Министерство науки и высшего образования Российской Федерации

Рязанский государственный радиотехнический университет им. В.Ф. Уткина

Управление пакетами в Linux.

Инсталляция пакетов

Методические указания к практическим занятиям

Рязань 2020

УДК 681.3.06

Управление пакетами в Linux. Инсталляция пакетов: методические указания к практическим занятиям / Рязан. гос. радиотехн. ун-т.; сост. А.А. Митрошин, В.Г. Псоянц. – Рязань, 2020. – 16 с.

Содержат описание практического занятия, используемого в курсе «Операционная система Linux». Могут использоваться при изучении других курсов, связанных с операционной системой Linux.

Предназначены для студентов очной, заочной и очно-заочной форм обучения направления подготовки «Информатика и вычислительная техника». Могут использоваться для студентов других направлений подготовки.

Могут использоваться как методические указания к лабораторным работам в курсах, связанных с изучением операционной системы Linux и свободно распространяемого программного обеспечения.

Ил. --. Библиогр.: -- назв.

Операционная система Linux, пакет, rpm, md5sum

Печатается по решению редакционно-издательского совета Рязанского государственного радиотехнического университета.

Рецензент: кафедра САПР вычислительных средств Рязанского государственного радиотехнического университета (зав. кафедрой засл. деят. науки и техники РФ В.П.Корячко)

Управление пакетами в Linux. Инсталляция пакетов

Составители: Митрошин Александр Александрович

Псоянц Владимир Грикорович

Редактор \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Корректор \_\_\_\_\_\_\_\_\_\_\_\_\_

Подписано в печать \_\_\_\_\_\_\_\_. Формат бумаги 60×84 1/16.

Бумага газетная. Печать трафаретная. Усл. печ. л. 1,0.

Уч-изд. л. 1,0. Тираж 50 экз. Заказ

Рязанский государственный радиотехнический университет.

390005, Рязань, ул. Гагарина, 59/1.

Редакционно-издательский центр РГРТУ.

**Проверка подлинности пакетов**

Перед инсталляцией пакета необходимо выполнить проверку его подлинности, поскольку злоумышленник может изменить содержимое пакета, например, добавив в него вирус. Особенно важно осуществлять проверку при получении пакетов из непроверенных источников. Проверку подлинности пакетов можно осуществлять несколькими способами.

**Проверка подлинности с помощью функции хэширования**

Основная форма проверки подлинности пакетов подразумевает использование функции хэширования. Велична, получаемая с помощью функции хэширования, называется хэшем. Хэш характеризует набор данных произвольного размера посредством фрагмента данных фиксированной длины. В отличии от контрольной суммы, вывод хэша трудно предсказуем, то есть очень сложно модифицировать данные, а затем сгенерировать идентичный хэш. Большинство алгоритмов используют длинный ключ (например, 128 битный), то есть вероятность сгенерировать аналогичный ключ чрезвычайно мала. Если загружается файл из незнакомого источника, но есть ключ из доверенного источника, то можно быть уверенным, что:

- шансы получить модифицированный файл с идентичным хэшем очень невелики;

- вероятность того, что злоумышленник может взять файл, модифицировать его и сгенерировать идентичный хэш, бесконечно мала.

Популярным инструментом генерирования хэшей является программа md5sum на основе алгоритма MD5 (Message Digest номер 5). Программа md5sum может создавать хэши и проверять их. Для того, чтобы сгенерировать хэш, нужно после имени программы указать имя файла (или файлов), для которого хэш генерируется.

Хэш имеет вид шестнадцатиричного числа, состоящего из 32 цифр (каждое шестнадцатиричное число – 4 бита). Хэш можно проверить, сравнив его с значением из доверенного источника и убедившись, что данные корректны. Если хэши совпадают, то можно быть уверенным, что файл не подвергался изменению с момента создания хэша.

Пример создания и проверки хэша файла приведен на рис 1.

