CA Chorus™ Software Manager

Administration Guide

Release 5.1

Fourth Edition

CA Technologies Product References

This document references the following CA Technologies products:

- CA Chorus™ Software Manager (CA CSM)
- CA ACF2™ for z/OS
- CA Allocate™ DASD Space and Placement (CA Allocate)
- CA Auditor for z/OS
- CA Chorus™
- CA Common Services for z/OS
- CA Database Management Solutions for DB2 for z/OS
- CA Datacom®/DB
- CA Datacom/MSM
- CA Disk Backup and Restore (CA Disk)
- CA Distributed Security Integration for z/OS (CA DSI Server)
- CA Easytrieve® Simplified Design System (CA Easytrieve)
- CA Panvalet® (CA Panvalet)
- CA PDSMAN® PDS Library Management (PDSMAN)
- CA SMF Director
- CA SYSVIEW
- CA Top Secret® for z/OS
- CA View®

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.

Documentation Changes

4th Edition (May 2014)

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

- Introduction (see page 17): restructured the chapter, moved the Overview topic to the *Release Notes*
- How the Setup and Installation Process Works: removed the section
- Preparing for Installation (see page 27): restructured the chapter, moved information to the *Installation Guide* and *Site Preparation Guide*
- Installing and Setting Up CA CSM (see page 39): restructured the chapter, moved information to the *Installation Guide* and Site *Preparation Guide*
- Set Up User Security in CA ACF2 for z/OS, Set Up User Security in CA Top Secret for z/OS, Set Up User Security in IBM RACF: removed the sections, the information is found in the scenarios.
- SCS Address Space Setup: removed the section, the information is found in: How the SCS Address Space Administration Process Works (see page 114)
- CA CSM Implementation and Status > Implementation Checklist > Security Administrator (see page 154): added information about access when using CA SAF HFS

3rd Edition (October 2013)

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

- Preparing for Installation > Disk Space Requirements: added an important note about changes in the utility program IOEAGFMT in z/OS V2.1

2nd Edition (September 2013)

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

- Preparing for Installation > Software Requirements: added a note about Microsoft Internet Explorer 10 compatibility
- Installing and Setting Up CA CSM > Install and Set Up CA CSM > Configure Mount Parameters for CA CSM File Systems (see page 59): added a new topic
- Troubleshooting > SMP/E Environment Does Not Appear on the Tree (see page 226): added a section

1st Edition (January 2013)

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

- Preparing for Installation > Upgrade Tasks > Upgrade Scenarios: added a scenario to upgrade from CA MSM V5.0 to the latest version
- Preparing for Installation > Upgrade Tasks > Upgrade Process > Post-Installation: added information about cleaning up deployment snapshots
- Preparing for Installation > Upgrade Tasks > Upgrade Process > Long-Term Maintenance: updated information about the msmtmp directory
- Preparing for Installation > Prerequisite Validator > Prerequisite Validator Requirements (see page 27): updated to support the latest CA CSM version
- Preparing for Installation > Disk Space Requirements: updated the allocation for the Hierarchical File System (HFS) or zSeries File System (zFS) space
- Preparing for Installation > Software Requirements: updated to support the latest CA CSM version
- Preparing for Installation > Web Access Requirements > added sdownloads.ca.com
- Preparing for Installation > Security Setup > Security Setup on the CA CSM Application Server > Set Up User Security for CA CSM Functions (see page 34): added information about the SAF resource class name
- Preparing for Installation > Security Setup > Security Setup on the CA CSM Application Server > Set Up User Security in CA ACF2 for z/OS: added information about the SAF resource class name
- Preparing for Installation > Security Setup > Security Setup on the CA CSM Application Server > Set Up User Security in CA Top Secret for z/OS: added information about the SAF resource class name
- Preparing for Installation > Security Setup > Security Setup on the CA CSM Application Server > Set Up User Security in CA ACF2 for z/OS > Define the CAMSM Resource Class in CA Top Secret for z/OS: added information about the SAF resource class name
- Preparing for Installation > Security Setup > Security Setup on the CA CSM Application Server > Set Up User Security in IBM RACF: added information about the SAF resource class name
- Preparing for Installation > Security Setup > Security Setup on the CA CSM Application Server > Set Up User Security in IBM RACF > Define the CAMSM Resource Class in IBM RACF: added information about the SAF resource class name
- Preparing for Installation > CA CSM Associated Security IDs - OMVS Segment and Home Directory: updated information about the home directory
- Preparing for Installation > USS Path Details > USS Path Setup (see page 38): removed information about the msmtmp directory; updated the required space

- Installing and Setting Up CA CSM > Specify Installation and Setup Options > Specify Options Automatically with ISPF UI Tool (see page 41): added a note about the ISPF command line
- Installing and Setting Up CA CSM > Install and Set Up CA CSM (see page 43): restructured and updated the topic
- Installing and Setting Up CA CSM > Install and Set Up CA CSM > Installation Jobs (see page 51): restructured and updated the section
- Installing and Setting Up CA CSM > Install and Set Up CA CSM > Set Up CA CSM User ID Without UID(0) (see page 54): updated the procedure instructions
- Installing and Setting Up CA CSM > Install and Set Up CA CSM > Override the Path Naming Standard for Deployment: moved the topic to the User Guide
- Installing and Setting Up CA CSM > Start CA CSM > Configuring Output Descriptors: (see page 66) added a section on configuring output descriptors in the CA CSM server startup JCL
- Installing and Setting Up CA CSM > Configuring FTP Connections for an Existing Installation: (see page 68) updated to state that there are no FTP configuration changes for an existing installation; removed the underlying topics
- Installing and Setting Up CA CSM > Upgrade CA Common Services with CETN500 (see page 80): removed upgrade scenarios from CA Common Services for z/OS r11.0 because it is no longer supported
- Installing and Setting Up CA CSM > Upgrade CA Common Services with CETN500 (see page 80): added a link to Software Requirements
- Post-Installation Tasks > Set Up CAIRIM to Load CA Datacom/MSM SVC at IPL: removed information about upgrading from CA MSM r3.0
- Post-Installation Tasks > CA CSM Backup and Recovery > How You Back Up CA CSM (see page 92): updated the information about the file systems
- Database Administration > Database Allocation Management > JCL Allocation Adjustment (see page 100): updated the section with new installation job names and details
- CA CSM Implementation and Status > Implementation Checklist > Network Administrator (see page 153): added sdownloads.ca.com
- CA CSM Implementation and Status > Implementation Checklist > USS Administrator (see page 156): updated the file system structure
- CA CSM Implementation and Status > Options File Keywords > CA Datacom/MSM (see page 160): removed information about upgrading from CA MSM r3.0 from the SVCNO keyword section
- CA CSM Implementation and Status > Options File Keywords > Mount Point Manager (see page 161): added the TempSpaceCleanupInterval keyword

- CA CSM Implementation and Status > Options File Keywords (see page 157): removed the section Product Acquisition Service
- CA CSM Implementation and Status > Options File Keywords > Software Installation Service (see page 164): removed the keyword sisServerUnpaxTempDir; updated information about sisGimunzipTempPrefix
- CA CSM Implementation and Status > Options File Keywords > Security (see page 165): added the safResourceClass keyword
- CA CSM Implementation and Status > Options File Keywords > CA CSM Installer Execution Control Parameters (see page 170): removed information about upgrading from CA MSM r3.0 from the InstallSVC keyword section
- CA CSM Implementation and Status > USS File Systems > USS Path Setup Details (see page 175): updated information about the file system structure
- CA CSM Implementation and Status > USS File Systems > USS Path Setup Details > Single File System (see page 177): updated information about the file system structure
- CA CSM Implementation and Status > USS File Systems > Use of Temporary File Systems (see page 179): added a topic describing how CA CSM handles temporary file systems
- CA CSM Implementation and Status > CA CSM Data Sets and File Systems > CA CSM Data Set Types (see page 181): updated the data set types
- CA CSM Implementation and Status > CA CSM Data Sets and File Systems > CA CSM File Systems (see page 182): updated system path details
- CA CSM Implementation and Status > Security for CA CSM Functions > Resource Profiles (see page 189): added a new resource profile, SC.@HIDE, to control access to the Hide menu item within the Products tree
- CA CSM Implementation and Status > Security for CA CSM Functions > Resource Profiles (see page 189): added a new resource profile, TM.TASK.ARCHIVE, to control access to Manage History functionality within the Task tab and allow authorized users to create, run, or delete policies
- CA CSM Implementation and Status > DBINIT and DBUPDATE Settings (see page 195): removed the settings sisServerUnpaxTempDir and pasTemporaryDownloadDirectory; updated information about GIMUNZIP Temporary Prefix
- CA CSM Implementation and Status > Job Allocation Details (see page 204): updated the section to reflect new names of installation jobs and up-to-date allocation details

- Troubleshooting > CA CSM Application Server Timeout (see page 216): added a new section
- Troubleshooting > Software Configuration Service Address Space Encounters an ABEND under z/OS V1.11 RSU 1106: removed the section as out-of-date

Contents

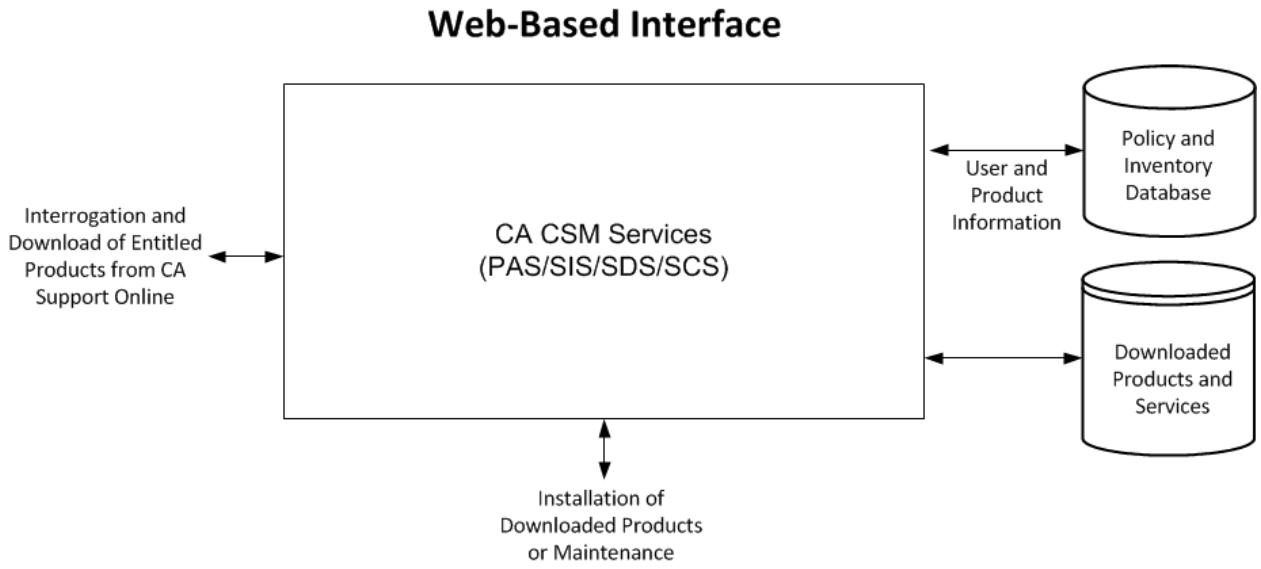
Chapter 1: Introduction

This section contains the following topics:

How CA CSM Works

CA CSM is a program that runs in the address space of an application server environment hosted on a z/OS system. Typically, this system is where you use SMP/E to install and maintain your products. The system is known as the SMP/E driving system. The CA CSM web-based interface enables you to perform SMP/E processing dynamically without having to code and submit the batch jobs manually.

The following illustration shows the main components and data flows:



CA CSM has the following main components:

CA CSM Services

Provides the following services:

Product Acquisition Service (PAS)

Facilitates the acquisition of CA Technologies mainframe products and the service for those products, such as program temporary fixes (PTFs). The service retrieves information about the products to which your site is entitled and records these entitlements in a software inventory. The inventory is maintained on your driving system. The service can also download the LMP keys (licenses) for those products. The web-based interface enables you to browse the software inventory for available software and fixes, and makes them available within the driving system.

Software Installation Service (SIS)

Facilitates the installation and maintenance of CA Technologies mainframe products in the software inventory of the driving system. The web-based interface enables you to browse and manage the software inventory, and automate installation tasks. You can browse downloaded software packages, and can browse and manage SMP/E environments on the driving system.

Software Deployment Service (SDS)

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

Software Configuration Service (SCS)

Facilitates the mainframe products configuration from the software inventory of the driving system to the targeted z/OS mainframe operating system. SCS guides you through the configuration creation process, and through the manual steps to implement the configuration. In addition, SCS includes an address space communications service running on each targeted z/OS system.

Database

Stores information for use by CA CSM.

Policy

Stores site and user information for downloading and processing CA Technologies mainframe products.

Inventory

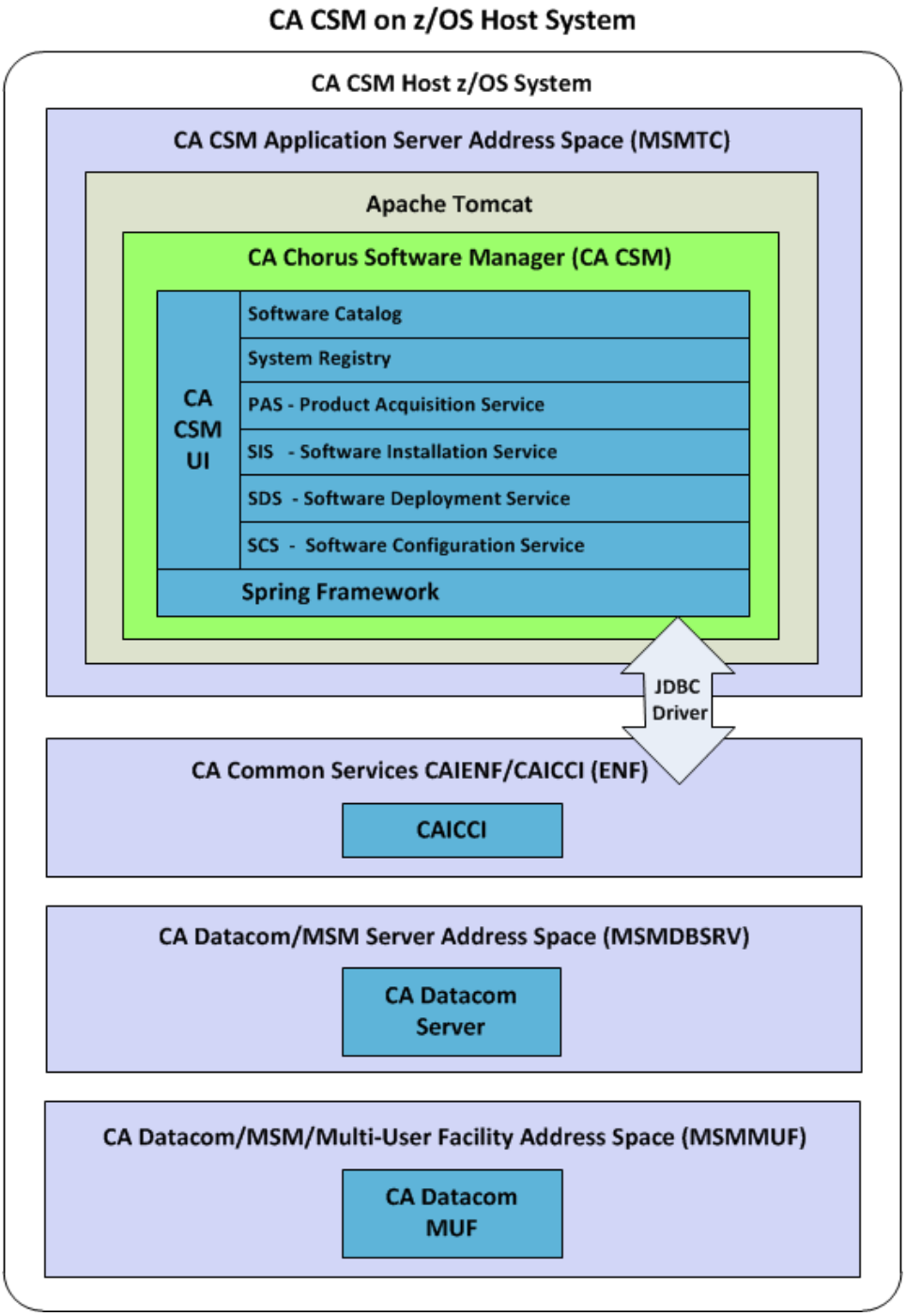
Stores information about the CA Technologies mainframe products to which you are entitled.

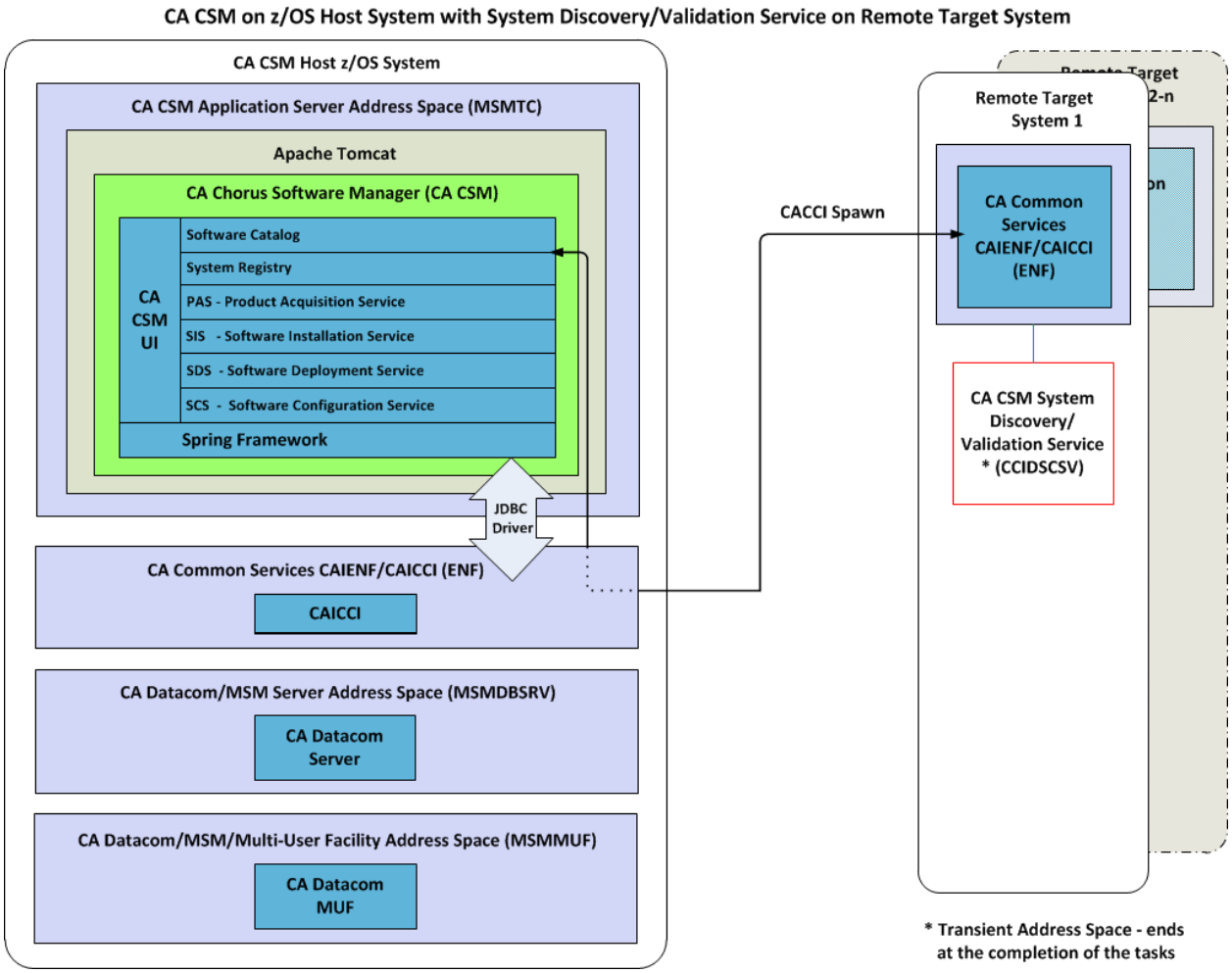
The web-based Interface

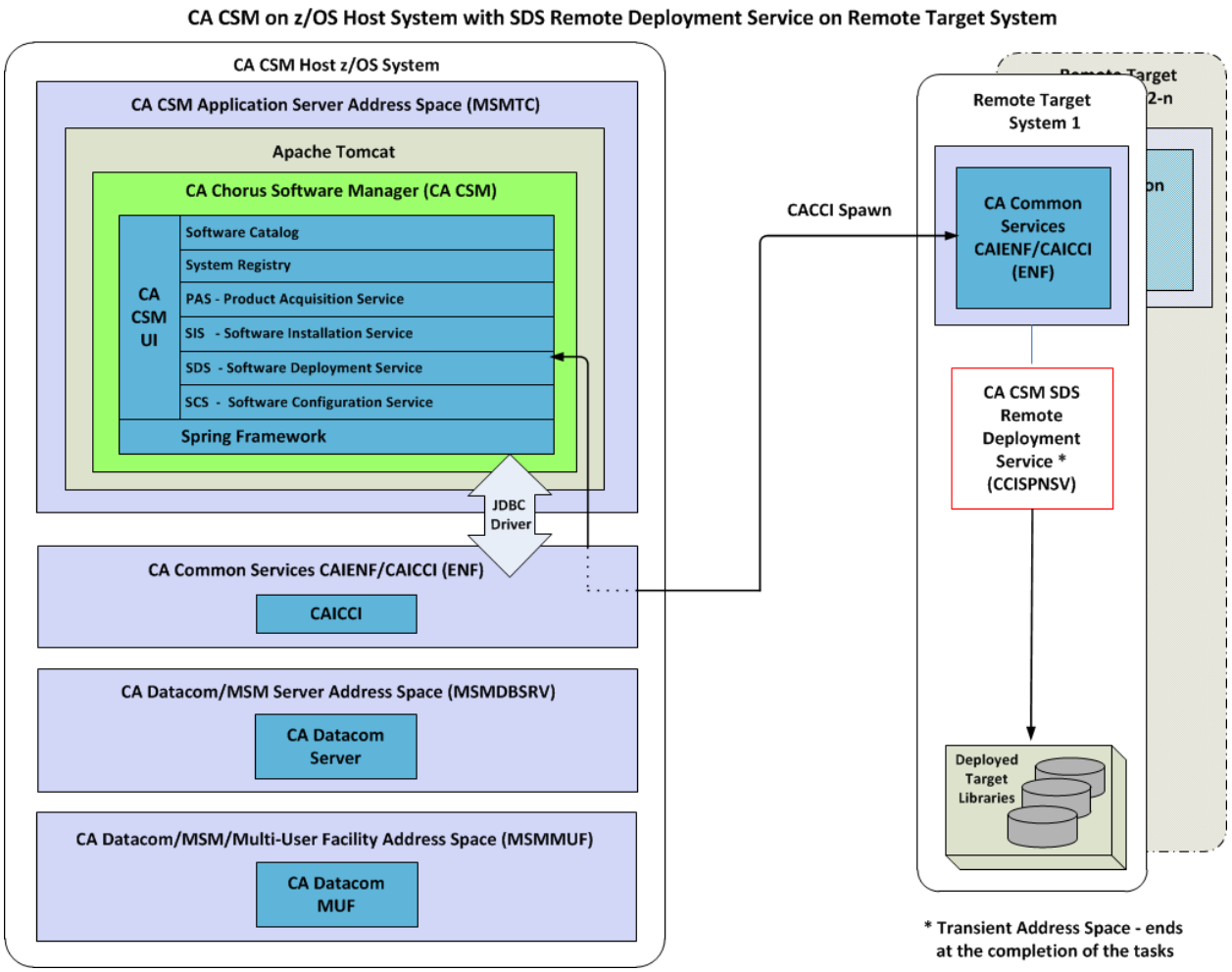
Enables you to acquire, install, maintain, deploy, and configure your CA Technologies mainframe products from the CA CSM catalog, and manage your SMP/E environments. The web-based interface includes online help that provides information about how to use CA CSM.

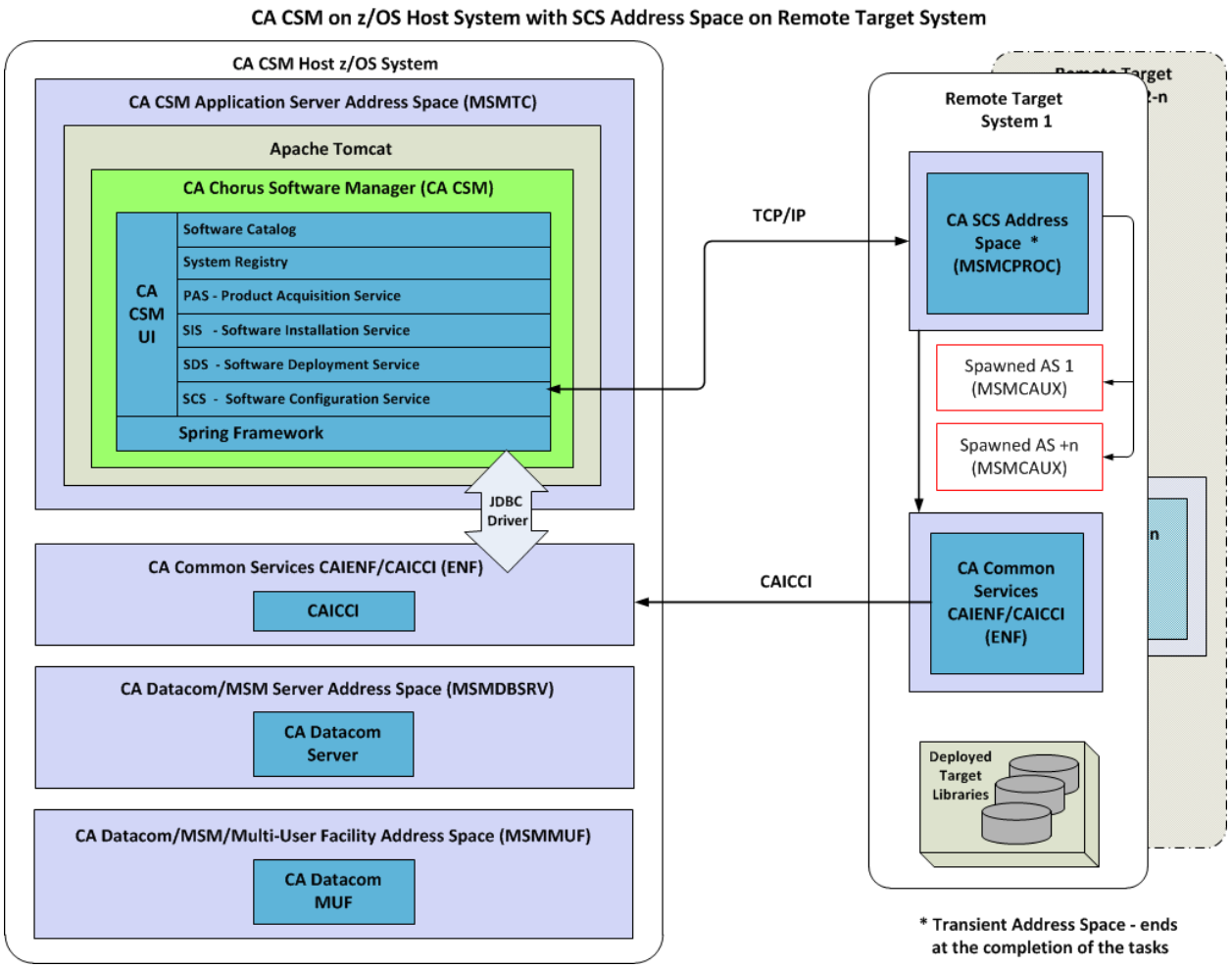
CA CSM Operational Architecture Diagrams

The following diagrams show configurations of CA CSM with CA Common Services for z/OS on remote and local systems.

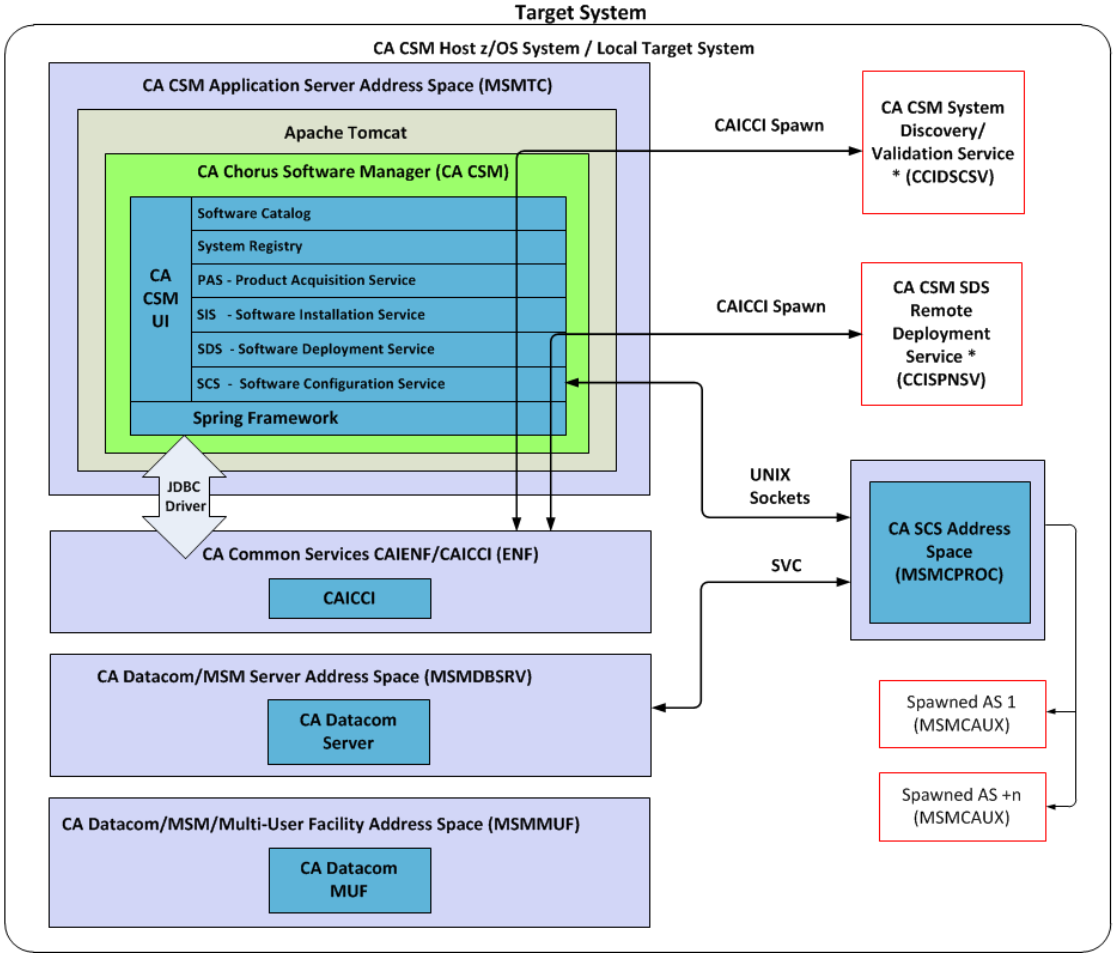



CA CSM on z/OS Host System with System Discovery/Validation Service on Remote Target System
CA CSM Host z/OS System
CA CSM Application Server Address Space (MSMTC)
Apache Tomcat
CA Chorus Software Manager (CA CSM)
CA CSM UI
Software Catalog
System Registry
PAS - Product Acquisition Service
SIS - Software Installation Service
SDS - Software Deployment Service
SCS - Software Configuration Service
Spring Framework
JDBC Driver
CA Common Services CAIENF/CAICCI (ENF)
CAICCI
CA Datacom/MSM Server Address Space (MSMDBSRV)
CA Datacom Server
CA Datacom/MSM/Multi-User Facility Address Space (MSMMUF)
CA Datacom MUF
CACCI Spawn
Remote Target System 1
CA Common Services CAIENF/CAICCI (ENF)
CA CSM System Discovery/ Validation Service * (CCIDSCSV)
* Transient Address Space - ends at the completion of the tasks


CA CSM on z/OS Host System with SDS Remote Deployment Service on Remote Target System
CA CSM Host z/OS System
CA CSM Application Server Address Space (MSMTC)
Apache Tomcat
CA Chorus Software Manager (CA CSM)
CA CSM UI
Software Catalog
System Registry
PAS - Product Acquisition Service
SIS - Software Installation Service
SDS - Software Deployment Service
SCS - Software Configuration Service
Spring Framework
JDBC Driver
CA Common Services CAIENF/CAICCI (ENF)
CAICCI
CA Datacom/MSM Server Address Space (MSMDBSRV)
CA Datacom Server
CA Datacom/MSM/Multi-User Facility Address Space (MSMMUF)
CA Datacom MUF
CACCI Spawn
Remote Target System 1
CA Common Services CAIENF/CAICCI (ENF)
CA CSM SDS Remote Deployment Service * (CCISPNSV)
Deployed Target Libraries
* Transient Address Space - ends at the completion of the tasks


CA CSM on z/OS Host System with SCS Address Space on Remote Target System
CA CSM Host z/OS System
CA CSM Application Server Address Space (MSMTC)
Apache Tomcat
CA Chorus Software Manager (CA CSM)
CA CSM UI
Software Catalog
System Registry
PAS - Product Acquisition Service
SIS - Software Installation Service
SDS - Software Deployment Service
SCS - Software Configuration Service
Spring Framework
JDBC Driver
CA Common Services CAIENF/CAICCI (ENF)
CAICCI
CA Datacom/MSM Server Address Space (MSMDBSRV)
CA Datacom Server
CA Datacom/MSM/Multi-User Facility Address Space (MSMMUF)
CA Datacom MUF
TCP/IP
Remote Target System 1
CA SCS Address Space * (MSMCPROC)
Spawned AS 1 (MSMCAUX)
Spawned AS +n (MSMCAUX)
CA Common Services CAIENF/CAICCI (ENF)
Deployed Target Libraries
* Transient Address Space - ends at the completion of the tasks

CA CSM on z/OS Host System with System Registry Validation Service + SDS Remote Deployment Service + SCS Address Space on Local Target System



Network Flows

CA CSM uses the following process to connect you directly to the appropriate CA Technologies website, where they can manage your CA Technologies software:

1. You connect to CA CSM from within your corporate Intranet (locally connected or tunneled in through VPN) using the HTTP protocol such as http://*yourmainframe*:*yourport*/MSM).
   - Your systems programmers initiate all actions.
   - No port is exposed to the Internet.
   - No communication is initiated from outside your Intranet.

