CompTIA Linux+

Working with Access Control List

Introduction

Welcome to the **Working with Access Control List** Practice Lab. In this module you will be provided with the instructions and devices needed to develop your hands-on skills.

Access Control
Linux System
ACL

Learning Outcomes

In this module, you will complete the following exercise:

- Exercise 1 - Working with Access Control List

After completing this lab, you will be able to:

- Implement Access Control List

Exam Objectives

The following exam objectives are covered in this lab:

- **LPI:** 104.5 Manage file permissions and ownership
- **LPI:** 110.1 Perform security administration tasks
- **CompTIA:** 3.1 Given a scenario, apply or acquire the appropriate user and/or group permissions and ownership.

Note: *Our main focus is to cover the practical, hands-on aspects of the exam objectives. We recommend referring to course material or a search engine to research theoretical topics in more detail.*

Lab Duration

It will take approximately **1 hour** to complete this lab.

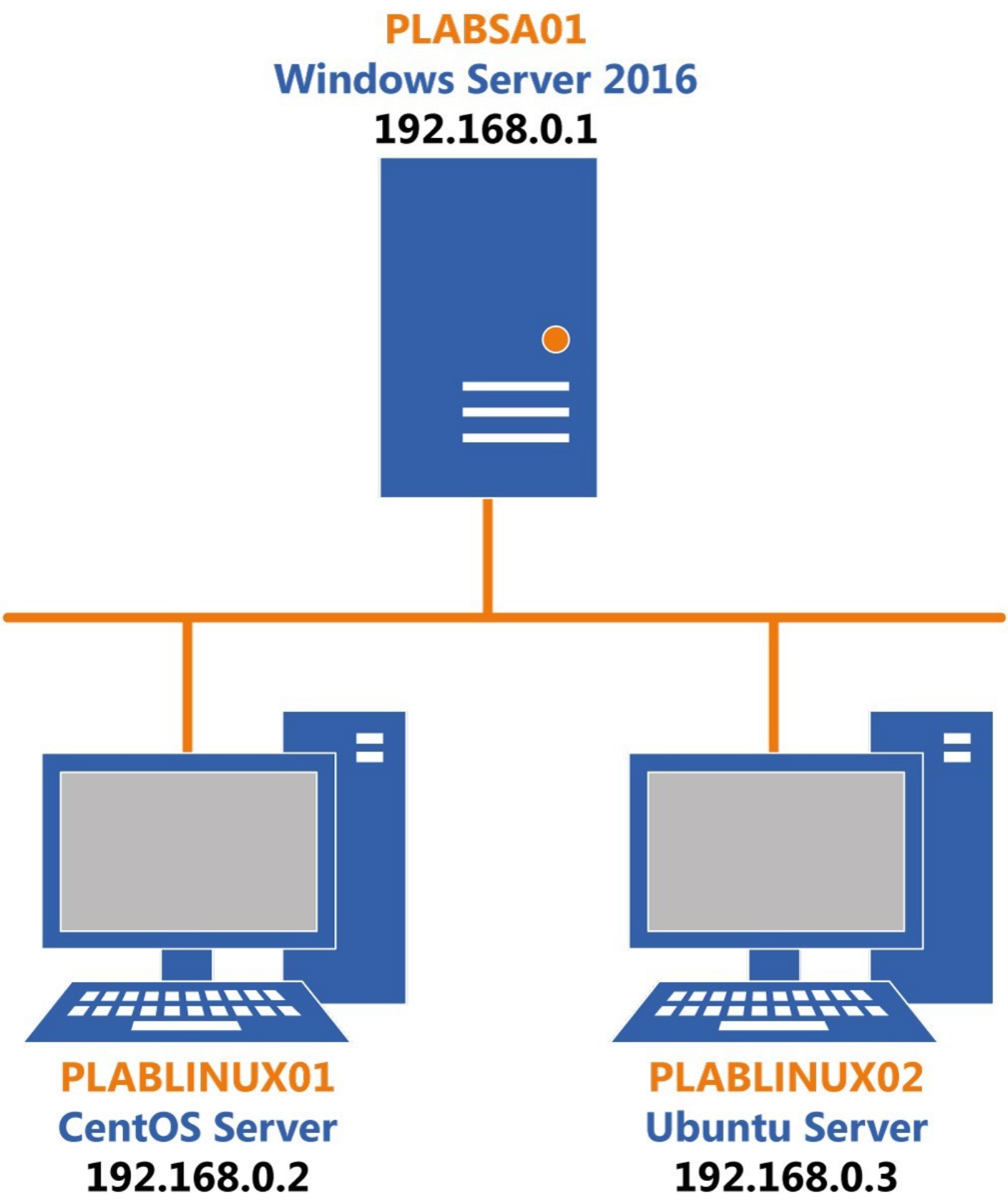
Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

Click Next to view the Lab topology used in this module.

Lab Topology

During your session, you will have access to the following lab configuration.



Depending on the exercises you may or may not use all of the devices, but they are shown here in the layout to get an overall understanding of the topology of the lab.

- **PLABSA01** (Windows Server 2016)
- **PLABLINUX01** (CentOS Server)
- **PLABLINUX02** (Ubuntu Server)

Click Next to proceed to the first exercise.

Exercise 1 - Working with Access Control List

CentOS uses permissions on the files and directories. However, the issue is that the permissions apply same for all the users in a system. For example, if you assign the Read permission, then it would apply to all the users. Each user can be assigned different permissions. Setting up access control lists on files and directories allows you to control the access to files and directories strictly.

In this exercise, you will learn to work with Access Control List (ACL).

Learning Outcomes

After completing this exercise, you will be able to:

- Log into a Linux System
- Implement Access Control List

Your Devices

You will be using the following device in this lab. Please power these on now.

- **PLABLINUX01** (CentOS Server)

Task 1 - Implement Access Control List

ACLs can be configured in four different ways, which are as follows:

- Per-user basis
- Per group basis

- Using an effective right mask
- For users other than the ones in the group for a file

In this task, you will learn to implement the access control list. To do this, perform the following steps:

Step 1

On the desktop, right-click and select **Open Terminal**.

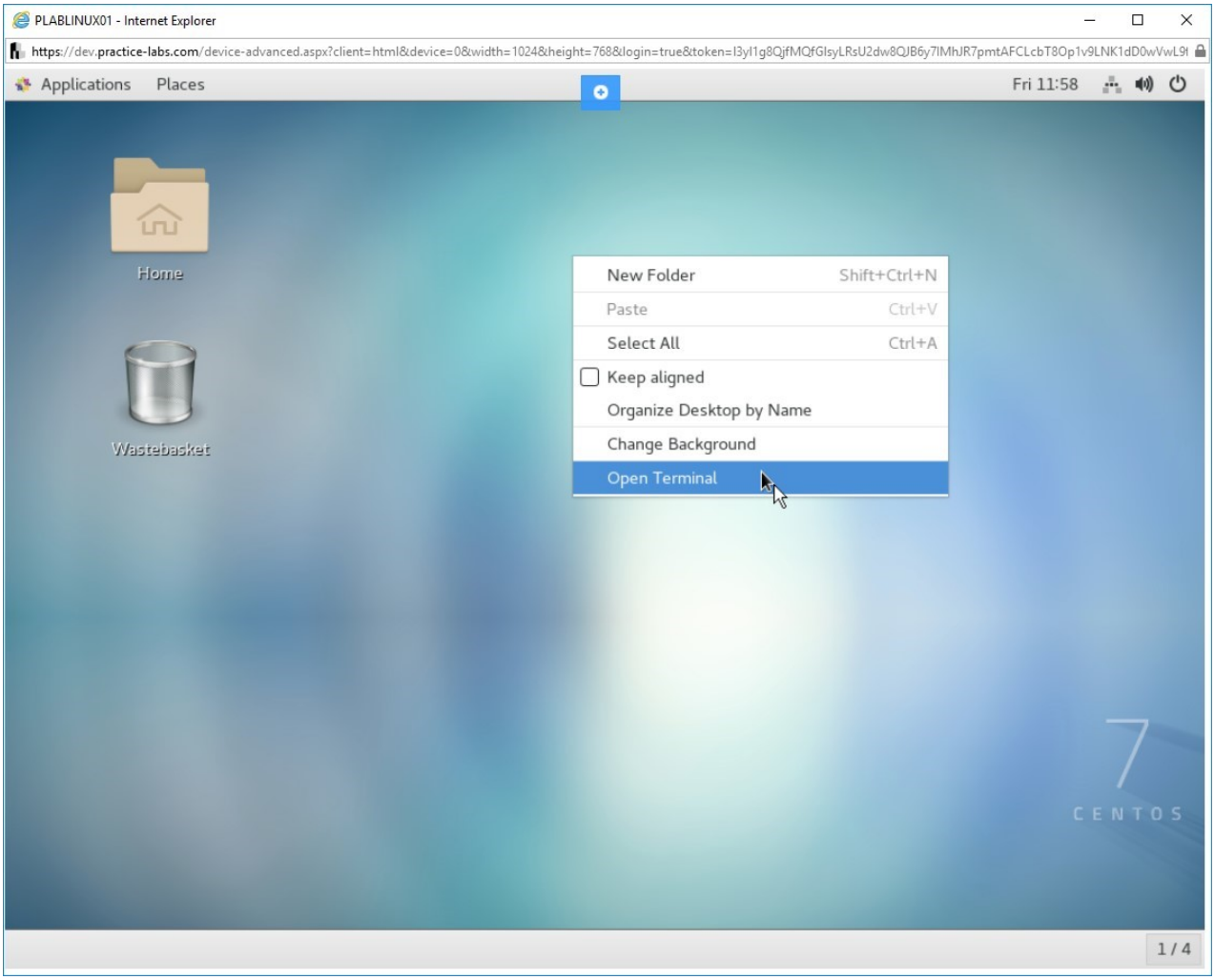


Figure 1.1 Screenshot of PLABLINUX01: Selecting the Open Terminal option from the context menu.

