CompTIA Linux+

Configure SELinux

Introduction

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

SELinux
CentOS
Domain Transitions

Learning Outcomes

In this module, you will complete the following exercise:

- Exercise 1 - Configure SELinux

After completing this lab, you will be able to:

- Configure Network on CentOS
- View Current Status of SELinux
- Change the SELinux Mode
- View SELinux Contexts for Processes, Domain Transitions, and Users
- Install and use the policycoreutils-gui Package

Exam Objectives

The following exam objectives are covered in this lab:

- **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.
- **CompTIA:** 4.4 Given a scenario, analyze and troubleshoot application and hardware issues.

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.

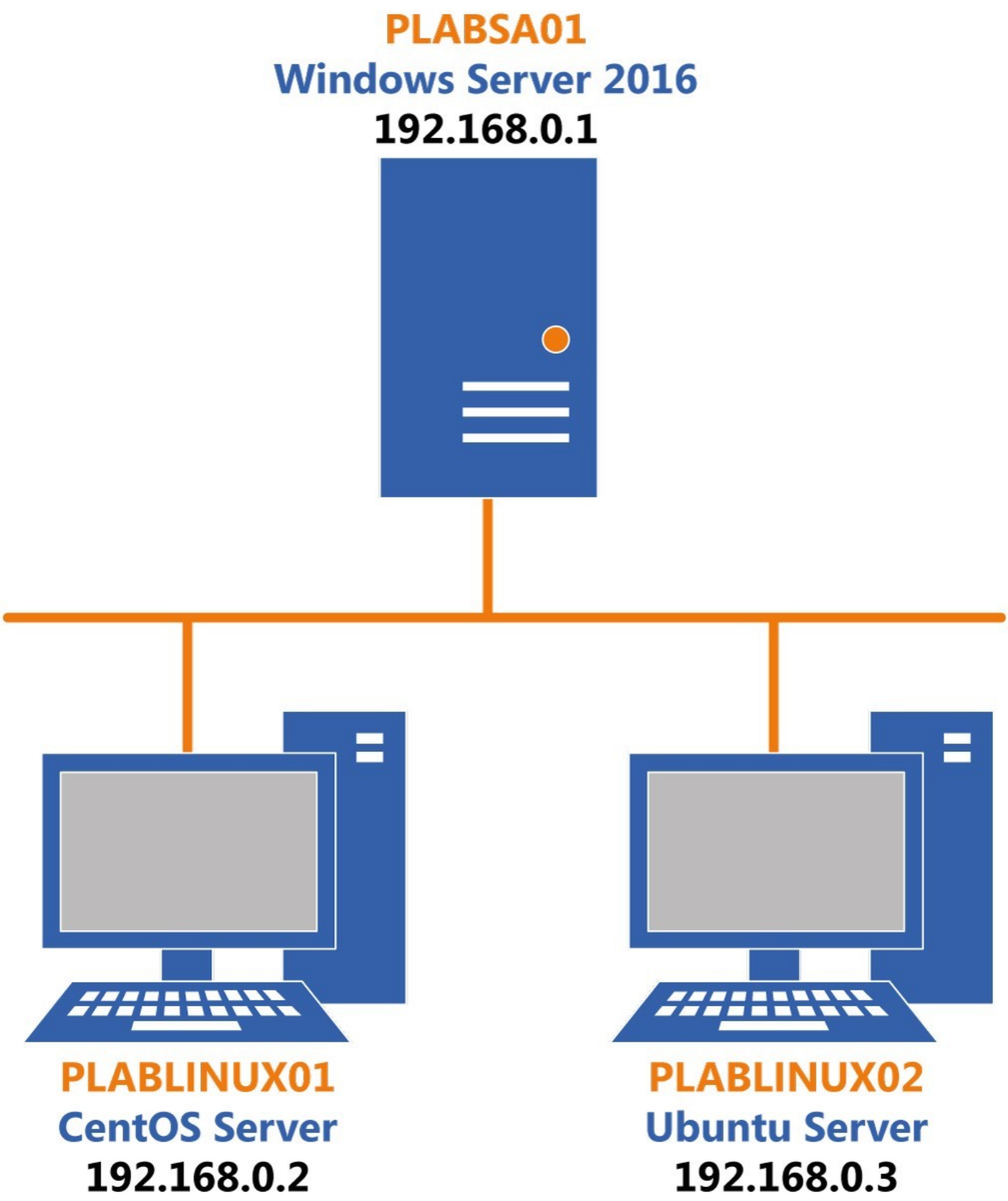
Help and Support

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 SELinux

SELinux, Security Enhanced Linux, is enabled by default on CentOS. Its default mode is enforcing, and SELinux should be kept in this mode as a recommended practice.

In this exercise, you will learn to configure SELinux.

Learning Outcomes

After completing this exercise, you will be able to:

- Log into a Linux System
- Configure Network on CentOS
- View Current Status of SELinux
- Change the SELinux Mode
- View SELinux Contexts for Processes, Domain Transitions, and Users
- Install and use the policycoreutils-gui Package

Your Devices

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

- **PLABLINUX01** (CentOS Server)

Task 1 - Configure Network on CentOS

For a client to communicate on the network, it needs to have an IP address. If the client exists on the IPv4 network, then the client must have an IPv4 address. On the IPv6 network, the client must have IPv6 address.

In this task, you will configure an IP address on the client. To do this, perform the following steps:

Step 1

Connect to **PLABLINUX01**.

Click **Applications**, select **System Tools**, and then select **Settings**.

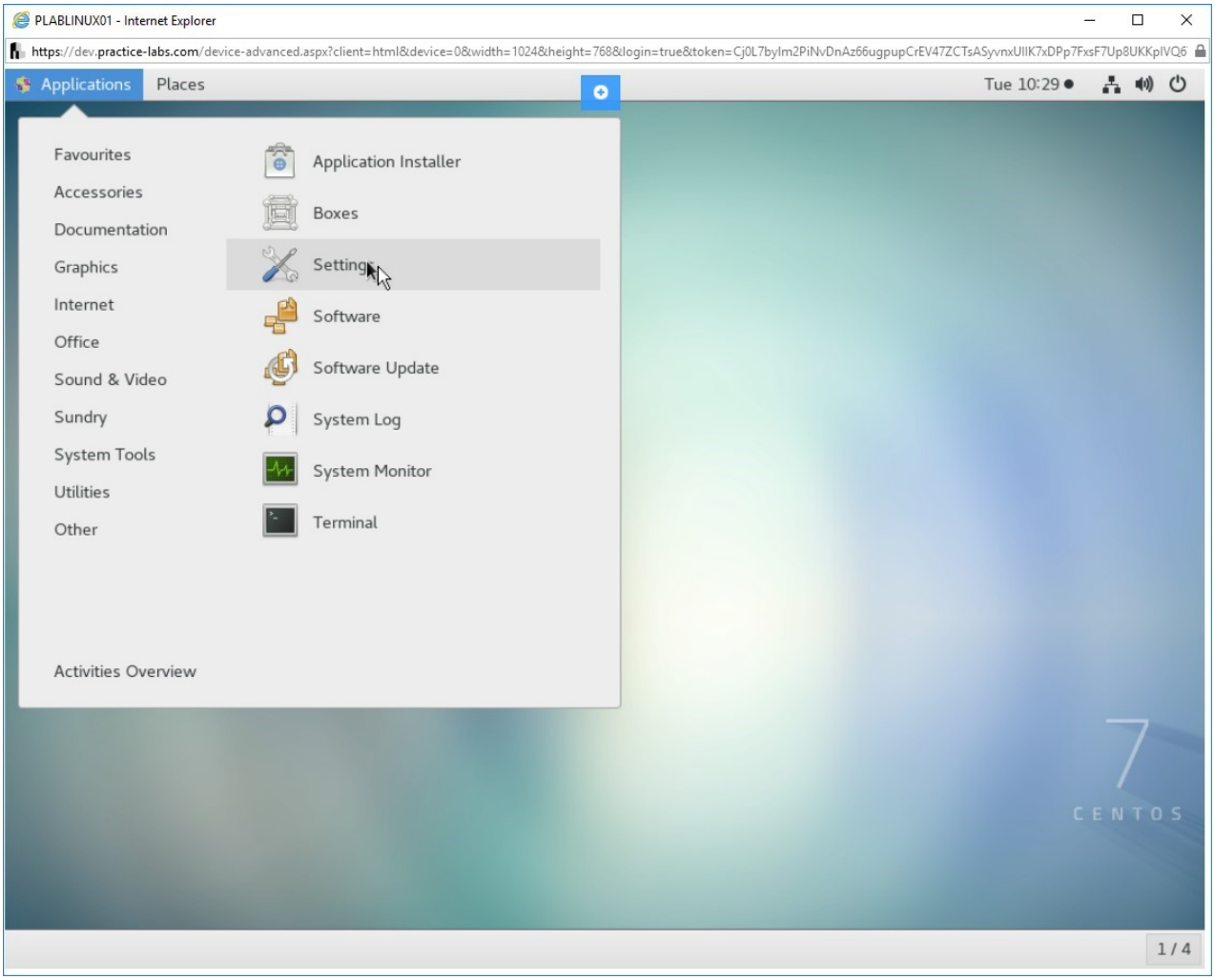


Figure 1.1 Screenshot of PLABLINUX01: Selecting the Settings option from the Applications > System Tools menu.

Step 2

From the **Settings** window, click **Network** in the left pane and then click the icon next to **ON** in the **Wired** section.

Note: *If the Wired button is set to* ***OFF****, click the button on its left to switch it to* ***ON****.*

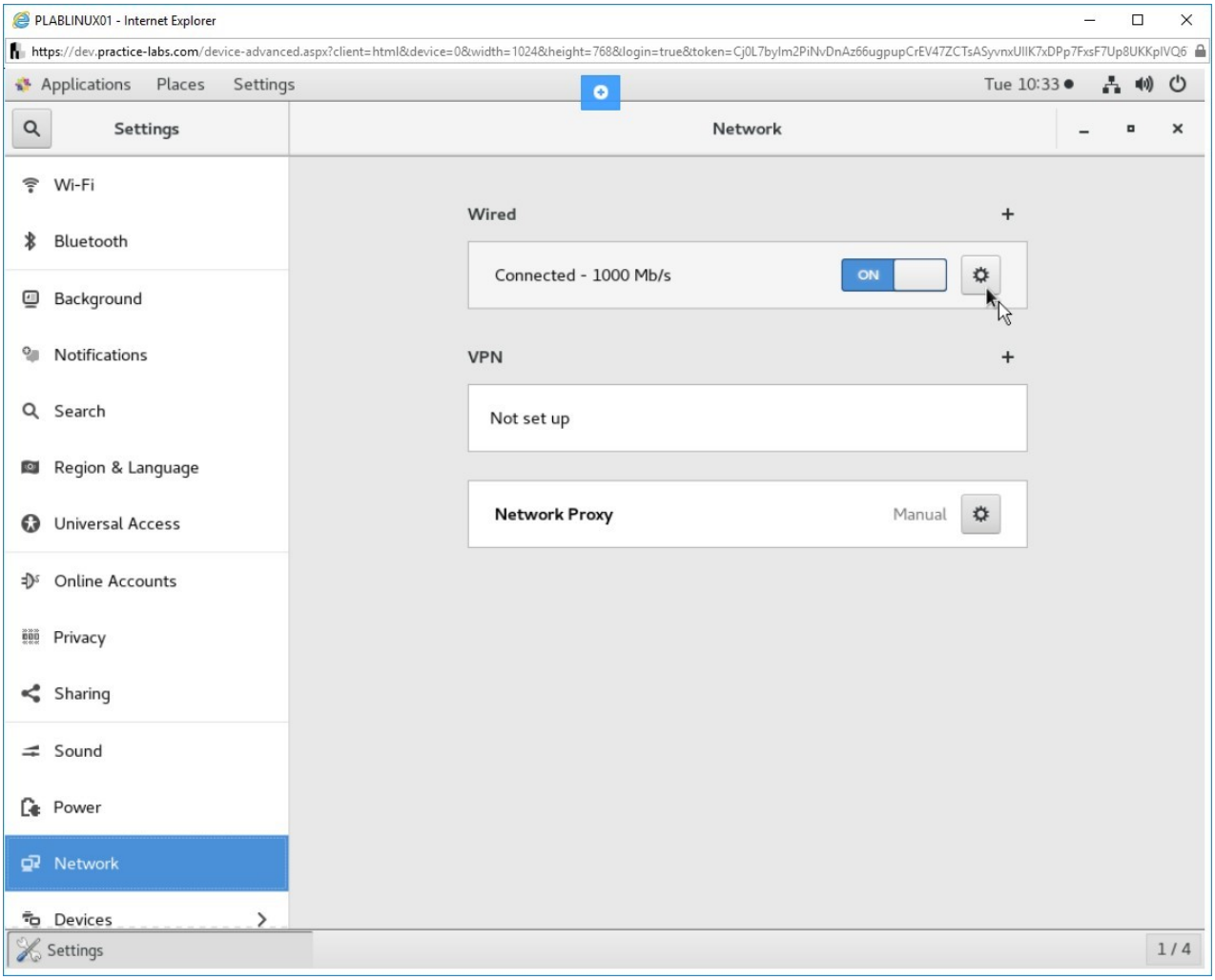


Figure 1.2 Screenshot of PLABLINUX01: Clicking the button to invoke the Wired dialog box.

Step 3

In the **Wired** dialog box, click the **IPv4** tab.

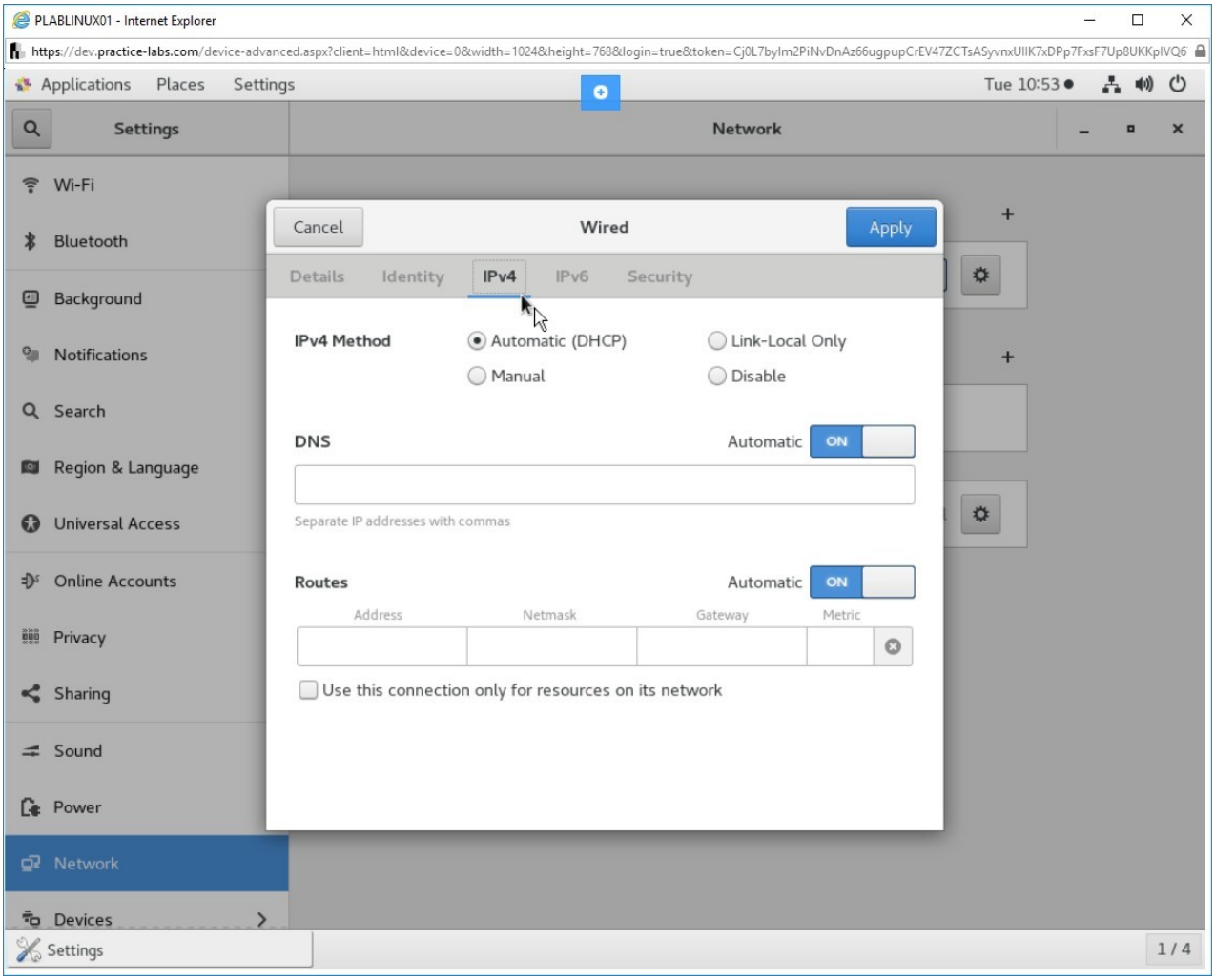


Figure 1.3 Screenshot of PLABLINUX01: Selecting the IPv4 tab in the Wired dialog box.

Step 4

Select **Manual** and provide the following details:

Address:

```
192.168.0.2
```

Netmask:

```
255.255.255.0
```

Gateway:

```
192.168.0.250
```

Click **Apply**.

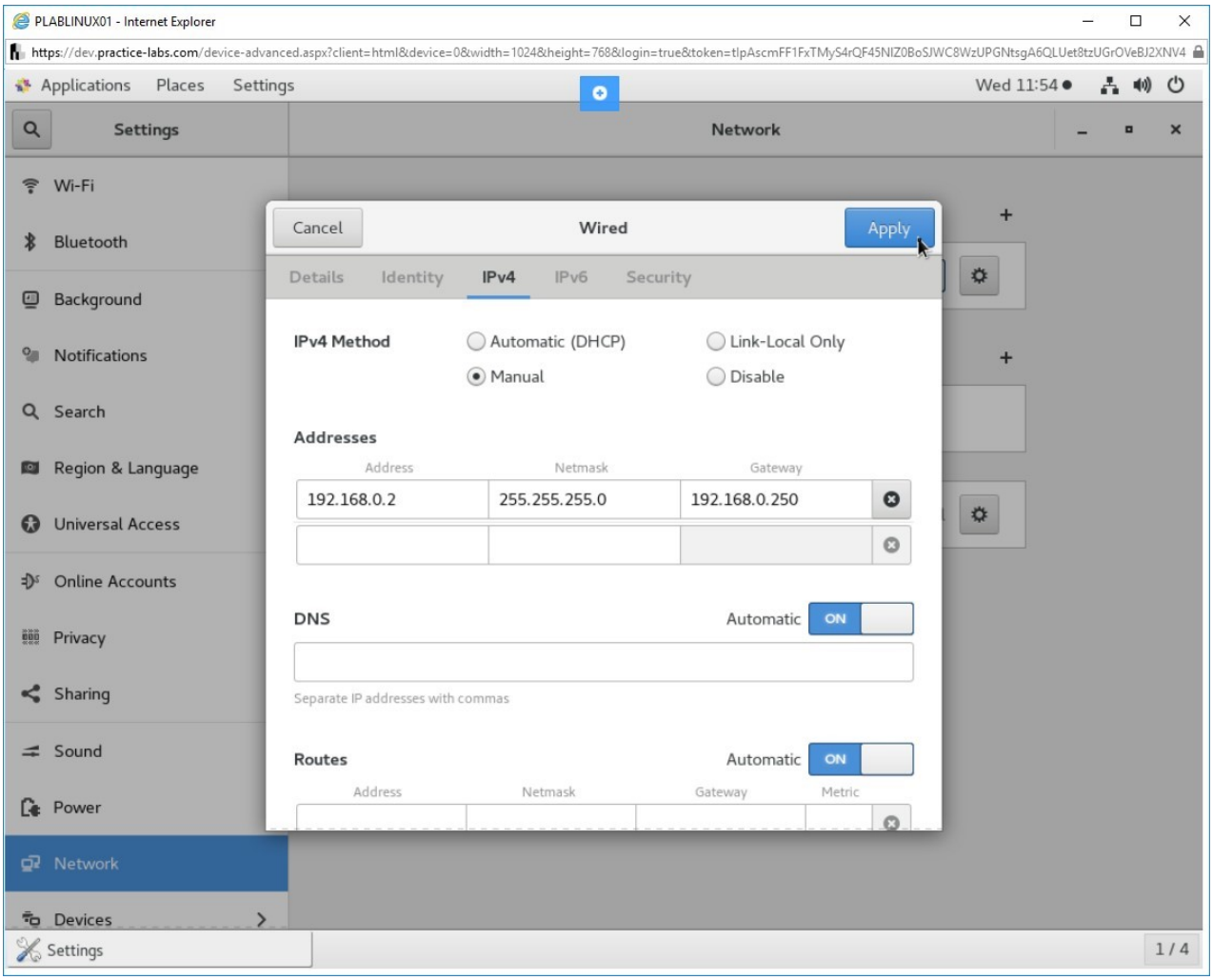


Figure 1.4 Screenshot of PLABLINUX01: Entering the network information and then clicking the Apply button.

Step 5

The **Wired** dialog box is closed automatically. Close the **Settings** window.

