FUJ00173193

Export

Peak Incident Management System

Call Reference	**PC0280466**	Call Logger	Farzin Denbali -- Security Ops
Release	Targeted At -- HNG-X 19.51	Top Ref	AUDIT_QUERIES_V2_1951_D022-D021A
Call Type	Live Incidents	Priority	B -- Business restricted
Contact	Farzin Denbali	Call Status	Closed -- Administrative Response
Target Date	07/10/2019	Effort (Man Days)	3.00
Summary	Audit Data extract filtering failing for July 2015		

All References	Type	Value
	Release PEAK	PC0281542
	Product Baseline	WINDOWS_PERL_64_5P20_V2_1951_V002-V001
	Product Baseline	WINDOWS_PERL_64_5P20_V2_1951_D002-D001
	Clone Call	PC0280793
	Release PEAK	PC0281821
	DevIntRel-Director	Live Supp.Test
	Product Baseline	AUDIT_QUERIES_V2_1951_V022
	Product Baseline	WINDOWS_PERL_64_5P20_V2_1951_D002-D001A
	Release PEAK	PC0280892
	Product Baseline	WINDOWS_PERL_64_5P20_V2_1951_V002
	Product Baseline	AUDIT_QUERIES_V2_1951_D022-D021
	Jira	POA-3069
	Document	DEV/SPP/SPG/0020
	Product Baseline	AUDIT_QUERIES_V2_1951_V022-V021
	Product Baseline	AUDIT_QUERIES_V2_1951_D022-D021A
	Jira	POA-3067

Impact Statement	User	Date
	John Simpkins	14-Nov-2019 11:30:47

Problem Statement

Any ARQ containing financial data sent to the Post Office must have an accompanying check of any events raised. Currently a check is made that there is at least one event at the beginning of the range and an event at the end. Recently it was discovered that the files containing events were missing for many days and they were all in a bigger file at a later day. Because of this possibility the checking of events needs to change to there being a check that there is at least one event for every single day of the period in question.

Risk of not fixing:

It is possible a financial spread sheet will be sent to the Post Office with some relevant events not being checked by the SSC because there were no events in the file of events for one of the days of the spread sheet.

Benefit of fixing:

We can be sure that all events relevant to financial spread sheets sent to the Post Office have been checked.

ASM Utilization Capacity (Number of Man Days required to fix this issue) :

Another 3 days is required to fix this problem.

Progress Narrative

FUJ00173193

Date:**04-Oct-2019 14:10:34** User:**Farzin Denbali**
CALL PC0280466 opened
Details entered are:-
Summary:Audit Data extract filtering failing for July 2015
Call Type:L
Call Priority:B
Target Release:HNG-X Rel. Ind.
Routed to:PODG-Dev - Gerald Barnes

Date:**04-Oct-2019 14:10:34** User:**Farzin Denbali**
The Audit Data extract for July 01 to July 14 2015 fails with 'Filtering Failed' message. Perl Error log shows:

The supplied date Tue Jul 14 23:59:59 2015
minus the largest message date found 20150706 is greater than 1. Files need to be extracted with a bigger upper date.

I ran the ARQ for 2 branches and the result was the same. When ARQ is run for the entire month the query completes and the gaps in the Events data is visible. The Events spreadsheet shows there are no events between July 3 and July 10 (see attached) but there is transaction data between those dates.

Date:**04-Oct-2019 14:11:14** User:**Farzin Denbali**
Evidence **Added** - Perl Error

Date:**04-Oct-2019 14:11:28** User:**Farzin Denbali**
Evidence **Added** - Events

Date:**04-Oct-2019 14:17:24** User:**Jason Muir**
The Call record has been transferred to the team: Audit-Dev
The Call record has been assigned to the Team Member: Gerald Barnes

Date:**04-Oct-2019 16:51:57** User:**Gerald Barnes**
[Start of Response]
I gathered the event data EVENTS EDS1 from 1st July 2015 to 31st August 2015 and then the problem became clearer.

I attach the spread sheet "Date Gathered" which illustrates the problem.