2. The CA CSM Product Acquisition Service communicates with CA Technologies using the same methods that you previously used when manually accessing the website, as follows:

   HTTPS

   Passes credentials to, and obtains product information from the appropriate CA Technologies website.

   FTP

   Downloads software packages from CA FTP Services to your mainframe system using an anonymous FTP, with no credentials passed. CA CSM accesses one of the following locations:

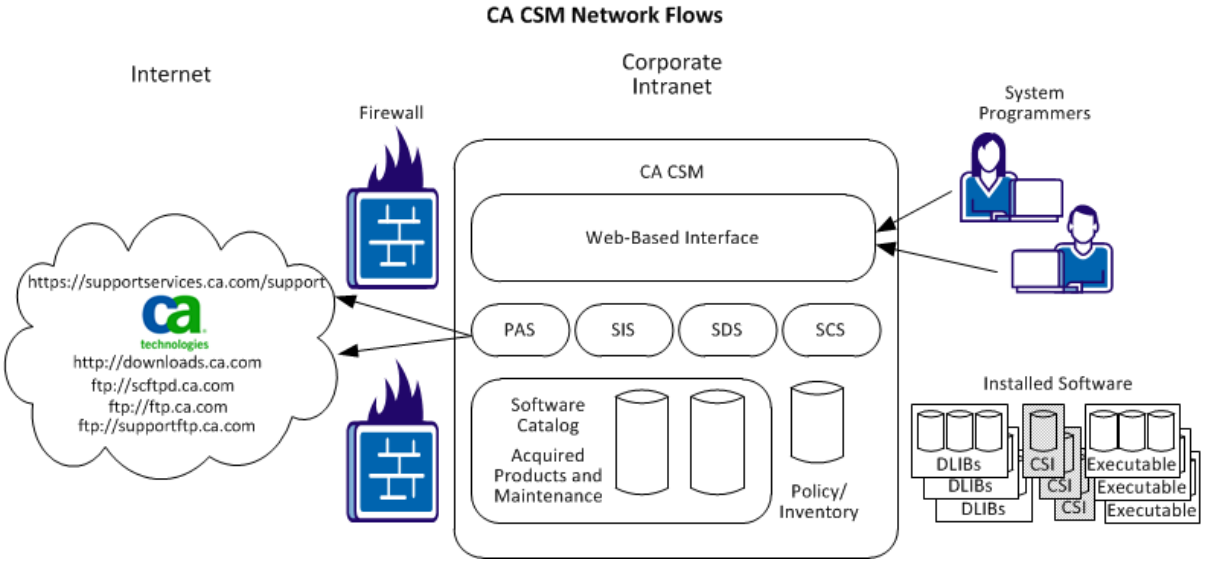
   - ftp://scftpd.ca.com
   - ftp://ftp.ca.com
   - ftp://supportftp.ca.com

Note: The following information is the only unencrypted data sent to and from CA Technologies:

- Your email address for anonymous FTP (no password)
- The CA Technologies product information, either base install packages or solutions.

None of this data is part of any privacy or encryption standards.

This process is depicted in the following illustration:



Web-based Interface

You access and use CA CSM from a web browser. The web-based interface has online help that provides information about acquiring, installing, maintaining, deploying, and configuring products.

When you first log in, the initial page appears showing the following functions in tabs:

Software Status

Warns you of maintenance and task issues.

Products

Helps you manage CA Technologies products, including downloading and installing of product packages and applying maintenance.

SMP/E Environments

Helps you manage your SMP/E environments and installed products.

Deployments

Lets you create deployments, manage existing deployments, and create configurations.

Configurations

Lets you manage and implement existing configurations.

System Registry

Lets you create a system registry and maintain data destinations.

Tasks

Helps you manage CA CSM tasks in support of your activities (for example, installation tasks).

Settings

Defines settings for CA CSM (for example, software acquisition).

Chapter 2: Preparing for Installation

This section contains the following topics:

Prerequisite Validator

The CA CSM Prerequisite Validator is a utility that lets you verify that you have all necessary authorizations in place before you attempt to install CA CSM.

The packed CA CSM Prerequisite Validator product package is available on the CA Chorus Software Manager page in the Download Center on the CA Support Online website. You can download and unpack it in the same way you download and unpack other CA CSM files.

Prerequisite Validator Requirements

You must have the following minimum requirements to use this utility:

- The latest version of z/OS or the last previous version
- OMVS segment for the user
- Java

  Your system has IBM Java SDK for z/OS:

  - Java 6.0, build 2.4, at maintenance level SR9 (31 bit or 64 bit).
  - Java 6.0, build 2.4, at maintenance level SR10 (31 bit or 64 bit).
  - Java 6.0, build 2.6, base build (31 bit or 64 bit).

    Note: Java 6.0, build 2.6 is the equivalent of IBM Java 6.0.1. For Java 6.0, install PTF UK56434, APAR PM08437, SDK6 SR8.
  - Java 6.0.1, build 2.6, at maintenance level SR1 (31 bit or 64 bit).
  - Java 7.0, build 2.6 (31 bit or 64 bit).
- Minimum TSO REGION size 128 MB
- BPX.SERVER READ resource access for verifying SAF resources that are required for CA CSM installation.

Note: Prerequisite Validator Utility verifies user access to particular resources and does *not* verify general user access rights (for example, NORESCHK for CA Top Secret for z/OS). The Prerequisite Verification report can indicate that you do not have access to the resources.

Execute from Native USS

The Prerequisite Validator utility can be executed directly from the native USS command prompt.

Follow these steps:

1. Download the Prerequisite Validator pax file to a directory in your USS environment.
2. Open the native USS command prompt in your z/OS system.
3. Change to the directory where you downloaded the Prerequisite Validator pax file using the following command:

   `cd path_where_Prerequisite_Validator_is_downloaded`

   For example:

   `cd /u/users/MSMpre`
4. Issue the following command:

   `pax -rvf 51000068XU1.pax.Z`

   Note: The full pax file name, including the Z suffix, is case-sensitive. Verify that you use the exact case of the file name on the system where you issue the pax command. Rename the file, if necessary.

   The Bin folder contents are extracted.
5. Issue the following command:

   `cd Bin`
6. (Optional) Modify the default properties file parameters (see page 29) if necessary.
7. Issue the following command to invoke the utility:

   `./MSMVal.sh JavaHomePath`

   For example:

   `./MSMVal.sh /usr/lpp/java/J6.0`

   The license agreement appears.
8. Review the license agreement, and press F3.

   You are prompted to accept the agreement.

Enter **Y** to accept the agreement.

The utility gathers the host name and IP address from the system and attempts an FTP connection to verify the JESINTERFACELEVEL.

9. (Optional) If you did not provide a host name when you modified the default file parameters (see page 29) or the gathered host name fails to connect, provide the host name in response to the prompt. Alternatively, you can provide this value using the default properties file as documented in the subsequent section.

At the end of a successful execution, the Prerequisite Verification report appears in browse mode and the following files are generated:

- MSMPre-RequisiteVerificationReport.txt
- MSMPre-RequisiteLog*yyyy-mm-dd*,*hh-mm-ss*,*ttt*.log

Setting Default Values

The following file lets you set default values per your site requirements:

unpax_directory/Bin/lib/MSMSetupDefault.properties

This file contains the following parameters:

Hostname or IP Address

HOSTNAME=

Specify the host name or IP address of your system. The Prerequisite Validator utility uses the host name or the IP address of your system to test the FTP connection and to verify the JESINTERFACELEVEL value.

Local Host FTP Port

ftp.port=

Specify the FTP port number for the host name or IP address you specified. The Prerequisite Validator utility tests the FTP connection and verifies the JESINTERFACELEVEL value.

Default: 21

Authorization for Issuing FTP Command

ftp.stat.check.credential=

Specify ftp.stat.check.credential=y if your site requires authorization to issue FTP quote STAT commands. The command appears in the log as follows:

```
503 Login required, enter USER
```

When set to **y**, the utility prompts you for a user ID and password.

Default: n

Proxy Server for FTP Request

The following parameters are related to FTP proxy checks. Set the parameter to **yes** to activate FTP check through the proxy.

```
ftp.proxy.enabled=
ftp.proxy.host=
ftp.proxy.port=
ftp.proxy.credential.check=
ftp.proxy.fireCmd.proxy_userid=
ftp.proxy.fireCmd.site=
ftp.proxy.fireCmd.acct=
ftp.advanced.session.options=
```

The utility verifies the connection to the external CA Support FTP servers. If your site requires these requests to go through a proxy server, then modify these parameters as shown in the following example:

```
ftp.proxy.enabled=yes
ftp.proxy.host=host_name_or_IP_address
ftp.proxy.port=port_number
ftp.proxy.credential.check=n_or_y
```

When ftp.proxy.credential.check=y, change the following parameters:

```
ftp.proxy.fireCmd.proxy_userid=proxy_userid
```

The following parameters can be changed based on your proxy requirements:

```
ftp.proxy.fireCmd.site=
ftp.proxy.fireCmd.acct=
ftp.advanced.session.options=
```

Proxy Server for HTTP Request

The following parameters are related to HTTP proxy checks. Set the following parameter to **yes** to activate HTTP check through the proxy.

```
http.proxy.enabled=
http.proxy.host=
http.proxy.port=80
http.proxy.credential.check=
http.proxy.type=
http.domain=
```

The utility verifies the connection to the external CA Support HTTP servers. If your site requires these requests to go through a proxy server, then modify these parameters as shown in the following example:

```
http.proxy.enabled=yes
http.proxy.host=company_proxy_name
http.proxy.port=80
http.proxy.credential.check=y_or_n
http.proxy.type=NTLM
http.domain=company_domain_name
```

SAF Resource Access Check

SafSecurityResourceAccess=

The utility verifies user access for the following resources:

```
BPX.SERVER(UPDATE)
BPX.FILEATTR.SHARELIB(READ)
BPX.FILEATTR.PROGCTL(READ)
BPX.FILEATTR.APF(READ)
```

Specify SafSecurityResourceAccess=n to turn off the resource access check.

Default: y

MSMServerPortNo

MSMServerPortNo=

Specifies the port number to use as the application server HTTP port for web-based access to CA CSM.

Default: 22120

MSMDSIPORTNO

Specifies the port number for CA DSI Server, which CA CSM uses internally to provide security features.

Default: 22130

MSMConnectorRedirectPortNo

Specifies the port number to which a request is redirected. Redirection occurs if a request comes in on a non-SSL port and is subject to a security constraint with a transport guarantee that requires SSL.

Default: 22140

MSMTomcatServerShutdownPortNo

Specifies the port number to which the CA CSM application server listens for the shutdown command.

Default: 22150

Security Setup

To implement CA CSM successfully, your security administrator must set up the required security:

- Grant the required access to the user who downloads, installations, and sets up CA CSM.
- Grant the required access to the user ID associated with the CA CSM application server (see page 229) (MSMTC (see definition on page 232) job or started task).
- Set up security for users who use the web-based interface to log in to CA CSM.

More information:

Set Up User Security for CA CSM Functions (see page 34)

Security Setup on the CA CSM Application Server

The topics in this section describe how to set up security for CA CSM on the CA CSM application server (see page 229).

Configure CA CSM to Use HTTPS

Use this procedure to configure CA CSM to use HTTPS instead of HTTP for user access manually.

Follow these steps:

1. Perform the following steps to generate keystore:
   a. Start an OMVS session and enter the following command:

      ```
      keytool -genkey -alias tomcat -keyalg RSA
      ```

      A prompt appears.

      Note: *keytool* is a Java command that resides in the Java libraries. These libraries have a name similar to /*Customer-Java-Prefix*/ java/J6.0.1/bin/, where *Customer-Java-Prefix* is the Java USS directory name at your site. You can add this directory name in your USS profile path variable for successful command execution.

   b. Follow the prompt, remember your keystore password, and press Enter when you are prompted if you want to keep the default password.

      A default keystore is created in your home directory with one self-signed certificate inside.

c. (Optional) If you want a different location, enter the following command, replacing the /path/to/my/keystore portion with your site-specific information:

```
keytool -genkey -alias tomcat -keyalg RSA \ -keystore /path/to/my/keystore
```

2. Perform the following steps to configure Apache Tomcat:

a. Go to tomcat/conf and open the server.xml file.

b. Uncomment or replace the part with the SSL connector, as follows:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
   <Connector port="30308" maxHttpHeaderSize="8192"
              maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
              enableLookups="false" disableUploadTimeout="true"
              SSLEnabled="true"
              keystorePass="tomcat"
              keystoreFile="/a/path/to/my/keystore/.keystoreFile"
              algorithm="IbmX509"
              acceptCount="100" scheme="https" secure="true"
              clientAuth="false" sslProtocol="TLS"
               sslEnabledProtocols="TLSv1.2,TLSv1.1,TLSv1" />
```

c. Change the port and keystoreFile parameters to fit your needs.

d. Ensure that keystorePass matches the password that you specified in the previous step.

e. In the standard HTTP connector, provide the redirectPort to match the one you specified in the SSL connector, as follows:

```
<!-- Define a non-SSL HTTP/1.1 Connector on port 8080 -->
    <Connector port="30305" maxHttpHeaderSize="8192"
               maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
               enableLookups="false" redirectPort="30308"
               acceptCount="100"
               connectionTimeout="20000" disableUploadTimeout="true" />
    <!-- Note : To disable connection timeouts, set connectionTimeout
     value to 0 -->
```

3. Start (or restart) Apache Tomcat.

4. Enable your browser to use TLS encryption:

- If you use Microsoft Internet Explorer, click Tools, Internet Options, Advanced, and select the Use TLS 1.0 check box under Security.
- If you use Mozilla Firefox, click Tools, Options, Advanced, and select the Use TLS 1.0 check box on the Encryption tab.

5. Restart your browser.

6. Access the HTTPS URL.

   Note: When you access the HTTPS URL from your browser for the first time, you may be prompted to confirm that you trust the certificate.

7. Click Yes to add this certificate to your trusted certificates.

Note: For more information, see documentation for the Apache Tomcat 7.0 Servlet/JSP Container.

Set Up User Security for CA CSM Functions

CA CSM uses resource profiles (see page 189) in the CAMSM resource class to grant access to resources on the web-based interface. You use these profiles to configure user security. If you plan to enable security checking for CA CSM functionality, your security administrator must configure the security before users access the web-based interface.

The default name of the SAF resource class is CAMSM. You can change the resource class name during CA CSM installation. To change the name, edit the safResourceClass keyword in the CA CSM options file (see page 165).

If you want to change the setting after CA CSM is installed and set up, you can update the following statement in the SAMPLIB(MSMLIB) member:

```
IJO="$IJO-Dsaf.resource.class=saf_resource_class_name"
```

The safSecurity keyword in the CA CSM options file (see page 157) controls whether SAF resources are used to control access to CA CSM functions. If you want to change the setting after CA CSM is installed and set up, you can update the following statement in the SAMPLIB(MSMLIB) member. The value, false, disables security; and the value, true, enables security.

```
IJO="$IJO -Dactivate.saf.manager=false_or_true"
```

Important! If CA CSM fails to start with SAF security enabled (see page 217), the following error is displayed in the CA CSM job log:

SafError - Error during DSI java open. RC=13

The resource profiles provide granular access to resources. However, for a start, configure security for two generic roles, administrator and general user.

Follow these steps:

1. Configure user security by using the resource profiles.

   The users are secured for various roles.

2. Recycle the CA CSM application server.

   The configured security takes effect.

Note: We recommend that you use the same credentials that are used for performing product management work before CA CSM. Using the same credentials ensures that you have the same access rights within CA CSM that you have through TSO, BATCH, ISPF, and SMP/E.

For a change to user security privileges to take effect, recycle the CA CSM application server.

More information:

CA CSM Fails to Start with SAF Security Enabled (see page 217)
Security for CA CSM Functions (see page 187)

Security Setup on the Target Systems

The topics in this section describe how to set up security for CA CSM on the target systems.

More information:

SCS Address Space Security Setup (see page 119)

Authorizations and Permissions for SDS Access

Your System Administrator must ensure these requirements for usability. The CA CSM host must retrieve and delete output under the user credentials, so read and write permission is needed.

The Software Deployment Service (SDS) and CA Common Services need read and write access permissions to use and access your target system in the following areas:

- The remote SDS uses the SMP Work Directory (SMPWKDIR) as a scratch pad. GIMUNZIP and the SDS using PROC CCISPNSV use the scratch pad. Permissions must be set to allow users the correct access for read/write/delete/execute. The owner UID/GID must be the one that allows deployment users the ability to have read/write/execute within that work directory.

  Note: Only Started Task Class (STC) needs read access. The user needs read/write access.

- FTP and the landing directory are accessible by the CA CSM deployment remote services on the target system and permissions are based on the user credentials.

  Note: User needs read/write access.

- The security ID associated with the CCISPNSV started task requires a valid OMVS segment. CCISPNSV attaches a task that performs the utility functions for the deployment in your security context on the target system.

- Mount point is a directory path that must have write permission and must exist on the target system. The user ID that is doing the deployment must have write permission to this directory.

  The deployment user ID must have write permissions for the mount directory. The deployment user ID must have a mount that is authorized on the target system.

  Note: A mount user must have UID(0) or at least have READ access to the SUPERUSER.FILESYS.MOUNT resource found in the UNIXPRIV class.

Remote System Deployment Security Requirements

SDS relies on the SMP/E GIMZIP program. If you perform a deployment operation, you must have READ access to the GIM.PGM.GIMZIP SAF facility class resource on the CA CSM driving system. Also, you must have READ access to the GIM.PGM.GIMUNZIP SAF facility class resource on the CA CSM remote system.

If you are using the SAF CSFSERV (Cryptographic Services Facility) class, you must set permission to allow access using the CSFSERV class profile, CSFOWH (READ authority). SMP/E GIMUNZIP uses the CSFSERV class profile to perform the SHA-1 hash validation to ensure complete data integrity at your site.

Deployments with USS Parts and SUPERUSER Authority

If you create a deployment to a target system with USS parts and your UID has SUPERUSER authority, GIMUNZIP performs in a different manner than it does for non-SUPERUSER authority.

Note: CA CSM creates the Software Deployment Service (SDS) on the target system with the credentials that you define in CA CSM.

GIMUNZIP with SUPERUSER authority

When your UID has SUPERUSER authority, GIMUNZIP runs as the ROOT user. All directories that GIMUNZIP creates as ROOT, have the ROOT UID/GID .

The deployment USS parts (Owner and Permission) can be different from your expectations. Review the USS items that are created on the directory level. If necessary, switch to SUPERUSER mode to access the results of the USS parts on the target system. Use the deployed product documentation and your organization guidelines and standards to reset owner UID/GID and permissions as necessary.

GIMUNZIP without SUPERUSER authority

GIMUNZIP always attempts to switch to ROOT. If it cannot switch, it issues an information message to SMPOUT and continues to operate with your UID/GID.

Remote Deployment Service USS Considerations

The Software Deployment Service (SDS) runs as a batch z/OS UNIX program. If your system CEEOPTXX member has MSGFILE(SYSPRINT), then CEEOPTS DD is required in CCISPNSV to override MSGFILE to MSGFILE(SYSOUT,FBA,121,0,NOENQ). MSGFILE(SYSOUT,FBA,121,0,NOENQ) is the non-CICS default.

Authorizations and Permissions for SCS Address Space Access

Perform specific tasks to get the SCS address space running on a system (see page 113). The SCS address space security setup is performed on every target system which can include the CA CSM driving system.

USS Path Setup

Note: We recommend using zFS file systems. For information about how to migrate from HFS file systems to zFS file systems, see the latest *IBM z/OS Migration* guide.

You can define the file systems to mount at system initialization in the SYS1.PARMLIB(BPXPRM*xx)* member using the MOUNT statement. Specify the file systems with the SETUID option as part of the MSMSetup process.

More information:

USS File Systems (see page 175)

USS Paths

CA CSM can use HFS or zFS file systems for its download, installation, setup, and general usage.

Note: We recommend using zFS file systems. For information about how to migrate from HFS file systems to zFS file systems, see the latest *IBM z/OS Migration* guide.

Before you download and install CA CSM, your USS administrator must set up directory paths for these files. A simple setup is to create four directories with 775 permissions in your existing file system, for example:

/parent_path/msmserv/mpm
/parent_path/msmserv/*version_number*/msm
/parent_path/msmserv/*version_number*/msmruntime
/parent_path/msmserv/*version_number*/msminstall

where *parent_path* is the CA CSM parent path name as defined at your site as the primary mount point or directory, for example:

```
/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.

The required space is 2500 cylinders.

/u/users/msmserv/mpm is a special path that serves as a mount point for file systems that CA CSM allocates and mounts during startup.

Chapter 3: Installing and Setting Up CA CSM

This section contains the following topics:

Download and Unpack CA CSM Files

The packed CA CSM product package is available on the CA Support Online website. Before you install CA CSM, download and run the Prerequisite Validator utility (see page 27).

Note: The Prerequisite Validator is also available on the CA Support Online website. You can separately download the Prerequisite Validator and the associated information.

After you have successfully run the Prerequisite Validator utility, you can go back to the CA Support Online website and download the full CA CSM package. Then, you are ready to install CA CSM.

Follow these steps:

1. Go to the Download Center on the CA Support Online website.
2. Enter CA Chorus Software Manager in the Select a Product field, select the latest version and the Select all components check box, and click Go.

   Note: If you cannot find CA Chorus Software Manager in the product list, follow the instructions from the Free Service area on the top of the product page.

   A list of product downloads is displayed.
3. Download the software package.

After you download the software package, unpack and extract the files for installation.

Important! Verify that the unpacked CA CSM packages are stored on permanent storage volumes, and not on work or temporary volumes.

Follow these steps:

1. Go to the directory where the CA CSM package is downloaded, and enter the following command to unpack the package:

   ```
   pax -rvf 51000068X01.pax.Z
   ```

   Note: The full pax file name, including the Z suffix, is case-sensitive. Verify that you use the exact case of the file name on the system where you issue the pax command. Rename the file, if necessary.

   The MSMInstaller directory is created, and the package is unpacked into the directory.

2. Customize the UNZIPJCL file in the MSMInstaller directory to conform to the data set and USS directory naming standards at your site. Submit the job (for example, using the submit z/OS shell command in USS OMVS), and review the output for successful completion.

   The UNZIPJCL job creates the MSMSetup and the MSMProduct directories that contain the CA CSM installation files.

   - Replace the following text with the path where the MSMInstaller directory was created:

     ```
     <-- YOUR USS HFS DIRECTORY -->
     ```

   - Replace the following text with the path where you want to create the MSMSetup and MSMProduct directories:

     ```
     <-- YOUR CA CSM USS HFS DIRECTORY -->
     ```

     Note: We recommend that the directories <-- YOUR USS HFS DIRECTORY --> and <-- YOUR CA CSM USS HFS DIRECTORY --> are set to the same path.

   - Replace **yourHLQ** with the high-level qualifier for the ISPF UI Tool data set. The length of the high-level qualifier must not be greater than 26 characters.

   The MSMSetup directory, the MSMProduct directory and the CA CSM Installation ISPF UI tool z/OS data set are created, and the CA CSM files are extracted.

   Note: When you open the UNZIPJCL file, a warning message can appear at the bottom of the screen. This message indicates that any trailing blanks are removed from the UNZIPJCL file. Removing or retaining trailing blanks does not affect job execution. You can ignore this message.

Specify Installation and Setup Options

The directory (…/MSMSetup) where you extracted the CA CSM files contains the MSMSetupOptionsFile.properties options file. The CA CSM setup utility uses the contents of this file to tailor the CA CSM installation and setup process. The file contains preset values. Customize the contents of this file to reflect your requirements. You specify each option in the following format:

option_keyword=value

To specify installation and setup options manually, review and customize the options (see page 157) using an EBCDIC character set capable text editor. For example, use Interactive System Productivity Facility (ISPF). If necessary, consult with other team members at your site to gather the values.

If you already use CA CSM, you can run a USS shell utility to copy values from the previous version options file to the current options file (see page 49).

You can also use the CA CSM Installation ISPF UI Tool (see page 41), which helps to gather site values and prefill most of the options file parameters. Consult with other team members at your site to review these prefilled values as necessary.

Note: If your site uses Storage Management Subsystem (SMS) automatic class selection (ACS), ACS overrides the storage parameter values in the options file.

More information:

Options File Keywords (see page 157)

Specify Options Automatically with ISPF UI Tool

You can use the CA CSM Installation ISPF UI Tool to specify options automatically. The tool helps you perform the following tasks:

- Gather site values for most of the parameters
- Provide JCLs to create required USS file systems, and make edits to this options file before installing CA CSM

Your 3270 emulator must be able to support ISPF dialogs that are up to 35 rows.

Note: If the setting that shows the ISPF command line at the bottom of the dialog is enabled, the ISPF UI Tool may not display some ISPF dialogs correctly. It may result in displaying an option on the bottom line of the ISPF dialog and out of place with the other options. To avoid this situation, exit the ISPF UI Tool, temporarily disable this option, and then start the UI Tool. You can later enable this option again.

Important! The UI Tool does not detect the complete hostname when the hostname is longer than 26 characters.

Follow these steps:

1. Go to TSO/ISPF option 6 and run the following command:

   exec '*data_set_name*(#RUNTOOL)'

   data_set_name

   Defines the name of the CA CSM Installation ISPF UI Tool z/OS data set extracted using UNZIPJCL.

   Example: CAI.MF20.MSMI.UITOOL

   The main ISPF panel appears.

2. Enter 1 to gather your site values for prefilling the options file parameters.

   You are prompted to provide the Java home path and MSMSetup directory path.

   The programs located in the USS MSMSetup folder get executed through this interface and it gathers site values for some of the parameters. The gathered values are stored in an XML file. This file is used to prefill the options file queries for easier and faster editing of the CA CSM installation options file.

3. Enter 6 or 7 to edit the options file.

   The options in this group let you prefill the options file with site-gathered values, or edit it directly from TSO using the ISPF editor.

   Using prefilled site values

   Use this option (option 6) to review all the installation option parameters and their prefilled value. The values are already included with Installer-set defaults to facilitate editing and reviewing.

   - Values that are prefaced with S indicate gathered site values.
   - Values that are prefaced with D indicate product default values.
   - Values that are prefaced with U indicate that the value has been edited.

   Enter **/** before each parameter to display the available values (S/D/U), which you can also select and modify.

Parameters are listed on multiple pages. You can move forward (Enter) and backward (PF3) to review each screen after all the parameters have been edited and verified.

The ISPF UI tool edits all the panels and it verifies them. Then the tool displays the path and command to invoke the installation utility.

Using ISPF Editor

Use this option (option 7) to edit the options file manually using the ISPF editor from TSO/ISPF.

After the CA CSM Installer is invoked, if any of the parameter validations fail, you can edit the options file again.

Install and Set Up CA CSM

The directory (.../MSMSetup) where you extract the CA CSM files contains the MSMSetup.sh setup utility that installs and sets up CA CSM.

Note: CA CSM is an SMP/E-installed and serviceable product.

The utility uses the contents of the options file to tailor the overall process. The utility sets up an Apache Tomcat application server, the CA Datacom/MSM database, the CA CSM service components, and the web-based interface. The utility creates and sets up a runtime environment for CA CSM.

If you are an existing CA CSM customer, the utility sets up the new environment. The utility also migrates the previous version database according to the options file values.

The utility has a restart mechanism to continue installation when reinvoked after addressing an earlier failed run. The utility also lets you select installation from scratch on earlier failed runs. If any of the options file parameters affect the completed stages during restart mode, the utility forces a start from scratch installation.

At the start, the utility checks if data sets and USS folders with the values set in option parameters exist. If they exist, the utility prompts you to overwrite the previous installation files or continue the process without overwriting.

The utility verifies availability of port numbers that are passed through the options file. If they are reserved, already in use or unavailable for other reasons, the utility prompts you to use the provided values and continue the installation.

Consider the following information:

- Before you start installing CA CSM, verify that your TSO region size is at least 143360 KB.
- Invoke the MSMSetup.sh script directly from the TSO OMVS environment (native USS command prompt).
- You cannot invoke the MSMSetup.sh utility from a z/OS Telnet session or an ISHELL command shell.
- MSMSetup.sh requires a userid with UID(0) or SUPERUSER authority.
- If your site has SMS ACS rules to force POU to PDSE, these settings cause the installation job CSMN5102 (for a new installation) or CSMU*xx*02 (for an upgrade) to fail. The MSMSetup.sh requires POU data sets to be created as PDS data sets.
- If you want to adjust JCL space allocation (see page 100), run the CA CSM installer in a Manual mode or Review installation mode.

Follow these steps:

1. Verify that you extracted the files from the downloaded CA CSM package (see page 39).

   The MSMSetup and MSMProduct directories exist, and CA CSM files are extracted to the directories.

2. Edit the MSMSetupOptionsFile.properties options file (see page 157) to ensure that the file conforms to the requirements of your site.

   - If you already use CA CSM, you can run a USS shell utility to copy values from the previous version options file to the current options file (see page 49).
   - Migrate your current database (see page 50) to the new version by setting options in CA CSM for upgrades.

3. Verify that the required USS paths (see page 38) are available.
4. Verify that you are using a userid with UID(0). If you are not, issue the su command to switch to UID(0).

5. Go to the directory where the MSMSetup.sh setup utility resides, and execute the utility, for example, from OMVS:

   ```
   sh MSMSetup.sh
   ```

   This utility verifies the existence of the following:

   - MSMSetupOptionsFile.properties file in the current path.
   - Valid JAVAPATH parameter field in the Options file.
   - Supported Java SDK version is installed.

   Note: The setup utility is interactive, requiring user responses until completion. The output is written to a log file, MsminstallerLog*yyyy-mm-dd*,*hh-mm-ss*,*ttt*.log, in the MSMSetup directory. If you rerun the utility after a failure, the utility will perform the necessary cleanup steps for the previous execution.

   A panel appears that provides information about the utility. Then, the license agreement appears.

   This license agreement covers an agreement to allow CA Technologies to accumulate minimal information pertaining to the product acquisition activity. This information includes the site ID, the product, and the user ID for the CA Support Online website. Sometimes site access rules deny an FTP connection that is established for this purpose or the connection cannot be established for any other reason. Then CA CSM still continues to function.

   Note: If you are migrating to the latest version of CA CSM, verify that the previous CA CSM version is not running during this migration.

6. Review the license agreement, and press PF3.

   You are prompted to accept the agreement.

   Note: If the license agreement is not displayed, verify that the TSO OMVS libraries are allocated in your TSO environment.

7. Enter **Y** to accept the agreement.

   (Non-UID(0) installation only) If you are executing the installation utility with a userid that is not assigned UID(0), you are asked whether the installer should immediately stop to switch to a userid that is assigned UID(0).

   Note: A userid with UID other than 0 may encounter errors while files are copied and their attributes and permissions are modified. These errors typically indicate that the *Operation is not permitted*. Usually, the installation utility catches this type of errors and results in a premature, unsuccessful termination. In most cases, restarting the installation utility with a userid that has UID(0) assigned successfully restarts and completes the installation.

   However, this type of errors may go undetected. In such cases, a successful restart of the installation utility may be very difficult. You are required to delete all unpaxed files, installed files, and restart the installation from the beginning.

8. (Non-UID(0) installation only) Enter Y (Yes) or N (No) in response to the prompt. We highly recommend that you reply N (No) to the installation utility, stop the installation, and switch to a userid that is assigned UID(0). You do so by running in superuser mode. To run in superuser mode, issue the su command at the OMVS command prompt, and then rerun the installation utility.

   If you reply Y (Yes), the installation continues.

9. Monitor the utility as it verifies that system and software prerequisites are satisfied, and validates the contents of the options file.

   (Optional) If the IP address taken from the system fails to connect, provide a host name or IP address that supports FTP for processing batch jobs.

10. Specify one of the following installation modes for processing the CA CSM installation jobs:

    A

    In Automatic mode, installation jobs are submitted automatically in non-stop mode (the submitted jobs are not shown before submission).

    R

    In Review mode, you are prompted to review each installation job before submission.

    M

    In Manual mode, submit each installation job manually after the setup process.

    Note:

    - If you submit your installation job using TSO, the installer only runs in Manual mode.
    - The Installer can require more memory than 17200 KB.
    - If you restarted after an earlier failed point, you are prompted to select a start from an earlier failed point or scratch.
    - If you have selected FTP mode for installation job submission, you are prompted to enter your z/OS credentials.

11. (FTP mode only) Enter your user ID and then your password.

    If you make a mistake entering the user ID or password, you have two more attempts to reenter your credentials. A Yes/No prompt precedes the second and third attempts.

    Yes

    Allows you to reenter your credentials.

    No

    Terminates the installation procedure.

    The installation procedure terminates after the third failed attempt to validate your FTP credentials. Once you resolve this issue, restart the installation script.

    The utility displays the JOB statement, and the JOBPARM statement (for JES2 environment) or the MAIN statement (for JES3 environment) for review and modification (if necessary).

12. Take one of the following steps in response to the Edit Job Card question:

    - If your site does not require additional parameters, enter **N**. The installation process continues.
    - If your site requires additional parameters, enter **Y**. The job card opens in edit mode. Modify the job card, and press PF3 to save the changes and continue the installation process.