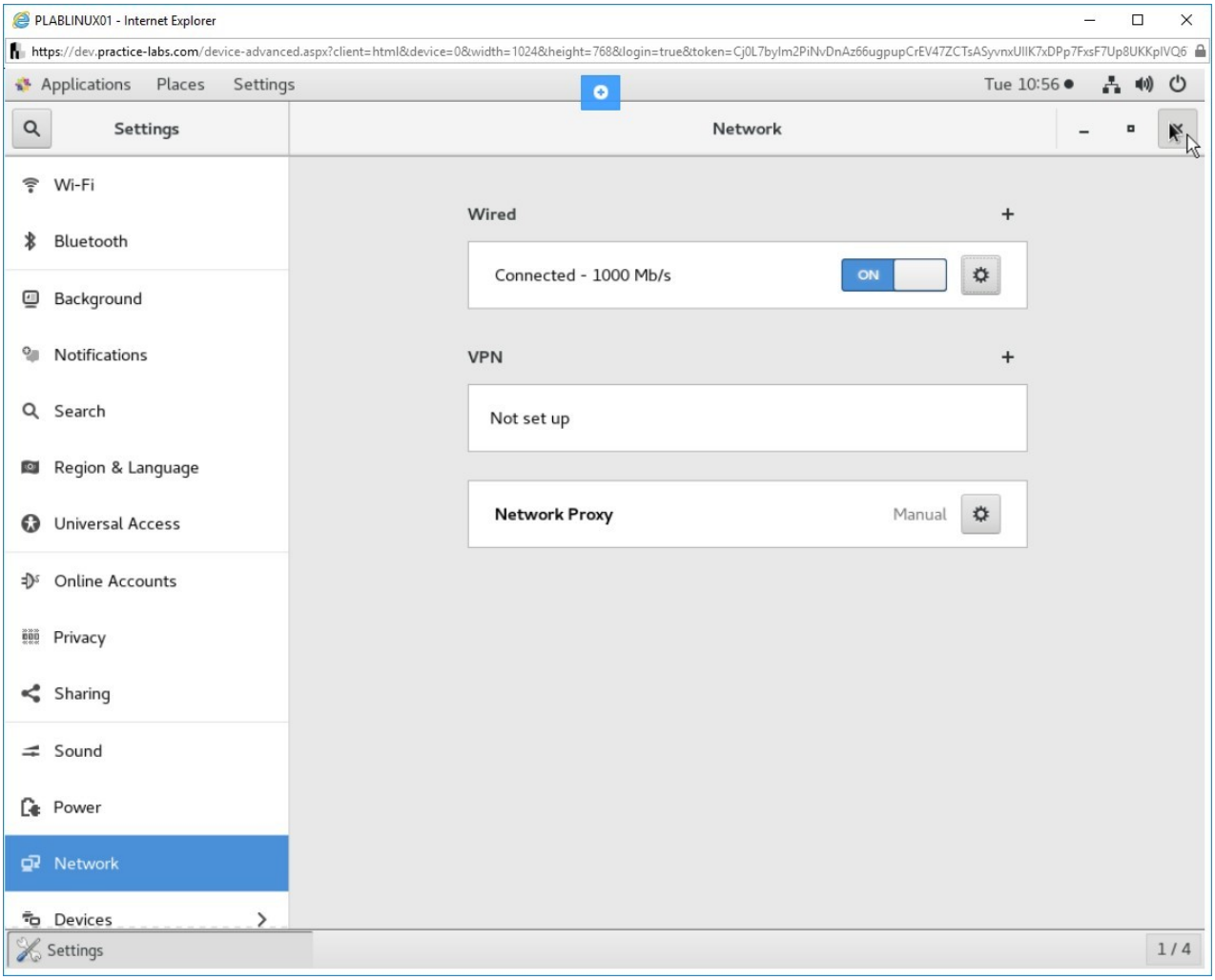


Figure 1.5 Screenshot of PLABLINUX01: Displaying the Settings window.

Task 2 - View Current Status of SELinux

By default, SELinux is configured to work in Enforcing mode. Overall, there are three different modes of SELinux:

- Enforcing: If an event occurs against the defined policy of SELinux, then the event is blocked and logged.
- Permissive: If an event occurs against the defined policy of SELinux, then the event is not blocked and logged.
- Disabled: If an event occurs against the defined policy of SELinux, then the event is not blocked or logged.

In this task, you will learn to view the current status of SELinux. To view the current status of SELinux, perform the following steps:

Step 1

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

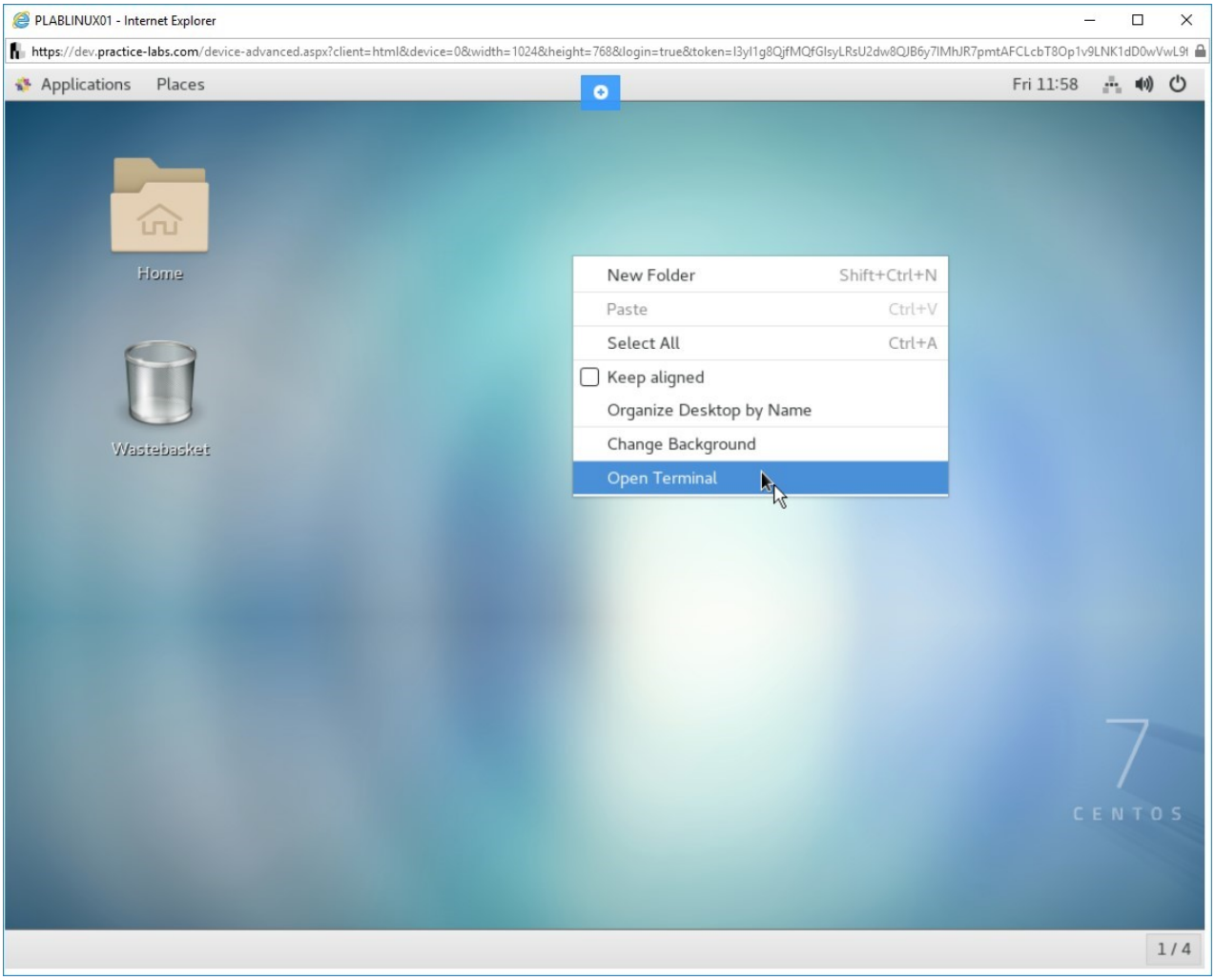


Figure 1.6 Screenshot of PLABLINUX01: Selecting the Open Terminal option from the context menu.

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**.

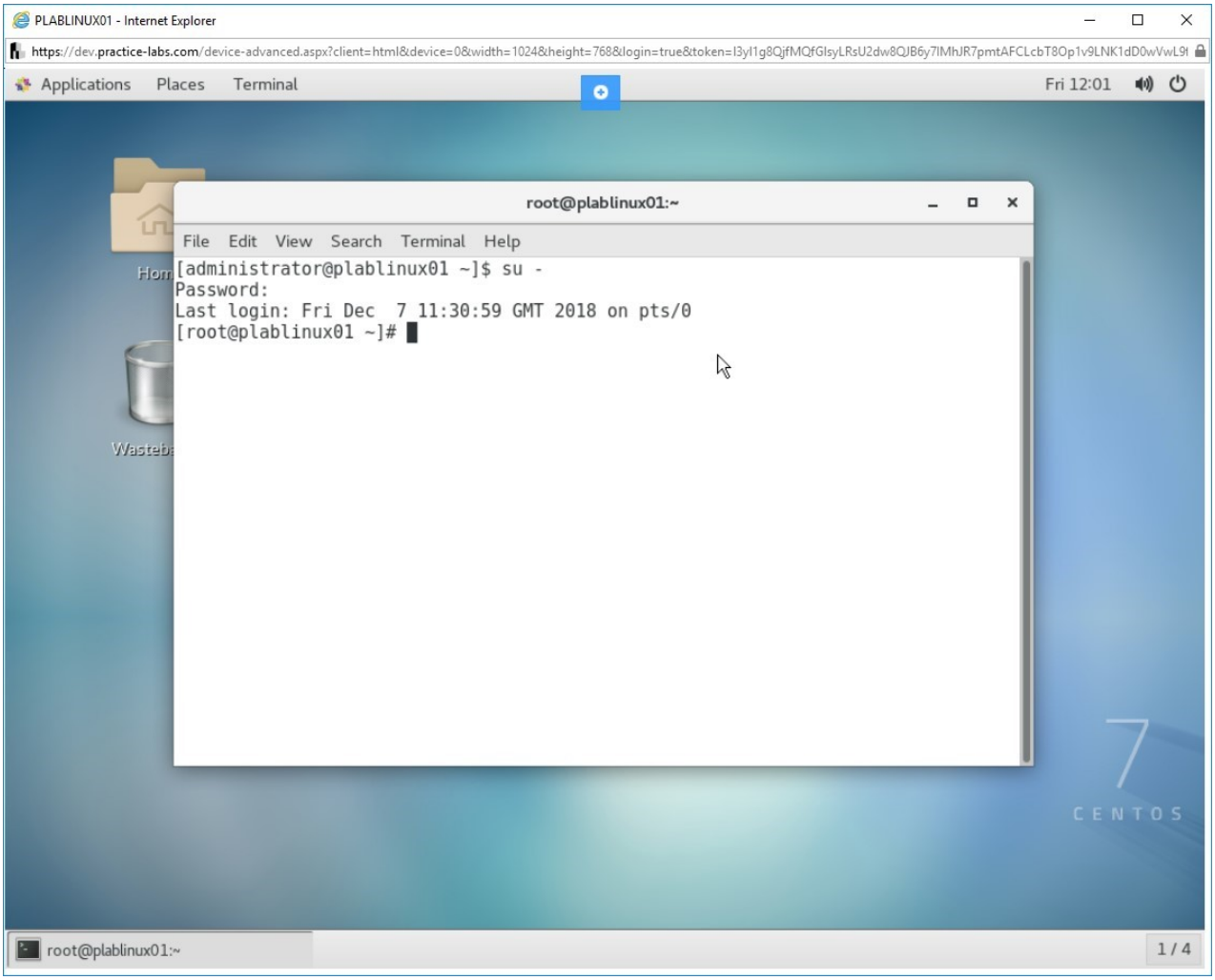


Figure 1.7 Screenshot of PLABLINUX01: Changing the account to the root account with the su command.

Step 3

Clear the screen by entering the following command:

```
clear
```

To see the current status of SELinux, type the following command:

```
getenforce
```

Press **Enter**. The current status of SELinux is displayed.

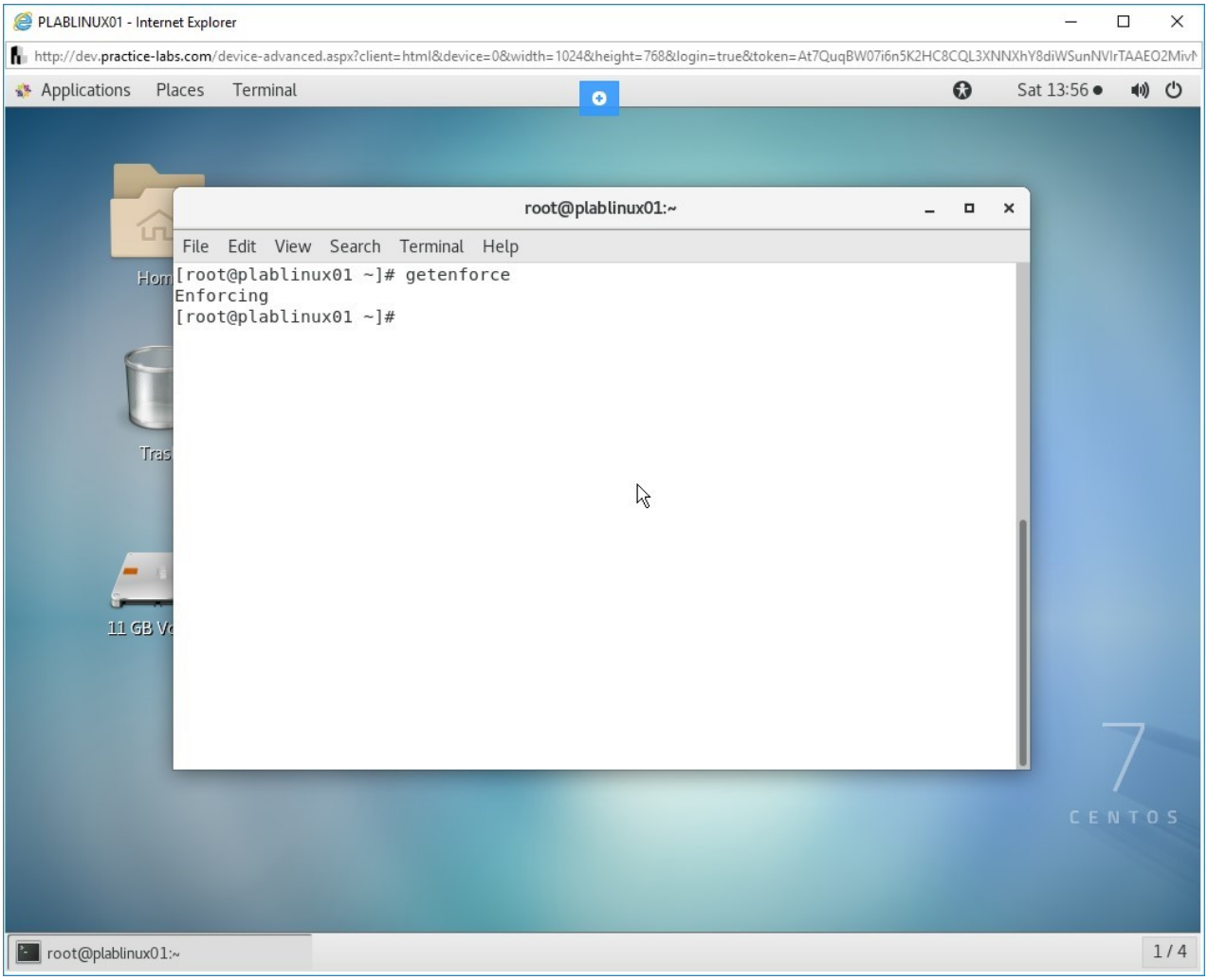


Figure 1.8 Screenshot of PLABLINUX01: Verifying the current status of SELinux.

Step 4

You can also get an overview of the SELinux configuration. Type the following command:

```
sestatus
```

Press **Enter**. The overview of SELinux configuration is displayed.

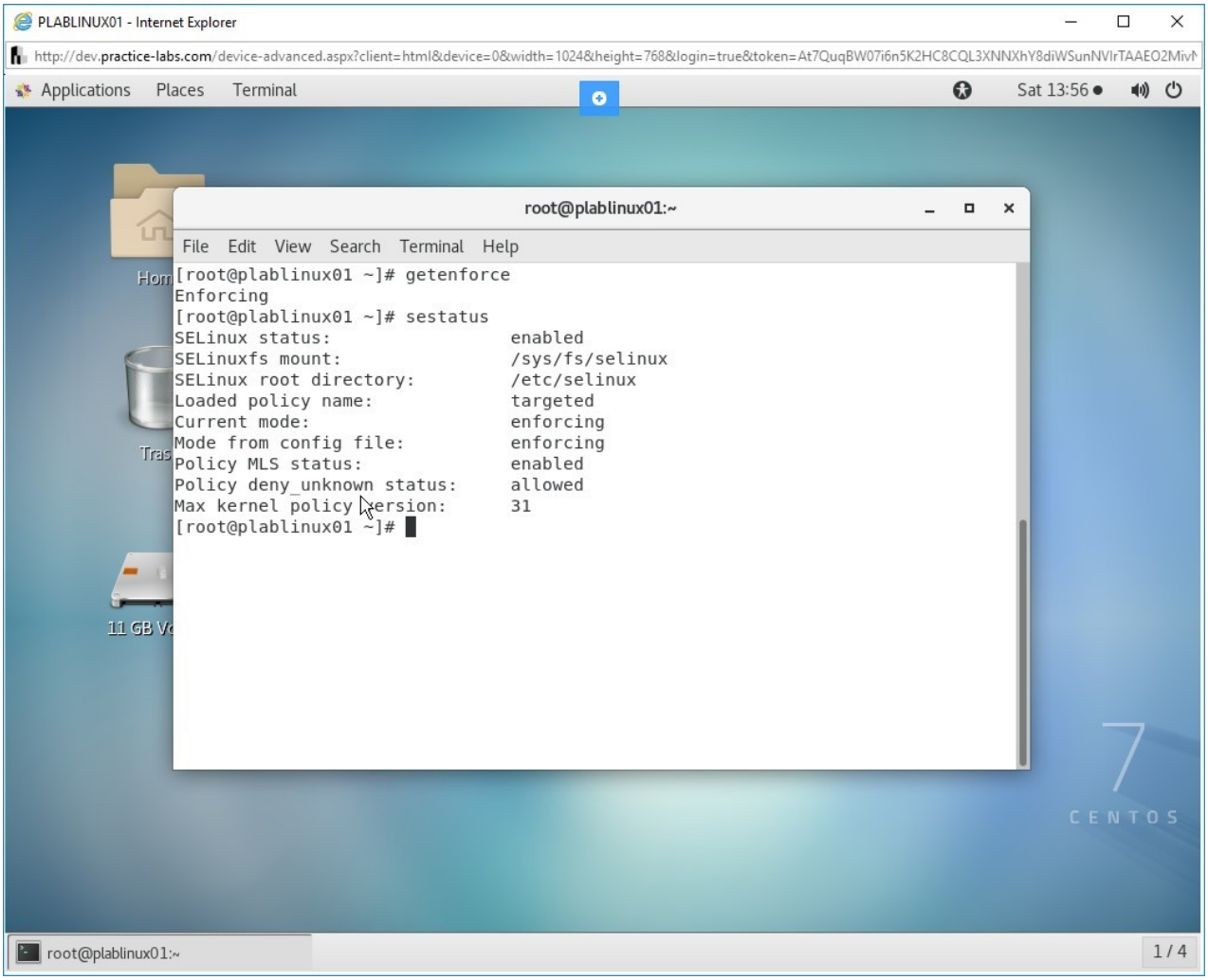


Figure 1.9 Screenshot of PLABLINUX01: Checking the SELinux configuration.

Step 5

Clear the screen by entering the following command:

```
clear
```

You can also get an overview of the SELinux configuration in the **/etc/selinux/config** file. Type the following command:

```
cat /etc/selinux/config
```

Press **Enter**. The overview of SELinux configuration is displayed.

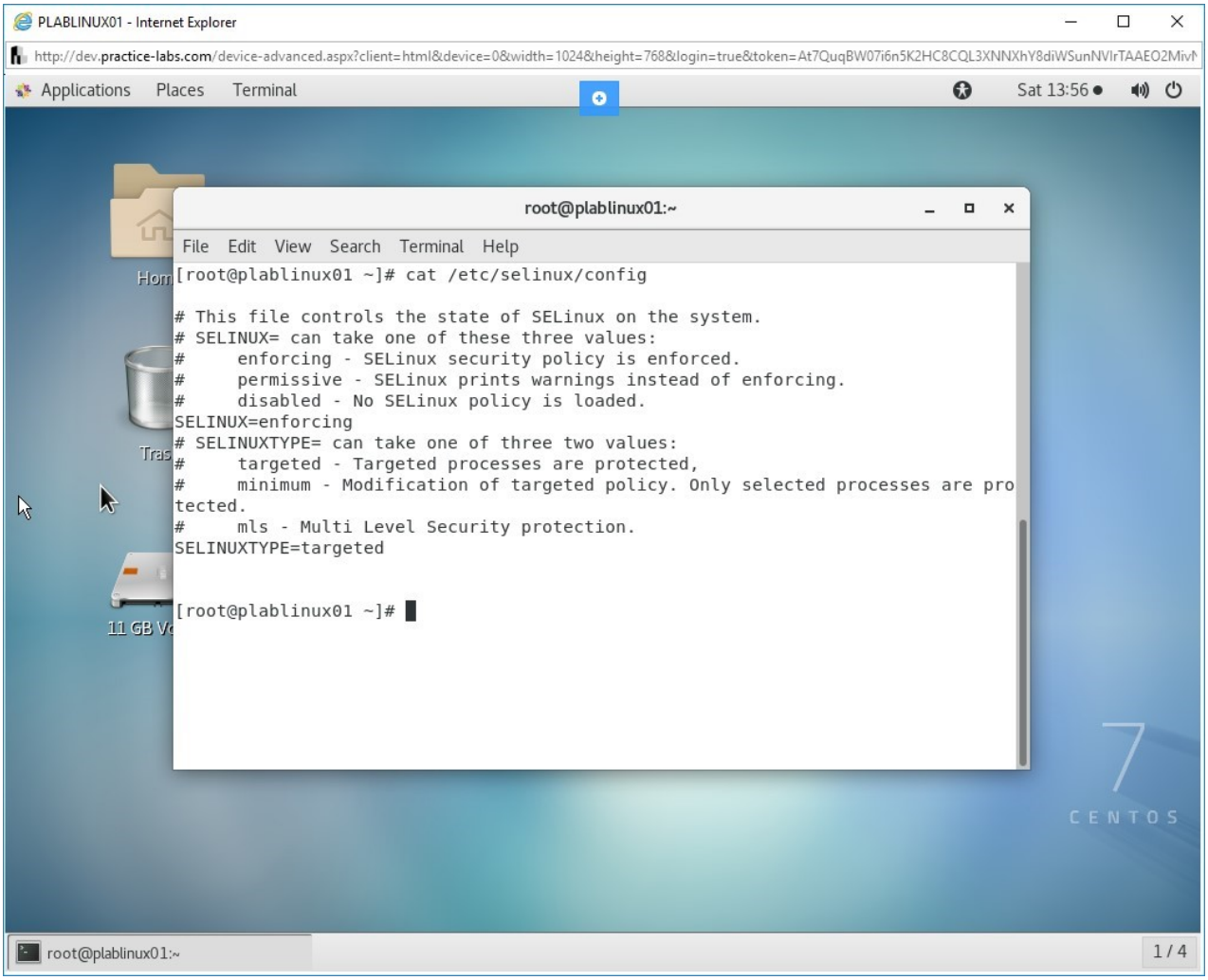


Figure 1.10 Screenshot of PLABLINUX01: Viewing the /etc/selinux/config file.

