Stratusphere SpotCheck for Physical Laptop/Desktop

Last Updated: 06/17/2022

SpotCheck Methodology Guide

Contents

Document Purpose: To define metrics and thresholds for a SpotCheck as it relates to User Experience in a Physical Laptop/Desktop environment utilizing Liquidware Stratusphere UX.

This document is designed to bring together recommendations from many experts in the industry about the metrics that need to be monitored and the thresholds that are deemed acceptable as it relates to User Experience. This document does not make recommendations on changes needed due to the many industry, usage, costing, and application variables that are in play.

What is a "SpotCheck"

A SpotChecks is a point in time healthcheck that focuses on key User Experience metrics with known acceptable performance levels. The review of data from multiple dates and times is critical before making recommendations or changes to the environment. These thresholds represented below are taken at a one hour level of granularity unless otherwise specified in the description and are key areas that affect User Experience. Normal/High Usage dates and times should be examined based on the industry and user requirements.

Critical Notes:

A. Know your company!

- Know your industry/company/department work habits, loads and applications are critical for data interpretation and threshold evaluation.
    1. Example: Moderate/High storage latency may be acceptable during shift changes with large amount of users logging in and out, but this is not acceptable during normal work hours as this impedes productivity.
    2. Example: Law firms and healthcare organizations generally need/want sub ten second login times whereas most other industries are satisfied with under 30 second.

B. Know your data!

- There are many monitoring and diagnostic solutions out on the market. Each of the solutions e collect data differently and have different levels of granularity. All of these solutions render/report the data in differently and with unique granular roll ups that can drastically change the data and perspective for the user. For this reason, the metric values represented in this document are only for Liquidware Stratusphere and may not apply well to other products.
    1. Example: Depending on the view, you could be looking at averages, peaks or peak averages.
       Did the data come from the Broker, Hypervisor, "In-Guest", "In Band" or "Out of Band"?
       How much impact did the "In-Guest" Agent put on the OS?
       How much impact and time lag is on the "Out of Band" Agent, Broker and Hypervisor?

C. Good Blogs

- SpotCheck Methodology
- Grey Matter is Required – Automated Solutions don't work
- Monitoring vs. Diagnostics

D. Liquidware Community Site

- **Liquidware Community** - Answers to common and advanced questions.

Information Needed for Analysis, Conclusions and Recommendations:

A. Multiple Spot Check Dates
- MM/DD/YYYY (Monday), MM/DD/YYYY (Wednesday), MM/DD/YYYY (Friday)

B. Multiple Time Frames Examined on each date
- (Time frames for review are based on business requirements)
  9-10AM, 10-11AM, 2-3PM, 4-5PM

The system(s) should be examined on multiple dates and times for the following information based on the max values shown below. **Please do not make a change based on a single data point.**

Critical Sections for Review:

A. Machines/OS Criteria:
- Machine Last Boot – Critical Question – How long has the machine been running?
  1. See Appendix R for more details.
- Login Delay (Industry Average is under 30 Seconds – This is a company preference
  1. See Appendix L for more details.
- Application Load Time (Industry Average is under 3 Seconds – Company Preference)
- CPU Utilization (Max 80%) – Higher than 50% generally is bad over 60 Minutes
  1. This generally denotes stuck or run-away process(es) on the machine.
- CPU Queue (Should not be more than 1 per CPU assigned to machine)
  https://technet.microsoft.com/en-us/library/Cc940375.aspx
- Memory Usage (Should be less than 80%)
- Best Practice is to reduce Windows Paging
- Page File Usage (Should be as close to zero as possible)
  1. Windows paging cannot be stopped.
  2. Do not turn off the paging file in windows. Set to minimum and maximum size of the page file.
  3. Do not use "System Managed" – Set the page file start size to ¼ the memory.
  4. Windows Paging causes CPU and Disk Overhead and should be reduced whenever possible. To reduce paging, allocate more memory to the virtual machine.
  5. Soft Page Faults occur in memory and Hard Page Faults occur to the disk.
- Disk Queue (Should be ZERO for 99% of Users)
  1. Disk Queue shows that the OS is waiting on disk reads/writes.
  2. This can be caused by antivirus holding up the IO or latency of the disk sub system.
- Graphics Intensity will be noted has high when over 100 for more than 1/3 of users.
  1. This must be examined to see if graphics off load processor would help
  2. See Appendix G for more details.
- Applications Non-Responsive – (1 per Day/Per Machine/App is OK)
  1. Any more than this requires investigating the apps and services used by the application.