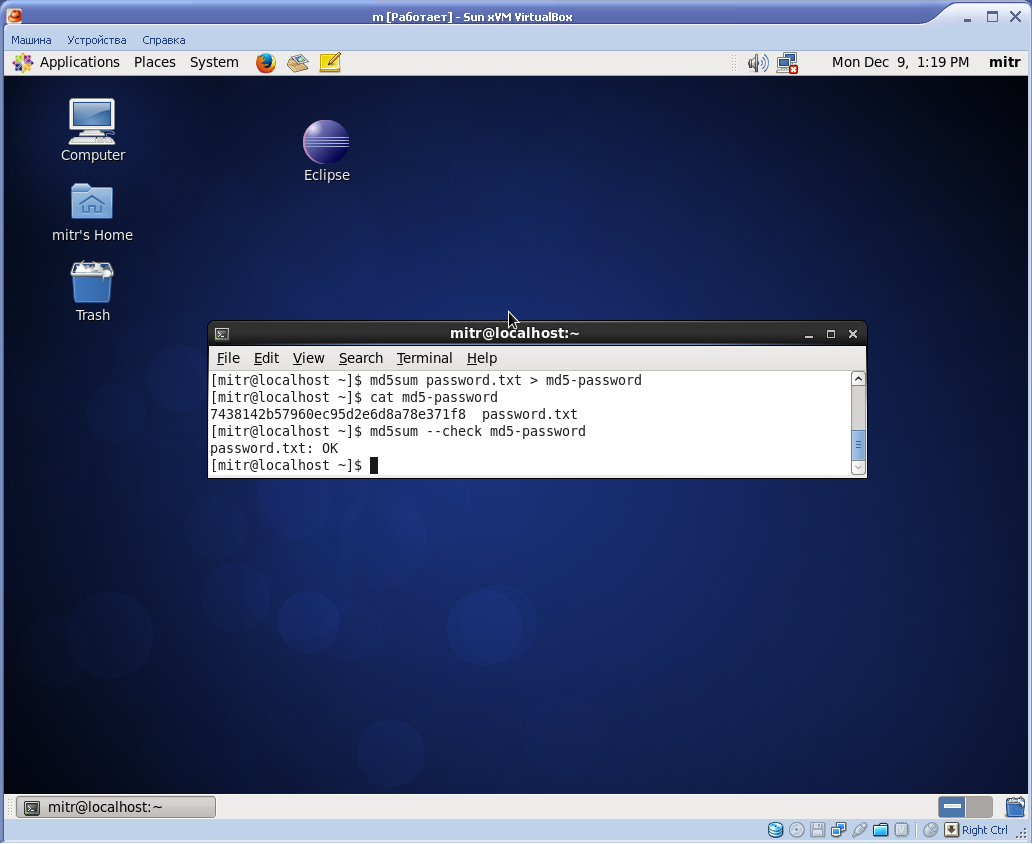


Рисунок 1. Создание и проверка хэша с помощью md5sum

Если теперь изменить файл password.txt то проверка даст результаты, показанные на рис. 2.

