Windows Event Viewer

Opening a web browser is a simple task that most people are familiar with. Similarly, Windows event logs are records of events that occur on a Windows operating system. These logs can be used to identify and troubleshoot system problems. Let's break down the information you need to know about Windows event logs.

Windows event logs are detailed records of events related to the system, security, and applications stored on a Windows operating system. They contain information such as the severity of the event, date and time of occurrence, event ID, source, task category, user, and computer. Event logs can be used by network administrators to track system problems and predict future issues.

An event log is made up of:-

* Level –Severity of the recorded event log. This includes information, error, verbose, warning, and critical.
* Date/Time – Includes the Date and Time when the event occurred.
* Event ID – A windows identification number that uniquely identifies a specific logged event.
* Source - Software or Program causing the event log.
* Task Category – Identifies the type of recorded event. This can be defined to serve as extra information about the event
* User-Username of the user who logged onto the windows computer when the event occurred.
* Computer – Name of the computer logging the event.

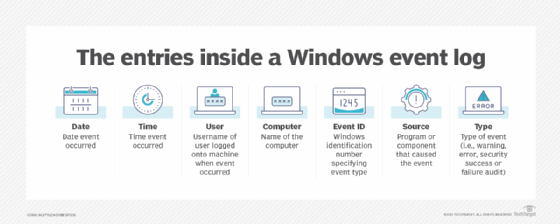


Figure : Elements of An Event Log

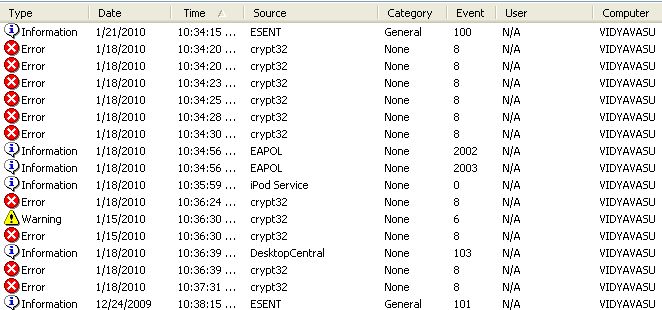


Figure : Event Logs

# Types of Windows Event Logs

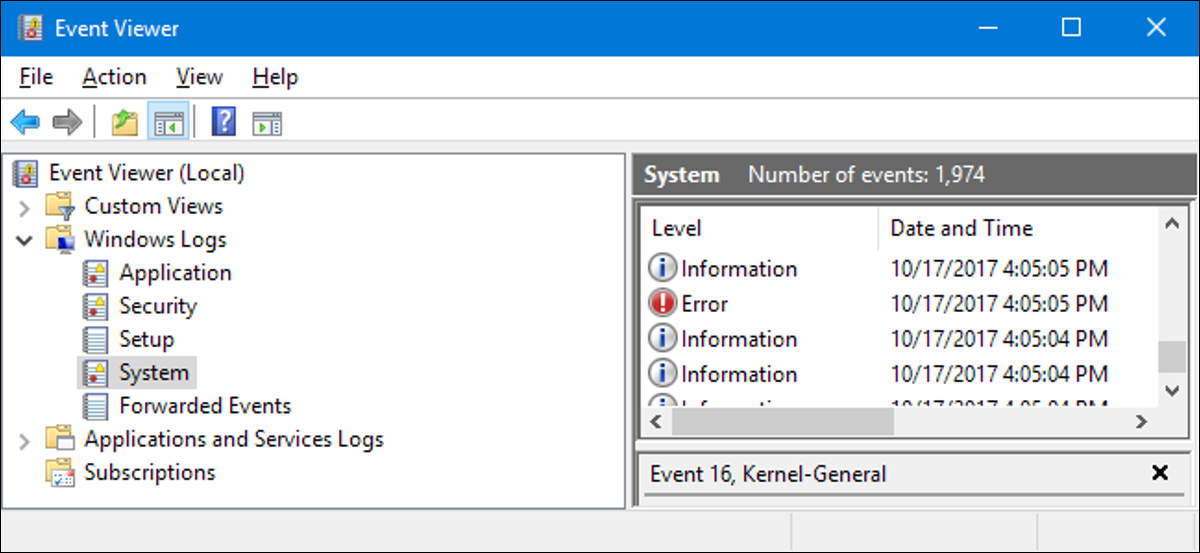


Figure : Event Viewer Dashboard

There are four types of Windows event logs: system logs, application logs, setup logs, and security logs.

