Tech Tips and Blogs 2016

.v01b 12/21/2016

Hallett German

hallett.german@ca.com

CA Technologies

Distribution Notes: This document may be freely distributed to all interested audiences to help APM Administrators and Users. However, no modifications may be made to this work.

Section 1: Introduction

It is another year and I continue the "new tradition" of making an e-book of all of my blogs/tech tips. I release this "AS-IS "with minimal proofing. I hope this is of use to someone and wish you all a happy 2017.

Hallett German

CA Technologies APM Support

Hallett.german@ca.com

Section 2: Blogs 2016

2.1 Why Problems and Outages are Blessings in Disguise

URL: https://communities.ca.com/community/ca-apm/blog/2016/01/24/apm-blog-why-problems-and-outages-are-blessings-in-disguise

Introduction

Thomas Johnston is exhausted after spending a good part of the weekend battling an APM outage. After making some configuration adjustments and an EM/agent restart, peace is restored and he can get some overdue sleep. All is good until the next issue needs resolving. But a wise person not knowing much about technology at the time told them, "Be grateful for the problem. You will learn something out of it and will work hard to enure that it never happens again."

In this blog, I discuss how APM problems and outages are really opportunities for improvement. This can take place in several phases.

1: Self-Investigation

Going through a "lessons learned" group exercise is key for ongoing success. This includes reviewing

- What was supposed to happen?

- What actually did happen?

- What went well during the problem-solving phase?

- What did not go well?

- What can be better done differently next problem?

If there are improvements to processes and resources as a result, then this is time well spent.

The same thing should be done at a personal level. Questions that can be asked are:

- How quickly did it take to determine what the problem was? What steps were important in achieving this?

- Were there some questions that I could ask or things that I could have done to find the issue quicker?

- Are there subject areas that need to brush up on?

- Are there third-party troubleshooting tools/field packs that I should consider using?

2: Short and Mid Term Fixes

Short-, mid-, and long-term stabilization measures should be investigated. This may include

- EM but not agent upgrades to interim releases.

- Adding new hardware to replace or supplement the current cluster load

- Doing ongoing health checks, oil change and architectural reviews to evaluate needed changes and optimize the environment

- Create or evaluate an APM personal training plan on new features, performance, troubleshooting, and optimization.

- Clean up network traffic/private keys for TIM.

- Implement APM Monitoring strategy and Roadmap

3. Longer-Term fixes

Most sites have a longer-term plan. It includes:

- Cluster upgrades to major/more current releases including agents.

- Ongoing cluster health trend analysis and capacity planning

- Having lifecycle APM cluster environments to act as a sandbox for suggested performance changes and to test future releases

Hopefully, this has been a helpful discussion. I would love to hear your comments on how past problems became opportunities for improvements

2.2 Contracted vs Reflective Mind -- An Owner's Manual

URL: https://communities.ca.com/community/ca-apm/blog/2016/02/14/contracted-vs-reflective-mind-an-owners-manual

2.3 On Service and APM Support

URL: https://communities.ca.com/community/ca-apm/blog/2016/02/21/on-service-and-apm-support

This is a follow-up to my last blog on why Outages are Blessings in Disguise.

Introduction
Imagine that it is 2 A.M. and you are woken out of a sound sleep to attend a bridge call about an APM outage. After you join in, you discover that you have been unknowingly given the ability to read people's minds and directly feel their emotions. What would discover? How would you react towards them?

You would likely find these two mind states:

1. The Contracted Mind

During times of stress (such as outages), some people are filled with low confidence and are driven by emotions such as fear, anger, doubt, or anxiety. Some of the questions they could be pondering are:

- Will I lose face or my job because of this?
- What other things am I doing wrong?
- If only I did....
- What can I really depend on?

By dwelling on questions like above, the attention is taken away from the present and the problem at hand. Their scope is quiet narrow and likely will miss subtle messages that a log or metric analysis will show.

Recognition that we are in this mind state is the first step of breaking out. This could be followed by pausing before further action is taken, re-focusing on the issue at hand, and diving back in.

2. The Reflective Mind

Others may be more philosophical -- "stuff happens." They have a higher degree of confidence and a wider scope of the world. They pause, deliberate, and then react. If they were on such a call, they might be asking questions such as:

- Do I have all the right resources on this call?
- Have we accurately defined the problem?
- Are we noting as we are going along the things that we are doing to solve this issue and how we could do it better?
- How can we ensure that this issue never happens again?

And thinking like this, the likelihood of issue resolution increases.

You can see the tremendous difference between the two worldviews. One drowning in a river of emotion, the other dedicated to the issue before them. **Which did you choose the last time a stressful situation happened to you?**

I want to conclude with two items:

First, the story of Mohini. She was a White Tiger being kept at the Washington Zoo. For most of the time there, she lived in a 12 by 12 cage. There was those that wanted her to experience greater freedom, so a far larger enclosure was built. But instead of seeing the larger space, Mohini stayed in an area that was still 12 by 12. So it is with the contracted mind.

http://itrustican.blogspot.com/2011/09/story-of-mohini-white-tiger.html

I end with this quote from Mark Twain -- “I've had a lot of worries in my life, most of which never happened.”

Here to wishing that your life be filled with happiness and be free from self-imposed stress.

2.4 Dealing with "Nothing Changed."

https://communities.ca.com/community/ca-apm/blog/2016/02/28/dealing-with-nothing-changed

[Author's Note: While I use APM examples below, this approach can apply to any system or application software.]

Introduction

It was 2 p.m. on an overbearingly hot August day. I had been roused out of a wonderful dream. It appears that that there was a matter needing serious investigation. There had been a heinous crime and the likely culprit was being detained. Within twenty minutes my eyeballs were staring hard into the tearful youthful offender. Their crime? Crashing a fellow eight-year old's birthday party and snatching a piece of cake without permission. Oh what an egregious deed! I could see the signs of their nefarious activity throughout this person including cake crumbs on the chin, smushed icing on one cheek, and much more that I refrain from telling. With as icy a glare that I could muster, I coldly spoke. "Well young Tommy Sherman, things look bad for you. Perhaps I can get a deal if you confess. Let's cut to the chase, what took place this afternoon at the birthday that you were unauthorized to attend? Spill it"

"Why mister nothing. Nothing happened."

While not as dramatic as the above scene, the response "nothing changed" does occur a good deal when initially looking at a case. This blog discusses why this is and what to do to counter it.

Why Do People Say Nothing Changed?

There are variety of reasons for this

- Customer sites have many networks and applications. So it can be hard to determine what was done and which networks/applications were impacted.
- People have limited scope. Someone in a network group may only know about some networks and not about applications. So they may not be aware of other changes.
- A complete analysis has not been done to date. So all changes/errors may not have been uncovered.
- Frog in boiling water. A rapidly growing environment that is not thoroughly monitored may have finally hit some capacity or metric limit.
- Understanding the impact of a single change. Someone may have been aware of a change but not its impact

How does one counter "Nothing Changed?"

- Take a larger view and look at change control approvals and results for that time period.
- Review operating system logs and events to see what was taking place. Perhaps it was an operating system error or third-party software was installed at that time.
- Use metric graphs to see what capacity and throughput looked like from the time of the issue and thirty days back. Is there a sudden spike in the present or all throughout? In some cases, such as MTP logs, you can determine the total number of packets across

seven days to determine if there is a sudden increase or decrease of traffic.
- See if new errors are only in the log at the time period of interest
- Check the date of when configuration files were last updated. If done around the same time as the issue of concern, there may be something worth investigating
- Implement a health check to assess the APM cluster health.

