CA 1™ Tape Management

Best Practices Guide

12.6.00

Fifth Edition

CA Product References

This document references the following CA Technologies products:

- CA Chorus™ Software Manager (CA CSM)
- CA Chorus™
- CA Mainframe Software Manager™ (CA MSM)
- CA 1® Tape Management (CA 1)
- CA ASM2® Backup and Restore
- CA Disk™ Backup and Restore (CA Disk)
- CA Dispatch™ (CA Dispatch)
- CA Earl™
- CA Mainframe Security Suite for ACF2™
- CA Mainframe Security Suite for Top Secret®
- CA MIM™ Resource Sharing (CA MIM)
- CA TLMS Tape Management (CA TLMS)
- CA Vtape™ Virtual Tape System (CA Vtape VTS)

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 are based on customer experience reported through interviews with development, technical support, and technical services. Therefore, many of these best practices are a collaborative effort stemming from customer feedback.

To continue to build on this process, we encourage you 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, c*ontact 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.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- Introduction (see page 9)—Streamlined and improved.
- Your Product Installation and Configuration Best Practices > Implement a proactive Preventive Maintenance Strategy (see page 11)—Added to the guide.
- Your Product Installation and Configuration Best Practices > CA Cloud Storage for System z Best Practices—Added to the guide.

Contents

Chapter 1: Introduction

The guide introduces the CA Technologies mainframe management strategy and features, and describes the best practices for installing and configuring your product.

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

Chapter 2: Installation and Configuration Best Practices

This section contains the following topics:

Implement a Proactive Preventive Maintenance Strategy

CA Technologies formerly delivered product maintenance using Service Packs. We have replaced this model with CA Recommended Service (CA RS) for z/OS, which provides more flexibility and granular application intervals. CA RS is patterned after the IBM preventive maintenance model, Recommended Service Upgrade (RSU). With CA RS, you can install preventive maintenance for most CA Technologies z/OS-based products in a consistent way on a schedule that you select (for example, monthly, quarterly, annually).

We recommend that you develop and implement a proactive preventive maintenance strategy whereby you regularly apply maintenance. You could follow the same schedule that you use to apply IBM maintenance, or you could implement a schedule for CA Technologies products only.

Business Value:

Keeping your products current with maintenance helps your team remain productive and minimize errors while safely protecting your systems. If you do not install preventive maintenance regularly, you risk encountering known problems for which we have published and tested fixes.

Our mainframe maintenance philosophy is predicated upon granting you the flexibility to maintain your sites and systems consistent with industry best practices and site-specific requirements. Our philosophy focuses on two maintenance types. Understanding each type can help you maintain your systems in the most efficient manner.

Note: This philosophy applies to the CA Chorus Software Manager Enabled Products. For legacy products, contact CA Support for maintenance details.

Corrective Maintenance

Helps you address a specific and immediate issue. This type of maintenance is necessary after you encounter a problem. We may provide a test APAR when a new problem is uncovered, or a confirmed PTF when the problem has been resolved. Your primary goal is to return your system to the same functional state that it was before you experienced the issue. This type of maintenance is applied on an as-needed basis.

Preventive Maintenance

Lets you apply PTFs that we have created and made public. You may have experienced the issues that each PTF addresses. CA RS provides a way to identify all published maintenance that has been successfully integration-tested. This maintenance has been tested with other CA Technologies products, current z/OS releases, and IBM subsystems, such as CICS and DB2. CA RS levels are published monthly that include PTFs, HIPERs and PRPs (PE-resolving PTFs). Before you download, apply, and test a new CA RS level, we recommend that you accept the previous CA RS level.

You can initiate a maintenance installation activity at any time. You can then install the current CA RS level of maintenance (recommended) or an earlier level. Additionally, you can install maintenance to support a new hardware device, software upgrade, or function using the FIXCAT method.

