IMAGE FOCUS

THE SUPPLEMENTAL INSPECTORS

The Image FOCUS Control Environment

The Image FOCUS Core

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

Image FOCUS Applications

(Separately licensed)

- **The Subsystem Inspectors**
  - JES2 – JES3
  - 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

The Stand Alone Environment

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

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

Go to www.newera.com for more information.

NEWERA

www.newera.com

The Image FOCUS Control Environment

The Image FOCUS Control Environment helps control four areas of z/OS System 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.

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

The Supplemental Inspectors extend the scope of the inspection and blueprinting process to include critical system components and system settings not necessarily prevailing or critical during an IPL. They monitor the modules and objects in system libraries, the members in partitioned datasets and the installation policies that are used to control system security (RACF, ACF2 & Top Secret), the overall system health (HZSPROC) and the defined hardware configuration (IODF).

ISNMBRS – The Member Inspector is unique in that it allows for unprecedented depth in what can be inspected when validating system and IPL Integrity. Today's leading security products validate change at the dataset level and changes to members are often overlooked. ISNMBRS allows users to drill down deeper, validating changes all the way down to the member level.

ISNLOAD – The Load Module Inspector inspects and reports on changes to load libraries, the module/objects they contain and their CSECTs. Typically, there are 40,000 z/OS system modules in an APF Authorization cycle. Generally, they are defined in LPALST and LNKLST concatenations and/ or mandated in vendor and/or user application program load libraries. They, in turn, are named to be APF Authorized in a specific prevailing PROGxx ParmLib member.

ISNPLCY – The Policy Inspector provides the transparency required in installations that are being held to higher standards. It inspects and reports on the health and security of the system and its hardware definitions.

Health (The IBM Health Checker for z/OS)

Health reports provide the documentation of the general health of the system and the systematic identification of changes to that documentation are critical z/OS Policy Considerations. If managed adequately, IBM Health Checker for z/OS documentation maintenance and the reconciliation of reported HZSPROC changes can help improve perceived and/or the actual integrity of a z/OS environment.

1. Exploit Image FOCUS HZS specific REXX Services;
2. Blueprint Check Status and compare Blueprints for Change;
3. Normalize Check Exceptions into Image FOCUS Message Formats;
4. Incorporate its Check Inspection Report into the Image FOCUS Report flow;
5. Send Emails with Check Exception/Change Alerts.

Hardware (IODF: IOCP/OSCP/SWCP)

The reliability of Input Output Definition File (IODF) documentation and the systematic identification of changes to that documentation are critical z/OS Policy considerations. If managed adequately, IODF documentation maintenance and the reconciliation of reported IODF changes can help improve perceived and/ or the actual integrity of a z/OS environment.

Image FOCUS:

1. Uses the Policy Inspector to process datasets containing IOCP, OSCP and Switch Configuration Macro Statements;
2. Uses Image FOCUS Auto Discovery to find and report on the specific location of a Named Image's Input Output Definition File (IODF);
3. Uses the Policy Inspector to extract definitions from the IODF, blueprint them, detect changes in them and report/notify as directed.

Security (RACF, CA-ACF2, CA-TSS)

The documentation of site/system Dataset Security and the systematic identification of changes to that documentation are critical z/OS Policy Considerations. Security documentation maintenance and the reconciliation of reported profile and application changes can help improve perceived and/or the actual integrity of a z/OS environment if managed adequately.

Image FOCUS uses the Policy Inspector to process the dataset's source list containing targets of security interest. It will blueprint the list, allowing comparisons to be made from current to prior and/or current to baseline/ benchmark.

When used in conjunction with The Control Editor, your installation will achieve a new level of security for the management of changes.

Corporate Headquarters
Morgan Hill, California 95037
800 421-5035
TEL: 408-201-7000
FAX: 408-201-7099
email: info@newera.com