

Tiered app

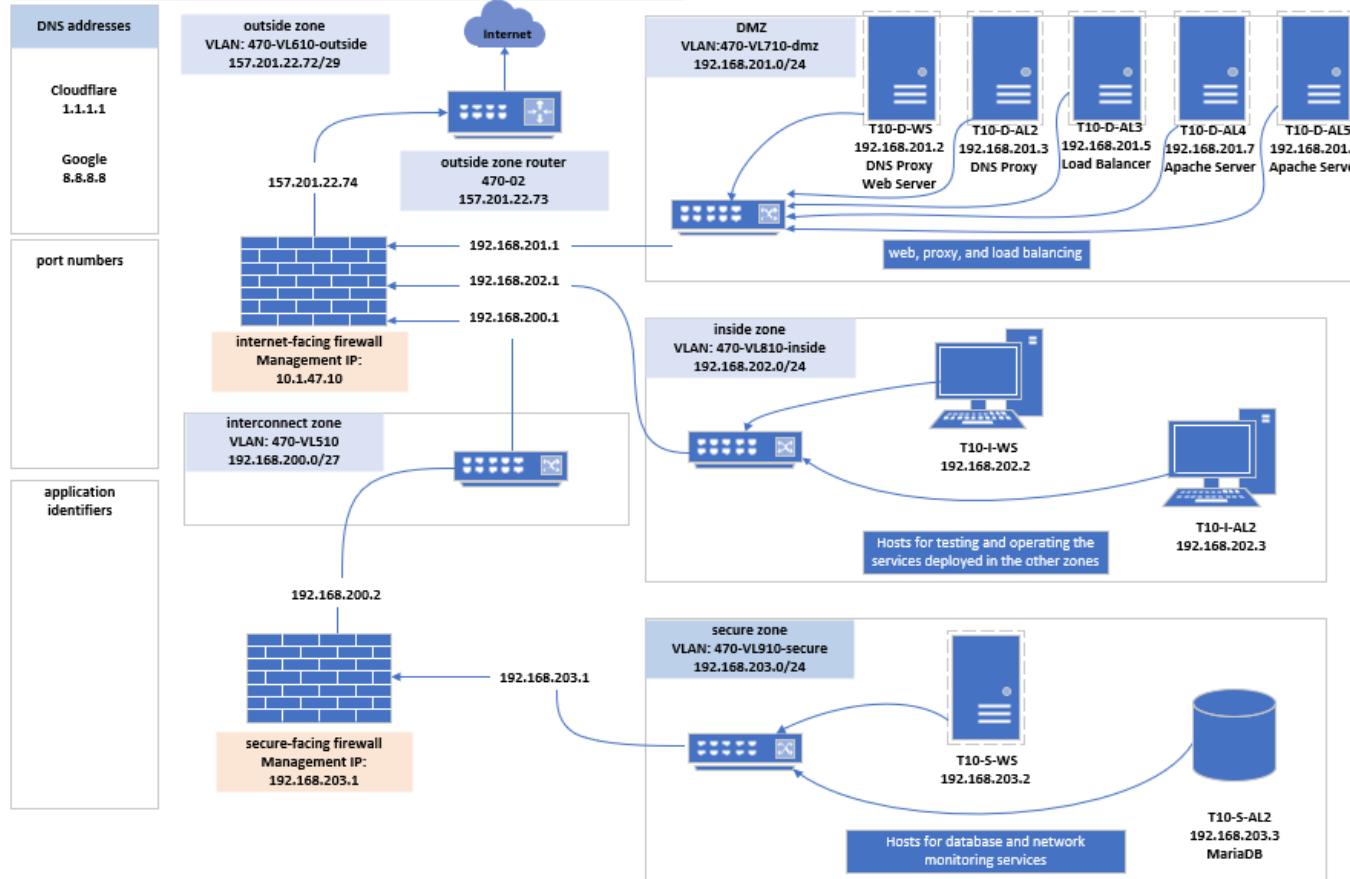
By Carlos Gerez, Christopher Ditto , and Mark Riley Slik

cit470

Task: Diagram

team 10 Layer 3: outside zones' public IPv4 address assignments

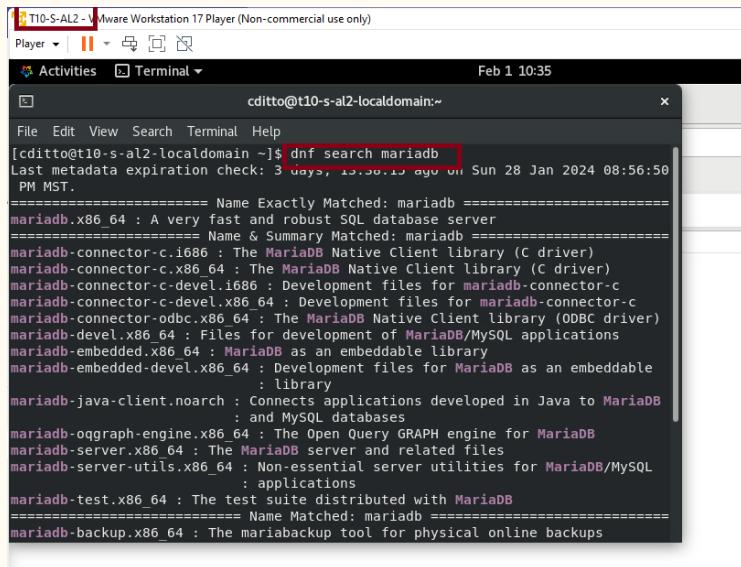
public space (IPv4 subnet ID)	router	firewall (dynamic NAT)	static NAT	(broadcast)
157.201.22.72/29	157.201.22.73	157.201.22.74	157.201.22.75-	157.201.22.79



Mariadb installation

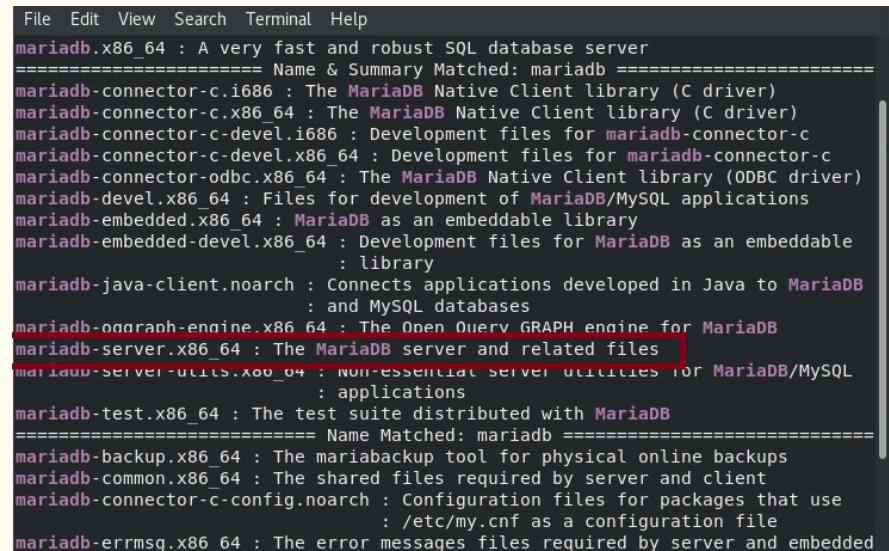
First search to see what options we have as mariadb. Mariadb-server is the one we will use.

```
dnf search mariadb
```



```
[T10-S-AL2 - VMware Workstation 17 Player (Non-commercial use only)
Player | Activities | Terminal | Help
Activities Terminal ~
Feb 1 10:35
cditto@t10-s-al2-localhost:~]
File Edit View Search Terminal Help
[cditto@t10-s-al2-localhost ~]$ dnf search mariadb
Last metadata expiration check: 3 days, 15:30:19 ago on Sun 28 Jan 2024 08:56:50
PM MST.
=====
Name Exactly Matched: mariadb =====
mariadb.x86_64 : A very fast and robust SQL database server
=====
Name & Summary Matched: mariadb =====
mariadb-connector-c.i686 : The MariaDB Native Client library (C driver)
mariadb-connector-c.x86_64 : The MariaDB Native Client library (C driver)
mariadb-connector-c-devel.i686 : Development files for mariadb-connector-c
mariadb-connector-c-devel.x86_64 : Development files for mariadb-connector-c
mariadb-connector-odbc.x86_64 : The MariaDB Native Client library (ODBC driver)
mariadb-devel.x86_64 : Files for development of MariaDB/MySQL applications
mariadb-embedded.x86_64 : MariaDB as an embeddable library
mariadb-embedded-devel.x86_64 : Development files for MariaDB as an embeddable
                               : library
mariadb-java-client.noarch : Connects applications developed in Java to MariaDB
                               : and MySQL databases
mariadb-oqgraph-engine.x86_64 : The Open Query GRAPH engine for MariaDB
mariadb-server.x86_64 : The MariaDB server and related files
mariadb-server-utils.x86_64 : Non-essential server utilities for MariaDB/MySQL
                               : applications
mariadb-test.x86_64 : The test suite distributed with MariaDB
=====
Name Matched: mariadb =====
mariadb-backup.x86_64 : The mariabackup tool for physical online backups

```



```
File Edit View Search Terminal Help
=====
mariadb.x86_64 : A very fast and robust SQL database server
=====
Name & Summary Matched: mariadb =====
mariadb-connector-c.i686 : The MariaDB Native Client library (C driver)
mariadb-connector-c.x86_64 : The MariaDB Native Client library (C driver)
mariadb-connector-c-devel.i686 : Development files for mariadb-connector-c
mariadb-connector-c-devel.x86_64 : Development files for mariadb-connector-c
mariadb-connector-odbc.x86_64 : The MariaDB Native Client library (ODBC driver)
mariadb-devel.x86_64 : Files for development of MariaDB/MySQL applications
mariadb-embedded.x86_64 : MariaDB as an embeddable library
mariadb-embedded-devel.x86_64 : Development files for MariaDB as an embeddable
                               : library
mariadb-java-client.noarch : Connects applications developed in Java to MariaDB
                               : and MySQL databases
mariadb-oqgraph-engine.x86_64 : The Open Query GRAPH engine for MariaDB
mariadb-server.x86_64 : The MariaDB server and related files
=====
mariadb-server-utils.x86_64 : Non-essential server utilities for MariaDB/MySQL
                               : applications
mariadb-test.x86_64 : The test suite distributed with MariaDB
=====
Name Matched: mariadb =====
mariadb-backup.x86_64 : The mariabackup tool for physical online backups
mariadb-common.x86_64 : The shared files required by server and client
mariadb-connector-c-config.noarch : Configuration files for packages that use
                               : /etc/my.cnf as a configuration file
mariadb-errmsg.x86_64 : The error messages files required by server and embedded
```

We can see his info and in the second command install it.

```
[cditto@t10-s-al2-localhost ~]$ dnf info mariadb-server
=====
Summary: MariaDB is a multi-user, multi-threaded SQL database server. It
is a client/server implementation consisting of a server daemon
(mysql) and many different client programs and libraries. This
package contains the MariaDB server and some accompanying files
and directories. MariaDB is a community developed branch of
MySQL.

=====
Available Packages
Name        : mariadb-server
Epoch       : 3
Version     : 10.3.39
Release    : 1.module_el8.8.0+3609+204d4ab0
Architecture : x86_64
Size        : 16 M
Source      : mariadb-10.3.39-1.module_el8.8.0+3609+204d4ab0.src.rpm
Repository   : appstream
Summary     : The MariaDB server and related files
URL         : http://mariadb.org
License     : GPLv2 with exceptions and GPLv2 and OSS
Description  : MariaDB is a multi-user, multi-threaded SQL database server. It
is a client/server implementation consisting of a server daemon
(mysql) and many different client programs and libraries. This
package contains the MariaDB server and some accompanying files
and directories. MariaDB is a community developed branch of
MySQL.

[cditto@t10-s-al2-localhost ~]$
```

`dnf info mariadb`

`sudo dnf -y install mariadb-server`

```
[cgarcia@t10-s-al2-localhost ~]$ sudo dnf -y install mariadb-server
[sudo] password for cgarcia:
Last metadata expiration check: 2:03:04 ago on Thu 01 Feb 2024 08:50:13 AM MST.
Dependencies resolved.
=====
Package          Arch      Version           Repo      Size
=====
Installing:
  mariadb-server    x86_64    3:10.3.39-1.module_el8.8.0+3609+204d4ab0  appstream  16 M
Installing dependencies:
  mariadb-errmsg    x86_64    3:10.3.39-1.module_el8.8.0+3609+204d4ab0  appstream 234 k
  perl-DBD-MYSQL   x86_64    4.046-3.module_el8.6.0+2827+49d66dc3    appstream 155 k
Installing weak dependencies:
  mariadb-backup    x86_64    3:10.3.39-1.module_el8.8.0+3609+204d4ab0  appstream 6.1 M
  mariadb-gssapi-server
                    x86_64    3:10.3.39-1.module_el8.8.0+3609+204d4ab0  appstream 51 k
  mariadb-server-utils
                    x86_64    3:10.3.39-1.module_el8.8.0+3609+204d4ab0  appstream 1.1 M
Enabling module streams:
  perl-DBD-MYSQL          4.046
Transaction Summary
```

Installation is complete, check for the following files in mariadb package using `rpm -ql mariadb-server`

```
[3/6]: mariadb-server-utils-10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_6 1/1
[4/6]: perl-DBD-MySQL-4.046-3.module_el8.6.0+2827+49d66dc3.x86_6 1/1
[5/6]: mariadb-backup-10.3.39-1.module_el8.8.0+3609+7.4 MB/s | 155 kB 00:00
[6/6]: mariadb-server-10.3.39-1.module_el8.8.0+3609+10 MB/s | 16 MB 00:01
-----
Total 11 MB/s | 24 MB 00:02

Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing : 1/1
  Installing : perl-DBD-MySQL-4.046-3.module_el8.6.0+2827+49d66dc3.x86_6 1/6
  Installing : mariadb-errmsg-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x 2/6
  Installing : mariadb-gssapi-server-3:10.3.39-1.module_el8.8.0+3609+204 3/6
  Installing : mariadb-server-utils-3:10.3.39-1.module_el8.8.0+3609+204d 4/6
  Running scriptlet: mariadb-server-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x 5/6
  Installing : mariadb-server-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x 5/6
  Running scriptlet: mariadb-server-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x 5/6
  Installing : mariadb-backup-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x 6/6
  Running scriptlet: mariadb-backup-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x 6/6
  Verifying : mariadb-backup-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x 1/6
  Verifying : mariadb-errmsg-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x 2/6
  Verifying : mariadb-gssapi-server-3:10.3.39-1.module_el8.8.0+3609+204 3/6
  Verifying : mariadb-server-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x 4/6
  Verifying : mariadb-server-utils-3:10.3.39-1.module_el8.8.0+3609+204d 5/6
  Verifying : perl-DBD-MySQL-4.046-3.module_el8.6.0+2827+49d66dc3.x86_6 6/6

Installed:
  mariadb-backup-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64
  mariadb-errmsg-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64
  mariadb-gssapi-server-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64
  mariadb-server-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64
  mariadb-server-utils-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64
  perl-DBD-MySQL-4.046-3.module_el8.6.0+2827+49d66dc3.x86_64

Complete!
[cgarcia@10-s-al2-localhost ~]$
```

/usr/lib/systemd/system/mariadb.service

/user/bin/mysql_secure_installation

```
Complete!
[centos@el10 ~]$ rpm -q mariadb-server
/etc/lokalestate.d/mariadb
/etc/my.cnf.d/mariadb_encryption.preset
/etc/my.cnf.d/mariadb-server.cnf
/etc/my.cnf.d/mariadb-user.map.cnf
/run/mariadb
/usr/bin/aria_chk
/usr/bin/aria_dump_log
/usr/bin/aria_error_log
/usr/bin/aria_pack
/usr/bin/aria_read_log
/usr/bin/innochecksum
/usr/bin/mariadb-service-convert
/usr/bin/mariadb-service-defaults
/usr/bin/myisam_fldump
/usr/bin/myisamchk
/usr/bin/myisamlog
/usr/bin/myisampack
/usr/bin/mysqlbinlog --raw --no-hdr
/usr/bin/mysql_secure_installation
/usr/bin/mysql_low_level
/usr/bin/mysql_safe
/usr/bin/mysql_secure_helper
/usr/bin/replace
/usr/bin/resolve_stack_dump
/usr/bin/resolveip
/usr/bin/mariabackup
/usr/bin/wsrep_sst_common
/usr/bin/wsrep_sst_mariabackup
/usr/bin/wsrep_sst_myisaldump
/usr/bin/wsrep_sst_rsync
/usr/bin/wsrep_sst_rsync_tunnel
/usr/bin/wsrep_sst_rsync_wan
/usr/lib/build_id
/usr/lib/build_id@/04
/usr/lib/build_id@/05
/usr/lib/build_id@/05/f61df238e13d6305b5fe629d5cf69084fce
/usr/lib/build_id@/09
/usr/lib/build_id@/09/004d57751b12c130e8bc588381edc194c57489100b0
/usr/lib/build_id@/09/004d57751b12c130e8bc588381edc194c57489100b0
/usr/lib/build_id@/4/8ca3f7b43a07e01e67ec7e61b79a65930
File Edit View Search Terminal Help
/usr/lib/build_id@/cc
/usr/lib/build_id@/cc5479440148119c89d35feed3dd46969f542e12
/usr/lib/build_id@/cd
/usr/lib/build_id@/cd00d1fe0848dc81aa67991283e2592812cd0
/usr/lib/build_id@/cd00d1fe0848dc81aa67991283e2592812cd0
/usr/lib/build_id@/cd/e6/c940979f2f3e31c188ccb05e59950917fc
/usr/lib/build_id@/cd/e6/c940979f2f3e31c188ccb05e59950917fc
/usr/lib/build_id@/cd/e8/3263a99c88ba70f934a19ffbc5fd197315b246
/usr/lib/build_id@/ea
/usr/lib/build_id@/ea68851a0893f2ebf4280888d5cb3921a
/usr/lib/build_id@/ea68851a0893f2ebf4280888d5cb3921a
/usr/lib/build_id@/ea68851a0893f2ebf4280888d5cb3921a
/usr/lib/build_id@/ea68851a0893f2ebf4280888d5cb3921a
/usr/lib/build_id@/ed
/usr/lib/build_id@/ed4a1fc359803190429efaf1f52b1c5e501f1
/usr/lib/build_id@/ed4a1fc359803190429efaf1f52b1c5e501f1
/usr/lib/build_id@/f1/27c268457cb026583a8948852d1ee9e31e6
/usr/lib/build_id@/f6
/usr/lib/build_id@/f6/c9e09667155725a1b052
/usr/lib/build_id@/fb/2432888406099975342d077e54c174fed5
/usr/lib/build_id@/fb
/usr/lib/unix/mariadb/mariadb_extras_new_0024_94b2008094f32b2e
/usr/lib/systemd/system/mariadb.service
/usr/lib/systemd/system/mariadb@.service
/usr/lib/systemd/system/mariadb@bootstrap.service.d
/usr/lib/systemd/system/mariadb@bootstrap.service.d/use_galera_new_cluster.conf
/usr/lib/tmpfiles.d/mariadb.conf
/usr/lib/ld.so
/usr/lib/ld.so.1
/usr/lib/ld.so.1.0.0
/usr/lib/ld.so.1.0.0/ldINFO.BIN
/usr/lib/ld.so.1.0.0/ldINFO.SRC
/usr/lib/ld.so.1.0.0/mariadb/plugin
/usr/lib/ld.so.1.0.0/mariadb/plugin/auth null.so
/usr/lib/ld.so.1.0.0/mariadb/plugin/auth pam.so
/usr/lib/ld.so.1.0.0/mariadb/plugin/auth pam.so
/usr/lib/ld.so.1.0.0/mariadb/plugin/auth socket.so
/usr/lib/ld.so.1.0.0/mariadb/plugin/auth socket.so
/usr/lib/ld.so.1.0.0/mariadb/plugin/daemon example.ini
/usr/lib/ld.so.1.0.0/mariadb/plugin/debug key management.so
/usr/lib/ld.so.1.0.0/mariadb/plugin/dialog examples.so
/usr/lib/ld.so.1.0.0/mariadb/plugin/dialog examples.so
/usr/lib/ld.so.1.0.0/mariadb/plugin/example key management.so
/usr/lib/ld.so.1.0.0/mariadb/plugin/file key management.so
/usr/lib/ld.so.1.0.0/mariadb/plugin/plug-in key management.so
```

Check status and enable/start the service

Use:

```
systemctl status mariadb
```

```
sudo systemctl enable mariadb
```

```
sudo systemctl start mariadb
```

```
[cgarcia@t10-s-al2-localhost ~]$ systemctl status mariadb
● mariadb.service - MariaDB 10.3 database server
  Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; vendor preset: d>
  Active: inactive (dead)
    Docs: man:mysqld(8)
          https://mariadb.com/kb/en/library/systemd/
[cgarcia@t10-s-al2-localhost ~]$ systemctl enable mariadb
Created symlink /etc/systemd/system/mysql.service → /usr/lib/systemd/system/mariadb.se>
rvice.
Created symlink /etc/systemd/system/mysqld.service → /usr/lib/systemd/system/mariadb.s>
ervice.
Created symlink /etc/systemd/system/multi-user.target.wants/mariadb.service → /usr/lib/>
/systemd/system/mariadb.service.
[cgarcia@t10-s-al2-localhost ~]$ systemctl start mariadb
Failed to start mariadb.service: Access denied
See system logs and 'systemctl status mariadb.service' for details.
[cgarcia@t10-s-al2-localhost ~]$ sudo systemctl start mariadb
[cgarcia@t10-s-al2-localhost ~]$ systemctl status mariadb
● mariadb.service - MariaDB 10.3 database server
  Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: d>
  Active: active (running) since Thu 2024-02-01 11:10:37 MST; 18s ago
    Docs: man:mysqld(8)
          https://mariadb.com/kb/en/library/systemd/
  Process: 135061 ExecStartPost=/usr/libexec/mysql-check-upgrade (code=exited, status=>
  Process: 134926 ExecStartPre=/usr/libexec/mysql-prepare-db-dir mariadb.service (cod>
  Process: 134902 ExecStartPre=/usr/libexec/mysql-check-socket (code=exited, status=0>
  Main PID: 135029 (mysqld)
    Status: "Taking your SQL requests now..."
      Tasks: 30 (limit: 23499)
     Memory: 85.4M
    CGroup: /system.slice/mariadb.service
           └─135029 /usr/libexec/mysqld --basedir=/usr

Feb 01 11:10:34 t10-s-al2-localhost systemd[1]: Starting MariaDB 10.3 database serv>
Feb 01 11:10:34 t10-s-al2-localhost mysql-prepare-db-dir[134926]: Initializing Mari>
Feb 01 11:10:37 t10-s-al2-localhost systemd[1]: Started MariaDB 10.3 database serv>
lines 1-18/18 (END)
```

```
[cgarcia@t10-s-al2-localhost ~]$ systemctl status mariadb
● mariadb.service - MariaDB 10.3 database server
  Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; vendor preset: d>
  Active: inactive (dead)
    Docs: man:mysqld(8)
          https://mariadb.com/kb/en/library/systemd/
lines 1-5/5 (END)
```

Use my_sql_secure installation to initialize security settings:

```
sudo mysql_secure_installation
```

Answer the prompts from the interactive script.

```
Feb 01 11:10:34 t10-s-al2-localhost systemd[1]: Starting MariaDB 10.3 database service.
Feb 01 11:10:34 t10-s-al2-localhost mysql-prepare-db-dir[134926]: Initializing MariaDB...
Feb 01 11:10:37 t10-s-al2-localhost systemd[1]: Started MariaDB 10.3 database service.
[cgarcia@t10-s-al2-localhost ~]$ sudo mysql_secure_installation
[sudo] password for cgarcia:
```

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
```

```
In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.
```

```
Enter current password for root (enter for none):
OK, successfully used password, moving on...
```

```
Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.
```

```
Set root password? [Y/n] 
```

```
Enter current password for root (enter for none):
OK, successfully used password, moving on...
```

```
Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.
```

```
Set root password? [Y/n] y
New password:
Re-enter new password:
Sorry, passwords do not match.
```

```
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!
```

```
By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.
```

```
Remove anonymous users? [Y/n] 
```

Use my_sql_secure installation to initialize security settings:

Answer the prompts from the interactive script.

```
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] n
... skipping.

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
[cgarcia@t10-s-al2-localhost ~]$
```

Connect to the database server with the MariaDB root account.
(The necessary -p command-line option tells the client to [p]rompt you for the password.)

