# Practice M7: Databases, Web Servers and Web Applications

\* NOTE: Most of the exercises included in this practice guide are **not suitable** for execution in **WSL** or **Docker** environment. It is recommended a virtual infrastructure to be used instead.

For the purpose of the current practice we will need one virtual machine. It could be with either **CentOS 8.x**, **openSUSE Leap 15.x**, or **Ubuntu 20.04**. Of course, another version of the listed or another distribution can be used, but there can be some differences.

All commands, that we will use until the end of this practice, will be accompanied by the appropriate prompt. This way it will be easier for us to know which user, in which folder, and on which machine is executing the command.

Next steps will be executed on **CentOS** machine. If there is a big difference in the way we issue the command, or in its result between distributions, it will be stated clearly.

## Part 1 (Apache Web Server)

If we do not have **unzip**, **pstree**, and **tree** installed, we can do it with:

[lsauser@centos ~]$ **sudo dnf install -y unzip psmisc tree**

Now, we can install the web server. The package is named **httpd** in **CentOS** and **apache2** in **openSUSE** and **Ubuntu**.

### Installation

Installation steps are the following:

[lsauser@centos ~]$ **sudo dnf install -y httpd httpd-tools**

...

[lsauser@centos ~]$ **sudo systemctl enable httpd**

...

[lsauser@centos ~]$ **sudo systemctl start httpd**

[lsauser@centos ~]$ **systemctl status httpd**

...

Alternatively, we can substitute both **systemctl enable** and **systemctl start** with one command:

[lsauser@centos ~]$ **sudo systemctl enable --now httpd**

### Processes and Configuration

We can check the process tree for the web server with:

[lsauser@centos ~]$ **pstree -ps $(pgrep -U 0 httpd)**

systemd(1)───httpd(4085)─┬─httpd(4086)

├─httpd(4087)

├─httpd(4088)

├─httpd(4089)

└─httpd(4090)

[lsauser@centos ~]$

Then we can examine the configuration files and folders hierarchy with:

[lsauser@centos ~]$ **tree /etc/httpd**

/etc/httpd

├── conf

│   ├── httpd.conf

│   └── magic

├── conf.d

│   ├── autoindex.conf

│   ├── README

│   ├── userdir.conf

│   └── welcome.conf

├── conf.modules.d

│   ├── 00-base.conf

│   ├── 00-dav.conf

│   ├── 00-lua.conf

│   ├── 00-mpm.conf

│   ├── 00-proxy.conf

│   ├── 00-systemd.conf

│   └── 01-cgi.conf

├── logs -> ../../var/log/httpd

├── modules -> ../../usr/lib64/httpd/modules

└── run -> /run/httpd

6 directories, 13 files

[lsauser@centos ~]$

Current configuration could be checked with:

[lsauser@centos ~]$ **apachectl configtest**

AH00558: httpd: Could not reliably determine the server’s fully qualified domain name, using fe80::20e4:7087:87b4:aa9e. Set the ‘ServerName’ directive globally to suppress this message

Syntax OK

[lsauser@centos ~]$

If we receive a message like the one above, it does not mean that the service is not working, but that it has difficulties to resolve the fully qualified domain name (**FQDN**) of our machine. We can tackle the issue by adding editing the main configuration file:

[lsauser@centos ~]$ **sudo vi /etc/httpd/conf/httpd.conf**

# If your host doesn’t have a registered DNS name, enter its IP address here.

#

ServerName centos.lsa.lab:80

...

Then, we must add a corresponding line in our **/etc/hosts** file:

[lsauser@centos ~]$ **echo ‘10.0.2.15 centos.lsa.lab centos’ | sudo tee -a /etc/hosts**

Where **10.0.2.15** should be changed to our **IP** address.

Now, we can re-execute the check and restart the web service eventually.

### Local Access

Next, we can try to open our default web page locally. For this, we can install a command line browser. Some of the most popular ones are **lynx**, **links**, **elinks**, and **w3m**. Let’s install one and navigate to our page:

[lsauser@centos ~]$ **sudo dnf install -y lynx**

...

[lsauser@centos ~]$ **lynx** [**http://centos**](http://centos)

We can quit with the **q** key.

Alternative and very common way of testing web pages is the curl command:

[lsauser@centos ~]$ **curl** [**http://centos**](http://centos)

### Remote Access

We can test our page from the host as well, but first we should take care of few things.