For all maintenance, *before* you initiate any maintenance action, obtain the current SMP/E HOLDDATA.

Important! CA Chorus™ Software Manager (CA CSM) - formerly known as CA Mainframe Software Manager™ (CA MSM) - is an intuitive web-based tool that can automate and simplify many CA Technologies product installation and maintenance activities. We strongly recommend that you use CA CSM to maintain your CA Technologies z/OS-based products.

More Information:

To apply preventive maintenance using CA CSM or from CA Support Online on http://ca.com/support, see the *Installation Guide* for your product and the CA CSM online help.

Installation

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

Business Value:

CA CSM 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 1.

CA CSM lets you download product and maintenance releases over the Internet directly to your system from the CA Support website. After you use CA CSM 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 CSM can continue to help you maintain your product.

More Information:

For more information about CA CSM, see the *CA Chorus 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 1 for optimal performance.

Audit File Placement

Allocate the Audit file on a different volume than the volume used for the Tape Management Catalog (TMC).

Business Value:

Allocating the Audit file on a different volume prevents the loss of your data if the volume is damaged or inaccessible. You also achieve better performance with the TMC and Audit on different volumes.

Additional Considerations:

The Audit file is created using the ISPF 3.2 Data Set Utility panel, or it can be allocated with JCL in batch. If you need to place the Audit file on a new DASD volume, you can execute the TMSFORMT utility to allocate and format an Audit file. Use the AUDIT DD to reference the Audit file in the TMSFORMT job.

A CA 1 Health Check has been created to raise an exception when it discovers the Audit file and TMC on the same volume.

Note: For more information about allocating the CA 1 Audit file and creating an Audit data set, see the *Installation Guide*. For more information about CA 1 health checks, see the *Administration Guide*.

Vault System Setup

Choose a vaulting strategy that uses simple rules based on days and a limited number of different vaulting criteria.

Business Value:

Choosing a simple vaulting strategy based on days (days since creation or days at the vault) allows you to easily monitor the movement of tapes to off-site locations (vaults) and prevents tapes from being accidentally left at the vault longer than required.

Additional Considerations:

The rules for automated off-site movement of tapes are defined in the Vault Pattern Description Data Set (VPD). While very specific rules can be defined in the VPD for an individual volume or tape data set using the VOL= or CDSN= selection statements, the most efficient way to do selection is to set up patterns using data set name (DSN) rules.

Data sets matching the explicit or pattern-masked data set rules will be selected for processing by VMS. Having fewer rules using pattern masking allows for easier control and prevents having obsolete entries that should be removed.

Tapes sent off-site can generally be placed into two categories. The first category includes tapes sent off-site for DR purposes (full-volume backups and incremental backups). The second category is long-term backups.

Full-volume Backups and Incremental Backups

For this category, use a rule-based on days since creation or days in the vault. It is best to keep everything at the vault the same length of time. Why you should keep some full-volume backups for 3 weeks and others for 4 weeks? They are all obsolete the next time a full volume backup is run. When setting this up, choose how many copies you want to keep off-site. If two is sufficient and you run full-volume backups once a week, then keeping DR backups off-site for 14 days is sufficient. If you only do full-volume backups every two weeks, then keep those DR backups off-site for 28 days.

Long Term Backups

For this category, keep the tapes at off-site either permanently or until they are expired. However, permanently keeping the tapes at off-site does not mean the data will be available forever; as tapes that are kept longer than 7 years may not be able to be read. Keeping the tapes at off-site until they are expired causes a file to expire accidentally and brings back the tape from the vault too early.

Note: For more information about VMS utilities, see the *Utilities and Reports Reference Guide*.

Multi-System Environment Considerations

When sharing the TMC between systems outside of a SYSPLEX configuration, a single CTAPOPTN parameter library shared between systems is recommended.

Business Value:

The use of a single CA 1 CTAPOPTN when sharing a TMC and AUDIT file ensures that all systems sharing the TMC use the same options. This reduces the chance of having tapes being retained, vaulted, or managed differently depending on which system they were created.

