CA TLMS® Tape Management

TLMS_BestPractices_ENU

Release 12.6 Second Edition

Second Edition

CA Technologies Product References

This document references the following CA products:

- CA ASM2® Backup and Restore (CA ASM2 Backup and Restore)
- CA Disk™ Backup and Restore (CA Disk)
- CA Dispatch™ (CA Dispatch)
- CA Earl™
- CA Mainframe Software Manager (CA MSM)
- CA TLMS® Tape Management (CA TLMS)
- CA Vantage™ Storage Resource Manager (CA Vantage SRM)

Contact CA Technologies

Contact CA Support

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

- 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

Providing Feedback About Product Documentation

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

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 CA TLMS Tape Management" so that we can easily identify and categorize them.

Contents

Chapter 1: Introduction

This section contains the following topics:

Purpose of this Guide

The guide provides a brief introduction to the CA Technologies mainframe management strategy and features, and describes the best practices for installing and configuring CA TLMS.

Audience

The intended audience of this guide is systems programmers and administrators who install, configure, deploy, and maintain CA TLMS.

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 and installation 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.

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 and Configuration Best Practices

This section contains the following topics:

Installation

Use CA MSM to acquire, install, and maintain your product.

Business Value:

CA MSM provides a web interface, which works with ESD and standardized installation, to provide a common way to manage CA mainframe products. You can use it to download and install CA TLMS.

CA MSM lets you download product and maintenance releases over the Internet directly to your system from the CA Support website. 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 Installation Guide to set it up. 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. For more information about product setup, see the Installation Guide.

Configuration for Optimal Performance

The following section explains the best practices for configuring CA TLMS for optimal performance.

Alternate Log (ALOG) File Placement

Allocate the ALOG on a different disk volume than the VMF.

Business Value:

Allocating ALOG on a different volume than the VMF allows you to recover the most recent tape activity in case the volume containing the VMF is damaged or inaccessible.

Additional Considerations:

The CA TLMS ALOG file (also known as the ALTLOG or alternate log) is used to retain all updates to the CA TLMS Volume Master File (VMF). Like other database log or journal files, the ALOG is a critical resource that you should recover from the loss of your VMF. The ALOG contains the transactions used to update the VMF volume and file records for a period of time, as determined by the size of the ALOG file.

CA TLMS provides JCL in member TLMJALGI of CAI.CTAPJCL to execute the procedure CATALOGI, which allocates an ALOG file during installation.

To allocate an ALOG on a different volume

1. Configure and run TLMJALGI.
2. A new ALOG with a different name is allocated on a different volume.
3. Stop CA TLMS by shutting down the CTS address space.
4. Run the ALOG backup utility CATALOGB.
5. A new ALOG backup is created and the disk ALOG data set is reset to empty status. That means that all the transactions have been saved in an ALOG backup data set.
6. Start CA TLMS after changing the CAIALOG DD to point to the new ALOG file in the CTS procedure.

Note: You must specify RECOVRY=ALTLOG in your TLMSIPO member of CAI.CTAPOPTN. This statement causes CA TLMS to use the ALOG.

CA TLMS provides the following health checks related to ALOG processing:

- The first health check warns if RECOVRY=ALTLOG or SMF is not set.
- The second health check raises an exception when it discovers the ALOG and VMF on the same volume.

Note: For more information about allocating the CA TLMS ALOG file, see the Installation Guide.

Multi-System Environment Considerations

Convert CA TLMS RESERVEs to global ENQUEUEs in environments where a single resource manager (MIM or GRS) controls the DASD.

Business Value:

By converting CA TLMS RESERVEs to global ENQUEUES you are reducing the possibility of experiencing application slowdowns or lockouts due to contention for other resources on the volume.

Additional Considerations:

Consider the following conditions when sharing the VMF and ALOG data sets among multiple systems:

- The sharing systems need not belong to the same SYSPLEX, and do not have to be at the same MVS level.
- The CA TLMS maintenance levels of the sharing systems need not be the same, but new features or enhancements may be usable only when supported by all systems.
- The CA TLMS installation libraries may or may not be shared or cloned. The use of a single CAI.CTAPOPTN parmlib simplifies maintenance and control of all system options and user modifications. When the Realtime Retention Assignment feature is used, the same Retention Master File (RMF) should be used on all the systems to ensure consistent results.

