MariaDB Authentication (PC)

Thank you for your interest in authenticated scanning! When you configure and use authentication, you get a more in-depth assessment of your hosts, the most accurate results and fewer false positives. This document provides tips and best practices for setting up MariaDB authentication for compliance scans.

A few things to consider

Why should I use authentication?

With authentication we can remotely log in to each target system with credentials that you provide, and because we're logged in we can do more thorough testing. This will give you better visibility into each system's security posture. Is it required? Yes, it's required for compliance scans.

Are my credentials safe?

Yes, credentials are exclusively used for READ ACCESS ONLY to your system. The service does not modify or write anything on the device in any way. Credentials are securely handled by the service and are only used for the duration of the scan.

Which technologies are supported?

For the most current list of supported authentication technologies and the versions that have been certified for VM and PC by record type, please refer to the following article:

Authentication Technologies Matrix

What are the steps?

First, set up a MariaDB user account and privileges (on target hosts) for authenticated scanning. Then, using Qualys Policy Compliance, complete these steps: 1) Add a MariaDB authentication record. 2) Launch a compliance scan. 3) Run the Authentication Report to find out if authentication passed or failed for each scanned host.

MariaDB Credentials

We've provided a set of scripts below to help you set up an account and privileges which must exist prior to running scans. These scripts require a super-user account. For example, root, or Administrator. Please run the scripts provided, in the order shown.

On-premise MariaDB Database

See the links below for quick sets of scripts for Amazon and Azure. For more details, refer to the full set of permission for scanning on-premise MySQL databases.

Amazon RDS for MariaDB

Azure Database for MariaDB

On-premise MariaDB Database

1) Create a User Account within the 'mysql' Database

This script creates a user account, called QUALYS_SCAN. Please provide a password before running the script. The usage of the '%' is required due to the fact that we are creating a remote user that can be run from our scanners.

CREATE USER 'QUALYS_SCAN'@'%' IDENTIFIED BY '[enter password here]' ;

NOTE – Creating a MariaDB user account this way does create some risk as we are using a wildcard for the host value. This generic way assures us that we will be able to successfully scan your database installation.

There are other ways of creating a user account that assumes more security. MariaDB allows you to create a user account using either an IP address or variations of sort. One way of doing this is figuring out what your Qualys scanner appliance IP address is and creating the user account that way. For example, if the scanner IP is 192.168.100.1, then the script would look like this:

CREATE USER 'QUALYS_SCAN'@'192.168.100.1' IDENTIFIED BY '[enter password here]' ;

You can also use a subnet, providing your database server(s) and the Qualys scanner are located within it. Using the wildcard, you can create the user account in various ways:

CREATE USER 'QUALYS_SCAN'@'192.168.100.%' IDENTIFIED BY '[enter password here]' ;
or
CREATE USER 'QUALYS_SCAN'@'192.168.%.%' IDENTIFIED BY '[enter password here]' ;

Another way to provide a more secure connection would be to address your network layer. By adjusting your firewall ACLs you could safeguard against any unwanted activity.

SSL Authentication

There is also SSL support for MariaDB authentication. Not only can server SSL certificates be setup and enforced in the MariaDB authentication record, but we also support additional security with the client SSL certificate, which can be configured for the QUALYS_SCAN user. By modifying the user, within the mysql.user table, to accept the client SSL certificate, there are multiple restrictions that can be added to increase security.

The MariaDB auth record allows adding optional client SSL certificate and the private key.

2) Grant Privileges to the Scan Account

This script grants privileges to the user account to be used for scanning. The following privileges are required for successful authentication and compliance scanning.

GRANT SELECT ON mysql.user TO QUALYS_SCAN;
GRANT SELECT ON mysql.db TO QUALYS_SCAN;
GRANT SELECT ON mysql.table_privs TO QUALYS_SCAN;

After performing these GRANTS, you'll need to flush the privileges in order to repopulate the grant tables:

FLUSH PRIVILEGES;

3) Check Privileges on the Scan Account

We provide a script in the zip archive to help you identify missing privileges from the user account to be used for scanning. These scripts are in the files QG_MariaDB_Auth_verx.x.txt. The script should be executed by a super-user against a database to determine if all the appropriate privileges have been setup correctly. The script will generate an output listing the status of all the prerequisites.

