FUJ00173153

Export

Peak Incident Management System

Call Reference	**PC0261282**	Call Logger	Deleted User -- Live Supp.Test
Release	Targeted At -- HNG-X 15.31	Top Ref	WIN_ITM_OS_AGENT_CFG_1520_D001
Call Type	Cloned call	Priority	C -- Progress restricted
Contact	Deleted Contact	Call Status	Closed -- Build Fix Available to Call Logger
Target Date	No Forcast	Effort (Man Days)	0
Summary	'The Monitoring Agent for Windows OS – Primary' pid is using 4.7gb of memory (C:\IBM\ITM\TMAITM~1\kn		

All References	Type	Value
	DevIntRel-Director	Live Supp.Test
	Clone Master	PC0261026
	Release PEAK	PC0269263
	MSC	043J0457573
	TRIOLE for Service	A16497108
	Release PEAK	PC0261780
	DevIntRel-Director	Live Supp.Test
	Release PEAK	PC0264301
	Product Baseline	WIN_ITM_OS_AGENT_CFG_1520_D001
	Release PEAK	PC0264293
	Product Baseline	WIN_ITM_OS_AGENT_CFG_1520_V001

Impact Statement	User	Date
	Gerald Barnes	04-Aug-2017 17:49:26
	SMG have suspended the saving of events because of this bug. This is a security issue. The problem has uncovered an inefficiency in the sealer. It is repeatedly checking folders to see whether anything needs to be done in a hard loop. It is always good practice to put a sleep of some duration if there is nothing that needs to be done so resources will be freed to do other things. This fix should make for examples prosecution queries quicker than before.	

Progress Narrative

Date:**10-Aug-2017 15:03:19** User:**David Bower**
CALL PC0261282 opened
Details entered are:-
Summary:'The Monitoring Agent for Windows OS - Primary' pid is using 4.7gb of memory (C:\IBM\ITM\TMAITM~1\kn
Call Type:C
Call Priority:C
Target Release:HNG-X Rel. Ind.
Routed to:Live Supp.Test - David Bower

Date:**02-Aug-2017 13:42:50** User:**_Customer Call_**
CALL PC0261026 opened
Details entered are:-
Summary:'The Monitoring Agent for Windows OS - Primary' pid is using 4.7gb of memory (C:\IBM\ITM\TMAITM~1\kn
Call Type:L
Call Priority:C
Target Release:HNG-X Rel. Ind.
Routed to:EDSC - _Unassigned_

Date:**02-Aug-2017 13:42:50** User:**_Customer Call_**
==========
INCIDENT MANAGEMENT
Date/Time Raised: Aug 2 2017 12:32PM
Priority: C
Contact Name: POA-SMC1
Contact Phone: GRO
Originator: XXXXXX@TFS01
Originator's reference: A16497108
Product Serial No:
Product Site:

FUJ00173153

==========

Transfer Note: Please pass to Tivoli-Dev via PEAK, thanks.:
Below mail was received from Michael Greene

From: Greene, Michael
Sent: Wednesday, August 02, 2017 1:27 PM
To: FC.IN.POA_SMC
Subject: TFS Call

Hi SMC, please raise a call for the following,

Priority : P(3)

Description: IRRELEVANT: Service Name - 'KNTCMA_Primary', 'The Monitoring Agent for Windows OS - Primary' pid is using 4.7gb of memory (C:\IBM\ITM\TMAITM~1\kntcma.exe)

Please pass call to 'POA-HNG NT Support'

Thanks

Michael Greene
FUJITSU

History:

2017-08-02 12:32:36 [Sahanir, Rajkumar]
INIT : Create a new request/incident/problem/change/issue

2017-08-02 12:35:13 [Sahanir, Rajkumar]
zneut_en_poa : Transfer Notification

2017-08-02 12:35:13 [Sahanir, Rajkumar]
zneun_en_poa : Open Notification

2017-08-02 12:35:43 [Sahanir, Rajkumar]
zneut_en_poa : Transfer Notification

2017-08-02 12:38:28 [Greene, Michael]
LOG : Noticed that the pid for 'Monitoring Agent for Windows OS - Primary' service on LPRPARC201 was using 4.7gb of memory, (pid C:\IBM\ITM\TMAITM~1\kntcma.exe), server has 8gb and memory was over 80% utilized. Service was stopped and started and memory has been freed up.

C:\IBM\ITM\TMAITM~1\kntcma.exe details
File Version : 6.3.0.0
Product Version : 6.3.0.0
Size : 2.28mb
Date Modified : 14/07/2017 10:55

Will attach log files from IRRELEVANT 'C:\IBM\ITM\TMAITM6_x64\logs' to PEAK.

