Unit 5: Logging, Forensics and Future Trends

1. Specify a logging configuration for Windows/Linux.

Windows:

According to Exabeam (N.D.), multiple logging systems can be used on Windows. The most popular way to keep track of system events is to use the Windows Event Log. Other logging systems are the Windows Performance Counter Log, which logs performance information, and the Windows Firewall Log, which logs network traffic.

The Windows event log records system, security and application notifications stored by the Windows operating system that network administrators use to diagnose system problems. Each event in a log entry contains information such as severity, date, time, source, event ID, task category, user and computer (Yasar & Gillis, N.D.).

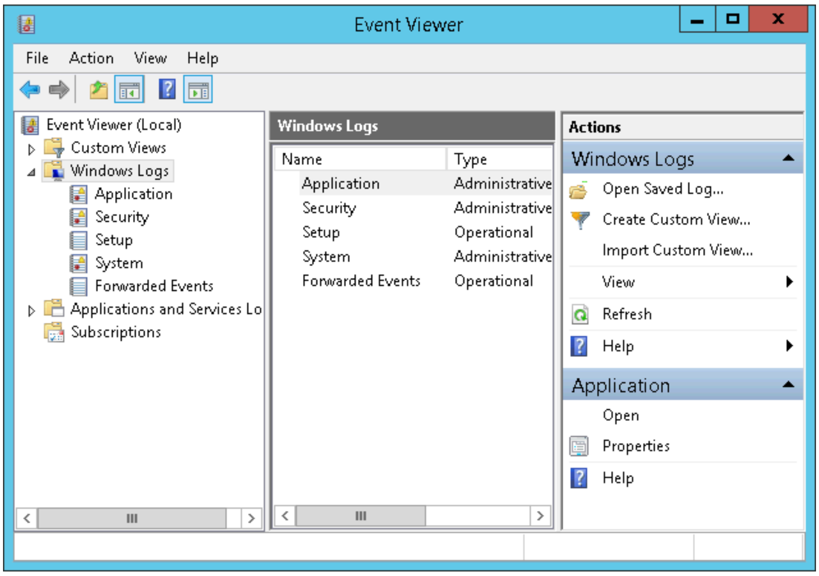
The Windows event log is a valuable tool for tracking and troubleshooting computer issues. It stores system and application events records, easily accessed and analysed through the Windows Event Viewer (Loggly, 2018). Logs are records of events on your computer that help you track what happened and troubleshoot problems. Windows event log contains logs from the OS and applications such as SQL Server or IIS. They use a structured data format, making them easy to analyse. Some applications write to log files in text format, like IIS Access Logs.

Loggly (2018) states that the Event Viewer application can configure Windows logging. The Event Viewer allows it to view, manage, and configure the event logs on the system. It can also use the Event Viewer to configure the logging level for each event log. The logging level determines how much information is recorded in the event log. The higher the logging level, the more information will be registered. However, more information will also take up more disk space.

Windows Event Viewer helps view and search Windows event logs. It can also export logs for analysis and more (IBM, 2021). Here is an illustration of how to set the logging configuration for Windows by exporting Windows event logs from Event Viewer:

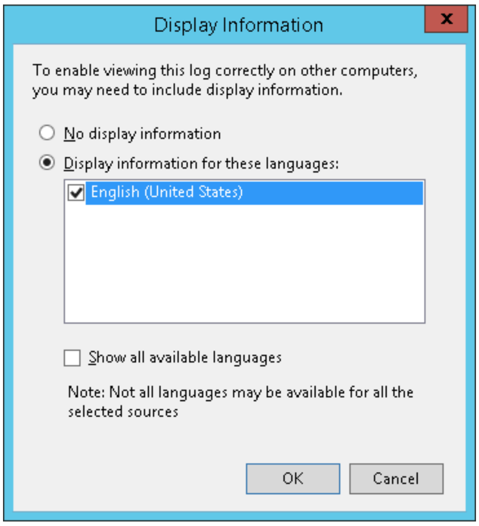
1 To launch Event Viewer, type *eventvwr* into the **Start** > search box (or hit the **Windows key + R** to bring up the **Run** dialogue box).

2 Open Event Viewer and select Windows Logs.



Name	Type
Application	Administrative
Security	Administrative
Setup	Operational
System	Administrative
Forwarded Events	Operational

- Select the log type that has to be exported.
- Select **Save All Events As**... under **Action**.
- Make sure the log file is saved to your chosen location and the **Save as type** is set to.*evtx*.
- If you are asked to display information, click the **Display information**...radio button, pick **English (United States)** as seen in the screenshot below (unless support instructs you differently), and then click **OK**.



To enable viewing this log correctly on other computers, you may need to include display information.

○ No display information

● Display information for these languages:

☑ English (United States)

□ Show all available languages

Note: Not all languages may be available for all the selected sources

Note: The full texts of most of the events are not included in the *evtx* file. Ensuring that everything is recorded is provided by adding the display information.

- This generates a LocaleMetaData folder and a.evtx file in the directory given in step 5. Include this file and its directories in a compressed file.

On Linux, Systemd provides a comprehensive approach to logging all kernel and userland processes using journalctl. This powerful tool enables easy access and manipulation of the data stored within the journal (Ellingwood, 2021). The systemd journal centralises log management across all sources and keeps them binary. This allows for easy viewing and manipulation of log data, including displaying logs according to specific needs and outputting data in various forms. The journal can be used alongside or replace existing syslog functionality.

Levinas (2022) defines Systemd as a suite of tools that manages vital aspects of Linux systems, including services, network configuration, runtime settings, and logging. It is also an init system that starts and works processes until the system shuts down. It's the default init system on many famous flavors of Linux, including Ubuntu, Debian, Fedora, and openSUSE.