Sample Output

```
+-------------------+-----------------------------------------+
| Prerequisites     | Status                                  |
+-------------------+-----------------------------------------+
| root@localhost    | <---Current logged on user              |
| QUALYS_SCAN       | PASSED - account exists                 |
| USER              | PASSED - SELECT privilege exists        |
| DB                | PASSED - SELECT privilege exists        |
| PLUGINS           | PASSED - SELECT privilege exists        |
| SLAVE_MASTER_INFO | FAILED - SELECT privilege does not exist |**
| TABLES_PRIV       | PASSED - SELECT privilege exists        |
+-------------------+-----------------------------------------+
```

** It is worth noting, that if you do NOT have replication setup, the entry for SLAVE_MASTER_INFO will have a status of 'FAILED'. Not to worry, the scans will still execute.

Amazon and Azure

Here are quick sets of scripts for setting up a user account in Amazon and Azure. For more details, please refer to the full set of permissions for scanning on-premise MariaDB databases.

Amazon RDS for MariaDB

Please note that this same script applies to MySQL, MariaDB, and Amazon Aurora (MySQL-compatible).

```
CREATE USER 'QUALYS_SCAN'@'%' IDENTIFIED BY '[password]' ;
GRANT SELECT ON mysql.user TO QUALYS_SCAN;
GRANT SELECT ON mysql.db TO QUALYS_SCAN;
GRANT SELECT ON mysql.tables_priv TO QUALYS_SCAN;
FLUSH PRIVILEGES;
```

Azure Database for MariaDB

```
CREATE USER 'QUALYS_SCAN'@'%' IDENTIFIED BY '[password]' ;
GRANT SELECT ON mysql.user TO QUALYS_SCAN;
GRANT SELECT ON mysql.db TO QUALYS_SCAN;
GRANT SELECT ON mysql.tables_priv TO QUALYS_SCAN;
```

For Azure Database for MariaDB, please indicate username in authentication record in <username@hostname> format.

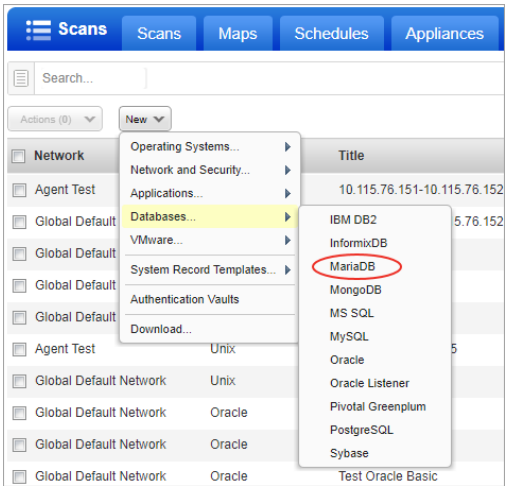
Remember to update connection security to allow scanner's IP to access the databases in Azure.

MariaDB Authentication Records

You'll need to create a separate authentication record for each MariaDB instance to be scanned. During scanning we'll authenticate to one or more MariaDB instances on a host using all the MariaDB authentication records in your account.

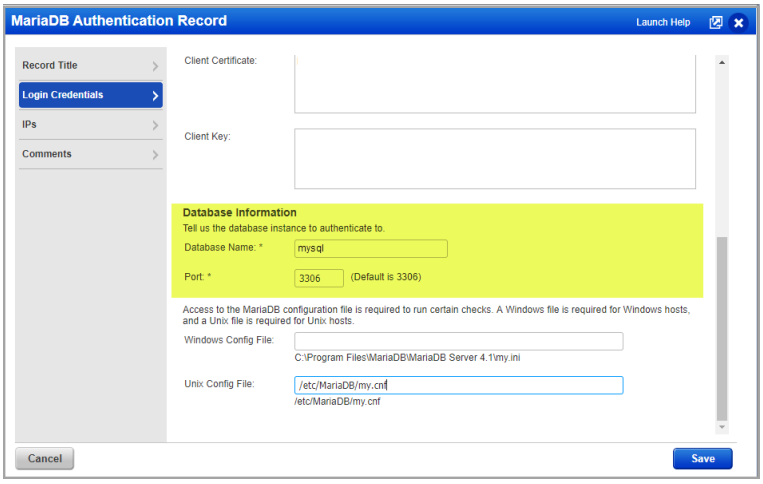
Where do I create records?

