zOS SYSLOG Analysis

See below for zOS SYSLOG analysis related mainframe concepts.

Python Program for zOS SYSLOG Analysis

Analyzes zOS daily SYSLOG or OPERLOG listing.
Multi-line messages are constructed from message types and request types.
Unique message-IDs and operator commands are also counted.
Messages types, request types, unique messages-IDs and operator commands are displayed to allow further filtering.
There are also some lines starting with dash character ("-"). These lines are created after each job and step completed.
These lines also analyzed and unique values are collected and printed together with counts.

Mainline steps of zOS SYSLOG Analysis Program:

1. Each syslog line is read.
2. When a primary type line is read, it is either added to a list or number of occurrence is incremented.
3. If the primary type line has a dash line, it is added to a list and incremented.
4. Messages other than dash messages are also recorded and counted.
5. When a continuation message type is read, it is also recorded and counted.
6. If the message and request type combination is not recognized, program issues a message and stop processing. The message type combination is expected to be added.
7. List of primary message types is sorted and printed.
8. List of unique message IDs is sorted and printed.
9. List of message types/ request types combinations is sorted and printed.
10. List of unique dash message types is sorted and printed.
11. Program epilog.

Software release information:

IBM z/OS v2.4
Python and Idle 3.11.6 with tcl/tk 8.6.13
Ubuntu 23.10 Desktop AMD 64

zOS SYSLOG analysis related concepts:

z/OS is IBM mainframe operating system.
in zOS, All programs communicate to operator through displaying messages.
All messages, commands and replies in a zOS system are written to SYSLOG (System Log).
All SYSLOGs in a SYSPLEX (Systems Complex, cluster of mainframes) are collected in OPERLOG (Operations Log).
Most messages have a message-ID at the beginning of the message.
There are both single line and multiple line messages.
Continuations of messages are specified in message type and request type characters at the beginning of messages.
Daily zOS SYSLOG/ OPERLOG message counts can be in the hundreds of thousands, if not millions. they needed to be analyzed before further filtering and log processing.

References:

Using the system log
https://www.ibm.com/docs/en/zos/3.1.0?topic=sdsf-using-system-log

Record Type Codes
https://www.ibm.com/docs/en/zos/3.1.0?topic=sdsf-using-system-log#isfa600_sdsflog__table_k52_m5r_wxb

JCL for the LOGR Subsystem
https://www.ibm.com/docs/en/zos/2.4.0?topic=format-jcl-logr-subsystem