EVENT LOG

12th Sep 2022

OVERVIEW

An event log is a basic "log book" that is analysed and monitored for higher level "network intelligence." It can capture many different types of information. For example, it can capture all logon sessions to a network, along with account lockouts, failed password attempts, etc. It can also record different types of application events, such as application errors, closures or other related events.

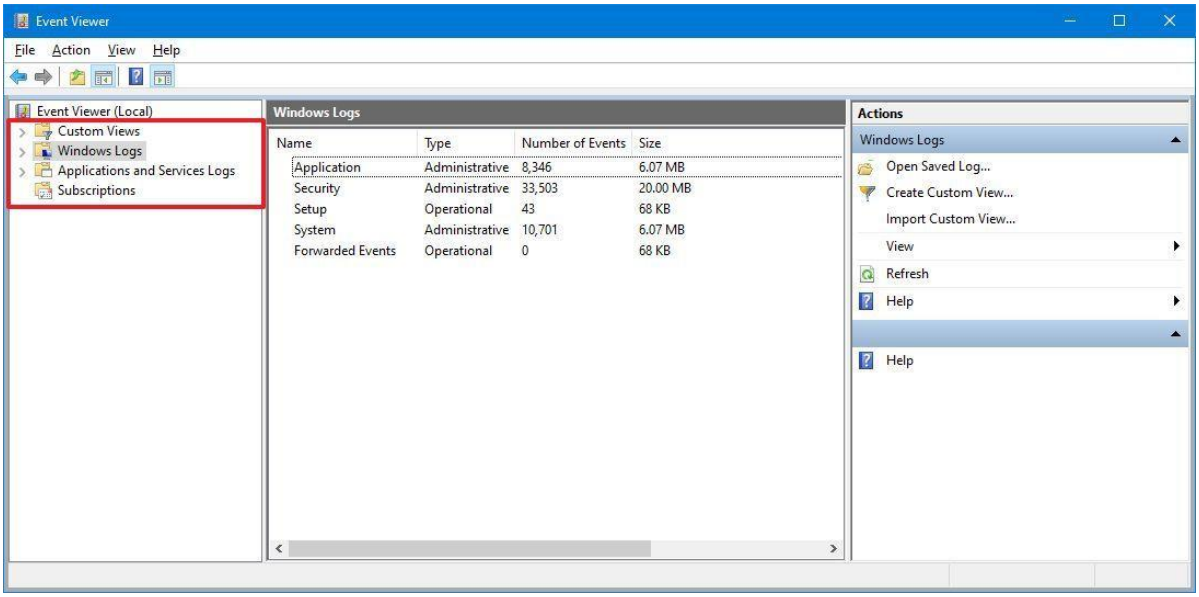
An event log is often used by a tool called security information and event management tool. This tool provides a higher level of analysis of the contents of an event log to help network administrators determine what is going on within a network.

Event Viewer displays these types of events:

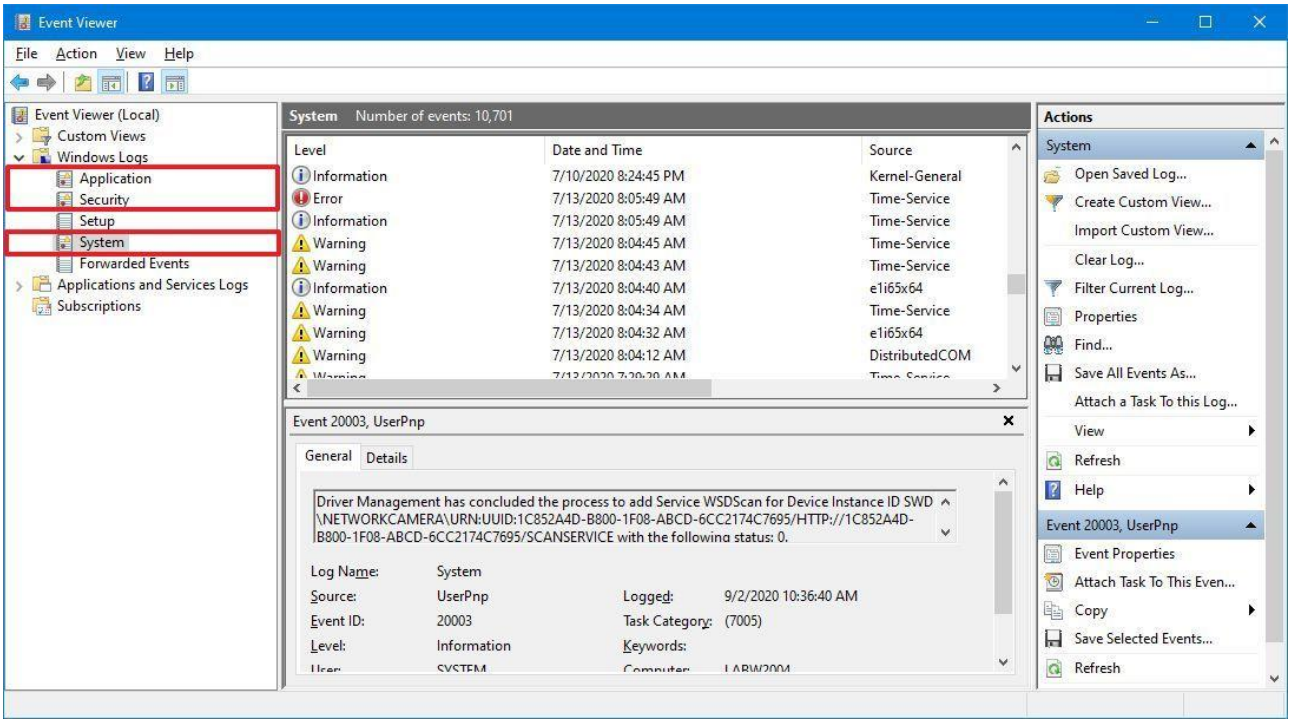
- **Error**: A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an error will be logged.
- **Warning**: An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a warning will be logged.
- **Information**: An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.
- **Success Audit**: An audited security access attempt that succeeds. For example, a user's successful attempt to log on to the system will be logged as a Success Audit event.
- **Failure Audit**: An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.

Interface navigation

To open the Event Viewer on Windows 10, simply open start and perform a search for **Event Viewer**, and click the top result to launch the console.
The experience is divided into four main groups, including "Custom Views," "Windows Logs," "Applications and Services Logs," and "Subscriptions," and each group stores related logs.

