CompTIA Linux+

Configure System Logging

- **Introduction**
- **Lab Topology**
- **Exercise 1 - Configure System Logging**
- **Review**

Introduction

Welcome to the **Configure System Logging** Practice Lab. In this module you will be provided with the instructions and devices needed to develop your hands-on skills.

Logging
Logrotate
Syslog Daemon

Learning Outcomes

In this module, you will complete the following exercise:

- Exercise 1 - Configure System Logging

After completing this lab, you will be able to:

- Configure the syslog daemon
- Configuration of logrotate

Exam Objectives

The following exam objectives are covered in this lab:

- **LPI:** 108.2 System logging
- **CompTIA:** 2.5 Summarize and explain server roles.

> ***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.

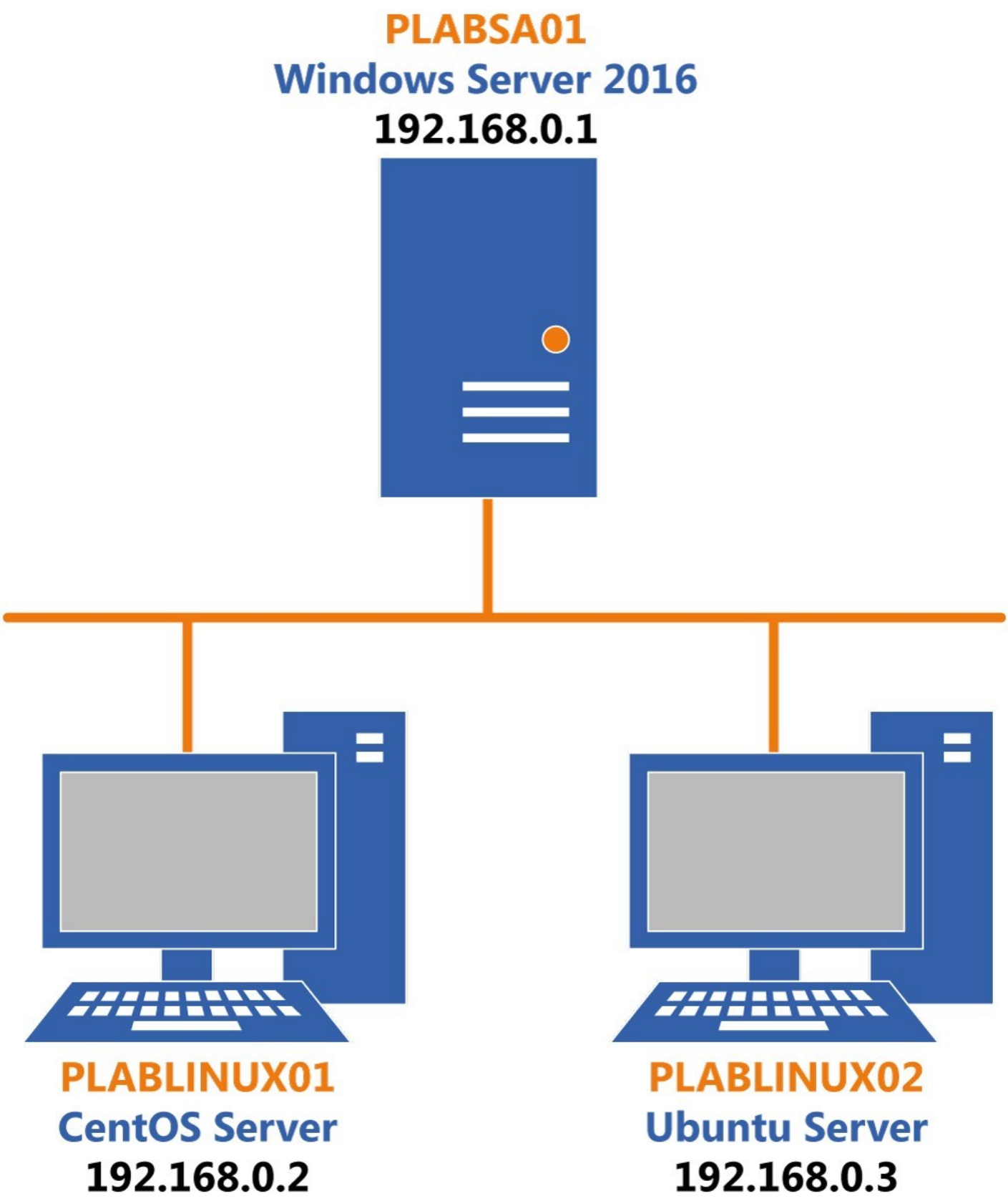
Help and Support

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 - Configure System Logging

Syslog daemon helps system administrators manage system security and analyze debug messages. All the hardware devices run their own syslog daemons. The output from all the devices are logged into a central repository for further usage.

In this exercise, you will understand how to configure syslog daemon.

Learning Outcomes

After completing this exercise, you will be able to:

- Log into a Linux System
- Configure the syslog daemon
- Configuration of logrotate

Your Devices

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

- **PLABLINUX01** (CentOS Server)

Task 1 - Configure the Syslog Daemon

It is essential for a system to maintain log files. The core intent of maintaining log files is to track messages about various system components, such as kernel, services, CPU, memory, security, and applications. Different log files can contain a different set of messages, which can be of different varieties like error or information. The system

administrator can use these logs to manage the system - whether it is troubleshooting an error message from the system or tracking the users logged onto the system.

In a Fedora Linux system, syslogd is replaced by rsyslog. It uses the syslog protocol and supports transportation of messages using TCP or UDP protocols.

To configure syslog (rsyslog) daemon, perform the following steps:

Step 1

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

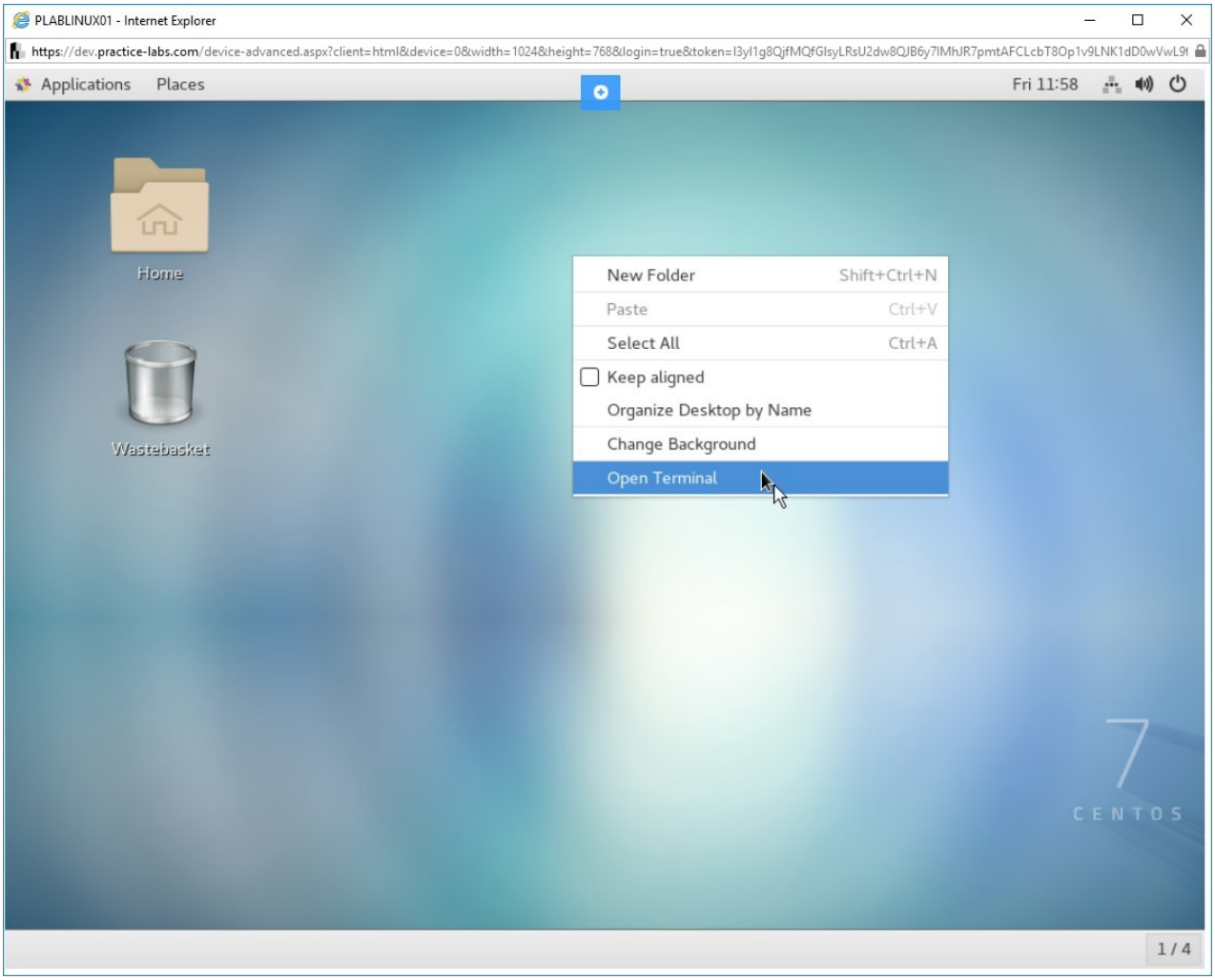


Figure 1.1 Screenshot of PLABLINUX01: Selecting the Open Terminal option from the context menu.

Step 2

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

```
su -
```

Press **Enter**.

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

`Passw0rd`

Press **Enter**.

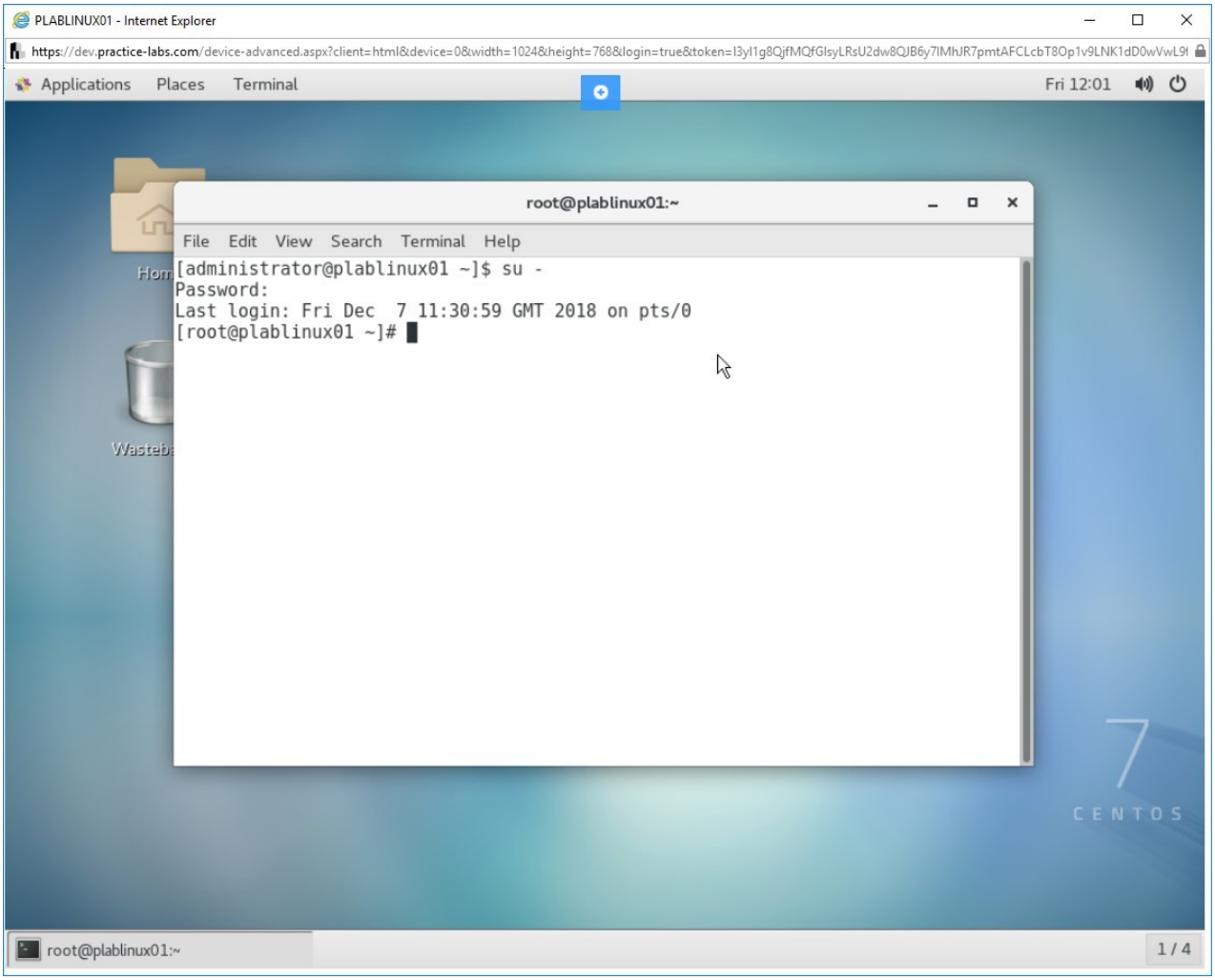


Figure 1.2 Screenshot of PLABLINUX01: Changing to the root account with the su command.

