CA Auditor for z/OS

Best Practices Guide

r12

technologies

CA Technologies Product References

This document references the following CA Technologies products:

- CA 7® Workload Automation
- CA Auditor for z/OS (CA Auditor)
- CA ACF2™ for z/OS (CA ACF2)
- CA Endevor® Software Change Manager (CA Endevor SCM)
- CA Mainframe Software Manager (CA MSM)
- CA Scheduler® Job Management (CA Scheduler JM)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA Technologies product documentation, complete our short customer survey, which is available on the CA Support website at http://ca.com/docs.

Best Practices Guide Process

These best practices represent years of product experience, much of which is based on customer experience reported through interviews with development, technical support, and technical services. Therefore, many of these best practices are truly a collaborative effort stemming from customer feedback.

To continue and build on this process, we encourage users to share common themes of product use that might benefit other users. Please consider sharing your best practices with us.

To share your best practices, contact us at techpubs@ca.com and preface your email subject line with "Best Practices for *product name*" so that we can easily identify and categorize them.

Contents

Chapter 1: Introduction

This section contains the following topics:

Purpose

The guide provides a brief introduction to CA's Mainframe 2.0 strategy and features, and describes the best practices for installing, configuring, and maintaining CA Auditor.

CA Auditor is a critical element in your installation's ability to help address compliance related laws, regulations, and other mandated controls. CA Auditor helps you verify z/OS system integrity, which is one of the foundational elements of any mainframe IT processing platform.

Audience

We created this guide for systems programmers and administrators who install, configure, deploy, and maintain the product, and for the security administrators, auditors, and compliance officers who use the product.

We designed CA Auditor specifically for auditors and compliance professionals to simplify and automate auditing complex mainframe z/OS environments and the applications that run under it.

Documentation Set Overview

This list offers a basic description of each guide in the CA Auditor documentation set:

Installation Guide

Details the steps to install CA Auditor.

Release Notes

Describes the features available in the latest release of CA Auditor.

System Review Checklist

Contains checklists to help you perform a state-of-the-art analysis of the z/OS system software environment using CA Auditor.

Technical Reference

Includes reference material to help you manage CA Auditor.

Usage Guide

Provides instructional information for data processing professionals who use CA Auditor to review the security, integrity, and control of the z/OS system.

Mainframe 2.0 Overview

Mainframe 2.0 is our strategy for providing leadership in the mainframe operating environment. We intend to lead the mainframe marketplace for customer experience, Out-Tasking solutions, and solution innovation. After listening to customer needs and requirements to keep the mainframe operating environment viable and cost-effective, we are providing new tools to simplify usage and to energize this operating environment for years to come.

CA Mainframe Software Manager™ (CA MSM) is an important step in realizing the Mainframe 2.0 strategy. CA MSM simplifies and standardizes the delivery, installation, and maintenance of mainframe products on z/OS systems. CA MSM has a browser-based user interface (UI) with a modern look and feel for managing those solutions. As products adopt Mainframe 2.0 features and CA MSM services, you can acquire, install, and manage your software in a common way.

CA MSM provides software acquisition and installation that make it easier for you to obtain and install CA mainframe products, and apply the recommended maintenance. The services within CA MSM enable you to manage your software easily based on industry accepted best practices. The common browser-based UI makes the look and feel of the environment friendly and familiar.

We follow the IBM z/OS packaging standards using SMP/E, with some additional CA qualities of service added, to make installation simple and consistent. Additionally, through the synchronization of product releases and the use of common test environments, we will declare a yearly mainframe software stack that includes many new releases with enhanced functionality. This stack is certified for interoperability across the CA mainframe product portfolio and the base IBM z/OS product stack.

Mainframe 2.0 Features

Mainframe 2.0 has the following main features:

CA Mainframe Software Manager (CA MSM)

Delivers simplified acquisition, installation, and deployment capabilities using a common z/OS-based web application delivered through a browser-based UI. CA MSM includes the following services:

Product Acquisition Service (PAS)

Facilitates the acquisition of our mainframe products and services, including product base installation packages and program temporary fixes (PTFs). This service integrates the inventory of products available on your system with CA Support, providing a seamless environment for managing and downloading software and fixes onto your system.

