



Red Hat System Administration I

Dr. Eng. Gamal Selim

Lecture 09

Agenda

- **Chapter 14: Analyze Servers and Get Support**

Goal	Investigate and resolve issues in the web-based management interface, getting support from Red Hat to help solve problems.
Objectives	• Activate the web console management interface to remotely manage and monitor the performance of a Red Hat Enterprise Linux server. • Describe and use the Red Hat Customer Portal key resources to find information from Red Hat documentation and the Knowledgebase. • Use Red Hat Insights to analyze servers for issues, remediate or resolve them, and confirm that the solution worked.
Sections	• Analyze and Manage Remote Servers (and Guided Exercise) • Create a Diagnostics Report (and Guided Exercise) • Detect and Resolve Issues with Red Hat Insights (and Quiz)

Analyze and Manage Remote Servers

Objectives

Activate the web console management interface to remotely manage and monitor the performance of a Red Hat Enterprise Linux server.

Describe the Web Console

The *web console* is a web-based management interface for Red Hat Enterprise Linux. The interface is designed for managing and monitoring your servers, and is based on the open-source Cockpit service.

You can use the web console to monitor system logs and to view graphs of system performance. Additionally, you can use your web browser to change settings by using graphical tools in the web console interface, including a fully functional interactive terminal session.

Enable the Web Console

Starting from Red Hat Enterprise Linux 7, the web console is installed by default in all installation variants except in a minimal installation. You can use the following command to install the web console:

```
[root@host ~]# dnf install cockpit
```

Then, enable and start the `cockpit.socket` service, which runs a web server. This step is necessary if you need to connect to the system through the web interface.

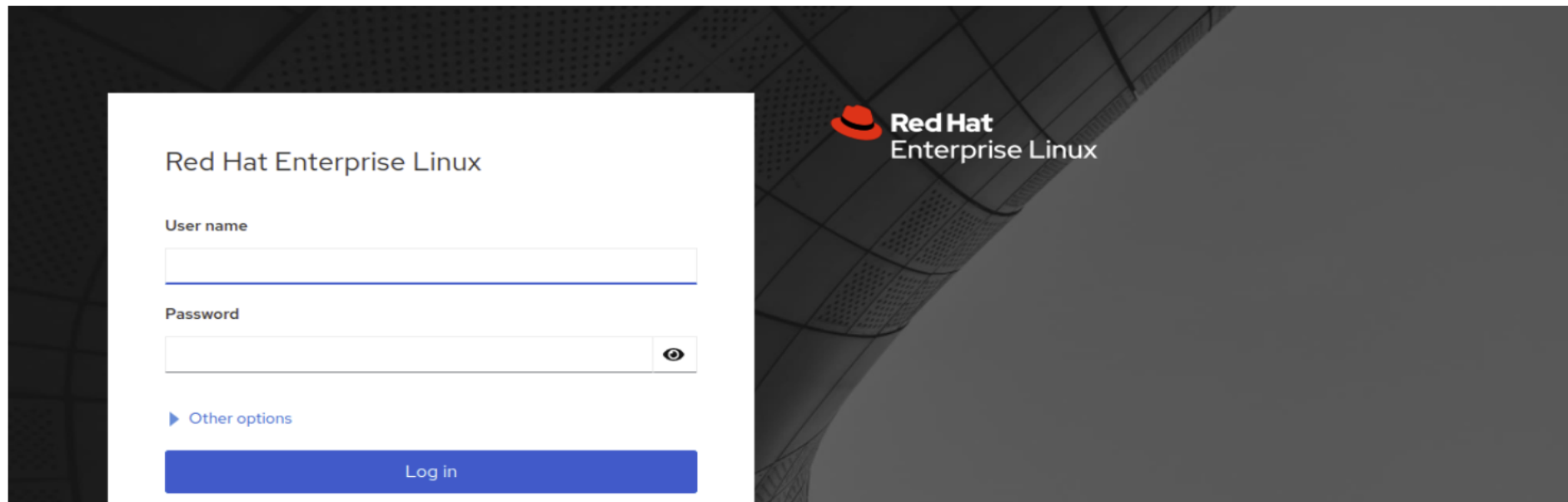
```
[root@host ~]# systemctl enable --now cockpit.socket  
Created symlink /etc/systemd/system/sockets.target.wants/cockpit.socket -> /usr/lib/systemd/system/cockpit.socket.
```

Log in to the Web Console

The web console provides its own web server. Launch your web browser to log in to the web console.