      Note: If CA View is running on the host system, uncomment the following statements. Then, fill them in based on the initialization parameters used in SARINIT upon setting up CA View:

      - The OUTPUT statements SARPRT and JESPRT in the JOBCARD
      - The CLASS option in both SARPRT and JESPRT statements

13. Monitor the utility as it customizes all the required installation jobs.

    (Optional) If you selected Review installation mode, you are prompted to review installation jobs one by one. Modify a job and press PF3 to save your changes and submit the job.

14. Monitor the utility as it creates the SMP/E environment for CA CSM, and sets up the CA CSM components.

    The utility performs the following steps:

    - Submits the previously modified jobs one by one and copies the customized JCL into the runtime JCL PDS.

      Note: If executing a job takes longer than the JobCompletionWaitMaxTime options file keyword specifies, the utility asks if you want to continue waiting. Enter **N** to terminate the whole installation process.

    - Customizes the CA Datacom/MSM environment including CA Datacom/MSM address spaces and connection pools.

- Customizes the Apache Tomcat environment including the server.xml and context.xml files, port numbers, the connection pool, and the user XML configuration.
- Customizes and copies JCL for the runtime PROCLIB PDS.
- Customizes and copies JCL for the runtime JCL PDS.
- Prepares CA CSM for the CAICCI interface and copies the LIBCCI and LIBCCI6E modules and the customized job COPYCCI to the run-time JCL PDS member COPYCCI. The COPYCCI job does *not* need to be run as part of the installation process. This job is provided as a convenience to reload these modules, if needed. For example, if these modules are updated through maintenance procedures, you can copy the updates into the CA CSM run time.

After the last step completes, the utility displays an installation summary report (MSMSummaryReport.txt). The report is stored in the MSMSetup directory. This report provides the URL required to access CA CSM from a web browser.

The setup utility completes its process.

15. Review the summary report, MSMSummaryReport.txt, for specific post-installation job submission that is required to complete the overall CA CSM installation.

    Submit the installation jobs CSMN51*yy* (if you are doing a new installation (see page 51)) or CSMU*xxyy* (if you are upgrading from a previous version (see page 53)), as specified in the summary report. *xx* indicates the version number that you are upgrading from, *yy* indicates the sequence number of the job.

    Note: Submit the installation jobs manually after MSMSetup.sh finishes, regardless of the installation mode that the CA CSM installer is running in.

16. Verify that the following libraries in the STEPLIB of the JCL(MSMMUF) job are APF-authorized:

    - CAAXLOAD and CUSLIB CA Datacom/MSM libraries
    - The CA Common Services for z/OS library that the CCSdsn keyword in the options file specifies

    For the libraries to remain APF-authorized after the next IPL, add the libraries to your permanent APF list.

    Note: If the value of the AddAPFauthDSdyn keyword in the options file is N, try to APF-authorize these libraries manually.

17. Verify that the user ID associated with the CA CSM application server (MSMTC job or started task) has the required USS access authority.

    CA CSM can create and mount file systems.

18. Verify that your network configuration permits CA CSM to access the following websites:

    - supportservices.ca.com (using HTTPS Port Number 443)
    - ftp.ca.com (using FTP Port Number 21)

- ftpca.ca.com (using FTP Port Number 21)

  Note: CA CSM uses this FTP server to accumulate minimal information. This information includes the site ID, the product, and the user ID for the CA Support Online website. Sometimes site access rules deny an FTP connection that is established for this purpose or the connection cannot be established for any other reason. Then CA CSM still continues to function.

- scftpd.ca.com (using FTP Port Number 21)
- ftpdownloads.ca.com (using FTP Port Number 21)
- supportftp.ca.com (using FTP Port Number 21)
- sdownloads.ca.com (using HTTPS Port Number 443)

  Note: sdownloads.ca.com is only required if you use the Use HTTPS for Downloads acquisition option under System Settings, Software Acquisition on the Settings page. If you authorize the ca.com domain for both ports 80 and 443, you do not need to authorize sdownloads.ca.com.

In addition, your network administrator must define a Domain Name System (DNS) entry for localhost.

19. Start CA CSM (see page 62).

    CA CSM becomes operational.

Copy Options File Keywords

You can copy keyword values from a previous version of CA CSM for easier and quicker customization.

Note: This procedure only applies if you are upgrading from a previous version of CA CSM, and it is optional.

Follow these steps:

1. Go to the directory where the MSMSetup.sh setup utility resides.

   You can use one of the following methods to find the MSMPATH for the previous version:

   - The path that is specified in CA CSM Product Installed Path of the summary report for the previous version (MSMSummaryReport.txt) for CA CSM Product Installed Path
   - The path that is specified in the MSMPATH keyword in MSMSetup folder MSMSetupOptionsFile.properties options file for the previous version

2. Execute the utility.

   For example, use the following command to execute the utility from USS OMVS:

   `sh MSMSetup.sh copyOPT PreviousRelease.MSMPATH`

   PreviousRelease.MSMPATH

   Path where CA CSM target files for the previous version are located.

   Example: /u/users/msmserv/msm

   The utility looks for the previous version options file in the following location:

   PreviousRelease.MSMPATH/CEGPHFS/MSMSetupOptionsFile.properties.

   The utility copies all available values from the previous version options file to the current options file to fill in missing corresponding keywords.

When the utility finishes, the modified MSMSetupOptionsFile.properties options file appears in edit mode. You can customize it to conform to the requirements of your site.

Important! Review keyword values against the previous system version and user configuration settings in the previous version of CA CSM user interface. During migration, two keywords, MVSHFSDsnPrefix and MountPath, specified in the options file must be the same as in the previous version. All other system and user setting keywords can be modified during the migration.

More information:

Options File Keywords (see page 157)

Database Upgrade

Note: This topic only applies if you are upgrading from a previous version of CA CSM. The setup process creates the migration jobs. The jobs are executed according to the selected installation mode.

The PreviousRelease.MSMPATH options file parameter in the MSMSetupOptionsFile.properties options file must be populated with the same value as the previous application installation path. This practice ensures that the migration jobs are automatically generated.

When migrating CA CSM from a previous version, verify that parameters MVSHFSDsnPrefix and MountPath in the current and previous MSMSetupOptionsFile.properties have the same values as the previous version of CA CSM. During installation, if these parameters are not the same between CA CSM versions, the CA CSM installer displays an error message for the corresponding property and exits the installation.

Note: Two installation jobs are run regardless of the selected install mode. The first job backs up the CA Datacom/MSM database files of your previous installed version of CA CSM, and the second job unpacks the contents of the CA CSM pax files.

The following installation modes are available while performing an upgrade:

A

In Automatic mode, installation jobs are submitted automatically in non-stop mode (the submitted jobs are not shown before submission).

R

In Review mode, you are prompted to review each installation job before submission.

M

In Manual mode, submit each installation job manually after the setup process.

Installation Jobs

The CA CSM setup utility submits jobs as part of a setup process. The job that unpacks the CA CSM contents (CSMN5102 for new installations and CSMU*xx*02 for upgrades) is submitted using a setup process by default regardless of the installation mode. The setup process performs the required configurations and creates the runtime path.

Notes:

- The installation job CSMU*xx*01 backs up your existing version data and prepares converted data for the latest version population. When upgrading from a previous version of CA CSM, the installation job CSMU*xx*01 is submitted first for all installation modes. In Manual mode, the script submits the installation jobs CSMU*xx*01 and CSMU*xx*02.
- If you are running in Manual mode, run all jobs in the sequence presented in this section.

Installation Jobs for a New Installation

The following jobs are created when you are performing a new installation of CA CSM:

CSMN5101

This member is only a placeholder to enforce and coincide with the job sequencing for an upgrade. It is not a job and it is not to be executed.

CSMN5102 (Unpack CA CSM Product)

Unpacks the z/OS and USS contents.

CSMN5103 (Customize CA CSM SMP/E Environment)

Customizes the SMP/E environment data set UCLIN statements with the site-specific values provided through the options file.

CSMN5104 (Assemble/Linkedit CA Datacom/MSM db system module)

Assembles and link-edits the CA Datacom/MSM system ID module with the site-specific values provided in the options file.

CSMN5105 (Load CA Datacom/MSM SVC)

Executes CAIRIM module to load the CA Datacom/MSM SVC.

CSMN5106 (Allocate and Load CA Datacom/MSM Database Data Sets)

Allocates and loads the CA Datacom/MSM database data sets.

CSMN5107

This member is only a placeholder to enforce and coincide with the job sequencing for an upgrade. It is not a job and it is not to be executed.

CSMN5108 (Start the CA Datacom MUF)

This job starts the CA Datacom/MSM MUF.

Note: Run this job manually, even if you are running the CA CSM installer in Automatic or Review mode. The job CSMN5108 is a running task. Before you submit the next job, review the JES Active Queue to determine if the job CSMN5108 is executing.

CSMN5109 (Confirm database tables and backup the new installed database)

Verify that MSMDBSVS (CA Datacom/DB server) and MSMTCSRV (Apache Tomcat) are not active.

This job confirms the CA Datacom/MSM database tables and creates a backup of the latest CA Datacom/MSM installed database.

Note: Run this job manually, even if you are running the CA CSM installer in Automatic or Review mode.

CSMN5110 (Stop the CA Datacom MUF)

This job stops the CA Datacom/MSM MUF.

Note: Run this job manually, even if you are running the CA CSM installer in Automatic or Review mode.

Installation Jobs for an Upgrade

The installer generates unique JCL necessary for the type of installation and installation options that you specified according to the following rules:

CSMU*xxyy*

xx

Indicates the version number that you are upgrading from.

yy

Indicates the sequence number of the job.

For example, if you are upgrading from CA MSM R4.1, the job numbers will be CSMU4101, CSMU4102, …, CSMU4110.

The following jobs are created if you are performing an upgrade of your current CA CSM database to the latest CA CSM version:

CSMU*xx*01 (Backs up existing CA CSM data)

Backs up your existing previous version CA Datacom/MSM data.

CSMU*xx*02 (Unpack CA CSM Product)

Unpacks the z/OS and USS contents.

CSMU*xx*03 (Customize CA CSM SMP/E Environment)

Customizes the SMP/E environment data set UCLIN statements with the site-specific values provided through the options file.

CSMU*xx*04 (Assemble/Linkedit CA Datacom/MSM db system module)

Assembles and link-edits the CA Datacom/MSM system ID module with the site-specific values provided in the options file.

CSMU*xx*05 (Load CA Datacom/MSM SVC)

Executes CAIRIM module to load the CA Datacom/MSM SVC.

CSMU*xx*06 (Allocate and Load CA Datacom/MSM Database Data Sets)

Allocates and loads the CA Datacom/MSM database data sets.

CSMU*xx*07 (Data migration)

Migrates the previous CA Datacom/MSM database to the latest version.

CSMU*xx*08 (Start the CA Datacom MUF)

This job starts the CA Datacom/MSM MUF.

Note: Run this job manually, even if you are running the CA CSM installer in Automatic or Review mode. The job CSMU*xx*08 is a running task. Before you submit the next job, review the JES Active Queue to determine if the job CSMU*xx*08 is executing.

CSMU*xx*09 (Confirm database tables and backup the new installed database)

Verify that MSMDBSVS (CA Datacom/DB server) and MSMTCSRV (Apache Tomcat) are not active.

This job matches the requirements specific to the CA CSM version that you are upgrading from. For all versions, this job confirms the CA Datacom/MSM database tables and creates a backup of the latest CA Datacom/MSM installed database. However, if you are upgrading to the latest version, this job contains additional JCL steps specific to the CA CSM version that you are upgrading from.

If this job fails, review the error message to determine the cause of the problem. Take appropriate actions to correct the situation. Before you resubmit this job, perform the following actions:

- Bring down the CA Datacom/MSM MUF by submitting the CSMU*xx*10 JCL member.
- Resubmit job CSMU*xx*07.
- Bring up the CA Datacom/MSM MUF by submitting the CSMU*xx*08 JCL member, or start the MSMMUF PROCLIB member.

Note: Run this job manually, even if you are running the CA CSM installer in Automatic or Review mode.

CSMU*xx*10 (Stop the CA Datacom MUF)

This job stops the CA Datacom/MSM MUF.

Note: Run this job manually, even if you are running the CA CSM installer in Automatic or Review mode.

Setting Up CA CSM User ID Without UID(0)

After the CA CSM installation is complete, you can configure CA CSM not to use UID(0) when running.

This section contains the following topics:

Prerequisites (see page 55)

Set Up CA CSM User ID Without UID(0) for CA Top Secret for z/OS (see page 55)

Set Up CA CSM User ID Without UID(0) for CA ACF2 for z/OS (see page 56)

Set Up CA CSM User ID Without UID(0) for IBM RACF (see page 58)

Prerequisites

To run CA CSM without UID(0), ensure that the following requirements are met:

- The CA CSM user ID that is associated with the CA CSM application server must have a UID other than 0.
- The first user to log in to CA CSM must have a UID other than 0.

  Note: The LJWK directory and the mount point are created using the user ID of the first user instead of the CA CSM user ID (*CA_CSM_USER_ID*).

Set Up CA CSM User ID Without UID(0) for CA Top Secret for z/OS

Modify this procedure according to your security system settings.

Follow these steps:

1. Review the prerequisites (see page 55).
2. After the installation of CA CSM finishes, create a group, for example, CACSMGRP with a GID definition in your security system, and perform the following steps:
   a. Add CACSMGRP as DFLTGRP to each CA CSM user.
   b. Add CACSMGRP as DFLTGRP to the CA CSM user ID.
3. Change the owner and the group by issuing the following commands under SUPERUSER authority:

   ```
   chown –R CA_CSM_USER_ID MSMPATH
   chgrp –R CACSMGRP MSMPATH
   chown –R CA_CSM_USER_ID MountPath
   chgrp –R CACSMGRP MountPath
   chown –R CA_CSM_USER_ID RunTimeUSSPath
   chgrp –R CACSMGRP RunTimeUSSPath
   ```

   where MSMPATH, MountPath, and RunTimeUSSPath (see page 157) are values that are referenced in the MSMSetupOptionsFile.properties file.

   Note: When you issue the commands for *RunTimeUSSPath*, the following message can appear:

   ```
   EDC5129I No such file or directory
   ```

   This message is issued against the ioeagfmt file and does not affect command completion in any way. You can ignore this message.

   Important! Also, issue these commands after you run the MSMDEPLY job.

4. Set the parameters for the CA CSM user ID:
   a. Assign Facility STC.
   b. Assign Master FAC=MSM.

      Note: Before you do so, verify that Master FAC exists.

   c. Assign this MASTFAC to each CA CSM user.
5. Assign the following required IBMFAC class permissions to the CA CSM user ID:

```
IBMFAC BPX.CONSOLE ACCESS(UPDATE)
IBMFAC BPX.SERVER  ACCESS(UPDATE)
IBMFAC BPX.FILEATTR.APF ACCESS(READ)
IBMFAC BPX.FILEATTR.PROGCTL ACCESS(READ)
IBMFAC BPX.FILEATTR.SHARELIB ACCESS(READ)
```

6. Assign the following required UNIXPRIV class permissions to the CA CSM user ID:

```
UNIXPRIV SUPERUSER.FILESYS.CHANGEPERMS ACCESS(READ)
UNIXPRIV SUPERUSER.FILESYS.MOUNT ACCESS(UPDATE)
UNIXPRIV SUPERUSER.FILESYS.PFSCTL ACCESS(READ)
```

7. Assign the following optional SERVAUTH class permissions, to the CA CSM user ID:

```
SERVAUTH EZB.FTP ACCESS(READ)
SERVAUTH EZB.STACKACCESS ACCESS(READ)
```

8. After the first task within CA CSM finishes, issue the following commands under SUPERUSER authority:

```
chown –R CA_CSM_USER_ID MountPath
chgrp –R CACSMGRP MountPath
```

   where MountPath (see page 157) is a value that is referenced in the MSMSetupOptionsFile.properties file.

Set Up CA CSM User ID Without UID(0) for CA ACF2 for z/OS

Modify this procedure according to your security system settings.

Follow these steps:

1. Review the prerequisites (see page 55).
2. After the installation of CA CSM finishes, create a group with a GID definition, for example, CACSMGRP, in your security system, and perform the following steps:
   a. Define the CA CSM user ID as a member of CACSMGRP.
   b. Define each CA CSM user as a member of CACSMGRP.

3. Change the owner and the group by issuing the following commands under SUPERUSER authority:

   ```
   chown –R CA_CSM_USER_ID MSMPATH
   chgrp –R CACSMGRP MSMPATH
   chown –R CA_CSM_USER_ID MountPath
   chgrp –R CACSMGRP MountPath
   chown –R CA_CSM_USER_ID RunTimeUSSPath
   chgrp –R CACSMGRP RunTimeUSSPath
   ```

   where MSMPATH, MountPath, and RunTimeUSSPath (see page 157) are values that are referenced in the MSMSetupOptionsFile.properties file.

   Note: When you issue the commands for *RunTimeUSSPath*, the following message can appear:

   ```
   EDC5129I No such file or directory
   ```

   This message is issued against the ioeagfmt file and does not affect command completion in any way. You can ignore this message.

   Important! Also, issue these commands after you run the MSMDEPLY job.

4. In the FACILITY resource class, define the following resource names with access rights to the CA CSM user ID:

   ```
   BPX.CONSOLE             UPDATE
   BPX.SERVER              UPDATE
   BPX.FILEATTR.APF        READ
   BPX.FILEATTR.PROGCTL    READ
   BPX.FILEATTR.SHARELIB   READ
   ```

5. In the UNIXPRIV resource class, define the following resource names with access rights to the CA CSM user ID:

   ```
   SUPERUSER.FILESYS.CHANGEPERMS    READ
   SUPERUSER.FILESYS.MOUNT          UPDATE
   SUPERUSER.FILESYS.PFSCTL         READ
   ```

6. In the SERVAUTH resource class, define the following resource names with access rights to the CA CSM user ID:

   ```
   EZB.FTP           READ
   EZB.STACKACCESS   READ
   ```

7. After the first task within CA CSM finishes, issue the following commands under SUPERUSER authority:

   ```
   chown –R CA_CSM_USER_ID MountPath
   chgrp –R CACSMGRP MountPath
   ```

   where MountPath (see page 157) is a value that is referenced in the MSMSetupOptionsFile.properties file.

Set Up CA CSM User ID Without UID(0) for IBM RACF

Modify this procedure according to your security system settings.

Follow these steps:

1. Review the prerequisites (see page 55).
2. After the installation of CA CSM finishes, create a group with a GID definition, for example, CACSMGRP, in your security system, and perform the following steps:
   a. Define the CA CSM user ID as a member of CACSMGRP.
   b. Define each CA CSM user as a member of CACSMGRP.
3. Change the owner and the group by issuing the following commands under SUPERUSER authority:

   ```
   chown –R CA_CSM_USER_ID MSMPATH
   chgrp –R CACSMGRP MSMPATH
   chown –R CA_CSM_USER_ID MountPath
   chgrp –R CACSMGRP MountPath
   chown –R CA_CSM_USER_ID RunTimeUSSPath
   chgrp –R CACSMGRP RunTimeUSSPath
   ```

   where MSMPATH, MountPath, and RunTimeUSSPath (see page 157) are values that are referenced in the MSMSetupOptionsFile.properties file.

   Note: When you issue the commands for *RunTimeUSSPath*, the following message can appear:

   ```
   EDC5129I No such file or directory
   ```

   This message is issued against the ioeagfmt file and does not affect command completion in any way. You can ignore this message.

   Important! Also, issue these commands after you run the MSMDEPLY job.
4. In the FACILITY resource class, define the following profiles with access rights to the CA CSM user ID:

   ```
   BPX.CONSOLE             UPDATE
   BPX.SERVER              UPDATE
   BPX.FILEATTR.APF        READ
   BPX.FILEATTR.PROGCTL    READ
   BPX.FILEATTR.SHARELIB   READ
   ```
5. In the UNIXPRIV resource class, define the following profiles with access rights to the CA CSM user ID:

   ```
   SUPERUSER.FILESYS.CHANGEPERMS   READ
   SUPERUSER.FILESYS.MOUNT         UPDATE
   SUPERUSER.FILESYS.PFSCTL        READ
   ```

6. In the SERVAUTH resource class, define the following profiles with access rights to the CA CSM user ID:

   ```
   EZB.FTP           READ
   EZB.STACKACCESS   READ
   ```

7. After the first task within CA CSM finishes, issue the following commands under SUPERUSER authority:

   ```
   chown –R CA_CSM_USER_ID MountPath
   chgrp –R CACSMGRP MountPath
   ```

   where MountPath (see page 157) is a value that is referenced in the MSMSetupOptionsFile.properties file.

Configure Mount Parameters for CA CSM File Systems

Depending on your site and environment requirements, you can configure mount parameters for CA CSM product, software catalog, temporary, and deployment file systems. For example, you can decide whether to perform security checks or how to proceed if the system that owns a file system goes down.

Initially, CA CSM uses the default values of these parameters. You can override the defaults.

Follow these steps:

1. Do one of the following:
   - Manually unmount all file systems.
   - In CA CSM, navigate to the Settings tab, the Mount Point Management page, and select the Unmount at Shutdown check box. Save the changes.
2. Stop the CA CSM application server.
3. Insert and modify the following line into the *RunTimeMVSHLQPrefix*.SAMPLIB(MSMLIB) member:

   ```
   IJO="$IJO -DADD_MOUNT_DEFAULT_OPTIONS=SETUID|NOSETUID,SECURITY|NOSECURITY,
   AUTOMOVE|NOAUTOMOVE|UNMOUNT"
   ```

SETUID|NOSETUID

Specifies whether the setuid() and setgid() mode bit is supported.

SETUID

Supports the setuid() and setgid() mode bit on an executable file. This option is the default.

NOSETUID

Disables the setuid() and setgid() mode bit support on an executable file. When the program is executed, the UID or GID are not changed, and the APF and Program Control extended attributes are not honored. The entire HFS is uncontrolled.

SECURITY|NOSECURITY

Specifies whether to perform the UNIX permissions checks.

SECURITY

Enables the UNIX permissions checks. This option is the default.

NOSECURITY

Disables the UNIX permissions checks. Any new files or directories that are created are assigned an owner of UID(0), no matter what UID issued the request. A user may access or change any file or directory.

AUTOMOVE|NOAUTOMOVE|UNMOUNT

For a sysplex where systems participate in a shared file system, specifies how to proceed if the system that owns a file system goes down.

AUTOMOVE

Automatically changes ownership of the file system to another system that participates in a shared file system. This option is the default.

NOAUTOMOVE

Keeps ownership of the file system. As a result, the file system becomes inaccessible.

UNMOUNT

Unmounts the file system when the node leaves the sysplex.

Note: For more information about these options, see the following:

- IBM *z/OS UNIX System Services Planning*
- *IBM z/OS UNIX System Services Command Reference*
- *IBM z/OS XL C/C++ Run-Time Library Reference*

4. Start the CA CSM application server.

   The mount parameters take effect.

5. If you enabled the Unmount at Shutdown feature in Step 1, navigate to the Settings tab, the Mount Point Management page, and clear the Unmount at Shutdown check box. Save the changes.

To restore the defaults, leave the parameters empty, or comment out the line in the *RunTimeMVSHLQPrefix*.SAMPLIB(MSMLIB) member.

Example

This example enables setuid() and setgid() mode bit on executable files, disables security checks, and does not allow file systems to change ownership:

```
IJO="$IJO -DADD_MOUNT_DEFAULT_OPTIONS=NOSECURITY,NOAUTOMOVE"
```

Specify Unit Parameters for SYSUT3 and SYSUT4 of the Remote System in the SAMPLIB(MSMLIB) Member

In the IEBCOPY utility, you can specify particular UNIT parameters for the SYSUT3 and SYSUT4 DD statements by adding statements in the SAMPLIB(MSMLIB) member. Remote Deployment Service picks up and uses the UNIT parameters that are specified in this way when allocating SYSUT3 and SYSUT4 DD statements. If no statements are defined, Remote Deployment Service uses the default UNIT(SYSDA) when allocating SYSUT3 and SYSUT4 DD statements. To specify parameters, add the following statements:

```
IJO="$IJO -Dmsmdutil.sysut3.unit=SYSALLDA"
IJO="$IJO -Dmsmdutil.sysut4.unit=SYSALLDA"
```

Binding the CA CSM Application Server to a TCP/IP Stack in a Multi-TCP/IP Stack Environment

When your LPAR with CA CSM has multiple TCP/IP stacks, establish a TCP/IP stack affinity to a desired stack. Establishing a stack affinity binds all socket communications to that stack.

To establish a stack affinity, select one of the following methods:

- Add a DD statement SYSTCPD DD to the CA CSM startup JCL (*RunTimeMVSHLQPrefix*.JCL(MSMTCSRV)) pointing to a specific TCPIP.DATA data set. For example:

  ```
  //SYSTCPD DD DSN=TCPIP.SEZAINST(TCPDATA),DISP=SHR
  ```

- Add the environment variable _BPXK_SETIBMOPT_TRANSPORT to the *RunTimeMVSHLQPrefix*.SAMPLIB(MSMLIB) member that is associated to the STDENV DD of the CA CSM application server. For example:

  ```
  export _BPXK_SETIBMOPT_TRANSPORT=stackname
  ```

- Add an extra step, AFFINITY, in the CA CSM startup JCL (*RunTimeMVSHLQPrefix*.JCL(MSMTCSRV)) before the MSMSRV step:

  ```
  //AFFINITY EXEC PGM=BPXTCAFF,PARM=stackname
  ```

Start CA CSM

The JCL members to start CA CSM are either in your JCL data set (*RunTimeMVSHLQPrefix*.JCL) or in your PROCLIB data set (*RunTimeMVSHLQPrefix*.PROCLIB). The member location is indicated in the summary report of the CA CSM installation and setup process. You can submit or start one of these members to run it as batch jobs or started tasks.

CA CSM allocates files on startup and during operation. If your site has products that interfere with file allocation, verify that DD statements to exclude such processing are included in the MSMTCSRV JCL member that starts the CA CSM application server (see page 229).

Note: The CA CSM application server (see page 229) uses a default region size of 512 MB. If you want to change this value, update the REGSIZE parameter in the MSMTCSRV JCL member. Also, update the Xmx value in the following statement in the SAMPLIB(MSMLIB) member:

```
IJO="-Xms128m -Xmx512m"
```

Follow these steps:

1. (CA CSM upgrade only) Verify that your address spaces from the previous version of CA CSM are down.
2. (CA CSM upgrade only) Unmount the APLROOT, SCROOT, and LJWK mount points from your previous version.
3. (CA CSM upgrade only) Optionally, back up your previous version of CA CSM start procedures and copy the latest version procedures to your production library.

4. If you are starting the latest CA Datacom/MSM MUF for the *first* time, verify that the following post installation jobs have previously been manually executed successfully.

   - For an upgrade (*xx* represents the CA MSM version you are upgrading from)
     - CSMU*xx*08
     - CSMU*xx*09
     - CSMU*xx*10
   - For a new installation
     - CSMN5108
     - CSMN5109
     - CSMN5110

5. Submit the MSMMUFS JCL member or start the MSMMUF PROCLIB member.

   The CA Datacom/MSM/Multi-User Facility (MUF) address space starts.

   Note: All data sets in STEPLIB must be APF-authorized.

   If the MUF starts up successfully, messages similar to the following example appear:

   ```
   DB00215I - CA Datacom/DB r12 at service pack: SP0
   DB00212I - CA Datacom SQL r12   at service pack: SP0
   DB00226I - MULTI-USER ACTIVATED XCF SUPPORT (RIMF20,mufname)
   DB00222I - MULTI-USER ACTIVATED CCI SUPPORT (caicci_sysid,mufname)
   DB00201I - MULTI-USER ENABLED, CXX=cxx_name    MUFNAME=mufname SVC=svc_number
   ```

   Important! Verify that the value of the MUF parameter in the runtime CUSMAC(DBDATIN1) member matches the value of the MUFname keyword in the options file (MSMSetupOptionsFile.properties). Otherwise, you cannot start the MUF.

6. Submit the MSMDBSVS JCL member or start the MSMDBSRV PROCLIB member.

   The CA Datacom/MSM server address space starts.

   If the server starts up successfully, messages similar to the following example appear:

   ```
   DB00101I - Started Job-MF2SRVR2 number-11326 CXX=CAMSM    Mufname=muf_name
   Svc=svc_number
   BPXM023I (USER01) DSV00049I-CA Datacom Server r11      INITIALIZED -server_name
   ```

7. Submit the MSMTCSRV JCL member or start the MSMTC PROCLIB member.

   The CA CSM application server address space starts.

   If the server starts up successfully, the following message appears in STDOUT:

   ```
   MSM0009I - CA CSM startup complete.
   ```

If the startup fails, the following message appears in STDOUT:

```
MSM0010E - CA CSM startup failed.
```

In addition, depending on the outcome of the startup, one of the following messages appears in the system console:

```
MSM0009I CA CSM STARTUP COMPLETE
MSM0010E CA CSM STARTUP FAILED
```

Note: The startup JCL for the CA CSM application server (see page 229) region has a SYSMDUMP DD statement that is commented out. If your site standards and system support the capture of this dump to the spool system, you can uncomment the DD statement to provide for dump captures in the case of failures.

After the successful startup of the CA CSM application server address space (see page 229), users can log in to CA CSM through a web browser.

Notes:

- Do not start the MSMTCSRV job (manually or with automation) until the MSMDBSRV job initialization completes and the BPXM023I message appears.
- After you successfully start up the CA CSM application server, if the following message appears, ignore it:

  ```
  INFO: The APR based Apache Tomcat Native library which allows optimal performance
  in production environments was not found on the java library.path:
  ```

  CA CSM does not require the installation of this library.
- Do not change any CA CSM application server startup JCL parameters unless CA Support requested it. Doing so could make CA CSM inoperable.
- If you are an existing CA CSM customer upgrading your database, comment out the DBUPDATE DD card in the MSMTCSRV JCL member or MSMTC PROCLIB after you successfully bring up CA CSM for the first time.
- If you restart the CA Datacom/MSM server, restart the CA CSM application server.

More information:

Stop CA CSM (see page 91)
Set Up User Security for CA CSM Functions (see page 34)

Configure MUF Message Printing

To help you distinguish between several MUF regions, the MUFMSG parameter in the DBDATIN1 member is used. This parameter is configured to specify the printing of the job name, SVC number, and SUBID. These properties precede the message number on messages that the MUF issued and some of the messages that concern communication with the MUF:

```
MUFMSG=YES,YES,YES
```

The prefixed message is displayed in the following format:

jobname:*svc_number*:*subid*:DB0*xxxx*I

If you use the FORCE_SVC MUF startup option, the MUF chooses the lowest SVC number with the highest Service Pack of the same version as the MUF.

If you run only one MUF region, you can change this parameter to disable the printing. To do so, set the MUFMSG parameter as follows:

```
MUFMSG=NO,NO,NO
```

Enable IEC988I Message in MUF Startup

CA CSM provides the option of displaying the following informational message:

```
IEC988I jjj,sss,ddn{-#},dev,volser,dsn DATA SET NOT UNALLOCATED DURING
            CLOSE RCxx
```

To minimize messages that may be interpreted as errors during an upgrade or a new installation, CA CSM suppresses issuing these messages by default.

You can enable CA CSM to display the messages on the console log and job output.

Follow these steps:

1. Locate the MUF startup member CUSMAC(DBDATIN1).
2. Locate the following control card:

   ```
   PREVENT_IEC988 YES        PREVENT IEC988I MESSAGE
   ```

3. Comment out the card by inserting an asterisk (*) in the column directly in front of the control card.

   The control card looks like the following:

   ```
   *PREVENT_IEC988 YES          PREVENT IEC988I MESSAGE
   ```

4. Recycle CA CSM.

   You can recycle CA CSM by bringing down CA CSM in the following order and then bringing it up in the reverse order using the commands:

   a. SCS address space (if available) – MSMCPROC. Issue the following command:

      ```
      P MSMCPROC
      ```

   b. CA CSM application server – MSMTCSRV. Issue the following command:

      ```
      P MSMTCSRV
      ```

   c. CA Datacom/MSM database server – MSMDBSVS. Execute the job member MSMDBSVP.

   d. MUF – MSMMUFS. Execute the job member MSMMUFP.

After you apply these changes, the console log may contain message IEC988I for jobs that issue CA Datacom/MSM utility open and close functions. The messages are displayed each time an open and close function is performed against CA Datacom/MSM data sets (specifically for data sets that are in multiple extent disk allocation).

Configuring Output Descriptors

To be able to select an Output Descriptor from the CA CSM Policy wizard, provide the output descriptor values in the CA CSM server startup JCL. The sample JCL provided in the CA CSM runtime JCL library is named MSMTCSRV. The sample JCL provided in the CA CSM runtime PROCLIB library is named MSMTC. You can use multiple output descriptors in the CA CSM startup JCL which gives you the ability to select one of them from the wizard. The selected output descriptor is used when the policy is executed for the processing of the CA CSM task output by the JES spool option. Output descriptors are only available through this wizard if they are specified in the CA CSM startup JCL.

The following examples show output descriptors using site-specific meaningful names:

```
//CAVIEW    OUTPUT  CLASS=9,FORMS=2UP
//CASPOOL   OUTPUT  CLASS=S
```

Note: For more information about output descriptors and the parameters for the OUTPUT JCL statement, see the *IBM z/OS MVS JCL Reference*.

Enable the Notice and Consent Banner in CA CSM

After you set up and install CA CSM, you can configure it so that it displays the Notice and Consent banner every time a user logs in to CA CSM.

When CA CSM is started for the first time, the file that is named MSMBanner.html is created in the following directory:

```
tomcat/webapps/MSM/
```

The file contains the sample banner.

Follow these steps:

1. Copy the sample file MSMBanner.html to the following directory:

   ```
   tomcat/webapps/
   ```

2. (Optional) Modify the contents of the file so that it conforms to the requirements of your organization.

