

Re: Audit logging an adp

Source:

<http://www.tech-archive.net/Archive/Access/microsoft.public.access.adp.sqlserver/2006-09/msg00021.html>

- *From:* Merlin <evalua@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 3 Sep 2006 16:32:01 -0700
-

Thanks David

Looks like there isn't going to be any easy solution.
Thanks for the sample code showing me how to get the value of Text fields.

"David Portas" wrote:

Merlin wrote:

Hello

I need to add an audit trail to an existing, large adp application, which was developed in AccessXP with a SQLServer 2000 backend.

I searched through all the Access pages and found numerous reference to Allen Browne's audit code.

This is very much the sort of log I would like to keep, but his solution won't work in an adp for a couple of reasons:

- * You need client side tempTables, which, as far as I can see, can not exist in an adp;
- * There are issues with event ordering; and
- * Autonumbering happens too late in new records to get the new ID.

I was wondering if anyone has adapted Allen Browne's solution for .ADPs, or if anyone can suggest an alternative method.

Some people may be tempted to suggest using SQL Server triggers, so I'll jump in early and say they won't help me for these reasons:

- * All connections to the SQL Server are done through a single account, so I can't get the user ID of the person making the change; and
- * Most of the tables contain NText and Text fields that will need to be auditted, and the triggers don't let you see the value of fields of that type

Thank you

Triggers are the obvious solution. You can easily detect updates to

Re: Audit logging an adp

TEXT columns using the UPDATE function. It is slightly harder to track actual changes to TEXT columns because they aren't exposed in the INSERTED and DELETED virtual tables but it can still be done by preserving the TEXT value for each update (see below).

By definition to accomplish any reliable kind of audit you need some form of access control. In a two-tier environment access control usually means some combination of either user roles, application roles and/or EXECUTE-only permission through procedures. If you aren't familiar with all these options then do read about users and roles in Books Online. It is not easy to add security as an afterthought because security needs to be factored in to your whole application architecture, but without an adequate security model your audit trail will be wide open to abuse.

In your case it sounds like you have your own application-level security model. To audit user activity you'll therefore have to pass the user name to a stored procedure for each auditable event or update it as a column value in each table you want to audit.

Hope this helps.

```
CREATE TRIGGER trg ON tbl for UPDATE, INSERT
AS
```

```
IF UPDATE(text_col)
BEGIN;
```

```
INSERT INTO dbo.audit (key_col,text_col)
SELECT key_col,text_col FROM dbo.tbl
WHERE EXISTS
(SELECT *
FROM inserted AS i
JOIN dbo.tbl AS t
ON i.key_col = t.key_col);
```

```
END;
```

```
GO
```

—
David Portas, SQL Server MVP

Whenever possible please post enough code to reproduce your problem. Including CREATE TABLE and INSERT statements usually helps. State what version of SQL Server you are using and specify the content of any error messages.

SQL Server Books Online:
[http://msdn2.microsoft.com/library/ms130214\(en-US,SQL.90\).aspx](http://msdn2.microsoft.com/library/ms130214(en-US,SQL.90).aspx)

—

Re: Audit logging an adp