```
mysql -u root -p
```

List the available databases, remember the “;” :

```
show databases;
```

The screenshot shows a terminal window with a black background and white text. At the top, it says "Thanks for using MariaDB!" followed by a red box around the command "[cgarcia@t10-s-al2-localhost ~]:". Below that is the prompt "mysql -u root -p" with a red box around it. The next line is "Enter password:" with a red box around it. Then it says "Welcome to the MariaDB monitor. Commands end with ; or \g." followed by "Your MariaDB connection id is 15" and "Server version: 10.3.39-MariaDB MariaDB Server". It then displays copyright information from 2000 to 2018. The next line is "Type 'help;' or '\h' for help. Type '\c' to clear the current input statement." followed by "MariaDB [(none)]> show databases;" with a red box around it. A table follows, showing three rows: "information_schema", "mysql", and "performance_schema". The last line is "3 rows in set (0.001 sec)". Finally, the prompt "MariaDB [(none)]>" is shown again.

```
Thanks for using MariaDB!
[cgarcia@t10-s-al2-localhost ~] mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 15
Server version: 10.3.39-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| mysql          |
| performance_schema |
+-----+
3 rows in set (0.001 sec)

MariaDB [(none)]>
```

Create a new database call q2a and create q2auser with passwords and privileges.

```
create database q2a;

grant all privileges on q2a.* to
'q2auser'@'localhost' identified by
'q2apass';
```

User from DMZ zone:

```
grant all privileges on q2a.* to
'q2auser'@'192.168.201.2' identified by
'q2apass';
```

See results:

```
show databases;
```

```
select user, host, password from mysql.user;
```

```
MariaDB [(none)]> create database q2a;
MariaDB [(none)]> grant all privileges on q2a.* to 'q2auser'@'localhost' identified by 'q2a10pass'
-> ;
Query OK, 0 rows affected (0.001 sec)
```

```
MariaDB [(none)]> grant all privileges on q2a.* to 'q2auser'@'192.168.201.2' identified by 'q2a10pass'
-> ;
Query OK, 0 rows affected (0.001 sec)
```

```
MariaDB [(none)]> show databases
-> ;
```

Database
information_schema
mysql
performance schema
q2a

4 rows in set (0.001 sec)

```
MariaDB [(none)]> select user, host, password from mysql.user;
+-----+-----+-----+
| user | host | password |
+-----+-----+-----+
| root | localhost | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |
| root | t10-s-a12-localhost | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |
| root | 127.0.0.1 | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |
| root | ::1 | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |
| q2auser | localhost | *30A7D7C55498E4F3D2A7F3B54088E19709BCC50B |
| q2auser | 192.168.201.2 | *30A7D7C55498E4F3D2A7F3B54088E19709BCC50B |
+-----+-----+-----+
6 rows in set (0.001 sec)
```

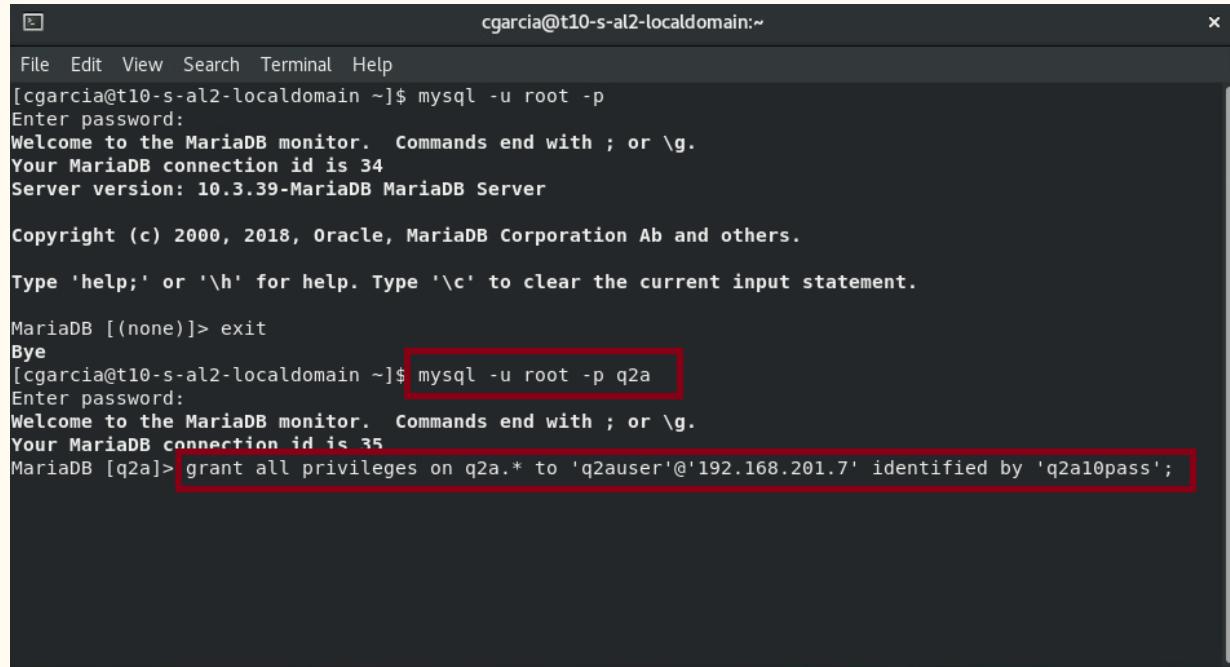
```
MariaDB [(none)]> ■
```

Create another user in the right machine.

```
mysql -u root -p q2a
```

```
grant all privileges on q2a.*  
to 'q2auser'@'192.168.201.7'  
Identified by 'q2a10pass';
```

This shows how to create new users and
Add privileges to connect from other
machines.



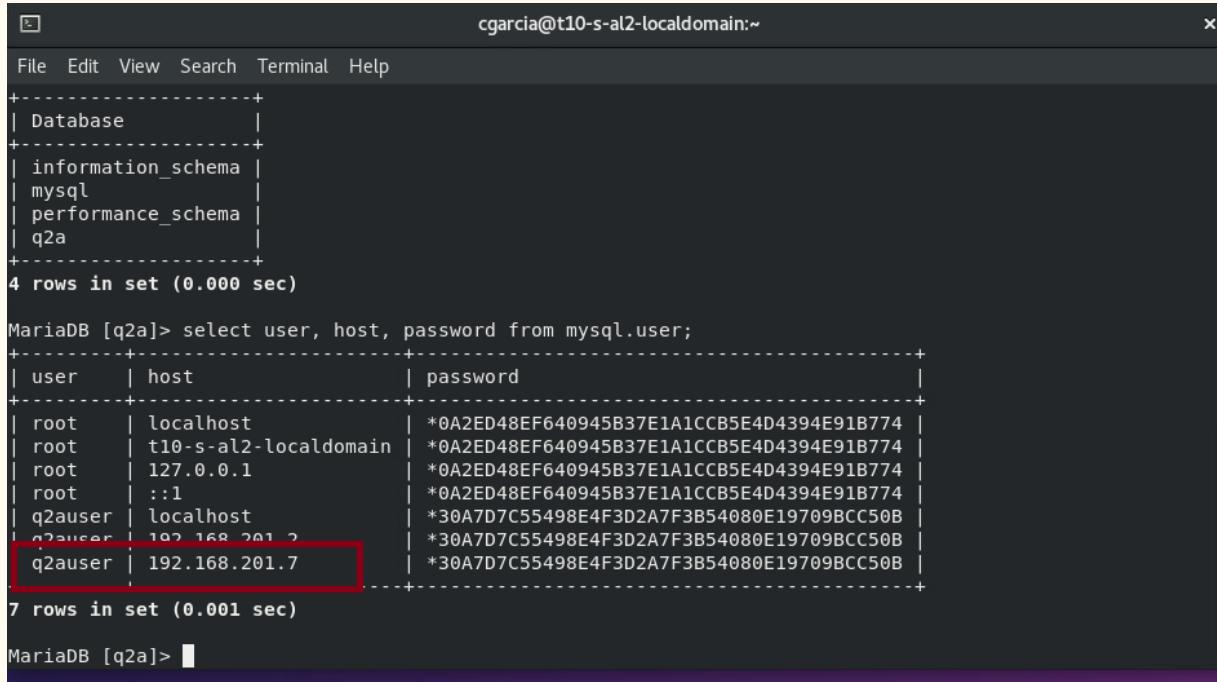
The screenshot shows a terminal window titled "cgarcia@t10-s-al2-localhost:~". The window contains the following text:

```
File Edit View Search Terminal Help  
[cgarcia@t10-s-al2-localhost ~]$ mysql -u root -p  
Enter password:  
Welcome to the MariaDB monitor. Commands end with ; or \g.  
Your MariaDB connection id is 34  
Server version: 10.3.39-MariaDB MariaDB Server  
  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
MariaDB [(none)]> exit  
Bye  
[cgarcia@t10-s-al2-localhost ~]$ mysql -u root -p q2a  
Enter password:  
Welcome to the MariaDB monitor. Commands end with ; or \g.  
Your MariaDB connection id is 35  
MariaDB [q2a]> grant all privileges on q2a.* to 'q2auser'@'192.168.201.7' identified by 'q2a10pass';
```

The command "grant all privileges on q2a.* to 'q2auser'@'192.168.201.7' identified by 'q2a10pass';" is highlighted with a red box.

The new user created previously shows in the database.

```
select user, host, password from mysql.user;
```



A screenshot of a terminal window titled "cgarcia@t10-s-al2-localhost:~". The window contains two MySQL queries and their results. The first query is "select user, host, password from mysql.user;" which returns four rows of system databases: information_schema, mysql, performance_schema, and q2a. The second query is "select user, host, password from mysql.user;" run within the q2a database, which returns seven rows of users: root, root, root, root, q2auser, q2auser, and q2auser. The last row, "q2auser | 192.168.201.7", is highlighted with a red rectangle.

```
cgarcia@t10-s-al2-localhost:~
```

```
File Edit View Search Terminal Help
```

```
+-----+  
| Database |  
+-----+  
| information_schema |  
| mysql |  
| performance_schema |  
| q2a |  
+-----+  
4 rows in set (0.000 sec)
```

```
MariaDB [q2a]> select user, host, password from mysql.user;
```

user	host	password
root	localhost	*0A2ED48EF640945B37E1A1CCB5E4D4394E91B774
root	t10-s-al2-localhost	*0A2ED48EF640945B37E1A1CCB5E4D4394E91B774
root	127.0.0.1	*0A2ED48EF640945B37E1A1CCB5E4D4394E91B774
root	::1	*0A2ED48EF640945B37E1A1CCB5E4D4394E91B774
q2auser	localhost	*30A7D7C55498E4F3D2A7F3B54080E19709BCC50B
q2auser	192.168.201.7	*30A7D7C55498E4F3D2A7F3B54080E19709BCC50B
q2auser	192.168.201.7	*30A7D7C55498E4F3D2A7F3B54080E19709BCC50B

```
7 rows in set (0.001 sec)
```

```
MariaDB [q2a]> 
```

Connect locally to the q2a database as q2auser

```
mysql -h localhost -u q2auser -p q2a
```

```
Bye
[cgarcia@t10-s-al2-localdomain ~]:: mysql -h localhost -u q2auser -p q2a
Enter password: [REDACTED]
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 16
Server version: 10.3.39-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [q2a]:: \q
Bye
[cgarcia@t10-s-al2-localdomain ~]$
```

The following adjustments will allow other hosts to connect to MariaDB:

```
sudo firewall-cmd --add-service=mysql --permanent
```

```
sudo firewall-cmd --reload
```

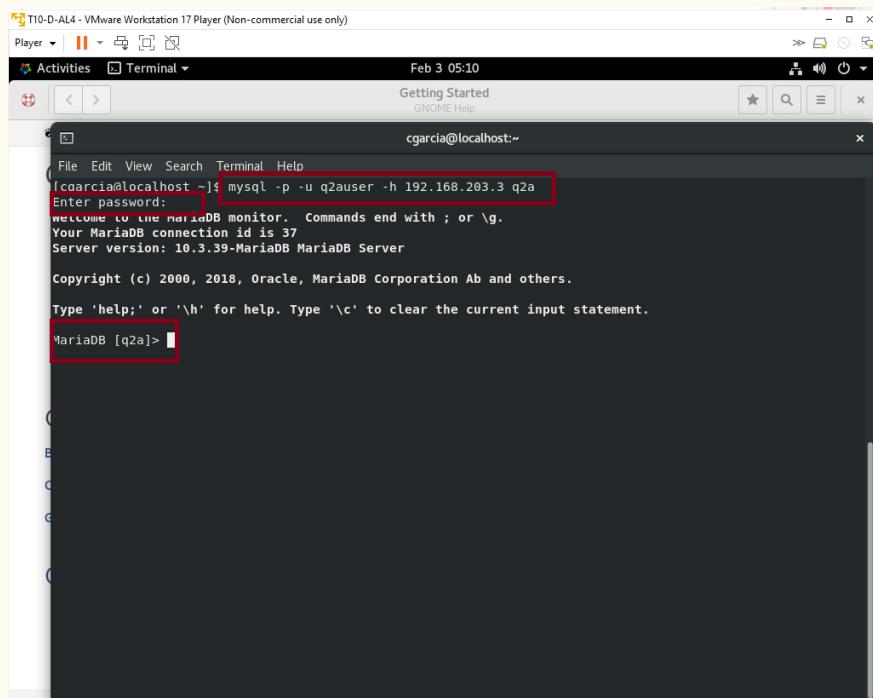
```
[cgarcia@t10-s-al2-localhost ~]$ sudo firewall-cmd --add-service=mysql --permanent  
[sudo] password for cgarcia:  
success  
[cgarcia@t10-s-al2-localhost ~]$ sudo firewall-cmd --reload  
success  
[cgarcia@t10-s-al2-localhost ~]$
```

Remote connection from the DMZ machine where the apache server resides.

```
mysql -p -u q2auser -h 192.168.203.3 q2a
```

Description:

- p ask for password
- u username (q2auser)
- h host ip address(192.168.203.3)
- (q2a) the name of the database



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "T10-D-AL4 - VMware Workstation 17 Player (Non-commercial use only)". The terminal session is running under the user "cgarcia" at the command line: [cgarcia@localhost ~]\$ mysql -p -u q2auser -h 192.168.203.3 q2a. A red box highlights the command line. The terminal then prompts for a password: Enter password: [redacted]. Another red box highlights this prompt. The MySQL monitor then displays its welcome message: "Welcome to the MariaDB monitor. Commands end with ; or \g." It also shows the connection information: "Your MariaDB connection id is 37" and "Server version: 10.3.39-MariaDB MariaDB Server". It then displays the copyright notice: "Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others." Finally, it shows the prompt: "Type 'help;' or '\h' for help. Type '\c' to clear the current input statement." [redacted] MariaDB [q2a]> [redacted]. A third red box highlights the prompt.

Apache server installation

Install Apache Server

Download,
install, and
initialize
Apache
HTTPD
server
software.

```
[cditto@localhost ~]$ dnf search apache
```

```
[cditto@localhost ~]$ sudo dnf -y install httpd
```

```
Installed:  
almalinux-logos-httpd-84.5-1.el8.noarch  
apr-1.6.3-12.el8.x86_64  
apr-util-1.6.1-9.el8.x86_64  
apr-util-bdb-1.6.1-9.el8.x86_64  
apr-util-openssl-1.6.1-9.el8.x86_64  
httpd-2.4.37-62.module_el8.9.0+3646+acd210d0.x86_64  
httpd-filesystem-2.4.37-62.module_el8.9.0+3646+acd210d0.noarch  
httpd-tools-2.4.37-62.module_el8.9.0+3646+acd210d0.x86_64  
mod_http2-1.15.7-8.module_el8.9.0+3660+29a7abf6.3.x86_64  
  
Complete!
```

Install Apache Server

Backup a copy of the primary configuration file

/etc/httpd/conf/httpd.conf

Change configuration file by changing the Listen directive to attach the service to the virtual ethernet.

To do this open nano and change the Listener directive to the Host server IP address and port 80

```
[cditto@localhost ~]$ cd /etc/httpd/conf
```

```
[cditto@localhost ~]$ sudo nano /etc/httpd/conf/httpd.conf
```

```
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 192.168.201.7:80
```

```
[cditto@localhost conf]$ sudo systemctl restart httpd
```

Install Apache Server

Check the server status.

Notice it is listening to the IP address and port we configured earlier.

```
[cditto@localhost conf]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor pres>
   Active: active (running) since Fri 2024-02-02 12:53:29 MST; 5min ago
     Docs: man:httpd.service(8)
   Main PID: 42400 (httpd)
      Tasks: 213 (limit: 23499)
    Memory: 29.1M
      CGroup: /system.slice/httpd.service
              └─42400 /usr/sbin/httpd -DFOREGROUND
                  ├─42401 /usr/sbin/httpd -DFOREGROUND
                  ├─42402 /usr/sbin/httpd -DFOREGROUND
                  ├─42403 /usr/sbin/httpd -DFOREGROUND
                  └─42404 /usr/sbin/httpd -DFOREGROUND
Feb 02 12:53:29 localhost.localdomain systemd[1]: Starting The Apache HTTP Serv>
Feb 02 12:53:29 localhost.localdomain httpd[42400]: AH00558: httpd: Could not r>
Feb 02 12:53:29 localhost.localdomain systemd[1]: Started The Apache HTTP Serve>
Feb 02 12:53:29 localhost.localdomain httpd[42400]: Server configured, listenin>
```

Install Apache Server

Enable service
to start at
startup.

Open browser
and surf to the
host servers
webpage.
You should
see the new
installation
“Test Page”

```
[cditto@localhost conf]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
```

```
[cditto@localhost conf]$ sudo systemctl start httpd
```

AlmaLinux Test Page

This page is used to test the proper operation of the HTTP server after it has been installed. If you can read this page, it means that the HTTP server installed at this site is working properly.

If you are a member of the general public:
The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

For information on AlmaLinux, please visit the [AlmaLinux website](#).

If you are the website administrator:
You may now add content to the webroot directory. Note that until you do so, people visiting your website will see this page, and not your content.

For systems using the Apache HTTP Server: You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

For systems using NGINX: You should now put your content in a location of your choice and edit the `root` configuration directive in the `nginx` configuration file `/etc/nginx/nginx.conf`.

 AlmaLinux

Apache™ is a registered trademark of the Apache Software Foundation in the United States and/or other countries.

Download & Install PHP

Download
and install
PHP.

Restart
Apache.

```
[cditto@localhost ~]$ sudo dnf install php
```

```
Installed:  
nginx-filesystem-1:1.14.1-9.module_el8.3.0+2165+af250afe.alma.noarch  
php-7.2.24-1.module_el8.3.0+2010+7c76a223.x86_64  
php-cli-7.2.24-1.module_el8.3.0+2010+7c76a223.x86_64  
php-common-7.2.24-1.module_el8.3.0+2010+7c76a223.x86_64  
php-fpm-7.2.24-1.module_el8.3.0+2010+7c76a223.x86_64
```

```
Complete!
```

```
[cditto@localhost ~]$ sudo systemctl restart httpd
```

Download & Install PHP

Check Apache server status.

Notice php-fpm is activated without having to enable it.

```
[cditto@localhost ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Drop-In: /usr/lib/systemd/system/httpd.service.d
             └─php-fpm.conf ←
     Active: active (running) since Fri 2024-02-02 13:47:02 MST; 27s ago
       Docs: man:httpd.service(8)
     Main PID: 45585 (httpd)
        Status: "Running, listening on: 192.168.201.7 port 80"
          Tasks: 213 (limit: 23499)
         Memory: 37.0M
        CGroup: /system.slice/httpd.service
                  ├─45585 /usr/sbin/httpd -DFOREGROUND
                  ├─45593 /usr/sbin/httpd -DFOREGROUND
                  ├─45595 /usr/sbin/httpd -DFOREGROUND
                  ├─45596 /usr/sbin/httpd -DFOREGROUND
                  └─45598 /usr/sbin/httpd -DFOREGROUND

Feb 02 13:47:02 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
Feb 02 13:47:02 localhost.localdomain httpd[45585]: AH00558: httpd: Could not reliably determine the server's
Feb 02 13:47:02 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
Feb 02 13:47:02 localhost.localdomain httpd[45585]: Server configured, listening on: 192.168.201.7 port 80
```

Download & Install PHP

Check php-fpm status.

In a later assignment Q2A will specify that we need to add the extension MySQLi but when we search for a MySQL extension we only find MySQLnd in Alma Linux.

```
[cditto@localhost ~]$ sudo systemctl status php-fpm
● php-fpm.service - The PHP FastCGI Process Manager
   Loaded: loaded (/usr/lib/systemd/system/php-fpm.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2024-02-02 13:47:01 MST; 11min ago
     Main PID: 45577 (php-fpm)
        Status: "Processes active: 0, idle: 5, Requests: 0, slow: 0, Traffic: 0req/sec"
          Tasks: 6 (limit: 23499)
        Memory: 9.0M
         CGroup: /system.slice/php-fpm.service
                 └─45577 php-fpm: master process (/etc/php-fpm.conf)
                     ├─45578 php-fpm: pool www
                     ├─45579 php-fpm: pool www
                     ├─45580 php-fpm: pool www
                     ├─45581 php-fpm: pool www
                     └─45582 php-fpm: pool www

Feb 02 13:47:01 localhost.localdomain systemd[1]: Starting The PHP FastCGI Process Manager...
Feb 02 13:47:01 localhost.localdomain systemd[1]: Started The PHP FastCGI Process Manager.
```

```
[cditto@localhost ~]$ dnf search php-mysql
```

```
php-mysqlnd.x86_64 : A module for PHP applications that use MySQL databases
[cditto@localhost ~]$ dnf info php-mysqlnd
Last metadata expiration check: 2:34:23 ago on Fri 02 Feb 2024 11:28:18 AM MST.
Available Packages
Name           : php-mysqlnd
```

Download & Install PHP

MySQLnd is an updated extension from MySQLi. It is fine to use it in this installation. Install this package.