Step 3

Clear the screen by entering the following command:

```
clear
```

A daemon called **rsyslogd** can control the log files. The log messages maintained by **rsyslogd** are listed in the **/etc/rsyslog.conf** configuration file. It is important to note that this file contains the following sections:

- **Modules** - contains various configuration directives that are loaded when the module is loaded.
- **Global directives** - apply to the rsyslogd daemon and start with $. One line contains one global directive.
- **Rules** - defines the cooperation of selector and action. A selector filters messages based on facility and priority. An action defines what needs to be done with the filtered messages.
- **Templates** - specify the format a user may need. You can also use them for dynamic file name generation.
- **Filter conditions** - can use one of the three types of filter conditions: RainerScript-based filters, severity and facility-based selectors, and property-based filters
- **Output channels** - defines the type of output a user wants

Each line contains three directives:

- Facility - is the message creator, for example, security or kernel
- Level - is the severity level
- Action - is the destination for the logged messages

To view the **/etc/rsyslog.conf** file, type the following command:

```
cat /etc/rsyslog.conf
```

Press **Enter**.

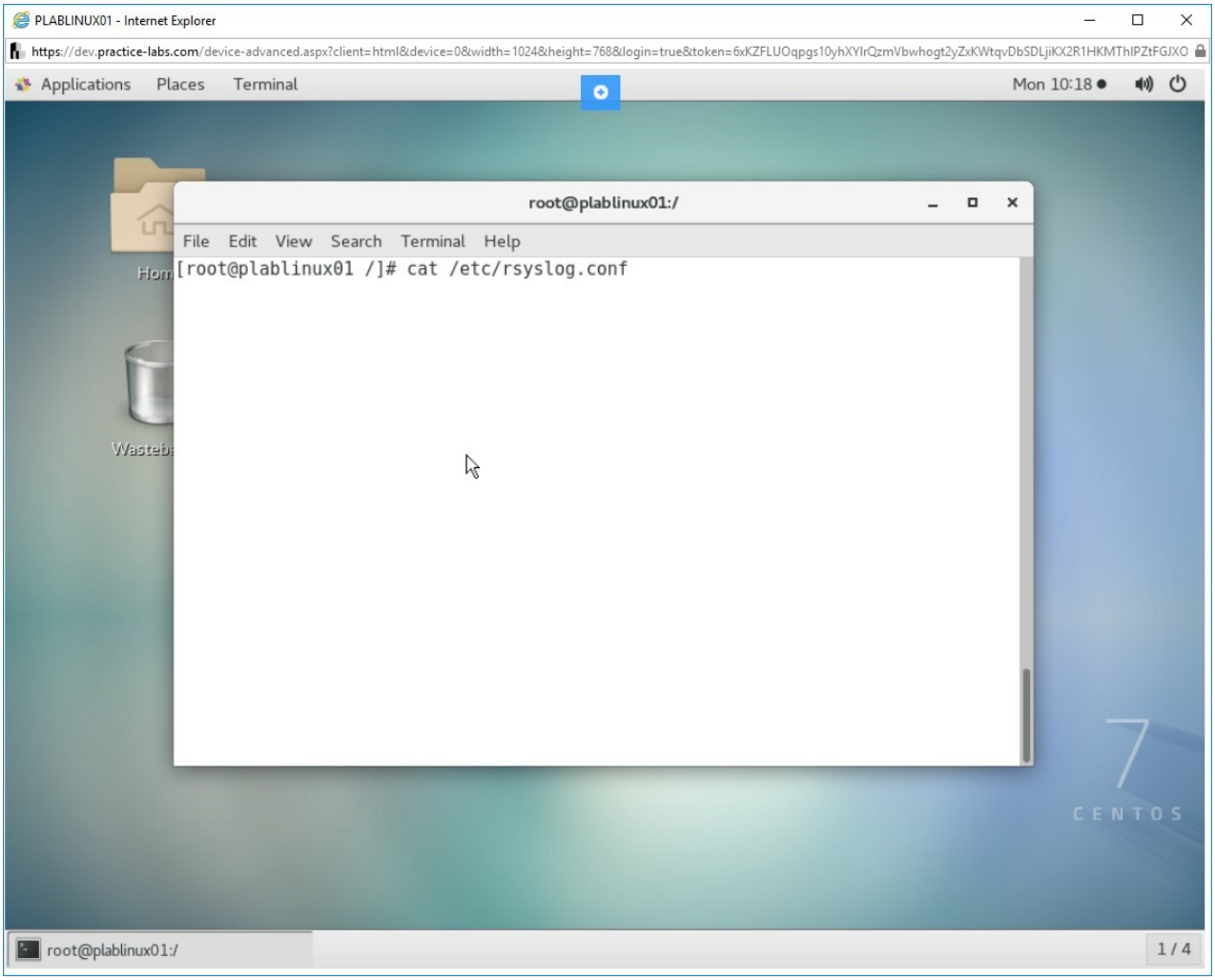


Figure 1.3 Screenshot of PLABLINUX01: Viewing the view the /etc/rsyslog.conf file.

The **/etc/rsyslog.conf** file is now displayed.

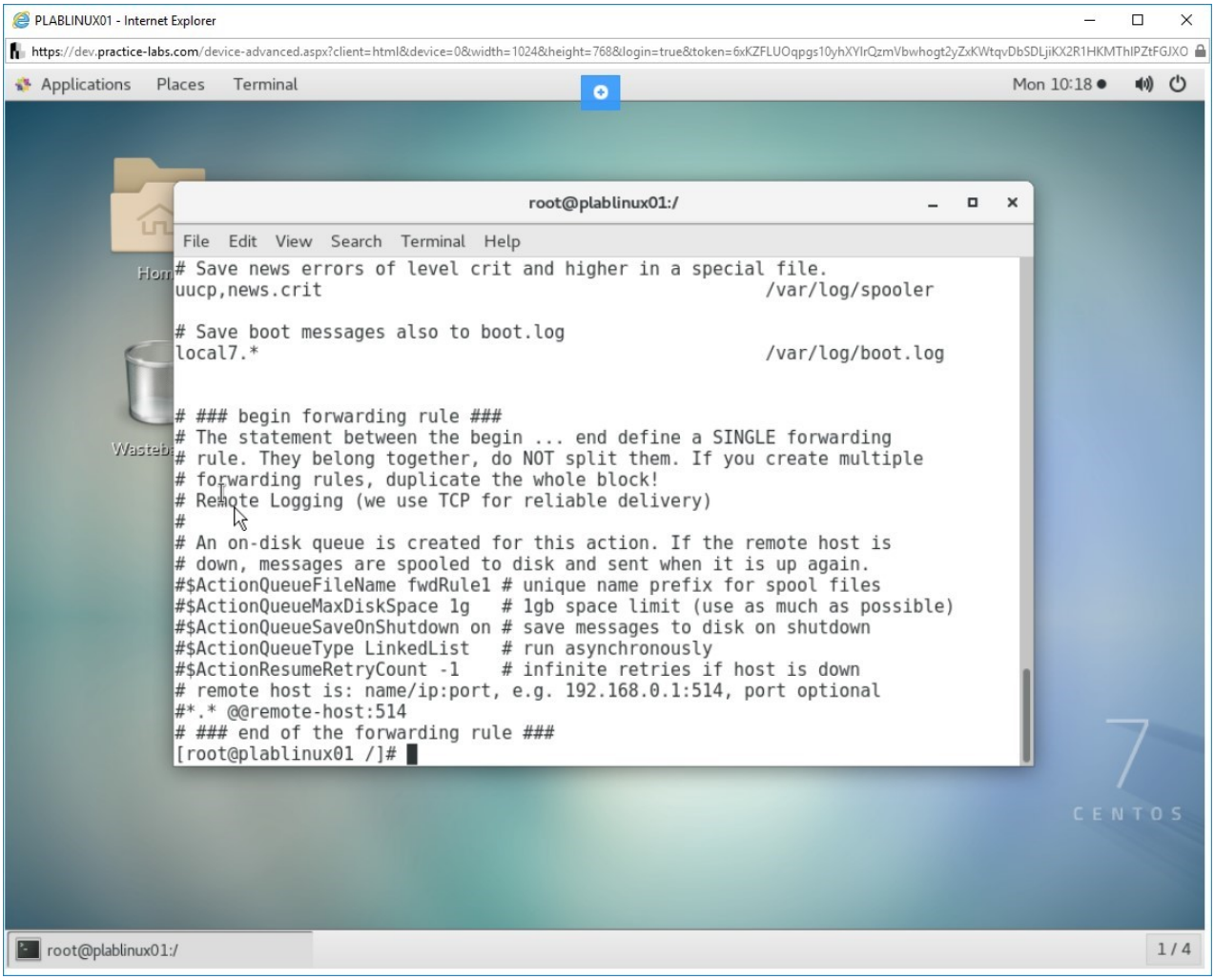


Figure 1.4 Screenshot of PLABLINUX01: Viewing the contents of the /etc/rsyslog.conf file.

Step 4

Clear the screen by entering the following command:

```
clear
```

To view the loaded modules, type the following command:

```
grep ModLoad /etc/rsyslog.conf
```

Press **Enter**.

The lines containing the word **ModLoad** are displayed from the **/etc/rsyslog.conf** file.

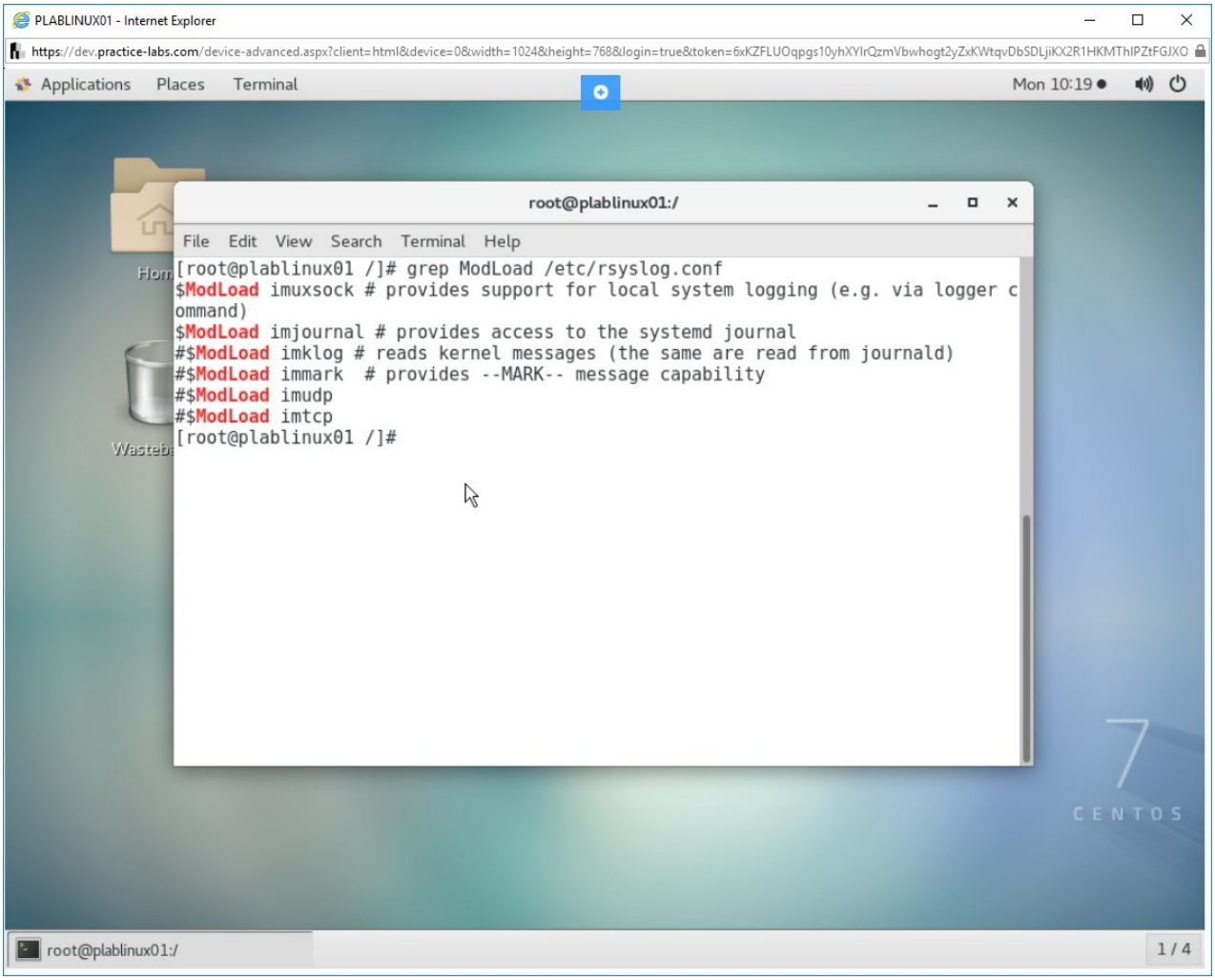


Figure 1.5 Screenshot of PLABLINUX01: Viewing the loaded modules.

Step 5

You can also check for global directives. To check for a global directive marked with $, type the following command:

```
cat /etc/rsyslog.conf
```

Press **Enter**.

Scroll to the **Global Directives** section. Note that there are multiple global directives.

