Title: Analysis and monitor system log using event viewer

Requirement: Event Viewer

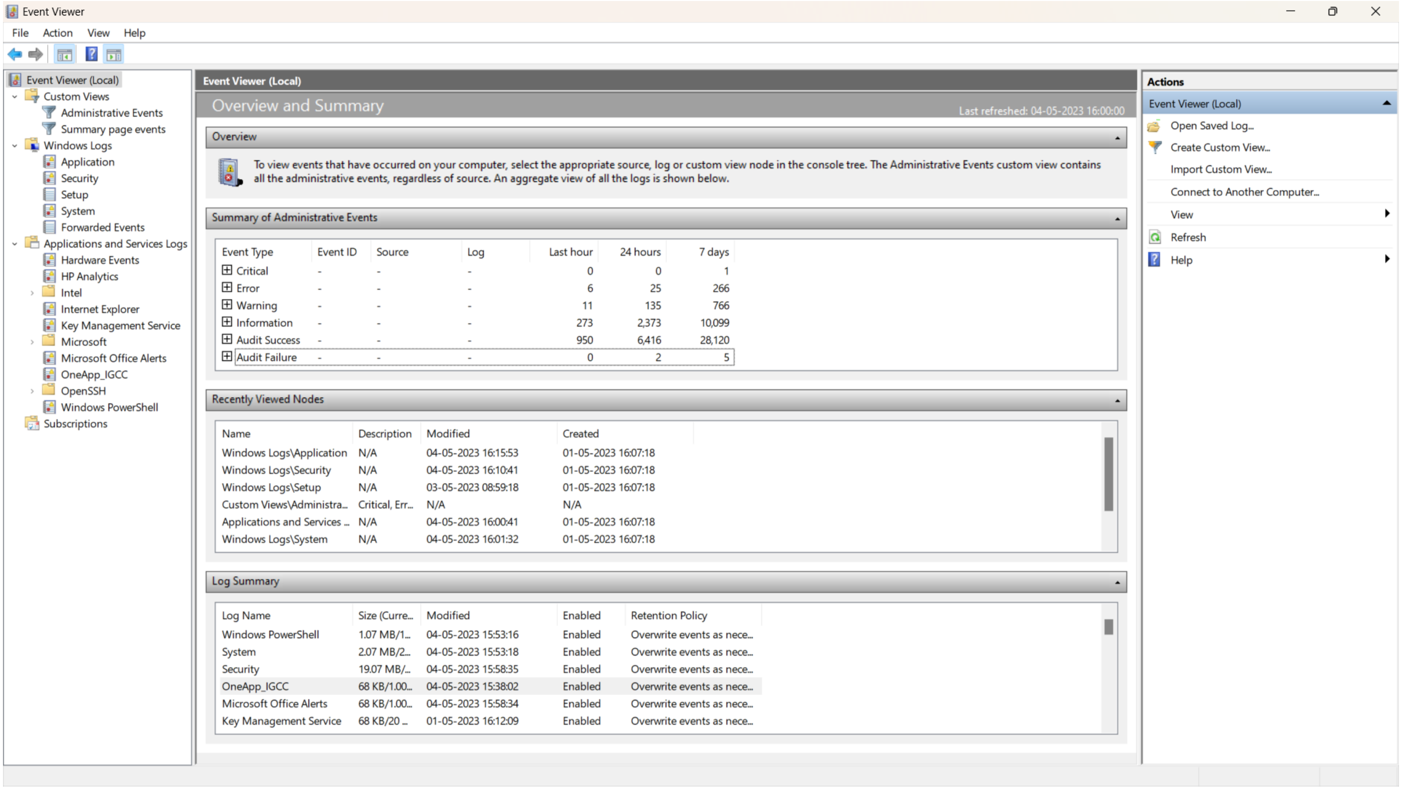
Procedure/experiment steps:

- 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:

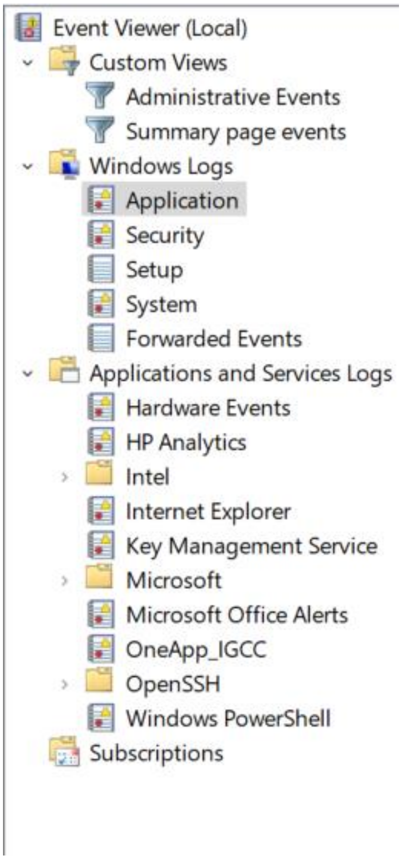


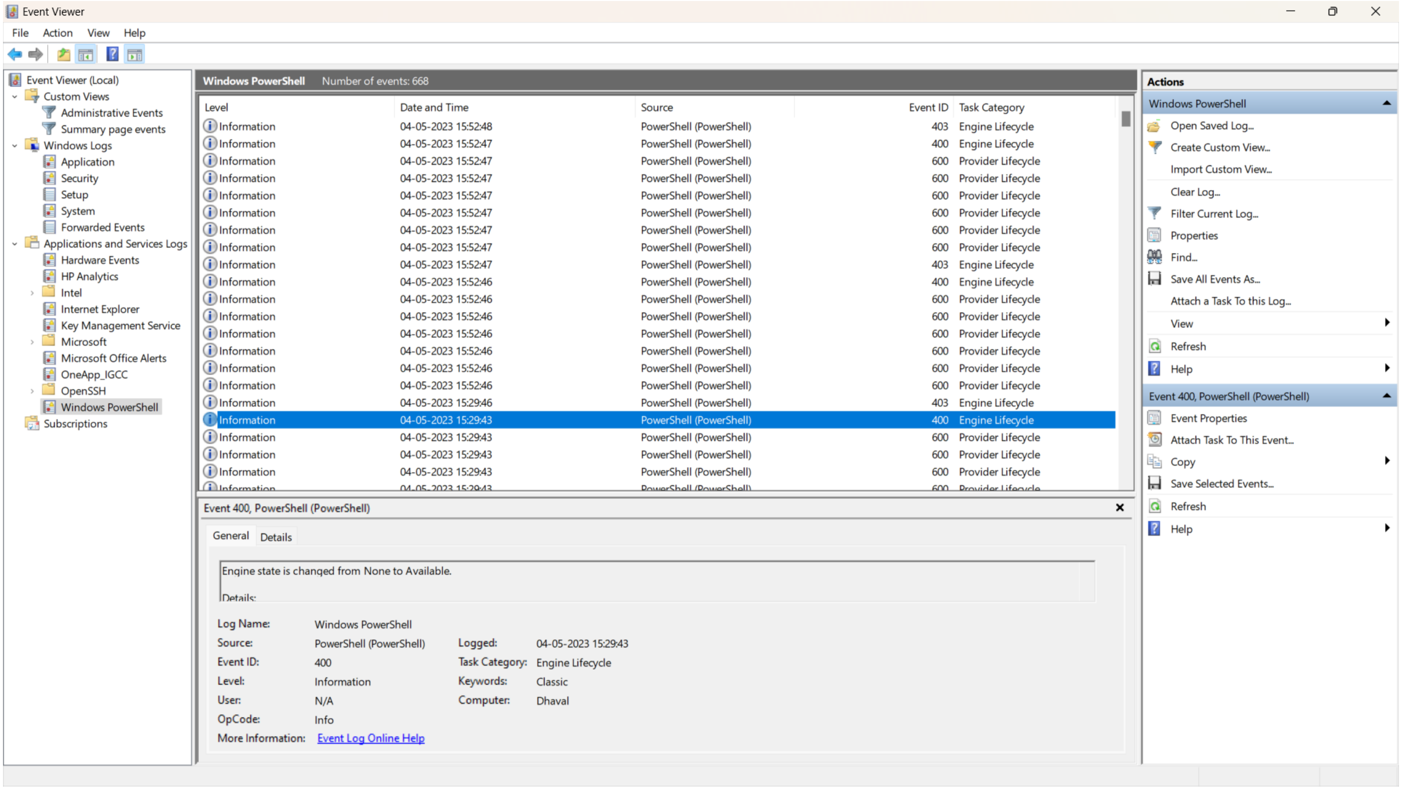
To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all the logs is shown below.