```
[cditto@localhost ~]$ sudo dnf -y install php-mysqlnd
[cditto@localhost ~]$ Installed:
[cditto@localhost ~]$ php-mysqlnd-7.2.24-1.module_el8.3.0+2010+7c76a223.x86_64
[cditto@localhost ~]$ php-pdo-7.2.24-1.module_el8.3.0+2010+7c76a223.x86_64
[cditto@localhost ~]$ Complete!
[cditto@localhost ~]$
```

Test the PHP Installation

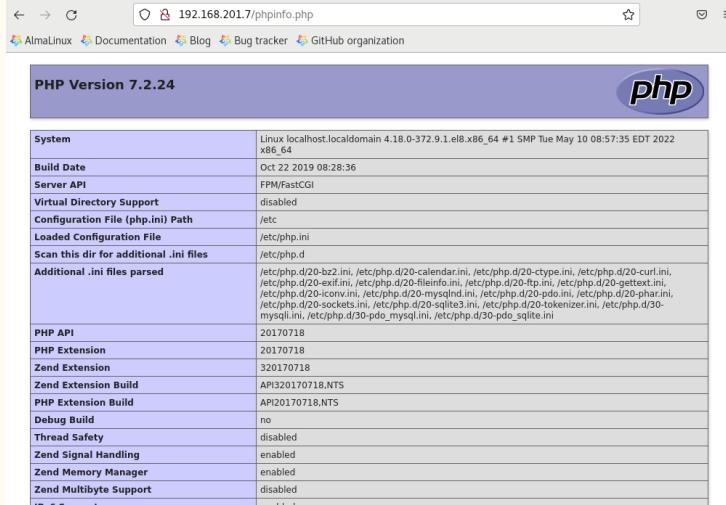
Create a PHP file in the Apache documentroot folder /var/www/html

Add the line <?php phpinfo(); ?> to the file.

Use the web browser to surf to that file, using the URL
`http://<DMZ server IP address>/phpinfo.php`

```
[cditto@localhost ~]$ sudo nano /var/www/html/phpinfo.php
```

```
GNU nano 2.9.8
<?php phpinfo(); ?>
```



Configure Policies on Internet Facing Firewalls

Configure
Static
NAT.

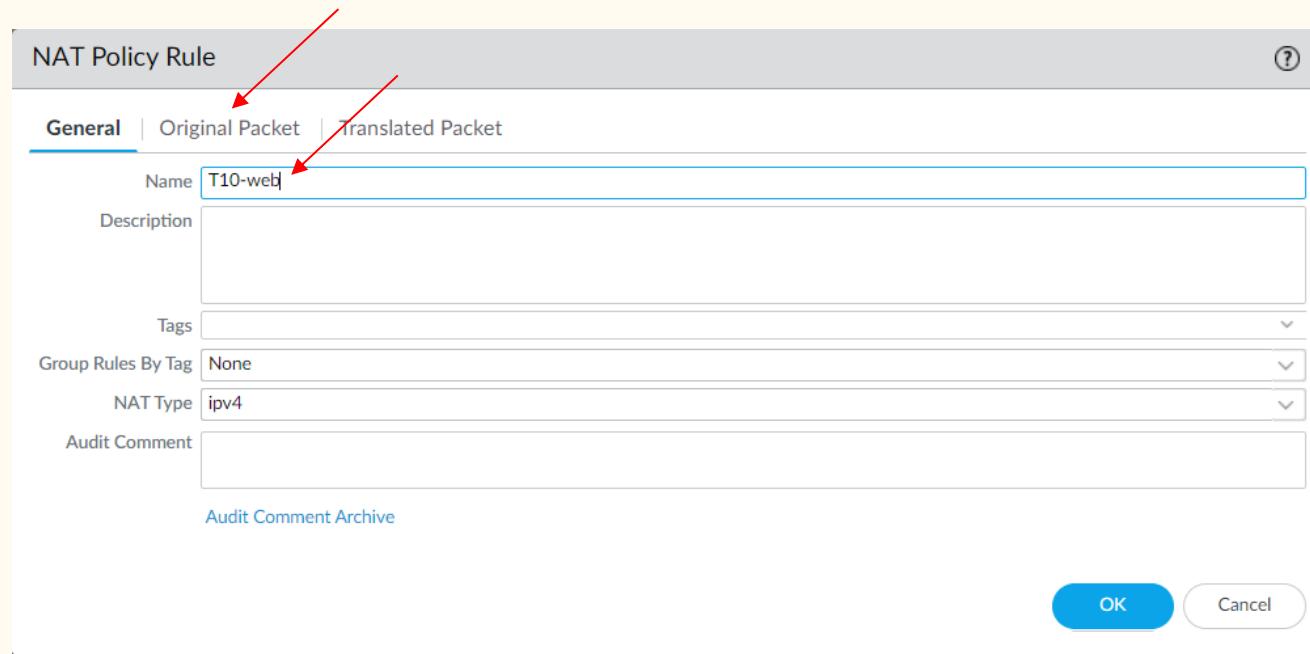
The screenshot shows a software interface for managing network policies. On the left, a sidebar lists various security features: Security, NAT (selected), QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. Below this is a 'Policy Optimizer' section with a 'Rule Usage' tree view showing counts for 'Unused in 30 days', 'Unused in 90 days', and 'Unused'. The main area displays a table of policy rules. A red arrow points to the 'NAT' tab in the sidebar. Another red arrow points to the '+ Add' button at the bottom of the main window. The table has columns for NAME, TAGS, SOURCE ZONE, DESTINATION ZONE, DESTINATION INTERFACE, SOURCE ADDRESS, DESTINATION ADDRESS, SERVICE, SOURCE TRANSLATION, DESTINATION TRANSLATION, and HIT CO. One rule is listed: T10-dynamic, with source zone dmz, destination zone outside, and destination interface ethernet1/3.610. The source address is 192.168.201.0... and destination address is 192.168.202.2.... The service is dynamic-ip-and-port, and the destination translation is 157.201.22.72/29. The hit counter is 64949.

Original Packet										Translated Packet		
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION	HIT CO	
1	T10-dynamic	none	dmz	outside	ethernet1/3.610	192.168.201.0...	any	any	dynamic-ip-and-port	none	64949	
			inside			192.168.202.2...			ethernet1/3.610			
									157.201.22.72/29			

Object : Addresses + + Add - Delete Clone Enable Disable Move PDF/CSV Highlight Unused Rules View Rulebase as Groups Reset Rule Hit Counter Group Test Policy Match

Configure Policies on Internet Facing Firewalls

Add a name to your NAT policy.



Configure Policies on Internet Facing Firewalls

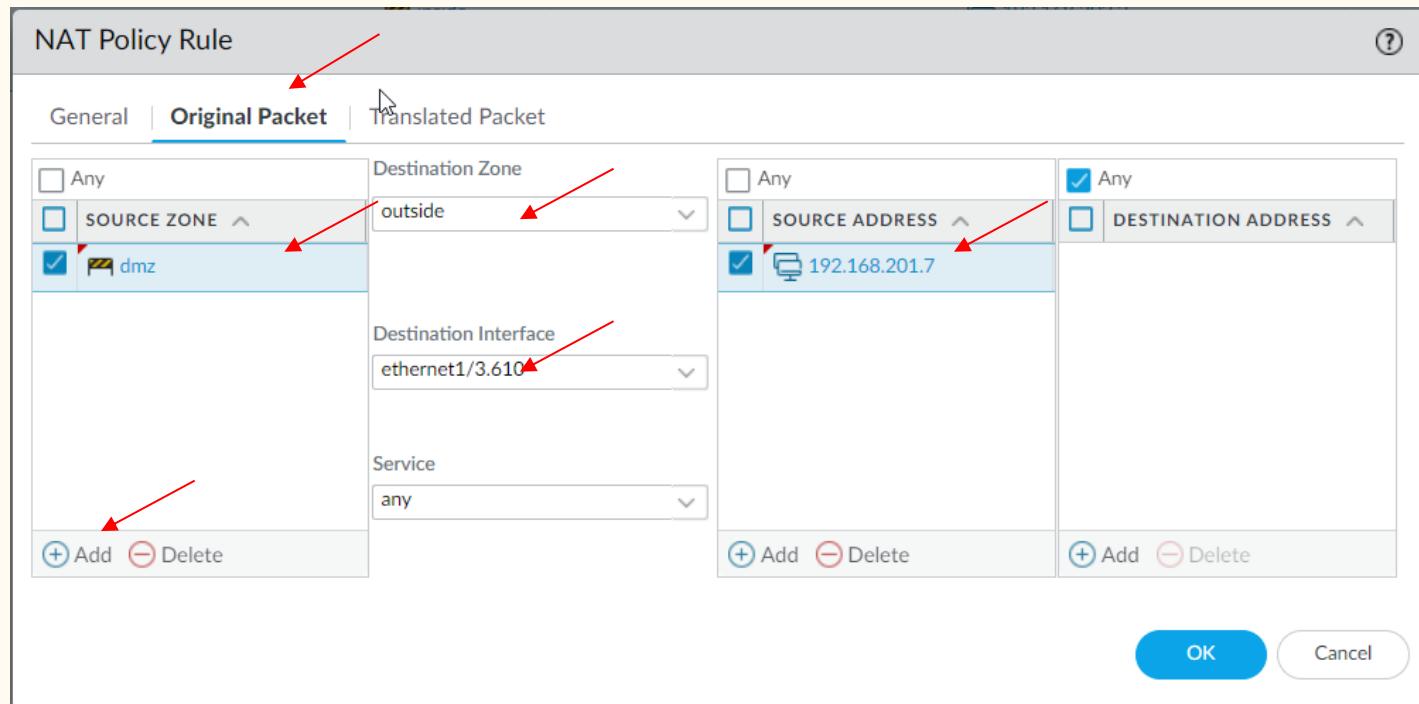
Select the “Original Packet” tab.

Change the “Source Zone” to DMZ.

Select the dropdown in the “Destination Zone” Select outside.

Select the dropdown for the “Destination Interface” then select the VPN interface in the outside zone.

Under “Source Address” add the IP address of the apache server.



Configure Policies on Internet Facing Firewalls

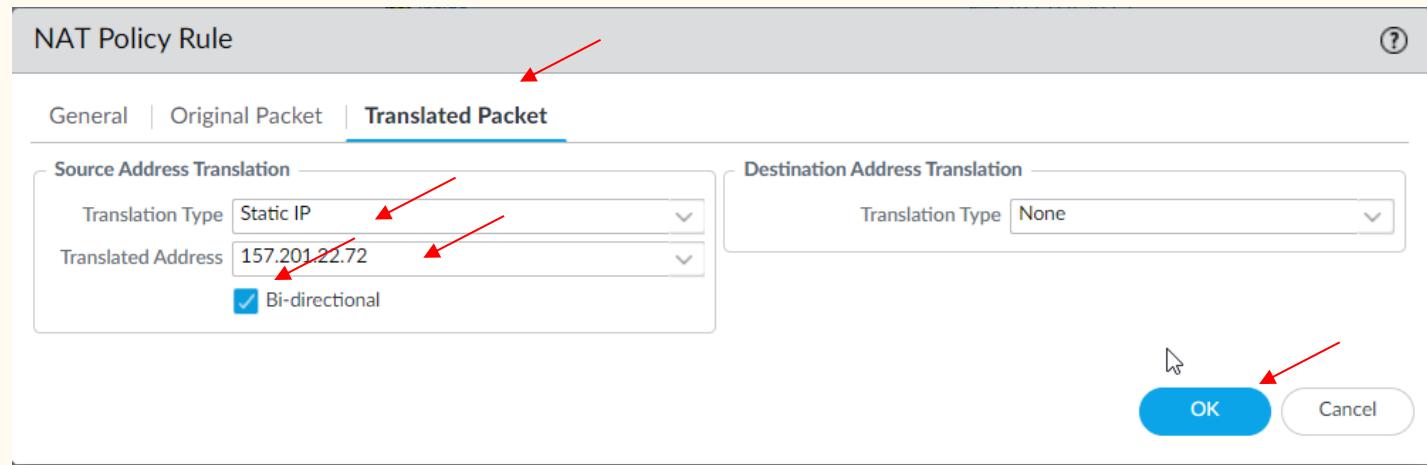
Select the “Translated Packet” tab.

Under “Translation Type” select the dropdown and then Static IP.

Under the “Translated Address” enter the public IP address.

Check the “Bi-directional box” so the rule translates both ways.

Click “OK”

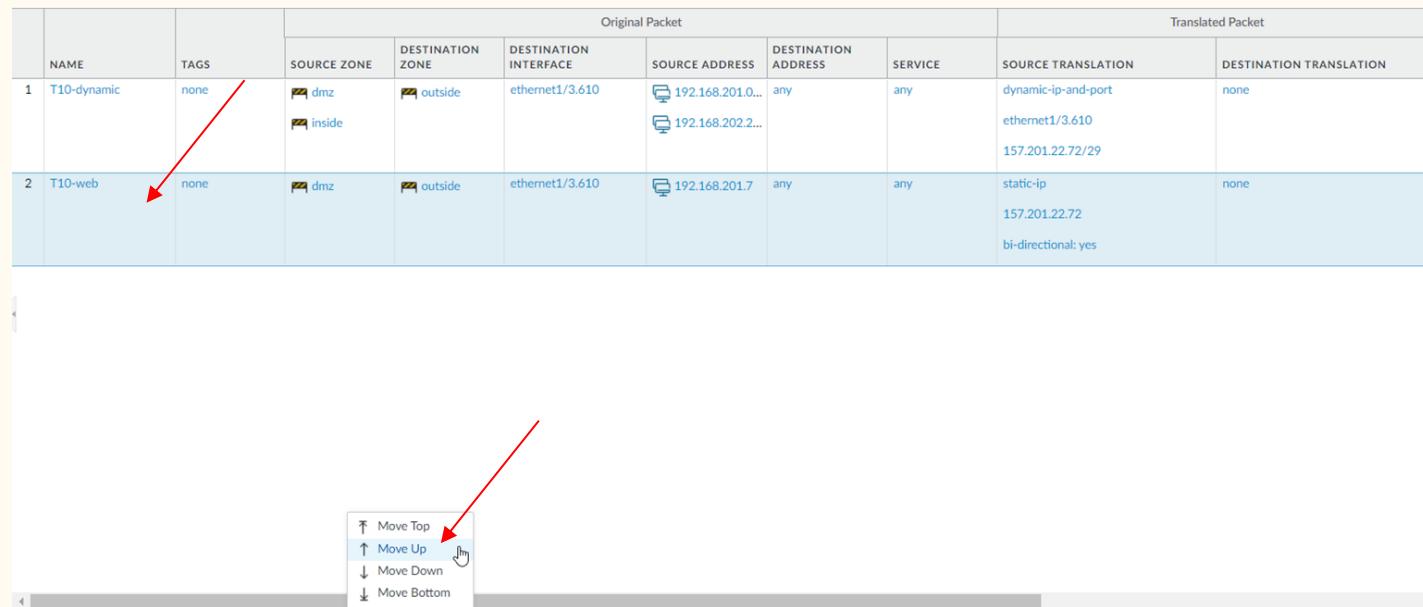


Configure Policies on Internet Facing Firewalls

Highlight the new rule and select “move up” from the “Move” interface at the bottom of the web-interface.

The rule needs to be before the team’s Dynamic rule.

	NAME	TAGS	Original Packet						Translated Packet	
			SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	T10-dynamic	none	dmz inside	outside	ethernet1/3.610	192.168.201.0... 192.168.202.2...	any	any	dynamic-ip-and-port ethernet1/3.610 157.201.22.72/29	none
2	T10-web	none	dmz	outside	ethernet1/3.610	192.168.201.7	any	any	static-ip 157.201.22.72 bi-directional: yes	none



Configure Policies on Internet Facing Firewalls

Configure a web-server security policy.

Select Security on the left just above NAT then click on Add.

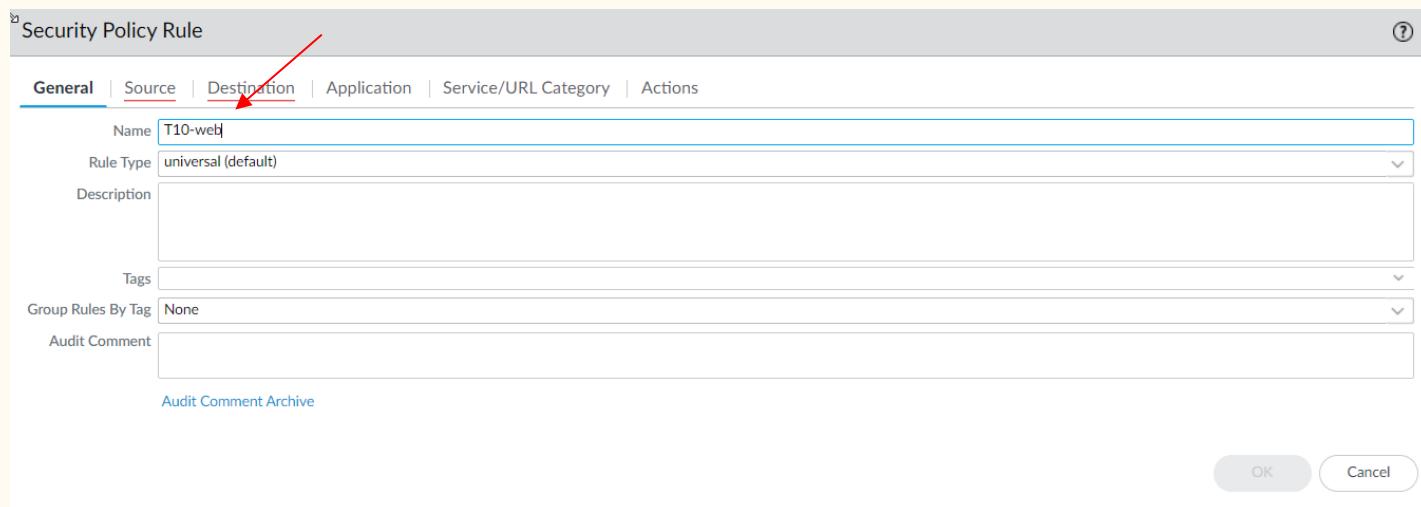
The screenshot shows a firewall policy configuration interface. On the left, there is a sidebar with various security features: NAT, QoS, Policy Based Forwarding, Description, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. A red arrow points from the text "Select Security on the left just above NAT" to the "Security" section in the sidebar. Below the sidebar is a "Policy Optimizer" section with metrics for New App Viewer, Rules Without App Controls, Unused Apps, Rule Usage, Unused in 30 days, Unused in 90 days, and Unused. Another red arrow points from the text "then click on Add." to the "Add" button at the bottom of the interface. The main area displays a table of rules:

ID	NAME	TAGS	TYPE	Source				Destination				APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
1	rule1	none	universal	trust	any	any	any	untrust	any	any	any	any	any	Allow
2	T10-outbound	none	universal	dmz	192.168.201.0...	any	any	outside	any	any	any	any	application-...	Allow
3	T10-dmz-to-inside	none	universal	dmz	192.168.201.0...	any	any	inside	192.168.202.0...	any	ms-rdp	application-...	Allow	
4	T10-inside-to-dmz-all	none	universal	inside	192.168.202.0...	any	any	dmz	192.168.201.0...	any	any	any	application-...	Allow
5	T10-secure-to-dmz-i...	none	universal	interconnect	192.168.203.0...	any	any	dmz	192.168.201.0...	any	any	any	application-...	Allow
6	T10-squid-proxy	none	universal	interconnect	192.168.203.0...	any	any	dmz	192.168.201.0...	any	any	any	service-squid	Allow
7	T10-to-Secure-Remo...	none	universal	dmz	192.168.201.0...	any	any	interconnect	192.168.203.0...	any	ms-rdp	application-...	Allow	
8	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	any	Allow
9	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	any	Deny

At the bottom, there is a toolbar with buttons for Object : Addresses, Add, Delete, Clone, Override, Revert, Enable, Disable, Move, PDF/CSV, Highlight Unused Rules, View Rulebase as Groups, Reset Rule Hit Counter, Group, and Test Policy Match.

Configure Policies on Internet Facing Firewalls

Under General add the team name followed by “web” under the “Name” selection.



Configure Policies on Internet Facing Firewalls

Select the “Source” tab.

Under the “Source Zone” click on “Add” then select “outside”.

Select the “Destination” tab

Under the “Destination Zone” Select “Add” then select outside.

Under “Destination Address” add the public IP address of the web server.

The image displays two side-by-side screenshots of a firewall's "Security Policy Rule" configuration interface. Both screenshots show the "Source" and "Destination" tabs respectively, with red arrows pointing to specific fields and buttons.

Left Screenshot (Source Tab):

- The title bar says "Security Policy Rule".
- The tabs at the top are General, **Source**, Destination, Application, Service/URL Category, and Actions.
- The "Source" tab is selected.
- Under "SOURCE ZONE", there is a dropdown menu with "Any" and an "Add" button. An arrow points to the "Add" button.
- Below the dropdown, there is a list of zones: "outside" (selected) and "dmz".
- At the bottom, there are "Add" and "Delete" buttons, and a "Negate" checkbox.

Right Screenshot (Destination Tab):

- The title bar says "Security Policy Rule".
- The tabs at the top are General, Source, **Destination**, Application, Service/URL Category, and Actions.
- The "Destination" tab is selected.
- Under "DESTINATION ZONE", there is a dropdown menu with "select" and an "Add" button. An arrow points to the "Add" button.
- Below the dropdown, there is a list of zones: "dmz" (selected) and "outside".
- At the bottom, there are "Add" and "Delete" buttons, and a "Negate" checkbox.

Configure Policies on Internet Facing Firewalls

Select the “Applications” tab, and specify web-browsing.

Select the “Actions” tab

Commit your changes.

The image consists of two screenshots of a firewall configuration interface, likely from a Juniper device. Both screenshots show a 'Security Policy Rule' configuration window.

Screenshot 1: Application Tab

This screenshot shows the 'Application' tab selected. Under the 'APPLICATIONS' section, the 'web-browsing' application is selected, indicated by a checked checkbox and a blue highlight. A red arrow points to the 'Application' tab at the top. Another red arrow points to the 'web-browsing' entry in the list.

Screenshot 2: Actions Tab

This screenshot shows the 'Actions' tab selected. In the 'Action Setting' section, the 'Action' dropdown is set to 'Allow'. A red arrow points to this dropdown. In the 'Log Setting' section, two checkboxes are checked: 'Log at Session Start' and 'Log at Session End'. A red arrow points to this section. At the bottom right of the window, there is an 'OK' button with a red arrow pointing to it, and a 'Cancel' button.

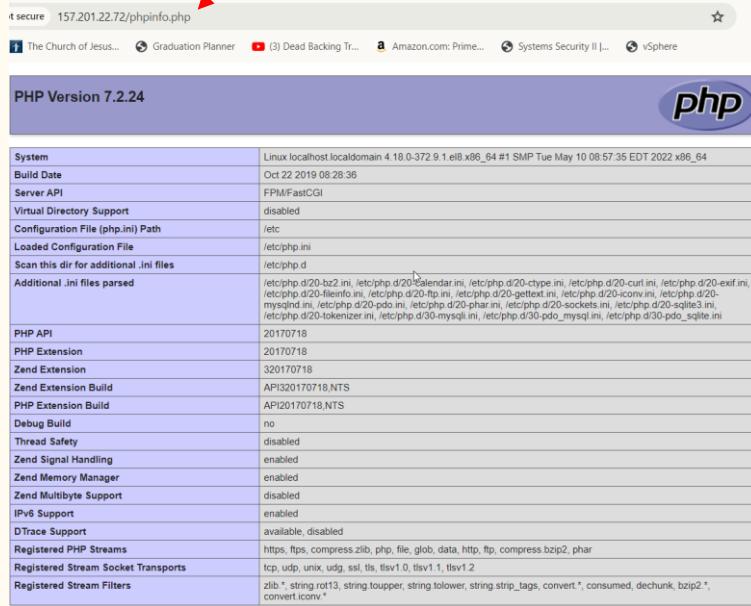
Configure Policies on Internet Facing Firewalls

Configure Apache server to accept HTTP and HTTPS requests through the firewall.

Enter http://<web server's public IP address>/phpinfo.php.

You should see the same info page that you saw at the in of the PHP test section of this instruction sequence.

```
[cditto@localhost /]$ sudo firewall-cmd --zone=public --permanent --add-service=http
success
[cditto@localhost /]$ sudo firewall-cmd --zone=public --permanent --add-service=https
success
[cditto@localhost /]$
```



The screenshot shows a web browser window displaying the PHPinfo page. The title bar indicates the page is secure and shows the URL as 157.201.22.72/phpinfo.php. The browser interface includes a star icon and a refresh button. Below the title bar, there is a horizontal bar with several links: The Church of Jesus... (highlighted), Graduation Planner, (3) Dead Backing Tr..., Amazon.com: Prime..., Systems Security II |..., and vSphere. The main content area is titled "PHP Version 7.2.24" and features a large "php" logo. The page contains a table with numerous rows of PHP configuration information, such as System (Linux localhost.localdomain 4.18.0-372.9.1.el8.x86_64 #1 SMP Tue May 10 08:57:35 EDT 2022 x86_64), Build Date (Oct 22 2019 08:28:36), Server API (FPM/FastCGI), and various extension status (disabled, enabled). The table continues with sections for PHP API, Zend Extension, PHP Extension, and many other PHP-related settings.

Configure Policies on Internet Facing Firewalls

Until the Question2Answer web app is installed and configured, it is a bad idea to leave the web server exposed to untrusted connections. Disable T10-Web rule until after the installation and configuration.

Highlight the T10-web rule then click “Disable” at the bottom of the web display.

Commit the change.

8	T10-web	none	universal	outside	any	any
9	intrazone-default	none	intrazone	any	any	any
10	interzone-default	none	interzone	any	any	any

Toolbar buttons: Add, Delete, Clone, Override, Revert, Enable, Disable, Move, PDF/CSV, Highlight.

Q2A Internet-Facing Firewall Configuration

Check to make sure that qtauser can log into MariaDB.

This will result in an error until secure-facing firewall is configured.

Create a rule on the Palo Alto firewall that allows the application mysql from the web server in the DMZ through to the interconnect zone.

On the top left of the web display click on “Security” and then select “Add” at the bottom of the display