Additional Considerations:

When the Real-time Expiration feature is used, the set of retention rules should be identical on all the systems to help ensure consistent results.

All systems sharing a single TMC must also share a single Audit data set.

Consider the following conditions when sharing the TMC and Audit data sets among multiple systems:

- The systems sharing a common TMC and AUDIT need not to belong to the same SYSPLEX and do not have to be at the same z/OS level.
- The CA 1 maintenance levels of the sharing systems need not to be the same but new features or enhancements may be usable only when supported by all systems.
- If all system catalogs are not shared across all the systems that share the TMC, set the option OCTLG to NO to enable real-time catalog control for these tapes. Also, the utility TMSUNCAT will need to be run daily on those systems that do NOT share the system catalogs with the system on which TMSCLEAN was run.

To avoid possible lockouts or performance degradation, we recommend that cross-domain management products like GRS or CA MIM do not handle CA 1 resources. Also, consider the following recommendations:

- If necessary, you can convert the CA 1 RESERVEs into global ENQUEUEs. This conversion can be done for the TMC and Audit resources only. The major name is TMSQNAME and the minor names are TMS-TMC and TMS-AUD. If you use the UNIQUE_RNAME in TMSXTEND, the minor names are TMS-TMC-*vvvvvv*-TMC.*data.set.name*, TMS-AUD-*vvvvvv*-AUDIT.*data.set.name*, and TMSAPEC-*vvvvvv*-TMC.*data.set.name*. If the RESERVEs are converted, they must be converted on all systems sharing the TMC and Audit. Which RNAME format is used depends on if you enabled the Unique_RNAME feature through the TMSXTEND utility or the TMSUDSNB utility.

- If the RESERVEs are not converted, the DASD volumes in which TMC and Audit 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, to prevent performance degradation or potential lockout situations.
- All CA 1 resources other than TMC, Audit, and TMSAPEC must be controlled locally. Do not share SYSTEM-level enqueues across multiple systems.

Note: For more information about the CTAPOPTN parameters OCTLG and UNCATA, see the *Programming Guide*. For more information about TMSUNCAT, see the *Utilities and Reports Reference Guide*.

Prevent the Creation of Tapes When CA 1 is Not Active

Implement the Failsafe USERMOD to prevent the creation of tapes if CA 1 has not been started.

Business Value:

The Failsafe USERMOD protects your critical company-data on tapes. Installing the Failsafe USERMOD prevents you from running any tape application, if one of the following conditions exists:

- CA 1 is not activated.
- CA 1 is batch activated.
- CA Common Services (CAS9) is not run.

Additional Considerations:

The Failsafe USERMOD is distributed as member CTSJUSAF in the CTAPJCL library. When the Failsafe USERMOD is enabled, WTORs are issued to indicate that the CA 1 intercepts are not active. CA 1 issues message CTS999D with either CTS997E or CTS998E. An example of the one of the messages issued (CTS998E) follows:

Example: CTS998E Message

CA TAPE MGMT INTERCEPTS ARE NOT ACTIVE!! TAPES ARE NOT PROTECTED AND TAPE ACTIVITY IS NOT BEING RECORDED! CTS999D WILL BE ISSUED FOR EACH TAPE MOUNT, REPLY U, M, OR C.

U TO USE THE TAPE WITHOUT TAPE MANAGEMENT.

C TO CANCEL THE JOB WITH A USER 222.

M TO REJECT THE TAPE.

The CTS999D message identifies the tape unit, volume serial number, and data set name being opened.

Example: CTS999D

CTS999D 01F4,V00014,APPL.TRANFILE.JULY

The message in the example would be issued for data set "APPL.TRANFILE.JULY" when the volume it resides on and V00014 is mounted on unit 01F4.

