CA Chorus™ Software Manager

Best Practices Guide

Release 5.1

First Edition

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2013 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following CA Technologies products:

- CA Chorus™ Software Manager (CA CSM)
- CA Datacom®

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 *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:

- Installation and Set Up Best Practices > Allocate Three Separate File Systems for Installation (see page 11): updated the topic to reflect the new file system structure
- Installation and Set Up Best Practices > Use System z Application Assist Processor (zAAP) (see page 13): updated the z/OS version
- Installation and Set Up Best Practices > Set Up USS File System and Directory Path (see page 22): updated the information about the USS file structure
- General Usage Best Practices > Hide Unwanted Products from the Software Catalog Tree (see page 31): added the topic

Contents

Chapter 1: Introduction

This section contains the following topics:

Purpose of This Guide

The guide describes the best practices for installing and setting up CA Chorus™ Software Manager (CA CSM), and how to use it to acquire, install, maintain, deploy, and configure your CA Technologies mainframe products.

Audience

The intended audience of this guide is systems programmers and administrators who install and set up CA CSM, and use it to install, maintain, deploy, and configure other CA Technologies mainframe products.

Chapter 2: Installation and Set Up Best Practices

This section contains topics to help you maximize your efficiency when installing and setting up CA CSM.

This section contains the following topics:

Allocate Three Separate File Systems for Installation

You must create four USS directory paths to install CA CSM. Although CA CSM can be installed with all four directory paths in a single file system, the recommended configuration is to create separate file systems for the msm, msmruntime, and msminstall directories. The mpm directory serves as a mount point for file systems that CA CSM creates and manages during operation.

Business Value:

Creating separate file systems for msm, msmruntime, and msminstall allows the space that is used for the CA CSM installation files to be reclaimed once the installation is completed. This represents approximately 2500 cylinders of DASD space.

Additional Considerations:

The use of separate file systems also eliminates single point-of-failure for the application by separating the CA CSM SMP/E USS environment from the application runtime USS environment.

More Information:

See USS File Systems in the *Administration Guide* for more details about the USS file system requirements.

Implement Using zFS File Systems

Although CA CSM can support both HFS and zFS file systems, we recommend using only zFS file systems for both the installation file systems, as well as the ongoing application file systems, because of the superior performance of zFS over HFS.

Business Value:

IBM announced that, beginning with z/OS 1.7, zFS is the strategic z/OS UNIX file system. IBM also formally recommends that you use zFS file systems and migrate all existing HFS file systems to zFS. Installing CA CSM with zFS file systems eliminates the need to migrate CA CSM from HFS to zFS at a later date. This migration activity includes steps to update the CA CSM internal mount table that resides in the CA CSM database CA Datacom/MSM. The zFS file system also has higher performance characteristic than HFS and will create better performance and throughputs than HFS.

Additional Considerations:

In order to implement using zFS file systems, you must verify that the zFS address space is running and configured for your environment. For a zFS file system to grow dynamically, you must specify AGGRGROW when you mount the file system. This can be set globally for all zFS file systems using the IOEFSPRM member of SYS1.PARMLIB.

More Information:

See the *IBM UNIX System Services Planning Guide* (z/OS release specific) and the *IBM HFS to zFS Migration Tool Redbook* (REDP4328.pdf) for more information. You can also reference the *IBM z/OS Distributed File Service zSeries File System Administration* for more details on setting up the zFS address space for your environment.

Install CA CSM on a Multiprocessor LPAR

Although CA CSM can run on any LPAR configuration, we recommend an LPAR that has at least two CPUs configured.

Note: CA CSM takes advantage of the zAAP processor, which may help increase general purpose processor productivity and contribute to lowering the overall cost of computing for z/OS Java technology-based applications.

Business Value:

CA CSM is an online application that runs three address spaces (MSMMUF, MSMDBSRV, MSMTC). Configuring multiple CPUs allows multiple instructions to be processed, ensuring less CPU wait delays, and improving overall response times for CA CSM users.

In a uniprocessor LPAR configuration, CA CSM users may experience significantly slower response time, which reduces some of the productivity gain that the tool provides.

Use System z Application Assist Processor (zAAP)

CA CSM uses IBM System z Application Assist Processors (zAAPs) to help you realize the following benefits:

- Simplify and reduce server infrastructures by integrating Java web applications mission critical data for high performance, reliability, availability, and security.
- Maximize the value of your mainframe investments through increased system productivity by reducing the demands and capacity requirements on general purpose processors which may then be available for reallocation to other mainframe workloads.
- Lower the overall cost of computing for Java technology-based applications, through hardware, software, and maintenance savings.

If you use z/OS V1.11 or later with IBM z Integrated Information Processors (zIIPs) installed, you can also use the zAAP on zIIP capability that brings the same benefits.

Business Value:

CA CSM is an online application that uses System z Application Assist Process (zAAP) to simplify and maximize performance and lower overall cost.

Use SMS for Allocations

Although CA CSM supports both non-SMS and SMS allocation environments, we recommend using only SMS for mount point management allocations and software installation temporary allocations.

Business Value:

CA CSM dynamically allocates temporary files during task initialization and GIMUNZIP processing for software installations. It also dynamically allocates new file systems as needed to store the product and maintenance files that are downloaded from the CA Support Center. All of these allocations are performed based on the configuration settings in the CA CSM web-based interface (Settings tab, User Settings). Setting these allocations up under SMS eliminates the need for someone to actively manage the CA CSM Settings based on individual volume utilization.

SMS also helps ensure optimal space utilization and to verify that the appropriate backup and migration rules are used for these data sets.

Additional Considerations:

The initial settings for the file system allocations are specified during the installation process, and can be easily modified in the CA CSM web-based interface (the Settings tab, System Settings).

The allocation settings for the temporary data sets must be set after the installation is complete and the CA CSM web-based interface is accessible. The interface allows for a system setting and a user-specific setting for these allocations. The user setting will override the system settings when they are populated. The system settings *should* be set by the first user who accesses the application. Each individual user can set their own user settings as needed for their environment. User settings for these parameters are only recommended if the security environment dictates different settings for each CA CSM user.

More Information:

For more information about the allocation settings, see the *Administration Guide*. In addition, see the *IBM DFSMS Implementing System-Managed Storage* for information about your specific z/OS release.

Reserve Application Ports in TCP/IP

CA CSM uses four TCP/IP ports that need to be reserved to the CA CSM address space for the CA CSM application server.

Business Value:

Reserving the four CA CSM application ports to the MSMTC address space helps to ensure that another application does not allocate the ports and prevent CA CSM from being accessible.

These ports are defined in several CA CSM configuration files under USS. These files are in XML format and are not easily modified using traditional z/OS utilities.

The process of reserving the ports also enhances the network team's ability to perform problem isolation in the environment.

More Information:

See the *Administration Guide* for more information about the application port requirements. In addition, see the *IBM IP Configuration Guide* for your z/OS release for further details about reserving ports in TCP/IP.

Define Address Space User IDs in System Programmer USS Group Profile

The CA CSM address spaces should be assigned a user ID that is defined to the same USS default group profile as the team of system programmers responsible for maintaining the application.

Business Value:

Adhering to this best practice helps you simplify the USS permissions structure that is required for ongoing support and can eliminate the need to set CA CSM USS directory path permissions to read/write/delete/execute. The owning UID/GID must be the one that allows deployment users the ability to have read/write/execute within that work directory.

More Information:

See the *Administration Guide* for more information about the application address space security setup requirements. You can also refer to your security package administration guide.