> ***Note**: You can similarly look for Rules etc. in this file.*

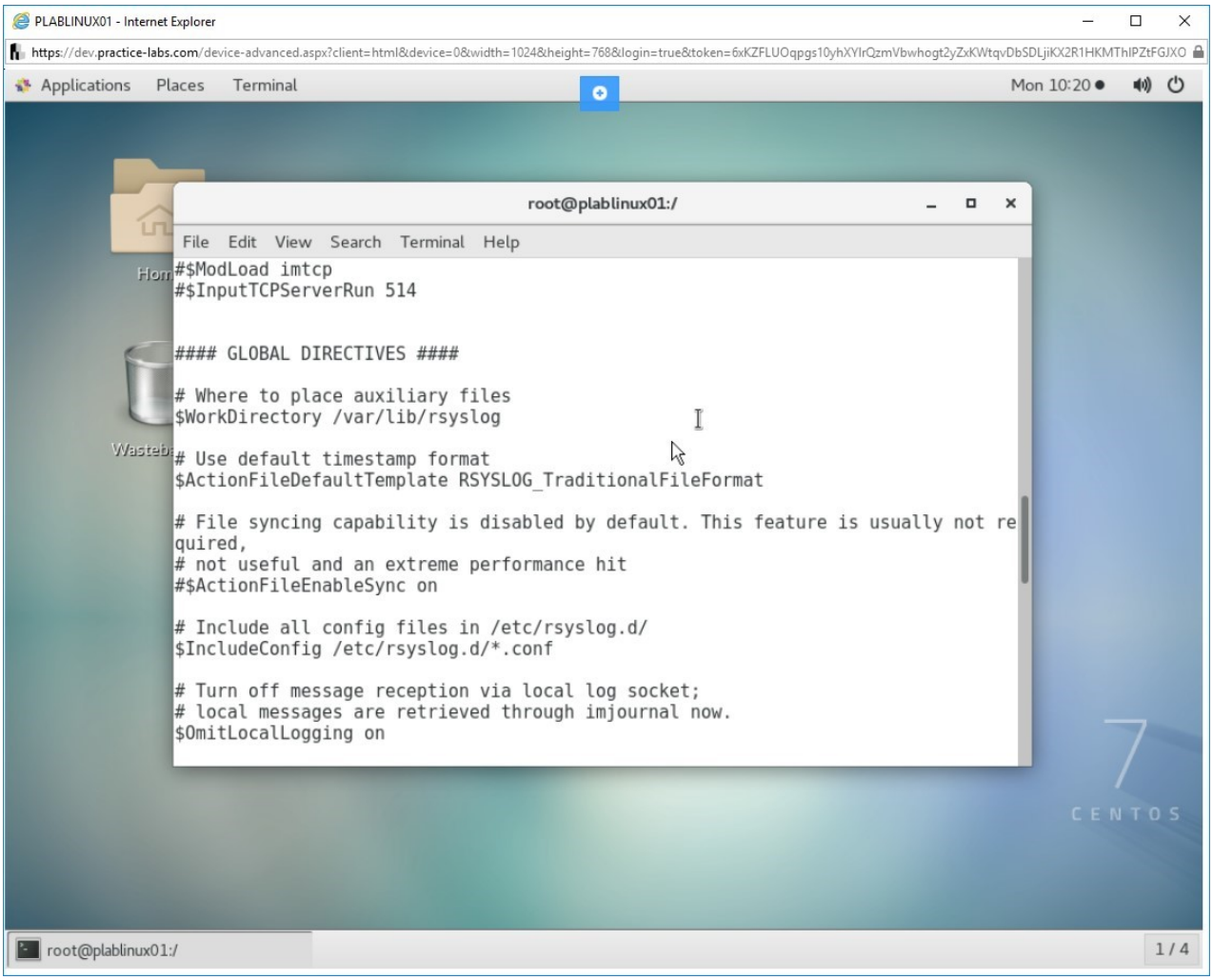


Figure 1.6 Screenshot of PLABLINUX01: Viewing the /etc/rsyslog.conf file.

Step 6

Clear the screen by entering the following command:

```
clear
```

The **syslog** service comprises of two key processes: **rsyslogd** and **klogd**. The **rsyslogd** process is responsible for logging events from user processes. The **klogd** process is used for logging events from the kernel.

To make sure both the processes are running, type the following command:

```
ps ax | egrep -i "(syslogd|klogd)"
```

Press **Enter**.

You will see the status of both the processes.

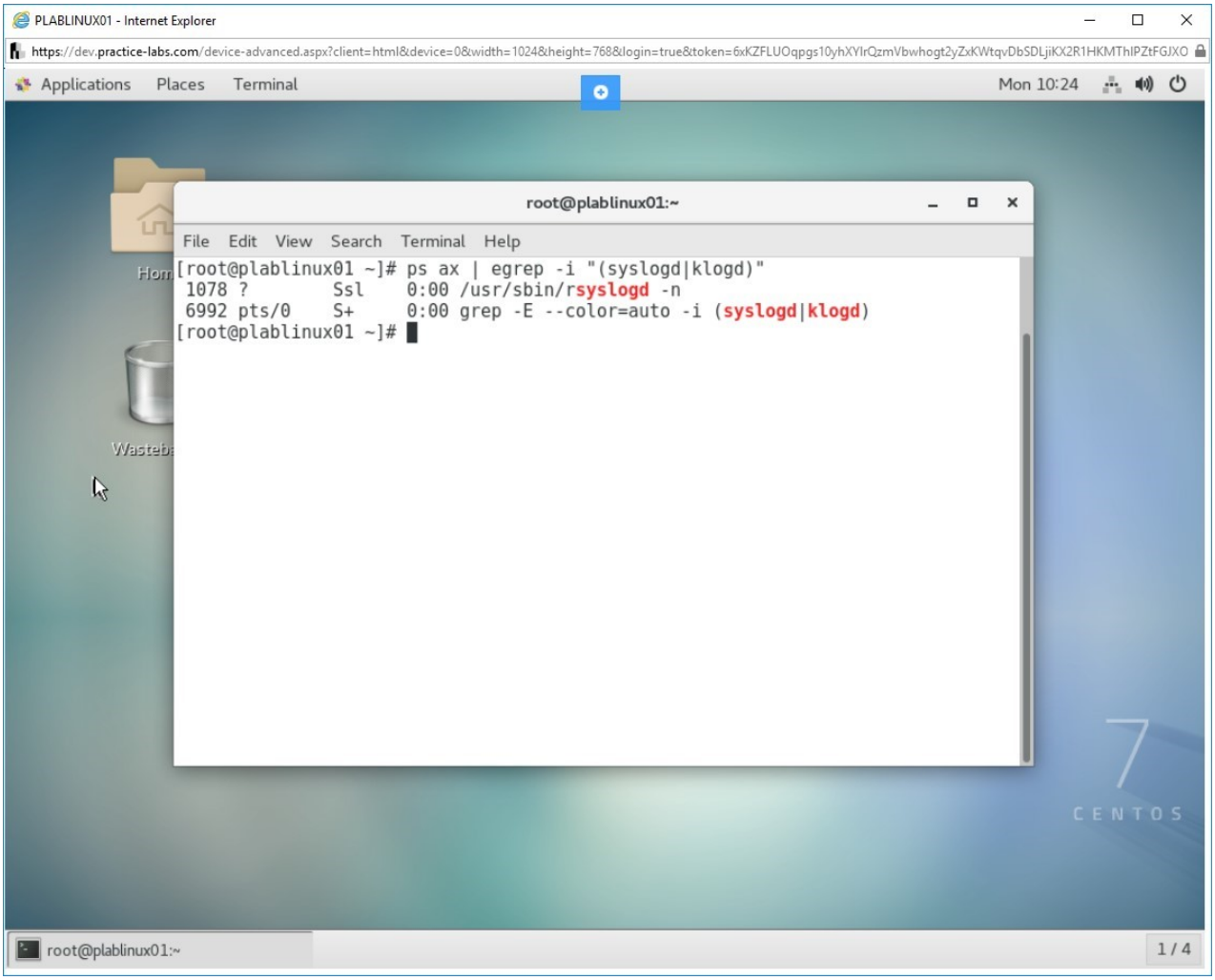


Figure 1.7 Screenshot of PLABLINUX01: Verifying the status of the rsyslogd and klogd processes.

Step 7

Clear the screen by entering the following command:

```
clear
```

You can log events locally as well as on a network server. The **rsyslog** daemon uses port **514** to log events. To view whether this is configured in **/etc/rsyslog.conf**, type the following command:

```
netstat -anp | grep -i ":514" /etc/rsyslog.conf
```

Press **Enter**.

> ***Note**: A network server is not configured as its line is commented using #.*

The line containing the port 514 is displayed.

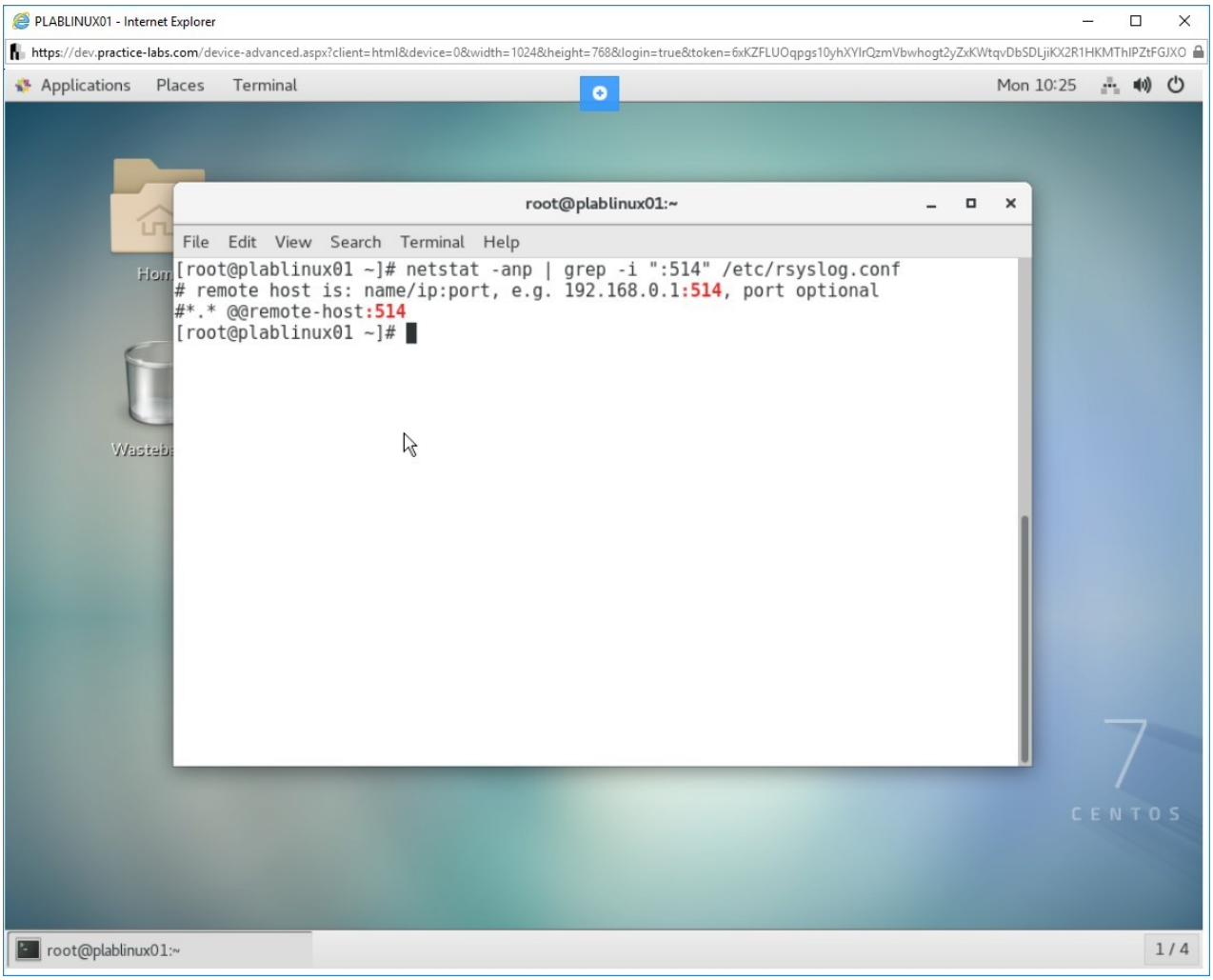


Figure 1.8 Screenshot of PLABLINUX01: Viewing the configuration of the rsyslog daemon.

Task 2 - Configuration of logrotate

The log files are by default contained in the **/var/log** directory. This directory contains various types of logs, such as **boot.log, cron**, and **yum.log**. The logs can grow to massive sizes and may become difficult to manage. To resolve this problem, the logrotate daemon is used. The logrotate daemon suffixes the current message file with the today's date and a new log file is created the next day.

Step 1

Clear the screen by entering the following command:

```
clear
```

To view the log files in the **/var/log** directory, type the following command:

```
ls -l /var/log
```

Press **Enter**.

