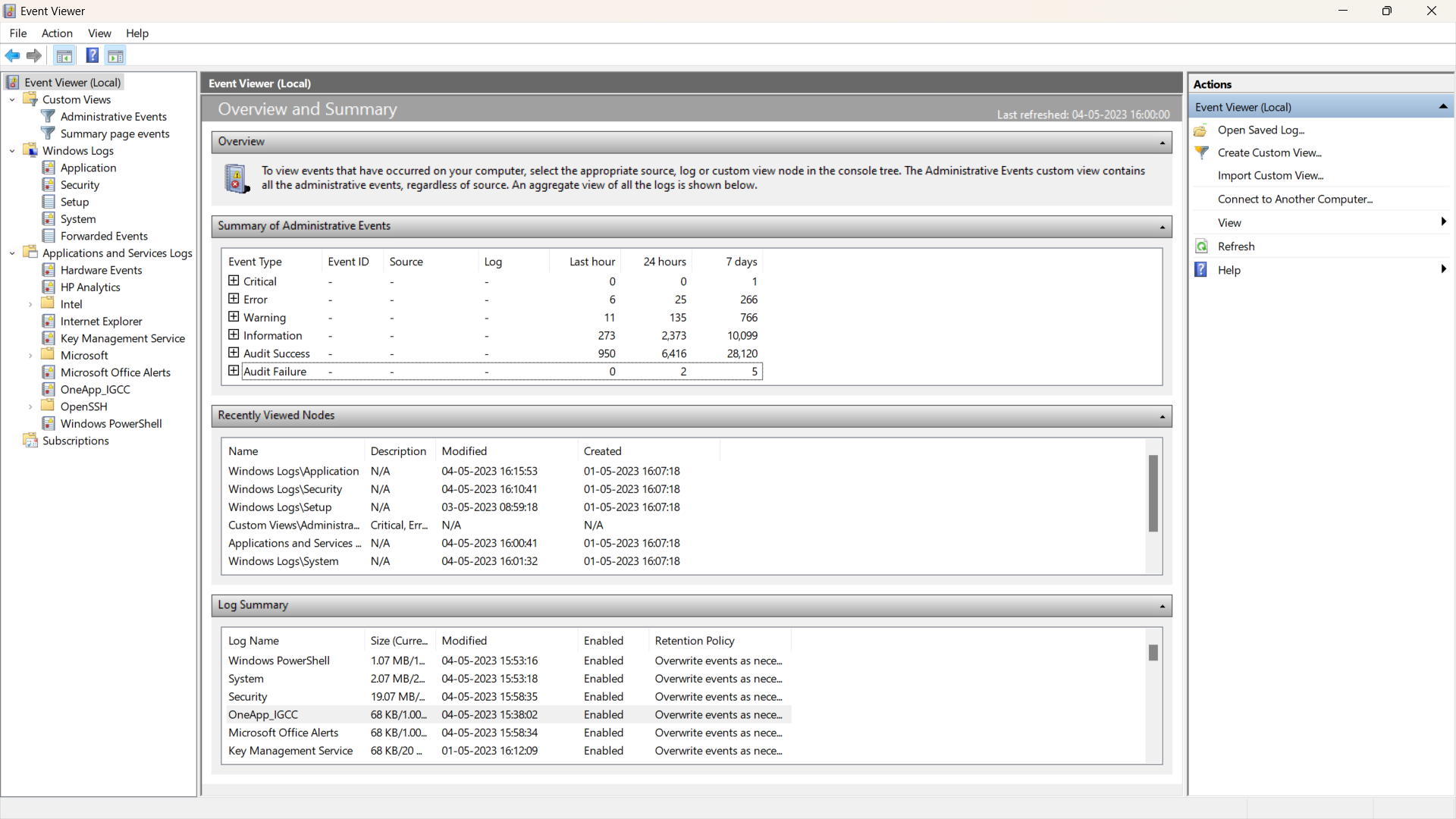
**Title: Analysis and monitor system log using event viewer**