```
[cditto@t10-s-al2-localhost ~]$ mysql -p -u q2auser -h 192.168.201.2  
Enter password:  
ERROR 2002 (HY000): Can't connect to MySQL server on '192.168.201.2' (115)
```

The screenshot shows the Palo Alto Firewall's configuration interface. On the left, there is a sidebar with various icons and sections like Security, NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. Below this is a 'Policy Optimizer' section with options like New App Viewer, Rules Without App Controls, Unused Apps, and Rule Usage. The main area is a table titled 'Source' with columns: NAME, TAGS, TYPE, ZONE, ADDRESS, and USER. There are 10 rows of rules listed:

NAME	TAGS	TYPE	Source		
			ZONE	ADDRESS	USER
rule1	none	universal	trust	any	any
T10-outbound	none	universal	dmz	192.168.201.0...	any
T10-dmz-to-inside-r...	none	universal	inside	192.168.202.0...	any
T10-inside-to-dmz-all	none	universal	inside	192.168.202.0...	any
T10-secure-to-dmz-i...	none	universal	interconnect	192.168.203.0...	any
T10-squid-proxy	none	universal	interconnect	192.168.203.0...	any
T10-to-Secure-Remo...	none	universal	dmz	192.168.201.0...	any
T10-web	none	universal	outside	any	any
intrazone-default	none	intrazone	any	any	any
interzone-default	none	interzone	any	any	any

At the bottom of the interface, there is a toolbar with buttons for Object : Addresses, Add, Delete, Clone, Override, Revert, Enable, Disable, Move, PDF/CSV, and a search bar.

Q2A Internet-Facing Firewall Configuration

Under the General tab
select Name and
enter your (team's
name)-database.

Select the “Source”
tab.

Under Source Zone
Click on “Add” and
then select DMZ.

Under Source
Address Select “Add”
then add the address
of your teams DMZ
web server.

Security Policy Rule

General | Source | Destination | Application | Service/URL Category

Name	T10-database
Rule Type	universal (default)
Description	
Tags	
Group Rules By Tag	None
Audit Comment	
Audit Comment Archive	

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions

<input type="checkbox"/> Any	<input type="checkbox"/> Any
<input type="checkbox"/> SOURCE ZONE	<input type="checkbox"/> SOURCE ADDRESS
<input checked="" type="checkbox"/> dmz	<input checked="" type="checkbox"/> 192.168.201.2
+ Add Delete	
+ Add Delete	
<input type="checkbox"/> Negate	

Q2A Internet-Facing Firewall Configuration

Select the
“Destination” tab.

Under the
Destination Zone,
click “Add” then
select
“interconnect.”

Under Destination
Address, click
“Add” then enter
the IP address to
your team’s DMZ
web server.

Security Policy Rule

General | Source | **Destination** | Application | Service/URL Category | Actions

select

DESTINATION ZONE
<input checked="" type="checkbox"/> interconnect

+ Add - Delete

Any

DESTINATION ADDRESS
<input checked="" type="checkbox"/> 192.168.201.2

+ Add - Delete

Negate

The screenshot shows a 'Security Policy Rule' configuration window. The 'Destination' tab is active. On the left, under 'DESTINATION ZONE', there is a dropdown menu and a list with 'interconnect' selected. On the right, under 'DESTINATION ADDRESS', there is a dropdown menu and a list with '192.168.201.2' selected. At the bottom of each list are '+ Add' and '- Delete' buttons. A red arrow points to the 'interconnect' entry in the zone list, another red arrow points to the '192.168.201.2' entry in the address list, and a third red arrow points to the '+ Add' button in the address section.

Q2A Internet-Facing Firewall Configuration

Select the Application tab.

Under "Applications" Click "Add" then select "mysql".

Select the Actions tab.

Make sure the Action setting is set to "Allow" and check the "Log at Session Start" check box.

Click OK and Commit your changes.

The screenshot displays a firewall configuration interface with two main tabs: "Application" and "Actions".

Application Tab:

- Under "APPLICATIONS", there is a dropdown menu and a list of applications. One application, "mysql", is selected and highlighted.
- At the bottom of the list, there are "Add" and "Delete" buttons.

Actions Tab:

- The "Action Setting" section shows the "Action" dropdown set to "Allow".
- The "Log Setting" section includes checkboxes for "Log at Session Start" and "Log at Session End", both of which are checked.
- The "Profile Setting" section shows "Profile Type" set to "None".
- The "Other Settings" section includes "Schedule" (set to "None"), "QoS Marking" (set to "None"), and a "Disable Server Response" checkbox.

Below the tabs, a summary bar provides details for each rule, including rule number, name, source, destination, and action status.

Rule	Name	Source	Destination	Action
9	T10-database	none	universal	Allow
	dmz		192.168.201.2	any
	interconnect	192.168.201.2	any	mysql
	application...			Allow

Q2A Secure-Facing Firewall Configuration

Login to FortiGate.

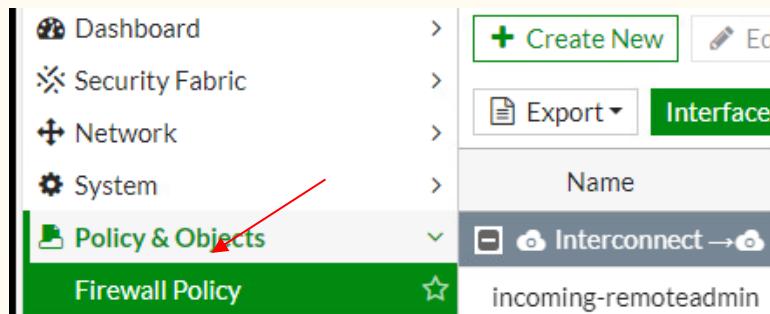
Select “Firewall Policy” from the right side menu.

Click “Create New”.

Name the new rule “database”.

Under Incoming Interface select “Interconnect”

Under Outgoing Interface select (Team number)-secure Under Service select “mysql”.



The screenshot shows the configuration of a firewall policy named "database". The policy is set to accept traffic on the "Interconnect" incoming interface and the "T10-secure (T10-secure)" outgoing interface. It is scheduled to run always and is configured to inspect MySQL traffic. The action is set to "ACCEPT". The inspection mode is "Flow-based". NAT is enabled. IP pool configuration is set to "Use Outgoing Interface Address". Preserve Source Port is disabled. Protocol options are set to "default".

Name	database
Incoming Interface	Interconnect
Outgoing Interface	T10-secure (T10-secure)
Source	[+] [+] []
Destination	[+] []
Schedule	always
Service	MySQL
Action	✓ ACCEPT ⚡ DENY
Inspection Mode	Flow-based Proxy-based
Firewall / Network Options	
NAT	ON
IP Pool Configuration	Use Outgoing Interface Address Use Dynamic IP Pool
Preserve Source Port	OFF
Protocol Options	PROT default

Q2A Secure-Facing Firewall Configuration

For the Source and Destination selections you must create two new address objects.

Select the Source selection window then select "Create".

Select "Address".

Enter "dmz-web" for the name.

Enter the IP address of the team's DMZ and subnet.

Click OK.

Repeat steps for the Destination selection.

The screenshot shows the configuration process for a secure-facing firewall. It consists of three main windows:

- Source Selection Window:** A dialog box where a new address object named "database" is being created. The "Source" field is highlighted with a yellow background. The "Incoming Interface" is set to "Interconnect" and the "Outgoing Interface" is set to "T10-secure (T10-secure)".
- Select Entries Dialog:** A list of existing address objects. It shows 14 entries under the "ADDRESS" tab, with an option to search or create more. One entry, "all", is selected.
- New Address Creation Dialog:** A form for creating a new address object named "dmz-web". The "Type" is set to "Subnet" with IP/Netmask "192.168.201.0/24". The "Interface" dropdown has "any" selected. The "Comments" field is empty. The "OK" button at the bottom right is visible.

Q2A Secure-Facing Firewall Configuration

Click OK.

Disable NAT

Configuration details:

Name	database
Incoming Interface	Interconnect
Outgoing Interface	T10-secure (T10-secure)
Source	dmz-web
Destination	secure-db
Schedule	always
Service	MYSQL
Action	<input checked="" type="radio"/> ACCEPT <input type="radio"/> DENY
Inspection Mode	<input checked="" type="radio"/> Flow-based <input type="radio"/> Proxy-based

Firewall / Network Options

NAT	<input checked="" type="checkbox"/>
IP Pool Configuration	<input checked="" type="radio"/> Use Outgoing Interface Address <input type="radio"/> Use Dynamic IP Pool
Preserve Source Port	<input checked="" type="checkbox"/>
Protocol Options	PROT default

incoming-remoteadmin				Secure	always	RDP SSH	ACCEPT	Disabled
database		dmz-web	secure-db	always	MYSQL	ACCEPT	Disabled	

Q2A Installation & Configuration

Login to the web server in the DMZ and check that you are able to connect to MariaDB located on the Secure zone host.

```
[cditto@localhost ~]$ mysql -p -u q2auser -h 192.168.203.3 q2a
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 57
Server version: 10.3.39-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

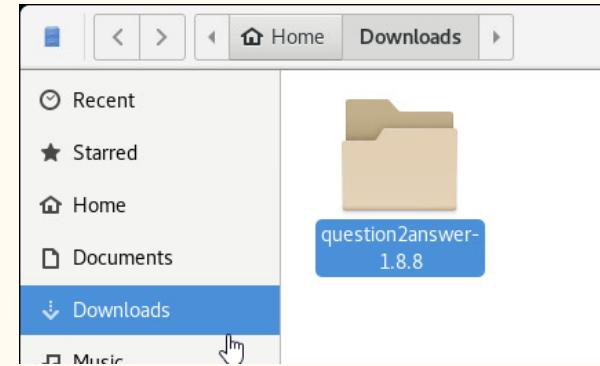
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [q2a]> █
```

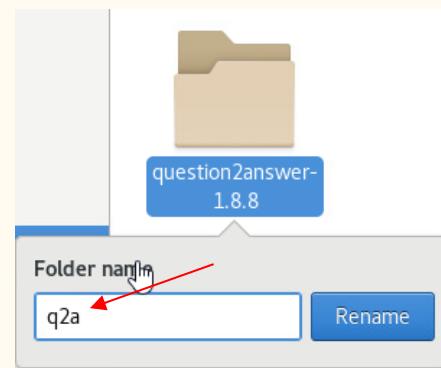
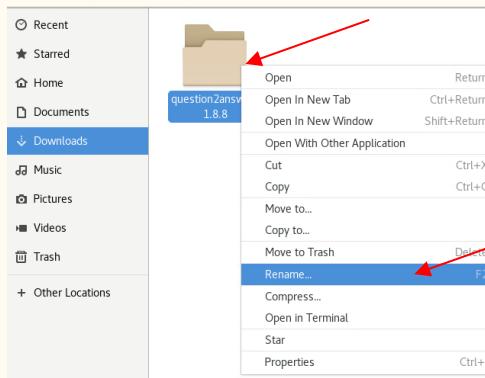
Q2A Installation & Configuration

Open the browser on the Apache server and download the Question2Answer package from the Question2Answer website.

A screenshot of a web browser displaying the Question2Answer website at <https://www.question2answer.org>. The page features a header with navigation links like 'Install', 'Customize', 'Plugins', 'Code', 'Contribute', 'Add-ONS', 'Services', 'Sites', and 'Q&A'. Below the header, there's a section titled 'Download Question2Answer', which includes a download button and a note about the latest version (1.8.8). Another note states that Q2A is open source and licensed under GPL v2+. To the right, there are sections for 'Easy to set up' and 'Core Q&A features'. A red arrow points from the top of the slide towards the download button on the website.



Extract the file into the downloads folder.

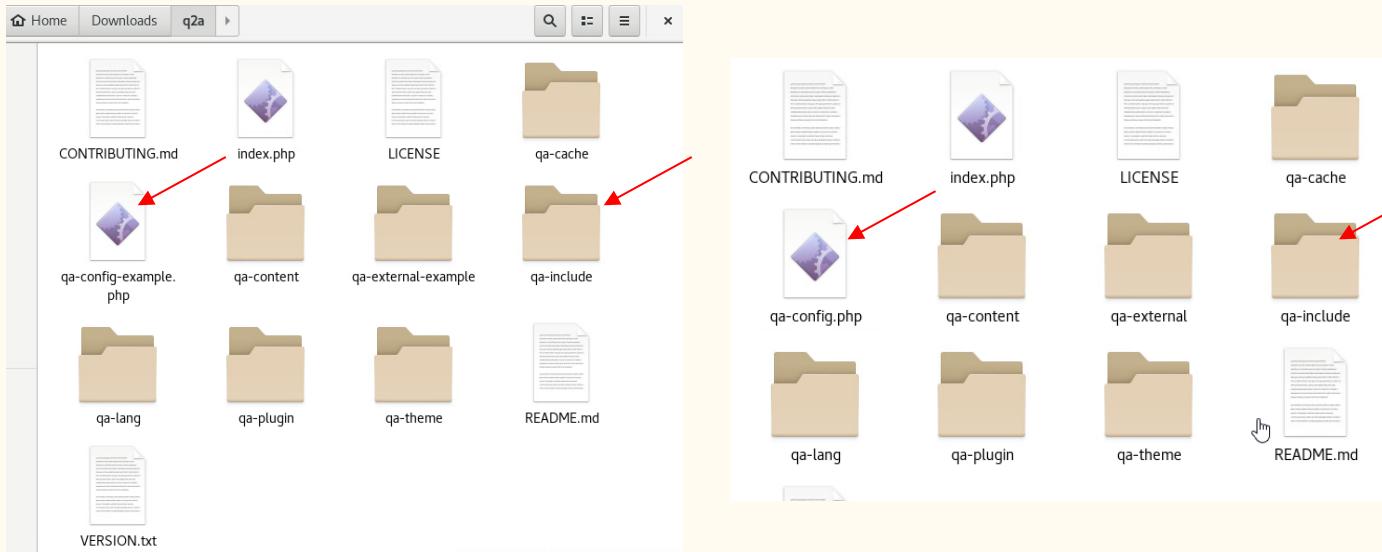


Rename the top file something easier like q2a.

Q2A Installation & Configuration

Open the q2a folder and change the names on the example files as per the instructions on the Question2Answer website.

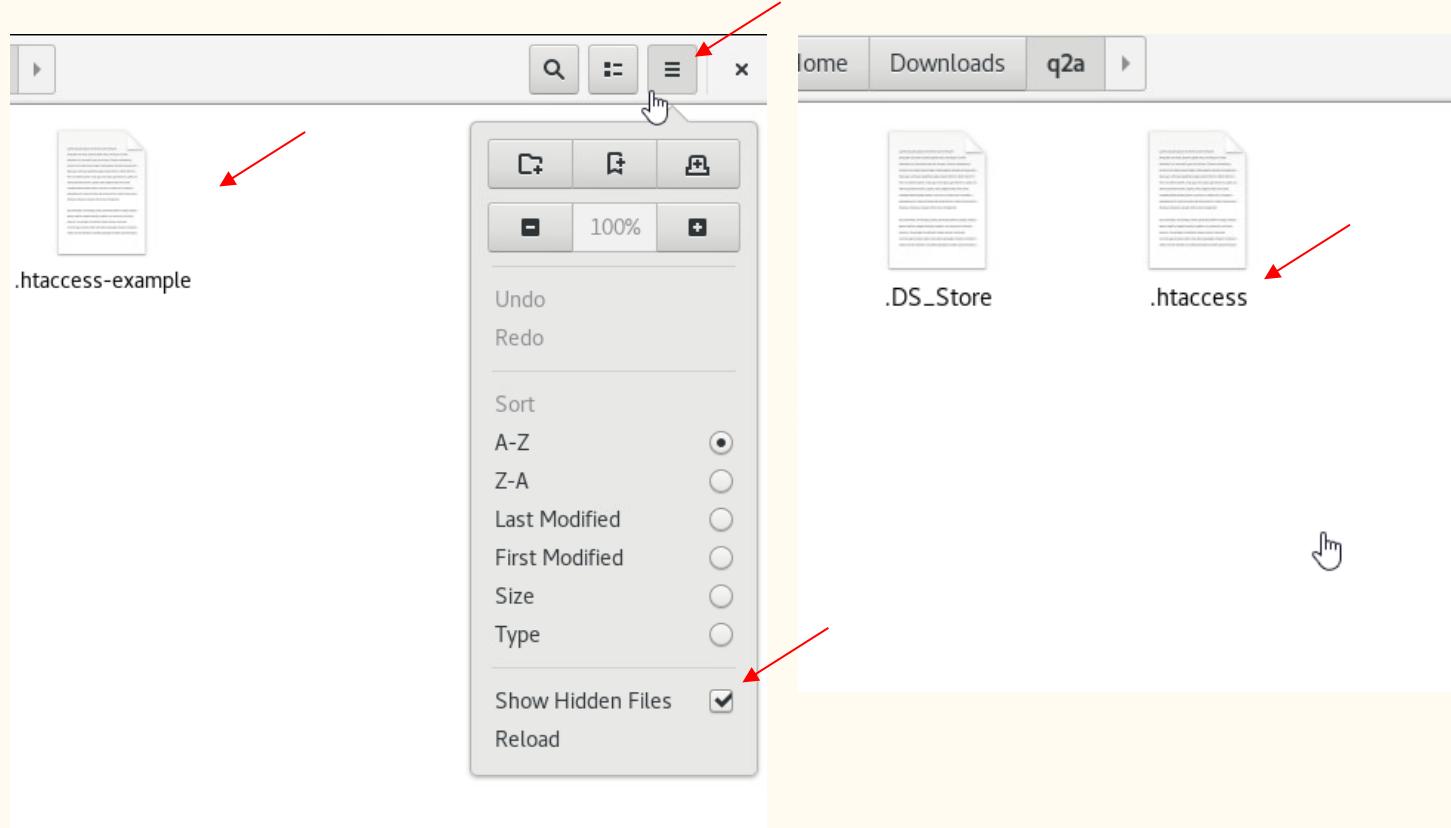
There is a hidden example file as well you will need to change.



Q2A Installation & Configuration

There is a hidden example file as well you will need to change.

Select the hamburger on the top right corner and check the box show hidden files. Now remove example from the filename.



Q2A Installation & Configuration

Open the config file
and

Scroll down to the PHP code that defines the database configuration file.

Change the settings to fit your teams database IP, username, password, and database name..

Save your changes
by clicking save in
the top right corner.

```
/*
=====
 THE 4 DEFINITIONS BELOW ARE REQUIRED AND MUST BE SET BEFORE USING!
=====

For QA_MYSQL_HOSTNAME, try '127.0.0.1' or 'localhost' if MySQL is on the same server.

For persistent connections, set the QA_PERSISTENT_CONN_DB at the bottom of this file; do NOT
prepend the hostname with 'p:'.

To use a non-default port, add the following line to the list of defines, with the appropriate port number:
define('QA_MYSQL_PORT', '3306');

+/
define('QA_MYSQL_HOSTNAME', '127.0.0.1');
define('QA_MYSQL_USERNAME', 'your-mysql-username');
define('QA_MYSQL_PASSWORD', 'your-mysql-password');
define('QA_MYSQL_DATABASE', 'your-mysql-db-name');

/*
...  

define('QA_MYSQL_HOSTNAME', '192.168.203.3');
define('QA_MYSQL_USERNAME', 'q2auser');
define('QA_MYSQL_PASSWORD', 'q2a10pass');
define('QA_MYSQL_DATABASE', 'q2a');
```

Q2A Installation & Configuration

Move the Question2Answer files to the web server's "DocumentRoot" folder using the following commands. The last two commands move the hidden files we explored earlier.

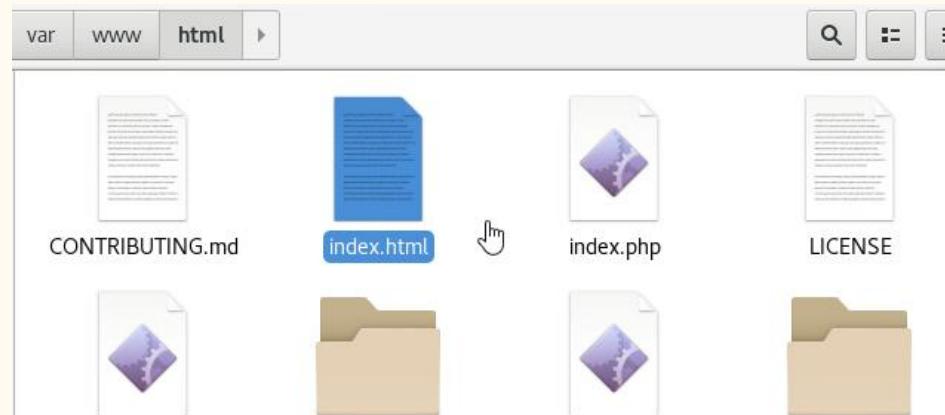
```
[cditto@localhost q2a]$ sudo mv * /var/www/html
```

```
[cditto@localhost q2a]$ sudo mv .htaccess /var/www/html
```

```
[cditto@localhost q2a]$ sudo mv .DS_Store /var/www/html
```

Q2A Installation & Configuration

In the web server's "DocumentRoot" folder, remove the index.html file so that the web server will serve the Question2Answer's index.php code instead.



```
[cditto@localhost q2a]$ sudo rm /var/www/html/index.html
```

Q2A Installation & Configuration

The Q2A files that were moved from the download directory to the html directory were automatically labeled when they were placed in the download folder.

These files need to be restored to the correct labels based on the context of where they reside in the file system.

```
[cditto@localhost html]$ ls -Z  
unconfined_u:object_r:user_home_t:s0 CONTRIBUTING.md  
unconfined_u:object_r:user_home_t:s0 index.php  
unconfined_u:object_r:user_home_t:s0 LICENSE  
unconfined_u:object_r:user_home_t:s0 qa-cache  
unconfined_u:object_r:user_home_t:s0 qa-config.php  
unconfined_u:object_r:user_home_t:s0 qa-content  
unconfined_u:object_r:user_home_t:s0 qa-external  
unconfined_u:object_r:user_home_t:s0 qa-include  
unconfined_u:object_r:user_home_t:s0 qa-lang  
unconfined_u:object_r:user_home_t:s0 qa-plugin  
unconfined_u:object_r:user_home_t:s0 qa-theme  
unconfined_u:object_r:user_home_t:s0 README.md  
unconfined_u:object_r:user_home_t:s0 VERSION.txt
```

```
[cditto@localhost www]$ restorecon -R html
```

```
[cditto@localhost html]$ ls -Z  
unconfined_u:object_r:httpd_sys_content_t:s0 CONTRIBUTING.md  
unconfined_u:object_r:httpd_sys_content_t:s0 index.php  
unconfined_u:object_r:httpd_sys_content_t:s0 LICENSE  
unconfined_u:object_r:httpd_sys_content_t:s0 qa-cache  
unconfined_u:object_r:httpd_sys_content_t:s0 qa-config.php  
unconfined_u:object_r:httpd_sys_content_t:s0 qa-content  
unconfined_u:object_r:httpd_sys_content_t:s0 qa-external  
unconfined_u:object_r:httpd_sys_content_t:s0 qa-include  
unconfined_u:object_r:httpd_sys_content_t:s0 qa-lang  
unconfined_u:object_r:httpd_sys_content_t:s0 qa-plugin  
unconfined_u:object_r:httpd_sys_content_t:s0 qa-theme  
unconfined_u:object_r:httpd_sys_content_t:s0 README.md  
unconfined_u:object_r:httpd_sys_content_t:s0 VERSION.txt
```

Q2A Installation & Configuration

In this app, PHP
uses json.

Download json to
the machine.

Restart the machine
so the PHP engine
will notice its new
functions.

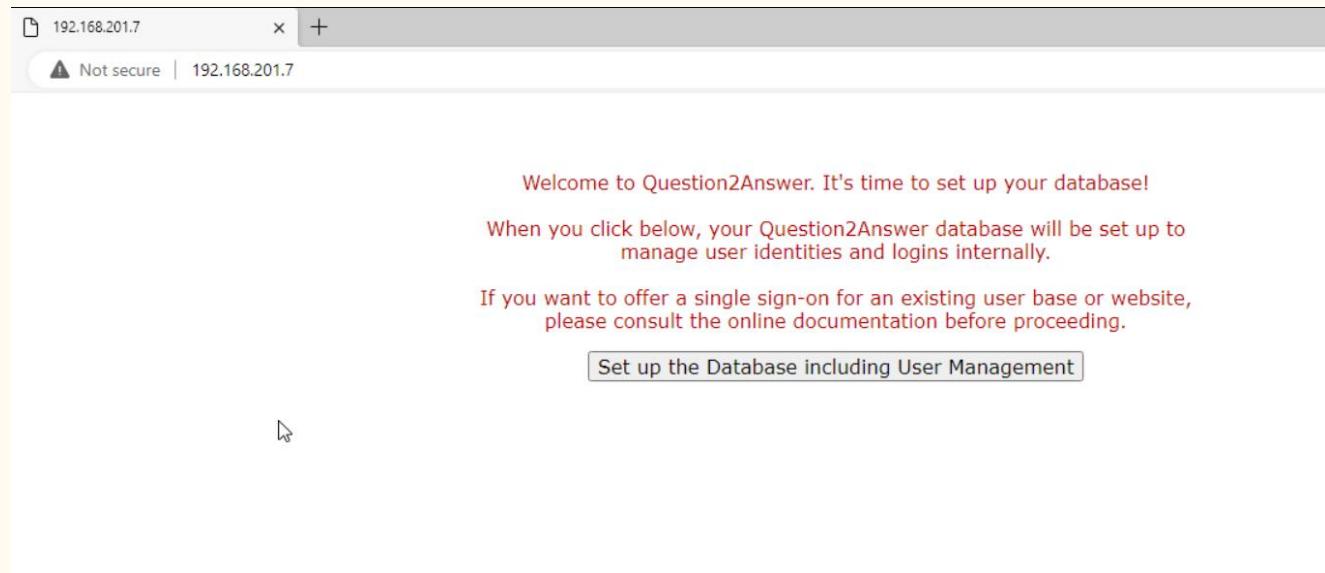
```
[cditto@localhost html]$ sudo dnf -y install php-json
```