   The banner is available and appears the next time a user logs in to CA CSM.

   Note: Do not change the CA CSM access URL in the following string:

   ```
   <a href="MSMMain.html">
   ```

Configure CA CSM

After you set up and install CA CSM, you configure it so that it can access the CA Support Online website for you to acquire products. You are prompted to configure CA CSM on the first login.

Follow these steps:

1. Start your web browser, and enter the access URL.

   The login page appears.

   Note: If the Notice and Consent Banner appears, read and confirm the provided information.

2. Enter your z/OS login user name and password, and log in.

   The initial page appears, and you are prompted to configure CA CSM.

   Note: For more information, click the online help link at the top right corner of the page.

3. Configure the following settings:

   - Proxies that CA CSM uses to communicate with the CA Support Online website

     If proxies are not used, CA CSM uses HTTPS Port Number 443 and FTP Port Number 21.

     Important! If your site uses proxies, review your proxy credentials on the User Settings, Software Acquisition page.

   - The USS path to the temporary directory for downloaded software packages

     If you do not specify the directory, CA CSM sets it up using default settings that you can change later.

   Note: These settings are also available on the System Settings, Software Acquisition page.

   Click Next.

   You are prompted to define your account on the CA Support Online website.

4. Click New.

   You are prompted for the credentials to use on the CA Support Online website.

5. Specify the credentials, click OK, and then click Next.

   You are prompted to review your user settings.

   Note: These settings are available on the User Settings page.

6. Change the settings or keep the defaults, and then click Finish.

   A dialog opens, which shows the progress of the configuration task. You can click Show Results to view the details of the actions in a finished task.

7. Click the Settings tab, and review other configuration settings.

You have configured CA CSM. Users can log in and can begin downloading mainframe products.

Configuring FTP and HTTP Connections

This section describes how to configure FTP connections for both new and existing CA CSM installations, and how to configure HTTP connections.

Note: Before you start, verify that you have a CA Support Online account. You can verify it on the System Settings, Software Acquisition page.

Configuring FTP Connections for an Existing Installation

No FTP configuration changes are needed when upgrading from a previous version of CA CSM to CA CSM Release 5.1.

Configuring FTP Connections for a New Installation

FTP Session Options

CA CSM uses a Java-based FTP client. This FTP client has several options that control how the session operates. These options are not considered to be related to FTP proxies that provide authentication services when logging in to the FTP server.

FTP session options are specified in the installed CA CSM data set *RunTimeMVSHLQPrefix*.CUSMAC(PASADVOP). This data set is an XML file and has an FTPOPTIONS section defining all the available FTP session options. Each option is set to the FTP client default.

The <FTPOPTIONS> XML tag is read for every FTP connection that CA CSM establishes. If the tag is not defined or empty, then the CA CSM FTP client uses the defaults as described in this section.

The following example is a code syntax sample for FTP session settings:

```
<FTPOPTIONS>key_1=value_1, key_2=value_2</FTPOPTIONS>
```

You can use the following keys:

firewall.friendly

The firewall.friendly FTP option is set to true by default:

```
<FTPOPTIONS>firewall.friendly=true</FTPOPTIONS>
```

You only specify this option if you want to override it.

The firewall.friendly option refers to FTP operating in passive mode. Passive mode causes the FTP server to open a listening port for the FTP data connection. If this option is set to false, then the FTP client opens the listening port for the server.

You can ask your network administrator if passive mode is supported. Alternatively, you can test if the default is acceptable by running a batch FTP program. After the statements that log you in to the FTP server as *anonymous*, insert QUOTE PASV.

The job output displays a message that contains the following text:

```
227 Entering Passive Mode (IP_address,FTP_server_code)
```

- If you see this message, you do not have to specify the firewall.friendly option.
- If you do not see this message, rerun the job with QUOTE PASV removed. The job output now displays a message that contains the following text:

  ```
  200 PORT command successful.
  ```

  If you see this message, set firewall.friendly to false.

verify.pasv.ip

The verify.pasv.ip FTP option is set to true by default:

```
<FTPOPTIONS>verify.pasv.ip=true</FTPOPTIONS>
```

You only specify this option if you want to override it.

Important! We recommend that you do not override this option unless your firewall support absolutely requires it.

Some firewall implementations may intercept and alter the IP address that is returned from the FTP server in response to the PASV command. In this case, you may see the following message in CA CSM application server (see page 229) logs:

```
Host attempting data connection ip_address_1 is not same as server ip_address_2
```

ip_address_1

Identifies the altered IP address from the firewall server.

ip_address_2

Identifies the IP address of the FTP server.

default.timeout

The default.timeout FTP option is set to zero (0) by default:

```
<FTPOPTIONS>default.timeout=0</FTPOPTIONS>
```

You only specify this option if you want to override it.

The value of this option represents time in milliseconds. The default value 0 is interpreted as an infinite timeout. Some environments can encounter timeout issues when downloading large files that are 200 MB or more.

For example, a large file is downloaded using an FTP command line session in OMVS. When the data transfer is complete, a subsequent FTP command, for example, **ls**, is entered. A timeout condition can result with a message, for example:

```
Connection to server interrupted or timed out. Waiting for reply.
```

In this case, a value of 10000 (representing 10 seconds) resolves this situation if CA CSM encounters it.

default.port

The default.port option is set to 21 by default. This port is the industry standard default port that FTP uses. There may be some firewall implementations that alter this default port, even if there are no FTP proxy authentication methods.

```
<FTPOPTIONS>default.port=21</FTPOPTIONS>
```

You can change the port number 21 to the required port number.

Note: This option has no affect if you enable FTP proxy settings.

control.keep.alive.timeout

Keepalive packets (no-operation packets) prevent routers from closing a control connection during large file transfers after a certain period of inactivity. The control.keep.alive.timeout option specifies how often (every *x* seconds) a keepalive packet is sent.

The control.keep.alive.timeout option is not specified by default (no keepalive packet is sent). You can set this option to the required frequency of sending keepalive packets (in seconds). For example, to force the file download methods to send a keepalive packet every five minutes (300 seconds), add the following statement in the *RunTimeMVSHLQPrefix*.CUSMAC(PASADVOP) data set:

```
<FTPOPTIONS>control.keep.alive.timeout=300</FTPOPTIONS>
```

More information:

FTP Proxy Settings (see page 71)

FTP Proxy Settings

FTP Basic Proxy Settings

When you select only the Enable Proxy Settings check box in the FTP Proxy section on the System Settings, Software Acquisition page, CA CSM supports the following basic FTP proxy authentication methods:

- Without user credentials (see page 71)
- With user credentials (see page 72)

Configure without User Credentials

Follow these steps:

1. On the Settings tab, go to System Settings, Software Acquisition.
2. In the FTP Proxy section, select the Enable Proxy Settings check box, and provide the FTP proxy port and address.
3. Click Apply.

   The changes take effect.
4. Go to User Settings, Software Acquisition.
5. In the FTP Proxy section, verify that the user name and password are *not* provided. If they are provided, remove both of them, and click Apply.

   The changes take effect.

CA CSM sends the following commands:

- An FTP USER command with the anonymous@ftp.ca.com parameter
- An FTP PASS command with your ID for the CA Support Online website as the password

Configure with User Credentials

Follow these steps:

1. On the Settings tab, go to System Settings, Software Acquisition.
2. In the FTP Proxy section, select the Enable Proxy Settings check box, and provide the FTP proxy port and address.
3. Click Apply.

   The changes take effect.
4. Go to User Settings, Software Acquisition.
5. In the FTP Proxy section, provide a user name and password for the FTP proxy server.
6. Click Apply.

   The changes take effect.

CA CSM connects to the specified proxy server and sends the following sequence of FTP commands to authenticate and log in to the FTP server:

```
USER FTP_proxy_user_ID@ftp.ca.com
PASS proxy_password
USER anonymous
PASS Support_Online_user_ID
```

Note: The same scenarios are applied to all other CA FTP servers where ftp.ca.com is mentioned.

FTP Advanced Proxy Settings

If the FTP basic settings do not support your FTP proxy authentication methods, FTP advanced proxy settings allow you to customize the FTP authentication and logon as your FTP proxy requires. These advanced settings are stored in a PDS member named PASADVOP. When CA CSM is installed, PASADVOP is placed into the *RunTimeMVSHLQPrefix*.CUSMAC data set. To see the current location of the PASADVOP, look in FTP Proxy, Advanced Settings Data Set, on the System Settings, Software Acquisition page. This member has a generic template containing advanced FTP and HTTP settings. You can use the default values in the member or can modify them using ISPF editor to match your FTP and HTTP proxy authentication methods.

Example PASADVOP Member

All XML elements must be specified between the tags <ADVOPTIONS></ADVOPTIONS>.

```
<ADVOPTIONS>
  <FIREWALL>
    <FIRECMD>HOST;</FIRECMD>
    <FIRECMD>USER;@REMOTE_USER;@REMOTE_HOST;</FIRECMD>
    <FIRECMD>PW;@REMOTE_PW;</FIRECMD>
  <FIREWALL>
</ADVOPTIONS>
```

The following example is a code syntax sample for FTP proxy settings:

```
<FIREWALL>
  <FIRECMD>keyword;</FIRECMD>
<FIREWALL>
```

Use the following keywords for supporting various FTP proxy authentication schemes:

HOST

Defines the name of your FTP proxy server. When this keyword is encountered, CA CSM substitutes the value that is entered for the FTP Proxy Server name on the System Settings, Software Acquisition page. The FTP client uses this value to connect initially.

USER

Defines the user for authenticating to the enabled proxies. When this keyword is encountered, it is substituted with the value that is entered for the FTP Proxy User that is specified on the User Settings, Software Acquisition page.

PW

Defines the password for authenticating to the enabled proxies. When this keyword is encountered, it is substituted with the value that is entered for the FTP Proxy Password that is specified on the User Settings, Software Acquisition page.

REMOTE_HOST

Defines the FTP address of the remote server. When this keyword is encountered, it is substituted with the appropriate FTP URL.

REMOTE_USER

Defines the user for authenticating to the remote server. When this keyword is encountered, it is substituted with *anonymous*.

REMOTE_PW

Defines the password for authenticating to the remote server. When this keyword is encountered, it is substituted with your user ID for the CA Support Online website.

ACCT

Instructs the CA CSM FTP client to issue an ACCT command to the FTP server. This keyword allows an accompanying parameter. This parameter is typically the proxy password that the PW keyword represents.

Follow the keywords with a semicolon (;). Outline the proxy authentication using these keywords. CA CSM substitutes the actual values from the System Settings, Software Acquisition page.

More information:

Defining FTP Advanced Settings (see page 74)

Defining FTP Advanced Settings

We recommend that you set up the advanced settings by running a batch job in z/OS executing the IBM FTP program. You can transpose the FTP proxy authentication scheme to the data set containing advanced settings.

For example, the input to your FTP batch job is the following sample:

```
//INPUT DD *
proxy_host_URL_or_IP
anonymous@ftp.ca.com proxy_userid
Support_Online_user_id
ACCT proxy_password
/*
```

Notes:

- A space precedes *proxy_userid*.
- If your network administrators require quotes, quotes can surround the second input line.

In this case, you would edit the advanced settings data set as follows:

```
<ADVOPTIONS>
  <FIREWALL>
    <FIRECMD>HOST;</FIRECMD>
    <FIRECMD>REMOTE_USER;@REMOTE_HOST; USER;</FIRECMD>
    <FIRECMD>REMOTE_PW;</FIRECMD>
    <FIRECMD>ACCT; PW;</FIRECMD>
  </FIREWALL>
</ADVOPTIONS>
```

- The HOST keyword is substituted with the FTP proxy name specified for the FTP Proxy Server name on the System Settings, Software Acquisition page.
- The REMOTE_USER keyword is substituted with anonymous.
- The USER keyword is substituted with the value specified for the user in the FTP Proxy section on the User Settings, Software Acquisition page.
- The REMOTE_HOST keyword is substituted with the appropriate CA Technologies FTP server URL.
- The ACCT keyword instructs the CA CSM FTP client to issue an ACCT command to the FTP server. This keyword allows an accompanying parameter. The parameter is typically the proxy password that the keyword PW represents, depending on what network administrators require.
- CA CSM substitutes your user ID on the CA Support Online website as specified in the CA Support Online Accounts section on the System Settings, Software Acquisition page for the REMOTE_USER keyword. The PW keyword is substituted with the value specified for the password in the FTP Proxy section, on the User Settings, Software Acquisition page. All of these substitutions are concatenated in the order that the FIRECMD statement specifies. The *at* symbol (@) is inserted into the resolved string exactly as specified.

Sometimes, the FTP input does not easily translate into the FIRECMD elements. In that case, you can use the SYSOUT of the batch FTP job. Use the //INPUT DD * batch job that is described at the beginning of this section to look for specific FTP commands and note the specific sequence.

The following SYSOUT is an abbreviated listing. The listing highlights the relevant statements that are used to formulate the FIRECMD statements.

Note: Comments are indicated by ==>.

```
EZA1450I IBM FTP CS V1R9
EZA1772I FTP: EXIT has been set.
    ==> The EZA1554I message shows the IP address of the FTP proxy server, and
    message 220 typically, but not always, displays the URL of the FTP proxy.
    Either of these can be specified in the CA CSM FTP Proxy settings as
    an IP address or the FTP proxy server name. This would translate to
    <FIRECMD> HOST;</FIRECMD>.
EZA1554I Connecting to:   123.456.789.1 port: 21.
220 Secure FTP server running on ftpproxyserver
    ==> The EZA1701I message indicates that the FTP USER command accepts a
    concatenated string to provide the FTP proxy user ID, the FTP user ID, and
    the actual FTP site to connect after the authentication is completed. This
    concatenated string would be translated as
    <FIRECMD>REMOTE_USERID;@USER;@REMOTE_HOST;</FIRECMD>.
EZA1459I NAME (123.456.789.1:ZOSUSERID):
EZA1701I >>> USER anonymous@proxy_userid@ftp.ca.com
    ==> Message 331 is an FTP proxy reply that indicates that the PASS command
    will accept a concatenated string to provide the passwords for both
    the FTP proxy server and the FTP server. As it does not specify which should
    be first, check the //INPUT DD * sample to see that the FTP server password
    is first (anonymous). Typically, but not always, if the user IDs are
    concatenated, the passwords are concatenated in the same order. That means,
    as in this case, the FTP user ID is first, therefore the FTP password is
    first. This concatenated string would be translated to
    <FIRECMD>REMOTE_PW;@PW;</FIRECMD>.
331 password: use password@password
EZA1789I PASSWORD:
EZA1701I >>> PASS
    ==> The following replies indicate the FTP proxy has successfully
    authenticated your FTP proxy credentials, and is logging in to the
    FTP server. The FTP server is acknowledging you have successfully
    logged in.
230-User proxy_userid authenticated by Secure FTP authentication
230-Connected to server. Logging in...
230-220 ftp.ca.com NcFTPd Server (licensed copy) ready.
230-331 User anonymous okay, need password.
230-230-You are user #18 of 4000 simultaneous users allowed.
```

The following sample is an example of using the SITE command. The server uses this command to provide system-specific services that are essential to file transfer but not sufficiently universal to be included as commands in the protocol.

```
<ADVOPTIONS>
  <FIREWALL>
    <FIRECMD>HOST;</FIRECMD>
    <FIRECMD>USER;</FIRECMD>
    <FIRECMD>PW;</FIRECMD>
    <FIRECMD>SITE;REMOTE_HOST;</FIRECMD>
    <FIRECMD>REMOTE_USER;</FIRECMD>
    <FIRECMD>REMOTE_PW;</FIRECMD>
  </FIREWALL>
</ADVOPTIONS>
```

FTP Advanced Proxy Settings Restrictions

The following restrictions are applied:

- CA CSM does not support actual user IDs and passwords within the <FIRECMD> element.
- CA CSM supports concatenating proxy user IDs with FTP user IDs (*anonymous*), and concatenating proxy passwords with FTP passwords (ID for the CA Support Online website). However, concatenating a proxy user ID and proxy password, or *anonymous* with the ID for the CA Support Online website is *not* supported.

  For example, the following sample is supported:

  ```
  <FIRECMD>USER;@REMOTE_USER;</FIRECMD>
  <FIRECMD>PW;@REMOTE_PW;</FIRECMD>
  ```

  The following sample is *not* supported:

  ```
  <FIRECMD>USER;PW;</FIRECMD>
  <FIRECMD>REMOTE_USER;REMOTE_PW;</FIRECMD>
  ```

  In this case, put the user ID and password on separate FIRECMD elements, for example:

  ```
  <FIRECMD>USER;</FIRECMD>
  <FIRECMD>PW;</FIRECMD>
  <FIRECMD>REMOTE_USER;</FIRECMD>
  <FIRECMD>REMOTE_PW;</FIRECMD>
  ```

Configuring HTTP Proxy Settings

The following scenarios are possible depending on your site configuration.

If you do not use an HTTP proxy server, your HTTP connection settings are complete.

HTTP Proxy Server without Authentication

Follow these steps:

1. On the Settings tab, go to System Settings, Software Acquisition.
2. In the HTTP Proxy section, select the Enable Proxy Settings check box, and provide the HTTP proxy port and address.
3. Click Apply.

   The changes take effect.
4. Go to User Settings, Software Acquisition.
5. In the HTTP Proxy section, verify that the user name and password are *not* provided. If they are provided, remove both of them, and click Apply.

   The changes take effect.

HTTP Proxy Server with Basic Authentication

Follow these steps:

1. On the Settings tab, go to System Settings, Software Acquisition.
2. In the HTTP Proxy section, select the Enable Proxy Settings check box, and provide the HTTP proxy port and address.
3. Click Apply.

   The changes take effect.
4. Go to User Settings, Software Acquisition.
5. In the HTTP Proxy section, provide a user name and password for the HTTP proxy server.
6. Click Apply.

   The changes take effect.

HTTP Proxy Server with NTLM Authentication

Use *one* of the following methods to configure HTTP connection settings and define NTML authorization.

- Specify the NTLM domain in the user name. We recommend that you use this method.

  Follow these steps:

  1. On the Settings tab, go to System Settings, Software Acquisition.
  2. In the HTTP Proxy section, select the Enable Proxy Settings check box, and provide the HTTP proxy address and port.

3. Verify that the Enable Advanced Settings check box is *not* selected.
4. Click Apply.

   The changes take effect.
5. Go to User Settings, Software Acquisition.
6. In the HTTP Proxy section, provide the NTLM domain, user, and password. This example provides the user name for the NTLM HTTP proxy:

   ```
   myNTLMdomain\user1
   ```
7. Click Apply.

   The changes take effect.

- Specify the NTLM domain as an XML element in the *RunTimeMVSHLQPrefix*.CUSMAC(PASADVOP) member.

  Follow these steps:

  1. On the Settings tab, go to System Settings, Software Acquisition.
  2. In the HTTP Proxy section, select the Enable Proxy Settings check box, and provide the HTTP proxy address and port.
  3. Select the Enable Advanced Settings check box.
  4. Click Apply.

     The changes take effect.
  5. Go to User Settings, Software Acquisition.
  6. In the HTTP Proxy section, enter the user name and password.

     Note: Do *not* add the NTLM domain in the user name.
  7. Click Apply.

     The changes take effect.
  8. In the *RunTimeMVSHLQPrefix*.CUSMAC(PASADVOP) member, specify the following XML elements. All XML elements must be specified between the tags <ADVOPTIONS></ADVOPTIONS>:

     ```
     <ADVOPTIONS>
       <HTTPPROXY ntlmDomain="myNTLMdomain"> </HTTPPROXY>
     </ADVOPTIONS>
     ```

     Note: The ntlmVersion attribute for the HTTPPROXY tag is obsolete.

Upgrading CA Common Services for z/OS with CETN500

CETN500 is a CA Common Services for z/OS function that is packaged in the pax file MSM50G0.pax.Z. This file includes RELFILES, SMP MCS and sample JCL to install CETN500 into your existing CA Common Services for z/OS SMP/E environment (r12 or Version 14). Install this feature to configure products using CA CSM into CA Common Services for z/OS. CETN500 installs modules into CA Common Services for z/OS PDSE CAIPLD (r12) or CAW0PLD (Version 14), which requires APF authorization and should be in the LINKLIST. CETN500 is incorporated in CA Common Services for z/OS Release 14.1.

Before you install CETN500, ensure that the software requirements are met.

Note: The System Discovery function needed by the SYSTEM REGISTRY VALIDATE action resides in the CCS LOAD Library (CAILOAD CAW0LOAD) for CA Common Services for z/OS.

CETN500 uses DDDEF names that are compatible with the names included in CA Common Services for z/OS Version 14.0. In addition, CETN500 deletes and supersedes CETN300 or CETN400 from your CA Common Services for z/OS SMP/E environment. CETN500 includes both the Software Configuration Service (SCS) and Software Deployment Service (SDS) common components. Set up CCIDSCSV and CCISPNSV on each target system before starting the SDS.

Upgrade r12 Using CA CSM

If you are using CA Common Services for z/OS r12 and cannot upgrade to CA Common Services for z/OS Version 14.0 or above, you can alternatively upgrade CA Common Services for z/OS r12 with CETN500 using CA CSM.

Follow these steps:

1. Download MSM50G0.pax.Z into your USS directory. To download the file, FTP it from the CA Technologies file server directly to your USS directory.
   a. Connect to the FTP site at the following location:

      ```
      ftp://ftp.ca.com
      ```

   b. Log in to ftp.ca.com as follows:

      ```
      user name: anonymous
      password: your-email-address
      ```

   c. Change to the following directory:

      ```
      cd /CAproducts/ca90s/MSMCCS50/GA/CCS_r12/
      ```

d. Download the following ESD distribution file, in binary format, to an HFS file on your mainframe:

```
bin
get MSM50G0.pax.Z MSM50G0-CCSR12.pax.Z
```

e. End the FTP session.

2. Log in to CA CSM and click the SMP/E Environments tab. Select your CA Common Services for z/OS r12 SMP/E environment in the right pane, and click Use as Working Set.

3. Click the Products tab, and click Install External Package under the Actions list in the left pane. In the Install External Package dialog that opens, enter the location of the pax file as follows, and click OK:

   /your_directory_path/MSM50G0-CCSR12.pax.Z

   The Install External Package dialog closes, and the Base Installation wizard opens to the Welcome step.

4. Click Next to advance to the Features step, select Full Install, and click Next.

   The Prerequisites step appears.

5. There are no prerequisites, click Next to skip this step.

   The SMP/E Environment step 1/3 appears with multiple options, including Create a New SMP/E Environment, and the SMP/E environments already in your working set.

   Note: If no SMP/E environment definition appears, click Cancel and restart this procedure with a different CA Common Services for z/OS r12 SMP/E environment in step 1. Do not click Create a New SMP/E Environment.

6. Select the CA Common Services for z/OS SMP/E environment, and click Next twice (you cannot update the SMP/E Environment step 2/3) to advance to the SMP/E Environment step 3/3.

7. Specify your work DDDEF parameters, and click Next to advance to the Target Zone step 1/3.

8. Select the zone associated with the CA Common Services for z/OS r12 installation, and click next to advance to the Target Zone step 2/3.

   CA CSM displays the SMS or data set target libraries allocation parameters in lower portion of the Target Zone step 2/3.

9. Specify the SMS or data set target libraries allocation parameters, and click Next to advance to the Target Zone step 3/3.

   Note: You can accept the values the CA CSM prefills in these fields. They are the values that we set when CA Common Services for z/OS r12 was installed.

10. Specify the Secure Socket Library target zone parameter.

    The following target data set appears:

    - CAW0SCST
    - CAW0XML0 (if you have none or only CETN300 installed)

11. Click Next to advance to the Distribution Zone step 1/3.

12. Select the zone associated with the CA Common Services for z/OS r12 installation, and click Next to advance to the Distribution Zone step 2/3.

13. Specify the SMS or data set distribution libraries allocation parameters, and click Next to advance to the Distribution Zone step 3/3.

    Note: You can accept the values that CA CSM prefills in these fields. They are the values that were set when CA Common Services for z/OS r12 was installed.

    The following distribution data sets appear:

    - AETNSCST
    - AETNEXP (if you have none or only CETN300 installed)
    - AETNJCL (if you have none or only CETN300 installed)
    - AETNSDF (if you have none or only CETN300 installed)
    - AETNXML0 (if you have none or only CETN300 installed)
    - AETNOPTN (if you have neither CETN300 nor CETN400 installed)
    - AETNPROC (if you have neither CETN300 nor CETN400 installed)
    - AETNPLD (if you have neither CETN300 nor CETN400 installed)

14. Click Next to advance to the Summary step, review the installation summary, and click Install to complete the installation process.

The CA Datacom/MSM SQL plans that match the load modules delivered in CETN500 reside in the library pointed to by DDDEF CAW0EXP, with member names formatted as MSMC*SQL. The sample JCL used to import a plan into CA Datacom/DB for CA CSM is supplied as the member MSMCXPLN in the sample JCL target library pointed to by CAW0JCL.

Upgrade Version 14.0 Using CA CSM

If you are using CA Common Services for z/OS Version 14.0, you can upgrade with CETN500 using CA CSM.

Important! Before installing CETN500, apply and accept RO44235. Follow the instructions provided in the HOLDDATA to allocate required libraries and add DDDEF entries. After you accept RO44235, remove the CA Common Services for z/OS Version 14.0 SMP/E environment from CA CSM and migrate it back to CA CSM. This will make CA CSM recognize externally added DDDEF entries.

Follow these steps:

1. Download MSM50G0.pax.Z into your USS directory. To download the file, FTP it from the CA Technologies file server directly to your USS directory.

   a. Connect to the FTP site at the following location:

      `ftp://ftp.ca.com`

   b. Log in to ftp.ca.com as follows:

      `user name: anonymous`
      `password: your-email-address`

   c. Change to the following directory:

      `cd /CAproducts/ca90s/MSMCCS50/GA/CCS_r14.0/`

   d. Download the following ESD distribution file, in binary format, to an HFS file on your mainframe:

      ```
      bin
      get MSM50G0.pax.Z MSM50G0-CCSR14.pax.Z
      ```

   e. End the FTP session.

2. Log in to CA CSM and click the SMP/E Environments tab. Select your CA Common Services for z/OS Version 14.0 SMP/E environment in the right pane, and click Use as Working Set.

3. Click the Products tab, and click Install External Package under the Actions list in the left pane. In the Install External Package dialog that opens, enter the location of the pax file as follows, and click OK:

   /your_directory_path/MSM50G0-CCSR14.pax.Z

   The Install External Package dialog closes and the Base Installation wizard opens to the Welcome step.

4. Click Next to advance to the Features step, select Full Install, and click Next.

   The Prerequisites step appears.

5. There are no prerequisites, click Next to skip this step.

   The SMP/E Environment step 1/3 appears with multiple options, including Create a New SMP/E Environment, and the SMP/E environments already in your working set.

   Note: If no SMP/E Environment definition appears, click Cancel and restart this procedure with a different CA Common Services for z/OS Version 14.0 SMP/E environment in step 1. Do not click Create a New SMP/E Environment.

6. Select the CA Common Services for z/OS Version 14.0 SMP/E environment, and click Next twice (you cannot update the SMP/E Environment step 2/3) to advance to the SMP/E Environment step 3/3.

7. Specify your work DDDEF parameters, and click Next to advance to the Target Zone step 1/3.

8. Select the zone associated with the CA Common Services for z/OS Version 14.0 installation, and click next to advance to the Target Zone step 2/3.

   CA CSM displays the SMS or data set target libraries allocation parameters in lower portion of the Target Zone step 2/3.

9. Specify the SMS or data set target libraries allocation parameters, and click Next to advance to the Target Zone step 3/3.

   Note: You can accept the values the CA CSM prefills in these fields. They are the values that we set when CA Common Services for z/OS Version 14.0 was installed.

10. Click Next to advance to the Distribution Zone step 1/3.

    Note: If you have RO44235 installed but the sample job provided in HOLDDATA was not run or not run properly, the CAW0SCST data set may appear.

11. Select the zone associated with the CA Common Services for z/OS Version 14.0 installation, and click Next to advance to the Distribution Zone step 2/3.

12. Specify the SMS or data set distribution libraries allocation parameters, and click Next to advance to the Distribution Zone step 3/3.

    Note: You can accept the values that CA CSM prefills in these fields. They are the values that were set when CA Common Services for z/OS Version 14.0 was installed.

13. Click Next to advance to the Summary step, review the installation summary, and click Install to complete the installation process.

    Note: If you have RO44235 installed but the sample job provided in HOLDDATA was not run or not run properly, the AETNSCST data set may appear.

The CA Datacom/MSM SQL plans that match the load modules delivered in CETN500 reside in the library pointed to by DDDEF CAW0EXP, with member names formatted as MSMC*SQL. The sample JCL used to import a plan into CA Datacom/DB for CA CSM is supplied as the member MSMCXPLN in the sample JCL target library pointed to by CAW0JCL.

CETN500 DDDEF Entries

CETN500 uses the following DDDEF names:

In Target Zone	In Distribution Zone	Usage
CAW0PLD	AETNMOD	Modules
CAW0JCL	AETNJCL	Sample JCL
CAW0PROC	AETNPROC	Sample PROCs
CAW0OPTN	AETNOPTN	Option Members
CAW0SDF	AETNSDF	Side Decks
CAW0EXP	AETNEXP	CA Datacom/MSM SQL Plans
CAW0XML0	AETNXML0	CA CSM SCS Address Space XML
CAW0SCST	AETNSCST	SCS Templates

Target DDDEF CAW0XML0 is only used by CETN500, while all other targets are also used by other functions in CA Common Services for z/OS.

Chapter 4: Post-Installation Tasks

This section contains the following topics:

Maintenance

After you set up and install CA CSM, you can use it to maintain itself.

Apply Maintenance to CA CSM

Important! To download maintenance, your CA CSM login user name must be associated with a registered user of the CA Support Online website on the Product Acquisition Settings page.

Follow these steps:

1. Update the Software Catalog with the CA CSM maintenance information from the CA Support Online website:
   a. Go to the Products tab and locate CA Chorus Software Manager in the Available Products panel on the left.

      Note: If you do not see CA Chorus Software Manager in the tree, use one of the products that are installable with CA CSM for this process. These products reflect CA CSM as a component so the maintenance is reflected there also. For more information, see CA Chorus Software Manager Enabled Products in the Recommended Reading section of the CA CSM page on the CA Support Online website.

   b. Right-click CA Chorus Software Manager and select Update Product.

      The task takes some time to complete, and after it does, a message appears confirming that the software was successfully acquired.

   c. Click Hide.

      The message disappears.

   d. Locate the CA CSM maintenance in the right panel.
2. (Optional) Add test fixes using external maintenance.

   Note: For more information about applying test fixes and managing maintenance downloaded external to CA CSM, see the online help.

3. Review and apply the maintenance.

   The contents of the SMP/E target libraries and USS paths for CA CSM are updated. These libraries and paths are set up using the TargetHLQ and MSMPATH keywords in the MSMSetupOptionsFile.properties options file.

   Note: For more information about applying and managing maintenance, see the online help.

4. Stop CA CSM (see page 91).

   CA CSM stops operation.

5. Deploy the maintenance for CA CSM to the CA CSM run-time libraries and USS paths. The libraries and USS paths are set up using the RunTimeMVSHLQPrefix and RunTimeUSSPath keywords in the MSMSetupOptionsFile.properties options file.

   a. Customize the JCL(MSMDEPLY) job. Update the JOB statement, and specify **deploy** for arg1.

   b. Submit the job.

6. Start CA CSM.

   CA CSM becomes operational with the maintenance.

Important! Distinguish between the SMP/E target libraries and USS paths, and the runtime libraries and USS paths. CA CSM executes out of the runtime libraries and USS paths. When you apply maintenance, only the SMP/E target libraries and USS paths are updated. You must stop CA CSM and submit the MSMDEPLY job to update the runtime libraries and USS paths. Those updates take effect when you restart CA CSM.

SQL Plan Updates

You may need to apply updates that affect CA Datacom/MSM SQL plans. These SQL plans are delivered as CA Common Services for z/OS maintenance. CA Common Services for z/OS include the sample JCL member MSMCXPLN that you can use to update these SQL plans in the MUF environment.

Implement Latest SQL Plans

The member MSMCXPLN, located in your CA Common Services for z/OS SMP/E environment sample JCL library, is modeled JCL that can be used to update CA Datacom/MSM SQL plans. Execute this JCL whenever you apply PTFs that contain at least one module element and a related SQL plan element. You will be notified that sample JCL member MSMCXPLN requires modification and execution by a ++HOLD condition action occurring during the process of applying the PTF. Follow the instructions that are provided in the ++HOLD comments to properly modify and execute this member.

Note: If CETN500 (MSMCCS 5.0) exists in your CA Common Services for z/OS, verify that the SQL plans are synchronized in the CA Datacom/MSM database Release 5.1 and your running CA Common Services for z/OS libraries. Submit the MSMCXPLN job from the CA Common Services for z/OS JCL library for each MSMC*SQL member in the CA Common Services for z/OS library that is represented by DDDEF CAW0EXP.

Data Set Reference for Sample JCL

To locate the data set name for the appropriate sample JCL library, refer to the DDDEF element CAW0JCL.

Data Set Reference for SQL Plan

To locate the data set name for the appropriate SQL plan library, refer to the DDDEF element CAW0EXP.

Running CA CSM Release 5.1 with the SCS Address Spaces Containing Code from a Previous Version

CA CSM Release 5.1 does not contain all of the SQL plans for CA MSM V4.0. This may cause you to receive an SQL -124 return code when connecting to an SCS address space of a previous version (CETN400).

After completing an upgrade to CA CSM Release 5.1 from CA MSM V4.0, follow the instructions provided in this section to import SQL plans from the CETN400 library. In the instructions, replace CETN500 with CETN400. Do so if you plan to connect to one or more CA CSM address spaces, which still contain code of a previous version (CETN400), and you cannot upgrade your CA Common Services for z/OS with CETN500.

