

Липецкий государственный технический университет

Факультет автоматизации и информатики

Кафедра автоматизированных систем управления

ЛАБОРАТНАЯ РАБОТА №7

по дисциплине «OS Linux»

на тему «Работа с SSH»

Студент

Сухоруких А.О.

Группа АС-18

Руководитель

Кургасов В.В.

к.т.н

Липецк 2020 г.

Оглавление

Цель работы	3
1 Ход работы.....	5
Вывод.....	9

Цель работы

Ознакомиться с программным обеспечением удалённого доступа к распределённым системам обработки данных.

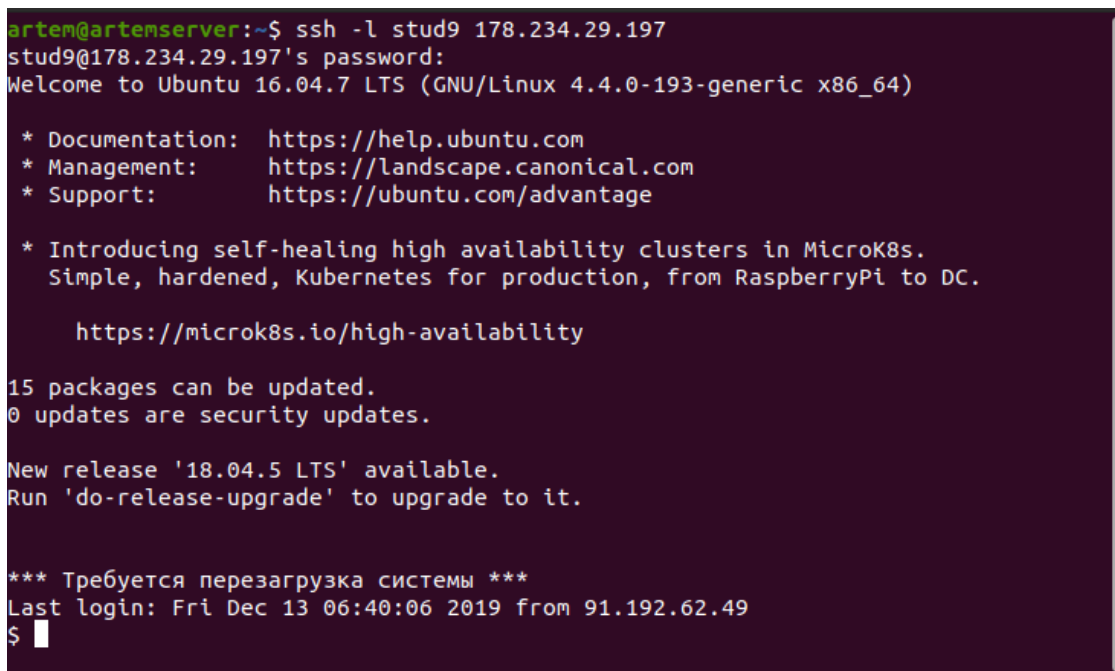
Задание

1. Подключиться к удалённому серверу по паролю;
2. Просмотреть окружение пользователя;
3. Сгенерировать пару ключей доступа к серверу, передать публичный ключ на сервер;
4. Проверить работоспособность подключения к хосту по ключу;
5. Организовать подключение к хосту по имени.

1 Ход работы

1.1 Подключиться к удалённому серверу по паролю

Для авторизации на сервере по выданным данным воспользуемся командой `ssh`, с использованием в качестве операнда `-l stud9`, где `stud9` – это имя пользователя, и введем выданный нам пароль. Результат выполнения команды показан на рисунке 1



```
artem@artemserver:~$ ssh -l stud9 178.234.29.197
stud9@178.234.29.197's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-193-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

   https://microk8s.io/high-availability

15 packages can be updated.
0 updates are security updates.

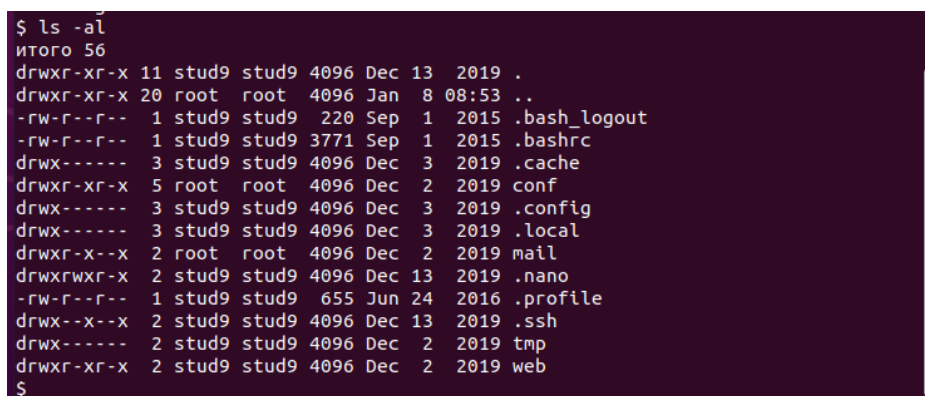
New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** Требуется перезагрузка системы ***
Last login: Fri Dec 13 06:40:06 2019 from 91.192.62.49
$
```

