

To: Jennings, Graham [GRO]; Stewart, Paul [GRO]; Parker, Steve [GRO]  
Cc: Norman, Russell [GRO]; Haywood, Dave [GRO]; Seemungal, Gareth [GRO]; Ogunlana, Folusho [GRO]; Honey, Stuart [GRO]; Goddard, Steve [GRO]; Ascott, Mark MA [GRO]  
From: Beardmore, Andy [/O=FUJITSU EXCHANGE ORGANIZATION/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=82C2805D9ECD4451AAE0B2F0922]  
Sent: Wed 8/10/2016 10:52:46 AM (UTC)  
Subject: RE: 9b - Deloitte audit (AKA Appsup role)

Yes, thanks Graham. Needs to go to SSC afterwards to assess impact on any existing tooling.

Regards, Andy.

-----Original Message-----

From: Jennings, Graham  
Sent: 10 August 2016 11:36  
To: Beardmore, Andy [GRO]; Stewart, Paul [GRO]; Parker, Steve [GRO]  
Cc: Norman, Russell [GRO]; Haywood, Dave [GRO]; Seemungal, Gareth [GRO]; Ogunlana, Folusho [GRO]; Honey, Stuart [GRO]; Goddard, Steve [GRO]; Ascott, Mark MA [GRO]  
Subject: RE: 9b - Deloitte audit (AKA Appsup role)

Andy

Bit of a convoluted email but if you asking if I care if we remove APPSUP access - Then the answer is no - It is not an issue in LST test.  
And if it is then I guess we will find it out and raise a peak to get it sorted in some way.

So happy to raise a peak :- Requesting removal of APPSUP role and permissions referencing PC208119 and routing to ISD to confirm they are happy with the approach which may incur more overtime. All this as in Steve Parkers point 1 below  
1) This needs to be accepted by Belfast Operations: Potential for more overtime for them to set the required access up for SSC when we are working on issues out of hours.

Is that the sort of wording you want on the peak?

Where does the peak need to go after ISD? Host Dev ?

Cheers  
Graham Jennings  
Test Consultant  
Post Office Account  
Fujitsu  
Lovelace Rd, Bracknell, Berkshire RG12 8SN  
Tel: [GRO] or Internally [GRO]  
Mob: [GRO] or Internally [GRO]  
Email: graham.jennings@[GRO]  
Web: http://uk.fujitsu.com

-----Original Message-----

From: Beardmore, Andy  
Sent: 10 August 2016 11:07  
To: Jennings, Graham [GRO]; Stewart, Paul [GRO]; Parker, Steve [GRO]  
Cc: Norman, Russell [GRO]; Haywood, Dave [GRO]; Seemungal, Gareth [GRO]; Ogunlana, Folusho [GRO]; Honey, Stuart [GRO]; Goddard, Steve [GRO]; Ascott, Mark MA [GRO]  
Subject: RE: 9b - Deloitte audit (AKA Appsup role)

Hi Graham,

Given the focus on this issue please could you review the approach again, as we must remove the APPSUP role from individual

support user accounts. If you have any concerns with this, then any suggestions to move this forward would be gratefully received. Otherwise please could you raise a new PEAK, referencing PC208119, and send to Belfast Operations to assess Steve's point 1) below.

Regards,

Andy Beardmore

Mob: [GRO] or Internally: [GRO]

-----Original Message-----

From: Beardmore, Andy

Sent: 08 August 2016 12:14

To: Honey, Stuart [GRO]; Goddard, Steve [GRO]; Jennings, Graham [GRO]; Stewart, Paul [GRO]; Parker, Steve [GRO]  
Cc: Norman, Russell [GRO]; Haywood, Dave [GRO]; Seemungal, Gareth [GRO]; Ogunlana, Folusho [GRO]  
Subject: RE: 9b - Deloitte audit (AKA Appsup role)

And the platform owner (me) says:-

This is an historical issue (carried over from Horizon into HNG-X) highlighted in a previous audit, see Peak PC208119, which was supposed to resolve the APPSUP issue on BRDB, but seems to have withered as Test rejected the PEAK fix and it got kicked out of R6 (PC0221150), see below (copying Graham in). We need Test team to agree this approach is valid for HNG-X databases and allow Host-Dev to redeliver the scripts for new SSC users (if they haven't made it into live). We also need a subsequent MSC to mop up removal of APPSUP from any outstanding SSC users as stated in the PEAK. Steve Parker is correct that we need SSC to revisit/identify any possible tooling remaining that relies on APPSUP and address any issues in SSC/Host-Des&Dev, e.g. via supporttooluser.