First, we must open a port in the firewall if running. Please note, in which zone is your network interface:

[lsauser@centos ~]$ **sudo firewall-cmd --add-service=http --zone=public --permanent**

success

[lsauser@centos ~]$ **sudo firewall-cmd --reload**

success

[lsauser@centos ~]$

Then we must check how our virtual network adapter was set up. If it is in **Bridge** mode, then we must check what it our **IP** address. Then open a browser tab and navigate to **http://[ip-of-our-vm]**

If we are in **NAT** mode, then we must set up a port forwarding rule. For example, port **8000** on the host to point to port **80** of the **VM**. Then open a browser tab and navigate to [**http://localhost:8000**](http://localhost:8000)

It is time to change the default web page to something custom. Let’s create a tiny static web page:

[lsauser@centos ~]$ **echo '<h1>My test site! :)</h1>' | sudo tee /var/www/html/index.htm**l

<h1>My test site! :)</h1>

[lsauser@centos ~]$ **lynx** [**http://centos**](http://centos)

### Deploy a Web Page

Let’s go to the next level. We will deploy a set of files that belong to a web page.

For this we can either download the archive on our host, and then with the help of the **scp** (or **WinSCP** if we are on **Windows**) command to copy it on the **VM** or use a command line tool to download it directly on the **VM**.

In any case the archive is available on the page of the current module and via a direct link: <https://zahariev.pro/files/lsa-m7-practice.zip>

Should we choose the first option, we must execute something like:

[dimitar@lenovo-e450-dz ~]$ **scp -P 30001 lsa-m7-practice.zip lsauser@localhost:.**

Of course, we should adjust both **the port and the path**.

As stated above, we can do all the tasks while on the **VM**. For this purpose, we can download the archive either with:

[lsauser@centos ~]$ **curl -o lsa-m7-practice.zip** [**https://zahariev.pro/files/lsa-m7-practice.zip**](https://zahariev.pro/files/lsa-m7-practice.zip)

Or with:

[lsauser@centos ~]$ **wget** [**https://zahariev.pro/files/lsa-m7-practice.zip**](https://zahariev.pro/files/lsa-m7-practice.zip)

Now, that we have the archive, we can first check what it contains with:

[lsauser@centos ~]$ **unzip -l lsa-m7-practice.zip**

Archive: lsa-m7-practice.zip

Length Date Time Name

--------- ---------- ----- ----

281 01-16-2018 09:39 index.html

78024 10-23-2017 19:25 wizard.png

--------- -------

78305 2 files

[lsauser@centos ~]$

Then extract it in the target folder:

[lsauser@centos ~]$ **sudo unzip lsa-m7-practice.zip -d /var/www/html**

Because in the target folder exists file with name **index.html**, we will be asked if we want to overwrite it. If we are sure in our actions since the beginning, we can execute a modified version of the command. It will overwrite files in the target directory without asking:

[lsauser@centos ~]$ **sudo unzip -o lsa-m7-practice.zip -d /var/www/html**

Now, we can check the result either locally or on our host.

### Virtual Hosts

We can end up in situation when there is a need to serve more than one site on a single host. There are many ways to solve this task. One viable option is to use the virtual hosts. There are slight differences how this is achieved amongst different distributions.

Let’s create a new configuration file **/etc/httpd/conf.d/main.conf**:

[lsauser@centos ~]$ **sudo vi /etc/httpd/conf.d/main.conf**

<VirtualHost \*:80>

ServerName "centos.lsa.lab"

DocumentRoot "/var/www/html"

</VirtualHost>

You should change the server name value to match yours.

Now, we can test the changes with:

[lsauser@centos ~]$ **apachectl configtest**

If everything is okay, we can make a copy of the configuration file and change it a bit:

[lsauser@centos ~]$ **sudo cp /etc/httpd/conf.d/main.conf /etc/httpd/conf.d/secret.conf**

[lsauser@centos ~]$ **sudo vi /etc/httpd/conf.d/secret.conf**

<VirtualHost \*:80>

ServerName "secret.lsa.lab"

DocumentRoot "/var/www/secret"

</VirtualHost>

Let’s check the configuration again:

[lsauser@centos ~]$ **apachectl configtest**

AH00112: Warning: DocumentRoot [/var/www/secret] does not exist

Syntax OK

[lsauser@centos ~]$

It appears that we must create the folder in question. Let’s do it and then check the configuration again:

[lsauser@centos ~]$ **sudo mkdir /var/www/secret**

[lsauser@centos ~]$ **apachectl configtest**

Syntax OK

[lsauser@centos ~]$

We can create a simple html page:

[lsauser@centos ~]$ **echo "<h1>Secret Web Site</h1>" | sudo tee /var/www/secret/index.html**

