IMAGE FOCUS

The Image Control Environment (ICE)

The Image FOCUS Core

- OS Inspector
- Release Analysis
- Dynamic Element Inspector
- System Component Inspector
- z/OS Change Detection

Image FOCUS Applications

(Separately licensed)

- **JES Inspector**
  - JES2 – JES3
- **CICS Inspector**
  - SIT
- **NET Inspectors**
  - VTAM
  - TCP/IP (Profile, Data, Resolver, FTP, SMTP, Telnet)
- **The Supplemental Inspectors**
  - ISNMBRS – Data Sets
  - ISNLOAD – Load Modules
  - ISNCSDS – CSD Datasets
- **The Control Editor**
- **Image SENTRY**
  - IODF Explorer
  - UACC Explorer
  - DFHz Explorer

The Stand Alone Environment

- **SAE**
- **Fast DASD Erase**

- **Fast DASD Erase for z/OS**

NEWERA

www.newera.com

The Image Control Environment – ICE

z/OS systems staff optimize the most sophisticated computing environments for their organizations. The near-perfect uptime of these systems testifies to their expertise. Software applications such as the Image Control Environment help systems staff to examine the system and document for management, security and audit teams that their job is being done correctly. The Image Control Environment helps control four areas of z/OS systems management:

1. z/OS software (OS & Subsystems)
2. Security (RACF, CA-ACF2, CA-TSS)
3. Health (The IBM Health Checker for z/OS)
4. Hardware (IODF: IOCP/OSCP/SWCP)

It detects risks to the integrity of the system, points of failure, and changes. It documents and reports its findings.

ICE provides the platform for Image FOCUS, which is the industry standard for business continuity in z/OS data centers. It is a unique system management application that systematically identifies, locates, inspects and processes the thousands of critical parameters that define z/OS images. It supports real-time change control and management (including validating changes detected) by monitoring and reporting on events that would result in a loss of service, up to and including an IPL failure.

Image FOCUS "blueprints" the system automatically as Sysplexes and Images are tested and documented. User-defined reports are automatically sent following an Inspection.

The Image FOCUS Core consists of an Operating System Inspector, a Dynamic Element Inspector, a System Component Inspector, New Release Analysis capabilities, Blueprinting and z/OS configuration change detection.

MVS and z/OS-based systems often evolve into a complex of system Images coupled together to form a Sysplex. Such a Sysplex will often function as the organizations' back office, processing and storing critical customer and financial data. Information System customers and users often gain access to this back office data via the Internet through presentation applications housed on UNIX and/or Windows servers. The availability of each of these elements in an Information System is critical to the success of the organization and its partners, its customers, and its employees, and increasingly to comply with government regulations.

The sole purpose of ICE is to ensure, to the extent possible, the maximum availability of the Sysplex and its Images. To accomplish this, the power of Image FOCUS and its companion, the Inspection Server, are grouped into selections – Production, Workbench and Recovery. Each selection is designed to support a focused set of management activities that will enable the Image FOCUS user to quickly gain an understanding of the configuration and the integrity of any given Sysplex and/or Image(s). Such an understanding will lead directly to an improvement in overall Information System availability and integrity. Other selections include CONTROL and SENTRY, which allow users to access The Control Editor and Image SENTRY.

The Image FOCUS Inspection Server

The Image FOCUS Inspection Server is a collection of Operating System and Subsystem "Rule Sets" that were developed from available IBM documentation and real-world experiences. These "Rule Sets", which include an understanding of the configuration syntax and the IPL search order process, are used by the Image FOCUS Inspection Server to perform a "Virtual IPL" of the Sysplex, its Images and their Subsystems. One of the results we generate during the "Virtual IPL" is an Inspection Log; we call the others "Packages" and "Alerts".

Inspection Logs

The Inspection Log contains the step-by-step detail of the IPL. It begins with the validation of the IPL Unit and LOADPARM Address and it continues from there, processing each PARMLIB and PROCLIB member for syntactical correctness and related data sets for referential integrity and attribute characteristics. Sysplex relationships defined within the Sysplex parameters of an Image are crosschecked with other Images to ensure Image eligibility in the Sysplex. In final form, the Inspection Report will appear to you as a very detailed IPL Logic Map. This Map documents and validates each and every step of the "Virtual IPL" process and often will become an integral part of your system documentation. Elements which fail to validate during Inspection are flagged as Errors, Warnings or Notices. As you review your first set of Inspection Logs, you will find that, depending on certain optional settings, the logs can be quite detailed. It is common for a full Inspection Log to exceed a length of 10,000 records. Several tools are provided within Image FOCUS to help you limit the output of an Inspection Log and/or quickly navigate to points of interest.

