WebSphere. software

IBM Enhanced Access Control for Software Configuration and Library Manager (SCLM) for z/OS™

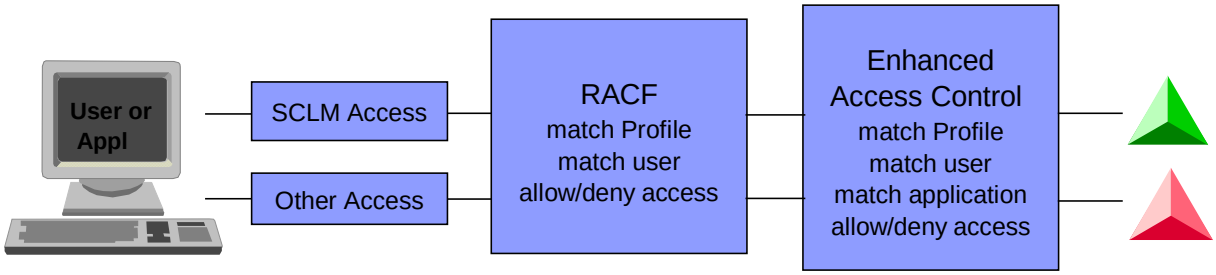
Highlights

- ***Improves granularity and protection for SCLM managed data***
- ***Provides the ability to specify which programs can be used to access SCLM data***
- ***Allows users to be authorized only to specific functions (Edit, Build, Promote…)***
- ***Reports access violations***
- ***Provides an easy to use, menu driven end-user interface***
- ***Improved access control is based on IBM RACF®***

IBM Enhanced Access Control for Software Configuration Library Manager (SCLM) for z/OS is a new addition to the SCLM Suite. Security interfaces and user exit points within Enhanced Access Control for SCLM provide improved granularity and protection for SCLM data sets so that authorized modifications can be made only by a native SCLM user. Enhanced Access Control for SCLM will allow the addition of new rules that specify exactly which programs can be used to access which data sets, thereby adding the flexibility beyond that found in IBM Resource Access Control Facility (RACF) to define specific users read or write access to specific documents. Validation profiles, accessing programs, and user or user group privileges can be defined through a menu driven end-user interface. The Enhanced Access Control for SCLM product provides an easy to use, CUA® compliant, menu driven end-user interface to maintain the security rules needed for this support.

IBM's Enhanced Access Control for SCLM augments RACF controls. After normal RACF security controls are applied, Enhanced Access Control for SCLM can be used to grant access when a specific set of applications like SCLM are used. The Applications can even define various sub functions of SCLM, such that, for example, an SCLM Promote may be allowed access whereas an SCLM Edit may be denied access.

Without Enhanced Access Control for SCLM, SCLM users operating in a RACF environment must be granted UPDATE access to manipulate SCLM managed data sets. Otherwise, they would receive RACF data set violations when performing various SCLM functions. However, the UPDATE access applies even if the data set is accessed using facilities other than SCLM, thus allowing access to potential users from facilities other than SCLM.



e business

The central concept of Enhanced Access Control for SCLM is that access to SCLM resources is provided when SCLM programs are used. This avoids the potential for accidental damage or unexpected changes to SCLM data sets resulting from updates using non-SCLM programs. The SCLM programs are described using Applications. The data sets to be controlled and their access rules are described using Profiles.

When Enhanced Access Control for SCLM is active, it monitors RACF data set violations. If a violation occurs for a data set managed according to the Enhanced Access Control for SCLM profiles, then the defined access rules are used to assign access privileges. If sufficient access privilege is not defined, then a RACF data set violation occurs.

Like RACF, Enhanced Access Control for SCLM has its own rules database that describes the conditions under which access is granted. These are contained in the Rule File, a VSAM KSDS that is administered via the ISPF Dialog. From these on-line panels, the Enhanced Access Control for SCLM administrator can:

- define the data sets or generic RACF data set Profiles to be controlled
- define SCLM and its sub functions as Applications
- define the users granted access privileges to a Profile via an Application
- view violation records collected by Enhanced Access Control for SCLM.

Features

- Granular access controls
- Authorization flexibility and efficiency
- Attractively priced
- Fully functional and centralized S/390 Software Change and Configuration Management (SCM) solution

Benefits

- Allows continued use of OS/390 or z/OS application development environments while ensuring top-of-the-line security is maintained
- Improves the protection of SCLM-managed application development environments
- Adds flexibility beyond the access controls found in IBM Resource Access Control Facility (RACF)

Summary

IBM Enhanced Access Control for z/OS is a new addition to the SCLM Suite which augments RACF controls. It provides efficiency and flexibility of authorization though the implementation of granular access controls in order to improve the protection of SCLM-managed application environments.

System Requirements:

Hardware

IBM mainframe, or compatible system, capable of running OS/390™ or z/OS™

Software

- IBM OS/390 V2R10, or later (5647-A01)
- IBM z/OS V1, or later (5694-A01)
- IBM Resource Access Control Facility (RACF)

For More Information

Contact your IBM representative or IBM Business Partner or visit the Enhanced Access Control for SCLM web site at: http://www-3.ibm.com/software/awdtools/sclmsuite/accesscontrol/.

When ordering the IBM Enhanced Access Control for SCLM for z/OS, specify program number 5697-H59.

Services Available

While services are often considered discretionary or optional in many other parts of an IT shop, IBM's services are a key factor for the successful implementation of the SCLM Suite.

Whether our Quick Start offering is chosen or Full Customization is preferred, IBM's Services will pave the way to being able to deliver on your own service commitments.

Quick Start
Base Services
Customized Services

IBM United States
Silicon Valley Laboratory
555 Bailey Avenue
San Jose, CA 95141

Printed in United States of America
03-2003