Open `https://servername:9090` in your web browser, where *servername* is the hostname or IP address of your server. The web console protects the connection by a *Transport Layer Security (TLS)* session. By default, the `cockpit` service installs the web console with a self-signed TLS certificate. When you connect to the web console for the first time, the web browser probably displays a security warning. The `cockpit-ws(8)` man page provides instructions on how to replace the TLS certificate with a correctly signed one.

To log in to the web console, enter your username and password at the login screen. You can log in with the username and password of any local account on the system, including the `root` user.



After you log in, the web console displays the username on the left side of the title bar. The default access to the web console is with limited rights, as you can see in the following **Limited access** button and in the "Web console is running in limited access mode" message.



Figure 14.2: Non-privileged user's title bar

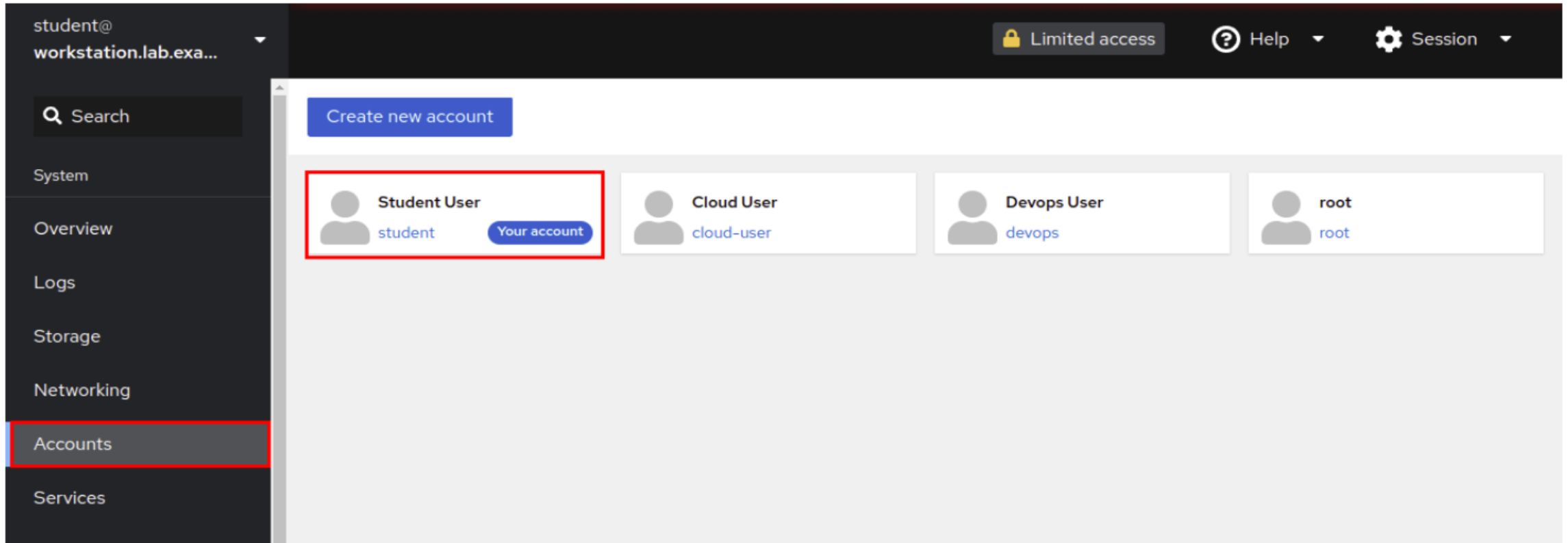
If your account is configured with the appropriate privileges, then you can escalate privileges by switching to administrative access, by clicking the **Limited access** or **Turn on administrative access** buttons. During the escalation privileges process, you need to enter your password. When you have escalated privileges, the **Limited access** button changes to **Administrative access**.

You can switch back to limited access mode by clicking the **Administrative access** button and then clicking the **Limit access** button in the pop-up window that it shows.



Change Passwords in the Web Console

You can change your own password when logged in to the web console. Click the **Accounts** button on the navigation bar. Click your account label to open the account details page.



As a non-privileged user, you are restricted to setting or resetting your password and managing public SSH keys. To set or reset your password, click the **Set password** button.

The screenshot shows the Red Hat Accounts web interface. On the left is a dark sidebar with a search bar and navigation links: System, Overview, Logs, Storage, Networking, Accounts (highlighted), Services, and Tools. The top header shows the user 'student@workstation.lab.exa...' and 'Limited access' status, along with Help and Session menus. The main content area is titled 'Accounts > Student User'. It displays user details for 'Student User': Full name (Student User), User name (student), Roles (checked 'Server administrator'), Last login (Logged in), and Options (unchecked 'Disallow interactive password', 'Never expire account', and an 'edit' link). The 'Password' section shows a 'Set password' button (highlighted with a red box), 'Never expire password', and an 'edit' link.

