CA Auditor for z/OS

At a Glance

CA Auditor for z/OS (CA Auditor) is a powerful mainframe tool architected to help you achieve and maintain compliance with the myriad regulatory requirements that govern your business and IT systems. It enables you to perform an automated technical review of the system, hardware and software environment and to identify integrity exposures in z/OS®. CA Auditor is designed to help you simplify auditing activities and eliminate manual processes so that users without in-depth experience can perform an extensive operating system review.

Key Benefits/Results

- **Simplifies management.** Robust auditing, integrity check and verification capabilities

- **Improves operational efficiency.** Greater visibility and insight into systems

- **Reduces time-consuming tasks.** Provides auditing and customizable system functions

- **Reduces learning curve.** Comprehensive tutorial and support materials

Key Features

- **Gathers and displays system hardware and software information.** Capability to perform a high-level look at the computer system.

- **Monitors operator consoles.** Displays the active and inactive consoles defined to the system, system ID and Sysplex ID of the console, as well as other vital information.

- **Analyzes system customization variables.** Details the options used to customize the operating system.

- **Reviews executables.** Enables you to minimize this task and provide accurate information.

- **Inspects programs.** Ability to inspect programs and monitor their use.

- **Monitors file usage.** Provides the capability to monitor usage and ensure the integrity of your files.

Business Challenges

With each new generation of mainframes, operating systems become more complex, and auditing processes grow in difficulty. Any operating system can experience security exposures as a result of errors in installation, customization, bugs or maintenance. The efficiency of every environment depends on such factors as the type of mainframe used, the hardware configuration and the types of software. However, gathering the information that helps ensure the integrity of the libraries and functions controlling operating system functions is a time-consuming—and therefore expensive—task.

Solution Overview

CA Auditor helps identify the system, application and security exposures in z/OS environments that arise from improper system configuration and operational errors as well as intentional circumvention of controls and malicious attacks. As a part of an overall program of compliance, security and software management, CA Auditor can help you ensure the integrity of your base operating system and application processing environments. As such, it helps you establish and maintain the platform operating system integrity to meet such compliance regulations and your business auditing requirements.

CA Auditor addresses a significant exposure point in the z/OS operating system by providing you with comprehensive auditing, integrity check and verification capabilities. The product helps you perform these tasks through capabilities that gather and display system hardware and software information, analyze system customization variables, review executables, inspect programs, monitor file usage, make suggestions, answer questions and more.

Critical Differentiators

CA Auditor provides the capability to perform a high-level review of your system. The System Hardware Overview provides information about the CPU, its serial number, the date and time of the last IPL and the version of the operating system. CA Auditor also monitors hardware errors, delivering reports that aid in monitoring and summarizing error rates from tape drivers and disk drives.

To ensure that the proper events are being recorded, CA Auditor provides information about the current System Management Facility (SMF) options in use and SMF files, identifies SMF exits and displays selected SMF records in an easy-to-read format. In addition, CA Auditor displays the active and inactive consoles defined to the system, Sysplex ID and system ID of the console, as well as other vital information.

The Program Information option in CA Auditor provides details and statistics about the origins of programs in use. You can also compare two source modules, compare two load modules, freeze programs for later comparison and locate load modules with no source code. These functions are useful not only for operating system-provided programs and libraries, but also for application programs and libraries.

Release 12.0 Key Features:

Comprehensive compliance, security and software management. Comprehensive tool that enables you to perform an automated technical review of the system, hardware and software environment, and identify integrity exposures in z/OS.

Extended capabilities for baseline analysis. A baseline audit is a standard auditing principle by which a known, audited configuration (baseline) is established, and all future audits of that configuration are made against the saved results.

Analysis of customization variables. Details the options used to customize the operating system

System and hardware overviews. Provides the capability to perform a high level look at the computer system.

Monitors file usage. The integrity of your files is important because they contain all the data stored on your system and often reflect erroneous information. CA Auditor provides the capability to monitor and ensure the integrity of these files.

Online help and tutorial. The complexity of the operating system has increased to such a degree that it is often difficult to know what information is needed to complete a comprehensive review. CA Auditor addresses this challenge by providing online help and tutorials.

For more information, please visit **ca.com/mainframe-security**