The SYSLOG is a SYSOUT data set provided by the job entry subsystem (either JES2 or JES3).

In a CF log stream, interim storage for log data is in CF list structures supporting the ability for exploiters on more than one system to view log data from a single log stream concurrently.

Log record data is written to the SYS1.LOGREC data set and is also written to internal storage that is included in a dump.

- The SYS1.LOGREC data set can be interrogated using the ICFERP1 program, or if the head has triggered a dump, the EREP data can be reviewed using the IPCS VERBX LOGDATA command.

- Generally, there is no influence on the problem being reviewed, have time stamps that relate to or immediately precede the actual event; although there is no guarantee the error records will be written in the order they occurred.

- The EREP log stream is also written to an internal storage buffer that is included in the dump.

- Using a log record stream rather than a log data set (SYS1.LOGREC, by default for each system can streamline log record error records.

Concluding: Log record data that the installation specifically chooses to log.

Log record The log record is a record of the system message traffic that the installation chooses to log, such as messages in log data sets and output messages for the operator (using the OPERLOG command).

In a dump, these messages are in the master trace and with JES3, the log record is always written to the SYSLOG.

With JES2, the log record is typically written to the SYSLOG, but can also be written to a console printer, if your installation chooses to do so.

Cheat Sheet #59 zTidBits

- Logs and the Logger

- Logs are an essential tool for analyzing and troubleshooting problems in the system.
- Logs provide valuable information about the system's operation and can help identify issues before they become severe.

System Logger

- System Logger is an zOS component that provides a logging facility for applications running in a single-system or multi-system sysplex.
- The advantage of using System Logger is that it enables the logging of data (with the requested persistence), retrieving the data (potentially from any system in the sysplex), archiving the data, and expring the data is required from the user, application or subsystem of the log records.
- Log records contain various types of data, including event logs, audit logs, and error logs.
- System Logger is implemented as part of the z/OS System Logger service, which is enabled by default in z/OS environments.
- It provides a flexible and scalable approach to managing log data across multiple systems.

Logger

- The Logger controls the log stream file creation and management.
- It can be configured to retain log data for a specified period or to remove it after a certain amount of time.
- Additionally, the Logger allows for customizing the log file size, retention period, and other parameters to meet specific requirements.

How System Logger is used:

- There are basically two types of users of System Logger:
  - Some exploiters use System Logger as an archival facility for log data.
    - These exploiters dump their log data into System Logger and rely on it to manage the archival and expiration of the data from there on.
  - These exploiters have the ability to subsequently retrieve the data that they need to do so, but their normal monitoring role is to just give data to System Logger and look for it back again.

Example: CICS' Forward Recovery logs, where CICS stores data away in case a forward recovery is required some time in the future. NOTE: We call these exploiters tunnel-type exploiters.

Example: The CICS DFLHLOG where CICS stores information in DFLHLOG after running transactions, and deletes them after some expiration period. NOTE: We call these types of exploiters active exploiters.

As you can imagine, the performance requirements of these exploiters will offer. The exploiters that use Logger primarily to archive data are not particularly concerned about retrieval speeds, whereas an active use of the data requires that performance be kept in a high priority.

Where System Logger stores its data: When an application passes log data to System Logger, the data can initially be stored to DASD before being moved to secondary storage, known as a DASD-only log stream, or it can be stored in a Coupling Facility (CF) in what is known as a CF-Structure log stream.

- The major differences between these two types of log stream configurations are the storage medium System Logger uses to store log data, and how many systems can use the log stream concurrently.
- In a CF log stream, interim log data is stored in a CF list structure and is available for use by the system that created the log stream, as well as any other CF systems that have the appropriate storage and bandwidth requirements.
- In a DASD-only log stream, log data is stored in a dedicated log data set available to any system in the sysplex that has access to the data set, and can be used by multiple systems concurrently.

System Logger requires that the System Managed Storage (SMS) subsystem be active on any system using System Logger.

This is true even if you do not use SMS to manage offload or staging data sets, since System Logger requires SMS to be active to allocate them.

In a DASD-only log stream, log data is stored in a dedicated log data set available to any system in the sysplex.

- The data spaces are associated with the System Logger address space, XGLOGR.
- DASD-only log streams can only be used by exploiters on one system at a time.

System Logger takes advantage of the operating system's storage management services. This component is commonly referred to as the MVS System Logger, z/OS System Logger, or simply as System Logger or just Logger. While there are enhancements that have been introduced by specific releases of the operating system, these terms are generally used interchangeably.

Remote Storage: Log data can be stored in remote storage, either through the use of networked file systems or by using remote storage services provided by the operating system.

Log Streams:

- The log stream is defined by the log stream name and the log stanza name.
- Log streams can be partitioned, with each partition representing a different type of log data, such as error logs, warning logs, or audit logs.

Interim Storage:

- Interim storage is the primary storage used to hold log data that has not yet been offloaded.
- The storage medium used depends on how the log stream has been defined; it may be a Coupling Facility (CF) structure or a staging data set.

LOGR Couple Data Set: The LOGR Couple Data Set (CDS) holds the System Logger policy information and information about all defined log streams, and must be accessible by all the systems in the sysplex.

- Log stream definitions: The log streams are defined using the MVSICMPR program, and the definitions are stored in the System Logger policy in the LOGICR.