FUJ00235322

From: Jenkins Gareth GI[/o=Exchange/ou=AdminGroup1/cn=Recipients/cn=Gareth.Jenkins]

Sent: Thur 30/05/2013 9:23:54 AM (UTC)

To: Newsome Pete[GRO]

Cc: Membery Bill[GRO]; Stewart Paul[GRO]; Davidson James[GRO]; Parker Steve (PostOfficeAccount)[GRO]; Tarran Keith[GRO]

Subject: RE: Audit trail - Branch database

Pete,

I don't have a problem with what Paul is saying. I also agree that it is unlikely that anyone with access to the data has the full skills to manipulate it cleanly and there is no incentive to do so.

However the point I had made to POL was that access to BRDB was audited and should be minimal (and therefore presumably fairly easy to prove).

I've spoken to Andy Beardmore and he tells me that any access to BRDB at the SQL level should be audited at the following audit point:

From DEV/INF/ION/0001 v10:

SP #	Sub Point	Audit Point	Gath 11	Gath 19	Gath 19DR	Sub Point Description
962	HOST	BRDB(69)	BRDB(6)	DUMMY(14)	BRDB(6)	HNG-X BRDB Oracle audit data

Therefore if required we could retrieve these audits and examine them.

However it may turn out that when we examine such audits that it isn't clear easy to relate info in the audit to what has occurred. I would suggest it is worh at least having a look and seeing how big this audit trail is.

I don't think we need to do any work on the integrity of BRDB. Our claim is that the Audit trail (recorded in BRDB_RX_MESAGE_JOURNAL) is tamperproof (because everything is signed by a key that is only know to the counter) and that all updates to BRDB can be derived from this audit. What we have never attempted to do is to do such a reconstruction.

Please note that Penny is no longer responsible for Audit retrievals. She has moved to SSC and any requests for Audit retrieval should go to Donna's replacement (Kumudu Amaratunga).

Hopefully he can answer the questions you posed to Penny below.

Regards

Gareth

Gareth Jenkins
Distinguished Engineer
Business Applications Architect
Post Office Account

FUJITSU
Lovelace Road, Bracknell, Berkshire, RG12 8SN
Tel: GRO Internal: GRO
Mobile: Internal:
email: GRO
Web: http://uk.fujitsu.com

FUJ00235322

From: Newsome Pete
Sent: 30 May 2013 09:20
To: Jenkins Gareth GI
Cc: Membery Bill; Stewart Paul; Davidson James; Parker Steve (PostOfficeAccount)
Subject: FW: Audit trail - Branch database

Gareth
In answer to Q3 below:

Could you have a look at Paul's email. The essence is that we could set up some sort of audit of access to the BRBD but this would be time consuming and expensive and potentially inconclusive as it will only show changes in the audit trail for the branches involved that Second Sight already have the raw data . Having shown our processes, security clearance of personnel and audit of our audit processes the more efficient and forensic method would be to identify when these transactions affected the branches in question. As it is easily identifiable (please confirm this statement is correct) when a manual change has been made in the audit trail we can then confirm the true situation.

If Alan has been able to identify and MSC we can then track how and who made a change to show our process in action.

Any thoughts?

Pete

Pete Newsome
Business Change Manager
Post Office Account, Fujitsu UK&I
Tel: GRO
E-Mail: GRO
Web: http://uk.fujitsu.com

From: Stewart Paul
Sent: 29 May 2013 20:08
To: Newsome Pete; Thomas Penny
Cc: Flack Alan J
Subject: RE: Audit trail - Branch database

Pete,

It would be worth checking my end to end view with Gareth Jenkins

FUJ00235322

Horizon is effectively two separate data processing engines.

Online transaction engine consisting of BRDB/NPS - with associated resilience (BDS) and reporting (BRS) databases
Reconciliation service - TPS/APS/DW/TES/DRS

In order to truly change the data you must have access and the business knowledge to alter the data associated with a transaction in each of the flows within a relatively small time window otherwise the transaction will not appear in the correct state at each of the reconciliation points. We also feed the raw data from our reconciliation databases (TPS) into reconciliation systems which are both operated by Fujitsu (POLSAP) and operated by third parties Credence. The APS reconciliation database sends Post Office clients transactional information on a daily basis.