- Implement after action reviews (AAR) to limit negative impact of configuration changes.

Conclusion

In conclusion, while investigating, do not jump to conclusions whether something changed or not. Do your due diligence by analyzing logs, metric graphs, traffic etc. and a clearer determination of root cause and likely events will be probably reached.

As for young Tommy Sherman, he got off with a stiff warning. As far as I know, he never crashed another birthday party ever again.

2.5 How I Blew Up my First APM Cluster

URL: https://communities.ca.com/community/ca-apm/blog/2016/03/06/how-i-blew-up-my-first-apm-cluster

[Some months ago, I received an oddly-shaped oversized package in the mail with no return address. It contained a barely readable handwritten document and a Betamax video. I reflected for some time whether to release or not. But with April Fools' Day around the corner, it seemed like a good time to publish. Unfortunately, the video had nothing on it but the manuscript provided the following chilling tale. Read at your own risk.]

This may the last thing that I ever write. I have been running for such a long time and about to be cornered.

Oh my company, I am so sorry for what I did. If only I could go back in time and undo my misdeeds.

It started so simply. I was hired as an Application Performance Management administrator at Glowski's Insurance, a fifty-person company, gently nestled somewhere in a western mountain range.

My whole job was to keep the application performance metrics coming in and the dashboards lit up. I wasn't given much training so I let pretty much things run themselves. That was my first mistake. The monitoring software needs to be managed actively.

I also aggravated the situation by adding many more applications to monitor. That made the application teams happy while they could graphically depict how their systems were doing in peak times, analyze historical trends, and much more.

That was mistake #2. You should never make a system do more than it is capable of handling.

As I increased the load on the monitoring system, I kept the default settings and failed to adjust them to the new conditions. That was my biggest and last mistake. Capacity monitoring and configuration modifications are always needed when conditions change.

Then one day, all things came to a head. The system became sluggish, dashboards and graphs were blank, and the application went down. The company was running blind. All heads started to turn in my direction with scornful looks. I could not take it any more and fled.

So if you are an APM admin, I beg and plead with you, don't follow my example:

- Read the manuals to understand what is going on.
- Tune your settings to increases in metrics and monitored applications.
- Study if later releases can improve performance.
- Review the logs twice a week at least to see what is happening.

Looks like this is it. I see bright lights flooding the windows and the pounding steps of many people heading ever closer to my door. If only I...

[The manuscript ends there. What happened afterwards may never be known.]

2.6 The Case of the Failed APM Administrator Turnover

URL: https://communities.ca.com/community/ca-apm/blog/2016/03/13/blog-the-case-of-the-failed-apm-administrator-turnover

[This is inspired by true events.]

Three Months Before:
I am an APM administrator at Fracas Boating. We are the number 3 manufacturer in the 8 polluted rivers region. I just gave my notice as I get to live in my dream location of Lower Pluto. My current bosses want me to prepare a turnover document before I leave to help my successor. Sure. There was nothing written down before I came on board. Why should I help the next gal or guy? They should be smart enough to pick it up on their own. No, far better use of time is planning my first climbing expedition after I arrive on my new home

Two Months Before:
I am so happy. I just started my dream of being an APM Administrator at Fracas. What a joy this is. Everyone is so nice to me. I am going to greatly enjoy this.

One Month Before:
I am enjoying the job but found out my predecessor left nothing behind. I am digging into the manuals and trying to figure out the operational procedures, location of configuration files, etc. This is taking a good deal of time.

D-Day (Ending One)
Today I gave my notice. It is too much stress with everything breaking down and trying to document how things should work. Well, I will delete my "ramp-up" document before I leave. Why should I help the next gal or guy? They should be smart enough to pick it up on

their own. Hmm, maybe I should read more about the rumors about the next **Galactic Chef** movie. The action scenes are rumored to be over the top!!!

D-Day (Ending One)
Today was a true nightmare from start to finish. The network configuration was changed, the private keys expired, the configuration files were modified, and everything stopped working. I learned my lesson. I am going to dig in, document all this, and start saving important files. I vow to not only help myself but my successor as well.

Aftermath

Sadly, I hear this story far too often. A new APM Administrator comes into an office filled with piles of paper and has to figure out how to keep things running and what to do if they break. Some never succeed in doing this.

When writing a turnover document, you should think, "What would I need to know to have a running start on the job?"

A turnover document may include
- Location of key configuration, backups and other files.
- Any expiration dates
- Key stakeholders and contacts
- A run book of operational tasks
- Best practices
- Suggested next steps for the next one, three, and six months.

If you are truly customer-focused, then a turnover document will increase the possibility of operational stability for your present and soon to be former customer. It helps maintain good relations and many more benefits

2.7 When Software Goes Bad Part 1: Occam's Razor

URL: https://communities.ca.com/community/ca-apm/blog/2016/04/10/when-software-goes-bad-part-1-occams-razor

Introduction

This should be the best of times. Being in the earliest twenty-first century, application software should be moving along swimmingly transparently transitioning changes made in capacity, configuration, and architecture. We should be the golden age of computers as described in glowing terms years before by science fiction writers. But this is not the case.

This and the next blog will explore several reasons why this is so.

Occam's Razor Cases

One such category is Occam's Razor problems. It basically states *"Among competing hypotheses, the one with the fewest assumptions should be selected."* This is popularly said as *the simplest explanation is usually the correct one*.

15-20% of the cases that reach Support are "Occam's Razor cases.

That means they can be solved by undoing some fairly avoidable simple causes. In theory, these should be easy to detect. This includes

- The AC adaptor is not plugged in.
- The network cable is not plugged in.
- The switch is not configured to send traffic to a network card.
- The software was never configured to capture traffic from a particular server. Instead, it is filtering it out.
- The network cable is plugged into eth1 instead of eth2 on a Linux box.
- There is a typo in a configuration setting.
- A configuration setting is disabled when it should be enabled.
- Multiple people are changing a configuration file, each without talking with one another.
- The network team makes a change in network traffic without telling the application administrator.
- A third-party software is installed on a server without anyone's knowledge causing issues due to changes in security settings/ports.

Can you see a pattern?

- Changes made but not told to relevant stakeholders.

- Causes and conditions as a result of human error.

- Non-verification after a change is made.

What can I do about this?

So how can one determine if you have an Occam's Razor situation? Here are five suggestions:
1) Determine if truly nothing changed.

2) Question your assumptions and expectations that all is really well.
3) Verify your assumptions.
4) Do a weekly inspection of the server and software settings. That is to check all is as expected.
5) Do an After-Action Review if running into an Occam's Razor case to avoid it happening in the future.

6) Deliberate and research before making a change. Verify afterwards that the change has taken place.

I would be interested in hearing if this has happened to you and what you did to avoid it happening again

2.8: When Software Goes Bad Part 2: Edge and Corner Cases

URL: https://communities.ca.com/community/ca-apm/blog/2016/04/10/when-software-goes-bad-part-2-edge-and-corner-cases

When Software Goes Bad Part 1: Occam's Razor -- Part 1

Each day, the decommissioned USS Yorktown (CG-48) sits in some Navy Yard in Philadelphia awaiting the order to be dismantled. Once this happens, then there will be no trace of the mistake caused by a simple *edge case*. In the Yorktown's situation, it was part of the leading edge "Smart Ship" program that used computers to control ship's systems. But human intervention outsmarted the application. Someone entered in a zero as a value. This caused a division by zero error. After this simple entry, the ship's propulsion system became non-operable. (For how long the ship was out and whether or not they were towed back to port remains a topic of hot debate.) In the long term, this made little difference. The *Yorktown* has a stellar record in keeping the United States and her allies safe overseas.

