FUJ00176517

From: Barnes, Gerald[/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=E8B49E113CF64EE2BBE69D133846A7BE-BARNES, GER]
Sent: Sat 04/12/2021 8:28:12 PM (UTC)
To: Browell, Steven[GRO]; Kemp, Alex[GRO]; Holmes, Alan[GRO]; Gauntlett, Paul[GRO]
Cc: Muir, Jason[GRO]; Baker, Geoff[GRO]
Subject: RE: CONFIDENTIAL - Notes from our catch up earlier - ARQ focused

Hi Steve,

Answered in line.

Regards,
Gerald Barnes

From: Browell, Steven <GRO>
Sent: Friday, December 3, 2021 5:07 PM
To: Kemp, Alex <GRO>; Holmes, Alan <GRO>; Barnes, Gerald <GRO>; Gauntlett, Paul <GRO>
Cc: Muir, Jason <GRO>; Baker, Geoff <GRO>
Subject: CONFIDENTIAL - Notes from our catch up earlier - ARQ focused

All,

Below are my working notes. They are NOT a final outcome. Yellow text is where I am unsure on accuracy. Actions at the bottom. **Do not share this email** please.

ARQs - could we have shared a response to POL that had missing data as it was absent in the audit archive

Summary

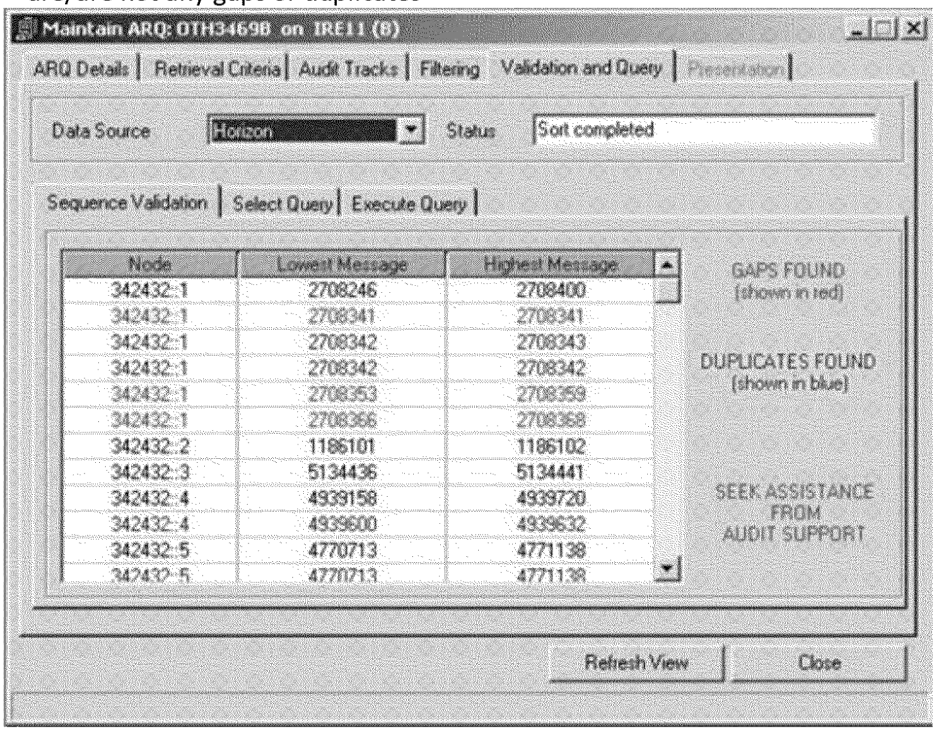
- Yes. However, if we did, it would have been shown within the ARQ response shared with POL **[to be confirmed]**

