



Integrity Controls Environment (ICE) Unique Tools from NewEra Software, Inc.

GENERAL DESCRIPTION

NewEra Software provides unique products within the Integrity Controls Environment (ICE) to users of the IBM mainframe using the z/OS operating system. These products assist the z/OS professional to provide a high level of operational readiness and integrity for the z/OS SYSPLEX, LPARS and the applications that are supported on the z/OS platform.

The two major products provided with the Integrity Controls Environment are Image FOCUS, (IFO) and The Control Editor (TCE). Each has separate functional capabilities but also works in concert with each other to provide a total management solution for the added protection and availability of the z/OS system and its most critical subsystems, JES, VTAM, TCP/IP, PAGENT, and CICS.

Both products have the usual ISPF interfaces for administration and analysis but also support by a web-based application that can be used instead or in addition to the ISPF access. This web-based application is named ICEDirect and can provide additional functionality for the administration and analysis of the RACF security definitions and setting.

IMAGE FOCUS (IFO) MAJOR FUNCTIONS

IFO's primary purpose is to evaluate the readiness for an IPL or restart of a z/OS SYSPLEX and LPARS. This includes the complex structure of the configuration files needed to initialize the core operating system as well as those configuration files for the major subsystems.

This is done through several processes beginning with taking a full inventory of the elements needed to support an IPL. Then IFO continues by profiling the configuration through a complete detailed inspection of the IPL or start process by executing an IPL logically to determine if all configuration elements are properly defined. This inspection will determine if those definitions are complete and correct and if all named resources within those definitions are available. Any problem detected by the inspection will result in alert messages and notifications.

IFO provides the ability to execute this inspection on request by an authorized user, by a monitor established by the professional support

NewEra Software, Inc.

support@newera.com

www.newera.com

staff, by a BATCH job or within the IBM HEALTH CHECKER for z/OS as an additional CHECK.

In addition to the inspection evaluation results, IFO also provides a method of identifying changes made to any of the configuration elements or the environment where the configuration files are defined. This change detection will create and store backups of those elements if a change has been detected. It also provides an audit and restore record to complete the change detection services.

This change detection can be executed with prior versions of the configuration elements stored in IFO against the current version in the datasets and files. It can also be executed between the datasets and the running system values to detect dynamic changes not recorded properly within the definition element.

IFO also provides a comprehensive testing and simulation capability to allow for confirmation testing of planned changes and simulation of the effect of any changes, including upgrading to new release levels. This provides a process of verification of changes to reduce the risk of having an IPL or Start command failing or resulting in loss of time or availability of your z/OS systems and applications.

IFO. Screen 1.

```
IFO 17.0 - IMAGE      Report Index for IMAG0002      Row 1
from 136
COMMAND ==>
==> PAGE                                SCROLL

Line Commands:  S - Select  E - Edit Mode
Report  Line Commands      Report  Line Commands
INDEX    SF M  P  ME MX MQ
Report Filtering for SF, M, and P line commands:
Report Level ==> 1 (1, 2, 3, or 4) Member Display ==> Y (Y/N)
1 - All 2 - Error & Warning 3 - Error Only 4 - Final Result Only

LINE Member      Status      Description
CMD  Name        Code
..  ++ALL        ERROR      Inspection Log 17.0 P4.
..  -OPSYS       ERROR      Operating System Inspection
..  -JES2        ERROR      JES2 Subsystem Inspection
..  -JES3        OK        JES3 Subsystem Inspection
..  -HCKR        OK        Health Checker Inspection
..  -ICSF        OK        ICSF Inspection
..  -ZOSMF       NOTICE   ZO
..  -ZFS         OK        ZF
..  -VTAM        OK        VT
..  -RESOLVE     OK        RES
..  -TCPIP       OK        TCP
..  -TCPDATA     OK        TCP
```

Al,
This would have warned us
about the problem we had
with the IPL earlier this?
T H

IFO. Screen 2.

```
Image Focus - IMAGE      Report Index for IMAG0002      Row 25 from 136
COMMAND ==>                                SCROLL ==> PAGE
SORT ==> R (R - Result; M - Member; S - Sequence)
Line Commands:  S - Select  E - Edit Mode
Report  Line Commands      Report  Line Commands
INDEX    SF M  P  ME MX MQ
Report Filtering for SF, M, and P line commands:
Report Level ==> 1 (1, 2, 3, or 4) Member Display ==> Y (Y/N)

LINE Member      Status      Description      Record
CMD  Name        Code
..  COMMNDIF     ERROR      -- Data Records --      43
..  MPFLST00     WARNING   -- Data Records --      138
..  PROGCM       NOTICE   -- Data Records --      40
..  PROGLL       NOTICE   -- Data Records --      140
..  AUTOR00     OK        -- Data Records --      919
..  AXR00        OK        -- Data Records --      26
..  BPXPRMBP     OK        -- Data Records --      171
..  BPXPRMIZ     OK        -- Data Records --      17
..  BPXPRMRZ     OK        -- Data Records --      73
..  BPXPRMU1     OK        -- Data Records --      17
..  BPXPRM00     OK        -- Data Records --
..  BPXPRM01     OK        -- Data Records --
..  CEAPRM00     OK        -- Data Records --
```

Ben,
Investigate this; we do
not want another delay
of service due to an IPL
problem.