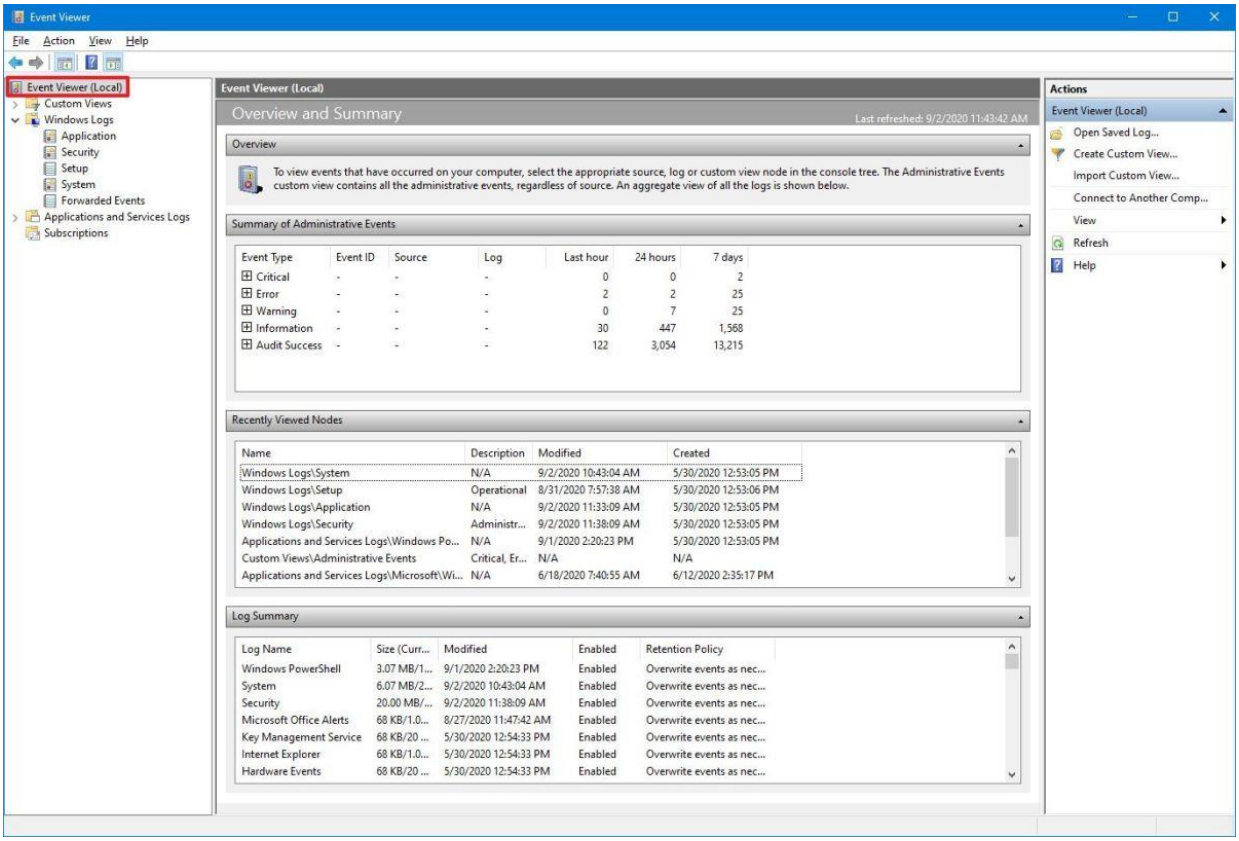


Although each group can hold different app and system logs, most of the time, you'll only be analyzing the **Application**, **Security**, and **System** logs inside the "Windows Logs" group to investigate an issue.