Packages

The Package is the "Blueprint" of a valid, viable Sysplex and/or Image. It contains the content of the members and configuration files used in the IPL process. Each Image Package is automatically updated and maintained by the Image FOCUS Inspection Server during a Monitoring Interval. This continuous update process ensures you that there is a working copy of the most current configuration. These Packages are used to automatically detect configuration changes, pinpoint configuration problems and create recovery points for restoring.

Alerts

With each designated Monitor Interval, the Image FOCUS Inspection Server performs a complete check of the Sysplex and its Images. During this automated process, the Inspection Server is looking for configuration changes by comparing the current configuration to the last valid Package "Blueprint". The content of the current members and configuration files would be used to IPL the system or to evaluate potential problems. If changes or problems are detected, notification messages are sent.

It is important to note two things: first, the importance of the Package in this process and, second, that by default Packages ARE NOT updated when problems are detected. This ensures that you always have a copy of the configuration components that comprise a viable IPL.

Once you have installed Image FOCUS and logged on, you will access the **Image Control Environment – ICE**.

The Production Selection supports functions that are used to enable the interval monitoring of an Image FOCUS-managed Sysplex or Image. Once active, this critical monitoring function will call the Image FOCUS Inspection Server as scheduled to perform a Sysplex-wide validation of the current configuration components that define a running production environment. As directed by optional settings, Packages are updated and "Need to Know" notices sent.

The Workbench Selection will assist in the analysis of each Image Component by providing Operating System and Subsystem Inspection, New Release and Configuration Change Management Tools. Each of these tools will generate Inspection Logs or Change Reports that focus attention on changes to critical configuration components and/or their integrity.

The Recovery Selection gives you access to critical system resources when JES, VTAM, RACF, and/or TSO are not available. In addition, the proven NoTSO Environment and IFOR (IFO Recovery) ensure that you retain access to Image FOCUS for problem analysis, repair and recovery under these adverse conditions. The Recovery Selection also provides access to Fast DASD Erase for z/OS. It is patterned after the Fast DASD Erase Application found in NewEra Software's Stand Alone Environment (SAE). ERASE is used to erase critical data directly under z/OS.

The CONTROL Selection gives you access to The Control Editor, which extends ICE by providing users an IFO/ISPF or TSO/ISPF platform from which they both control and manage access and change to critical datasets.

The SENTRY Selection provides access to Image SENTRY, which provides users with the ability to do analysis and/or reporting using the IODF Explorer for Hardware settings and changes, and the UACC Explorer, which joins information from RACF woth Image FOCUS Trusted Reports to detect weaknesses in security settings.

The New Release Analysis tool in Image FOCUS allows users to save time and limit frustration often associated with trying to manually figure out what it will take to implement your next z/OS upgrade. New Release Analysis isolates areas in your current operating system or subsystem configuration that will need to change in order to become functional when used with a new release of z/OS.

ICE 8.0

ICE 8.0 includes enhancements to its Subsystem Inspectors. A CICS Subsystem Inspector joins ICE's JES, VTAM and TCP/IP Subsystem Inspectors. The CICS Subsystem Inspector will monitor, detect and validate changes in the CICS System Initialization File (SIT).

ICE 8.0 includes enhancements to its Supplemental Inspectors. The CSDS Supplemental Inspector (ISNCSDS) will join the other Supplemental Inspectors (ISNLOAD and ISNMBRS) and will monitor, detect and validate changes to the CICS System Definition File (CSD).

ICE 8.0 also includes a new Image SENTRY Application, the DFHz Explorer which provides a framework for auditors as well as technical users. It addresses the organization, maintenance and auditing of crucial CICS resources, focusing on Load Libraries, the External Security Manager, System Definition Dataset (CSD) Groups and Lists, System Startup JCL and related procedures, and the System Initialization Table (SIT).

ICE 8.0 includes enhancements to The Control Editor (TCE). The Control Editor allows for the tracking of changes such as edits, adds, deletes and renames to critical datasets. In ICE 8.0, the use of these datasets are also tracked by capturing the SUBMIT command when using a member of these critical datasets, creating not only a notice of use but also a copy of the JCL as it was submitted.

In addition, The Control Editor will allow the user to test the integrity of a JCL member during an edit session by allowing the user to simply enter a single command, SCAN, and receive the analysis of the JCL, in the edit session, as if it had been executed with a TYPRUN=SCAN JCL statement. This will help users save both time and CPU resources to perform these simple yet important validation tests.

All NewEra Software products are available for a free, 30-day trial.

Go to www.newera.com for more information

Corporate Headquarters
Morgan Hill, California 95037
800 421-5035
Tel. 408-201-7000
Fax: 408-201-7099
Email: info@newera.com

www.newera.com