T H

THE CONTROL EDITOR (TCE) MAJOR FUNCTIONS

```
TCE SCREEN 1
NSIMCTL 0530      TCE 17.0 - Control Boundary Selection
Option ==>

D  Datasets  .. - Dataset Categories - .. Padlock On   Userid   - GBAGS2
L  LoadLibs .. - LoadLib Categories - .. Padlock On   Time     - 13:24
U  USSFiles  .. - USSFile Categories - .. Padlock On   Sysplex  - ADCDPL
C  Commands  .. - Command Categories - .. Padlock Off  System   - BDCD23C
M  Messages  .. - Message Categories - .. Padlock Off  ApplId   - IFOB
                                           ICE 17.0 - TCE 17.0
                                           Patch Level P5

+-----Global Settings-----+
| .. Padlock Control Modes .. Warn |
| .. External Notification .. Send |
| .. SysMonitor Intercepts .. On  |
| .. Command Event Logging .. Off |
+-----+-----+-----+-----+
```

Ben,
I think this will allow us to
protect ALL our critical
files and datasets beyond
what we do with RACF.
T H

TCE SCREEN 2

```
TCE 17.0 SAMPLE CUSTOM PANEL DESCRIPTOR

Your Company Name Here:  Descriptor Data Entry DDE@PNL9

Change request #       : 0987654321      Implementor: GHB
Project #              : 1234567890
Implementation date: 2022/08/01

Change details:

TEST CHANGED ON SYSTEM B
```

Al, Joan,
I really like this forced
documentation for each
event. This will satisfy the
audit finding about having
documentation for each
change.
T H

TCE provides the ability to both monitor changes and provide added levels of protection to the most critical datasets, files, and LOAD libraires. These are not only the resources needed during an IPL or start processes but can be extended to named resources deemed essential by the organization's policies and procedures.

TCE has two major roles in the overall integrity management of the z/OS LPARS and SYSPLEX.

1. TCE provides extended access rights that protect beyond what is provided by the existing External Security Manager products, RACF, ACF2 and TSS.

This protection is established at a dataset or group of datasets. This can be in the form of an additional PASSWORD required for any type of access to the dataset. Individual member access activity can be granted or denied by USERID. Notifications of any activity can be generated to notify others of the activity immediately when the action is taken.

Stricter security can be added that would require a one-time token to be generated by the ESM and delivered to the requestor, or designated other team member, to allow access. This process will improve any BREAK GLASS procedure that requires temporary access rights to be provided.

2. TCE also provides the capability to establish and enforce standards and best practices that are required for the implementation of a ZERO TRUST Architecture, or compliance with site standards.

TCE tracks changes to defined critical resources, such as PDS and PDSE datasets, that are critical to operational readiness of the z/OS LPARS and the applications. TCE can also provide the same level of protection to UNIX files, and Load Libraries and maintains it in our highly secure data recording Journals.

These journal records provide audit and recovery capabilities with backups created automatically at the point in time the change is made with an ISPF edit request, or if a change is detected, with any other method.

The datasets, UNIX files and LOAD Libraries are

defined by the user community and can include any resource deemed critical.

Optionally a process to capture and document any change event can be enforced by TCE at the point the action is taken. This documentation will be recorded along with the change record in the TCE journals. A record of ALL activity of changes to the defined resources are recorded by TCE in a Journal system.

TCE also provides limited inspection of PDS members that would be processed during an IPL while in ISPF EDIT. This inspection is like the member inspection with IFO.

SUMMARY

The Integrity Controls Environment (ICE) from NewEra Software provides capabilities not available in any other software products from any other source.

Image FOCUS provides for:

- Inspection and risk analysis of any IPL and start up configuration
- Validation in all logic including symbols, variables, parameters, etc. and impact of any changes – static & dynamic - across all defined Members, LPARS, SYSPLEX
- Change detection of the configuration elements and inspection results
- Testing and simulation functions to reduce the risk of failures or loss of service
- Optimum Operation integrity and Readiness

The Control Editor provides for:

- Extended and Improved access rights controls
- Enforcement of standards for change activity
- Backup of changes
- Enforcement of documentation requirements
- Immediate notification of events
- Audit compliance for recording changes to critical resources
- A method to creating a ZERO TRUST Architecture, or enforcement of organization standards

ICEDirect provides for an easy-to-use modern interface into the data space for both IFO and TCE as well as other applications.