It has a column "Date Gathered". None are gathered from 7th July to 21st July but on the 22nd July you can see all the missing event files, all of which are much bigger than usual.
[End of Response]
Response code to call type L as Category 40 -- Pending -- Incident Under Investigation
Hours spent since call received: 2 hours

Date:**04-Oct-2019 16:54:37** User:**Gerald Barnes**
Evidence **Added** - Date Gathered

Date:**23-Oct-2019 14:25:06** User:**Gerald Barnes**
Call has been cloned to Call:PC0280793 by User:Gerald Barnes

Date:**23-Oct-2019 14:46:41** User:**Gerald Barnes**
[Start of Response]
I have cloned the PEAK and sent the clone to Tivoli_dev. Until we have some feed back from them it is not certain what needs to be done from an audit perspective. There is no fault in the audit software. However we need to be aware of when it has occurred since it means that prosecution queries must always include the catch-up day where the query spans days with no events.
[End of Response]
Response code to call type L as Category 40 -- Pending -- Incident Under Investigation
Hours spent since call received: 1 hours

Date:**30-Oct-2019 15:21:59** User:**Gerald Barnes**
[Start of Response]
What I am thinking at the moment is that the audit filtering will change from checking that there are events at the beginning and end of the range they are being asked to check to checking that there is at least one event on each day between the beginning and the end of the range they are being asked to check.
[End of Response]
Response code to call type L as Category 40 -- Pending -- Incident Under Investigation
Hours spent since call received: 20 hours

Date:**30-Oct-2019 15:27:13** User:**Gerald Barnes**
Reference Added: Jira POA-3067

Date:**30-Oct-2019 15:42:25** User:**Gerald Barnes**
I have created the feature branch https://subversion.apt.fs.fujitsu.com/svn/repository/POA/poa-audit/branch/FEATURE_PC0280466/AUDIT_QUERIES_V2 to try out a fix.

Date:**11-Nov-2019 12:33:02** User:**Gerald Barnes**
A new Business Impact has been added:
Any ARQ containing financial data sent to the Post Office must have an accompanying check of any events raised. Currently a check

FUJ00173193

is made that there is at least one event at the beginning of the range and an event at the end. Recently it was discovered that the files containing events were missing for many days and they were all in a bigger file at a later day. Because of this possibility the checking of events needs to change to there being a check that there is at least one event for every single day of the period in question.

Date:**11-Nov-2019 12:33:31** User:**Gerald Barnes**
Product HNG-X Platforms -- Audit Server (ARC) (version:V2) added.

Date:**11-Nov-2019 12:36:00** User:**Gerald Barnes**
Reference Added: Document DEV/SPP/SPG/0020

Date:**11-Nov-2019 12:59:50** User:**Gerald Barnes**
Development Cost updated: new cost is 3 (Man Days)
[Start of Response]
DEVELOPMENT IMPACT OF FIX:

SPECIFY THE HNG-X PLATFORMS IMPACTED:

The platform is specified and it is the audit server.

TECHNICAL SUMMARY:

Currently for any spread sheet of transactions presented to the Post Office a check is made that of all the events. It is confirmed that there is at least one event at the beginning of the range and one at the end. It now has been shown possible that there are no event files on a particular day and therefore a check is going to be made that there is an event for each and every day of the query.

There will be a supporting control file on the audit server showing any dates identified as having events on a later day that can be referred to see where the missing events may be (usually on this later day and so by extending the data range of the query the events can be found).

LIST OF KNOWN DIMENSIONS DESIGN PARTS AFFECTED BY THE CHANGE:

AUDIT_QUERIES_V2

DEPENDENCIES:

There are no particular dependencies.

DEPLOYMENT DETAIL:

Install in the evening backup of the audit servers.

DEV EFFORT IN MANDAYS:

3 additional days. Quite a bit of work has already been done on this stored in a feature branch.

IMPACT ON USER:

We will be more certain that all events relevant to financial queries have been checked.

IMPACT ON OPERATIONS:

We will be more certain that all events relevant to financial queries have been checked.

HAVE RELEVANT KELS BEEN CREATED OR UPDATED?

The problem is a bit to broad for a KEL. We need this fix.

IMPACT ON TEST:

They can run slow ARQs and repeat the filtering (with events) having moved aside all the event files for a given day in the EXTRACXTED_AT folder.

They can alter the MissingEvents.txt file documented in DEV/APP/SPG/0020 and confirm it works as expected.

RISKS (of releasing and of not releasing proposed fix):

If we do not do this then a financial spread sheet may not have all associated events checked.

LIST OF LIKELY DELIVERABLES:

EventFilter.pl
ContiguousDateChecker.pm
MissingEvents.txt

To get the perl date time functionality.

