|  |  |  |
| --- | --- | --- |
| SCHOOL OF INFORMATION AND TECHNOLOGY | | |
| NAME: Zhaun Gabrielle F. Pasion | DATE PERFORMED: 17/10/24 | /50 |
| Section: IDC2 | DATE SUBMITTED: 17/10/24 |

# SYSADM1 – Platform Services

# Requirement:

* A virtual machine running Windows Server

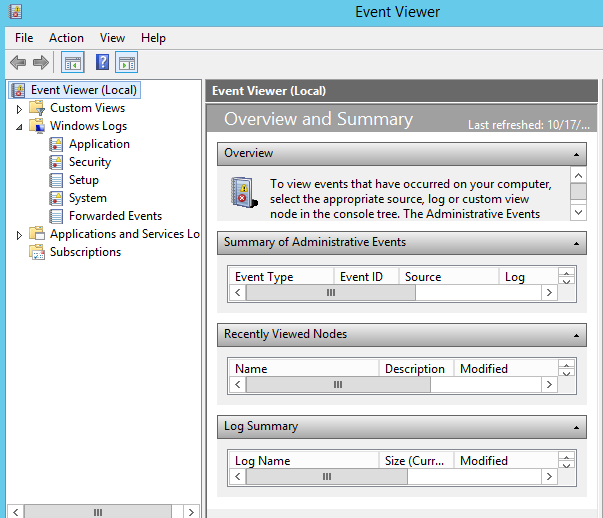
**Objective/s:**

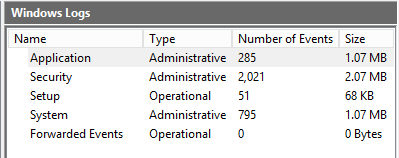
To analyze IIS logs in the Event Viewer to identify critical web service metrics, understand common error codes, and learn how to monitor the health of web applications.

**Instructions**

**Part 1: Opening Event Viewer and Loading Logs**

1. Access the event viewer in the server.

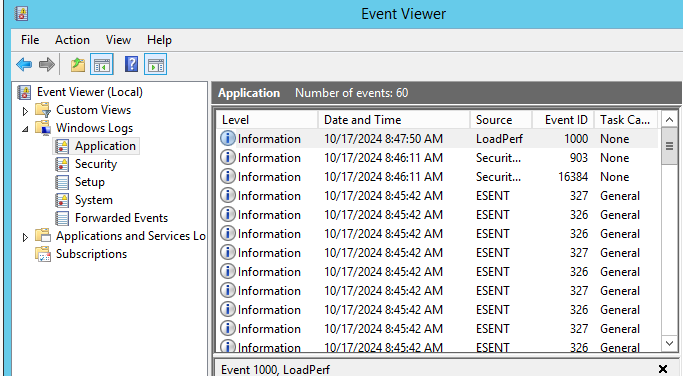




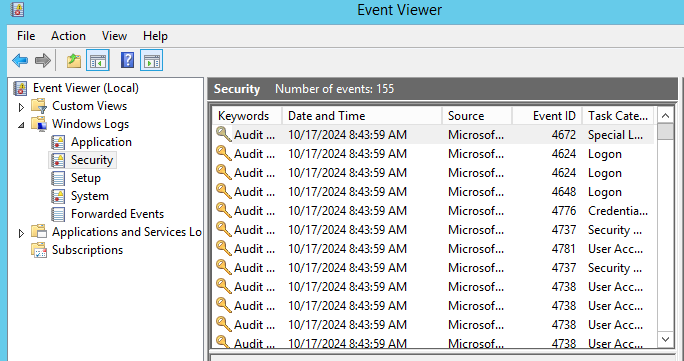
1. From the event viewer, explore the windows log and list down its major categories