<h1>Secret Web Site</h1>

[lsauser@centos ~]$

Let’s restart the web server:

[lsauser@centos ~]$ **sudo systemctl restart httpd**

We must add a row in our **/etc/hosts** file:

[lsauser@centos ~]$ **echo '127.0.0.1 secret.lsa.lab secret' | sudo tee -a /etc/hosts**

127.0.0.1 secret secret.lsa.lab

[lsauser@centos ~]$

And finally, let’s test both virtual hosts locally:

[lsauser@centos ~]$ **curl http://centos.lsa.lab**

<html>

<head>

<title>Congratulations!</title>

</head>

<body>

<div align="center">

<h1>Congratulations You Made It!</h1>

<img src="wizard.png" />

<h1>May the force be with you on your journey as Linux Administrator!</h1>

</div>

</body>

</html>

[lsauser@centos ~]$ **curl http://secret.lsa.lab**

<h1>Secret Web Site</h1>

[lsauser@centos ~]$

### **Logs**

Let’s change the default log configuration for one of the virtual hosts:

[lsauser@centos ~]$ **sudo vi /etc/httpd/conf.d/main.conf**

<VirtualHost \*:80>

ServerName "centos.lsa.lab"

DocumentRoot "/var/www/html"

**ErrorLog "logs/centos\_error.log"**

**CustomLog "logs/centos\_access.log" common**

</VirtualHost>

Should we want to learn more about logs in general, we can explore the main configuration file:

[lsauser@centos ~]$ **cat /etc/httpd/conf/httpd.conf | grep -B 1 -A 1 -i logformat**

#

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined

LogFormat "%h %l %u %t \"%r\" %>s %b" common

--

# You need to enable mod\_logio.c to use %I and %O

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio

</IfModule>

[lsauser@centos ~]$

We can test the configuration and if everything is okay, we must restart the service:

[lsauser@centos ~]$ **apachectl configtest**

Syntax OK

[lsauser@centos ~]$ **sudo systemctl restart httpd**

Now, we can ask for the access log, then access the site, and finally ask for the log again:

[lsauser@centos ~]$ **cat /var/log/httpd/centos\_access.log**

[lsauser@centos ~]$ **curl http://centos.lsa.lab**

...

[lsauser@centos ~]$ **cat /var/log/httpd/centos\_access.log**

127.0.0.1 - - [19/Mar/2019:20:49:29 +0200] "GET / HTTP/1.1" 200 281

[lsauser@centos ~]$

### Access Control by IP

We can open the configuration file of one of the virtual hosts and add a restriction by IP address:

[lsauser@centos ~]$ **sudo vi /etc/httpd/conf.d/main.conf**

...

**<Location />**

**Require ip 127.0.0.1**

**</Location>**

...

Save and close the file. Now test the configuration and then restart the service:

[lsauser@centos ~]$ **apachectl configtest**

Syntax OK

[lsauser@centos ~]$ **sudo systemctl restart httpd**

Now, we can try to access the site locally both on the localhost address and the external address. The first try must succeed, while the second should fail.

### Access Control by Users

Now, let’s change the configuration of the second virtual host:

[lsauser@centos ~]$ **sudo vi /etc/httpd/conf.d/secret.conf**

<VirtualHost \*:80>

ServerName "secret.lsa.lab"

DocumentRoot "/var/www/secret"

**<Directory "/var/www/secret">**

**Require valid-user**

**AuthType Basic**

**AuthName "Private Access"**

**AuthBasicProvider file**

**AuthUserFile "/etc/httpd/conf.d/secret"**

**</Directory>**

</VirtualHost>

Now, we must save and close the file. Then check the configuration and restart the service:

[lsauser@centos ~]$ **apachectl configtest**

Syntax OK

[lsauser@centos ~]$ **sudo systemctl restart httpd**

Before we can test the secured access to our resources, we must create two users:

[lsauser@centos ~]$ **sudo htpasswd -c /etc/httpd/conf.d/secret john**

New password: **12345**

Re-type new password: **12345**

Adding password for user john

[lsauser@centos ~]$ **sudo htpasswd /etc/httpd/conf.d/secret jane**

New password: **qwerty**

Re-type new password: **qwerty**

Adding password for user jane

Please note, that the passwords won’t be displayed on the screen.