Per Wikipedia, edge case is "a problem or situation that occurs only at an extreme (maximum or minimum) operating parameter." A corner case is one outside of typical parameters. This may involve multiple factors

Capturing and resolving edge and corner cases may be one of toughest things to determine or track.

This can include

- Minimum or maximum values

- Invalid or random values

- Non-compliant conditions for a protocol.

- Any unexpected condition or combination of conditions.

So what can be done about edge cases?

- Allow time to test extreme values and unanticipated conditions.

- Have users do "random entry" testing the system's interface.

- Use software that is fully compliant with a protocol rather than compliant-like.

- Perform rigorous testing of various expected and unexpected conditions.

- Use something like Fuzz testing to test for "invalid, unexpected and random data."

In the end, you may not get all of the weird and offbeat conditions that may cause crashes under the control. Still, you do the best that you can to minimize the "surprise factor" when an application gets put to good use.

As always, your comments on this topic are welcomed.

2.9 Disarming the Power and Frustration of Error Messages

URL: https://communities.ca.com/community/ca-apm/blog/2016/04/24/disarming-the-power-and-frustration-of-error-messages

Introduction

It was another non-memorable Friday when Sam entered the building. The place was deserted like any island resort on receiving a tsunami alert. Inside the entrance was a large hallway. At the end of the hallway was a large automated teller. He pressed the appropriate buttons and saw the following error, "E201a: Your money is not withdrawn yet since the end of this location is coming in the next ten minutes. Please wait."

This blog is about error messages and what can be done about them. Wikipedia defines an error message as " information displayed when an unexpected condition occurs, usually on a computer or other device."

This may be accompanied by a graphic that may or not be amusing.

Error Messages: The Current State
People do not like bad surprises such as crashes, slowness, freezing etc. with their software and hardware. Since nanites are not yet shipped with hardware/software, they are not yet self-correcting.

That means that we must rely on error messages that:

- Are terse
- Do not tell us what is happening/has happened
- Provide no steps on how to correct it
- Tell us where the error has taken place
- State the importance of the error message
- Whether or not it can be ignored
- Cannot provide historical context if this has happened before.

Given most of these appear in a pop up box, their level of detail is purposely limited.

As a result, you may search online or through a knowledge base for an answer. But knowing that error message may not give you the complete context as to what is happening. That is why Support people like full logs rather than snippets.

In some places in the code, there may be no error messages at all. So a special debug version may have to be created to get a better understanding as to what is taking place.

Error Messages: What Could be Done.

In addition to minimizing software exceptions, the following should be done.

- Provide an error guide or all or top 20 errors.

The former is done by Oracle and APM Agent Command Center. I expect this effort to be expanded for future APM features.

The latter is done also by APM see Troubleshooting common-errors and resolution

For Oracle and APM, the message has a taxonomy on the error number range and what each means. Each Number has a description, cause, and action. A description of the associated file is provided.

- Make errors highly visible AND readable.

In addition to the above, the exception handling should ideally:

- Capture logs at time of exception. Not doing this hampers support case resolution
- Not corrupt files
- Provide an undo feature
- Provide a simple way to resolve the issue
- Tie this to alerting & graphical performance system screen to view historical trends of this exception

I am making it a personal mission for 2016 to document as many error of the APM CE (CEM) messages as I can. Recently, I documented many of the previously published Transaction Discovery (autogen) Error messages

Other Knowledge Documents will follow.

I look forward to your comments on this topic

Other Sources:

Four H's of Writing Error Messages

Error Message Guidelines

2.10 Is Software Support a Good Career Choice for You?

URL: https://communities.ca.com/community/ca-apm/blog/2016/05/15/blog-is-software-support-a-good-career-choice-for-you

[The opening is a nod to Jack London's *The Scarlet Plague*. Learn more about this work at https://en.wikipedia.org/wiki/The_Scarlet_Plague]

It was to be the last camp fire for the Old One. He had lived during the time that there were cities, car, planes, and other amazing things. But life as he knew it changed in such a short period of time. The water supply became infected with an unknown virus. And almost all humankind rapidly perished. Only a few survivors remained, living in forests. In time, the remaining vestiges of an advanced civilization would be covered over by vegetation.

The Old One did not have long to live. Before leaving, he wanted to impart his wisdom on those that would succeed him. He started to tell his story.

...Then one of the impatient youngsters interrupted, "Didn't once tell us that you used to do one time something called Software Support? Tell us more about this."

Just by the mention of the words "Software Support" opened the floodgates of wonder and horror for the Old One. He declined to discuss that topic further and talked instead about his treasure trove of knowledge that he was leaving behind.]

This article discusses the tradeoffs of going into Software Support as a career. It does not have to be the horror show alluded to above. In fact, the opposite is more often true.

The Advantages

1. You get to refine your problem-solving skills and knowledge across multiple disciplines. Today's software touches across many areas such as integrations, networks, databases, applications, hardware. You get to be an expert in many areas.

2. The camaraderie is tremendous. Management and employees are all working together to have happy customers and produce stable, scalable environments. I found that the case here at CA Technologies.

3. Time and training is provided to keep you current. This is often taught by the developers themselves. You can also install and work with beta software before public release.

4. You get to work with a lot of internal groups. Product Management, Professional Services, Pre-Sales, Communities, Knowledge Management, Documentation and more. Together you can make a big difference as to the customer experience

5. You have an opportunity to improve the product through submission of documentation and software bugs. Or through knowledge documents.

6. You have a chance to provide a sense of service to others and yourself. See https://communities.ca.com/community/ca-apm/blog/2016/02/21/on-service-and-apm-support

The Disadvantages

1. You are often on your own. It may involve looking at terse error messages. See https://communities.ca.com/community/ca-apm/blog/2016/04/24/disarming-the-power-and-frustration-of-error-messages. Things are underdocumented or undocumented. New scenarios are discovered. This can be a challenge for some people dealing with heavy periods of uncertainty.

2. You get to deal with some people very emotionally charged due to ailing systems. See https://communities.ca.com/community/ca-apm/blog/2016/02/14/contracted-vs-reflective-mind-an-owners-manual. On the other side of the coin, it offers a chance to develop a reflective mind.

3. Time and issue management is always a challenge. You may have the day planned out and something may come along to take up the next two weeks. You may also have the occasional on-call support.

4. Mental and physical challenges. It may be a struggle for some not to become cynical, burned out, or have health issues.

In summary, Software Support is not for everyone. But for those that enjoy its numerous rewards, it can be a very rewarding career.

2.11 Thriving in Times of Certainty

URL: https://communities.ca.com/community/ca-apm/blog/2016/05/28/blog-thriving-in-times-of-certainty

Introduction: It's a VUCA World?

(Thanks to Pixabay for providing commercial-free photos.)

There are those that see the world as bursting with **VUCA** (**V**olatility, **U**ncertainty, **C**omplexity, and **A**mbiguity) as if this is a unique and new thing. They spend countless hours attempting to offset the great unknowns of their times.

But you can look at most time periods in history, you pretty much find the same thing. So this is not a new trend. Just maybe a little more of it. When dealing with computing infrastructures there are at least five themes that keep reoccurring. Some IT veterans have worked both sides of the issue spectrum at least twice. If you understand the tradeoffs, your career and organization will stay afloat and move ahead. What is the right answer depending on what is best for your organization for the present and near future.