**Major Categories:**

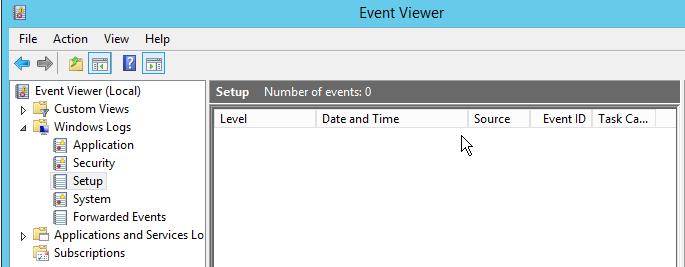
* Application



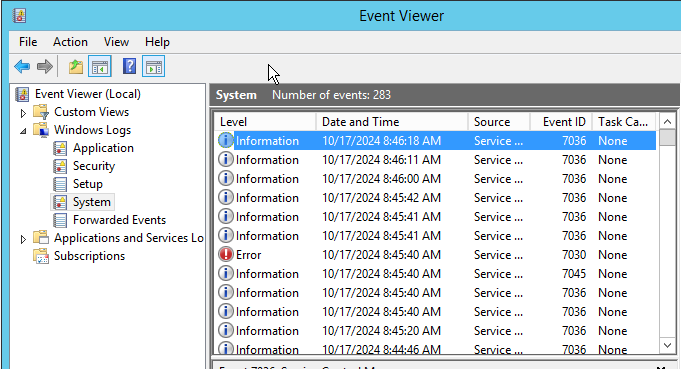
* Security



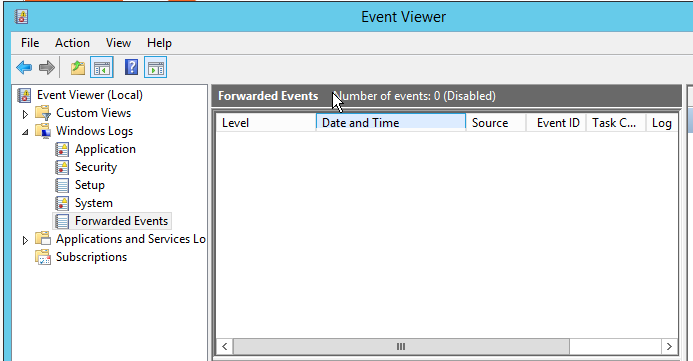
* Setup



* System

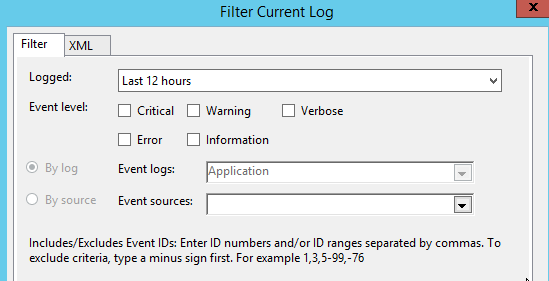


* Forwarded Events

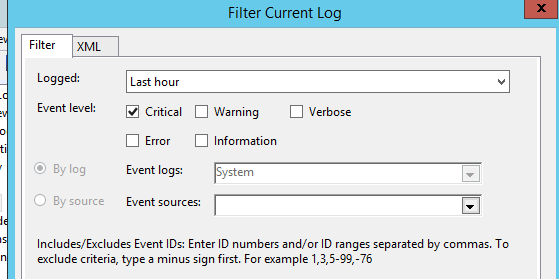


**Part 2: Filtering and Analyzing IIS Events**

1. Apply filter to the windows log categories to display errors for the past 12 hours.



1. **Identify Critical Events** or recurring events.



1. **Analyze the Events**:
   * For each critical or recurring event, **record the following details**:
     + **Event ID**
     + **Source**
     + **Timestamp**
     + **Description**