Accessibility for Temporary Unpax Directory for GIMUNZIP

CA CSM requires a USS directory path to temporarily unpax product package files during a product installation. This USS directory path needs to be accessible by all CA CSM users.

Business Value:

The system setting for the required temporary unpax location must be set in the CA CSM web interface (Settings tab, System Settings, Software Installation) after CA CSM is initialized for the first time. This setting is used by all CA CSM users during a product installation and therefore has to be set to a directory path that all CA CSM users can write to, read from, and execute on. If there are security policies in your environment that do not let all users have access to the same directory path, those without access to the path set here must specify a different directory path in the CA CSM web interface (Settings tab, User Settings, Software Installation). The user setting overrides the system setting for the user.

More Information:

See the online help for more information about the Settings tab.

Back Up Installation Options File and Summary Report

The CA CSM installation USS directory path can be deleted after the installation is completed, but there are two files that you should back up before deleting this directory path. The files are located in the following path:

/parent_path/msmserv/*version_number*/msminstall/MSMSetup

where *parent_path* is the CA CSM parent path name defined at your site, for example, one of the following:

```
/u/users/
/usr/lpp/
/cai/
```

The following files are the files that you need to back up:

MSMSetupOptionsFile.properties

The CA CSM installation process uses the MSMSetupOptionFile to customize the installation based on your environment. This file contains all of the information that would be required to reinstall in the event of a disaster, or to install on another LPAR within your environment. We recommend creating a backup of this file (either in another USS directory or in a z/OS data set).

MSMSummaryReport.txt

The installation script creates a summary report of the installation that includes critical information about the installation. This information is a good reference document and can be used for identifying information about the files being used, as well as the URL required to access the application. We recommend creating a backup of this file (either in another USS directory or in a z/OS data set).

Business Value:

This helps ensure you are prepared to recover CA CSM in the event of a disaster.

More Information:

See the *Administration Guide* for more information about the installation MSMSetupOptionsFile.properties and MSMSummaryReport.txt files.

Disable SAF Security on Initial Startup

CA CSM includes functionality that lets you control access to CA CSM, as well as to specific functions within CA CSM. We recommend that you disable this functionality when you start CA CSM for the first time.

This functionality is controlled through the safSecurity keyword in the MSMSetupOptionsFile.properties used during the installation process. It can be enabled after the installation by updating the following statement in the SAMPLIB(MSMLIB) member:

```
IJO="$IJO -Dactivate.saf.manager=false|true"
```

false

Disables security.

true

Enables security.

Business Value:

The CA CSM security functions are established and managed using resource profiles defined in your enterprise security manager software. The setup requires an extensive understanding of the CA CSM functionality and how the product will be used to manage software, but the additional security administration work may be unnecessary in your environment. This security functionality also adds an additional level of complexity to the CA CSM installation.

We recommend you disable this security functionality until the product has been thoroughly verified.

More Information:

See the *Administration Guide* for more information about setting up user security for CA CSM functions.

Enable Automount for Mount Point Management

CA CSM dynamically creates and mounts these file systems as needed to manage space required for downloaded products and maintenance files. These file systems and their associated mount points are maintained in an application mount table in the CA Datacom/MSM database. The Automount setting specifies whether the MSMTC address space will mount these file systems at initialization. We recommend that Automount for Mount Point Management should always be enabled.

Business Value:

CA CSM dynamically creates file systems and manages them. It is essential that all of these file systems be mounted and available under USS for CA CSM to function correctly. The Automount setting directs the CA CSM Mount Point Management Services to verify that all of these file systems are mounted during initialization. If the file systems are not mounted, the Mount Point Management Service mounts them according to the application mount table during initialization. This verification ensures that CA CSM will have access to all of the required file systems and will prevent application failures.

This application parameter is initially set during the installation process using the mpmAutomount keyword in the MSMSetupOptionsFile.properties file used. It can be changed in the web-based interface (Settings, System Settings, Mount Point Management).

Additional Considerations:

CA CSM can also unmount all of the application file systems whenever the application shuts down. This functionality is controlled using the web-based interface (Settings, System Settings, Mount Point Management).

More Information:

See the online help for more information about the Settings tab.

Run Prerequisite Validator Before Installing CA CSM

We recommend that you install and execute the CA CSM Prerequisite Validator utility on the LPAR where you intend to install CA CSM before beginning the CA CSM installation.

Business Value:

CA CSM includes a Prerequisite Validator utility that lets you verify that all software, network, and security authorizations are in-place on the LPAR where you will install CA CSM. The utility produces a Verification Summary report that identifies any gaps from the CA CSM installation prerequisites. This report can be used in the planning process and identifies any additional activities that must be performed before CA CSM can be successfully installed.

You should verify that all issues identified by this utility are addressed before installing CA CSM.

More Information:

For more information, see the *Administration Guide*.

Use Customized JCL for Initial Startup

The CA CSM installation script creates customized jobs (JCL) and cataloged procedures (PROCs) for each of the three CA CSM address spaces. These address spaces should be started as jobs during the initial startup after the installation script completes, and the jobs should be submitted by the same user who executed the installation script.

Business Value:

The security requirements for the user ID executing the CA CSM installation script are the same as the requirements for the three CA CSM address spaces. By initially starting CA CSM as jobs using this user ID, you eliminate the need to introduce additional security settings before completing the installation verification, which will simplify problem determination and resolution.

After the installation verification is completed, we recommend running the CA CSM address spaces as Started Tasks, and moving the customized PROCs created by the installation script to an appropriate PROCLIB in your environment.

More Information:

For more information, see the *Administration Guide*.

Reorganize Database

After you apply maintenance to your product using CA CSM, we recommend that you reorganize your database. Reorganizing your database improves overall access to data the next time you use CA CSM. Use the database reorganization backup and load process to reclaim space and reposition data.

Follow these steps:

1. Stop the CA CSM application server.
2. Stop the CA Datacom/MSM server (MSMDBSRV) by using the MSMDBSRP job.
3. Verify that your CA CSM Multi-User Facility (MSMMUF) is active.
4. Review and edit the B4KBKUP member to reflect your naming standards.
5. Submit the job B4KBKUP.

   The job B4KBKUP creates a current backup of the CA Datacom/MSM database 4000 to a sequential file on the disk.
6. Review and edit the B4KLOAD member.

   Edit the JCL so that it conforms to your site standards, verifying that the input data set matches the output data set created in the previous step.

   Important! You must execute the job B4KLOAD immediately following the job B4KBKUP.
7. Start the CA Datacom/MSM server (MSMDBSRV).
8. Start the CA CSM application server.

Business Value:

Using this best practice can help you improve database response time, CPU time, and the number of I/O operations.

Additional Considerations:

A database reorganization (execution of a backup followed immediately by a load) against a database that has little fragmentation (indicated by a low value count in the output display named OVERFLOWS IN AREA of a current CXX report) does not result in a measurable improvement in performance.

More Information:

For more information, see the *CA Datacom/DB Database and System Administrator Guide*.

Set Up UNIX File System and Directory Path

We recommend that you set up your z/OS UNIX System Services (USS) file system and directory path as described in this topic.

USS Directory Path Structure

CA CSM uses the following z/OS UNIX System Services (USS) directory path structure:
/parent_path/msmserv/mpm
/parent_path/msmserv/*version_number*/msm
/parent_path/msmserv/*version_number*/msmruntime
/parent_path/msmserv/*version_number*/msminstall

Note: The /mpm directory should not have a version number. This is a common directory that is shared between CA CSM versions.

***/parent_path*/msmserv/**

Specifies the CA CSM parent path name as defined at your site as the primary mount point or directory, for example, one of the following:

```
/u/users/msmserv
/usr/lpp/msmserv
/cai/msmserv
```

Note: We recommend that you use /msmserv as the final portion of the parent path; however, you can change it if necessary for your site standards.

