Практическая работа к занятию №5

# Работа с утилитами диагностики и мониторинга сетевых соединений в Linux

**Цель работы:** получить практические навыки по диагностики сетевых соединений и базовому мониторингу сетевых соединений ы 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://yadi.sk/d/Tnre3kp97Oi1YA> . 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 перовой 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 apropos 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, traceroute, 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 ИмяСервиcа

systemctl start ИмяСервиcа

**Порядок выполнения работы:**

Далее описан порядок выполнения работы. Пункты работы, результаты которых прямо или косвенно используются в отчете, помечены знаком **(!)**.

**Часть 1. Настройка инфраструктуры**

1. Подготовьте две виртуальные машины.
2. Одну машину назовите c7-1, другой с7-2
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 c машиной c7-2 через внутреннюю сеть.
6. Для внутренней сети задайте для машин с7-1 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:
   1. nload,
   2. iftop,
   3. bmon
   4. nethogs
   5. mtr
   6. traceroute
   7. vnstat

**Часть 3. Диагностика соединения**

1. Познакомитесь с ключами утилиты ping.
2. На машине c7-2 напишите команды ping, которые **(!)**:
   1. отправляют 10 пакетов на c7-1
   2. отправляют 10 пакетов с интервалом 10 секунд на машину c7-1
   3. отправляет 5 пакетов размером 1500 байт на машину с7-1
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. Познакомитесь с ключами утилиты traceroute.
2. На машине c7-1 напишите команды traceroute, которые **(!)**:
   1. определяют маршрут до хоста 8.8.8.8 с помощью ICMP
   2. определяют маршрут до хоста 8.8.8.8 с помощью UDP
   3. определяют маршрут до хоста 8.8.8.8 с помощью TCP
   4. позволяет определить используется ли по маршруту фрагментация IPv4

**Часть 5. Диагностика качества соединения**

1. Познакомитесь с ключами утилиты mtr.
2. С хоста c7-1 соберите статистику соединения с хостом [www.itmo.ru](http://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. Познакомитесь с ключами утилиты nethogs.
2. С хоста c7-2 подключитесь по ssh к машине с7-1. В терминале ssh запустите утилиту top.
3. На хосте c7-1 с помощью утилиты nethogs определите **(!)**
   1. Среднюю скорость передачи данных до sshd.
   2. 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 загрузки сетевого интерфейса**

1. На хосте с7-1 запустите демон vnstat.
2. Поставите 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 **(!)**.

**Содержание отчета**

Требуется подготовить отчеты в формате DOC\DOCX или PDF. Отчет содержит титульный лист, артефакты выполнения и ответы на вопросы и задания.

Артефакты:

* 1. Тексты команд и консольный вывод из Части 3, п.2.
  2. Текст команды и консольный вывод из Части 4, п.2.
  3. Текст команды и консольный вывод из Части 5, п.4.
  4. Текст команды и консольный вывод из Части 6, п.3.
  5. Текст команды и консольный вывод из Части 8, п.2,4.

Вопросы и задания:

1. Прокомментируйте результаты, полученные в Части 7, п.3
2. Для тестирования соединения была использована утилита mtr. Были получены большие значения Best, маленькие значения Wrst, средние между первыми параметрами значения Avg и высокие значения StDev. Какие данные можно использовать для анализа?
3. Какие еще данные статистики передачи можно получить из команды mtr.

Отчет выслать в течение 4-х недель на адрес [edu-net@yandex.ru](mailto:edu-net@yandex.ru).

В теме письма: №группы ФИО (латинскими буквами) №работы (например: 5555 Fedor Sumkin 3)

**Поддержка работы**

Дополнительные материалы по теме курса публикуются на Telegram-канале ITSMDao (t.me/itsmdao). Обсуждать работу и задавать вопросы можно в чате ITSMDaoChat (t.me/itsmdaochat).