Enter your information in the **Old password**, **New password**, and **Confirm new password** fields. Click the **Set password** button to activate the new password.

Set password

Old password

.....

New password

.....

Excellent password

Confirm new password

.....

Set password

Cancel

Troubleshoot with the Web Console

The web console is a powerful troubleshooting tool. You can monitor system statistics in real time, inspect system logs, and switch to a terminal session within the web console to gather additional information from the command-line interface.

Monitor System Statistics in Real Time

Click the **Overview** button on the navigation bar to view information about the system, such as its type of hardware, operating system, hostname, and more. If you log in as a non-privileged user, then you can see all the information but not modify any value. The following image displays the **Overview** page.

student@workstation.lab.example.com

Search

System

Overview

Logs

Storage

Networking

Accounts

Services

Tools

Applications

Diagnostic Reports

Kernel Dump

Limited access

Help

Session

Web console is running in limited access mode. Turn on administrative access

workstation.lab.example.com running Red Hat Enterprise Linux 9.0 (Plow)

Health

! Loading available updates failed

⚠ Not connected to Insights

👤 Last successful login: May 19, 04:27 PM
from 172.25.250.254 on pts/0
[View login history](#)

Usage

CPU

0% of 4 CPUs

Memory

0.7 / 5.5 GiB

[View details and history](#)

System information

Model	Red Hat OpenStack Compute
Machine ID	633680e38e32491899fbd3a7f6129842
Uptime	about 2 hours

Configuration

Hostname	workstation.lab.example.com
System time	May 19, 2022, 11:23 AM ⓘ
Domain	Join domain

Click **View details and history** on the **Overview** page to view details of current system performance for CPU activity, memory use, disk I/O, and network usage.

The screenshot displays the Red Hat Workstation interface. The top bar shows the user 'student@workstation.lab.exa...' and a 'Limited access' status. The left sidebar contains navigation links: System, Overview (selected), Logs, Storage, Networking, Accounts, and Services. The main content area is titled 'Overview > Performance Metrics' and is divided into four panels: CPU, Memory, Disks, and Network.

CPU

4 CPUs 0%

Load
1 min: 0.00, 5 min: 0.00,
15 min: 0.00

Service	%
cockpit-wsinstance-https...	0.0
dbus-broker	0.0
cockpit	0.0
systemd-logind	0.0
cups	0.0

Memory

RAM 4.8 GiB available

Service	Used
firewalld	39.3 MB
user@42	23.9 MB
polkit	21.9 MB
systemd-udev	15.5 MB
systemd-journald	11.1 MB

Disks

Read	Write
0	20.3 B/s

/ 5.20 GB free

/boot 327 MB free

/boot/efi 202 MB free

Network

Interface	In	Out
lo	0	0
eth0	231 B/s	710 B/s

Inspect and Filter Syslog Events

The **Logs** section in the navigation bar provides access to analysis tools for the system logs. You can use the scroll menus on the page to filter log messages by a logging date range, or priority, or both. The web console uses the current date as the default; you can click the date menu and specify any range of dates. Similarly, the **Priority** menu provides options that range from **Debug and above** (at the lowest level) to more specific severity conditions such as **Alert and above** or **Error and above**.

The screenshot displays the Red Hat web console interface. On the left, a navigation sidebar shows the 'Logs' section highlighted. The main content area features a filter bar with three dropdown menus: 'Last 24 hours' (selected), 'Priority' (set to 'Debug and above'), and 'Identifier' (set to 'All'). Below these, a search bar contains the text 'priority:debug'. A list of log entries is shown, dated 'May 19, 2022'. The 'Priority' dropdown menu is open, showing a list of severity levels: 'Only emergency', 'Alert and above', 'Critical and above', 'Error and above', 'Warning and above', 'Notice and above', 'Info and above', and 'Debug and above' (which is selected with a blue checkmark). The log entries include timestamps, messages, and source identifiers like 'cockpit-tls', 'REQUEST localhost', 'pam_unix(sudo:session)', 'released daemon: :1.121', and 'client gone away: :1.121'.

Click a row to view details of the log report. In the following example, note the first row that reports on a `sudo` log message.

student@
workstation.lab.exa...