Who has the access - SSC, Unix and DBA support have the required access to manipulate data - of the staff in these areas there is a very small subset that have the end to end business knowledge to know which tables would require altering to ensure that all of the records associated with a transaction are updated in each data source. Staff in the support teams are security checked by Fujitsu, those in the Unix support team have been SC checked via MOD. The level of fraud to make it worthwhile for any of our support staff to become involved would need to be significant. Counter transactions would not provide a suitable avenue for this type of fraud, in my opinion

What is the time window - Transactions are harvested from the BRDB database on a nightly basis into the TPS and APS databases - in real terms any transaction which occurs between 19:00:01 DAY A and 19:00:00 DAY B (19:00 is the notional end of trading day) are copied into the APS and TPS databases by automated processing effectively, a 24 hour window. However if the transaction involves a payment via the banking engine (NPS) the window narrows. We have a contractual SLA which ensures that all banking transactions are visible in the TES database within 15 minutes of the transaction being confirmed at the counter.

We provide the raw data from TPS to POLSAP and Credence they undertake their own processing of our raw data a separate reconciliation process.

If we focus on cash transactions there is a theoretical 24 hour window, but the other audit information from the counters and BRSS should highlight if a transaction has been updated.

We could spend a lot of time and resource requalifying the audit trail or we could focus on a targeted Post Office with a defined time frame - as narrow as possible. Producing all available reports and raw data from the pertinent databases. This is not an insignificant undertaking but it will be more cost effective than requalifying the audit trail.

Yours

Paul Stewart

From: Newsome Pete
Sent: 29 May 2013 17:33
To: Thomas Penny
Cc: Stewart Paul; Flack Alan J
Subject: FW: Audit trail - Branch database

Penny

FUJ00235322

These are the questions we are trying to answer:

I don't need the answers straight away just can we do it and how and then how long it will take.

Hope you can help.

Pete

1. ***For the last 24 months:***
    a. How many times has the branch database been updated directly
    b. For what reasons. For each time:
    c. What records were updated
    d. What records were added
    e. What records were deleted

Pete Newsome
Business Change Manager
Post Office Account, Fujitsu UK&I
Tel: GRO
E-Mail: GRO
Web: http://uk.fujitsu.com
P Please consider the environment - do you really need to print this email?

From: Newsome Pete
Sent: 29 May 2013 13:15
To: Thomas Penny
Cc: Flack Alan J; Jenkins Gareth GI; Flack Alan J
Subject: FW: Audit trail - Branch database

Penny

As part of the work we are doing with second sight to look at Horizon and HNGx Post Office has asked about any manual changes made to the database.

What we are trying to show is that any manual changes to the transactions stored in the database can be identified. Ideally we would like to be able to identify all manual changes in the last 2 years.

Are either, or both of the above possible? Any details on timings etc would be gratefully received.

Look forward to hearing from you.

Pete

Pete Newsome
Business Change Manager

FUJ00235322

Post Office Account, Fujitsu UK&I
Tel: GRO
E-Mail: GRO
Web: http://uk.fujitsu.com
P Please consider the environment - do you really need to print this email?

From: Stewart Paul
Sent: 29 May 2013 09:06
To: Newsome Pete
Cc: Flack Alan J
Subject: RE: Audit trail - Branch database

Pete

We should be able to track the actual change using the external audit system alongside the internal audit mechanisms. Penny Thomas should be able to give a more accurate overview of everything we capture in a transaction flow from the counter to reconciliation.

Yours

Paul Stewart

From: Newsome Pete
Sent: 29 May 2013 09:03
To: Stewart Paul
Cc: Flack Alan J
Subject: RE: Audit trail - Branch database

Paul

If asked I assume can we identify if a transaction was done manually in the audit trail when we view the data in more detail?

Pete

Pete Newsome
Business Change Manager
Post Office Account, Fujitsu UK&I
Tel: GRO
E-Mail: GRO
Web: http://uk.fujitsu.com
P Please consider the environment - do you really need to print this email?

From: Stewart Paul
Sent: 29 May 2013 08:28
To: Newsome Pete
Cc: Flack Alan J
Subject: RE: Audit trail - Branch database

FUJ00235322

Pete,

Sorry for the delay in responding, I was tied up all day with Brocade yesterday.

You are correct it would be very difficult to determine from BRDB, plus there a short retention of data in BRDB.

There may be value in getting SSC to confirm that they always raise an MSC for any changes to data prior to , plus confirmation that they actually change data in BRDB rather than correct data in the databases that perform the reconciliation activities. The MSC search may need to be wider than just BRDB.

Yours

Paul Stewart

From: Newsome Pete
Sent: 28 May 2013 10:59
To: Stewart Paul
Cc: Flack Alan J
Subject: RE: Audit trail - Branch database

Paul

Thanks you for looking at the problem. If I have interpreted this properly we would find it difficult to audit the BRDB to find manual changes? These would be useful to direct Alan at to look for the correct MSCs. We are interested in the last 24 months.