Software Installation Service (SIS)

Facilitates the installation and maintenance of our mainframe products in the software inventory of the driving system. This service enables you to browse and manage the software inventory using a web interface, and automates tasks for products that use SMP/E to manage installation. You can browse downloaded software packages, and browse and manage one or more consolidated software inventories (CSIs) on the driving system.

Software Deployment Service (SDS)

Facilitates the deployment of CA Technologies mainframe products from the software inventory of the driving system. This service enables you to deploy installed products that are policy driven with a set of appropriate transport mechanisms across a known topology. The enterprise system topology can include shared DASD environments, networked environments, and z/OS systems. Policies represent a combination of metadata input that identifies the component parts of a product and user-supplied input that identifies the deployment criteria, such as where it will go and what it will be called.

Electronic Software Delivery (ESD)

Enables you to get our products from an FTP server. We have improved this process so that you no longer need to build a tape to install the product.

Best Practices Management

Integrates with IBM Health Checker for z/OS to verify that deployed software follows our best practices. The health checks continually monitor the system and software to provide feedback on whether the software continues to be configured optimally.

Best Practices Guide

Provides best practices for product installation and configuration.

Note: For additional information about the CA Mainframe 2.0 initiative, see http://ca.com//mainframe2.

Chapter 2: Installation Best Practices

CA Mainframe Software Manager

We recommend that you use CA MSM to acquire, install, and maintain your product.

Business Value:

CA MSM provides a web interface, which works with Electronic Software Delivery (ESD) and standardized installation, to provide a common way to manage CA mainframe products. You can use it to download and install this product.

CA MSM lets you download product and maintenance releases over the Internet directly to your system from http://ca.com/support. After you use CA MSM to download your product or maintenance, you use the same interface to install the downloaded software packages using SMP/E.

Additional Considerations:

After you install the product, use the product documentation set at http://ca.com/support to configure your product. CA MSM can continue to help you maintain your product.

More Information:

For more information about CA MSM, see the *CA Mainframe Software Manager* guide at http://ca.com/support.

Note: If you are using external and internal travel tapes, you can continue to follow the installation process for these tapes.

Chapter 3: Configuration Best Practices

This section contains the following topics:

System Review Checklist

We recommend that you use the *System Review Checklist*.

Business Value:

The *System Review Checklist* is a CA Auditor document that describes all of the steps to complete a full audit. Each CA Auditor function also includes, as part of its online help, checklist items pertaining to that function.

This checklist is a proven method of auditing a z/OS system. We developed this tool for auditing and compliance professionals of all skill and experience levels with the z/OS system.

Using the *System Review Checklist* with CA Auditor helps maintain a desirable level of segregation of duties (SOD) that is consistent with generally accepted auditing principles. Many clients engage their technical support staff to conduct z/OS system audits, which is an SOD violation because the technical support staff cannot audit their own work.

The *System Review Checklist* not only identifies the required auditing steps, it also explains the significance of each line item from an auditing and risk point of view, which helps manage expectations, define auditing requirements, and interpret CA Auditor results.

More Information:

To review this checklist, see the Checklist section in the online help under each CA Auditor function.

Expediting Audits Using Online Help

We recommend that all CA Auditor clients use the online help as a primary information source.

Business Value:

All CA product online help offers useful information, but the CA Auditor online help is especially useful for auditors who often need information immediately. By using this tool, auditors can expedite the audit process by quickly finding answers to their questions without the need to confer with technical support personnel. CA Auditor provides comprehensive online help. We designed the online help to promote auditor independence, thereby facilitating a segregation of duties (SOD).

Additional Considerations:

The online help provides consistent information and guidance across the full range of CA Auditor functions by explaining:

- What the CA Auditor function does
- Why the CA Auditor function is significant from a security and integrity perspective
- How to use the CA Auditor function and understand its results
- Checklist items pertinent to this function
- Pertinent primary and line commands pertinent to this function

More Information:

To access online help, press the HELP key within any CA Auditor function. In typical mainframe environments, the help function maps to the PF1 key.

