Performance Analysis and Troubleshooting

Service Overview

Phil Storey
Phil@NetworkDetective.com.au
+61 401 993 927

Overall Service

Assist organisations in analysis of application and infrastructure performance

- Quickly identify the root causes of undiagnosed service problems with technology platforms, networks and applications.
- Identify exact application behaviours and forecast user impacts of server moves between data centres.

- Ideally also used as a due diligence activity to prove optimal performance and identify known and unknown bottlenecks and performance inhibitors.

Methods

- The primary method and technique utilised is to examine the behaviour of applications and networks via detailed packet analysis using powerful analytic software. Successful outcomes rely on the availability of network packet trace data from appropriate network locations.

- Main analytic software is “NetData” from Measure IT Pty Ltd in Sydney.
- Engagement fee includes software licence for NetData.

Component Services

- Initial consultation to assess whether the environment is suitable for packet analysis.
- Information gathering on the technology environment, architecture, problem symptoms and history of the environment.
- Assessment of any previous analysis and investigations.
- Assist client staff with data collection tools setup and configuration. Where capture tools such as NetScout, ExtraHop, Riverbed, etc. are already available, then working with staff to configure those systems to collect the necessary packet data sets.
- Verification that the installed environment actually matches the documented (or assumed) architecture/design.
- Detailed analysis of application behaviours, at all tiers from user, load balancers, web servers, application servers, authentication services and back-end systems such as databases & mainframes.
- Identification of intermediate network components such as firewalls, WAN accelerators, etc. that may modify TCP behaviours and cause unintended performance consequences.
- Participation in workshops, “Crit Sit” conferences and working with staff, support contractors and other relevant parties to present and examine findings. This may also involve ruling components in or out as well as suggesting further tests to prove or disprove any working hypotheses.
- Once root cause(s) are identified, recommendations and advice for mitigations.
- Identification of components that are not causing any issues.
- Working with the appropriate personnel to implement any changes and then performing follow up analysis to verify that the environment is operating at optimal capacity.

Benefits

- Quickly knowing the exact behaviour of application and network components removes guesswork and saves time.
- Decisions on where to spend troubleshooting efforts will be based on factual evidence rather than guesses and “maybes”.
- Identification of components that don’t contribute to the problem saves wasted efforts in those areas.
- Identification of the problem component(s) as well as the exact problem behaviour(s) means that proper fixes or work-arounds can be applied.
- The facts will be presented to relevant stakeholders in a way that they understand.
- The effectiveness of any changes can be measured and evaluated.

Engagement

The method that I use falls under the general heading of “Packet Capture and Analysis”. However, I’m able to produce very fast results thanks to powerful analysis software called “NetData” – which provides deep detail of transaction, application, server and network behaviours.

NetData is developed in Sydney by Bob Brownell of Measure IT Ltd – and is also known as, “The Dr Bob Tool”.

An engagement consists of my time and skills – as well as a software licence fee for NetData. The licence fee can be included in my daily rate or can be paid separately for longer term engagements.

There are 4 distinct phases in an engagement:

A. Capturing network packet data in the correct locations (i.e., that contains all network and application traffic that is relevant to the current issue).

B. Analysing that data to determine the exact application and network behaviours – and then determining the exact reasons for any performance or other problems.

C. Presenting the findings to relevant stakeholders, in a way that they can properly understand, to describe the underlying behaviours and causes.
   - The right people can then know what options are available and what changes are needed to “fix” any issues that are found.
   - May need to loop back to step (A) if other locations for captures are needed (e.g., more application “tiers” or other in-line devices such as WAN accelerators, proxy servers, load balancers, etc. are found).

D. Working with those right people to suggest and implement alternative solutions or options. Perhaps performing “post fix” analysis to prove that the expected improvements actually do occur.

The (A) and (D) phases are the ones that tend to take more elapsed time, because they involve other people or groups – often doing things that they have never done before. The (A) phase may also require “Security” approval or authorisation to allow packet capture to take place.

Therefore, I’d suggest that we try to focus my time mostly on (B) & (C). As much as possible, we should make sure that mechanisms for (A) are in place before I come on site. Time spent on (D) can be decided later, based on the findings.

Phil Storey

+61 401 993 927

www.NetworkDetective.com.au

au.linkedin.com/in/philipstorey3

@PhilStorey24

www.youtube.com/c/NetworkDetective