The CTS997E message is issued when a foreign tape is being opened (as identified by the EXPDT=98000 JCL parameter). Otherwise, the CTS997E message is similar to the CTS998E message.

Note: For more information about the FAILSAFE USERMOD, see the *Installation Guide.* For more information about the CTS999D, CTS997E, and CTS998E messages, see the *Message Reference Guide*.

Activate the Database Services Subtask

Configure the Data Base Services (DBS) subtask of the Common Tape System to automatically start whenever the CTS task starts.

Business Value:

Configuring the DBS subtask prevents the accidental archival, deletion, or movement of the CA 1 TMC to another volume while CA 1 is active.

Additional Considerations:

You can start the DBS subtask by specifying the START DBS command in the member CTSSTART in CAI.CTAPOPTN. In the ENFCMDS member of CAI.CTAPOPTN, you can specify S CTS to have CA Common Services (CAS9) start the CTS address space itself. In the CTS startup procedure, the CTSSTART member in CAI.CTAPOPTN is read and any subtasks (such as DBS) specified in the member are started.

Note: For more information about the DBS subtask, see the *Administration and Operators Guide*.

Back up the TMC and Audit Data Daily

Back up the TMC and Audit data set daily by running the TMSCOPY utility. You should also maintain at least 6 months of Audit data.

Business Value:

Running TMSCOPY on a daily basis ensures that you have multiple backup copies of the TMC and provides for quick recovery of the TMC if the TMC is lost or damaged.

Additional Considerations:

TMSCOPY is used to back up the TMC and Audit data set transactions written since the previous backup. TMSCOPY may also be used to restore the TMC if it is corrupted or destroyed.

CA recommends that you use a generation data group (GDG) to manage the TMC and Audit file backups created by TMSCOPY. The Audit file includes all updates to the TMC from real-time Open/Close/EOV events, batch jobs, ISPF, and tape inquiry command (TIQ) updates. A separate utility—TMSAUDIT—can be used to read the backup and produce a report that shows the following:

- What changes were made to a TMC record?
- When the changes were made?
- What utility or CA 1 component was made the changes?
- Who made the change?

You can use IEBGENER to concatenate the daily backup to fewer tapes. Using this method, you can create a weekly or a monthly tape instead of individual daily tapes.

To allow you to maintain a history of tape activity, CA recommends that you to keep Audit files for 6–12 months. If you find that a tape has been scratched or modified, and you need to understand what has happened to that tape, the Audit data can provide you the answer. You can use CA Earl to read the Audit file and search for a specific volume or data set. You can also use the CA Vantage GMI user interface, which allows you to browse the Audit file records and use advanced filtering to search for a specific volume or data set.

Note: For more information about TMSCOPY or TMSAUDIT, see the *Utilities and Reports Reference Guide*. For more information about concatenating the Audit backups to fewer tapes, see the *Administration Guide.*

Review Tape Inventory at Offsite Vaults

Review the TMEVLT03 inventory report of your off-site tapes and identify those tapes that may no longer need to be off-site and can be returned from vault management.

Business Value:

The inventory report of your off-site tape allows you to avoid the loss of tapes in the vault and prevents paying for off-site storage of obsolete tapes.

Additional Considerations:

You can lose sight of tapes in the vault if they are vaulted by cycle control and the data set is a GDG that is no longer created. You could also have tapes that are vaulted longer than necessary due to the fact that the vault pattern holds them off-site longer than their expiration date. You can modify the TMEVLT03 report written in the CA Earl reporting language (which is distributed in CAI.CTAPECPB) to change the sort order to creation-date (CDATE) or the date the volume was sent to the vault (OUTDATE) by changing the CONTROL statement like the following:

```
CONTROL (P_VAREA) SKIP
        (VAULT_OUT_SUBCODE 'VAULT SUBCODE TOTAL') SKIP
         CDATE   or OUTDATE
         VOLSER
```

