
Работа с утилитами диагностики и мониторинга сетевых соединений в Linux

Цель работы: получить практические навыки по диагностики сетевых соединений и базовому мониторингу сетевых соединений в Linux.

Требования: для выполнения работы необходимы базовые навыки работы с командной строкой Linux и установленная виртуальная машина Linux, или Linux на реальном хосте с доступом в сеть. Описание конфигурационных файлов и работы пакетного менеджера дается для Linux Centos 7. Скачать виртуальную машину для среды Virtual Box можно по адресу: https://disk.yandex.ru/d/PM_qnSdXSFWoXA

Пароль root – jango123#

Краткие теоретические сведения

Linux – UNIX-подобная, многозадачная операционная система. Основным для нее является текстовый интерфейс, хотя для Linux разработаны (или портированы) графические оболочки, такие как KDE или Gnome.

Обычно в Linux запускаются несколько консолей, переключаться между которыми можно по кнопкам Alt + F1 для первой консоли, Alt + F2 для второй и т. д.

Краткую справку по каждой команде можно получить с помощью команды `man`, краткую с помощью ключа `-h` (`-help`). Например: `man ifconfig`. Также полезными для получения справки могут оказаться команды `argropos` и `whatis`.

Если утилиты окажутся недоступны, то их можно установить через менеджера пакетов. Например, так: `yum install netload`.

Чтобы узнать, к какому пакету относится та или иная утилита можно воспользоваться командой:

`yum whatprovides имя_утилиты`.

Для диагностики сетевых соединений служит протокол ICMP. Его используют консольные утилиты `ping`, `tracert`, `mtr`. Эти утилиты позволяют проверять доступность удаленного хоста и диагностировать соединение. Для мониторинга интерфейсов используются множество утилит. Среди них `nload`, `iftop`, `bmon`. Для сбора статистики используются демон `vnstat`. Диагностировать соединения приложений позволяют такие утилиты как `nethogs`

Для того, чтобы разрешить запуск службы и запустить ее используются команды:

`systemctl enable ИмяСервиса`

`systemctl start ИмяСервиса`

Порядок выполнения работы

Часть 1. Настройка инфраструктуры

1. Подготовьте две виртуальные машины.
2. Одну машину назовите c7-1, другой c7-2
3. Для виртуальной машины c7-1 добавьте второй сетевой интерфейс.
4. Для машины c7-1 один из интерфейсов настройте в режим NAT.
5. Через второй интерфейс свяжите машину c7-1 с машиной c7-2 через внутреннюю сеть.
6. Для внутренней сети задайте для машин c7-1 и c7-2 адреса 10.0.0.1 и 10.0.0.2 с маской 255.255.255.0.
7. Для интерфейса c7-1, настроенного на NAT оставьте получение адреса автоматически.

Часть 2. Установка программного обеспечения

1. Установите на машину c7-1 программы:
 - a. nload,
 - b. iftop,
 - c. bmon
 - d. nethogs
 - e. mtr
 - f. traceroute
 - g. vnstat

Часть 3. Диагностика соединения

1. Познакомьтесь с ключами утилиты ping.
2. На машине c7-2 напишите команды ping, которые:
 - a. отправляют 10 пакетов на c7-1
 - b. отправляют 10 пакетов с интервалом 10 секунд на машину c7-1
 - c. отправляет 5 пакетов размером 1500 байт на машину c7-1
3. Выясните что означат использование ключа -f (используйте его **только** при использовании утилиты ping между хостами c7-1 и c7-2)

Часть 4. Определение маршрута прохождения пакета

1. Познакомьтесь с ключами утилиты traceroute.
2. На машине c7-1 напишите команды traceroute, которые:
 - a. определяют маршрут до хоста 8.8.8.8 с помощью ICMP
 - b. определяют маршрут до хоста 8.8.8.8 с помощью UDP
 - c. определяют маршрут до хоста 8.8.8.8 с помощью TCP
 - d. позволяет определить используется ли по маршруту фрагментация IPv4

Часть 5. Диагностика качества соединения

1. Познакомьтесь с ключами утилиты mtr.
2. С хоста c7-1 соберите статистику соединения с хостом www.itmo.ru
3. Определите значение всех параметров, выводимых утилитой mtr.
4. Напишите команду, которая сохранит в файл расширенную статистику работы mtr при отправке 40 пакетов.

Часть 6. Диагностика работы приложений через сеть

1. Познакомьтесь с ключами утилиты nethogs.
2. С хоста c7-2 подключитесь по ssh к машине c7-1. В терминале ssh запустите утилиту top.
3. На хосте c7-1 с помощью утилиты nethogs определите
 - a. Среднюю скорость передачи данных до sshd.
 - b. PID процесса sshd.

Часть 7. Текущий мониторинг сетевых интерфейсов

1. С хоста c7-2 запустите отправку запросов утилитой ping в режиме flood.
2. На хосте c7-1 последовательно с помощью утилит nload iftop и bmon получите данные о загрузке интерфейса, через который подключен хост c7-2.
3. Изменяйте размер пакета, передаваемой утилитой ping пакета от 100 до 60100 с шагом 10000. Определите, как меняется загрузка на сетевом интерфейсе.

Часть 8. Сбор статистики о загрузке сетевого интерфейса

1. На хосте c7-1 запустите демон vnstat.
2. Поставьте на мониторинг интерфейс, через который машина c7-1 подключена к c7-2
3. С хоста c7-2 запустите отправку запросов утилитой ping в режиме flood, так чтобы работа утилиты прекратилась после отправки 500 пакетов.
4. Выведите статистику собранного трафика.