Security Logs

A)


```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Microsoft-Windows-Eventlog" Guid="{fc65ddd8-d6ef-4962-83d5-
        6e5cfe9ce148}" />
      <EventID>1101</EventID>
      <Version>0</Version>
      <Level>2</Level>
      <Task>101</Task>
      <Opcode>0</Opcode>
      <Keywords>0x4020000000000000</Keywords>
      <TimeCreated SystemTime="2024-06-27T11:19:31.3760221Z" />
      <EventRecordID>2633316</EventRecordID>
      <Correlation />
      <Execution ProcessID="1628" ThreadID="2532" />
      <Channel>Security</Channel>
      <Computer>PC22</Computer>
      <Security />
    </System>
  - <UserData>
    - <AuditEventsDropped
        xmlns="http://manifests.microsoft.com/win/2004/08/windows/eventlog">
        <Reason>0</Reason>
      </AuditEventsDropped>
    </UserData>
  </Event>
```


System Section:

- **Provider:** Microsoft-Windows-Eventlog (Standard Windows event log provider)
- **EventID:** 1101 (Specific code for dropped audit events)
- **Level:** 2 (Success - Similar to the previous application error log, this indicates informational purposes)
- **Task:** 101 (Likely system startup or general housekeeping task)
- **Opcode:** 0 (Informational operation code)
- **Keywords:** 0x4020000000000000 (Security auditing keyword)
- **TimeCreated:** 2024-06-27T11:19:31.3760221Z (Coordinated Universal Time timestamp)
- **EventRecordID:** 2633316 (Unique identifier for this event log entry)
- **Channel:** Security (Category of the event log)
- **Computer:** PC22 (Name of the computer where the event was generated)

UserData Section:

- **AuditEventsDropped:** This element confirms the event is related to dropped audit events.
- **Reason:** 0 (Unfortunately, the reason code "0" doesn't provide a specific explanation for why the events were dropped).

Interpretation:

This log entry indicates that some security audit events were dropped on computer PC22. The specific reason for dropping the events is not provided in this log (Reason code 0). Security Event ID 1101 event can occur during dirty shutdown, after a reboot , during a period of high system stress or under unusual circumstances (malicious behaviour).

Recommendations:

- Ensure proper system shutdowns to minimize the chance of dropped events.
- You can research online resources for troubleshooting Event ID 1101 to see if there are known causes related to your system configuration.
- Consider checking the Windows Security logs for other events around the same timeframe that might provide additional context on potential security-related activities.
- If dropped audit events are a persistent issue, you might need to investigate your system's security settings and event log configuration to ensure sufficient storage space and proper forwarding mechanisms are in place.
- Run DISM and SFC scan
- Reset windows update components
- Update device drivers