***/parent_path*/msmserv/mpm**

Specifies the mount point for file systems that CA CSM allocates and mounts. The mount point is the directory that CA CSM uses to mount the software catalog root application file system. You specify this path in the MountPath keyword of the options file.

Note: If you are an existing CA CSM customer and are upgrading, you do not need to create this path. The upgrade process reuses the previous version path by default.

/parent_path*/msmserv/*version_number

Specifies the parent directory for all version-specific data, when using the multiple file system structure.

Note: We recommend that you set up your USS file system using a multiple file system structure.

***/parent_path*/msmserv/*version_number*/msminstall**

Specifies the directory for CA CSM installation data, including all downloaded and unpacked CA CSM files.

Space: 1000,100 cylinders

Note: This directory can be deleted after the installation is completed.

***/parent_path*/msmserv/*version_number*/msm**

Specifies the directory for target USS files for CA CSM products. The content is managed through SMP/E.

Space: 750,100 cylinders

***/parent_path*/msmserv/*version_number*/msmruntime**

Specifies the directory for CA CSM runtime files, that is, the directory that the running CA CSM application executes from. You specify this path in the RunTimeUSSPath keyword of the options file.

Space: 750,100 cylinders

Recommended Guidelines

We recommend that you use the following settings and adhere to the following guidelines:

- Use a CA CSM parent path name as defined at your site, for example, one of the following:

  ```
  /u/users/msmserv
  /usr/lpp/msmserv
  /cai/msmserv
  ```

  Note: We recommend that you use /msmserv as the final portion of the parent path; however, you can change it if necessary for your site standards.
- Configure the path name to meet your site needs.
- Set the permissions on these directories to 775.
- Mount the file system with the SETUID option.
- Although CA CSM supports either HFS or zFS, we recommend zFS (see page 12).
- For zFS file systems only, specify the mount parameter AGGRGROW, either explicitly on the mount command, or as default in the IOEPRM*xx* member.

Recommended Guidelines for New Installations

Note: If you are upgrading, skip this section and go to the next section.

- Structure your USS paths as multiple file systems to allow for upgrading from a previous version of CA CSM. Structuring the USS paths ensures that you have a single file system for each required directory path.
  - Create the directory /*release_number* as a child of /msmserv.
  - Create the following version-specific directories as children of /*release_number*:
    - /msm
    - /msmruntime
    - /msminstall
- Create z/OS file systems with the following space allocations and mount locations:
  - CYLS(750,100) mounted at /*release_number*/msm
  - CYLS(750,100) mounted at /*release_number*/msmruntime
  - CYLS(1000,100) mounted at /*release_number*/msminstall

  Total primary: 2500 cylinders
- Update the UNIX BPXPRM*xx* control member with each of the four file systems and associated mount points. For example:

```
MOUNT FILESYSTEM('dsnpref.release_number.ZFS.MSM')
      MOUNTPOINT('/parent_path/msmserv/release_number/msm')
      TYPE(ZFS)  MODE(RDWR) PARM('AGGRGROW')
MOUNT FILESYSTEM('dsnpref.release_number.ZFS.MSMINST')
      MOUNTPOINT('/parent_path/msmserv/release_number/msminstall')
      TYPE(ZFS)  MODE(RDWR) PARM('AGGRGROW')
MOUNT FILESYSTEM('dsnpref.release_number.ZFS.MSMRUN')
      MOUNTPOINT('/parent_path/msmserv/release_number/msmruntime')
      TYPE(ZFS)  MODE(RDWR) PARM('AGGRGROW')
```

  Note: Starting with Release 5.1, CA CSM does not use the msmtmp directory. If you are not reusing the msmtmp file system from the previous release in the latest release, you can remove the auto-mount entry from the SYS1.PARMLIB(BPXPRMxx) member:

```
MOUNT FILESYSTEM('dsnpref.ZFS.MSMTMP')
      MOUNTPOINT('/parent_path/msmserv/msmtmp')
      TYPE(ZFS)  MODE(RDWR) PARM('AGGRGROW')
```

- After installation completes, unmount the USS file system that is mounted at /*parent_path*/msmserv/*release_number*/msminstall and delete both the directory and file system.

Recommended Guidelines for Upgrade Installations

Note: If you are not upgrading, skip this section and go to the next section.

- Structure your USS paths as multiple file systems to allow for upgrading from a previous version of CA CSM. Structuring the USS paths helps ensure that you have a single file system for each required directory path.
  - Create the following directories as children of /msmserv:
    - /mpm
    - */release_number*
  - Create the following version-specific directories as children of */release_number*:
    - /msm
    - /msmruntime
    - /msminstall
- Create z/OS file systems with the following space allocations and mount locations:
  - CYLS(750,100) mounted at */release_number*/msm
  - CYLS(750,100) mounted at */release_number*/msmruntime
  - CYLS(1000,100) mounted at */release_number*/msminstall

  Total primary: 2500 cylinders

  For example:

  - To create zFS file systems, you can use the following sample JCL:

```
//S010  EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
 DEFINE CLUSTER (NAME(dsnpref.release_number.ZFS.MSM) -
 VOLUMES(??????) -
 LINEAR -
 CYL(250 50) -
 SHAREOPTIONS(3))
/*
//S020  EXEC PGM=IOEAGFMT,REGION=0M,COND=(0,LT),
// PARM=('-aggregate dsnpref.release_number.ZFS.MSM -compat')
//SYSPRINT DD SYSOUT=*
```

- To mount the file systems, you can use the following sample JCL:

```
//S030     EXEC  PGM=IKJEFT01,COND=(0,LT)
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
 MOUNT FILESYSTEM(' dsnpref.release_number.ZFS.MSM') -
       MOUNTPOINT(' /u/users/msmserv/release_number/msm') -
       TYPE(ZFS) MODE(RDWR) PARM('AGGRGROW')
/*
```

Note: dsnpref is the high-level qualifier of your z/OS data set name for this file system.

Additional Considerations:

If you are upgrading, you do not need to update the UNIX BPXPRM*xx* control member. In addition, do not change the MPM path after installing CA CSM. If you must change the MPM path, contact CA Support.

More Information:

For more information, see the *Administration Guide*.

Install Products in Same Zone as Common Components

The Software Configuration Service (SCS) requires that when you install a CA Technologies product that has its own set of common components, they should all be installed into the same SMP/E CSI zone. Otherwise, you will need separate instances of the common components for each of the products that are in different zones.

Note: A CA Technologies product that uses CA Common Services for z/OS does not have to be installed into the same SMP/E CSI zone unless the product documentation specifies so.

Business Value:

This can help you avoid errors when using the Software Configuration Service (SCS), and help save you time by not having to install and maintain separate instances of a CA Technologies product with its common components.

Using a single SMP/E CSI zone also ensures that the correct levels of products are in an operational situation that can be easily used for disaster recovery purposes, and save on DASD space at your site.

Additional Considerations:

If you are currently using a CA Technologies product with its components spread across several SMP/E CSI zones, you should consider using the SMP/E commands ZONECOPY or ZONEMERGE to create a single SMP/E CSI zone.

More Information:

Compare Working Set of SMP/E Environments against Software Catalog

You should use the SMP/E Environments section of the Software Status tab to review a defined working set of SMP/E environments against the maintenance available in the Software Catalog. The SMP/E Environments section displays an alert to the user if any of the SMP/E environments in their working set have maintenance available in the CA CSM Software Catalog that has not been installed.