Convert CA TLMS RESERVEs to global ENQUEUES for the VMF and ALOG resources only. The following table lists the resources:

Resource	Major Name	Minor Name
VMF	TLMSVMFQ	TLMSVMFQ
VMF (extend)	TLMSVMFQ	TLMSVMFX
ALOG	UPDCTL	TLMSALOG

If the RESERVEs are converted, this must be done on all sharing systems. If the RESERVEs are not converted, the DASD volumes which VMF and ALOG reside on should not contain other data sets that are frequently used during tape processing, like system catalogs or control data sets of DASD management or security products. You prevent performance degradation or potential lockout situations this way. All CA TLMS resources other than the VMF and ALOG must be controlled locally.

Implement the Failsafe USERMOD

Implement the Failsafe USERMOD into the operating system.

Business Value:

The Failsafe USERMOD ensures the protection of your tape data by warning you if any tape is read or written by an application when CA TLMS is not actively tracking tapes.

Additional Considerations:

The Failsafe USERMOD-CTSUSAF is distributed as member CTSJUSAF in the CAI.CTAPJCL library. This USERMOD should be installed into the operating system to prevent any tape processing from occurring before running the CAS9 (CA Common Services). With USERMOD CTSUSAF, WTORs are issued to indicate that the CA TLMS intercepts are not active. CA TLMS issues messages CTS999D along with either CTS997E or CTS998E. The Failsafe USERMOD will prevent you from running tape applications without having activated CA TLMS, which would result in CA TLMS not being able to protect these tapes.

CTSUSAF will replace IBM's tape management exit IFG019VM in module IFG019RB which resides in SYS1.LPALIB. An IPL is required to implement this change.

CA TLMS VMF Backup

Backup the CA TLMS VMF regularly.

Business Value:

Regular backups of the VMF are required to allow you to recover critical tape data in case of a failure.

Additional Considerations:

The CA TLMS Volume Master File (VMF) is a critical system resource. You must regularly back up the VMF and retain multiple versions of these backups to enable point in time recovery. The CATVMFB procedure is provided to create a backup of the VMF on tape that can be sent off site.

ALOG File Backup

Backup the ALOG file regularly.

Business Value:

You must back up the ALOG file regularly to enable you recover critical tape data in case of a VMF failure.

Additional Considerations:

The ALOG file is a critical part of VMF recovery processing. You should back up the ALOG file on a daily basis, or more frequently, if the volume of tape processing is very high. The ALOG file is used to record the individual transactions applied to the VMF and is similar to a database journal or log file. The CATALOGB procedure is provided to back up the ALOG transactions to tape.

The ALOG file is reset each time you run the CATALOGB procedure, only the transactions created since the last time CATALOGB was run will be written to the ALOG backup tape.

More Information:

For more information on the CATALOGB or CATVMFB procedures and recovering a VMF from a VMF backup tape and ALOG backups, see the *Configuration Guide*.

ALOG File Size

Allocate sufficient space for the ALOG file.

Business Value:

Allocating sufficient space for the ALOG file helps you capture all the CA TLMS transactions. This helps you to recover all the tape data if the VMF is lost, damaged, or deleted.

Additional Considerations:

The ALOG is unblocked and the CATALOGB process creates a report (TLMS055) that shows the number of ALOG records (blocks) used. A threshold limit is provided to inform you when the ALOG is nearly full. You can use this report to know how full the ALOG is before any threshold is triggered.

Schedule the CATALOGB Process

Schedule the CATALOGB process to run daily, before the daily retention processing job (CATTRS).

Business Value:

Scheduling the CATALOGB process to run daily gives you the ability to recover from possible problems in retention processing.

Additional Considerations:

This best practice recommends that by scheduling this daily utility before you schedule the daily retention job CATTRS, you have the ability to recover the VMF to a state prior to it being updated by CATTRS, should there be any problems in CATTRS processing.

Retain ALOG Versions

You must retain enough versions of ALOG backups since the VMF was last backed up by CATVMFB.

Business Value:

Retaining ALOG backups helps you recover all the tape data in case the VMF is lost or damaged and provides you an audit trail to determine what has happened to a volume over time.

Additional Considerations:

We recommend that you retain VMF and ALOG backups for six months. These backups allow you to go back in time to research detailed activity for tape volumes. If you find that a tape has been scratched or modified and you need to understand what has happened, the ALOG data will provide the answer. The ALOG records show all the updates to the VMF from real-time Open/Close/EOV events, batch jobs, and CATLTP updates.

