A Broadcom Company
technologies

Product Brief

CA Cleanup for z/OS

Key Benefits

- Automate and streamline compliance processes.
- Monitor security activity and quickly gain insight into active or inactive IDs and entitlements.
- Remove obsolete IDs and entitlements.
- Remove entitlements to align with the principle of least privileged access.

Key Features

- **Continuous 24x7 monitoring:** Executes continuously to monitor your security system activity and 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 rollback:** Creates the commands to enact cleanup as it recreates the original ID or access.
- **Security Technical Implementation Guide (STIGs) articles for CA Cleanup:** Reduces the security risk of configuration-based vulnerabilities using step-by-step guidance to remediate potential security exposures.

At a Glance

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

Business Challenges

Digital transformation made every business a software-first digital enterprise. The mainframe continues to play a critical role in supporting increased workloads with the highest performance and availability. 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 (the definitions 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 and consultants 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

The Broadcom® mainframe cybersecurity portfolio helps you advance your mainframe security with identity and access management plus compliance and data protection solutions to minimize risk in today's hybrid IT environment. Broadcom offers advanced security tools and best practices that cover the entire security lifecycle. CA Cleanup can help you maintain your security database and meet regulatory and audit requirements.

CA Cleanup automates labor-intensive tasks that plague security administrators:

- Identifying items that can be deleted
- Creating security commands to remove obsolete IDs or access
- Creating commands to restore what was removed

Related Products

CA ACF2 Option for DB2: Externalizes security for IBM DB2 without the need for an exit.

CA Top Secret Option for DB2: Simplifies the complex process of managing access to critical DB2 resources, privileges, and utilities. It also provides consistent security and logging, and easy auditing and reporting.

CA Trusted Access Manager for Z: Monitor and control privileged users by granting time-bounded just-in- time access to the system, critical resources and regulated data, or resources with 1:1 accountability and auditing.

CA Advanced Authentication for Mainframe: True multi-factor authentication for mainframe users. Supports RSA hard and soft tokens, and radius protocol.

CA Compliance Event Manager: A single source for the collection and monitoring of real-time, compliance-related information and events that occur within the mainframe environment. It has the ability to send information to Splunk or to an enterprise SIEM solution.

CA Auditor (formerly CA-Examine Auditing): In-depth auditing, integrity checks, and verification for z/OS.

CA Data Content Discovery: Find and classify regulated and sensitive data to ensure that proper security and privacy controls are in place for the data.

Solution Overview (con't)

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 cleanup 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 for information security, protection, and privacy.

Why CA Cleanup?

- **Efficient cleanup:** CA Cleanup helps you identify active and inactive logon IDs, entitlements, and generate commands to perform cleanup.
- **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 that is correct in one location is not 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.

Supported Environments

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

Next Steps

- To learn about CA Cleanup, see: CA Cleanup
- To learn more, see: mainframe.broadcom.com/security
- Try the Broadcom free Security Assessment, visit: Security Essentials

A Broadcom Company
technologies

For product information and a complete list of distributors, visit our website at: broadcom.com

Cleanup-zos-PB101 December 16, 2020