Business Value:

CA CSM eliminates the need for you to manually identify what maintenance files have not been installed in your environment, freeing your time for more productive activities.

This also lets you easily assess the CA environment defined to CA CSM and ensure that the mainframe software is current. This simplifies this oversight responsibility and improves your ability to do project and staff planning related to CA software support.

More Information:

For more information, see the *User Guide*.

Chapter 3: General Usage Best Practices

This section contains topics to help you maximize your efficiency when using CA CSM to acquire and install the mainframe software at your site.

This section contains the following topics:

Design Your Environments Using CA CSM

You can use CA CSM to design, plan, and manage your mainframe environments.

You can do this using the following techniques:

- Deploy CA Technologies products using CA CSM.
- Deploy any nonexecutable files, such as readme, and data files, using the custom data set feature of CA CSM.
- Create an inventory matrix or map of all your systems and CA Technologies products that are in your mainframe environment. This will give you a map of systems that need to have products deployed to them.
- Categorize each system type into non-sysplex, sysplex, monoplex, shared DASD cluster, or staging system using your inventory matrix or map.
- Add to CA CSM System Registry only those systems in your environment that are your driving systems and those target systems that will receive the deployment.
- Use the validate procedure of the System Registry to define a system. This procedure will detect whether the system is a non-sysplex, monoplex or sysplex system.

- Maintain your system on a quarterly basis, except for hot fixes.
- During the methodology assignment in the deployment, use the Create Only feature when you deploy your products to environmental test systems, sandbox systems, staging systems, or products systems.

Business Value:

These procedures enable you to easily and accurately manage the deployment of your CA Technologies products with fewer manual steps and chances for errors. In addition, the manager responsible for your mainframe systems can use CA CSM to flexibly create and manage a mainframe system plan that scales to the organization environment.

More Information:

For more information, see the *User Guide*.

Run Update Product List Monthly

CA CSM lets you initiate a background process to populate and update the inventory of licensed products based on your site IDs. This process should be initiated at least monthly.

Business Value:

The Update Product List function automatically populates the CA CSM product catalog with the available releases and gen levels available from the CA Download Center for each of your licensed mainframe products. By running this task at least monthly, you help to ensure that you have awareness of all product packages as they become available. It also ensures that you have access to acquire these newly released products (releases and gen levels) using the CA CSM Product Acquisition Service.

Additional Considerations:

If you have multiple site IDs defined to your account on the CA Support Online website, CA CSM uses the site ID specified for the Login SiteId setting in your account profile on the CA Support Online website.

More Information:

For more information, see the *User Guide*.

Run Update Product Release Regularly

CA CSM lets you initiate a background process to download the product and maintenance files associated with a specific release for a licensed CA mainframe product. This process should be initiated on a periodic basis for each licensed product release installed to verify that all current maintenance is available to review and install.

Business Value:

CA CSM automates the acquisition of CA Technologies product and maintenance files to your mainframe system. This process compares your current CA CSM software catalog to what is currently available and downloads only what is missing. This process eliminates the need for someone to manually review the files available and manually transfer the files to your mainframe using FTP. By eliminating the manual effort, the support staff has more time to analyze the available maintenance and to easily install maintenance as needed. This will help you keep your CA Technologies mainframe products current and reduce the risk to your environment.

Additional Considerations:

Although CA CSM lets you initiate an Update Product at the product level, we strongly recommend *not* doing this because it downloads *all* product and maintenance files for all releases available in the CA Download Center for the selected product. This will potentially download releases that are older and possibly not needed, could cause confusion, and could significantly increase the space required for CA CSM USS file systems.

More Information:

For more information, see the *User Guide*.

Hide Unwanted Products from the Product List

You should hide a product, product release, or gen level from the product list when you know that you will not need or use them for a long time. When you hide a product, product release, gen level from the product list, CA CSM hides the corresponding entry from the software catalog and deletes associated packages from your system.

Business Value:

When you hide a product, product release, or gen level from the product list, CA CSM deletes associated packages from your system. CA CSM excludes hidden products, releases, and gen levels from processing when updating the product list. No packages are downloaded for hidden products, releases, and gen levels. This lets you free up DASD space on your system.

You can restore visibility of a product, release, or gen level that you previously hid from the product list. However, the associated files will only be downloaded again when a CA CSM user initiates an Update Product List task for that restored product, product release, or gen level.

The SMP/E environment for the product-release is not deleted using this function.

More Information:

For more information, see the *User Guide*.

Delete Unwanted Product Releases from Product List

You should delete a product release from the CA CSM Software Catalog when the product and maintenance files are no longer needed. When you use CA CSM to delete a product release, it deletes all of the USS files, directories, and file systems associated with the release.

Business Value:

When you delete the release from the CA CSM Software Catalog, CA CSM deletes all of the product files and maintenance files that CA CSM has downloaded. This ensures that CA CSM space utilization is kept at a minimum requirement for your environment.

The release will be added back to the Software Catalog on the next execution of the Update Product List task. However, the associated product and maintenance files will only be downloaded again when a CA CSM user initiates an Update Product task for that product or product release.

The SMP/E environment for the product-release is not deleted using this function.

More Information:

For more information, see the *User Guide*.

Establish Working Set of Product SMP/E Environments for Each User

Each CA CSM user should define a working set of product SMP/E environments.

You can put as many products as you need in an SMP/E environment, and when you deploy, you can pick which products to deploy at deployment time. You should place products in the same SMP/E environment for the following reasons:

- If the products have the common target and distribution libraries.
- If the products have unique target and distribution zones and libraries where the zone names are unique and there is no intersection in the DDDEF.

Business Value:

CA CSM gives each user the flexibility to establish and maintain their own working set of product SMP/E environments. This working set establishes the subset of SMP/E environments.

Each user can easily make changes to this working set as needed without concern over negatively affecting other users' working sets.

More Information:

For more information, see the *User Guide*.

Rerun Failed Tasks with Debug Logging

When a CA CSM task fails, we recommend that you turn on debug logging and redo the steps that led to the error.

Follow these steps:

1. Navigate to the Settings page and click the Change Diagnostic Log Level link in the Action area in the left pane.

   The Change Diagnostic Log Level dialog appears.

2. Set the following values, and click OK:

   Log Level

   Set to DEBUG.

   Reset the Log Level After the First Task Is Started

   Ensure that this check box is selected (default).

   Include Logs in the Task Output

   Select this check box.

   Task Logging Directory

   Specify the USS directory where log information is stored. The directory should have sufficient space for saving log files. Otherwise, no log information is displayed for new tasks in the task output browser.

3. Redo the steps that led to the problem.

   The details of the tasks you performed are saved to the task output browser. A dialog that shows the progress of the task opens. When the task completes, you can click Show Results on the Progress tab to close this dialog. The task output browser opens and you can view the action details. Click Close to close the task output browser.

   Note: While a task is in progress, you can perform other work. You can click Hide to exit the dialog and view the task status later on the Tasks tab.

4. Go to the Task tab, locate the new task with a Diagnostic Log entry, and export it to ZIP.

   The ZIP file is saved to your computer.

5. Open an issue on the CA Support Online website and attach the ZIP file to this issue.

   Note: You can review this file in preparation for your communication with CA Support.

Business Value:

Using this best practice can help save you time collecting the appropriate information when you encounter problems with CA CSM and are working with CA Support.

Additional Considerations:

After contacting support and resolving the issue, do the following:

- Consider deleting the task because it can take up valuable space in your CA Datacom/MSM database and USS directories.
- Purge logs files regularly because, depending on your settings, logs are written whenever a task is run by any user, so they can accumulate quickly.
- Change the Log Level setting back to NONE. Only turn on debug logging when you are experiencing problems.