Appendix:

Appendix G: Graphics Intensity

1. Graphics rendering is a large part of the user experience. Depending on the application it can use MS GDI, DirectX, OpenGL, CUDA, etc… or many other video interface drivers/protocols.
2. There is always a misconception that since there are no extremely graphic intensive applications that GPUs (Graphics Processing Units) are not needed. This is not true, Windows and normal Microsoft Office applications have a lot of graphics requirements. All desktops/laptops built in the last 10 years have a GPU. These processors are used by the OS and applications to offload drawing of boxes, circles and other complex shapes from the main CPU and rendering them on the monitor.
3. GPUs are not all the same! Manufactures pick from many vendors to meet a cost point for the desktop or laptop they are selling.
   - Laptops: Tend to have energy/heat constrained GPUs.
   - Desktops: Have many tiers and options for expansion with more power and cooling available.
   - Driving multiple monitors at high resolution can often overload the built in GPU and then offload that back onto the main CPU.
   - Improperly installed video drivers and older versions can also cause off load back to the main CPU.
   - Graphic rendering does not show up in Task Manager, Resource Monitor or Stratusphere because this is a Kernel process and very hard to break out.
   - When looking at a physical machine with no obvious constrains on memory or disk we must look at CPU Utilization and CPU Queue. Low to moderate CPU utilization with HIGH CPU Queue is sign of overloaded graphics process. Also examine the GDI (Graphics Device Interface) objects in Task Manager or Stratusphere. GDI Objects average for the machine over 1 hour greater than 100 is consider high graphics intensity.

     - Example Application GDI Usage: Microsoft Outlook:
       First Monitor (1024x768) – 800-900 GDI Objects
       Second Monitor (1320x1024) – 1,200-1,400 GDI Objects
4. This is a complex topic and often difficult to identify. Stratusphere does show GPU utilization for many of the manufactures on the market. If you see no GPU load in Stratusphere for a physical machine the GPU is not reporting information, supported, drivers are bad, or resolution is not supported by the GPU/Driver.
5. If you find that you are overloading the GPU in the machine you have 2 options. First, turn off hardware acceleration for the applications or second, buy machines with faster GPUs.
6. Microsoft Office, Google Chrome and Mozilla Firefox all have Group Policy settings to disable hardware acceleration.
7. Good Video on GPU Usage - Machine and Application GPU Usage

Appendix L: Login Delay

- Time consumed with users logging into a machine is a large part of the user experience. Stratusphere can breakdown the machine boot and login processes. Due to the complexity of active directory and the environments we can only offer a few guiding hints in this document. For a complete login breakdown session please engage Liquidware SE/support or partner.
- Domain Controller(DC) Discovery Time
    1. DC Discovery happens at boot and login time.
    2. Healthy response times are 300-500 milliseconds.
- Changing of the DC during boot and login shows a potential issue.
    1. DC Discovery Times over 500ms:
        - DC Overloaded – Cannot process request fast enough.
        - Network latency from the machines to the DC.
        - Sites and Services – Machine/User is talking to a DC in another location.
- Long running processes
    1. AD GPOs, Item Level Targeting and Scripts.
        - Need to review these in Stratusphere Login Breakdown.
        - AD Lookups and Local machine WMI Queries are very slow.
        - Mapping a drive/printer to a machine that does not exist or the user does not have access to can make the login excessively long.
    2. Antivirus Scanning
        - Don't forget that batch files, PowerShell, VB Scripts are all interpreted languages. Meaning that each line in the batch file or script is executed one line at a time. AV systems scan each line then all the previous lines of the script to ensure it is not a virus.
- Domain Overview
    1. Understand which Domain Controllers are processing logins.
    2. How long was the average authentication process on each Domain Controller?
    3. Understand which Domain Controllers have a large amount of abnormal events.
- Physical Desktops and Persistent virtual machines need to be treated differently than non-persistent virtual desktops.
    1. Broken and/or Corrupt GPOs.
        - A yearly (at a minimum) review of the GPOs should be performed.
          Example: IE7 GPOs should not be applied to Windows 10.
        - Conducting reviews of GPOs can help dramatically with user login times and also security.
    2. Sites and Services
        - This is one of the top issues found with Stratusphere login break down.
        - A machine in New York it should not be authenticating from a domain controller in Canada.
        - With the speed on needing to provide Work from Home/Work from Anywhere new virtual desktop pools or new VLANs were deployed support these initiatives and zoning properly in the correct sites and services for authentication can be something that is missed.
- Good Video on Boot and Login Breakdown - Boot and Login Breakdown
- Animated GIF on how to get to Login Breakdown - Login Breakdown
- Animated GIF on how to get to Domain Overview – Domain Overview