Five Themes

These themes include:

1) **Company-staffed or third-party?**

The days of companies' performing all IT functions are of the distant past. Companies are outsourcing various staffing needs as well as their computing infrastructure. Physical versus virtual, in or out of the cloud are related concerns. Costs, level of service, outsourcing company culture and infrastructure stability are all factors to consider. Outside of the computing industry, many of these arguments are being replayed recently with the debate over the possible outsourcing of TSA responsibilities to be more responsive to long security lines. (Note: This is done already at San Francisco and smaller airports.)

2) **Centralized versus decentralized?**

This is somewhat like the first item. Centralized environments may be able to set company-wide standards and have less redundant staff. But they could be more bureaucratic to the needs of a business unit than a local group. Sometimes overlooked is a hybrid model which is centralizing those things that make sense and decentralize all others. Dialogue on this topic can also be found between federal and state governments, state and local governments, regional versus city government. Don't expect this to be solved soon as the pendulum swings back and forth.

3) **Reactive versus Proactive?**
I have discussed this at length in earlier articles. Proactive takes more organization and time. But eventually should result in optimized, secure systems having less downtime. Others would rather "pay as you go" and only deal with things when they break. And if outages occur, then do typically minimal changes. A real-world version of this can be found on how visits you have go to the dentist. This can depend on the degree of proactive flossing and brushing versus benign neglect.

4) **Standard versus Proprietary?**
In theory, standards mean that you would expect a minimum set of behavior across hardware or software. Some vendors either ignore standards and make their own internal approach or "improve" the standard with proprietary add-ons. Others reverse-engineer proprietary software with their own clone. One example of what may happen with standards is HTML. No two browsers handle a HTML 5 web-page the same way. So rigorous testing and requirements gathering is recommended on what product(s) make sense for you.

5) **Legacy versus New Software?**
This is not an easy question. Do you keep your old software that is dependable and you know in or out? Or do you buy something that may be more modern, responsive, scalable, and feature rich? And a secondary issue is do you build your own or buy technology. Again, the answer is always what makes sense for your organization as opposed to being a given answer.

I would love to get your take on how much of your work life is spent on grappling with these larger themes and what have you learned in the process. Please share your thoughts.

2.12 The Gentle Art of Remote Support Communications

URL: https://communities.ca.com/community/ca-apm/blog/2016/05/29/blog-the-gentle-art-of-remote-support-communications

[My thanks to the fine folks at Pixabay for their free illustrations.]

Introduction

In the modern world, many conversations are not face-to face. They are often with people that we never have or ever will meet. We may not know what they look like or what their favorite food is. What are some of the things that we can do to make this a success -- especially for Technical Support Staff?

Nine Guidelines

1. Remote communications even under optimal conditions are never easy. So work hard at it. Don't assume that your words were understood. Take nothing for granted. Always ask if there are questions or concerns.

2. Come from a place of service. Offer a caring attitude to your audience. They are the most important thing in your life at that time.

3. Offer a reflective mind. Add nothing extra to the equation regardless how you feel that day. Keep the feelings to yourself.

4. Have a Beginners Mind. Treat the conversation as this is the first time you ever had this discussion rather than go in with preconceived notions and set objectives.

5. It is all a dance. So have fun with it and enjoy the ride. Let the conversation go through its various twists and turns. Sometimes it may drift. But that's okay. Being slightly off-topic may reveal other insights.

6. Deep Listening. Listen beyond the words to what is really being said, what is not being said, and what the person is feeling.

7. Humor at Times It may not work with all audiences and all situations. But keeping things light can be an invaluable aid.

8. Active Listening. Show you understand through reflective listening. Give the speaker the needed time to be heard and understood.

9. WebEx's/Illustrations. Both parties seeing the same thing rather than verbally describing something can help move things along.

Please let me know the techniques that **you** use for this increasingly important area.

2.13 Life Choice: Scarcity or Abundance

[Thanks to the folks at Pixabay for their fine free images.]

A journal entry from an 9-year old girl.

"Dear Diary
Today was such a hard day. We were going to visit Grandma and Grandpa which is always FUN!!! We were taking a BIG plane. To get to the plane we went to an airport. It was so pretty with many colors, sounds, and things to see. I just wanted to look at each one of the places we passed because they were so fascinating. But Daddy kept screaming and pulling at me, 'C'mon Penelope, we have five minutes to get to the plane.' It seemed SO UNFAIR. I just wanted to stay and explore. But no, we had to rush. Now, I will never know what I missed."

Introduction

The hyphen between our birth and death years is what constitutes our life. Along the way, we make many choices on how we live it. An often overlooked selection is *do we come from a viewpoint of scarcity or one of abundance*?

Many things happen in our world from a scarcity viewpoint. Television content is spoken at accelerated speed. Headlines talk about the impending lack of resources. Multiple things need resolution NOW. And our lives are overbooked to the max between sunrise and sunsets.

If we follow a path of scarcity, there is eventually regrets about lack of something or other. We wonder where the time was spent between all the rushing here and there. We may be more productive in one sense. But life may seem to be unfulfilling. We may recognize the discomfort but keep on doing the same old same old.

Is Abundance a Real Possibility?

If we follow a life of abundance, then...

* You don't schedule things back to back. You allow things to take as much time as they require for resolution.

Tasks and meetings may take longer or shorter than expected.
* You allow time to look at alternatives and distractions which may lead to a stronger result.
* You are kinder to yourself as well as others.
* You are more likely to have higher sense of satisfaction and accomplishment.
* You are less likely to have the baggage of disappointment from not meeting pre-conceived expectations. There is also less fatigue and disorientation from overscheduling.
* There is more time for silence, deliberation, needed kindness to yourself, and reflection.

Can such a lifestyle be achieved during much of the 12 hour work day? I believe that it can if you keep working at it. Just raising the question opens us to infinite possibilities.

Conclusion

As I create this article, I have no outline in front of me. There is no expectation on how long it will take or how many words it will contain.

I just write and revise as many times as needed while listening music that also has a sense of spaciousness.

This is my last article in a loose series of articles of thriving in these challenging times. I plan to shortly put these in a PDF for distribution. Keep watching this space for availability.

Please let me know if they have been helpful and share your survival techniques

2.14 TIM Deployment Failures and the Rebirth of a Documentation Classic

URL: https://communities.ca.com/community/ca-apm/blog/2016/06/19/tim-deployment-failures-and-the-rebirth-of-a-documentation-classic

Introduction
Some of the best documentation that I have ever created was out of strong motivation to improve dramatically a situation. *The TIM Readiness Guide* or as it is officially known as *TIM Network Connection Readiness Guide -- Setting Up and Validating a TIM Network Connection for all CEM/APM Versions* was no exception.

Dooming a TIM deployment.

Along the way, there are a series of things that can be done ensuring a TIM was ready to monitor traffic before a successful Services engagement. Those that did so generally ran into no monitoring issues. Not being completed meant that the engagement was highly likely to have difficulties hindering completion. This is one area you should not wait typically until the engagement starts.

Typical failure points were:

1) Tim being placed in the wrong place. So it was not seeing any traffic, traffic from the wrong subnets, or seeing one-way traffic. This also could be impacted by load balancers, firewalls, and reverse proxies.