Detail

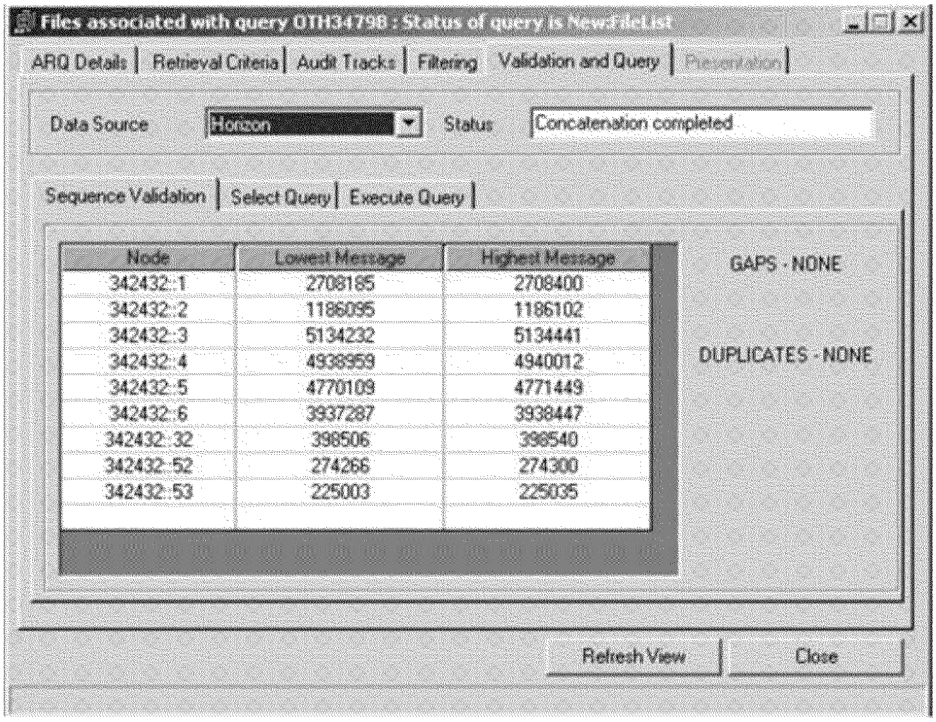
- Each ARQ is run by POA SecOps from a secure room using a bespoke AE client retrieval application
- An ARQ is fulfilled by a query executing within the Query Manager
- The Query Manager checks for the correct sequencing of JSNs
- JSNs are assigned by the counter and constantly advance as each transaction is processed
- JSNs are not reset, but after extended periods - perhaps c15 years - JSNs can loop back to start their counter again
- The ARQ query options are FAST or SLOW
- The ARQ query will run against one of the 2 Audit Archives (they are assumed to be identical)
- SLOW has always been available
- FAST was newly introduced in HNG-X R2 2011 by CP to automate additional event checks **[or did I misunderstand and this is when Windows event logs were included in the process with the intention of SSC review via Peak?]**
- POA SecOps use the FAST query by default
- A FAST ARQ query will abort if the sequence of JSNs has gaps
- A SLOW ARQ query will handle both gaps and duplicates in JSNs
- The SLOW query has looked for gaps and duplicates since **[date when the documentation said we did this - perhaps in DEV/INF/ION/0001 or DES/APP/HLD/0029]**
- The POA SecOps is alerted on the AE client screen when it has collated the result set to confirm if there

FUJ00176517

are/are not any gaps or duplicates



or



- If POA SecOps is alerted to gaps, and this is pre-HNG-X, they should rerun the SLOW query against the other archive as it is unlikely that BOTH archives will have gaps **[this relies on POA SecOps deciding to do this and could be subject to human error]**
- If POA SecOps is alerted to gaps, and this is HNG-X OR the second run against a pre-HNG-X archive, they should raise an Incident as this is not expected **[this relies on POA SecOps deciding to do this and could be subject to human error]**
- The gaps/duplicates alert will appear on the Summary tab of the Excel extract the AE Client creates
- The Summary tab will be shared with POL so they will know if there are any gaps or duplicates **[we need to ensure that the SLOW query has always reported on gaps before we can say this]**

FUJ00176517

- The POA SecOps team record the details of the ARQ requested by POL and also the type of query run (FAST/SLOW) and the archive against which the result set was derived. Notes can also be added. We have records going back to 2004 in an old MS Access database, from 2014 we have good excel records. Our ability to access to MS Access databases has been an issue in the past as the version of MS Access the database was created in isn't compatible with modern versions of Windows
- POA no longer retain copies of ARQ responses sent to POL - they are permanently deleted once confirmed as received
- ARQ responses used to be saved on a secure drive which is held in the secure room. The NAS drive died around 2017, and around the same time a PCI audit finding advised us that we should no longer be keeping the ARQ spreadsheets as they contain PAN numbers, so we stopped storing them and deleted the spreadsheets once POL confirmed they had received a copy. We also around the same time deleted any copies of old ARQ spreadsheets we could find except for any that we were told to keep as a result of the litigation.