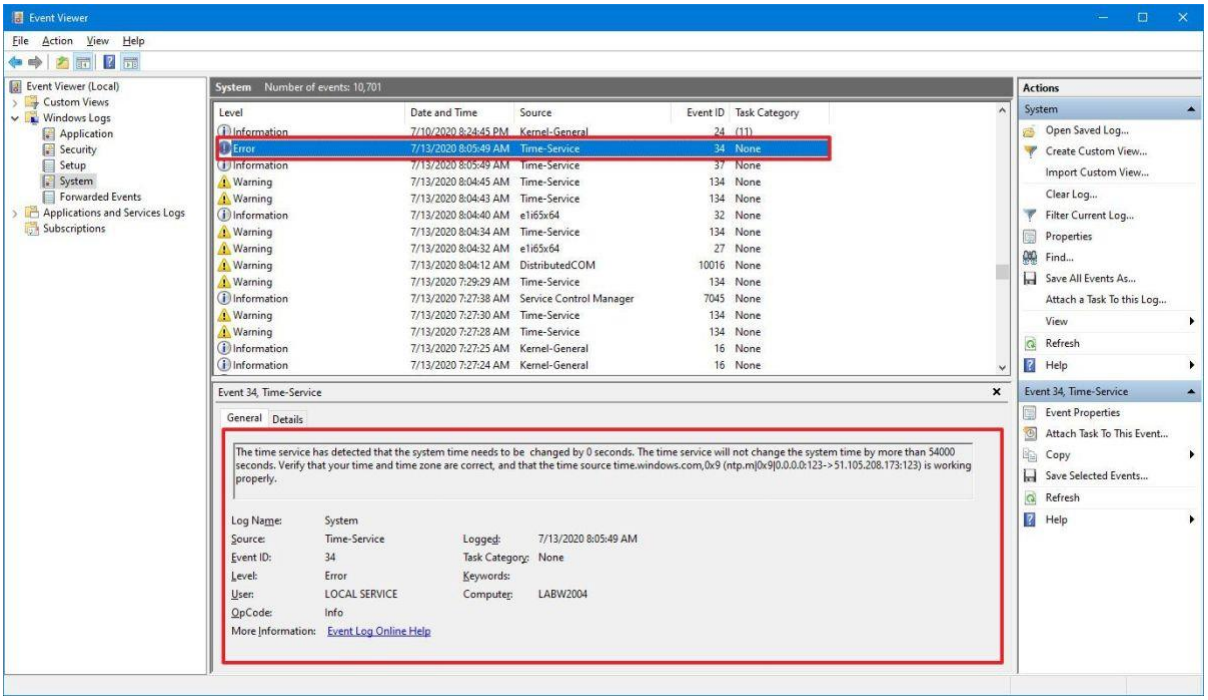


While in the console, you can select one of the main groups to view additional information, such as the number of events and size on the disk for each view. Or you can select "Event Viewer"

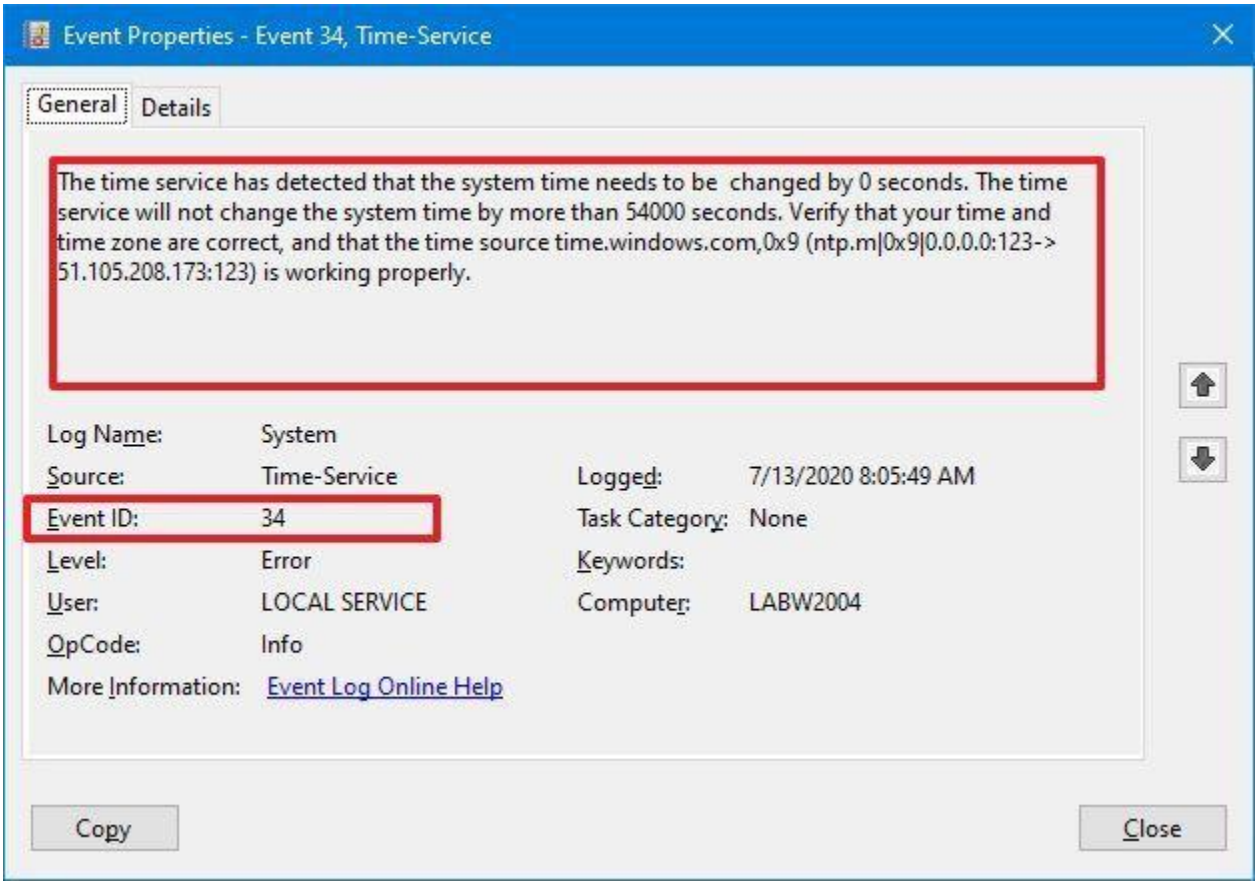
from the top-left to get an overview and summary of events, recently view notes, and log summary.



