CA TPX™ Session Management

Best Practices Guide

Release 5.3

CA Technologies Product References

This document references the following CA Technologies products:

- CA TPX™ Session Management (CA TPX)
- CA Mainframe Software Manager (CA MSM)

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, 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 7) — Streamlined and improved.
- Your Product Installation and Configuration Best Practices > Implement a proactive Preventive Maintenance Strategy (see page 9) — Added to the guide.

Contents

Chapter 1: Introduction

This section contains the following topics:

Audience

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

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, and so on).

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 in a manner that is consistent with industry best practices and your site-specific requirements. Our philosophy focuses on two maintenance types. Understanding each of these types can help you maintain your systems in the most efficient manner.

Note: This philosophy applies to the CA Next-Generation Mainframe Management stack 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. CA Technologies may provide a test APAR if a new problem is uncovered, or a confirmed PTF if the problem has already 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 CA Technologies has created and made public. You may or may not have experienced the issues that each PTF addresses. CA RS provides a way to easily identify published maintenance that has been successfully integration-tested with other CA Technologies products, current z/OS releases, and IBM subsystems, such as CICS and DB2. Major CA RS service levels are published quarterly, with updates for HIPER and PE-resolving PTFs that are published monthly. After you test the CA RS level, we recommend that you accept that level before you apply a new CA RS level.

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

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

More Information:

For the steps 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

The following section explains the best practices for installing CA TPX for optimal performance.

Use CA MSM

Use the CA Mainframe Software Manager (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 TPX.

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.

More Information:

For more information about CA MSM, see the *CA Mainframe Software Manager Product Guide*.

Use Electronic Software Delivery

Download the product and maintenance releases using Electronic Software Delivery (ESD). Although CA MSM is the preferred method for installing your CA mainframe products, some sites may decide to use ESD method instead.

Business Value:

ESD lets you download the product and maintenance releases over the Internet directly to your system from the CA Support website. When you order the product, you receive the authorizations and instructions to access, download, and prepare the installation files without the need for a physical tape. Thus, ESD is timelier, cost-effective, and environment friendly.

It uses standard z/OS utilities to prepare the product installation image on your system.

More Information:

For sites who have decided to use ESD, download the installation files from ca.com/support and install directly from your disk.

For information on the steps to download your CA products from the CA Support Online web site for installation using the enhanced ESD pax process, see the *Mainframe Enhanced Electronic Software Delivery guide* posted on the Download page of support.ca.com.

Install CA TPX on Test System

Before installing CA TPX on production system, perform your installation and initial evaluations of the product and its components on a test system.

Business Value:

Evaluating CA TPX in a test environment helps you detect any possible problems before you roll out the product to a production system. New releases of CA TPX are always compatible with previous releases, letting you run a new release on a test system while still running the older version on a production system.

Use Latest Version of CA Common Services

Make sure you have installed the latest version of CA Common Services.

Business Value:

The latest release of CA Common Services contains the latest infrastructure updates. These updates let you use the latest features, and prevents potential errors that can occur from using out-of-date services.

More Information:

For more information about CA Common Services, see the *Installation Guide*.

Configuration

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

Use Latest Version of CA TPX

Check that you are running the latest version of CA TPX.

Business Value:

To obtain full support from CA Support, you must run a supported version of the product.

To determine the release you are running, start a session to TPXOPER. The release is displayed in the top right-hand corner of the initial TPXOPER screen.

```
TPX11B - CA11 ************* TPX Operator      ************* 5.3/00 TEN0200
```

Apply High Priority PTFs

Apply all high priority PTFs. Check regularly for recent maintenance.

Business Value:

Being current on maintenance avoids system failures, makes problem resolution go smoothly, and maximizes your investment by providing access to the latest features and functionality of CA TPX.

Install Latest Version of IBM APARs

Install all of the latest IBM APARs appropriate for your environment.

Business Value:

If pertinent APARS are missing, it may impact the operation or performance of your CA products.

Additional Considerations:

We recommend that you review our current list of IBM APARs and apply only those that are appropriate to your environment.

More Information:

The list of IBM APARs is documented in TPX APAR QI05737 and can be accessed from Support Online.

Separate User Code from CA Delivered Software

Create a separate library for user-created code. It should be concatenated ahead of the CA delivered library. For example, custom exits should be assembled and kept in a separate library concatenated ahead of the CA TPX Load library (CB0VLOAD). Similarly, any customized panels or libraries can be saved in separate library.

Business Value:

By saving your customizations in a separate library, you can easily:

- Identify customizations that need to be ported to a new release
- Fallback to the CA version of a module or member

Additional Considerations:

- Always reassemble the exits with new release libraries.
- Always compare customized items to see if the original delivered version has been changed in the new release.

  For example, if you have customized a specific panel, compare the earlier version of that panel from CA with the same panel from the new release.

