

Tiered app

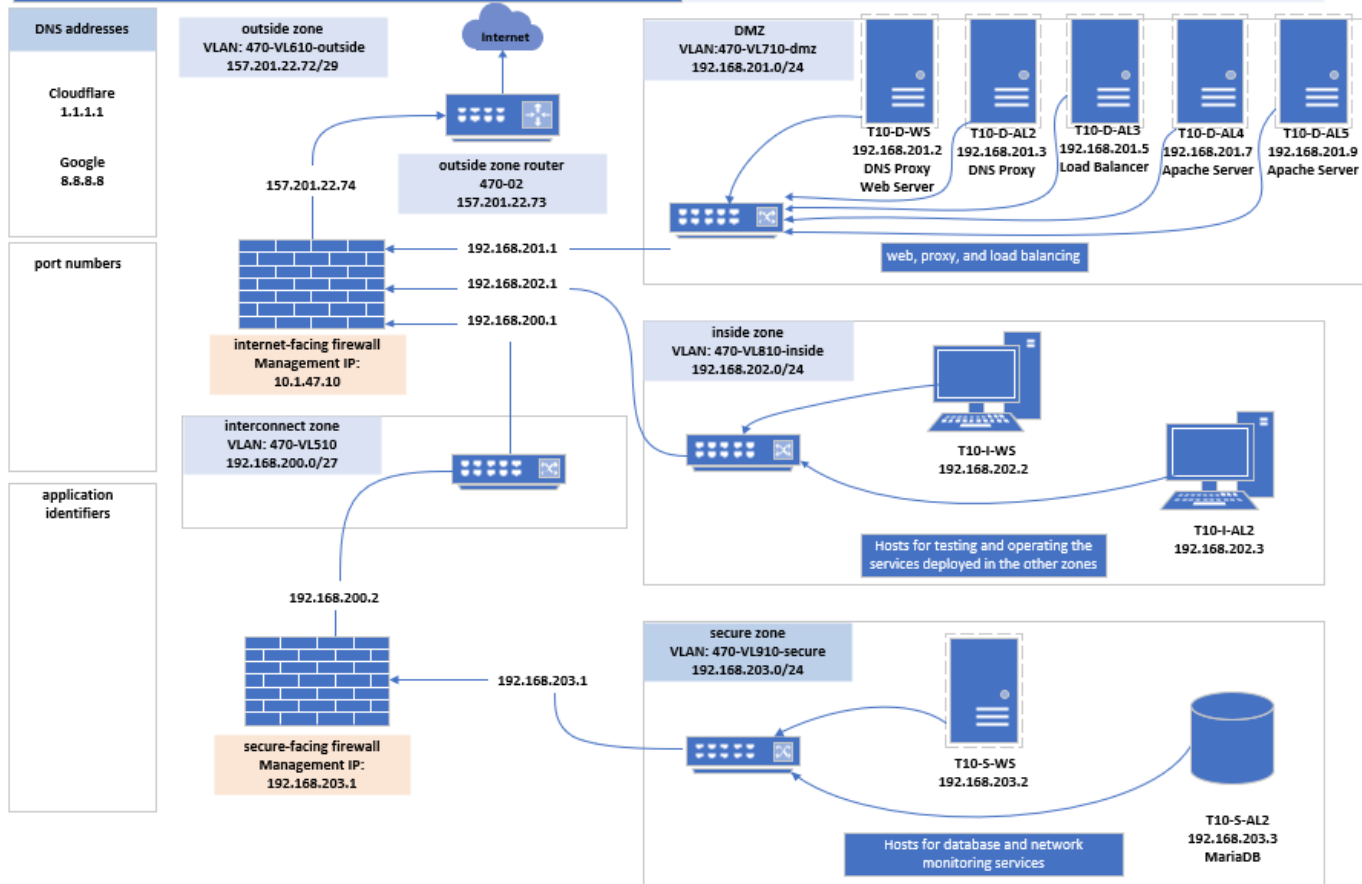
By Carlos Gerez, Christopher Ditto , and Mark Riley Slik

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 470t10ra.cit.byui.edu	157.201.22.75- 157.201.22.78	157.201.22.79

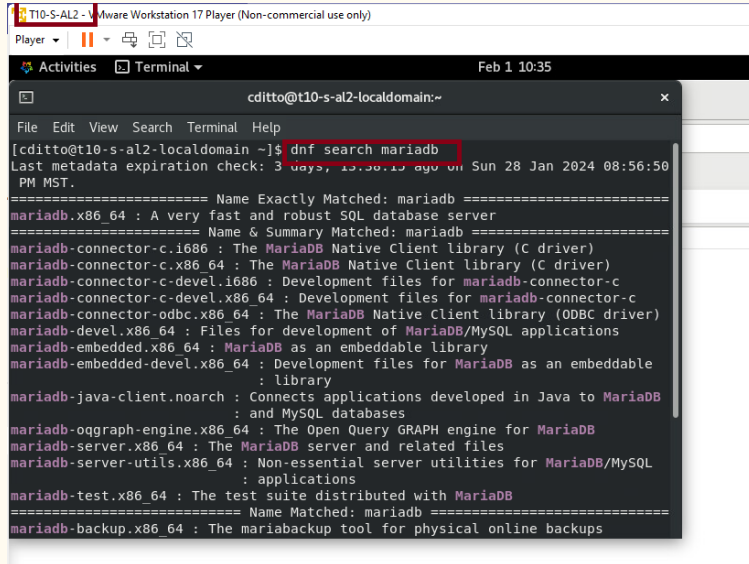


Mariadb installation

—

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 Feb 1 10:35
cditto@t10-s-at2-localdomain:~
File Edit View Search Terminal Help
[cditto@t10-s-at2-localdomain ~]$ dnf search mariadb
Last metadata expiration check: 3 days, 15:50:15 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-oggraph-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-oggraph-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.

```
mysql-server-galera-01 : the configuration files and scripts for galera
                        : replication
===== Summary Matched: mariadb =====
mysql-selinux.noarch : SELinux policy modules for MySQL and MariaDB packages
[cditto@t10-s-al2-localdomain ~] $ dnf info mariadb-server
AlmaLinux 8 - BaseOS           0.0 kB/s | 3.8 kB      00:00
AlmaLinux 8 - BaseOS           4.4 MB/s | 5.2 MB      00:01
AlmaLinux 8 - AppStream        16 kB/s | 4.1 kB      00:00
AlmaLinux 8 - AppStream        6.3 MB/s | 12 MB       00:01
AlmaLinux 8 - Extras           14 kB/s | 3.8 kB      00:00
AlmaLinux 8 - Extras           76 kB/s | 20 kB       00:00
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 LGPLv2 and BSD
Description: MariaDB is a multi-user, multi-threaded SQL database server. It
            is a client/server implementation consisting of a server daemon
            (mysqld) 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-localdomain ~]$
```

```
dnf info mariadb
```

```
sudo dnf -y install mariadb-server
```

```
[cgarcia@t10-s-al2-localdomain ~] $ 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`

```

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

(3/6): mariadb-server-utils-10.3.39-1.module_el8.8.0+3609+ 1.1 MB 00:00
(4/6): perl-DBD-MySQL-4.046-3.module_el8.8.0+2827+49 155 kB 00:00
(5/6): mariadb-backup-10.3.39-1.module_el8.8.0+3609+ 6.1 MB 00:00
(6/6): mariadb-server-10.3.39-1.module_el8.8.0+3609+ 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 :
Installing : perl-DBD-MySQL-4.046-3.module_el8.8.0+2827+49d66dc3.x86_64 1/1
Installing : mariadb-errmsg-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64 2/6
Installing : mariadb-gssapi-server-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64 3/6
Installing : mariadb-server-utils-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64 4/6
Running scriptlet: mariadb-server-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64 5/6
Installing : mariadb-server-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64 5/6
Running scriptlet: mariadb-server-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64 5/6
Installing : mariadb-backup-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64 6/6
Running scriptlet: mariadb-backup-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64 6/6
Verifying : mariadb-backup-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64 1/6
Verifying : mariadb-errmsg-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64 2/6
Verifying : mariadb-gssapi-server-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64 3/6
Verifying : mariadb-server-utils-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64 4/6
Verifying : mariadb-server-3:10.3.39-1.module_el8.8.0+3609+204d4ab0.x86_64 5/6
Verifying : perl-DBD-MySQL-4.046-3.module_el8.8.0+2827+49d66dc3.x86_64 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_el8.8.0+2827+49d66dc3.x86_64

Complete!
[cgarcia@t10-s-al2-localdomain ~]$

```

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

```
/user/bin/mysql_secure_installation
```

```

[comptel@t0-s-a2-localdomain ~]$ rpm -q mariadb-server
/etc/logrotate.d/mariadb
/etc/my.cnf.d/enabled-encryption.pretest
/etc/my.cnf.d/mariadb-server.cnf
/etc/security/user_map.conf
/run/mariadb
/usr/bin/arila chk
/usr/bin/arila dump log
/usr/bin/arila ftdump
/usr/bin/arila pack
/usr/bin/arila read log
/usr/bin/timocheksum
/usr/bin/mariadb-service-convert
/usr/bin/mysql_print_defaults
/usr/bin/mysqld_ftdump
/usr/bin/mysiamchk
/usr/bin/mysiamlog
/usr/bin/mysiamsecure
/usr/bin/mysiamsql_installation
/usr/bin/mysiamsql_safe
/usr/bin/mysiamsql safe helper
/usr/bin/replace
/usr/bin/resolve_stack_dump
/usr/bin/resolvcpid
/usr/bin/wrep sst backup
/usr/bin/wrep sst common
/usr/bin/wrep sst mariabackup
/usr/bin/wrep sst mariadump
/usr/bin/wrep sst rsync
/usr/bin/wrep sst rsync tunnel
/usr/bin/wrep sst rsync wan
usr/lib/.build-id
usr/lib/.build-id/04
usr/lib/.build-id/04/3751b2c138e8b5883819cd5474891808b
usr/lib/.build-id/05
usr/lib/.build-id/05/f61d238e13d633ab5f6ee29dc5f690bf4ce
usr/lib/.build-id/09/4bc5f7b430e7e167ecf61b127b97da630fa
usr/lib/.build-id/14/d837f7385154abb820672f0d8c54516f2a
usr/lib/.build-id/14/84737b30e7e167ecf61b127b97da630fa
File Edit View Search Terminal Help
usr/lib/.build-id/cc
usr/lib/.build-id/cc/53749440148119c9d35fe3d446069f542e12
usr/lib/.build-id/e3
usr/lib/.build-id/e3/dedddfefeb4dcacba1ae791923e255281c2d0
usr/lib/.build-id/e6
usr/lib/.build-id/e6/9c4095792f37ee3c1308ce0e5c99501d07fc
usr/lib/.build-id/e6
usr/lib/.build-id/e6/326399cb8ba70f93aa199fbcf5d197315b246
usr/lib/.build-id/e6
usr/lib/.build-id/e6/68851ba839272b780ff420868dd6df2b3921a
usr/lib/.build-id/e6
usr/lib/.build-id/e6/d168712780ff4f28706b6188d5cb54463615
usr/lib/.build-id/e6
usr/lib/.build-id/e6/4a1fc63598d3198492efa4f152b35c2e581f1
usr/lib/.build-id/fd1
usr/lib/.build-id/fd1/27268457aba2e58349405821d5ee93e1f6
usr/lib/.build-id/fd6
usr/lib/.build-id/fd6/cace0b96a17557252a2a25121db06ba01b52
usr/lib/.build-id/fd6
usr/lib/.build-id/fd6/c43288840809975342f067f54cc17af4d5
usr/lib/.build-id/fd9
usr/sbin/.x86_64/xz/xzmodem.cxx.exe.repro.rux4.194b200994f32be2
usr/lib/systemd/system/mariadb.service
usr/lib/systemd/system/mariadb@boottrap.service
usr/lib/systemd/system/mariadb@boottrap.service.d/use_galera_new_cluster.conf
usr/lib/sysusers.d/mariadb.conf
usr/lib/tmpfiles.d/mariadb.conf
usr/lib64/mariadb
usr/lib64/mariadb/INFO BIN
usr/lib64/mariadb/INFO SRC
usr/lib64/mariadb/plugin
usr/lib64/mariadb/plugin/auth_null.so
usr/lib64/mariadb/plugin/auth_e08100.so
usr/lib64/mariadb/plugin/auth_ed25519.so
usr/lib64/mariadb/plugin/auth_pam.so
usr/lib64/mariadb/plugin/auth_socket.so
usr/lib64/mariadb/plugin/auth_test_plugin.so
usr/lib64/mariadb/plugin/demon_example.ini
usr/lib64/mariadb/plugin/debug_key_management.so
usr/lib64/mariadb/plugin/dialog_examples.so
usr/lib64/mariadb/plugin/disks.so
usr/lib64/mariadb/plugin/example_key_management.so
usr/lib64/mariadb/plugin/file_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-localdomain ~]$ systemctl status mariadb
● mariadb.service - MariaDB 10.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; vendor preset: en
   Active: inactive (dead)
     Docs: man:mysqld(8)
           https://mariadb.com/kb/en/library/systemd/
[cgarcia@t10-s-al2-localdomain ~]$ 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-localdomain ~]$ systemctl start mariadb
Failed to start mariadb.service: Access denied
See system logs and 'systemctl status mariadb.service' for details.
[cgarcia@t10-s-al2-localdomain ~]$ sudo systemctl start mariadb
[cgarcia@t10-s-al2-localdomain ~]$ systemctl status mariadb
● mariadb.service - MariaDB 10.3 Database Server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: en
   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-localdomain systemd[1]: Starting MariaDB 10.3 database serv
Feb 01 11:10:34 t10-s-al2-localdomain mysql-prepare-db-dir[134926]: Initializing Mari
Feb 01 11:10:37 t10-s-al2-localdomain systemd[1]: Started MariaDB 10.3 database serv
lines 1-18/18 (END)
```

```
[cgarcia@t10-s-al2-localdomain ~]$
[cgarcia@t10-s-al2-localdomain ~]$ systemctl status mariadb
● mariadb.service - MariaDB 10.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; vendor preset: en
   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-localdomain systemd[1]: Starting MariaDB 10.3 database server: mysqld.
Feb 01 11:10:34 t10-s-al2-localdomain mysql-prepare-db-dir[134926]: Initializing MariaDB
Feb 01 11:10:37 t10-s-al2-localdomain systemd[1]: Started MariaDB 10.3 database server: mysqld.
[cgarcia@t10-s-al2-localdomain ~]$ 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-a12-localdomain ~]$
```

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;
```

```
Thanks for using MariaDB!  
[cgarcia@tl0-s-al2-localdomain ~]: 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;
```

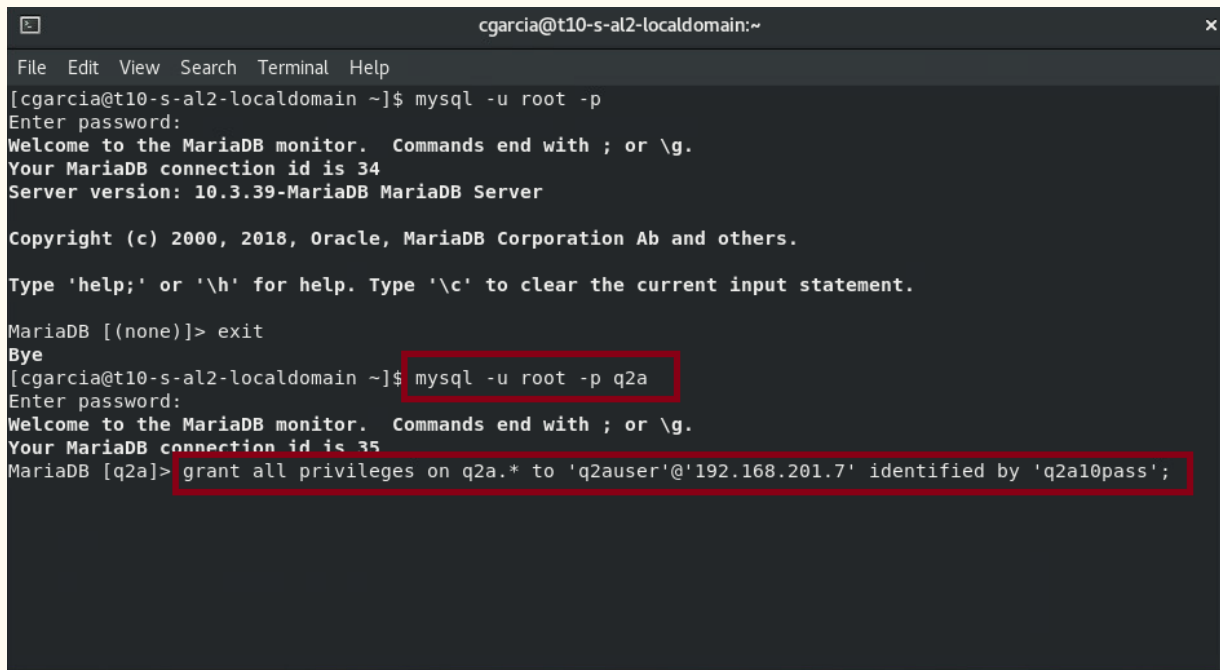
```
MariaDB [(none)]> create database q2a;  
MariaDB [(none)]> grant all privileges on q2a.* to 'q2auser'@'localhost' identified by 'q2a10pass'  
-> ;  
Query OK, 0 rows affected (0.001 sec)  
  
MariaDB [(none)]> grant all privileges on q2a.* to 'q2auser'@'192.168.201.2' identified by 'q2a10pass'  
-> ;  
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-al2-localdomain | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |  
| root | 127.0.0.1 | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |  
| root | ::1 | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |  
| q2auser | localhost | *30A7D7C55498E4F3D2A7F3B54080E19709BCC50B |  
| q2auser | 192.168.201.2 | *30A7D7C55498E4F3D2A7F3B54080E19709BCC50B |  
+-----+-----+-----+  
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';
```