Task 3 - Change the SELinux Mode

You can also toggle between Enforcing and Permissive modes.

In this task, you will learn to toggle between two modes of SELinux. To change the SELinux modes, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

By default, Enforcing is the default mode. To change the mode to Permissive, type the following command:

```
setenforce 0
```

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

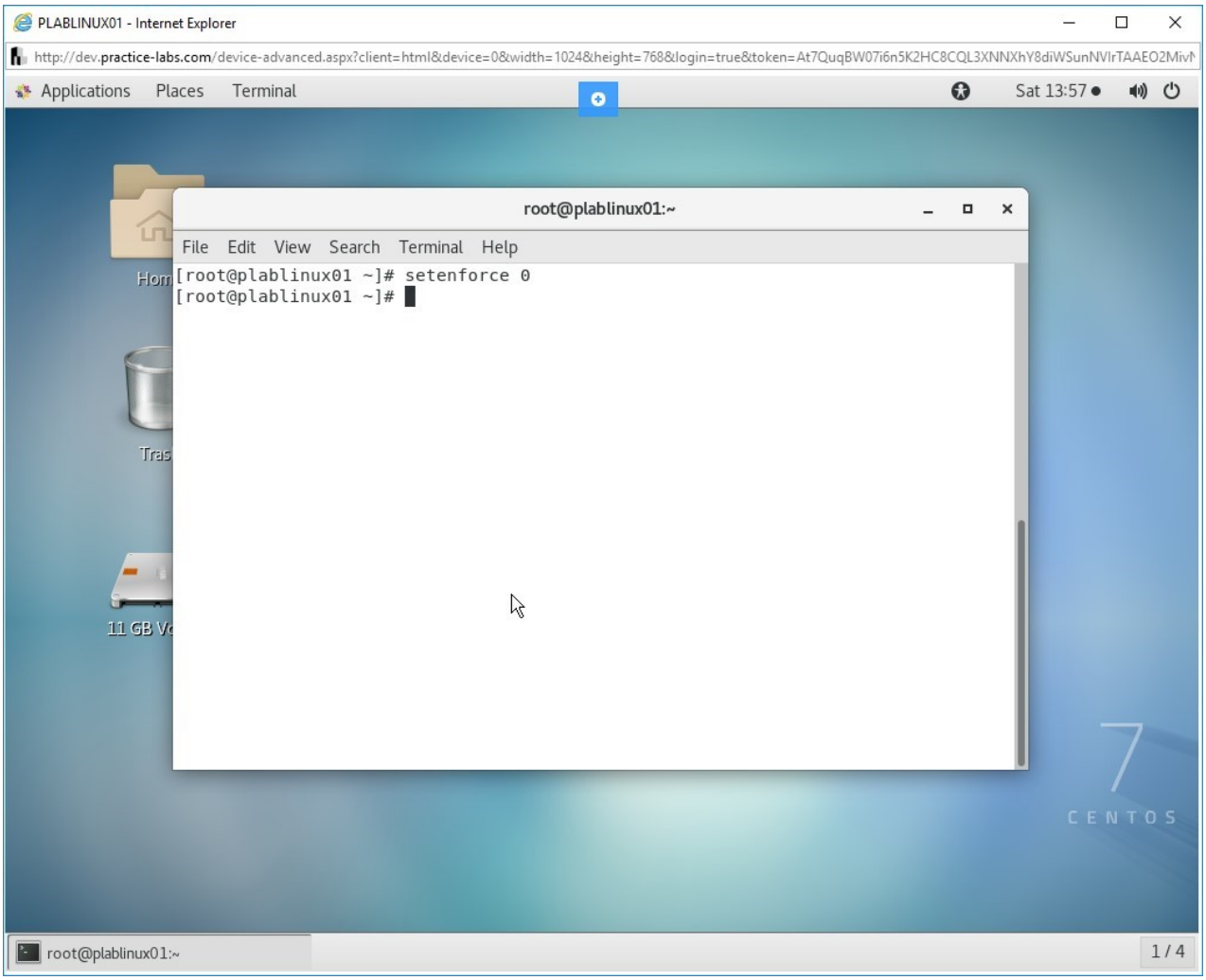


Figure 1.11 Screenshot of PLABLINUX01: Changing the SELinux mode to Permissive.

Step 2

You can verify the changed mode using the **sestatus** command. Type the following command:

```
sestatus
```

Press **Enter**. Notice that the mode is now changed. This is only the temporary change until the time the system reboots. After the system reboots, the mode in the /etc/selinux/config file will be used. To make the change permanent, you should change the /etc/selinux/config file.

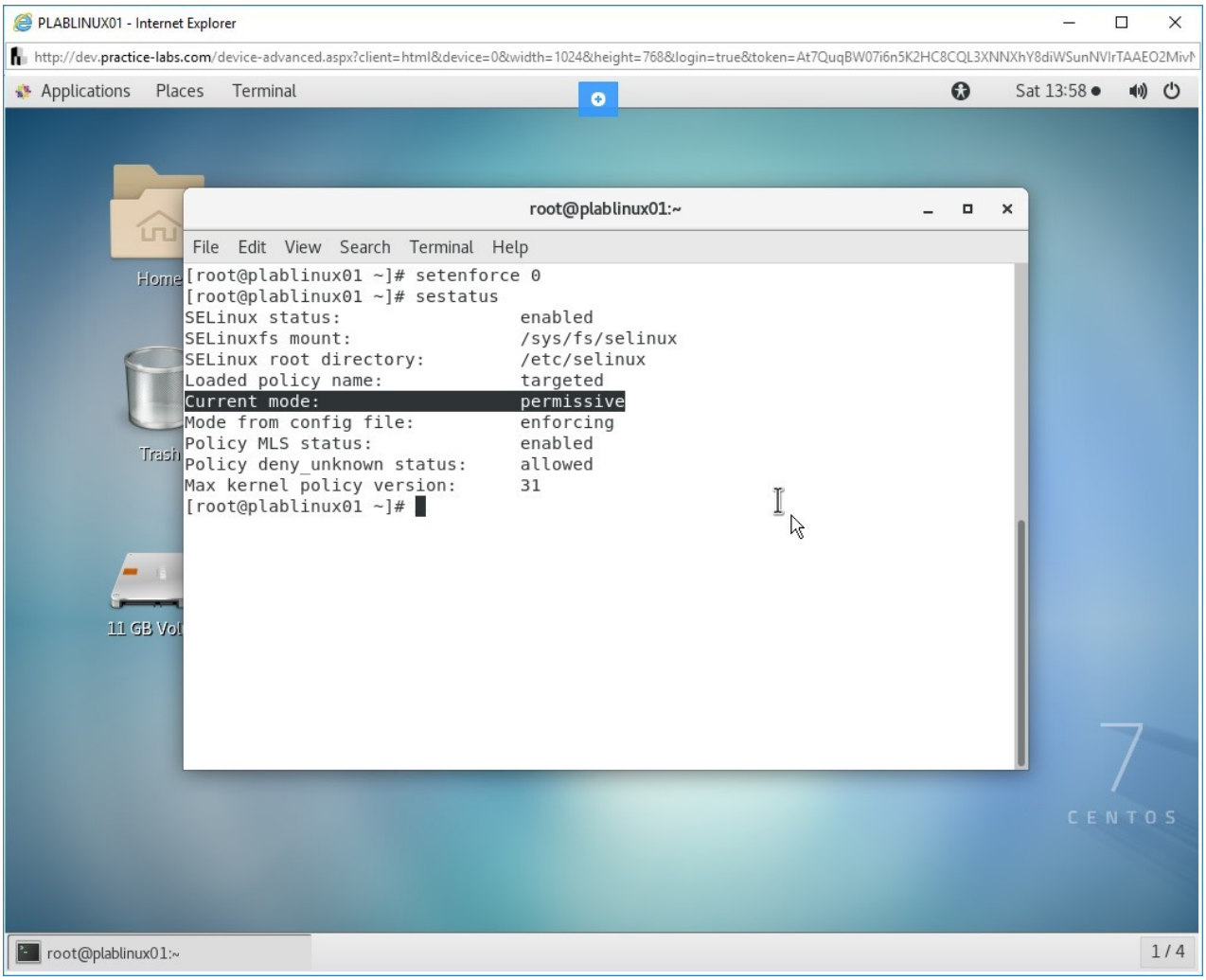


Figure 1.12 Screenshot of PLABLINUX01: Verifying the changed mode using the sestatus command.

Step 3

You can verify the changed mode using the **getenforce** command. Type the following command:

```
getenforce
```

Press **Enter**. Notice that the mode is now changed. This is only the temporary change until the time the system reboots. After the system reboots, the mode in the

/etc/selinux/config file will be used. To make the change permanent, you should change the /etc/selinux/config file.

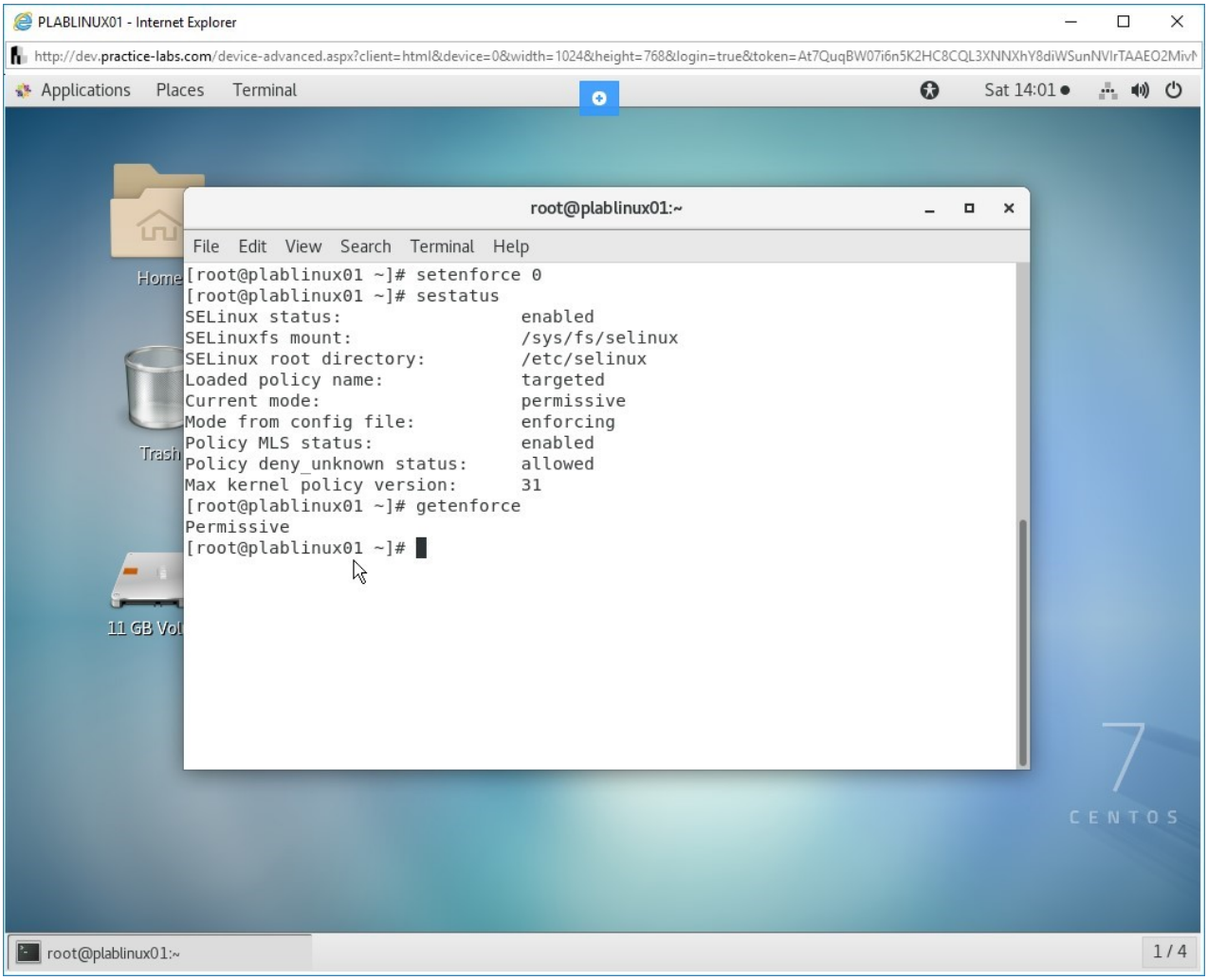


Figure 1.13 Screenshot of PLABLINUX01: Verifying the changed mode using the getenforce command.

Step 4

Clear the screen by entering the following command:

```
clear
```

To change the mode of Enforcing, you will again use the **setenforce** command. Type the following command:

```
setenforce 1
```

Press **Enter**.

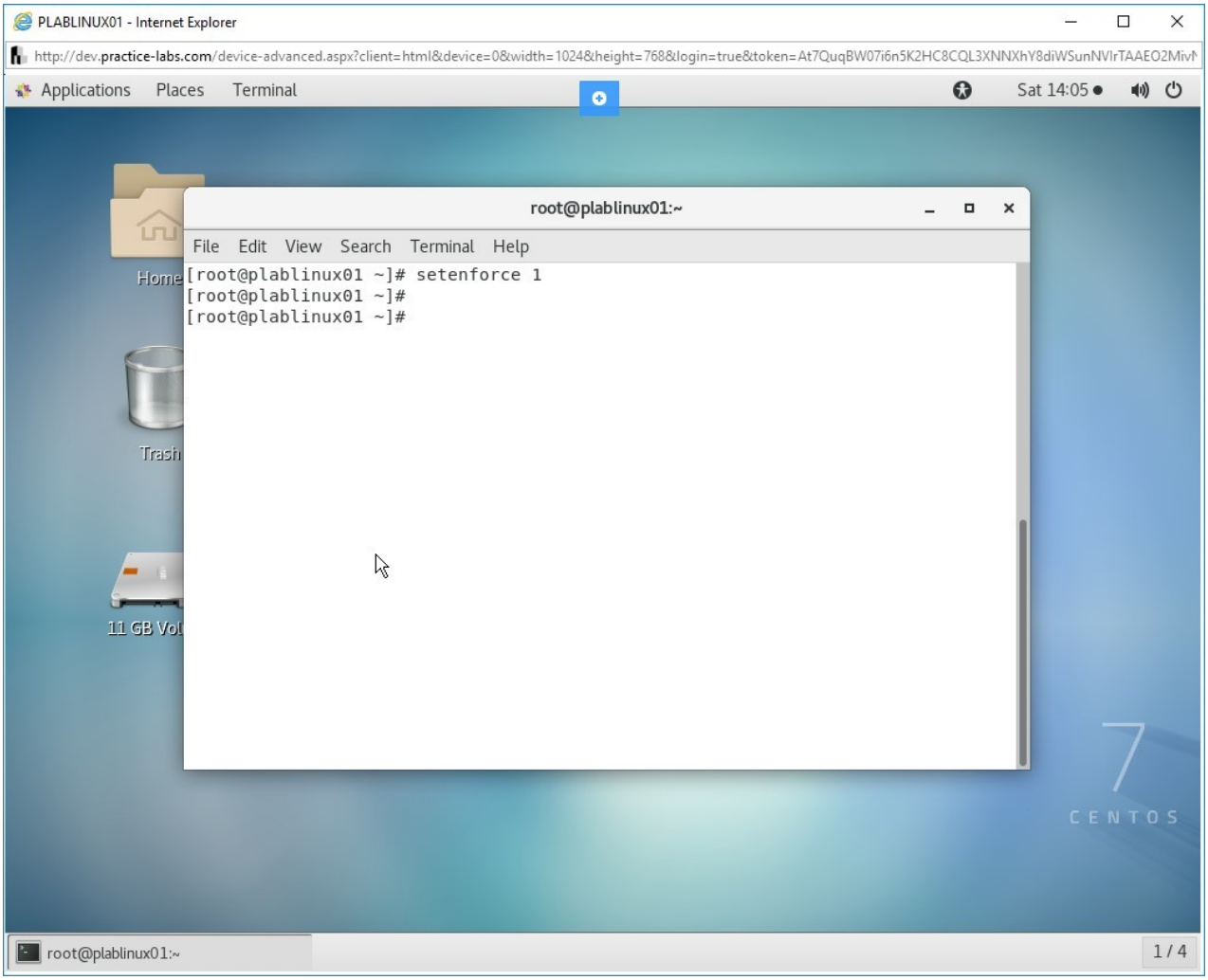


Figure 1.14 Screenshot of PLABLINUX01: Changing the mode to Enforcing.

Step 5

You can verify the changed mode once again. Type the following command:

```
getenforce
```

Press **Enter**. Notice that the mode is now changed.

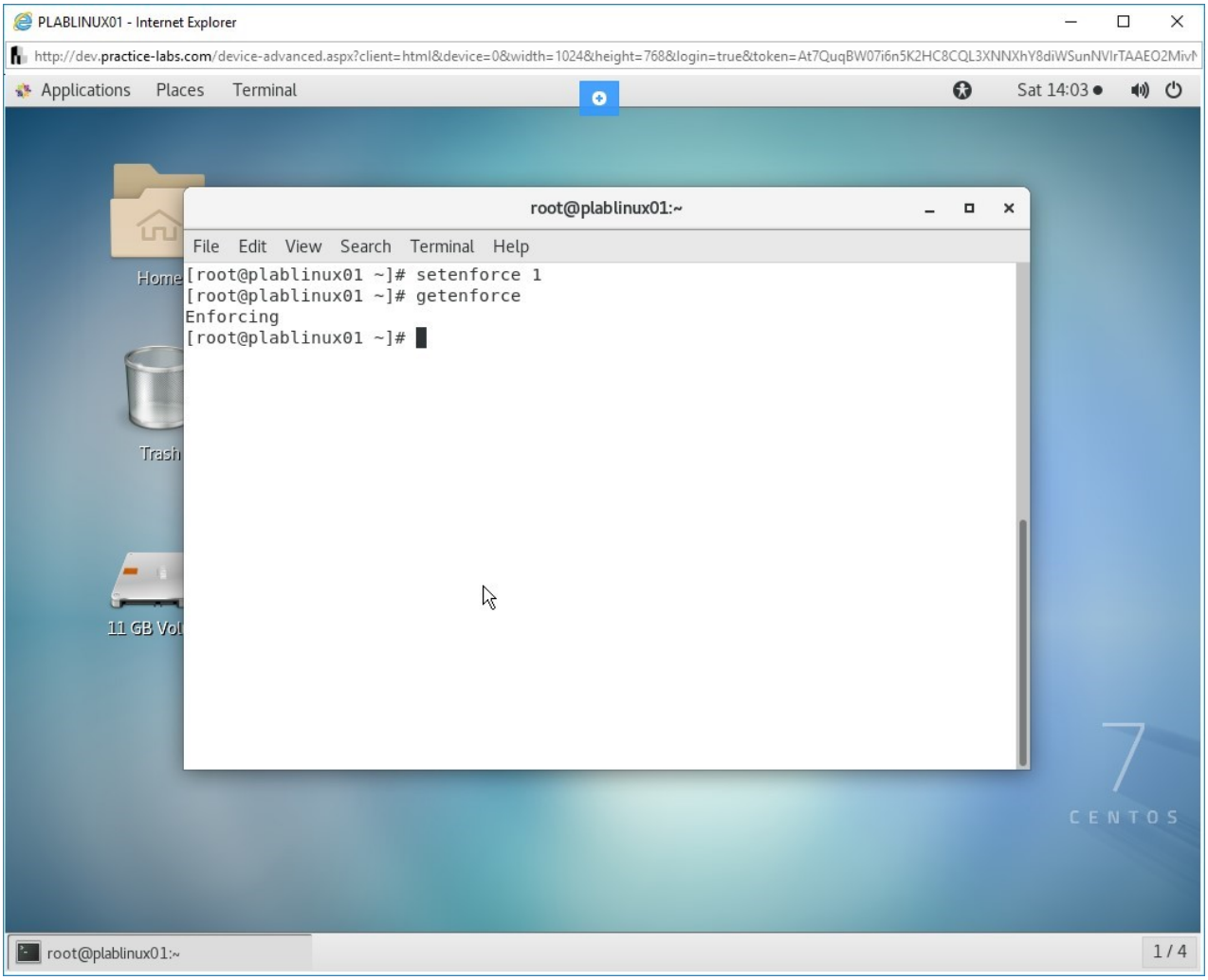


Figure 1.15 Screenshot of PLABLINUX01: Verifying the changed mode once again.