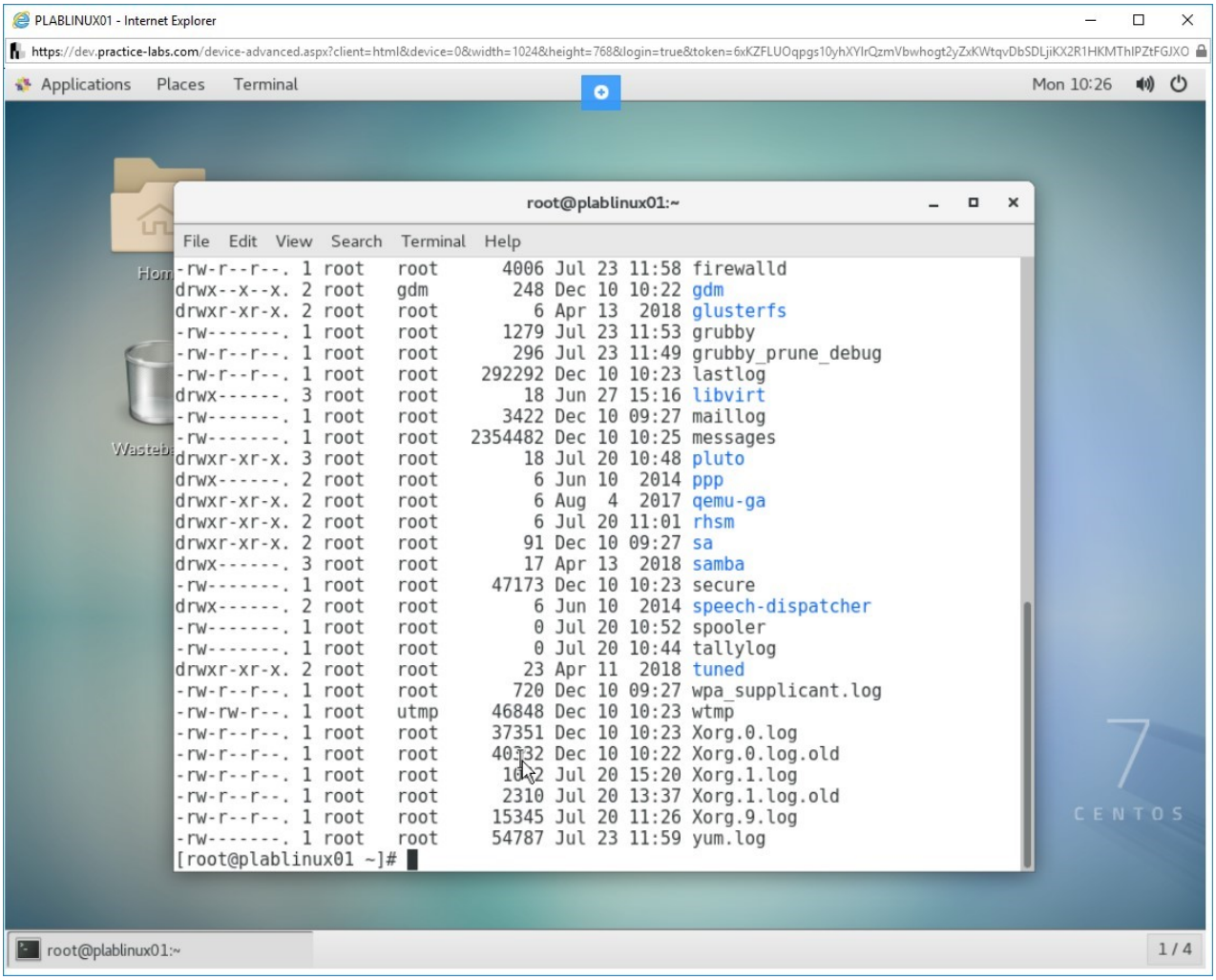


Figure 1.9 Screenshot of PLABLINUX01: Viewing the log files in the /var/log directory.

Note that some files are marked with the older dates.

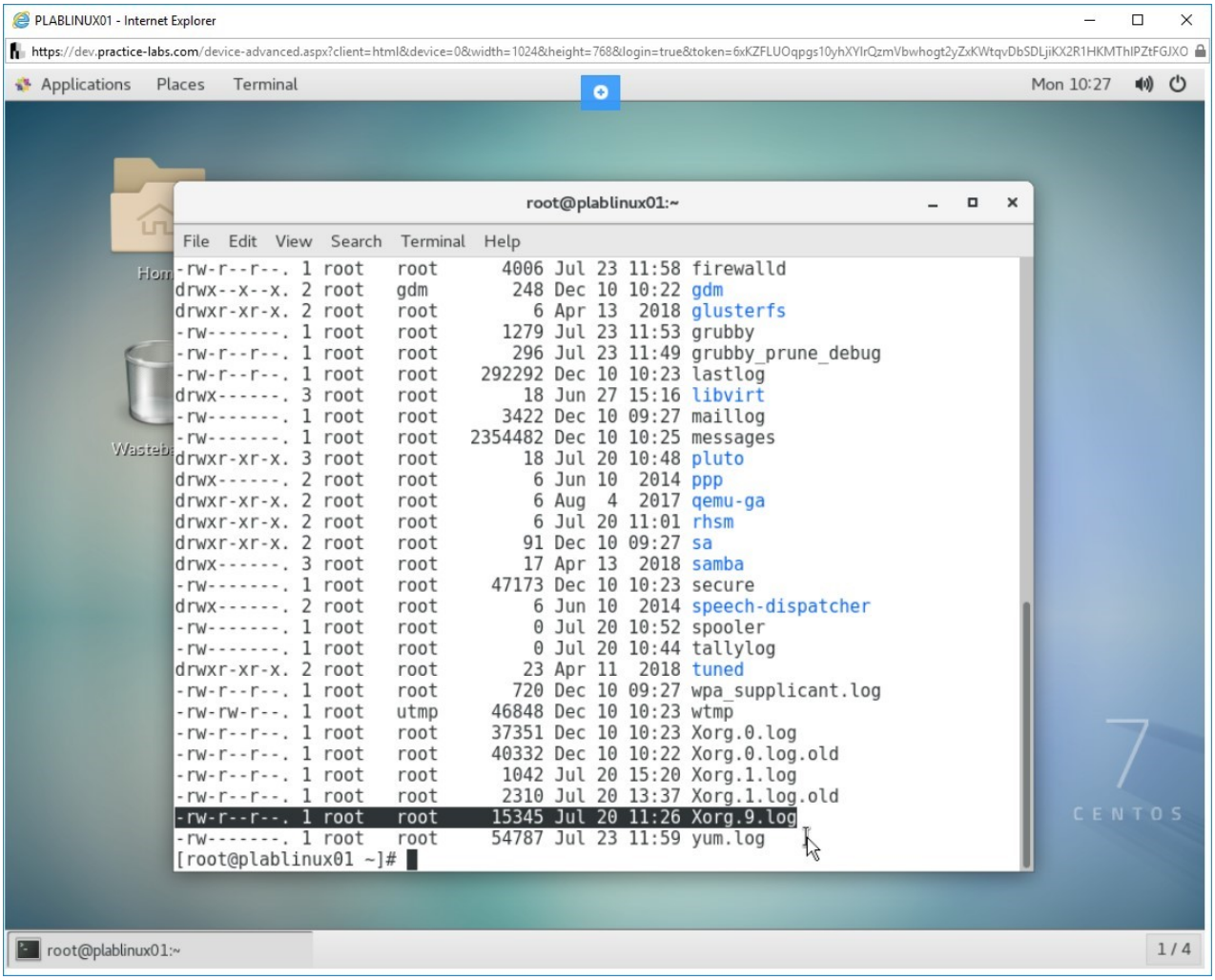


Figure 1.10 Screenshot of PLABLINUX01: Viewing the log files with the older dates.

Step 2

Clear the screen by entering the following command:

```
clear
```

The **logrotate** utility uses the configuration defined in the **/etc/logrotate.conf** file. To view this file, type the following command:

```
cat /etc/logrotate.conf
```

Press **Enter**.

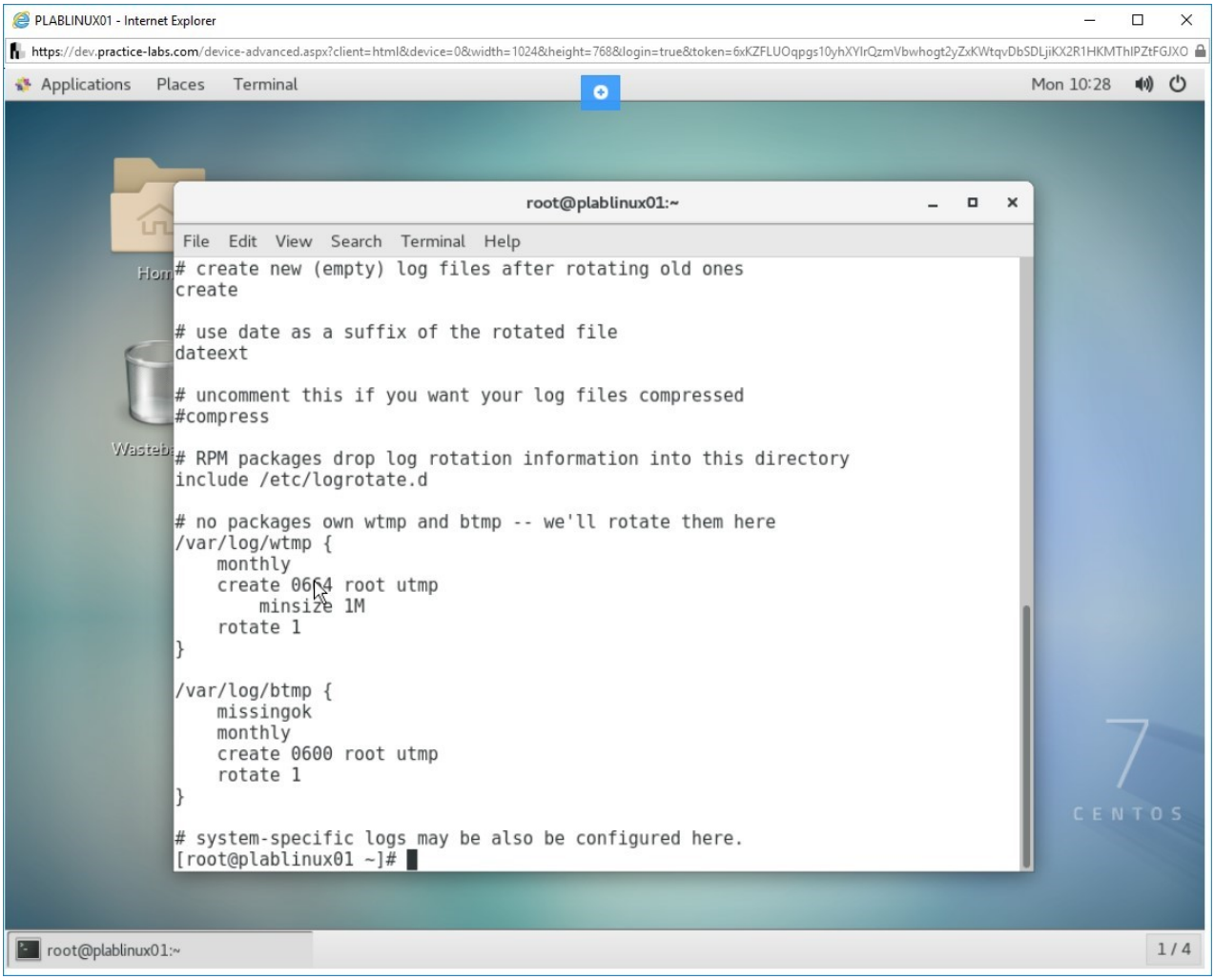


Figure 1.11 Screenshot of PLABLINUX01: Viewing the /etc/logrotate.conf file.

Note that the **/etc/logrotate.conf** file contains a few key parameters, such as;

- When to create
- What to do after rotating old log files
- The naming convention for the rotated log files

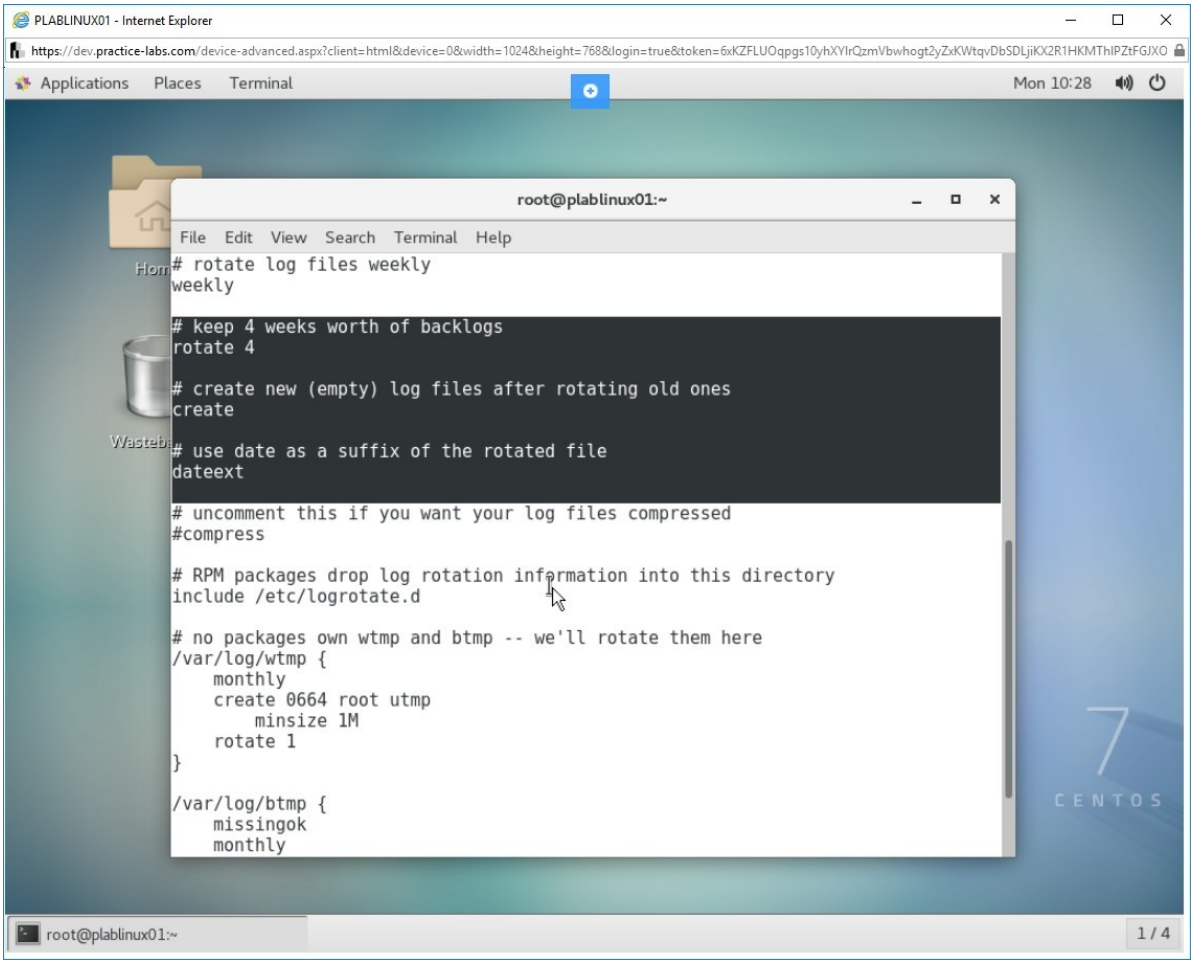
1. 