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
⊞ Critical	-	-	-	0	0	1
⊞ Error	-	-	-	6	25	266
⊞ Warning	-	-	-	11	135	766
⊞ Information	-	-	-	273	2,373	10,099
⊞ Audit Success	-	-	-	950	6,416	28,120
⊞ Audit Failure	-	-	-	0	2	5

Name	Description	Modified	Created
Windows Logs\Application	N/A	04-05-2023 16:15:53	01-05-2023 16:07:18
Windows Logs\Security	N/A	04-05-2023 16:10:41	01-05-2023 16:07:18
Windows Logs\Setup	N/A	03-05-2023 08:59:18	01-05-2023 16:07:18
Custom Views\Administra...	Critical, Err...	N/A	N/A
Applications and Services ...	N/A	04-05-2023 16:00:41	01-05-2023 16:07:18
Windows Logs\System	N/A	04-05-2023 16:01:32	01-05-2023 16:07:18

Log Name	Size (Curre...	Modified	Enabled	Retention Policy
Windows PowerShell	1.07 MB/1...	04-05-2023 15:53:16	Enabled	Overwrite events as nece...
System	2.07 MB/2...	04-05-2023 15:53:18	Enabled	Overwrite events as nece...
Security	19.07 MB/...	04-05-2023 15:58:35	Enabled	Overwrite events as nece...
OneApp_IGCC	68 KB/1.00...	04-05-2023 15:38:02	Enabled	Overwrite events as nece...
Microsoft Office Alerts	68 KB/1.00...	04-05-2023 15:58:34	Enabled	Overwrite events as nece...
Key Management Service	68 KB/20 ...	01-05-2023 16:12:09	Enabled	Overwrite events as nece...





Windows PowerShell Number of events: 668

Level	Date and Time	Source	Event ID	Task Category
Information	04-05-2023 15:52:48	PowerShell (PowerShell)	403	Engine Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	400	Engine Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	403	Engine Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	400	Engine Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:29:46	PowerShell (PowerShell)	403	Engine Lifecycle
Information	04-05-2023 15:29:43	PowerShell (PowerShell)	400	Engine Lifecycle
Information	04-05-2023 15:29:43	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:29:43	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:29:43	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:29:43	PowerShell (PowerShell)	600	Provider Lifecycle

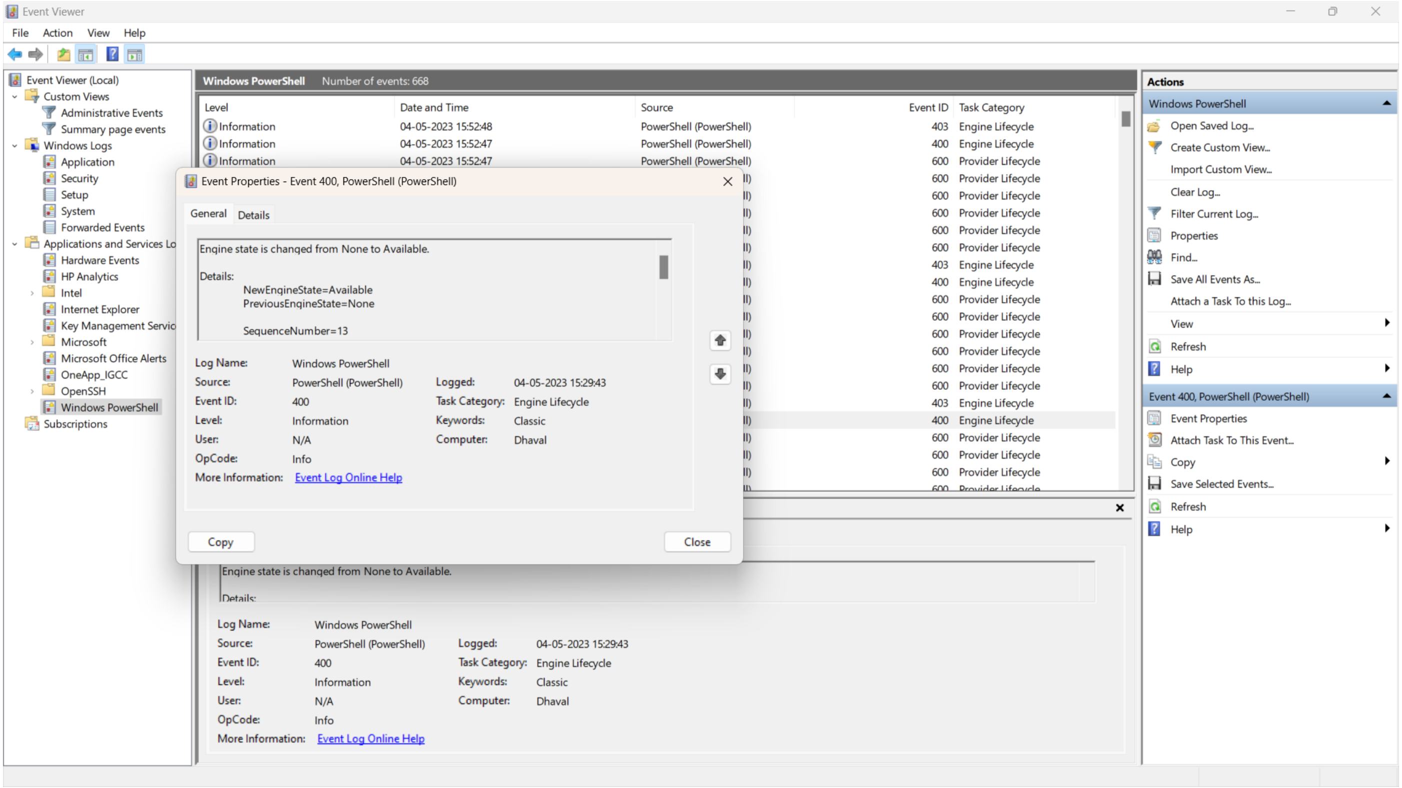
Event 400, PowerShell (PowerShell)