Task 4 - View SELinux Contexts for Processes, Domain Transitions, and Users

Each process and file is marked with an SELinux context, which contains additional information, such as:

- SELinux user
- Role
- Type
- Level

The SELinux context information is used for making access control decisions.

To view SELinux contexts for the processes, domain transitions, and users, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

Create a new file named **plab.txt**. Type the following command:

```
touch plab.txt
```

Press **Enter**.

You can view the security context of the file **plab.txt**. Type the following command:

```
ls -Z plab.txt
```

Press **Enter**. Notice that the output displays the **user:role:type:level** information.

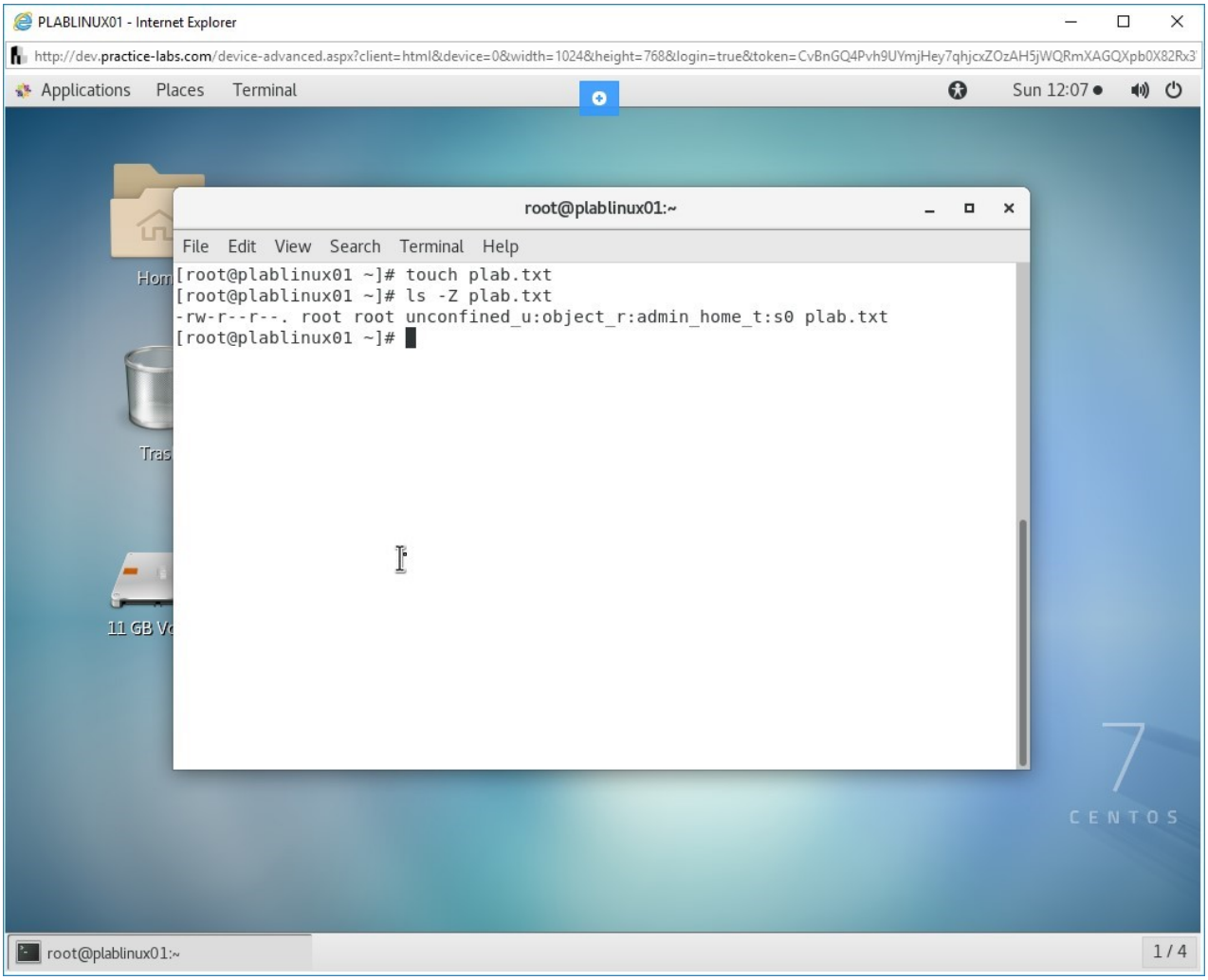


Figure 1.16 Screenshot of PLABLINUX01: Checking the security context of the plab.txt file.

Step 2

Clear the screen by entering the following command:

```
clear
```

You can also view a list of mappings between SELinux and Linux user accounts. Type the following command:

```
semanage login -l
```

Press **Enter**.

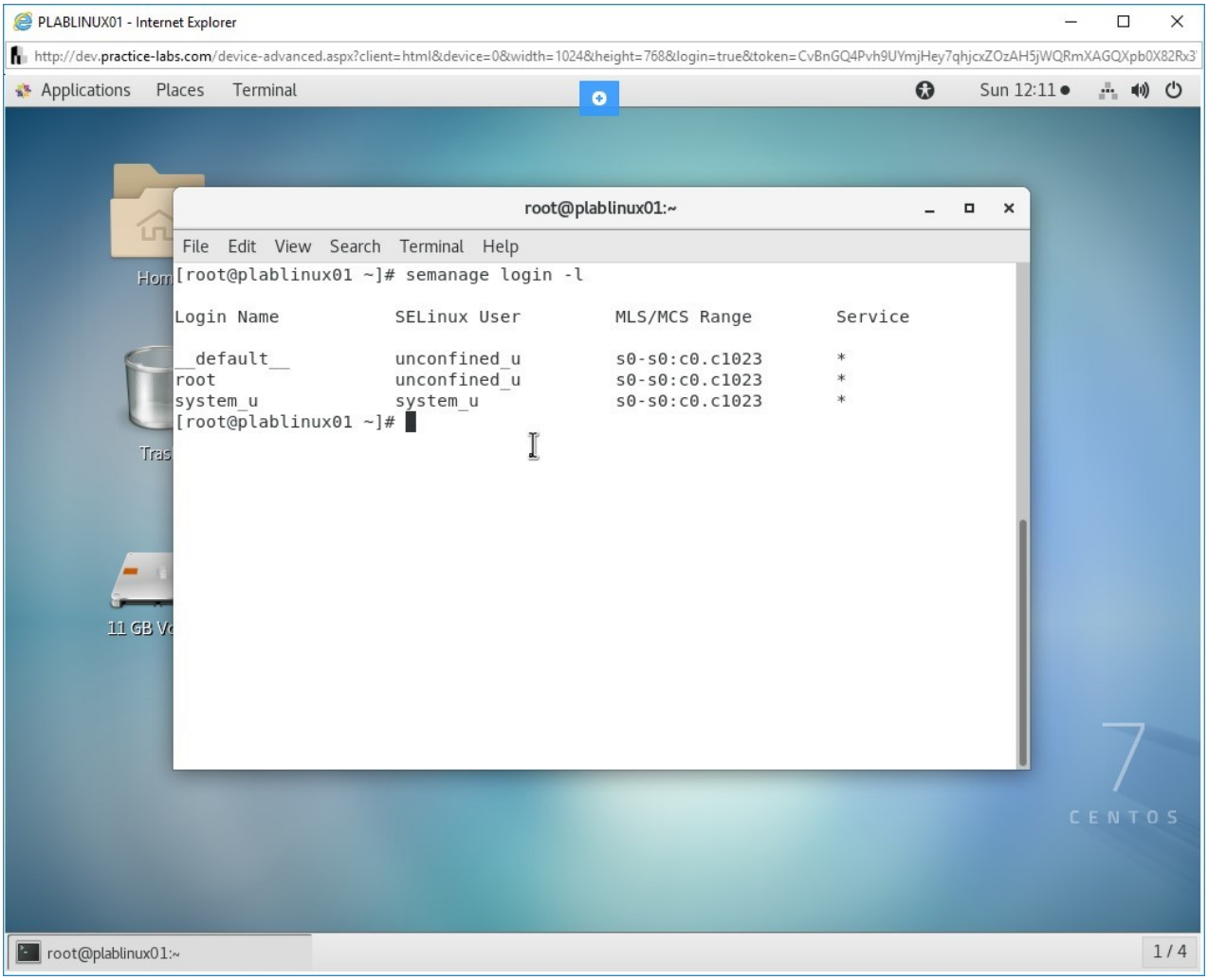


Figure 1.17 Screenshot of PLABLINUX01: Viewing a list of mappings between SELinux and Linux user accounts.

Step 3

Each application in Linux has an **entrypoint** permission, which is used by the SELinux policy. The **entrypoint** permission controls which applications can be used to enter a domain. For example, The **/usr/bin/passwd** executable is marked with the **passwd_exec_t** label. Type the following command:

```
ls -Z /usr/bin/passwd
```

Press **Enter**. Notice the label, **passwd_exec_t**.

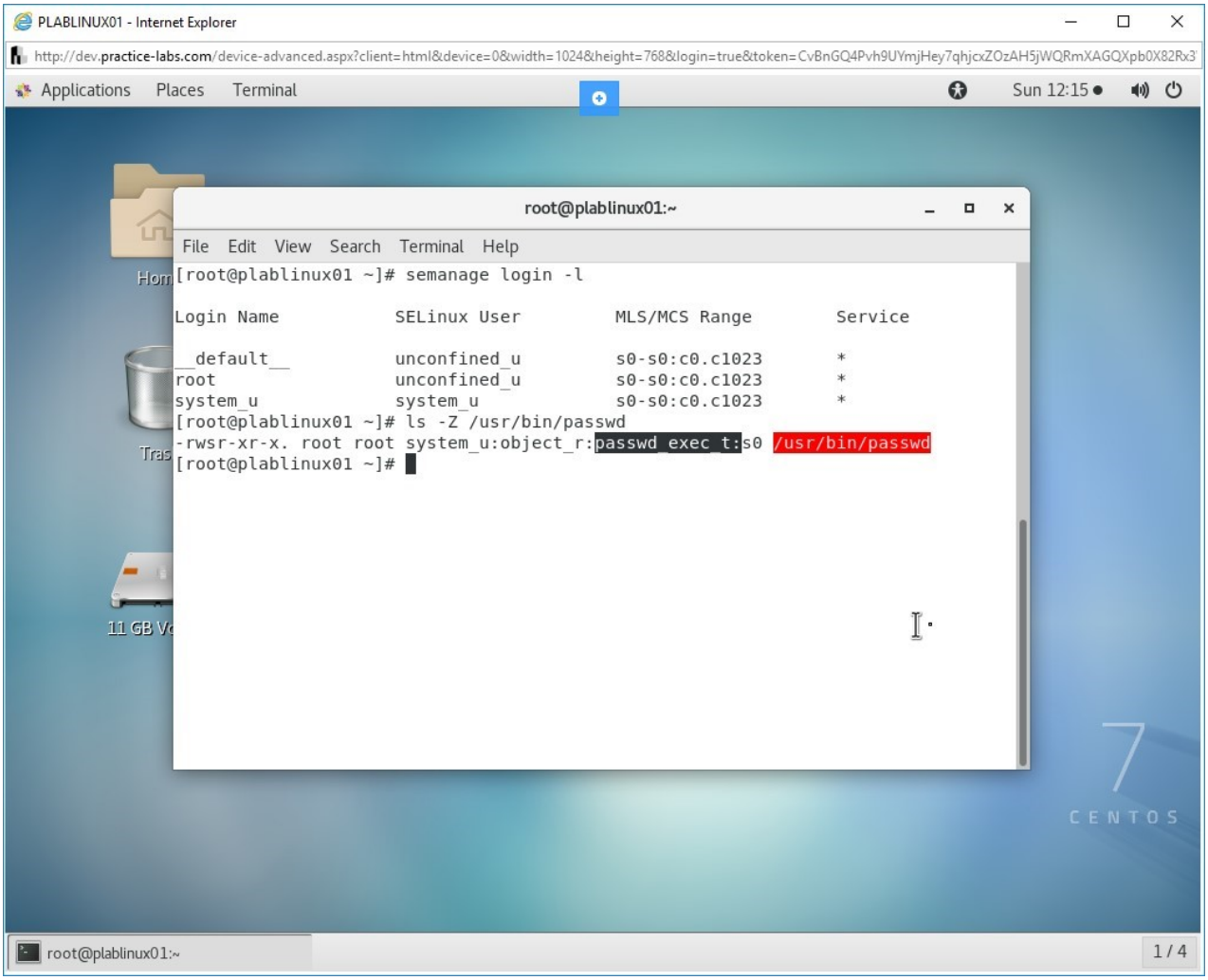


Figure 1.18 Screenshot of PLABLINUX01: Verifying the label for the /usr/bin/passwd file.

Step 4

Clear the screen by entering the following command:

```
clear
```

You can view the SELinux context for processes that are running on the system. For example, type the following command:

```
passwd
```

Press **Enter**. Do not enter any password and keep the terminal window open.

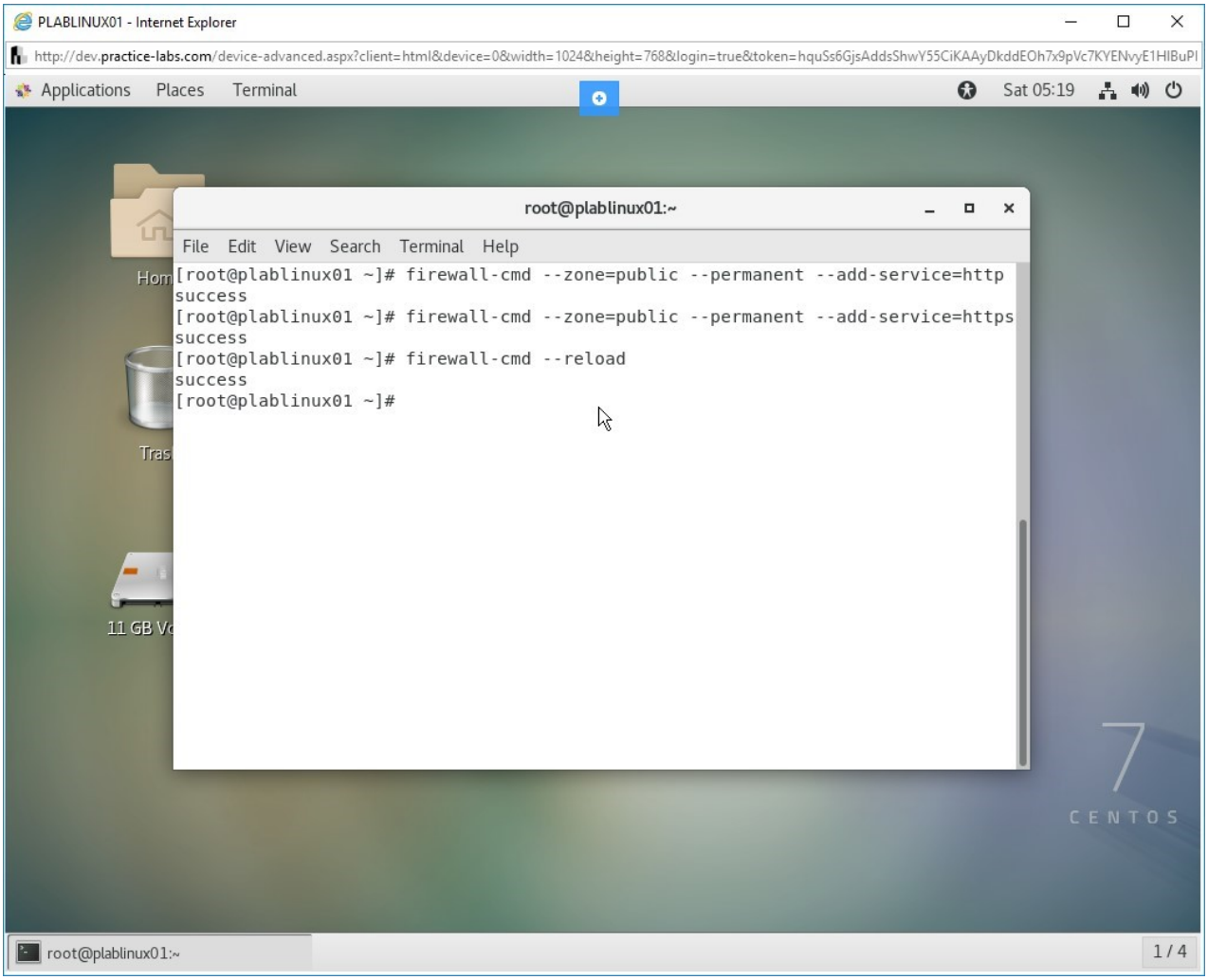


Figure 1.19 Screenshot of PLABLINUX01: Viewing the SELinux context for processes that are running on the system.

Step 5

Open a new terminal window. You will now view the security context for the **passwd** process. Type the following command:

```
ps -eZ | grep passwd
```

Press **Enter**. Do not enter any password and keep the terminal window open.

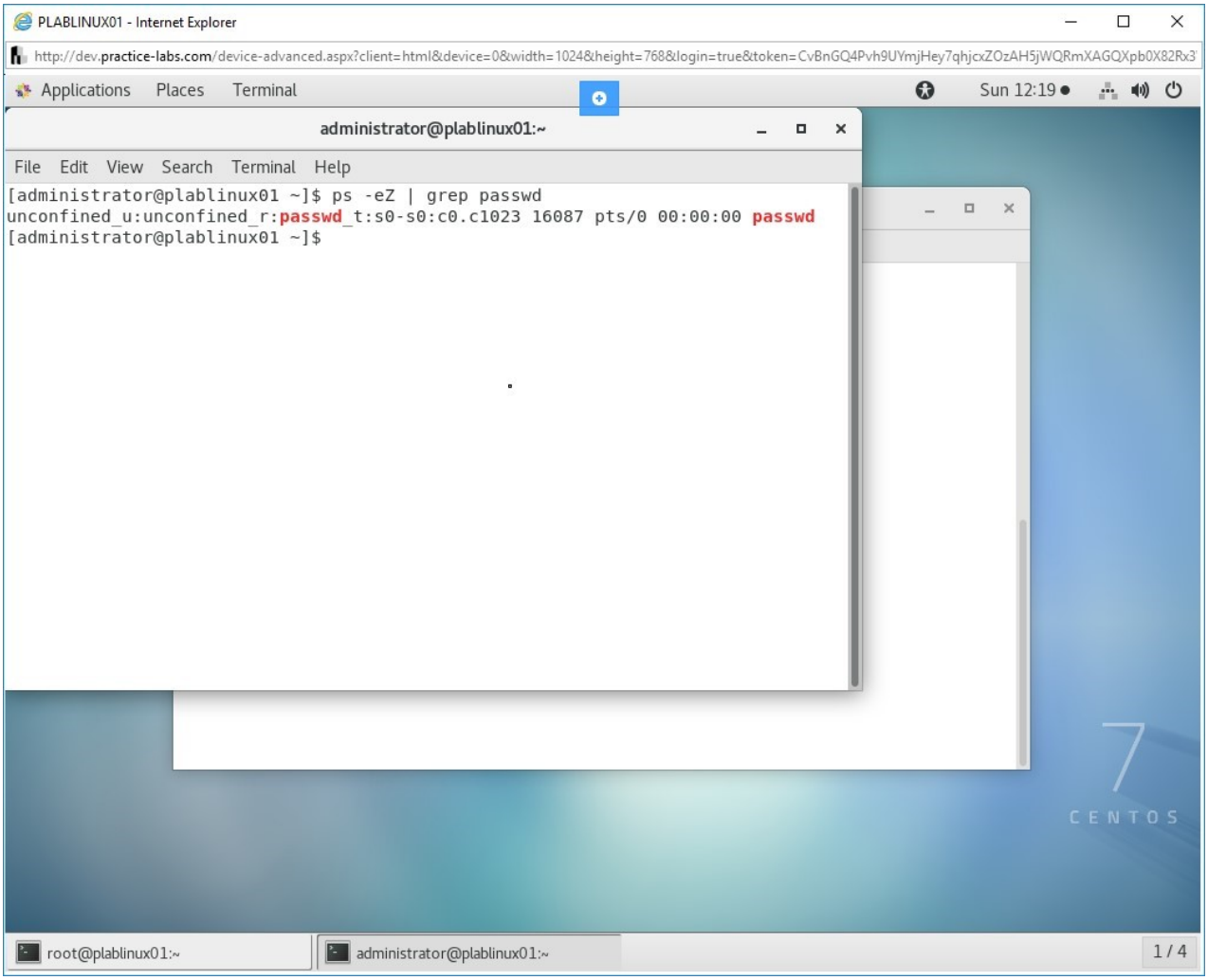


Figure 1.20 Screenshot of PLABLINUX01: Viewing the security context for the passwd process.

Step 6

Go back to the first terminal window where entered the passwd command. Press **Ctrl + C.**

Go back to the second terminal window. Type the following command:

```
ps -eZ
```

Press **Enter**. You will see the SELinux contexts for running processes.

