

Monitoring Queries

IP Related Queries

List Blocked IP per Users
<pre>select event_timestamp, user_name, client_ip, reported_client_type reported_client_version, first_authentication_factor, second_authentication_factor from login_history where error_message = 'INCOMING_IP_BLOCKED' order by event_timestamp desc;</pre>
IPs where login failures are most often coming from
<pre>select distinct client_ip, count(client_ip) from login_history where is_success='NO' group by client_ip;</pre>
Most blocked IP addresses
<pre>select distinct client_ip as blocked_source_ip ,count (client_ip), user_name ,reported_client_type as driver ,first_authentication_factor as authn_type from login_history where error_message = 'INCOMING_IP_BLOCKED' group by user_name, client_ip, reported_client_type, first_authentication_factor order by count (client_ip) desc</pre>
Monitor Network Policies
<pre>select end_time, query_type, query_text, user_name, role_name from query_history where execution_status = 'SUCCESS' and query_type in ('CREATE_NETWORK_POLICY', 'ALTER_NETWORK_POLICY', 'DROP_NETWORK_POLICY') or (query_text ilike '% set network_policy%' or query_text ilike '% unset network_policy%') order by end_time desc;</pre>