More Information:

For more information, see the online help.

Retrieve Beta Packages

You can use CA CSM to retrieve beta packages (for example, test PTFs or unpublished PTFs) from an FTP site that is protected by a user ID and password. You can then install, maintain, and deploy the beta packages.

If you retrieve beta packages for the products that you do not have listed in your software catalog, add an entry for the product to your product list first.

Follow these steps:

1. Navigate to the Products tree on the Products tab, and select the beta product. Copy the text for this product so that you have it on the clipboard.
2. Click Add Product, in the Actions section in the left pane.

   The Add Product dialog appears.

3. Paste the contents of the clipboard in the Product field, enter the new beta release and gen level, and click OK.

   Note: For beta projects, the gen level is an arbitrary notation that reflects whatever is appropriate for the beta process, such as Beta1, Beta2 or RC1. Using a nomenclature similar to this helps ensure that they are not confused with the GA version of the product.

   CA CSM starts a task to add the new information.

4. When the task completes, click Refresh.

   The Product List displays the new release and gen level for this beta product.

After you add an entry for the tested product or if you already have an entry for the product, you can retrieve installation packages.

Follow these steps:

1. In the catalog tree, navigate to the gen level of the tested product, right-click, and select Add External Package.

   The Add External Package dialog appears.

2. Select the FTP File option button.

   You are prompted to specify the package details.

3. Enter the FTP path, which the CA Technologies beta program manager provided you with.

   Note: This path is typically the root directory, a forward slash (/).

4. Enter the package name.

   CA CSM searches for the package name. If none are found, an asterisk (*) is appended to the package name. If no packages are found again, then an error message appears.

   Note: To retrieve multiple pax files, enter an asterisk (*) for part or all of the package name.

5. Enter the FTP user ID and password, which the CA Technologies beta program manager also provided you with, and click OK.

   CA CSM starts a task to retrieve the packages in that directory.

6. When the task completes, click Refresh on the Products page.

   The new packages for that gen level appear on the Products page, and they are now downloaded and ready for processing.

Later on, after initial beta testing has begun and problems have been reported, you can retrieve PTFs to the beta product.

Follow these steps:

1. Select the beta release that was previously added, right-click, and select Add External Maintenance.

   The Add External Maintenance dialog appears.

2. Select the FTP File option button.

   You are prompted to specify the package details.

3. Enter the following information, and click OK:

   - A maintenance name, such as RO0111
   - The FTP path name, such as /outgoing/

     Note: The path must start with a forward slash (/). CA CSM automatically supplies ftp.ca.com at the beginning of the path.

   - The FTP user ID and password

   The CA Technologies beta program manager provided this information.

   CA CSM starts a task to retrieve the solution in that directory.

4. When the task completes, click Refresh.

   The Software Catalog displays the new maintenance, and it is now downloaded and ready for processing.

Business Value:

Using this best practice can help save you time when you are downloading, installing, and testing CA Technologies beta products.

Additional Considerations:

The difference between maintenance and installation is that maintenance retrieves one solution at a time, while the installation retrieves all of the product packages simultaneously.

More Information:

For more information, see the online help.

Update Catalog with an Unpublished PTF

You can use CA CSM to retrieve maintenance not yet published on the CA Support Online website (for example, test PTFs) from an FTP site that is protected by a user ID and password. You can then install and deploy these test solutions.

Follow these steps:

1. Navigate to the Products tree on the Products tab, select the product and release, right-click, and select Add External Maintenance.

   The Add External Maintenance dialog appears.

2. Select the FTP File option button.

   You are prompted to specify the package details.

3. Enter the following information, and click OK:

   - A maintenance name, such as RO0111
   - The FTP path name, such as /outgoing/

     Note: The path must start with a forward slash (/). CA CSM automatically supplies ftp.ca.com at the beginning of the path.
   - The FTP user ID and password

   The CA Technologies support engineer provided this information.

   CA CSM starts a task to retrieve the solution in that directory.

4. When the task completes, click Refresh.

   The Software Catalog displays the new maintenance, and it is now downloaded and ready for processing.

Business Value:

Using this best practice can help save you time when you are retrieving unpublished PTFs.

Additional Considerations:

The Add External Maintenance operation retrieves one solution at a time.

Update Catalog with a Published PTF

You can use CA CSM to retrieve a maintenance solution published on the CA Support Online website.

Follow these steps:

1. Navigate to the Products tree on the Products tab, select the product and release, right-click, and select Add External Maintenance.

   The Add External Maintenance dialog appears.

2. Select the Solutions option button.

   The Solutions field appears.

3. Enter a maintenance name such as RO0111 in the Solution field, and click OK.

   CA CSM starts a task to retrieve the solution.

4. When the task completes, click Refresh.

   The Software Catalog displays the new maintenance, and it is now downloaded and ready for processing.

Business Value:

Using this best practice can help save you time when you are retrieving published PTFs.

Additional Considerations:

The Add External Maintenance operation retrieves one solution at a time.

Schedule CA RS Processing

CA Recommended Service (CA RS) is a set of maintenance packages that have been tested in a mainframe integrated system test environment. We recommend that you install CA RS maintenance to keep your products up-to-date. To keep yourself informed about new CA RS maintenance available, you must download (either manually or automatically) all CA RS files that list published maintenance for that CA RS level. Using CA CSM when working with CA RS is not only easier, but also less error-prone.

We recommend that you set up your CA RS scheduling to spread the updates out to accommodate your other nightly activities. This will help you avoid downloading the updates for all products for all your SMP/E environments at the same time.

Business Value:

Using this best practice can help save you time when you are maintaining your CA Technologies products.

More Information:

For more information, see the online help.

Determine Whether to Ignore Common Products During Discovery

CA CSM lets you ignore common products during the product discovery process. At this time, this refers to CA Common Services for z/OS, including CA CSM.

You can activate this feature from the Settings tab, Software Acquisition page, but you first need to determine if you want to use this feature:

- If CA Common Services for z/OS or CA CSM is always in its own SMP/E environment and maintaining them is not the responsibility of the person who is managing the product that is being managed, then we recommend that you use this feature.
- If you have a single SMP/E environment, or just a few SMP/E environments, then do not use this feature. It may be better to have all maintenance viewable and applicable within a single display. Otherwise, you need to select the product you are managing, then select CA Common Services for z/OS or CA CSM to ensure you get any new maintenance that may affect the product you are managing.

Business Value:

This can help provide a concise view of applicable installation packages, including the maintenance related to those packages, when managing your environments from the Products page.

Create New Deployment and Configuration after Maintenance

You have deployed and configured a product across your enterprise. Now you are applying maintenance to this product. Create a deployment and a configuration for this product to get this maintenance to your target systems.

More Information:

For more information, see the *User Guide*.

Check for HOLDDATA Updates Daily

You can configure CA CSM to automatically download the available error HOLDDATA that CA CSM uses for each maintenance installation, and we recommend that you configure it to check for these updates daily.

Follow these steps:

1. Click the Settings tab, and click the Software Catalog link under System Settings in the Settings section on the left side.

   The Software Catalog page opens.

2. In the HOLDDATA Settings section, select the Enable Automatic Updates check box, verify that Daily is selected in the Recurrence drop-down list, and click Apply.

Business Value:

This helps ensure that you have current HOLDDATA and up-to-date information about which what maintenance packages are marked as PE (PTF in Error).

More Information:

For more information, see the *User Guide*.

Chapter 4: System Registry Best Practices

This section contains topics related to setting up a system registry.