Regards

Pete

Pete Newsome
Business Change Manager
Post Office Account, Fujitsu UK&I
Tel: GRO
E-Mail: GRO
Web: http://uk.fujitsu.com

From: Stewart Paul
Sent: 24 May 2013 18:16
To: Newsome Pete
Subject: Audit trail - Branch database

Pete

FUJ00235322

Not sure if this is of any help -

We have auditing turned on in the various databases the items we audit are best discussed with Andy Beardmore and Pete Jobson. I can query the audit table and see what actions have been undertaken by individuals but only on those items targeted by the audit. I could run a simple query to determine which user has actively changed anything but I am not sure what value it has as it is unclear what is being audited.

We also deal with auditing in different ways on the various databases. Andy Beardmore would be best placed to explain the audit mechanisms we agreed.

Example below

From a previous discussion with a colleague I have the following example

This may help as an example of auditing from BRDB:

```
SQL> l
  1* select username, action_name, obj_name,  timestamp, logoff_time , returncode from dba_audit_trail where timestamp>trunc(sysdate) and
username ='OPS$IRRELEVANT order by timestamp
SQL> /

USERNAME                       ACTION_NAME                    OBJ_NAME                       TIMESTAMP           LOGOFF_TIME         RETURNCODE
------------------------------ ---------------------------- ------------------------------ ------------------- ------------------- ----------
OPS$IRRELEVANT                 LOGOFF                                                      08-MAY-2013 10:29:33 08-MAY-2013 10:29:35          0
OPS$IRRELEVANT                 LOGOFF                                                      08-MAY-2013 12:44:41 08-MAY-2013 12:47:32          0
OPS$IRRELEVANT                 LOGOFF                                                      08-MAY-2013 13:11:36 08-MAY-2013 13:14:39          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 13:12:18                        904
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 13:12:45                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 13:12:53                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 13:13:07                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 13:14:35                          0
OPS$IRRELEVANT                 LOGOFF                                                      08-MAY-2013 13:14:51 08-MAY-2013 13:33:43          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 13:17:04                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 13:17:55                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 13:17:58                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 13:18:10                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 13:19:07                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 13:20:26                          0
OPS$IRRELEVANT                 LOGON                                                       08-MAY-2013 13:59:07                        0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 15:21:38                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 15:22:05                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 15:22:28                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 15:23:55                        904
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 15:24:30                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 15:24:51                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 15:24:56                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 15:26:31                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 15:26:34                          0
OPS$IRRELEVANT                 SELECT                         AUD$                           08-MAY-2013 15:26:40                          0

26 rows selected.
```

So from above we can see that I logged onto BRDB at 10:29:33, 12:44:41, 13:11:36, 13:14:51 and 13:59:07 today (the last one shows I'm still logged on), it also shows me selecting from the AUD$ table successfully (the returncode 0 rows) and unsuccessfully (the returncode 904 rows).

The 904 refers to the ORA-00904 error:

```
IRRELEVANT ~]$ oerr ora 904
00904, 00000, "%s: invalid identifier"
// *Cause:
// *Action:
```

Which I got from typos in my SQL query, for example:

```
SQL> select objs_name from dba_audit_trail;
select objs_name from dba_audit_trail
       *
```

FUJ00235322

ERROR at line 1:
ORA-00904: "OBJS_NAME": invalid identifier

The column is actually OBJ_NAME.

The problem with the example is that it concentrates on the audit table rather than any of the transaction based tables.

Whilst we may be able to edit the data the reconciliation reports sent by the various data streams and systems (not just Fujitsu) would quickly high light unusual activity. For a simple DVLA Car tax purchase paid for by debit card - I think all of the following databases would need to tally for the transaction,

NPS - TES - BRDB - BRSS - APS - TPS

BRDB will feed APS and TPS databases but the NPS feeds TES in virtual real time - any banking transaction which passes through NPS must be visible within 15 minutes in TES.

Fraud at a transaction level would be complex and difficult. The best scenario for fraud would be for the cash deliveries but it would require external assistance to run the end to end fraud.

Paul Stewart
Principal Technical Services Specialist
Hosting & Network Services

FUJITSU
Trident House, 301 Airport Road West, Belfast BT3 9AE
Tel: GRO or Internally GRO
Mob: GRO or Internally GRO
E-mail: GRO
Web: http://uk.fujitsu.com

<< OLE Object: Picture (Device Independent Bitmap) >> << OLE Object: Picture (Device Independent Bitmap) >> << OLE Object: Picture (Device Independent Bitmap) >> << OLE Object: Picture (Device Independent Bitmap) >>