InstallDateTime.bat
Class-Inspector-1.31.ppmx
Class-Singleton-1.5.ppmx
DateTime-1.42.ppmx
DateTime-Locale-1.16.ppmx
DateTime-TimeZone-2.11.ppmx
DateTime-TimeZone-Local-Win32-1.98.ppm
File-Share-0.25.ppmx
File-ShareDir-1.102.ppmx

FUJ00173193

namespace-autoclean-0.28.ppmx
Params-Validate-1.28.ppmx
Params-ValidationCompiler-0.23.ppmx
Role-Tiny-2.000005.ppmx
Scalar-List-Utils-1.47.ppmx
Specio-0.22.ppmx
Test-Fatal-0.014.ppmx
Test-Requires-0.10.ppmx
Test-Warnings-0.026.ppmx
Win32-TieRegistry-0.30.ppmx
[End of Response]
Response code to call type L as Category 55 -- Pending -- Live Fix Impact Supplied
Hours spent since call received: 3 hours

Date:**11-Nov-2019 13:01:22** User:**Gerald Barnes**
The call Target Release has been moved to Proposed For -- HNG-X 19.51

Date:**11-Nov-2019 13:01:49** User:**Gerald Barnes**
Action placed on Team:BIF

Date:**12-Nov-2019 13:04:51** User:**Gerald Barnes**
The Business Impact has been updated:
Problem Statement

Any ARQ containing financial data sent to the Post Office must have an accompanying check of any events raised. Currently a check is made that there is at least one event at the beginning of the range and an event at the end. Recently it was discovered that the files containing events were missing for many days and they were all in a bigger file at a later day. Because of this possibility the checking of events needs to change to there being a check that there is at least one event for every single day of the period in question.

Risk of not fixing:

It is possible a financial spread sheet will be sent to the Post Office with some relevant events not being checked by the SMC because there were no events in the file of events for one of the days of the spread sheet.

Benefit of fixing:

We can be sure that all events relevant to financial spread sheets sent to the Post Office have been checked.

ASM Utilization Capacity (Number of Man Days required to fix this issue) :

Another 3 days is required to fix this problem.

Date:**13-Nov-2019 10:28:34** User:**Adam Harney**
BIF approved as per BIF meeting on 13/11/2019, to go to customer BIF meeting for final approval. Peak also targeted to 19.51

Date:**13-Nov-2019 10:28:46** User:**Adam Harney**
The call Target Release has been moved to Targeted At -- HNG-X 19.51

Date:**14-Nov-2019 11:30:47** User:**John Simpkins**
The Business Impact has been updated:
Problem Statement

Any ARQ containing financial data sent to the Post Office must have an accompanying check of any events raised. Currently a check is made that there is at least one event at the beginning of the range and an event at the end. Recently it was discovered that the files containing events were missing for many days and they were all in a bigger file at a later day. Because of this possibility the checking of events needs to change to there being a check that there is at least one event for every single day of the period in question.

Risk of not fixing:

It is possible a financial spread sheet will be sent to the Post Office with some relevant events not being checked by the SSC because there were no events in the file of events for one of the days of the spread sheet.

Benefit of fixing:

We can be sure that all events relevant to financial spread sheets sent to the Post Office have been checked.

ASM Utilization Capacity (Number of Man Days required to fix this issue) :

Another 3 days is required to fix this problem.

Date:**14-Nov-2019 11:46:50** User:**James Guy**
Action has been removed from the call

Date:**14-Nov-2019 11:47:04** User:**James Guy**

FUJ00173193

Action placed on Team:PTF

Date:**14-Nov-2019 11:47:17** User:**James Guy**
Approved in Customer BIF @ 14/11

Date:**14-Nov-2019 12:42:37** User:**Gerald Barnes**
Reference Added: Jira POA-3069

Date:**14-Nov-2019 12:43:57** User:**Gerald Barnes**
[Start of Response]
POA-3069 is the jira for copying the fix from the FEATURE branch into trunk.

[End of Response]
Response code to call type L as Category 40 -- Pending -- Incident Under Investigation
Hours spent since call received: 2 hours

Date:**19-Nov-2019 17:46:20** User:**Adam Sobot**
Action has been removed from the call

Date:**19-Nov-2019 17:47:19** User:**Adam Sobot**
Note - has already been to PTF and correctly targeted - no need for revisiting. So action on PTF remove.