Go to Scans > Authentication > New > Databases > MariaDB Record.



What database information is required?

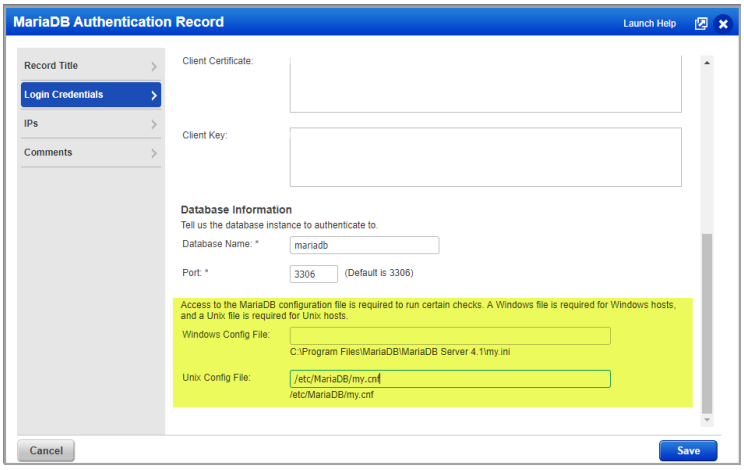
Tell us the database name to authenticate to and the port the database is running on (or use the default database name and port).



Tip – Please keep in mind that MariaDB actively protects from port scanning by maintaining an unsuccessful login counter. An attempt to connect to a MariaDB port without completing a successful login will increment this counter. Administrators need to be aware of this because eventually the server will stop accepting TCP connections to the database. It is recommended that Administrators issue a 'mysqladmin flush-hosts' command to reset the counter and look into possibly raising the counter number which may be set too low.

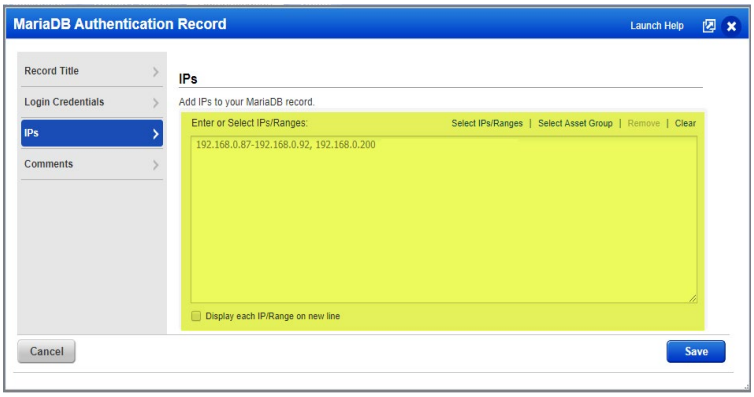
Your MariaDB configuration file

It is essential, though not required, that you provide the location of the MariaDB configuration file within the authentication record. This file is required for certain checks. For Unix & Windows, this file helps us gather the information needed to provide the information you are looking for.



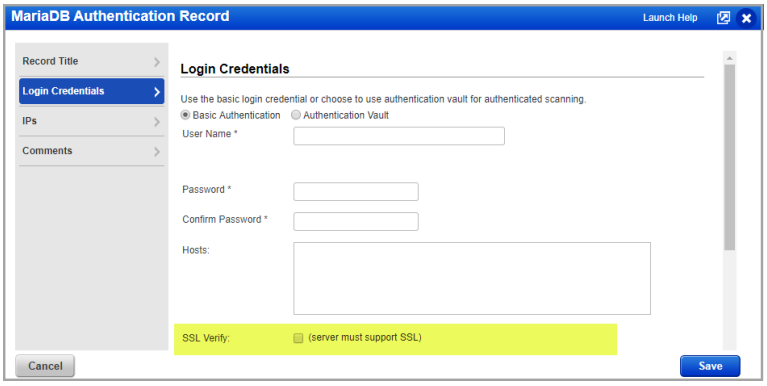
Add IPs to the record

Select the IP addresses for the MariaDB databases that the scanning engine should log into using the provided credentials.



Should I use SSL?

Using SSL provides a secure connection to your database. By selecting “SSL Verify”, and if your database server supports SSL, you will be requesting a SSL secured link. The server SSL certificate verification is also enforced. By default, this option is set to false.



Last updated: May 27, 2022