The *system registry* is a repository of variable data that all CA CSM managed products share. The system registry repository contains information about the systems that have been defined to CA CSM and selected as a target for deployments and configurations. You can create non-sysplex, sysplex, shared DASD cluster, and staging systems. You can maintain, validate, view, and delete a registered system and you can investigate a failed validation.

This section contains the following topics:

How CA Common Services for z/OS Work in CA CSM

CA Common Services for z/OS are an important working part of CA CSM. CA, Inc. Common Communications Interface (CAICCI) contributes to CA CSM as follows:

- Validates a system.
- Spawns the remote system discovery and the CA CSM Software Deployment Service (SDS).

Business Value:

CA Common Services for z/OS creates universal procedures used by all CA Technologies mainframe products. This allows for all CA Technologies products to work together using a common set of programs and procedures.

More Information:

For more information, see the *User Guide*.

Enter Target Systems as Non-Sysplex Systems

The non-sysplex is a stand-alone z/OS system that is not part of a sysplex or a monoplex system.

You should enter all of your target systems as non-sysplex systems, do the validation and let the CCS discovery function determine if the target system is a non-sysplex, monoplex, or sysplex system. From there, you can build your shared DASD clusters and staging systems.

For small enterprises, we recommend that you add one non-sysplex system and then validate against that system before entering another system.

Business Value:

CA CSM detects what type of system the target system is, easing the process of defining each target system correctly.

More Information:

For more information, see the *User Guide*.

Use Sysplex Systems

The sysplex is the IBM mainframe system complex that is a single logical system running on one or more physical systems. Each of the physical systems that make up a sysplex, is often referred to as a member system.

You should enter all sysplex systems as non-sysplex systems and let the System Registry validate procedure choose the system type.

If you decide to enter a sysplex system as a sysplex, first verify that you have the correct name for this system before validating.

If you have two or more sysplex systems that share DASD between them, you may want to set these systems up as a shared DASD cluster. You would first create the two sysplex systems and then add them to a shared DASD cluster.

For a sysplex, the Uniform Resource Identifier (URI), defined on the FTP Locations information section, must be the URI of the contact system. You must also set up remote credentials for the contact system, because they will be used to transmit the deployment (if FTP is selected), unpackage the deployment through the CA CSM Software Deployment Service (SDS), and to retrieve the results of the deployment.

Business Value:

The CA CSM Software Deployment Service (SDS) enables you to choose a sysplex system for your product deployments. The value of deploying to a sysplex system directly relates to the prevalence of these types of systems in most mainframe environments. This also means that to deploy to all members of a sysplex, only one deployment is needed (to the contact system).

More Information:

For more information, see the *User Guide*.

Use Monoplex Systems

A *monoplex* is a sysplex that has only one member system and minimally a single coupling facility. Currently, a monoplex is tracked in the same manner as a sysplex, except the sysplex name shown in the web-based interface is actually the monoplex system name.

Business Value:

You can use monoplex systems in many ways, providing you the flexibility to dynamically design, create, maintain, and deploy to systems with a managed plan.

More Information:

For more information, see the *User Guide*.

Use Shared DASD Clusters

A shared DASD cluster is a set of systems that share DASD and it can contain any combination of sysplex or non-sysplex systems. This lets you minimize the amount of deployment activity with the largest exposure to target systems. A deployment to this type of system makes the software available to all members of the shared cluster environment.

For a shared DASD cluster, the Uniform Resource Identifier (URI), defined on the FTP Locations information section, must be the URI of the contact system. You must also set up remote credentials for the contact system, because they will be used to transmit the deployment (if FTP is selected), unpackage the deployment through the remote Software Deployment Service (SDS), and to retrieve the results of the deployment through FTP.

Business Value:

Using this best practice lets you do a single deployment to multiple systems that are not part of a sysplex, including multiple sysplexes. This will minimize the amount of deployed software, while at the same time maximizing the system coverage.

More Information:

For more information, see the *User Guide*.

Use Staging Systems

A staging system is a CA CSM Software Deployment Service (SDS) term and it refers to a virtual system. A staging system deploys the deployment to the computer where the CA CSM driving system is located. To use a staging system, the CA CSM driving system must be registered in the CA CSM System Registry. A staging system cannot be part of a shared DASD cluster.

You should use staging systems when you want to perform the following tasks:

- Deploy outside your firewall, so that you copy data sets to a known location and then you can back up and ship to another site.
- Prepare your installed software to use on systems outside the scope of CA CSM managed systems.
- Create model systems for replication to other than CA CSM network locations within your enterprise.
- Test a deployment quickly.
- Create an environmental testing system or sandbox.

Business Value:

CA CSM lets you use staging systems for performing many tasks that ultimately provide you flexibility in building and executing deployments according to the needs and specifications of your environment.

More Information:

For more information, see the *User Guide*.

Define Data Destinations

You must define a data destination for every system to specify which technique to use to transport the deployment data to the remote system. The two choices are FTP and Shared DASD.

When FTP transport is specified as the transport mechanism, the deployment data is shipped to the target system through FTP. It is temporarily placed on the target system at the landing directory specified in the FTP Location information section of the System Registry.

When shared DASD is specified, CA CSM uses a virtual transport technique. That is, it does not actually copy the data from one system to the other. Because the two systems share DASD, there is no need to do this. All of the deployment data is kept in USS file systems managed by CA CSM.

The remote system, even though the DASD is shared, may not be able to find the deployment data in the USS file system. During the Deploy Product step, CA CSM temporarily unmounts the file system from the CA CSM driving system and mounts it in read-only mode on the remote system. For CA CSM to determine where to mount the file system on the remote system, you must specify a mount point location in the data destination. In addition, you can provide allocation information for the creation of the deployment file system, so that when the file system is created on the CA CSM driving system, it will be on the DASD that is shared.

If you have defined in the data destination that the transport is Shared DASD, the mount point that is defined in the data destination must exist on the contact system.

Example:

PLEXA contains Systems: SYSA and SYSB.

SYSA uri: usilsysa

SYSB uri: usilsysb

PLEXA contact system: SYSA

FTP Location:

URI should be set to SYSA – usilsysa

Path should be set to a directory located on SYSA

Data Destination: Shared DASD

Business Value:

CA CSM lets you use data destinations to specify how to transport the deployment and, if you choose, to specify the locations of the target libraries. Data destinations are done at the system level, allowing deployments to a given system to be performed in a consistent manner. This additional flexibility enables you to implement an automated, standardized, and less error-prone deployment process.

More Information:

For more information, see the *User Guide*.

Define Remote Credentials

Remote credentials set up accounts by owner, remote user ID, and remote system name.

Remote credentials are validated during the deployment process. You must adhere to the following guidelines:

- Before creating a new remote credential, make sure that you have the correct owner, remote user ID, remote system name, password, and authenticated authorization.
- Verify that your remote credentials have not expired due to your organization's standards and rules.
- Use all caps when entering the password if that is required on the target system. CA CSM does not automatically fold passwords to uppercase characters.

A remote credential default can be set up by creating a remote credential without the system name. This default would be for the user creating these remote credentials only.

Business Value:

Use remote credentials to secure that your deployment transmits using authenticated authorization procedures.

More Information:

For more information, see the *User Guide*.

Configure Remote Credential Processing to Your Business Needs

Configure how CA CSM handles remote credentials during a deployment. For example, CA CSM can be configured to prompt users for their user ID and password for target systems, or prompt them to enter their missing credentials and optionally save these credentials to the CA CSM database.

Business Value:

Takes full advantage of the flexibility of CA CSM, saves time updating settings, and ensures that proper security policies are maintained. For example, you can set your credentials once and only change your password when it expires, or if it changes periodically, you can enter your credentials during each deployment.