Step 2

The terminal prompt window is displayed. Type the following command:

```
su -
```

Press **Enter**.

At the **Password** prompt, type the following password:

```
Passw0rd
```

Press **Enter**.

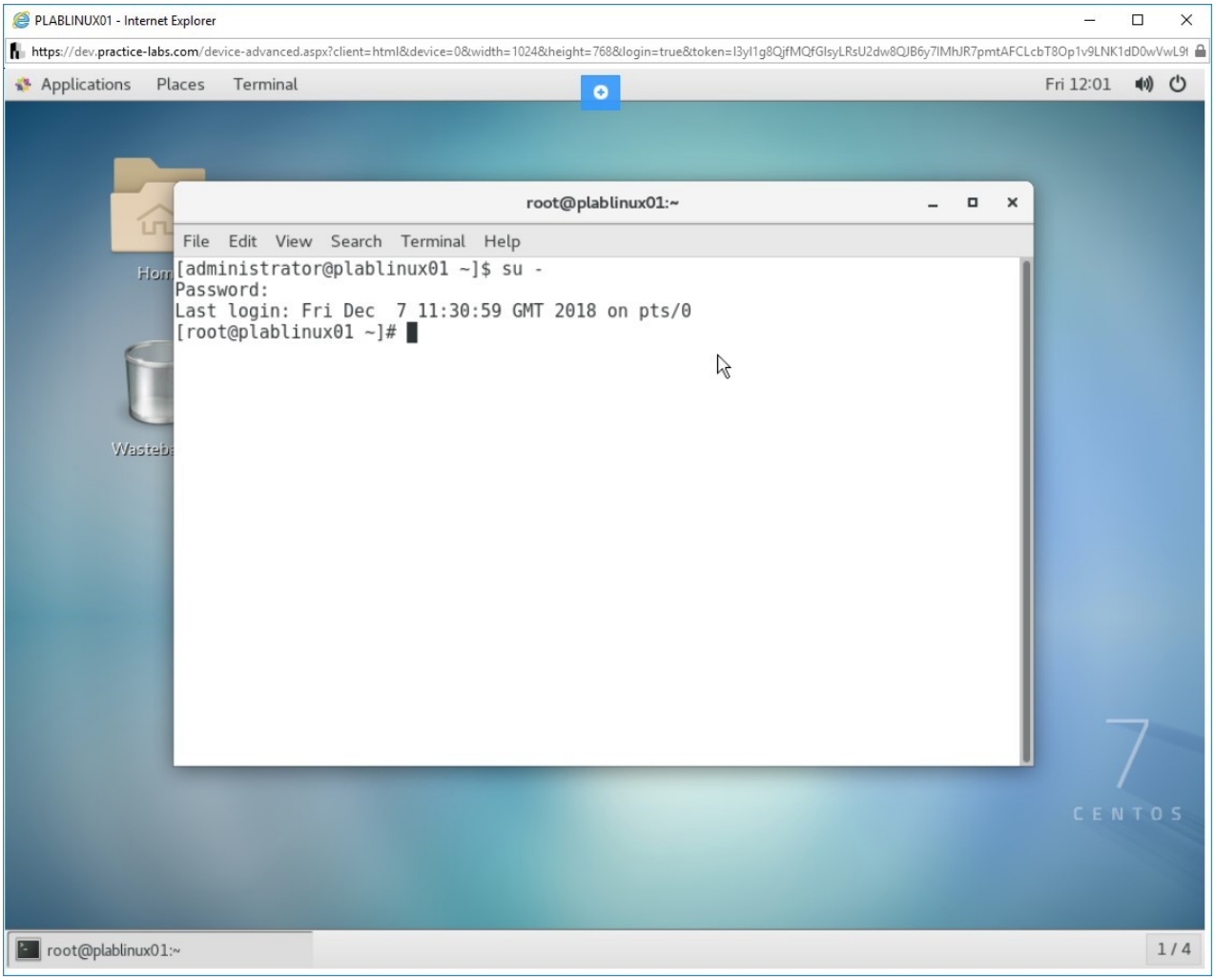


Figure 1.2 Screenshot of PLABLINUX01: Changing the account to the root account with the su command.

Step 3

Clear the screen by entering the following command:

```
clear
```

You need to need first to check if the kernel supports ACL. Type the following command:

```
cat /boot/config-3.10.0-957.1.3.el7.x86_64 | grep _ACL
```

Note: *The l character can sometimes look like the number 1*

Press **Enter**.

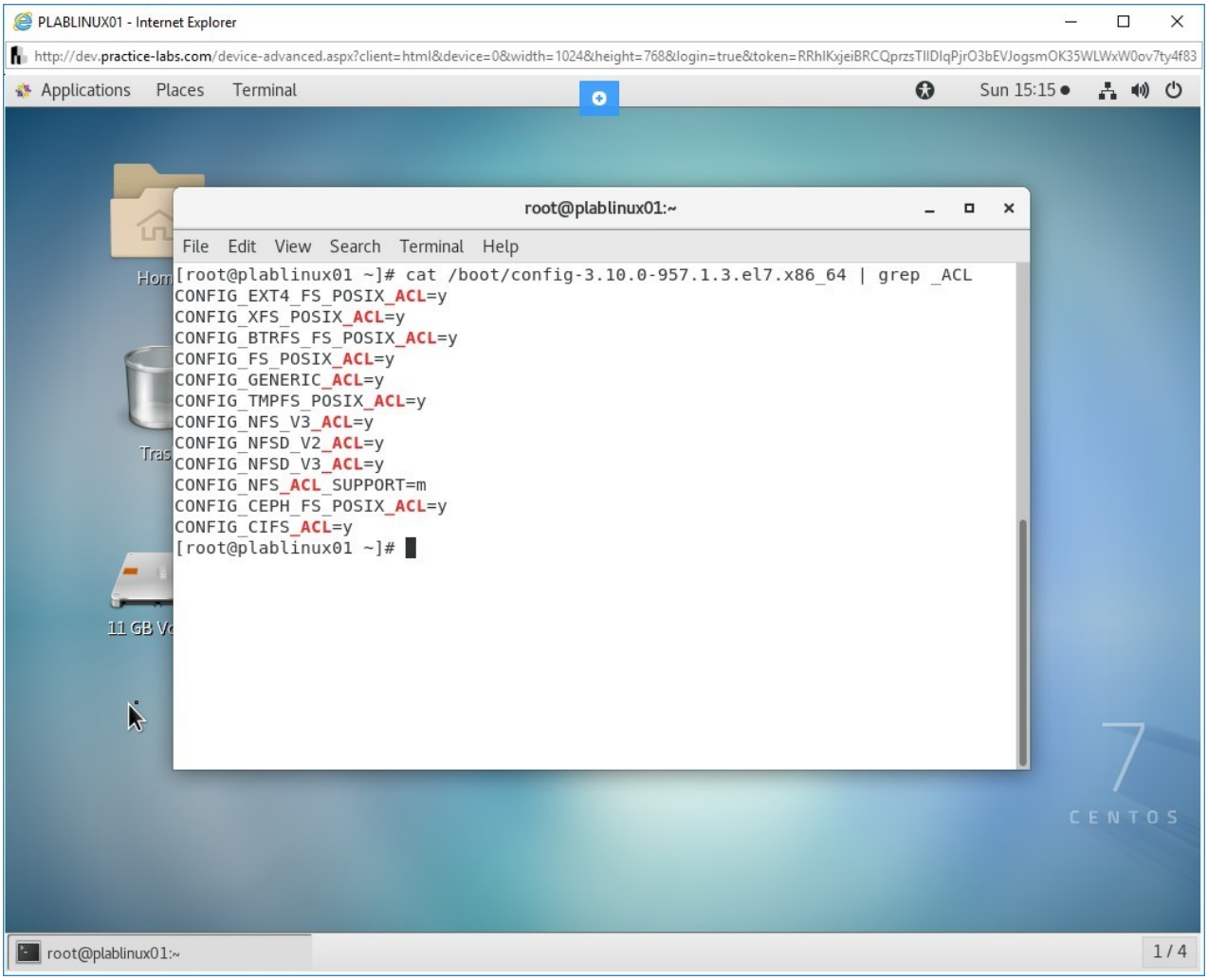


Figure 1.3 Screenshot of PLABLINUX01: Checking if the kernel supports ACL.

Step 4

Clear the screen by entering the following command:

```
clear
```

You need to check if the ACL package is installed on the system. Type the following command:

```
rpm -qa | grep acl
```

Press **Enter**.

