Resolving APM CE Business Transaction/Defect Count Issues

Version .01b January 27th 2015
Preview Draft -- Comments Appreciated!

Hallett German
Principal Support Engineer
CA Technologies
Hallett.German@ca.com

Table of Contents

---

1. Introduction

This tech note is an expansion of "Top Three Researched APM Issues" that was created both as a Tech Tip and as a knowledgebase (KB) article.

Transaction/Defect counts is a particular issue that takes time to research. This typically follows one of these scenarios:

1. There are more/less in the total daily APM CE business transactions/transactions **count** as compared to third-party tool x.

2. There are more/less daily APM CE business transactions/transactions **defects** as compared to third-party tool x.

The third party tool may be a web server or a synthetic transaction generator. This Tech Note covers common causes of this issue and how to resolve it.

Versions:
.01 Preview Version. Publically distributed for review..

2. Guiding Principles

- APM CE (also called CEM) attempts to create consistent and complete statistical/defect reports.
- Various non-product factors can impact defect and statistical counts. Some of these are included below.

3. Out of scope

The following scope for this document:

- Synthetic script debugging.
- Tutorial on network traffic, SSL, Wireshark etc.
- Details on Business Service hierarchy.

4. Factors Impacting Accurate Counts

These product and non-product factors can impact complete and accurate APM CE defect/statistical counts.

Factor	How it Impacts
Network quality (Are packets being lost, out of order, retransmitted, filtered out?)	Transactions are incomplete or missing due to network quality issues.
SSL factors (cipher suites, TLS versions and features)	Transactions are incomplete or missing due to SSL decoding issues.
Transaction definitions having too many/too few matches. Overlapping definitions. Definitions are too broad/restrictive.	Transaction counts are higher than expected due to overlapping definitions. Transaction counts are higher/lower than expected due to broad/restrictive definitions.
Business transaction/transaction defect thresholds both set.	Double defects for a single transaction
Synthetic scripts	May be running more often than believed. Recent changes to scripts can also impact counts.

5. Overall technique

Do the following for 20-60 minutes. Performing these steps may result in large logs.

General	Possible Root Cause	APM	Third-Party
Run as many transactions during a timeframe.	Network Quality	Look in TIM Status Screen and Logs for Out of Order packets.	Compare traffic between switch/network and TIM using a third-party tool.
	Network Filtering	Check TIM Log with just connections enabled.	Check pcap between switch and TIM monitoring connection.
	SSL Issues	Check SSL decode failures/successful transactions in TIM log. .	Get a pcap of transactions from the timeframe. Add private key to Wireshark or use ssldump to see if SSL traffic decodes.
	Network Quality	Look at TIM logs to see if it completes. Get the transaction & defect count. See if sessions are opening but not closing.	Get a count accessing same URLs as the APM CE definitions from the web or synthetic application server logs.

	Transaction definitions having too many/too few matches.	Check the TIM logs to see if the defects/transaction counts are showing up in another definition. This may be due to the same transaction component in two definitions. Check the APM CE GUI to see if the transaction definition is too broad. Check the TIM logs for URL string matches	Compare to a third party logs for count. Compare third-party definition for URL matches.

6. Technique details

Here are some techniques that you can use in the analysis:

Technique	Overview	Technique Details
Wireshark Filters	To reduce the amount of traffic that you are seeing, enter Wireshark filter strings.	Showing http traffic when 10.10.10.10 is a source or destination address: *http and ip.addr==10.10.10.10* Showing http traffic when 10.10.10.10 or a 10.10.10.11 is a source address: *http and (ip.src==10.10.10.10. or ip.src==10.10.10.11)* If these two addresses are only communicating with each other, then you would see two-way http traffic only between these two addresses in the TIM log. Showing one-way http traffic between

Technique	Overview	Technique Details
		these two IP addresses. *http and (ip.src==10.10.10.10 and ip.dst==10.10.10.11)* Once using any of the above filters, then count the URLs for that time period for that client/server IP combination.
TIM logs	Review for transaction counts and matches	Do the following in the TIM logs: Start by looking at the URL used in the APM CE request definition and the component number. Below we are looking for www.pizzarentals.com/pz/rentalsearch.htm with a client IP of 10.10.20.10 We see that the component number is 15229672 Wed Jan 27 11:26:54 2015 5629 Trace: Component #15229672 request: www.pizzarentals.com/pz/rentalsearch.htm client=[10.10.20.10]:2133 server=[10.10.10.10]:80 at 11:26:54 Follow that component number to see one of two conditions: The transaction does not match: Wed Jan 27 11:26:54 2015 5629 Trace: Component #15229672 does not match a transet definition or an expected component The transaction matches: Wed Jan 27 11:26:55 2015 5629 Trace: TranSet #15229672: start TranSetDef=70000000000001560/"Pizza Rental Search" at 11:26:55 Wed Jan 27 11:26:55 2015 5629 Trace: TranUnit #15229672: start TranUnitDef=70000000000002868/"Pizza Rental Search" at 11:26:55 Wed Jan 27 11:26:55 2015 5629 Trace: TranComp #15229672: start TranCompDef=70000000000009574/"Pizza Rental

Technique	Overview	Technique Details
		Search" at 11:26:55 Wed Jan 27 11:26:55 2015 5629 Trace: Component #15229672: found user group "NJ Pizza" in request Wed Jan 27 11:26:55 2015 5629 Trace: TranComp #15229672: TranSet=#15229672 TranUnit=#15229672 This gives you the transaction count for that time period from a TIM perspective.
TIM Logs	Transaction definitions having too many/too few matches.	Follow steps in "TIM Logs/Review for Transaction Counts and Matches." You can see above if you are matching the correct definition. (For example if looking for "Pizza Rental Delivery instead of Pizza Rental Search", then the same component is in both definitions and the incorrect definition is being matched The other technique is to compare if the definitions are too broad or too restrictive. A transaction definition matching on five parameters may miss out on some transactions that only matches on two or three. (I.e. Condition 1 AND Condition 2 AND Condition 3… must all be true.) This could result in an undercount. A transaction definition that is too broad will match on more than desired. (Such as /pz/* will be a catchup for the many URLs under /pz/.) The solution is to use as specific a definition as possible.

Technique	Overview	Technique Details
TIM logs	Review for transaction defect counts	Follow the steps in "TIM Logs/Review for Transaction Counts and Matches." Then look for something like the following after the responses section: Wed Jan 27 11:28:26 2015 5629 Trace: TranSet #15229672: defect type=1 id=700000000000013748 Wed Jan 21 11:28:26 2015 5629 Trace: TranSet #15229672: end size=7658, time=*, defects=1, total-defects=1 at 11:28:26 The above would generate a defect for a slow time transaction.
Third-party logs	Review for transaction counts and transaction defect counts.	Look for the appropriate host/URL/Client IP/Server IP combination. Get a count for that time period.

7. Acknowledgements

Credits & Acknowledgements

- Thanks to Raju Kanumuri for his case analysis where many of these basic ideas came from.

References

Some of the above information was directly pulled from the following sources:

- German, Hallett "CA Tech Tip: Three Researched APM CE Issues (KB TEC598247)" September 7 2013 https://communities.ca.com/message/101730901

- German, Hallett Three Researched APM CE Issues (KB TEC598247) http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/tec598247.aspx