
From: Gauntlett, Paul[o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=20fad69c1be541619bbf58bbefdae198-Gauntlett,]
Sent: Wed 01/12/2021 11:50:57 AM (UTC)
To: Browell, Steven [GRO]
Cc: Barnes, Gerald [GRO]; Mistry, Manisha [GRO]; Boardman, Phil [GRO]
Subject: Historical Issue with Audit Data

Hi Steve

I am Migration Lead for the Audit Migration to AWS.

Myself and Gerald Barnes (Audit SME) are currently working with POL to define requirements for the migration of historical Audit data

An historical issue has been identified and is detailed below.

This issue was discussed yesterday with John Nelis the POL PM & also Dean Bessell who I understand is your POL opposite.

POL requested that we write up what was communicated in the meeting so they can take it to their legal team ahead of making a decision regarding the scope of the data to be migrated.

On that basis I don't wish to send anything over without it being reviewed and agreed by relevant parties. Happy to have a call to discuss further.

Problem Summary:

Post Office counter audit transaction files gathered prior to the HNGx software rewrite in 2010 are not consistent across both IRE11 & IRE19 servers. Holistically no data is missing but in rare instances transaction data exists only on one server or the other. The problem was caused by the occasional malfunction of the Harvester process of the previous Horizon system - Riposte.

Background:

Audit Gathering Method up to approx 2010

- Originally a system called Riposte was used to gather audit transactions from all the Post Office counters.
- Riposte was a big distributed database.
- At that time Riposte was deployed into Bootle & Wigan data centres.
- Each evening all Post Office counter transactions were harvested and stored in files.
- The Bootle audit server gathered Bootle transaction files and the Wigan audit server gathered Wigan transactions files.
- Different files were produced in each data centre. The files were different because although the same transactions were harvested they were processed in a different order and for different FADs. Filenames were also different.
- Although there was an option to robocopy files from one server it was switched off because there were already two copies of each transaction (one in each data centre).
- It is now known that due to the occasional malfunction of the Harvester process in one or other of the data centres transactions may be missing from the files gathered in that data centre.
- There is no recorded instance of both harvesters failing at the same time so although data may be missing from one server it will be present in the other.
- TBC - In a DR situation data could have been lost was this captured as an operational risk and communicated to POL?

Audit Gathering Method from 2010 onwards

- Around 2010 the contract came up for renewal.

- Fujitsu's proposal was a rewrite called HNGx which eliminated Riposte (for which there was a big annual licence fee).
- As a part of this rewrite each Post Office counter transaction was only processed into a one file on a single server.
- This drove the decision to change the Audit gathering approach.
- From this point forward all transaction and non-transaction files were gathered by the IRE11 Audit Server only and robocopied to the IRE19 Audit Server.
- Therefore from 2010 all audit files (transaction and non-transaction) are consistent across both audit servers.

Impact on ARQ requests

- When ARQ requests for a FAD code are made all relevant files are retrieved from the target audit server .
- Then the files are processed by the Query Manager service on the audit server.
- Each Horizon or HNGx transaction has a unique number associated with it. The Query Manager checks that the transactions
 - have not been tampered with
 - that there are no duplicates or gaps in the sequence of transactions.
- Due to the Riposte harvester issue, for ARQ queries from 2010 or earlier, there may be gaps in the results from one or other of the servers.
- If this occurs then a Peak is raised and the ARQ request is rerun on the other server. This resolves any issues with data gaps.
- There have been no reported instances of unsuccessful ARQ request once a query has been executed on the second server.

Regards,

Paul Gauntlett
Customer Solution Architect
Cloud Transformation & Development - AMCS

Fujitsu
Central Park, Northampton Road, Manchester, M40 5BP
United Kingdom