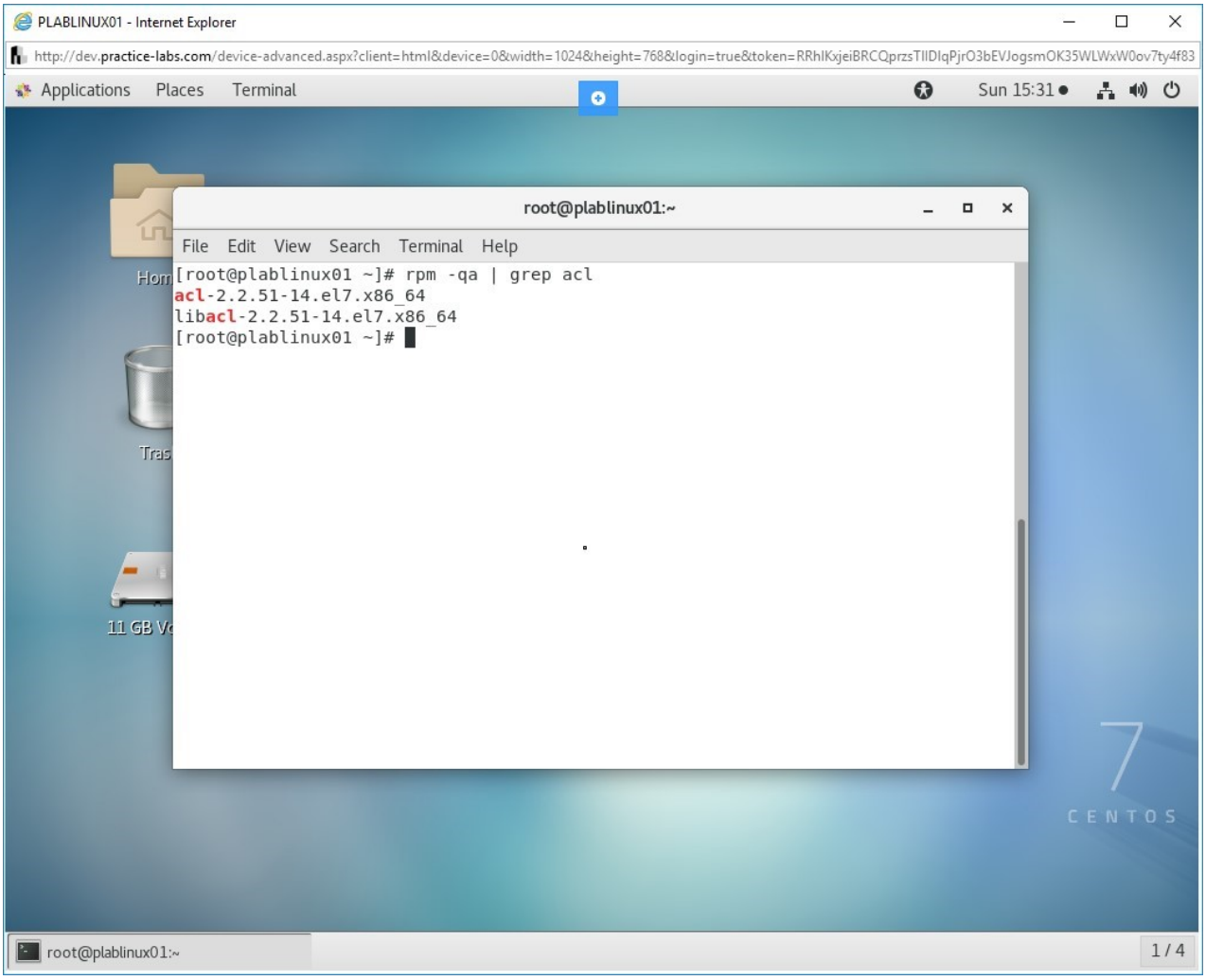


Figure 1.4 Screenshot of PLABLINUX01: Checking if the ACL package is installed on the system.

Step 5

Clear the screen by entering the following command:

```
clear
```

You will apply the ACL to a partition. Let's first check the partition that has been mounted. Type the following command:

```
df -h
```

Press **Enter**. Notice that **/dev/sdb1** is mounted on **/data**. You will create files in this directory and then assign ACL.

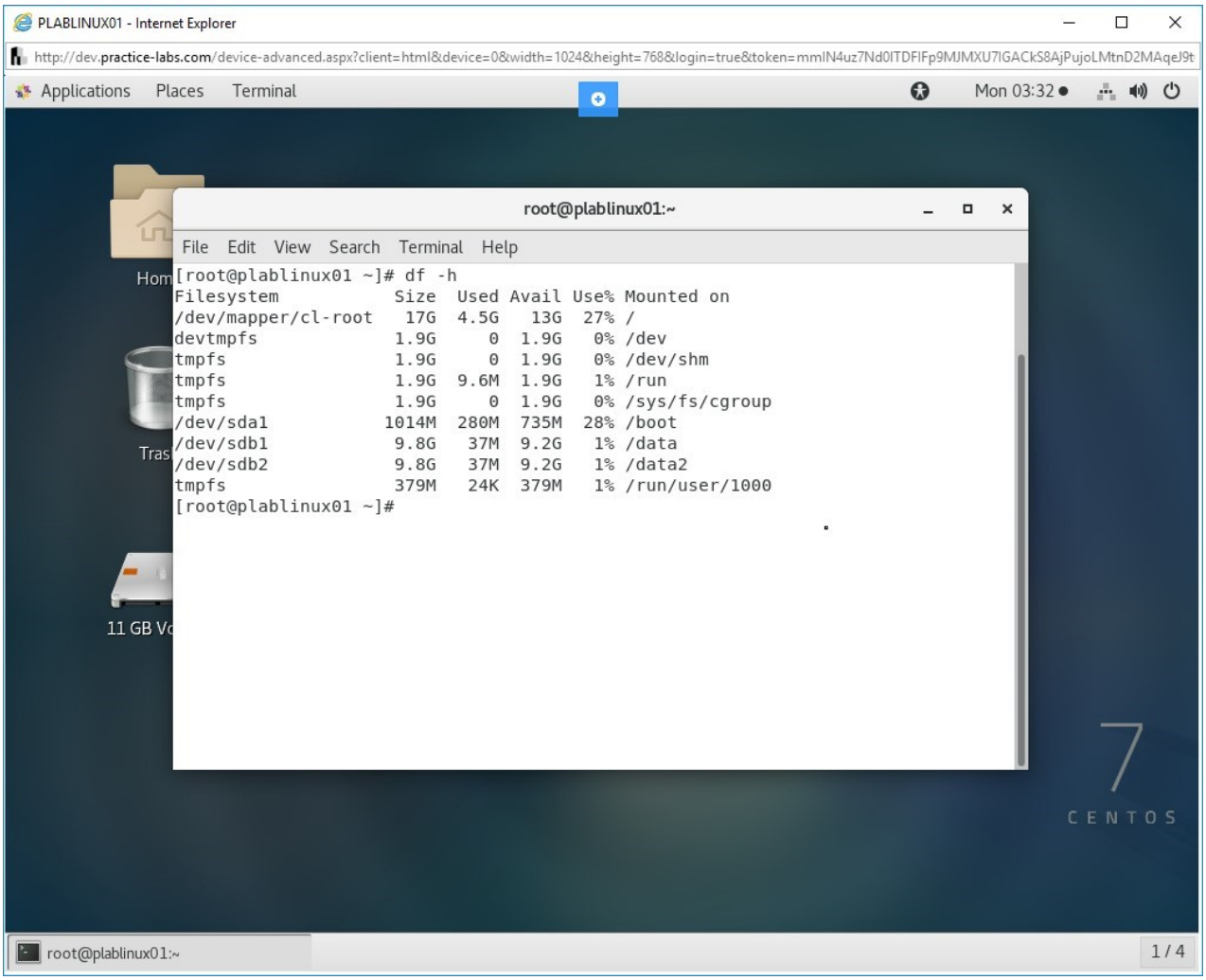


Figure 1.5 Screenshot of PLABLINUX01: Applying the ACL on a partition.

Step 6

Clear the screen by entering the following command:

```
clear
```

Create a file in the **/data** directory. Type the following command:

```
touch /data/plab.txt
```

Press **Enter**.