|  |  |  |  |
| --- | --- | --- | --- |
| **Event ID** | **Source** | **Timestamp** | **Description** |
| 6006 | Winlogon | 10/17/2024/ 9:01:31 AM | The winlogon notification subscriber <GPClient> took 120 second(s) to handle the notification event (Create Session) |
| 6005 | Winlogon | 10/17/2024/ 9:00:30 AM | The winlogon notification subscriber <GPClient> is taking too long to handle the notification event (Create Session) |
| 16387 | Security | 10/17/2024/ 9:00:11 AM | Failed to run task \Microsoft\Windows\WS\License Validation. Error Code 0x80041326. |
| 1008 | Perflib | 10/17/2024/ 8:59:47 AM | The Open Procedure for Service “BITs” in DDL “C:\Windows\System32\bitsperf.dll” failed. Performance data for this service will not be available. The first four bytes (DWORD) of the Data section Contains the error code. |
| 8198 | Security | 10/17/2024/ 8:44:10 AM | License Activation (slui.exe) failed with the following error code: hr=0xC004C003 |
| 1014 | Security | 10/17/2024/ 8:44:10 AM | Acquisition of End User License failed. He=0xC004C003 Sku id=439e8c91-ff38-4ecb-ba0b-326586080c953 |
| 8200 | Security | 10/17/2024/ 8:44:10 AM | License acquisition failure details  Hr=0xC004C003 |
| 1014 | DNS Client Event | 10/17/2024/ 9:09:29 AM | Name resolution of the name ipv6.msftncsi.com timeout after none of the DNS servers responded |
| 10154 | Windows Remote Management | 10/17/2024/ 9:09:06 AM | The WinRM service failed to create the following SPNs: WSMAN/PasionServer.SRVR.org; WSMAN/PasionServer |
| 1014 | DNS Client Events | 10/17/2024/ 9:08:37 AM | Name resolution for the name\_ldap.\_tcp.dc.\_msdcs.SRVR.org timed out after none of the configured DNS servers responded. |
| 34 | disk | 10/17/2024/ 9:08:35 AM | The driver disabled the write change on the device \Device\Harddisk0\DR0 |
| 34 | disk | 10/17/2024/ 9:08:35 AM | The driver disabled the write change on the device \Device\Harddisk0\DR0 |
| 34 | disk | 10/17/2024/ 9:08:35 AM | The driver disabled the write change on the device \Device\Harddisk0\DR0 |
| 34 | disk | 10/17/2024/ 8:58:42 AM | The driver disabled the write change on the device \Device\Harddisk0\DR0 |
| 34 | disk | 10/17/2024/ 8:58:42 AM | The driver disabled the write change on the device \Device\Harddisk0\DR0 |
| 1014 | DNS Client Events | 10/17/2024/ 8:53:42 AM | Name resolution for the name 6t04.ipv6.microsoft.com timed out after none of the configured DNS server responded |
| 1014 | DNS Client Events | 10/17/2024/ 8:53:00 AM | Name resolution for the name ipv6.msftncsi.com timed out after none of the configured DNS server responded |
| 1014 | DNS Client Events | 10/17/2024/ 8:44:46 AM | Name resolution for the name ipv6.msftncsi.com timed out after none of the configured DNS server responded |
| 1014 | DNS Client Events | 10/17/2024/ 8:44:45 AM | Name resolution for the name win8.ipv6.microsoft.com. timed out after none of the configured DNS server responded |
| 1014 | DNS Client Events | 10/17/2024/ 8:44:45 AM | Name resolution for the name win8.ipv6.microsoft.com timed out after none of the configured DNS server responded |
| 7023 | Service Control Manager | 10/17/2024/ 8:58:43 AM | The windows Time service Terminated with the following error: An attempt was made to logon, but the network logon service was not started |
| 46 | Time-Service | 10/17/2024/ 8:44:45 AM | The time service encountered an error and was forced to shut down. The error was: 0x80070700: An attempt was made to logon, but the network logon service was not started |
| 7030 | Serve Control manager | 10/17/2024/ 8:45:40 AM | The Printer Extensions and Notification services is marked as an interactive service. However the system is configured to not allow interactive services. This service may not function properly. |

**Part 3: Troubleshooting and Solution Development**

1. Review the logs and check for recurring errors.
2. Is there a specific time or pattern to these errors?

Based on the event at event viewer, warning and errors most likely happed after I have setup the server. The errors exhibit a pattern of occurring primarily within the first hour of system activity (8:44 AM to 9:09 AM).

1. Draft a Troubleshooting Report:
   * Based on the events found, create a short report with the following sections:

**Report Structure**

**1.** Overview

* A brief summary of the issue and scope of your analysis.

**2.** Key Findings

* List the critical events you found. Example:
  + **Event ID 503**: Application pool stopped at 10:05 AM.
  + **Event ID 404**: Page not found error at 11:15 AM.

**3.** Root Causes and Solutions

* Describe the likely cause of each error and how you would fix it.

**Event Viewer Report**

This report analyzes multiple events logged on 10/17/2024, highlighting recurring issues related to license activation, DNS resolution failures, and disk write changes.

**Key Findings:**

* **Event ID 6006/6005:** GPClient took excessive time to handle session creation. Error at 9:01:31 AM (6006), 9:00:30 AM (6005)
* **Event ID 16387:** Task failure for License Validation (Error Code 0x80041326). Error at 9:00:11 AM
* **Event ID 8198/1014:** License activation failed (hr=0xC004C003). Error at 8:44:10 AM
* **Event ID 1014 (DNS Client Events):** Multiple DNS resolution timeouts for various addresses.