The TMEVLT03 report can also be modified to list those volumes that are off-site when the expiration date is less than the current date. To modify the TMEVLT03 to show volumes whose retention rules keep them off-site even though the file is expired, change the SELECT statement like the following:

```
SELECT EXPDT < RUNDATE
```

Note: For more information about CA Earl, see the Utilities and Reports *Reference Guide* and the *CA Earl Reference Guide.*

Use the Dynamic TMC Extend Feature

Use the TMSXTEND and TMSBLDVR utilities to dynamically add volumes or DSNBs (records used to track secondary data sets on tape) to the CA 1 Tape Management Catalog (TMC).

Business Value:

As companies increase the tape usage or implement virtual tape systems, new volumes and DSNBs must be defined or added to the TMC. This should be done without disruption to the normal tape processing. Using the TMSXTEND and TMSBLDVR utilities, you can create a TMC, update a TMC, or add or remove volume ranges or DSNB records without impacting the production workload. This helps your business to maintain application and processing availability 24 hours a day, 7 days a week.

Additional Considerations:

The TMSXTEND and TMSBLDVR utilities dynamically create a new TMC format, which is known as an extended format TMC, because of the new control records that are used to maintain volume ranges. When you have converted the TMC to extended format, you no longer need to maintain exits TMSXITE and TMSXITU to convert alphanumeric VOLSER ranges to an internal numeric range (except for a few very rare cases). The new format internally takes care of conversion.

To add ranges or DSNB records, you need to allocate a new TMC with a name that is identical to the active TMC except that it has a suffix of ".N" (for "new") before TMSXTEND is executed. TMSXTEND uses this new TMC with the existing TMC to add the volumes, DSNB records, or both.

The TMSXTEND utility is designed for multi-system environments, where the TMC is shared and performs checks to ensure that all systems sharing the TMC are at the required level before proceeding.

Note: For more information about the TMSXTEND and TMSBLDVR utilities, see the *Utilities and Reports Reference Guide*.

Implement the Automatic Pointer Errors Correction Subtask

Use the Automatic Pointers Error Correction (APEC) subtask of the Common Tape System (CTS).

Business Value:

The APEC subtask continually verifies the integrity of the TMC in real time to prevent any possible chaining problems from impacting your tape activity. Any errors found in the TMC are immediately corrected.

Additional Considerations:

CA 1 multi-volume and multi-data set chaining errors and errors in the free chain of unused DSNBs occur as a result of invalid manual updates. However, any of the following conditions may also cause invalid chains:

- System failure during CA 1 processing
- TMC restore failure without having all available Audit data (as in a disaster recovery)

The APEC subtask is designed to replace the TMSPTRS utility, which scans for pointer errors and generates reports and control statements that can be used to fix the TMC. The APEC subtask provides the following benefits:

- APEC identifies additional problems and corrects pointers errors directly in the TMC.
- APEC can also be run in a NOUPDATE mode. Running in a NOUPDATE mode causes APEC to report the errors found and to generate control statements for the TMSUPDTE, TMSUDSNB, and TMSAGGR utilities.
- In addition to the errors identified by TMSPTRS, APEC also verifies that all of the DSNBs on the free chain are truly free.

Note: For more information about the APEC subtask of CTS, see the *Administrator and Operators Guide.*

Review the Use of CA 1 User Exits

Review your use of CA 1 user exits as new releases are introduced. New features introduced in CA 1 can eliminate the need for user exits.

Business Value:

Exploiting the capabilities of new CA 1 features such as the TMSXTEND utility and Real-time Retention simplifies the process of upgrading to a new CA 1 release by reducing the number of user exits that must be re-installed.

Additional Considerations:

Use the SMP/E LIST SYSMODS command to show the usermods you have applied to your CA 1 target zone. You may be able to eliminate the following exits:

- Use the TMSXTEND utility to eliminate TMSXITE and TMSXITU (used for alphanumeric volume serial number support).