* **System logs** contain events related to Windows-specific systems and their components. Failure to load the boot-start driver is an example of a system log.
* **Application logs** contain events related to software or applications hosted on a Windows computer. Power Point Crushing will be logged as an application log .
* **Setup logs** contain events that occur during the installation of a Windows operating system.
* **Security logs** contain events related to the safety of the system. These may include file deletions , verification of account credentials

Windows event logs are further categorized into five different types: information, warning, error, success audit, and failure audit.

* **Information** indicates that an application or service is operating well.
* **Warning** highlights potential problems that system administrators should monitor.
* **Error** describes a significant issue when a system cannot function normally,
* **Success audit** records a valid attempt of audited security access.
* **Failure audit** records a failure of audited security access.

# Levels of Severity

Windows Events Logs have different levels of severity indicating the importance of the recorded event:-These are Categorized as follows:-

* Information – Indicates event occurred without issues.
* Verbose -represents progress or success messages for a specific event.
* Warning -Highlights potential problem system administrators should monitor

**Error:** Describes issues in the system or service that don't require immediate troubleshooting.

* **Critical:** Indicates a significant issue in an application or a system needing urgent attention.

Windows event logs can be viewed using the Windows Event Viewer, third-party tools such as DataDog, or by using the Event Viewer.

The Event Viewer tool scans through text log files and gathers and presents them in an intuitive user interface.

In Windows event logs are stored in **C:\WINDOWS\system32\config\ folder**. Event logs can be checked with the help of 'Event Viewer' to keep track of issues in the system.

To access the Event Viewer

* Press the **Windows key + R** on your keyboard to open the run window
* In the run dialog box, type in **eventvwr** and click OK
* In the Event Viewer window, expand the **Windows Logs** menu
* Under the **Windows Logs** menu, you'll notice different categories of event logs—application, security, setup, system, and forwarded events
* Click on one of the event logs to check and view the events recorded under it

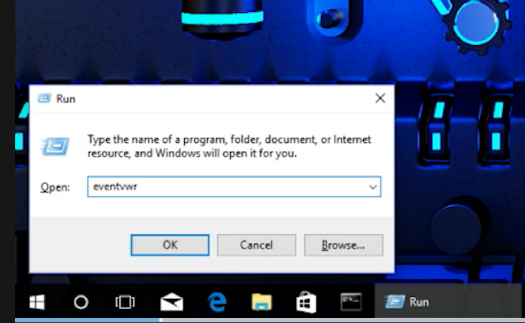


Figure : Registry editor

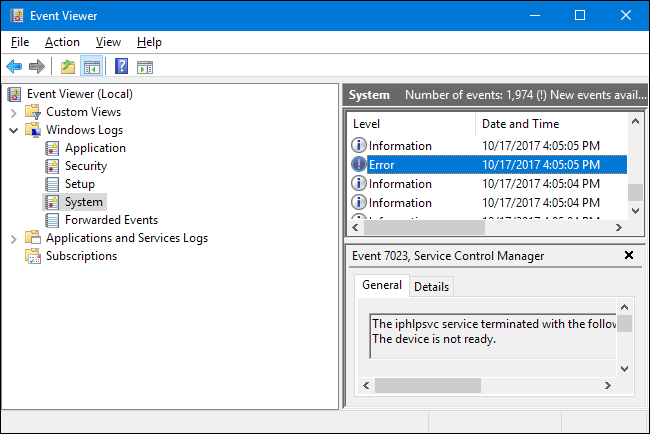


Figure : Event Viewer