Baseline Analysis to Detect Configuration Changes

We recommend that you use the baseline analysis feature to monitor select z/OS configuration controls and detect specific changes.

Business Value:

You can use the baseline analysis feature on a subset of CA Auditor analysis functions to detect if a change to a configuration element occurred and to report on the specific change. This practice is especially useful when you are verifying internal change control procedures.

Additional Considerations:

Examples of CA Auditor functions that can employ baseline analysis include:

- APF list analysis
- Key library analysis
- Parmlib analysis
- System overview analysis
- SMF exit analysis

Most of these elements are based on z/OS configuration controls that have their foundation in parmlib members selected at IPL. However, because most of these elements can be modified dynamically using z/OS interfaces, z/OS commands, and OEM/ISV product capabilities post-IPL, you must monitor these key configuration elements while the system is up.

You can use the CA Auditor freezer with the baseline analysis function. For example, you can use baseline analysis to monitor the contents of the various configuration lists, and you can then use the freezer to monitor the contents of each library within the list.

More Information:

To use the baseline analysis feature, see the *Technical Reference* guide.

Detecting Changes with CA Auditor Freezer

We recommend that you use the CA Auditor freezer to detect changes to source libraries, executable libraries, configuration libraries, and memory-resident programs, such as LPA modules.

Business Value:

The CA Auditor freezer offers a high-performance, low-risk, and low-impact means to detect critical system component changes. This practice helps satisfy general compliance-related requirements mandated by Sarbanes-Oxley (SOX), the Payment Card Industry-Data Security Standard (PCI-DSS), other compliance requirement and regulations, as well as generally accepted auditing principles.

Additional Considerations:

To understand the role of the CA Auditor freezer, consider an auditor's typical process. An auditor begins an object audit by examining current data, ascertaining adequacy of controls, and establishing a baseline view. This view becomes the standard against which auditors check for changes. The auditor then periodically compares the present state to the baseline data.

Finding a difference does not necessarily indicate a problem; however, if upon investigation, an auditor determines that users did not follow change control procedures, the auditor must address why.

You can use the CA Auditor freezer with the baseline analysis function. For example, you can use baseline analysis to monitor the contents of the various configuration lists, and you can then use the freezer to monitor the contents of each library within the list.

More Information:

For detailed CA Auditor freezer information, see the *Usage Guide* and the *Technical Reference* guide.

Processing Multi-Line CA Auditor Displays

We recommend that you use the SORT command to more effectively use large volumes of audit information that CA Auditor returns through multi-line table displays. We also recommend that you use the LOCATE command to quickly navigate to specific entries that you want to review.

Business Value:

CA Auditor returns complex multi-line audit findings in a default order that depends on the function being executed. Some functions produce modest findings, and you can hand-navigate through them using Up and Down keys. Other functions can produce tens of thousands of lines, making hand navigation ineffective.

The SORT command can reorder the list of entries per the auditor's direction. The LOCATE command can locate a specific entry, such as a specific SVC number, data set, or subsystem name.

Additional Considerations:

Use the LOCATE command to locate a specific data set name.

Use the SORT command to locate a grouping of related entities, for example, APF data sets that are granted authorization by virtue of being included in the system linklist when the IEASYS*xx* member specifies LNKAUTH=LINKLIST. You might also use the SORT command within the USER SVC display to quickly navigate to active SVC entries.

The applicable sort fields on each display correspond to the column headings. Issue the following command to determine the specific column names:

```
SORT ?
```

By default, the target of the LOCATE command is the first column in the display. The SORT command changes the key field against which CA Auditor performs the Locate.

More Information:

To manage description fields, see the *Technical Reference* guide and the *Usage Guide*.

Batch CA Auditor Interface

We recommend that you use the CA Auditor batch interface to simplify and automate routine audit processing. The CA Auditor batch interface is also known as the *Silent Auditor*.

