Defending System z Configuration Control Boundaries

Achieving **Role Based Access Control** with **The Control Editor** (TCE/RBAC)

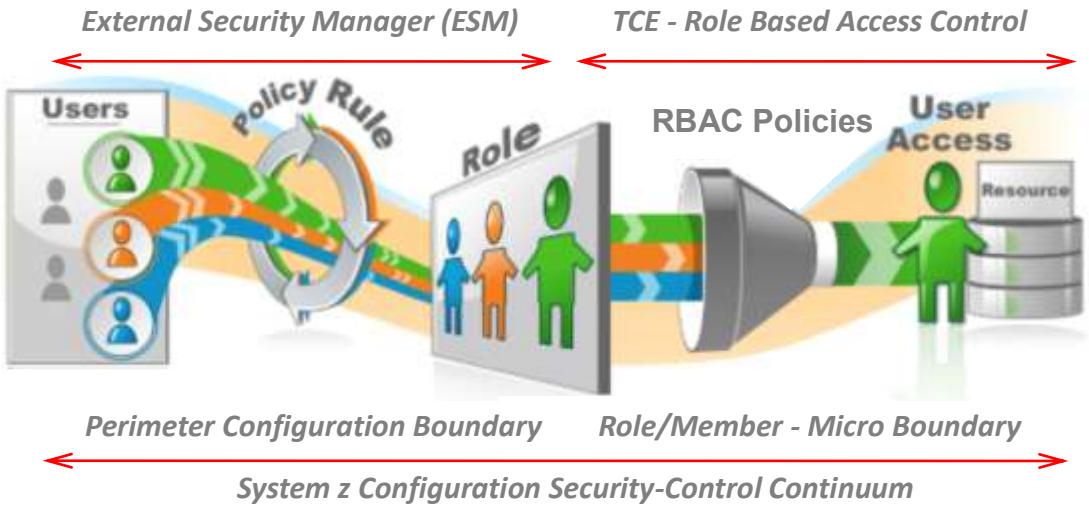
A NewEra Software White Paper

NewEra Software, Inc.
155 East Main Avenue
Suite 130
Morgan Hill, CA 95037
800-421-5035
www.newera-info.com/New.html

Role Based Access Control (RBAC)

Role Based Access Control (RBAC) is a Management Technique in which roles are defined for various job functions. The permissions to perform certain system operations are assigned to one or more of these roles. Technical Support Staff (or other system users) are then assigned to those roles that best fit the scope of their support responsibilities.

When RBAC is employed, users are not assigned access rights/permissions directly, but only acquire them through their role (or roles). Management of individual user rights becomes a matter of simply assigning individual users to appropriate roles, thus simplifying common operations such as adding or deleting users, or changing the operational scope of an existing Role.



When applied within the System z Environment, RBAC can be seen as reinforcing the Configuration Control Boundaries maintained by the Policy Rules defined to and enforced by the External Security Manager (ESM). Used in this way, RBAC establishes and enforces 'Fine-Grained, Micro-Perimeter' controls around critical System z Configuration Resources – IPLParm, ParmLib, ProcLib - and as a result, enhances and extends the System z Configuration Security-Control Continuum.

RBAC is an acceptable response to Audit Findings that question existing Managerial Control Processes that appear to convey excessive access privileges to users, thus weakening existing ESM Policy Rules. In many cases, ESM Policy Rules provide access to system resources that ARE NOT actually required by Technical Support Staff in the normal course of them performing their assigned duties. RBAC resolves this dilemma by enforcing a second set of Access Policies that are specifically designed and deployed to ensure that resource access is provided only to those who actually require it.

Within the Image Control Environment (ICE), RBAC is - Defined, Assigned, Enforced - using functions found within The Control Editor (TCE). But TCE is much more than a Control Tool. The TCE Development Team creates a balance between reinforcing legacy security and enhancing staff productivity in the enterprise-wide System z Environment.

Reinforcing Legacy Security

The examples listed below raise questions concerning the responsibility and accountability between colleagues and consultants supporting the System z environment and speak to the need for enhanced configuration control; control that focuses on an individual's Role within the Technical Support Organization.

Consider the following:

- Do "READ" only users access, alter/submit and cancel out without documentation?
- Do outside consultants need view/update access to every configuration component?
- Do Application Programmers need access to everything in a shared configuration?
- Do ESM policies enforce accountability when Parmlib is shared across functions?
- Do controls over APF Authorization allow for the assignment of responsibility?
- Do access rights to network configurations invite mainframe intrusions?

These represent but a few examples of issues that may be inching your organization ever closer to a state of non-compliance when actual control over System z changes is brought into question. They speak to a need for the collection and reporting of configuration event detail beyond that supported by Legacy Security Systems, the System Management Facility (SMF) and conventional Change Management Processes.

Enhancing Staff Productivity

Configuration Access Control is first of two TCE goals. The second is to improve Staff Productivity through a product design that 'leads them' toward the achievement of System z Support Best Practices. These practices include:

- Taking a *Backup* before making changes to a system configuration component.
- *Testing* changes to configuration components before committing them to production.
- Researching the *History* of prior changes before attempting new ones.
- Documenting *Actual* changes at the point where the changes actually take place.
- *Notifying* those that need to know that a change has been made.

These sound System Support ***Best Practices*** are straightforward and simple enough. However, we're all human, we're all busy, and we all forget. Our best intentions to conform to these practices sometimes go unfulfilled. TCE can ensure that these practices are achieved, automatically guiding its users, without interruption of normal workflow - "no ifs, ands, or buts". In doing so changes are fully documented, system configuration integrity is enhanced, and when necessary, regulatory requirements can be satisfied.

For more information on TCE/RBAC:

Visit	www.newera-info.com/New.html
Call	800-421-5035 or 408-520-7100
Email	support@newera.com