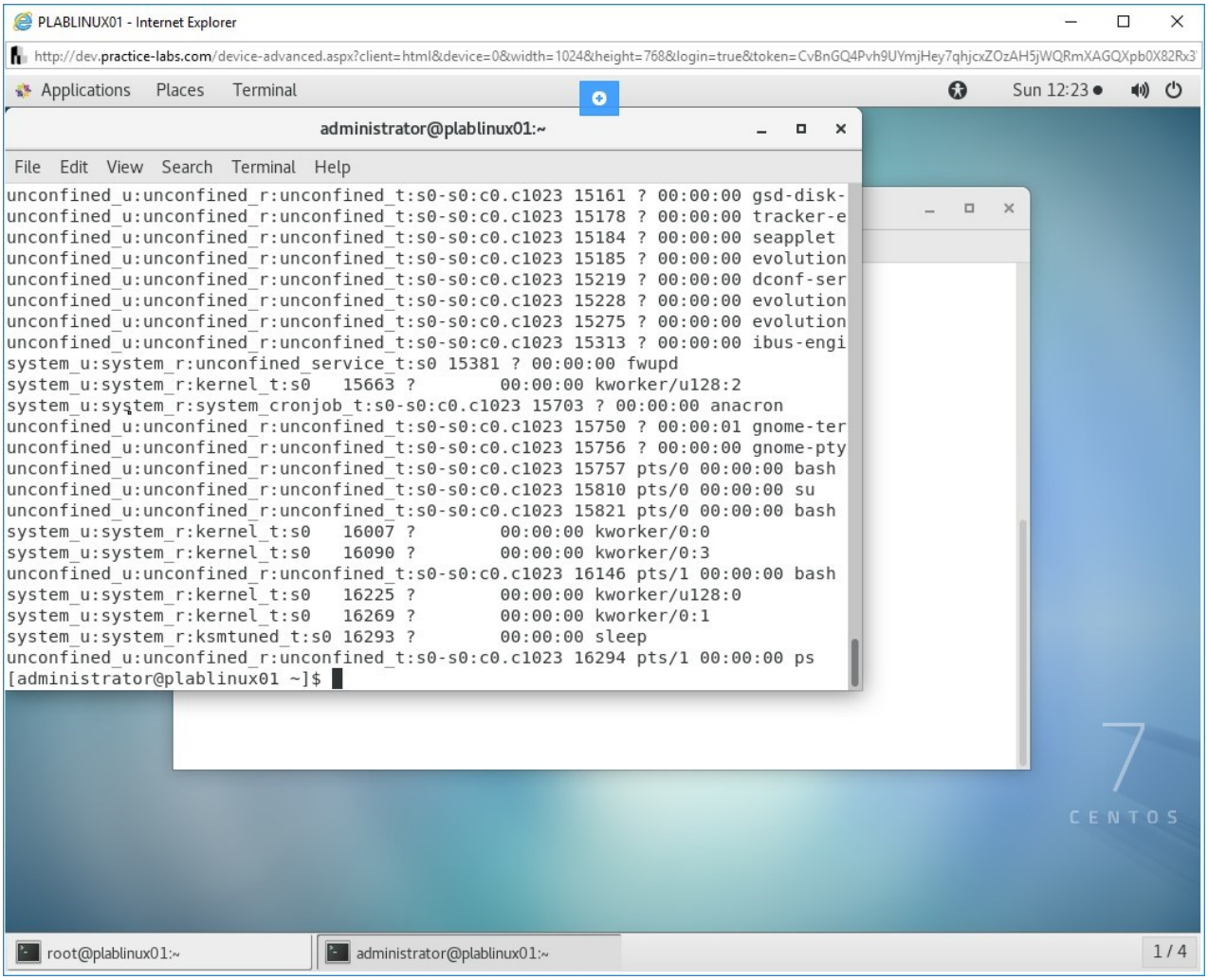


Figure 1.21 Screenshot of PLABLINUX01: Viewing the SELinux contexts for running processes.

Step 7

Go back to the first terminal window.

Clear the screen by entering the following command:

```
clear
```

You can view the security context for the user. Type the following command:

```
id -Z
```

Press **Enter**. In CentOS, users are marked with unconfined_u. They also run with the unconfined_r role. The output of this command displays this. It also shows the user is running in the unconfined_t domain.

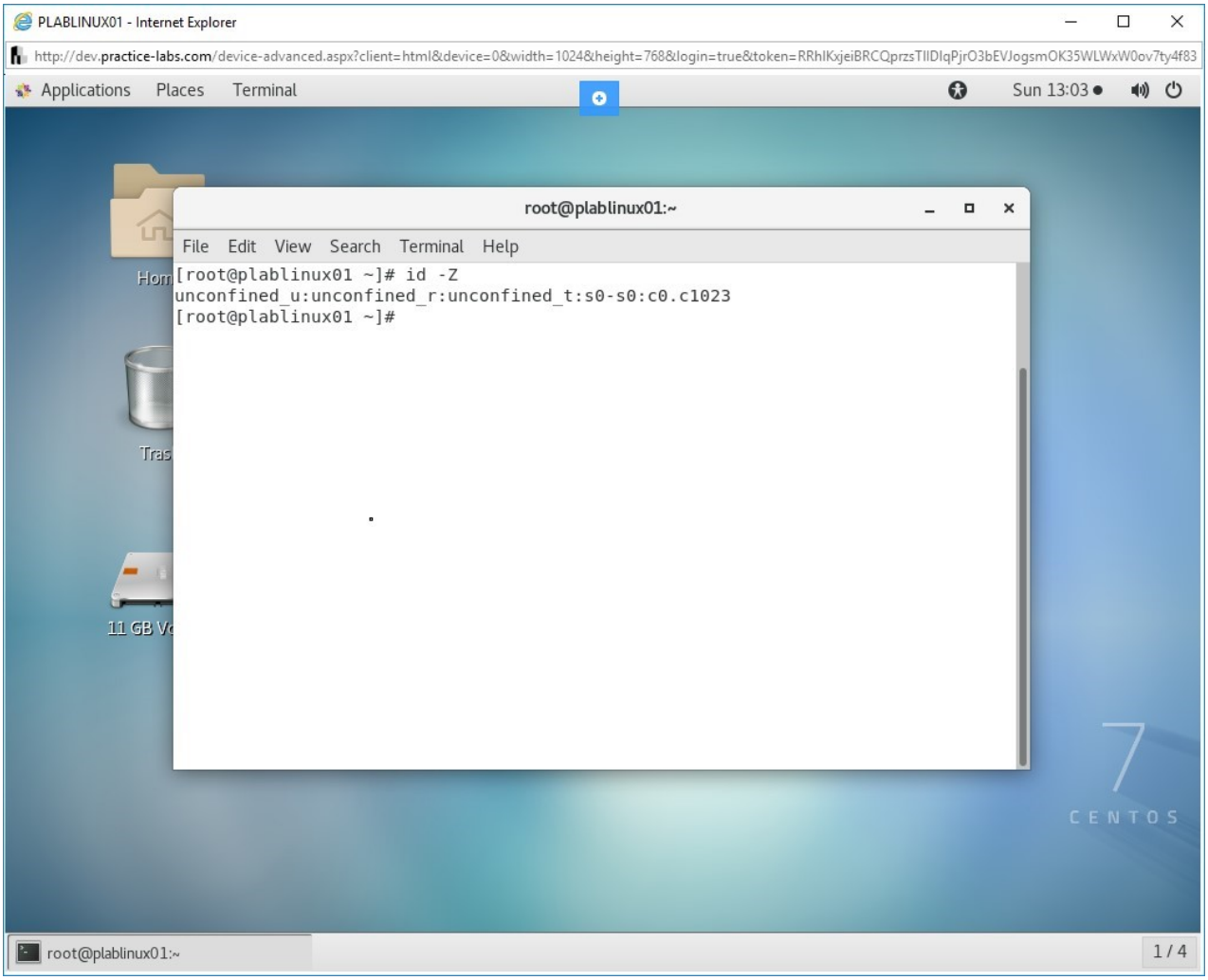


Figure 1.22 Screenshot of PLABLINUX01: Viewing the security context for the user.

Task 5 - Install and Use the policycoreutils-gui Package

It is a pretty tedious task to manage SELinux in the command line environment. To make life easy, you can install the policycoretutils-gui package, which provides a graphical environment for you to manage SELinux. In this task, you will test the install the policycoreutils-gui package.

To install the policycoreutils-gui package, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

Type the following command:

```
yum install policycoreutils-gui
```

Press **Enter**.

When prompted for confirmation, type the following:

```
y
```

Press **Enter**.

After downloading and installing the package, you will be prompted with the Complete! message.

Minimize the command prompt window.

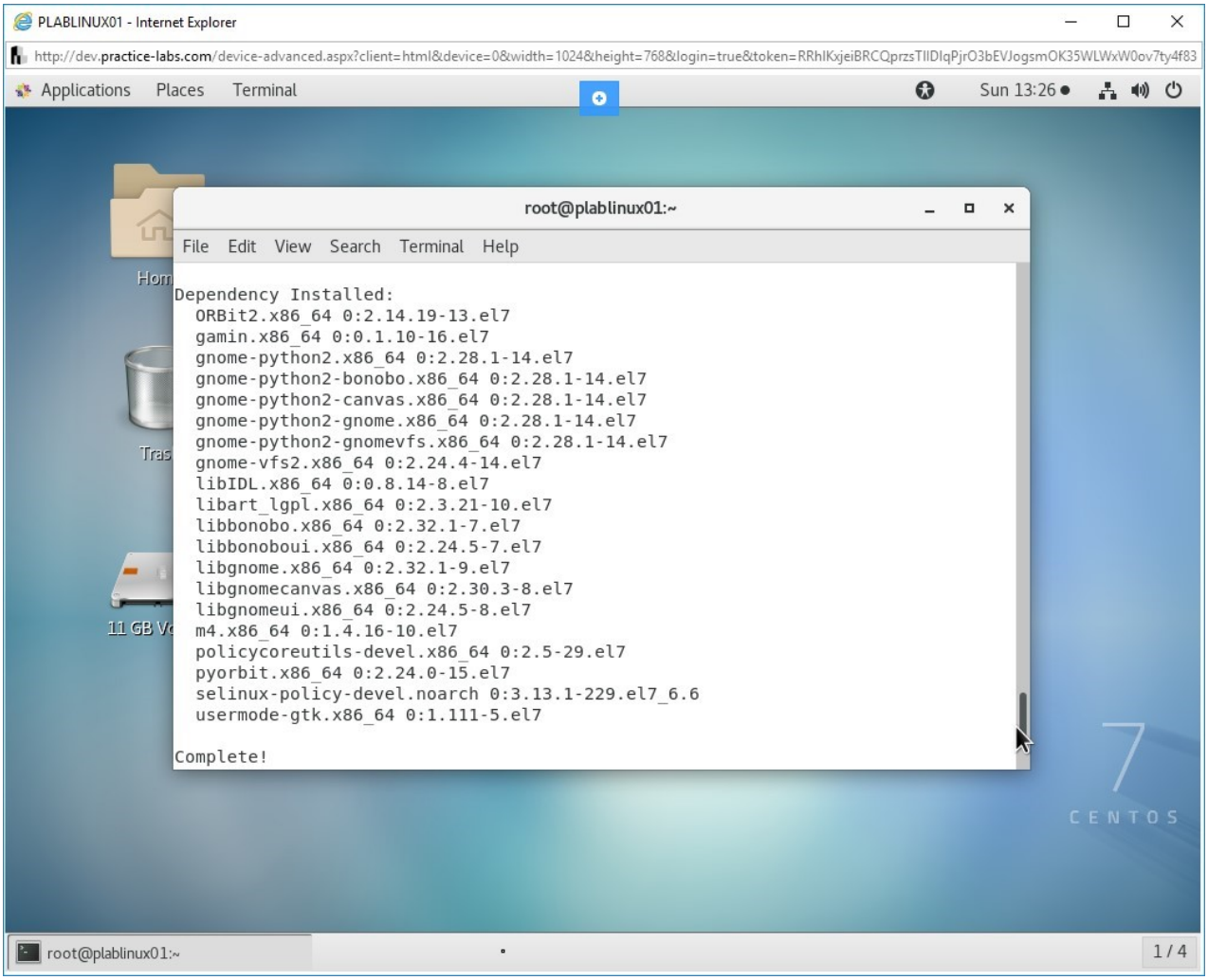


Figure 1.23 Screenshot of PLABLINUX01: Downloading the install the policycoreutils-gui package.

Step 2

Click **Applications**, select **Other** and then select **SELinux Management**.

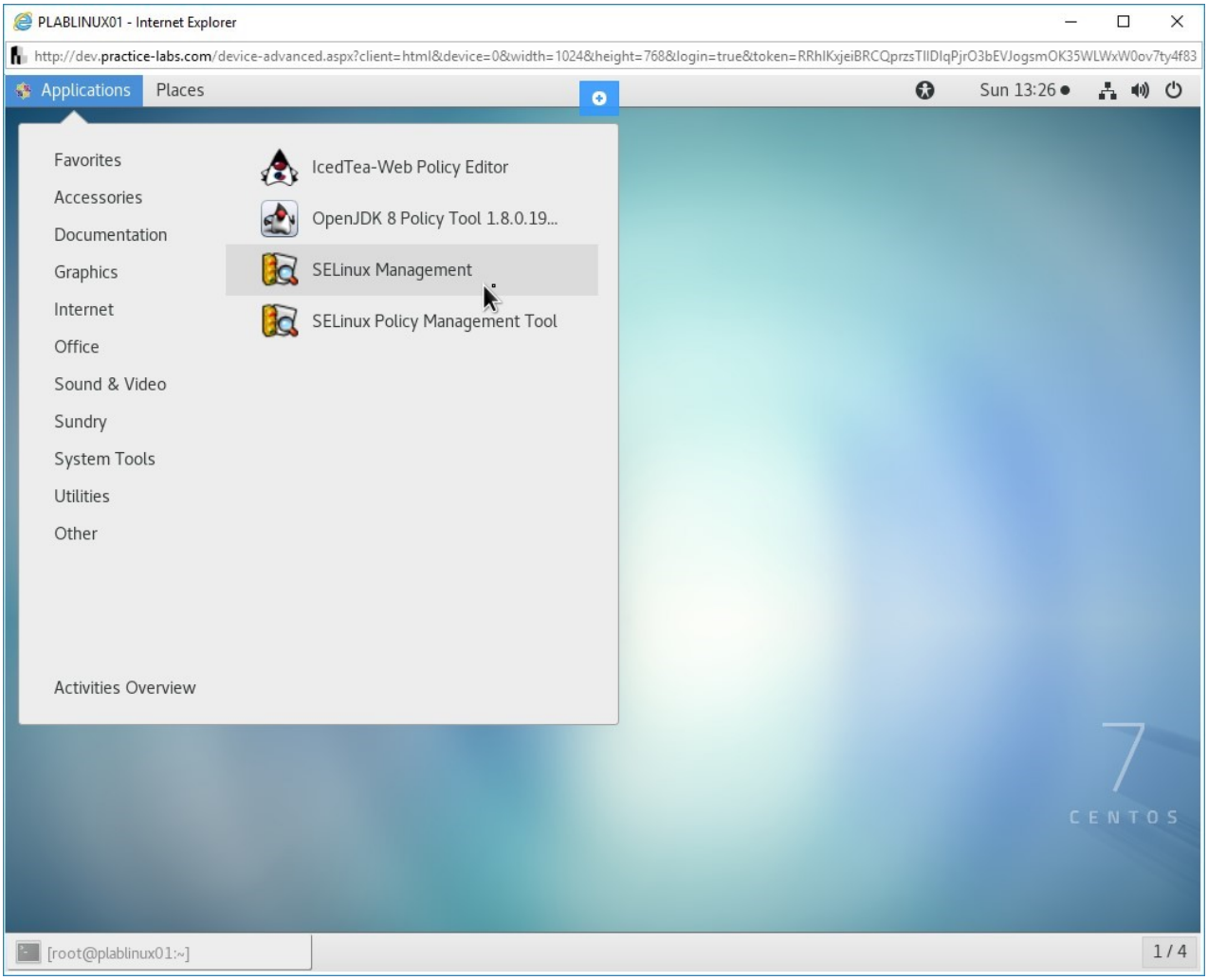


Figure 1.24 Screenshot of PLABLINUX01: Opening SELinux Management from the Application menu.

Step 3

When prompted for the password, type the following password:

```
Passw0rd
```

Click **Authenticate**.

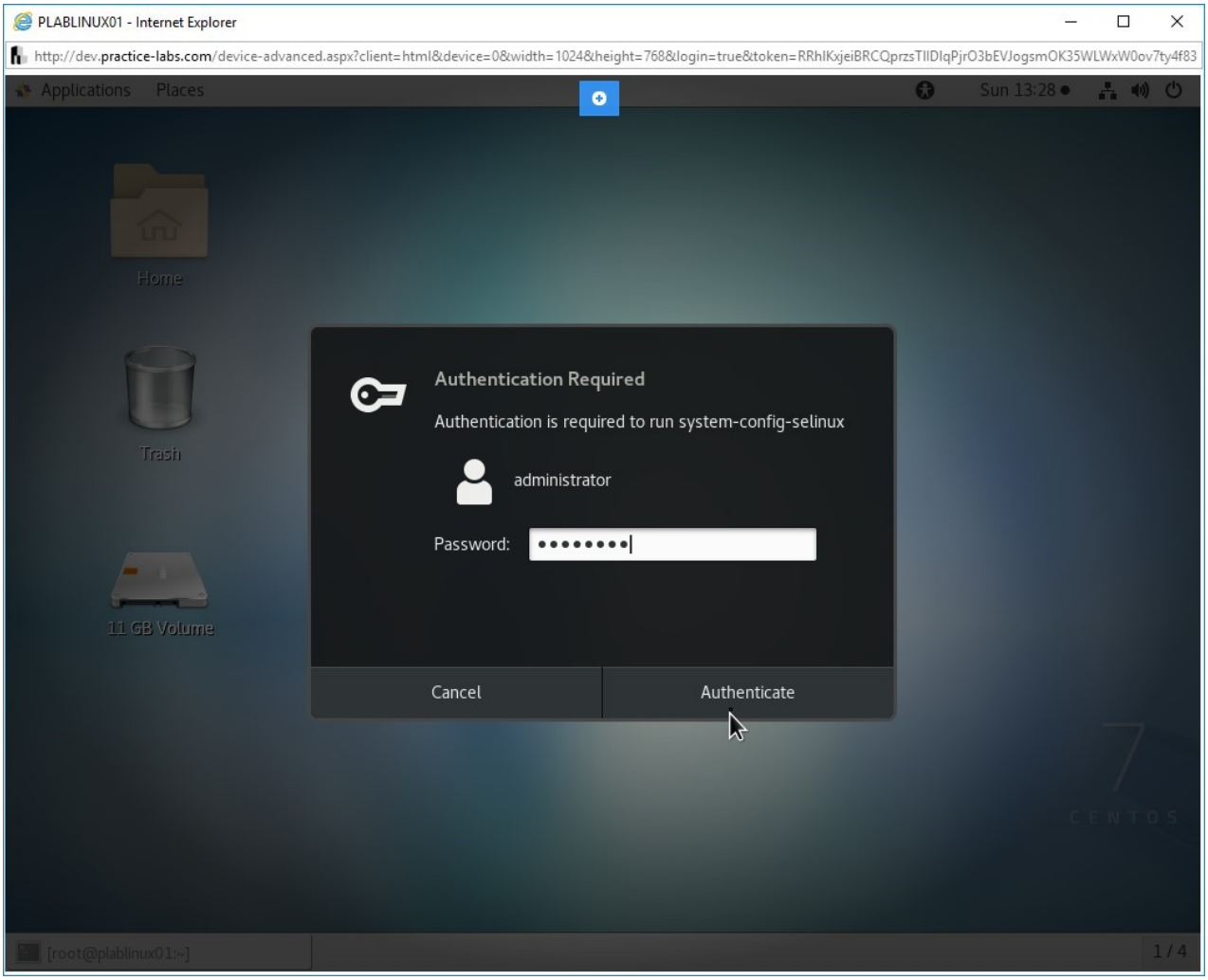


Figure 1.25 Screenshot of PLABLINUX01: Entering the password.

Step 4

The **SELinux Administration** window is displayed.

> ***Note:*** *Maximize the window if required.*

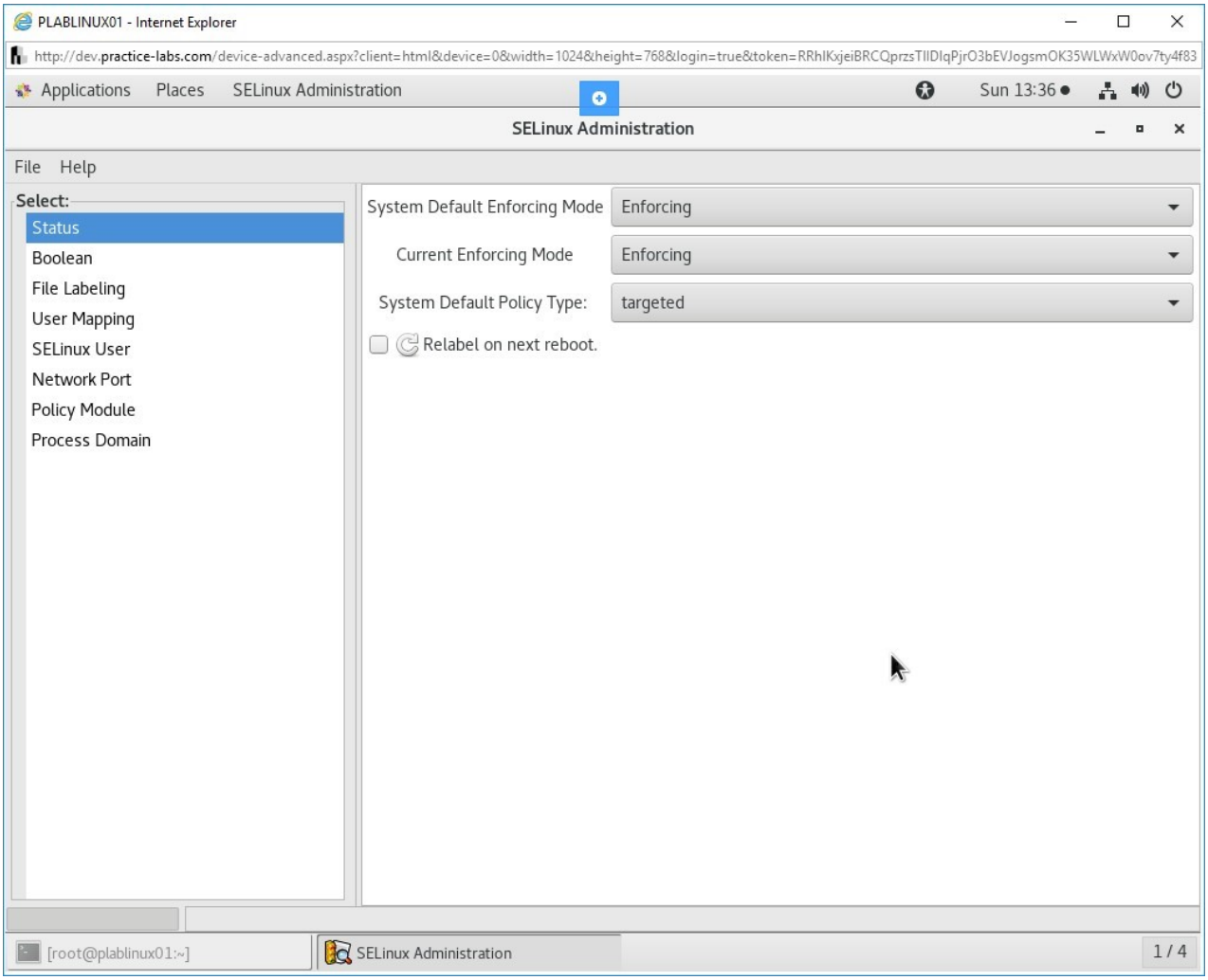


Figure 1.26 Screenshot of PLABLINUX01: Showing the Status tab in the SELinux Administration window.