Figure 1.12 Screenshot of PLABLINUX01: Viewing the /etc/logrotate.conf file.

Step 3

Clear the screen by entering the following command:

```
clear
```

The **logrotate** file uses two key files:

- **/usr/sbin/logrotate** - This is the logrotate command.
- **/etc/cron.daily/logrotate** - This is a shell script that executes the logrotate command on a daily basis.

To view the **/etc/cron.daily/logrotate** shell script, type the following command:

```
cat /etc/cron.daily/logrotate
```

Press **Enter**.

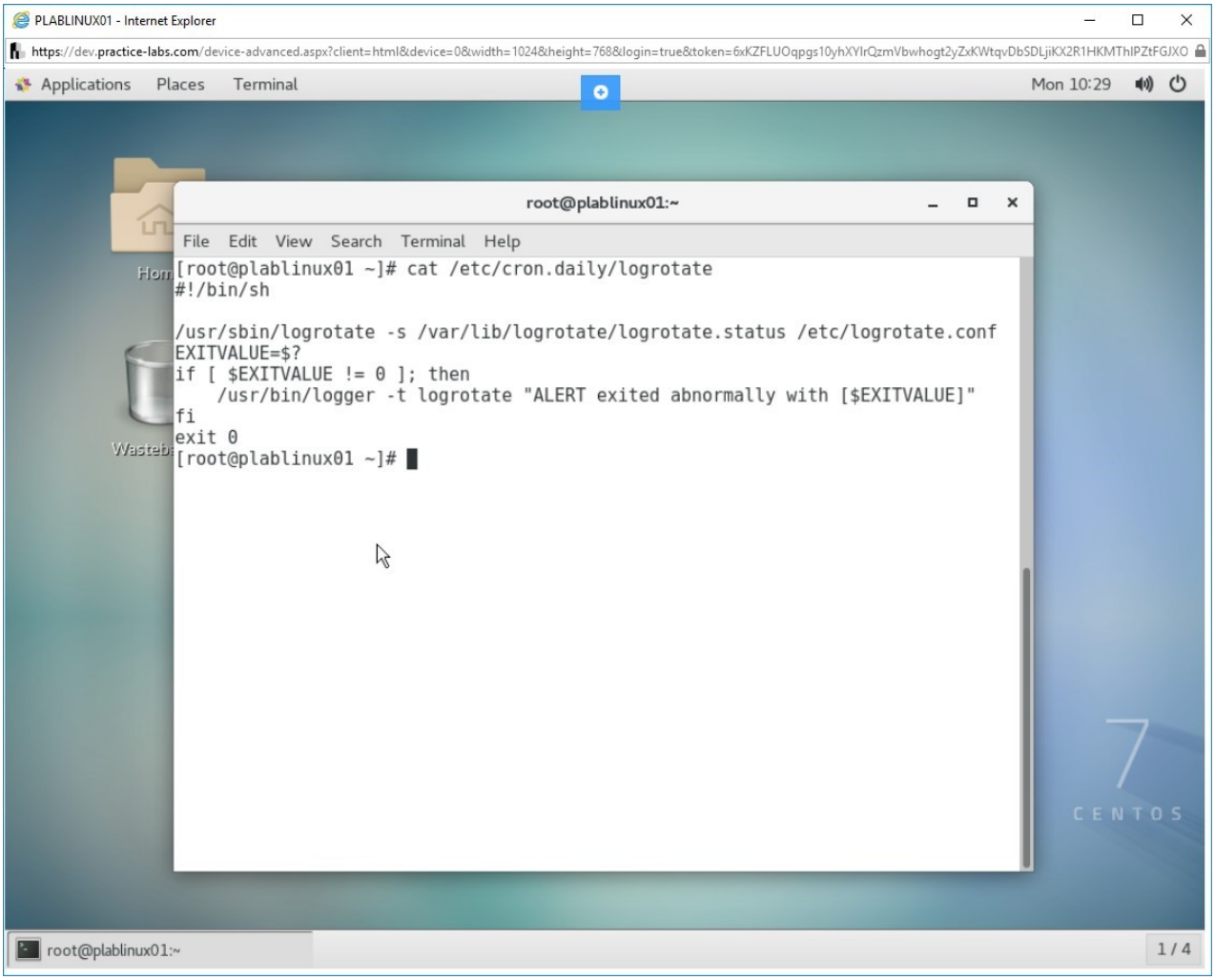


Figure 1.13 Screenshot of PLABLINUX01: Viewing the /etc/cron.daily/logrotate shell script.

Step 4

Clear the screen by entering the following command:

```
clear
```

The **/etc/logrotate.d** file contains the log rotation information for the packages. This means that when you install a package in **CentOS**, the log rotation information will be collected in this directory. For example, you can view the log rotation information on the **yum** package.

To view the log rotation information for the **yum** package, type the following command:

```
cat /etc/logrotate.d/yum
```

Press **Enter**.

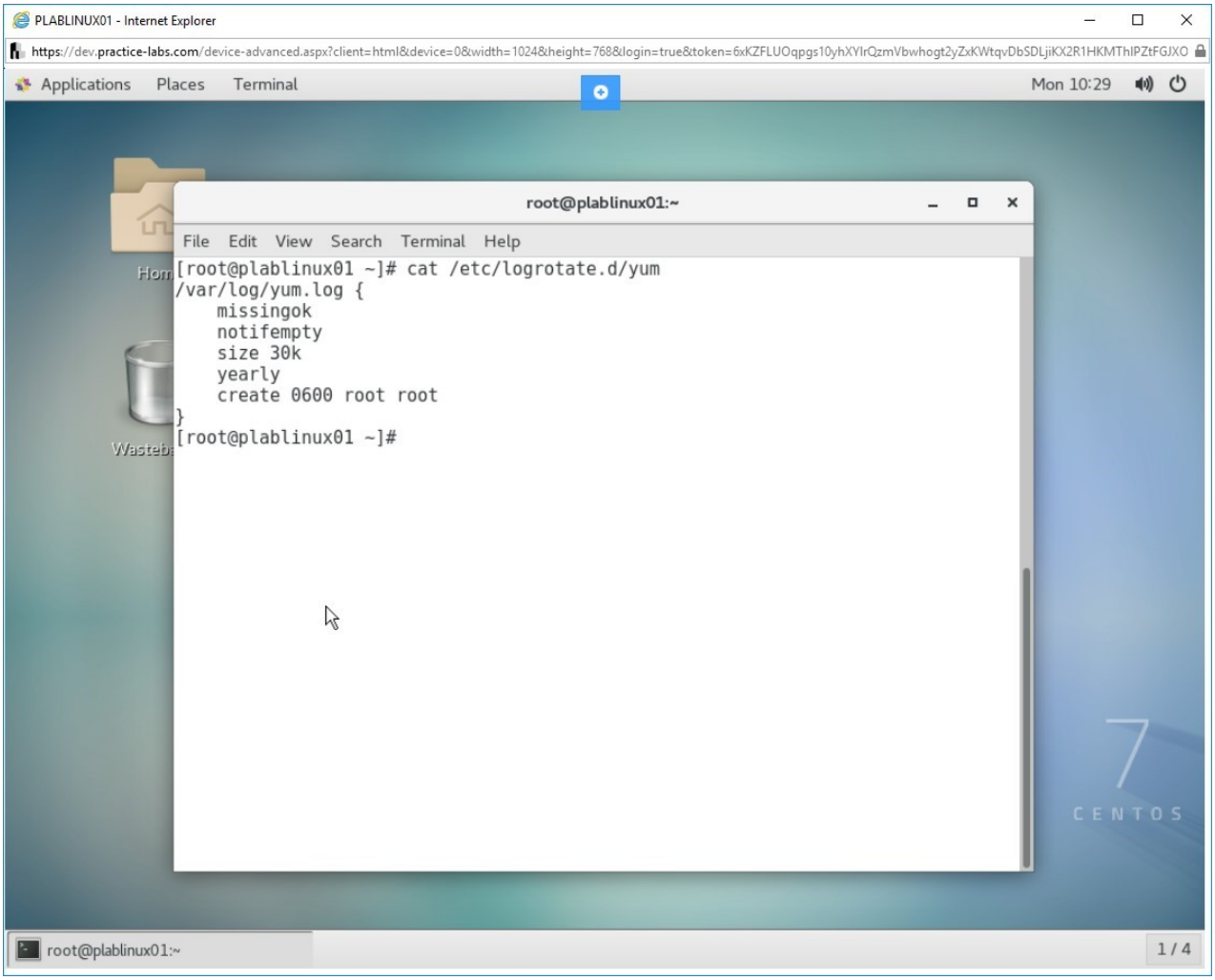


Figure 1.14 Screenshot of PLABLINUX01: Viewing the log rotation information for the yum package.

Step 5

Clear the screen by entering the following command:

```
clear
```

When you run the **logrotate** command, you can write the status with the help of **-s** parameter. To run the **logrotate** command, type the following command:

```
logrotate -s /var/log/logstatus /etc/logrotate.conf
```

Press **Enter**.

The logrotate messages are written to the **/var/log/logstatus** file. Whenever you need of log rotation for specific files, you will need to prepare the logrotate configuration and then manually run the **logrotate** command.

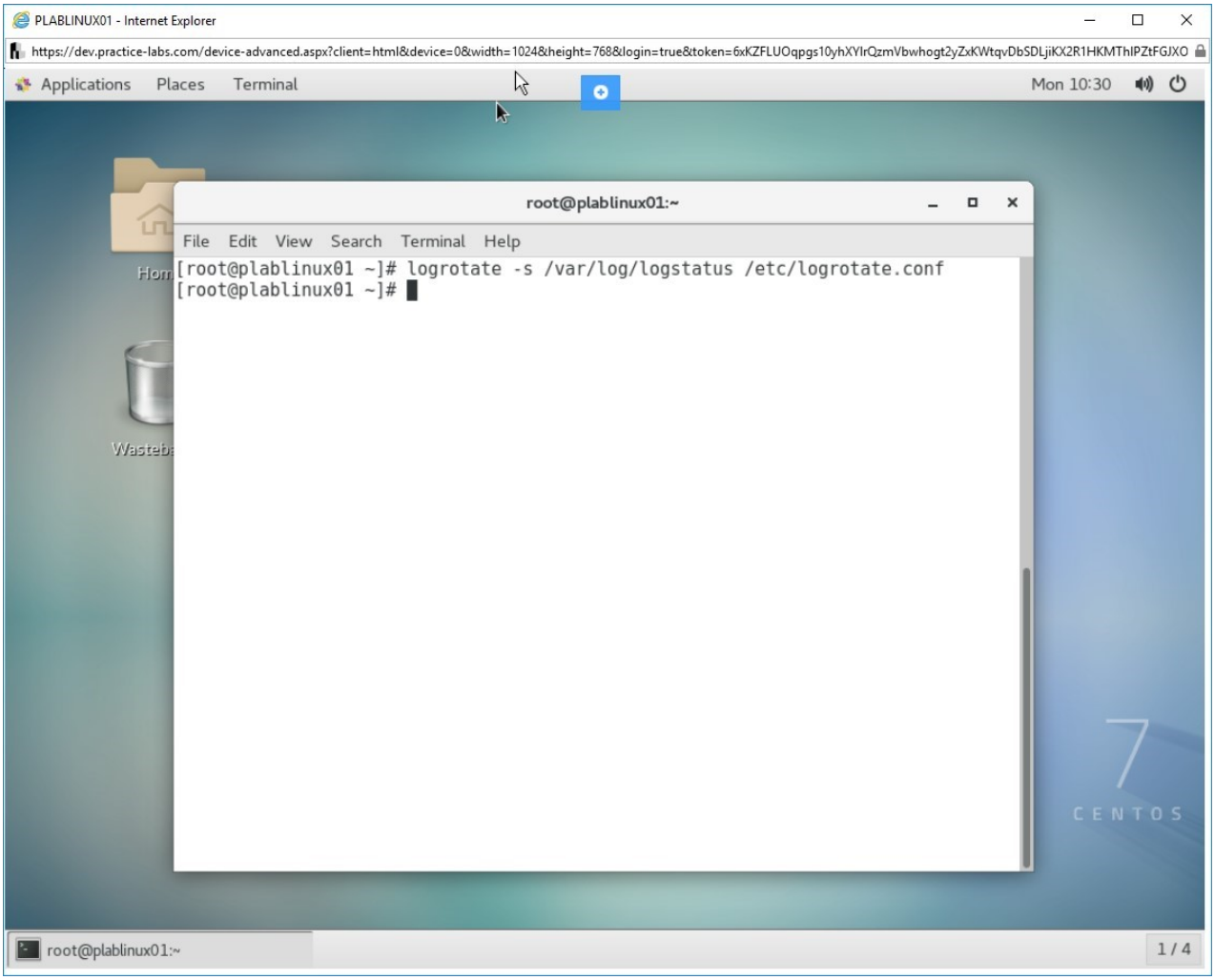


Figure 1.15 Screenshot of PLABLINUX01: Executing the logrotate command.