Search

System

Overview

Logs

Storage

Networking

Last 24 hours Priority Error and above Identifier All

Filters priority:err

May 19, 2022

5:25 PM	student : 3 incorrect password attempts ; TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/bash	sudo
3:27 PM	Exec failed for mail command: No such file or directory	atd
3:27 PM	error: kex_exchange_identification: Connection closed by remote host	sshd

The following example shows the details that the web console displays when you click the `sudo` row. Details of the report include the selected log entry (`sudo`), the date, time, priority, and syslog facility of the log entry, and the hostname of the system that reported the log message.

The screenshot shows the Red Hat web console interface. On the left is a dark sidebar with a search bar and a menu containing 'System', 'Overview', 'Logs' (highlighted with a red box), 'Storage', 'Networking', 'Accounts', 'Services', and 'Tools'. The top header shows the user 'student@workstation.lab.exa...' and navigation links for 'Limited access', 'Help', and 'Session'. The main content area is titled 'Logs > Entry at May 19, 2022, 5:25:51 PM'. It displays a log entry for 'sudo' (highlighted with a red box) with the message: 'student : 3 incorrect password attempts ; TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/bash'. Below this is a table of log details:

PRIORITY	1
SYSLOG_FACILITY	10
SYSLOG_IDENTIFIER	sudo
SYSLOG_TIMESTAMP	May 19 11:25:51
_AUDIT_LOGINUID	1000
_AUDIT_SESSION	15
_BOOT_ID	a3621f8f9f8244c5abdb98292735c10f

Run Commands from a Terminal Session

The **Terminal** button in the navigation bar provides access to a fully functional terminal session within the web console interface. In this web console terminal, you can run arbitrary commands to manage and work with the system, and for tasks that the other web console tools do not support.

The following image displays examples of commands to gather additional information. For example, listing the contents of the `/var/log` directory provides reminders of log files that might have valuable information. The `id` command provides information such as group membership that might help to troubleshoot file access restrictions. The `ps -au` command provides a view of processes that are running in the terminal and of the user that is associated with the process.

Networking

Accounts

Services

Tools

Applications

Diagnostic Reports

Kernel Dump

SELinux

Software Updates

Subscriptions

Terminal

student@workstation:~Font size-16+AppearanceBlackReset

```
[student@workstation ~]$ ls /var/log
audit          dnf.log        maillog        speech-dispatcher
boot.log       dnf.rpm.log    messages       spooler
btmpt          firewallld     part-handler.log sssd
chrony         gdm            private        tallylog
cloud-init.log hawkey.log     qemu-ga        tuned
cloud-init-output.log heat-provision.log README         wtmp
cron           insights-client rhsm
cups           kdump.log      samba
dnf.librepo.log lastlog         secure
```

```
[student@workstation ~]$ id
uid=1000(student) gid=1000(student) groups=1000(student),10(wheel) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

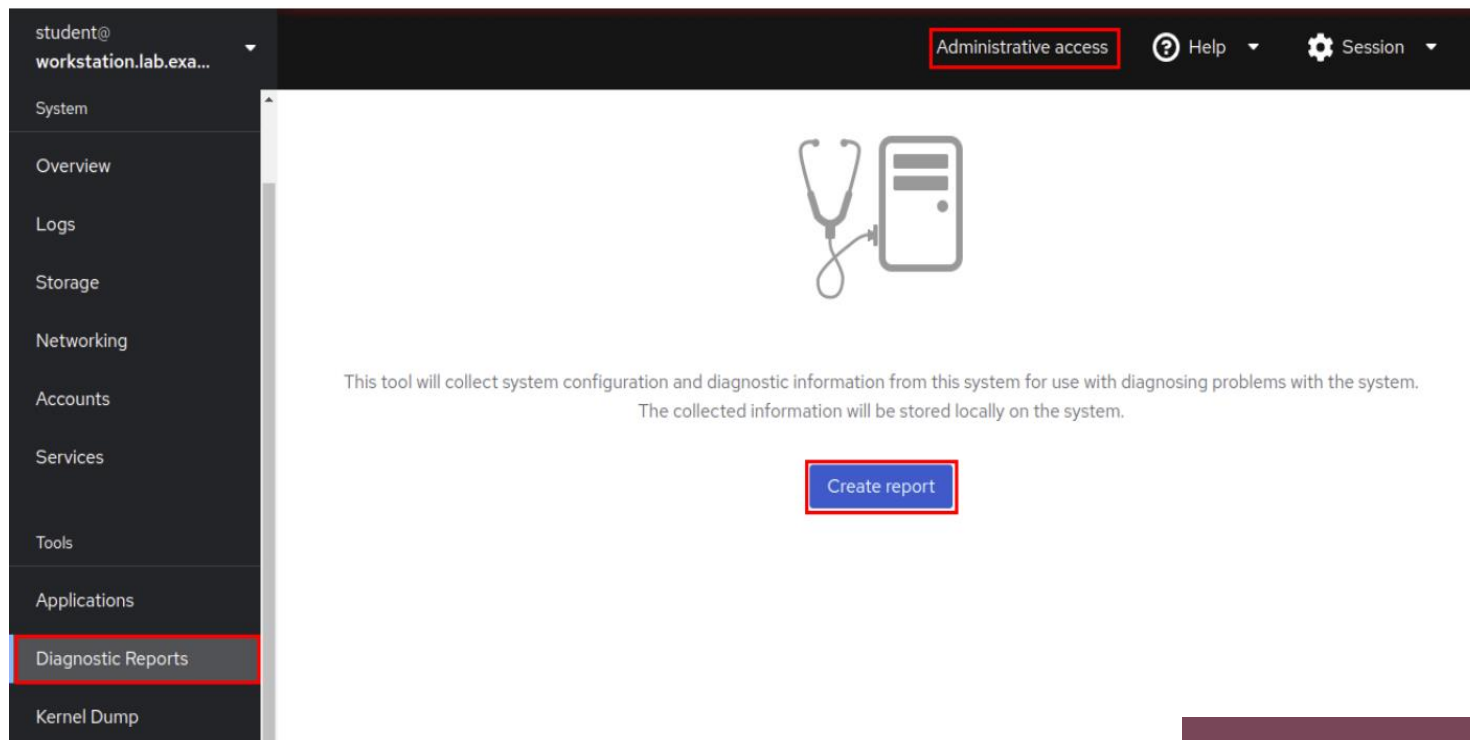
```
[student@workstation ~]$ pwd
/home/student
```