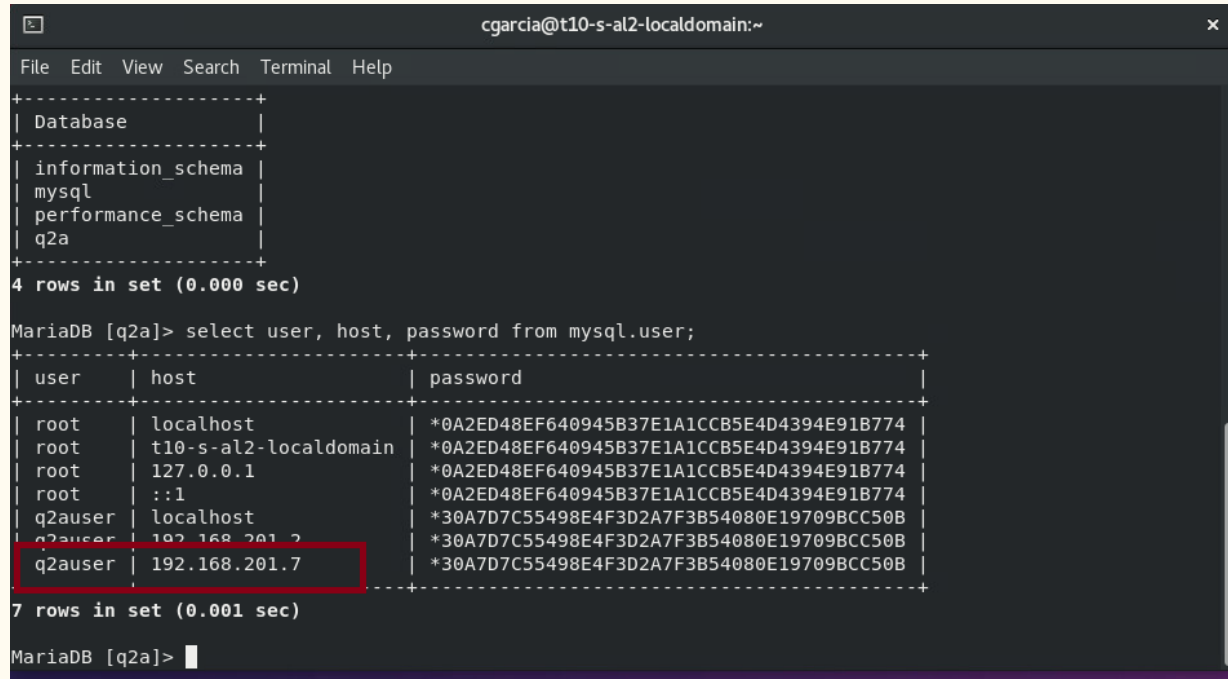
This shows how to create new users and
Add privileges to connect from other
machines.

A terminal window titled 'cgarcia@t10-s-al2-localdomain:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows a sequence of commands and outputs. First, '[cgarcia@t10-s-al2-localdomain ~]\$ mysql -u root -p' is entered, followed by 'Enter password:', 'Welcome to the MariaDB monitor. Commands end with ; or \g.', 'Your MariaDB connection id is 34', and 'Server version: 10.3.39-MariaDB MariaDB Server'. Then, 'Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.' and 'Type \'help;\' or \'h\' for help. Type \'c\' to clear the current input statement.' are displayed. The user enters 'MariaDB [(none)]> exit', and the prompt changes to 'Bye'. Finally, '[cgarcia@t10-s-al2-localdomain ~]\$ mysql -u root -p q2a' is entered, followed by 'Enter password:', 'Welcome to the MariaDB monitor. Commands end with ; or \g.', 'Your MariaDB connection id is 35', and the command 'MariaDB [q2a]> grant all privileges on q2a.* to \'q2auser\'@\'192.168.201.7\' identified by \'q2a10pass\';' is entered. The last command and its preceding prompt are highlighted with a red box.

```
cgarcia@t10-s-al2-localdomain:~  
File Edit View Search Terminal Help  
[cgarcia@t10-s-al2-localdomain ~]$ 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-localdomain ~]$ 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 new user created previously shows in the database.

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

A terminal window titled 'cgarcia@t10-s-al2-localdomain:~' with a menu bar (File, Edit, View, Search, Terminal, Help). It shows the output of a MySQL query. The first part shows a list of databases: information_schema, mysql, performance_schema, and q2a. The second part shows the results of 'select user, host, password from mysql.user;', which lists 7 rows. The last row, for 'q2auser' at host '192.168.201.7', is highlighted with a red rectangle.

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

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

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

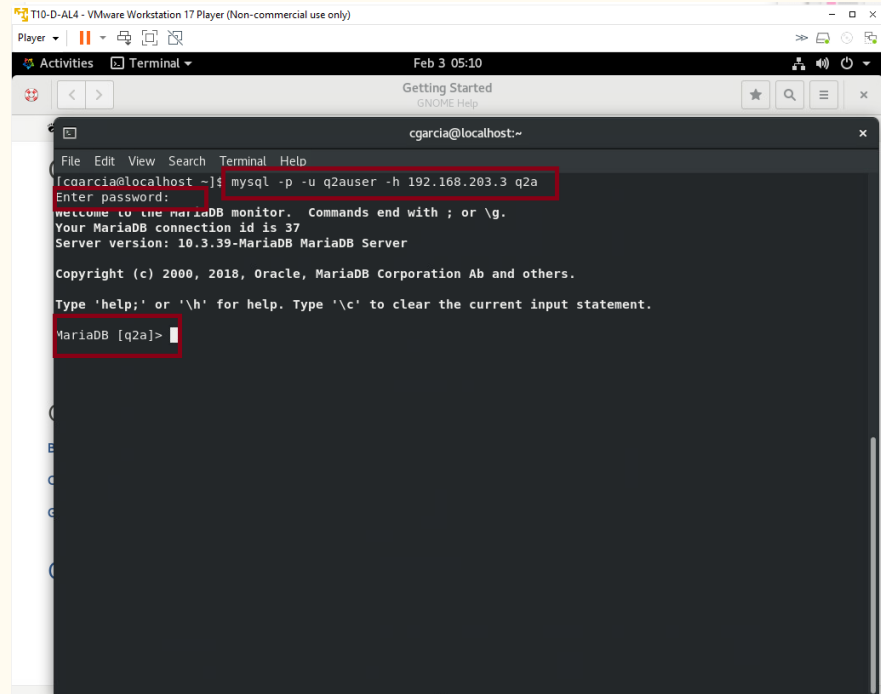
Description:

-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 terminal window titled 'T10-D-AL4 - VMware Workstation 17 Player (Non-commercial use only)'. The terminal output shows the command `mysql -p -u q2auser -h 192.168.203.3 q2a` being executed. The prompt 'Enter password:' is shown, followed by the message 'welcome to the MariaDB monitor. Commands end with ; or \g. Your MariaDB connection id is 37. Server version: 10.3.39-MariaDB MariaDB Server'. The prompt 'MariaDB [q2a]>' is shown at the bottom.

```
T10-D-AL4 - VMware Workstation 17 Player (Non-commercial use only)
Feb 3 05:10
Getting Started
GNOME Help
cgarcia@localhost:~
File Edit View Search Terminal Help
cgarcia@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 37
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]>
```

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

```
cditto@localhost ~]$ cd /etc/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 ~]$ 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 preset: enabled)
   Active: active (running) since Fri 2024-02-02 12:53:29 MST; 5min ago
     Docs: man:httpd.service(8)
  Main PID: 42400 (httpd)
    Status: "Running, listening on: 192.168.201.7 port 80"
    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 Server: httpd.
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 Server: httpd.
Feb 02 12:53:29 localhost.localdomain httpd[42400]: Server configured, listenin
```


Install Apache Server

Enable service
to start at
startup.

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

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

```
[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](https://www.almaLinux.org).

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`.



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
```

```
Installed:
```

```
php-mysqlnd-7.2.24-1.module_el8.3.0+2010+7c76a223.x86_64  
php-pdo-7.2.24-1.module_el8.3.0+2010+7c76a223.x86_64
```