  The TMSXTEND utility automatically converts alphanumeric volume serial numbers in the TMC to their CA 1 internal format. Unless you are using non-standard VOLSERs, this new functionality helps you to eliminate the TMSXITE and TMSXITU exits. After converting the TMC to the new format, the TMSXITE and TMSXITU exits will no longer be invoked and can be removed at any time.

- Use the CA 1 Real-time Retention feature to eliminate TMSXITB (used for controlling retention during ABEND processing).

  The Retention Data Set (RDS) changes the retention on files that have been created correctly and if they have the ABEND bit on in FLAG1 X'10'. These rules reduce the need for TMSXU2B to set the retention during ABEND processing. You can use the RDS in real time by including a TMSRDS DD in the TMSINIT JCL, or in batch with the TMSEXPDT job. For ABEND retention, you would use a rule with the LABEL=ABEND=RETPD/EXPDT keyword. If you are using the real-time processing method, at close of file, CA 1 will apply the matching RDS rule and update the record in the TMC.

The TMSXTEND utility automatically converts alphanumeric volume serial numbers to their CA 1 internal format. Unless you are using non-standard VOLSERs, this new functionality helps you to eliminate the TMSXITE and TMSXITU exits. When converting to the new format, you need not immediately remove these exits; CA 1 will not use them.

The Retention Data Set (RDS) changes the retention on files that have been created correctly and if they have the ABEND bit on in FLAG1 X'10'. These rules reduce the need for TMSXU2B to set the retention during ABEND processing. You can use the RDS in real time by including a TMSRDS DD in the TMSINIT JCL, or in batch with the TMSEXPDT job. For ABEND retention, you would use a rule with the LABEL=ABEND=RETPD/EXPDT keyword. If you are using the real-time processing method, at close of file, CA 1 will apply the matching RDS rule and update the record in the TMC.

Note: For more information about the use of the TMSXTEND utility and Real-time Retention processing, see the *Programming Guide* and the *Utilities and Reports Reference Guide*.

Implement the Real-time Catalog Interface

Use the Real-time Catalog Interface to automatically keep your TMC record in sync with the z/OS Catalogs and eliminate having to run the TMSCTLG batch utility on a daily basis.

Business Value:

With the Real-time Catalog Interface, CA 1 updates the TMC as you catalog or uncatalog tape data sets. This feature helps ensure that the CA 1 TMC and system catalogs are properly synchronized and allows you to reduce the number of CA 1 daily maintenance jobs.

Additional Considerations:

When you set the option OCTLG (found in the *TMOOPTxx* member of the CTAPOPTN library) to NO, you can stop running the catalog maintenance program TMSCTLG, removing two steps of your daily job for CA 1.

Using this option, TMSCLEAN program processes the tapes under CATALOG control by checking the tape catalog to help ensure that the tape is not cataloged before CA 1 expires, and scratches the tape. TMSCLEAN does the processing that TMSCTLG used to do. This feature eliminates two programs from the CA 1 daily job stream and also eliminates the time spent by TMSCTLG to locate the ICF catalogs for every data set under CATALOG control. If you have unshared ICF catalogs, this feature eliminates the need to do IDCAMS LISTCAT for every catalog, which is used as input to TMSCTLG.

A CA 1 Health Check has been created to raise an exception, when it discovers the OCTLG option is set to YES.

Note: For more information about the OCTLG option, see the *System Programmer Guide.* For more information about the programs TMSOSCAT and TMSCLEAN, see the *Utilities and Reports Reference Guide.* For more information about CA 1 health checks, see the *Administration Guide*.

Implement the Real-time Expiration Feature

Use the Real-time Expiration feature to apply your retention rules specified in the Retention Data Set (RDS) during tape creation, when the file is closed.

Business Value:

The Real-time Expiration feature reduces the number of maintenance utilities that you need to run daily.

