

# Appliquer des filtres aux requêtes SQL

## Description du projet

L'entreprise pour laquelle je travaille s'efforce de rendre son système plus sûr. Il est de mon devoir de veiller à ce que le système soit sûr, d'enquêter sur tous les problèmes de sécurité potentiels et de mettre à jour les ordinateurs des employés si nécessaire. Les étapes suivantes offrent des exemples de la manière dont j'ai utilisé SQL avec des filtres pour effectuer des tâches relatives à la sécurité.

## Récupérer les tentatives de connexion échouées après les heures d'ouverture

```
MariaDB [organization]> SELECT *  
-> FROM log_in_attempts  
-> WHERE login_time > '18:00' AND success = FALSE;
```

event_id	username	login_date	login_time	country	ip_address	success
2	apatel	2022-05-10	20:27:27	CAN	192.168.205.12	0
18	pwashing	2022-05-11	19:28:50	US	192.168.66.142	0
20	tshah	2022-05-12	18:56:36	MEXICO	192.168.109.50	0

Un incident de sécurité potentiel s'est produit après les heures de travail (après 18 h 00). J'ai filtré les tentatives de connexion échouées ayant eu lieu après cette heure pour en faciliter l'enquête. J'ai utilisé une clause **WHERE** avec **AND** pour extraire les tentatives de connexion après 18 h 00 (**login\_time > '18:00'**) et celles qui ont échoué (**success = FALSE**).

## Récupérer les tentatives de connexion à des dates spécifiques

```
MariaDB [organization]> SELECT *  
-> FROM log_in_attempts  
-> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
```

event_id	username	login_date	login_time	country	ip_address	success
1	jrafael	2022-05-09	04:56:27	CAN	192.168.243.140	0
3	dkot	2022-05-09	06:47:41	USA	192.168.151.162	0
4	dkot	2022-05-08	02:00:39	USA	192.168.178.71	0

Un événement suspect est survenu le 09/05/2022, et j'ai dû examiner les connexions du **08/05/2022** et du **09/05/2022**. J'ai filtré ces tentatives en utilisant une clause **WHERE** avec **OR** pour obtenir les tentatives effectuées à ces dates précises (**login\_date = '2022-05-09'** et **login\_date = '2022-05-08'**).

## Récupérer les tentatives de connexion en dehors du Mexique

```
MariaDB [organization]> SELECT *
-> FROM log_in_attempts
-> WHERE NOT country LIKE 'MEX%';
```

event_id	username	login_date	login_time	country	ip_address	success
1	jrafael	2022-05-09	04:56:27	CAN	192.168.243.140	0
2	apatel	2022-05-10	20:27:27	CAN	192.168.205.12	0
3	dkot	2022-05-09	06:47:41	USA	192.168.151.162	0

Après analyse, il semblait que des tentatives de connexion avaient lieu en dehors du Mexique. J'ai donc utilisé une requête SQL pour filtrer les connexions hors Mexique en employant **NOT** et **LIKE MEX%** afin de capturer toutes les tentatives provenant d'autres pays.

## Récupérer les employés du Marketing

```
MariaDB [organization]> SELECT *
-> FROM employees
-> WHERE department = 'Marketing' AND office LIKE 'East%';
```

employee_id	device_id	username	department	office
1000	a320b137c219	elarson	Marketing	East-170
1052	a192b174c940	jdarosa	Marketing	East-195
1075	x573y883z772	fbautist	Marketing	East-267

Mon équipe devait mettre à jour les ordinateurs des employés du service marketing situés dans le bâtiment Est. J'ai utilisé une clause **WHERE** avec **AND** pour filtrer les employés du département marketing (**department = 'Marketing'**) et ceux ayant un bureau dans le bâtiment Est (**office LIKE 'East%'**).

## Récupérer les employés des services finances (Finance) ou commerciaux (Sales)

```
MariaDB [organization]> SELECT *
-> FROM employees
-> WHERE department = 'Finance' OR department = 'Sales';
```

employee_id	device_id	username	department	office
1003	d394e816f943	sgilmore	Finance	South-153
1007	h174i497j413	wjaffrey	Finance	North-406
1008	i858j583k571	abernard	Finance	South-170

Une mise à jour distincte devait être effectuée sur les ordinateurs des employés des services financier et commercial. J'ai utilisé une clause **WHERE** avec **OR** pour récupérer tous les employés travaillant dans l'un ou l'autre de ces départements (**department = 'Finance'** ou **department = 'Sales'**).

## Récupérer tous les employés qui ne sont pas dans l'informatique (IT)

```
MariaDB [organization]> SELECT *
-> FROM employees
-> WHERE NOT department = 'Information Technology';
```

employee_id	device_id	username	department	office
1000	a320b137c219	elarson	Marketing	East-170
1001	b239c825d303	bmoreno	Marketing	Central-276
1002	c116d593e558	tshah	Human Resources	North-434

Il fallait aussi effectuer une mise à jour sur les ordinateurs des employés ne faisant pas partie du service informatique. J'ai utilisé une clause **WHERE** avec **NOT** pour exclure les employés du service IT (**department != 'IT'**).

## Synthèse

En appliquant des filtres SQL, j'ai pu extraire des informations spécifiques sur les tentatives de connexion et les ordinateurs des employés. J'ai utilisé les opérateurs **AND**, **OR**, **NOT**, ainsi que **LIKE** avec des modèles, pour affiner mes recherches dans les tables **log\_in\_attempts** et **employees**, répondant ainsi aux besoins de l'entreprise en matière de sécurité.