2) Connection between switch and TIM misconfigured or not optimal. So the unneeded protocol traffic was sent to the TIM was sending more data than the TIM could handle (resulting in dropped packets, or traffic sent was of different speeds (resulting in high out of order packets.).

3) TIM installation not approved by a client's security group.

4) Private keys not obtained or deployed successfully.

5) Application groups giving incorrect information on which IP addresses to monitor. Or it was not decided in time which applications to be monitored at all.

The interesting thing is that many of these were avoidable with proper planning. Proactive sites successfully performing the required tasks generally meant that Services would have a smooth engagement.

Not completing this meant the engagement could be delayed or never completed. In those rare cases that this was discovered after the fact, the Services person could be sent home until the environment was ready.

The TIM Readiness Guide

Out of the desire of wanting all engagements to be successful,, I created the TIM Readiness Guide.

It basically takes you through a series of questions and steps to verify that your TIM is truly ready to monitor traffic. I tried to also make it easy to do and verifiable.

Over the years, this Guide was expanded to include APM 9.x, more on SSL, TIM networking tools, MTP, the APM Field Pack, and more. It has saved countless deployments from starting off on the wrong foot.

It also was provided as part of a starter kit that included a site application monitoring questionnaire, a readiness checklist and deployment schedule. A high-level document on TIM setup was also sent to CA project managers.

The TIM Success Guide

Tired of travelling each week, I moved over to APM Support. And I learned all about the TIM over again from a different perspective. I started to see how an equivalent effort was needed to keep the TIM healthy after deployment. Proactive administration meant not seeing sluggish performance, crashes, dropped packets, delays to reporting or no reporting at all.

So that's when I decided to do a rewrite of the *TIM Readiness Guide* to talk about the major things (many that are simple) to detect an unhealthy TIM and how to rectify it. The new name is the *TIM Success Guide*. I expect part one (Overview) to be out shortly. Early reviewers have found it helpful.

The TIM continues to be an undocumented and underdocumented area of APM. I am trying to rectify this by writing an onslaught of KBs, Tech Tips, and blogs. I don't plan to stop anytime soon.

Thank you to those that had shared this journey and provided me feedback on how to improve these documents.

2.15: Why I stopped writing APM Blogs and then Started Again: Part 1

URL: https://communities.ca.com/community/ca-apm/blog/2016/12/18/2016-why-i-stopped-writing-apm-blogs-and-then-started-again-part-1

Introduction

The first half of this year I was writing at a fast pace:

- 14 Blogs
- 7 Tech Tips (One a month as I have done since 2011).

Then I went silent for five months until now.

This was unnoticed apparently since there were no comments or emails to me asking why

So what happened?

In July, I was nominated to take a Lean Six Sigma Green Belt course at a CA campus.

This was the first year that they allowed Support Engineers to attend.

From Wikipedia -- Lean Six Sigma "is a methodology that relies on a collaborative team effort to improve performance by systematically removing waste."

To obtain the Green Belt, I had to

- Attend all five days of the INTENSE class
- Take and pass an in-class exam
- And complete a Lean Six Sigma Project in 6 months (By January 31 2016) including getting the participation of an executive sponsor.
- Still do my day job and keep my wits about me.

I will save for my next blog about the project itself. I made a decision early on to go "all in" which meant long hours on nights and weekends.

It also meant giving up things temporarily that I love doing like publishing APM blogs and Tech Tips.

So until the project was completed, I stopped writing articles in my favorite Community. Happily, the project got completed (in 5 months with an option to go on for one more month.) So now that I have all this free time , I will resume writing again.

And there is a lot to write about with all of the changes and opportunities with APM. I hope that you "watch this space" and read them when published.

Thank you for all of the support and kind words throughout the years.

Happy Holidays and may 2017 fulfill all of your wildest dreams!!!

Section 3: Tech Tips 2016

3.1 TIM Trace Options -- The Missing Pages Part 1

URL: https://communities.ca.com/message/241847328#241847328

Introduction

Proper use of the TIM trace options can be useful in solving a variety of issues. Some of these include:

1) If seeing network traffic at all
2) Which servers the TIM is seeing traffic from.
3) Is the traffic to the TIM two-way showing the HTTP request and response?
4) SSL issues such as ciphersuites and TLS versions used.
5) Network data quality issues (OOO packets, packet resets/terminations, etc.)
6) Transaction definition issues such as transaction counts, respone time, transaction component issues, etc.
7) HTTP Plugin issues.

This article gives an overview on TIM Trace options and responsible use.

Overview

The TIM Trace options are configured on each individual TIM. This is done by going to the **System Setup page**, then select TIM, **Configure TIM Trace Options**.

The appropriate programs read the trace options checked and saves it in a text file named tim.options in the TIM config directory. This file cannot be edited. The TIM web server is notified of the changed trace options

Here are some guidelines on TIM trace options.

1. **TIM Trace options should be turned off unless needed for debugging**. This is especially true for busy production networks. If left on, the TIM may restart due to excess CPU/Memory. On MTPs, it may also result in a full RAMdisk directory. TIM logging levels should be checked early if there are TIM performance issues.

2. If debugging with Trace options, only turn on the trace options truly needed. This is discussed in Part 2 to be published next month.

3. Note that certain TIM settings may add or subtract what appears in the TIM log or the content of the messages. Especially of note are the following:

- Enabling plugins

  FlexPlugin/Enabled = 1

  FlexAMFParser/Enabled = 1

  FlexAMFXParser/Enabled = 1,

  and XmlPlugin/Enabled = 1
- Enabling tracing
  SiteMinder/Trace = 1
  AllXmlParams = 1 if wanting every XML element and attribute rather than those that match a parameter definition
  BtStats/LogLevel = 1 or 2

  (1 = Messages are written to the TIM log when BtStats files are written,

  or 2 = Same as messages, verbose mode)
- Autogen/Trace = 1 or 2. This is for transaction discovery. 1 = Traces autogen definitions creation 2 = Additional detail messages

3. Use the TIM Trace Filters to limit traffic to a particular client/server IP address, browser language setting, or HTTP parameter.

4. Try to make TIM trace options the same across all TIMs. This produces consistent logging.

Additional Information.

Here is an incomplete where to look to find more:

-- Using TIM Trace - https://docops.ca.com/pages/viewpage.action?pageId=275682398 options for troubleshooting.
-- Using TIM Trace options for transaction identification.
- https://docops.ca.com/display/APMDEVOPS101/Transaction+Identification - https://docops.ca.com/display/APMDEVOPS101/Setting+up+CEM+to+support+nCipher
-- Using TIM trace options with nCipher.
- http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/TEC1281821.aspx

-- Which TIM trace options to use when debugging issues. We will return to this next month.
- http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/tec610515.aspx

-- How to parse a TIM log by IP
address.
- http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/tec600884.aspx

-- TIM loggings can create a MTP
no space or TIM restart condition.

3.2 APM Tech Tip: TIM Trace Options -- The Missing Pages Part 2

URL: https://communities.ca.com/message/241853574#241853574

Introduction
Last month, we started to dive into the underdocumented and largely misunderstood area of TIM Trace options.

See https://communities.ca.com/message/241847328#241847328 for Part 1. We went over some guidelines for TIM Trace options.

This month we continue the overview.

Behind the scenes

So from the TIM System Setup page via your browser, you can view and set the TIM trace settings. But what is happening behind the scenes at a high-level?