CA CSM prompts you to enter your credentials during each deployment when you remove existing remote credentials. This helps ensure that you always use valid and up-to-date credentials.

More Information:

For more information, see the *User Guide*.

Restrict Access to SYSREG.@PROFILE

The SYSREG.@PROFILE is a resource profile that controls access within the system registry. You should only allow authorized users for your production environments to update the profile information for a system within the system registry.

Business Value:

This eliminates unintended system registry changes by users who should not be making these types of changes.

More Information:

For more information, see the *Administration Guide*.

Chapter 5: Deployment Best Practices

This section contains topics to help you maximize your efficiency when using CA CSM to deploy the mainframe software to the target systems at your site.

A *deployment* is a CA CSM object that you create to deploy libraries and data sets using a process that copies target libraries defined to SMP/E and user data sets across both shared DASD and networked environments.

This section contains the following topics:

Deploy Your CA Technologies Products Using CA CSM

Deployments create an automated process for deploying multiple products to one or more systems in the same manner and the same time. In a one-to-one manual scenario, you have to do the same thing for every product and every system one by one. One or more products to one or more systems immediately increase the scalability of this effort. This reduces errors that could typically result from manual efforts despite best intentions.

CA CSM helps ensure that you are adhering to your company's system and naming standards exactly the same way every time you deploy a product.

You can use your company's system and naming standards when performing the following tasks:

- Creating systems
- Adding products
- Creating methodologies

You should create an inventory matrix or map of all your systems and CA Technologies products that are on each system. This will give you an idea of systems that need to have products deployed to them.

Business Value:

CA CSM lets you easily deploy CA Technologies products. This gives your company dynamic abilities for designing, creating, and maintaining systems.

This also provides the manager responsible for systems the flexibility to design, create, deploy, and maintain systems.

More Information:

For more information, see the *User Guide*.

Establish Security Controls

As with any product, establishing the correct security controls for your deployments and methodologies is a key component to protecting your environments. While your SMP/E data sets and their access are controlled by your normal security practices, deployments, methodologies and the systems defined within the System Registry require special consideration to control who can do what within the CA CSM environment.

We recommend establishing strict controls on who can define and update the systems that are available to deploy products too. Except for those few people that are allowed to maintain those system definitions, display access (that is, SYSREG.@DISPLAY) to the system registry should be all the security authority that most people need to effectively manage product deployments.

As you have read, methodologies control the naming convention that will be used for the creation of the data sets on the system where the deployment is being targeted. The usage of a methodology should conform to any established naming standards for the platform. Additionally, setting up a methodology that does not meet your established standards could result in a failed deployment. We recommend that adding and changing methodologies be controlled within your security environment so that users do not inadvertently change methodologies that meet your standards.

If users need to be able to create their own methodologies for a specific system or a special test, we recommend setting the security permissions to METHOD.@SELF. This lets a CA CSM user with this authority create their own methodologies and limits their ability to update methodologies to only those that they have created. For most CA CSM users, METHOD.@DISPLAY is enough authority for deploying products.

Business Value:

CA CSM lets you use security considerations to protect your company's environments.

This also provides the manager responsible for these systems the flexibility to manage security considerations as required by your company.

More Information:

For more information, see the *User Guide*.

Create the Deployment

This section contains topics related to creating a deployment.

Add Custom Data Sets

There are conditions when additional data sets other than the normal SMP/E managed target libraries need to be deployed. Sometimes these conditions are specified by the vendor in the metadata, and instructions are displayed in the Deployment wizard.

Sometimes, these conditions arise out of your own business needs.

When a product contains USS parts, CA CSM will automatically utilize the custom data set mechanism to specify these parts through automatic generation of custom data set entries.

Any deployment allows the inclusion of user-specified data sets that should be included with this deployment. These data sets can be PDSs, sequential data sets, VSAM data sets, or USS paths or data sets.

Each custom data set specified requires you to specify a separate data set mask to specify what the deployed data set should be called on the remote system.

Business Value:

CA CSM lets you use custom data sets for the deployment of products where additional, product-unique data sets are necessary to deploy them successfully. The CA CSM Software Deployment Service (SDS) gives you the flexibility to tailor your deployment to accommodate these products.

More Information:

For more information, see the *User Guide*.

Construct a Data Set Name Mask

A *data set name mask* is a unique name that identifies each data set. It consists of one or more qualifiers separated by periods, and has a maximum input length of 64 characters, including the periods. When the data set name mask is translated, it has a maximum length of 44 characters including the periods.

To construct a data set name mask for your environment, determine the following:

- How do you plan to utilize deployment services?
  - Do you want each deployment to have a unique set of deployed data set names?

    or

  - Do you want to re-use a set of deployed data set names?

  If you want each deployment to have a unique set of deployed data set names:

  - The symbolic qualifier &MSMDID can be utilized to give each deployed library a unique name based upon the deployment.
  - This symbolic qualifier is unique for each deployment that is created. It is a numeric value and must be used in a mask at a place where numeric values are valid.

    Examples: Assume the deployment has an ID of 4700, and the LLQ of the data set is CAILOAD:

    - VENDOR.D&MSMDID.. would resolve to VENDOR.D4700.CAILOAD

      Note: The double dots in the mask represent two uses, the first dot delimits the variable name and the second dot is included as text in the resolved name.

    - SYSCA.D&MSMDID.T would resolve to SYSCA.D4700T.CAILOAD
  - The symbolic qualifier &YYMMDD provides you a value based on Julien Date format for the day you created the deployment. It is a numeric value that must be used in a mask at a place where numeric values are valid. This value can be used to help create unique name values.

    Examples: Assume the day the deployment was created was April 1st, 2010, and the LLQ of the data set is CAILOAD:

    - VENDOR.D&YYMMDD.. would resolve to VENDOR.D100401.CAILOAD

      Note: The double dots in the mask represent two uses, the first dot delimits the variable name and the second dot is included as text in the resolved name.

    - SYSCA.D&YYMMDD.T would resolve to SYSCA.D100401T.CAILOAD

  If you want to reuse a set of deployed data set names because this is a sandbox, and you do not need to preserve any prior deployments:

  - A constant name could be used as the mask.

    Examples: Assume the LLQ of the data set is CAILOAD:

    - SYSCA.VENDOR.PRODSET would resolve to SYSCA.VENDOR.PRODSET

- Is it possible that deployed libraries, in a multi-system deployment, could end up on Shared DASD between those systems or a shared catalog?
  - The data set names must be unique from deployment to deployment.
  - The symbolic qualifier &SYSNAME can be utilized to give each deployed library a unique name based upon the remote system name.
  - The symbolic qualifier &MSMDID can be utilized to give each deployed library a unique name based upon the deployment.
  - This symbolic qualifier is unique for each deployment that is created. It is a numeric value. It must be used in a mask at a place where numeric values are valid.

    Examples: Assume the deployment has an ID of 4700, and the LLQ of the data set is CAILOAD and the remotes systems are SYSA and SYSX:

    - VENDOR.&SYSNAME..D&MSMDID.. would resolve to VENDOR.SYSA.D4700.CAILOAD and VENDOR.SYSX.D4700.CAILOAD

      Note: The double dots in the mask represent two uses, the first dot delimits the variable name and the second dot is included as text in the resolved name.

    - SYSCA.D&MSMDID.T.&SYSNAME would resolve to SYSCA.D4700T.SYSA.CAILOAD and SYSCA.D4700T.SYSX.CAILOAD

- Is it possible that the product you are deploying does not have unique low-level qualifiers?