You can use IEBGENER to concatenate the daily ALOG backup tapes onto fewer tapes. Using this method, you can create a weekly or a monthly tape instead of individual daily ALOG tapes. As is the case when using multiple ALOG files as input, they should always be processed in the order OLDEST to NEWEST.

Review Tape Inventory at Offsite Vaults

Review the inventory report of your offsite tapes and identify those tapes that may no longer need to be offsite and can be returned from offsite retention. We recommend that you use CA Earl to run a report (TLERPT06) to identify such tapes.

Business Value:

Reviewing the inventory report of your offsite tape allows you to identify tapes in the vault that can be returned for scratch. This will reduce the number of tapes maintained at the vault, thereby reducing the associated expenses of vaulting tapes.

Additional Considerations:

You can lose tapes in the offsite location, if they are retained by cycle control (Type 4) and the data set is a GDG that is no longer created. You could also have tapes that are sent offsite longer than necessary due to the fact that the retention schedule holds them offsite longer than their expiration date. You should also check for errors in TLMSTRS processing, because this can result in tapes being left at an offsite location longer than intended.

Review the Use of CA TLMS User Exits

Review the new features introduced in CA TLMS.

Business Value:

You can eliminate some of the commonly used user exits and thereby the need to code and maintain these user exits.

Additional Considerations:

Use the RMF Pattern Masking feature introduced in CA TLMS r12 to eliminate the TLMSXTRS Tape Retention System user exit used for controlling retention of FDR tapes. You have to set up the RMF retention rules using the new advanced pattern masking characters.

Note: User written TLMSXTRS exits may not have been updated to support the use of the Retention Types A, B, and C introduced in Release 5.5.

Use the External Data Manager (EDM) feature introduced in CA TLMS 5.5 to eliminate the TLMSXUPD user exit used for controlling the DFSMShsm tape expiration.

Any user exit that has device tables should be reviewed for new device support.

More Information:

For information about CA TLMS user exits, see the *Configuration Guide*.

Identify Virtual Volumes

While adding volume ranges to your VMF, identify the tape volumes that are virtual volumes.

Business Value:

This best practice allows you to easily identify and efficiently manage your virtual volumes.

Additional Considerations:

When executing the CATVMFRS procedure to add volumes, you should use the ATL(VIBM, *nnn*), ATL(VSTORTEK,*nnn*), or ATL(VTAPE *nnn*) parameter to identify the virtual tape system that manages these volumes. For existing ranges or volumes that should be converted to use as virtual volumes, use the UPV command to update the ATLTYP field to the appropriate virtual tape system. Following are examples of using the UPV command to mark volumes as virtual tapes:

UPV volser ATL(VIBM,1)

UPV volser ATL(VSTORTEK,1)

UPV volser ATL(VTAPE,1)

Use External Data Managers

Use the External Data Manager (EDM) feature to manage tapes for products that maintain their own catalog of tape files and volumes.

Business Value:

The EDM feature gives an additional level of protection against tape volumes from being erroneously expired before the controlling application is finished with the tape.

Additional Considerations:

The following list shows the most common products that are supported by the EDM feature:

- IBM DFSMShsm
- CA Disk
- CA Dispatch
- CA ASM2

Within the CA TLMS VMF, the tapes from these products will look like they are single file, and single volume. In reality, they will have multiple files on each tape. CA TLMS will not scratch an EDM tape. The EDM must notify CA TLMS when each tape should be scratched by calling the appropriate scratch routine for each EDM. CA TLMS provides a version of the scratch program for each EDM.

EDM rules are set up in the CAI.CTAPOPTN library in the member CTOEDMxx. The rules must contain the EDMid. The DSN, DD, JOB, and PGM names are optional, but you must specify at least one name.

If you are specifying the PGM name in the rule, you may need to write multiple rules. If the program that creates the tape is not the same as the program that releases it, you will need to have at least two rules. The EDMid must be the same for all of the rules for that product.

Example for CA Dispatch:

Creating programs: CAISYS01, XTARMAIN, and CADSARUT

Releasing program: ARBATCH

Sample rules might be:

```
EDM=DISP,PGM=CAISYS01
EDM=DISP,PGM=XTARMAIN
EDM=DISP,PGM=CADSARUT
EDM=DISP,PGM=ARBATCH
```

These rules will cause any data set written by the three programs to be marked as EDM controlled and ARBATCH will need to notify CA TLMS that they should be expired and scratched.