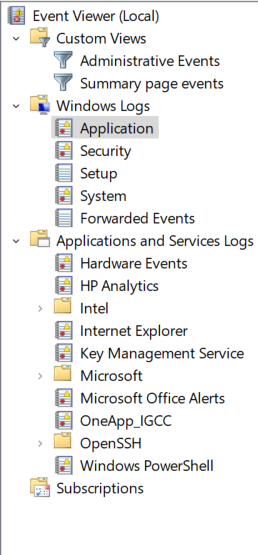
**Requirement: Event Viewer**

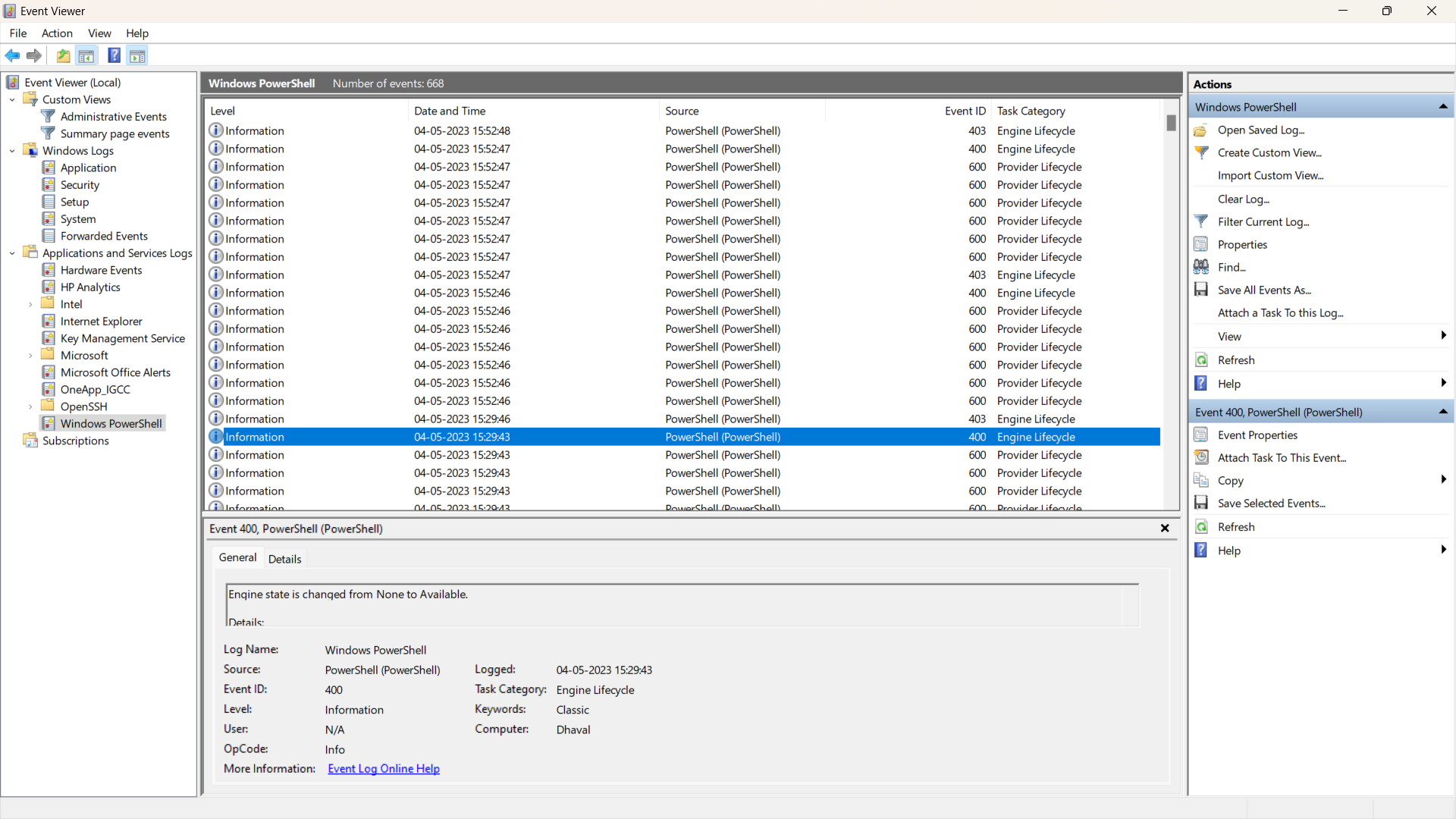
**Procedure/experiment steps:**

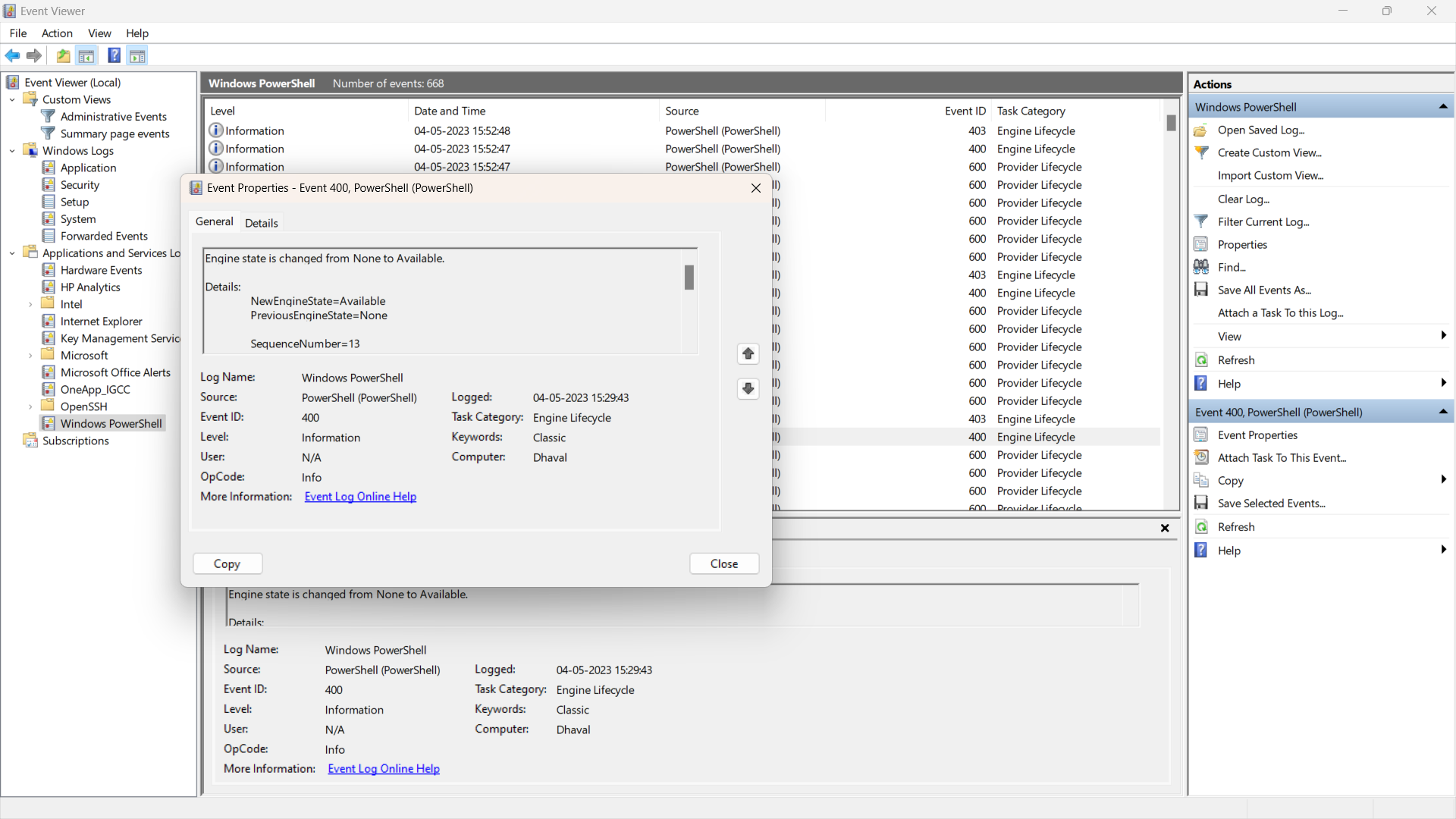
* Open Event Viewer : Start > event viewer
* In general we can see information in a middle Pannal as
  + Summary of administrative event
    - Event type
      * Critical
      * Error
      * Warning
      * Information
      * Audit Success
      * Audit Failure
    - Event id
    - Source
    - Log
    - Last hour
    - 24 hour
    - 7days
  + Recently View Nods
  + Log summary
    - Log name
    - Size
    - Modified
    - Enable
    - Retention policy
* There is different log type in the left Pannal
  + Custom
  + Windows Log
  + Application and Service logs
  + Subscription
* Select and view different logs
* Select any section and sub section and see the different logs and what this log contains