In your <tim_home>/config directory is a dynamically created file called tim.options. The contents look something like this:

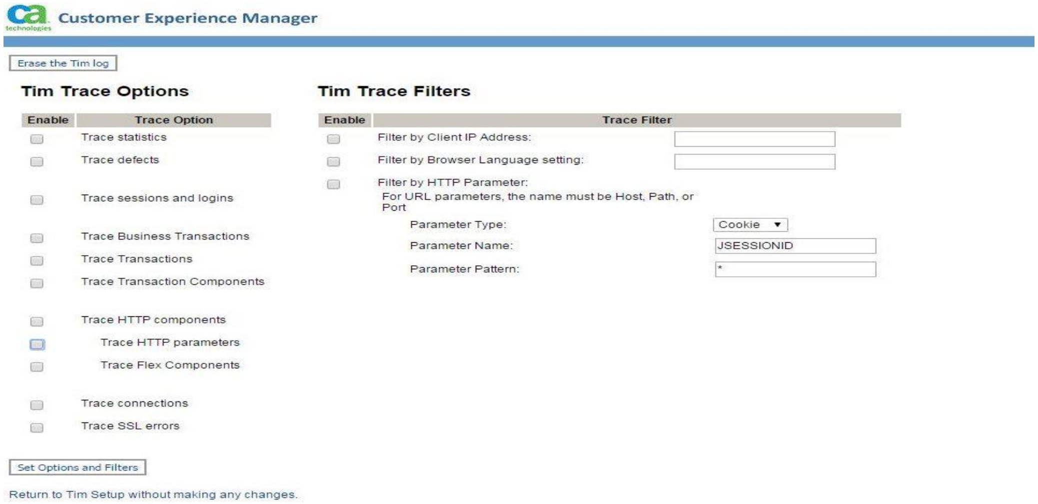
```
# This file is generated automatically -- do not edit.
# The script that starts tim reads options from this file.
-tracetransets
```

-tracetranunits
-tracematchedtrancomps
-traceallcomponents
-traceparameters
-traceconnections
-tracessldebug

So, depending on your operation on the web page, you are either reading or writing values to this file. Fortunately, this can be done without a TIM service restart. In addition to writing these new values, the TIM also has to be informed of the TIM trace options and immediately start using them.

TIM Trace Options

Below is what the TIM Trace Options page looks like.



Customer Experience Manager

Erase the Tim log

Tim Trace Options

Enable	Trace Option
□	Trace statistics
□	Trace defects
□	Trace sessions and logins
□	Trace Business Transactions
□	Trace Transactions
□	Trace Transaction Components
□	Trace HTTP components
□	Trace HTTP parameters
□	Trace Flex Components
□	Trace connections
□	Trace SSL errors

Tim Trace Filters

Enable	Trace Filter
□	Filter by Client IP Address:
□	Filter by Browser Language setting:
□	Filter by HTTP Parameter: For URL parameters, the name must be Host, Path, or Port Parameter Type: Cookie Parameter Name: JSESSIONID Parameter Pattern: *

Set Options and Filters

Return to Tim Setup without making any changes.

What does each setting show?

- *No options* -- Shows startup log output, OOO Packets Web Server status
- *Trace Statistics* -- provides various system statistics
- *Trace Defects* -- Gives useful information on whether a defect or not was produced and for which transaction(s).
- *Trace Session and logins* -- Gives session and login values for each monitored transaction being processed. Useful in knowing if a login/session id was found or not.
- *Trace Business Transactions, Transactions, and Transaction Components*. -- These three options provide information about the various levels of monitored transactions including parameter/value pairs, client/server IPs, transaction name, etc.
- *Trace HTTP Components/Parameters/Flex Components* -- These three options act like a sniffer displaying HTTP/HTTPS/XML/Flex Request & Response information.
- *Trace connections* -- Trace the connection Open, Reset, and Close operations for the traffic that the TIM is seeing.

- *Trace SSL errors* -- Shows messages about unsuccessful TIM SSL processing including cipher suites, SSL/TLS version, ability to decode SSL packet, and more.

In addition to this, there are TIM Trace Filters on the right hand side to show only traffic:
- from a specific IP address (Note this can be set to a client or server IP)
- browser language setting
- HTTP Parameters
    - Parameter Type (Cookie,Post, URL)
    - Parameter Name (Such as JSESSION except for URL Parameter Type that must be Host,Port,Path.)

Notes:

1) This is an include not exclude filter and only one HTTP parameter filter can be reset.

2) Selecting Erase the TIM log only clears what displays on the screen for a log. The log physically still exists. Again, changes made on this page do not require a restart

Next month we wrap up by telling when to use each option. Until then I see you on the Community and webexes :-)

3.3 TIM Trace Options -- The Missing Pages Part 3

URL: https://communities.ca.com/message/241858839#241858839

[Personal Note: This is my **60th** Tech Tip more or less. Number one was created July 2011 and can be found at https://communities.ca.com/message/22049399#22049399.]

Introduction

This month we conclude our look at TIM Trace Options. The prior chapters can be found below:

https://communities.ca.com/message/241847328#241847328 **Part 1: Overview**
APM Tech Tip: TIM Trace Options -- The Missing Pages Part 2 **Part 2: What options are available.**

But the real purpose for the examination of this overlooked area is going into the rationale behind the following Knowledge Document.
http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/TEC1281821.aspx

Tim Trace Options Rationale

1) Going up the OSI Stack

Using the OSI (Open Systems Interconnection model) Model can be helpful in debugging TIM issues. The following is a typical bottom-up approach that may not be needed for all cases

2) Do I have a network connection and seeing HTTP/HTTPS/Flex traffic correctly?
This includes answering a series of questions like the following progression:

- Do I have traffic at all?
- Is it HTTP/HTTPS/Flex traffic?
- Is it two way traffic?
- Is it traffic from the desired web servers?

Note that the TIM Readiness Guide also covers this. See https://communities.ca.com/docs/DOC-101446785

To determine this, tracing connections and HTTP Components/parameters are helpful. You can see the IP addresses the TIM sees, if the traffic has Opens, Resets, and Closes, see if HTTP Requests/Responses, determine if the network/servers changes the IP address along the way, is truncating information and so forth

3) Am I decoding SSL traffic correctly?
- TIM is limited what it can give you currently. More information is

  provided about unsuccessful than successful transactions. What can be provided is the following:
  - Connection and IP information
  - TLS version and ciphersuite used
  - HTTPS decoded requests and responses
  - Out of order and other SSL-related errors

- This should be supplemented by a PCAP analysis with the private key installed on the packet analysis computer.

4) Am I having User/User Group Issues?
- TIM Trace options can be enabled to provide
  - Session identification values for monitored transactions
  - User values
  - Whether or not a user was assigned to a user group as well as the user group name.

5) Am I having Defect or Transaction Definition issues?
- TIM Trace options can be set to tell you:
  - If a transaction matches against a transaction definition
  - Which transaction definition was matched.
  - How many defects were created?
  - Which defect type was created and for which business transaction?

There are other uses of TIM trace options that I have left. Please respond to this posting on some of the other uses of TIM Trace options that you may deploy.

Thank you for positive feedback for the last five years on these Tech Tips. I plan to continue discussing APM best practices for some time to come. Please keep sending your topic suggestions, stories, and feedback to hallett.german@ca.com.

3.4 The Missing Manual Part 1: TIM Analysis, Monitoring, and Other Tools

URL: https://communities.ca.com/message/241870019

Introduction

This Tech Tip (#61) starts a new series about various tools that can help with analyzing SSL and TIM processing, monitoring the TIM's health, and other various TIM-related concerns..