Step 5

Using the **Status** tab, you can configure the mode for **SELinux**. Instead of using the **setenforce** command, you can use this tab to change the mode.

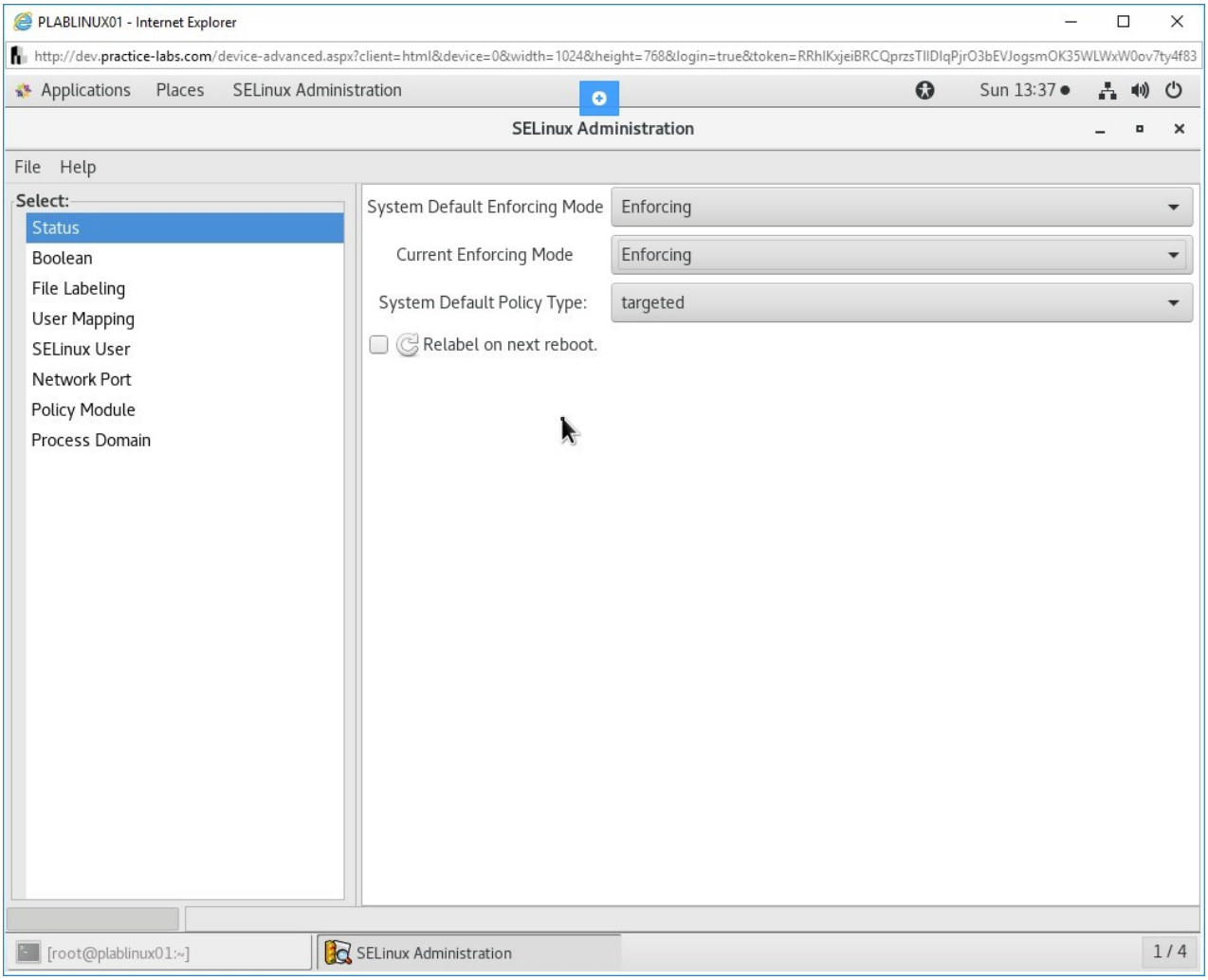


Figure 1.27 Screenshot of PLABLINUX01: Showing the Status tab in the SELinux Administration window.

Step 6

Click the **Boolean** tab. A Boolean can change the SELinux policy at the runtime, which does not require a reboot. For example, you can allow the httpd service to act as a relay service. If you choose to select this, this Boolean will change the policy, and you are not required to restart the server.

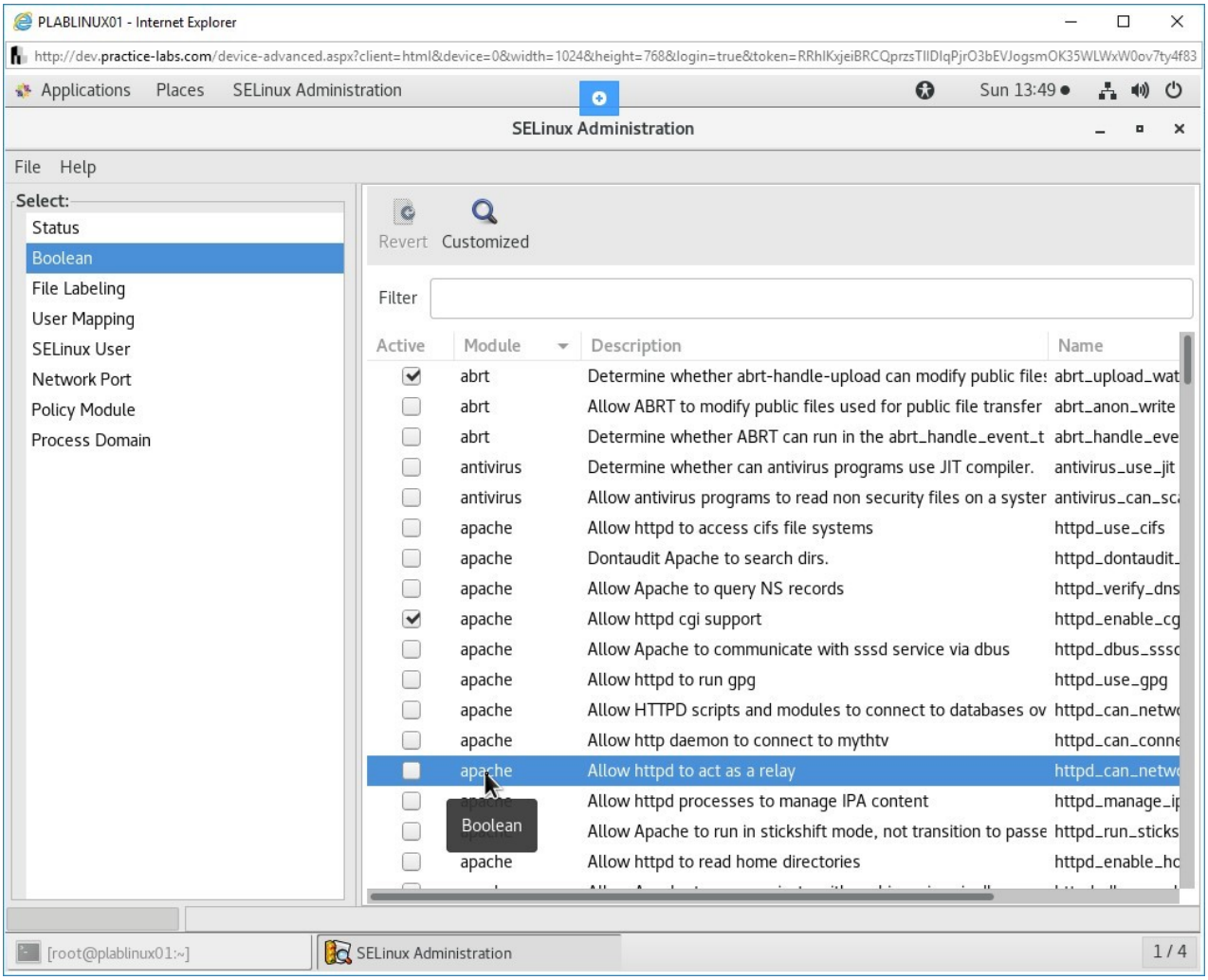


Figure 1.28 Screenshot of PLABLINUX01: Showing the Boolean tab in the SELinux Administration window.

Step 7

Click the **File Labeling** tab. A label is an extended attribute of a file. Note that each file has a label under the Selinux File Type.

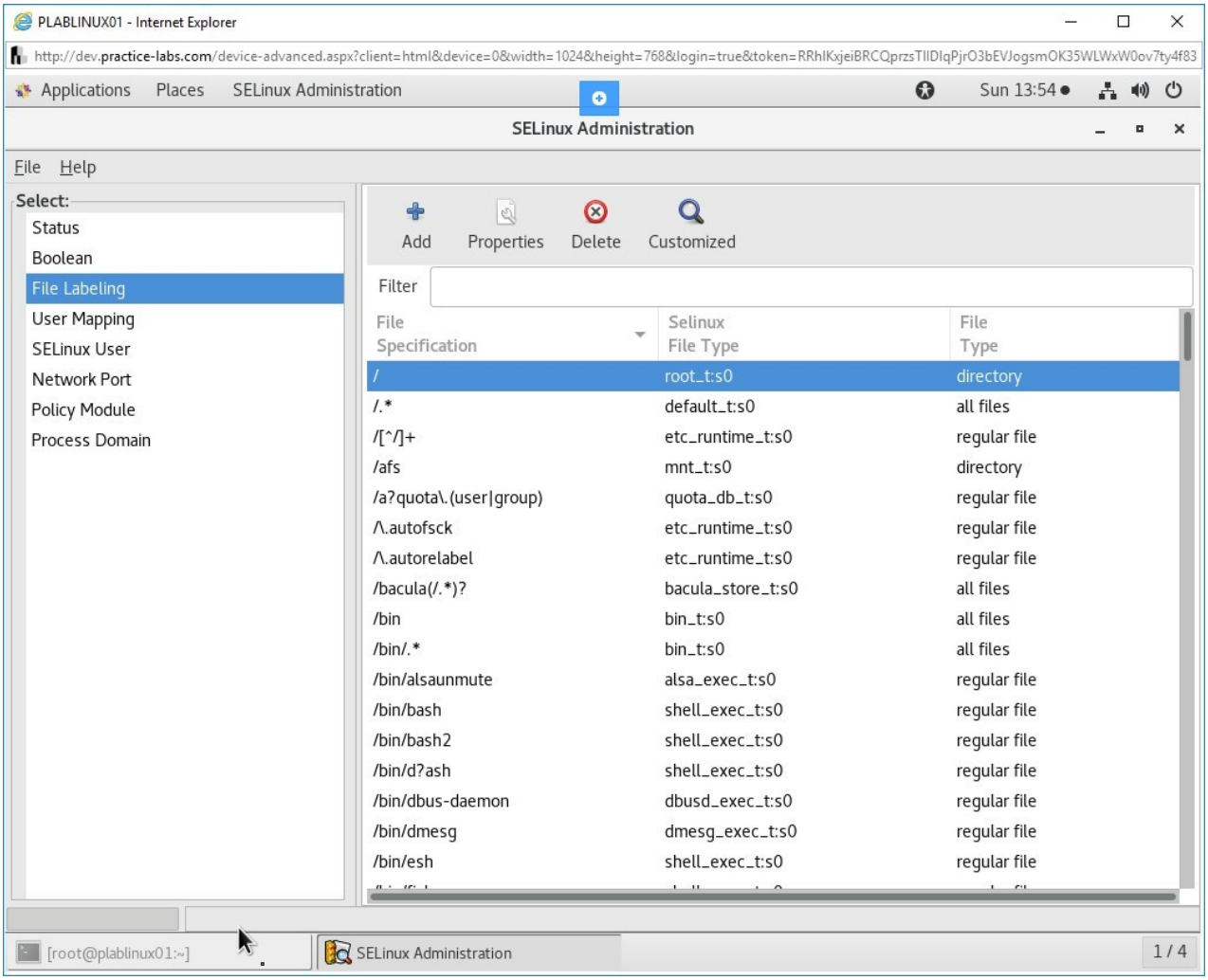


Figure 1.29 Screenshot of PLABLINUX01: Showing the File Labeling tab in the SELinux Administration window.

Step 8

Click the **User Mapping** tab. This tab displays the SELinux and user accounts mapping. Note that **system_u** user is mapped to the **system_u** SELinux user.

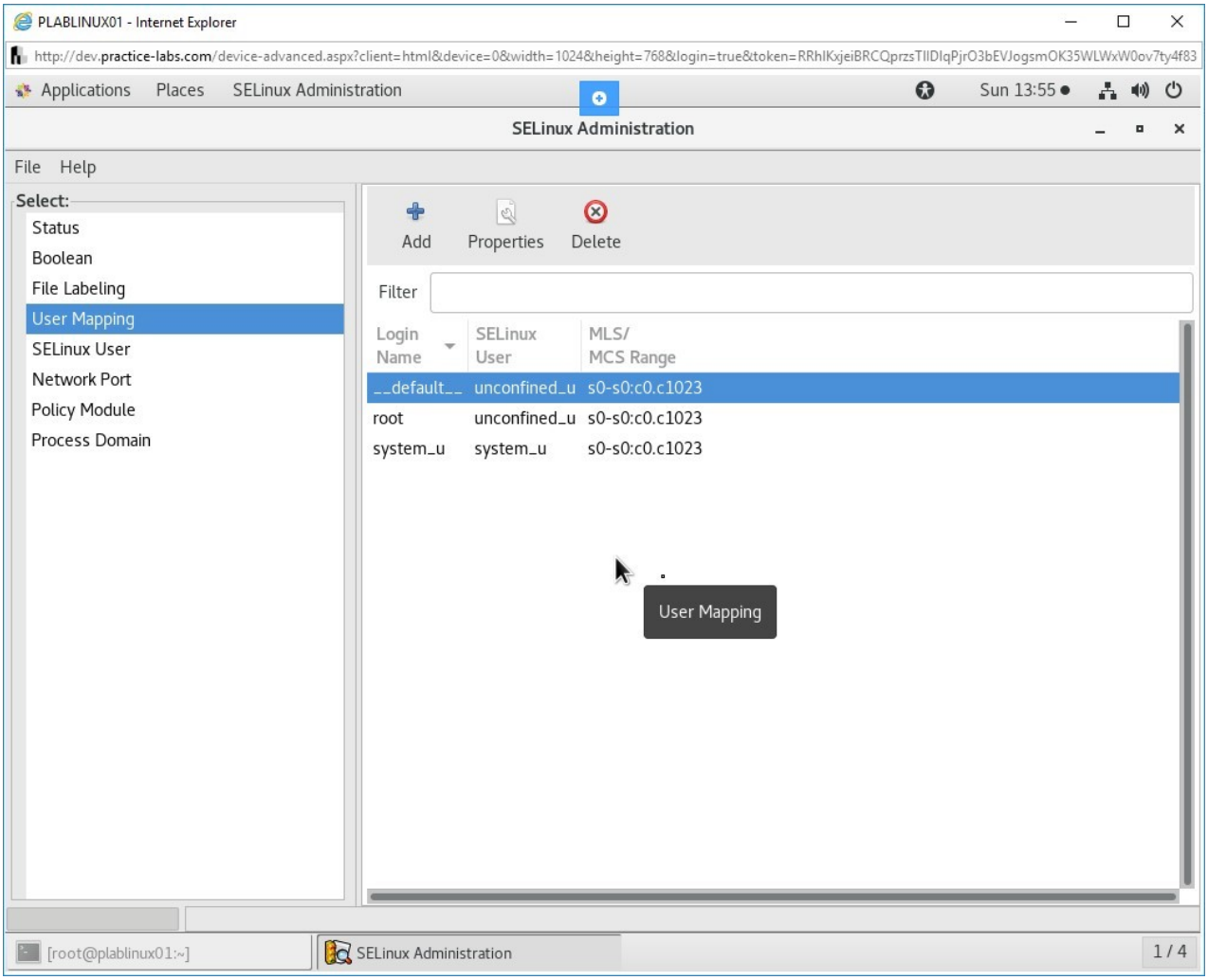


Figure 1.30 Screenshot of PLABLINUX01: Showing the User Mapping tab in the SELinux Administration window.

Step 9

Click the **SELinux User** tab. This tab displays the SELinux user and SELinux role mapping.

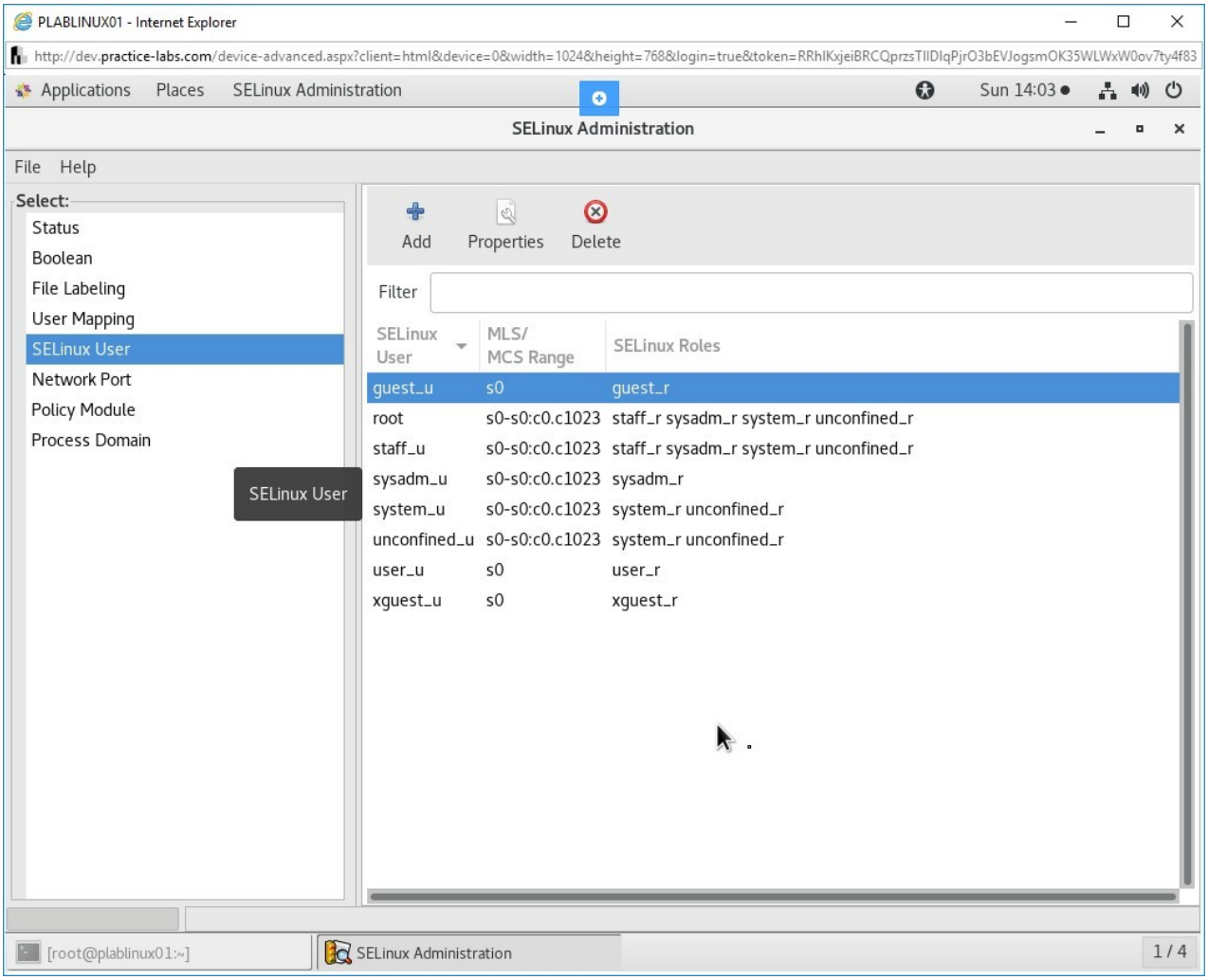


Figure 1.31 Screenshot of PLABLINUX01: Showing the SELinux User tab in the SELinux Administration window.

Step 10

Click the **Network Port** tab. This tab displays the network ports configured. You can add or delete a network port from this tab. To view the properties of a network port, you can click **Properties**.