The pid is using 623mb memory on IRRELEVANT

Please pass to Tivoli-Dev via PEAK to investigate, thanks.

2017-08-02 12:42:12 [Greene, Michael]
zneut_en_poa : Transfer Notification

Date:**02-Aug-2017 13:57:01** User:**Joe Harrison**
Product Infrastructure -- Tivoli (version unspecified) added.

Date:**02-Aug-2017 13:57:48** User:**Joe Harrison**
The Call record has been transferred to the team: Tivoli-Dev
Progress was delivered to Consumer

Date:**02-Aug-2017 14:01:12** User:**Michael Greene**
Evidence **Added** - IRRELEVANT C:\IBM\ITM\TMAITM6_x64\logs

Date:**02-Aug-2017 14:14:36** User:**Shaun Wood**
The Call record has been assigned to the Team Member: Shaun Wood
Progress was delivered to Consumer

Date:**02-Aug-2017 14:51:05** User:**Shaun Wood**
Target Date/Time updated: new value is 31/12/9999 00:00
[Start of Response]
I have checked platforms on LST HDCR, the ARC201 has similar issues to live. This is a 4GB machine which is at 88% memory and 55% CPU, the kntcma.exe was using 1.9gb of memory so nearly half the memory.

I have checked other Windows 2012 platforms on LST as all Windows 2012 are running ITM OS Agent 6.3.0.6 but none have memory usage as high as the ARC201 platform.

FUJ00173153

TEM201 193,516k
ACD201 50,184k
SSC201 40,400k

I have checked IBM, there is a Fix Pack 7 available i.e. 6.3.0.7 but nothing documented about memory leaks. I did find APAR IV62549 for a memory leak issue on the Windows OS Agent but this was fixed in 6.3.0.5. It may be that 6.3.0.6 re-introduced the issue ?

I will stop/start the ITM OS Agent on IRRELEVANT on LST and monitor plus I will get a PMR logged with IBM if over the next few days we see an increase in memory usage on the Live and LST ARC201 platforms.

549

[End of Response]
Response code to call type L as Category 40 -- Pending -- Incident Under Investigation
Response was delivered to Consumer

Date:**02-Aug-2017 14:58:53** User:**Shaun Wood**
ITM OS Agent restarted on IRRELEVANT @ 02/08/17 14:55

Checked memory usage after this which was :-

40,904
40,968
40,984
40,968
40,916
40,900

This shows a low memory usage which does up/down as we'd expected, I will check again tomorrow.

Date:**02-Aug-2017 15:22:56** User:**Shaun Wood**
I have asked Michael to keep an eye on the live ARC201.

Date:**03-Aug-2017 15:40:43** User:**Shaun Wood**
We've just hit another issue with IRRELEVANT as ITM OS Agent is using 5.5GB, there have been a large number of security events generated 1.8million since 15:04 15:24 - log has been overwritten

I suspect the ITM OS agent is grabbing memory to read all of the events as it does provide details of OS Log Files.

According to Michael

[ý03/ý08/ý2017 15:33] Greene, Michael:
I can see a lot of audit type security events against the sealer.exe - An attempt was made to access an object. then The handle to an object was closed - @ 15:04:25, thousands of them
thats whats filled the sec event log up
probably need to relax the audit settings

Date:**03-Aug-2017 15:54:49** User:**Shaun Wood**
Looking at the Security log there are vast amounts of Audit Success Events around 15:05 of ID 4663 and 4658 for auditsvrcomp.

The Security log goes from 15:04 to 15:48, there are 1.8 million records in 44 minutes. Of the 1,833,927 of these 1,825,830 are Audit Success.

So based on this rate of 2.4 million security events per hour this server along will rack up 59 million security events per day.

This is being done due to new security measure for auditing. I would question what is running which is creating so many of these events as these are Success so this looks to be normal running which I'm guessing will only increase as we move into R16 & R17 are most systems will be audited.

Date:**03-Aug-2017 15:59:08** User:**Shaun Wood**
NT have now stopped and disabled the ITM OS Agent so that we don't hit this issue. In order to progress this issue I need Gerald Barnes to check the platform to explain why we are getting so many security events for Audit, this is to be expected ? If so then we may need to consider relaxing the security auditing as this will also be creating millions of events to go into audit which I'm sure will be 100 times more or higher than the current system. I won't raise a call with IBM at this moment as I suspect they may just advise us to reduce event loads as we don't have any issues on other platforms.

I will pass this over to the audit team.

