P47 Stops S047

Many z/OS users have encountered the S047 abend (“An unauthorized program issued a restricted Supervisor Call (SVC) instruction”) that cannot be immediately explained. They generally know that their executable libraries are APF authorized. They have double checked the PROGxx member in SYSx.PARMLIB or re-issued the ‘SETPROG APF’ operator command but these failed to explain and/or resolve the abend. S047 continues, indicating that something is seriously and/or fundamentally wrong along the IPL path or with the submitted system and/or application JCL or the z/OS execution environment.

Here is a quick checklist of the Image FOCUS functions that can **pinpoint** and **report** the likely cause of the problem and FOCUS attention on a solution to S047.

Parmlib Member Errors: An Image FOCUS Inspection begins with the supplied unit address and/or volume name and LOADPARM. From this information, the LOADxx member is evaluated for a path way to IEASYSxx where the PROG=(xx,xx) and SCH=xx control directives and LNKAUTH control parameter are found. PROG and LNKAUTH determine which system and user datasets will be APF Authorized while SCH determines the content of the Program Properties Table (PPT). The PPT will contain entries that could affect and likely override a module’s authorization.

During this process, Image FOCUS will:

1. Pinpoint any changes that may occurred to all the PROG or SCH Member noting Last Update UserId, Date and Time
2. Report syntax or configuration construction errors that might cause an S047 condition to occur.

All steps and inspection findings are reported in the Image FOCUS Inspection Log. The log should be reviewed in detail to confirm that the expected LOADxx and IEASYSxx Members were evaluated.

Problems with IPL Path JCL: Armed with the information described above, Image FOCUS next begins an evaluation of the system and subsystem JCL and the start commands found in the COMMNDxx member. It first determines the authorization (AC) attribute of the program named on the EXEC PGM= JCL control card and the Authorized Program Facility (APF) status of the dataset and/or dataset concatenation defined for this related Job Step. It is well known that if a named program has the attribute of AC=01 then all JOBLIB/STEPLIB datasets must be APF authorized to prevent an S047.

If a program has the AC=00 attribute, and it has a matching PPT entry with a KEY that is a system key, then any JOBLIB/STEPLIB datasets must be APF authorized for that PPT entry to take effect, otherwise an S047 would occur.

Image FOCUS evaluates and reports system and subsystem JCL that, when executed, would result in an S047 from either of these conditions.

Problems with other JCL: Of course, there are many other possible JCL Decks that may contain problems like those defined above that also require evaluations. Within the Integrity Control Environment (ICE), these are defined to Image FOCUS on an image-by-image basis using the optional Image FOCUS COMMNDxx member. This member MUST be unique to the Image FOCUS inspection process and therefore not actually used by z/OS.

A typical Image FOCUS S047 finding: (OK, THIS IS A SAMPLE NOT THE REAL MESSAGE)

```
IFO0000E S047 CONDITION DISCOVERED IN THE JCL SHOWN ABOVE.
```

NewEra Software, Inc.

18625 Sutter Blvd., Suite 950 • Morgan Hill, CA 95037 • 800-421-5035 • 408-520-7100
www.newera.com • www.newera-info.com/Docs.html

Image FOCUS (IFO) is one of three foundational products of the Integrity Controls Environment (ICE), along with The Control Editor (TCE) and ICE/PSWD. IFO provides the capability to perform inspections of an IPL structure and determine if there are any risks, problems or points of failure within the use of the configuration datasets and members for any version of z/OS.

1. IFO inspections can be performed for an entire SYSPLEX, an individual LPAR, or a named member. These inspections can be executed online, in batch, or automatically on a preset schedule.
2. IFO can also monitor z/OS configurations to identify changes made to datasets and can provide an automated method of sending alerts when a problem or a change is detected. In addition, IFO can take backups of the configuration whenever a change is detected, creating an audit and recovery point automatically.
3. IFO also provides integrated testing and simulation functions, such as simulating a release level change, or testing planned changes through the use of a temporary or staged parmlib dataset.
4. IFO can provide a unique Recovery capability that will allow access to ISPF without the requirement of JES, VTAM or TSO.
5. IFO also provides additional change detectors that monitor other vital areas of z/OS that are not part of the IPL process directly. These detectors will monitor for changes to such things as RACF, SVC's, IODF, the OMVS system profile, and many more. Each detector will build a baseline and perform a comparison on a scheduled interval, or on demand, and will send email notifications when changes have been detected.
6. IFO can perform Subsystem Inspections by simultaneously inspecting critical systems, perform full inspections for JES 2/3, VTAM, TCP/IP, CICS, RESOLVER, TELNET, OMPROUTE, and more. The Inspectors perform the same level of analysis and will track changes in the same way that the base IFO products manages the Operating System.
7. IFO uses Supplemental Inspectors to extend the inspection process to include Load Libraries and datasets not included in the IPL process. The inspection of load modules named to the Supplemental Inspectors will identify critical problems such as orphaned aliases or duplicate modules in an operational list such as the LPALST.

For more information about NewEra Software products, send an email to support@newera.com.

NewEra Software, Inc.

18625 Sutter Blvd., Suite 950 • Morgan Hill, CA 95037 • 800-421-5035 • 408-520-7100
www.newera.com • www.newera-info.com/Docs.html