```
Installed:  
  php-json-7.2.24-1.module_el8.3.0+2010+7c76a223.x86_64
```

```
Terminal Feb 7 9:57 AM cditto@localhost:/etc/httpd/conf
```

```
success
[cditto@localhost conf]$ firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens192
  sources:
  services: cockpit dhcpv6-client http https ssh
  ports: 80/tcp 8443/tcp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[cditto@localhost conf]$ systemctl restart http
Failed to restart http.service: Unit http.service not found.
[cditto@localhost conf]$ systemctl restart httpd
[cditto@localhost conf]$ sudo nano httpd.conf
[sudo] password for cditto:
[cditto@localhost conf]$ systemctl restart httpd
[cditto@localhost conf]$ sudo semanage boolean --modify --on httpd_can_network_connect
[cditto@localhost conf]$ sudo semanage boolean --modify --on httpd_can_network_connect_db
```

Q2A Installation & Configuration



Q2A Installation & Configuration

Congratulations - Your Question2Answer site is ready to go!

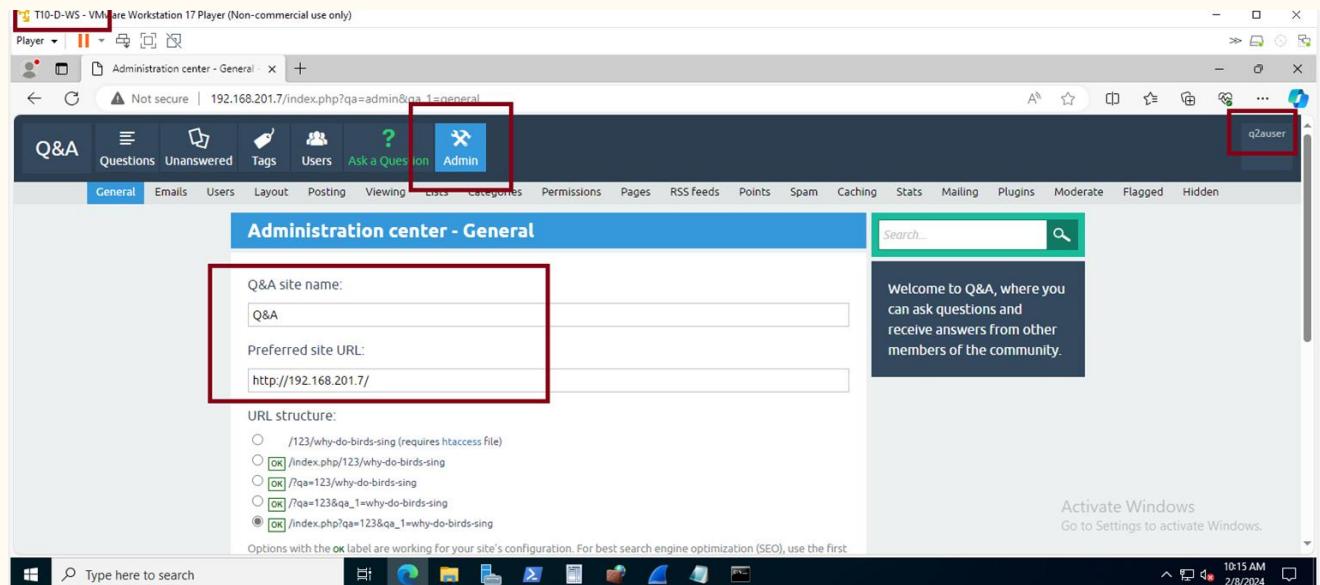
You are logged in as the super administrator and can start changing settings.

Thank you for installing Question2Answer.

[Go to admin center](#)

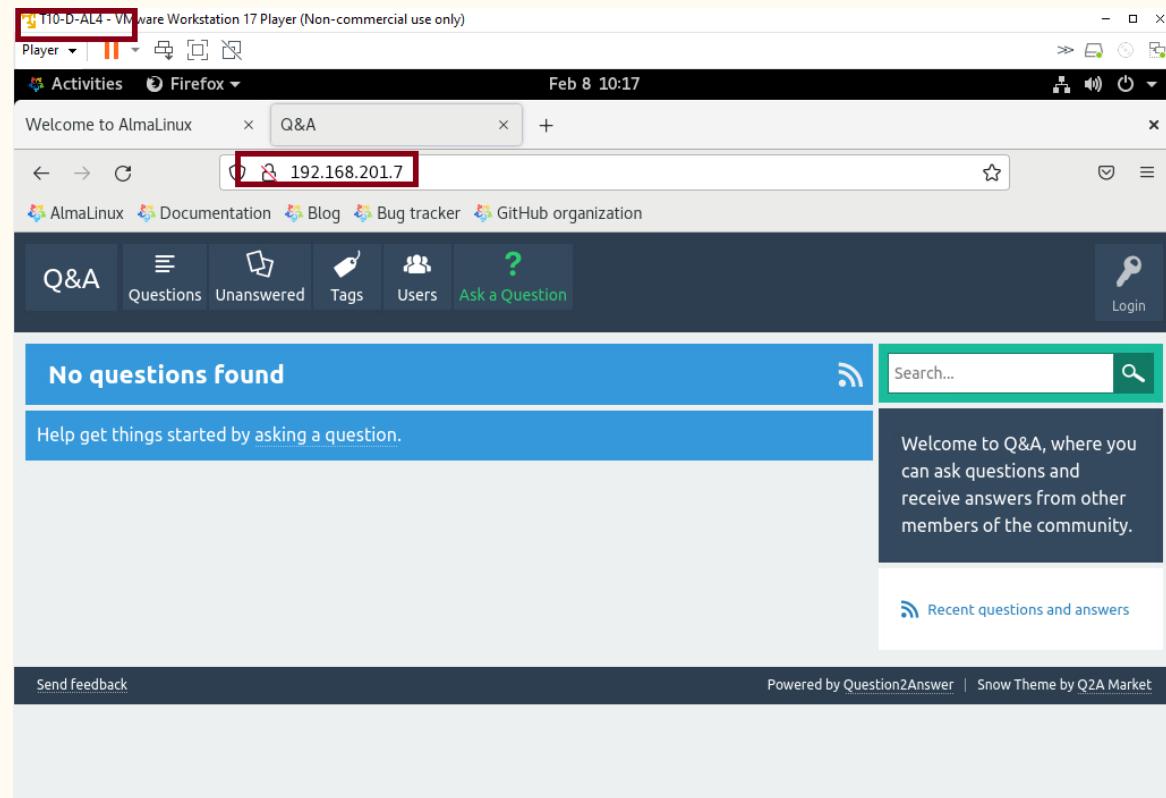
Q2A Installation & Configuration

Q2a page open in windows system in the DMZ zone



Q2A Installation & Configuration

Q2a page open in Linux system in the DMZ zone. This system is the one that host the apache server.



Q2A Installation & Configuration

Restrict access to phpinfo.php .

Since we expose our app to the untrusted internet before we restrict access using chown command .

```
sudo chown -R /var/www/html/phpinfo.php
```

Q2A Installation & Configuration

Enable the web browsing rule to test the internet connection from outside.

Remember to commit the changes after enable the rule.

PA-440 DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE Commit

Security

NAME	TAGS	TYPE	Source				Destination				APPLICATION	SERVICE	ACTION	PROFILE	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE						
rule1	none	universal	trust	any	any	any	untrust	any	any	any	any	any	Allow	none	
T10-outbound	none	universal	dmz	192.168.201.0/24	any	any	outside	any	any	any	any	application-d...	Allow	none	
T10-dmz-to-inside-remote-access	none	universal	dmz	192.168.201.0/24	any	any	inside	192.168.202.0/24	any	ms-rdp	ssh	application-d...	Allow	none	
T10-inside-to-dmz-all	none	universal	inside	192.168.202.0/24	any	any	dmz	192.168.201.0/24	any	any	any	application-d...	Allow	none	
T10-secure-to-dmz-inside	none	universal	interconnect	192.168.203.0/24	any	any	dmz	192.168.201.0/24	any	any	any	application-d...	Allow	none	
T10-squid-proxy	none	universal	interconnect	192.168.203.0/24	any	any	dmz	192.168.201.0/24	any	any	any	service-squid	Allow	none	
T10-to-Secure-Remote-Admin	none	universal	dmz	192.168.201.0/24	any	any	interconnect	192.168.203.0/24	any	ms-rdp	ssh	application-d...	Allow	none	
T10-web	none	universal	outside	any	any	any	dmz	192.168.201.22.22	any	any	any	web-browsing	application-d...	Allow	none
T10-database-maria	none	universal	dmz	192.168.201.7	any	any	interconnect	192.168.203.3	any	mysql	any	application-d...	Allow	none	
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	any	Allow	none	
interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	any	Deny	none	

Policy Optimizer

New App Viewer	1
Rules Without App Controls	4
Unused Apps	0
Rule Usage	
Unused in 30 days	1
Unused in 90 days	1
Unused	1

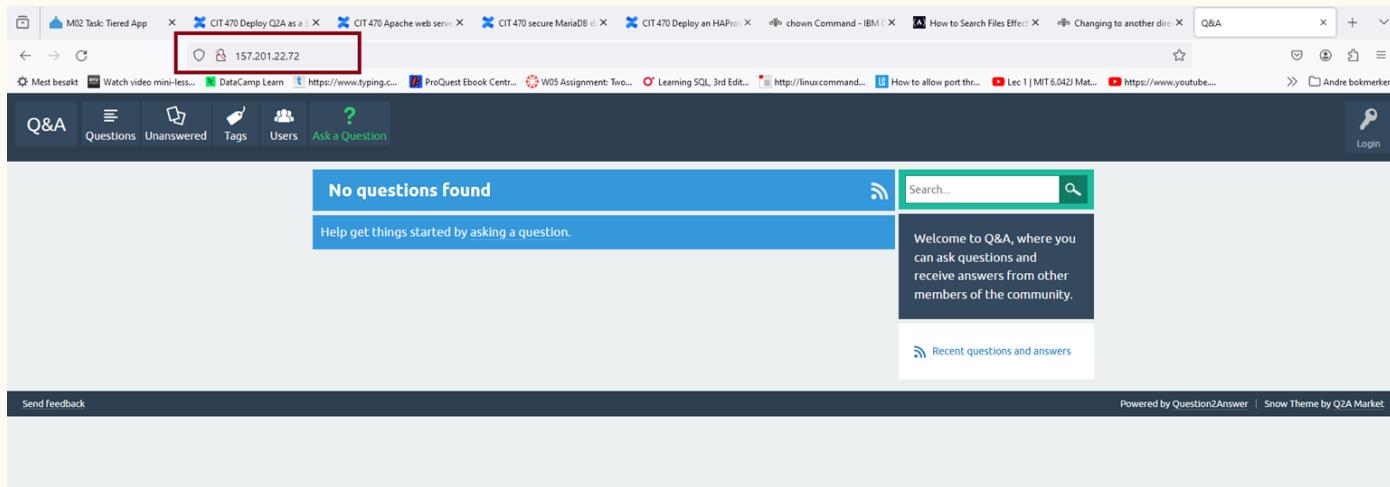
Object : Addresses + Add Delete Clone Override Refresh Enable Disable Move PDF/CSV Highlight Unused Rules View Rulebase as Groups Reset Rule Hit Counter Group Test Policy Match

cgerer | Logout | Last Login Time: 02/05/2024 14:01:24 | Session Expire Time: 03/09/2024 10:55:47 | Tasks | Language | [Paloalto](#)

Q2A Installation & Configuration

Access the q2a from a computer outside our network. Use the browser and put the outside address, in this case:

157.201.22.72

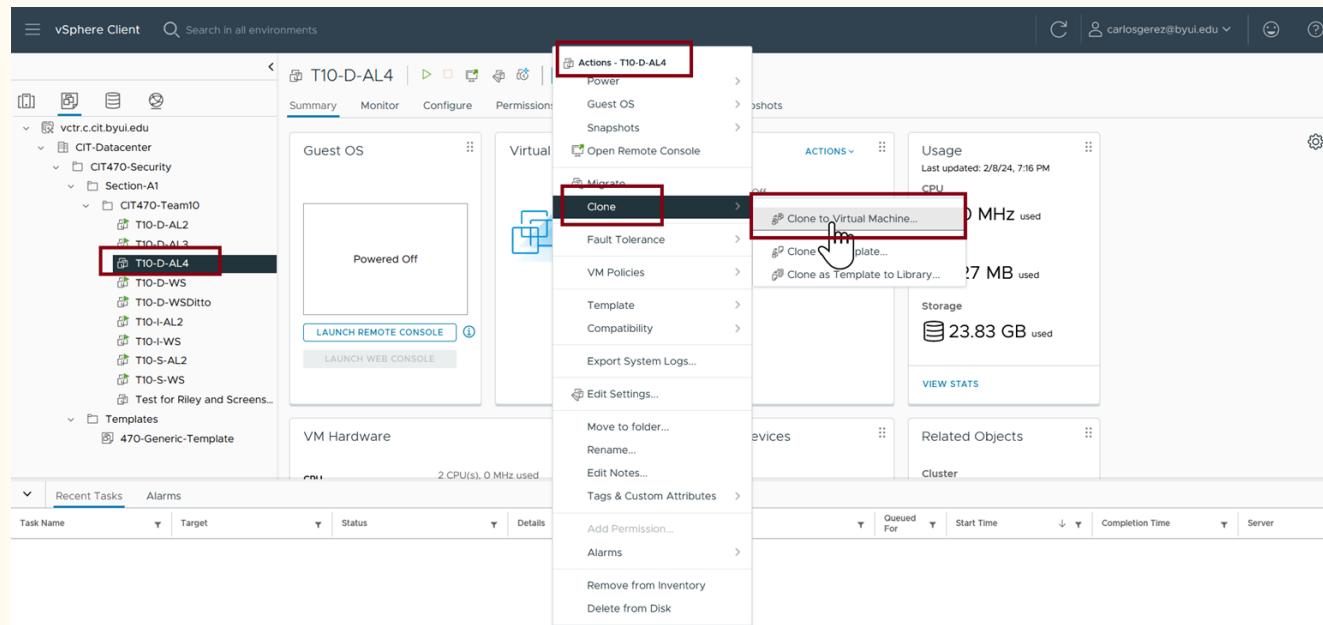


HAProxy load balancer configuration

Cloning the machine that holds the apache server.

Before start, power off the machine that will be cloned.

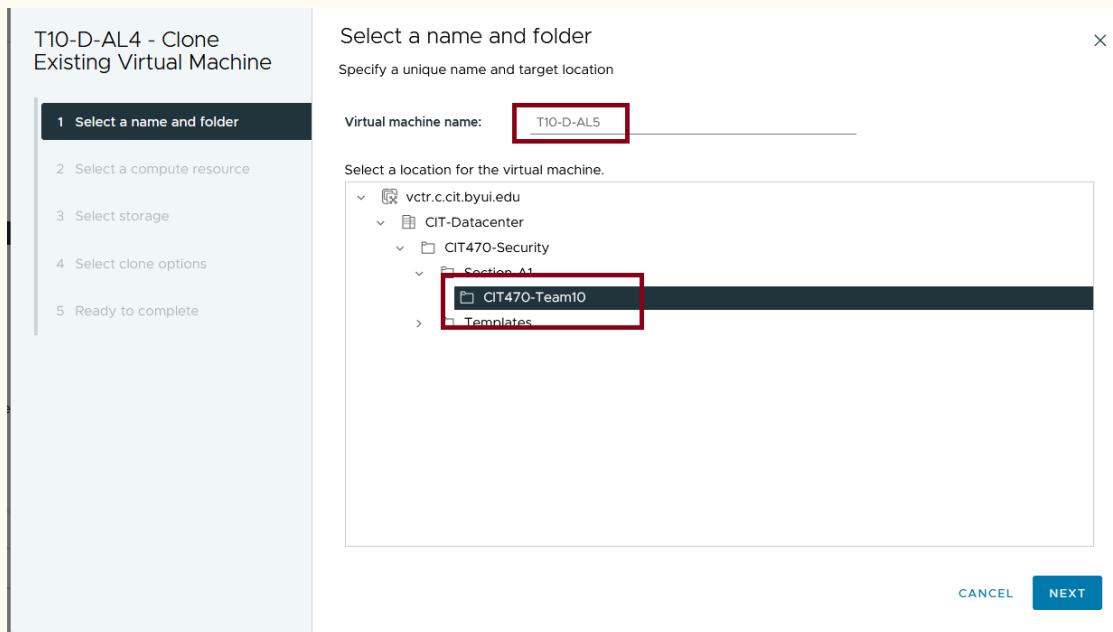
Use actions tab in sphere to get to the clone options menu.



Cloning the machine that holds the apache server.

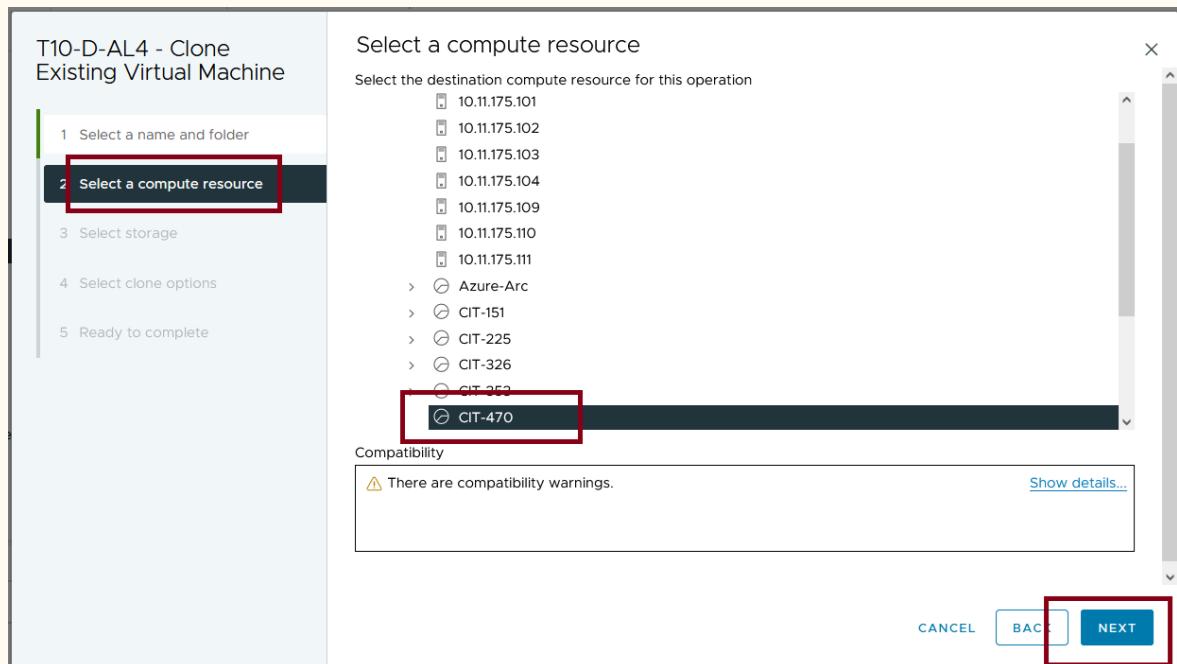
From now on follow the indications in the screen.

First select a name and a folder were the machine will reside. Press next.



Cloning the machine that holds the apache server.

Select a computer resource, in our class the assigned for our class. Press next.



Cloning the machine that holds the apache server.

Select the storage and click in same format as source. Press next.

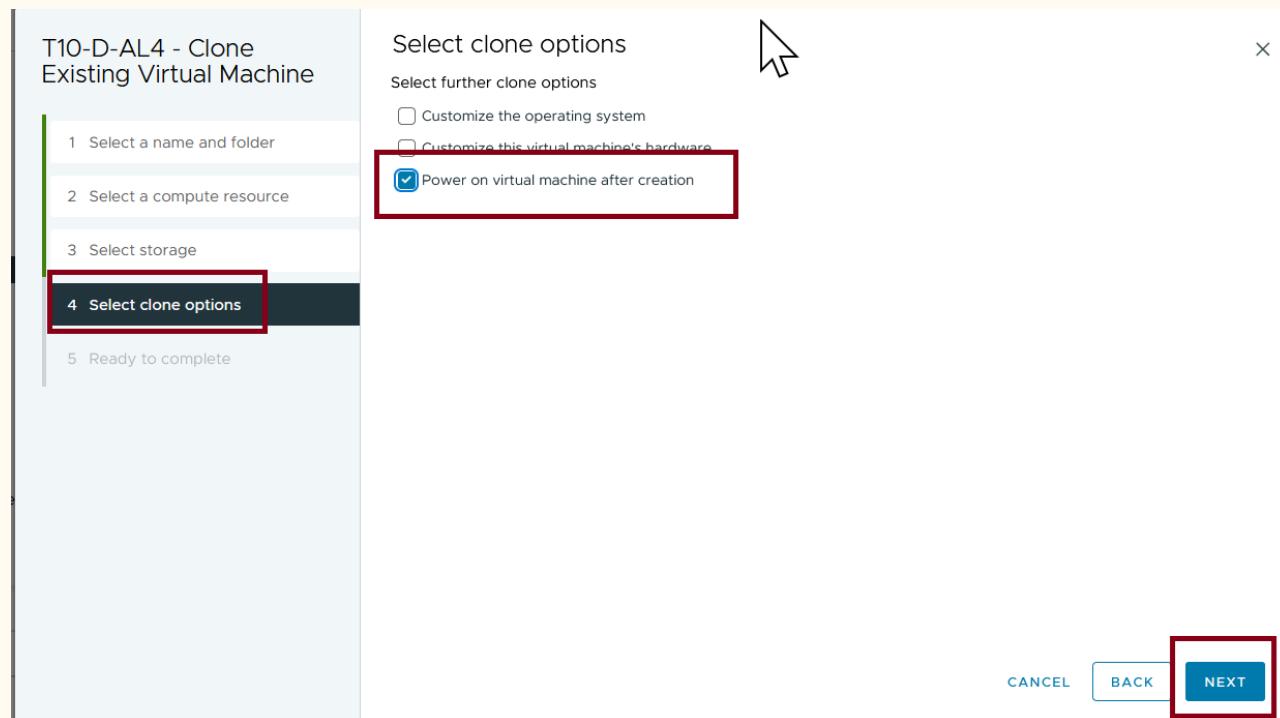
The screenshot shows the 'T10-D-AL4 - Clone Existing Virtual Machine' wizard at step 3: 'Select storage'. A red box highlights the 'Select storage' button. The 'CONFIGURE PER DISK' tab is selected. Under 'Select virtual disk format', a dropdown menu is open with 'Same format as source' selected, also highlighted with a red box. A warning icon is shown next to the dropdown. Below it is the 'VM Storage Policy' section. The main area displays a table of storage resources:

Name	Storage Compatibility	Capacity	Provisioned	Free
CIT	--	64 TB	47 TB	17 TB

A red box highlights the 'CIT' row. At the bottom, a compatibility message states: 'Compatibility checks succeeded.' with a green checkmark. The 'NEXT' button is highlighted with a red box.

Cloning the machine that holds the apache server.

On clone options select power on virtual machine after creation. Press next.



Cloning the machine that holds the apache server.

Review and
press finish.

T10-D-AL4 - Clone Existing Virtual Machine

1 Select a name and folder

2 Select a compute resource

3 Select storage

4 Select clone options

5 Customize hardware

6 Ready to complete

Ready to complete

Click Finish to start creation.

Source virtual machine: T10-D-AL4

Virtual machine name: T10-D-AL5

Folder: CIT470-Team10

Resource pool: CIT-470

Datastore: CIT [UCS ESXi v104 - SMIF700] (Recommended) [more recommendations](#)

Disk storage: Same format as source

Hard disk 1

Capacity: 96 GB

Datastore: CIT [UCS ESXi v104 - SMIF700] (Recommended) (Same format as source) [more recommendations](#)

Virtual device node

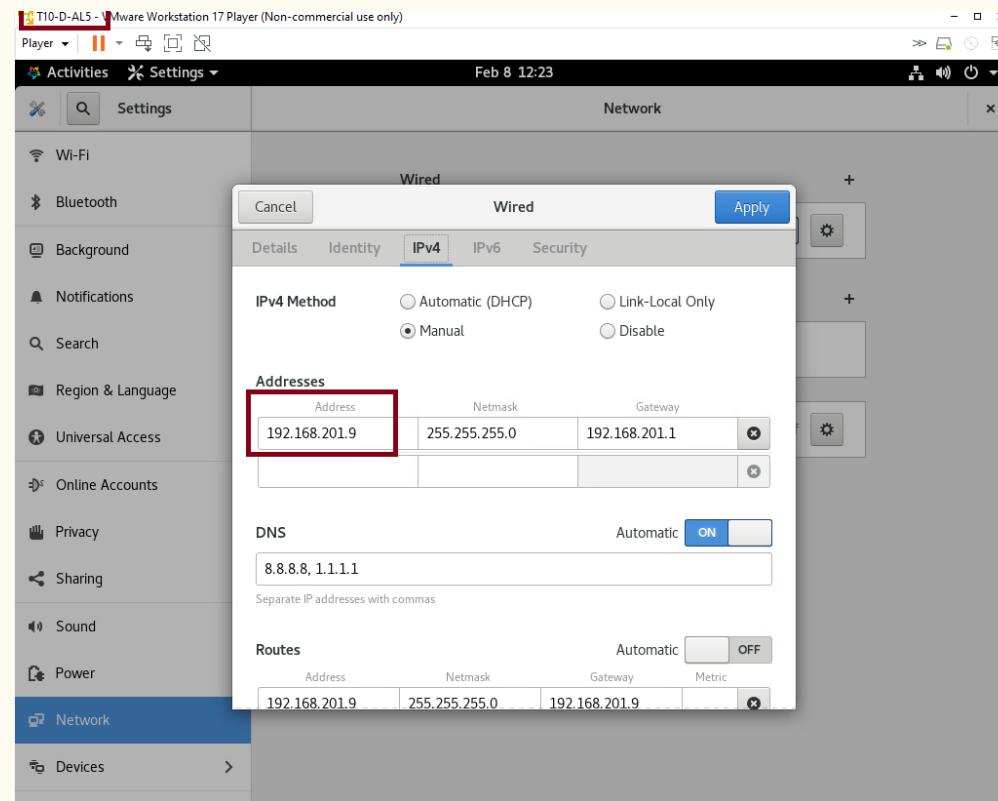
Mode



CANCEL BACK FINISH

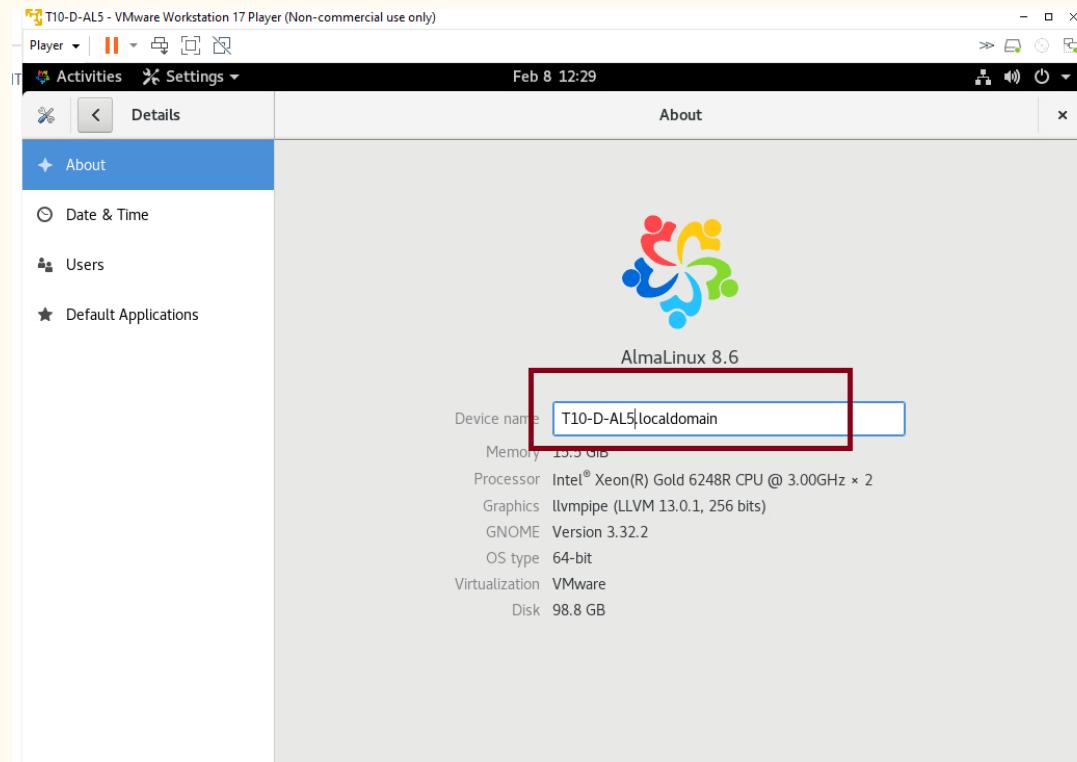
Cloning the machine that holds the apache server.

Change the ip addresses to the new machine address.



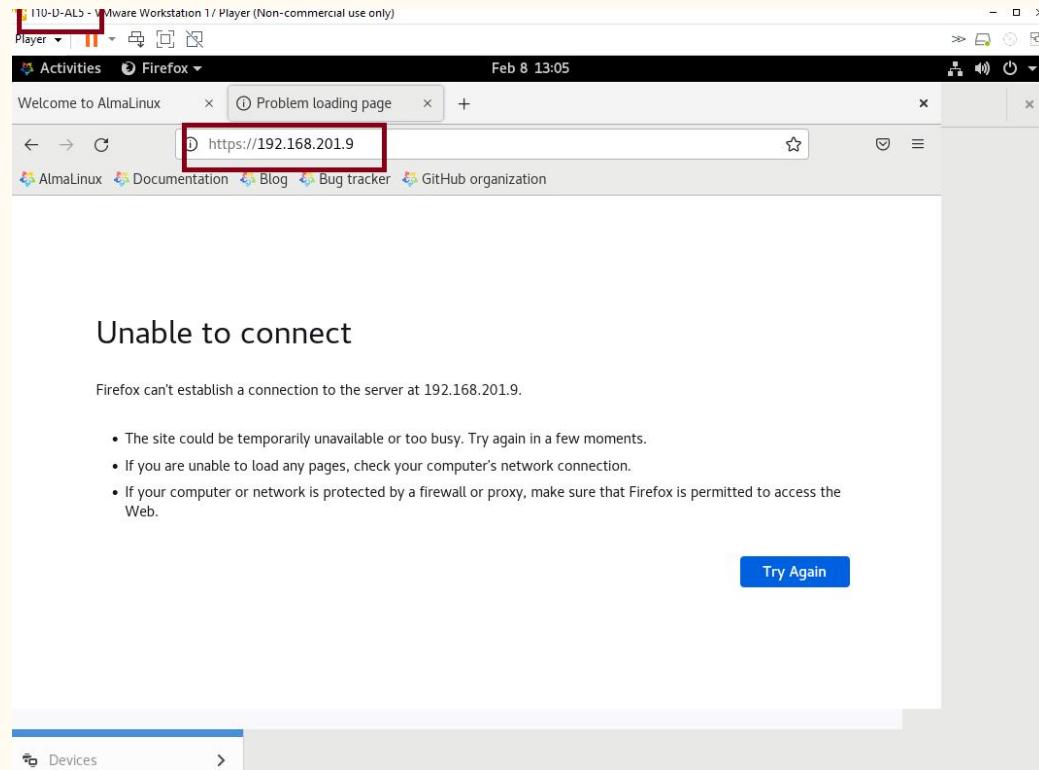
Cloning the machine that holds the apache server.

Change the name
to the correct
new name.



Configuring the app in the cloned machine.

When trying to connect to the server in the cloned machine we cannot.



Configuring the app in the cloned machine.

We have to edit the configuration file to put the new listening address. The file we have to update is httpd.conf. We use the following commands:

1. change to the directory:

```
cd /etc/httpd/conf
```

1. edit the file with vi and change the Listen address.

```
sudo vi httpd.conf
```

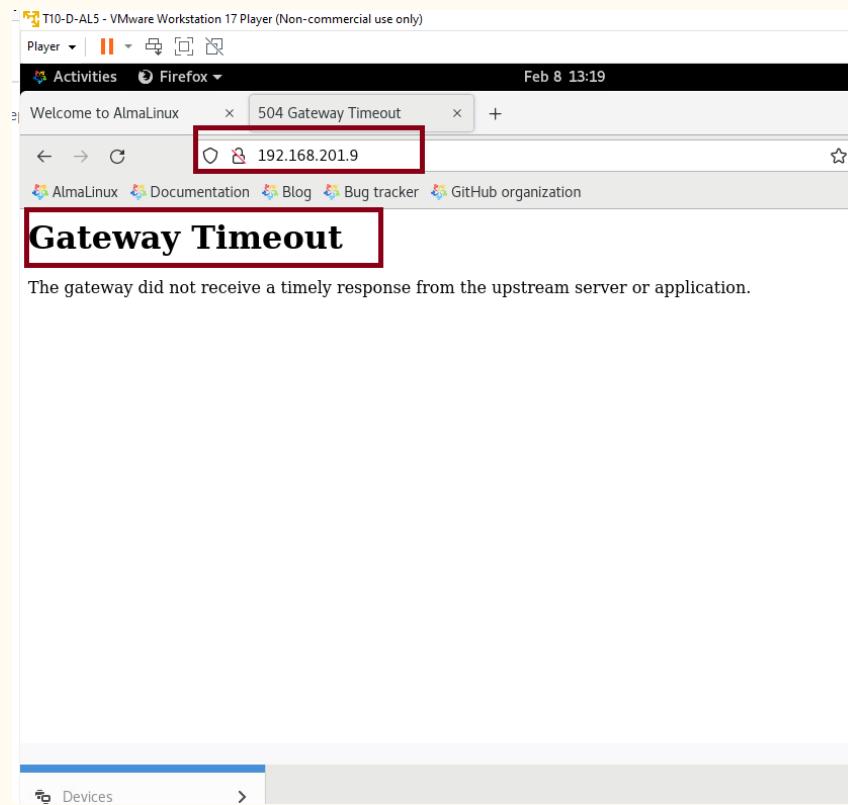
1. restart the service to apply the changes.

```
systemctl restart httpd
```

```
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
# ServerRoot "/etc/httpd"
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 192.168.201.9:80
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
-- INSERT --
```

Configuring the app in the cloned machine.

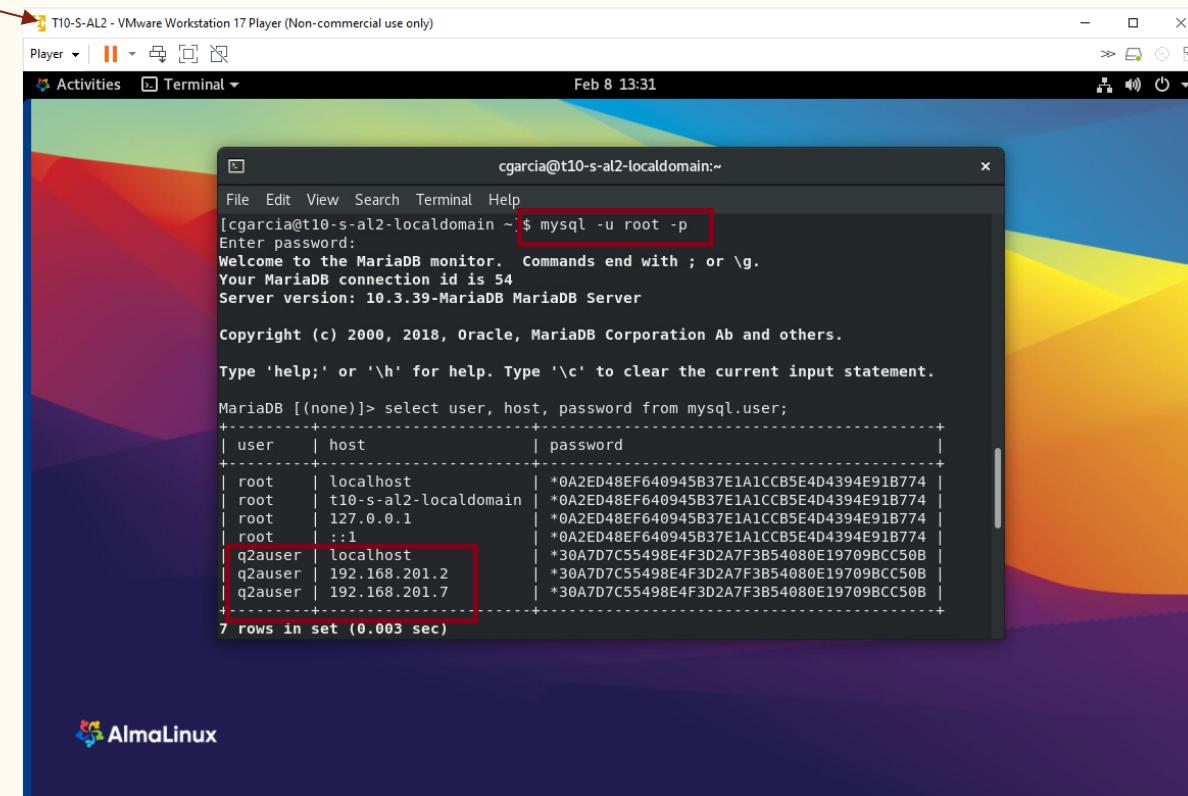
We get this new message because the mariadb database is not yet configured to connect with this machine.



Configuring the app in the cloned machine.

In the secure zone machine that host the mariadb we must configure the access from the new server. The first command give access as root to the database:

```
mysql -u root -p
```



Configuring the app in the cloned machine.

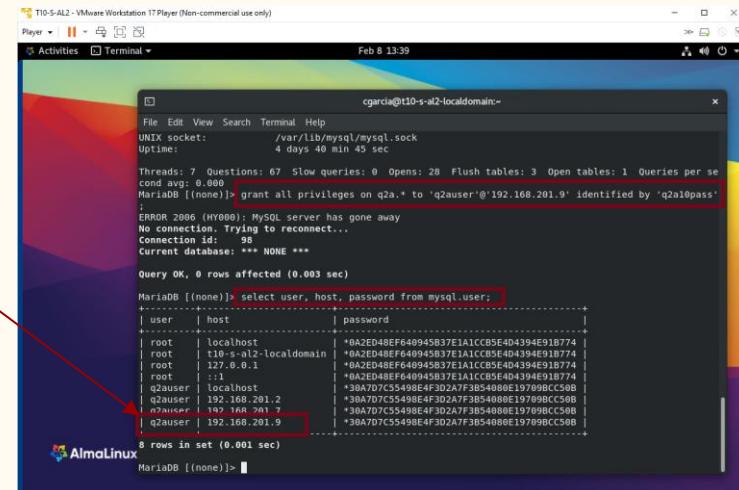
To give access use the following command:

```
grant all privileges on q2a.* to q2auser'@'192.168.201.9' identified by 'q2a10pass';
```

Then you can use the following command to check the result:

```
select user, host, password from mysql.user;
```

In the last line appears the new access.



The screenshot shows a terminal window titled "T10-S-AL2 - VMware Workstation 17 Player (Non-commercial use only)". The terminal output is as follows:

```
File Edit View Search Terminal Help
UNIX socket: /var/lib/mysql/mysql.sock
Uptime: 4 days 40 min 45 sec
Threads: 7 Questions: 67 Slow queries: 0 Opens: 28 Flush tables: 3 Open tables: 1 Queries per second avg: 0.000
MariaDB [(none)]> grant all privileges on q2a.* to q2auser'@'192.168.201.9' identified by 'q2a10pass';
ERROR 2006 (HY000): MySQL server has gone away
No connection. Trying to reconnect...
Connection id: 95
Current database: *** NONE ***
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> select user, host, password from mysql.user;
+-----+-----+-----+
| user | host | password |
+-----+-----+-----+
| root | localhost | *0A2E048EF640945837E1A1CC05E4D4394E91B774 |
| root | t10-s-al2-localhost | *0A2E048EF640945837E1A1CC05E4D4394E91B774 |
| root | 127.0.0.1 | *0A2E048EF640945837E1A1CC05E4D4394E91B774 |
| root | ::1 | *0A2E048EF640945837E1A1CC05E4D4394E91B774 |
| q2auser | localhost | *30A7D7C55498E4F3D2A7F3B54080E19709BCC50B |
| q2auser | 192.168.201.2 | *30A7D7C55498E4F3D2A7F3B54080E19709BCC50B |
| q2auser | 192.168.201.7 | *30A7D7C55498E4F3D2A7F3B54080E19709BCC50B |
| q2auser | 192.168.201.9 | *30A7D7C55498E4F3D2A7F3B54080E19709BCC50B |
+-----+-----+-----+
6 rows in set (0.001 sec)

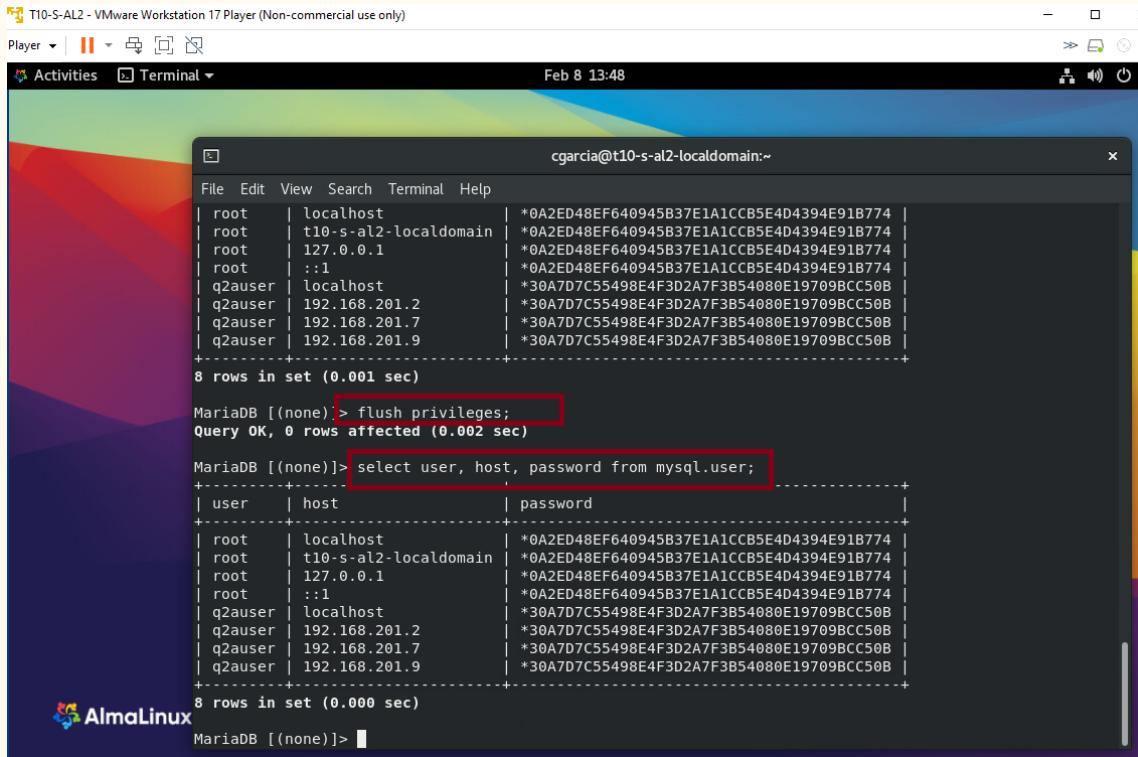
MariaDB [(none)]>
```

A red arrow points from the text "In the last line appears the new access." to the line containing the IP address 192.168.201.9 in the terminal output.

Configuring the app in the cloned machine.

Remember to
flush those
privileges:

flush privileges;



```
File Edit View Search Terminal Help
cgarcia@t10-s-al2-localhost:~
```

```
+-----+-----+
| user | host          | password |
+-----+-----+
| root | localhost     | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |
| root | t10-s-al2-localhost | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |
| root | 127.0.0.1      | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |
| root | ::1            | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |
| q2auser | localhost    | *30A7D7C55498E4F3D2A7F3B54080E19709BCC50B |
| q2auser | 192.168.201.2 | *30A7D7C55498E4F3D2A7F3B54080E19709BCC50B |
| q2auser | 192.168.201.7 | *30A7D7C55498E4F3D2A7F3B54080E19709BCC50B |
| q2auser | 192.168.201.9 | *30A7D7C55498E4F3D2A7F3B54080E19709BCC50B |
+-----+-----+
8 rows in set (0.001 sec)
```

```
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.002 sec)
```

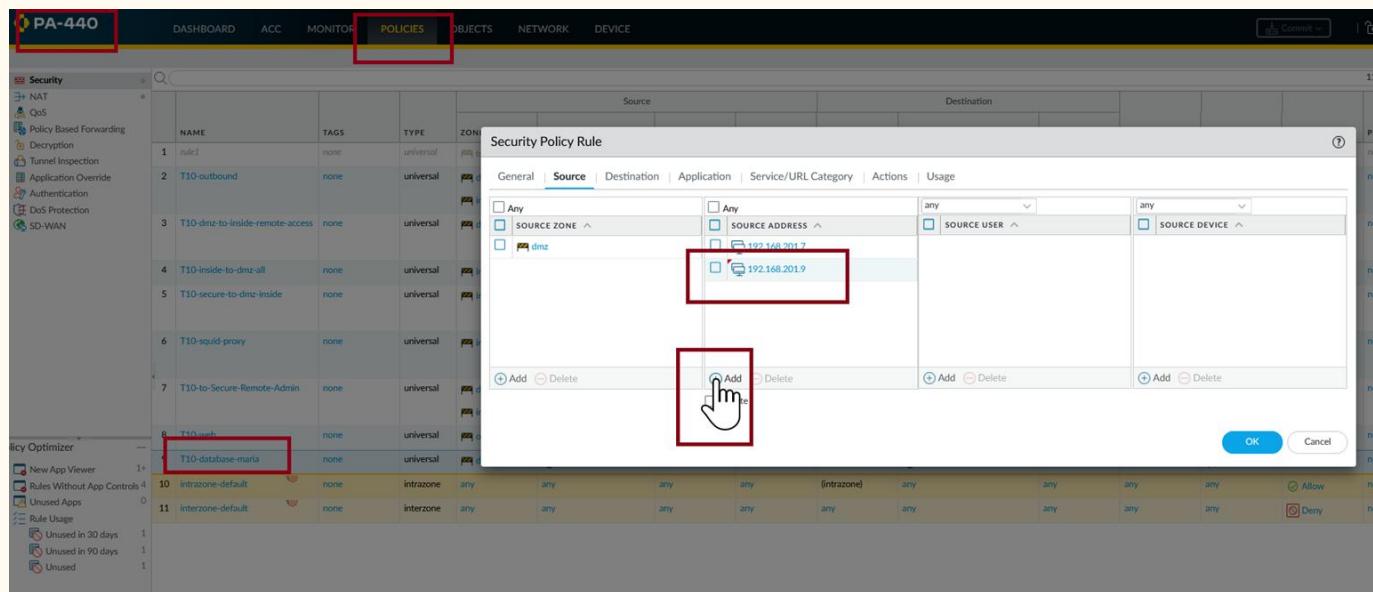
```
MariaDB [(none)]> select user, host, password from mysql.user;
+-----+-----+
| user | host          | password |
+-----+-----+
| root | localhost     | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |
| root | t10-s-al2-localhost | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |
| root | 127.0.0.1      | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |
| root | ::1            | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |
| q2auser | localhost    | *30A7D7C55498E4F3D2A7F3B54080E19709BCC50B |
| q2auser | 192.168.201.2 | *30A7D7C55498E4F3D2A7F3B54080E19709BCC50B |
| q2auser | 192.168.201.7 | *30A7D7C55498E4F3D2A7F3B54080E19709BCC50B |
| q2auser | 192.168.201.9 | *30A7D7C55498E4F3D2A7F3B54080E19709BCC50B |
+-----+-----+
8 rows in set (0.000 sec)
```