Business Value:

The CA Auditor batch interface provides an easy-to-use mechanism whereby you can capture CA Auditor functions as batch audit scripts and subsequently execute them in a batch job environment on a repeatable, as-needed basis. Using the batch interface saves time and streamlines the cost of performing repetitive auditing functions.

Using the batch interface lets you establish constant auditing that monitors critical system configuration elements. This proof of constant auditing and compliance oversight can help satisfy compliance requirements.

Additional Considerations:

For example, when setting up a full audit regimen using CA Auditor, the results may list different tasks to be executed at different time intervals with each task corresponding to a different batch audit script. When used with automated job scheduling solutions, such as CA 7 Workload Automation or CA Scheduler Workload Automation, each individual batch audit script can run automatically at the desired intervals.

More Information:

For detailed information, see the *Usage Guide* and the *Technical Reference* guide.

Using the CA Auditor CAIPVI Interface

We recommend that you use the CA Auditor CA Product Validation Interface (CAIPVI) to streamline identification of the origin of many z/OS modifications and elements.

Business Value:

We designed the CAIPVI interface to streamline the audit process by helping to identify common operating system modifications installed by select CA, IBM, and non-IBM operating system components and products.

Through CAIPVI, CA Auditor can quickly identify and display CA product modifications such as SMF records, program properties table (PPT) definitions, SVC definitions, exits, authorized TSO commands, modules, and SMP/E function modifier IDs (FMIDs).

Additional Considerations:

You can use CAIPVI when you execute various CA Auditor functions and review the description fields. For example, in the USER SVC display, CA Auditor uses CAIPVI information to display whether a particular SVC entry is *unknown*, meaning that its origin and ownership cannot be determined, or *known*, meaning the specific product or component to which the SVC belongs is identifiable.

More Information:

For detailed information, see the *Technical Reference* guide and the *Usage Guide*.

Symbolic Substitution for Batch SMF Reporting

We recommend that you use symbolic substitution variables when generating batch CA Auditor scripts that perform SMF file analysis.

Business Value:

When you generate batch scripts, CA Auditor stores the specific values that you enter within the script file. If you execute an SMF search function in batch, the date value stored may default to the creation date of the script, which means that the date may be in the past the next time the script runs.

CA Auditor lets you define symbolic substitution variables within the CA Auditor Central Parameter File, which lets you make symbolic references to the current date value instead of making specific date references, thereby providing a consistent, reliable means of identifying and reporting the information represented by specific records.

Additional Considerations:

Although many SMF search functions are ad-hoc, running certain pre-defined SMF search sequences on a daily or weekly basis adds substantial value. The following SMF records provide information about significant system activity; therefore, using symbolic substitution for these records can provide substantial benefits:

00

Indicates an IPL record.

07

Indicates an SMF data lost record.

09

Indicates a device is varied online.

11

Indicates a device is varied offline.

22

Indicates that the configuration may have changed by use of the CONFIG command.

More Information:

For detailed record and substitution information, see the *Technical Reference* guide and the *Usage Guide*.

Customizing Description Fields

We recommend that you customize CA Auditor description fields.

Business Value:

A number of CA Auditor functions have user-modifiable description fields that let you customize CA Auditor results. You can use these description fields to document site-specific audit findings. This information resides in the CA Auditor DBASE1 data store. Proper use of CA Auditor descriptions can save time and let auditors complete their auditing tasks in a more efficient manner.

Additional Considerations:

For example, consider the case of auditing z/OS console devices. You may have physical consoles throughout your data center in different physical locations. Because securing consoles often requires that proper physical security controls be in place to control user command entry, you should know the physical location of each console. To do so, update the description field on the console display function to denote the physical location of the console when you complete physical asset discovery.

You can also update descriptions for a number of other CA Auditor functions, for example, the user SVC analysis function.

More Information:

For detailed information about descriptions, see the *Technical Reference* guide.

Notebook Facility for Data Sharing

We recommend that you use the CA Auditor Notebook facility to log site-specific information pertaining to CA Auditor functions.