The default logging system for Linux is called Systemd. It may be set up to transmit logs to a remote server and be used to record events from several sources. On the other hand, Linux distributions based on systems use Journald as their default logging system. It may be set up to store logs in multiple forms and is more efficient than Syslog (Loggly, N.D.).

According to Ellingwood (2021), the journalctl command-line utility can configure logging, viewing, searching, and filtering journal entries. The journal's logging level can also be set using the journalctl command. The main configuration file for systemd-journald can be located at /etc/systemd/journald.conf. Packages may also generate configuration files in directories with a .conf extension. Custom configurations precede the default parameters specified in the main configuration file. The default configuration file includes parameters commented out and recognised by systemd as default values. Any uncommented parameters must be edited, and the systemd-journald service must be restarted accordingly.

Here are Isaiah's (2023) instructions on how to use journalctl to view and manage systemd logs:

1. users can only see log entries from systemd services under their control to view system logs. Running the journalctl command without any arguments may show a message at the top of the output:

```
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
```

2. To view every log that the journald daemon has gathered, enter the following command:

```
journalctl
```

Using the 'journalctl' command alone outputs all journal entries. Adding the '--no-pager' flag prints output directly to stdout, which is useful for text processing tools like grep, awk, or sed or redirecting output to a file: journalctl --no-pager.

10 '-n' option can limit the number of printed entries to a preset number to print only the most recent few log entries:

```
journalctl -n 10 # print the last 10 entries.
```

2. Select and utilise forensic tools.

Computer forensics is investigating and analysing a computing device to gather and preserve evidence in a way that is admissible in a court of law. This data recovery practice determines what happened on a computing device and who was responsible for it. It is also used for data recovery processes to gather data from a crashed server, failed drive, reformatted operating system (OS), or any other situation where a system has unexpectedly stopped working (Lutkevich, 2021).

Poston (2021) states that evidence can manifest in various forms and platforms in today's digital age. Forensic investigations scrutinise files, emails, network activity, and more to uncover clues. The field of digital forensics boasts a range of specialised tools, each designed to cater to different aspects of an investigation. For instance, Autopsy and the Sleuth Kit are popular toolkits for analysing hard drives and smartphones. The Sleuth Kit is a command-line tool, while Autopsy is more user-friendly with a GUI-based system that utilises The Sleuth Kit in the background.

Autopsy: Autopsy is a user-friendly, graphical user interface (GUI) application that makes it simple to analyse smartphones and hard discs. Because of its plug-in architecture, it can create custom Python or Java modules or find add-on modules (Sleuthkit, 2019).

The Sleuth Kit (TSK): Disc image analysis and file recovery are made possible by the Sleuth Kit, a set of C library and command line utilities. It is a hidden feature of many other commercial and open-source forensics products, including Autopsy. (Sleuthkit, 2019).

FTK Imager, Volatility, Registry Recon, Cellebrite UFED, Wireshark, and CAINE are some of the most commonly used tools in digital forensics investigations. These powerful tools aid in various aspects of the investigation process, such as image creation, memory forensics, Windows registry analysis, mobile forensics, network analysis, and Linux distributions (Poston, 2021).

References:

- Exabeam (N.D.). *Event Log: Leveraging Events and Endpoint Logs for Security*. [online] Available at: https://www.exabeam.com/explainers/event-logging/event-log/.
- Yasar, K. & Gillis, A. S. (N.D.). *What is a Windows event log? - Definition from WhatIs.com*. [online] Available at: https://www.techtarget.com/searchwindowsserver/definition/Windows-event-log.
- Loggly (2018). *Windows Logging Basics - The Ultimate Guide To Logging*. [online] Available at: https://www.loggly.com/ultimate-guide/windows-logging-basics/.
- IBM (2021). *Exporting Windows event logs from Event Viewer*. [online] Available at: https://www.ibm.com/support/pages/exporting-windows-event-logs-event-viewer.
- Ellingwood, J. (2021). *How To Use Journalctl to View and Manipulate Systemd Logs*. [online] Available at: https://www.digitalocean.com/community/tutorials/how-to-use-journalctl-to-view-and-manipulate-systemd-logs.
- Levinas, m. (2022). *An Ultimate Guide of How to Manage Linux Systemd Services With Systemctl Command*. [online] Available at: https://www.cherryservers.com/blog/an-ultimate-guide-of-how-to-manage-linux-systemd-services-with-systemctl-command [Accessed 19 Dec. 2023].
- Loggly. (N.D.). *Centralizing with Syslog - The Ultimate Guide To Logging*. [online] Available at: https://www.loggly.com/ultimate-guide/centralizing-with-syslog/ [Accessed 19 Dec. 2023].
- Loggly. (N.D.). *Linux Logging with Systemd - The Ultimate Guide To Logging*. [online] Available at: https://www.loggly.com/ultimate-guide/linux-logging-with-systemd/.
- Isaiah, A. (2023). *How to View and Manage Systemd Logs with Journalctl | Better Stack Community*. [online] Available at: https://betterstack.com/community/guides/logging/how-to-control-journald-with-journalctl/.
- Lutkevich, B. (2021). *What is Computer Forensics (Cyber Forensics)?* [online] TechTarget. Available at: https://www.techtarget.com/searchsecurity/definition/computer-forensics.
- Poston, H. (2021). *Top 7 Computer Forensics Tools for Digital Evidence Collection | Infosec*. [online] Available at: https://resources.infosecinstitute.com/topics/digital-forensics/7-best-computer-forensics-tools [Accessed 19 Dec. 2023].
- Sleuthkit (2019). *The Sleuth Kit (TSK) & Autopsy: Open Source Digital Forensics Tools*. [online] Sleuthkit.org. Available at: https://www.sleuthkit.org/.