  Note: If CA has made changes to the panel then you will need to implement those in your custom version too.

Reassemble User Exits During Release Upgrade

Always re-assemble user exits when migrating to a new release of CA TPX.

Business Value:

Reassembling the user exits when upgrading the product, will help to avoid potential failures and loss of productivity.

Additional Considerations:

New releases of CA TPX are packaged with the required macro libraries that are needed for reassembling the customized user exits.

A sample JCL is also included to assist in the assembling of the user exits and is available in the SAMPLIB (CB0VSRC) member ASMUXIT.

Re-evaluate SMRT Defaults After An Upgrade

Take advantage of new parameters and improved default settings by evaluating the differences in the new release with the previous release.

Business Value:

With a new release of TPX, there may be new fields added to the SMRT or there could be changes to the recommended values of existing SMRT fields such as slot pool sizes.

Additional Considerations:

If you apply no changes to your SMRT in the new release, the defaults for any new fields introduced since your prior release will be retained.

To compare your existing SMRT with the new release defaults

1. Take screen prints of each SMRT panel in your existing release.
2. Create a new SMRT in the new release.
3. Take screen prints of the SMRTs. These screen prints have the recommended default values.
4. Compare the SMRTs to identify the new fields and their defaults, or identify where your SMRT differs form the recommended values.

Set Up CA TPX to Create SVC Dumps

Set up CA TPX so that SVC dumps are created when abends occur. SYSUDUMPs usually do not provide adequate information for problem investigation. You may need to remove the SYSUDUMP DD from the delivered TPXPROC.

Note: Verify the requirements within your own environment.

Business Value:

You do not need to wait for the reoccurrence of the problem to capture the required dump for diagnosis.

Additional Considerations:

Whenever sending a dump to CA for TPX, the corresponding TPX started task log is also required.

Performance and Maintenance

The following section explains the best practices for optimal performance of CA TPX.

Backup CA TPX VSAM Files

Backup CA TPX VSAM files periodically.

Business Value:

Backing up the VSAM files provides a recovery point if the active VSAM files become unusable.

Additional Considerations:

All CA TPX regions which access the VSAM files being backed up should be taken down while the backups are being run.

Regular VSAM Maintenance for CA TPX VSAM Files

Use VSAM tools such as the IDCAMS utility on a regular basis.

Business Value:

This preventative maintenance can help avoid corruption of VSAM files and improve performance by removing excessive CA/CI splits, for example.

This recommendation is a general VSAM best practice that is important for CA TPX.

Additional Considerations:

Frequency of this maintenance will depend upon the amount of change activity. A REORG using the IDCAMS utility should include:

- Taking a backup of the VSAM file beforehand
- Performing a DELETE or REDEFINE of the VSAM cluster
- Restoring the VSAM file from the data portion of the backup file; letting the INDEX be rebuilt to cut down on possible VSAM INDEX corruptions

This preventive maintenance procedure (REORG) mitigates Control Area(CA) and Control Interval(CI) splits and VSAM file corruption.

Note: If the CA or CI splits are excessive even after a REORG has been done, increasing the FREESPCE parameter in the VSAM cluster DEFINE will help to alleviate this problem. Excessive CA/CI splits most typically occur during a new install when performing a high volume ADD maintenance activity for information stored on the CA TPX VSAM files. You can lower the FREESPCE parameter when the high volume of activity has ended.

When you are performing a REORG of your CA TPX VSAM files, you should first review the DASD definitions and make sure the current definitions are still adequate for the volume of data stored on each CA TPX VSAM file. If you are at or near the maximum space capacity, you should increase your DASD specifications so that the next VSAM REORG *DEFINE* of the cluster reflects the new DASD specifications or requirements for the VSAM file.

Sample JCL members for CA TPXVSAM file backup (VBACKUP/LSBACKUP*), file restore from file backup (VRESTORE/LSRESTOR*) and cluster definition (VADMIN1/VADMIN2/VMAIL/VNOTES/VVIEW) can be found in the CB0VJCL library.

Note: If your CA TPX VSAM files are managed by LSERV, refer to member $INDEX for a list and definition of subsequent members provided in the CB0VJCL library.

We also recommend that you run the CA TPX Batch Reset Integrity process (refer to library SAMPLIB, member BATCHINI for sample JCL) after any CA TPX VSAM file REORG/restore process before starting CA TPX.

Adjust Timeout Parameters in SMRT Option 4

Timeout Parameters in SMRT option 4 need to be carefully adjusted to take advantage of the functionality provided by this parameter.

Business Value:

It is good practice to setup *session timeouts* properly. It helps avoiding situations where users tend to ignore closing application sessions at the end of usage or work day. The values, if applied properly can enforce a clean shut down of user sessions and eliminates any need for VTAM / TPX inconsistencies. They should be applied prudently keeping in view, environmental requirements and what organizational policy dictates. This is very useful in facilitating proper TPX administration and reducing overheads.