More information:

CA CSM Address Space Functions Incorrectly (see page 214)

Back Out Maintenance from CA CSM

You can back out applied (but not accepted) maintenance from CA CSM. When you back out CA CSM maintenance, you first use the CA CSM Restore action to update the SMP/E target libraries and USS paths. Then, stop CA CSM and submit the MSMDEPLY job to update the runtime libraries and USS paths. Those updates take effect when you restart CA CSM.

Follow these steps:

1. Back out the maintenance using the Restore action.

   The contents of the SMP/E target libraries and USS paths for CA CSM are updated. These libraries and paths are set up using the TargetHLQ and MSMPATH keywords in the MSMSetupOptionsFile.properties options file.

   Note: For more information about backing out maintenance, see the online help.

2. Stop CA CSM (see page 91).

   CA CSM stops operation.

3. Deploy the contents of the updated SMP/E target libraries and USS paths to the CA CSM runtime libraries and USS paths. The libraries and USS paths are set up using the RunTimeMVSHLQPrefix and RunTimeUSSPath keywords in the MSMSetupOptionsFile.properties options file.

   a. Customize the JCL(MSMDEPLY) job. Update the JOB statement, and specify *backout* for arg1.

   b. Submit the job.

4. Start CA CSM (see page 62).

   CA CSM becomes operational without the maintenance.

Fail-Safe Backout

Rarely, a bad test fix for CA CSM can render CA CSM itself inoperable. To correct the problem, you can use the MSMDEPLY job to restore the CA CSM runtime libraries and USS paths to an operable condition. Customize and submit the MSMDEPLY job with *backout* specified for arg1. After the job completes, restart CA CSM, and follow the normal procedure to use CA CSM to back out the bad test fix.

When the MSMDEPLY job is run with *deploy* specified, a copy of the current CA CSM runtime libraries and USS paths is saved before deployment. When the MSMDEPLY job is run with *backout* specified, that last saved copy of the CA CSM runtime libraries and USS paths is deployed.

Important! Only one saved copy of the CA CSM runtime libraries and USS paths is maintained. Each execution of the MSMDEPLY job with *deploy* specified replaces the last saved copy of the runtime libraries and USS paths with a new copy. You cannot back out multiple saved copies by running the MSMDEPLY job multiple times with *backout* specified.

Stop CA CSM

If you want to stop CA CSM (for example, during maintenance), you stop CA CSM in the reverse order as you start CA CSM (see page 62).

Follow these steps:

1. Enter the following z/OS system command:

   ```
   P MSMTC
   ```

   The CA CSM application server (see page 229) has successfully terminated, the following message appears in the system console:

   ```
   MSM0011I CA CSM HAS TERMINATED SUCCESSFULLY
   ```

   Note: If this message does not appear, CA CSM has failed to stop its operation, and you have to force a shutdown using the following command:

   ```
   F MSMTC,APPL=FORCESHUTDOWN
   ```

   After the forced shutdown has completed, the following message appears in the system console:

   ```
   MSM0012W CA CSM TERMINATION WAS FORCED
   ```

   Important! If you force a shutdown, some of your data may be lost. Therefore, use this method only if the standard stop method is not working.

   The Tomcat job stops after CA CSM application server is terminated.

2. Submit the MSMDBSVP JCL member or start the MSMDBSRP PROCLIB member.

   The CA Datacom/MSM server stops.

3. Submit the MSMMUFP job or started task.

   The MUF stops, and CA CSM stops operation.

CA CSM Backup and Disaster Recovery

We recommend you perform periodic backups of your CA CSM environment in case of a disaster.

Before you start the disaster recovery process, back up all SMP/E environments and data sets managed by CA CSM.

When you perform disaster recovery, you do the following:

1. Recover all SMP/E environments managed by CA CSM.
2. Recover CA CSM itself.

CA CSM has to be recovered into an environment identical to the one that CA CSM was initially installed in. That is, the following configuration settings on the recovery system must be the same as on the original system:

- Operating system settings, such as TCP/IP ports, DASDs, and HLQs
- CA Datacom/MSM SVC
- Settings of APF-authorized data sets required for CA CSM
- Java

  Note: The Java version must be supported by CA CSM.
- TCP/IP configuration, host names, IP addresses, and CCI SYSID of systems specified in deployment

Notes:

- SAF settings for the recovery system must contain all changed SAF settings used when setting up CA CSM.
- Periodic backups of the CA Datacom/MSM database data areas, using the CA Datacom/DB utility function DBUTLTY, lets you safeguard your CA Datacom/MSM data during scheduled or unscheduled events that can impact accessibility to your product. For more information about how to reorganize your database, see the *Best Practices Guide*.

How You Back Up CA CSM

CA CSM backup is a several-step process.

Note: For backup, select and use a method that is appropriate for your site and environment. Managing the backup should be a part of your disaster backup routine.

Follow these steps:

1. Stop the CA CSM application server (see page 229).
2. Back up the following operating system settings:
   - Settings of the operating system such as ports, DASDs, HLQs
   - Java

     Note: The Java version must be supported by CA CSM.
   - TCP/IP
   - SAF

   Note: CA Datacom/MSM SVC is expected to be the same, and a list of APF-authorized data sets is preserved.

3. Obtain a list of data sets representing deployment file systems, software catalog file systems, and so on. The data sets are stored in the mountpoint table, the MP_DATASET column.

   Note: To obtain a list of the data set, you can submit JCL that runs a SQL statement (see page 93).

4. Stop the CA Datacom/MSM server and the MUF.

5. Back up the following CA CSM data sets:

   - Data sets representing mount points (see page 175)

     If you did not allocate individual file systems for these mount points, perform the following steps:

     a. Unmount all file systems that are mounted under the following file systems if they exist:

     ```
     /u/users/msmserv/msminstall
     /u/users/msmserv/msm
     /u/users/msmserv/msmruntime
     /u/users/msmserv/mpm
     ```

     b. Back up the directory structure corresponding to /u/users/msmserv.

   - All the data sets that you obtained from the mountpoint table.
   - All data sets under HLQs (CSIHLQ, TargetHLQ, DlibHLQ, DatabaseHLQ, and RunTimeMVSHLQPrefix) specified in the options file (MSMSetupOptionsFile.properties).

JCL for Executing SQL Statements

The following sample is an example of JCL that you can submit to run the SQL statement that discovers the content of the mountpoint table:

```
//*******************************************************************************
//*******************************************************************************
//*                                                                             *
//*JOBLIB DD DSN=HLQ.CUSLIB replace HLQ with HLQ of your CA CSM installation  *
//*          DSN=HLQ.CAAXLOAD replace HLQ with HLQ of your CA CSM installation*
//*                                                                             *
//*******************************************************************************
//*******************************************************************************
```

```
//B2UP     OUTPUT DEST=LOCAL,JESDS=ALL,DEFAULT=Y,
//         PAGEDEF=32D3,CHARS=GT20,FORMDEF=P2B111
//JOBLIB   DD DSN=HLQ.CUSLIB,
//         DISP=SHR
//         DD DSN=HLQ.CAAXLOAD,
//         DISP=SHR
//         DD DSN=SYSDEV.CCS.LINKLIB,
//         DISP=SHR
//         DD DSN=CEE.SCEERUN,DISP=SHR
//         DD DSN=CEE.AIGZMOD1,DISP=SHR
//*
//SQLEXEC  EXEC PGM=DBSQLPR,
//       PARM='prtWidth=1500,inputWidth=80'
//SYSUDUMP DD  SYSOUT=*
//SYSPRINT DD  SYSOUT=*
//STDERR   DD  SYSOUT=*
//STDOUT   DD  SYSOUT=*
//OPTIONS  DD  *
AUTHID=CASWMGT
/*
//SYSIN    DD  *
   SELECT MP_DATASET
   FROM MOUNTPOINT WHERE NOT MP_TYPE='PRODUCT' OR MP_TYPE IS NULL;
/*
```

The following sample is a fragment of output that you receive after submitting the JCL for discovering the content of the mountpoint table:

```
Command Line Options

____________________
INPUTWIDTH=80
PRTWIDTH=1500
Option File Options

____________________
AUTHID=CASWMGT
INPUT STATEMENT:
SELECT MP_DATASET
   FROM MOUNTPOINT WHERE NOT MP_TYPE='PRODUCT' OR MP_TYPE IS NULL;
MP_DATASET
VARCHAR(45)

_____________________________________________
OMVSUSR.CAMSM.APLROOT
OMVSUSR.CAMSM.LJWK
OMVSUSR.CAMSM.MSMT1
OMVSUSR.CAMSM.MSMT3
...
```

The data sets that are returned after the input statement are the data sets that you have to back up:

```
OMVSUSR.CAMSM.APLROOT
OMVSUSR.CAMSM.LJWK
OMVSUSR.CAMSM.MSMT1
OMVSUSR.CAMSM.MSMT3
```

How You Recover CA CSM from the Backup

To recover CA CSM from the backup, perform the following steps:

1. Recover operating system settings.
2. Recover CA CSM data sets.
3. Start CA CSM (see page 62).

Recovery If CA CSM Fails Because of Maintenance

Maintenance that has been applied to software that CA CSM depends on can sometimes cause CA CSM to fail. It is possible that you will not be able to use CA CSM to correct the problem.

- If the maintenance was applied to CA CSM itself, use the fail-safe backout method (see page 90) to return CA CSM to an operable condition.
- If the problem occurs because maintenance was applied to software belonging to another product that affects CA CSM, use SMP/E batch jobs to either apply new corrective maintenance or back out the maintenance. Then, restart CA CSM. This process could include applying new corrective maintenance to CA CSM itself. If you apply new corrective maintenance to CA CSM itself, you must deploy the maintenance before restarting CA CSM.

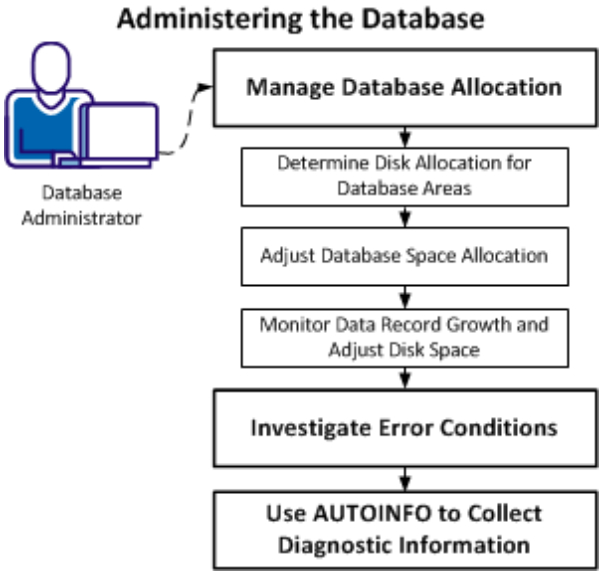
Chapter 5: Database Administration

CA CSM includes a variation of CA Datacom/MSM customized for CA CSM. It is referred to as CA Datacom/MSM, and CA CSM uses it as its underlying data repository.

This section contains the following topics:

How the Database Administration Process Works

You perform the following high-level tasks to administer the CA Datacom/MSM database:



1. Manage database allocation:
   a. Determine current disk allocation for existing CA CSM database areas (see page 98).
   b. Adjust database space allocation (see page 100).
   c. Monitor data record growth and adjust disk space (see page 100).
2. Investigate error conditions (see page 105) if occur.
3. Use the AUTOINFO function (see page 107) to collect diagnostic information.

Database Allocation Management

You may need to increase your disk allocation because of a file full condition caused by one or more of the following situations:

- An increase in frequency of product updates
- Installation of new products
- A CA CSM upgrade

A change to your disk allocation for your CA Datacom/MSM data areas and indexes may have occurred due to one or more of the following reasons:

- An internal automatic execution of the CA Datacom/MSM Dynamic Extend function
- A manual execution of the CA Datacom/MSM DBUTLTY EXTEND function
- You performed the following:
  - Ran a CA Datacom/MSM data area backup
  - Deleted associated CA Datacom/MSM data area data set
  - Reallocated data set
  - Ran the CA Datacom/MSM DBUTLTY INIT LOAD to reload the data area

Note: We recommend that you ensure the disk allocation for all of your CA CSM database data sets are at least equal to the current allocation at your site.

To successfully manage your disk allocation, you need to perform the following procedures:

1. Determine the current disk allocations (see page 98) for your existing CA CSM database data sets.
2. Adjust CA Datacom/MSM disk space allocation (see page 100) before starting the CA CSM upgrade.
3. Monitor data record growth over time (see page 100), and based on the results, adjust CA Datacom/MSM disk space after CA CSM is functional.

Determine Current Disk Allocation for Existing CA CSM Database Areas

You can use this procedure to determine the current database allocation of your site and prepare to make appropriate changes to the CA CSM upgrade job stream.

Note: You need to perform the steps in this procedure before you submit any jobs in the samplib data set.

Follow these steps:

1. Ensure that CA Datacom/MSM is active.

   a. Enter the following online console command:

      `/F dbjobnm,STATUS`

      dbjobnm

      Specifies the CA CSM multi-user facility (MUF) executable job name.

      A console DB status command is issued. The output from this command is displayed on the mainframe console, as well as in the SYSOUT class JESMSGLG of the CA Datacom/MSM job.

      If CA Datacom/MSM is active, the following informational message appears:

      `DB01327I - MULTI-USER AVAILABLE`

   b. If necessary, take appropriate action for any other messages that appear.

   c. If CA Datacom/MSM is not active, you can submit the job member MSMMUFS from the samplib data set to bring up the CA Datacom/MSM environment.

2. Run the Directory (CXX) Space report.

   Use the Directory (CXX) Report Sample JCL (see page 103) to produce a space report for CA CSM DBID 4000.

   Information is generated about the number of tracks allocated to a CA Datacom/MSM area and other important space utilization information. Enter TYPE=A for the keyword and value in the control statement to produce this information.

   Note: For more information about the functions of the Directory (CXX) report, see the chapter REPORT (Generate Reports) in the *CA Datacom/DB DBUTLTY Reference Guide z/OS*. The information in this guide also applies to CA Datacom/MSM.

3. Review the output of the Directory (CXX) Space report to analyze disk space.

   Note: You can look at the Directory (CXX) Report Sample JCL (see page 103).

   The report shows the data area name (three characters). Each data area is associated with a mainframe data set. The data area name is the suffix of the associated data area data set name found in the DD card of the JCL.

4. For each of the data areas, identify the percentage full and the number of allocated tracks.

JCL Allocation Adjustments

You may need to adjust disk allocations to any JCL job stream.

For a new installation, the job CSMN5106 performs the initial CA Datacom/MSM disk allocations that are suitable for normal CA CSM usage. For an upgrade from a previous version, the job CSMU*xx*06 performs the initial CA Datacom/MSM disk allocations that are suitable for normal CA CSM usage.

xx

Indicates the version number that you are upgrading from.

Based upon your planned usage of CA CSM and your current DASD disk pool resources, you may need to adjust primary and secondary CA Datacom/MSM disk space to meet your site requirements. If you are performing an upgrade, verify that the new disk allocations are at least equal to the CA Datacom/MSM disk space currently in use.

To adjust disk space allocations when executing the MSMSetup.sh shell script, do one of the following:

- If in Review installation mode, enter **Y** (Yes) in response to the prompt if you want to preview JCL before automatic job submission.
- If in Manual installation mode, modify the *runtimeHLQ*.JCL data set as necessary before job submission.

You can adjust the disk allocation based on your expected usage of CA CSM Software Configuration Service (SCS) functions. The following disk allocations can be used for CA Datacom/MSM data area XML, the data set *dbHLQ*.XML4000, where *dbHLQ* is your high-level qualifier for the CA Datacom/MSM data sets:

- A minimum of one cylinder is sufficient if you are not using CA CSM functions to configure products.
- A minimum of 300 cylinders is sufficient if you are using a low volume of CA CSM functions to configure products.
- A minimum of 3,000 cylinders is sufficient if you are using an average to high volume of CA CSM functions to configure products.

Monitor Data Record Growth and Adjust Disk Space

You may need to increase your organization's disk space over time.

You can run the Directory (CXX) report periodically, and every period, compare the current Directory CXX report with a history report to help predict growth over time and adjust the CA Datacom/MSM disk allocation accordingly after CA CSM is functional.

The following methods are available to adjust disk space:

- Use the DBUTLTY EXTEND function (see page 101).
- Adjust disk space manually (see page 101). This method requires you to back up your data, delete the associated data set, reallocate the data set, initialize, and reload the data.

DBUTLTY EXTEND Function

Use the DBUTLTY EXTEND function to increase the space available in a data area or index area. You can use the DBUTLTY EXTEND function for the following:

- When planning for future growth
- When an area or index becomes full or nearly full

The EXTEND function of DBUTLTY expands an existing data area or index area and formats the space acquired. The function also updates the data or index area control record, informing CA Datacom/DB that additional space is available.

Note: You cannot use EXTEND to decrease the size of an area.

Once the EXTEND function completes, the new area is immediately available for use without any further changes to the system. Any job that starts after the completion of the EXTEND function can use this newly allocated space.

Note: For more information, see the chapter EXTEND (Extend Data or Index Areas) in the *CA Datacom/DB DBUTLTY Reference Guide z/OS*.

Adjust Disk Space Manually

Adjusting the disk space manually requires you to do the following:

- Back up your data
- Delete the associated data set
- Reallocate the data set
- Initialize
- Reload the data

Follow these steps:

1. Run Directory (CXX) report to determine current disk allocation (see page 98).
2. Ensure that all activity requiring the use of the CA CSM database is stopped, including bringing down your CA CSM application server and the CA Datacom/MSM server regions associated with the CA CSM database.

   Bring down your CA CSM application server and the CA Datacom/MSM server:

   - Stop the CA CSM application server.
   - Submit the MSMDBSVP JCL member or MSMDBSRP PROCLIB member to stop (pause) the CA Datacom/MSM server.
3. Ensure that CA Datacom/MSM is active.

   a. Enter the following online console command:

      `/F dbjobnm,STATUS`

      dbjobnm

      Specifies the CA CSM multi-user facility (MUF) executable job name.

      A console DB status command is issued. The output from this command is displayed on the mainframe console, as well as in the SYSOUT class JESMSGLG of the CA Datacom/MSM job.

      If CA Datacom/MSM is active, the following informational message appears:

      `DB01327I - MULTI-USER AVAILABLE`

   b. If necessary, take appropriate action for any other messages that appear.

   c. If CA Datacom/MSM is not active, you can submit the job member MSMMUFS from the samplib data set to bring up the CA Datacom/MSM environment.
4. Run the CA Datacom/MSM DBUTLTY BACKUP function to back up the CA Datacom/MSM database (DBID 4000). You can use the member B4KBKUP in the samplib data set to model from and build a backup job stream.
5. After you have successfully created a backup of your CA Datacom/MSM database, delete the associated CA CSM database (DBID 4000) area and index data sets using TSO or an IBM utility.
6. Reallocate the CA CSM Database (DBID 4000) area and index data sets, with new disk allocations, using one of the following methods:

   - TSO
   - IBM utility
   - Include data set names as part of the CA Datacom/MSM DBUTLTY INIT job stream

7. Run a CA Datacom/MSM DBUTLTY INIT and LOAD function using the current backup performed in the DBUTLTY BACKUP step. You can copy the member B4KLOAD in the samplib data set and customize it to restore the CA CSM database.

   The disk allocation is adjusted and you are ready to provide the necessary space to accommodate your site's CA CSM activity.

   Note: Ensure that you replace the input DD card with the current backup created in the previous step.

8. Run the Directory (CXX) report to confirm that you have made your changes successfully.

9. Bring up the CA Datacom/MSM server and your CA CSM application server.

   CA CSM is ready to be used for normal operations.

Directory (CXX) Report Sample JCL

The following shows the command to generate a Space Utilization Report for the Directory.

```
//jobname (see note)
// EXEC PGM=DBUTLTY,REGION=2M
//STEPLIB (see note)
//CXX      DD DISP=SHR,DSN=RunTimeMVSHLQPrefix.cxx   Directory (CXX) data set
//SYSIN  DD * Command Input
REPORT AREA=CXX,DBID=4000,TYPE=A
```

Note: Use this sample JCL as a guide to prepare your JCL. Verify that you adhere to the following guidelines:

- Replace *RunTimeMVSHLQPrefix.cxx* with your site's mainframe data set name for the CA Datacom/MSM CXX directory.
- Lowercase letters in a statement indicate a value you must supply.
- Code all statements to your site and installation standards and specifications, including any JOB statements.
- All data set names and library names should be specified with the correct names for the installation at your site.
- In many examples, a REGION= or SIZE= parameter is displayed in an EXEC statement. The value displayed should be adequate in most instances, but you can adjust the value to your specific needs.

Directory CXX Report Sample

```
CONTROL CARD(S)
                    .........1.........2.........3.........4.........5.........6.........7.........8
                      REPORT AREA=CXX,DBID=4000,TYPE=A

                    FUNCTION=REPORT
                       AREA=CXX
                       DBID=04000
                       TYPE=A
```

The report shows the following:

- The command exactly as entered.
- An analysis of keywords encountered and expected. Any errors found are flagged with a note in the left margin.
- Any messages related to syntax processing.

```
 DATACOM/AD                  DATA AREA SPACE UTILIZATION REPORT
-AREA DATA        TOTAL        TOTAL       TOTAL        USED     PERCENT     PARTIALLY  AREA REUSE
 NAME BASE       TRACKS      RECORDS      BLOCKS      BLOCKS  FULL   MAX  EMPTY BLKS    OPTION

 CXX                525          N/A       6,300         342     5     5         N/A  N/A
 IXX  4000          900          N/A      10,800       5,445    50    50         N/A  N/A
  AUD 4000        5,010      254,258      10,020       4,398    43    43           1  RANDOM
  INV 4000        3,000      148,724      18,000      14,538    80    80           0  RANDOM
  JNL 4000        1,125       91,359       6,750       5,182    76    76           0  RANDOM
  PCY 4000          510       34,573       6,120       2,449    40    40           1  RANDOM
  SCS 4000        2,010       59,111      12,060       1,136     9     9           1  RANDOM
  SDS 4000          750       16,809       4,500       3,145    69    69           1  RANDOM
  SRG 4000        1,005        1,616       6,030         142     2     2           1  RANDOM
  XML 4000       33,000       61,858      66,000      61,860    93    93           0  RANDOM
```

The report provides the following information:

AREA NAME and DATA BASE

DATACOM-ID of the database containing the area. Summary statistics for the Directory (CXX) are always displayed on the first line.

TOTAL TRACKS

The number of tracks allocated and accepted by CA Datacom/MSM for use in the area. If the actual number of tracks (blocks) allocated is larger, execute an EXTEND function to make the space available to CA Datacom/MSM.

TOTAL RECORDS

For data areas, the number of records in the area. If a system failure has occurred during maintenance processing, this number can be inaccurate.

TOTAL BLOCKS

Number of blocks in the area.

USED BLOCKS

Number of blocks that contain data. If a system failure has occurred during maintenance processing, this number can be inaccurate.

PERCENT FULL and MAX

Percentage full is calculated by dividing used blocks by total blocks. The value reported is an even percent. Decimals are truncated.

Maximum percentage, sometimes referred to as *high-water mark*, is calculated by dividing maximum used blocks by total blocks. The value for maximum used blocks is computed internally. This percentage is higher than FULL percentage in the following situations:

- When all records are deleted in a data block with space management option 1 or 3 (random or cluster)

  Note: For information about the data area space management options, see the *CA Datacom/DB Database and System Administration Guide*.

- When all Index entries are deleted in an Index block

PARTIALLY EMPTY BLKS

Blocks that contain sufficient space to hold the largest record in the area are considered to be partially empty. If partially empty blocks exist and a space reclamation option has been selected, even when all blocks contain data (100 percent full), records can still be added.

AREA REUSE OPTION

The data area space management option used for the data area.

Note: CA Support uses this information.

Database Error Conditions

You can attend to some error conditions from the CA CSM web-based interface without contacting CA Support. These errors have the following text in the message details:

`UNEXPECTED ENGINE ERROR: n(o)`

***n*(*o*)**

Is the CA Datacom/MSM MUF error or return code.

If an error is not covered here, use the AUTOINFO function (see page 107) to collect diagnostic information before contacting CA Support.

MUF Canceled or Abended

Symptom:

I receive the following error:

```
UNEXPECTED ENGINE ERROR: 86(186)
```

Solution:

The CA Datacom/MSM MUF was canceled or has abended.

If the MUF was canceled, perform the following actions to restart it:

1. Enter **P** MSMTC to stop the CA CSM application server.
2. Use the MSMDBSVP JCL member or MSMDBSRP PROCLIB member to stop the CA Datacom/MSM server.
3. Use the MSMMUF JCL member or MSMMUFS PROCLIB member to start the MUF.
4. Use the MSMDBSVS JCL member or MSMDBSRV PROCLIB member to start the CA Datacom/MSM server.
5. Use the MSMTCSRV JCL member or MSMTC PROCLIB member to start the CA CSM application server.

If the MUF abended, use the AUTOINFO function (see page 107) to collect diagnostic information before contacting CA Support.

Data Area Full

Symptom:

I receive the following error:

```
UNEXPECTED ENGINE ERROR: 07(07)
```

Solution:

The CA Datacom/MSM MUF database data area is full. Enlarge the database.

Index Full

Symptom:

I receive the following error:

```
UNEXPECTED ENGINE ERROR: 08(08)
```

Solution:

The CA Datacom/MSM MUF database index is full. Enlarge the database.

AUTOINFO Function

The DBUTLTY AUTOINFO function collects diagnostic information from the memory of a MUF and selected dynamic system tables. The output is in print form and written to a sequential data set that can be sent to CA Support.

How You Execute AUTOINFO

You execute the DBUTLTY AUTOINFO function on the same system as the targeted MUF. You execute AUTOINFO while the MUF is experiencing a problem. If you execute AUTOINFO when the MUF is down, the function performs the following actions:

- Ends with a S000 U0004 condition code
- Notifies you that no data was available

You can use the following JCL statements as a guide for executing the function. Customize the statements to suit the requirements at your site.

```
//job_card
//AUTOINFO EXEC PGM=DBUTLTY,REGION=6M
//STEPLIB  DD DSN=prefix.CUSLIB,DISP=SHR
//         DD DSN=prefix.CAAXLOAD,DISP=SHR
//TABLES   DD DSN=output_data_set,DISP=(NEW,CATLG,CATLG),
//         UNIT=SYSDA,SPACE=(TRK,(3,1),RLSE)
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
AUTOINFO DDNAME=TABLES
/*
//
```

Chapter 6: Additional Administration Tasks

This section contains the following topics:

Send a Message to Current Users

You can use a z/OS modify command to send a message to a single user or all users who are logged in to the CA CSM web-based interface. For example, before you shut down CA CSM for maintenance, you can send a message to all CA CSM users that are logged in to the CA CSM application server to let them know that CA CSM is about to shut down.

To send a message to all CA CSM users currently logged in, enter the following command:

```
/F jobname,APPL=MSG,message text
```

Note: To send a message to a single user, add their TSO user ID, for example:

```
/F jobname,APPL=MSG,TSOuserID,message text
```

jobname

Specifies the name of the CA CSM application server on your system.

APPL=MSG

Specifies to the CA CSM address space to process this modify request as a messaging request.

TSOuserID

(Optional) Specifies the TSO user ID of the person you want to send the message to. If the TSO user ID is not included, the message is sent to all users who are currently logged in to the server.

message text

Specifies a body of a message. Enter free format message text to display to all users logged in to the CA CSM application server, or, if the TSO user ID is included, a single user.

Limitations: Do not include commas, even if you are using quotes for the message text itself.

More information:

Stop CA CSM (see page 91)

Sample JCL to Send Message to Users

The following sample JCL shows how to send a message to all users logged in to CA CSM, and to a single CA CSM user with a TSO user ID of DOEJON01:

Proclib member INFORMSM below:

```
//*****************************************************************************
//*****                                                                   *****
//*****  Send Message to CA CSM users                                    *****
//*****                                                                   *****
//*****  SERVER= is the number of the server to receive message.         *****
//*****  MSMMSG= is the message you want sent to the server user(s)      *****
//*****                                                                   *****
//*****  EXAMPLE JCL shown below how to send message to ALL users         *****
//*****                                                                   *****
//*****  /*JOBPARM SYSAFF=MACHINE31                                      *****
//*****  //          EXEC INFORMSM,SERVER=2,                             *****
//*****  // MSMMSG='CA CSM - IS SHUTTING DOWN - RESTART REQUESTED'       *****
//*****                                                                   *****
//*****  EXAMPLE JCL shown below how to send message to a CA CSM User     *****
//*****                                                                   *****
//*****  /*JOBPARM SYSAFF=MACHINE31                                      *****
//*****  //          EXEC INFORMSM,SERVER=2,                             *****
//*****  // MSMMSG='DOEJON01,TEST MESSAGE FROM JCL'                      *****
//*****                                                                   *****
//*****************************************************************************
//*
//INFORMSM  PROC  MSMMSG=,
//             SERVER=
//*
//OPSCMD   EXEC PGM=OPSCMD,PARM='F MF2T&SERVER.SRV,APPL=MSG,&MSMMSG.'
//*
//OPS$OPSP DD DUMMY         Direct request to production subsystem OPSP
//*
//INFORMSM  PEND
//*
```

```
JCL to send message Below:

//INFORM5S  JOB (129300000),'Inform CA CSM user',
//        COND=(4,LT),
//        CLASS=A,
//        MSGCLASS=X,
//        NOTIFY=&SYSUID,
//        MSGLEVEL=(1,1)
//*
/*JOBPARM SYSAFF=MACHINE31
//*
// JCLLIB ORDER=(MF20.MSM.PROCLIB)
//*
//*********************************************************************
//*****                                                          *****
//*****  send message to CA CSM server user(s)                  *****
//*****                                                          *****
//*********************************************************************
//*
//          EXEC INFORMSM,SERVER=5,
// MSMMSG='CA CSM - Server is closing down in fifteen minutes       '
//          EXEC INFORMSM,SERVER=5,
// MSMMSG='CA CSM - Server will be restarted soon after             '
//
//*
// MSMMSG='DOEJON01, send a message to a user on a CA CSM server    '
//*
```

Check for Executing Tasks

Before you bring down CA CSM, be aware of executing tasks and the impact of ending them abruptly. The users that started those tasks may no longer be logged in to CA CSM.

Follow these steps:

1. Log in to the CA CSM web-based interface, click the Tasks tab, and ensure that the Current Tasks subtab is selected.

   The Tasks page appears showing only your tasks.

2. Select All tasks from the Show drop-down list.

   A list of all tasks appears.

3. Check the status of tasks, and if any have a status of Executing, consider contacting the owner of the task before you bring down CA CSM.

Reassign the Java Home Directory

You may want to reassign the Java home directory, for example, when you install a new minor version of Java into a different directory to preserve the old version. When you change the Java directory, you must correct the Java path in the following places:

- Change the value of the JAVA_HOME variable In the SAMPLIB(MSMLIB) member.

  Example: In the following sample SAMPLIB(MSMLIB) member, replace *original_path* with the new path.

  ```
  export JAVA_HOME=original_path
  ```

- Change the SMPJHOME DDDEF value in the CA CSM CSI that points to the Java home directory. The CA CSM CSI is located in CSIHLQ.SMPCSI.CSI. Change the SMPJHOME DDDEF value in the global (GLOBAL), target (CAIT) and distribution (CAID) zones. Use the UCLIN statement to change the SMPJHOME DDDEF value.

  Example: Use this UCLIN statement to change the SMPJHOME DDDEF value for all CA CSM CSI zones by replacing the zone variable with each zone name: CAID, CAIT and GLOBAL.

  ```
  SET
  BOUNDARY(zone).
  UCLIN.
  REP  DDDEF(SMPJHOME)
       PATH('new_path').
  ENDUC.
  ```

Note: Once you start the MSMTC job, the JAVA_HOME path in the job log message has to match the path in the SMPJHOME DDDEF in the CA CSM CSI:

```
JVMJZBL1006I JAVA_HOME = new_path
```

- Change the JAVAPATH option in the MSMSetupOptionsFile.properties option file located in the *MSMPATH*/CEGPHFS directory.

  Example: In the following MSMSetupOptionsFile.properties option file sample, replace *original_path* with the new path.

  ```
  JAVAPATH=original_path
  ```

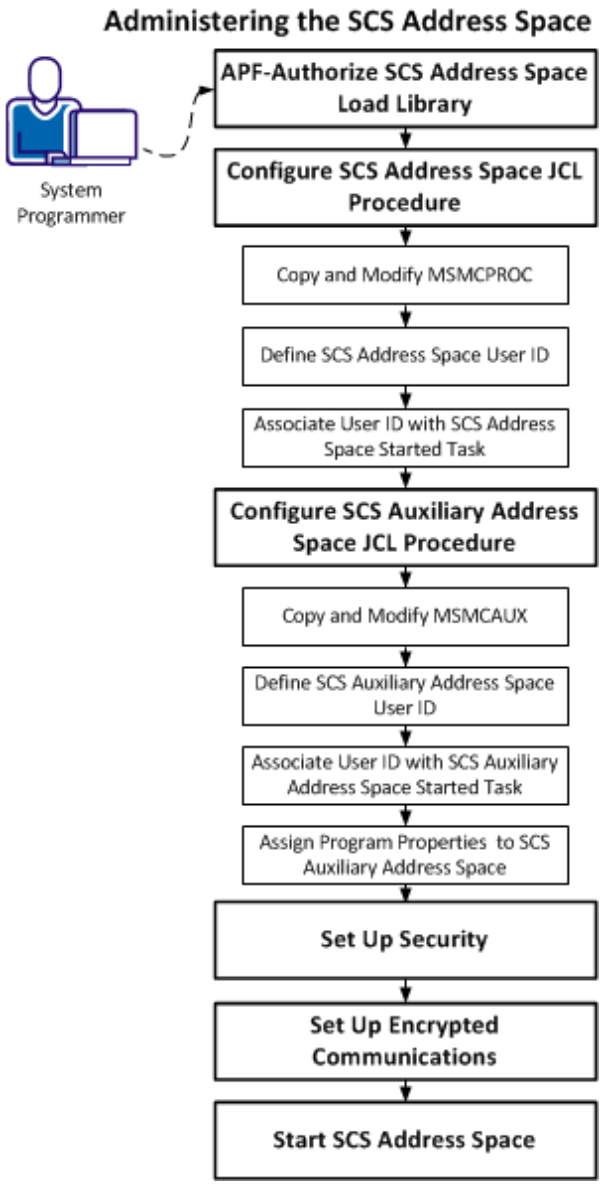
Chapter 7: SCS Address Space Administration

The *SCS address space* is a specially defined location where the system registry and commands for interrogating output and console traffic reside within the operating system. The SCS address space provides the services and processing necessary to implement configurations across your targeted z/OS systems. Each target system that is expected to support SCS processing must execute an SCS address space.