```
[student@workstation ~]$
```

Create Diagnostic Reports

A diagnostic report is a collection of configuration details, system information, and diagnostic information from a Red Hat Enterprise Linux system. Data that is collected in the report includes system logs and debug information that you can use to troubleshoot issues.

To generate a diagnostic report, log in to the web console as a privileged user. Click the **Diagnostic Reports** button on the navigation bar to open the page that creates these reports. Click the **Create report** button to generate a new diagnostic report.



Create diagnostic report



i The generated archive contains data considered sensitive and its content should be reviewed by the originating organization before being passed to any third party.

Done!

100%

Download report

Manage System Services with the Web Console

As a privileged web console user, you can stop, start, enable, and restart system services. Additionally, you can configure network interfaces, configure firewall services, administer user accounts, and more.

System Power Options

In the web console, you can restart or shut down the system. To access the system power options, log in to the web console as a privileged user. Click the **Overview** button on the navigation bar to access system power options.

From the menu on the upper right, select the appropriate option to either reboot or shut down a system.

student@
workstation.lab.exa...

System

Overview

Logs

Storage

Networking

Accounts

Services

workstation.lab.example.com running Red Hat Enterprise Linux 9.0 (Plow)

Administrative access

Help

Session

Reboot

Reboot

Shutdown

Health

- ! Loading available updates failed
- ! Not connected to Insights
- Last successful login: May 19, 04:27 PM
from 172.25.250.254 on pts/0
[View login history](#)

Usage

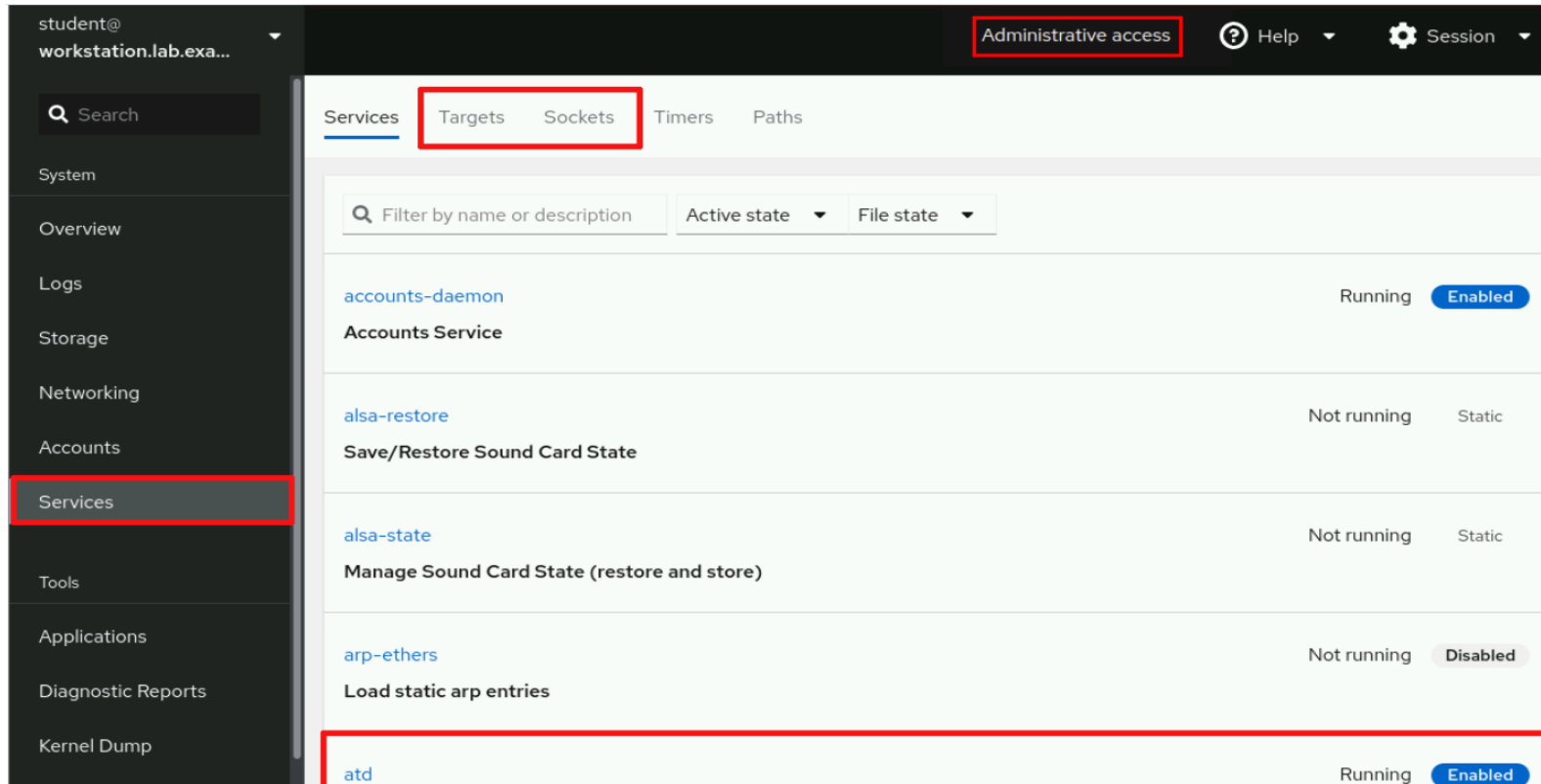
CPU 0% of 4 CPUs

Memory 0.9 / 5.5 GiB