This may be different because it ranges somewhere between a Tech Tip and a Blog. I want to also present these in a historical context and discuss what we are doing today in these areas.

Capturing TIM Artifacts

If you have opened even one TIM-related support case, you know that you are typically requested to provide a packet capture and ssldump output. I outlined the reasons for this in TEC596476 -- *Why am I being requested to provide a SSLDump/packet capture (PCAP) for the TIMSoft/MTP?*
. More on SSL and private keys.

TIM Analysis Tools

What are the tools typically used to analyze these artifacts?

* On the TIM, the packet capture is created using tshark or tcpdump. (Originally tethereal). How to use these tools to analyze network traffic is presented in the TIM Readiness Guide
* Generally we request a 25-30 minute pcap of TIM traffic and the corresponding TIM logs. Sometimes the packet captures are too large to analyze. So using the free tools splitcap or(editcap) can create smaller pcap files based on various criteria such as pairs of IP addresses.

* **Wireshark** or **NetQos Observer** can be used to analyze pcap files. In a relatively short period of time, you can determine:
- The quality of network data including number of packets that are out-of-order, missing data, duplicate ACKs, are empty. This can be done through following TCP streams, Expert Info mode, and Conversations. Most of these are available under

Analyze or Statistics menu options.
- Number of protocols (Analyze>Protocol Hierarchy), http servers, and requests (Analyze>HTTP or Analyze>HTTP2).
- SSL cipher suites available/used on server and client, alert codes, and more..
- And much more

* For Domainconfig files, I use the internal tool **TimConfigTool.jar** to do a simple graphical depiction of a domainconfig.xml. Since these files can grow quite large, it can be useful in determining issues with this important file.

* The TIM configuration/log compressed file displays the TIM settings in a helpful text format. However, if this was not the case, you could run **configtool** in the TIM console as outlined in https://communities.ca.com/message/241784125.

*SSLdump was last updated in 2004. https://sourceforge.net/projects/ssldump/files/ssldump/0.9b3/ It will show the cipher suits used and if a transaction is decoded or not. The TIM uses a modified version of ssldump to decode HTTPS transactions. SInce it is so old, it does not understand many of the current cipher suites and protocols. Use TEC1667615 to learn about your application(s) SSL setup.

I hope this has been of help. Next month, we will get into TIM Monitoring.

Questions for Discussion:
1. Which TIM-related tools/utilities do you use?
2. How are they helpful?

3.5 The Missing Manual Part 2: TIM Monitoring 1

URL: https://communities.ca.com/message/241876573

APM Tech Tip -- The Missing Manual Part 2: TIM Monitoring 1

Part 1

Introduction:

Last month, a new Tech Tip series was launched on TIM add-ons. At that time, we talked about some of tools that can be used to analyze TIM packet captures and SSL Health. This month we review the various present and historical tools to assess TIM health. I want to thank Joerg Mertin, creator of many of these utilities (unless otherwise noted) for his input on these articles.

He wanted me to correctly stress that regardless of which of these programs you use, a good understanding what is normal, sub-optimal, and unexpected behavior is key for keeping the **T**ransaction **I**mpact **M**onitors (also known as TIM) in your life happily humming along. Analysis without context means jumping at every error in the logs without comprehending the behavior behind the performance.

Historical Tools

The historical review below shows what was done in the past and how these tools have evolved since then.

SNMP Traps on TIM Health

In 2009, cemlogs2snmp came out. Its function was to provide SNMP traps monitoring TIM performance. This included applications running on the TIMs, hard disk health review, performance and load checks, and authentication history. Although it was meant for TIM appliances, it could be used today for those environments still relying on SNMP for alerting. However, if not using SNMP, the more powerful Monit solution discussed below may be appropriate.

netStat.sh

In 2010, Joerg came up with a handy script to assess the network health of the TIM. It would collect key information such as hostname, system name, memory/disk usage, network card information, TIM release, SSL key names, system files and more. This was a nice supplement to the information that TIM already collected. Around the same time, he created a variety of other scripts performing related TIM information gathering. So this evolved into apm-scripts starting in 2014 according to the changelog.

Today's Add-Ons

TIM Monitor Fieldpack

Chris Kline created the TIM Fieldpack in 2012 which is now maintained by Guenter Grossberger. Pat Shueh also helped with the fieldpack. It comprises of an EPAgent plugin and a management module with various APM dashboards. These show a graphical representation of the TIM watchdog status, TIM packet statistics, plugins enabled, TIM settings and releases, and TIM out of order packets summary information, and more. Metrics are provided every five minutes. Once implemented, then alerting can be enabled to notify about those times when expected thresholds are exceeded. The fieldpack works with MTP or TIM software versions. The last update was in 2015 and supports up to APM 9.5.

One of the limitations of the program is that it scrapes information from the TIM screens. So if the information is not on the screen, it cannot be captured. An example would be the number of files in the data/out" directory which would be a useful addition.

Monit System Monitor for MTP/TIM

Monit is an free, open source software package to monitor Unix-type servers. See https://mmonit.com/wiki/Monit/Monit. A TIM fieldpack using Monit was created by Joerg Mertin in 2015 working on MTP or TIM. It monitors key processes and file directories. If needed, it will restart the process or provide an alert. This includes when data/out and other directories gets filled up. Note that Monit is highly configurable so other scripts can provide additional monitoring if required.

Next month, I will dedicate an entire column to apm-scripts. Then wrap up in June with some of the miscellaneous TIM scripts available.

3.6 The Missing Manual Part 3: Tim Monitoring 2 (apm-scripts)

For those wanting to read the prior parts!

https://communities.ca.com/message/241870019 Part 1

https://communities.ca.com/message/241876573 Part 2

Also, a happy Mother's day to all!

Introduction:

This is the third of four tech tips on TIM monitoring tools. The topic will be a high-level look at apm-scripts. I want to thank Joerg Mertin for creating this tool and his insights used in the article.

Why is this needed?

The network has become a victim of its own success. It is relied on heavily to carry an ever increasing load of data of multiple and state-of-the-art protocols. Because of this, there may be issues with how clean network data is. (Such as dropped packets, out of order packets, TCP empty packets and traffic that is not compliant with TCP, SSL, or HTTP.) So having a tool to access TIM health and how it is handling network data and load is increasing crucial. This does not replace having knowledge of the operating system, SSL, TCP, and network/application performance behavior.

Overview

Originally this was a series of unrelated scripts created sometime around 2010 to gather network information (netstat.tar.gz) This evolved into multiple scripts that became complex to use. Instead, a GUI interface was created.Note this works for non-MTP and MTP TIMs. For the sake of simplicity, TIM here will refer to both types.

The most current version is 1.20-86 which collects pcaps. To help gather the most information about TCP and SSL, a copy of tshark and pstack is required to be installed on the TIM.

Installation of apm-scripts is done by untarring the included files and running a shell script. (apm-interact.sh). The software installs the various modules and files to perform the options below

The GUI and various collection options.

Once in the GUI, you may capture information using one or more options. These include: (Note that this goes far beyond just TIM to the EM, PHP agent, and APM database.)

1) CIPHER - If possible, gathers the SSL ciphersuites used by the web servers monitored by the TIM. It then checks if they are supported by the TIM or not.

2) EM -- Collects information from an EM including tess-default/customer.properties settings, versions, directories, errors, and warings, and more.

3) EXIT. Using EXIT,exit,quit, or q to leave the GUI.