So we need to:

1. **Gerald** - Check whether checking for gaps has always been in the SLOW query used by POA SecOps - and if not, state the applicable dates it was [this will tell us if we have always known about this and have always been notifying POL - and will give us an idea if we were doing this prior to 2007 for which we no longer have records]

   I have only been working on audit since it was changed as a part of HNGx (2010 or thereabouts – I was actually the very last member of the Horizon counter team working on the migration of data from Horizon to HNGx before this – my work there finished when the last counter migrated). I started as a very junior member of the team but once I got into it a bit (within a year or so) I was fully aware that it checked the integrity of each transaction, whether there were GAPs and whether there were duplicates. For one reason or other I often tested that these things worked – for example I once gave a demonstration to auditors of all 3 and when doing the two migrations of audit I performed I always checked these still worked. Going back though versions of DEV/GEN/MAN/0015 "Audit Extraction Client User Manual" I see gaps were mentioned in the very first version 0.1 published on 24/01/09. However something did trouble me. Duplicates were not mentioned until you got to version 2.1 on 12/01/2011. Now duplicates are far more common than gaps. I have investigated a lot of gaps and duplicate reports from CSPOA. When asked to investigate I always ask them to raise a PEAK so that there is an audit trail. Going back though PEAK records so far I have only found 1 gap one but maybe 20 duplicate ones. In all cases of duplicates I investigated I found that the same transaction had been put in different TMS files and , as far as audit is concerned, correctly gathered. I developed special tooling to check these out. In all cases I checked out all duplicates were exactly that – complete and utter duplicates (not just the message number the same). Now (and presumably since 2011) duplicates are clearly reported on the spreadsheet. If the operator understands there are duplicates in the spreadsheet he is looking at all is well. However if he does not understand there are duplicates there is double accounting of transactions going on as far as he is concerned with no explanation. I am sorry to report that this might have serious implications. Note it is quite possible that the previous pre-HNGx audit system silently merged duplicates (I do not know for sure) but our present system definitely does not.

2. **Gerald** - Confirm that the gap checking applies to both pre-HNG-X extracts and HNG-X extracts

   I have been unable to find any documents on this but I did find PEAK PC0133634 from 20-Mar-2006 which clearly indicated to me that GAPS were reported. It attached spread sheets as evidence that are archived and I have asked them to be got back.

3. **Gerald** - confirm when the FAST query was introduced

   CP4867 (HNG-X CP0336) 02/03/2009. Not sure when it went live exactly.

FUJ00176517

4. **Gerald** - summarise what the FAST event checks are [so we can be clear why this query came into existence]

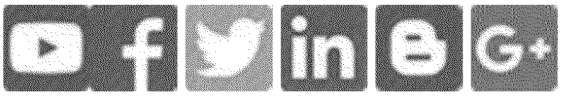
   Slow ARQs can do it too by the way. As an option (they do not use it now) all the events are got back for the time of the query. Then all critical/major events for the FAD in question and the BAL servers are checked against stored rules written in perl. If they are deemed benign they go into a csv file for optional examination else they go into a spreadsheet that will be definitely checked by the SSC. The SSC examine the spreadsheet and if they find that the new ones are benign too they inform the audit team and we amend the perl filters to exclude them in the future too.

5. **Geoff/Jason** - Collate the POA SecOps ARQ records from the earliest date to the present so it can be looked at (will include converting an old version of MS Access)
6. **Geoff/Jason** - Check the POA SecOps ARQ records to see if any have notes stating gaps were present [this will overtly show examples where we have alerted POL]
7. **Geoff** - check if there are any notes in the secure rooms that refer to gaps that we may want to check
8. **Geoff** - Identify the secure drive holding previous ARQ responses - may be controlled by Matt Lenton. We will need to provide very careful controls on the sharing of this data if it is deemed 'sensitive'
   a. **SSC** - identify the earliest and latest ARQ response dates on the secure drive [we will know the period for which we can provide more confident views - and this should go back prior to 2007]
   b. **SSC** - run a query against the data to find any files with "Gaps Found" on any Summary tabs [this will tell us ranges of dates when POL were alerted to gaps]
9. **Geoff/Jason** - Confirm that POA SecOps will re-run a query for gaps pre-HNG-X and will raise a ticket for gaps in a second run for pre-HNG-X or any gaps at all for HNG-X. Write this into the Work Instruction

Steve Browell
Post Office Account
Management Consultant & CISO

Fujitsu Enterprise & Cyber Security
Fujitsu Services, Trafalgar House, Temple Court, Risley, Warrington, Cheshire, WA3 6GD, United Kingdom

Mob: GRO
E-mail: GRO



Planned leave: 18 December 2021 – 04 January 2022