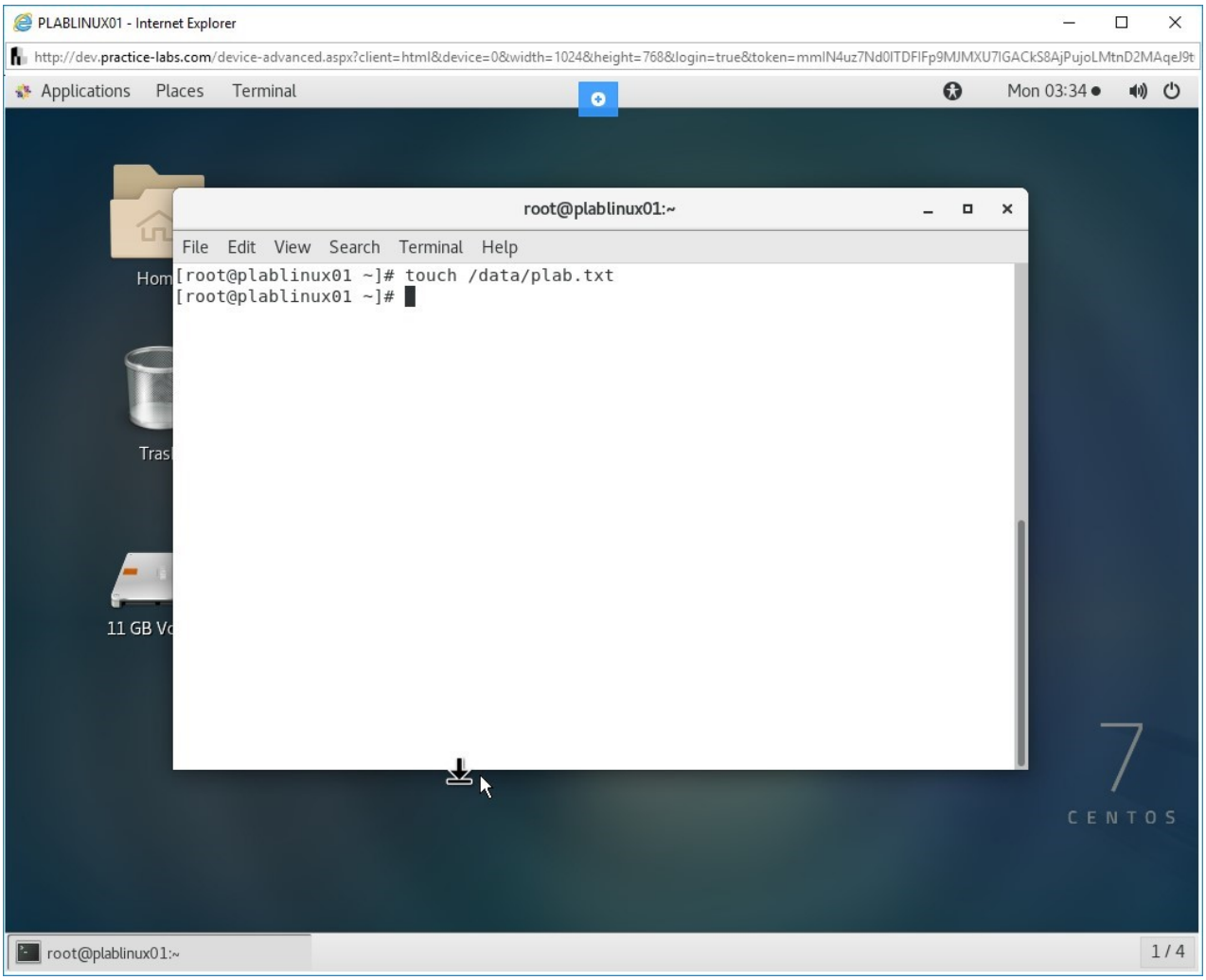


Figure 1.6 Screenshot of PLABLINUX01: Creating a file in the /data directory.

Step 7

You need to verify the permissions on the **/data/plab.txt** file. Type the following command:

```
ls -l /data/plab.txt
```

Press **Enter**. The permissions for **/data/plab.txt** are now displayed. Notice that other users will be able to read the file.

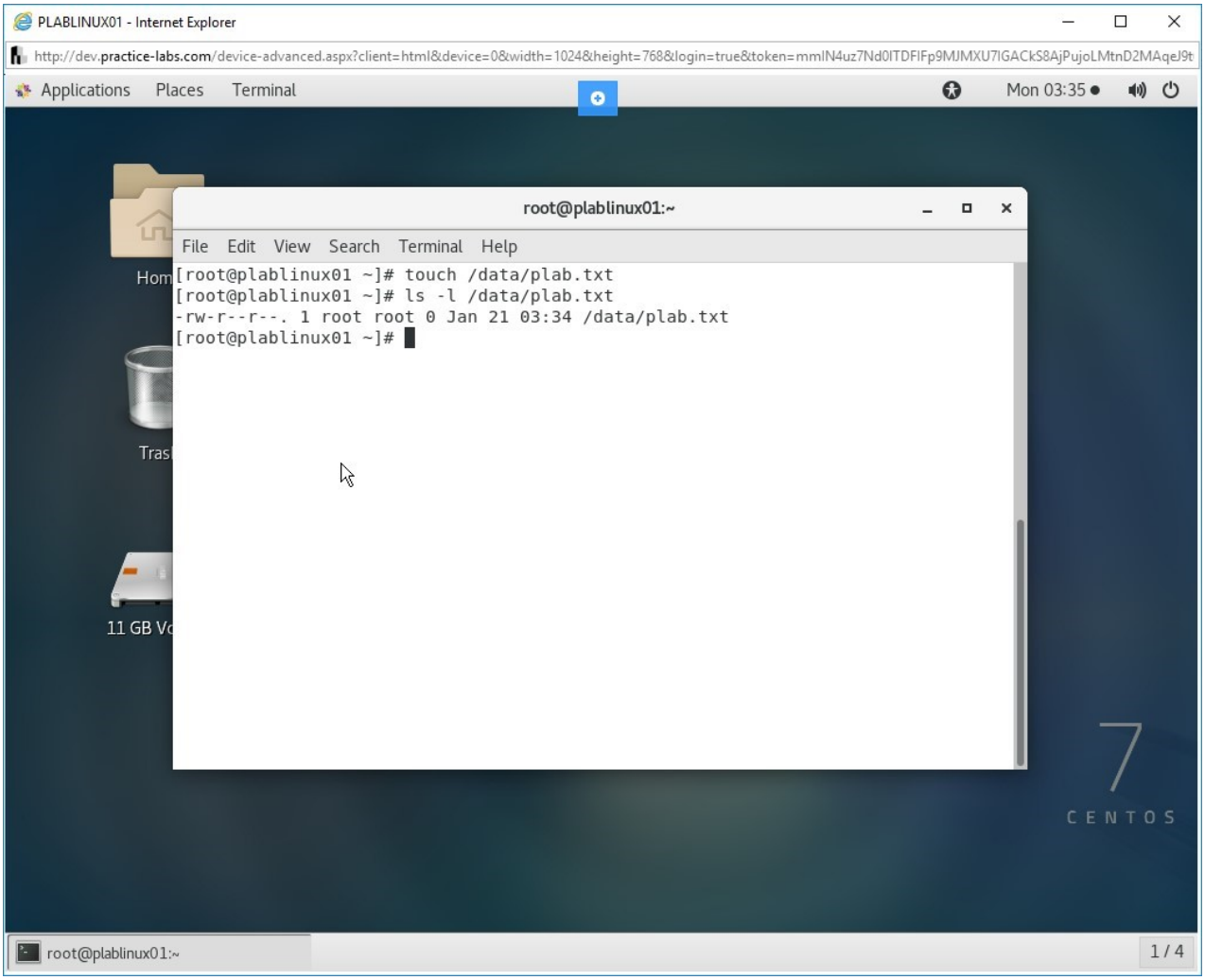


Figure 1.7 Screenshot of PLABLINUX01: Verifying the permissions on the /data/plab.txt file.

Step 8

You need to ensure that other than the root user, no one has **read**, **write**, and **execute** on the **/data/plab.txt** file. Type the following command:

```
chmod 700 /data/plab.txt
```

Press **Enter**. The permissions for **/data/plab.txt** are now displayed. Notice that other users will be able to read the file.

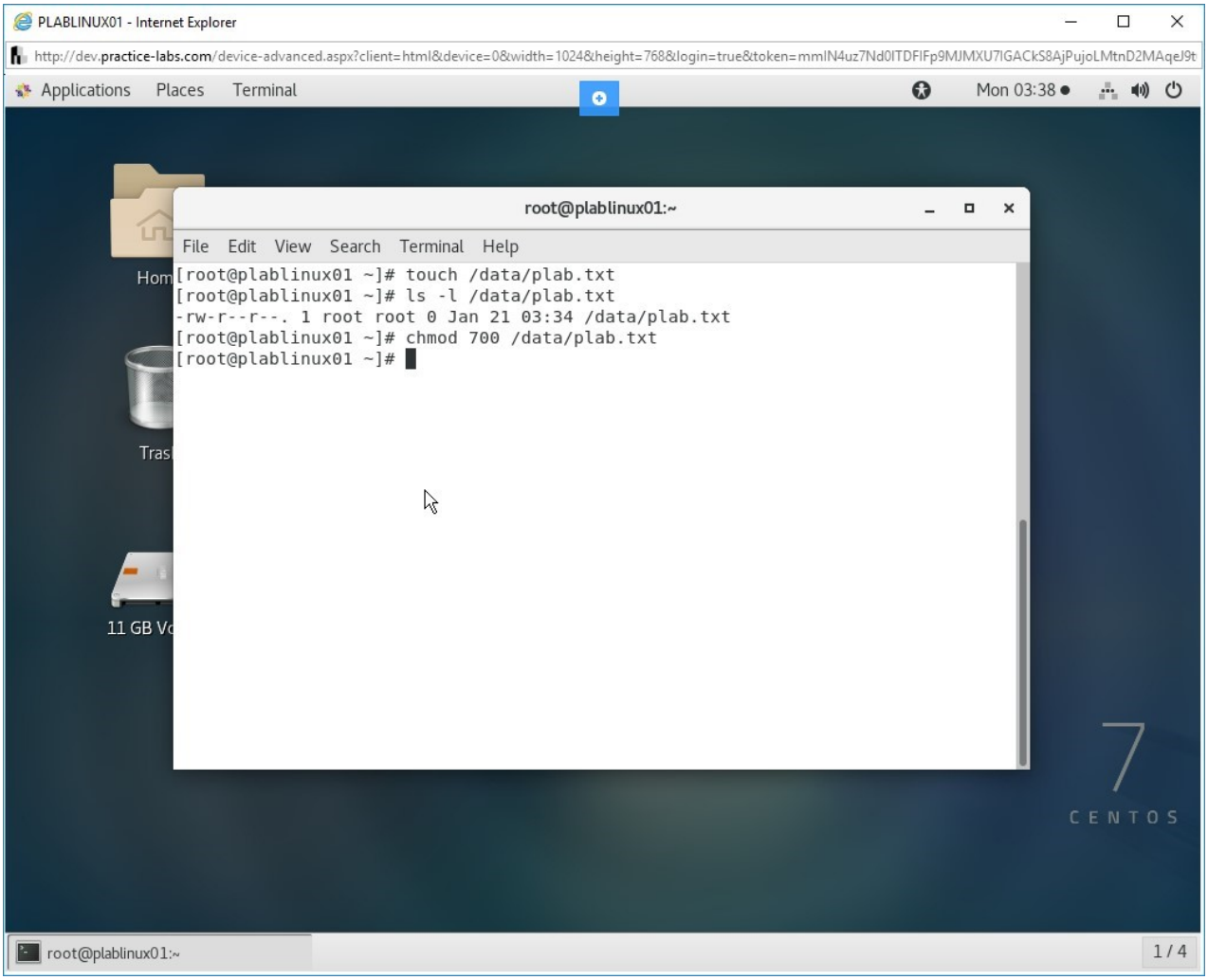


Figure 1.8 Screenshot of PLABLINUX01: Assigning read, write, and execute permissions only to the root user.