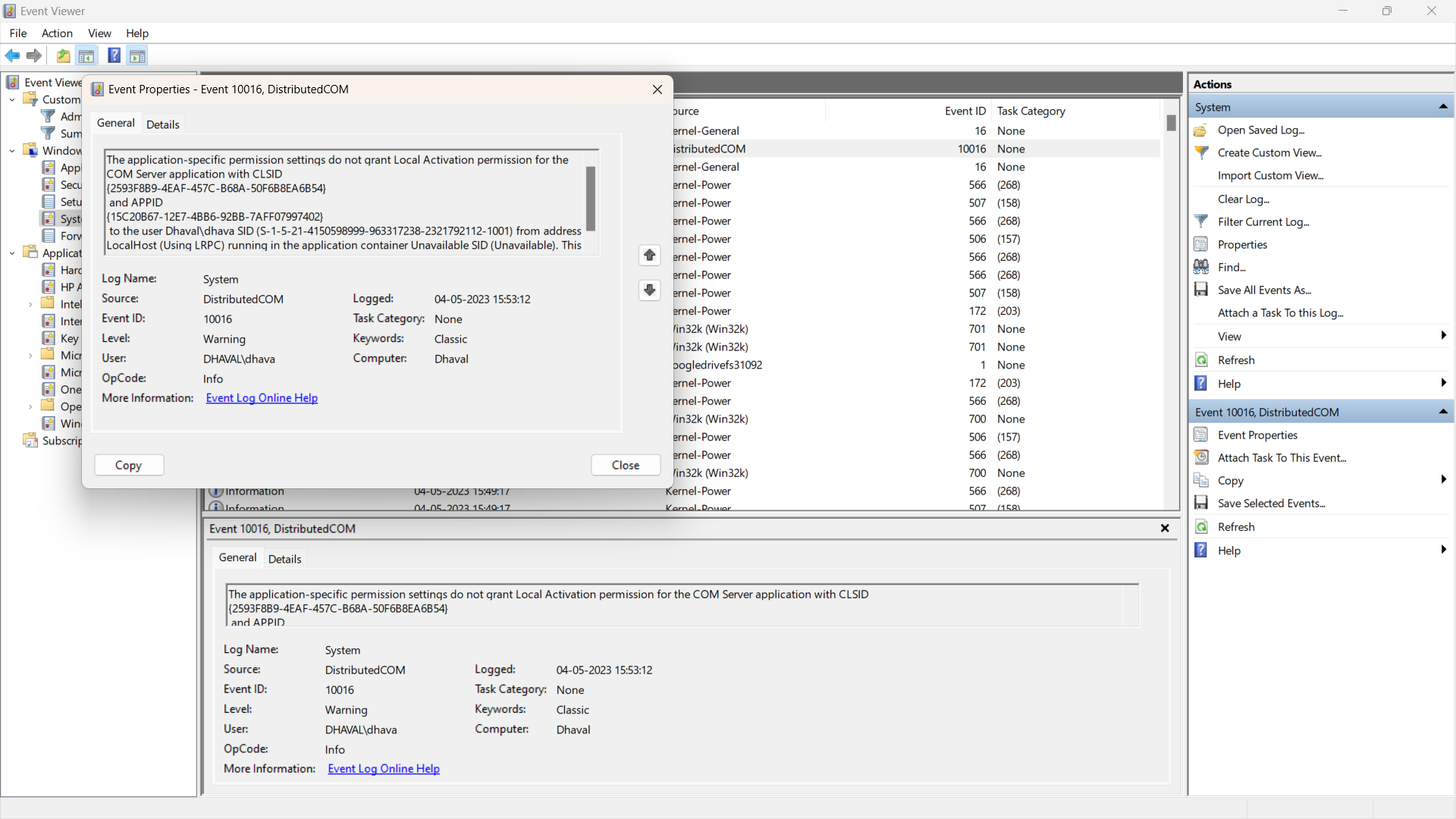
**Result:**











**Result analysis:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Summary of Administrative Events** | | | |
| **Event Type** | **Last Hour** | **24 hour** | **7 days** |
| Critical | 0 | 0 | 1 |
| Error | 6 | 25 | 266 |
| Warning | 11 | 135 | 766 |
| Information | 273 | 2373 | 10099 |
| Audit Success | 950 | 6416 | 28120 |
| Audit Failure | 0 | 2 | 5 |

**Conclusion:**

* With event view we can see different events that workers in our system. With the help of event view we can also see a different logs in the specific groups and specific filter work we can see what lock contains and the information which is passed through it.

**Future scope:**

* Even if you can use by your system administrator or by the security person To check what kind of event occur in the system to prevent if there is any suspicious event is there and protect the system. We can also see a warning and error the logs like bonding logs error logs informational logs then audit logs.