|  |  |  |
| --- | --- | --- |
| SCHOOL OF INFORMATION AND TECHNOLOGY | | |
| NAME: Caccam, Jesus Allyson O | DATE PERFORMED: 10/17/2024 | /50 |
| Section: IDC2 | DATE SUBMITTED: 10/17/2024 |

# SYSADM1 – Platform Services

# Requirement:

* A virtual machine running Windows Server

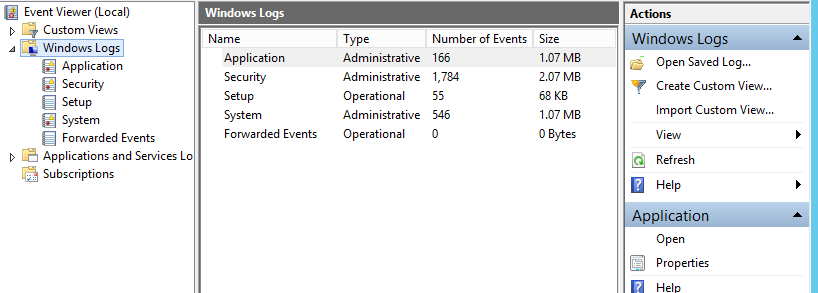
**Objective/s:**

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**

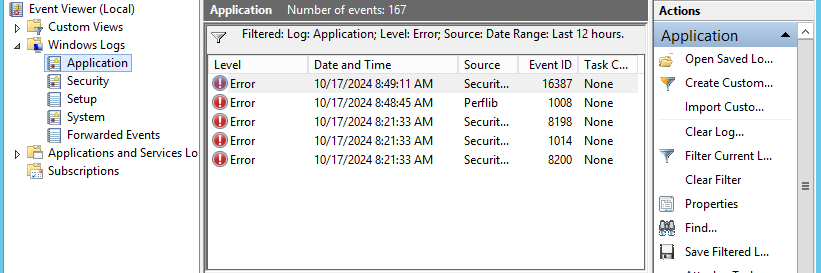
1. Access the event viewer in the server.
2. From the event viewer, explore the windows log and list down its major categories

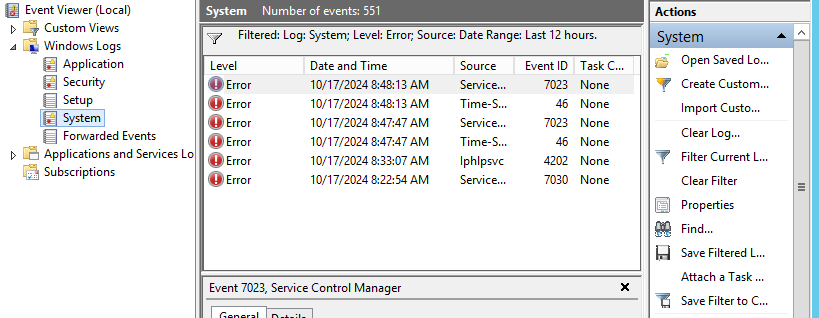


* **The Major list categories are Administrative and Operational**

**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.

* **The critical events or recurring events that I encounter are Source and EventID. And the events that I encounter are:**

-Service Control Manager – Event 7023

-Time-Service – Event 46

-Iphlpsvc – Event 4202

- Perflib – Event 1008

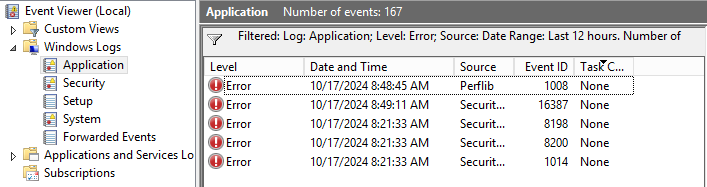
- Security-SSP – Event 16387, 8198, 8200, 1014

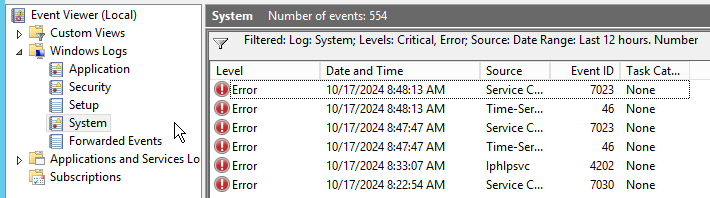
1. **Analyze the Events**:
   * For each critical or recurring event, **record the following details**:
     + **Event ID**
     + **Source**
     + **Timestamp**
     + **Description**

|  |  |  |  |
| --- | --- | --- | --- |
| **Event ID** | **Source** | **Timestamp** | **Description** |
| 1008 | Perflib | 10/17/2024 – 8:48 AM | Performance data for this service will not be available. |
| 16387 | Security-SPP | 10/17/2024 – 8:49 AM | Failed to run task |
| 8198 | Security-SPP | 10/17/2024 – 8:21 AM | License Activation (slui.exe) failed. |
| 8200 | Security-SPP | 10/17/2024 – 8:21 AM | License acquisition failure: hr=0xC004C003 |
| 1014 | Security-SPP | 10/17/2024 – 8:21 AM | Acquisition of End User License Failed. |
| 7023 | Service Control Manager | 10/17/2024 – 8:48 AM | An attempt was made to logon, but network logon service was not started. |
| 46 | Time-Service | 10/17/2024 – 8:48 AM | Time service encountered an error and was forced to shut down. |
| 7023 | Service Control Manager | 10/17/2024 – 8:48 AM | An attempt was made to logon, but network logon service was not started. |
| 46 | Time-Service | 10/17/2024 – 8:48 AM | Time service encountered an error and was forced to shut down. |
| 4202 | Iphlpsvc | 10/17/2024 – 8:33 AM | Unable to update the IP address on Isatap Interface Local Area Connection \*11 Update Type: 0. Error Code: 0x57. |
| 7023 | Service Control Manager | 10/17/2024 – 8:48 AM | An attempt was made to logon, but network logon service was not started. |