```
Complete!
```

```
[cditto@localhost ~]$
```

Test the PHP Installation

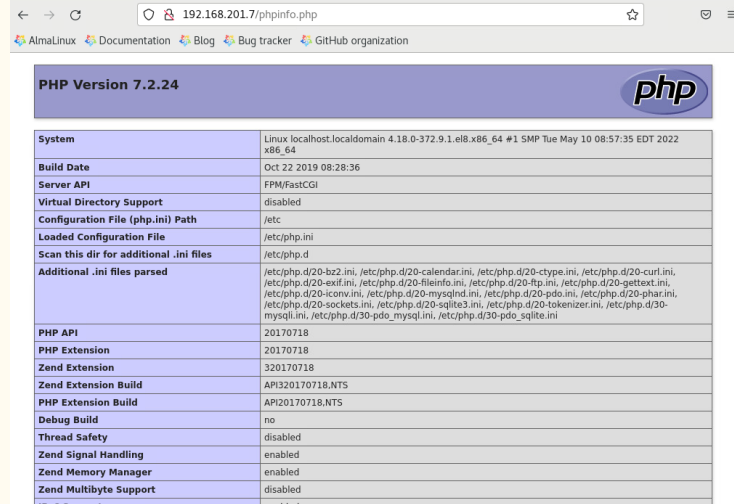
Create a PHP file in the Apache documentroot folder /var/www/html

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

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

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



PHP Version 7.2.24	
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
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bc2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysqli.ini, /etc/php.d/30-pdo_sqlite.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718.NTS
PHP Extension Build	API20170718.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled

Configure Policies on Internet Facing Firewalls

Configure
Static
NAT.

Under the
“Policies”
tab, select
“NAT” and
then select
“ADD”

The screenshot displays the Palo Alto Networks Security configuration interface. On the left, the 'Security' tab is selected, and the 'NAT' policy is highlighted in the left-hand menu. A red arrow points to the 'NAT' option. Below the menu, the 'Policy Optimizer' section shows 'Rule Usage' with 'Unused in 30 days', 'Unused in 90 days', and 'Unused' counts, all set to 0.

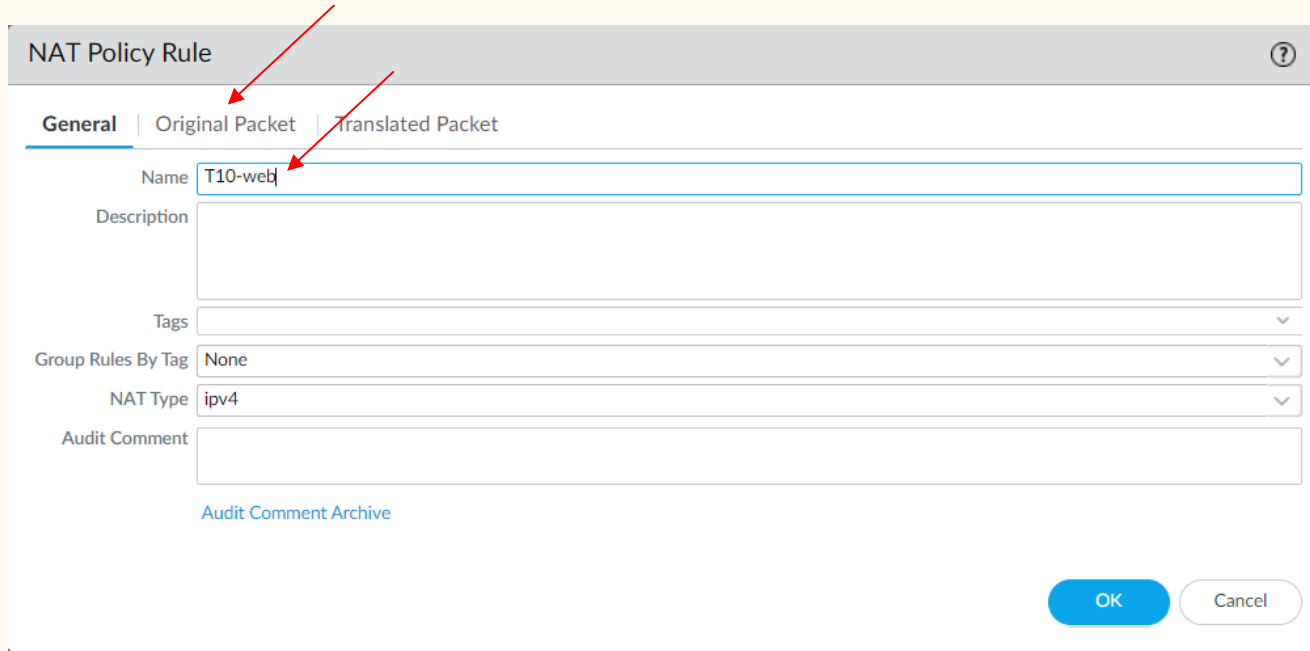
The main configuration area shows a table with one NAT policy, 'T10-dynamic'. A red arrow points to the 'Add' button at the bottom of the table.

NAME	TAGS	Original Packet							Translated Packet		HIT CO
		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	64949	

At the bottom of the interface, the 'Object : Addresses' section is visible, and the 'Add' button is highlighted with a red arrow.

Configure Policies on Internet Facing Firewalls

Add a name to
your NAT
policy.



The screenshot shows a configuration window titled "NAT Policy Rule" with a help icon in the top right corner. Below the title bar are three tabs: "General", "Original Packet", and "Translated Packet". The "General" tab is currently selected. The form contains the following fields:

- Name:** A text input field containing "T10-web". A red arrow points to this field from the text "Add a name to your NAT policy."
- Description:** A large empty text area.
- Tags:** A dropdown menu.
- Group Rules By Tag:** A dropdown menu with "None" selected.
- NAT Type:** A dropdown menu with "ipv4" selected.
- Audit Comment:** A large empty text area.

Below the "Audit Comment" field is a link labeled "Audit Comment Archive". At the bottom right of the window are two buttons: "OK" (blue) and "Cancel" (grey).

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.

The screenshot shows the "NAT Policy Rule" configuration window with the "Original Packet" tab selected. Red arrows point to the following elements:

- The "Original Packet" tab.
- The "SOURCE ZONE" dropdown menu, with the "dmz" option selected.
- The "Destination Zone" dropdown menu, with the "outside" option selected.
- The "Destination Interface" dropdown menu, with the "ethernet1/3.610" option selected.
- The "SOURCE ADDRESS" dropdown menu, with the "192.168.201.7" option selected.

The configuration details are as follows:

General	Original Packet	Translated Packet
Source Zone		
<input type="checkbox"/> Any		
<input checked="" type="checkbox"/> SOURCE ZONE ^		
<input checked="" type="checkbox"/> dmz		
Destination Zone		
<input type="checkbox"/> Any		
<input type="checkbox"/> SOURCE ADDRESS ^		
<input checked="" type="checkbox"/> 192.168.201.7		
Destination Interface		
<input type="checkbox"/> Any		
<input checked="" type="checkbox"/> DESTINATION ADDRESS ^		
<input type="checkbox"/> SOURCE ADDRESS ^		
<input checked="" type="checkbox"/> 192.168.201.7		
Service		
<input type="checkbox"/> Any		
<input checked="" type="checkbox"/> DESTINATION ADDRESS ^		
<input type="checkbox"/> SOURCE ADDRESS ^		
<input checked="" type="checkbox"/> 192.168.201.7		

Buttons: + Add - Delete

Buttons: OK Cancel

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”

The screenshot shows the "NAT Policy Rule" configuration window. The "Translated Packet" tab is selected. Under "Source Address Translation", the "Translation Type" is set to "Static IP" and the "Translated Address" is "157.201.22.72". The "Bi-directional" checkbox is checked. The "Destination Address Translation" section shows "Translation Type" set to "None". The "OK" button is highlighted in blue.

NAT Policy Rule			
General	Original Packet	Translated Packet	
Source Address Translation		Destination Address Translation	
Translation Type	Static IP	Translation Type	None
Translated Address	157.201.22.72		
<input checked="" type="checkbox"/> Bi-directional			
		OK Cancel	

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

Move Top

Move Up

Move Down

Move Bottom

Configure Policies on Internet Facing Firewalls

Configure a web-server security policy.

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

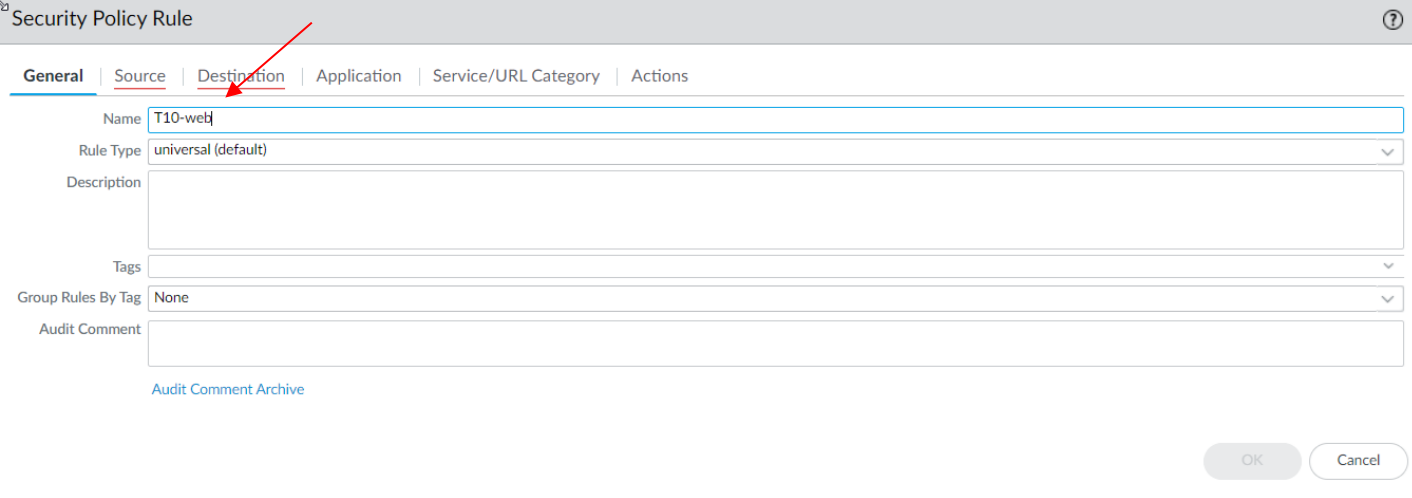
The screenshot displays the Palo Alto Networks firewall configuration interface. On the left sidebar, the 'Security' menu item is highlighted with a red arrow. Below it, the 'Policy Optimizer' section is visible. The main area shows a table of security rules. A red arrow points to the 'Add' button at the bottom of the table.

	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	Allow
2	T10-outbound	none	universal	dmz	192.168.201.0...	any	any	outside	any	any	any	application...	Allow
3	T10-dmz-to-inside-r...	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	ssh	application...	Allow
5	T10-secure-to-dmz-i...	none	universal	interconnect	192.168.203.0...	any	any	dmz	192.168.201.0...	any	any	application...	Allow
6	T10-squid-proxy	none	universal	interconnect	192.168.203.0...	any	any	dmz	192.168.201.0...	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	Allow
9	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny

Object : Addresses + Add Delete Clone Override Revert 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

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



The screenshot shows the 'Security Policy Rule' configuration window. The 'General' tab is selected, and a red arrow points to the 'Name' field, which contains the text 'T10-web'. Other fields include 'Rule Type' set to 'universal (default)', 'Description', 'Tags', 'Group Rules By Tag' set to 'None', and 'Audit Comment'. At the bottom right are 'OK' and 'Cancel' buttons. A link for 'Audit Comment Archive' is located below the 'Audit Comment' field.

Security Policy Rule	
General	Source
Destination	Application
Service/URL Category	Actions
Name	T10-web
Rule Type	universal (default)
Description	
Tags	
Group Rules By Tag	None
Audit Comment	
Audit Comment Archive	
OK Cancel	

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 screenshot shows the 'Security Policy Rule' configuration window with the 'Source' tab selected. The 'General' tab is also visible. The 'Source' tab has two sections: 'SOURCE ZONE' and 'SOURCE ADDRESS'. In the 'SOURCE ZONE' section, the 'Any' checkbox is unchecked, and the 'outside' zone is selected with a checkmark. In the 'SOURCE ADDRESS' section, the 'Any' checkbox is checked. At the bottom of the 'SOURCE ZONE' section, there are '+ Add' and '- Delete' buttons. A red arrow points to the '+ Add' button. At the bottom of the 'SOURCE ADDRESS' section, there are '+ Add' and '- Delete' buttons, and a 'Negate' checkbox is unchecked.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Destination' tab selected. The 'General' tab is also visible. The 'Destination' tab has two sections: 'DESTINATION ZONE' and 'DESTINATION ADDRESS'. In the 'DESTINATION ZONE' section, the 'select' dropdown is open, and the 'dmz' zone is selected with a checkmark. In the 'DESTINATION ADDRESS' section, the 'Any' checkbox is unchecked, and the IP address '157-201.22.72' is selected with a checkmark. At the bottom of the 'DESTINATION ZONE' section, there are '+ Add' and '- Delete' buttons. A red arrow points to the '+ Add' button. At the bottom of the 'DESTINATION ADDRESS' section, there are '+ Add' and '- Delete' buttons, and a 'Negate' checkbox is unchecked.

Configure Policies on Internet Facing Firewalls

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

Select the “Actions” tab
Commit your changes.

The image displays two screenshots of a network security configuration interface, specifically the 'Security Policy Rule' configuration page. Red arrows indicate the steps described in the text.

Top Screenshot (Application Tab):

- The 'Application' tab is selected.
- The 'Any' checkbox is unchecked.
- The 'APPLICATIONS' checkbox is checked.
- The 'web-browsing' application is selected (checked).

Bottom Screenshot (Actions Tab):

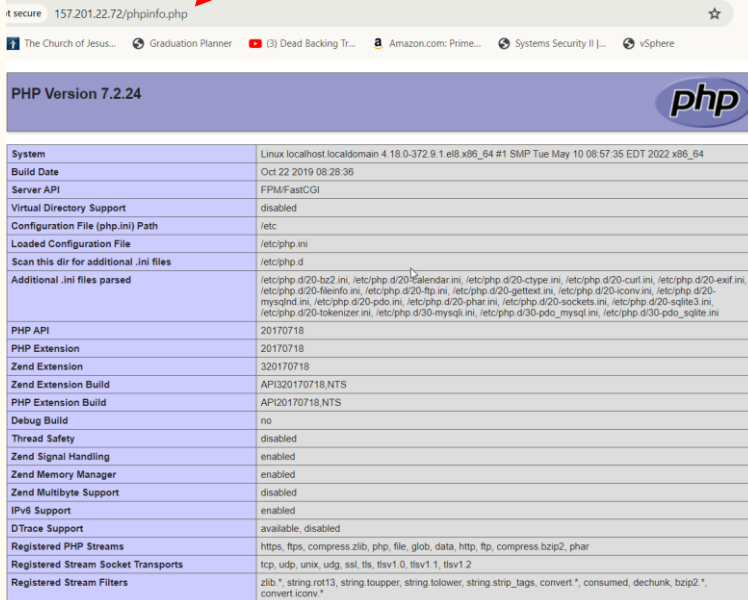
- The 'Actions' tab is selected.
- The 'Action' is set to 'Allow'.
- The 'Log at Session Start' checkbox is checked.
- The 'Log at Session End' checkbox is checked.
- The 'Log Forwarding' is set to 'None'.
- The 'Profile Type' is set to 'None'.
- The 'Schedule' is set to 'None'.
- The 'QoS Marking' is set to 'None'.
- The 'Disable Server Response Inspection' checkbox is unchecked.
- The 'OK' button is highlighted.

Configure Policies on Internet Facing Firewalls

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

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

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



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
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-mysqli.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/30-mysql.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718.NTS
PHP Extension Build	API20170718.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib *, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, bzip2 *, convert.iconv *

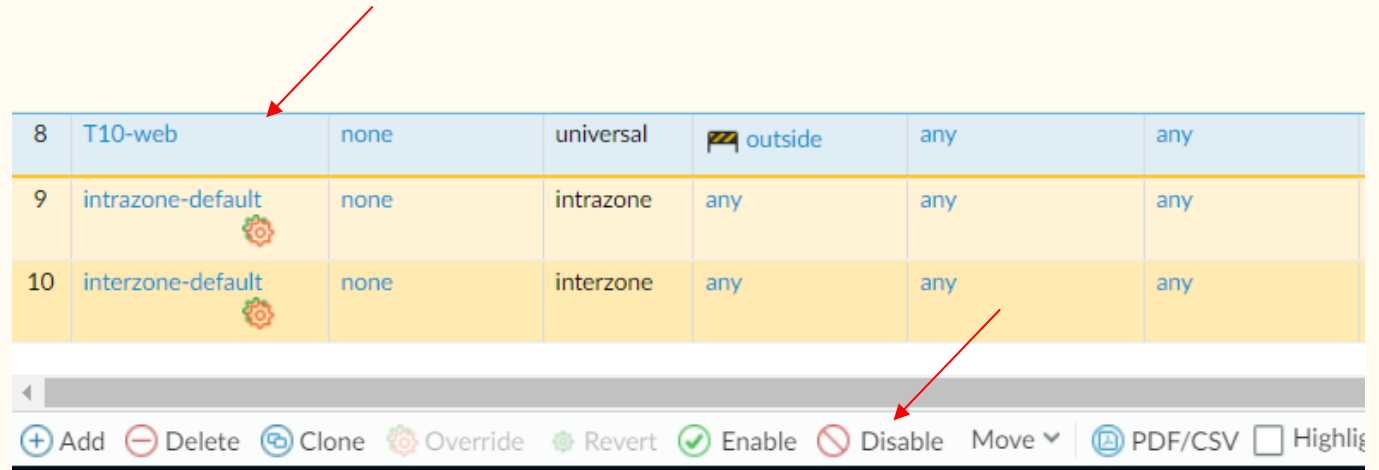
You should see the same info page that you saw at the in of the PHP test section of this instruction sequence.

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

◀

⊕ 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 MariahDB.

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

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

Create a rule on the Palo Alto 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

The screenshot shows the Palo Alto Networks Security Rules configuration interface. The 'Security' tab is selected, and a list of rules is displayed. A red arrow points to the 'Add' button at the bottom left of the interface.

	NAME	TAGS	TYPE	ZONE	ADDRESS	USER
1	rule1	none	universal	trust	any	any
2	T10-outbound	none	universal	dmz	192.168.201.0...	any
3	T10-dmz-to-inside-r...	none	universal	dmz	192.168.202.0...	any
4	T10-inside-to-dmz-all	none	universal	inside	192.168.202.0...	any
5	T10-secure-to-dmz-i...	none	universal	interconnect	192.168.203.0...	any
6	T10-squid-proxy	none	universal	interconnect	192.168.203.0...	any
7	T10-to-Secure-Remo...	none	universal	dmz	192.168.201.0...	any
8	T10-web	none	universal	outside	any	any
9	intrazone-default	none	intrazone	any	any	any
10	interzone-default	none	interzone	any	any	any

Object : Addresses + Add Delete Clone Override Revert Enable Disable Move PDF/CSV

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"/> SOURCE ZONE ^	<input type="checkbox"/> Any			
<input checked="" type="checkbox"/> dmz		<input checked="" type="checkbox"/> 192.168.201.2			
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>		<input type="button" value="+ Add"/> <input type="button" value="- 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.

The screenshot shows the 'Security Policy Rule' configuration window. The 'Destination' tab is selected, indicated by a red arrow. The interface is divided into two main sections: 'DESTINATION ZONE' and 'DESTINATION ADDRESS'. In the 'DESTINATION ZONE' section, a dropdown menu is set to 'select', and a table lists 'interconnect' as the selected zone, with a red arrow pointing to it. In the 'DESTINATION ADDRESS' section, a table lists '192.168.201.2' as the selected address, with a red arrow pointing to it. Both sections have an 'Add' button (indicated by red arrows) and a 'Delete' button. A 'Negate' checkbox is located at the bottom right of the 'DESTINATION ADDRESS' section.

General	Source	Destination	Application	Service/URL Category	Actions
select					
<input type="checkbox"/> DESTINATION ZONE ^					
<input checked="" type="checkbox"/> interconnect					
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>					

<input type="checkbox"/> Any
<input type="checkbox"/> DESTINATION ADDRESS ^
<input checked="" type="checkbox"/> 192.168.201.2
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>
<input type="checkbox"/> Negate

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” box.

Click OK and Commit your changes.

The image displays two screenshots of the Security Policy Rule configuration interface, illustrating the steps to configure an application rule.

Left Screenshot (Application Tab):

- Security Policy Rule** (Title)
- Tabs:** General, Source, Destination, **Application** (selected), Service/URL Category.
- Applications:** A list of applications is shown. The **mysql** application is selected (checked).
- Buttons:** + Add, - Delete.

Right Screenshot (Actions Tab):

- Security Policy Rule** (Title)
- Tabs:** General, Source, Destination, Application, Service/URL Category, **Actions** (selected).
- Action Setting:**
 - Action:** Allow (selected)
 - ☐ Send ICMP Unreachable
- Profile Setting:**
 - Profile Type:** None (selected)
- Log Setting:**
 - ☒ Log at Session Start
 - ☒ Log at Session End
 - Log Forwarding:** None
- Other Settings:**
 - Schedule:** None
 - QoS Marking:** None
 - ☐ Disable Server Response

9	T10-database	none	universal	dmz	192.168.201.2	any	any	interconnect	192.168.201.2	any	mysql	application-...	Allow
---	--------------	------	-----------	-----	---------------	-----	-----	--------------	---------------	-----	-------	-----------------	-------

Q2A Secure-Facing Firewall Configuration

Login to FortiGate.

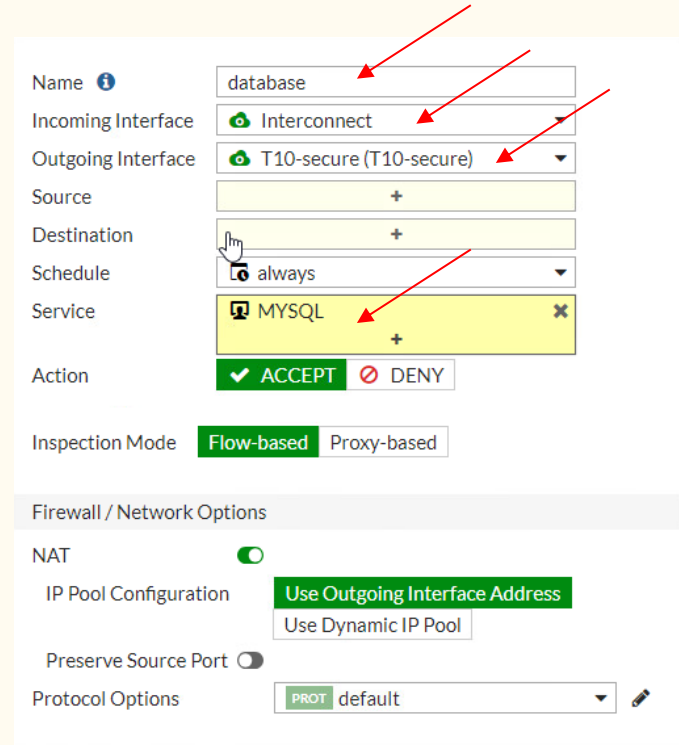
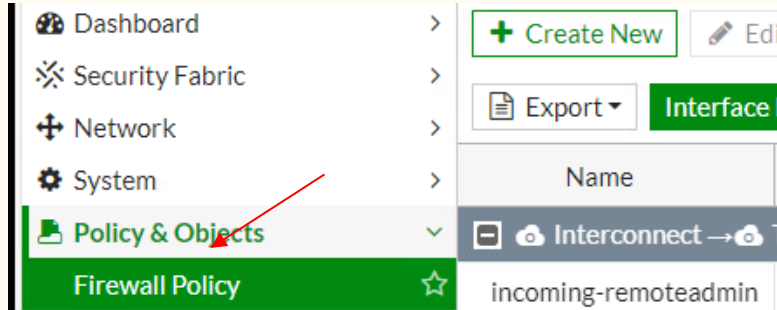
Select “Firewall Policy”
from the right side
menu.

Click “Create New”.

Name the new rule
“database”.

Under Incoming
Interface select
“Interconnect”

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



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 'Source' selection window in the firewall configuration. The 'Name' field is set to 'database'. The 'Incoming Interface' is 'Interconnect' and the 'Outgoing Interface' is 'T10-secure (T10-secure)'. The 'Source' field has a yellow button with a '+' sign. To the right, the 'Select Entries' dialog is open, showing the 'Address' tab selected. The 'Search' field is empty, and the 'Create' button is highlighted. Below the search field, there is a list of 'ADDRESS (14)' and an entry 'all'.

The screenshot shows the 'Select Entries' dialog with the 'Address' tab selected. The 'Search' field is empty, and the 'Create' button is highlighted. Below the search field, there is a section titled 'CREATE NEW' with two options: '+ Address' and '+ Address Group'. The '+ Address' option is selected.

The screenshot shows the 'New Address' dialog. The 'Name' field is 'dmz-web'. The 'Color' field has a 'Change' button. The 'Type' is 'Subnet'. The 'IP/Netmask' field is '192.168.201.0/24'. The 'Interface' is 'any'. The 'Static route configuration' is disabled. The 'Comments' field is 'Write a comment...'. The 'OK' button is highlighted.

Q2A Secure-Facing Firewall Configuration

Click OK.

Disable NAT

The screenshot shows the configuration for a firewall rule named 'database'. The 'Incoming Interface' is set to 'Interconnect' and the 'Outgoing Interface' is 'T10-secure (T10-secure)'. The 'Source' is 'dmz-web' and the 'Destination' is 'secure-db'. The 'Schedule' is 'always' and the 'Service' is 'MYSQL'. The 'Action' is set to 'ACCEPT'. Under 'Inspection Mode', 'Flow-based' is selected. In the 'Firewall / Network Options' section, the 'NAT' toggle is turned on, and 'Use Outgoing Interface Address' is selected for 'IP Pool Configuration'. 'Preserve Source Port' is disabled, and 'Protocol Options' are set to 'default'.

incoming-remoteadmin	MZ Inside	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

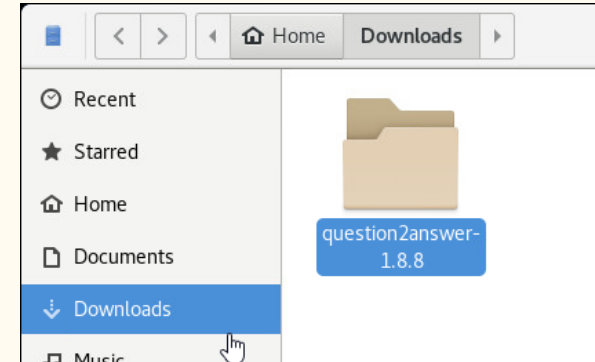
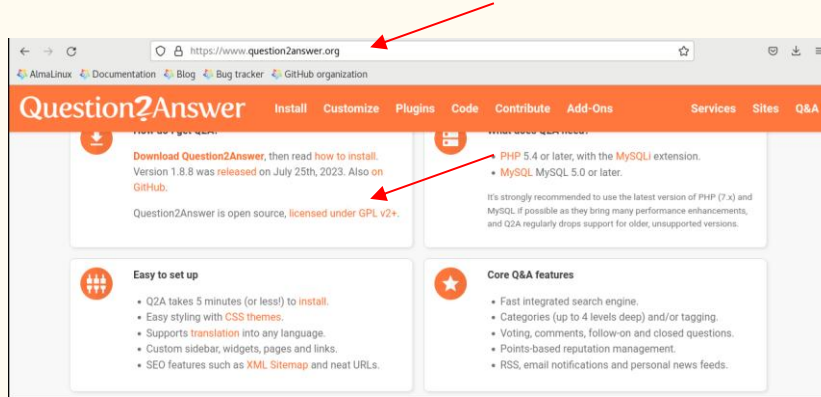
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

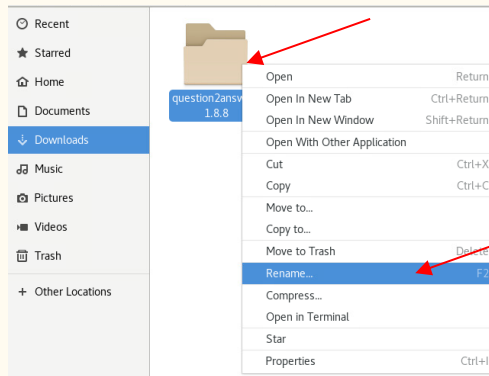
MariaDB [q2a]> █
```

Q2A Installation & Configuration

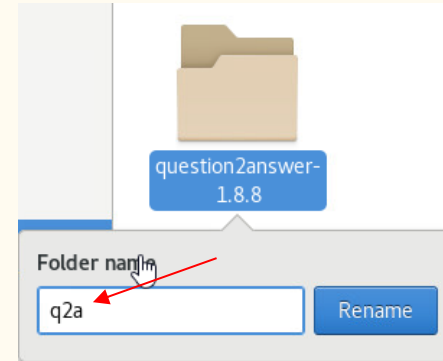
Open the browser on the Apache server and download the Question2Answer package from the Question2Answer website.