Step 9

You need to verify the permissions on this file again. Type the following command:

```
ls -l /data/plab.txt
```

Press **Enter**. The permissions for **/data/plab.txt** are now displayed. Notice that other users do not have permissions on this file.

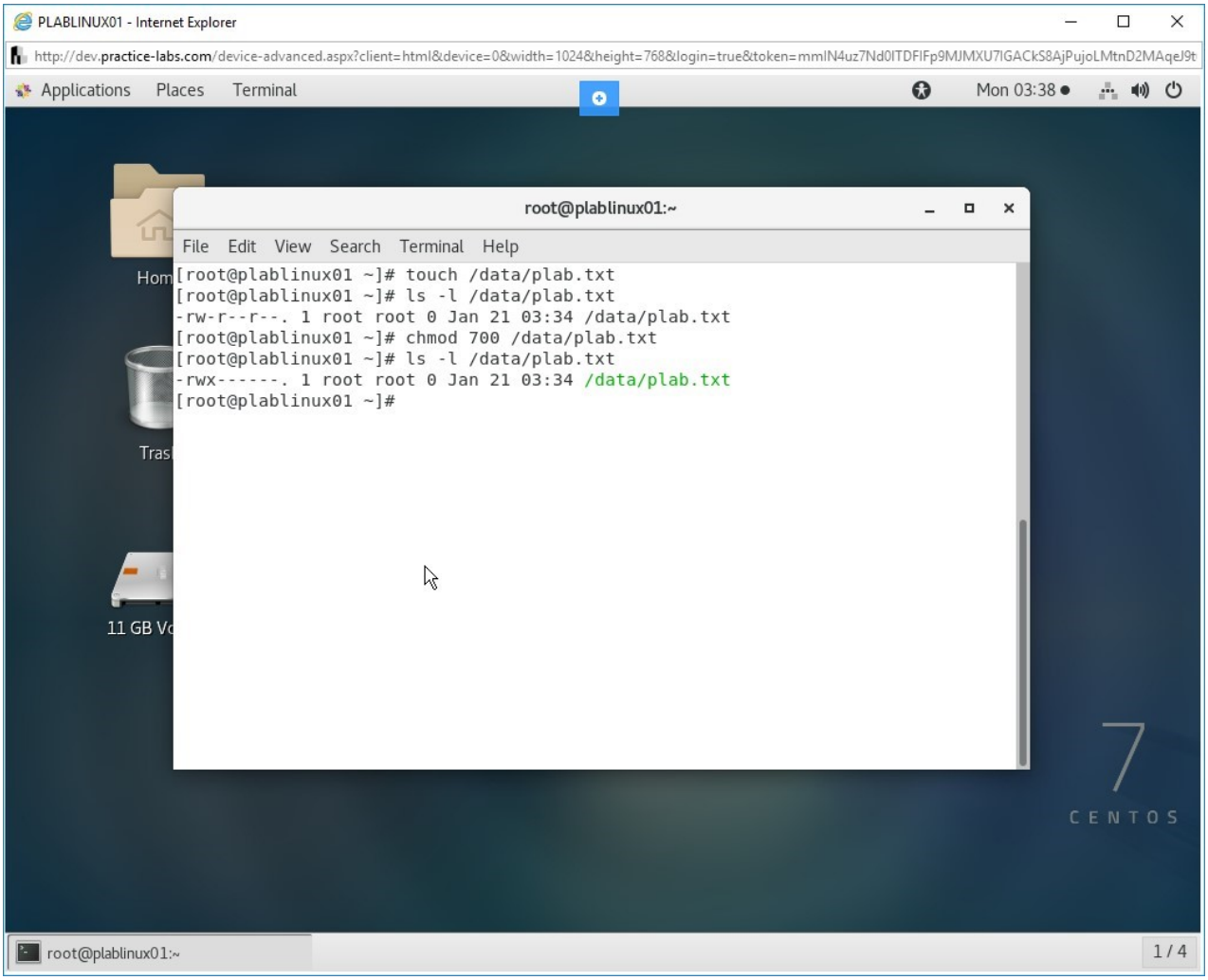


Figure 1.9 Screenshot of PLABLINUX01: Verifying the permissions on the /data/plab.txt file.

Step 10

Clear the screen by entering the following command:

```
clear
```

You can verify the permissions on this file using the **getfacl** command. Type the following command:

```
getfacl /data/plab.txt
```

Press **Enter**. Notice that the only the **root** user has **read, write,** and **execute** permissions. No other group or user has read, write, permissions.

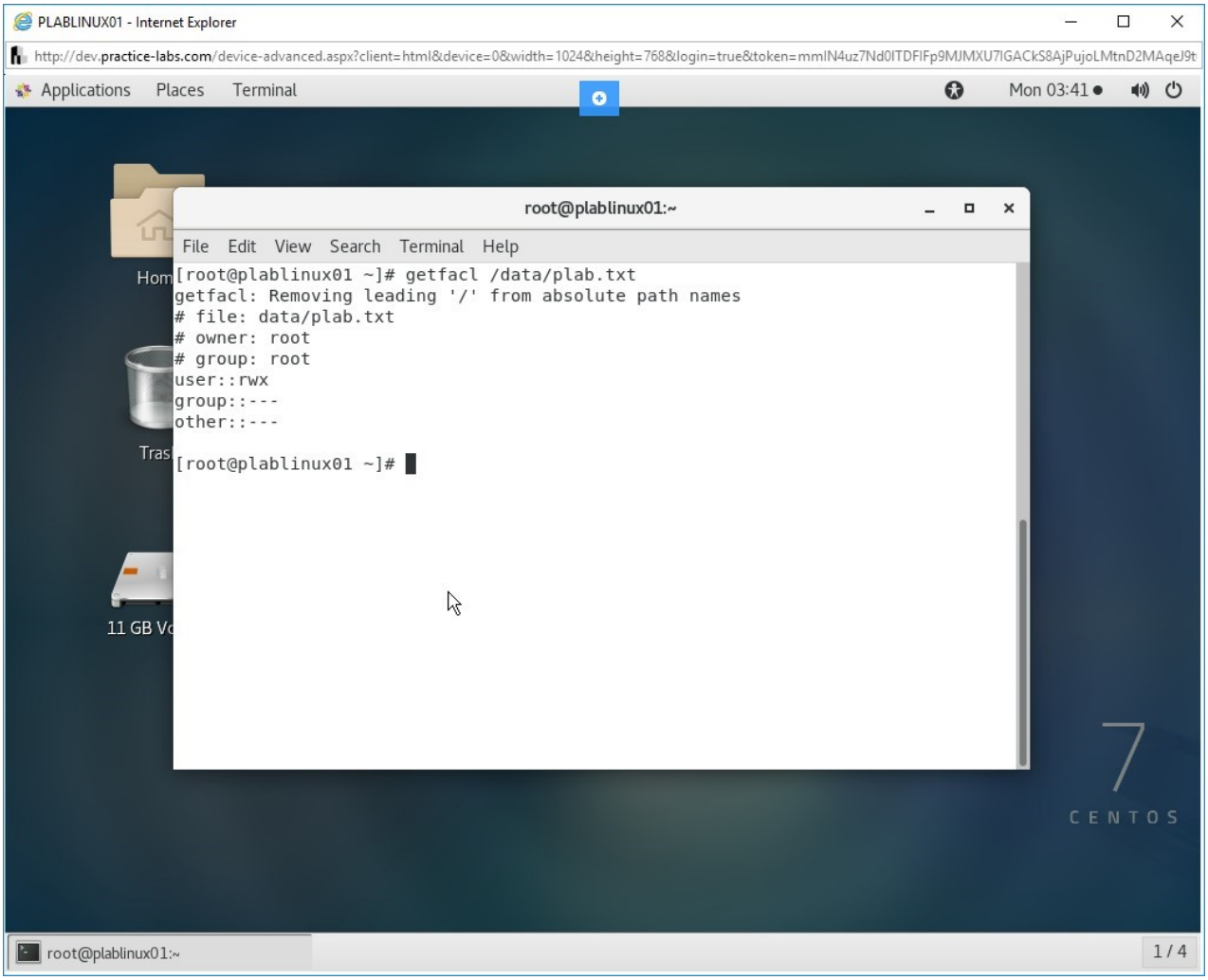


Figure 1.10 Screenshot of PLABLINUX01: Verifying the permissions on this file using the getfacl command.

Step 11

You need to confirm if the administrator can access the **/data/plab.txt** file. First, you need to exit from the **root** shell. Type the following command:

```
exit
```

Press **Enter**. Notice that you are back on the administrator prompt.

