FUJ00230912

From: Chambers Anne O[/O=EXCHANGE/OU=ADMINGROUP1/CN=RECIPIENTS/CN=ANNE.CHAMBERS]

Sent: Fri 14/05/2010 10:08:57 AM (UTC)

To: Simpkins John GRO ; Parker Steve (PostOfficeAccount) GRO

Subject: RE: ARQ and event filtering

Truncation of event text: PC0198988
Missing request id: PC0198991
Carry forward of SYSMAN2 filters: PC0198993

Anne
* GRO
external GRO

-----Original Message-----
From: Simpkins John
Sent: 14 May 2010 10:28
To: Parker Steve (PostOfficeAccount); Chambers Anne O
Subject: RE: ARQ and event filtering

Consolidation of events that may be filtered: PC0198982

Regards
John

-----Original Message-----
From: Parker Steve (PostOfficeAccount)
Sent: 14 May 2010 10:00
To: Chambers Anne O
Cc: Simpkins John
Subject: RE: ARQ and event filtering

Since anything filtered at SYSMAN2 has already been justified then yes, please raise a Peak on that basis.

-----Original Message-----
From: Chambers Anne O
Sent: 14 May 2010 09:59
To: Parker Steve (PostOfficeAccount)
Cc: Simpkins John
Subject: RE: ARQ and event filtering

Counter events - I think we should apply the same filters to SYSMAN3 as have already been applied for SYSMAN2 (since SYSMAN3 will contain events from Horizon counters post-branchrouter, pre-migration). However I don't have a list of these. I'm reluctant to put much effort into justifying each exclusion in this area.

Can I just raise a Peak saying that everything filtered out for SYSMAN2 should be filtered for SYSMAN3?

Anne
* GRO
external GRO

-----Original Message-----
From: Parker Steve (PostOfficeAccount)
Sent: 14 May 2010 09:38
To: Simpkins John; Chambers Anne O
Subject: RE: ARQ and event filtering

FUJ00230912

Anne,

If you agree, lets get the necessary Peaks raised against audit to get this going.

I'm concerned that some of the events are not complete (full event text) so unable to classify. We need to raise another Peak on audit to the effect and quoting a sample event.

Let me know Peak numbers so we can get them progressed

Steve

-----Original Message-----
From: Simpkins John
Sent: 14 May 2010 09:30
To: Parker Steve (PostOfficeAccount); Chambers Anne O
Subject: RE: ARQ and event filtering

Anne, Steve,

My comments:

The full event text was not included in the sample, most events are probably not work keeping unless they specify a specific transaction/journal number such that it can be tied back to a financial issue.

I suggest removing the following events:

AlertKey:CNIM_information
Reason:Information only
Count:15

AlertGroup: CNIM2
Reason:Not financial
Count:7

AlertGrooup:InstallSW
Reason:Not financial
Count:3

AlertGroup:TuneableTrace
Reason:Not financial
Count:12

***** Not sure about this one yet - may be too high level ***** AlertGroup:ITM_Linux_Process Reason:Not financial - Tivoli Monitoring
Count:144
****

AlertGroup:/opt/IBM/ITM/.*/lz/bin/klzagent
Reason:Not financial - Tivoli OS Monitoring - normall that the Tivoli monitor is not running
Count:39

Agent:104
AlertGroup:SYSMGT
EventText:SYSMGT 104: SMG_Execute_Tripwire_Client% Reason:Not financial - Tivoli Monitoring
Count:48

Agent:63
AlertGroup:OSR

FUJ00230912

Event:%Unable to service download package inventory request from branch counter% Reason:Not financial - Tivoli Monitoring
Count:4794

Agent:NNM
AlertGroup:NNM
Reason:Not financial - Typically reporting when a network link is unavailable
Count:57

AlertKey:/opt/OSR/horizon_server_%.properties
Event:%su - osruser -c /opt/OSR/OSRstart.sh% Reason:Not financial - Attempts to restart the OSR
Count:814

Agent:ITM
Manager:tivoli_eif probe on lprpemm001
Reason:Not financial - Tivoli Server Monitor
Count:14

Regards
John

-----Original Message-----
From: Parker Steve (PostOfficeAccount)
Sent: 13 May 2010 13:30
To: Simpkins John; Chambers Anne O
Subject: ARQ and event filtering

John, Anne

The event lists we are being asked to check on HNGX ARQ requests are just unmanageable (7-10,000 rows in the SYSMAN3 details). We are allowed to filter out where the event is known to have no financial impact on the counter. We need to get the ARQ event filters up-to-date for HNGX quickly to make the situation manageable.

According to Gerald Barnes the way to get the filters changed is:

"The events need to be all checked by someone who understands them. Whilst doing this they may well identify certain patterns which they know to be benign. They should then raise a PEAK stating which patterns they consider benign and assign it to the audit team. We will then alter our filters to ensure that these events are always filtered out.
This seems a little tedious but it has the advantage that we have an audit trail for the reason behind filtering out particular events."

Can you co-operate on looking at these event lists and getting the Peaks raised into Audit. Suggest John runs the list and Anne advises on counter events. If you supply me with the Peak numbers I'll get them pushed through. This is likely to be an iterative process until we can get the events driven down.

I've attached a sample ARQ output. There are some obvious ones on the list that can be knocked off quickly.

Possible?

Steve