[View details and history](#)

Control Running System Services

You can start, enable, disable, and stop services with graphical tools in the web console. To do so, click the **Services** button on the navigation bar to access the web console's services initial page. The **Services** page shows the system services tab by default. You can change to **Targets** or **Sockets** by clicking the appropriate tab. Use the search bar or scroll through the page to select the service to manage.



The screenshot shows the Red Hat web console interface. On the left is a navigation sidebar with the 'Services' tab highlighted. The top header shows 'student@workstation.lab.exa...' and 'Administrative access'. The main content area has tabs for 'Services', 'Targets', 'Sockets', 'Timers', and 'Paths'. The 'Targets' tab is selected and highlighted with a red box. Below the tabs is a search bar and filters for 'Active state' and 'File state'. A list of services is displayed, including 'accounts-daemon' (Running, Enabled), 'alsa-restore' (Not running, Static), 'alsa-state' (Not running, Static), 'arp-ethers' (Not running, Disabled), and 'atd' (Running, Enabled). The 'atd' service row is highlighted with a red box.

Service Name	Description	Active state	File state
accounts-daemon	Accounts Service	Running	Enabled
alsa-restore	Save/Restore Sound Card State	Not running	Static
alsa-state	Manage Sound Card State (restore and store)	Not running	Static
arp-ethers	Load static arp entries	Not running	Disabled
atd		Running	Enabled

Click the **Stop**, **Restart**, or **Disallow running (mask)** buttons as appropriate to manage the service. In this view, the service is already running. To view additional information about the service, click any of the highlighted links or scroll through the service logs that are displayed below the service management section.

student@workstation.lab.exa... Administrative access ? Help Session