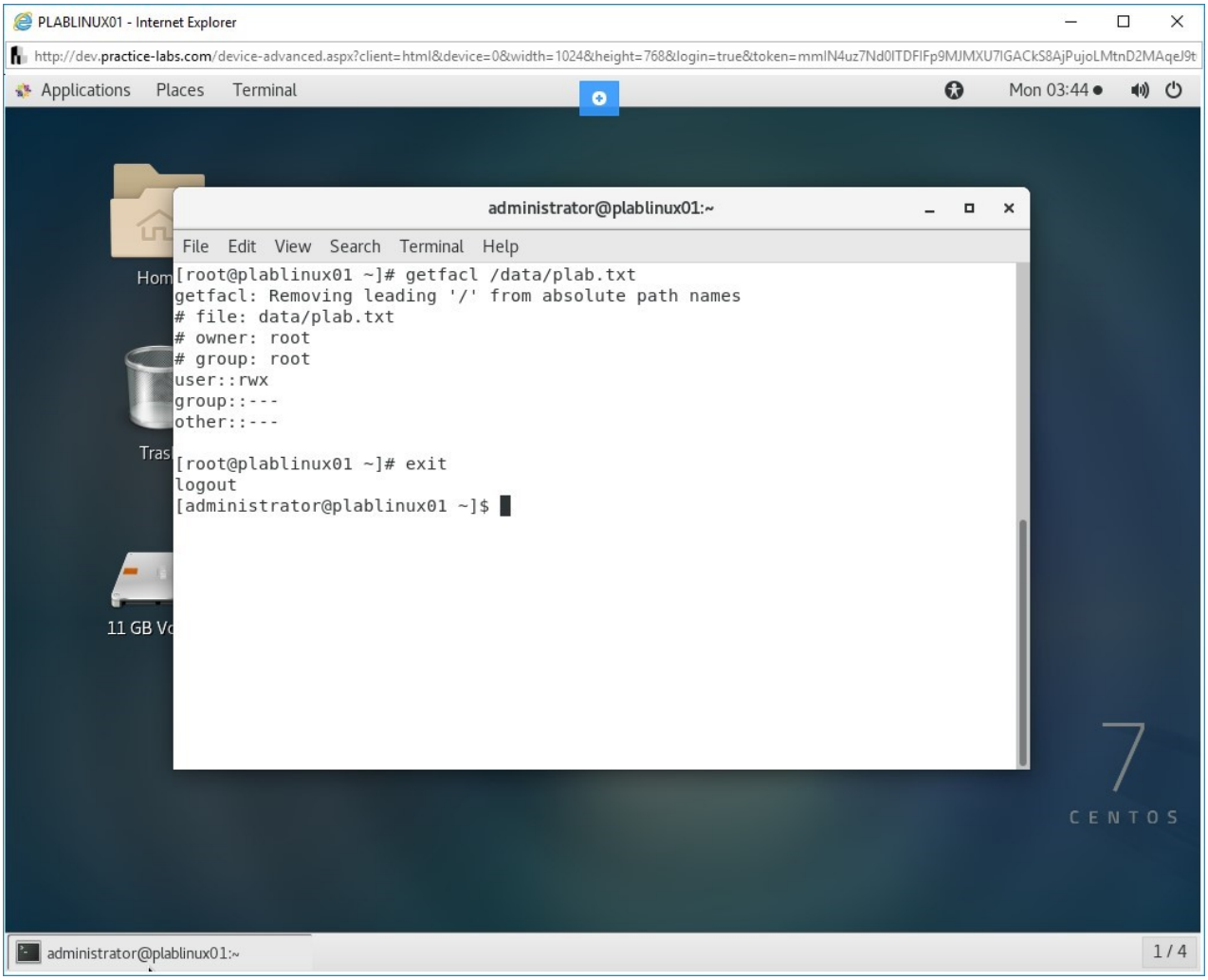


Figure 1.11 Screenshot of PLABLINUX01: Confirming if the administrator can access the /data/plab.txt file.

Step 12

Let's attempt to access the **/data/plab.txt** file with the administrator user account. Type the following command:

```
cat /data/plab.txt
```

Press **Enter**. Notice that you get the permission denied message.

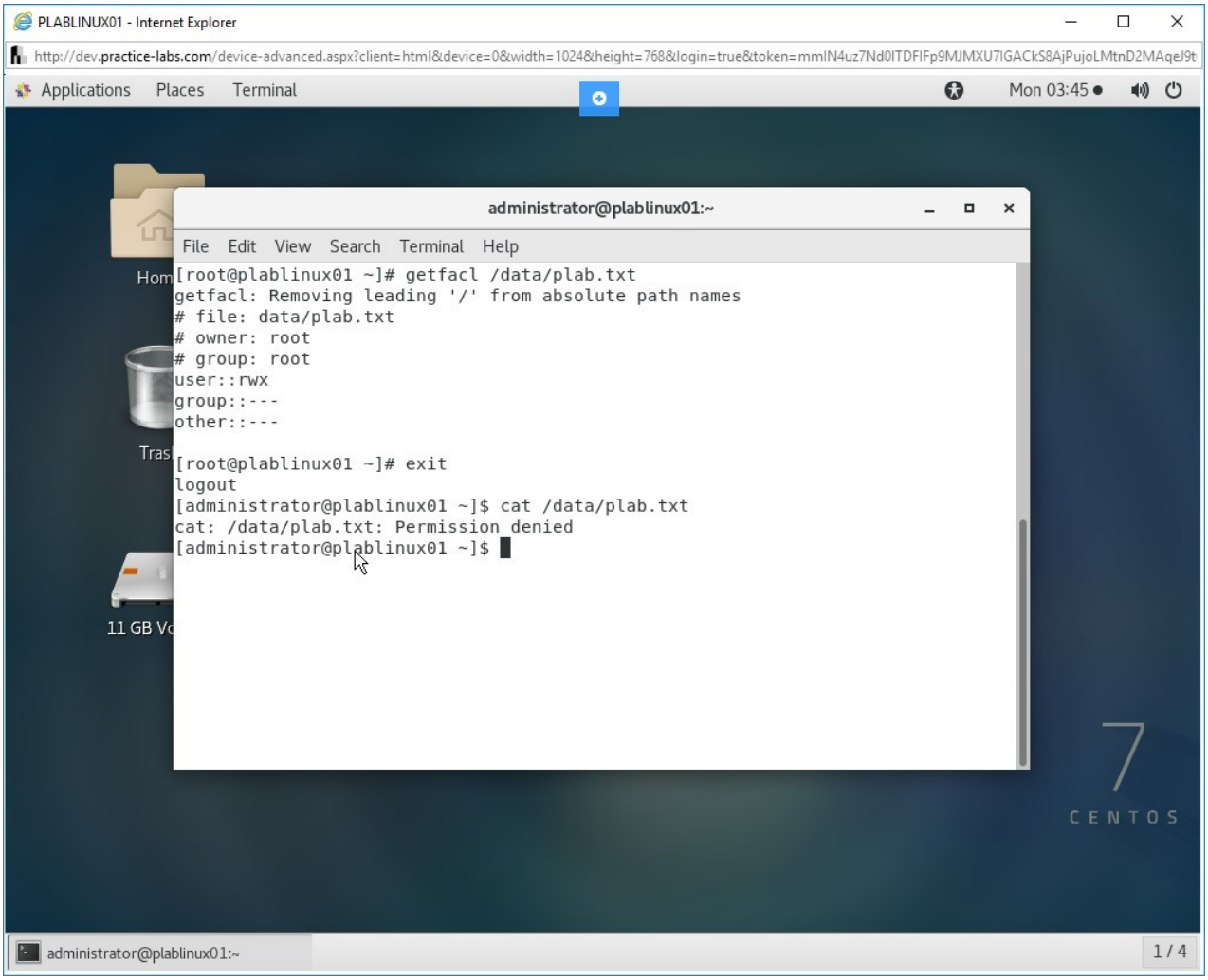


Figure 1.12 Screenshot of PLABLINUX01: Attempting to access /data/plab.txt file using the administrator account.

Step 13

Clear the screen by entering the following command:

```
clear
```

You can use ACL to assign permission to the **administrator** account. Type the following command:

```
sudo setfacl -m user:administrator:rwx /data/plab.txt
```

Press **Enter**.

When prompted, type the following password:

```
Passw0rd
```

Press **Enter**.

