DATA SHEET

CA Cleanup for z/OS

At a Glance

CA Cleanup for z/OS (CA Cleanup) reduces the effort and pressure associated with maintaining current regulatory, statutory and audit requirements. It does this by removing obsolete, unused, redundant and excessive access rights through easily automated, virtually unattended and continuous cleanup of mainframe security databases CA ACF2™, CA Top Secret® and IBM RACF®.

Key Benefits/Results

- Improve security control.
- Manage administration costs.
- Increase risk mitigation.
- Enhance privacy control.
- Improve ease of audit.
- Increase system performance.

Key Features

- **Continuous 24x7 monitoring.** Executes continuously, monitoring your security system activity to record the actual security definitions that the system is or is not using.
- **Enhanced security recertification.** Monitors security activity and can identify used and unused access for any user or application.
- **System and administrative overhead reduction.** Removes unused access rights and IDs from the security system, improving performance and productivity.
- **Report generator.** Provides a batch utility program to produce reports for specific purposes.
- **Command generation to perform or restore cleanup.** Removes obsolete IDs or access and creates commands to restore what was removed.
- **Built-in contingency and back out.** Creates the commands to enact cleanup as it recreates the original ID or access.

Business Challenges

Information security and personal information privacy are at the core of many federal regulations and consumer privacy requirements. Organizations face potentially significant security exposures when unused and obsolete user IDs—and entitlement definitions that may be valid, but are inappropriate for individuals' roles—accumulate in mainframe security databases. This build-up also hampers operating and security system performance, administrator productivity and audit effectiveness.

System process IDs such as vendors, partners, contractors/consultants that are used for batch jobs, started tasks, CICS, terminal, FTP and others are rarely cleaned up. These IDs often pose the greatest threat because they can be highly authorized, privileged with bypass security options, require no password and are commonly known (for example, IBMUSER, OMVS, JES and others). While this area is often judged as too sensitive and difficult for manual cleanup, these IDs pose no challenge for CA Cleanup and require no special handling.

Solution Overview

CA Cleanup automates two labor-intensive tasks that plague security administrators: creating security commands to remove obsolete IDs or access and creating commands to restore what was removed. When using CA Cleanup, you can easily identify active and inactive user IDs, profiles and permissions, as well as user-defined resource classes. It will detect and remove sensitive IDs with an option to initially suspend. By generating contingency commands for everything flagged for deletion, IDs that may need to be restored can be recreated on demand.

When the standard monitoring report is executed from the tracking file, the commands can automatically be produced, but you choose when to execute the cleanup—and what is actually cleaned up.

CA Cleanup also helps you comply with many regulations and laws requiring due diligence to information security, protection and privacy.

Critical Differentiators

- **Efficient cleanup.** CA Cleanup helps you identify active and inactive logon IDs, rule sets and rules, including user-defined resource classes and NEXTKEY source and target rules. When the standard monitoring report is executed from the tracking file, the commands can be automatically produced. It remains your choice as to when cleanup occurs and what is actually cleaned up.
- **Remote synchronized environment.** It supports the processing of multiple concurrent databases to maintain synchronization.
- **Multiple remote security database capability.** It performs a correlation and produces a collective composite report based on usage across all of your security databases. This means that a user ID or user access right in one location will not be targeted for cleanup unless it is unused across all locations.
- **Role-based reorganization and process support.** It can reorganize and restructure your security file to a role-based structure, identifying both obsolete and active access rights. Active rights can be moved to newer, smaller, reorganized rule sets or groups that match your role-based structure. You can continue to monitor these user IDs and the access rights to help ensure proper setup.

Related Products/Solutions

- **CA Chorus™ for Security and Compliance Management.** Reduce the time and effort required to more securely manage the mainframe environment and enable faster issue resolution.
- **CA Cleanup for z/OS.** Easily automate continuous and unattended security file cleanup.
- **CA Auditor for z/OS.** Help identify and control z/OS security exposures.
- **CA ACF2 Option for DB2 for z/OS.** Provides protection against unauthorized destruction, disclosure, or modification of DB2 data and protects DB2 resources by default using standard ACF2 syntax.

Supported Environments

- **z/OS**
- **CA ACF2**
- **CA Top Secret**
- **IBM RACF**

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

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200-94776-1014