Рисунок 1 – Подключение к серверу с паролем

1.2 Просмотреть окружение пользователя

Для просмотра окружения пользователя воспользуемся командой `ls -al`. Результат выполнения команды показан на рисунке 2.



```
$ ls -al
итого 56
drwxr-xr-x 11 stud9 stud9 4096 Dec 13  2019 .
drwxr-xr-x 20 root  root  4096 Jan  8 08:53 ..
-rw-r--r--  1 stud9 stud9  220 Sep  1  2015 .bash_logout
-rw-r--r--  1 stud9 stud9 3771 Sep  1  2015 .bashrc
drwx-----  3 stud9 stud9 4096 Dec  3  2019 .cache
drwxr-xr-x  5 root  root  4096 Dec  2  2019 conf
drwx-----  3 stud9 stud9 4096 Dec  3  2019 .config
drwx-----  3 stud9 stud9 4096 Dec  3  2019 .local
drwxr-x--x  2 root  root  4096 Dec  2  2019 mail
drwxrwxr-x  2 stud9 stud9 4096 Dec 13  2019 .nano
-rw-r--r--  1 stud9 stud9  655 Jun 24  2016 .profile
drwx--x--x  2 stud9 stud9 4096 Dec 13  2019 .ssh
drwx-----  2 stud9 stud9 4096 Dec  2  2019 tmp
drwxr-xr-x  2 stud9 stud9 4096 Dec  2  2019 web
$
```

Рисунок 2 – Просмотр окружения пользователя

1.3 Сгенерировать пару ключей доступа к серверу, передать публичный ключ на сервер

Для генерации ключей воспользуемся командой `ssh-keygen`. После указание места хранения ключей и ввода секретной фразы для входа сгенерируется пара ключей: приватный (по умолчанию хранится в `~/.ssh/id_rsa`) и публичный (по умолчанию хранится в `~/.ssh/id_rsa.pub`). Результат выполнения команды показан на рисунке 3.



```
Connection to 178.234.29.197 closed.
artem@artemserver:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/artem/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/artem/.ssh/id_rsa
Your public key has been saved in /home/artem/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:2du4UcSPwu2Xh9Kqe74Rv69mS6DxGxDD2o7hde3xjba artem@artemserver
The key's randomart image is:
+---[RSA 3072]---+
|
| . .
| + o
| * = +
| S O O +
| . = & O *.
| o * E X +
| o.Ooo
| +==+++.
+-----[SHA256]-----+
artem@artemserver:~$
```

Рисунок 3 – Генерация ключей

1.4 Проверить работоспособность подключения к хосту по ключу

После нам необходимо передать публичный ключ на сервер. Для этого воспользуемся командой `ssh-copy-id`, с использованием параметра `-i`, который позволяет передать в качестве операнда расположение файла, хранящего публичный ключ. Результат выполнения команды показан на рисунке 4.

```

+----[SHA256]-----+
artem@artemserver:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud9@178.234.29.197
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/artem/.ssh/
id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
stud9@178.234.29.197's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'stud9@178.234.29.197'"
and check to make sure that only the key(s) you wanted were added.

artem@artemserver:~$

```

Рисунок 4 – Передача публичного ключа

Попробуем подключиться к серверу без использования пароля, результат выполнения команды показан на рисунке 5.

```

artem@artemserver:~$ ssh stud9@178.234.29.197
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-193-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

   https://microk8s.io/high-availability

Могут быть обновлены 15 пакетов.
0 обновлений касаются безопасности системы.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** Требуется перезагрузка системы ***
Last login: Sun Jan 17 16:14:29 2021 from 100.113.139.26
$

```

Рисунок 5 – Подключение к серверу без пароля

1.5 Организовать подключение к хосту по имени

Для подключения к серверу по имени, нам необходимо создать файл конфигурации в директории .ssh. Содержание файла показано на рисунке 6.