4) PHP -- Gathers information on the APM PHP agent.

5) PCAP -- If the required libraries are in place, gathers a pcap (packet capture) file. I believe that this is done automatically in the new release.

6) PSQL -- Pulls key information from the APM database once it can log in such database processes information, database version, active queries, database file size, and much more.

7) SYS -- Retrieves summary data about the TIM's operating system. This may help quickly pinpoint system problems. Information gathered is OS version, Memory usage, network cards, drivers used, TIM thread analysis via pstack, TIM settings from TIM configuration files, network protocol statistics, SSL versions, network packet lengths, and much more.

8) TIM -- Collects TIM information such as operating system release, memory usage, system uptime, TIM version, network data statistics (such as OOO packets, SSL decodes), routing tables, iptables information, host tables, ethtool output ifcfg configuration file settings, and more.

9)TIMPERF -- Pulls in protocolstats, some system, and card information.

10) HWCOLL-- This last option gathers the TIM hardware and operating setting overlap

APM Performance Database

Once this information is attached to the case, it is uploaded to the APM Performance Database which produces graphical output that can be used to show how the TIM is doing over time. This visualization can help quickly nail unexpected behavior. This includes looking at CPU Load versus various operations (Connecting to TCP, SSL Sessions, captured packets), Memory use, Analyzed Packets,Login Sessions, Transactions, Packets forwarded, space on RAM Disk, and much more.

This only gives a small flavor what this powerful tool can do.

Next month we wrap up with some of the minor but still important TIM tools.

3.7 The Missing Manual Part 4: Tim Monitoring 3 (Miscellaneous)

URL: https://communities.ca.com/message/241894680

Previous Articles:
https://communities.ca.com/message/241870019 -- Part 1
https://communities.ca.com/message/241876573 -- Part 2
https://communities.ca.com/message/241882115 -- Part 3

Introduction
This is the last in a series on TIM add-ons and tools. This month we look at the miscellaneous TIM Add-on utilities . I thank Joerg Mertin for his updates on these tools . I hope this series on this previously underdocumented area were helpful.

Miscellaneous tools

1. APM OS root-password recovery fieldpack
This utility is useful for APM TIM appliances up to 9.5 and for MTPs (no release information provided.) It requires a web-based installer interface to use. This is a temporary workaround for those customers that may have forgotten or misplaced the root password. (Stuff like this happens. Be glad there was a workaround.)

What this does is add a rescue account (caddadmin) with a standard password. After installation, simply log into caadmin using puttty/ssh Afterwards, this is removed due to security concerns.

2. CEM SNMP Monitoring Fieldpack (CEM@Logssnmp)

In the past, monitoring everything with SNMP was important. (Although it is still heavily used by some customers today.) So with this fieldpack and using SNMP, the health of the TIM can be monitored. This includes

- Application monitoring
- Hard disk space monitoring

- System load monitoring
- Authentication failure monitoring

It can be configured to send out traps for all TIM events. There is also read-only SNMP Polling capability.

Note that the Monit and TIM Field Packs are more powerful and flexible than the above field pack. (These were previously discussed.)

3. TESSDocs

Sometime back, I used to create more Tech Docs than I do now. (Some of the long KDs that I create now could be transformed to Tech Docs.) A list of most of them can be found at https://communities.ca.com/docs/DOC-18610776

Joerg created a rpm file that included the various Tech Tips PDFs that both of us of created. Once installed, you could then access them on your TIM menu. These were updated from time to time.

4 . TIM Hardening scripts

While the TIM software/hardware in 9.0-9.6 was already hardened, some customers wanted it even more restricted. (In APM 9.6 onward, the customer is responsible for the operating system and related hardening. See https://communities.ca.com/message/241696644 for details.)

So a hardening script for RHEL 5 update 11 and RHEL 6 update 5.6 and later for APM 9.1.-9.7 was provided on request. Note that the hardening script does a minimum installation of the software and the hardening script can be configured as to what to harden.. This is the standard approach used for hardening

Joerg created in 2011 a detailed PDF that explains what is taking place during this hardening process. It includes step by step hardening including
- User access
- System startup
- Limit services to start
- Root remote password denial & password security
- Security fixes
- Sendmail hardening
- Directory hardening and more

This provides a thorough methodology that could be used to harden an APM 10.x TIM

That is it on this topic. Next month I will be back with another Tech Tip. Until then, stay cool and have some fun.

3.8 TIM/MTP Administration Responsibilities: Part 1 -- Model Shift

URL: https://communities.ca.com/message/241897636

Introduction

It has been two years since the TIM Administration model last changed. This new series discusses the changing responsibilities for APM administrators since the transition.

Since there are new readers to these Tech Tips (welcome!), it is best to review where we have been and are now.

Three Phases of APM TIM Administration Responsibilities

The paradigm of TIM and MTP Administration has gone through three distinct phases:

1) TIM as an Appliance (CEM 1-4.x) and MTP as an appliance (1-10.5).

What happened:

- The hardware, operating system, and TIM software were provided to the customer.
- The customer would open a support case to deal with security, operating system, and third-party concerns.
- The system was not to be modified unless given the okay by Support.
- Customer did not have to plan for TIM sizing but simply determine how many TIM appliances. were needed.

2) TIM was no longer an appliance -- aka "TimSoft". (APM 9.0-9.5)

What happened:
- The operating system and TIM software was supplied to customers
- Customers had to plan spend time determining TIM sizing .
- The customer would open a support case to deal with security, operating system, and third-party concerns.
- The compatibility guide specified a list of hardware choices. The hardware market changed at a faster pace than the certification of TIM servers.
- The system was not to be modified unless given the okay by Support.

3) TIM as software only (APM 9.6 onward) /MTP as software only (vMTP 10.6 onward)

- This was documented in APM 9.6 New Unofficial Rules

The documentation noted the transition as the following:
TIM installation is now available as software. Because the TIM is no longer a "software appliance", it is easier for you to maintain and upgrade the software.

TIM installation is now available as software that can be installed on any hardware that complies with the security policies of your organization. You can hence maintain and control the underlying operating system according to your IT policies

The vMTP April 2016 release notes talk about the product change only and little on the corresponding administration model change.

This is a new, non-appliance product that provides a similar kind of traffic monitoring to CA Multi-Port Monitor (CA MTP). It runs on a user-managed CentOS 6 system, running on third-party supplied hardware.

What happened:
- Only the TIM or MTP software only was provided
- Customers are responsible for providing the Linux OS and necessary license.
- Customers had the freedom to install the third-party and security updates on their TIMs provided it did not interfere with/slow down TIM performance.

-There should be less of a need to open Support cases because customers were responsible for operating system, security, and third-party software/hardware.
- But other customers had to deal with for the first time obtaining Linux resources and becoming Linux administrators.
- Customers provided their own hardware. For MTP, the hardware choices are specified such as the TIM second phase.

- Customers are responsible for providing the Linux OS and necessary license.

- Customers had to ensure that their server met the necessary software pre-requisites:

TIM: https://docops.ca.com/ca-apm/10-3/en/installing/apm-installation-and-upgrade/install-and-configure-tim-for-ca-cem

vMTP: https://docops.ca.com/ca-virtual-multi-port-monitor/en/installing/software-specifications

Next time we will discuss the impact of the "software-only TIM" administration model.

Questions for Discussion:
1. What TIM administration model worked best for your site?
2. What are the tradeoffs for your site in TIM administrator responsibilities
3. What other topics would you like me to cover?