Note APPSUP actions are audited via SYS\$AUD.

>>>>>

PC208119 Date:01-Feb-2011

.....  
Date:10-Apr-2013 11:20:18 User:Andy Beardmore The initial motive for this PEAK was to ensure all SSC users had the SSC role assigned to be able to execute the data correction toolset on BRDB. Initially the SSC users were manually set up incorrectly against the HNG-X BRDB HLD, being given the same permissions as per Horizon, and had too many privileges via the APPSUP role. Host-Dev have delivered the live scripts to ensure new SSC users have the correct permissions, but a follow-on MSC is required to adjust the privileges of existing users. Graham Jennings rejected this response as the approach is not consistent across the older Horizon DB's. The fact is that HNG-X did not include this change to these Horizon environments, so I believe this to be a mute point for this PEAK but more of an interest for PCI and other Audits. As such I am transferring this PEAK to the new security architect Dave Haywood for further consideration of tidying up any existing SSC users on BRDB with APPSUP role, only to have RESOURCE & SSC roles.

.....  
Date:09-Jun-2015 08:25:26 User:Mark Wright [Start of Response]  
Date:2015-06-08 11:04:58 User:Catherine Obeng [Start of Response] From DH's updated from 4th-Jul-2014, I am routing this call to UNIX/DBA to carry out the tasks in items 1 and 2 of DH's recommendations.  
Could Unix or DBA team please advise if either of your teams is in a position to develop the one-time script to implement the correct ORACLE user access (item 3).  
Please route to TfS FAO: Unix / DBA.  
[End of Response]  
Response code to call type L as Category 38 -- Pending -- Potential Problem Identified

[End of Response]  
Response code to call type L as Category 68 -- Final -- Administrative Response Routing to Call Logger following Final Progress update.

Date:09-Jun-2015 08:25:35 User:Mark Wright CALL PC0208119 closed: Category 68 Type L <<<<<<

If there isn't an existing open PEAK on this, please can whoever is driving the Deloitte Audit fixes initiate one, referring to PC208119, and initially send to Belfast Operations to comment on SP's item 1, the to Test for agreement on the approach, then SP item 4 SSC to review the tooling for possible Host-Des/Dev implementation of platform fixes. SP item 2&3 will need addressing separately when we have agreement from all.

Regards,

Andy

Mob: [GRO] or Internally: [GRO]

Email: andy.beardmore@[GRO]

-----Original Message-----

From: Honey, Stuart

Sent: 08 August 2016 11:05

To: Seemungal, Gareth [GRO]; Beardmore, Andy [GRO]

Cc: Stewart, Paul [GRO]; Parker, Steve [GRO]; Norman, Russell

[GRO]; Haywood, Dave [GRO]

Subject: RE: 9b - Deloitte audit (AKA Appsup role)

Hi Gareth,

After my conversation with you on Friday Afternoon, could you comment on Dave's statement below. I think they all sound very reasonable but I realised this was a HOST DEV area rather than Audit then it seemed sensible to run it past yourself first.

Cheers,

Stuart

-----Original Message-----

From: Haywood, Dave

Sent: 05 August 2016 17:59

To: Norman, Russell [GRO]

Cc: Stewart, Paul [GRO]; Honey, Stuart [GRO]; Parker, Steve

[GRO]

Subject: RE: 9b - Deloitte audit (AKA Appsup role)

Russell,

> Attached is the Appsup doc Paul S dug out which I believe is the  
> centre of the below debate.

Controls:

4.3 Fujitsu support staff will have privileges of only inserting balancing/correcting transactions to relevant tables in the database. SSC will not have any privileges to update or delete records in the database.

4.12 SSC will have privileges of only inserting balancing/correcting transactions to relevant tables in the database. SSC will not have any privileges to update or delete records in the database.

Question:

Deloitte phase 1 asked: "1) Evidence that the APPSUPP roles are the only roles which have access to update / delete records of balancing transactions."

Proposed response (Needs agreement with Paul Stewart / Stuart Honey & Steve Parker):

APPSUP is a legacy role not used by the SSC, the team responsible for running transaction queries and corrections. The SSC use transaction correction tool scripts as defined in DESAPPSPG0001 sec 5.6. The scripts operate as the Oracle OPS\$SUPPORTTOOLUSER and usage is audited. Any changes are made under change control.