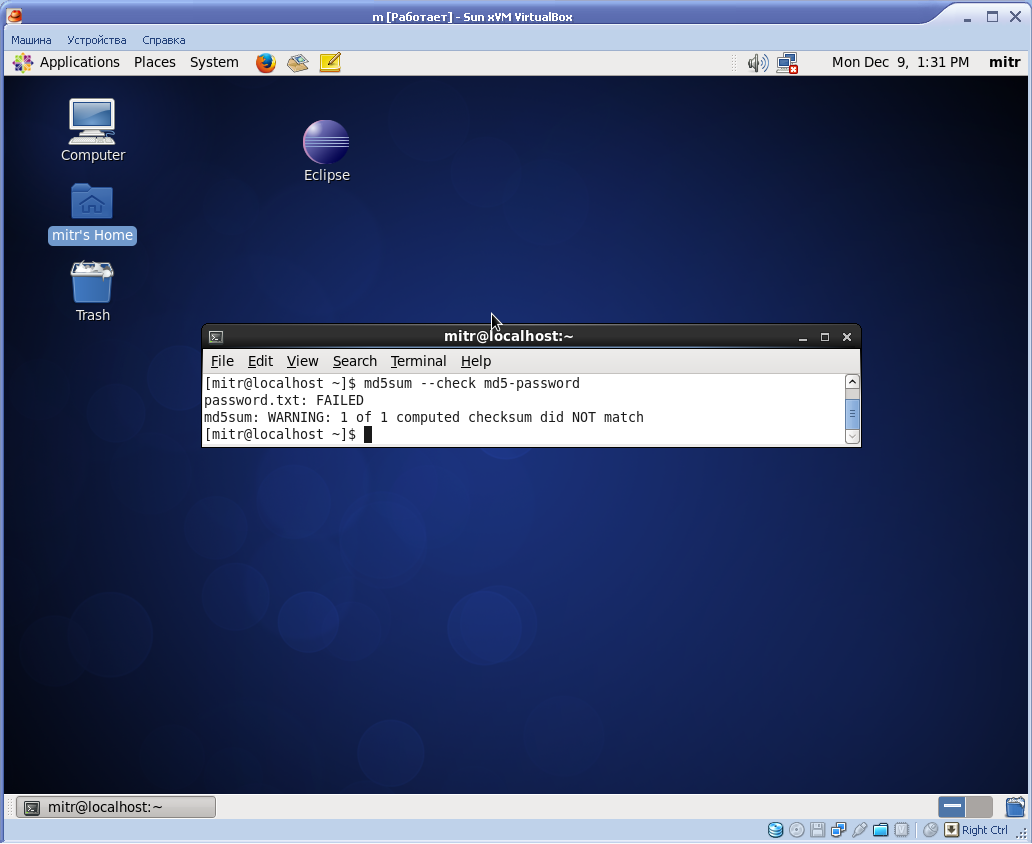


Рисунок 2. Результат проверки с помощью md5sum измененного файла

**Проверка подлинности с использованием цифровой подписи**

Цифровая подпись – некоторая разновидность хэша, которая, однако, не требует никаких уникальных сведений о данных, подвергающихся проверке подлинности. Для проверки подлинности цифровой подписи нужен только публичный ключ, предоставляемый лицом или организацией, которую необходимо аутентифицировать. Имея публичный ключ можно подвергать проверке любые данные, подписанные таким лицом или организацией.

Лицо, которое желает подписать данные, генерирует два ключа: публичный и приватный. В основе ключей лежит пароль, который известен только создателю ключей. Создатель лежит пароль и приватный ключ в секрете, а публичный ключ доступен для всех желающих.

При работе с цифровыми подписями в сфере свободного программного обеспечения наиболее популярен инструмент GNU Privacy Guard (GPG). Процесс подписи данных с использованием PGP показан на рис. 3.

Данные

Приватный ключ

Провайдер

Подписанные данные

Потребитель

Публичный ключ

Рисунок 3. Использование GPG при работе с электронной подписью

Менеджер пакетов rpm позволяет подписывать пакеты электронной подписью для последующей проверки их подлинности.

Общая форма команды проверки подлинности rpm:

**rpm –checksig имя\_пакетного файла**

Очевидно (рис. 3), чтобы произвести проверку, нужен публичный ключ. Дистрибутивы Linux могут содержать несколько публичных ключей, которые использованы для подписи пакетов, входящих в состав дистрибутива. Если необходимого публичного ключа нет, то его можно постараться получить на сайте производителя пакета. Если публичный ключ PGP доступен в текстовом виде, то нужно сохранить его в файле и импортировать с помощью команды

**rpm --import имя\_файла\_с\_ключем\_GPG**

**Проверка пакетов**

Проверку содержимого пакета можно выполнить до его установки. Например, содержимое екоторого rpm-файла можно запросить с помощью команды

**rpm –qip имя\_файла.rpm**

Часто используемые запросы к файлу, содержащему пакет, приведены в табл. 1.

Таблица 1. Часто используемые запросы к файлу пакета

|  |  |
| --- | --- |
| Запрос | rpm |
| Базовые сведения о пакете | rpm –qpi имя\_файла |
| Список файлов для установки | rpm –qpl имя\_файла |
| Сценарии установки и удаления | rpm –qp -scripts имя\_файла |
| Показать пакеты, необходимые для данного пакета | Rpm –qp - -requires имя\_файла |
| Показать, какой пакет представляет этот файл | rpm –qp - -provides имя\_файла |

**Порядок выполнения работы**

1) Изучите теоретический материал.

2) Выполните практическое задание.

3) Ответьте на контрольные вопросы.

**Практическое задание**

1) Создайте два текстовых файла.

2) С помощью md5sum получите их хэши.

3) Проверь эти файлы на отсутствие изменений с использованием md5sum.

4) Измените один из файлов и снова выполните проверку.

5)

**Контрольные вопросы**

1) Что представляет собой функция хэширования?

2) Как с помощью md5sum получить хэш файла и проверить корректность файла?