Date:**03-Aug-2017 15:59:26** User:**Shaun Wood**
The Call record has been transferred to the team: Audit-Dev
The Call record has been assigned to the Team Member: Gerald Barnes
Progress was delivered to Consumer

Date:**03-Aug-2017 18:58:15** User:**Gerald Barnes**
[Start of Response]

FUJ00173153

I have sent an email to Dave Haywood asking whether we can stop generating these success events.

I have no reason to believe it is anything other than BAU.
[End of Response]
Response code to call type L as Category 40 -- Pending -- Incident Under Investigation
Response was delivered to Consumer
Hours spent since call received: 4 hours

Date:**04-Aug-2017 10:24:58** User:**Dave Haywood**
Before I agree to considering relaxing event logging on the ARC servers, I would like to understand why the auditsvrcomp userid is (I presume) opening and closing so many files over such a short period of time. The evidence doesn't seem to contain details of which files are being accessed and why. I would like to rule out a software issue that is causing a large number of events to be logged. Please provide some analysis of which files are being opened / closed, at what rate and why.

The events in question are:
An attempt was made to access an object - Event ID 4663
The handle to an object was closed - Event ID 4658

Please supply further analysis / evidence as requested above.

Date:**04-Aug-2017 17:44:10** User:**Gerald Barnes**
Product HNG-X Platforms -- Audit Server (ARC) (version:2) added.

Date:**04-Aug-2017 17:49:26** User:**Gerald Barnes**
A new Business Impact has been added:
SMG have suspended the saving of events because of this bug. This is a security issue.

The problem has uncovered an inefficiency in the sealer. It is repeatedly checking folders to see whether anything needs to be done in a hard loop. It is always good practice to put a sleep of some duration if there is nothing that needs to be done so resources will be freed to do other things. This fix should make for examples prosecution queries quicker than before.

Date:**04-Aug-2017 18:08:52** User:**Gerald Barnes**
Development Cost updated: new cost is 2 (Man Days)
[Start of Response]
DEVELOPMENT IMPACT OF FIX:

SPECIFY THE HNG-X PLATFORMS IMPACTED:

The platform has been specified and it is the audit server.

TECHNICAL SUMMARY:

In routine RGSchedule of SealContol.c it gets into a hard loop of checking ?

D:\Archiveserver\CONTROL\SEALER_MODULE
D:\Archiveserver\INTERFACES\IMPORT_CAT\Data
D:\Archiveserver\CONTROL\SEALER_2_MODULE
D:\Archiveserver\INTERFACES\IMPORT_CAT\Md5

waiting for something extra to do.

This is not efficient.

It will be wasting a lot of machine resources doing this.

The code does sleep for a second of so in the loop when there is absolutely nothing to do.

It has multiple threads and the problem occurs when some threads are doing things and it is trying to decide whether to start another one or not.

So in conclusion a sealer fix is required.

This fix will greatly reduce the number of events and make processing much more efficient at the same time!

LIST OF KNOWN DIMENSIONS DESIGN PARTS AFFECTED BY THE CHANGE:

AUDIT_SERVER_APP_V2

DEPENDENCIES:

There are no dependencies.

DEPLOYMENT DETAIL:

Replacement files to be supplied during the evening backup.

DEV EFFORT IN MANDAYS:

2 man days. I have another fix to work on which may need to be done first for 16.21. We may decide to schedule this first in which case I can start immediately.

IMPACT ON USER:

It will speed things up for SecOps though I am not sure by how much.

FUJ00173153

IMPACT ON OPERATIONS:

They will be able to harvest events again.

HAVE RELEVANT KELS BEEN CREATED OR UPDATED?

No KEL is needed from the audit team.

IMPACT ON TEST:

They need to check that gathering, ARQs and the evening robocopy works as before without filling up the event log.

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

releasing

I cannot see any disadvantage.

not releasing

We will continue to get flooded with these audit success events.

We will continue to needlessly keep checking the same folders hundreds of times a second when it would be sufficient to do it once a second.

LIST OF LIKELY DELIVERABLES:

sealer.exe definitely

We may decide to make the sleep configurable so as to fine tune the fix later.