Extract the file into the downloads folder.



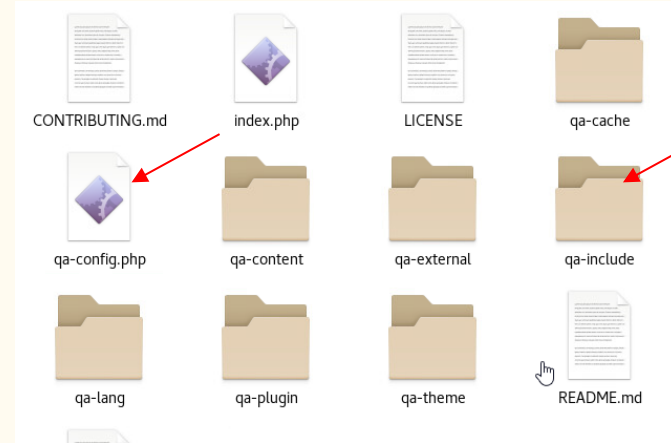
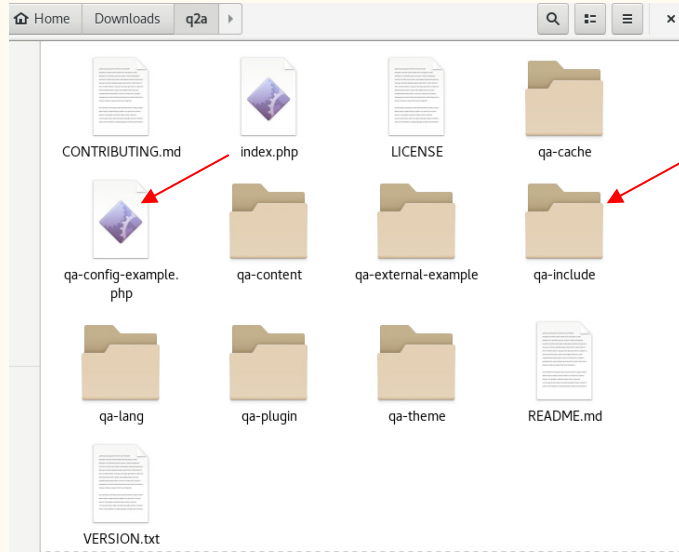
Rename the top file something easier like q2a.



Q2A Installation & Configuration

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

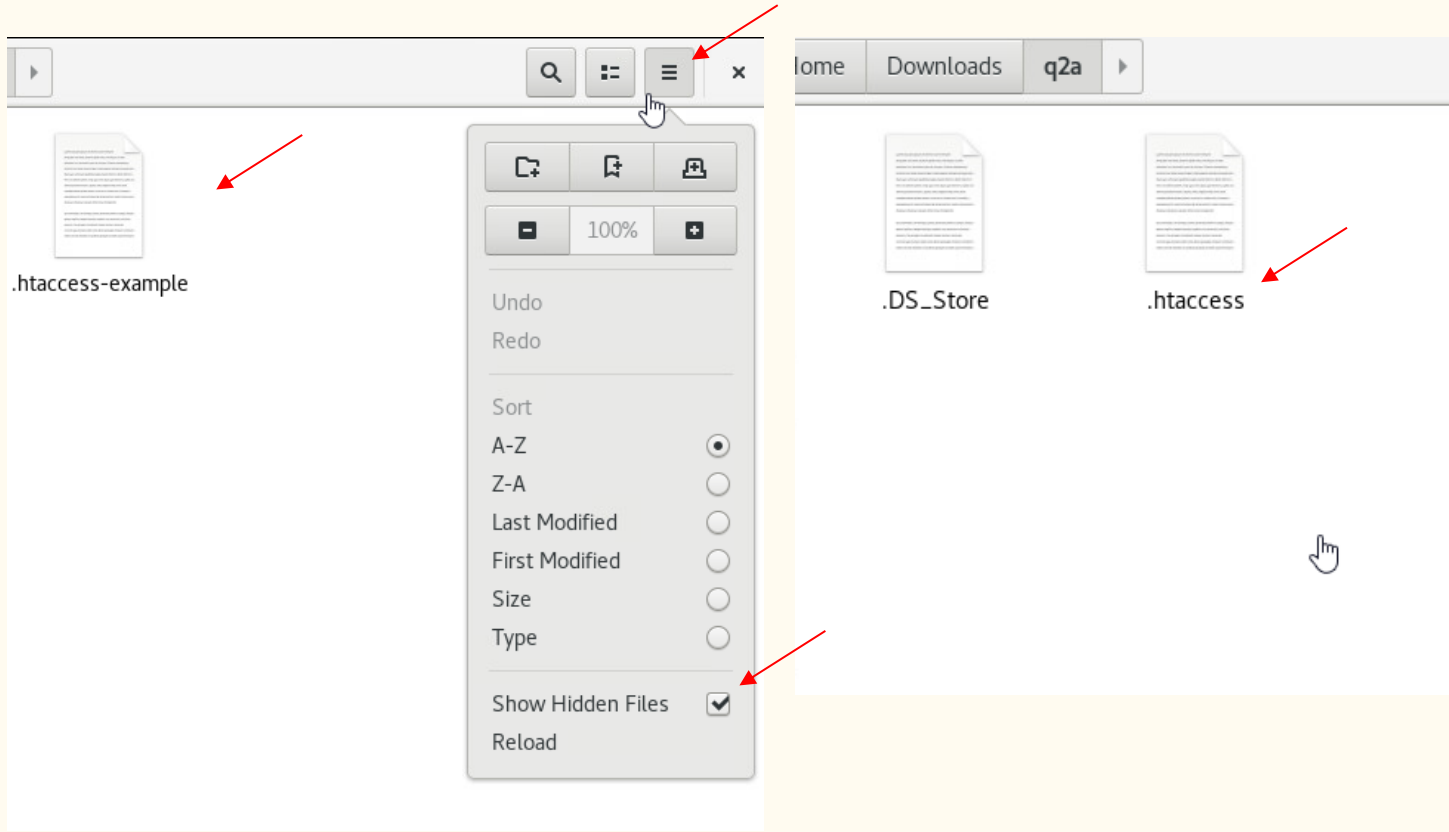
There is a hidden example file as well you will need to change.



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.