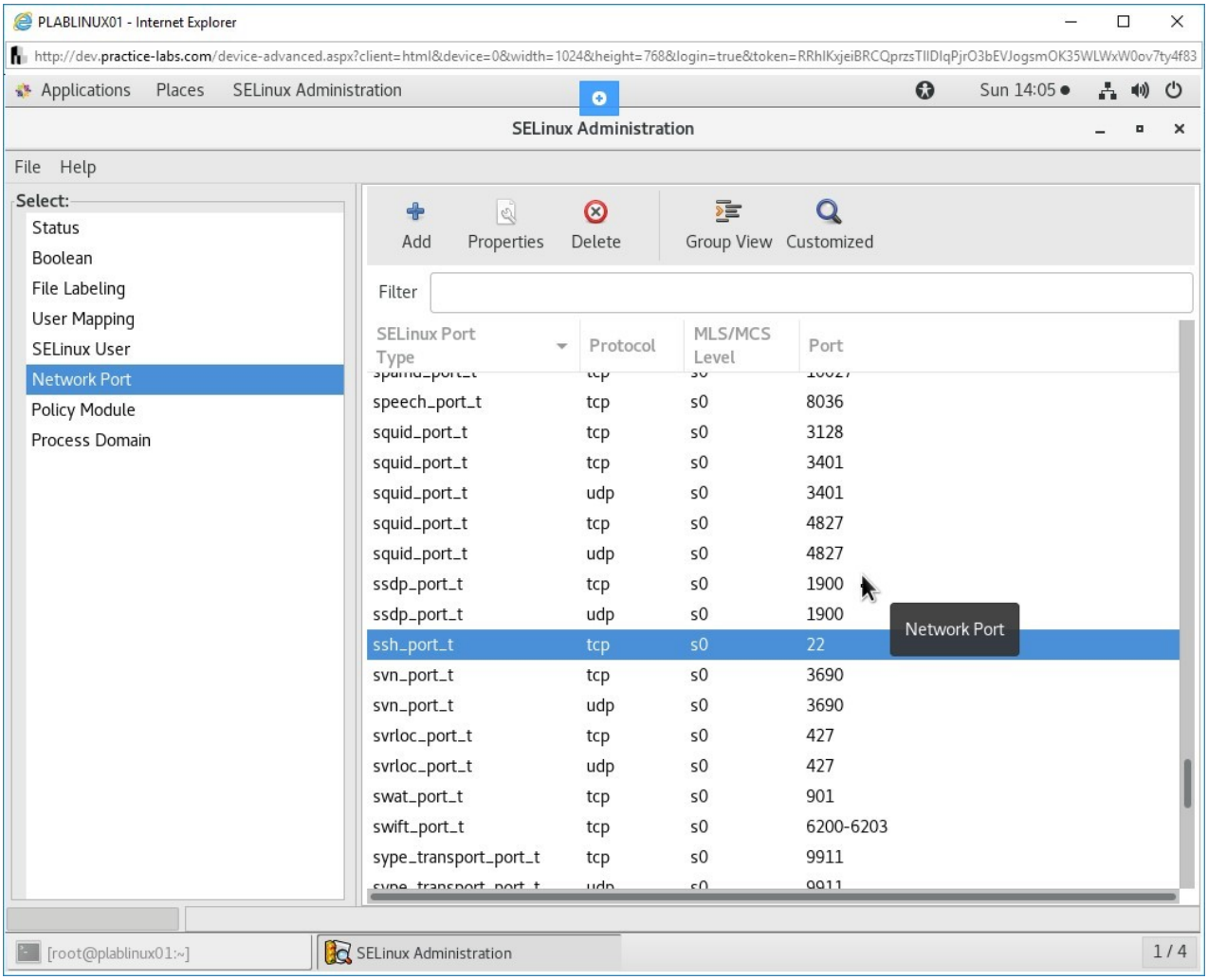


Figure 1.32 Screenshot of PLABLINUX01: Showing the Network Port tab in the SELinux Administration window.

Step 11

Click the **Policy Module** tab. This tab displays the policy modules that are loaded.

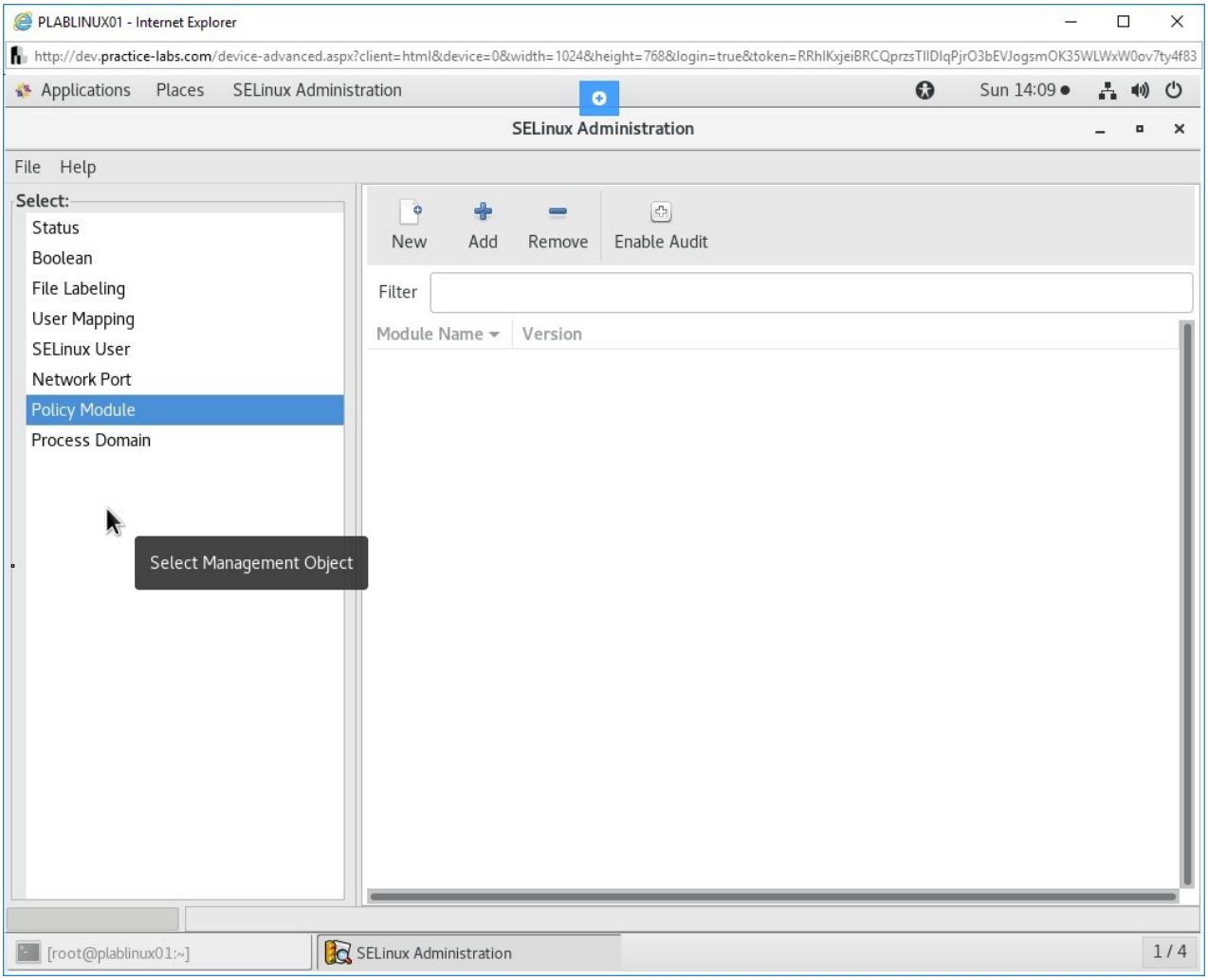


Figure 1.33 Screenshot of PLABLINUX01: Showing the Policy Module tab in the SELinux Administration window.

Step 12

Click the **Process Domain** tab. This tab displays the process domains. You can scroll down and select **cinder_volume**. Note that the default mode is **Enforcing**. You can change this by clicking on **Permissive**.

> ***Note:*** *By default, all domain names are set to Enforcing as this is the default mode of SELinux at present.*

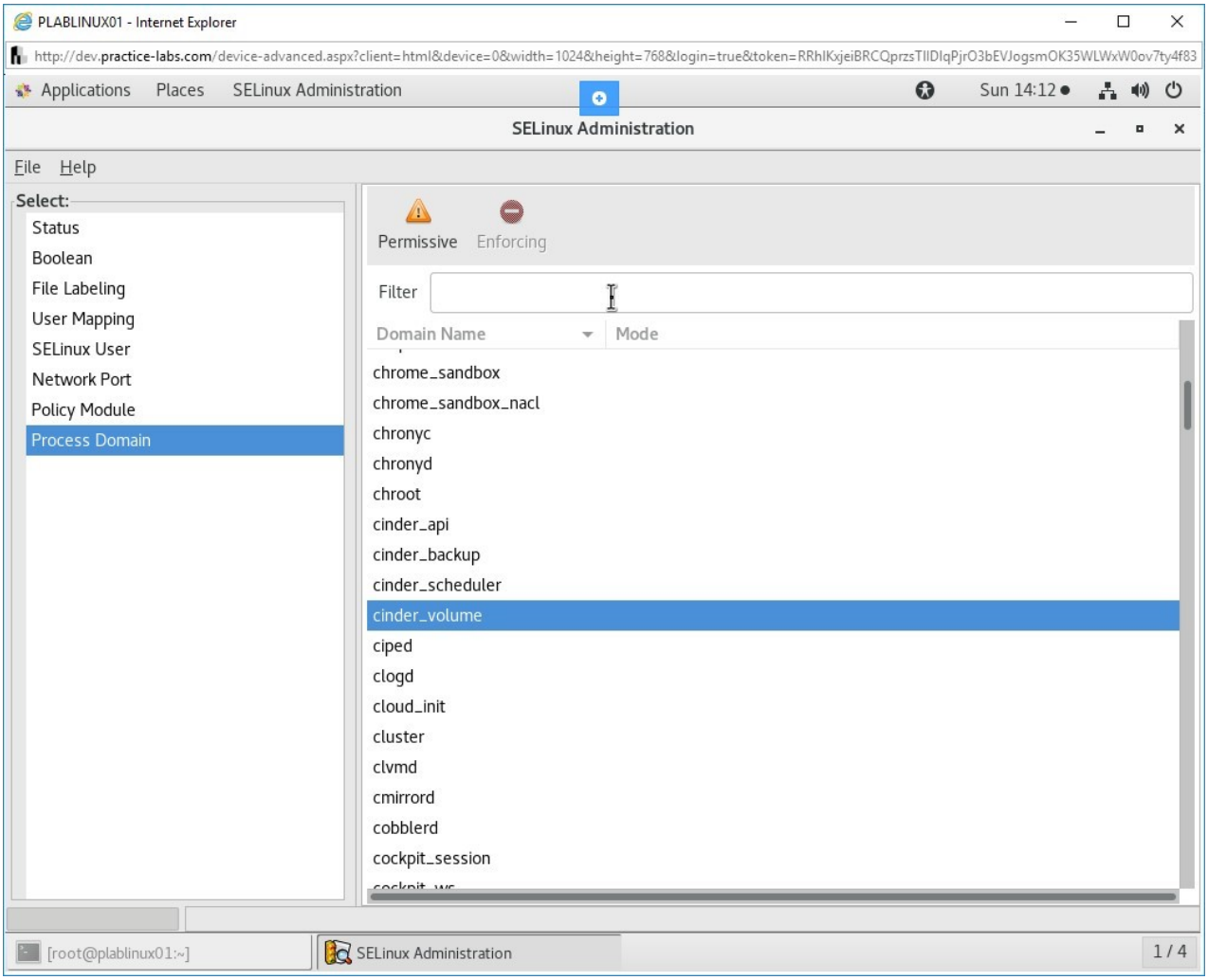


Figure 1.34 Screenshot of PLABLINUX01: Showing the Process Domain tab in the SELinux Administration window.

Step 13

Close the **SELinux Administration** window.

> ***Note:*** *By default, all domain names are set to Enforcing as this is the default mode of SELinux at present.*

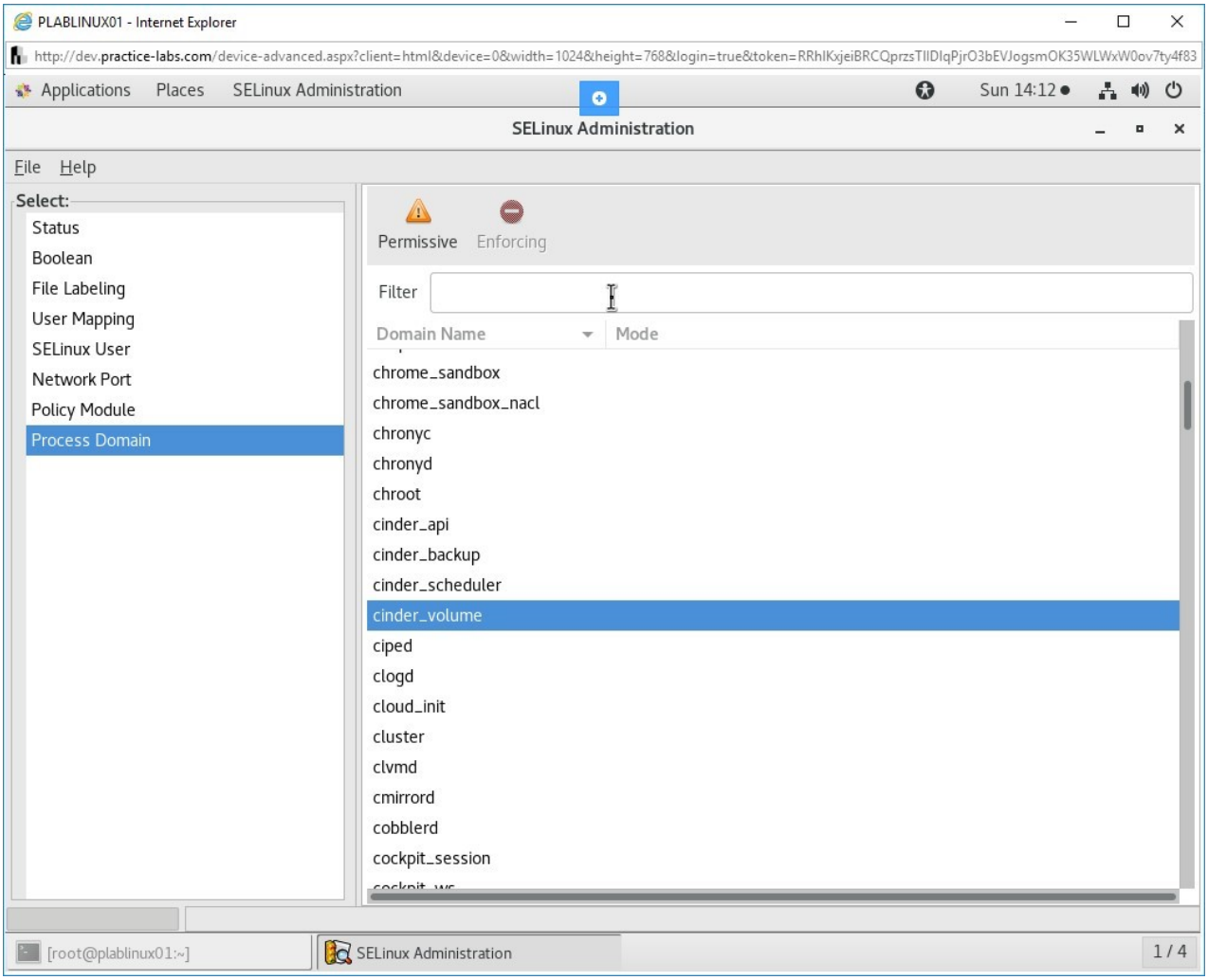


Figure 1.35 Screenshot of PLABLINUX01: Closing the SELinux Administration.

Step 14

Click **Applications**, select **Other** and then select **SELinux Policy Management Tool**.

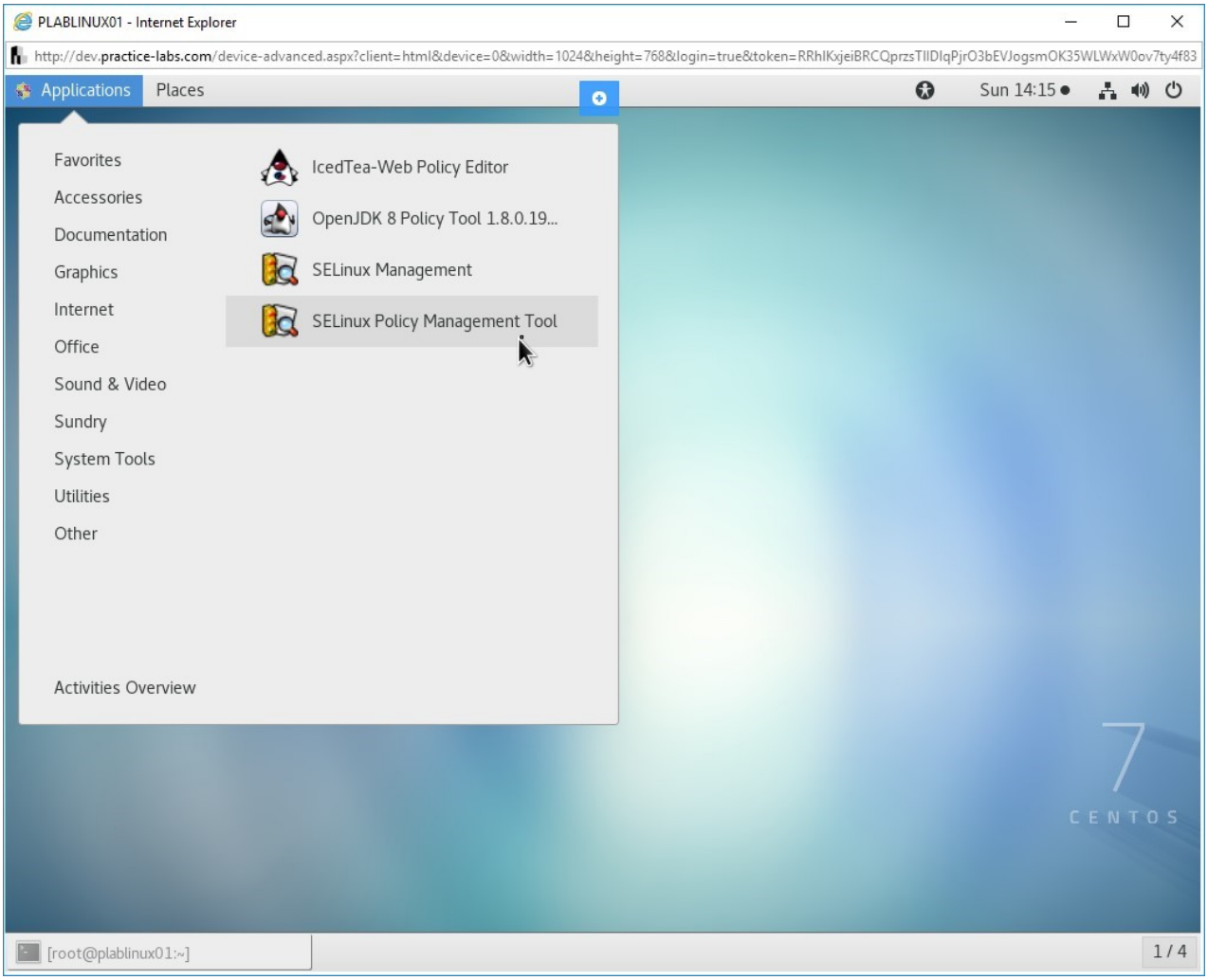


Figure 1.36 Screenshot of PLABLINUX01: Selecting the SELinux Policy Management Tool on the Applications menu.

Step 15

When prompted for the password, type the following password:

```
Passw0rd
```

Click **Authenticate**.

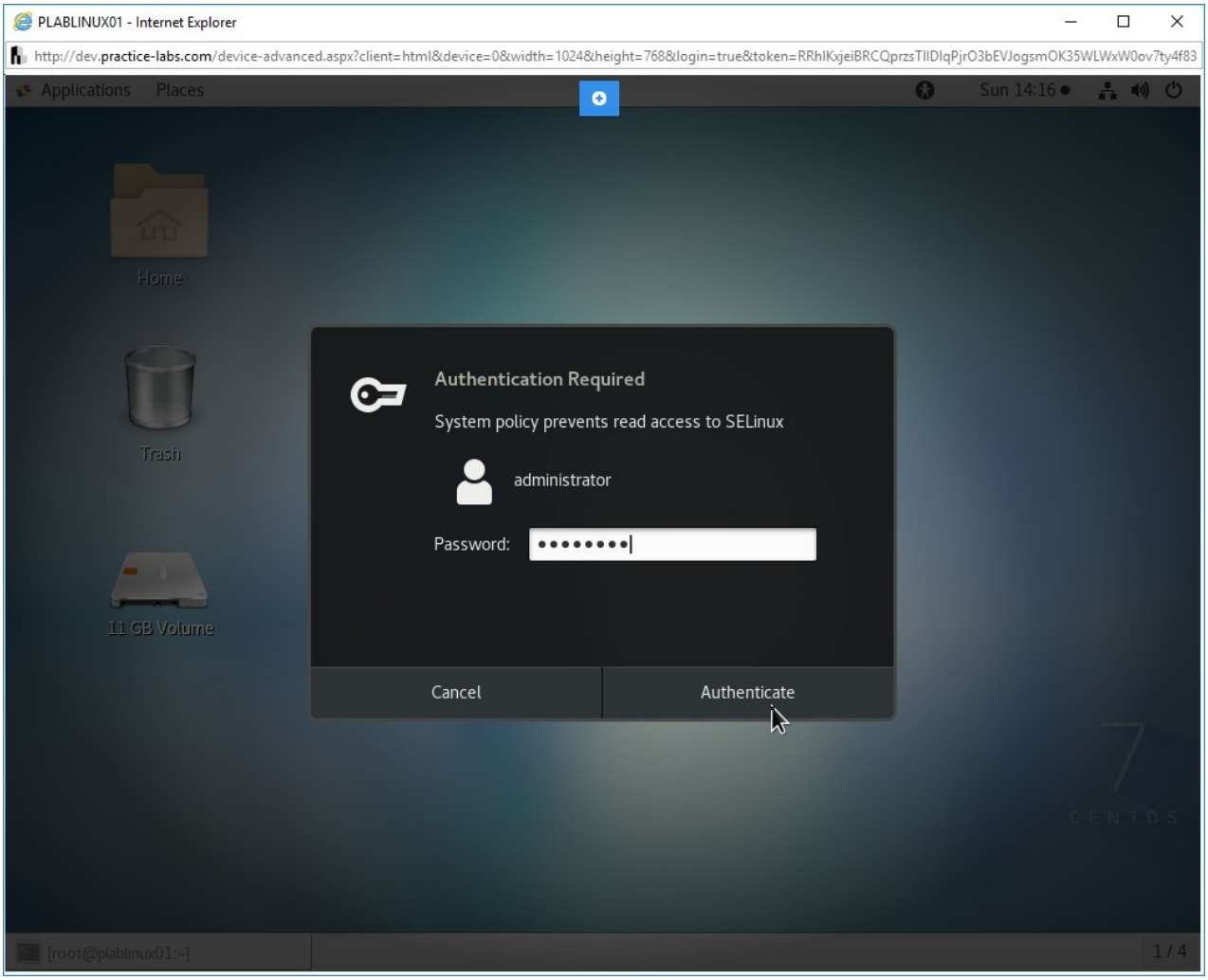


Figure 1.37 Screenshot of PLABLINUX01: Entering the password.