If we are curios, we can check what is inside the secret file:

[lsauser@centos ~]$ **cat /etc/httpd/conf.d/secret**

john:$apr1$TyQmtE43$ozVKcS0ZumoAlzqHLqU7n1

jane:$apr1$rbaWsVZN$PtF41XwxSJwHxlnq85WmS1

[lsauser@centos ~]$

Finally, we can test if our security mechanism is working as expected:

[lsauser@centos ~]$ **lynx** [**http://secret**](http://secret)**.lsa.lab**

## Part 2 (MariaDB)

### Installation

Let’s install one of the most common relational databases under Linux – **MariaDB**:

[lsauser@centos ~]$ **sudo dnf install -y mariadb mariadb-server**

The corresponding packages in **openSUSE** are named **mariadb** and **mariadb-client**, while in **Ubuntu** they are **mariadb-server** and **mariadb-client**.

After the installation is finished, we could enable the service to start on boot and start it in the current session:

[lsauser@centos ~]$ **sudo systemctl enable --now mariadb**

[lsauser@centos ~]$ **systemctl status mariadb**

…

It is a good practice to strengthen the security a bit of a new installation:

[lsauser@centos ~]$ **sudo mysql\_secure\_installation**

### Work with the Database

As with other client-server solutions, here there is also a client tool, which is named **mysql** (still).

Let’s try to connect to the database:

[lsauser@centos ~]$ **mysql -u root -p**

…

MariaDB [(none)]>

### User and Database Creation

It is time to create an empty database. Let’s create one, named employees:

**create database employees;**

We must restrict the access to the database. For this purpose, we will create a user:

**grant all on employees.\* to user@localhost identified by 'Password1';**

...

**flush privileges;**

### Our First Table

What is a database without its tables? Let’s create one. It will store our employees:

**USE employees;**

**CREATE TABLE persons (**

**id INT,**

**department\_id INT,**

**person\_name VARCHAR(50),**

**person\_sex CHAR(1),**

**person\_salary DECIMAL(15, 3)**

**);**

Having an empty table is not a big deal. Let’s add few records:

**INSERT INTO persons (id, department\_id, person\_name, person\_sex, person\_salary)**

**VALUES (1, 1, 'John Smith', 'M', 5000),**

**(2, 2, 'Tony James', 'M', 3000),**

**(3, 3, 'Kate Hudson', 'F', 1500),**

**(4, 1, 'Ann Evans', 'F', 3500);**

### Work with Data

Now, that we have a table with some data, it is time to ask questions against it. For example, we can ask for the identification number and person name of all records:

**SELECT id, person\_name**

**FROM persons;**

Then we can change our question to – give me identification number and person name of all women:

**SELECT id, person\_name**

**FROM persons**

**WHERE person\_sex='F';**

Even though there are only few rows, we can start experimenting. We can add more rows if needed.

### Second Table

It would be good to have a second table with some data. This way, could test our knowledge about multi table queries. Let’s create one named departments:

**CREATE TABLE departments (**

**id INT,**

**department\_name VARCHAR(25)**

**);**

Now, let’s add few records:

**INSERT INTO departments (id, department\_name) VALUES**

**(1, 'IT'),**

**(2, 'Accounting'),**

**(3, 'Sales');**

### Combine and Update Data

Even though it is not considered a good practice when querying for data, we will break the rules, and will construct a query, that will answer a question like – give me everything about all rows in the table:

**SELECT \***

**FROM departments;**

Now, let’s combine information from both tables. We will create a list of all employees and the department to which they belong:

**SELECT p.person\_name, d.department\_name**

**FROM persons p**

**INNER JOIN departments d**

**ON p.department\_id = d.id;**

Sooner or later, we will find ourselves in a need to update records. Let’s do it now. We will increase the salary of all women with 2000 units:

**UPDATE persons**

**SET salary=salary+2000**

**WHERE person\_sex = 'F';**

We can check what we did:

**SELECT \***

**FROM persons;**

### Backup and Restore

Let’s try a simple backup-restore routing, but first we must close our session to the database:

**quit**

Now, in order to create a backup of our database, we must execute:

[lsauser@centos ~]$ **mysqldump -u root -p employees > employees.sql**

Enter password:

[lsauser@centos ~]$ **ls -al employees.sql**

-rw-rw-r--. 1 lsauser lsauser 2775 19 мар 22,31 employees.sql

[lsauser@centos ~]$

In order to test the backup, we must connect again to the database and delete something:

[lsauser@centos ~]$ **mysql -u root -p**

**USE employees;**

**DELETE FROM persons;**

Close again the session with:

**quit**

It is time to check if we can restore the database as it was before the deletion:

[lsauser@centos ~]$ **mysql -u root -p employees < employees.sql**

...