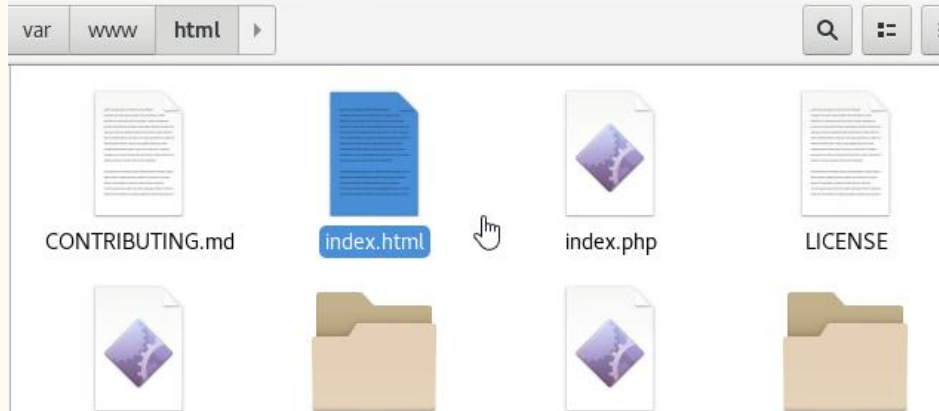
```
[cditto@localhost q2a]$ sudo mv * /var/www/html
```

```
[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

File Edit View Search Terminal Help

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

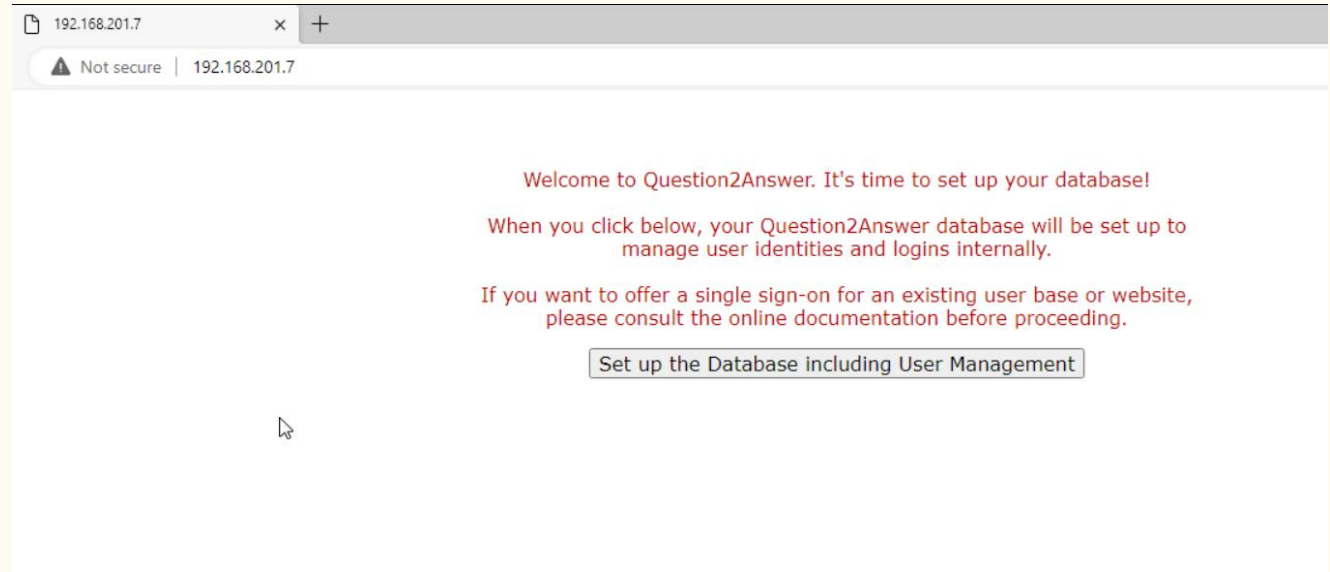
[sudo] password for cditto:

[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!

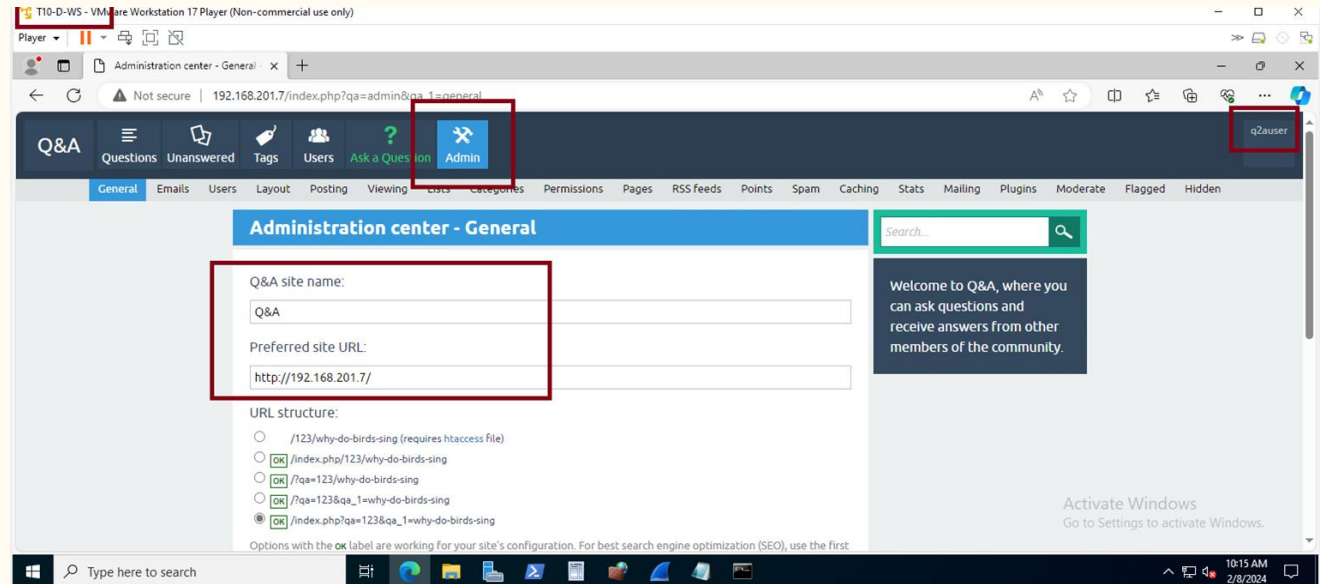
You are logged in as the super administrator and can start changing settings.

Thank you for installing Question2Answer.

[Go to admin center](#)

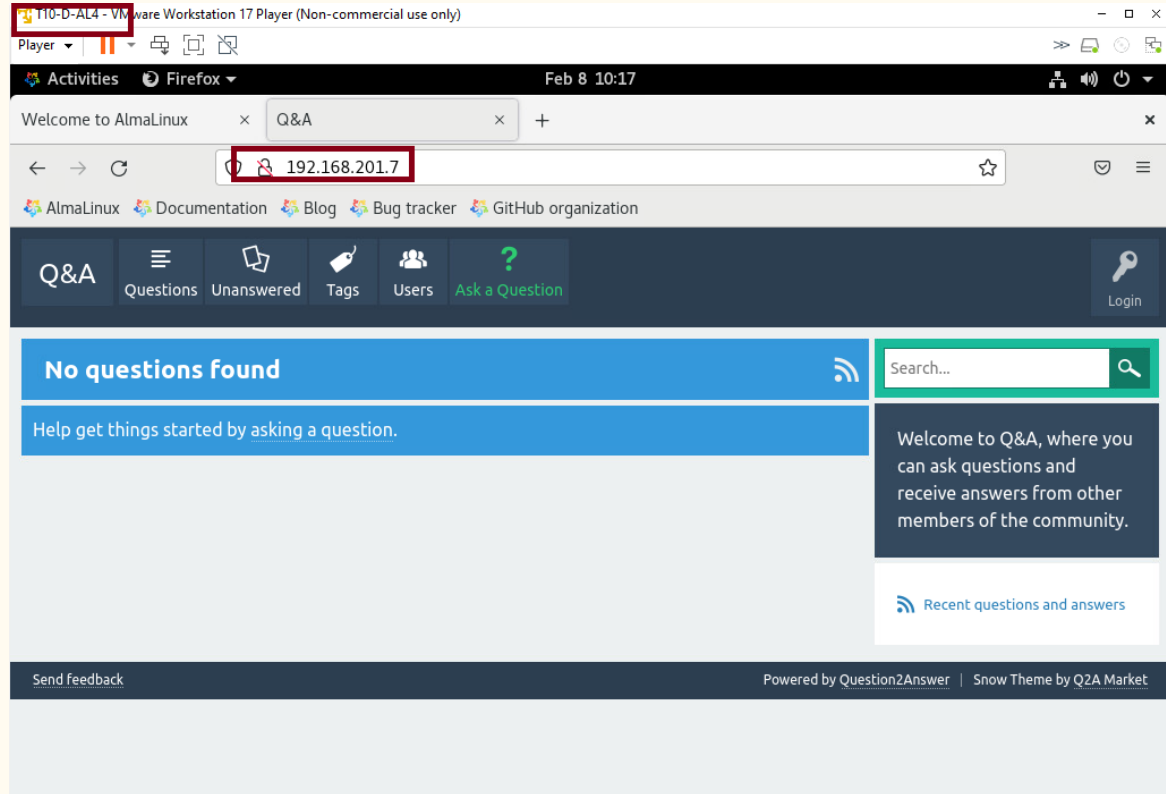
Q2A Installation & Configuration

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

Security 11 Items

	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE
1	rule1	none	universal	trust	any	any	any	untrust	any	any	any	any	Allow	none
2	T10-outbound	none	universal	dmz	192.168.201.0/24	any	any	outside	any	any	any	application...	Allow	none
3	T10-dmz-to-inside-remote-access	none	universal	dmz	192.168.202.0/24	any	any	inside	192.168.202.0/24	any	ms-rdp	ssh	Allow	none
4	T10-inside-to-dmz-all	none	universal	inside	192.168.202.0/24	any	any	dmz	192.168.201.0/24	any	any	application...	Allow	none
5	T10-secure-to-dmz-inside	none	universal	interconnect	192.168.203.0/24	any	any	dmz	192.168.201.0/24	any	any	application...	Allow	none
6	T10-squid-proxy	none	universal	interconnect	192.168.203.0/24	any	any	dmz	192.168.201.0/24	any	any	service-squid	Allow	none
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	ssh	Allow	none
8	T10-web	none	universal	dmz	192.168.202.0/24	any	any	dmz	172.201.22.12	any	web-browsing	application-...	Allow	none
9	T10-database-maria	none	universal	dmz	192.168.201.7	any	any	interconnect	192.168.203.3	any	mysql	application...	Allow	none
10	Intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none
11	Interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none

Policy Optimizer

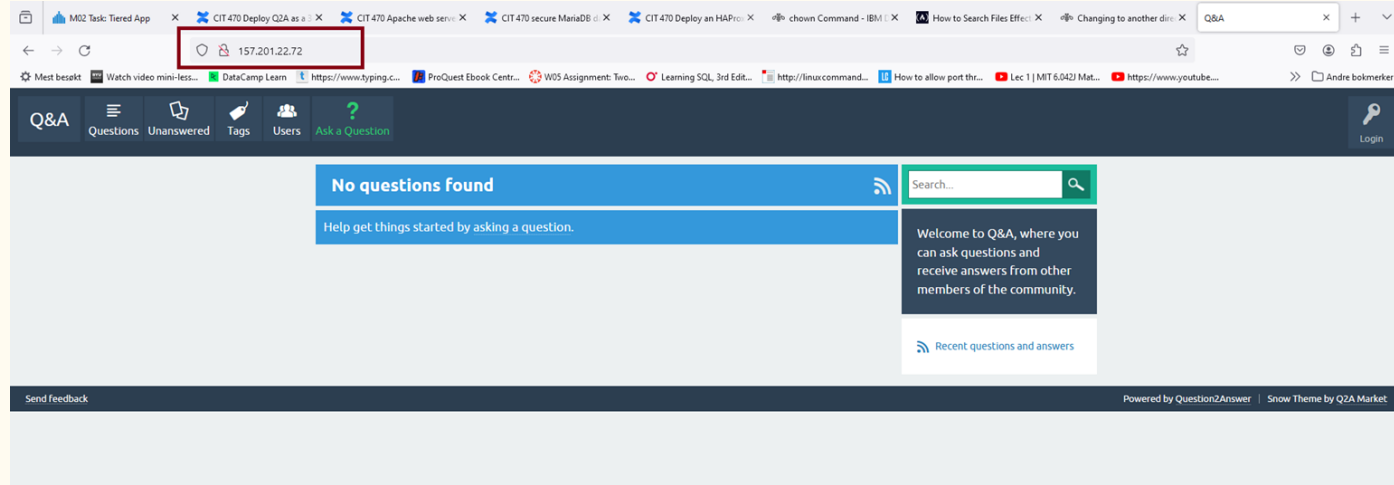
- New App Viewer
- Rules Without App Controls 4
- Unused Apps 0
- Rule Usage
 - Unused in 30 days 1
 - Unused in 90 days 1
 - Unused 1

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

Logout | Last Login Time: 02/05/2024 14:01:24 | Session Expire Time: 03/09/2024 10:55:47 |

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



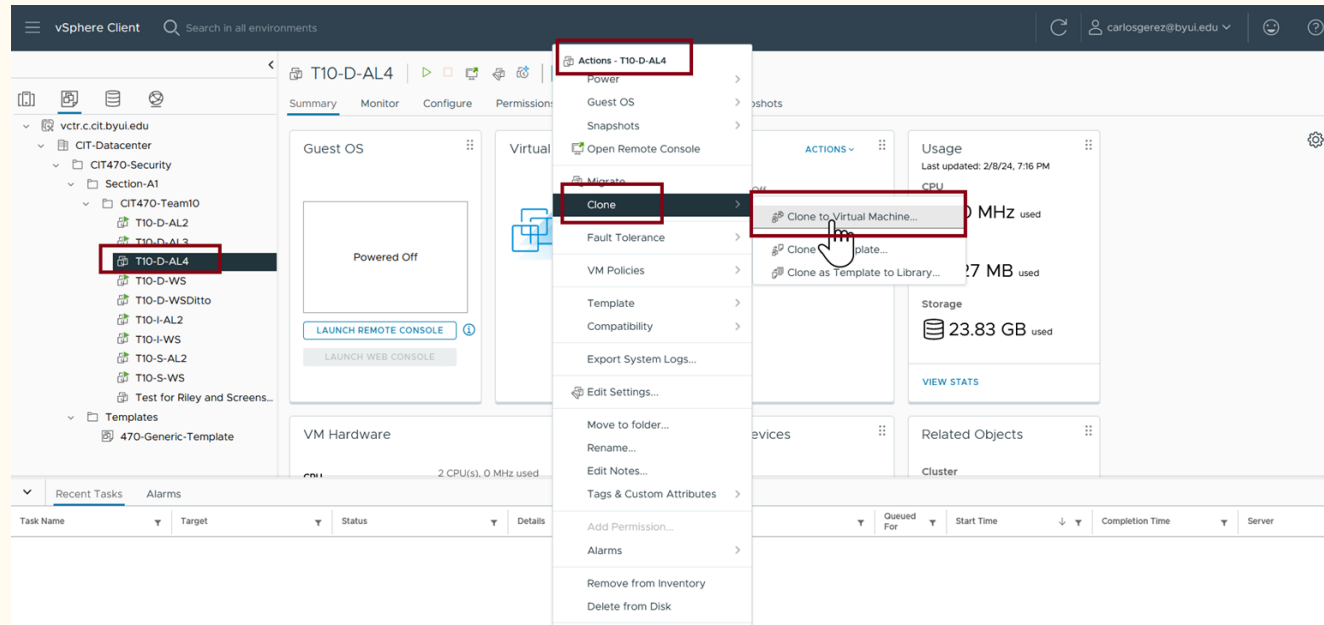
HAProxy load balancer configuration

—

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 where the machine will reside. Press next.

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 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: T10-D-AL5

Select a location for the virtual machine.

- vcitr.c.cit.byui.edu
 - CIT-Datacenter
 - CIT470-Security
 - Section A1
 - CIT470-Team10**
 - Templates

CANCEL NEXT

Cloning the machine that holds the apache server.

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

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 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

- 10.11.175.101
- 10.11.175.102
- 10.11.175.103
- 10.11.175.104
- 10.11.175.109
- 10.11.175.110
- 10.11.175.111
- > Azure-Arc
- > CIT-151
- > CIT-225
- > CIT-326
- > CIT-353
- CIT-470

Compatibility

⚠ There are compatibility warnings. [Show details...](#)

CANCEL BACK NEXT

Cloning the machine that holds the apache server.

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

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 Ready to complete

Select storage

Select the storage for the configuration and disk files

BATCH CONFIGURE

CONFIGURE PER DISK

Select virtual disk format

Same format as source

VM Storage Policy

☐ Disable Storage DRS for this virtual machine

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

Manage Columns

Items per page 10 1 item

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

Cloning the machine that holds the apache server.

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

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 Ready to complete

Select clone options

Select further clone options

- ☐ Customize the operating system
- ☐ Customize this virtual machine's hardware
- ☒ **Power on virtual machine after creation**

CANCEL BACK **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

Virtual machine name

Folder

Resource pool

Datastore

Disk storage

✓ Hard disk 1

Capacity

Datastore

Virtual device node

Mode

T10-D-AL4

T10-D-AL5

CIT470-Team10

CIT-470

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

Same format as source

96 GB

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

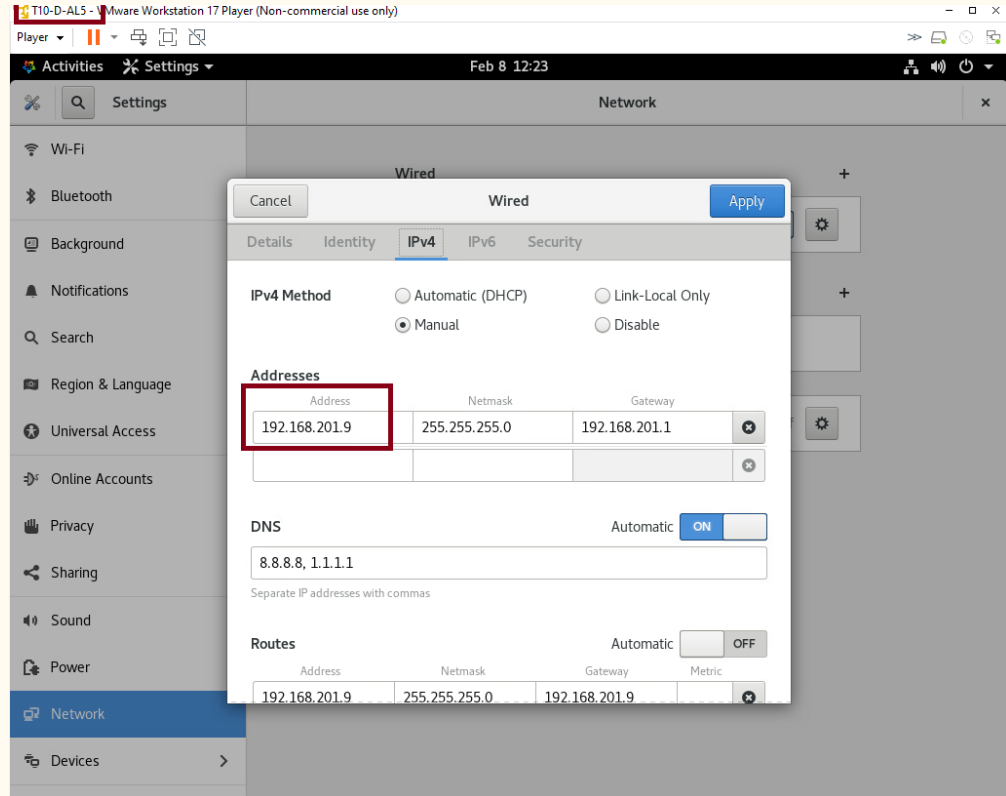
CANCEL

BACK

FINISH

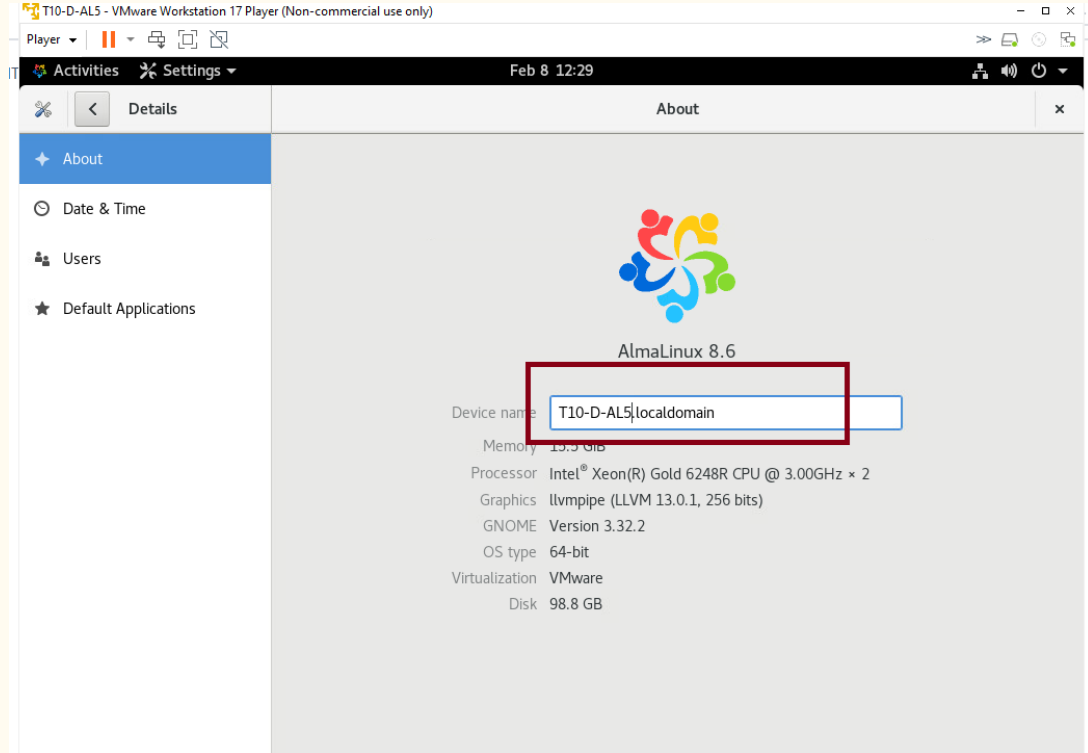
Cloning the machine that holds the apache server.

Change the ip addresses to the new machine address.



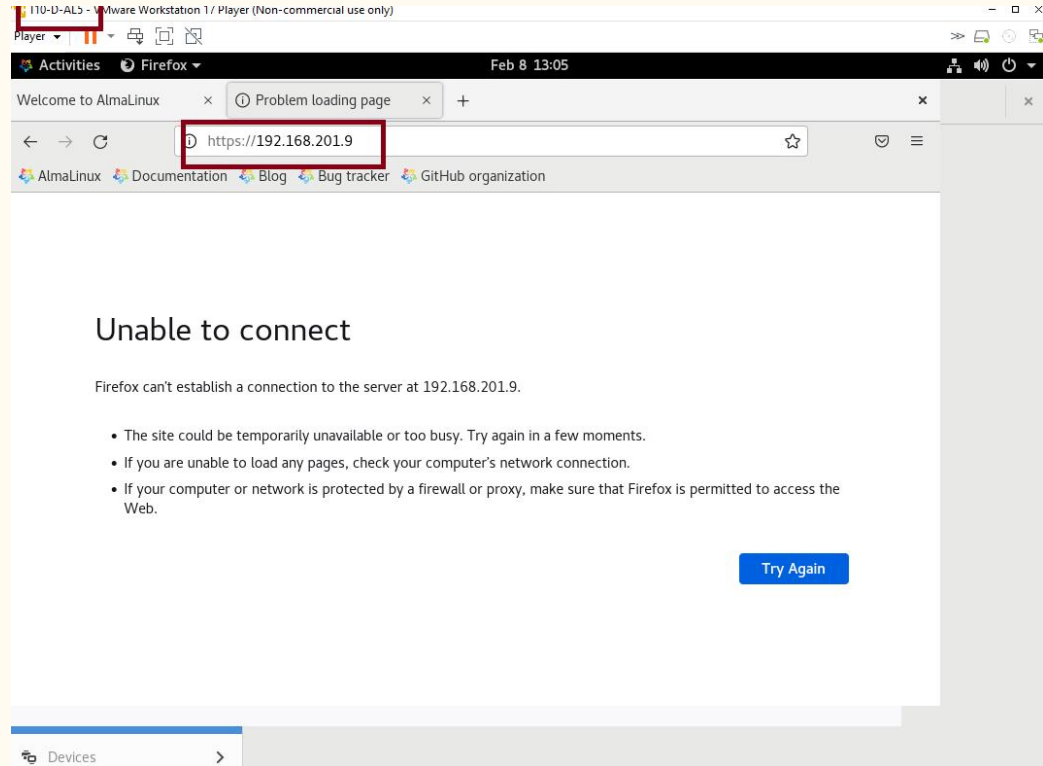
Cloning the machine that holds the apache server.

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:

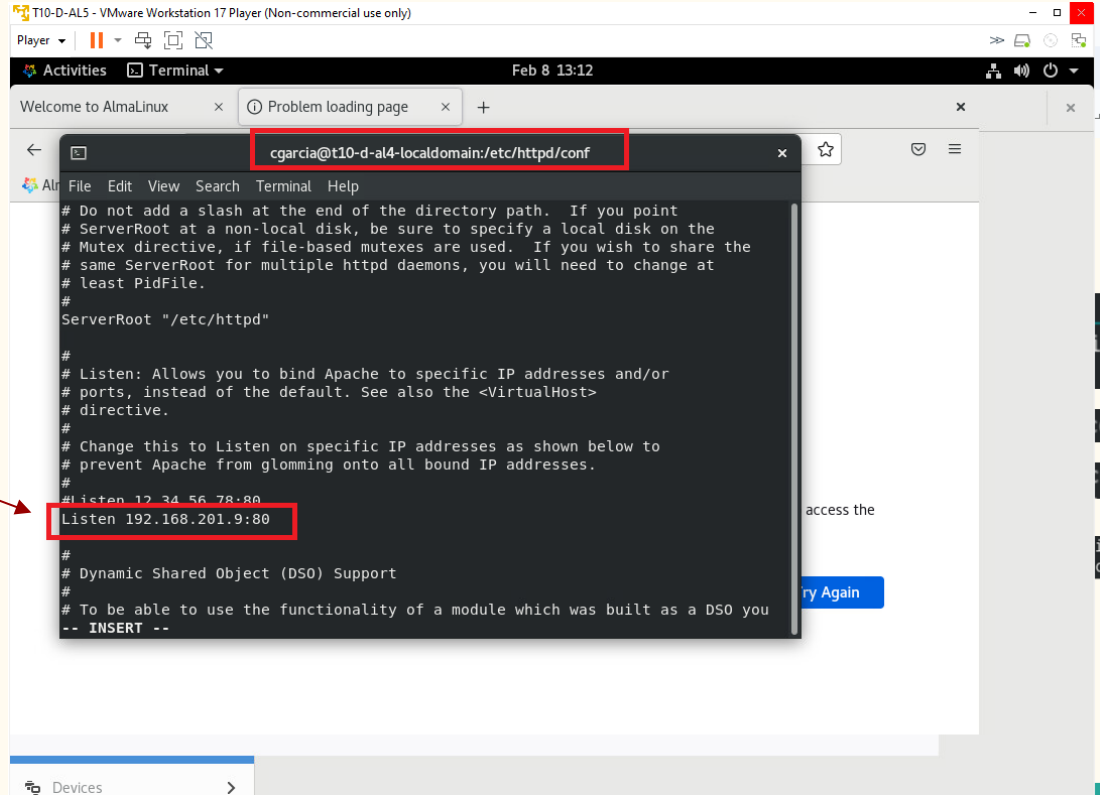
```
cd /etc/httpd/conf
```

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

```
sudo vi httpd.conf
```

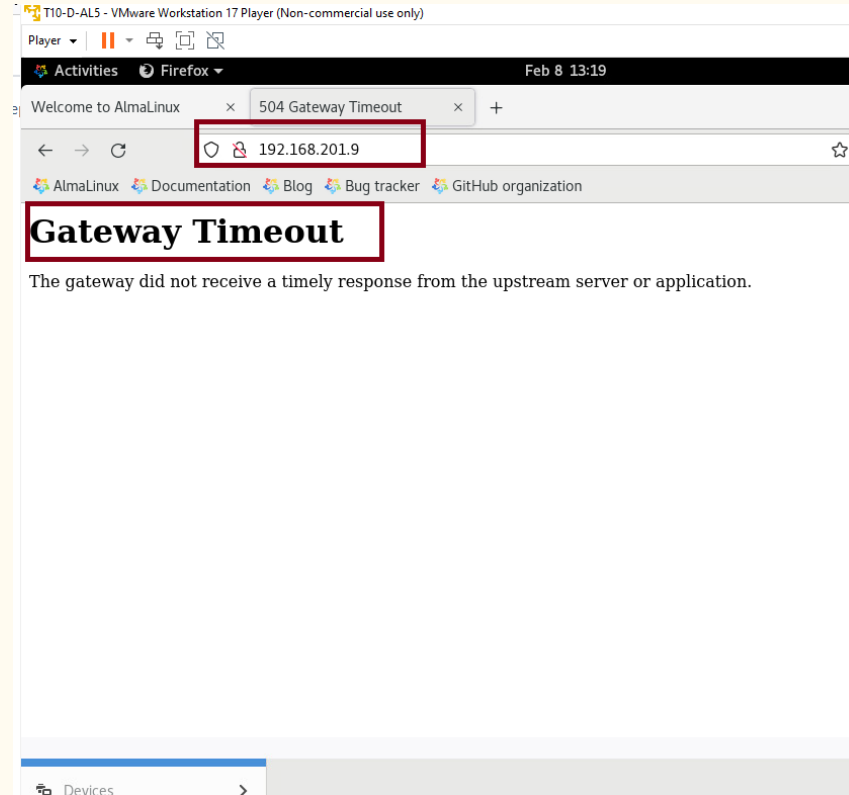
1. restart the service to apply the changes.