This section contains the following topics:

How the SCS Address Space Administration Process Works

Perform the following tasks to get the SCS address space running in your environment:



1. APF-authorize the SCS address space load library (see page 115).
2. Configure the SCS address space JCL procedure (see page 116).
   a. Copy MSMCPROC (see page 232) to a system PROCLIB and modify it to suit the installation environment.
   b. Define a user ID for the SCS address space.
   c. Use the security system to associate the user ID with the SCS address space started task. Perform this step if you are starting the SCS address space as a started task.
3. Configure the SCS auxiliary address space JCL procedure (see page 117).
   a. Copy MSMCAUX (see page 232) to a system PROCLIB and modify it to suit the installation environment.
   b. Define a user ID (see page 118) for the SCS auxiliary address space.
   c. Use the security system to associate the user ID with the SCS auxiliary address space started task.
   d. Assign special program properties (see page 118) to the SCS auxiliary address space.
4. Set up security (see page 119).
5. Set up encrypted communications (see page 128).
6. Start the SCS address space (see page 134).

Authorized Program Facility

Important! In SCS address space documentation, all references to the SYS1.PARMLIB data set indicate any data set that is defined in the logical PARMLIB concatenation.

Use the Authorized Program Facility (APF) to identify programs that use sensitive system functions. The SCS address space must be started as an APF-authorized job step. The SCS address space load library must be APF-authorized on each z/OS system where the SCS address space is started.

To ensure that the SCS address space is started as an APF-authorized job step, APF-authorize all libraries you include in the SCS address space STEPLIB concatenation. Putting a library in the concatenation that is not APF-authorized causes the entire library concatenation to lose its APF-authorization.

The APF lists are in the SYS1.PARMLIB member PROG*xx*. The lists contain the names of APF-authorized libraries. The order of the entries in the lists is not significant.

If you use the PROG*xx* members with dynamic format, you can issue the z/OS command SET PROG=*xx.* The changes take effect before the next IPL.

Note: For more information about APF lists, see the *IBM Initialization and Tuning Reference*.

MSMCPROC JCL Procedure

The SCS address space uses the MSMCPROC (see page 232) JCL procedure. Copy this procedure to a system PROCLIB that the z/OS START commands use, and modify it to suit your installation environment.

You can:

- Specify the JCL EXEC statement parameters (see page 141) that can be used with the PARM keyword parameter of the JCL EXEC statement.
- Add or change any DD statements as required. The MSMCPROC sample member describes the changes that are required.

  Note: MSMCPROC is the common name of the SCS address space JCL procedure. You can change the name to suit your installation environment.

If the z/OS UNIX System Services environment on your system is not configured with an AF_INET6 domain in the SYS1.PARMLIB(BPXPRM*xx*) member, update the TCP/IP parameters in the SCS address space parameter member MSMCPARM (see page 142). Change <TCPIP ipaddr="::" port="49152"/> to <TCPIP ipaddr = "0.0.0.0" port="49152"/>.

Define a security system user ID for the SCS address space. The user ID must have an OMVS segment. The segment must be defined and have read access to the data sets that the SCS address space JCL procedure allocated. The user ID does not need OMVS superuser privileges.

You can start the SCS address space as a started task or as an initiated job.

- To start the SCS address space as a started task, use the START (see page 134) command. Use your security system to associate a user ID with the SCS address space started task.
- To start the SCS address space as an initiated job, execute the MSMCPROC JCL procedure within a batch job stream. Use the USER parameter of the JCL JOB statement to associate a user ID with the SCS address space initiated job.

Auxiliary Address Space

An initial auxiliary address space is created from a service request that the SCS address space makes. More auxiliary address spaces are created as needed.

The auxiliary address spaces are created and managed dynamically, depending on the level of concurrent configuration requests. They handle service requests on behalf of the SCS address space.

The SCS address space performs service requests on behalf of a user who is implementing a configuration. The SCS address space creates the auxiliary address spaces and schedules service requests to the auxiliary address spaces once they are active. The auxiliary address space executes the requests and the results are returned to the SCS address space.

Auxiliary Address Space Operation

The SCS address space automatically creates an auxiliary address space, when needed, to schedule a request. The auxiliary address space executes in a workload manager (WLM) dependent enclave that the SCS address space creates. If there are scheduled services, all SCS auxiliary address spaces remain active. When there are no more requests to run, the inactive auxiliary address spaces are stopped.

Note: The SCS address space creates and manages up to 20 auxiliary address spaces depending on the number of concurrent service requests processed.

You can specify SCS address space parameters to limit the maximum number of concurrently active auxiliary address spaces to a number less than 20.

You do not have to perform automated operations for the auxiliary address spaces; the SCS address space dynamically initiates them. In the unlikely event that the SCS address space fails, all auxiliary address spaces stop.

Installation Considerations

CA CSM includes the MSMCAUX (see page 232) sample member. The auxiliary address space uses the JCL procedure MSMCAUX (see page 232). You must copy this procedure to a System PROCLIB that z/OS START commands use, and modify it to suit your installation environment.

You can add or change any DD statements as required. The MSMCAUX sample member describes the changes.

Do not start the MSMCAUX procedure manually. The MSMCAUX procedure is started by the SCS address space (MSMCPROC).

Note: MSMCAUX is the common name of the auxiliary address space JCL procedure. You can change the name to suit your installation environment. If you do change the name, update the AUX *procname* in the SCS address space parameters (see page 142).

Auxiliary Address Space User ID

You must define a security system user ID for the auxiliary address space. The user ID can be the same as the one defined for the SCS address space. The user ID must have read access to the data sets allocated by the auxiliary address space JCL procedure. If the user ID for the auxiliary address space is different from the user ID for the SCS address space, it does not need an OMVS segment.

The auxiliary address space is always started as a started task. Use your security system to associate a user ID with the auxiliary address space started task.

Special Program Properties

Special program properties are a requirement. They must be assigned to the system for the program MSMCAUX (see page 232) named on the EXEC PGM= JCL card in the MSMCAUX PROC.

MSMCAUX must be defined in the SCHED*xx* member of SYS1.PARMLIB to execute in storage protect key 4.

To define MSMCAUX to execute in storage protect key 4, use the following statement:

```
PPT PGMNAME(MSMCAUX) KEY(4) SYST PRIV
```

Note: Special program properties are only assigned to programs that are retrieved from an APF-authorized library concatenation. All MSMCAUX PROC STEPLIB data sets must be properly defined in the APF library list.

For more information about the definition of special program properties, see the *IBM Initialization and Tuning Reference*.

SCS Address Space Security Setup

The Security Setup (see page 32) that is required for CA CSM is only set up on the driving system. To set up the SCS address space security, do so on every target system, which can include the CA CSM driving system.

The SCS address space verifies the user ID assigned to the requesting started task or initiated job and authorizes it to connect.

Note: An unauthorized CA CSM user ID is denied access to the selected target system.

If security profiles are not defined, CA CSM cannot connect to the SCS address space, including from within the address space.

The security administrator must configure permission to access the entity SCSAS.CONNECT (READ authority) of the class CAMSM. The permission allows connections to the SCS address space through the CA CSM application server and the SCS address space.

Set up security in one of the three major external security manager (ESM) products (CA ACF2 for z/OS, CA Top Secret for z/OS, or IBM RACF) being utilized.

The following topics describe how to set up a rule to provide READ access to the entity SCSAS.CONNECT in the resource class named CAMSM. Setting up a rule to provide READ access to the entity depends on the security software you are using.

Set Up SCS Address Space Security in CA ACF2 for z/OS

If you are using CA ACF2 for z/OS to set up security in the SCS address space, you must define the global systems options (GSO) record and define the rule to permit access to a user ID.

Follow these steps:

1. Define the GSO record:

```
SET C(GSO)
INSERT CLASMAP.MSM ENTITYLN(246) MUSID() RESOURCE(CAMSM) RSRCTYPE(MSM)
```

2. Define the rule to permit access to a user ID:

```
SET R(MSM)
COMPILE STORE
$KEY(SCSAS) TYPE(MSM)
CONNECT.-     UID(*****userid)                SERVICE(READ)     ALLOW
CONNECT.-     UID(*****userid2)               SERVICE(READ)     ALLOW
```

userid

Specifies the user ID assigned to the SCS address space.

userid2

Specifies the user ID assigned to the CA CSM application server driving system.

Set Up SCS Address Space Security in CA Top Secret for z/OS

If you are using CA Top Secret for z/OS, set up security in the SCS address space.

Follow these steps:

1. Add the resource class to the RDT:

```
TSS ADDTO(RDT) RESCLASS(CAMSM) ATTR(MASK) MAXLEN(246)
TSS REPL(RDT) RESCLASS(CAMSM)
                ACLST(READ=4000,UPDATE=8000,CONTROL=0400,NONE=0000)
                DEFACC(READ)
```

2. Create a CA CSM departmental ACID:

```
TSS CREATE(MSMDPT) NAME('CA CSM Department') TYPE(USER)
```

3. Define the resource profiles within the CAMSM class:

```
TSS ADDTO(MSMDPT) CAMSM(SCSAS.CONNECT)
```

4. Create a CA Top Secret for z/OS profile.

```
TSS CREATE(SCSPRF1) NAME('CA CSM SCS AS PROFILE')
DEPT(MSMDPT)   TYPE(PROFILE)
```

5. Permit the resource to access the profile:

```
TSS PERMIT(SCSPRF1) CAMSM(SCSAS.CONNECT)   ACCESS(READ)
```

6. Assign the profile to the ACID:

```
TSS ADDTO(userid) PROFILE(SCSPRF1)
```

userid

Specifies the user ID assigned to the SCS address space.

Set Up SCS Address Space Security in IBM RACF

If you are using IBM RACF, set up security in the SCS address space.

Note: If you have already defined and activated the CAMSM resource class in IBM RACF, you can skip steps 1 through 4.

Follow these steps:

1. Issue the SETROPTS LIST command to verify that the CDT resource appears within both the CLASSACT and RACLIST list of entries.
2. Define the generic profile:

   ```
   RDEFINE CDT CAMSM UACC(NONE) CDTINFO(GENERIC,MAXLENGTH(246) POSIT(nnn)
   OTHER(ALPHA,NATIONAL,NUMERIC,SPECIAL) RACLIST(ALLOWED))
   ```

   nnn

   Defines a posit number that does not conflict with IBM reserved values.

   Note: For more information about posit numbers, see the *IBM Server RACF Command Language Reference*.

   The generic profile is defined.
3. Make the generic profile changes take effect:

   ```
   SETROPTS RACLIST(CDT) REFRESH
   ```
4. Activate the CAMSM class:

   ```
   SETROPTS RACLIST(CAMSM) CLASSACT(CAMSM)
   ```
5. Define the resource profiles within the CAMSM class:

   ```
   RDEFINE CAMSM SCSAS.CONNECT UACC(NONE)
   ```
6. Permit the resource to a user:

   ```
   PERMIT SCSAS.CONNECT CLASS(CAMSM) ID(userid) ACCESS(READ)
   ```

   userid

   Specifies the user ID assigned to the SCS address space.
7. (Optional) If the CAMSM class is RACLISTed, refresh the class:

   ```
   SETROPTS RACLIST(CAMSM) REFRESH
   ```

PassTickets

PassTickets are used to verify the started task ID of the CA CSM application server to allow secure connections from a remote system to the SCS address space.

You must set up PassTickets on the system where the CA CSM application server is executing and on each system where the SCS address space is running.

Note: To generate a valid PassTicket, use the values for the remote SCS address space on the system where the CA CSM application server is running.

To set up PassTickets, use the commands in the following examples on both the server and remote target systems, depending on the security software you are using (CA ACF2 for z/OS, CA Top Secret for z/OS, or IBM RACF).

Note: These examples are provided as a guideline and are intended for security administrators familiar with PassTicket configuration.

CA ACF2 for z/OS PassTicket Examples

You can use CA ACF2 for z/OS to configure PassTickets for the CA CSM application server to communicate with the remote systems.

Note: For detailed information about using the commands in these examples, see the *CA ACF2 for z/OS Administration Guide*.

Example: Configure PassTickets for CA CSM Application Server

You can use CA ACF2 for z/OS to configure PassTickets on the system where the CA CSM application server is executing.

Follow these steps:

1. Define the session key for the CA CSM application server:

   ```
   SET PROFILE(PTKTDATA) DIVISION(SSIGNON)
   INSERT MSMCAPPL SSKEY(0123456789ABCDEF) NOMULT-USE
   ```

   MSMCAPPL

   Defines the session key for the SCS address space ID used during CA CSM Configuration processing. This name may have been overridden when you installed CA CSM, so it should reflect the real application name.

   Note: This example demonstrates a complete session key value of 16 hex digits (creating an 8-byte or 64-bit key). Change your key so that it consists of 16 random hex digits, and is different from the values in this example. Each application key must be the same on all systems in the configuration, and the values must be kept secret and secured.

2. Enable READ access to the MSMCAPPL PassTicket key value:

   ```
   SET RESOURCE(PTK)
   RECKEY IRRPTAUTH ADD(MSMCAPPL.stc-userid UID(uid-of-stc-userid)
   SERVICE(READ,UPDATE) ALLOW)
   ```

   stc-userid* and *uid-of-stc-userid

   Specifies the user ID and UID associated with the CA CSM application server started task.

   Note: You can also use the ACFNRULE utility program to add rule lines to an existing rule. For more information about this option, see the *CA ACF2 for z/OS Administration Guide*.

3. Complete the PassTicket setup:

   ```
   F ACF2,REBUILD(PTK),CLASS(P)
   F ACF2,REBUILD(PTK)
   ```

Example: Configure PassTickets for SCS Address Space on Remote Systems

You can use CA ACF2 for z/OS to configure PassTickets on the remote systems where the SCS address space is running.

Follow these steps:

1. Define the MSMCAPPL session keys:

   ```
   SET PROFILE(PTKTDATA) DIVISION(SSIGNON)
   INSERT MSMCAPPL SSKEY(0123456789ABCDEF) NOMULT-USE
   ```

   MSMCAPPL

   Defines the session key for the SCS address space ID used during CA CSM Configuration processing. This name may have been overridden when you installed CA CSM, so it should reflect the real application name.

   Note: This example demonstrates a complete session key value of 16 hex digits (creating an 8-byte or 64-bit key). Change your key so that it consists of 16 random hex digits, and is different from the values in this example. Each application key must be the same on all systems in the configuration, and the values must be kept secret and secured.

2. Enable READ access to the MSMCAPPL PassTicket key value:

   ```
   SET RESOURCE(PTK)
   RECKEY IRRPTAUTH ADD(MSMCAPPL.stc-userid UID(uid-of-stc-userid)
   SERVICE(READ,UPDATE) ALLOW)
   ```

   stc-userid* and *uid-of-stc-userid

   Specifies the user ID and UID associated with the SCS address space.

   Note: You can also use the ACFNRULE utility program to add rule lines to an existing rule. For more information about this option, see the *CA ACF2 for z/OS Administration Guide*.

3. Complete the PassTicket setup on the remote systems:

```
F ACF2,REBUILD(PTK),CLASS(P)
F ACF2,REBUILD(PTK)
```

CA Top Secret for z/OS PassTicket Examples

You can use CA Top Secret for z/OS to configure PassTickets for the CA CSM application server to communicate with the remote systems.

Note: For detailed information about using the commands in these examples, see the *CA Top Secret for z/OS Administration Guide*.

Example: Configure PassTickets for CA CSM Application Server

You can use CA Top Secret for z/OS to configure PassTickets on the system where the CA CSM application server is executing.

Follow these steps:

1. Update the resource descriptor table (RDT) to define the PTKTDATA class (which is not a predefined class):

   ```
   TSS ADDTO(RDT) RESCLASS(PTKTDATA) RESCODE(n) ACLIST(ALL,READ,UPDATE) MAXLEN(37)
   ```

   Note: Include RESCODE(*n*) in the range of 101 to 13F to make PTKTDATA a prefixed resource class.

2. Assign ownership to a department for the PassTicket session key (SESSKEY) resource:

   ```
   TSS ADDTO(department) PTKTDATA(IRRPTAUTH)
   ```

   department

   Specifies a preexisting department. The ownership of the application is defined to this department. This ownership lets the department administrator (or higher) define permissions for PassTicket generation and validation.

3. Define the CA CSM application server PassTicket session key:

   ```
   TSS ADDTO(NDT) PSTKAPPL(MSMCAPPL) SESSKEY(0123456789ABCDEF)
   ```

   MSMCAPPL

   Defines the session key for the SCS address space ID used during CA CSM Configuration processing. This name may have been overridden when you installed CA CSM, so it should reflect the real application name.

   Note: This example demonstrates a complete session key value of 16 hex digits (creating an 8-byte or 64-bit key). Change your key so that it consists of 16 random hex digits, and is different from the values in this example. Each application key must be the same on all systems in the configuration, and the values must be kept secret and secured.

4. Permit access to the CA CSM application server PassTicket session key value for the Started Task User for the CA CSM application server:

   ```
   TSS PERMIT(stc-userid) PTKTDATA(IRRPTAUTH.MSMCAPPL.) ACCESS(READ,UPDATE)
   ```

   stc-userid

   Specifies the ACID that you defined the access requirements for user ID associated with the CA CSM application server.

Example: Configure PassTickets for SCS Address Space on Remote Systems

You can use CA Top Secret for z/OS to configure PassTickets on the remote systems where the SCS address space is running.

Follow these steps:

1. Define the SCS address space PassTicket session key:

   ```
   TSS ADDTO(NDT) PSTKAPPL(MSMCAPPL) SESSKEY(0123456789ABCDEF)
   ```

   MSMCAPPL

   Defines the session key for the SCS address space ID used during CA CSM Configuration processing. This name may have been overridden when you installed CA CSM, so it should reflect the real application name.

   Note: This example demonstrates a complete session key value of 16 hex digits (creating an 8-byte or 64-bit key). Change your key so that it consists of 16 random hex digits, and is different from the values in this example. Each application key must be the same on all systems in the configuration, and the values must be kept secret and secured.

IBM RACF PassTicket Examples

You can use IBM RACF to configure PassTickets for the CA CSM application server to communicate with the remote systems.

Note: For detailed information about using the commands in these examples, see the IBM RACF documentation.

Example: Configure PassTickets for CA CSM Application Server

You can use IBM RACF to configure PassTickets on the system where the CA CSM application server is executing.

Follow these steps:

1. Activate the PassTicket class:

   ```
   SETROPTS CLASSACT(PTKTDATA)
   SETROPTS RACLIST(PTKTDATA)
   SETROPTS GENERIC(PTKTDATA)
   ```

2. Define a profile for the application and specify the session key:

   ```
   RDEFINE PTKTDATA MSMCAPPL SSIGNON(KEYMASKED(0123456789ABCDEF)) UACC(NONE)
   ```

   MSMCAPPL

   Defines the session key for the SCS address space ID used during CA CSM Configuration processing. This name may have been overridden when you installed CA CSM, so it should reflect the real application name.

   Note: This example demonstrates a complete session key value of 16 hex digits (creating an 8-byte or 64-bit key). Change your key so that it consists of 16 random hex digits, and is different from the values in this example. Each application key must be the same on all systems in the configuration, and the values must be kept secret and secured.

3. Define a profile and permit access to the MSMCAPPL PassTicket session key value for the Started Task user ID so that it can access the SCS address space:

   ```
   RDEFINE PTKTDATA IRRPTAUTH.MSMCAPPL.stc-userid UACC(NONE)
   ```

   stc-userid

   Specifies the user ID associated with the CA CSM application server started task. This user ID only needs the ability to generate a PassTicket for itself.

4. Permit access to the MSMCAPPL PassTicket session key value for the CA CSM application server:

   ```
   PERMIT IRRPTAUTH.MSMCAPPL.stc-userid CLASS(PTKTDATA) ID(stc-userid)
   ACCESS(READ,UPDATE)
   ```

5. Refresh the PTKTDATA class:

   ```
   SETROPTS RACLIST(PTKTDATA) REFRESH
   ```

Example: Configure PassTickets for SCS Address Space on Remote Systems

You can use IBM RACF to configure PassTickets on the remote systems where the SCS address space is running.

Follow these steps:

1. Activate the PassTicket class:

   ```
   SETROPTS CLASSACT(PTKTDATA)
   SETROPTS RACLIST(PTKTDATA)
   ```

2. Define a profile for the application and specify the session key:

   ```
   RDEFINE PTKTDATA MSMCAPPL SSIGNON(KEYMASKED(0123456789ABCDEF)) UACC(NONE)
   ```

   MSMCAPPL

   Defines the session key for the SCS address space ID used during CA CSM Configuration processing. This name may have been overridden when you installed CA CSM, so it should reflect the real application name.

   Note: This example demonstrates a complete session key value of 16 hex digits (creating an 8-byte or 64-bit key). Change your key so that it consists of 16 random hex digits, and is different from the values in this example. Each application key must be the same on all systems in the configuration, and the values must be kept secret and secured.

3. Permit access to the MSMCAPPL PassTicket session key value for the SCS address space Started Task user ID:

   ```
   RDEFINE IRRPTAUTH.MSMCAPPL.stc-userid CLASS(PTKTDATA) UACC(NONE)
   ```

   stc-userid

   Specifies the SCS address space Started Task user ID.

4. Refresh the PTKTDATA class:

   ```
   SETROPTS RACLIST(PTKTDATA) REFRESH
   ```

UNIX Socket Requirements

The SCS address space uses UNIX sockets for internal communication.

Set up the following requirements on the target system:

- Define the AF_UNIX domain in the BPXPRMxx PARMLIB member.
- Verify that the /var/sock directory exists in the UNIX file system, or that MSMCPROC has authority to create the directory.
- Verify that MSMCPROC has write authority to the /var/sock directory.

Encrypted Communications

To enable encrypted communications with the SCS address space, configure one of the following encryption methods:

- IBM System Secure Socket Layer (SSL)
- IBM Application Transparent Transport Layer Security (AT-TLS)

If a connection is made to the SCS address space from the web-based interface remote host, the address space detects the use of System SSL or IBM AT-TLS. If neither method is detected, the communication with the web-based interface is performed in clear text.

Implement Support for SSL Transmission

Set up the SCS Address Space to use *one* of the following:

- IBM System Secure Socket Layer (SSL) toolkit using a key store file that is located on a Hierarchical File System (HFS).

  Note: Execute the program *gskkyman* under OMVS at a shell prompt. Executing this program creates a key store file on the HFS, generates a self-signed certificate authority certificate, and generates a server certificate.

- External Security Manager (ESM)

  Note: Generate a server certificate by executing the commands of your ESM.

Create a Key Store File

You can create a key store file on zFS or HFS when setting up the SCS address space to use SSL.

Follow these steps:

1. From a mainframe console, execute *gskkyman*.
2. Select Create new database and enter the path and file name to the new key store file or database.

   Note: The path and file names must be writeable path/file names.

3. Enter a database password and enter the password expiration in days.

   Note: Press ENTER if the password never expires.

4. Enter **5000** for the database record length and enter **0** for the database mode.
5. Wait for acknowledgment that the key database is created.
6. Select Exit program.

   The key store file is created.

Create a Self-Signed Certificate Authority Certificate

You can create a self-signed certificate authority certificate when setting up the SCS address space to use SSL.

Follow these steps:

1. From a mainframe console, execute *gskkyman*.
2. Select Open database, enter the path to the database that you created, and enter the database password.

   The Key Management menu appears.
3. Select Create a self-signed certificate.
4. Select certificate authority certificate with 1024-bit RSA key and select SHA-512.

   Note: Selecting certificate authority certificate with 1024-bit RSA key creates the certificate authority.
5. Enter a label for the self-signed certificate authority certificate and enter a common name.

   Note: The common name can be the same as the label.
6. Provide data for the prompts regarding ownership of the certificate. Ownership includes the following data:
   - Organizational unit
   - Organization
   - Organization city, state, and country
7. Enter the number of days the certificate is valid and enter **0** to continue.
8. Wait until the certificate is created.
9. Select Exit program.

   The self-signed certificate authority certificate is created.

Create a Server Certificate

You can create a server certificate when setting up the SCS address space to use SSL.

Follow these steps:

1. From a mainframe console, execute *gskkyman*.
2. Select Open database, enter the path to the database that you created, and enter the database password.

   The Key Management menu appears.

3. Select Manage keys and certificates, and enter the number of the certificate authority certificate to use.

   Note: You can use the number that you previously created.

4. Select Create a Signed Certificate and Key, and select User or server certificate with 1024-bit RSA key.

5. Enter a label for the server certificate and enter a common name.

   Note: The common name can be the same as the label.

6. Provide data for the prompts regarding ownership of the certificate. Ownership includes the following data:

   - Organizational unit
   - Organization
   - Organization city, state, and country

7. Enter the number of days the certificate is valid and enter **0** to continue.

8. Wait until the certificate is created.

9. Select Exit program.

   The server certificate is created.

Set the Server Certificate as the Default Certificate

You can set the server certificate as the default certificate when setting up the SCS address space to use SSL.

Follow these steps:

1. From a mainframe console, execute *gskkyman*.

2. Select Open database and enter the path to the database you created.

3. Enter the database password.

   The Key Management menu appears.

4. Select Manage keys and certificates and enter the number of the label for the server certificate.

5. Select the option to set the key as default.

6. Select Exit program.

   The server certificate is set as the default certificate.

Export the Certificate Authority Certificate

You can export the certificate authority certificate when setting up the SCS address space to use SSL.

Follow these steps:

1. From a mainframe console, execute *gskkyman*.
2. Select Open database and enter the path to the database that you created.
3. Enter the database password.

   The Key Management menu appears.
4. Select Manage keys and enter the number of the label for the certificate authority certificate to export.
5. Select Export certificate to a file and select Binary ASN.1 DER.
6. Enter the path name and file to export the certificate to and press Enter.
7. Select Exit program.

   The certificate authority certificate is exported.

Store the Database or Key Store Password Into a Stash File

You can store the database or key store password into a stash file when setting up the SCS address space to use SSL.

Follow these steps:

1. From a mainframe console, execute *gskkyman*.
2. Select Open Database and enter the path to the database that you created.
3. Enter the database password and select Store Database Password.

   The file, database_*name*.sth, is stored where the database file is stored.
4. Select Exit program.

   The database or key store password is stored into a stash file.

Import the Certificate Authority Certificate Into a Java Key Database

You can import the certificate authority certificate into a Java key database when setting up the SCS address space to use SSL.

Follow these steps:

1. Execute the keytool program that came with your Java SDK installation in superuser mode.
2. Enter the keystore password.

   Default: changeit
3. Enter yes to trust the certificate.

   Note: If the certificate is added successfully, then the configuration is complete.

   The certificate authority certificate is imported into a Java key database.

Example: Execute the keytool program

The following sample is an example of how to execute the keytool program:

```
keytool –import –trustcacerts –file /path/to/exported/ca/certificate –keystore
$JAVA_HOME/lib/security/cacerts
```

Set Up to Use System SSL

For the SCS address space to use System SSL, the PDSE member GSKSSL must be accessible to the program by one of two methods:

- Adding the PDSE named *pdsename*.SIEALNKE to the dynamic LPA (PROG*xx* member).

  Note: For more information about setting up System SSL, see the IBM guide, *z/OS Cryptographic Service System Secure Sockets Layer Programming.*
- Modifying the PROCLIB member containing the JCL procedure that is used to start the SCS address space. The name is commonly MSMCPROC (see page 232). Include a reference to *pdsename*.SIEALNKE by adding a DD statement for STEPLIB.

Go to the SCS address space configuration XML and enable SSL in the address space.

Once you have created the certificate authority certificate and server certificate, modify the parameter file that is named *MSMCPARM* (see page 142) for the SCS address space.

Default: MSMCPARM

Locate the SSL tag in the XML document, and set the keyring attribute to the key store/database file. Set the stashfile attribute to the equivalent stash file.

Update the SCS address space configuration XML by setting the keyring and stashfile in the SSL element of the XML document to point to the keystore database and password stash file.

Implement Support for AT-TLS Transmission

Application Transparent Transport Layer Security (AT-TLS) is a component of z/OS that provides encryption services for applications that exchange sensitive data but have not been instrumented to include encryption. This service lets you encrypt data being sent to the application without adding the extra API calls to do encryption.

To use the AT-TLS with the SCS address space, you must have completed the following:

- Configuration of the Communications Policy Agent
- Configuration of AT-TLS policies
- Installation of Server Certificate and Certificate Authority Certificate

Note: For more information about IBM Policy Agent, see the *IBM z/OS V1R11 Communications Server TCP/IP Implementation Volume 4: Security and Policy-Based Networking*.

Operator Communications Interface

z/OS operator commands are used to control the operation of the SCS address space.

You can control the groups of users who can issue operator commands. Use CA ACF2 for z/OS, CA Top Secret for z/OS, or IBM RACF to authorize or restrict users from issuing some or all commands.

To control the use of operator commands, create profiles in the SAF OPERCMDS class.

The command descriptions describe the authorization requirements for the command. In most cases, more than one level of authority is required and the user issuing the command must have all indicated access privileges.

SCS Address Space Operator Commands

This section contains descriptions of the commands that the SCS address space supports.

START Command—Start the SCS Address Space

The START command starts the SCS address space. You can enter START or the S abbreviation. You must have UPDATE authority to the SAF OPERCMDS class resource named *MVS.START.STC.procname* to use this command.

Note: Do not start the MSMCAUX procedure manually. The MSMCAUX procedure is started by the SCS address space (MSMCPROC).

The START command guidelines are as follows:

- START command parameter values override the JCL EXEC statement PARM keyword parameter values.
- Separate the keywords with two or more parameters with a comma or a space.
- Separate the keywords with two or more subparameters with a comma or a space.
- Parameters are specified as keyword parameters. Subparameters of a keyword can be positional.
- Parameters can be specified in any order.
- Parameter strings can include comments any place there is a space. Begin a comment with the starting comment delimiter (/*). (Optional) End the comments with the ending comment delimiter (*/).
- Parameters that are specified incorrectly are ignored.

This command has the following format:

```
Start procname[,,,(start_parameters)][,REUSASID=YES][,PARMS='exec_parameters']
```

procname

Specifies the name of the system PROCLIB member containing the JCL procedure that is used to start the SCS address space. The name is commonly MSMCPROC (see page 232).

,,,(start_parameters)

(Optional) Specifies the START command parameters (see page 141) for the SCS address space. The START command parameter values override the JCL EXEC statement PARM parameter values.

,REUSASID=YES

(Optional) Specifies that z/OS assigns a reusable address space identifier (ASID) to the SCS address space.

,PARMS='*exec_parameters*'

(Optional) Specifies overriding the JCL EXEC statement PARM parameters (see page 141) for the SCS address space with the parameters you specify. The exec_parameter values that you specify override the JCL EXEC statement PARM parameter values.

Examples: Start the SCS Address Space

These examples identify how to start the SCS address space using the START command.

```
S MSMCPROC,REUSASID=YES,PARMS='CONFIG(SCSPARMS)'
```

```
S MSMCPROC,,,(CONFIG(SCSPARMS)),REUSASID=YES
```

SCS Address Space Initialization

The SCS address space is initialized when the following message is received:

```
MSMC0002I SCS initialization complete. SYSNAME=system_name, CCINAME=CAICCI_name
```

The SCS address space is fully operational when the following messages are received:

```
MSMC0423I Task MSMCIENG database connection opened
MSMC0424I Task MSMCFCOM database connection opened
```

To verify that the SCS address space is listening for connections, look for the following messages:

```
MSMC0617I The SCS address space is now listening for connections on the UNIX socket
MSMC0618I The SCS address space is now listening for connections on the INET/INET6
socket, port nnnn
```

STOP Command—Stop the SCS Address Space

The STOP command initiates the normal termination of the SCS address space. You can enter STOP or the P abbreviation. Provide CONTROL authority to the SAF OPERCMDS class resource named CAMSMSCS.STOP to use this command.

To authorize, use one of the following methods, depending on how the SCS address space was started:

- If the SCS address space was started as a started task, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.STOP.STC.procname.
- If the SCS address space was started as an initiated job, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.STOP.JOB.jobname.

This command has the following format:

```
stoP jobname
```

jobname

Specifies the SCS address space started task or initiated job name. The common name is MSMCPROC (see page 232).

Example: Stop the SCS Address Space

This example identifies how to stop the SCS address space using the STOP command.

```
P MSMCPROC
```

MODIFY Command—Modify the SCS Address Space

The MODIFY commands are used to control the operation of the SCS address space. You can enter MODIFY or the F abbreviation.

To authorize, use one of the following methods, depending on how the SCS address space was started:

- If the SCS address space was started as a started task, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.STC.*procname*.
- If the SCS address space was started as an initiated job, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.JOB.*jobname*.

The MODIFY commands are:

- ABEND
- DUMP
- STOP

The MODIFY command specifications are as follows:

- Parameters are specified as keyword parameters. Subparameters of a keyword can be positional.
- Parameters can be specified in any order.
- Parameter strings can include comments anywhere a space could appear. Start a comment with the starting comment delimiter (/*). (Optional) End the comment with the ending delimiter (*/).
- Separate the keywords with two or more specified parameters (each keyword with optional value) with a comma or a space.
- Separate the keywords with two or more subparameters with a comma or a space.