Step 6

You can also add customized messages into a system log using the **logger** utility. To add a custom message, type the following command:

```
logger -i -p mail.err "Error Message"
```

Press **Enter**.

This will log "**Error Message**" to the **/var/log/maillog** file with the process ID, user account, and the time stamp for the error message.

> ***Note**: You can use the **man logger** command to get more help on this command.*

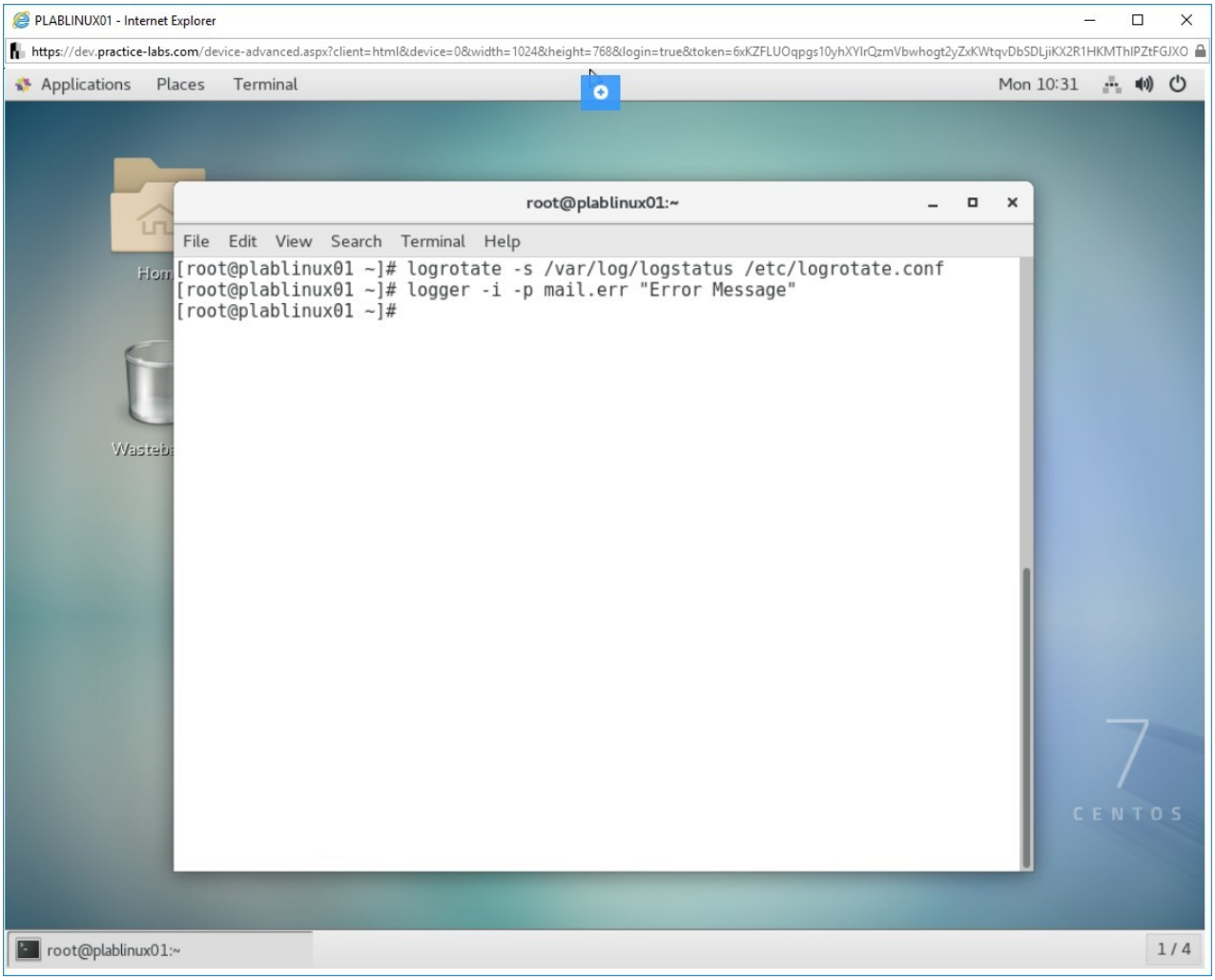


Figure 1.16 Screenshot of PLABLINUX01: Enabling the logging of Error Messages to the /var/log/mail.err file.

Step 7

Clear the screen by entering the following command:

```
clear
```

To log the system reboot message, type the following command:

```
logger System reboot
```

Press **Enter**.

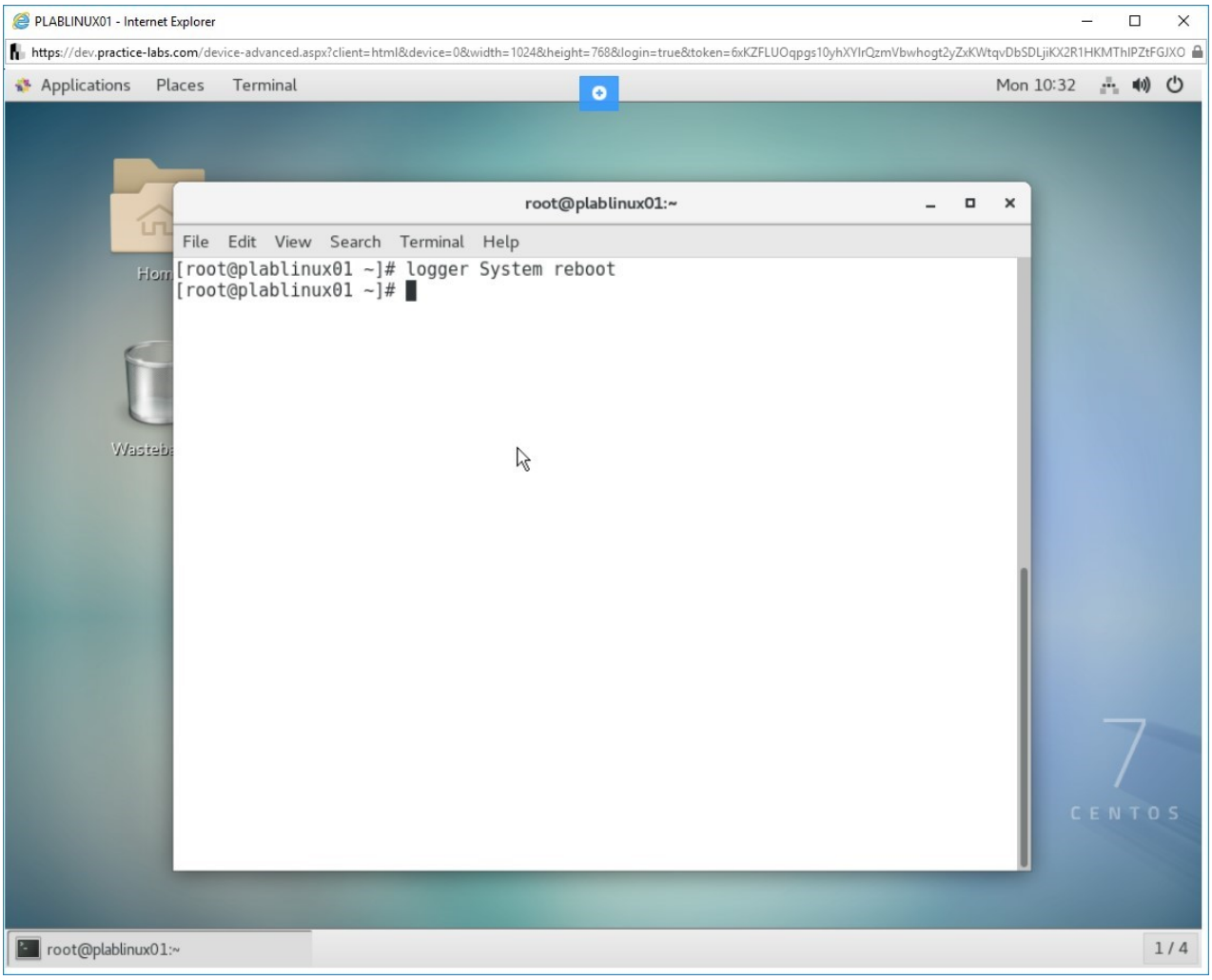


Figure 1.17 Screenshot of PLABLINUX01: Logging the system reboot messages.

Step 8

The **syslog** command is now replaced with the journal command, which stores similar information to **syslog**.

The **/etc/systemd/journald.conf** file contains the configuration settings for **journald**. To view the **journald** configuration file, type the following command:

```
cat /etc/systemd/journald.conf
```

Press **Enter**.

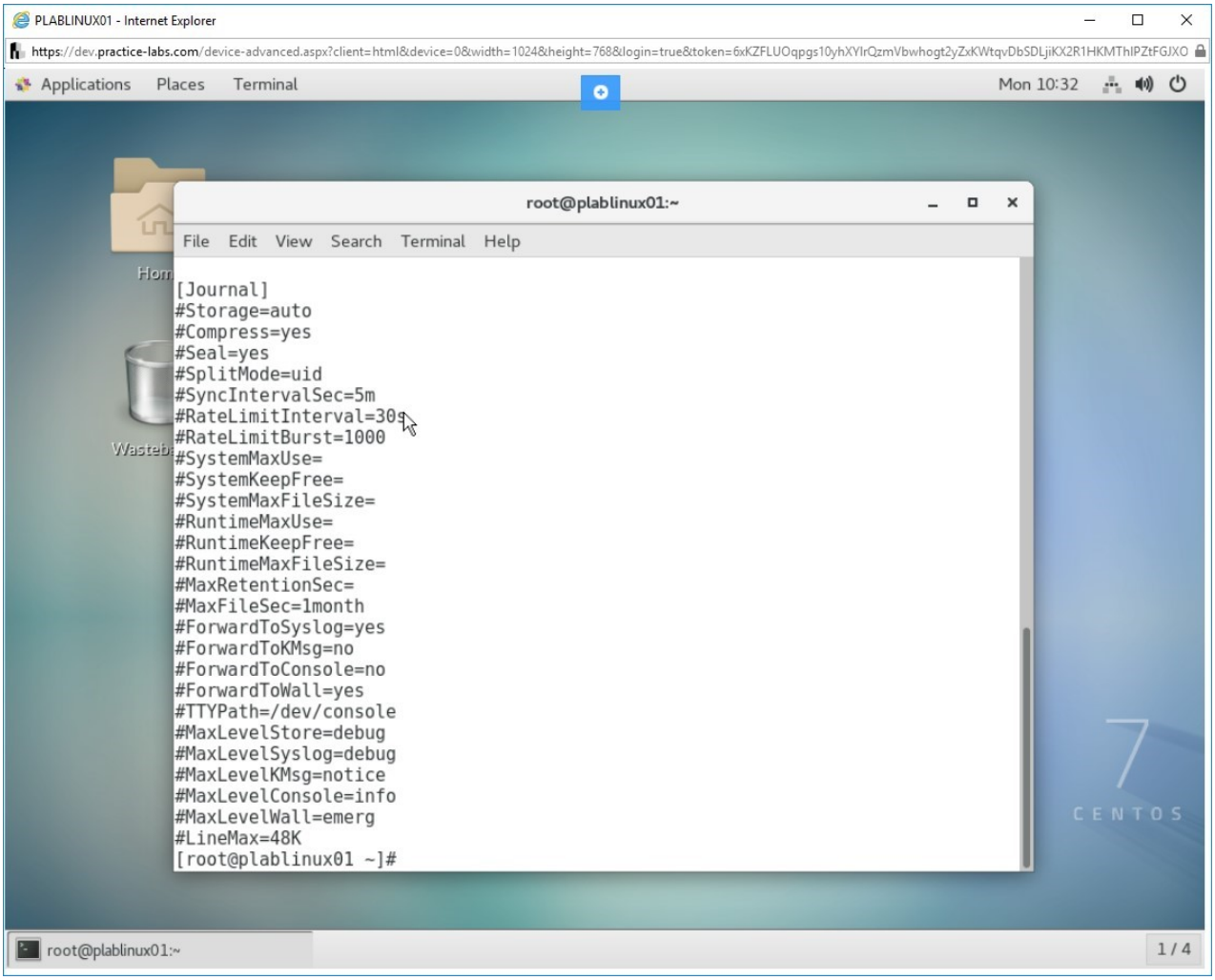


Figure 1.18 Screenshot of PLABLINUX01: Viewing the contents of the /etc/systemd/journald.conf file.

Step 9

You can run the **journalctl** command to get the messages from the **/var/log/** directory. By default, the **journalctl** command provides unfiltered messages, but you can use various filters to filter messages.

To run **journalctl**, type the following command:

```
journalctl
```

Press **Enter**.