Date:**20-Nov-2019 10:50:01** User:**Dimensions Automated User**
Reference Added: Product Baseline WINDOWS_PERL_64_5P20_V2_1951_V002
Reference Added: Product Baseline WINDOWS_PERL_64_5P20_V2_1951_V002-V001

Date:**20-Nov-2019 11:45:00** User:**Dimensions Automated User**
Reference Added: Product Baseline AUDIT_QUERIES_V2_1951_V022
Reference Added: Product Baseline AUDIT_QUERIES_V2_1951_V022-V021

Date:**20-Nov-2019 11:51:23** User:**Gerald Barnes**
Defect cause updated to 97: General - 3rd Party issue

Date:**20-Nov-2019 11:52:41** User:**Gerald Barnes**
[Start of Response]
Fixed by baselines WINDOWS_PERL_64_5P20_V2_1951_V002-V001 and AUDIT_QUERIES_V2_1951_V022-V021.
[End of Response]
Response code to call type L as Category 46 -- Pending -- Product Error Fixed
Hours spent since call received: 2 hours

Date:**20-Nov-2019 11:52:53** User:**Gerald Barnes**
The Call record has been transferred to the team: Dev-Int-Rel

Date:**20-Nov-2019 13:00:00** User:**Dimensions Automated User**
Reference Added: Product Baseline AUDIT_QUERIES_V2_1951_D022-D021

Date:**20-Nov-2019 13:37:36** User:**PIT Automated User**
[Start of Response]
Assigning Peak to PIT Automated User
[End of Response]
Response code to call type L as Category 40 (Incident Under Investigation)
The incident has been transferred to the Team: Dev-Int-Rel
The incident has been assigned to the Team Member: PIT Automated User

Date:**20-Nov-2019 14:10:01** User:**Dimensions Automated User**
Reference Added: Product Baseline WINDOWS_PERL_64_5P20_V2_1951_D002-D001

Date:**20-Nov-2019 16:15:00** User:**Dimensions Automated User**
Reference Added: Product Baseline WINDOWS_PERL_64_5P20_V2_1951_D002-D001A

Date:**20-Nov-2019 17:16:42** User:**Matt Swain**
Reference Added: DevIntRel-Director Live Supp.Test

Date:**20-Nov-2019 17:37:31** User:**PIT Automated User**
[Start of Response]
Peak 0280466 handled by integration auto handler

FUJ00173193

The following baselines attached to this peak have the targeting flags set:
AUDIT_QUERIES_V2_1951_D022-D021 FOR (LIVE:YES TEST:YES RDT:YES) Integrator: Swadesh Sureshkumar
WINDOWS_PERL_64_5P20_V2_1951_D002-D001A FOR (LIVE:YES TEST:YES RDT:YES) Integrator: Swadesh Sureshkumar

These baselines have completed integration testing, moving to holding stack awaiting peak ejection.
[End of Response]
Response code to call type L as Category 47 (Fix Processed by PIT)
The incident has been transferred to the Team: Int-Rel
The incident has been assigned to the Team Member: Olu Peters

Date:**20-Nov-2019 17:38:24** User:**PIT Automated User**
[Start of Response]
AUTOMATED UPDATE - INTEGRATION PEAK BOT

Fix processed by integration, routing to dev-int-rel director...

PLEASE NOTE: If this fix has failed, to send this peak back to integration it MUST have the response code Fix Failed or Response Rejected on it, otherwise the peak will bounce.
[End of Response]
Response code to call type L as Category 49 (Fix Available for IndependentTest)
The incident has been transferred to the Team: Live Supp.Test

Date:**21-Nov-2019 08:19:20** User:**Adam Harney**
Reference Added: Release PEAK PC0280892

Date:**21-Nov-2019 10:50:55** User:**Mark Ascott**
The Call record has been assigned to the Team Member: Timothy Harris

Date:**10-Dec-2019 05:30:00** User:**Dimensions Automated User**
Reference Added: Product Baseline AUDIT_QUERIES_V2_1951_D022-D021A

Date:**10-Dec-2019 11:48:29** User:**Raj Bains**
Reference Added: Release PEAK PC0281542

Date:**18-Dec-2019 11:37:19** User:**Timothy Harris**
Tested successfully on LST rig (R19.51 Audit Maintenance Release) as follows:-

On IRRELEVANT invoked Audit Client and executed slow ARQ (on IRE11B) OTH31380B. Search criteria Date range 11 December 2019 - 13 December 2019 FAD 015010 and Include Events. Resulted in 143 files being returned and ALL were restored and seal checked. Prior to filtering stage all files relating to date 20121212 were removed from the ARQ folder i.e. IRRELEVANT F:\USERAREA\OTH31380B\EXTRACTED_AT.

At filtering stage applying filter resulted in "Filtering Complete with Errors ".

Following the Support Guide DEV/APP/SPG/0020 the file PerlErr.txt (in F:\USERAREA\OTH31380B) was checked and the following information had been recorded -

perl output started at 17:22:09 on 12/16/19.
The date 20191212 has no events at all for it.

Manually updated the file F:\USERAREA\ConmmonScripts\MissingEvents.txt (on IRRELEVANT - from IRRELEVANT) as mentioned in Support Guide DEV/APP/SPG/0020 - as follows :

#This file contains a list of dates in date order in the format YYYYMMDD.
#Ones which are bare are genuinely missing. Ones preceded with a "-" are missing on the
#day in question but are available at a later date.