If you select one of the groups, on the right side, you'll see all the events with their "Level" information, "Date and Time" of creation, "Source," "Event ID," and "Task Category." If you want to see more details, you can select the event, and the information will be displayed at the bottom of the console, or you can double-click the event to access more details.



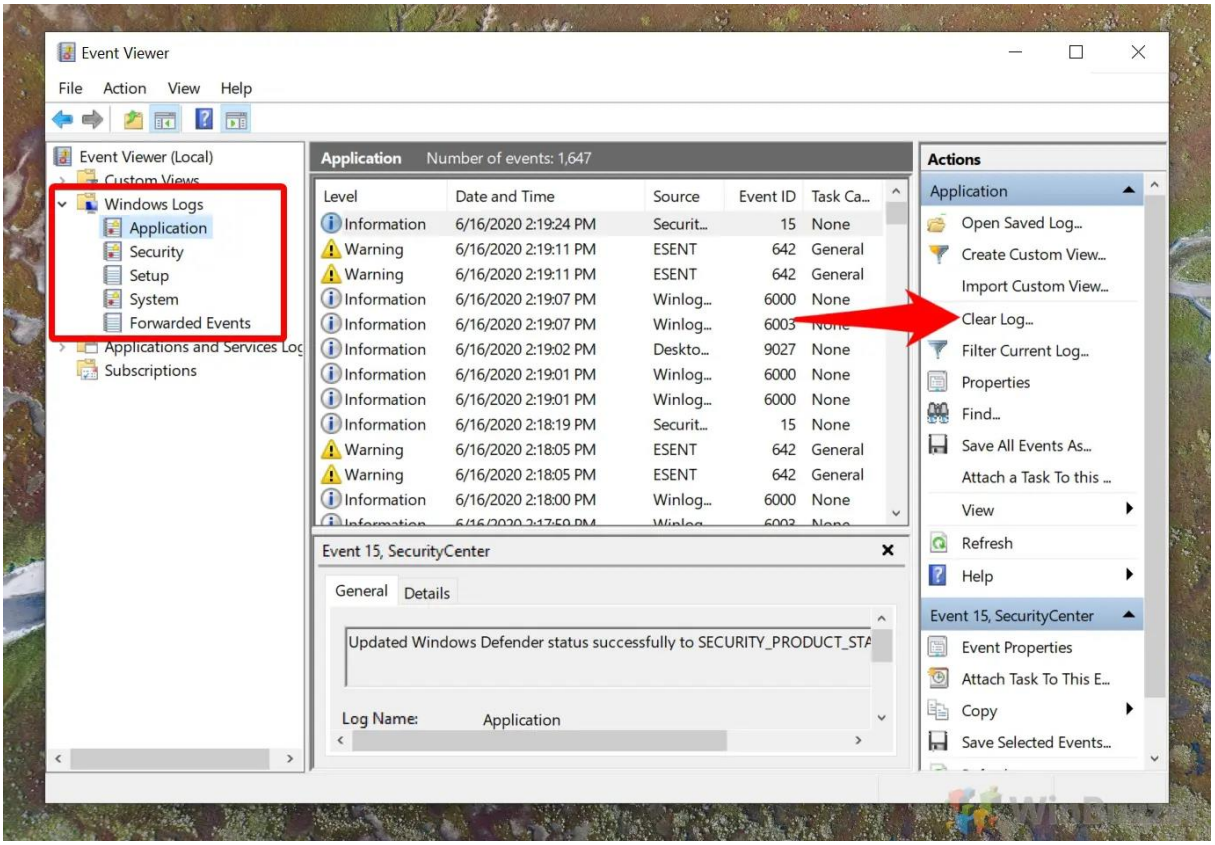
In the event properties window, the "General" tab includes an easy-to-understand description of the error, warning, or information.