```
systemctl restart httpd
```



Configuring the app in the cloned machine.

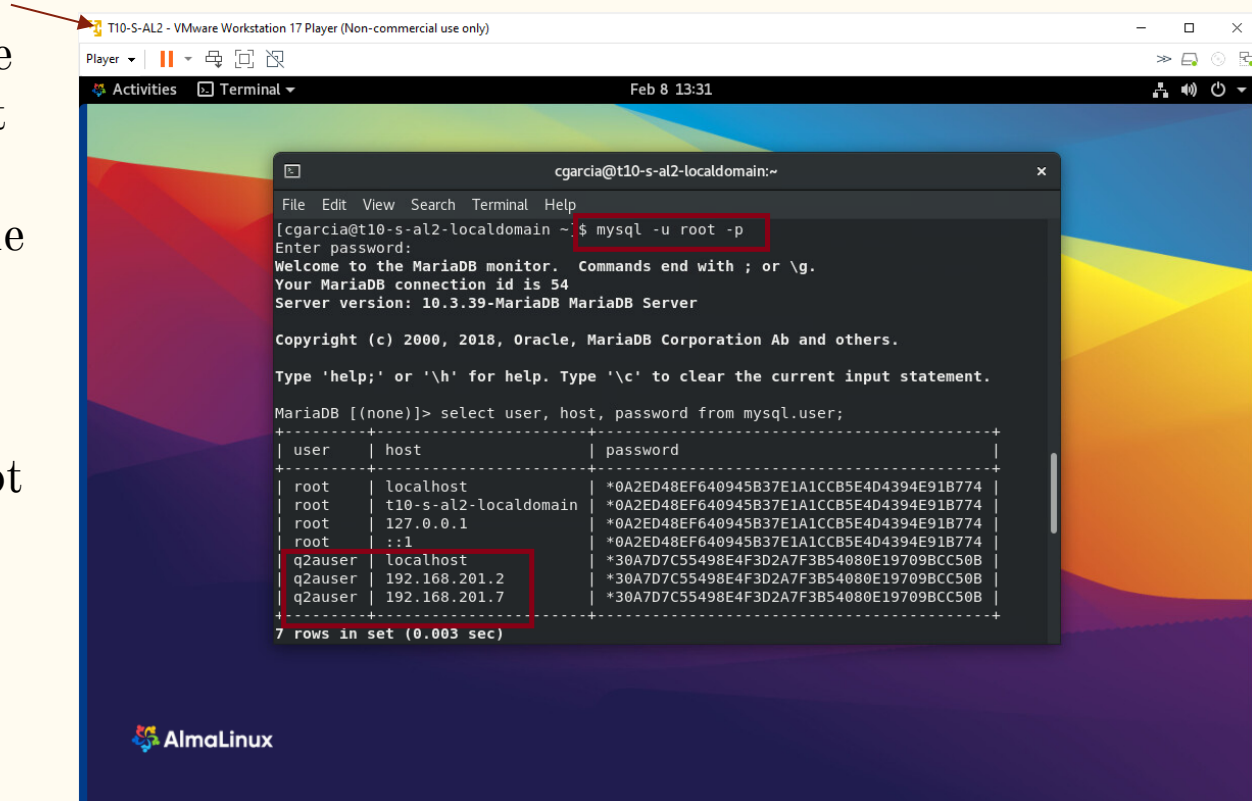
We get this new message because the mariadb database is not yet configured to connect with this machine.



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.

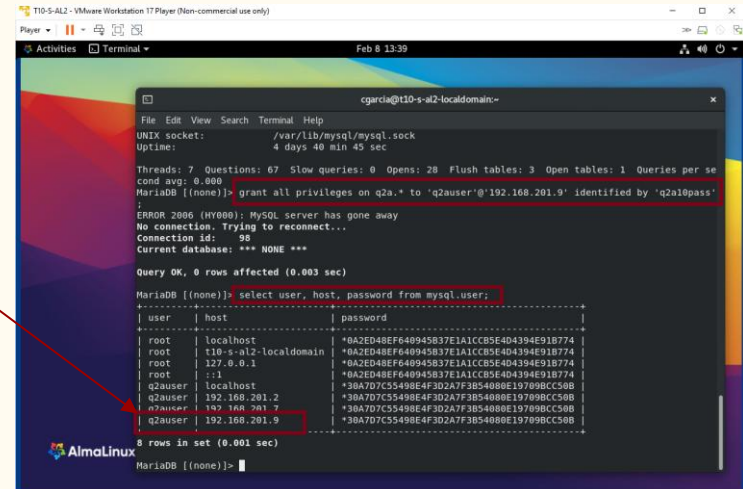
To give access use the following command:

```
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.



```
T10-S-AL2 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities Terminal Feb 8 13:39
cgarcia@t10-s-al2-localdomain~
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 se
cond 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: 98
Current database: *** NONE ***

Query OK, 0 rows affected (0.003 sec)

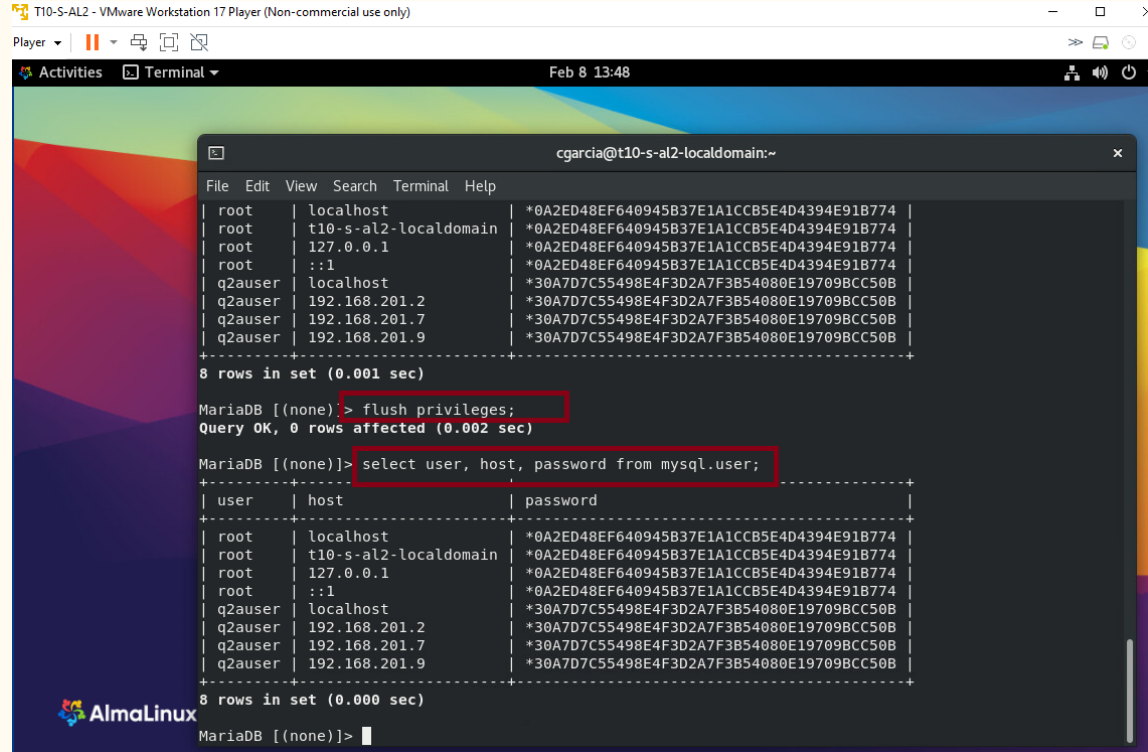
MariaDB [(none)]> select user, host, password from mysql.user;
+-----+-----+-----+
| user | host | password |
+-----+-----+-----+
| root | localhost | *0A2ED48EF648945837E1A1CC85E4D4394E918774 |
| root | t10-s-al2-localdomain | *0A2ED48EF648945837E1A1CC85E4D4394E918774 |
| root | 127.0.0.1 | *0A2ED48EF648945837E1A1CC85E4D4394E918774 |
| root | ::1 | *0A2ED48EF648945837E1A1CC85E4D4394E918774 |
| q2auser | localhost | *30A707C55498E4F3D2A7F3B54080E197098CC508 |
| q2auser | 192.168.201.2 | *30A707C55498E4F3D2A7F3B54080E197098CC508 |
| q2auser | 192.168.201.9 | *30A707C55498E4F3D2A7F3B54080E197098CC508 |
+-----+-----+-----+
8 rows in set (0.001 sec)

MariaDB [(none)]>
```

Configuring the app in the cloned machine.