**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?





* **Yes, there is a specific time and pattern to these errors. When a source generates an error, even if the event ID is different, the error time is consistent across all event IDs.**

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.
* The summary of my documentation is to use the Event viewer and analyze the errors that are critical and errors that are recurring. And based on my findings, Errors like Security Control Manager, Security-SPP, and Time-Service. These errors occurred on the same time but with different Event IDs. So with these errors, I learned that event viewer helps a system administrator to fully monitor and check errors in its server and to easily troubleshoot any errors may encounter.

**2.** Key Findings

* **Event ID 1008 –** Data Section Contains error code at 8:48 AM.
* **Event ID 16387 –** BITS Service failed to run task at 8:49 AM.
* **Event ID 8198 –** License Activation (slui.exe) Failed with hr=0xC004C003 error code at 8:21 AM.
* **Event ID 8200 –** License Acquisition Failed at 8:21 AM.
* **Event ID 1014 –** Acquisition of End User License Failed at 8:21 AM.
* **Event ID 7023 –** Time service terminated due to attempt to logon but network service was not started at 8:48 AM.
* **Event ID 46 –** Time service encountered an error and was forced to shut down at 8:48 AM.
* **Event ID 4202 –** Unable to update IP address on Isatap Interface Local Area Connection at 8:33 AM.
* **Event ID 7030 –** Printer Extension and Notifications service was marked Inactive services at 8:22 AM.

**3.** Root Causes and Solutions

* **Service Control Manager**

**Errors:**

**-** An attempt was made to logon, but the network logon service was not started.

**Likely Causes:**   
- Network logon is not running

**-**Service dependencies not started

**-**Configuration issues

**How to fix:**

-Restart network logon service

- Check Server Dependencies

- Review Network Configurations

* **Security-SPP**

**Errors:**

**-** License Activation (slui.exe) failed" and "License acquisition failure: hr=0xC004C003.

**Likely Causes:**

-Issues with the licensing server.

- Corrupted license files.

- Insufficient permissions for the activation process.

**How to fix:**

**-** Run activation as Administrator

- Check internet Connectivity

- Check Event Viewer

- Reinstall Licensing Components

* **Time-Service**

**Errors:**

**-**Time service encountered an error and was forced to shut down.

**Likely Causes:**

- Incorrect time zone settings.

- Issues with the Windows Time service configuration.

- Network connectivity issues preventing time synchronization

**How to fix:**

**-** Restart the Windows Time Service

**-** Check Time Zone Settings

**-** Reconfigure Time Service

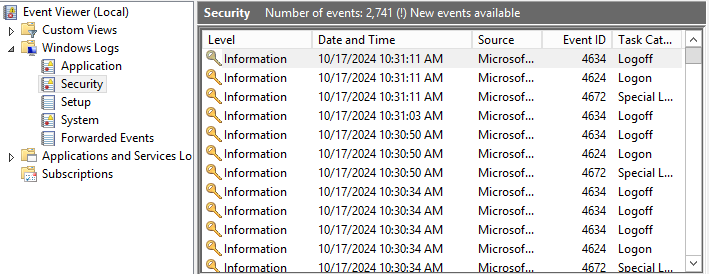
**-** Review Event Logs

**Part 4: Reflection Questions**

1. What are the most common causes of a **Security-SPP** and **Service Control Manager** errors?

* The common causes of Security-SSP and Service Control manager errors are often due to corrupted files, which occurs when you shut down your device improperly or because of malwares. It is also causes when you have incomplete windows update or failed update which may also leads to compatibility errors that affects the service management. And lastly, it may also cause to other third party tools or software, which may conflict and causes to interfere the normal operation and management.

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

* To monitor login attempts, you can use the Event viewer to enable auditing logon events. And in the event viewer you can expand in Windows Logs and Select Security. This logs will contain events related to login attempts. And by filtering, you can see the Event id like 4624 and 4625, which these serve as the successful logins and logoff events. You can also review these events for unusual patterns such as multiple failed attempts and successful logins.  
  

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

* Monitoring logs in Event Viewer is crucial for administrators because it helps them keep track of system activity and identify potential security issues. By regularly reviewing these logs, admins can spot unusual behaviors, like repeated failed login attempts, which may indicate attempted breaches or unauthorized access. This proactive approach allows them to respond quickly to threats and take necessary actions to protect sensitive data. Additionally, monitoring logs helps ensure compliance with security policies and regulations, as it provides a clear record of user activity and system changes. Overall, using Event Viewer is an essential practice for maintaining system security and stability in any organization.

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** |