And the final proof:

[lsauser@centos ~]$ **mysql -u root -p**

**USE employees;**

**SELECT \***

**FROM persons;**

**quit**

## Part 3 (PHP + Apache HTTP + MariaDB)

The only missing **LAMP** component so far is the **PHP**. We will add it during this part.

### PHP Installation

Let’s first install **PHP** itself and one library used to connect from **PHP** to **MySQL/MariaDB** and then restart the web server:

[lsauser@centos ~]$ **sudo dnf install -y php php-mysqlnd**

...

[lsauser@centos ~]$ **sudo systemctl restart httpd**

Before we continue further, we can check if everything with the PHP installation is okay:

[lsauser@centos ~]$ **php -i**

Then, we can test the integration with the web server:

[lsauser@centos ~]$ **sudo vi /var/www/html/index.php**

**<h1>Current PHP configuration:</h1>**

**<?php**

**phpinfo();**

**?>**

[lsauser@centos ~]$ **lynx http://localhost/index.php**

### Combine PHP with MariaDB

It won’t be a good practice without a working example combining **PHP** with **MariaDB**. We will prepare a script, which will list all employees and the departments they belong to.

The task can be achieved in many ways. For our approach, we will use this script:

[lsauser@centos ~]$ **sudo vi /var/www/secret/index.php**

<!DOCTYPE HTML>

<html>

<head>

<title>Employees List</title>

</head>

<body>

<h1>Employees List</h1>

<?php

// variables initialization

$host="localhost";

$user="user";

$password="Password1";

$db="employees";

// establish a connection

if ($dbh=mysqli\_connect($host, $user, $password, $db)) {

// initialize the query statement

$query="SELECT p.person\_name, d.department\_name FROM persons p LEFT JOIN departments d ON p.department\_id=d.id";

if ($result=mysqli\_query($dbh, $query)) {

// we have data, so let's list it

echo "<ol>";

while ($row=mysqli\_fetch\_array($result, MYSQLI\_ASSOC)) {

echo "<li>".$row['person\_name'].", ".$row['department\_name']."</li>";

}

echo "</ol>";

}

else

echo "<h2>ERROR: No data!</h2>";

}

else

echo "<h2>ERROR: No connection!</h2>";

?>

</body>

</html>

Save and close the file.

Now, it is time to test what we produced:

[lsauser@centos ~]$ **lynx http://secret.lsa.lab/index.php**

## Part 4 (Web Interfaces)

### Cockpit

This is one of the available solutions for remote web management of Linux servers.

There are different installation options. We will go with the easiest – we will install it like an ordinary package:

[lsauser@centos ~]$ **sudo dnf install -y cockpit**

[lsauser@centos ~]$ **sudo systemctl enable --now cockpit.socket**

[lsauser@centos ~]$ **sudo firewall-cmd --permanent --zone=public --add-service=cockpit**

[lsauser@centos ~]$ **sudo firewall-cmd --reload**

When the installation is finished, we can test it with:

<https://ip-address-of-machine:9090>

### Webmin

This is one of the oldest solutions with rich set of functionalities. As usual, there are multiple ways for installation.

**Option 1:**

Download the package:

[lsauser@centos ~]$ **wget http://prdownloads.sourceforge.net/webadmin/webmin-1.974-1.noarch.rpm**

Then install required dependencies:

[lsauser@centos ~]$ **dnf -y install perl perl-Net-SSLeay openssl perl-IO-Tty perl-Encode-Detect**

And then install it:

[lsauser@centos ~]$ **sudo rpm -ivh webmin-1.974-1.noarch.rpm**

**Option 2:**

We can add a new repository and then install it like a standard package:

[lsauser@centos ~]$ **cat << EOF | sudo tee /etc/yum.repos.d/webmin.repo**

**[Webmin]**

**name=Webmin Distribution Neutral**

**#baseurl=https://download.webmin.com/download/yum**

**mirrorlist=https://download.webmin.com/download/yum/mirrorlist**

**enabled=1**

**EOF**

Then download and import the key:

[lsauser@centos ~]$ **wget https://download.webmin.com/jcameron-key.asc**

[lsauser@centos ~]$ **rpm --import jcameron-key.asc**

And finally install it:

[lsauser@centos ~]$ **sudo dnf install -y webmin**

Now, we can test it, by visiting the following address:

<https://ip-address-of-machine:10000/>

You must use the **root** user to login

Should we want to access it from other hosts, we must open the appropriate port:

[lsauser@centos ~]$ **sudo firewall-cmd --zone=public --add-port=10000/tcp --permanent**

[lsauser@centos ~]$ **sudo firewall-cmd --reload**