```
MariaDB [(none)]>
```

AlmaLinux

Configuring the app in the cloned machine.

We have to give access also in the Firewalls. On the Palo Alto policies add the new address to the rule to allow mysql from the dmz zone. In policies select the rule, and in the source tab add the new address. Don't forget to commit your changes.



Configuring the app in the cloned machine.

Then to add access in the Fortigate, opened from a machine in the secure zone create a new address object to add to the rule that allows connections from the DMZ.

In **Policy & Objects** tab, select **Addresses**, and the **Create New** tab.

The screenshot shows the FortiGate 61F 470FGOL configuration interface. The left sidebar navigation bar is highlighted with red boxes around the 'Policy & Objects' tab, the 'Addresses' sub-tab under 'Internet Service Database', and the 'Create New' button in the top right of the main content area. The main content area displays a table of existing address objects, including 'DMZ', 'FABRIC_DEVICE', 'FIREWALL_AUTH_PORTAL_AD...', 'Inside', 'SSLVPN_TUNNEL_ADDR1', 'Secure', 'all', 'dmz-web', 'none', and 'secure-db'. Below this table are sections for 'FortiClient EMS Tag (IP Address)' and 'FQDN'. The URL in the browser bar is https://192.168.203.1/ng/firewall/service.

Configuring the app in the cloned machine.

Then create the new address as the one created before to allow connections for the other machine and press **OK**.

The screenshot shows the FortiGate 61F 470FGOL web interface. The left sidebar navigation menu includes: Dashboard, Security Fabric, Network, System, Policy & Objects (selected), Firewall Policy, Addresses (selected), Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shapers, Traffic Shaping Policy, Traffic Shaping Profile, Security Profiles, VPN, User & Authentication, WiFi & Switch Controller, and Log & Report. The main content area displays the 'New Address' configuration dialog. The 'Name' field contains 'dmz-web2'. The 'Type' dropdown is set to 'IP Range', and the 'IP Range' field shows '192.168.201.9 - 192.168.201.9'. The 'Interface' dropdown is set to 'Interconnect'. A red box highlights the 'Name' field and the 'IP Range' field. At the bottom right of the dialog are 'OK' and 'Cancel' buttons. The top right corner of the interface shows the VDOM as 'OLTeam10' and various system status icons.

Configuring the app in the cloned machine.

Then select Firewall Policy tab and select the database rule by clicking into that line. Then select Edit.

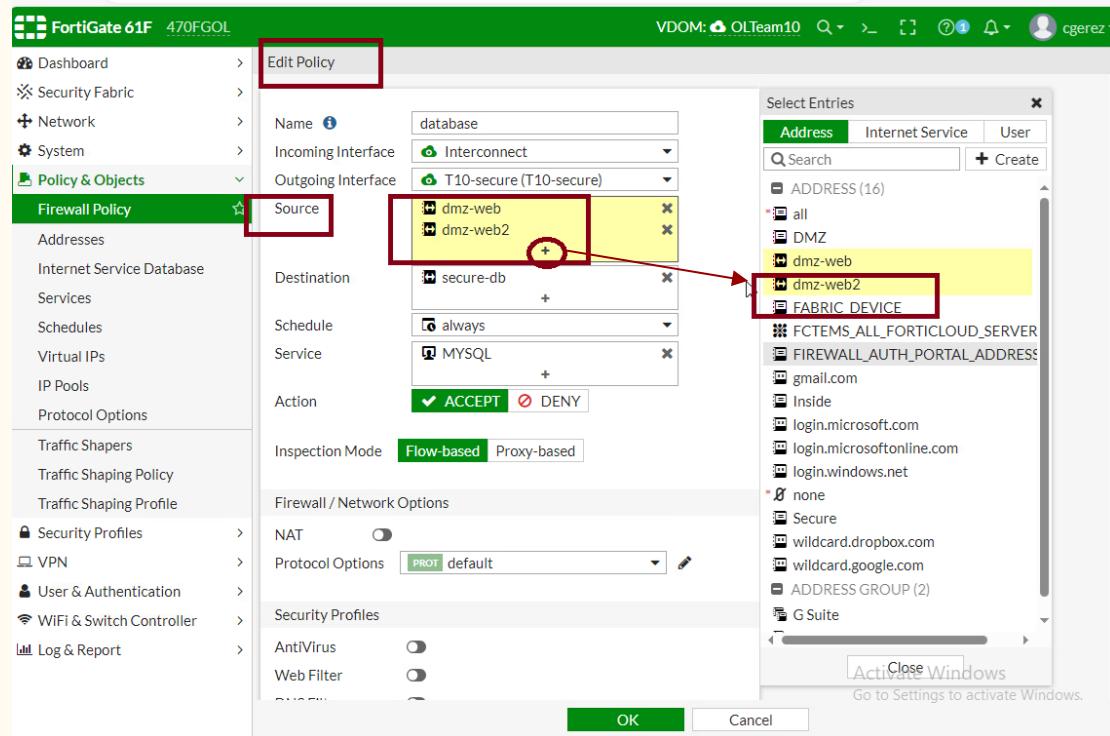
The screenshot shows the FortiGate 61F 470FGOL interface. The left sidebar menu is open, showing various system and policy-related options. The 'Firewall Policy' option is highlighted with a red box. In the main content area, a table lists firewall rules. One specific rule, 'database', is highlighted with a red box and has a cursor pointing at the 'Edit' button, which is also highlighted with a red box. The table columns include Name, Source, Destination, Schedule, Service, Action, NAT, and Security Profiles. The 'database' rule is defined with the following parameters:

Name	Source	Destination	Schedule	Action	NAT	Security Profiles
database	dmz-web	secure-db	always	MySQL	ACCEPT	Disabled, SSL no-inspect

Below the table, there are other sections like Outbound-all, Implicit, and Traffic Shapers. A message at the bottom right says 'Activate Windows Go to Settings to activate Windows.' The bottom navigation bar includes icons for Start, Search, Task View, File Explorer, Edge, and File History.

Configuring the app in the cloned machine.

A Edit Policy interface will be open and in the line of the Source select the + sign that opens another tab with a list. In that list select the new address (dmz-web2) that you created and finish with OK.



Configuring the app in the cloned machine.

This is how it should looks at the end. If the line still is colored , just reload the page with the option at the bottom of the screen, and it should look as in the picture.

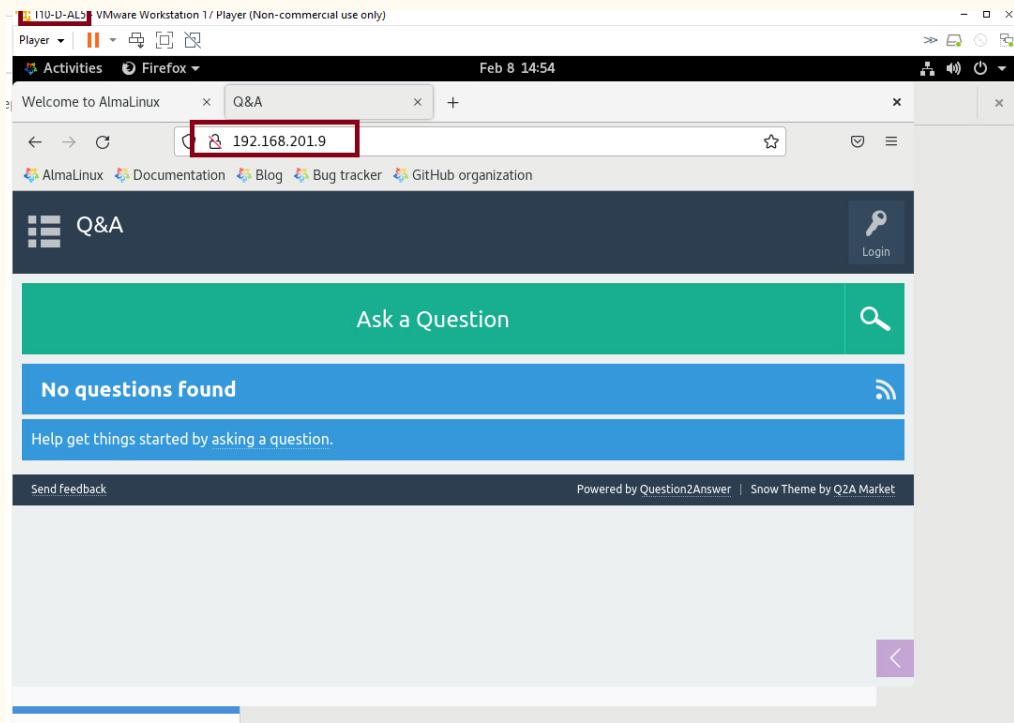
The screenshot shows the FortiGate 61F 470FGOL interface under the 'Policy & Objects' section, specifically the 'Firewall Policy' tab. The main table displays several policy entries:

Name	Source	Destination	Schedule	Action	NAT	Security Profile
Interconnect → T10-secure (T10-secure) ②	DMZ Inside	Secure	always	RDP SSH ACCEPT	✓ ACCEPT	Disabled SSL no-inspec
database	dmz-web dmz-web2	secure-db	always	MySQL ACCEPT	✓ ACCEPT	Disabled SSL no-inspec
T10-secure (T10-secure) → Interconnect ①	Secure	DMZ Inside	always	ALL ACCEPT	✓ ACCEPT	Disabled SSL no-inspec
Implicit ①	all	all	always	ALL DENY	✗ DENY	

A red box highlights the 'database' policy entry, which includes the 'MySQL' service and 'ACCEPT' action. A blue box highlights the 'Implicit' policy entry, which includes the 'DENY' action. The top navigation bar shows 'VDOM: OLTTeam10' and the user 'cgerez'. The left sidebar lists other policy objects like 'Addresses', 'Services', and 'Schedules'.

Configuring the app in the cloned machine.

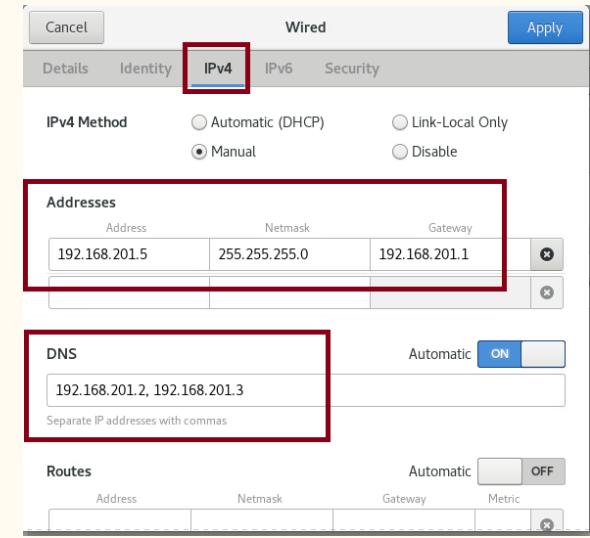
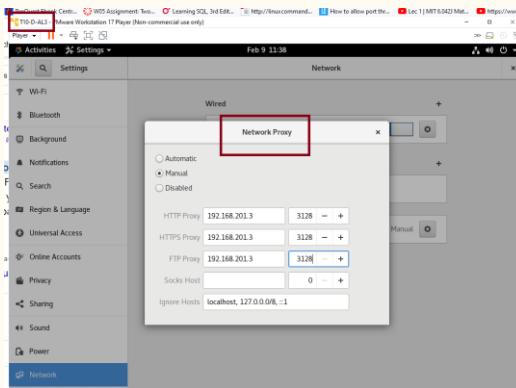
Now from any machine on the dmz zone you are able to start the app with the address of the new machine. Then, the app is working as it should from the DMZ zone now in the new cloned machine.



Configuring a load balancer in Alma Linux T10-D-AL3.

We have an extra machine created for testing purposes that is up and ready to install software, then we will use this machine. In case a new machine were necessary, refer to the first presentation on installing VM's.

Here you can see the machine settings for connectivity.



Configuring a load balancer in Alma Linux T10-D-AL3.

Since I already have internet connectivity, I first upgrade and update the system to start with the last version and patches.

we used:

```
sudo dnf upgrade almalinux-release
```

```
sudo dnf update
```

```
zlib-1.2.11-25.el8.x86_64
Installed:
  grub2-tools-efi-1:2.02-150.el8.alma.1.x86_64
  kernel-4.18.0-513.11.1.el8_9.x86_64
  kernel-core-4.18.0-513.11.1.el8_9.x86_64
  kernel-modules-4.18.0-513.11.1.el8_9.x86_64
  libvirt-client-8.0.0-22.module_el8.9.0+3714+46544554.x86_64
  libwpe-1.10.0-4.el8.x86_64
  podman-gvproxy-3:4.6.1-4.module_el8.9.0+3643+9234dc3b.x86_64
  podman-plugins-3:4.6.1-4.module_el8.9.0+3643+9234dc3b.x86_64
  python3-magic-5.33-25.el8.noarch
  wpebackend-fdo-1.10.0-3.el8.x86_64
```

```
Complete!
```

```
[cgerez@T10-D-AL3 ~]$ sudo dnf update
```

Configuring a load balancer in Alma Linux T10-D-AL3.

Here are the commands to find install and examine haproxy in alma linux.

`dnf search haproxy`

`sudo dnf -y install haproxy`

`rpm -ql haproxy`

```
cgerez@T10-D-AL3:~$ dnf search haproxy
Complete!
[cgerez@T10-D-AL3 ~]$ dnf search haproxy
AlmaLinux 8 - BaseOS          831 kB/s | 5.2 MB   00:06
AlmaLinux 8 - AppStream        6.0 MB/s | 12 MB    00:01
AlmaLinux 8 - Extras           65 kB/s | 20 kB   00:00
Extra Packages for Enterprise Linux 8 - x86_64  1.6 MB/s | 16 MB   00:10
=====
==== Name & Summary Matched: haproxy ====
haproxy.x86_64  HAProxy is a reverse proxy for high availability environments
pcp-pmda-haproxy.x86_64  Performance counter plugin (PCP) metrics for HAProxy
[cgerez@T10-D-AL3 ~]$ sudo dnf -y install haproxy
[sudo] password for cgerez:
Last metadata expiration check: 0:26:37 ago on Fri 09 Feb 2024 11:51:22 AM CST.
Dependencies resolved.
=====
Transaction Summary
=====
Installing:
haproxy           x86_64     1.8.27-5.el8      appstream    1.4 M
Transaction Summary
Install 1 Package
Total download size: 1.4 M
Installed size: 4.2 M
Downloading Packages:
haproxy-1.8.27-5.el8.x86_64.rpm          4.2 MB/s | 1.4 MB   00:00
```

```
cgerez@T10-D-AL3:~$ rpm -ql haproxy
[cgerez@T10-D-AL3 ~]$ rpm -ql haproxy
=====
Installed:
haproxy-1.8.27-5.el8.x86_64
=====
[cgerez@T10-D-AL3 ~]$ rpm -ql haproxy
/etc/haproxy
/etc/haproxy/conf.d
/etc/haproxy/proxy.cfg
/etc/haproxy/uhaproxy
/etc/sysconfig/haproxy
/usr/bin/HaLog
/usr/bin/IpRange
/usr/lib/build-id
/usr/lib/build-id/42
/usr/lib/build-id/62/a67b0fa2d0ed351c84ef425b1573e0a692c6a2
/usr/lib/build-id/69
/usr/lib/build-id/69/b38ffbb6cb4f1bebea22d76fe7857e3aa0d3e
/usr/lib/build-id/fd
/usr/lib/build-id/fd/c48075d72ad4837eba460e609ddc8cfcd23e
/usr/lib/system/haproxy.service
/usr/lib/systemd/system/haproxy.service
/usr/share/doc/haproxy
/usr/share/doc/haproxy/510degree-device-detection.txt
/usr/share/doc/haproxy/CHANGELOG
/usr/share/doc/haproxy/DeviceAtlas-device-detection.txt
/usr/share/doc/haproxy/README
/usr/share/doc/haproxy/ROADMAP
```

Configuring a load balancer in Alma Linux T10-D-AL3.

The configuration file `/etc/haproxy/haproxy.cfg` usually contains a demo config, which we won't use.

For best-practices sake, make a backup of the config:

```
cd /etc/haproxy
```

```
sudo cp haproxy.cfg haproxy.cfg.orig
```

```
/usr/share/licenses/haproxy
/usr/share/licenses/haproxy/LICENSE
/usr/share/man/man1/halog.1.gz
/usr/share/man/man1/haproxy.1.gz
/var/lib/haproxy
[cgerez@T10-D-AL3 ~]$ cd x/etc/haproxy
bash: cd: x/etc/haproxy: No such file or directory
[cgerez@T10-D-AL3 ~]$ cd /etc/haproxy
[cgerez@T10-D-AL3 haproxy]$ sudo cp haproxy.cfg haproxy.cfg.orig
[sudo] password for cgerez:
[cgerez@T10-D-AL3 haproxy]$
```

Configuring a load balancer in Alma Linux T10-D-AL3.

Edit the file with vi:

```
sudo vi haproxy.cfg
```

Find and delete all of the “frontend” and “backend” configuration stanzas, and replace them with a frontend and backend suitable to balance your original and cloned web servers.

```
frontend q2aWeb
    bind 192.168.201.5:80
    default_backend q2aBack
```

```
backend q2aBack
    balance roundrobin
    server T10-D-AL4 192.168.201.7:80 check
    server T10-D-AL5 192.168.201.9:80 check
```

This configures round robin in our balancer, haproxy will listen for connections in this system and forward them to each of the servers.

```
cgerez@T10-D-AL3:/etc/haproxy
File Edit View Search Terminal Help
timeout queue 1m
timeout connect 10s
timeout client 1m
timeout server 1m
timeout http-keep-alive 10s
timeout check 10s
maxconn 3000
#-
# main frontend which proxys to the backends
#-
frontend q2aWeb
    bind 192.168.201.5:80
    default_backend q2aBack
# static backend for serving up images, stylesheets and such
#-
#-
# round robin balancing between the various backends
#-
backend q2aBack
    balance roundrobin
    server T10-D-AL4 192.168.201.7:80 check
    server T10-D-AL5 192.168.201.9:80 check
:wq
```

Configuring a load balancer in Alma Linux T10-D-AL3.

As all new services starts being disabled and inactive, we use this commands to check and start the service:

```
systemctl status haproxy
```

```
sudo systemctl enable haproxy
```

```
sudo systemctl start haproxy
```

```
systemctl status haproxy
```

```
[cgerez@T10-D-AL3 haproxy]$ systemctl status haproxy
● haproxy.service - HAProxy Load Balancer
   Loaded: loaded (/usr/lib/systemd/system/haproxy.service; disabled; vendor preset: disabled)
   Active: inactive (dead)

[re] [cgerez@T10-D-AL3 haproxy]$ sudo systemctl enable haproxy
[sudo] password for cgerez:
Created symlink /etc/systemd/system/multi-user.target.wants/haproxy.service → /usr/lib/systemd/system/haproxy.service.

[cgerez@T10-D-AL3 haproxy]$ sudo systemctl start haproxy
[cgerez@T10-D-AL3 haproxy]$ systemctl status haproxy
● haproxy.service - HAProxy Load Balancer
   Loaded: loaded (/usr/lib/systemd/system/haproxy.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2024-02-09 12:58:58 CST; 5s ago
     Process: 373806 ExecStartPre=/usr/sbin/haproxy -f $CONFIG -f $CFGDIR -c -q $OPTIONS (c>
      Main PID: 373808 (haproxy)
        Tasks: 2 (limit: 23500)
       Memory: 2.4M
      CGroup: /system.slice/haproxy.service
              └─373808 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -f /etc/haproxy/co>
                  ├─373811 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -f /etc/haproxy/co>

Feb 09 12:58:58 T10-D-AL3.localdomain systemd[1]: Starting HAProxy Load Balancer...
Feb 09 12:58:58 T10-D-AL3.localdomain systemd[1]: Started HAProxy Load Balancer.
[cgerez@T10-D-AL3 haproxy]$
```

Configuring a load balancer in Alma Linux T10-D-AL3.

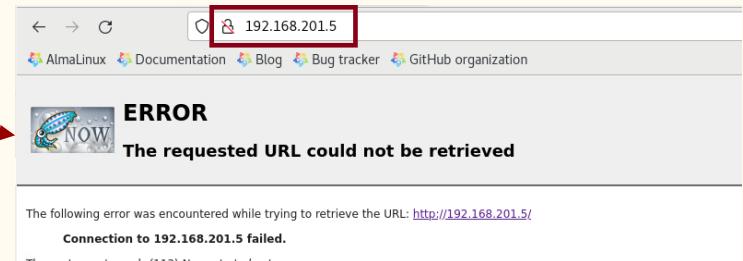
Is possible that you get this screen after all configurations are done. To solve this problem we have to configure the firewall in the balancer host machine to allow the http service with:

```
sudo firewall-cmd --add-service=http --permanent
```

```
sudo firewall-cmd --reload
```

```
Feb 09 13:48:27 T10-D-AL3.localdomain systemd[1]: Started HAProxy Load Balancer.
[cgerez@T10-D-AL3 haproxy]$ systemctl status ssh.service
Unit ssh.service could not be found.

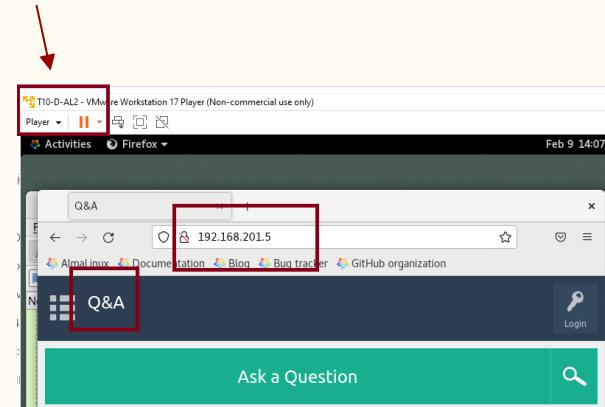
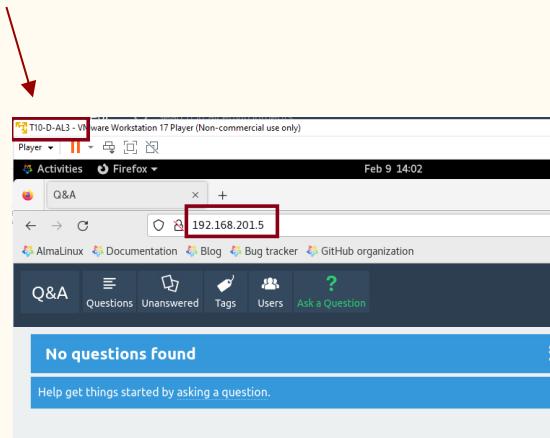
[cgerez@T10-D-AL3 haproxy]$ sudo firewall-cmd --add-service=http --permanent
[sudo] password for cgerez
success
[cgerez@T10-D-AL3 haproxy]$ sudo firewall-cmd --reload
success
[cgerez@T10-D-AL3 haproxy]$
```



Configuring a load balancer in Alma Linux T10-D-AL3.

Now we can access the app through the load balancer in the ip 192.168.201.5

Here you can see access from the load balancer host and from another endpoint in the dmz.



Test HAProxy, and verify that is balancing properly.

In the Palo Alto firewall we will adjust the rule to give clients in the internet to access the app. We are opening the balancer machine to untrust areas.

On NAT select the T10-web rule and change the source address to point to the load balancer hosting machine by selecting the address and change the address in the window that pop up. Remember to commit the changes.

NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	Original Packet			Translated Packet	
					SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTIN
T10-web	none	dmz	outside	etherenet1/3.610	192.168.201.7	any	any	static-ip 157.201.22.72 bi-directional: yes	none
T10-dynamic	none	dmz	outside	etherenet1/3.610	192.168.201.0/24	any	any	dynamic-ip-and-port etherenet1/3.610 157.201.22.72/29	none

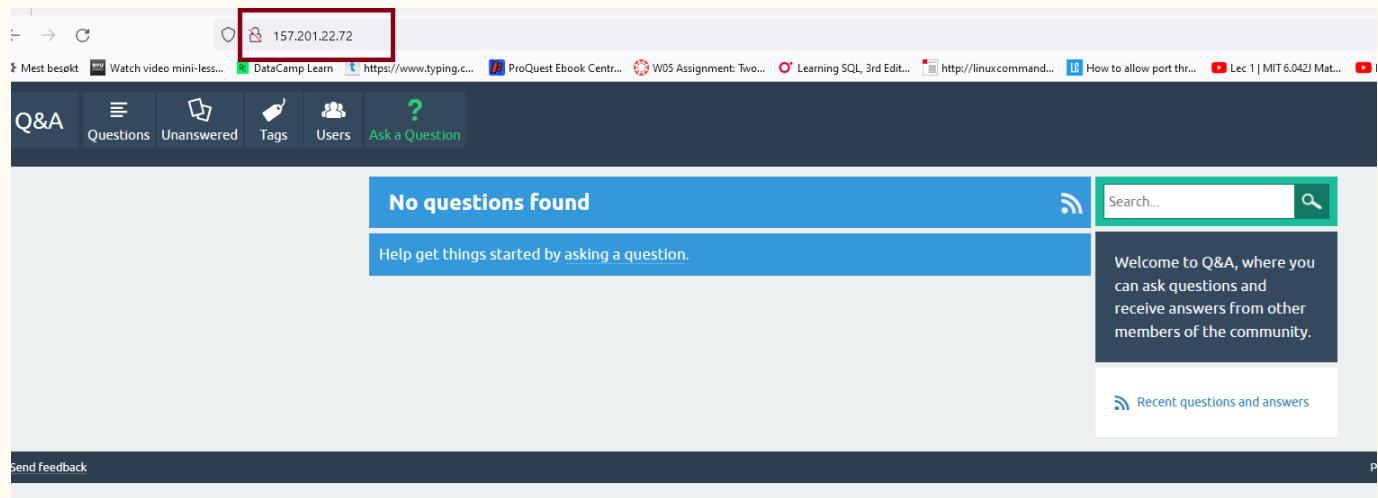
The screenshot shows the 'Source Address' configuration dialog for the T10-web rule. It lists several IP addresses, with the '192.168.201.7' entry highlighted. Below the list is a 'New Address' button, which is the key action to change the source address.

NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	Original Packet	Translated Packet			
T10-web	none	dmz	outside	etherenet1/3.610	192.168.201.7	any	any	static-ip 157.201.22.72 bi-directional: yes	none
T10-dynamic	none	dmz	outside	etherenet1/3.610	192.168.201.0/24	any	any	dynamic-ip-and-port etherenet1/3.610 157.201.22.72/29	none

Test HAProxy, and verify that is balancing properly.

Now the app is accessible from the internet through the load balancer that alternate the servers use.

Now we explore several ways to test that this is occurring.



Test HAProxy, and verify that is balancing properly.

First option is use rsyslog to collect logs of the service.

Check that rsyslog is working:

```
systemctl status rsyslog
```

Find his configuration file

```
rpm -ql rsyslog | less
```

Edit his configuration file with vi and uncomment this lines:

```
sudo vi /etc/rsyslog.conf
```

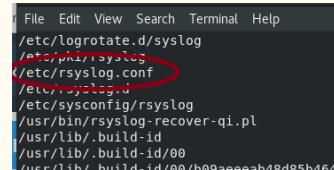
```
#module(load="imudp")  
  
#input(type="imudp" port="514")
```

Then restart the service and check on the logs.

