ss - утилита, которая показывает все сокеты и установленные или неустановленные соединения в системе.

ss –n - ускоряет отображение (нет разрешения адресов)

ss –napu

По какому протоколу работает DNS?

И по udp и по tcp

tcp в двух случаях:

1) Для трансфера зон(slave обращается к master чтобы выкачать данные зон)
2) Бывает такое что данные не помещаются в udp пакет и идет запрос на установление tcp соединения.

ss –tulpan – информативный вывод

ss –napt – все соединения

ifstat

ifstat – показывает по всем интерфейсам сколько входит/выходит трафика.

iftop – показывает с какого порта и на какой идет трафик и в каком количестве.

iostat – информация о дисках

iotop – как top только для i/o

---

wget –O name url – скачать файл с url и назвать его name

unzip – разархивировать

nginx изначально создавался, чтобы быстро и параллельно отдавать статику, т.к апач делал это медленно.

В идеале – 1 виртуалка на nginx, другая на php-fpm, третья – на БД.(типа микросервисы) (Вдруг надо провести тех.работы, заменить диски и тд).

cron задача – задача по расписанию.