Appendix R: Machine Last Reboot Time

- Knowing how long a machine has been running is a critical question. Applications can have memory, graphics and CPU process "Leaks" over time which can/will degrade performance. Machines running longer than one month are also missing critical security/feature patches that put them out of security compliance and at risk.
- Below is a recommendation only of reboot policies based on experience of Liquidware engineers. This is not a Liquidware recommendation as there are no official recommendations from Microsoft.

  Note: The below recommendations also must conform to company business practices and change control policies.

  1. ***Domain Controllers:***
     - Monthly Reboot – Primarily for OS Security Patches
  2. ***Critical infrastructure machines running Windows Server OS:***
     - Monthly Reboot – Primarily for OS Security Patches
  3. ***Physical Laptop/Desktop Machines:***
     - Minimum of a Weekly Reboot – Your mileage will vary based on the applications being used by the users. A Daily reboot is ideal to ensure users have the best experience.
     - Minimum of a Monthly Reboot for OS Security Patching.

Appendix W: WiFi Statistics

- Home WiFi is often overlooked and hard to prove as a significant factor in performance issues in Work from Anywhere scenarios. Stratusphere can provide the empirical proof that WiFi connectivity is the cause of these performance issues.
- Stratusphere can show if the distance the user is from the access point, the type of WiFi protocol used, the signal strength and of the user is flipping back and forward between the 5Ghz and the 2.4Ghz WiFi frequency.
    1. The minimum WiFi signal strength that is recommended to maintain is -67 dBM, anything greater can result in performance degradation.
    2. Legacy WiFi protocols (802.11a, 802.11b and 802.11c) should no longer be used as modern day WiFi protocols should be 802.11g, 802.11n, 802.11ac, or 802.11ax. If there are devices in the environment still using legacy protocols, they should be replaced to achieve the best possible WiFi performance.
    3. Consistent WiFi roaming should be kept to minimum and consistently switching Wireless Access Points cannot guarantee WiFi performance.
    4. 5Ghz WiFi frequency provides the best speed but does not penetrate walls as well and does not cover as much distance. 2.4Ghz WiFi frequency provides less speed but does cover more distance and penetrates walls better. If it is determined that users are flipping back and forward between 5Ghz and 2.4Ghz WiFi frequencies it is a best practice the force their endpoint to only stay on the 2.4Ghz WiFi frequency.
- Animated GIF on how to get to WiFi Network with Details - WiFi Details w/ Network

Appendix V: VoIP – Voice over IP

- Voice over IP Solutions are critical to business meetings and user to user calls. There are many solutions on the market for VoIP and team chat solutions, but they all rely on the network to provide good call quality.
- Most voice over IP solutions and chat systems can sustain a good voice quality up to 200 milliseconds of latency.
  Poor voice quality is introduced when "Jitter" is over 5 Milliseconds.
  Jitter: Is the difference in latency millisecond to millisecond.
- CPU being overloaded can cause latency and this is commonly overlooked. See Machines/OS Criteria section for more information on CPU utilization.
- Why does Jitter Happen:
  1. User network overloaded with other apps downloading/uploading information.

     Note: Many VoIP solutions have the ability to offload voice connections from a virtual machine back to the end user device thereby reducing latency and jitter.