```
sudo systemctl restart rsyslog
```

```
[cgerez@T10-D-AL3 haproxy]$ systemctl status rsyslog  
● rsyslog.service - System logging Service  
  Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)  
  Active: active (running) since Fri 2024-02-09 12:06:13 CST; 2h 27min ago  
    Docs: man:rsyslog(8)
```

```
[cgerez@T10-D-AL3 haproxy]$ rpm -ql rsyslog | less  
[cgerez@T10-D-AL3 haproxy]$ rpm -ql rsyslog | less  
[cgerez@T10-D-AL3 haproxy]$ rpm -ql rsyslog | less  
[cgerez@T10-D-AL3 haproxy]$
```



```
cgerez@T10-D-AL3:/etc/haproxy  
File Edit View Search Terminal Help  
  
# For more information see /usr/share/doc/rsyslog-/rsyslog.conf.html  
# or latest version online at http://www.rsyslog.com/doc/rsyslog.conf.  
# If you experience problems, see http://www.rsyslog.com/doc/troubleshooting.html  
  
### MODULES ###  
module(load="imusock")  
  Syslog.Use="off" # Turn off message reception from a local log  
  # local messages are retrieved through imjournal  
module(load="imjournal"  
      UsePID="system" # PID number is retrieved as the ID of the program  
      StateFile="imjournal.state") # File to store the position in the journal  
module(load="imklog") # read kernel messages (the same are read from imjournal)  
#module(load="immark") # provides access to the system journal  
  
# Provides UDP syslog reception  
# For parameters see http://www.rsyslog.com/doc/imudp.html  
module(load="imudp") # needs to be done just once  
  input(type="imudp" port="514")  
  
# Provides TCP syslog reception  
# For parameters see http://www.rsyslog.com/doc/intcp.html  
module(load="intcp") # needs to be done just once  
  input(type="intcp" port="514")  
  
```

```
[cgerez@T10-D-AL3 haproxy]$ rpm -ql rsyslog | less  
[cgerez@T10-D-AL3 haproxy]$ sudo vi /etc/rsyslog.conf  
[sudo] password for cgerez:  
[cgerez@T10-D-AL3 haproxy]$ sudo systemctl restart rsyslog  
[cgerez@T10-D-AL3 haproxy]$
```

Test HAProxy, and verify that is balancing properly.

With the previous configuration one can see the logs generated by the app with this command. The request take turns in each server. You can see machines al4 and al5 alternate.

`sudo tail /var/log/messages`

```
[cgerez@T10-D-AL3 haproxy]$ sudo tail /var/log/messages
Feb  9 14:53:50 localhost haproxy[374848]: 192.168.201.3:48138 [09/Feb/2024:14:53:50.526] q2aWeb q2aBack/t10-d-al5 0/0/0/1/1 30
"GET /qa-content/qa-global.js?1.8.8 HTTP/1.1"
Feb  9 14:53:50 localhost haproxy[374848]: 192.168.201.3:48136 [09/Feb/2024:14:53:50.528] q2aWeb q2aBack/t10-d-al4 0/0/1/0/1 30
"GET /qa-theme/SnowFlat/js/snow-core.js?1.8.8 HTTP/1.1"
Feb  9 14:53:51 localhost haproxy[374848]: 192.168.201.3:48136 [09/Feb/2024:14:53:51.703] q2aWeb q2aBack/t10-d-al5 0/0/0/33/33
"/0 "GET / HTTP/1.1"
Feb  9 14:53:51 localhost haproxy[374848]: 192.168.201.3:48144 [09/Feb/2024:14:53:51.773] q2aWeb q2aBack/t10-d-al5 0/0/0/0/0 30
"GET /qa-theme/SnowFlat/js/snow-core.js?1.8.8 HTTP/1.1"
Feb  9 14:53:51 localhost haproxy[374848]: 192.168.201.3:48136 [09/Feb/2024:14:53:51.772] q2aWeb q2aBack/t10-d-al4 0/0/1/1/2 30
"GET /qa-content/jquery-3.5.1.min.js HTTP/1.1"
Feb  9 14:53:51 localhost haproxy[374848]: 192.168.201.3:48138 [09/Feb/2024:14:53:51.772] q2aWeb q2aBack/t10-d-al4 0/0/1/0/2 30
"GET /qa-content/qa-global.js?1.8.8 HTTP/1.1"
Feb  9 14:53:52 localhost haproxy[374848]: 192.168.201.3:48136 [09/Feb/2024:14:53:52.766] q2aWeb q2aBack/t10-d-al5 0/0/0/39/39
"/0 "GET / HTTP/1.1"
Feb  9 14:53:52 localhost haproxy[374848]: 192.168.201.3:48138 [09/Feb/2024:14:53:52.828] q2aWeb q2aBack/t10-d-al5 0/0/1/0/1 30
"GET /qa-theme/SnowFlat/js/snow-core.js?1.8.8 HTTP/1.1"
Feb  9 14:53:52 localhost haproxy[374848]: 192.168.201.3:48136 [09/Feb/2024:14:53:52.828] q2aWeb q2aBack/t10-d-al4 0/0/0/1/1 30
```

Test HAProxy, and verify that is balancing properly.

As a good practice we will redirect the logs to a separate file. We edit again the configuration file:

```
sudo vi /etc/rsyslog.conf
```

Find this rule:

```
*.info;mail.none;authpriv.none;cron.none      /var/log/messages
```

And change it to:

```
*.info;mail.none;authpriv.none;cron.none;local2.none      /var/log/messages
```

And add a new rule that sends local2 facility to haproxy.log

```
local2.*      /var/log/haproxy.log
```

As before save and restart the service will apply the changes.

```
sudo systemctl restart rsyslog
```

```
#### RULES ####
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                     /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none;local2.none      /var/log/messages
local2.*   /var/log/haproxy.log
# The authpriv file has restricted access.
authpriv.*

# Log all the mail messages in one place.
mail.*                                       -/var/log/maillog

:wq
```

```
crond          gdm      MailLog-20240121      secure    20240121      systemd-tuned      wtmp      Xorg.9.log
crond@20240121 glusterfs maillog-20240128      secure    -20240121      tuned
[cgerez@T10-D-AL3 haproxy]$ sudo vi /etc/rsyslog.conf
[cgerez@T10-D-AL3 haproxy]$ sudo systemctl restart rsyslog
[cgerez@T10-D-AL3 haproxy]$ sudo tail /var/log/haproxy.log
tail: cannot open '/var/log/haproxy.log' for reading: No such file or directory
[cgerez@T10-D-AL3 haproxy]$ sudo tail /var/log/haproxy.log
Feb  9 15:25:58 localhost haproxy[374848]: 88.90.190.47:64576 [09/Feb/2024:15:25:55.471] q2aWeb q2aBack/t10-d-al4 0 0/0, 0 "GET / HTTP/1.1"
Feb  9 15:25:58 localhost haproxy[374848]: 88.90.190.47:64576 [09/Feb/2024:15:25:58.756] q2aWeb q2aBack/t10-d-al5 0 0/0, 0 "GET / HTTP/1.1"
Feb  9 15:26:00 localhost haproxy[374848]: 88.90.190.47:64576 [09/Feb/2024:15:26:00.278] q2aWeb q2aBack/t10-d-al4 0 0/0, 0 "GET / HTTP/1.1"
Feb  9 15:26:02 localhost haproxy[374848]: 88.90.190.47:64576 [09/Feb/2024:15:26:02.523] q2aWeb q2aBack/t10-d-al5 0 0/0, 0 "GET / HTTP/1.1"
Feb  9 15:26:17 localhost haproxy[374848]: 192.168.201.3:48230 [09/Feb/2024:15:26:17.766] q2aWeb q2aBack/t10-d-al4 0 0/0, 0 "GET / HTTP/1.1"
[cgerez@T10-D-AL3 haproxy]$
```

Test HAProxy, and verify that is balancing properly.

There are 2 optional ways to check the alternate of the servers on this task. Today I will leave here. If you feel to continue are welcome. Look at the end of the class tutorial where stay optional.

(Optional) Syslogs and event logs are reliable tools for troubleshooting server software, but sometimes it just feels more satisfying to see load balancing evidence in the web browser client. Here's one way to do this:

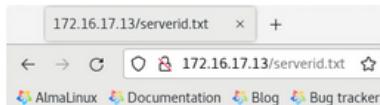
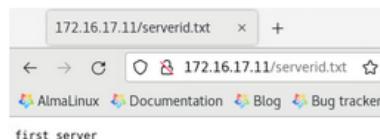
On the first web server, create a "static page" file that contains some identifying content. Example:

```
echo "first server" | tee -a /var/www/html/serverid.txt
```

On the second web server, create the same file, but put different content in that file:

```
echo "second server" | tee -a /var/www/html/serverid.txt
```

Launch a browser on a DMZ VM, and verify the contents each identifier file on its respective host:



Challenges we faced

If mariadb is not running use the following commands.

Use the command sudo systemctl status mariadb to look if is enable and had start. If not use the same command changing to enable and start, to start the service.

```
cgarcia@localhost:~
```

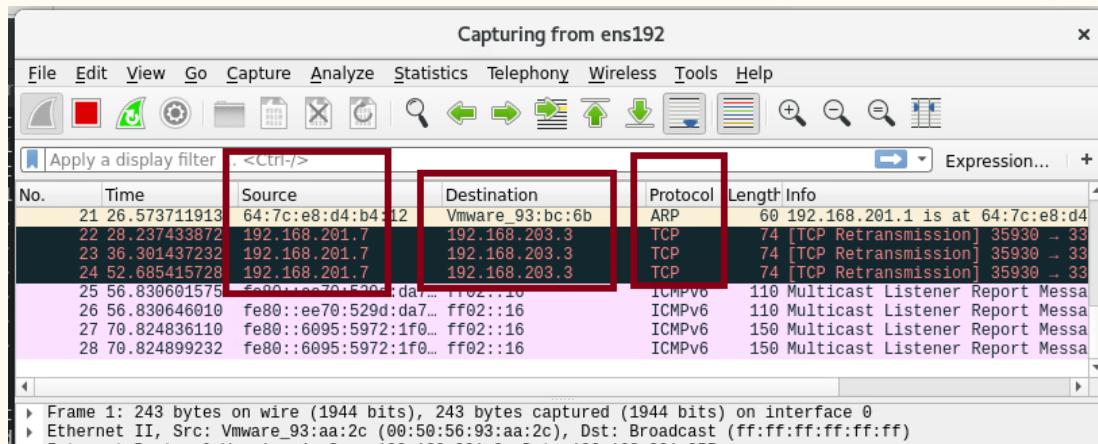
```
File Edit View Search Terminal Help
perl-DBD-MySQL-4.046-3.module_el8.6.0+2827+49d66dc3.x86_64

Complete!
[cgarcia@localhost ~]$ sudo systemctl status mariadb
● mariadb.service - MariaDB 10.3 database server
  Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; vendor preset: disabled)
  Active: inactive (dead)
    Docs: man:mysqld(8)
          https://mariadb.com/kb/en/library/systemd/
[cgarcia@localhost ~]$ sudo systemctl enable mariadb
Created symlink /etc/systemd/system/mysql.service → /usr/lib/systemd/system/mariadb.service.
Created symlink /etc/systemd/system/mysqld.service → /usr/lib/systemd/system/mariadb.service.
Created symlink /etc/systemd/system/multi-user.target.wants/mariadb.service → /usr/lib/systemd/system/mariadb.service.
[cgarcia@localhost ~]$ sudo systemctl start mariadb
[cgarcia@localhost ~]$ sudo systemctl status mariadb
● mariadb.service - MariaDB 10.3 database server
  Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: disabled)
  Active: active (running) since Sat 2024-02-03 03:45:25 CST; 9s ago
    Docs: man:mysqld(8)
          https://mariadb.com/kb/en/library/systemd/
Process: 61000 ExecStartPost=/usr/libexec/mysql-check-upgrade (code=exited, status=0/SUCCESS)
Process: 60866 ExecStartPre=/usr/libexec/mysql-prepare-db-dir mariadb.service (code=exited, status=0/SUCCESS)
Process: 60841 ExecStartPre=/usr/libexec/mysql-check-socket (code=exited, status=0/SUCCESS)
Main PID: 60969 (mysqld)
  Status: "Taking your SQL requests now..."
    Tasks: 30 (limit: 23499)
   Memory: 83.5M
      CPU: 0.000 CPU(s)
     CGroup: /system.slice/mariadb.service
             └─60969 /usr/libexec/mysqld --basedir=/usr

Feb 03 03:45:21 localhost.localdomain systemd[1]: Starting MariaDB 10.3 database server...
Feb 03 03:45:21 localhost.localdomain mysql-prepare-db-dir[60866]: Initializing MariaDB database
Feb 03 03:45:25 localhost.localdomain systemd[1]: Started MariaDB 10.3 database server.
```

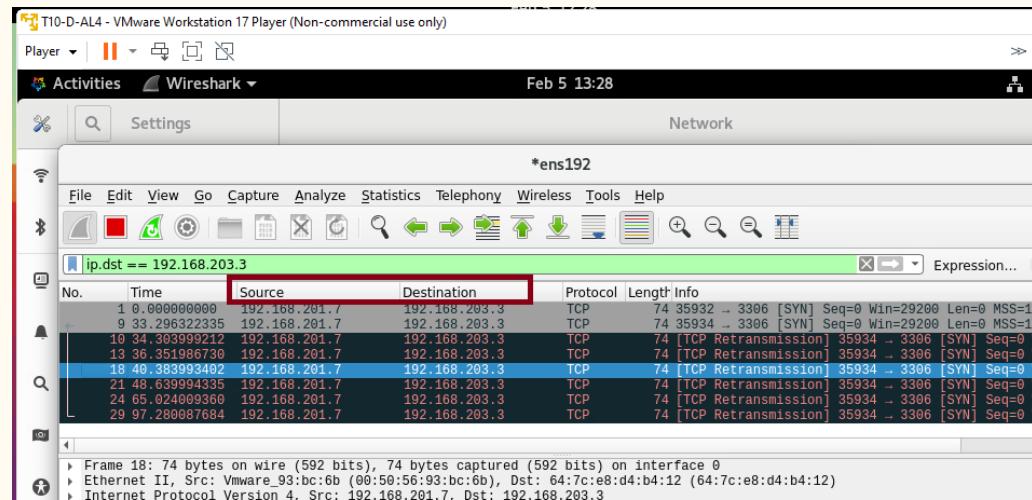
We experienced connections problems from the DMZ with the database in the secure zone.

We used wireshark to test why we didn't have app connections between the DMZ and the secure zone. The firewall was already configured with a policy to allow mysql.



Connections problems from the DMZ zone.

Filtering our capture from Wireshark on the apache DMZ machine we saw that the packages were send but somehow not receiving responses. Black color is an indicator of something not working in the connections.



In the Palo Alto firewall the packages were dropped, and not allowed.

Checking in the Palo Alto monitor tab and filtering between the 2 address that we were interested in, we find some dropped packages when trying the connections.

Then we review the policy and found that was disabled.

After enable and commit it start to work again. See next slide.

The screenshot shows the Palo Alto PA-440 Firewall's monitor interface. The top navigation bar includes tabs for DASHBOARD, ACC, MONITOR (which is selected), POLICIES, OBJECTS, NETWORK, and DEVICE. A search bar at the top right contains the query "(addr.src in 192.168.201.7) and (addr.dst in 192.168.203.3)". Below the search bar is a toolbar with icons for Commit, Undo, Redo, and Help. The main area is titled "Logs" and "Traffic". On the left, a sidebar lists various monitoring categories: Threat, URL Filtering, WildFire Submissions, Data Filtering, HIP Match, GlobalProtect, IP-Tag, User-ID, Decryption, Tunnel Inspection, Configuration, System, and The main table displays a list of dropped packages. The columns are: RECEIVE TIME, TYPE, FROM ZONE, TO ZONE, SOURCE, SOURCE USER, DYNAMIC ADDRESS GROUP, DESTINATION, DYNAMIC ADDRESS GROUP, DYNAMIC USER GROUP, TO PORT, APPLICATION, and ACTION. The first four rows of the table are highlighted with a red box, showing entries for receive times from 02/05 12:20:07 to 02/05 12:20:02, type drop, source 192.168.201.7, destination 192.168.203.3, and action deny. The remaining rows show similar patterns for receive times from 02/05 12:19:32 to 02/05 12:19:02.

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DYNAMIC ADDRESS GROUP	DESTINATION	DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION
02/05 12:20:07	drop	dmz	interconn...	192.168.201.7			192.168.203.3			3306	not-applicable	deny
02/05 12:20:07	drop	dmz	interconn...	192.168.201.7			192.168.203.3			3306	not-applicable	deny
02/05 12:20:02	drop	dmz	interconn...	192.168.201.7			192.168.203.3			3306	not-applicable	deny
02/05 12:19:32	drop	dmz	interconn...	192.168.201.7			192.168.203.3			3306	not-applicable	deny
02/05 12:19:12	drop	dmz	interconn...	192.168.201.7			192.168.203.3			3306	not-applicable	deny
02/05 12:19:07	drop	dmz	interconn...	192.168.201.7			192.168.203.3			3306	not-applicable	deny
02/05 12:19:02	drop	dmz	interconn...	192.168.201.7			192.168.203.3			3306	not-applicable	deny
02/05 12:19:02	drop	dmz	interconn...	192.168.201.7			192.168.203.3			3306	not-applicable	deny

The allow policy to mysql from DMZ to secure working.

Is always good to know where to find the tabs to enable or disable a policy to troubleshoot, and remember to commit changes. Here in policies tab and after highlight the rule that is grey (disabled), we use the bottom line tab enable to get it to the right blue color again. But remember that not change is done before we committed.

The screenshot shows the Palo Alto Networks PA-440 interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES (selected), OBJECTS, NETWORK, and DEVICE. On the left, a sidebar lists security features like NAT, QoS, Policy Based Forwarding, and Tunnel Inspection. The main area displays a table of rules under the 'Security' tab. Rule 9, titled 'T10-database-mysql', is highlighted with a red box and is currently disabled (grey). At the bottom of the table, there is a row of buttons for actions: Add, Delete, Clone, Override, Review, Enable (which is also highlighted with a red box), and Disable. The status bar at the bottom indicates the current session information: 'pa10.1.47.10:443', 'User: [redacted]', 'Login Time: 02/05/2024 12:44:44', and 'Session Expire Time: 03/06/2024 1:14:30'.

NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	Rule Usage		
															HIT COUNT	LAST HIT	FIRST HIT
1 rule1	none	universal	dmz trust	any	any	any	dmz untrust	any	any	any	any	Allow	none	0	-	-	
2 T10-outbound	none	universal	dmz	192.168.201.0/24	any	any	outside	any	any	any	any	Allow	none	152917	2024-02-05 13:14:41	2024-01-20 23:32:17	
3 T10-dmz-to-inside-remote-access	none	universal	dmz	192.168.201.0/24	any	any	inside	192.168.202.0/24	any	ms-rdp	application-...	Allow	none	62	2024-01-27 05:46:41	2024-01-22 12:12:08	
4 T10-inside-to-dmz-all	none	universal	inside	192.168.202.0/24	any	any	dmz	192.168.201.0/24	any	any	any	Allow	none	102	2024-01-27 13:29:54	2024-01-22 11:49:52	
5 T10-secure-to-dmz-inside	none	universal	interconnect	192.168.203.0/24	any	any	dmz	192.168.201.0/24	any	any	any	Allow	none	15103	2024-02-05 12:54:43	2024-01-24 11:54:48	
6 T10-squid-proxy	none	universal	interconnect	192.168.203.0/24	any	any	dmz	192.168.201.0/24	any	any	any	Allow	none	1914	2024-02-05 12:54:43	2024-02-02 17:12:50	
7 T10-to-Secure-Remote-Admin	none	universal	dmz	192.168.201.0/24	any	any	interconnect	192.168.203.0/24	any	ms-rdp	application-...	Allow	none	105	2024-01-27 14:27:10	2024-01-24 12:07:45	
8 T10-web	none	universal	outside	any	any	any	dmz	157.201.22.72	any	web-browsing	application-...	Allow	none	1031	2024-02-05 12:53:10	2024-02-02 17:13:44	
9 T10-database-mysql	none	universal	dmz	192.168.201.7	any	any	interconnect	192.168.203.3	any	mysql	application-...	Allow	none	5	2024-02-05 12:44:36	2024-02-02 23:35:43	
10 intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	any	any	Allow	none	10414	2024-02-05 13:10:08	2024-01-20 23:31:59	
11 intrazone-default	none	intrazone	any	any	any	any	any	any	any	any	any	Deny	none	1953	2024-02-05 13:07:39	2024-01-22 10:37:08	

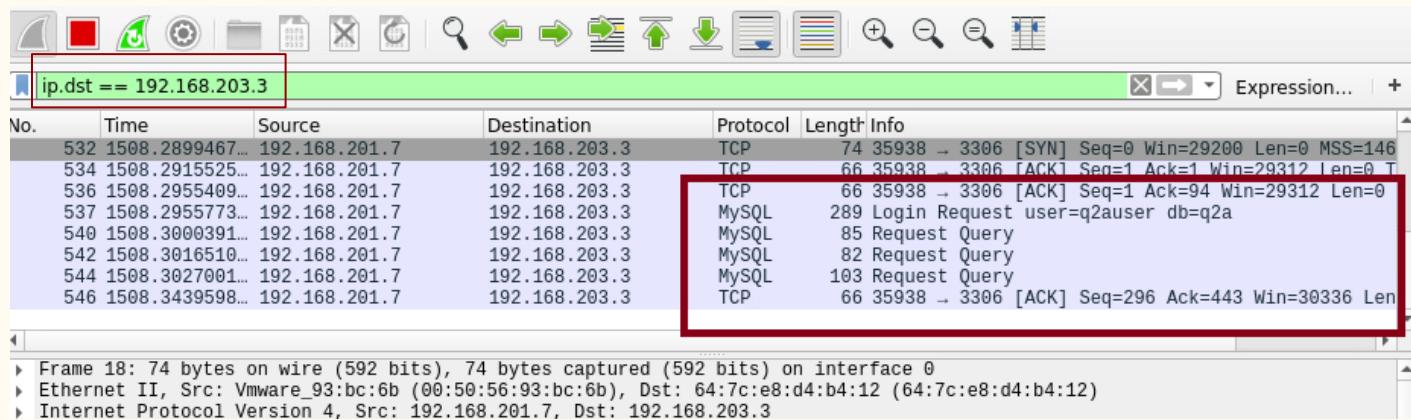
Results before and after the policy was enabled.

The packages now flow through the firewall as we can see in the monitor of the firewall.

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES	HTTP/2 CONNECTION SESSION ID
02/05 12:44:37	start	dmz	interconn...	192.168.201.7			192.168.203.3			3306	mysql	allow	T10-database-maria	n/a	389	0
02/05 12:43:02	drop	dmz	interconn...	192.168.201.7			192.168.203.3			3306	not-applicable	deny	interzone-default	policy-denied	0	0
02/05 12:42:52	drop	dmz	interconn...	192.168.201.7			192.168.203.3			3306	not-applicable	deny	interzone-default	policy-denied	0	0
02/05 12:42:47	drop	dmz	interconn...	192.168.201.7			192.168.203.3			3306	not-applicable	deny	interzone-default	policy-denied	0	0
02/05 12:42:47	drop	dmz	interconn...	192.168.201.7			192.168.203.3			3306	not-applicable	deny	interzone-default	policy-denied	0	0
02/05 12:42:47	drop	dmz	interconn...	192.168.201.7			192.168.203.3			3306	not-applicable	deny	interzone-default	policy-denied	0	0

After enable the firewall policy that allow transmission.
Connections were established.

This is a
screenshot of
wireshark
monitor that
shows the
reconnected
status. Is filtered
by the
destination
address
192.168.203.3



ip.dst == 192.168.203.3

No.	Time	Source	Destination	Protocol	Length	Info
532	1508.2899467...	192.168.201.7	192.168.203.3	TCP	74	35938 → 3306 [SYN] Seq=0 Win=29200 Len=0 MSS=146
534	1508.2915525...	192.168.201.7	192.168.203.3	TCP	66	35938 → 3306 [ACK] Seq=1 Ack=1 Win=29312 Len=0 T
536	1508.2955409...	192.168.201.7	192.168.203.3	TCP	66	35938 → 3306 [ACK] Seq=1 Ack=94 Win=29312 Len=0
537	1508.2955773...	192.168.201.7	192.168.203.3	MySQL	289	Login Request user=q2auser db=q2a
540	1508.3000391...	192.168.201.7	192.168.203.3	MySQL	85	Request Query
542	1508.3016510...	192.168.201.7	192.168.203.3	MySQL	82	Request Query
544	1508.3027001...	192.168.201.7	192.168.203.3	MySQL	103	Request Query
546	1508.3439598...	192.168.201.7	192.168.203.3	TCP	66	35938 → 3306 [ACK] Seq=296 Ack=443 Win=30336 Len

Frame 18: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: Vmware_93:bc:6b (00:50:56:93:bc:6b), Dst: 64:7c:e8:d4:b4:12 (64:7c:e8:d4:b4:12)
Internet Protocol Version 4, Src: 192.168.201.7, Dst: 192.168.203.3