  Examples: Assume a product had two target libraries with the same LLQ:

  - SYINST.PROD.SYSTEM.RULES and SYINST.PROD.CUSTOM.RULES.
  - Because the mask, after resolution, is prepended in front of the LLQ, a technique is required for uniqueness.

  CA CSM provides the following symbolic qualifiers that could be utilized for low-level qualifiers:

  MSMSLQ

  This is the secondary low-level qualifier (SYSTEM and CUSTOM in the preceding examples).

  MSMDLIBN

  This is the deployed library number.

  MSMMLQ

  This is middle-level qualifier (PROD.SYSTEM and PROD.CUSTOM in the preceding examples).

  Examples:

  - SYSCA.&MSMSLQ. would resolve to SYSCA.SYSTEM.RULES and SYSCA.CUSTOM.RULES
  - SYSCA.RULES&MSMDLIBN. would resolve to SYSCA.RULES1.RULES and SYSCA.RULES2.RULES.
  - SYSCA.&MSMMLQ. would resolve to SYSCA.PROD.SYSTEM.RULES and SYSCA.PROD.CUSTOM.RULES

- Are there naming conventions on the remote system, and, for multi-system deployments, are the naming conventions similar enough to allow for a single mask to provide the desired results?
  - If, in your multi-system deployments, the naming conventions are similar enough to allow for a single mask to provide the desired results, use symbolic qualifiers and constants to construct well formed masks.
  - If, in your multi-system deployments, the naming conventions are *not* similar enough to allow for a single mask to provide the desired results, create multiple deployments, one for each remote system.

Note: There may be other considerations that are specific in your environment.

Keep the following points in mind when considering the construction of your data set name masks:

- They control what the deployed library is to be called. This makes it a critical element for deployment services to provide the desired results.
- The deployed libraries are cataloged on the remote system where they are created.
- The deployed libraries are created and accessed under the remote credentials for the remote system.
- Masks are methodology-based, which in turn are deployment-based. That means that one mask is utilized for all deployed libraries on any given deployment.
- Symbolic qualifiers are the key that lets a single mask provide a variety of data set names.

Business Value:

A methodology gives you the power and flexibility of creating and assigning unique data set name masks that are automatically applied when you deploy a product. This is especially useful in helping you adhere to your organization’s best practices for data set naming and standardization.

More Information:

For more information, see the *User Guide*.

How to Use a Methodology

A methodology is required for each deployment. You use a methodology to name the data sets on the target system.

A methodology provides the *what* of a deployment, that is, what you want to call your data sets. It is a named object with a description that is assigned to an individual deployment.

You should use your company's naming standards and conventions when setting up data set names. A methodology lets you copy products and data sets to the target system and rename them as you copy. The methodology also enables you to specify a disposition, that is, you can overwrite the data set if it exists, or create new data sets on the target system.

Business Value:

CA CSM lets you set up data set names that use your company's naming standards and conventions by using the flexible and many different symbolic qualifiers supplied with CA CSM.

This also helps you ensure that company naming standards and conventions are followed and that the data sets are transferred to the target system correctly.

More Information:

For more information, see the *User Guide*.

Test Your Deployment

Deployments should be tested before you deploy to a production system.

You should do the following:

- Use an environmental test system or a sandbox system to test your deployment.
- Deploy to your production system only after verifying that the deployment is successful on your environmental test system and on your program system.

Business Value:

Testing your deployments before implementing them on your production systems will help you avoid errors on your production system and save you time when deploying products.

More Information:

For more information, see the *User Guide*.

Delete Deployment Snapshots

Delete deployment snapshots when they are no longer useful, for space cleanup.

Note: Consult with other members of your organization if you need to confirm whether a snapshot is still useful to someone.

Follow these steps:

1. From the Deployments page, click Snapshot Completed.

   A list of completed deployment snapshots appears.

2. Find a snapshot that is no longer useful, and from the Actions drop-down list on the right side, select Delete.

   The deployment snapshot is deleted.

3. Find any remaining snapshots that are no longer useful, and repeat the previous step for each of these.

Business Value:

This can help free up space in your database.

More Information:

For more information, see the *User Guide*.

Chapter 6: Configuration Best Practices

This section contains topics to help you maximize your efficiency when using CA CSM to configure the mainframe software to the target systems at your site.

A *configuration* is a CA CSM object that you create to tailor your deployed software and make it usable in your environment. It contains the profiles, variables and resources specific to your environment.

This section contains the following topics:

Establish Configuration Naming Conventions

You can create multiple configurations from the same deployed product. To avoid confusion, you should establish naming conventions to differentiate these configurations. For example, you can associate the name of the configuration with the high-level qualifier (HLQ) data set name.

Business Value:

This can help your site improve the planning and organization of configurations, and assist when handing over the work to new employees.

More Information:

For more information, see the *User Guide*.

Review Configurations Thoroughly Before Building

The last step of the Create Configuration wizard lets you print and export the configuration summary, including the details of the previous steps of the wizard.

Although it may be tempting to minimize your reviewing effort and breeze through it, we strongly encourage you to utilize the full capabilities of CA CSM and thoroughly review the configuration summary before building the configuration.

You can read the summary directly from the wizard, print it out to read from hardcopy, or export to a TXT file that can be saved in your mainframe environment as a data set, or directly to your computer.

Beyond just proofreading the summary, you need to analyze the summary and imagine the effect the configuration will have on your mainframe environment.

If during the review of your configuration you discover a change is needed, you can navigate to a previous step in the wizard to amend the configuration definition.

After you click Build, if there is an error you missed, you will have to throw this configuration away and create a new one from scratch.

Business Value:

This can help ensure that you do not configure products incorrectly, and save time by not having to go back and create your configuration.

More Information:

For more information, see the *User Guide*.

Validate Configuration Before Implementing

The CA CSM configuration process includes a function that lets you validate the configuration before you implement it to your target systems. This can help you verify that you have the required access to the resources that are going to be utilized when you implement the configuration.

Business Value:

This can help save you time and avoid implementation failures.

Additional Considerations:

You must build the configuration before you can validate or implement it. Configurations that are in the process of being built cannot be validated or implemented until the process completes.

More Information:

For more information, see the *User Guide*.

Clean Up Implementation Tasks

We recommend that you delete all validation and implementation tasks as soon as they are no longer needed. Unlike other CA CSM tasks, these tasks take up valuable space in your database.

Business Value:

This can help free up space in your database.

Additional Considerations:

Deleted tasks still appear in the Audit Task History subtab on the Tasks page.

More Information:

For more information, see the *User Guide*.

Import Configuration Variables when Build Fails

When you arrive at the last step of the Create Configuration wizard, even if you thoroughly review your configuration before building, you still may encounter an error when building. If this happens, you will need to create a new configuration from scratch, but you can save yourself some time by importing the products variables from the configuration that failed.

Follow these steps:

1. Go to the Deployments tab and create a new configuration.
2. When you reach the fourth step of the wizard (Create Target Settings), import the values from the configuration that failed from the Use Configuration Values drop-down list, and then change any errant variables.
3. Do *one* of the following:
   - Save your progress, exit the wizard and delete the previous configuration. This will prevent duplicate resource problems if you did not change for things such as HLQs and PDS member names from their previous values.
   - Change values for things such as HLQs and PDS member names to prevent duplicate resources from being created, and optionally delete the old configuration now as well.
4. Make any additional changes to the Target Settings to ensure that the required resources are set up for the fifth step (Create Target Resources).
5. Complete the remaining steps of the wizard and build the configuration.

Business Value:

This can save you time when creating configurations.

More Information:

For more information, see the *User Guide*.

Index

N

P

R

S

T

U

W

Z