Additional Considerations:

All timeouts should be tested and applied prudently so as not to adversely impact user productivity but at the same time enforce security, standards and organizational needs and requirements.

Add Virtual Terminals and Printers in a 24x7 Environment

Add virtual terminals or virtual printers while CA TPX is running.

Business Value:

The TPXOPER VTADD command can add virtual terminals or virtual printers to CA TPX dynamically without recycling CA TPX for the changes to take effect.

Additional Considerations:

VTADD is a method to dynamically add virtual terminals. Use the VTADD command when all of the currently defined virtual terminals are in use and more than those virtual terminals defined in the TPX startup VTAM node are required. This TPXOPER command eliminates the need to recycle tpx.

To add virtual terminals and printers

1. Build a new VTAM member to define the new additional GROUP and/or UNIQUE virtual terminals as shown in the following screen:

```
TPXNEW VBUILD TYPE=APPL
*TPX,UNIQUE DO NOT REMOVE - THIS COMMENT IDENTIFIES UNIQUE VIRT TERM\
*
Z44IJSU0 APPL MODETAB=ISTINCLM,DLOGMOD=T3278M2,SRBEXIT=NO,EAS=1
Z44IJSU1 APPL MODETAB=ISTINCLM,DLOGMOD=T3278M2E,SRBEXIT=NO,EAS=1
Z44IJSU2 APPL MODETAB=ISTINCLM,DLOGMOD=T3278M3,SRBEXIT=NO,EAS=1
*     END OF UNIQUE VIRTUAL TERMINALS
*
*TPX,GROUP DO NOT REMOVE - THIS COMMENT INDENTIFIES GROUP VIRT TERM
*
Z44IGRU0 APPL MODETAB=ISTINCLM,DLOGMOD=T3278M2,SRBEXIT=NO,EAS=1
Z44IGRU0 APPL MODETAB=ISTINCLM,DLOGMOD=T3278M2E,SRBEXIT=NO,EAS=1
Z44IGRU0 APPL MODETAB=ISTINCLM,DLOGMOD=T3278M3,SRBEXIT=NO,EAS=1
*     END OF GROUP VIRTUAL TERMINALS*
```

2. Vary the new member ACTIVE in VTAM.
3. Use TPXOPER to issue the VTADD command (VTADD TPXNEW) to add the newly created VTAM member TPXNEW.

Prevent User Administrators from Controlling Profile and User Security

Setting the *Only Master and System Admin. can update profile/user security:* parameter in the SMRT table disallows User Administrators from controlling Profile and User Security.

Business Value:

Setting this parameter to *Y* prevents the lower level administrators from updating the security changes. It helps the security administrators to enforce strict policies.

Additional Considerations:

To implement the *Only Master and System Admin. can update profile/user security:* parameter

1. Logon to TPXADMIN.
2. Select Option 2 (TPX System Options).
3. Select Option 1 (System Options).
4. Select the active (STARTUP) SMRT table.
5. Select Option 9 (Security Parameters).
6. Enter Y in the Parameter field .
7. Reload the SMRT table in TPXOPER (cmd: RELOAD SMRT=tablename).

Review the List of TPX Knowledge Documents

Review the list of TPX knowledge documents on a regular basis.

Business Value:

The TPX knowledge base contains a broad variety of knowledge documents, for categories such as installation, customization, optimization, problem determination and resolutions.

Additional Considerations:

To find CA TPX knowledge base documents

1. Log on to CA Support Online.
2. Select Knowledge Base Search.
3. Enter TPX as a keyword.
4. Click Search.

Adjust Slot Pool Percentages in SMRT

The partition of storage into several Slots in SMRT Option 2 (below 16MB) and 3 (above 16MB) need to be reviewed and adjusted to your installation's needs to have a well maintained usage of storage.

Business Value:

It is good practice to have a well maintained partition of the Storage into the available Slots. The default storage settings, provided in each release, allow CA TPX to start when initially installed. As every installation differs, you need to check the settings of the SMRT by using display Commands D STOR and D STORXA respectively. Depending on their result, you need to change the Slot parameters in the SMRT.

Additional Considerations:

We recommend that you change the percentage used by the slot pools and do not change any slot sizes. The percentages must add up to 100%.

Slot pool overflow messages (TPB300 or TPX300) should be monitored. One slot overflowing is not generally a problem because TPX will start to use space from another pool. When two or three slot pools overflow, you can get into performance degradation and you should consider adjusting the slot pool percentages. Take 1-2% from a pool with lowest of the maximum value and give it to the pools that overflowed.

Note: If you have one pool that consistently overflows, then it should receive attention.

You might use the concept of an Opengate User to get regular reports on storage usage.

More Information:

For more information, see our technical document TEC424715.