**Warnings at**:

* 9:09:29 AM
* 9:08:37 AM
* 8:53:42 AM
* 8:53:00 AM
* 8:44:46 AM
* 8:44:45 AM
* **Event ID 34 (Disk)**: Multiple instances of write changes being disabled on the hard disk. Warning at 8:58:42 AM and 9:08:35 AM on multiple instances
* **Event ID 7023**: Windows Time service terminated due to network logon service not being started. Error at 8:58:43 AM
* **Event ID 46 (Time-Service)**: Time service encountered an error and shut down. Error at 8:44:45 AM
* **Event ID 7030**: Printer Extensions and Notification services marked as interactive, but system disallows it.Errorat 8:45:40 AM

#### **Root Causes and Solutions**

* **GPClient Delays:** Likely due to policy processing delays; I would consider optimizing group policies or checking for network issues.
* **License Validation Failure:** This may indicate activation issues; I will verify the licensing status and try reactivating Windows.
* **DNS Timeouts:** Checking the DNS server configurations or consider using alternate DNS servers to improve resolution would possibly fix this error.
* **Disk Write Changes Disabled:** This could indicate hardware issues or driver problems; checking the disk health and updating drivers, I will also check if the disk is properly installed.
* **Windows Time Service Termination:** Ensure the network logon service is started and configured correctly to prevent time service failures.
* **Time-Service Error:** Investigate network logon issues and ensure proper service dependencies are active.
* **Printer Extensions Service Warning:** Either configure the system to allow interactive services or adjust the service configuration to avoid functional issues.

**Part 4: Reflection Questions**

1. What are the most common causes of a **503 Service Unavailable** error? (most reoccurring errors)

The most common recurring errors in the logs include DNS resolution timeouts, service terminations related to the Windows Time service and GPClient delays, and license activation failures. These issues indicate potential network problems, service misconfigurations, and activation issues that may affect system stability and performance.

1. How would you **monitor login attempts** to detect potential security threats?

To monitor login attempts and detect potential security threats using Event Viewer, I would start by ensuring that the audit policy for logon events is enabled to log both successful and failed logins. I would then access the Security logs in Event Viewer, focusing on Event IDs 4624 (successful logon) and 4625 (failed logon). Creating custom views to filter these events would streamline the review process. Regularly reviewing the logs would help identify patterns, such as repeated failed attempts or unusual logins from unfamiliar IP addresses. If possible, setting up alerts for specific Event IDs would allow for real-time notifications of suspicious activities. Finally, documenting any anomalies would aid in further investigation and refine monitoring practices.

1. Why is **monitoring logs** in Event Viewer important for administrators?

Monitoring logs in the Event Viewer is important for administrators because it helps them track and identify problems on the system. In this activity, we used Event Viewer to find critical and recurring errors, which helped me notice issues that might not be obvious right away. Similarly, administrators can look for errors and warnings to understand what’s happening in the system. Regularly checking these logs allows them to fix problems before they become bigger issues and helps keep the system running smoothly. It also helps detect unauthorized access and other security threats, making sure sensitive information is protected. Overall, checking logs in Event Viewer is key to keeping the system healthy and secure.

**Additiional Reflection:**

I have noticed that there are extra event logs that are not documented in the servers Event Viewer. On the Event Viewer, errors started while I was setting up the server. In the server manager I have noticed that there is a similar event logs like the events vieser but it is not detailed. I have also noticed that there are logs that are advanced. I have been looking at the server currently at 17/10/2024 10:28:00 AM however there are logs that are 10/17/2024 11:40:34 PM which is advanced. I have checked that the time and date configuration of the serve is correct and it using the current date and time in which the server is located.

Grading Rubric

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Criteria** | **Excellent** | **Good** | **Needs Improvement** | | **Poor** | | **Points** |
| **Log Analysis** | Identifies all key events (503, 404, 500, etc.) with accurate event details. | Identifies most key events with minor errors in details. | Identifies some events, but with incomplete or incorrect details. | | Fails to identify key events or provides incorrect details. | | /10 |
| **Troubleshooting Solutions** | Proposes logical, effective solutions to all identified issues. | Solutions are mostly correct but miss some key points. | Solutions are somewhat vague or incomplete. | | Solutions are unclear or incorrect. | | /10 |
| **Report Structure & Clarity** | Well-organized report with all sections clearly completed. | Report is mostly organized with minor formatting issues. | Report is disorganized or missing sections. | | Report is unclear or incomplete. | | /10 |
| **Recommendations for Monitoring** | Provides thoughtful, proactive recommendations to prevent future issues. | Recommendations are relevant but lack depth. | | Recommendations are vague or incomplete. | | Fails to provide relevant recommendations. | /10 |
| **Participation & Effort** | Actively engaged in the activity, followed instructions thoroughly. | Participated but required some guidance. | | Minimal participation, needed significant help. | | Did not participate meaningfully. | /10 |
| **Score** | | | | | | | **/50** |

Screenshots of Errors and Warnings:  