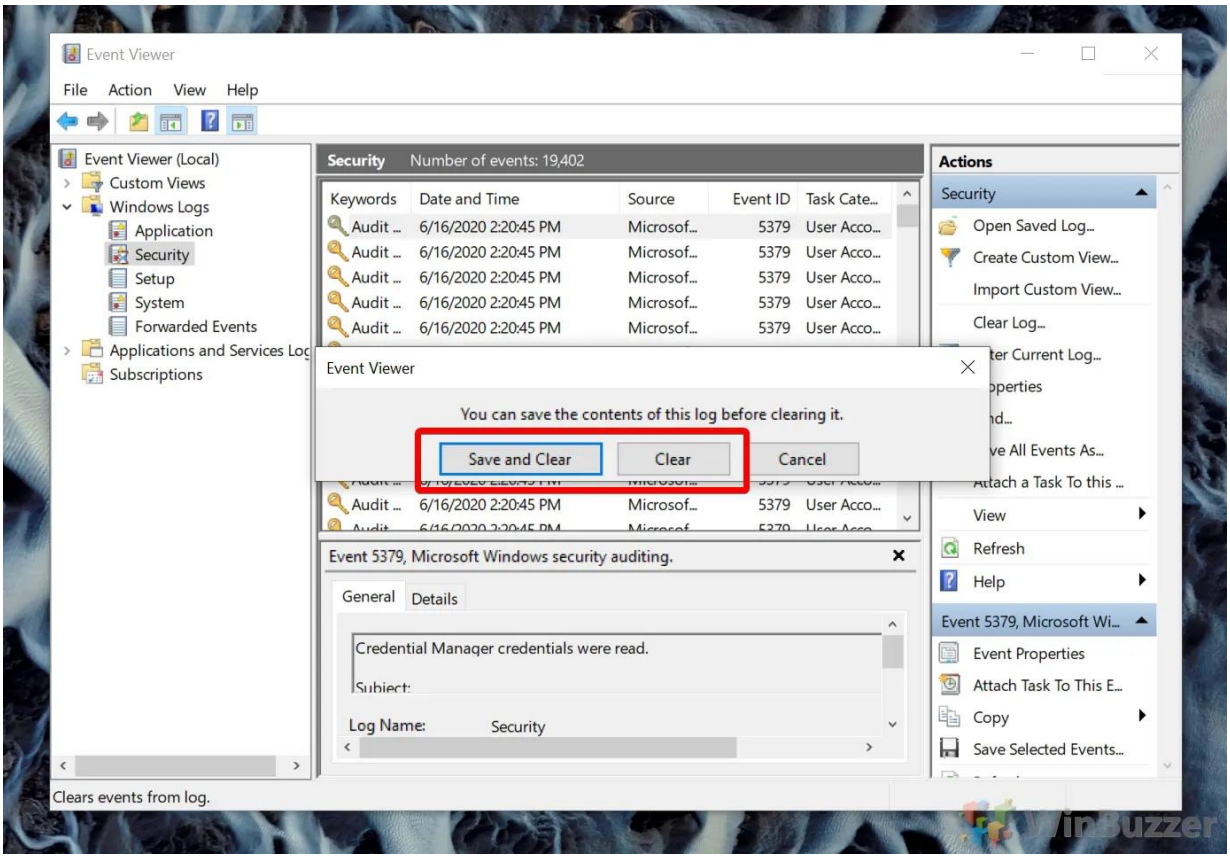
Usually, the description should give you enough information to understand and resolve the issue. However, the "Event ID" is also an important piece of information, as you can use it to search online to find out more information, and possible instructions to fix the problem.

Clear a Windows log file with the Event Viewer App

You can clear multiple logs at once by selecting them with Shift + click.



Click “Save and Clear” or “Clear”



As well as event viewer, logs from applications and services are stored. You can find them under the “Application and Services Logs” heading. Click the one you wish to delete and press **“Clear Log…”**.