  Note: Ending a comment delimiter is optional if the comment is at the end of the parameter string.

MODIFY ABEND Command—Initiate Abnormal Termination of the SCS Address Space

The MODIFY ABEND command is used to initiate the abnormal termination of the SCS address space. You can enter MODIFY or the F abbreviation. Provide CONTROL authority to the SAF OPERCMDS class resource named CAMSMSCS.ABEND to use this command.

To authorize, use one of the following methods, depending on how the SCS address space was started:

- If the SCS address space was started as a started task, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.STC.procname
- If the SCS address space was started as an initiated job, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.JOB.jobname

This command has the following format:

```
modiFy jobname,ABEND
```

jobname

Specifies the SCS address space started task or initiated job name. The name is commonly MSMCPROC (see page 232).

Example: Modify the SCS Address Space using MODIFY ABEND command

This example identifies how to modify the SCS address space using the MODIFY ABEND command.

```
F MSMCPROC,ABEND
```

MODIFY DUMP Command—Capture an SVC Dump of the SCS Address Space

The MODIFY DUMP Command is used to capture an SVC dump of the SCS address space. You can enter MODIFY or the F abbreviation. Provide CONTROL authority to the SAF OPERCMDS class resource named CAMSMSCS.DUMP to use this command.

To authorize, use one of the following methods, depending on how the SCS address space was started:

- If the SCS address space was started as a started task, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.STC.*procname*.
- If the SCS address space was started as an initiated job, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.JOB.*jobname*.

This command has the following format:

```
modiFy jobname,DUMP[ASID(asid_list)]JOBNAME(job_list)[DSPNAME(dsp_list)]
```

jobname

Specifies the SCS address space started task or initiated job name. The common name is MSMCPROC (see page 232).

Default: The SCS address space if the JOBNAME is not specified.

ASID (*asid_list*)

(Optional) Specifies the address space identifier operator input (see page 139) of one or more address spaces to include in the dump.

Limits: 1-32767 decimal range or 1-7FFF hexadecimal range

Default: The SCS address space if the ASID parameter is not specified.

JOBNAME (*job_list*)

Specifies the name of one or more address spaces to include in the dump.

Note: The *jobname* can include wildcard characters with a question mark (?), or an asterisk (*). A question mark indicates a single mask character. An asterisk indicates a 0 or more mask characters.

Limits: 1-8 characters that are expressed as a quoted, *'abc'*, or a nonquoted, *abc*, character string. A separator or delimiter indicates the end.

DSPNAME (*dsp_list*)

(Optional) Specifies the data space identifier (see page 140) of one or more data spaces to include in the dump.

Default: The data spaces that are owned by the SCS address space if the DSPNAME is not identified

Note: Wildcard characters that are used in the JOBNAME and DSPNAME parameters can result in multiple address spaces being selected for inclusion in the dump.

Example: Dump the SCS address space and the Auxiliary address spaces using MODIFY DUMP command

This example identifies how to dump the SCS and Auxiliary address spaces using the MODIFY DUMP command.

```
F MSMCPROC,DUMP JOBNAME(MSMCPROC,MSMCAUX)
```

MODIFY STOP Command—Initiate Normal Termination of the SCS Address Space

The MODIFY STOP command is used to initiate the normal termination of the SCS address space. You can enter MODIFY or the F abbreviation. Provide CONTROL authority to the SAF OPERCMDS class resource named CAMSMSCS.STOP to use this command.

Note: The results of the STOP command and the MODIFY STOP command are identical.

To authorize, use one of the following methods, depending on how the SCS address space was started:

- If the SCS address space was started as a started task, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.STC.procname.
- If the SCS address space was started as an initiated job, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.JOB.jobname.

This command has the following format:

```
modiFy jobname,STOP
```

jobname

Specifies the SCS address space started task or initiated job name. The common name is MSMCPROC (see page 232).

Example: Modify the SCS Address Space using MODIFY STOP command

This example identifies how to modify the SCS address space using the MODIFY STOP command.

```
F MSMCPROC,STOP
```

SCS Address Space ASID Operator Input Examples

Example:

The following example shows the SCS address space ASID operator input value that is expressed as a hexadecimal digit (A-F, 0-9):

X'nnnn'

The following example shows the SCS address space ASID operator input value that is expressed as a decimal digit (0-9):

ddddd

If the following address spaces exceed 15 when combined, only the first 15 are included in the dump:

- SCS address space
- Address spaces that the ASID parameter specifies
- Address spaces that the JOBNAME parameter specifies
- Address spaces owning the data spaces that the DSPNAME parameter specifies

SCS Address Space Data Space Identifier Input

The accepted data space identifier input designators are as follows:

asid.name

Specifies the hexadecimal address space identifier (ASID) of the owning address space and the *data_space_name* of the data space to include in the dump.

Limits: 1-7FFF hexadecimal range (ASID)

Default: SCS address space ASID and data spaces

Note: The first character of the specified ASID value must be a decimal digit. If the first significant digit of the ASID of the owning address space is not a decimal digit, specify the ASID with a leading zero.

jobname.name

Specifies the *jobname* of the owning address space and the *data_space_name* to include in the dump. The *jobname* can include wildcard characters with a question mark (?), or an asterisk (*). A question mark indicates a single mask character. An asterisk indicates a 0 or more mask characters.

Limits: 1-8 nonquoted characters

Note: No more than 256 data spaces are included in the dump. The wildcard characters that are used in the parameters could result in multiple data spaces being selected for inclusion in the dump.

If a data space is owned by an address space that is not included in the dump, add the address space of the ASID to the list of included address spaces. A maximum of 15 address spaces are allowed. The address space limitation could prevent specifying as many as 256 data spaces.

JCL EXEC Statement PARM Keyword and START Command Parameters

The SCS address space parameters are specified in a parameter library member. Sometimes, the SCS address space parameters are specified with the following elements:

- The PARM keyword parameter of the JCL EXEC statement in the address space startup JCL
- The START command that is used to start the SCS address space.

Parameters that can be specified with the PARM keyword parameter of the JCL EXEC statement and with the START command are identical.

If the SCS address space parameters are specified using one of these alternate methods, adhere to the following guidelines:

- START command parameter values override the JCL EXEC statement PARM keyword parameter values.
- Separate the keywords with two or more parameters with a comma or a space.
- Separate the keywords with two or more subparameters with a comma or a space.
- Parameters are specified as keyword parameters. Subparameters of a keyword can be positional.
- Parameters can be specified in any order.
- Parameter strings can include comments any place there is a space. Begin a comment with the starting comment delimiter (/*). Optionally, end the comments with the ending comment delimiter (*/).
- Parameters that are specified incorrectly are ignored.

The parameters that are used with the JCL EXEC Statement PARM keyword parameter and START command are as follows:

CONFIG(*name)*

Specifies the name of the parameter library member containing the SCS address space configuration parameters.

Limits: 1-8 characters that are expressed as a quoted, *'abc'*, or a nonquoted, *abc*, string. A separator or delimiter indicates the end.

Default: MSMCPARM when CONFIG is not specified.

ROUTCDE(*routing code list*)

Specifies a routing code or a range of routing codes that are assigned to WTO messages.

Two values that are separated by a dash (-) specify an inclusive range of routing codes.

Routing codes that are specified are in addition to the specific routing codes defined for each message.

Limits: 1-128

Example: *ddd* (where *d* is a valid decimal digit (0-9))

CASE(MIXED|UPPER)

Specifies if WTO messages are written using mixed or uppercase only characters.

MIXED

The WTO messages can be written in mixed uppercase and lowercase characters.

UPPER

The WTO messages can be written using uppercase characters.

Default: MIXED

DAE(YES|NO)

Specifies if DAE dump suppression is allowed or prevented.

YES

DAE dump suppression is allowed.

NO

DAE dump suppression is prevented.

Default: YES

Parameter Libraries

SCS address space parameters are specified as configuration parameters in a member of the parameter library.

The parameter library is the data set or data sets allocated to the MSMPARM DD statement in the SCS address space JCL procedure.

The parameter library must be a partitioned data set or a concatenation of partitioned data sets and each partitioned data set must have variable-length records. Each parameter library member contains an XML document that specifies the address space parameters and contains various elements.

To facilitate using common configuration parameters for multiple instances of the SCS address space, configuration parameters in a member of a parameter library can contain z/OS system symbols.

Note: CA CSM includes the MSMCPARM parameter library member, which contains the default SCS address space parameters.

MSMCPARM Member

You can include the following elements in the MSMCPARM member documents that specify the address space parameters:

Data Recovery Parameters

Sets the parameters related to the SCS address space use of disk storage for data recovery purposes. The parameters are used when allocating data sets created to save existing data for recovery purposes.

The Data Recovery Parameters are specified using the following attributes:

dsnhlq

Specifies the data set name high-level qualifier used when allocating data sets created for data recovery purposes.

Limits: 1 to 17 bytes. The value can include static and dynamic system symbols and installation defined static system symbols.

Note: See the IBM *z/OS MVS Initialization and Tuning Reference* guide for a list of system symbols.

(Optional) *&SYSUID*

Specifies the user ID of the CA CSM user that initiated the configuration request for which data sets are created for recovery purposes.

Limits: The ampersand character (&) cannot be specified as a literal in the attribute value of an XML document. The character must be used to convert subsequent characters to a control sequence using the character string *'&'*.

Example: '&SYSNAME..MSM', dsnhlq='&SYSNAME..MSM'

Default: &SYSUID..MSMDATA

unit

Specifies unit name used when allocating z/OS data sets created for data recovery purposes.

Limits: 1 to 8 bytes

Default: None

volser

Specifies the volume serial number used when allocating data sets created for data recovery purposes.

Limits: 1 to 6 bytes. The characters of the serial number must be alphabetic, national, or a hyphen.

Default: None

mgmtclas

Specifies the SMS management class used when allocating data sets created for data recovery purposes.

Limits: 1 to 8 bytes. The first character of the class name must be alphabetic or national. Remaining characters must be alphanumeric or national.

Default: None

storclas

Specifies the SMS storage class used when allocating data sets created for data recovery purposes.

Limits: 1 to 8 bytes. The first character of the class name must be alphabetic or national. Remaining characters must be alphanumeric or national.

Default: None

TCP/IP

Specifies the address space parameters for the interface between the SCS address space and TCP/IP for communicating with other components of CA CSM.

The TCP/IP parameters are specified using the following attributes:

ipaddr

Specifies the IP address of the interface through which the SCS address space accepts TCP connection requests from other CA CSM components.

Limits: IPv4 address using standard dotted decimal notation.

(Optional) IPv6 address using one of the standard text forms that are defined in RFC 4291, IPv6

Example 1: 0.0.0.0

Example 2: ::

Note: The IPv4 unspecified address, 0.0.0.0, is used to indicate that the SCS address space accepts TCP connection requests through all IPv4 interfaces. The IPv6 unspecified address, :: , can be used to indicate that the SCS address space accepts TCP connection requests through all IPv4 and IPv6 interfaces.

Default: ::

port

Specifies the port number the SCS address space uses to listen for TCP connection requests from other CA CSM components.

Limits: 65535

Default: 49152

Console

Sets the parameters related to the SCS address space usage of extended MCS consoles that issue z/OS commands, receive command responses, and receive unsolicited message traffic.

The console parameters are specified using the following attributes:

prefix

Used in the construction of extended MCS console names.

Limits: 1 to 5 bytes. The first character must be alphabetic or national. Remaining characters must be alphanumeric or national.

Default: CAMSM

auth

Specifies the authority the extended MCS consoles have to issue z/OS commands.

The assigned authority specifies the commands that can be entered from the console. Separate multiple values with a blank space or a comma.

Enter one or more of the following values from the console:

MASTER

Allows the consoles to act as a master console, which issues all MVS commands.

ALL

Allows the consoles to issue system control commands, input/output commands, console control commands, and informational commands.

SYS

Allows the consoles to issue system control commands and informational commands.

IO

Allows the consoles to issue input/output commands and informational commands.

CONS

Allows the consoles to issue console control commands and informational commands.

INFO

Allows the consoles to issue informational commands.

Default: INFO

Note: SYS, IO, and CONS can be specified together in any combination. All others are mutually exclusive.

See the IBM *z/OS MVS System Commands Reference* guide for information about which commands can be entered from a console with a specific authority level.

Note: The security product settings override the console command authority settings for z/OS commands protected by a security product. For example, CA ACF2 for z/OS, if the OPERCMDS class is active and a profile is defined to protect the command.

SAF

Sets the parameters related to the SCS address space interface to the System Authorization Facility (SAF).

The SAF parameters are specified using the following attributes:

application

Specifies the application name assigned to the SCS address space.

Limits: 1 to 8 bytes. The first character must be alphabetic or national. Remaining characters must be alphanumeric or national.

Default: MSMCAPPL

requestor

Specifies the name assigned to the SCS address space that assigns a unique control point within a set of control points that exist in a subsystem.

Note: If you specify a requestor name and IBM RACF is installed, you must update the IBM RACF router table with a matching entry. If you do not update the table, IBM RACF processing is bypassed.

Limits: 1 to 8 bytes. The first character must be alphabetic or national. Remaining characters must be alphanumeric or national.

Default: None

subsystem

Specifies the subsystem name, version, and release level assigned to the SCS address space.

Note: If you specify a subsystem name and IBM RACF is installed, you must update the IBM RACF router table with a matching entry. If you do not update the table, IBM RACF processing is bypassed.

Limits: 1 to 8 bytes. The first character must be alphabetic or national. Remaining characters must be alphanumeric or national.

Default: None

SSL

Sets the parameters related to the SCS address space interface to the System SSL Cryptographic Services.

The SSL parameters are specified using the following attributes:

keyring

Specifies the path and file name of the key ring database file used for encrypting data from remote systems, or the SAF key ring label defined in the external security manager such as CA ACF2 for z/OS, CA Top Secret for z/OS, or IBM RACF for the user ID assigned to the SCS address space.

Used to retrieve the default certificate to send to the client side to begin the process of securing the connection for communication.

Default: None

stashfile

Specifies the path and file name of the stashfile if the key ring attribute is set to the path and file name of a key ring database file.

The stashfile contains the password to access the key ring database file.

Limits: Required if the key ring attribute is set to a key ring database file name.

Default: None

AUX

Sets the parameters that are related to the SCS AUX address space.

The SCS AUX address space parameters are specified using the following attributes:

procname

Specifies the name of a JCL procedure library member that contains the source JCL for the SCS AUX address space.

Limits: 1-8 bytes. The first character must be alphabetic or national. The remaining characters must be alphanumeric or national.

Default: MSMCAUX (see page 232)

jobname

Specifies the job name that is assigned to the SCS AUX address space.

Limits: 1-8 bytes. The first character must be alphabetic or national. The remaining characters must be alphanumeric or national.

Default: The JCL procedure library member name (if the source JCL is a procedure), or the job name that is assigned on the JOB statement (if the source JCL is a job).

reusasid

Determines if a reusable ASID is requested for the SCS AUX address space.

The SCS AUX address space receives one of the following values:

YES

The SCS AUX address space is assigned a reusable ASID if REUSASID (YES) is also specified in the DIAG*xx* PARMLIB member.

NO

The SCS AUX address space is not assigned reusable ASID.

Default: YES

Note: Using a reusable ASID results in an ABEND of system 0D3 if products or programs that are used in the configuration of a CA Technologies product are not upgraded to tolerate reusable ASIDs.

See the IBM *z/OS MVS Programming: Extended Addressability Guide* for more information about reusing ASIDs.

maxactive

Specifies the maximum number of concurrently active SCS AUX address spaces.

Limits: 1 to 20 numeric

Default: 20

SCS Address Space Message Log (SCSLOG)

The SCS address space message log (SCSLOG) is a detailed log of all messages that the SCS address space writes.

SCS address space messages that are written to the z/OS hardcopy message log are also written to the SCSLOG. In addition, the SCSLOG is used for messages that are more detail-oriented and that can be useful when diagnosing problems. The SCSLOG is therefore a more complete record of the activities of the SCS address space.

The SCSLOG is implemented using the z/OS UNIX System Services (USS) syslog daemon. The syslog daemon is part of the z/OS system product. The syslog daemon must be explicitly started using the USS syslogd command.

Note: For more information about the syslog daemon, see the IBM *z/OS Communications Server: IP Configuration Guide* and the *z/OS Communications Server: IP Configuration Reference*.

Configure Syslog Daemon

A configuration file controls the syslog daemon (syslogd) processing.

Default: `/etc/syslog.conf`

Statements in the configuration file define logging rules and output destinations for log messages. You define logging rules in the syslog daemon configuration file to send SCS address space messages to specific destinations.

The logging rules are defined using a facility name and a priority code. The user ID and job name of the program that generates the message can also be specified in the logging rule.

Note: AUX address space messages are written to the syslog daemon by a process executing in the SCS address space. Only define logging rules for the SCS address space job name. No logging rules are needed for the AUX address space job name.

All SCS address space messages that are written to the syslog daemon specify a facility name of ‘user’.

Each SCS address space message that is written to the syslog daemon specifies one of the following priority codes:

info

Messages with this priority code are informational messages.

warning

Messages with this priority code are warning messages.

error

Messages with this priority code are error messages.

crit

Messages with this priority code are severe error messages.

debug

Messages with this priority code are debugging messages.

Example: Add statements to the syslog daemon

To allow all messages that job MSMCPROC writes to write to the file /tmp/syslogd/msmcproc.syslog, add the following statements to the syslog daemon configuration file and activate the changes.

```
#
#  CA CSM SCS message log (SCSLOG)
#
*.MSMCPROC.*.* /tmp/syslogd/msmcproc.scslog
```

Activate Syslog Daemon Configuration Changes

After you update the syslog daemon configuration file, send a SIGHUP signal to the syslog daemon. You do so to cause the daemon to reread the configuration file and activate any modified parameters.

Use the USS kill command to send the SIGHUP signal.

This command has the following format:

`kill –s SIGHUP` *`pid`*

pid

Specifies the syslog daemon process ID.

Depending on how it is started, the syslog daemon stores its process ID in a file. The file can be used to reconfigure the daemon.

- If the syslog daemon is started in normal or local-only mode, the file is named as follows:

  /etc/syslog.pid

- If the syslog daemon is started in network-only mode, the file is named as follows:

  /etc/syslog_net.pid

The syslog daemon continues to append log messages to the files you specify in the configuration, after reading the configuration file again.

Note: All log files that the syslog daemon uses must be created in the z/OS UNIX file system before the syslog daemon is started or reconfigured, unless the syslog –c option is specified. If the –c option is specified, the syslog daemon dynamically creates log files that are not already in existence.

Generalized Trace Facility

The SCS address space uses the generalized trace facility (GTF) to capture data for diagnostic purposes. GTF is a part of the z/OS system product. GFT must be explicitly activated by issuing a START GTF command.

Note: For more information about GTF, see the *IBM MVS Diagnosis Tools and Service Aids*.

Start the GTF

To start the GTF, enter a START GTF command. You can start the GTF by using the IBM-supplied procedure or your internal procedure for starting GTF.

Note: Multiple instances of GTF can be active simultaneously. Each instance operates as a system task in its own address space.

Each instance of GTF can be assigned a unique identifier that is specified on the START GTF command. The identifier lets you recognize and control specific instances of GTF. If a unique identifier is not specified, the operating system assigns the device number of the device where the trace data set resides.

The events that GTF traces are specified as options. You specify the USRP and JOBNAMEP options for the SCS address space.

After you specify the USRP GTF option, GTF prompts you for the list of event identifiers (EIDs).

The SCS address space uses the following EIDs:

301

Captures diagnostic data for the infrastructure component of the SCS address space.

302

Captures diagnostic data for the communications server component of the SCS address space.

303

Captures diagnostic data for the communications server event API component of the SCS address space

304

Captures diagnostic data for the container section component of the SCS address space.

305

Captures diagnostic data for the implementation engine component of the SCS address space.

306

Captures diagnostic data for the services section component of the SCS address space.

307

Captures diagnostic data for the system information agent component of the SCS address space.

Note: To avoid unwanted information, limit the GTF trace output using the USRP option.

If the JOBNAMEP GTF option is specified, you are prompted for the list of job names that trace output is captured for. Specify the names of the SCS address space, both main and auxiliary. The common names are MSMCPROC (see page 232) and MSMCAUX (in this order).

Example

CA CSM includes the MSMCGTFP sample member that contains the following GTF trace options:

```
TRACE=USRP,JOBNAMEP
USR=(301,302,303,304,305,306,307)
JOBNAME=(MSMCPROC,MSMCAUX)
END
```

Stop the GTF

To stop the GTF, issue a STOP GTF command. Specify the identifier on the START GTF command. If an identifier is not specified on the START GTF command, specify it on the device number of the device where the trace data set resides.

Appendix A: CA CSM Implementation and Status

This section contains the following topics:

Implementation Checklist

Use the checklists in this section to confirm that each role has completed the tasks that are associated with them.

Network Administrator

Configure access to the following websites:

- supportservices.ca.com (using HTTPS Port Number 443)
- ftp.ca.com (using FTP Port Number 21)
- ftpca.ca.com (using FTP Port Number 21)

  Note: CA CSM uses this FTP server to accumulate minimal information. This information includes the site ID, the product, and the user ID for the CA Support Online website. Sometimes site access rules deny an FTP connection that is established for this purpose or the connection cannot be established for any other reason. Then CA CSM still continues to function.
- scftpd.ca.com (using FTP Port Number 21)

- ftpdownloads.ca.com (using FTP Port Number 21)
- supportftp.ca.com (using FTP Port Number 21)
- sdownloads.ca.com (using HTTPS Port Number 443)

  Note: sdownloads.ca.com is only required if you use the Use HTTPS for Downloads acquisition option under System Settings, Software Acquisition on the Settings page. If you authorize the ca.com domain for both ports 80 and 443, you do not need to authorize sdownloads.ca.com.

In addition, your network administrator must define a Domain Name System (DNS) entry for localhost.

Security Administrator

1. Grant UPDATE authority to the following data sets or libraries to the user who implements CA CSM:
   - SYS*x*.PARMLIB
   - Procedure library that stores the JCL jobs that are used to start the CA CSM address spaces, for example, SYS3.PROCLIB
   - (Optional) The master catalog if you decide to define alias entries for the CA CSM data set prefixes
2. Grant the following access to the user ID associated with the CA CSM setup utility, MSMSetup.sh:
   - Access to USS
   - Permission to access the following FACILITY class profiles that are related UNIX:
     - BPX.FILEATTR.APF (READ authority)
     - BPX.FILEATTR.PROGCTL (READ authority)
     - BPX.FILEATTR.SHARELIB (READ authority)
     - BPX.SERVER (UPDATE authority)
     - BPX.CONSOLE (READ authority)
   - Permission to access the SERVAUTH class profile, EZB.STACKACCESS (READ authority)
   - CA ACF2 for z/OS only: MUSASS permission for users who start CA CSM
   - If your site uses CA SAF HFS security, the following access:
     - BPX.CAHFS.SET.RLIMIT (READ authority)
     - BPX.CAHFS.PTRACE (READ authority)
     - BPX.CAHFS.MOUNT (READ authority)

- BPX.CAHFS.UNMOUNT (READ authority)
- BPX.CAHFS.CHANGE.FILE.MODE (READ authority)

Note: CA SAF HFS security is a feature in CA ACF2 for z/OS and CA Top Secret for z/OS.

- Permission to access the CSFSERV class profile, CSFOWH (READ authority) providing you want to perform SMP/E GIMUNZIP hash validation
- Permission to create and modify data sets for the qualifiers (CA CSM MVS SMP/E and runtime data sets) specified in the options file (see page 157).

  Note: Your user ID can have BPX.SUPERUSER access and it can switch to SUPERUSER. Then the switched SU ID requires a create and modify access to the MVS data set qualifiers specified in the options file (see page 157).
- If you are using IBM RACF, access to the following data sets for program control:
  - SYSx.MIGLIB
  - CEE.SCEERUN2
  - Members IEANTCR, IEANTDL, and IEANTRT of SYS1.CSSLIB
  - Member JVMLDM60 (for 31-bit Java 6.0) or JVMLDM66 (for 64-bit Java 6.0) of the data set where Java load modules are installed.

    Or
  - Member JVMLDM61 (for 31-bit Java 6.0.1) or JVMLDM67 (for 64-bit Java 6.0.1) of the data set where Java load modules are installed.

    Or
  - Member JVMLDM70 (for 31-bit Java 7.0.) or JVMLDM76 (for 64-bit Java 7.0)
  - (Optional) member IDIXCEE of SYS1.IDI.SIDIAUTH, only if you use IDIXCEE as an optional exit.

  Note: To display the resources, issue the RLIST command.

  You can set IBM RACF to control programs. If the resources do not exist, issue the following command:

  ```
  RDEFINE PROGRAM member ADDMEM('hlq.libraryname'//NOPADCHK) UACC(READ)
  ```

  For example:

  ```
  RDEFINE PROGRAM IEANTCR ADDMEM('SYS1.CSSLIB'//NOPADCHK) UACC(READ)
  ```

  If the resources exist, issue the following command:

  ```
  RALTER PROGRAM member ADDMEM('hlq.libraryname'//NOPADCHK) UACC(READ)
  ```

  For example:

  ```
  RALTER PROGRAM IEANTCR ADDMEM('SYS1.CSSLIB'//NOPADCHK) UACC(READ)
  ```

Note: To set all members of a data set as a controlled program, replace the member name with an asterisk (*). For example:

```
RDEFINE PROGRAM * ADDMEM('SYS1.CSSLIB'//NOPADCHK) UACC(READ)
```

Important! If you are planning to use zFS, add IOE.SIOELMOD (or equivalent library) to program control.

3. Grant the following access to the user ID associated with the CA CSM application server (MSMTC job or started task):
   - Access to USS
   - Authority to create and mount file systems
   - Permission to access the following FACILITY class profiles that are related UNIX:
     - BPX.FILEATTR.APF (READ authority)
     - BPX.FILEATTR.PROGCTL (READ authority)
     - BPX.FILEATTR.SHARELIB (READ authority)
     - BPX.SERVER (UPDATE authority)
     - BPX.CONSOLE (READ authority)
   - Permission to access the SERVAUTH class profile, EZB.STACKACCESS (READ authority)
4. Set up OMVS segments for CA CSM users.

USS Administrator

Set up the USS paths using the following structure:

```
/u/users/msmserv (primary mount point)
     msminstall (1000 cylinders)
     msm (750 cylinders)
     msmruntime (750 cylinders)
     mpm (mount point for CA CSM use)
```

Systems Programmer

1. Ensure that prerequisite requirements are met.
2. Review the options file keywords and gather the required values.
3. Download CA CSM.

4. Unpack CA CSM:

   ```
   pax -rvf 51000068X01.pax.Z
   ```

   Note: The full pax file name, including the Z suffix, is case-sensitive. Verify that you use the exact case of the file name on the system where you issue the pax command. Rename the file, if necessary.

5. Customize and submit UNZIPJCL to extract CA CSM product files.
6. Customize the MSMSetupOptionsFile.properties file.
7. Execute MSMSetup.sh.
8. Start CA CSM using the following members in sequence:
   - MSMMUFS JCL member or MSMMUF PROCLIB member
   - MSMDBSVS JCL member or MSMDBSRV PROCLIB member
   - MSMTCSRV JCL member or MSMTC PROCLIB member
9. Access CA CSM using a web browser and perform initial configuration.
10. Set up CAIRIM to load CA Datacom/MSM SVC at IPL.
11. Clean up the USS directory.
12. To support product deployment, ensure that the deployment activation elements for each CA Technologies product have been acquired and installed.

    Note: For more information about product deployment, see the chapter *Deploying Products* in the *User Guide*.

Options File Keywords

The CA CSM setup utility uses the contents of the MSMSetupOptionsFile.properties options file in the MSMSetup directory to tailor the CA CSM installation and setup process.

The file uses the following keywords to specify the option values in the format *option_keyword=value*.

Important! The keywords that are used in the options file are specific to the CA CSM installation setup process. The values for some keywords are transformed to values that are acceptable to CA CSM during this process. Do not use these values for similar keywords in other areas of CA CSM unless requested by CA Support.

MSMProdPaxPath

Specifies the path to the extracted CA CSM files. The value is the path defined for the CA CSM Product archive ID in the UNZIPJCL job.

Example: /u/users/msmserv/msminstall/MSMProduct

JAVAPATH

Specifies the path to the IBM Java SDK for z/OS components.

Example: /usr/lpp/java/J6.0

SMP/E Installation Data Set and Location Details

Important! If you are an existing CA CSM customer migrating to the latest CA CSM version, specify a unique value for all of the keywords described in this section. The new keyword value must be different from the value in any other previous CA CSM version.

CSIHLQ

Specifies the prefix (high-level qualifier) for the consolidated software inventory (CSI) data set, and other SMP/E data sets such as SMPPTS and SMPSTS.

Default: CAI

TargetHLQ

Specifies the prefix for the target data sets.

Default: The value of CSIHLQ

Important! The value of TargetHLQ must be different from RunTimeMVSHLQPrefix and DatabaseHLQ.

TargetZoneName

Specifies the SMP/E environment target zone name.

Default: CAIT

DlibHLQ

Specifies the prefix for the distribution data sets.

Default: The value of CSIHLQ

Important! The value of DlibHLQ must be different from RunTimeMVSHLQPrefix and DatabaseHLQ.

DlibZoneName

Specifies the SMP/E environment distribution zone name.

Default: CAID

MSMPATH (see page 178)

Specifies the path of the USS directory in which to install CA CSM. This directory becomes the CA CSM root and must be available and writable when you execute the CA CSM setup utility.

You must define the mount point. The required file system space is about 250 cylinders.

Runtime Data Set and Location Details

Important! If you are an existing CA CSM customer migrating to the latest CA CSM version, specify a unique value for all of the keywords described in this section. The new keyword value must be different from the value in any other previous CA CSM version.

RunTimeMVSHLQPrefix

Specifies the prefix for CA CSM runtime data sets, which are runtime copies of the target data sets.

Important! The value of RunTimeMVSHLQPrefix must be different from TargetHLQ and DlibHLQ.

RunTimeUSSPath (see page 178)

Specifies the path of the USS directory for CA CSM runtime use. This directory must be available and writable when you execute the CA CSM setup utility.

The required space is about 750 cylinders.

Database Data Set and Location Details

DatabaseHLQ

Specifies the prefix for CA Datacom data sets that are created during the installation process.

Default: The value of RunTimeMVSHLQPrefix

Important! The value of DatabaseHLQ must be different from TargetHLQ and DlibHLQ.

Important! If you are an existing CA CSM customer and planning to migrate to the latest CA CSM version, specify a unique value for this keyword. The new keyword value must be different from the value in any other previous CA CSM version.

CA Datacom/MSM

MUFname

Specifies your preferred name for the CA Datacom/MSM Multi-User Facility (MUF). CA Datacom uses the name to differentiate between multiple instances of MUF. If your site has multiple MUFs on a system or in a sysplex, verify that the name is unique within CAICCI Plex.

Example: MSMR5MUF

Limits: Eight characters

Note: If you are an existing CA CSM customer and migrating to the latest version, the parameter value can be the same as in the previous version.

ServerName

Specifies your preferred name for the CA Datacom/MSM server. CA Datacom uses the name to differentiate between multiple instances of the server. If your site has multiple CA Datacom/MSM servers on a system or in a sysplex, verify that the name is unique within CAICCI Plex.

Note: The name must be unique across the CAICCI Plex, and the server name and application ID must be unique within the sysplex. Keeping these values unique ensures that the database servers do not fail during startup.

Example: MSMR5SRV

Note: If you are an existing CA CSM customer and migrating to the latest version, the parameter value can be the same as in the previous version.

CXXNAME

Specifies the name of the identifier for the CA Datacom/AD Directory when it is initialized. This value is used for the CA Datacom DBUTLTY INIT CXX options, CXXNAME parameter.

Limits: Eight characters

Default: CAMSM

Note: For more information about CXXNAME naming conventions, see the *CA Datacom/DB DBUTILTY Reference Guide*.

SVCNO

Specifies an SVC number for CA Datacom/MSM.

Note: Do not use the same SVC used by a running instance of CA Datacom r11.

Limits: 200 through 255

Note: If you are upgrading from CA MSM r3.1, you must use a different SVC. If you are an existing CA CSM customer and migrating from CA MSM V4.0 or a later version, the parameter value can be the same as in the previous version.

Ports, Data Sets, and USS Directories

Note: If you are an existing CA CSM customer migrating to the latest CA CSM version, any keyword value described in this section can be the same as in the previous version.

MSMServerPortNo

(The CA CSM application server HTTP port) Specifies the port number to use for web-based access to CA CSM.

Default: 22120

MSMDSIPORTNO

(The CA DSI Server port) Specifies the port number for CA DSI Server, which CA CSM uses internally to provide security features.

Default: 22130

MSMConnectorRedirectPortNo

(The CA CSM application server redirect port) Specifies the port number to which a request is redirected. Redirection occurs if a request comes in on a non-SSL port and is subject to a security constraint with a transport guarantee that requires SSL.

Default: 22140

MSMTomcatServerShutdownPortNo

(The CA CSM application server shutdown port) Specifies the port number to which the CA CSM application server (see page 229) listens for the shutdown command.

Default: 22150

Mount Point Manager

MVSHFSDsnPrefix

Specifies the prefix for the names of file system data sets. The value sets the default for the Mount Point Management Data Set Prefix in the web-based interface. A CA CSM administrator can override this value.

Default: OMVSUSR.CAMSM

Important! If you are migrating from a previous version, verify that the value for this keyword is the same as the value for the previous version.

MountPath **(see page 178)**

Specifies the path to the USS directory that CA CSM can use for work files. This directory must be available when you execute the setup utility. The value sets the default for the Mount Point Management Application root in the web-based interface. A CA CSM administrator can override this value.

Important! If you are migrating from a previous version, verify that the value for this keyword is the same as the value for the previous version.

mpmAutomount

Specifies whether CA CSM mounts the file systems during startup.