Search

System

Overview

Logs

Storage

Networking

Accounts

Services

Services > **atd.service**

Deferred execution scheduler ☒ ⋮

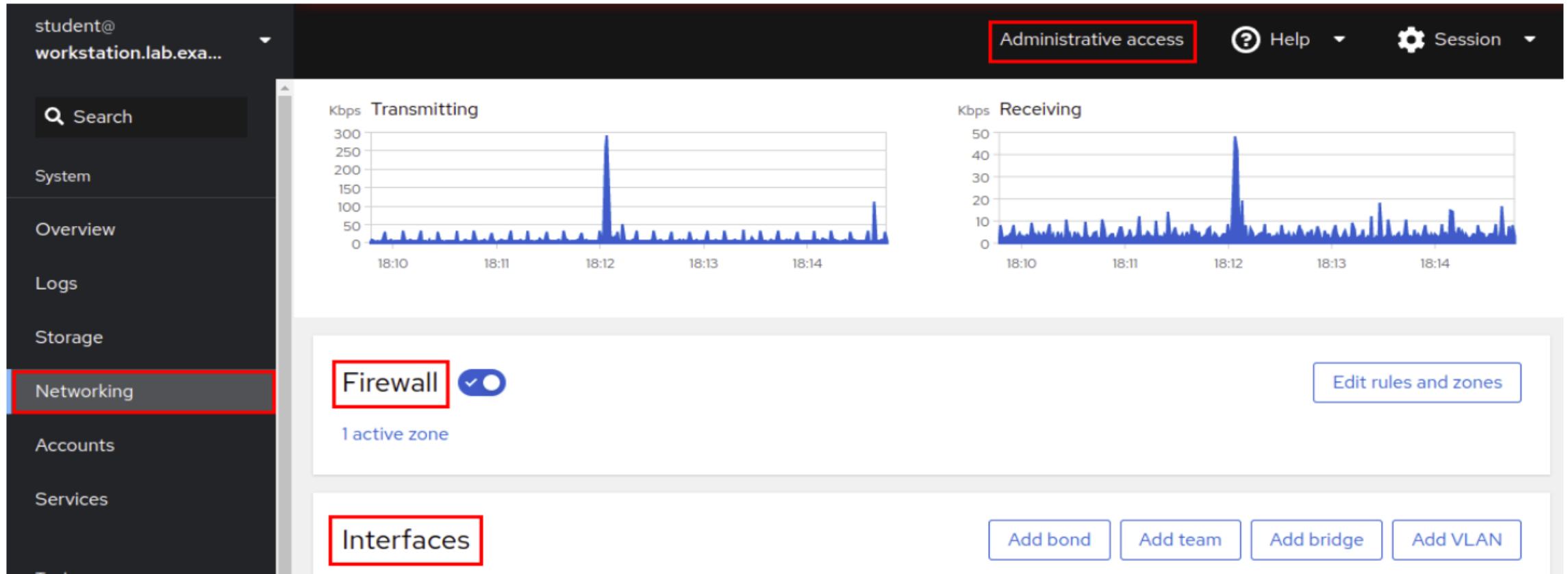
Status	Running	Restart
	Automatic	Stop
Path	/usr/lib/systemd/systemd	Disallow running (mask)
Memory	308 KiB	

> [Show relationships](#)

Service logs [View all logs](#)

Configure Network Interfaces and the Firewall

To manage firewall rules and network interfaces, click the **Networking** button on the navigation bar. The following example shows how to gather information about network interfaces and how to manage them.



Search

System

Overview

Logs

Storage

Networking

Accounts

Services

Tools

Applications

Diagnostic Reports

Kernel Dump

SELinux

Networking > eth0

Kbps Transmitting



Kbps Receiving



eth0

Red Hat, Inc. Virtio network device virtio_net 52:54:00:00:FA:09



Status 172.25.250.9/24, fe80:0:0:0:5054:ff:fe00:fa09/64

Carrier Yes

General ☒ Connect automatically

IPv4 Address 172.25.250.9/24 via 172.25.250.254
DNS 172.25.250.220
DNS search domains lab.example.com, example.com

edit

IPv6 Ignore edit

MTU 8942 edit

IPv4 settings

Addresses

Manual



Address

Prefix length or netmask

Gateway

172.25.250.9

24

172.25.250.254



Address

Prefix length or netmask

Gateway

172.25.250.100

24



DNS



Automatic



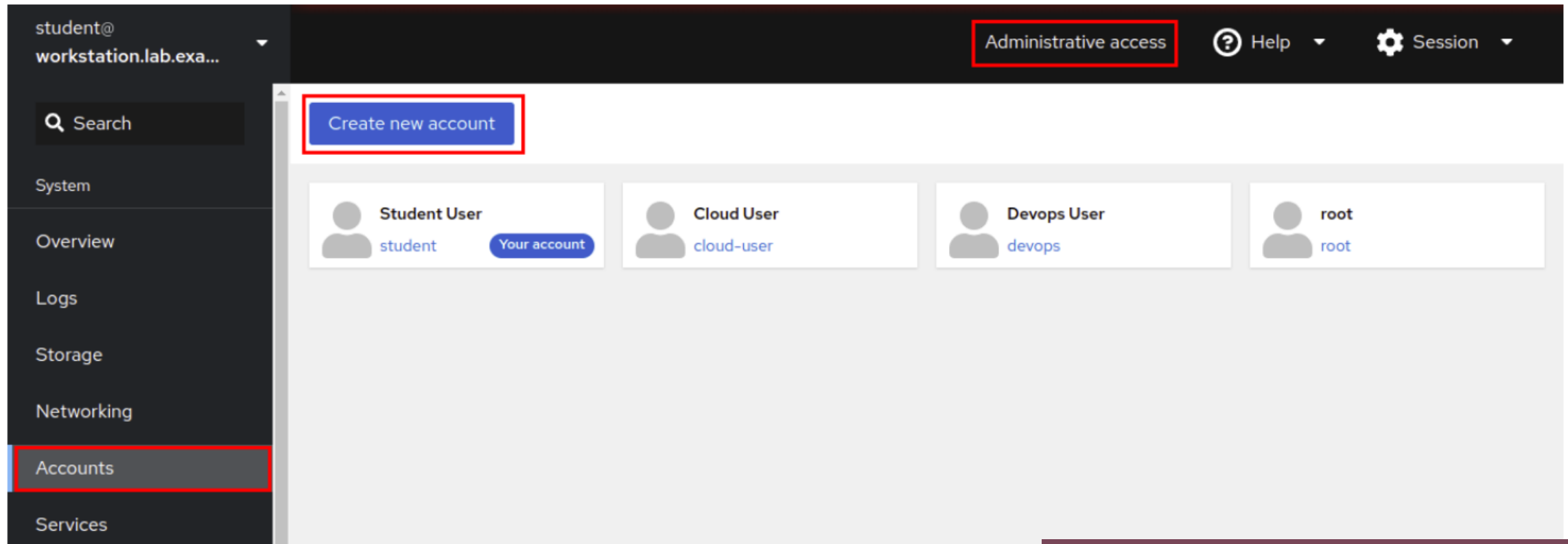
Server

172.25.250.220



Administer User Accounts

As a privileged user, you can create user accounts in the web console. Click **Accounts** on the navigation bar to view existing accounts. Click **Create new account** to open the account management page.



Create new account

Full name

New User

User name

nuser

Password

.....

Excellent password

Confirm

.....

Options

☐ Disallow interactive password ?

Create

Cancel

Generate an sos Report from the Command Line

Red Hat Enterprise Linux installs the `sos` report utility with the `sos` package:

```
[root@host ~]# dnf install sos
...output omitted...
Complete!
```

Generating the `sos` report requires root privileges. Run the `sos report` command to generate the report.

```
[root@host ~]# sos report
...output omitted...
Press ENTER to continue, or CTRL-C to quit.

Optionally, please enter the case id that you are generating this report for []:
...output omitted...
Your sosreport has been generated and saved in:
  /var/tmp/sosreport-host-2022-03-29-wixbhpz.tar.xz
..output omitted...
Please send this file to your support representative.
```

Verify that the `sos report` command created the archive file at the previous location.

```
[root@host ~]# ls -l /var/tmp/
total 9388
-rw-----. 1 root root 9605952 Mar 29 02:09 sosreport-host-2022-03-29-wixbhpz.tar.xz
-rw-r--r--. 1 root root      65 Mar 29 02:09 sosreport-host-2022-03-29-wixbhpz.tar.xz.sha256
...output omitted...
```

The `sos clean` command obfuscates personal information from the report.

```
[root@host ~]# sos clean /var/tmp/sosreport-host-2022-03-29-wixbhpz.tar.xz*
...output omitted...
Press ENTER to continue, or CTRL-C to quit.
...output omitted...
The obfuscated archive is available at
  /var/tmp/sosreport-host0-2022-03-29-wixbhpz-obfuscated.tar.xz
...output omitted...
Please send the obfuscated archive to your support representative and keep the mapping file private
```

Send an sos Report to Red Hat Technical Support

Select one of these methods to send an `sos` report to Red Hat Technical Support.

- Send an `sos` report by using the `sos report` command `--upload` option.
- Send an `sos` report to the Red Hat Customer Portal by attaching it with the support case.

End of Chapter 14

*Thank
you*

