# Apply filters to SQL queries

## Project description

This project simulates simple log and employee data lookups that a junior analyst might run during an investigation. Using basic SQL filters I retrieve after-hours failed logins, searches for specific dates, country-based exclusions, and department-based employee lists to narrow data for follow-up. The queries demonstrate how to reduce noise and find relevant records quickly so an analyst can build an evidence set or create a report.

## Retrieve after hours failed login attempts

SELECT \*

FROM log\_in\_attempts

WHERE login\_time > '18:00' AND success = 0;



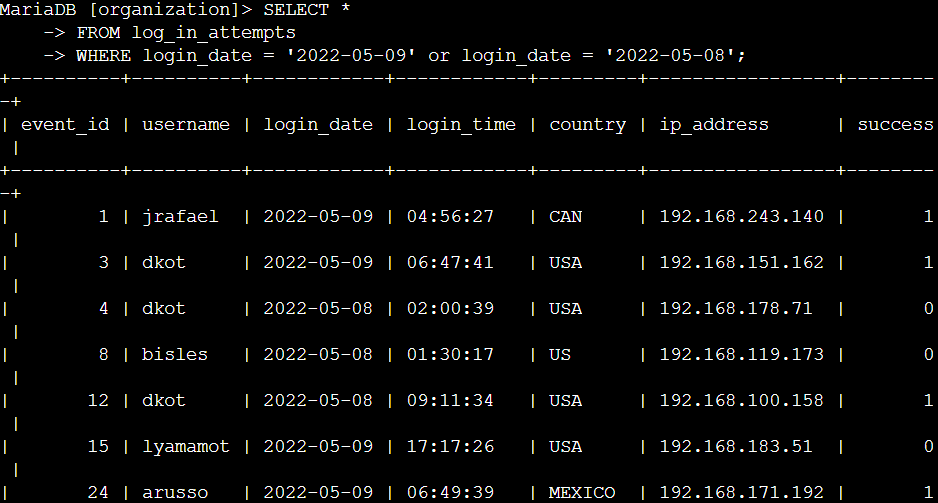
This query selects every column from the log\_in\_attempts table for rows where the recorded login time is later than 18:00 and the success flag equals 0 (meaning the attempt failed). In practice this finds failed authentication attempts that happened after working hours, which is useful to spot suspicious activity outside normal shifts. Using SELECT \* returns all fields for each matching row so we can inspect time, user, IP, and any other available columns.

## Retrieve login attempts on specific dates

SELECT \*

FROM log\_in\_attempts

WHERE login\_date = '2022-05-09' OR login\_date = '2022-05-08';



This command returns all columns from log\_in\_attempts for events that occurred on either 2022-05-09 or 2022-05-08. The OR allows matching multiple specific dates, which is handy when you know the incident window and want to see every login attempt on those days. You could later replace the two OR conditions with IN(...) or a BETWEEN if you need a larger continuous range.

## Retrieve login attempts outside of Mexico

SELECT \*

FROM log\_in\_attempts

WHERE not country LIKE 'MEX%';



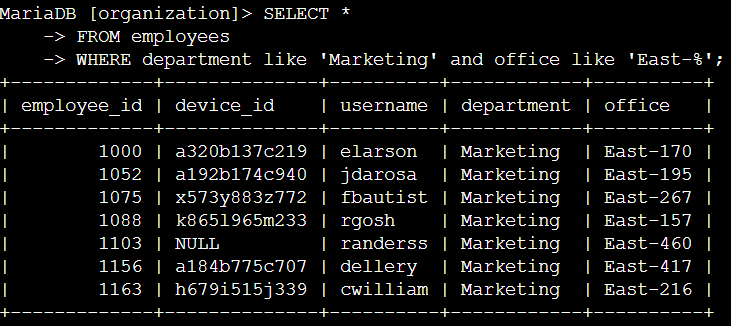
Here we select all records where the country column does not start with MEX. The LIKE 'MEX%' checks for values that begin with MEX (for example MEX or MEX-XX) and the NOT negates that test, so the result shows login attempts originating from countries other than Mexico. This is useful to filter out expected local traffic and focus on foreign sources.

## Retrieve employees in Marketing

SELECT \*

FROM employees

WHERE department like 'Marketing' and office like 'East-%';



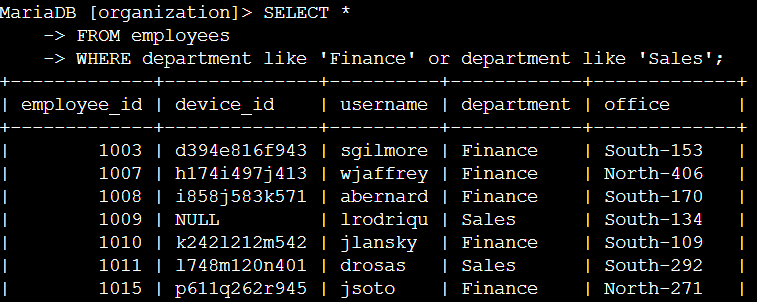
This query returns all columns from the employees table for rows where the department equals Marketing and the office value starts with East-. The LIKE 'Marketing' here behaves like an equality check (but can handle patterns), while office like 'East-%' matches any office name beginning with East- (for example East-170 or East-195 …). Combining the two conditions with AND ensures both department and office criteria must be true.

## Retrieve employees in Finance or Sales

SELECT \*

FROM employees

WHERE department like 'Finance' or department like 'Sales';



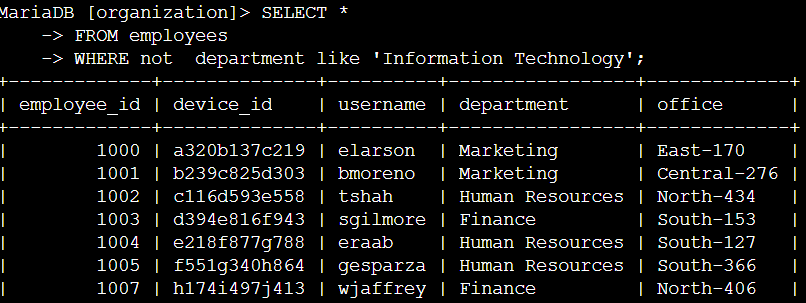
This command pulls all employee records whose department matches either Finance or Sales. The OR operator means a row is included if it satisfies at least one of the department tests. This is a simple way to get staff lists for multiple departments when you want to include both groups in a single result set.

## Retrieve all employees not in IT

SELECT \*

FROM employees

WHERE not department like 'Information Technology';



This query selects every employee whose department field does not match Information Technology. The NOT operator in front of the LIKE excludes IT personnel from the results, which can be useful when you need a list of non-IT staff for communications or for narrowing investigations away from administrative/system accounts.

## Summary

In this exercise we practiced basic SQL filtering techniques that let an analyst focus large log or personnel tables down to relevant subsets. By using filters such as time comparisons, date matching, LIKE, NOT, AND, and OR, we can quickly find after-hours failures, narrow by date or country, and pull department-based employee lists. These simple queries help form the first step of an investigation by producing manageable evidence sets that can be reviewed, exported, and attached to incident tickets.