In sites where CA Vtape is also in use, the expiration information is immediately available to be used to place virtual volumes in the correct subgroup for externalization processing. This integration is unique to CA Vtape and CA 1 or CA TLMS.

Additional Considerations:

Sites that set up a Retention Data Set (RDS) to supply or override tape expiration dates can process the retention rules in the following ways:

- Adding the TMSEXPDT utility to the daily maintenance procedure.
- Using the Real-time Expiration feature.

The TMSEXPDT utility processes the entire TMC sequentially, updates eligible records with EXPDTs from matching RDS rules, and creates reports.

Real-time Expiration performs the same checks as TMSEXPDT does. If the tape is going through abend close, the abend status is considered when searching the RDS rules. If the updated expiration date is higher than all previous dates on the tape, it is propagated to the volume record to help ensure the highest requested retention. The resulting expiration dates are the same as the dates assigned by TMSEXPDT, but the final retention is established during tape creation and is immediately available to users and to any product interfaces.

Real-time Expiration can be easily implemented by restarting CA 1 with a TMSRDS DD statement in the TMSINIT procedure, pointing to the RDS data set. In multi-system environments, the feature should be implemented on all systems sharing the TMC, and all systems should use the same retention data set.

Note: For more information about the Real-time Expiration feature, see the *Utilities and Reports Reference Guide*.

Use External Data Managers

Use the External Data Manager (EDM) feature to manage tapes for products such as CA Disk or IBM DFSMShsm 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—for z/OS storage management
- CA Disk Backup and Restore—for z/OS storage management
- CA Dispatch—for z/OS report distribution and management
- CA ASM2 Backup and Restore—for z/OS storage Management

Within the CA 1 TMC, 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. They will be kept with an EXPDT of PERMANENT. The EDM must notify CA 1 when each tape should be expired and scratched by calling an exit, ARCTVEXT. This exit is distributed with CA 1 and is always present when the CA 1 CTAPLINK library is part of the linklist.

EDM rules are set up in the CTAPOPTN library in the member *TMOEDMxx.* 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 program name in the rule (using the PGM= parameter), you may need to write multiple rules. If the program that creates the tape and the program that releases the tape are different, you need to have at least two rules. The EDMid must be the same for all of the rules for that product.

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

Enable Security Processing

Enable CA 1 security options to protect data on tape.

Business Value:

If the security options are not enabled and the security rules are not in place to protect certain resources, any data set on tape can be read and even updated regardless of the data set name rules that can be in effect. Tape volumes can be overwritten resulting in data loss. Enabling the security options protects your data and helps you achieve the security compliance goals ot your company.

More Considerations:

Enable the Data Set Name checking for tape data sets. Using any of the following ways you can enable this option:

- External Security System (CA Mainframe Security Suite for ACF2, CA Mainframe Security Suite for Top Secret, and IBM RACF). Five CA 1 Health Checks have been created to raise exceptions if the security settings do not meet best practice recommendations.
- DEVSUP*xx* in SYS1.PARMLIB
- OCEOV = YES in CA 1 CTAPOPTN

To control the READ and UPDATE access to the appropriate resources, enable the following options in the CTAPOPTNS member TMOOPT*xx* and put the security rules in place:

- YSVC = YES or EXT (Y-SVC external security parameter)
- FUNC = YES or EXT (FOREIGN/BLP/NL/NSL external security parameter)

The HDR1 tape label on a tape data set contains only the last 17 characters of the data set name. However, CA 1 maintains and verifies the full 44 characters of the data set name. When the YSVC and FUNC options are not enabled, anyone who is authorized to bypass CA 1 (by using EXPDT=98000, for example) can read any data set in the tape library by spoofing the data set name in their JCL.

Note: For more information about other security options and the security resources that to define and restrict, see the *Programming Guide*.

Use the Graphical Management Interface (GMI)

Use the CA Graphical Management Interface (CA GMI) to view and monitor CA 1 activity.