#Each group of dates listed should be preceded with a comment explaining why the date is missing for bare ones
#and at what date the events are actually there for ones starting with a "-".

#Note the syntax is very strict. Comment lines must start with "#". Special dates must start with "-". There must not be any initial spaces.
#Blank lines are allowed but they must not have any spaces in.

#Note that if any dates are not inserted in the correct order then the audit queries will fail pointing out the mistake.

#For ARQ OTH31380B there are no events for 20191212 - this is due to manual deletion within \Extracted_AT folder in order to test Peak PC0280466.
-20191212
#Only via manual deletion - Events for 20191212 are available

Date:**18-Dec-2019 11:38:08** User:**Timothy Harris**
Returning to Release to Live for closure.

Date:**18-Dec-2019 11:38:43** User:**Timothy Harris**
The Call record has been transferred to the team: RM-x

FUJ00173193

Date:**18-Dec-2019 11:39:02** User:**Timothy Harris**
The Call record has been assigned to the Team Member: Release to Live

Date:**03-Jan-2020 17:44:50** User:**Sarah Payne**
Reference Added: Release PEAK PC0281821

Date:**18-Feb-2020 12:16:31** User:**Sarah Payne**
[Start of Response]
Closing as deployed to live 04/02/20. Routing call back to call logger.
[End of Response]
Response code to call type L as Category 60 -- Final -- S/W Fix Available to Call Logger
Routing to Call Logger following Final Progress update.

Date:**18-Feb-2020 12:16:37** User:**Sarah Payne**
The Call record has been assigned to the Team Member: Farzin Denbali

Date:**25-Feb-2020 11:31:36** User:**Farzin Denbali**
Test failed on LIVE rig:

Slow ARQ POIA5459B executed on LPRPAUW202. Search criteria Date range 1/7/2015 - 14/7/2015 FAD 208840 (Include Events).

Filtering Failed.

PerlErr.txt shows:
perl output started at 21:25:22 on 02/24/20.
The date 20150707 has no events at all for it.

QueryHandler.log shows:
21:26:58 perl failed to run. The return code was 255
21:26:58 Exception whilst processing Events
21:26:58 There has been a problem processing events. See F:\UserArea\POIA5459B\QueryHandler.log on IRRELEVANT for more details.
21:26:58 The Query File Id is -99999, the message number is 300, the stage id is 1 and process halt is 1.
21:26:58 Process Request Completed

Date:**25-Feb-2020 11:35:12** User:**Farzin Denbali**
Evidence **Added** - Perl Error

Date:**25-Feb-2020 11:35:27** User:**Farzin Denbali**
Evidence **Added** - QueryHandler

Date:**25-Feb-2020 11:35:53** User:**Farzin Denbali**
The Call record has been transferred to the team: Audit-Dev
The Call record has been assigned to the Team Member: Gerald Barnes

Date:**25-Feb-2020 12:09:51** User:**Gerald Barnes**
[Start of Response]
The query range was 1/7/2015 to 14/7/2015.
The PerlErr.txt has "The date 20150707 has no events at all for it.
".
Now there is a file on the audit servers F:\UserArea\CommonScripts\MissingEvents.txt which has within it the line "There are no events from 20150707 to 20150721 but they all get caught up on 20150722. Make sure your end date is at least 20150722. PC0280466."

So if the query range is changed to "1/7/2015 to 22/7/2015" the query should work.
[End of Response]
Response code to call type L as Category 40 -- Pending -- Incident Under Investigation

Date:**10-Mar-2020 10:59:21** User:**Gerald Barnes**
The Call record has been transferred to the team: Security Ops
The Call record has been assigned to the Team Member: Farzin Denbali

Date:**10-Mar-2020 11:05:50** User:**Farzin Denbali**
[Start of Response]
Changed the date range to 01-22 Jul 2015 and query completed Successfully.
Closing the call.
[End of Response]
Response code to call type L as Category 68 -- Final -- Administrative Response
Routing to Call Logger following Final Progress update.

Date:**10-Mar-2020 11:06:02** User:**Farzin Denbali**
CALL PC0280466 closed: Category 68 Type L

Root Cause	General - 3rd Party issue

FUJ00173193

Logger	Farzin Denbali -- Security Ops
Subject Product	General/Other/Misc -- ACE (version unspecified)
Assignee	Farzin Denbali -- Security Ops
Last Progress	10-Mar-2020 11:06 -- Farzin Denbali