Remember to
flush those
privileges:

```
flush privileges;
```



```
T10-S-AL2 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities Terminal Feb 8 13:48
cgarcia@t10-s-al2-localdomain:~
File Edit View Search Terminal Help
| root | localhost | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |
| root | t10-s-al2-localdomain | *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)

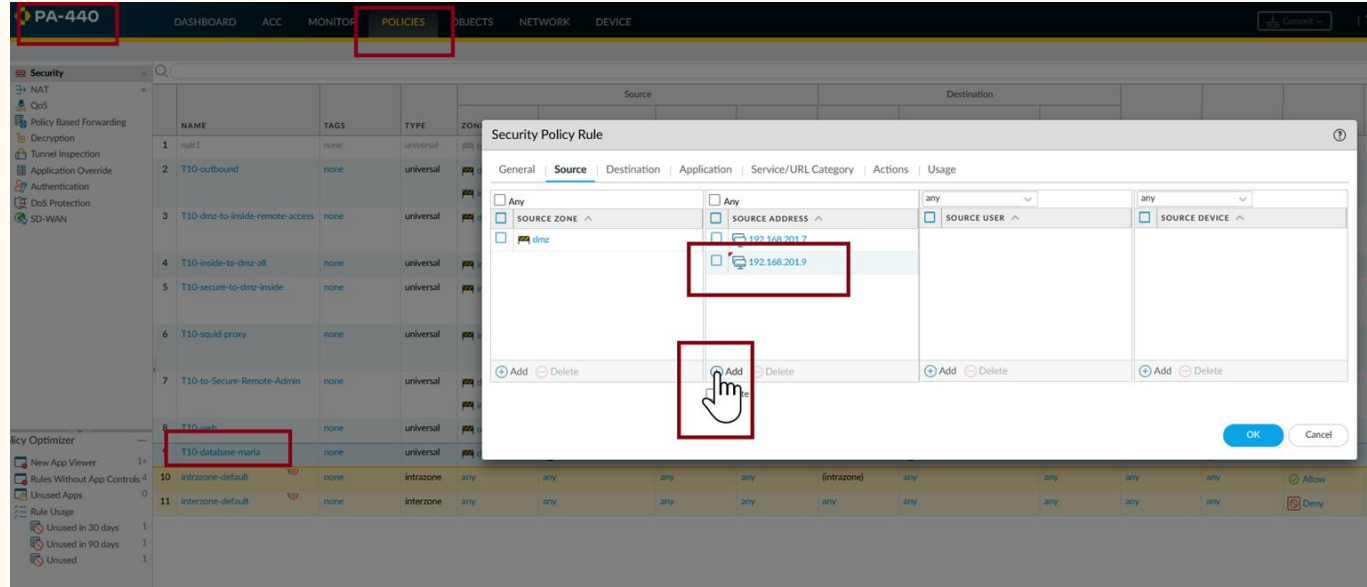
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> select user, host, password from mysql.user;
+-----+
| user | host | password |
+-----+
| root | localhost | *0A2ED48EF640945B37E1A1CCB5E4D4394E91B774 |
| root | t10-s-al2-localdomain | *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)

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

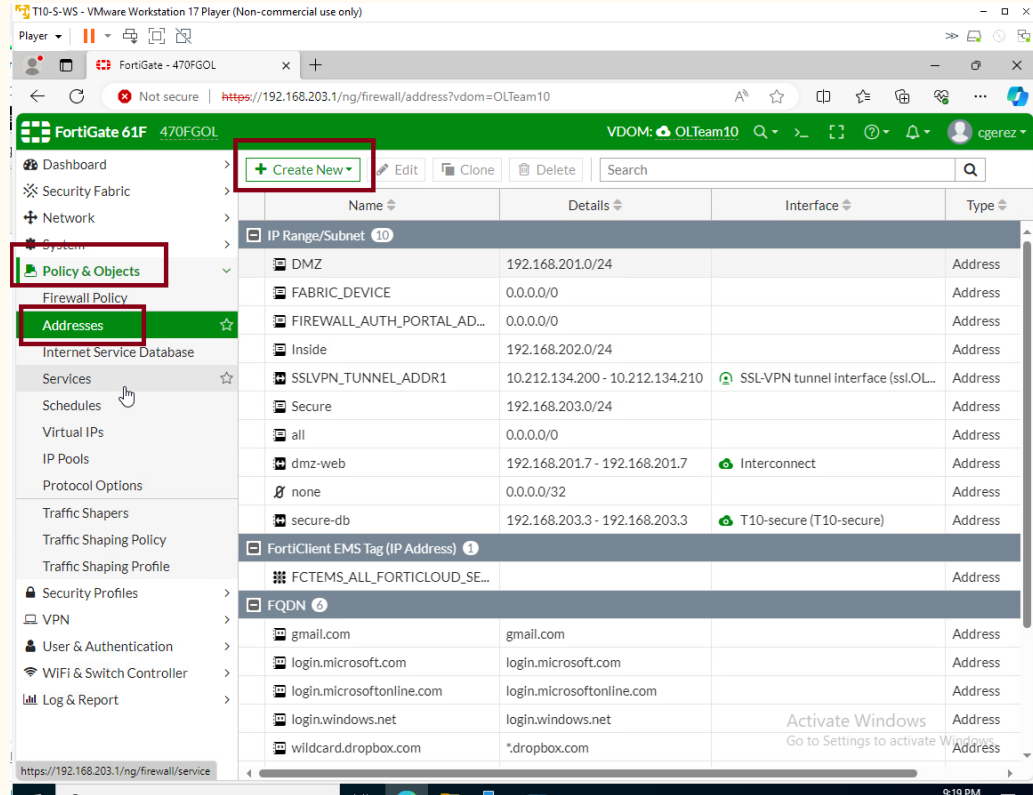

Configuring the app in the cloned machine.

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.



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**.

FortiGate 61F 470FGOL VDOM: OLTeam10

Dashboard > Security Fabric > Network > System > Policy & Objects > Firewall Policy > Addresses ☆

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 >
Log & Report >

New Address

Name: dmz-web2
Color: [Change]
Type: IP Range
IP Range: 192.168.201.9 - 192.168.201.9
Interface: Interconnect
Static route configuration: [Off]
Comments: Write a comment... 0/255

OK Cancel

FortiGate 470FGOL

Dynamic Address

Guides

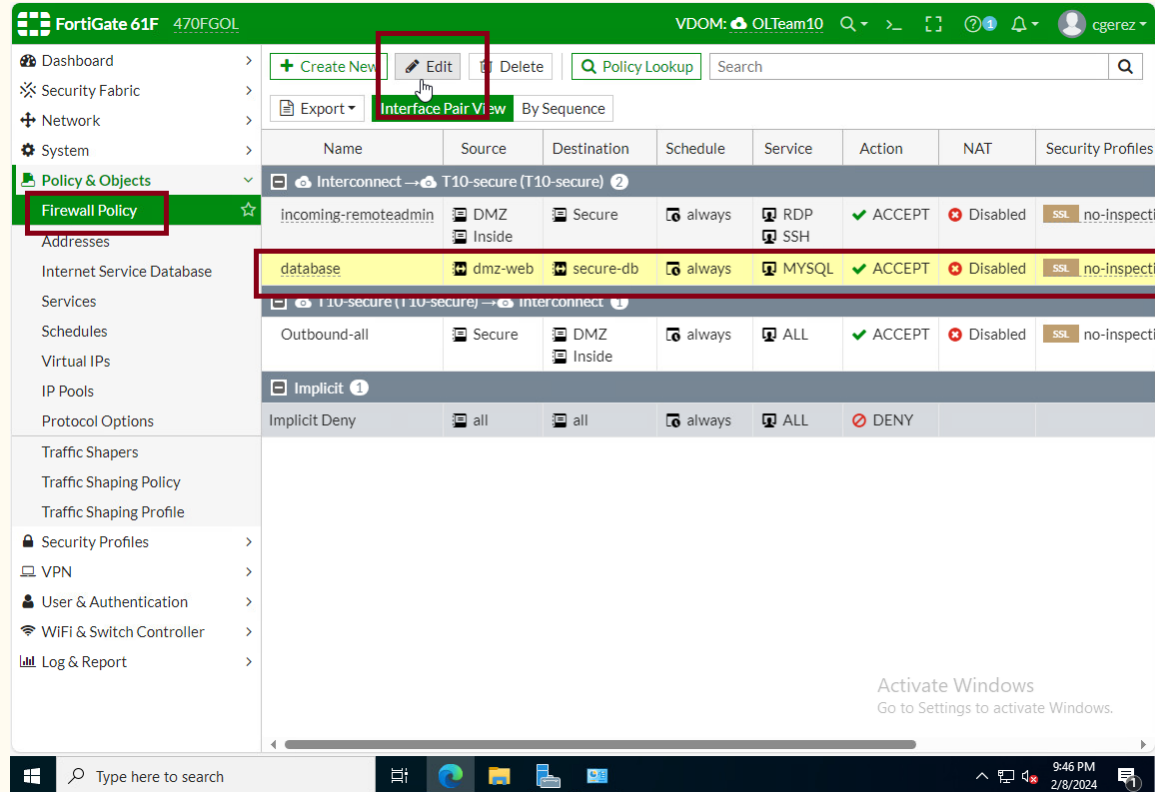
- Configuring an AWS Dynamic Address
- Configuring an Azure Dynamic Address
- Configuring a Google Cloud Platform Dynamic Address
- Configuring an Oracle Cloud Infrastructure Dynamic Address
- Configuring an OpenStack Dynamic Address

Documentation

- Online Help
- Video Tutorials

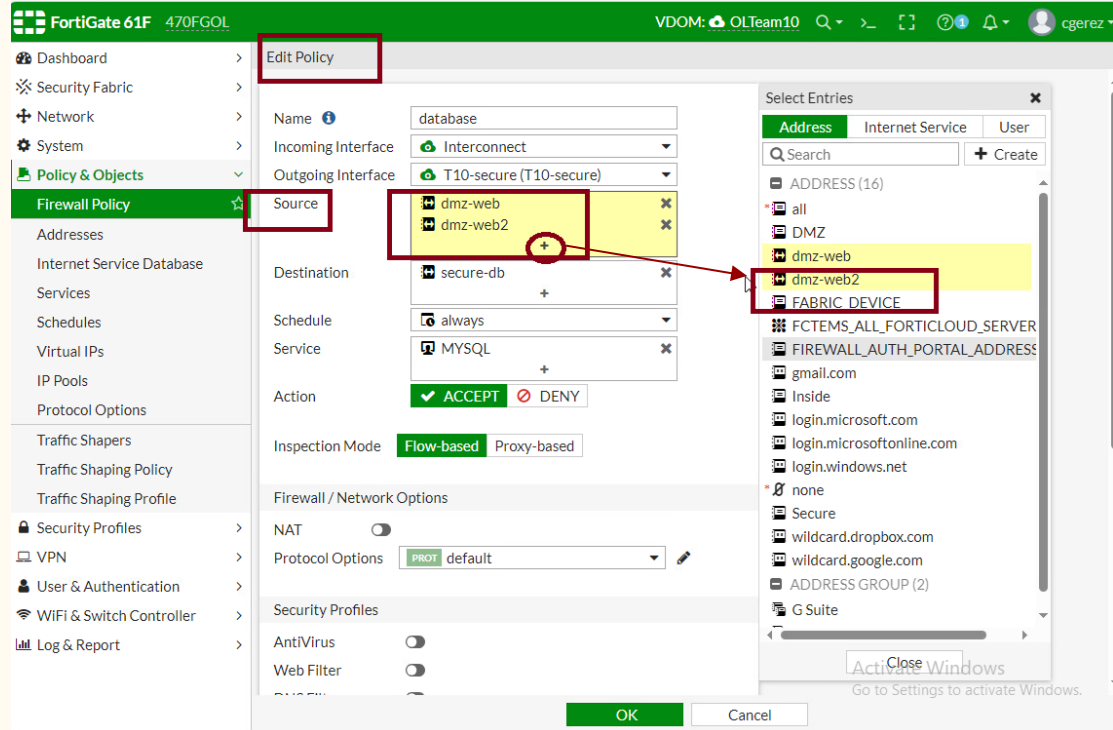
Configuring the app in the cloned machine.

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



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 look 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.

FortiGate 61F 470FGOL VDOM: OLTeam10

Dashboard Security Fabric Network System Policy & Objects Firewall Policy Addresses Internet Service Database Services Schedules Virtual IPs IP Pools Protocol Options Traffic Shapers Traffic Shaping Policy

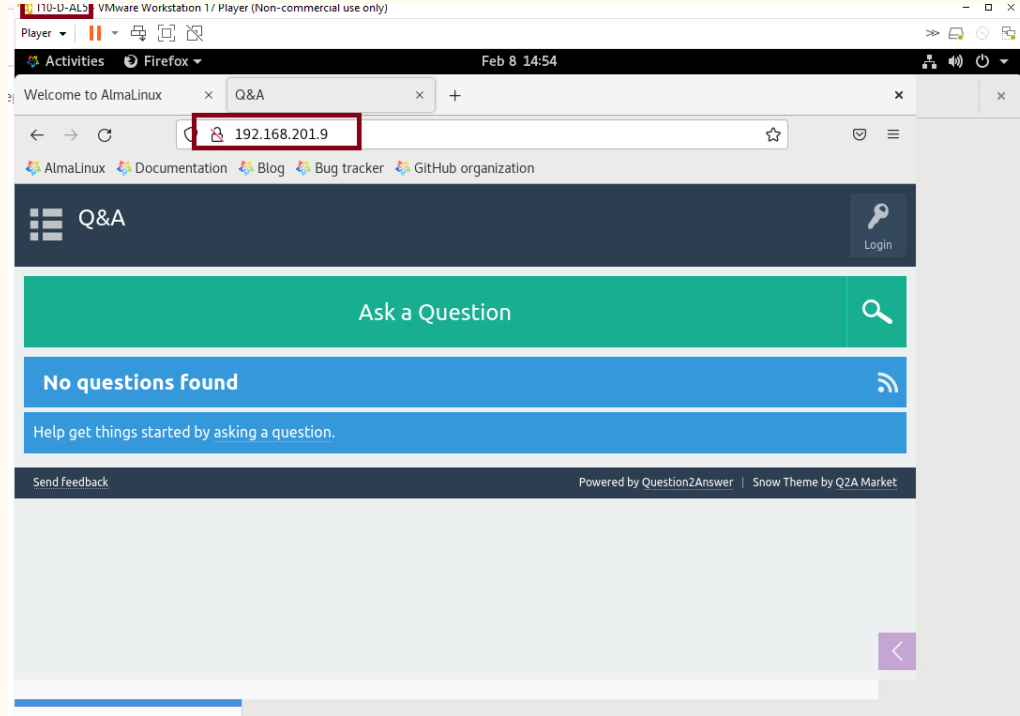
Create New Edit Delete Policy Lookup Search

Export Interface Pair View By Sequence

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

Configuring the app in the cloned machine.

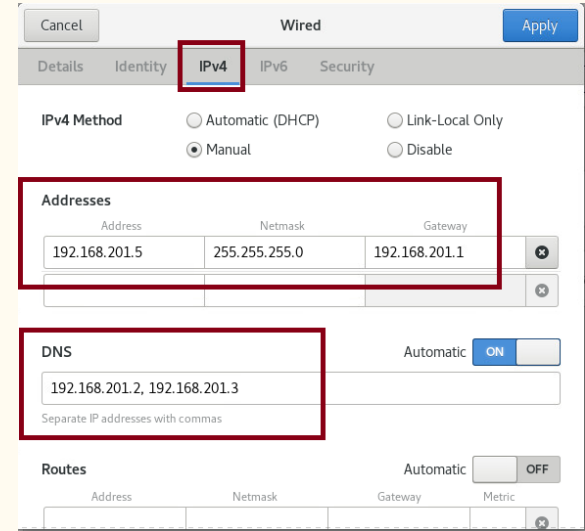
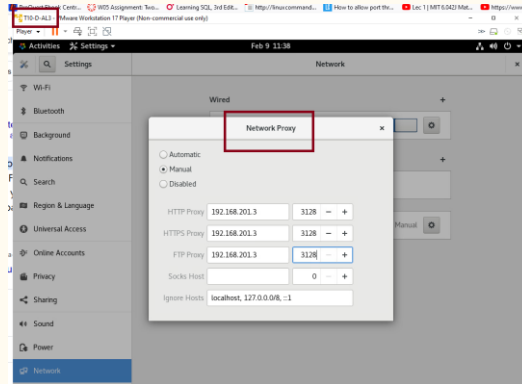
Now from any machine on the dmz zone you are able to start the app with the address of the new machine. Then, the app is working as it should from the DMZ zone now in the new cloned machine.



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
```

```

cgrerz@T10-D-AL3-~
File Edit View Search Terminal Help
Complete!
[cgrerz@T10-D-AL3 ~]$ dnf search haproxy
haproxy.x86_64 : HAProxy reverse proxy for high availability environments
pcp-pmda-haproxy.x86_64 : Performance Co-Monitor (PCoM) metrics for HAProxy
[cgrerz@T10-D-AL3 ~]$ sudo dnf -y install haproxy
[sudo] password for cgrerz:
Last metadata expiration check: 0:26:37 ago on Fri 09 Feb 2024 11:51:22 AM CST.
Dependencies resolved.

Package                               Architecture Version      Repository    Size
-----
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

```

```

cgeres@T10-D-AL3-~
File Edit View Search Terminal Help

Installed:
haproxy-1.8.27-5.el8.x86_64

Complete!

[cgeres@T10-D-AL3-~]$ rpm -ql haproxy
/etc/haproxy
/etc/haproxy/conf.d
/etc/haproxy/haproxy.cfg
/etc/cryptsetup/swap-ss
/etc/sysconfig/haproxy
/usr/bin/halog
/usr/bin/orange
/usr/lib/boost-id
/usr/lib/boost-id/62
/usr/lib/boost-id/62/a67b6a2d0ed53184ef425b1573e0a692c6a2
/usr/lib/boost-id/69
/usr/lib/boost-id/69/3bfff6b6ceb4f1beab22d47e7853aa8d3e
/usr/lib/boost-id/69d
/usr/lib/boost-id/6d/c48075472ad4837abae60e09add8cfc0d23e
/usr/lib/systemd/system/haproxy.service
/usr/sbin/haproxy
/usr/share/doc/haproxy
/usr/share/doc/haproxy/51Degrees-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 configure round robin in our balancer, haproxy will listen for connections in this system and forwarder taking turns 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
```

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)

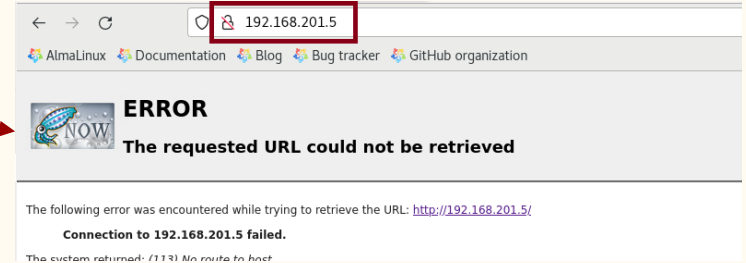
[cgerez@T10-D-AL3 haproxy]$ sudo systemctl enable haproxy
[sudo] password for cgerez:
Created symlink /etc/systemd/system/multi-user.target.wants/haproxy.service → /usr/lib/systemd/system/haproxy.service.

[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 (code=0)
    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/defaults.cfg
              └─373811 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -f /etc/haproxy/defaults.cfg

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 has to configure the firewall in the balancer host machine to allow the http service with:



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

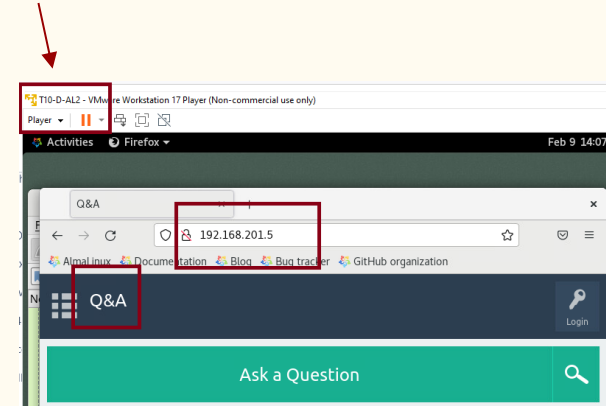
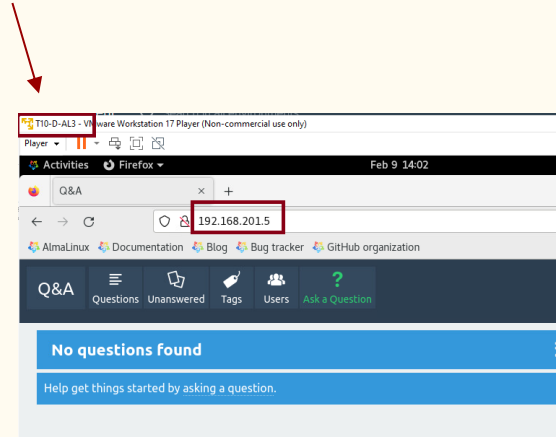
```
sudo firewall-cmd --reload
```

```
FEB 09 13:46:27 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

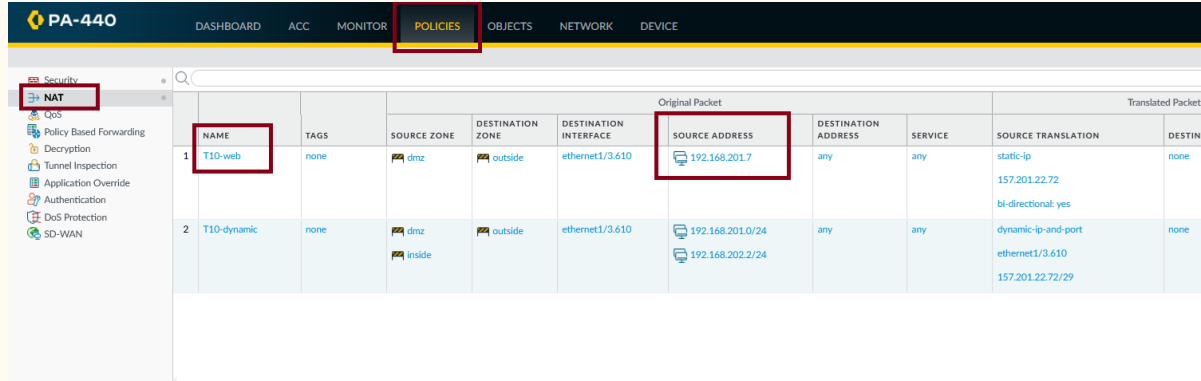
Here you can see access from the load balancer host and from another endpoint in the dmz.



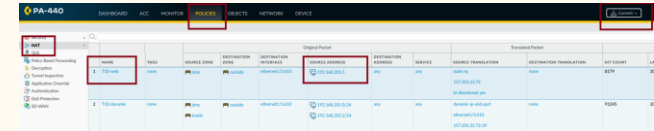
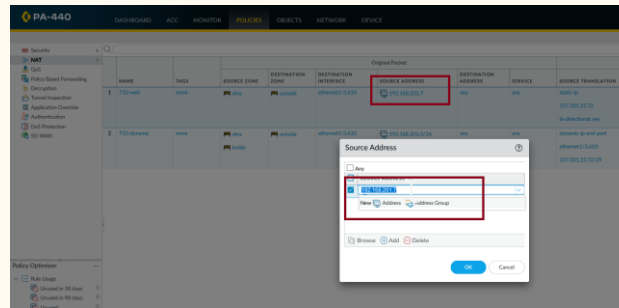
Test HAProxy, and verify that is balancing properly.

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	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	T10-web	none	dmz	outside	ethernet1/3.610	192.168.201.7	any	any	static-ip 157.201.22.72 bi-directional yes	none
2	T10-dynamic	none	dmz	outside	ethernet1/3.610	192.168.201.0/24 192.168.202.2/24	any	any	dynamic-ip-and-port ethernet1/3.610 157.201.22.72/29	none

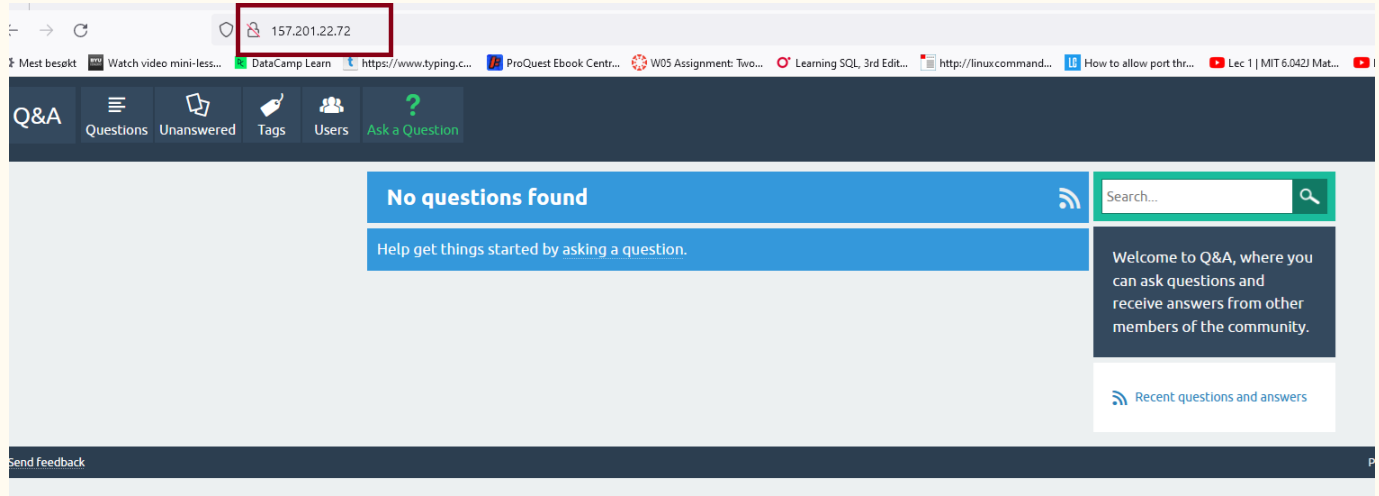


	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	T10-web	none	dmz	outside	ethernet1/3.610	192.168.201.7	any	any	static-ip 157.201.22.72 bi-directional yes	none
2	T10-dynamic	none	dmz	outside	ethernet1/3.610	192.168.201.0/24 192.168.202.2/24	any	any	dynamic-ip-and-port ethernet1/3.610 157.201.22.72/29	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
```

```
success
[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:rsyslogd(8)
```