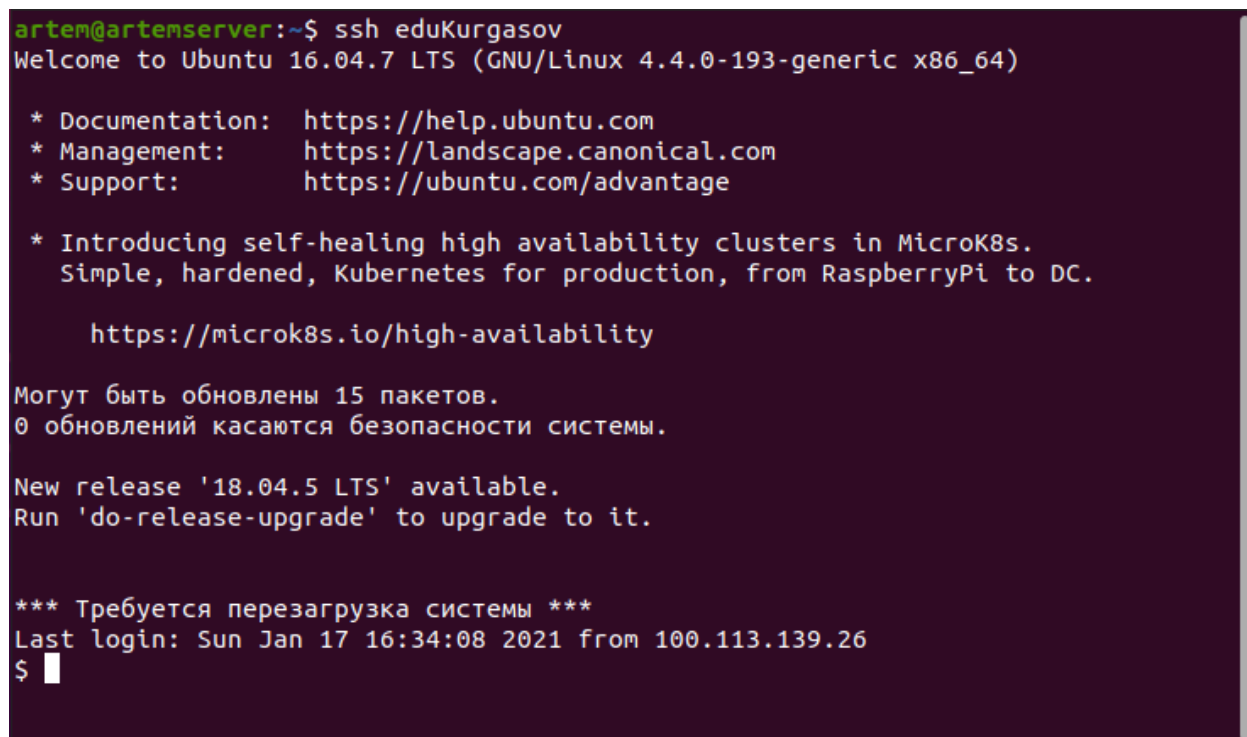


```
GNU nano 4.8 config
Host eduKurgasov
HostName 178.234.29.197
User stud9
Port 22
IdentityFile ~/.ssh/id_rsa

[ Wrote 5 lines ]
^G Помощь ^O Записать ^W Поиск ^K Вырезать ^J Выровнять ^C ТекПозиц
^X Выход ^R ЧитФайл ^\ Замена ^U Paste Text ^T Словарь ^_ К строке
```

Рисунок 6 – Содержание файла конфигурации

Попробуем подключиться к серверу по введённому нами значению имени. Результат выполнения команды показан на рисунке 7.



```
artem@artemserver:~$ ssh eduKurgasov
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-193-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

   https://microk8s.io/high-availability

Могут быть обновлены 15 пакетов.
0 обновлений касаются безопасности системы.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** Требуется перезагрузка системы ***
Last login: Sun Jan 17 16:34:08 2021 from 100.113.139.26
$
```

Рисунок 7 – Подключение к серверу по заданному имени

Вывод

В ходе выполнения лабораторной работы были получены основы работы с программным обеспечением удалённого доступа к распределённым системам обработки данных.

Ответы на контрольные вопросы

1. Что такое ключ ssh? В чем преимущество их использования?

SSH-ключи используются для идентификации клиента при подключении к удалённому серверу. SSH-ключи представляют собой пару ключей – приватный и публичный. Приватный ключ хранится в закрытом доступе у клиента, публичный отправляется на сервер. Преимущество использования ключей в удобстве (не нужно запоминать пароли) и безопасности (взломать приватный ssh-ключ достаточно сложно).

2. Как сгенерировать ключи ssh в разных ОС?

Генерация ssh-ключа в ОС Linux возможна с помощью команды `sshkeygen`. В ОС Windows можно использовать программу PuTTY для генерации ssh-ключей и подключения по ssh-протоколу.

3. Возможно ли из «секретного» ключа сгенерировать «публичный» и/или наоборот?

Нет, невозможно.

4. Будут ли отличаться пары ключей, сгенерированные на одном ПК несколько раз с исходными условиями (наличие/отсутствие пароля на «секретный» ключ и т.п.)

Да, будут. Утилита `ssh-keygen` каждый раз случайно генерирует пару ключей.

5. Перечислите доступные ключи для `ssh-keygen.exe`

- DSA;
- RSA;
- ECDASA;
- Ed25519.

6. Можно ли использовать один «секретный» ключ доступа с разных ОС, установленных на одном ПК/на разных ПК?

Можно, но безопасность такого ключа уже не гарантирована.

7. Возможно ли организовать подключение «по ключу» ssh к системе с ОС Windows, в которой запущен OpenSSH сервер?

Да, возможно, с использованием программы PuTTY.

8. Какие известные Вам сервисы сети Интернет позволяют организовать доступ к ресурсам посредством SSH ключей?

GitHub.