



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
- **NET Inspectors**
 - VTAM
 - TCP/IP
(Profile, Data, Resolver, FTP, SMTP, Telnet)
- **The Supplemental Inspectors**
 - ISNMBRS – Data Sets
 - ISNLOAD – Load Modules
 - ISNPLCY – z/OS Policies
- **The Control Editor**
- **Image SENTRY**
 - IODF Explorer
 - UACC Explorer
 - ACF2 Explorer
 - TOPS Explorer
 - CICS Explorer
- **Fast DASD Erase for z/OS**

The Stand Alone Environment

- SAE
- Fast DASD Erase



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. Four areas of systems management are documented:

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

ICE 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.

The sole purpose of ICE is to ensure, to the extent possible, the maximum availability of the Sysplex and its Images. To accomplish this, ICE uses the Image FOCUS family of Inspectors and the Image SENTRY family of Explorers to support a focused set of management activities that will enable the ICE 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.

Fast DASD Erase for z/OS

Fast DASD Erase for z/OS is patterned after the Fast DASD Erase tool found in the Stand Alone Environment (SAE). It uses the same erase algorithm and performs in a similar fashion, while offering the user the opportunity to erase data under native z/OS.

Fast DASD Erase for z/OS offers a cost effective alternative to standard data erasing utilities. It totally erases all user information and produces complete audit reports in a short amount of time. Fast DASD Erase provides the most complete MVS erasure method, an important factor to consider in this era of increased scrutiny over the security of personal information. With government regulations such as Sarbanes-Oxley, HIPAA, GLBA and others, Fast DASD Erase for z/OS fulfills the data protection standards that these regulations require.

Users of Fast DASD Erase for z/OS enjoy peace of mind knowing they have completely erased all confidential data, thereby safeguarding it from unwanted use. It is also invaluable when decommissioning DASD. The Fast DASD Erase for z/OS tool not only clips the VTOC; it completely destroys all data.

Government regulations and internal procedures may call for multiple erasure passes. Fast DASD Erase for z/OS provides user-selectable erasure patterns, allowing users to write a random byte value in addition to binary zeroes across tracks during the erase process.

Once the DASD is written to binary zeros there is no residual data and even the volume labels are changed.

Here is what our users are saying about Fast DASD Erase for z/OS:

“The ease of use of this product is outstanding!”

“Erasing DASD without having to IPL SAE is going to be very useful.”

“Fast DASD Erase for z/OS helps us to stay in compliance with government regulations for erasing DASD.”

“I believe with the (flexible) VOLSER selection feature, targeting specific volumes for the different business units will legally posture our corporation in a favorable way. I will feel confident that the data on our DASD volumes will no longer be accessible once erased using this application.”

“The embedded security is a nice peace-of-mind feature, because you know that you cannot erase anything without serious intent.”

“Fast DASD Erase for z/OS helps us get a jump on clean-up at DR because we don't have to wait for z/OS shutdown to begin erasing.”

“This product is very useful for DASD management tasks, such as looking for volumes that are offline.”

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

Fast DASD Erase for z/OS

Other company, product or service names may be trademarks or service marks of others.