Step 16

The **Analyzing Policy** dialog box is displayed.

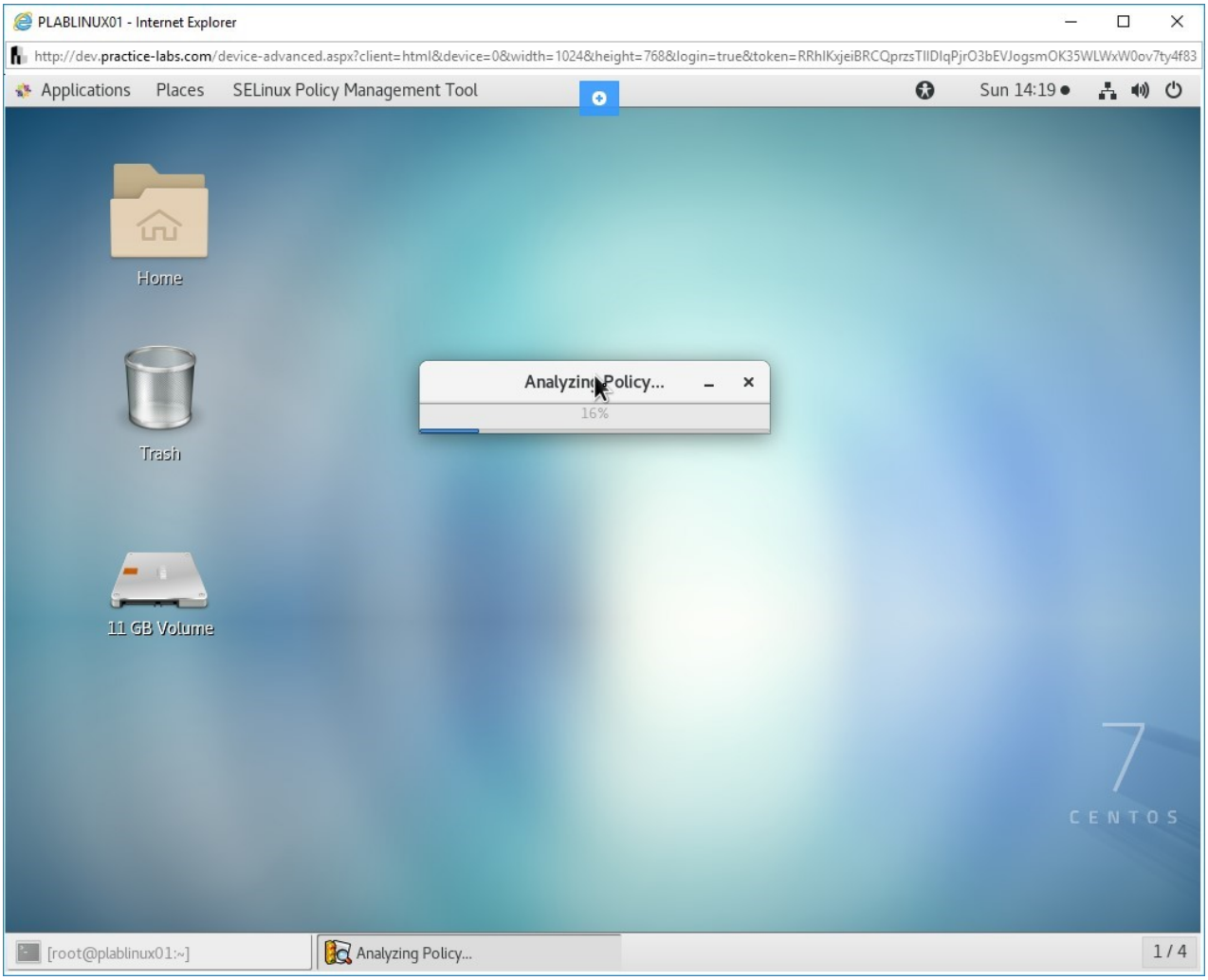


Figure 1.38 Screenshot of PLABLINUX01: Displaying the Analyzing Policy dialog box.

Step 17

The **SELinux Configuration** window is displayed.

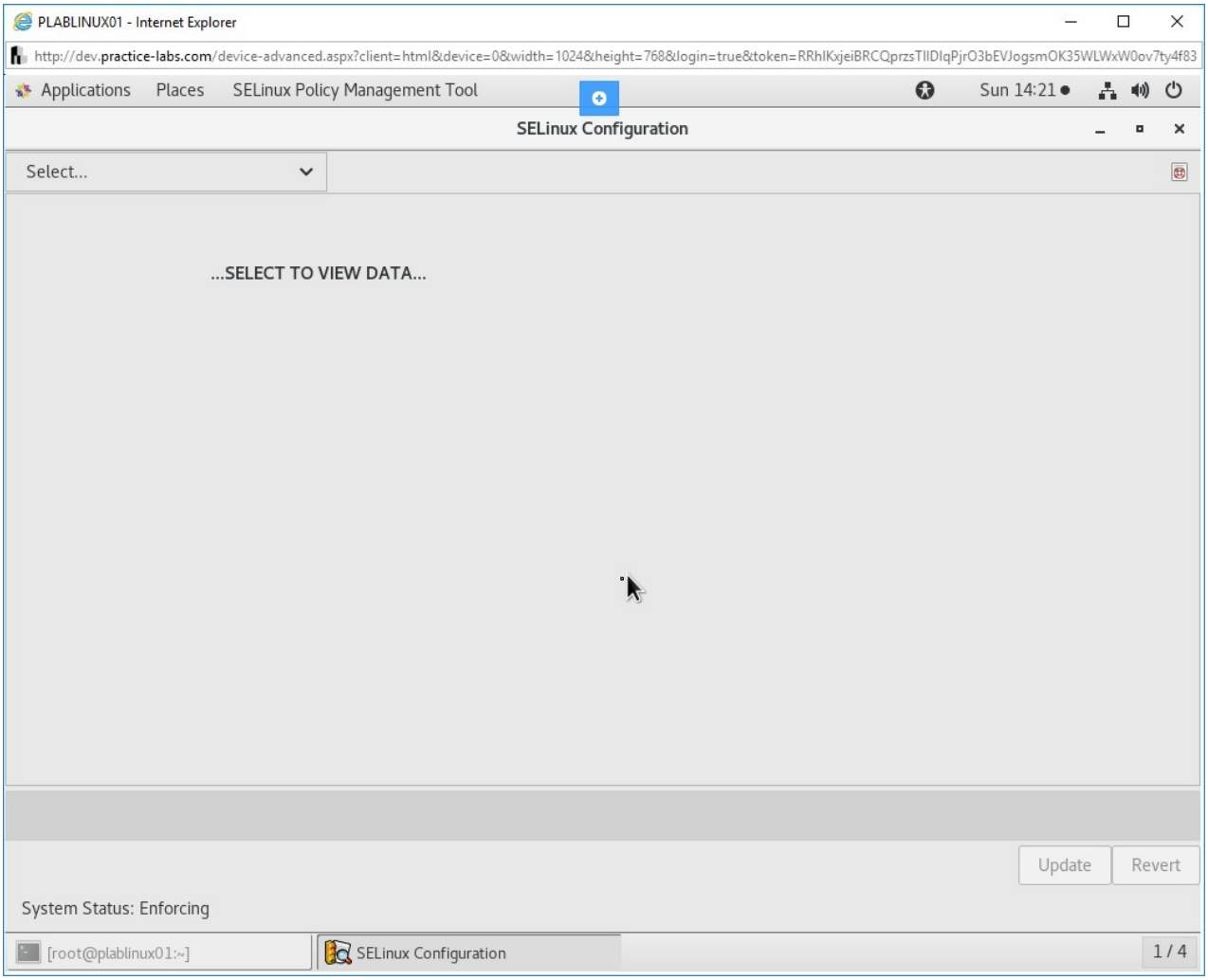


Figure 1.39 Screenshot of PLABLINUX01: Showing the SELinux Configuration window.

Step 18

Click **Select** and select **Users**.

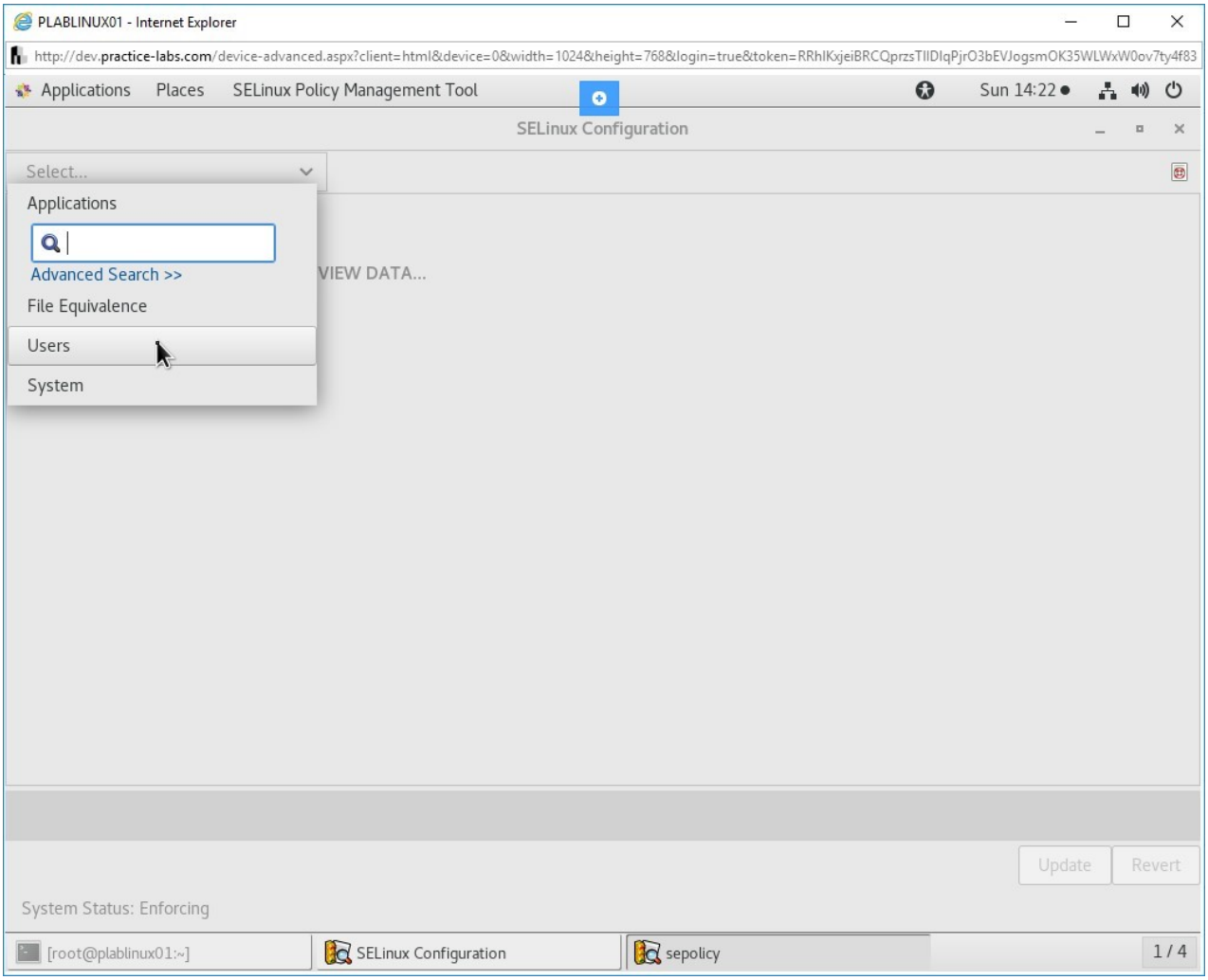


Figure 1.40 Screenshot of PLABLINUX01: Selecting Users from the drop-down.

Step 19

The **Login** names are displayed. Notice that **default** and **root** users are mapped to **unconfined_u**. By default, all users are mapped to **unconfined_u**. You can change this by modifying the user properties. When a user is mapped to **unconfined_u**, SELinux does not block access for the user.

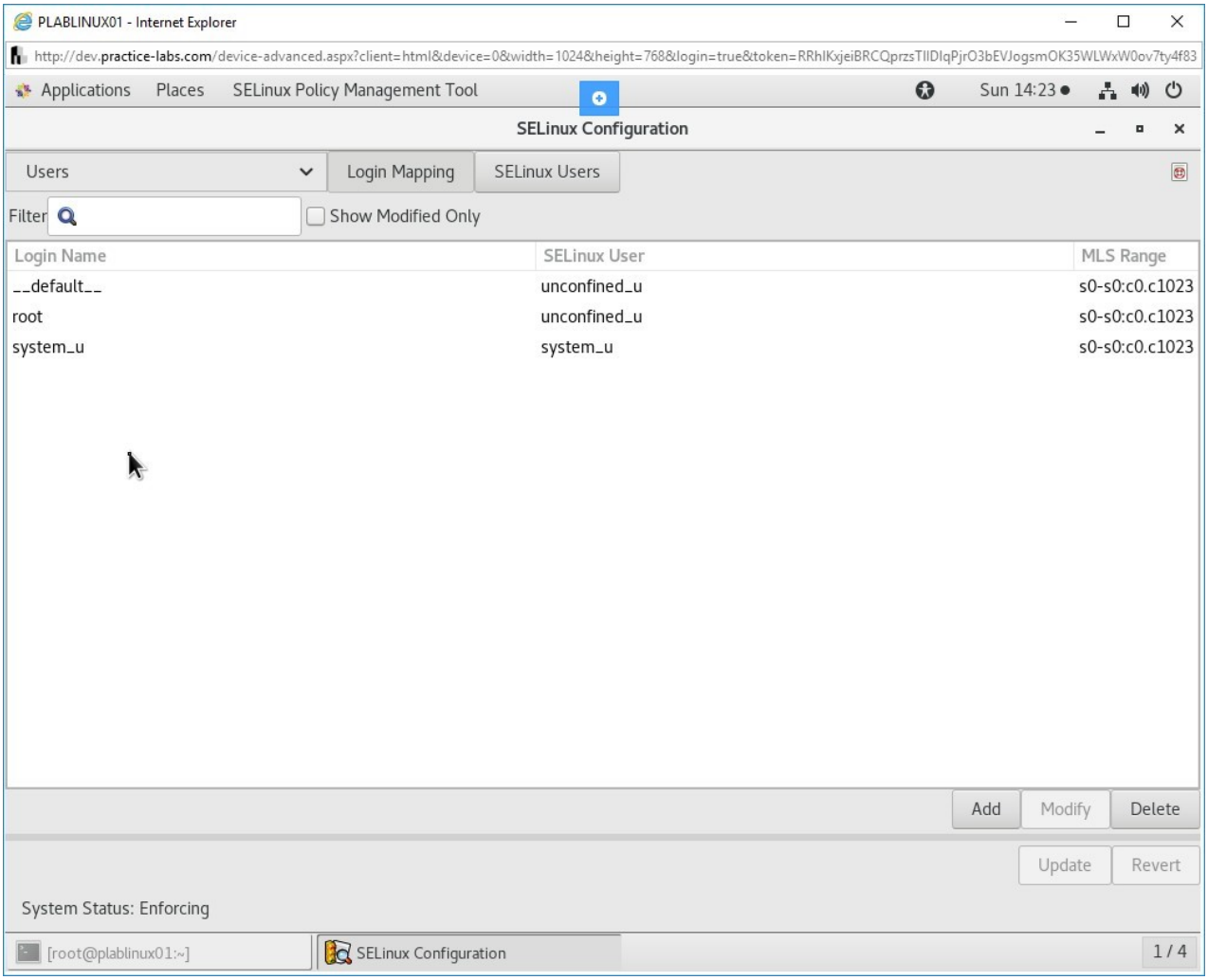


Figure 1.41 Screenshot of PLABLINUX01: Showing users on the SELinux Configuration.

Step 20

Click **Users** and select **System**. Here, you can configure the following settings:

- System mode when the system boots up
- System mode for the current session
- Importing system settings from another system
- Exporting the system settings.
- Relabel files to system default when the system boots up

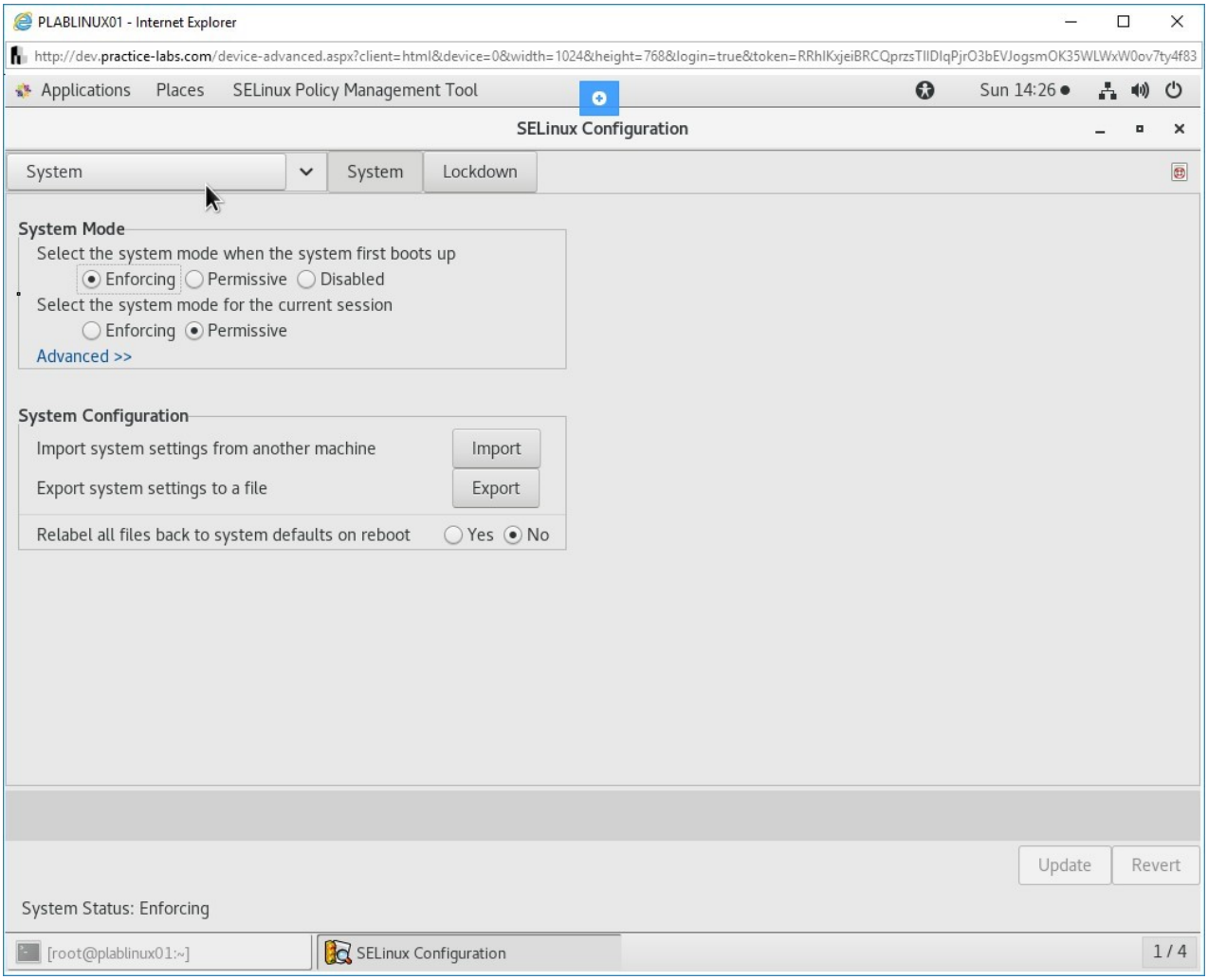


Figure 1.42 Screenshot of PLABLINUX01: Selecting System from the drop-down.

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

Review

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

Summary

You completed the following exercise:

- Exercise 1 - Configure SELinux

You should now be able to:

- Configure Network on CentOS

- View Current Status of SELinux
- Change the SELinux Mode
- View SELinux Contexts for Processes, Domain Transitions, and Users
- Install and use the policycoreutils-gui Package

Feedback

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