Business Value:

Proper use of CA Auditor notes can save time and streamline audit processing by allowing greater information sharing between auditors.

Each major CA Auditor function area, for example, APF analysis, I/O appendage analysis, Catalog analysis, and so on, lets you create a unique notebook in which you can store site-specific information about that function's audit findings. This information resides in the CA Auditor DBASE1 data store.

Additional Considerations:

You can use the notebook in many ways, including:

- Logging research done to explain exceptions and findings
- Logging status information on exceptions
- Logging sign-off information on exceptions

More Information:

For more information about the Notebook facility, see the *Technical Reference* guide.

DBASE1 Data Store

We recommend that you create periodic backups of the DBASE1 data store, particularly if you see significant activity on the DBASE1 file.

Business Value:

CA Auditor uses the DBASE1 file to store numerous installation-generated pieces of information. It contains site-specific data including profile information and preferences, results of freeze operations, auditor notes and descriptions, SMP/E analysis information, and so on.

More Information:

For detailed DBASE1 information, see the *Installation Guide*.

Collecting Hard Copies of Reports

We recommend that you use the CA Auditor Report feature to produce and save hard copies of online session reports.

Business Value:

A hard copy of data from a CA Auditor online session can serve many purposes:

- Provide evidence of required auditing activity
- Provide turnaround documentation and documentation for unexplained exceptions
- Document complex ad-hoc auditing sessions

Additional Considerations:

You can selectively print specific pages, or you can print all pages using the REPORT command.

More Information:

To configure reports, see the *Technical Reference* guide.

Chapter 4: Auditing Best Practices

This section contains the following topics:

Regular z/OS System Audit Regimen

We recommend that you constantly audit your mainframe z/OS system by using CA Auditor. We also recommend that you create procedures to audit your physical IT environment.

Business Value:

Regular auditing using CA Auditor offers the following benefits:

- Helps maintain z/OS integrity through timely identification of z/OS customization and modifications
- Helps verify internal compliance to change control procedures
- Minimizes z/OS auditing costs through CA Auditor usage, whether through direct license or through CA Out-Tasking, which is a CA Services initiative whereby customers can engage us to perform regular services

Maintaining the integrity of the z/OS system is necessary to maintain proper system and application functionality. Regular audits can also satisfy many common compliance regulations, laws, and requirements, such as Sarbanes-Oxley (SOX) and the Payment Card Industry-Data Security Standard (PCI-DSS).

Additional Considerations:

As you devise your auditing regimen, consider the following points:

- The z/OS system is the foundation for the applications and data that run your business; therefore, if the z/OS system has integrity exposures, the associated applications have the same exposures.
- A sound security policy bolsters z/OS integrity. Similarly, a proper z/OS implementation supports your overall security because a user could exploit any weakness to circumvent critical security controls and damage your applications.
- Sound system integrity is the result of careful planning, well-defined procedures, proper security and change control mechanisms, and regular auditing to verify that users are following these procedures.

Regular SMP/E Audit Regimen

We recommend that you regularly audit the SMP/E-maintained operating system, IBM program product, and OEM/ISV program product environments.

Business Value:

SMP/E is a complex but useful tool for operating systems and program products. Its complex nature creates challenges for auditors and technical support personnel.

CA Auditor provides a powerful, easy-to-use SMP/E auditing function that lets auditors identify all SMP/E environments present on the system and audit these environments. This function lets the auditor work without the need to confer with the technical support staff. Failing to audit SMP/E environments, which include critical system elements, could lead to improper system modifications.

Additional Considerations:

You must use the IBM SMP/E utility to install the z/OS system and most IBM and OEM/ISV program products. Vendors such as IBM, CA, and others use SMP/E to package their solutions for customer installation and to package product maintenance used to correct problems, provide new functionality, and accommodate changes in the operating environment.

In general, changes to SMP/E-maintained libraries can occur through:

- Changes applied through SMP/E
- Changes applied outside of SMP/E

More Information:

For detailed information about the SMP/E environment, see the *Technical Reference* guide.

Index