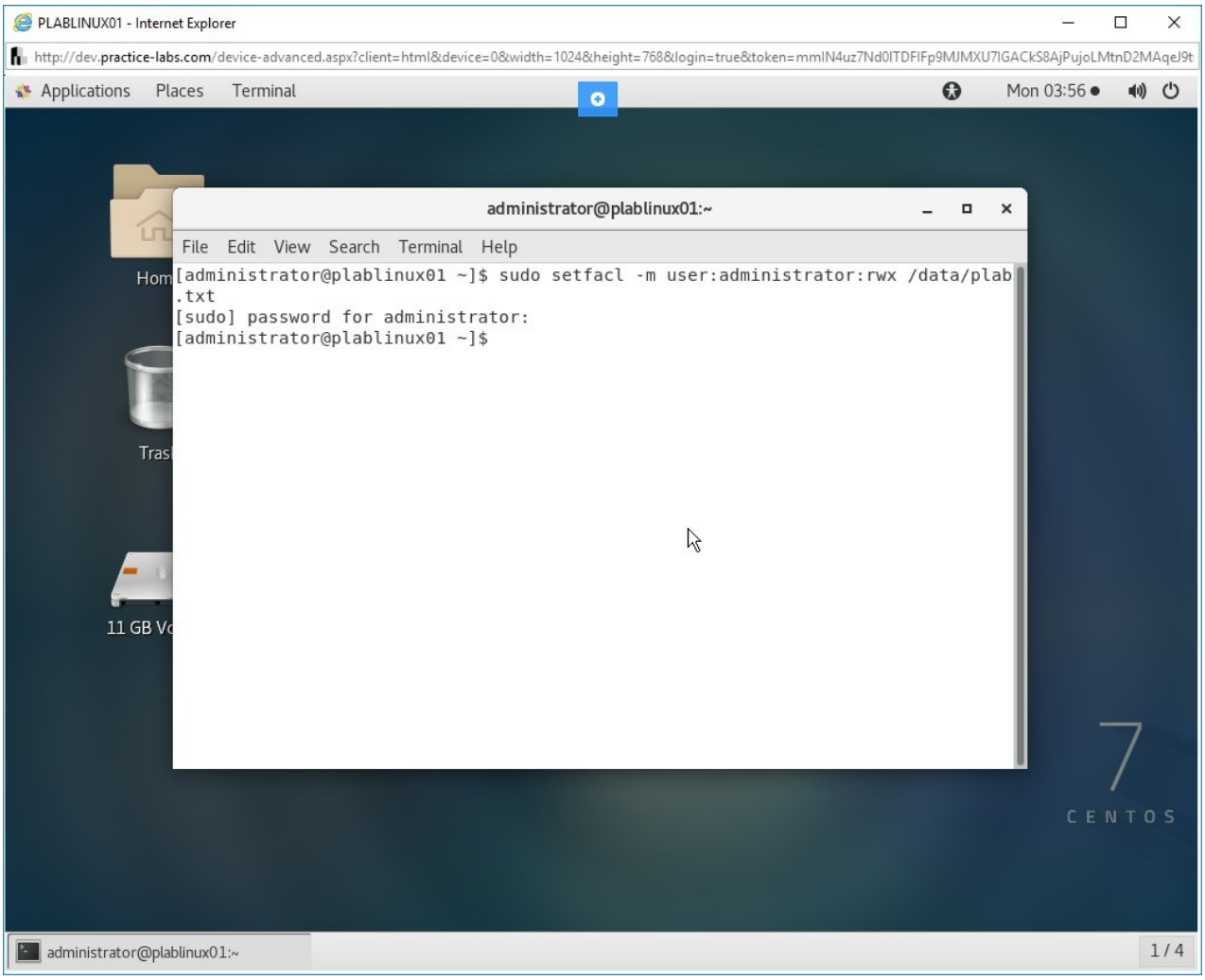


Figure 1.13 Screenshot of PLABLINUX01: Assigning permissions to the administrator account.

Step 14

You can now verify the permissions on the **/data/plab.txt** file. Type the following command:

```
getfacl /data/plab.txt
```

Press **Enter**. Notice that the administrator account now has **read**, **write**, and **execute** permissions.

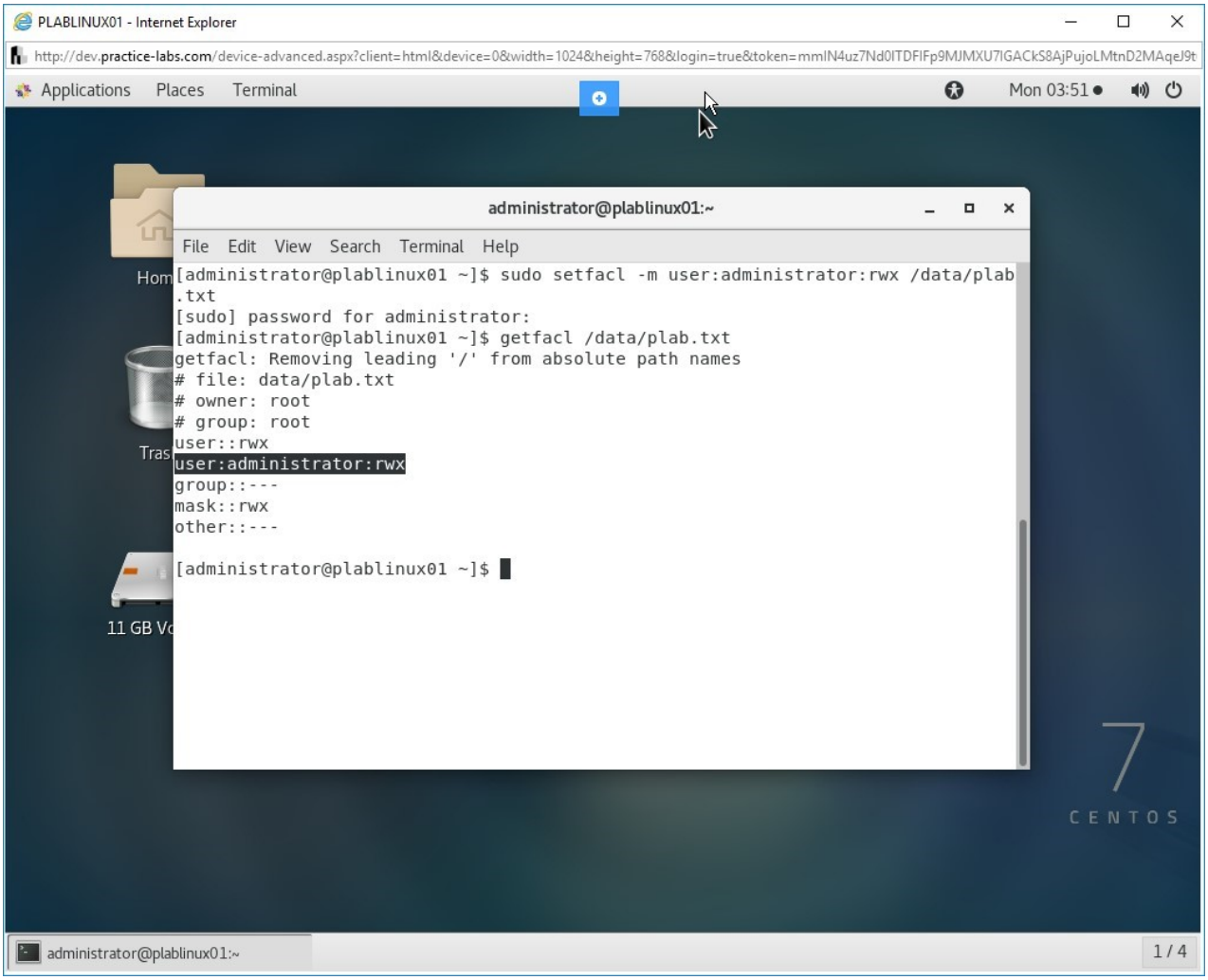


Figure 1.14 Screenshot of PLABLINUX01: Verifying the permissions on the /data/plab.txt file.

Step 15

Clear the screen by entering the following command:

```
clear
```

You can also verify the permissions with the **ls** command. Type the following command:

```
ls -l /data/plab.txt
```

Press **Enter**. Notice that the permissions are also assigned to the administrator user.

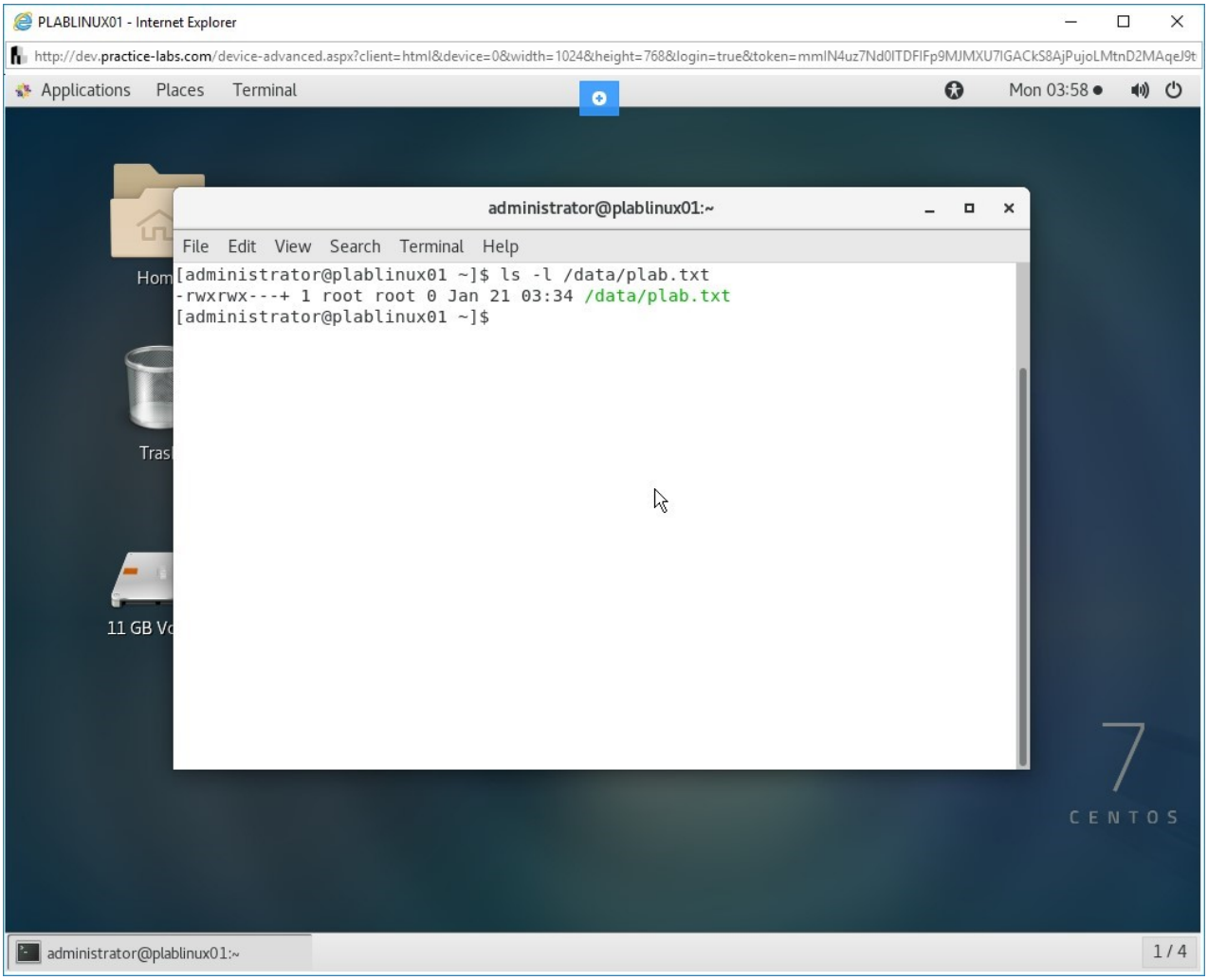


Figure 1.15 Screenshot of PLABLINUX01: Verifying the permissions on the /data/plab.txt file with the ls command.