Business Value:

CA GMI is CA's graphical management interface product that allows you to view and manage CA 1 activity from a Windows PC. CA 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:

CA 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 CA 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.

CA GMI is included free of charge with many CA products, including CA 1.

Note: For more information about CA GMI for CA 1, see the *CA 1 CA GMI Guide*.

Note: For more information about GMI for CA 1, see the *CA 1 CA Vantage GMI User Guide*.

Monitor the CA 1 Health Checks

Monitor the health checks generated for CA 1.

Business Value:

Health Checks alert you of conditions that could prevent CA 1 from running properly if left uncorrected, and they guide you in addressing the problem. These health checks provide best practices for running CA 1.

More Considerations:

The following health checks are provided for CA 1:

CA1_AUDIT_VRFY_WITHIN_LOW_THRSH

Monitors space in the CA 1 Audit file to help ensure that sufficient space is available to log all tape activity.

CA1_AUDIT_VRFY_WITHIN_MED_THRSH

Monitors space in the CA 1 Audit file that is triggered after no steps were taken to address the problem that the low threshold check identified.

CA1_FREE_DSNB_LOW_THRSH

Monitors the availability of free DSNBs as a percentage of the total number of DSNBs defined in the TMC. This first, low threshold check provides an early notification that DSNBs are being used up.

CA1_FREE_DSNB_MEDIUM_THRSH

Alerts users that they can be running short on free (unused) DSNB records in the TMC. This check is the secondary medium threshold check.

CA1_FREE_DSNB_QUICK_SCAN

Inspects the first *n* number of DSNBs in the free DSNB chain to help ensure that none of them are found to be in use.

CA1_TMC_AUDIT_PLACEMENT

Helps ensure that the CA 1 TMC and Audit data sets are placed on different volumes.

CA1_USED_DSNB_FREE_CHAIN

Inspects the free (unused) DSNB chain for any active (used) DSNBs; however this check scans the entire free chain. This check is similar to the CA1_FREE_DSNB_QUICK_SCAN check.

CA1_VRFY_OPTION_DCHG

Identifies possible problems that are associated with dynamic label change processing based on the CA 1 System Option DCHG.

CA1_VRFY_OPTION_LCHG

Identifies possible problems that are associated with changing a label type based on the CA 1 System Option LCHG.

CA1_VRFY_OPTION_TCHG

Identifies possible problems that are associated with changing the dynamic tape recording technique based on the CA 1 System Option TCHG.

CA1_VRFY_MIXED_EXPDT_OPTION

Alerts users of situations where the mixing expiration date is being done so that it can be followed up and corrected.

CA1_VRFY_SECURITY_EXIT_FUNC

Warns users that basic security setup has not been performed to protect the assets on tape. This exposure is associated with the setting of the CA 1 System Option FUNC. This feature controls the security checking to be done in the real-time nonresident (foreign) and label processing areas.

CA1_VRFY_SECURITY_EXIT_PSWD

Raises an exception when it finds that security has not been set up for the CA 1 ISPF panels.

CA1_VRFY_SECURITY_EXIT_YSVC

Verifies that access to the TMC is protected by the setting of CA 1 System Options YSVC and BATCH and rules in the external security system.

CA1_VRFY_SECURITY_PROFILE_TAPE

Warn users that basic security setup has not been performed to protect against unauthorized access to tapes. This exposure is associated with defining resource class CA@APE. If the external security is set to IBM RACF but the CA@APE resource class is not defined, tape jobs begin to fail.

CA1_VRFY_SECURITY_PROFILE_CMD

Warn users that basic security setup has not been performed to control access to tapes and commands. This exposure is associated with defining the resource class CA@MD. If the external security is set to IBM RACF but the CA@MD resource class is not defined, users are not able to issue commands in the CA 1 ISPF panels.

Note: For more information about health checks, see the *Administration Guide*.