Background (not for transmission):

The access to the Oracle APPSUP role is described in DES/APP/SPG/0001 v10.3 (sec 5.6 ) and DES/APP/HLD/0020 v6.0 (sec 5.6.2). I do not believe this role is relevant to the current SSC access and therefore Deloitte are really asking the wrong question, which should be something along the lines of: "1) Evidence that the SSC roles are the only roles which have access to update / delete records of balancing transactions."

Accessing the APPSUP role (Oracle user OPS\$SUPPORTTOOLUSER) gives the user access to the roles table(s) for the current database only. In reality, a number of scripts (see DESAPPSPG0001 sec 5.6) are used to make changes to the database when authorised by POL; for example the removal of failed AP/ADC sessions. Use of the scripts and database access are audited and changes are made under change control.

DES/APP/HLD/0020 v6.0 (sec 20.2.9) states APPSUP: "Used by the SSC (3rd line) users" and (sec 20.3) states: "Role has been defined for use by ISD Support which will act as first line support team for the Branch Database". This is historical and it is believed the APPSUP is no longer required in BDB.

DES/APP/HLD/0020 v6.0 (sec 7.2.12.1) states: "The shell script " (TCT BRDBX015) "will be owned by Linux user "supporttooluser" and it is deliberately kept separate from the standard \$BRDB\_SH directory so that access to the script and the associated components can be restricted to authorised users. The PL/SQL package PKG\_BRDB\_TXN\_CORRECTION will be owned by Oracle user "OPS\$SUPPORTTOOLUSER". The PL/SQL package PKG\_BRDB\_TXN\_CORRECTION will execute with the permissions of the OPS\$SUPPORTTOOLUSER account and can only insert rows into the transaction tables as controlled by an entry in BRDB\_SYSTEM\_PARAMETERS. The account will not have update or delete privileges."

There is nothing I can find in DES/APP/SPG/0001 or DES/APP/HLD/0020 that states the APPSUP role access is only available for the time of the correction and must be removed afterwards. I therefore cannot see why we are not compliant with the current design. Stuart, do you have a document reference / section that articulates your concerns around current SSC access to BRDB?

Because of the para above, I am inclined to retain the current level of SSC access on the basis the access is audited, performed under change control and we are not violating any (that we know of) current design statements.

It is believed that the APPSUP role is no longer required (and in fact was probably never required) in the BRDB. We should plan to have this role withdrawn from users and removed, assuming the platform owner agrees.

Regards,

Dave Haywood  
Security Architect  
Network & Telecoms  
Fujitsu

GRO

Tel: GRO or Internally GRO  
Mob: GRO or Internally GRO

> From: Parker, Steve  
> Sent: 05 August 2016 09:45  
> To: Honey, Stuart GRO; Haywood, Dave  
> GRO  
> Cc: Muir, Jason GRO; Thompson, Peter  
> GRO; Post Office Account Commercial  
> Mailbox GRO; Godfrey,  
> Stephen (Security) GRO; Norman, Russell  
> GRO  
> Subject: RE: 9b - Deloitte audit (AKA Appsup role)

> All,

> In principle yes, I would prefer that we have this removed so that we  
> go back to the security model as documented. This is not a simple "snap it back"  
> change. Need to get a few things lined up first, off the top of my head:

> 1) This needs to be accepted by Belfast Operations: Potential for more  
> overtime for them to set the required access up for SSC when we are  
> working on issues out of hours.

> 2) A risk needs to be registered (albeit low) that response time to  
> incidents (in particular priority A issues OOH) may be impacted by  
> process required to get access to Appsup

> 3) Process needs to be written for escalation, requirement for MSC  
> (retro in OOH emergencies), who approves request etc

> 4) SSC need to review existing zero financial impact tasks that  
> currently require APPSUP access. Examples are clearing zero value  
> recoveries from BRDB, dispatch report clear (in progress). These will  
> need to be added to transaction correction tool.

> Mini project needed here.

