

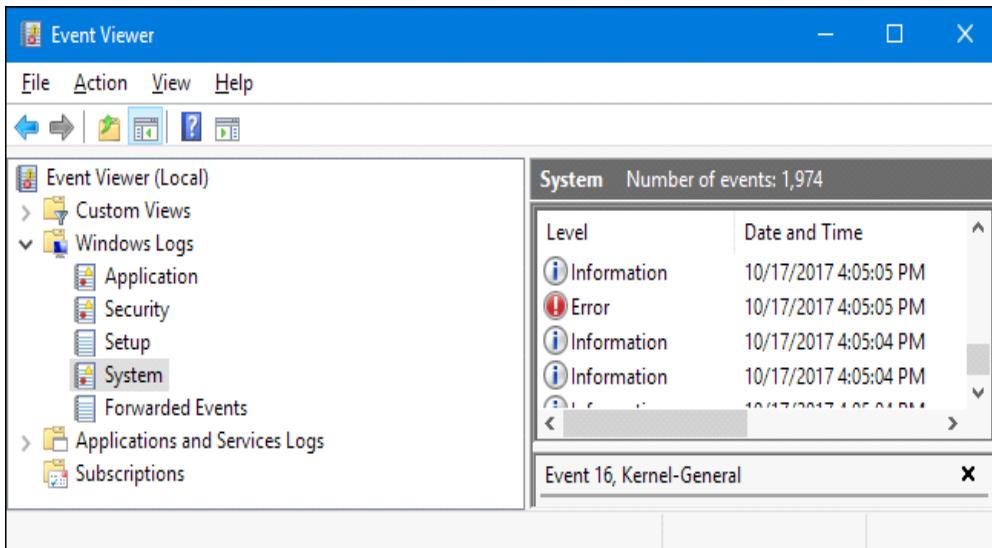
Operating Systems :

Thursday, December 25, 2025 10:26 PM

Operating Systems concepts focusing on Windows and Linux :



Event Viewer :

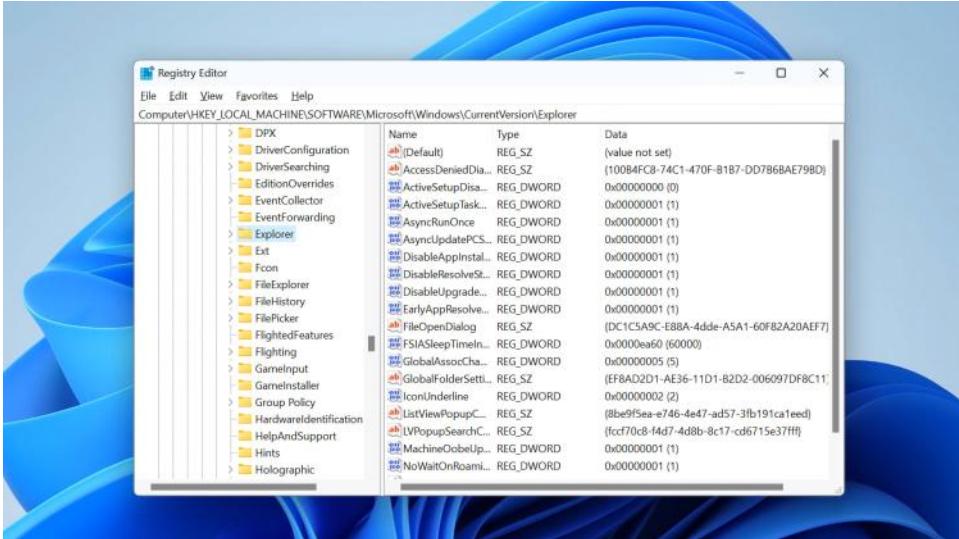


- ★ A built-in Windows tool used to view system logs.
- ★ Helps troubleshoot errors, warnings, crashes, and security events.
- ★ Logs are divided into:
 - Application – Software-related issues.
 - System – OS and hardware events.
 - Security – Login attempts, audits, policy changes.
- ★ Each event includes:
 - Event ID
 - Source
 - Severity (Information, Warning, Error, Critical)

Use cases :

- Diagnosing system crashes (BSOD)
- Investigating failed logins
- Tracking software or driver failures

Registry :



★ A central hierarchical database storing Windows configuration settings.

★ Contains settings for:

- Hardware
- Installed software
- User preferences
- System policies

★ Important Registry hives

- HKEY_LOCAL_MACHINE (system-wide settings)
- HKEY_CURRENT_USER (current user settings)
- HKEY_CLASSES_ROOT (file associations)

⚠ Incorrect changes can damage the OS, so backups are essential.



```
jasons@ip-172-31-11-241:~$ cd /var/log
jasons@ip-172-31-11-241:~/var/log$ ls
alternatives.log      btmp.1          dpkg.log.8.gz   news
alternatives.log.1    cloud-init.log  dpkg.log.9.gz   puppet
alternatives.log.2.gz  ConsoleKit     fontconfig.log  rsyslog-stats
alternatives.log.3.gz  datasync       fsck           syslog
alternatives.log.4.gz  dist-upgrade   kern.log      syslog.1
alternatives.log.5.gz  dmesg         kern.log.1    syslog.2.gz
alternatives.log.6.gz  dmesg.0       kern.log.2.gz  syslog.3.gz
alternatives.log.7.gz  dmesg.1.gz    kern.log.3.gz  syslog.4.gz
alternatives.log.8.gz  dmesg.2.gz    kern.log.4.gz  syslog.5.gz
apache2               dmesg.3.gz    landscape     syslog.6.gz
apport.log            dmesg.4.gz    lastlog      syslog.7.gz
apport.log.1          dpkg.log      mail.err      sysstat
apt                  dpkg.log.1    mail.err.1   tomcat6
auth.log              dpkg.log.10.gz  mail.err.2.gz udev
auth.log.1            dpkg.log.2.gz  mail.err.3.gz ufw.log
auth.log.2.gz          dpkg.log.3.gz  mail.log     unattended-upgrades
auth.log.3.gz          dpkg.log.4.gz  mail.log.1   upstart
auth.log.4.gz          dpkg.log.5.gz  mail.log.2.gz wtmp
boot.log              dpkg.log.6.gz  mail.log.3.gz wtmp.1
btmp                 dpkg.log.7.gz  mail.log.4.gz
```

Logs :

★ Plain text files that record system and application activity

★ **Stored mainly in /var/log/**

Common log files :

- /var/log/syslog – General system activity
- /var/log/auth.log – Authentication and sudo usage
- /var/log/dmesg – Kernel messages
- /var/log/boot.log – Boot process info

Viewing logs :

- cat, less, tail

Permissions :

Linux uses a permission-based security model for files and directories.

Permission types

- r – read
- w – write
- x – execute

User categories

- Owner
- Group
- Others

Example:

-rwxr-xr--

- Owner: read, write, execute
- Group: read, execute
- Others: read only

Commands :

- ls -l → View permissions
- chmod → Change permissions
- chown → Change file owner

Feature	Windows	Linux
Logs	Event Viewer	Text files in /var/log
Config Storage	Registry	Text config files
Permissions	GUI + ACL	rwx (owner/group/others)
Admin Tool	GUI-heavy	CLI-focused