In this case additionally -

Archive.exe
ConfigDLL.dll
Deleter.exe
Gatherer.exe
Messages.dll
Retriever.exe
Sealer.exe
Bootle\ConfigurationFile.txt
Wigan\ConfigurationFile.txt
Wigan\ConfiurationFile_DR.txt

[End of Response]
Response code to call type L as Category 55 -- Pending -- Live Fix Impact Supplied
Response was delivered to Consumer
Hours spent since call received: 7 hours

Date:**04-Aug-2017 18:10:17** User:**Gerald Barnes**
The call Target Release has been moved to Proposed For -- HNG-X 15.21

Date:**04-Aug-2017 18:10:46** User:**Gerald Barnes**
Action placed on Team:BIF

Date:**07-Aug-2017 10:37:33** User:**Jubita Gurung**
The call Target Release has been moved to Targeted At -- HNG-X 15.20

Date:**07-Aug-2017 10:58:57** User:**Jubita Gurung**
BIF approved and targeted at 15.20

Date:**07-Aug-2017 10:59:01** User:**Jubita Gurung**
Action has been removed from the call

Date:**07-Aug-2017 11:28:12** User:**Shaun Wood**
After discussing this issue with John Bradley I have raised PMR Ref 16388,019,866 with IBM as we don't think their agents should be utilising so much memory and need to know if there is a way of disabling checking event logs as we have Netcool monitoring the Windows event logs.

Date:**07-Aug-2017 11:54:30** User:**Gerald Barnes**
Reference Added: Jira POA-2216

Date:**08-Aug-2017 19:10:01** User:**Dimensions Automated User**

FUJ00173153

Reference Added: Product Baseline AUDIT_SERVER_APP_V2_1520_V019
Reference Added: Product Baseline AUDIT_SERVER_APP_V2_1520_V019-V009

Date:**08-Aug-2017 19:18:30** User:**Gerald Barnes**
[Start of Response]
Partially fixed by version 15.20.0.5 of sealer.exe.

If the sealer is not busy then you will get 259,200 of these success events per day.

This would increase to a maximum of 10 times this number if the sealer was very busy all the time which would never be the case.

So even in the very worst case there will be far less than 59 million security events a day.

[End of Response]
Response code to call type L as Category 46 -- Pending -- Product Error Fixed
Response was delivered to Consumer
Hours spent since call received: 15 hours

Date:**08-Aug-2017 19:18:35** User:**Gerald Barnes**
Defect cause updated to 14: Development - Code

Date:**08-Aug-2017 19:18:48** User:**Gerald Barnes**
The Call record has been transferred to the team: Dev-Int-Rel
Progress was delivered to Consumer

Date:**09-Aug-2017 08:30:01** User:**Dimensions Automated User**
Reference Added: Product Baseline AUDIT_SERVER_APP_V2_1520_D019-D009

Date:**09-Aug-2017 12:03:20** User:**PIT Automated User**
[Start of Response]
Peak 0261026 handled by integration auto handler

The following baselines attached to this peak have the targeting flags set:
AUDIT_SERVER_APP_V2_1520_D019-D009 FOR (LIVE:YES TEST:YES RDT:YES) Integrator: Geoff Inglis

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
Progress was delivered to Consumer

Date:**09-Aug-2017 12:05:53** 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
Progress was delivered to Consumer

Date:**09-Aug-2017 15:34:57** User:**Victoria Griffin**
Reference Added: Release PEAK PC0261232

Date:**10-Aug-2017 14:07:37** User:**Shaun Wood**
I need to get this call cloned so that I can test / change the ITM OS Agent as per advice from IBM.

Date:**10-Aug-2017 15:03:19** User:**David Bower**
Call cloned from original call:PC0261026 by User:David Bower

Date:**10-Aug-2017 15:04:30** User:**David Bower**
The Call record has been assigned to the Team Member: David Bower

Date:**10-Aug-2017 15:05:05** User:**David Bower**
The Call record has been transferred to the team: Tivoli-Dev
The Call record has been assigned to the Team Member: Shaun Wood

Date:**10-Aug-2017 16:55:16** User:**Shaun Wood**

FUJ00173153

This call be used to progress the changes provided by IBM, I will raise an Emergency MSC to make the changes on IRRELEVANT tomorrow to test as this platform will has the issue and so will prove if the IBM changes are successful.

Date:**11-Aug-2017 10:38:40** User:**Shaun Wood**
Reference Added: MSC 043J0457573

Date:**11-Aug-2017 10:39:54** User:**Shaun Wood**
Target Date/Time updated: new value is 31/12/9999 00:00
[Start of Response]
MSC raised to update KNTENV file on IRRELEVANT to address memory issues. Once this has been implemented we will then need to monitor for a few days to confirm this has addressed the issue. A formal fix will then be delivered.
[End of Response]
Response code to call type C as Category 41 -- Pending -- Product Error Diagnosed

Date:**11-Aug-2017 15:22:21** User:**Shaun Wood**
MSC has been implemented, the ITM OS Agent has started and is running fine. I have monitored memory for 5 mins, this as stayed fairly static around 41,000k. I will inform NT and then check the server again next week.