> Steve



>  
>  
>  
> From: Honey, Stuart  
> Sent: 04 August 2016 21:13  
> To: Norman, Russell <GRO>  
> <GRO>; Haywood, Dave  
> <GRO>  
> <GRO>; Parker, Steve <GRO>  
> <GRO>  
> Cc: Muir, Jason <GRO>  
> <GRO>; Thompson, Peter  
> <GRO>  
> <GRO>; Post Office Account  
> Commercial Mailbox <GRO>  
> <GRO>; Godfrey,  
> Stephen (Security) <GRO>  
> <GRO>  
> Subject: RE: section 9 - Deloitte audit

>  
>  
>  
> Hi Russell,

>  
>  
> 9b = I sent some information to Stuart Honey regarding this – I sent  
> some information to Stuart regarding this and I was not sure of the  
> outcome after that point. Was this linked to the Info Paul has  
> collated for Data flows = Paul/Dave/Stuart APSUPP = Steve raised the  
> point about whether the process should be changed to match the designs  
> or the designs changes to match the process as in the attached? – SJH  
> - sorry as I was cc'ed on your email I didn't realise you were asking  
> me for an answer but I believe we came to an agreement on the  
> meeting/conf call that the physical process should be changed to match  
> the documented process of SSC having to request and get access granted  
> for a time-boxed period via the MSC change mechanism to provide an  
> audit trail. Not my area but I presume to bring the real situation  
> into line with the documented procedure all staff (SSC only or  
> others?) should have any current access removed unless they are  
> actually working on a current issue and the documented process of  
> requesting and received time boxed access via the MSC process should be communicated  
> out to all staff that may require it. Steve/Dave, would you agree?

>  
> Assuming it is agreed I presume CS sec ops/NT Ops can raise a request  
> and remove the access from the list of users that currently have  
> permanent access.

>  
>  
>  
> I hope that is acceptable and can be progressed?

>  
>  
>  
> If not I suggest we discuss tomorrow morning to find another solution.

>  
>  
>  
> Cheers

>  
>  
>  
> Stuart

> From: Norman, Russell  
> Sent: 04 August 2016 19:34  
> To: Haywood, Dave <[REDACTED]> GRO; Godfrey, Stephen (Security) <[REDACTED]> GRO; Honey, Stuart <[REDACTED]> GRO; Muir, Jason <[REDACTED]> GRO; Thompson, Peter <[REDACTED]> GRO; Post Office Account <[REDACTED]> GRO; Commercial Mailbox <[REDACTED]> GRO; Parker, Steve <[REDACTED]> GRO  
> Subject: section 9 - Deloitte audit  
> Importance: High

> Evening all,

> The following needs to be completed and sent to Deloitte by COP tomorrow.

> For section 9 Deloitte still require the following:

> 9a = Jason has sent an email a 12:40 to Dave which needs validation  
> and then to be passed through commercial to be sent on for approval.

> 9b = I sent some information to Stuart Honey regarding this – I sent  
> some information to Stuart regarding this and I was not sure of the  
> outcome after that point. Was this linked to the Info Paul has  
> collated for Data flows = Paul/Dave/Stuart APSUPP = Steve raised the  
> point about whether the process should be changed to match the designs  
> or the designs changes to match the process as in the attached?

> 9c = a calculated response – I am not sure what stage we are at with this.

> 9e = We just have one last piece of the puzzle to complete here which  
> is the test docs to do with data purging. Jason is digging this out  
> and I will pass all the info through commercial which should be fairly  
> quick to approve (it will be some CTs, some test information and some  
> screenshots of relevant MSCs.

> Additionally

> 4ef = commercial are prepped to approve but I need as answer on the  
> attached regarding the 2 pieces of info I have (Steve's response and  
> the leavers Joiners, movers process.

> Regards,

> Russell Norman

> Project Manager – Post Office Account

>  
>  
>  
> Business & Application Services  
>  
>  
>  
> Fujitsu Services  
>  
> Lovelace Road, Bracknell, Berkshire, RG12 8SN  
>  
> Email: Russell.Norman@GRO  
> <mailto:Russell.Norman@GRO>  
> Mobile: GRO  
> Web: <http://uk.fujitsu.com> <<http://uk.fujitsu.com/>>  
>  
>  
>  
> <<http://www.youtube.com/user/fujitsuUK>>  
> <<http://www.facebook.com/fujitsuuk>> <[http://twitter.com/#!/fujitsu\\_uk](http://twitter.com/#!/fujitsu_uk)>  
> <<http://www.linkedin.com/company/fujitsu-uk-and-ireland>>  
> <<http://blog.uk.fujitsu.com/>>  
> <<https://plus.google.com/103287532874520008913/posts>>  
>  
>  
>  
> Fujitsu is proud to partner with Action for Children  
> <<http://www.actionforchildren.org.uk/>>  
>  
> I-CIO <<http://www.i-cio.com/>> : Global Intelligence for the CIO.  
> Fujitsu's online resource for ICT leaders  
>  
> Sponsors of the 2015 Rugby World Cup  
>  
> P Please consider the environment - do you really need to print this email?  
>  
>