When an EDM tape is created, CA TLMS updates the VMF with the DSN and sets the EDMid to the EDM name that you selected. As the tape is released, CA TLMS checks that the program releasing the tape is the correct program (owner) and then scratches the tape. Possible EDMs include but are not limited to:

EDM	Creating PGM	Releasing PGM
IBM ABARS	ARCWCTL	ARCCTL
TSM/ADSM	ANRSERV	ANRSERV
	DSMSERV	
CA DISK/DMS	ADSMI002	
	ADSMI000	
	ADSMI302	
DISPATCH	CAISYS01	ARBATCH
	XTARMAIN	
	CADSARUT	
DFSMShsm	ARCCTL	ARCCTL
FDRABR 5.4	FDRABR	FDRARCH
ASM2	$MAINT	
	$DASDMNT	

Note: For more information about the setup of the EDM rules, see the *Configuration Guide* and the *Installation Guide*.

Use the Graphical Management Interface (GMI)

Use the Graphical Management Interface (GMI) to view and monitor CA TLMS activity.

Business Value:

GMI is CA's graphical management interface product that allows you to view and manage CA TLMS activity from a Windows PC. GMI's structure is object oriented and provides a common layout consisting of an object tree, and consistent menu options and icons. This common layout makes it easy to remember how to navigate and use features. It also supports having multiple windows open at the same time (not hierarchical like the 3270), which allows you to view and compare information simultaneously.

This point-and-click interface provides a common and consistent method for viewing and managing multiple CA products, which can save considerable cost and time on training and learning.

Additional Considerations:

GMI consists of PC clients which interface with a z/OS server component to allow access to basic z/OS server functions.

The following are the available PC clients:

Windows-based Client

This client provides full functionality. That is, you can manually perform view and analysis functions, filter and sort desired entries, zoom (drill-down) to related objects, and take actions upon selected entries. You can create customized colored reports in different formats, for example, tables and graphs. These reports can be printed and exported to your PC directory, servers, intranet, and so on. You can create, manage, and view Summary objects. This client also provides designer wizards to create scripts to monitor and respond to any condition, exceptional or routine, in automatic ways. These automation services let you replace many if not all of the manual processes of managing your system.

Web-based Client

This client can be used from any PC with internet access to the GMI application server. The current version of the Web-based Client provides the user-driven functionality of view and analysis, filtering and sorting, zooming, and the ability to take actions on selected entries. You can create customized colored reports in different formats, for example, tables and graphs, and you can also view Summary objects.

More Information:

For more information about GMI for CA TLMS, see the CA Vantage SRM documentation set.

Monitor the CA TLMS Health Checks

Monitor health checks generated for CA TLMS.

Business Value:

Health Checks alert you of conditions that could prevent CA TLMS from running properly, if left uncorrected, and they guide you in addressing the problem. These health checks provide best practices for running CA TLMS.

Additional Considerations:

The following health checks are provided for CA TLMS:

TLMS_AUX_CUSHION_CRITICAL

Monitors the availability of AUX records in the CA TLMS VMF and triggers an exception when the number of AUX records used exceeds a critical percentage.

TLMS_AUX_CUSHION_WARNING

Raises an exception when the number of AUX records used exceeds a lower warning level.

TLMS_OPTION_NOTLMS

Examines the setting of the NOTLMS option, which controls what CA TLMS does when tape tracking is not available. An exception is raised when NOTLMS=CONT is specified.

TLMS_OPTION_PROTECT

Examines the setting of the PROTECT option and creates an exception when PROTECT=SELECT.

TLMS_OPTION_RECOVRY

Examines the setting of the RECOVRY option and creates an exception if RECOVRY=NONE or RECOVRY=SMF is specified.

TLMS_OPTION_SECOPN

Examines the setting of the SECOPN option which controls the call to your external security system and creates an exception if SECOPN=NO is specified.

TLMS_OPTION_SECURE

Examines the setting of the additional security processing controlled by the SECURE option and creates an exception if SECURE=NO is specified.

TLMS_QUEUE_ACTIVE

Monitors the status of the CA TLMS transaction queue and creates an exception if queue processing is stopped.

TLMS_VMF_ALOG_SEPARATION

Raises an exception if the VMF and ALOG reside on the same disk. volume.

TLMS_VMF_UPDATE_NOT_POSSIBLE

Monitors CA TLMS updates to the VMF to see if any volume chaining or other errors have occurred. This check provides an early warning if any VMF errors are detected.

More Information:

For more information about CA TLMS health checks, see the *Configuration Guide*.

Index