Date:**14-Aug-2017 10:22:16** User:**Shaun Wood**
I have just checked the ITM OS Agent on IRRELEVANT the memory usage is at 42,656k which looks fine as there have been millions of events so the agent is no longer consuming memory like this did prior to the changes. I will continue to monitor for the rest of this week, if all still looks fine I will get a formal release sorted.

Date:**14-Aug-2017 10:29:20** User:**Shaun Wood**
[Start of Response]
I will action QFP as I'm not sure what target release I should use for this Peak, Gerald has delivered his fix at R15.20 which I guess now needs to go through LST as a hot fix, this ITM OS Agent change also needs to do the same so R15.20 also ? The WIN_ITM_OSAGENT_V001 was delivered at R15.20 so I'd just need a V002-V001 incremental.
[End of Response]
Response code to call type C as Category 40 -- Pending -- Incident Under Investigation

Date:**14-Aug-2017 10:29:38** User:**Shaun Wood**
Action placed on Team:QFP Forum

Date:**17-Aug-2017 17:44:30** User:**Shaun Wood**
[Start of Response]
I have just checked the ITM OS Agent on IRRELEVANT, the memory usage is at 44,156k which confirms that we no longer have an issue so I now need to deliver a formal fix. QFP will need to sanction this and target, I'll propose R15.20 as Gerald has delivered his fix at this release.
[End of Response]
Response code to call type C as Category 41 -- Pending -- Product Error Diagnosed

Date:**17-Aug-2017 17:44:45** User:**Shaun Wood**
The call Target Release has been moved to Proposed For -- HNG-X 15.20

Date:**18-Aug-2017 09:03:52** User:**Nick Lawman**
The call Target Release has been moved to Targeted At -- HNG-X 15.20

Date:**21-Aug-2017 12:37:08** User:**Shaun Wood**
Action has been removed from the call

Date:**23-Aug-2017 13:50:02** User:**Dimensions Automated User**
Reference Added: Product Baseline WIN_ITM_OS_AGENT_CFG_1520_V001

Date:**23-Aug-2017 13:52:13** User:**Shaun Wood**
[Start of Response]
New ITM OS Agent config product released to amend agent values to address memory issues. This now needs to be installed onto all Windows 2012 Servers as a top-up to address this issue which has been tested on the live IRRELEVANT platform.
[End of Response]
Response code to call type C as Category 48 -- Pending -- Fix Released to PIT

Date:**23-Aug-2017 13:52:19** User:**Shaun Wood**
The Call record has been transferred to the team: Dev-Int-Rel

Date:**23-Aug-2017 14:25:01** User:**Dimensions Automated User**
Reference Added: Product Baseline WIN_ITM_OS_AGENT_CFG_1520_D001

FUJ00173153

Date:**24-Aug-2017 14:41:59** User:**Sarah Payne**
The call Target Release has been moved to Targeted At -- HNG-X 15.31

Date:**24-Aug-2017 14:42:30** User:**Sarah Payne**
Peak re-targeted to R15.31 as LST have signed off R15.21.

Date:**24-Aug-2017 16:14:11** User:**Karen Cooper**
Reference Added: Release PEAK PC0261780

Date:**30-Aug-2017 11:48:46** User:**Vijesh Pandya**
The Call record has been transferred to the team: Live Supp.Test

Date:**04-Sep-2017 14:16:05** User:**Mark Ascott**
The Call record has been assigned to the Team Member: David Bower

Date:**26-Oct-2017 15:53:03** User:**David Bower**
[Start of Response]
Baseline installed on all LST win 2012 servers and no issues encountered. This is a top up for changes that were tested by Shaun Woods on IRRELEVANT. This has passed LST testing.
[End of Response]
Response code to call type C as Category 61 -- Final -- Build Fix Available to Call Logger
Routing to Call Logger following Final Progress update.

Date:**26-Oct-2017 15:53:11** User:**David Bower**
CALL PC0261282 closed: Category 61 Type C

Date:**14-Nov-2017 15:36:48** User:**Victoria Griffin**
Reference Added: Release PEAK PC0264293

Date:**14-Nov-2017 16:58:50** User:**Victoria Griffin**
Reference Added: Release PEAK PC0264301

Date:**17-Apr-2018 16:02:05** User:**Jubita Gurung**
Reference Added: Release PEAK PC0269263

Root Cause	Development - Code
Logger	Deleted User -- Live Supp.Test
Subject Product	General/Other/Misc -- Unknown (version unspecified)
Assignee	Deleted User -- Live Supp.Test
Last Progress	17-Apr-2018 16:02 -- Jubita Gurung