Find his configuration file

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

```
Feb 09 12:06:13 T10-D-AL3.localdomain rsyslogd[2974]:
[cgerez@T10-D-AL3 haproxy]$ rpm -ql rsyslog | less
[cgerez@T10-D-AL3 haproxy]$ rpm -ql rsyslog | less
[cgerez@T10-D-AL3 haproxy]$
```

Edit his configuration file with vi and uncomment this lines:

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

```
File Edit View Search Terminal Help
/etc/logrotate.d/syslog
/etc/passwd
/etc/rsyslog.conf
/etc/rsyslog.d
/etc/sysconfig/rsyslog
/usr/bin/rsyslog-recover-qi.pl
/usr/lib/.build-id
/usr/lib/.build-id/00
/usr/lib/.build-id/00/b09aeeab48d8b16d
```

```
#module(load="imudp")
```

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

```
File Edit View Search Terminal Help
cgerez@T10-D-AL3retrohaproxy

# For more information see /usr/share/doc/rsyslog-*/rsyslog.conf.html
# or latest version online at http://www.rsyslog.com/doc/rsyslog.conf.html
# If you experience problems, see http://www.rsyslog.com/doc/troubleshooting.html

#### MODULES ####

module(load="imuxsock") # provides support for local system logging
                        # To turn off message reception via local log
                        # local messages are retrieved through injo
module(load="imjournal") # provides access to the systemd
                        # journal. Note that the journal needs to be
                        # started.
                        # Statefile="imjournal.state" # File to store the position in th
module(load="imklog") # reads kernel messages (the same as read from
module(load="immark") # provides --MARK-- message capability

# 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")

end
```

Then restart the service and check on the logs.

```
sudo systemctl restart rsyslog
```

```
[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.*                                          /var/log/secure

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

:wd
```

```
[cron-20240121] glusterfs maillog-20240121 secure-20240121 swap tuned wtmp
[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 15:25:55 localhost haproxy[374848]: 88.90.190.47:64576 [09/Feb/2024:15:25:55.471] q2aWeb q2aBack/t10-d-a14 0/0/1
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-a15 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-a14 0/0/1
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-a15 0/0/0
0 "GET / HTTP/1.1"
Feb  9 15:26:17 localhost haproxy[374848]: 192.168.201.3:48230 [09/Feb/2024:15:26:17.760] q2aWeb q2aBack/t10-d-a14 1/0/0
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:

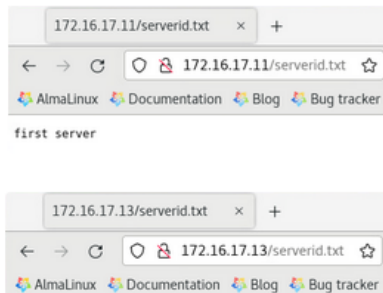
On the first web server, create a "static page" file that contains some identifying content. Example:

```
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
```

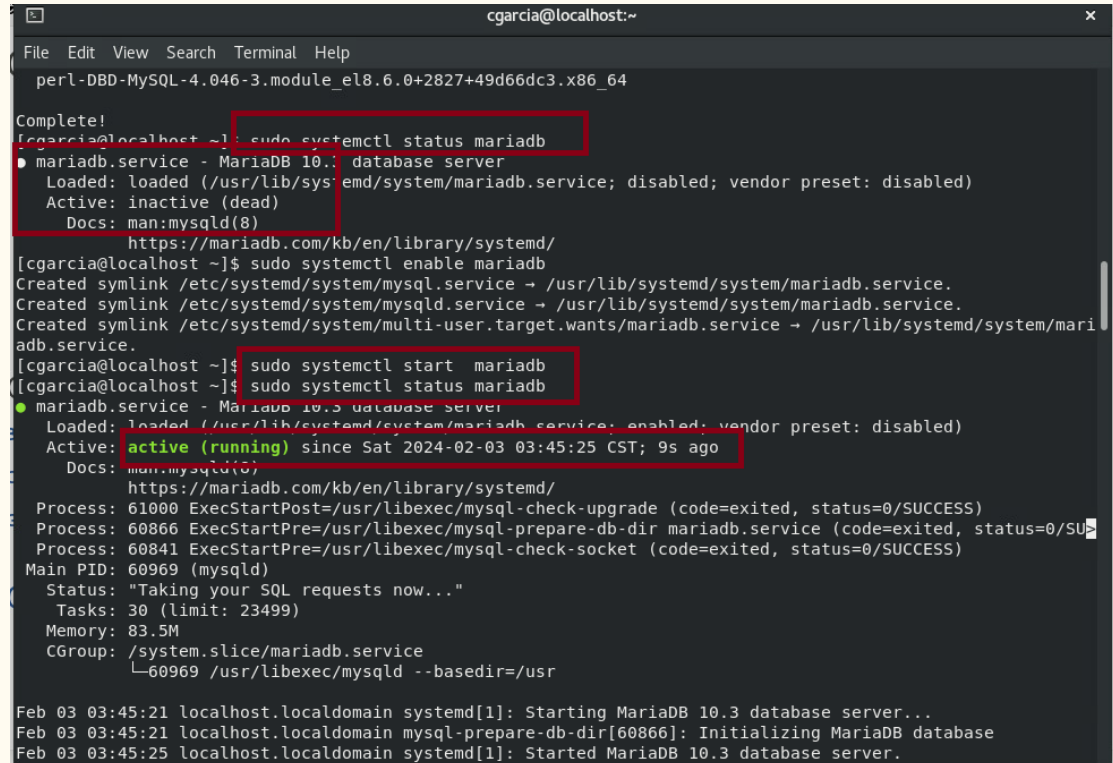
Launch a browser on a DMZ VM, and verify the contents each identifier file on its respective host:



Challenges we
faced

If mariadb is not running use the following commands.

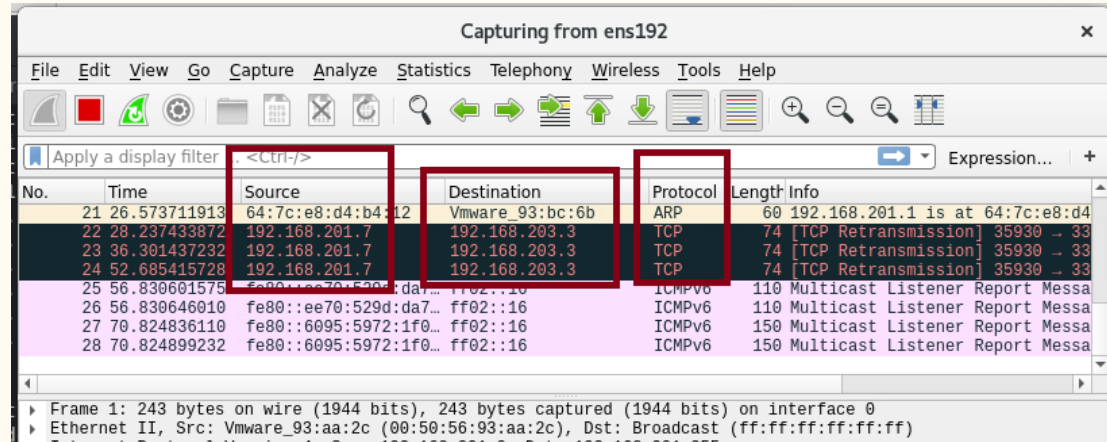
Use the command `sudo systemctl status mariadb` to look if is enable and had start. If not use the same command changing to enable and start, to start the service.



```
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  
    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.
```

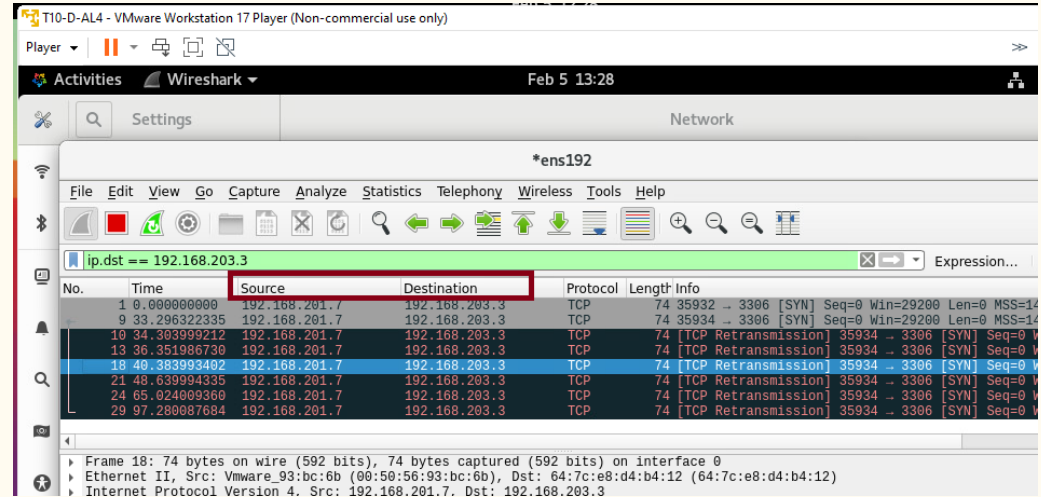
We experienced connections problems from the DMZ with the database in the secure zone.

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.

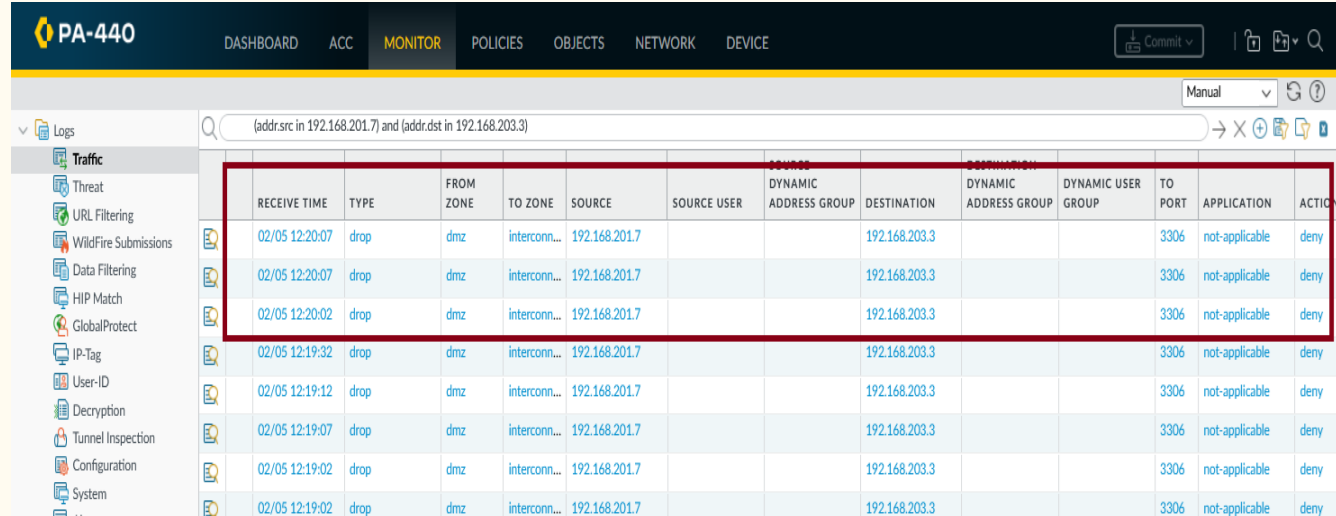


In the Palo Alto firewall the packages were dropped, and not allowed.

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.



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.

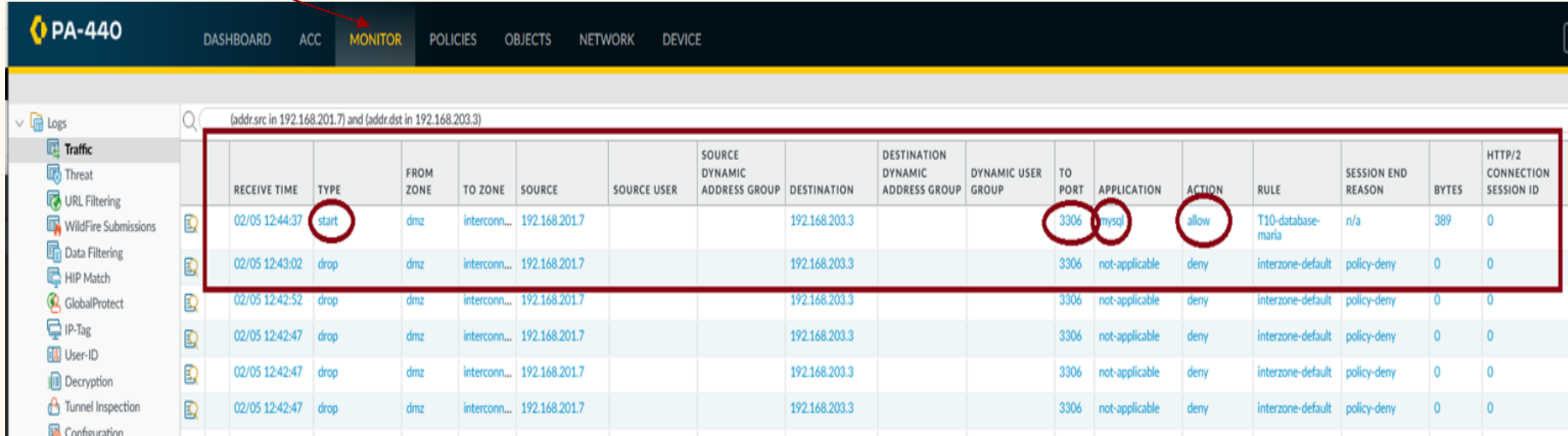
The screenshot shows the Palo Alto Networks PA-440 Security Policies configuration page. The 'Policies' tab is selected. A table lists 11 security rules. Rule 9, 'T10-database-mysql', is highlighted in grey, indicating it is disabled. At the bottom, the 'Enable' button is highlighted with a red box. The interface includes a left sidebar with navigation options like NAT, QoS, and Policy Based Forwarding, and a top navigation bar with tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device.

	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT	LAST HIT	FIRST HIT
1	rule1	none	universal	any	trust	any	any	any	trust	any	any	any	Allow	none		0	-	-
2	T10-outbound	none	universal	dmz	inside	192.168.201.0/24	any	any	outside	any	any	application...	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	inside	192.168.201.0/24	any	any	inside	192.168.202.0/24	any	ms-ftp	Allow	none		62	2024-01-27 05:46:41	2024-01-22 12:12:08
4	T10-inside-to-dmz-all	none	universal	inside	dmz	192.168.202.0/24	any	any	dmz	192.168.201.0/24	any	application...	Allow	none		102	2024-01-27 13:29:54	2024-01-22 11:49:52
5	T10-secure-to-dmz-inside	none	universal	interconnect	dmz	192.168.203.0/24	any	any	dmz	192.168.201.0/24	any	application...	Allow	none		15103	2024-02-05 12:54:43	2024-01-24 11:54:48
6	T10-squid-proxy	none	universal	interconnect	dmz	192.168.203.0/24	any	any	dmz	192.168.202.0/24	any	service-squid	Allow	none		1914	2024-02-05 12:54:43	2024-02-02 17:12:50
7	T10-to-Secure-Remote-Admin	none	universal	dmz	inside	192.168.201.0/24	any	any	interconnect	192.168.202.0/24	any	ms-ftp	Allow	none		105	2024-01-27 14:27:10	2024-01-24 12:07:45
8	T10-web	none	universal	outside	dmz	any	any	any	dmz	157.201.22.72	any	web-browsing	Allow	none		1031	2024-02-05 12:53:10	2024-02-02 17:13:44
9	T10-database-mysql	none	universal	dmz	interconnect	192.168.201.7	any	any	interconnect	192.168.203.5	any	mysql	Allow	none		5	2024-02-05 12:44:36	2024-02-02 23:35:43
10	Interzone-default	none	interzone	any	any	any	any	interzone	any	any	any	any	Allow	none		10414	2024-02-05 13:10:08	2024-01-20 23:31:59
11	Interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none		1953	2024-02-05 13:07:39	2024-01-22 10:37:08

At the bottom of the interface, the 'Enable' button is highlighted with a red box. The interface also includes a left sidebar with navigation options like NAT, QoS, and Policy Based Forwarding, and a top navigation bar with tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device.

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.



PA-440

DASHBOARD ACC **MONITOR** POLICIES OBJECTS NETWORK DEVICE

Logs (addr.src in 192.168.201.7) and (addr.dst in 192.168.203.3)

	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-deny	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-deny	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-deny	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-deny	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-deny	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

