BP4SM Audit

Greg Baker (gregb@ifost.org.au)

August 22, 2012

1 Introduction

Audit rules are configured to make the Audit functionality easy and flexible. The system logs historic changes to tickets in order to help trace information for reviews.

2 Looking at an existing Audit Rule

1. From the Service Manager System Navigator, go to **System Administration → BP4SM Administration Audit Specifications**.
2. For the Table Name, enter `probsummary`, and hit Search.
3. Make a note of some of the fields being audited (e.g. Assignment, Status.

3 Looking at the implementation of an Audit Rule

Auditing is implemented not as a background service, but by a trigger which is run before each update.

In general, most triggers of this kind are named **before.***tablename***.update**, although a few are named **before.update.***tablename*, and a few follow no particular convention at all.

1. In the command box (in the Windows client this is just underneath the ''Window'' menu; in the web client, this is near the top on the right-hand side), type `triggers`.
2. Select a trigger type of `3 - Before Update` and hit ''Search''.

3. Look through the list of existing triggers and look for some common tables, and what triggers are defined.

4. Find the `before.probsummary.update` trigger. Notice the script which it calls:

   ```
   system.library.BP4SM_Audit.addHistory(oldrecord,record,''probsummary'',record.categ
   ```

5. Now look for this JavaScript in the Script Library. In the command box, type `sl`.

6. In the ‘‘Name’’ field, enter ‘‘=BP4SM_Audit’’ and hit search.

7. Find the function `addHistory` (it should start on line 24). If you can read JavaScript, browse through the program code to see how it works.

8. Notice on line 165 that this function creates a new `activity` entry.

   ```
   var result = NewActivity.doInsert();
   ```

4 Testing an Audit Rule

1. If you don't have an existing incident, create an new one (**Incident Managment** → **Open New Incident**). Hit Submit to make sure there is a record.

2. Modify the assignment group of an incident ticket and hit save. Make a note of the Incident ID.

3. Enter ‘‘db’’ in the command box to bring up the database manager.

4. We want to look for records in the `activity` table, so enter ‘‘activity’’ in the Table field. The easiest-to-use form for searching is ‘‘activity.post’’ – enter this in the Form field. Hit the search icon (the flashlight icon).

5. In the number field, enter the name of the Incident ID you recorded above. Hit search.

6. A list of activity records should appear, sorted with the most recent activity at the top. Your assignment group change should appear at the top.

5 Adding an audit record to a table which is already triggered

You have discovered that staff are changing the titles of incident tickets, and you would like to understand better when this is happening and who is doing it. You decide to turn on auditing of the title field in incident tickets.

1. From the Service Manager System Navigator, go to **System Administration → BP4SM Administration Audit Specifications**.
2. For the Table Name, enter `probsummary`, and hit Search.
3. In the ‘‘Field Names’’ list, click in the first empty space. A dropdown box will appear. Select ‘‘Title’’ from the list.
4. Hit ‘‘Save’’. Notice that the Fields list suddenly adds ‘‘brief.discription’’ as an audited field.
5. Test your work by updating the title of an incident ticket. Follow the steps from section 4 to confirm that this has worked.

6 Challenge: adding an audit record to a currently-unaudited table

Hint 1: Look through the existing triggers for that table to find one which calls `system.library.BP4SM_Audit.addHistory`. If you can’t find anything, add one.

Hint 2: Create a new record in the `bpauditspecs` table for this table.