General Details

Engine state is changed from None to Available.

Details:

Log Name:	Windows PowerShell		
Source:	PowerShell (PowerShell)	Logged:	04-05-2023 15:29:43
Event ID:	400	Task Category:	Engine Lifecycle
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	Dhaval
OpCode:	Info		
More Information:	Event Log Online Help		



Event Properties - Event 400, PowerShell (PowerShell)

General Details

Engine state is changed from None to Available.

Details:

```
        NewEngineState=Available
        PreviousEngineState=None

        SequenceNumber=13
```

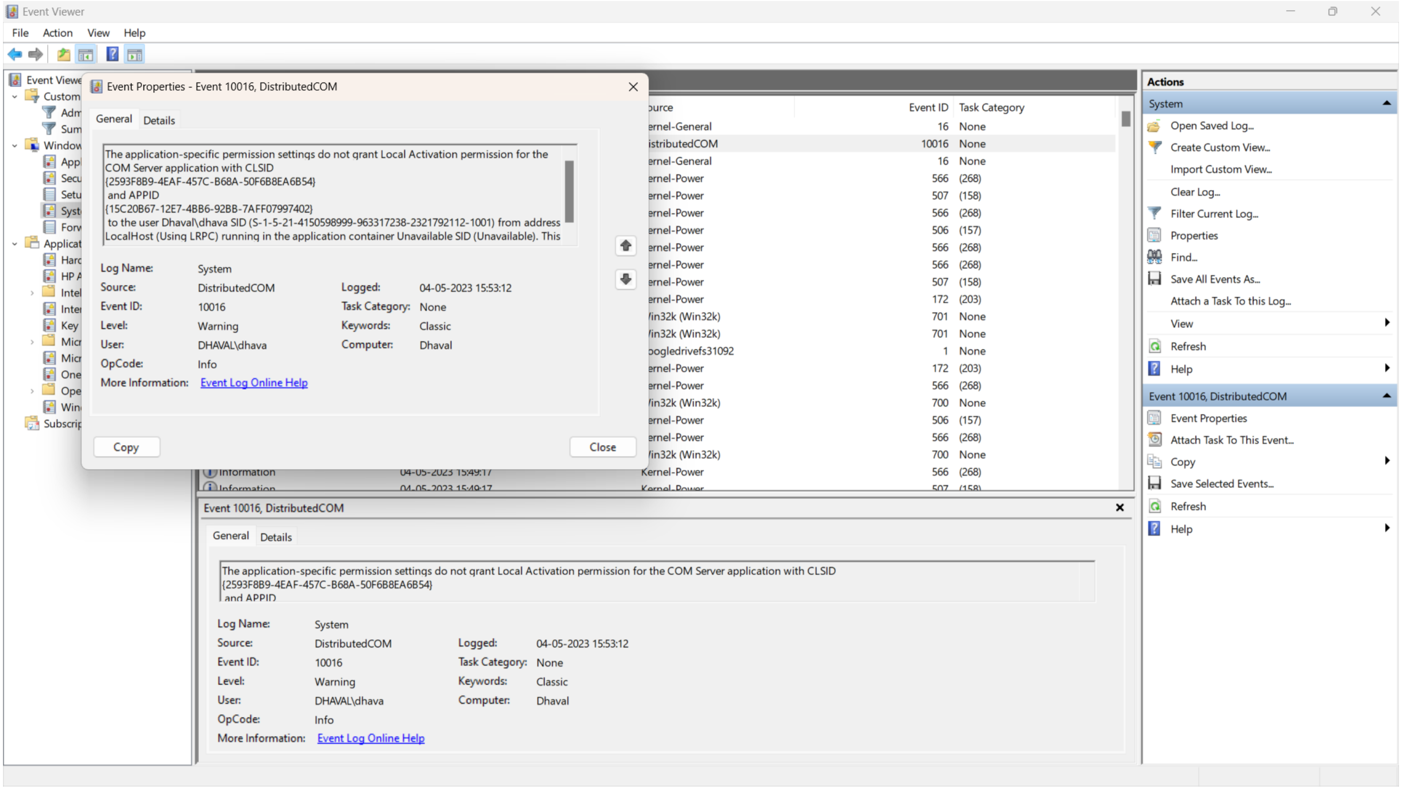
Log Name:	Windows PowerShell		
Source:	PowerShell (PowerShell)	Logged:	04-05-2023 15:29:43
Event ID:	400	Task Category:	Engine Lifecycle
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	Dhaval
OpCode:	Info		
More Information:	Event Log Online Help		

