Privilege escalation

```
log show --predicate 'process == "sudo" and eventMessage CONTAINS "TTY"'
```

Privilege escalation - Users not in sudoers

```
log show --predicate 'process == "sudo" and eventMessage contains "user NOT in sudoers"'
```

View Content Caching Logs

```
log show --predicate 'subsystem == "com.apple.AssetCache"'
```

Jamf Connect Login

```
log show --predicate 'subsystem == "com.jamf.connect.login"' --debug
```

Jamf Connect Menu Bar

```
log show --style compact --predicate 'subsystem == "com.jamf.connect"' --debug
```

Jamf Management Binary

```
log show --predicate 'subsystem == "com.jamf.management.binary"' --info
```

Jamf Intune Integration

```
log show --predicate 'subsystem CONTAINS "jamfAAD"'
```

macOS Login Examples. More can be found here: http://www.mac4n6.com/blog/2020/4/26/analysis-of-apple-unified-logs-quarantine-edition-entry-4-its-login-week

Screen Is locked

```
log show --predicate 'eventMessage contains "com.apple.sessionagent.screenIsLocked"'
```

Screen Is unlocked

```
log show --predicate 'eventMessage contains "com.apple.sessionagent.screenIsUnlocked"'
```

MacOS Logins

```
log show --predicate 'process contains "loginwindow" and eventMessage contains "com.apple.sessionDidLogin"' --last 24h
```

macOS Shutdown
More info on shutdown codes can be found here:
https://georgegarside.com/blog/macos/shutdown-causes

```
log show --predicate 'eventMessage contains "Previous shutdown cause"' --last 24h
```

Transparency Consent and Control

```
log stream--predicate 'subsystem == "com.apple.TCC" AND eventMessage BEGINSWITH “AttributionChain"' --debug
```

Messages related to the battery

```
log show --predicate 'processImagePath CONTAINS[c] "powerd" && eventMessage CONTAINS[c] "battery"'
```

App Store 10.15 and below

```
log show --predicate 'processImagePath contains "storedownloadd"' --debug
```

App Store 11.0 and above

```
log show --predicate 'processImagePath contains "appstored"' --debug
```

Native MDM Client

```
log show --predicate 'processImagePath contains "mdmclient"' --debug
```

Airdrop

```
log show --predicate 'subsystem == "com.apple.sharing" and category ==
"AirDrop"' --info
```

Screen Sharing Authentication attempts

```
log show --predicate 'processImagePath CONTAINS "screensharingd" AND
eventMessage CONTAINS "Authentication"'
```

Automated Device Enrolment

```
log stream --info --debug --predicate 'subsystem contains
"com.apple.ManagedClient.cloudconfigurationd"'
```

Apple Push Notification service daemon

```
log show --predicate 'sender contains[c] "apsd"'
```