*Note: Keep pressing **Enter** to display subsequent logs.*

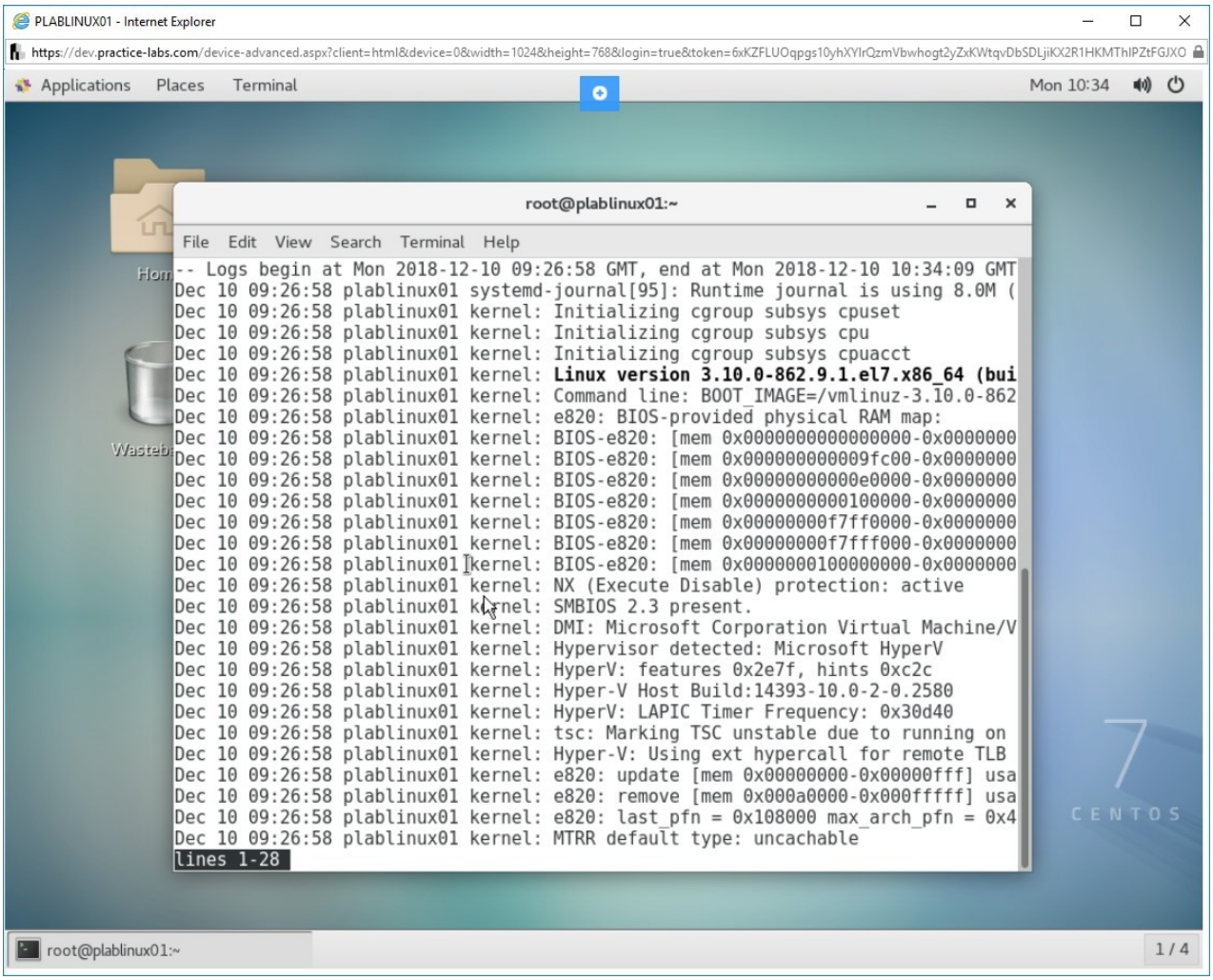


Figure 1.19 Screenshot of PLABLINUX01: Executing the journalctl command to view the logs.

Step 10

Press to the following to quit the display and reach the command prompt:

```
q
```

Press **Enter**. The command prompt is displayed.

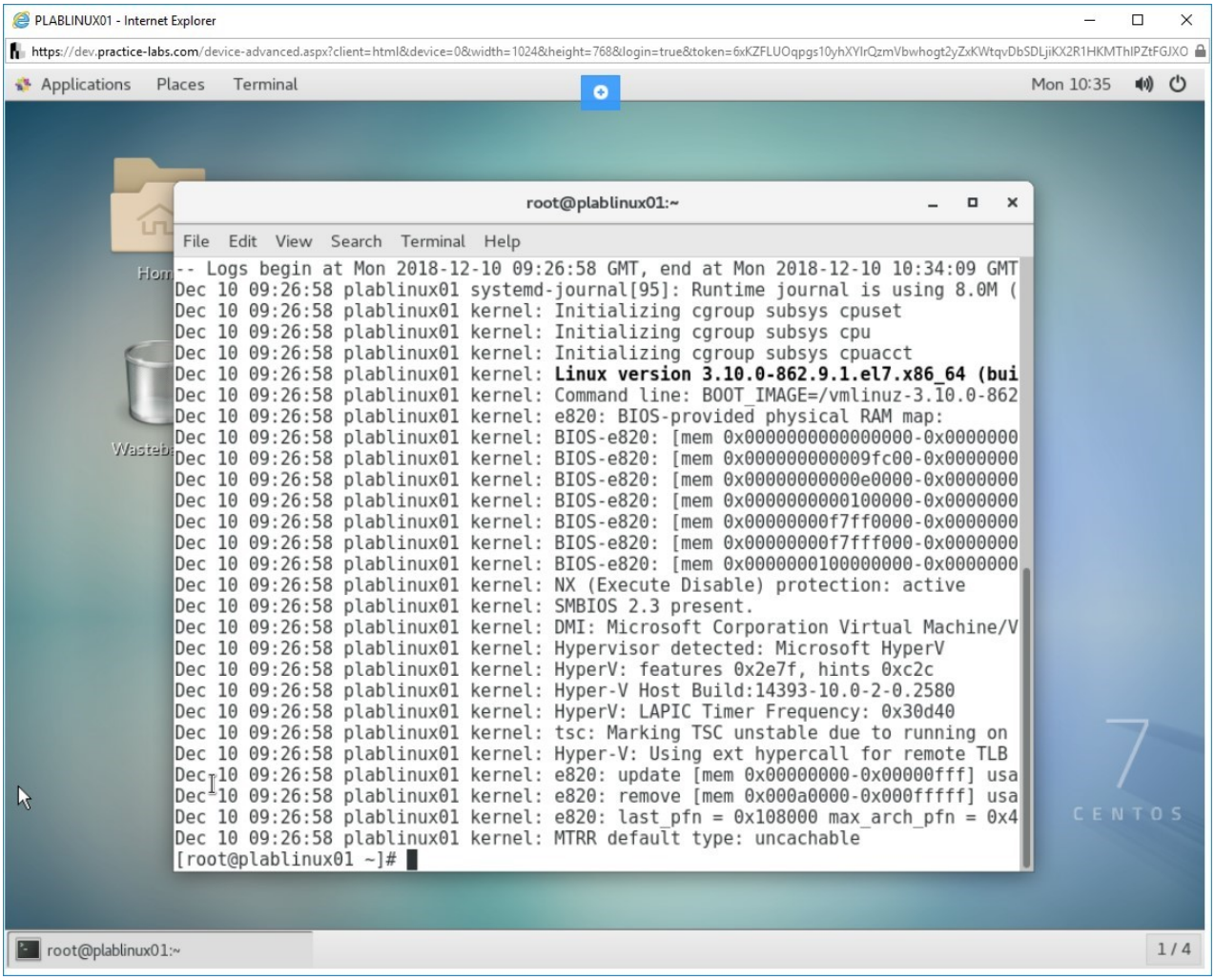


Figure 1.20 Screenshot of PLABLINUX01: Quitting the journalctl command.

Step 11

Clear the screen by entering the following command:

```
clear
```

Let's view the boot messages only. To view the boot messages, type the following command:

```
journalctl -b
```

Press **Enter**.

Keep pressing **Enter** to display subsequent logs.

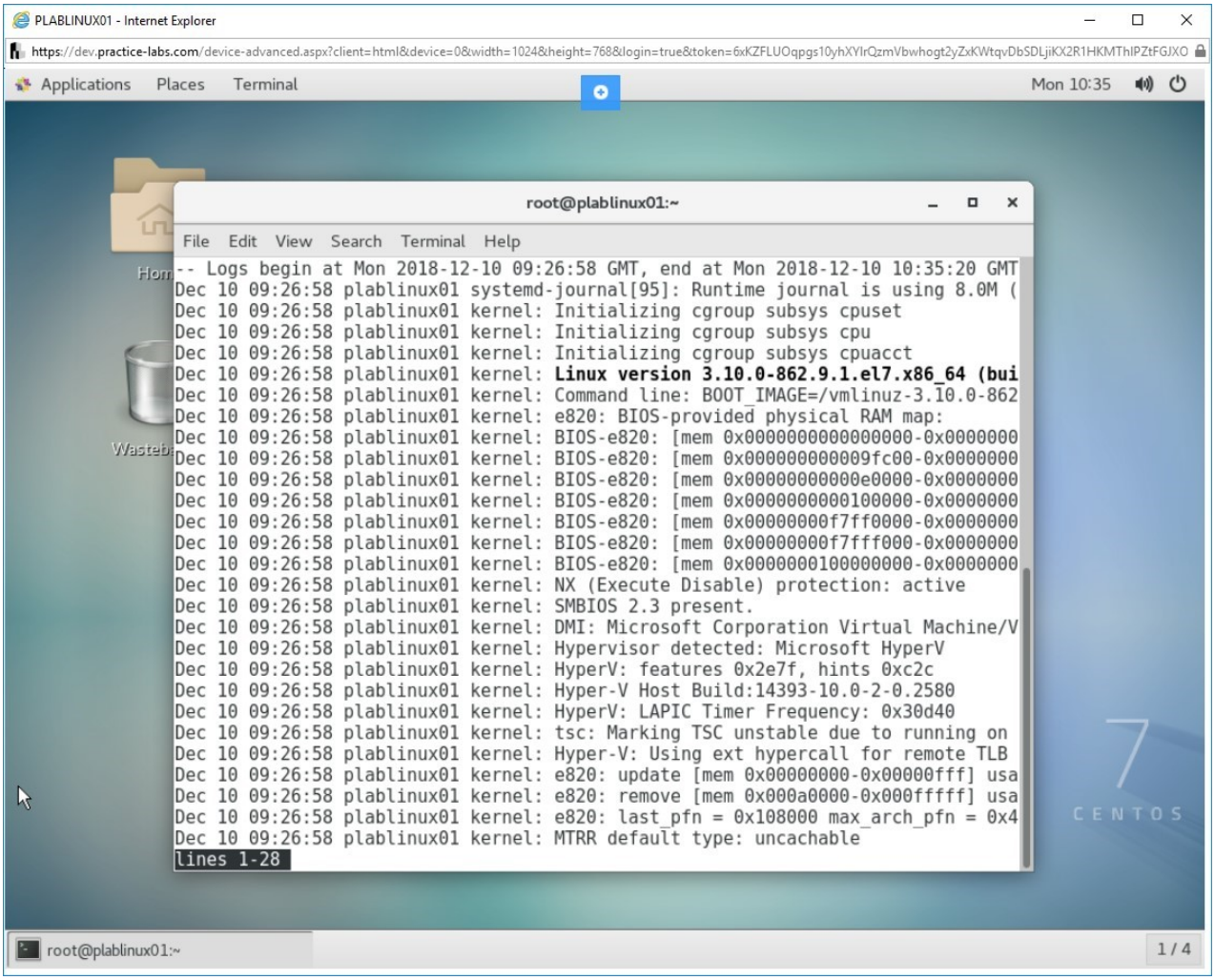


Figure 1.21 Screenshot of PLABLINUX01: Displaying the boot messages in the logs using the journalctl command.

Step 12

Press to the following to quit the display and reach the command prompt:

```
q
```

Press **Enter**.

You are back on the command prompt

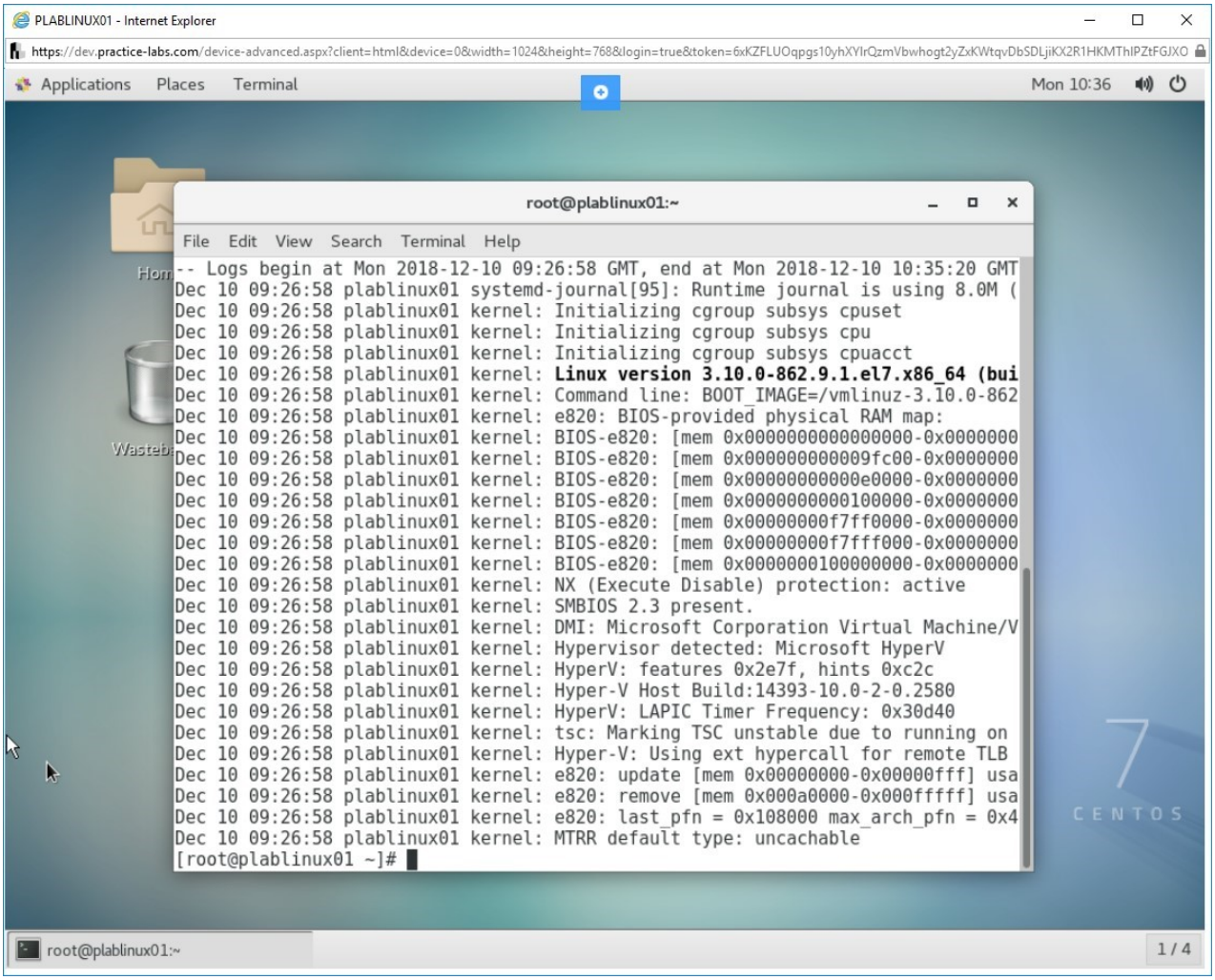


Figure 1.22 Screenshot of PLABLINUX01: Quitting the journalctl command.