Windows PowerShell Number of events: 668

Engine state is changed from None to Available.

Details:

Log Name: Windows PowerShell
Source: PowerShell (PowerShell) Logged: 04-05-2023 15:29:43
Event ID: 400 Task Category: Engine Lifecycle
Level: Information Keywords: Classic
User: N/A Computer: Dhaval
OpCode: Info
More Information: Event Log Online Help



Event Properties - Event 10016, DistributedCOM

The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID
{2593F8B9-4EAF-457C-B68A-50F6B8EA6B54}
and APPID
{15C20B67-12E7-4BB6-92BB-7AFF07997402}
to the user Dhaval\dhava SID (S-1-5-21-4150598999-963317238-2321792112-1001) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This

Log Name:	System		
Source:	DistributedCOM	Logged:	04-05-2023 15:53:12
Event ID:	10016	Task Category:	None
Level:	Warning	Keywords:	Classic
User:	DHAVAL\dhava	Computer:	Dhaval
OpCode:	Info		
More Information:	Event Log Online Help		

```
ource                     Event ID  Task Category
ernel-General                   16  None
istributedCOM                10016  None
ernel-General                   16  None
ernel-Power                    566  (268)
ernel-Power                    507  (158)
ernel-Power                    566  (268)
ernel-Power                    506  (157)
ernel-Power                    566  (268)
ernel-Power                    566  (268)
ernel-Power                    507  (158)
ernel-Power                    172  (203)
/in32k (Win32k)                701  None
/in32k (Win32k)                701  None
oogledrivefs31092                1  None
ernel-Power                    172  (203)
ernel-Power                    566  (268)
/in32k (Win32k)                700  None
ernel-Power                    506  (157)
ernel-Power                    566  (268)
/in32k (Win32k)                700  None
Information     04-05-2023 15:49:17     Kernel-Power     566  (268)
Information     04-05-2023 15:49:17     Kernel-Power     507  (158)
```

Event 10016, DistributedCOM

The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID
{2593F8B9-4EAF-457C-B68A-50F6B8EA6B54}
and APPID

Log Name:	System		
Source:	DistributedCOM	Logged:	04-05-2023 15:53:12
Event ID:	10016	Task Category:	None
Level:	Warning	Keywords:	Classic
User:	DHAVAL\dhava	Computer:	Dhaval
OpCode:	Info		
More Information:	Event Log Online Help		

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.