Step 16

Clear the screen by entering the following command:

```
clear
```

After assigning ACLs, you can remove ACLs if required. The **setfacl** command with the **-b** parameter removes all applied ACLs from a specific file or directory. Type the following command:

```
sudo setfacl -b /data/plab.txt
```

Press **Enter**. Notice that no response is returned.

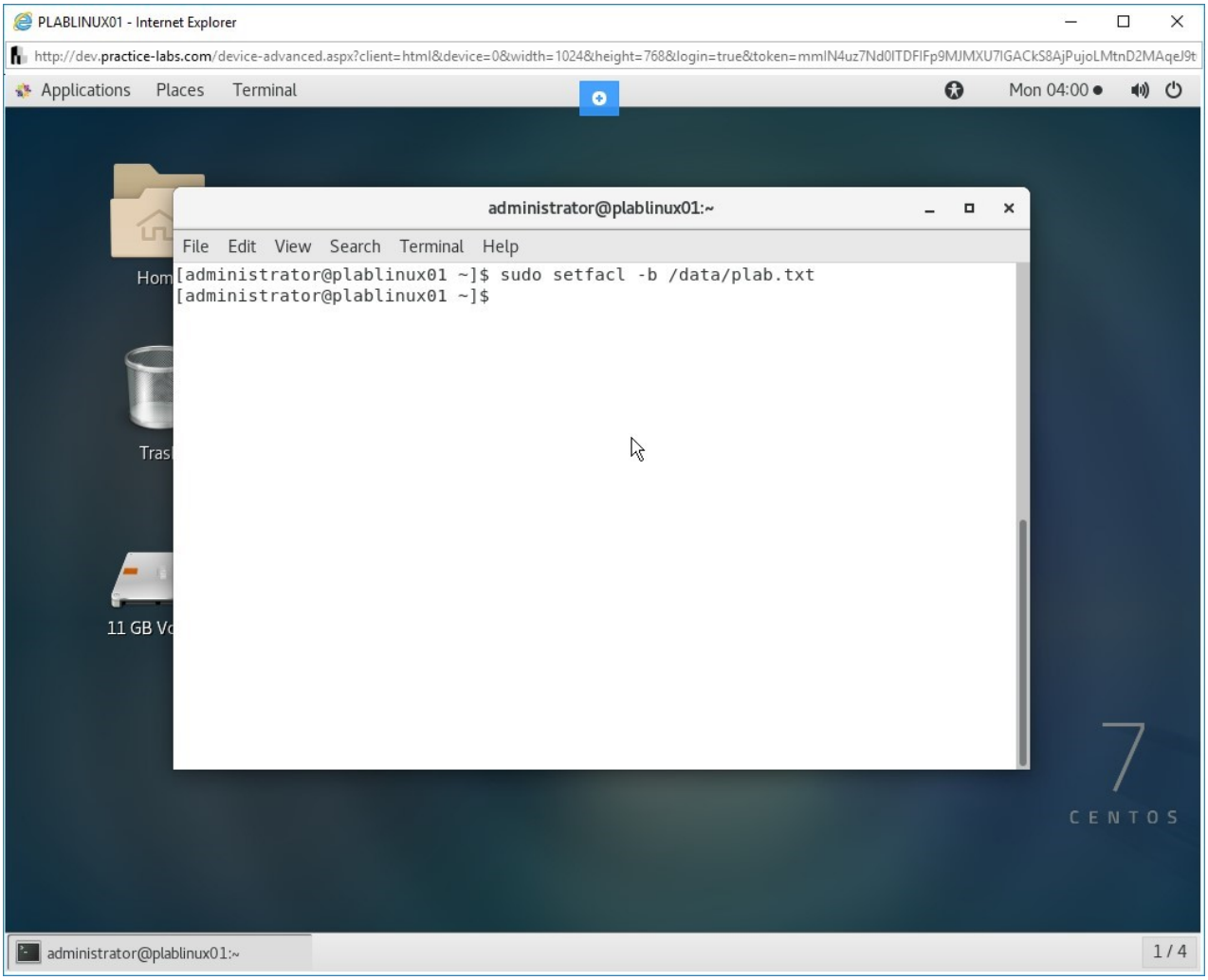


Figure 1.16 Screenshot of PLABLINUX01: Removing the ACL on the /data/plab.txt file.

Step 17

To verify the permissions on the **/data/plab.txt** file, type the following command:

```
getfacl /data/plab.txt
```

Press **Enter**. Notice that no ACL is assigned. The file has the permissions that you had earlier defined for the root user.

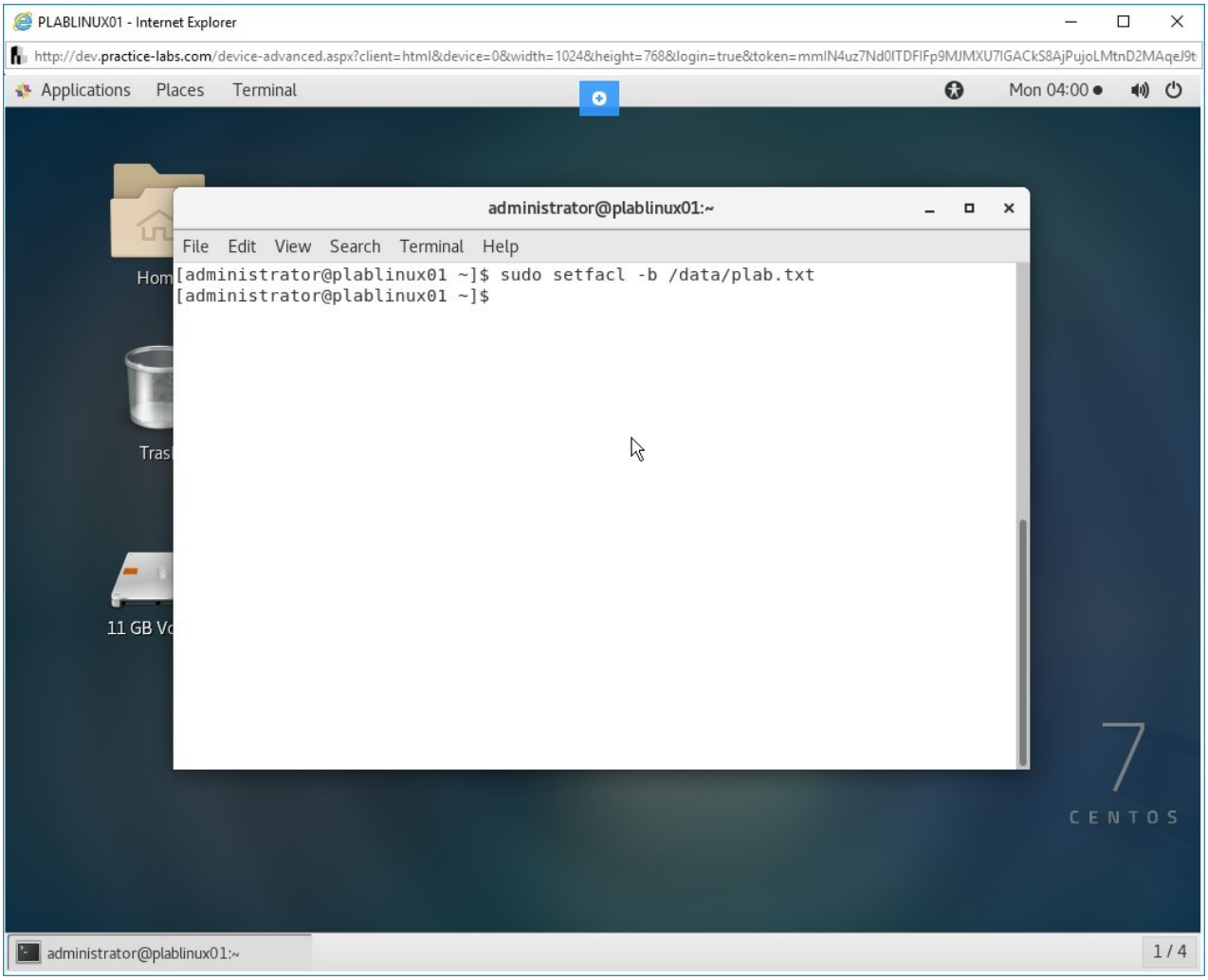


Figure 1.17Screenshot of PLABLINUX01: Verifying the permissions on the /data/plab.txt file.

Keep all devices in their current state and proceed to the next exercise.

Review

Well done, you have completed the **Working with Access Control List** Practice Lab.

Summary

You completed the following exercise:

- Exercise 1 - Working with Access Control List

You should now be able to:

- Implement Access Control List

Feedback

Shutdown all virtual machines used in this lab. Alternatively, you can log out of the lab platform.