Step 13

Clear the screen by entering the following command:

```
clear
```

Now, let's view the logs filtered based on priority. To do that, type the following command:

```
journalctl -p crit
```

Press **Enter**.

The logs are filtered based on the critical priority. Note that there are no critical entries.

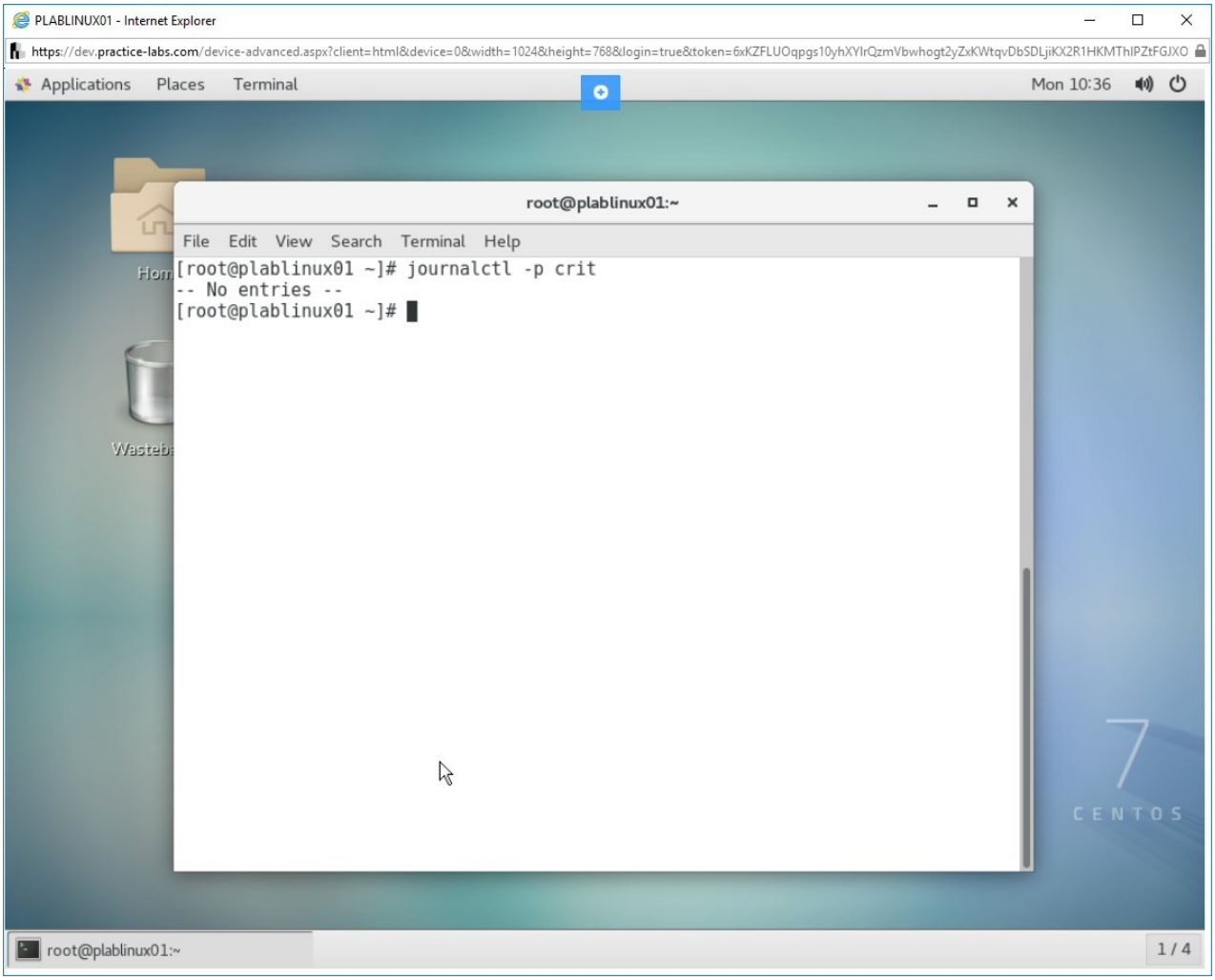


Figure 1.23 Screenshot of PLABLINUX01: Showing the logs based on the critical priority.

Step 14

To view logs by timestamp, type the following command:

```
journalctl --since=2018-12-01
```

Press **Enter**.

Keep pressing **Enter** to display subsequent logs since the day of December 1st, 2018.

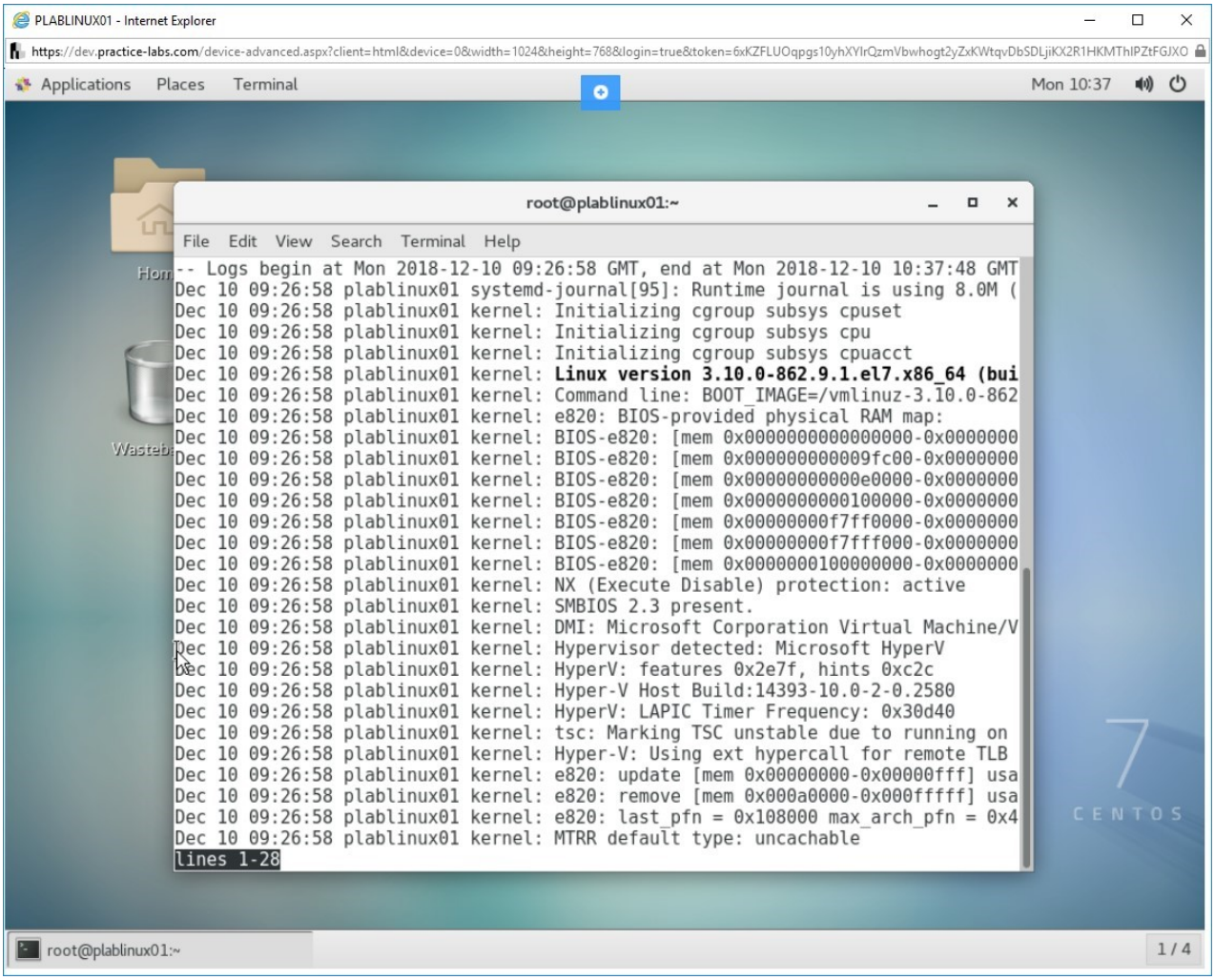


Figure 1.24 Screenshot of PLABLINUX01: Showing the logs from a specific time period.

Step 15

Press to the following to quit the display and reach the command prompt:

```
q
```

Press **Enter**.

You are back on the command prompt

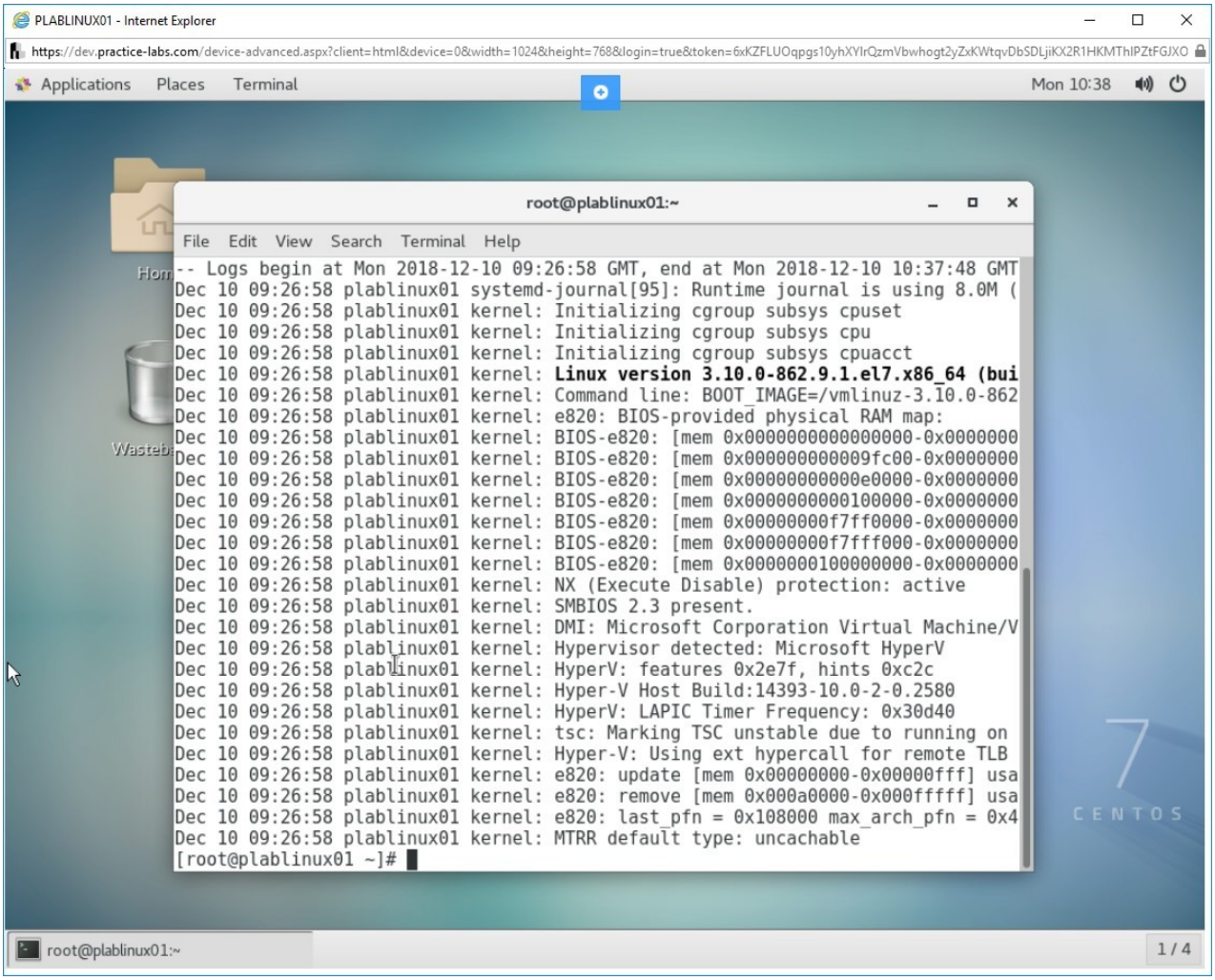


Figure 1.25 Screenshot of PLABLINUX01: Quitting the journalctl command.

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

Review

Well done, you have completed the **Configure System Logging** Practice Lab.

Summary

You completed the following exercise:

- Exercise 1 - Configure System Logging

You should now be able to:

- Configure the syslog daemon
- Configuration of logrotate

Feedback

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