MS SQL Queries How To Guide

Contents

Overview

When a MS SQL database of Swivel information is used it contains some information that is not available through the Swivel Administration Console. The majority of MySQL queries can be run against the MS SQL database with some exceptions. This document outlines some of the information that can be queried.

The **Audit Log** is where Swivel maintains an activity log for users. For more information on the Audit Log feature within Swivel, see the Audit Log How To Guide. For information on producing reports through the Swivel Administration console see Reporting How to guide.

For information on querying the Internal Swivel database see Reporting Using Agent-XML How to Guide

For information on MySQL database queries see MySQL Queries How To Guide. For information on using MS SQL as a database see MS SQL Database How To Guide

Prerequisites

- MS SQL Database;
- Audit log requires Swivel 3.4 or higher (for SQL queries on Swivel versions prior to Swivel 3.4 see the note at the bottom of the document).

Performing MS SQL Queries

Refer to the MS SQL documentation for performing MS SQL queries.

Some differences between MySQL and MS SQL queries

The equivalent function to NOW() in MS SQL Server is GETDATE(). However, SQL Server doesn't support the INTERVAL command either, so the DATEDIFF is used instead.

Querying individual Repositories

Each Repository may be queried my name or Repository ID. To find a Repository ID user:

SELECT A ID, B NAME FROM PINSAFEL

To query by NAME the following is used:

AND PINSAFEL.B = <NAME>

To query by ID the following is used:

AND I = <ID>

Example

Users who have never logged on (Successfully), for all repositories

USE pinsafe_rep; SELECT H Username FROM PINSAFEJ WHERE G NOT IN (SELECT DISTINCT A FROM PINSAFEN WHERE C=0)

Users who have never logged on (Successfully), for repositories <NAME>, Replace <NAME> with the name of the repository.

SELECT H Username FROM PINSAFEJ INNER JOIN PINSAFEL WHERE PINSAFEJ.I = PINSAFEL.A WHERE PINSAFEJ.G NOT IN (SELECT DISTINCT A FROM PINSAFEN WHERE C=0) AND PINSAFEL.B = <NAME>

Users who have never logged on (Successfully), for repository <ID>, Replace <ID> with the ID of the repository.

SELECT H Username FROM PINSAFEJ WHERE G NOT IN (SELECT DISTINCT A FROM PINSAFEN WHERE C=0) AND I = <ID>

MS SQL Queries

Count the number of users who have never logged in over the last 30 days but created more than 30 days ago

SELECT COUNT(*) FROM PINSAFEJ U JOIN PINSAFEN A1 ON U.G = A1.A AND A1.C = 3 LEFT OUTER JOIN PINSAFEN A2 ON U.G = A2.A AND A2.C=0 WHERE (A1.D < DATEADD(day, -30, GETDATE())) AND (A2.D IS NULL OR A2.D < DATEADD(day, -30, GETDATE()))

Show the number of users who have never logged in over the last 30 days but created more than 30 days ago

SELECT U.H FROM PINSAFEJ U JOIN PINSAFEN A1 ON U.G = A1.A AND A1.C = 3 LEFT OUTER JOIN PINSAFEN A2 ON U.G = A2.A AND A2.C=0 WHERE (A1.D < DATEADD(day, -30, GETDATE())) AND (A2.D IS NULL OR A2.D < DATEADD(day, -30, GETDATE()))

Troubleshooting

Are we able to isolate which regional Swivel server the user has logged in on from the database?

No not though SQL queries. However this information is available in the Swivel logs and obtainable through a log parser. Depending on how the Swivel agent is configured, there is a 'source' option in the Agent XML. This stores the IP information of the user logging on and there is a field in the database to store this information.

Locked user account list shows some users as not locked

The locked user count will report not only those that are flagged as locked but those accounts that have more than the number of failed authentications. When the user who has exceeded the maximum login attempts but whose account is not marked locked, next tries to login, the account will be marked as locked.