Options include:

- Y (Yes)
- N (No)

Default: Y

Note: If you are an existing CA CSM customer and migrating to the latest version, the parameter value can be the same as in the previous version.

USSFileSystemType

Specifies whether an HFS or a zFS file system be used for temporary files.

Value: HFS or ZFS

Default: ???

Note: We recommend using zFS file systems. For information about how to migrate from HFS file systems to zFS file systems, see the latest *IBM z/OS Migration* guide.

Note: If you are an existing CA CSM customer and migrating to the latest version, the parameter value can be the same as in the previous version.

mpmAllocation

Specifies whether to use SMS when allocating new data sets for file systems on the Mount Point Management page of the Settings tab.

Options include the following:

- SMS
- NONSMS

Default: SMS

mpmStorageClass

Specifies the SMS storage class of the DASD on the Mount Point Management page in the web-based interface. This value is used during product installation and maintenance.

When mpmAllocation is set to SMS, this parameter is used. Leave this parameter blank to use default site settings.

Default: Site-specific SMS default settings

Note: If you are an existing CA CSM customer and migrating to the latest version, the parameter value can be the same as in the previous version.

mpmMgmtClas

Specifies the SMS management class for file system data sets on the Mount Point Management page of the Settings tab.

When mpmAllocation is set to SMS, this parameter is used. Leave this parameter blank to use default site settings.

mpmDataClas

Specifies the SMS data class for file system data sets on the Mount Point Management page of the Settings tab.

When mpmAllocation is set to SMS, this parameter is used. Leave this parameter blank to use default site settings.

mpmUnit

Specifies the type of the DASD on which to place data sets on the Mount Point Management page of the Settings tab.

When mpmAllocation is set to NONSMS, this parameter is used. The value can be blank.

mpmVolumeSer

Specifies the NONSMS volume serial number of the DASD on the Mount Point Management page in the web-based interface. This value is used during product installation and maintenance.

When mpmAllocation is set to NONSMS, this parameter is used. The value can be blank. If specified it must be the volume serial number of an online volume.

Note: If you are an existing CA CSM customer and migrating to the latest version, the parameter value can be the same as in the previous version.

TempSpaceCleanupInterval

Specifies the time interval, in minutes, for CA CSM to clean up temporary workspace. A value of zero (0) disables this feature.

Default: 60

Limits: 1440

Software Installation Service

sisExecutorOutputStorclas

Specifies the SMS storage class for the data sets that executed programs use for temporary data during a product installation through the CA CSM Software Installation Service.

The value can be blank.

Default: Site-specific SMS default settings

Note: If you are an existing CA CSM customer and migrating to the latest version, the parameter value can be the same as in the previous version.

sisExecutorOutputUnit and sisExecutorOutputVolser

Specify the type and volume serial number of the DASD to use for the data sets that executed programs use for temporary data.

Both values can be blank. If specified, sisExecutorOutputVolser must be the volume serial number of an online volume and sisExecutorOutputUnit must be a valid unit device type.

sisGimunzipTempVolser

Specifies the volume serial number (SMS or NONSMS managed) of the DASD to use for the temporary data sets created by GIMUNZIP during a product installation through the CA CSM Software Installation Service.

The value can be blank. If specified, sisGimunzipTempVolser must be * (an asterisk) or the volume serial number of an online volume.

Note: If you are an existing CA CSM customer and migrating to the latest version, the parameter value can be the same as in the previous version.

sisGimunzipTempPrefix

Specifies the prefix CA CSM uses for GIMUNZIP output temporary data set names during product installation and maintenance. The created temporary work files are not SMP/E controlled data sets. CA CSM deletes them through the product installation process. These files are used as input relative files for SMP/E processing during the receiving of a product into the SMP/E environment global zone.

Limits: 12 through 19 characters (depending on the number of characters used for *jobname*)

Note: If you use the default 6-character *jobname*, you can enter up to 14 characters for the GIMUNZIP temporary prefix.

Note: If you are an existing CA CSM customer and migrating to the latest version, the parameter value can be the same as in the previous version.

DATASETSUFFIX

Specifies a qualifier CA CSM uses for the names of the file system data sets allocated for the software catalog to store packages during product installation and maintenance. The full data set name appears in the format: MVSHFSDsnPrefix.DATASETSUFFIX*nnnn*

nnnn

Represents the unique numeric identifier CA CSM automatically appends to the qualifier.

Default: CASC

Limits: Four characters

Example:

MVSHFSDsnPrefix = OMVSUSR.CAMSM

DATASETSUFFIX = CASC

Full data set name: OMVSUSR.CAMSM.CASC1234

Note: If you are an existing CA CSM customer and migrating to the latest version, the parameter value can be the same as in the previous version.

sisExecutorServerDsnPrefix

Specifies the data set prefix for storing temporary output files created by the execution of SMP/E during a product installation and maintenance. This value can be blank.

Default: *SAF_userid*

Limits: 24 characters

Note: If you are an existing CA CSM customer and migrating to the latest version, the parameter value can be the same as in the previous version.

Security

safSecurity

Specifies whether to enable security checking for the resources on the web-based interface.

Default: N

Note: If you are an existing CA CSM customer and migrating to the latest version, the parameter value can be the same as in the previous version.

safResourceClass

Specifies the SAF resource class name that CA CSM uses for security rules in resource profiles.

Default: CAMSM

If you disable the SAF security manager, the following parameter applies:

sysTaskDeleteOverrideEnabled

Specifies whether to let CA CSM users delete tasks.

Y

Any user can delete any competed task.

N

Users cannot delete completed tasks.

Default: N

SMP/E GIMUNZIP

HASH

Specifies whether to perform SMP/E GIMUNZIP hash validation.

Default: Y (recommended)

If you perform hash validation, the following parameter applies:

ICSF

Specifies whether the system has Integrated Cryptographic Services Facility (ICSF) installed.

Default: Y

If you perform hash validation and ICSF is not installed, the following parameter applies:

SMPCPATH

Specifies the path to the SMP/E Java application classes.

Example: /usr/lpp/smp/classes

SMP/E GIMSMP

CSIVOL

Specifies the volume serial number of the DASD on which to place CA CSM SMP/E data sets.

Default: *

If you want to use the SMS default volume, specify *.

Note: If you specify SmpeVOL=* and your site does not have any default or standard volume specified in SMS, then the first installation job (CSMN5102 for a new installation, or CSMU*xx*02 for an upgrade) may fail with an IDCAMS error while allocating the CA CSM SMP/E environment. In that scenario, specify a valid SMS or non-SMS volume and rerun the installer.

TargetVOL

Specifies the volume serial number of the DASD on which to place CA CSM SMP/E target data sets.

Default: The value of CSIVOL

If you want to use the SMS default volume, specify *.

DlibVOL

Specifies the volume serial number of the DASD on which to place CA CSM SMP/E distribution data sets.

Default: The value of CSIVOL

If you want to use the SMS default volume, specify *.

RuntimeVOL

Specifies the volume serial number of the DASD on which to place CA CSM runtime data sets.

Values: Blank or *, or valid SMS or non-SMS volume

If you want to use the SMS default volume, specify *.

Default: *

DatabaseVOL

Specifies the volume serial number of the DASD on which to place CA Datacom data sets created during the installation process.

Values: Blank or *, or valid SMS or non-SMS volume

If you want to use the SMS default volume, specify *.

Default: The value of RuntimeVOL

TEMPUNIT

Specifies the esoteric unit for temporary work data sets.

Default: SYSDA

SMP/E Storage

STORAGE

Specifies whether to let SMS manage the SMP/E temporary data sets.

Values: SMS or NONSMS

If SMS is used, the following storage parameters apply:

Note: If your site uses SMS ACS, ACS overrides the storage parameter values.

MGMTCLAS

Specifies the SMS management class to use for the temporary SMP/E data sets. Management classes define different levels of migration, backup, and retention services.

STORCLAS

Specifies the SMS storage class to use for the temporary SMP/E data sets. Storage classes define different levels of performance and availability services.

DATACLAS

Specifies the SMS data class to use for the temporary SMP/E data sets. Data classes define different allocation defaults.

If NONSMS is used, the following parameter applies:

UNIT and VOLUME

Specifies the type and volume serial number of the DASD on which to place temporary SMP/E data sets.

Example: 3390 and DASD01

JVM

JVMdsn

Specifies the name of the data set where the JVM load module is located.

Example: SYS1.SIEALNKE

CA Common Services for z/OS

CCSdsn

Specifies the fully qualified name of the CA Common Services for z/OS target load library. The library must be APF-authorized.

CCScaipdsedsn

Specifies the fully qualified name of the CA Common Services for z/OS CAIPDSE data set.

CCISSLPortNo

Specifies the CA Common Services for z/OS CCITCP or CCISSL port number configured on your system.

You can find this value through the following message:

`CAS9850I CAICCI TCP/IP server ready. PORT port-number ADDR host_address`

Default: 1202

ENF SystemID

Specifies the value of CA Common Services for z/OS CAICCI SYSID on your system.

You can find this value through the following console message:

`CAS9214I - CA-ENF Command: SYSID(caicci_sysid)`

You can issue the following operator command to obtain the value:

`ENF DISPLAY,SYSID`

Installation Job Processing

ActiveJES

Specifies the type of job entry subsystem (JES) used on the z/OS system.

Default: JES2

Value: JES2 or JES3

JOBNAME

Specifies the job name that is used in the JOB statement for all jobs that are submitted as part of installation.

Default: ID of the user who executes the CA CSM setup utility concatenated with #.

MSGCLASS

Specifies the JES output class for job logs. The class determines how the logs are handled (for example, held for later review).

Default: X

CLASS

Specifies the JES initiator class to use for jobs.

Default: A

ACCOUNT

Specifies the job accounting string to use in the JOB statement for all jobs.

Example: '1234,dept01,NY NY'

SYSAFF

Specifies the systems that are eligible to process jobs. The keyword specifies the value of the JOBPARM SYSAFF parameter.

You can specify the ID of a particular system so that jobs are processed on that system. If you do not want to use this feature, do not specify a value.

CA CSM Installer Execution Control Parameters

AddAPFauthDSdyn

Specifies whether the CA CSM installer dynamically adds data sets that the CA Datacom/MSM job requires to be APF-authorized to the APF list.

Y

Allows the CA CSM Installer to dynamically add the CA Datacom/MSM data sets to the APF list.

N

Lets you manually add the CA Datacom/MSM data sets.

Default: Y

InstallSVC

Specifies whether CA Datacom/MSM SVC should be installed.

Y

Installs CA Datacom/MSM SVC during a CA CSM installation process.

Note: If you are upgrading from CA MSM r3.1, you must use a different SVC. Set this parameter to **Y**.

N

Skips the CA Datacom/MSM SVC load step during a CA CSM installation process.

Note: If you reinstall CA CSM or upgrade from CA MSM V4.0 or a later version and have an available SVC installed at your site, set this parameter to **N**.

Default: Y

Site Defaults

HOSTNAME

Specifies the host name or IP address of your system. The Prerequisite Validator utility uses this keyword to test the FTP connection and verify the JESINTERFACELEVEL value.

MFASM

Specifies the name of the z/OS assembler program SMP/E is to use.

Default: ASMA90

MFZAP

Specifies the name of the system utility program used to install changes for modules, load modules, or CSECTs within modules.

Default: IMASPZAP

MFLKED

Specifies the name of the link-edit program or procedure to use.

Default: IEWL

TCPdsn

Specifies the name of the TCPIP.DATA data set.

Example: TCPIP.TCPIP.DATA

Note: This value can be left blank. If errors are encountered during the Apache Tomcat startup job (MSMTCSRV), you can uncomment the SYSTCPD DD card inside MSMTCSRV for diagnostic purposes.

TCPIPLinkDSName

Specifies the name of the TCPIP Services SEZATCP data set. This data set is part of the z/OS Communications Server. This data set is typically program controlled and in the z/OS linklist (LNKLST).

Default: TCPIP.SEZATCP

LangEnvLinkEditorDSN

Specifies the name of the Language Environment linkage editor data set.

Default: CEE.SCEELKED

C370linkEditDSN

Specifies the data set name of the C/370 linkage editor data set.

Default: CEE.SCEESPC

LangEnvSPCdsn

Specifies the name of the C/C++ Language library functions data set.

Default: CEE.SCEESPC

CSSLibDSN

Specifies the name of the IBM Linkage Assist Library data set.

Default: SYS1.CSSLIB

SSLLIBRARY

Specifies the data set name of the System SSL library.

Default: SYS1.SIEALNKE

SysUtilitiesPath

Specifies the path to the z/OS UNIX utilities such as mount and unmount.

Default: /usr/sbin

CA CSM Installer Defaults

job.submission.mode

Specifies the method that the CA CSM installation script (installer / MSMSetup.sh) uses to submit jobs, check status, and validate return codes as part of the installation. The following values are valid:

FTP

Installation jobs are submitted using FTP. The prerequisite is JESINTERFACELEVEL 2.

TSO

Installation jobs are submitted using TSO. The CA CSM Installer runs in Manual installation mode only.

Default: FTP

Note: If your local FTP is Secure FTP or FTP Secure, the CA CSM installer does not support this feature. Specify job.submission.mode=TSO and run the CA CSM Installer.

JobStatusCheckPollPeriod

Specifies the period in seconds to poll the status of the jobs submitted during the installation and setup process for CA CSM.

Default: 2

JobCompletionWaitMaxTime

Specifies the time in seconds to wait for job completion before prompting the user whether to continue. This field enables you to cancel the process if the system is busy.

Default: 30

HTTP or HTTPS Configuration

msm.ssl.secure.connection.enable

You can configure CA CSM to use HTTP or HTTPS.

Y

Use HTTPS

N

Use HTTP.

Default: N

If you set msm.ssl.secure.connection.enable=Y, specify the following set of parameters to configure CA CSM to use HTTPS.

Note: All of these parameters are optional. The Installer prompts you for keystore password at installation time.

first.name.and.last.name

Specifies your URL domain name.

Example: www.your.domain

organization.name

Specifies your organization name.

organization.unit.name

Specifies your organization unit name.

city

Specifies your city name.

state

Specifies your state name.

country.code

Specifies your state name.

keystore.location

Specifies the location of the keystore. Specify your own value if you need to use a different USS location than the default location.

Default: Created in your RunTimeUSSPath

validity.period

Specifies the validity period for the generated keystore certificate, in days.

Default: 365

Migration

Note: This keyword only applies if you are an existing CA CSM user and are upgrading from a previous version of CA CSM.

PreviousRelease.MSMPATH

Specifies the path of the USS directory in which the previous version of CA CSM is installed. This path has folders, for example, CEGPHFS and CEGPJAR.

Refer to the MSMSummaryReport.txt or the options file available in the MSMSetup folder from a previous version of CA CSM.

Example: PreviousRelease.MSMPATH=/u/users/msmserv/msm

CA CSM Software Deployment Spawn Procedure Entities

The following entities are installed within the CA CSM software deployment procedure, which is a component-dependent function for CA Common Services for z/OS and CAIENF/CAICCI.

SMPCPATH

Specifies the path to the SMP/E Java application classes.

Preset: /usr/lpp/smp/classes/

SMPJHOME

Specifies the Java home directory.

Example: /sys/java31bt/v6r0mo/usr/lpp/java/J6.0/

Note: If your installation has a different Java home directory, use that directory name.

SMPDRIWK

This entity must be defined with the permissions of 775.

Preset: /cai/msm/ccispnsv/smpe

Note: The procedure is set to /cai/msm/ccispnsv/smpe, the user should tailor this to their company standard.

USS File Systems

This section provides more information about setting up your z/OS UNIX System Services (USS) and file systems.

USS Path Setup Details

CA CSM can use HFS or zFS file systems for its download, installation, setup, and general usage.

Note: We recommend using zFS file systems. For information about how to migrate from HFS file systems to zFS file systems, see the latest *IBM z/OS Migration* guide.

Before you download and install CA CSM, your USS administrator must set up directory paths and optionally configure file systems for these files. You can set up the paths in a single file system or multiple file systems, depending on the policy at your site.

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

Minimally, you require four directories with 775 permissions.

During operation, CA CSM dynamically creates and mounts additional file systems. File systems are mounted during startup (see page 178), and as a product and maintenance are downloaded.

For a zFS file system to grow dynamically, specify AGGRGROW when you mount the file system. For example:

```
MOUNT FILESYSTEM('yourHLQ.MSM.ZFS') -
     MOUNTPOINT('/parent_path/msmserv/version_number/msm')          -
     TYPE(ZFS)                                  -
     MODE(RDWR)                                 -
     PARM('AGGRGROW')
```

For more information, see the IBM *Distributed File Service zFS Administration*.

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*/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

***/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.

Note: For more information about how to set up USS paths for multiple versions of CA CSM, see the *Best Practices Guide*.

More information:

Options File Keywords (see page 157)

Single File System

We recommend that you set up your USS file system using a multiple file system structure. However, if you must structure your USS file system as a single file system, ensure that it contains all of the space that is required for the product installation and ongoing operations.

- 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.

- Define the following required directories so that the structure looks like the following:

  /parent_path/msmserv/mpm
  /parent_path/msmserv/*version_number*/msm
  /parent_path/msmserv/*version_number*/msmruntime
  /parent_path/msmserv/*version_number*/msminstall

- Update the UNIX BPXPRM*xx* control member with the single file system and mount point.
- After installation completes, delete the directory /*parent_path*/msmserv/*version_number*/msminstall and its contents.

CA CSM Installation and Setup

Before you execute the MSMSetup.sh utility, define a mount point for the installation of CA CSM. The mount point includes the following directories:

- The installation directory (for example, /u/users/msmserv/msminstall) that the MSMPATH keyword refers to in MSMSetupOptionsFile.properties
- The runtime directory (for example, /u/users/msmserv/msmruntime) that the RunTimeUSSPath keyword refers to in MSMSetupOptionsFile.properties

CA CSM Download

CA CSM is delivered as a pax file, which is downloaded and installed into a mounted file system or a directory (for example, /u/users/msmserv/msminstall). The name of the file is 51000068X01.pax.Z. When the file is expanded, new directories are created.

CA CSM Startup

This section describes the CA CSM startup process for both new and existing CA CSM installations.

At startup, CA CSM allocates and mounts file systems and USS directories. Before you execute MSMSetup.sh, define a mount point (for example, /u/users/msmserv/mpm) for the APLROOT file system. CA CSM allocates the file system and mounts it to this mount point.

Note: The MountPath keyword in MSMSetupOptionsFile.properties specifies the APLROOT directory. MSMSetup.sh populates the mpmPath parameter in the SAMPLIB(DBINIT) member with this value. The DBINIT member is used when CA CSM starts for the first time. On startup, the value is stored in the database. You can modify the value using the Application Root field on the Mount Point Management page on the Settings tab in the web-based interface.

Under the APLROOT file system, CA CSM creates four USS directories: sdsroot, scroot, ljroot, and tmproot. The USS directory ljwk is created under the ljroot directory.

The following list identifies the permanent file systems and their mount points:

- *hfs_prefix*.APLROOT mounted at *mountpath* (105,105 tracks)
- *hfs_prefix*.LJWK mounted at *mountpath*/ljroot/ljwk (2370,105 tracks)
- *hfs_prefix*.SDSROOT mounted at *mountpath*/sdsroot (105,105 tracks)

hfs_prefix

This prefix is specified by the MVSHFSDsnPrefix keyword in MSMSetupOptionsFile.properties. MSMSetup.sh populates the mpmHlq parameter in the SAMPLIB(DBINIT) member with this value. On startup, the value is stored in the database. You can modify it using the Data Set Prefix field on the Mount Point Management page on the Settings tab in the web-based interface.

The tmproot USS directory is used for allocating and mounting temporary file systems (see page 179) as required during CA CSM operation.

You can define whether CA CSM mounts file systems at startup. The Mount Point Management page on the Settings tab in the web-based interface has an Automount option. If the option is enabled, CA CSM looks for and mounts all the file systems that it manages. If the option is not enabled, you manage the mount points by updating the BPXPRM*xx* member in SYS*x*.PARMLIB.

Use of Temporary File Systems

In addition, CA CSM allocates temporary file systems as required during product acquisition, product installation, and other tasks. By default, CA CSM keeps a temporary file system for 60 minutes. After the file system has been idle for 60 minutes, CA CSM deallocates and releases it.

The names of the file systems have the following format: *hfs_prefix*.T*x*.

x

Is an internally generated number of up to seven characters.

CA CSM mounts temporary files at the following path:

```
mountpath/tmproot/MSM.unique_number.scratchpad
```

You can modify the time slot during which CA CSM keeps a file system allocated and mounted. In the SAMPLIB(MSMLIB) member, set the following parameter to the required number of minutes, and restart the CA CSM application server:

```
IJO="$IJO –DCSM_MPM.TEMPSPACE.MINIMUM.IDLE.MINUTES=60"
```

The minimum allowed value is 60. If you set the parameter to a value less than 60, CA CSM resets it back to 60.

If this parameter is set to 0, CA CSM allocates the temporary space during execution and deallocates it at termination.

Software Catalog

CA CSM allocates and mounts file systems for use by the software catalog as required. CA CSM mounts these file systems under *mountpath*/scroot.

The names of the file systems have the following format: *hfs_prefix*.*suffixn*.

suffix

Defines the last part of the file system name and is specified by the scDatasetPrefix parameter in the SAMPLIB(DBINIT) member.

n

Defines an internally generated counter of up to four characters.

More information:

CA CSM Startup (see page 178)

CA CSM Data Sets and File Systems

This section provides more information about the CA CSM data sets and file systems.

This section contains the following topics:

CA CSM Data Set Types (see page 181)

CA CSM File Systems (see page 182)

CA CSM Data Set Types

CA CSM has five groups of data sets. They are organized in the following types:

Application Root: *hlq*.APLROOT

This data set is used as the root USS file system that stores the directory structure for CA CSM.

Temporary Areas: *hlq*.T*x*

These data sets are temporary file systems that are used as temporary areas for CA CSM processing. These data sets are allocated during CA CSM operation as required and are deleted when no longer needed.

Log Journal: *hlq*.LJWK*x*

These data sets are used to store task output results, and their content appears in the Tasks tab for the finished tasks. To delete this content using CA CSM, use the Delete Task button on the Task tab.

Software Catalog: *hlq*.CASC*x*

These data sets store all the downloaded products and maintenance packages that can be viewed in the software catalog. A data set with a suffix CASC is usually configurable, with a default value of CASC. The data sets are removed after deployment is completed or deleted.

Note: In previous versions of CA CSM, the default software catalog data set had the suffix MSMT.

Deployment Temporary Area: *hlq*.SDSROOT

This data set is a temporary file system that is used as a temporary area for CA CSM deployment processing. CA CSM deletes the content of this file system after the data is no longer needed. If any content remains there after CA CSM shuts down, you can manually delete the content from the appropriate USS directories without affecting CA CSM.

Deployment: *hlq*.D*x*

These data sets are used for deployment processing and contain deployment data. To remove this content using CA CSM, select Remove from the Action drop-down list on the Deployment tab.

Important! Do not delete these data sets or the content from these data sets manually outside of CA CSM. Manually deleting data sets causes missing task output or CA CSM to fail.

CA CSM File Systems

The following table lists the file systems that CA CSM allocates and uses. The following terms are used in the table:

mpm

Specifies the UNIX path to the application root. mpm specifies the mount point directory for the file systems. An initial mount point is configured during the CA CSM installation.

hlq

Specifies the HLQ for the data set names that are created for new file systems that CA CSM allocates.

Data Set Name (DSN)

Specifies the DSN of the file system that is mounted to this directory, or of the file system that contains this directory if no file system is mounted to this directory.

Typical Size

Specifies the typical size of the file system. The value is specified only for paths that have a file system mounted to them.

Path	Data Set Name	Data Set Mounted to Path	Type	Purpose	Typical Size
mpm	*hlq*.APLROOT	Yes	Application root	The main mount point directory for CA CSM. This directory resides in the *hlq*.APLROOT data set.	14400 KB
mpm/ljroot	*hlq*.APLROOT	No	Log journal root	The root directory for the log journal (task output).	N/A
mpm/scroot	*hlq*.APLROOT	No	Software catalog root	The root directory for the software catalog (stored products and maintenance packages).	N/A
mpm/sdsroot	*hlq*.SDSROOT	Yes	Deployment root	The root directory for deployment packages.	158400 KB
mpm/ljroot/ljwk	*hlq*.LJWK	Yes	Log journal	This directory resides in the *hlq*.LJWK data set.	137760 KB
mpm/scroot/tmp	*hlq*.APLROOT	No	Software catalog	The directory that contains Software catalog temporary directories.	N/A

Path	Data Set Name	Data Set Mounted to Path	Type	Purpose	Typical Size
mpm/scroot/tmp/tmp*x*	*hlq*.CASCn	Yes	Software catalog	The Software catalog temporary directory.	400000 KB
mpm/scroot/DatabaseM	*hlq*.APLROOT	No	Software catalog	The directory that contains the Software catalog database.	N/A
mpm/scroot/DatabaseM/CA	*hlq*.APLROOT	No	Software catalog	The CA Technologies vendor directory that contains all downloads for a vendor.	N/A
mpm/scroot/DatabaseM/CA/error_hold_data	*hlq*.APLROOT	No	Software catalog	The directory that contains the ALL-HOLDDATA.txt file. This file contains HOLDDATA for all CA Technologies products.	N/A
mpm/scroot/DatabaseM/CA/COMMONS	*hlq*.APLROOT	No	Software catalog	The directory that contains the installation for CA Common Services.	N/A
mpm/scroot/DatabaseM/cars	*hlq*.CASCn	Yes	Software catalog	The directory that contains CA RS files.	4800 KB
mpm/scroot/DatabaseM/CA/MAINTENANCE	*hlq*.CASCn	Yes	Software catalog	The directory that contains all maintenance packages	4800 KB
mpm/scroot/DatabaseM/CA/*product_name*	*hlq*.CASCn	Yes	Software catalog	The product directory for a specific product.	4800 KB
mpm/scroot/DatabaseM/CA/*product_name*/*release*/*servicepack*/*packagename*/*date*	*hlq*.CASCn	Yes	Software catalog	The directory for a specific product package that does not fit into the product directory.	4800 KB
mpm/sdsroot/*deployment_ID*	*hlq*.Dn	Yes	Software Deployment Service (SDS)	The directory that contains data stored for deployment with ID *deployment_ID*. This directory resides in the *hlq.deployment_ID* data set.	21024 KB
mpm/tmproot	*hlq*.APLROOT	Yes	Temporary area	The directory contains temporary mount points for temporary file systems.	N/A

Path	Data Set Name	Data Set Mounted to Path	Type	Purpose	Typical Size
mpm/tmproot/MSM.*n*.scraptchpad	*hlq*.T*n*	Yes	Temporary area	The directory serves as a mount point for a temporary file system that CA CSM allocates as required during product acquisition, product installation, and other tasks.	57408 KB

CA Common Services Component Requirements

CA Common Services is an open, cross-platform enterprise management infrastructure available on many operating system platforms, including z/OS. The infrastructure provides common services and enabling technology for CA Technologies IT management solutions.

CA Common Services for z/OS

CA Common Services for z/OS (CCS) includes distributed services common to CA Technologies implementations and solutions specific to z/OS. CCS provides a common interface and event services to create multiple, unified resource views.

This z/OS hosted enterprise management architecture expands the choice of what and where to manage, similar to how CCS works on Windows and UNIX platforms. CCS also contains the essential components and functionality to enable integrated management of z/OS.

CCS includes support for applications that are based on z/OS UNIX System Services. CCS also furnishes the Agent Technology infrastructure to run z/OS Agents.

CA Common Services for z/OS let you:

- Integrate your mainframe with other distributed platforms.
- Manage emerging z/OS workloads such as web servers, Java applications, and UNIX applications.
- Use existing CA Technologies z/OS management solutions to create events that can be routed to other enterprise platforms where such events can create desired business outcomes.
- Achieve enterprise-wide, automated, high-level monitoring and management of critical resources using sophisticated manager and agent technology, together with CA Technologies products.

Note: For more information about CA Common Services for z/OS, see the CA Common Services for z/OS user documentation.

Software Services

CA Common Services for z/OS Software Services provide CA CSM with a number of software components that perform various functions.

CAICCI

CAICCI provides CA enterprise applications with a common communications software layer. This layer insulates the applications from dealing with protocol specifics, error recovery, and system connection establishment.

CAIENF (Base)

CAIENF (Base) is a software component that provides comprehensive operating system interfacing services to any of the CA Technologies z/OS applications, exploiting technologies for the benefit of the entire product line. The level of integration is improved by enabling operating systems and CA Technologies software generated event information to be driven through a standard interface. This simplifies multiple product-to-product interfaces and associated maintenance that would otherwise be necessary.

CAIRIM

CAIRIM is a software component that prepares your operating system environment for all CA applications and starts them. It is the common driver for a collection of dynamic initialization routines that eliminate the need for user SVCs, SMF exits, subsystems, and other installation requirements commonly encountered when installing systems applications.

Two integral parts of CAIRIM are CAISSF and CA LMP.

CAISSF

Provides an external security mechanism for controlling and monitoring access to all system and application resource processes. CAISSF is integrated into many CA enterprise applications and is also used by other CA Common Services for z/OS services. It provides security services for user signin, resource access control, process use control, and recording and monitoring of violation activity.

CA LMP

Provides a standardized and automated approach to the tracking of licensed software.

CA-C Runtime

CA-C Runtime is a support services component providing a C run-time facility that insulates programs from system and release dependencies.

FMIDs

CA CSM requires CA Common Services for z/OS r12 or Version 14.0 and above components to perform various functions. The function modification identifiers (FMIDs) are provided for these components.

The FMIDs in the following table are based on CA Common Services for z/OS r12:

FMID	Component
CAF3C00	CA-C Runtime
CAS9C00	CAIRIM
CAW1C00	CAIENF
CAW4C00	CAICCI with SSL

The FMIDs in the following table are based on CA Common Services for z/OS Version 14.0 and above:

FMID	Component
CAF3E00	CA-C Runtime
CAS9E00	CAIRIM
CAW1E00	CAIENF
CAW4E00	CAICCI with SSL

The FMID in the following table is based on CA Common Services for z/OS r12 and Version 14.0 and above. This is a CA Common Services for z/OS dependent function that is only used for SDS and SCS.

FMID	Component
CETN500	MSM Common Services, which uses CAICCI

Note: For information about setup and configuration steps that must be completed, see the *CA Common Services for z/OS Installation Guide.*

Set Up CAICCI

Use this procedure if you have not set up CAICCI at all. For more information, see the *CA Common Services for z/OS Installation Guide*.

Follow these steps:

1. Define the CAICCI SYSID, either in the CAIENF parameter file or as a separate CCIPARM PDS member concatenated to ENFPARMS, using the following format:

   `SYSID(sysid)`

   sysid

   Specifies the CAICCI identifier.

   Limit: Eight characters

2. Define the CAICCI data collection module (DCM), CAS9DCM3, in your CAIENF parameter file. For example:

   ```
   DCM(CAS9DCM3)          * ENF V1.0 CCI Event
   ```

Security for CA CSM Functions

Many of the resources and activities that CA CSM provides are protected by security profiles that are defined to your external security manager (ESM). When you attempt to perform an action in the web-based interface (for example, logging in or changing a setting), CA CSM invokes the System Authorization Facility (SAF) with the associated resource profile. CA CSM resource profiles (see page 189) are defined in the CA CSM resource class. The resource profiles enable your site to assign authorities to various resources and actions to specific users or to provide generic access with few settings.

Resource Names

CA CSM does not use the distinctions of READ, UPDATE, CONTROL, and ALTER for access to resources. Instead, access is encoded into the resource name. If you have access to a resource, you can perform the specified action on the resource.

The granted authority level is immaterial. Access to the resource is managed in a binary manner: either you can access the resource (any combinations of READ, UPDATE, CONTROL, or ALTER), or you cannot access the resource. For example, the following resource profiles control access to the system settings on the Settings tab:

ADMIN.SETTINGS.SYSTEM

Enables a user to display and update the system settings.

ADMIN.SETTINGS.SYSTEM.@DISPLAY

Enables a user to display the system settings.

ADMIN.SETTINGS.SYSTEM.@UPDATE

Enables a user to update the system settings.

For resources that have both an @DISPLAY and an @UPDATE profile, granting access to only the @UPDATE profile is an error. Because you have no authority to display the value, you cannot change the value, even though that level of access is granted.

Because all the system settings are organized under ADMIN.SETTINGS.SYSTEM, you can give access to all system settings by granting one or more users to the ADMIN.SETTINGS.SYSTEM profile. These users would be taking on the administration role for CA CSM.

User settings are organized under ADMIN.SETTINGS.USER. The settings are maintained separately in CA CSM for each user. Access to display or update a resource is managed through the @SELF qualifier in the resource profile. For example, authorizing the user IDs, USER01 and USER02, to the ADMIN.SETTINGS.USER.@SELF.@DISPLAY and ADMIN.SETTINGS.USER.@SELF.@UPDATE profiles enable the users to update their own web-based interface settings. However, USER01 cannot display or update the settings for USER02. We recommend that you grant permission to ADMIN.SETTINGS.USER.@SELF to all CA CSM users.

Resource Profiles

You can secure certain parts of CA CSM by granting or denying access using security rules, which are named *resource profiles*. Create these resource profiles in their associated security package using resource class CAMSM.

Important! If you grant a user permission to a *.@UPDATE resource profile, you must also grant that user permission to the corresponding *.@DISPLAY resource profile.

LOGON

Grants access to CA CSM.

ADMIN.SETTINGS

Grants full access to all settings on the Settings tab.

ADMIN.SETTINGS.SYSTEM

Grants full access to all system settings.

ADMIN.SETTINGS.SYSTEM.@DISPLAY

Grants DISPLAY authority to all system settings.

ADMIN.SETTINGS.SYSTEM.@UPDATE

Grants UPDATE authority to all system settings.

ADMIN.SETTINGS.USER.@SELF

Grants full access to a user's own settings, including the user's account on the CA Support Online website.

ADMIN.SETTINGS.USER.@SELF.@DISPLAY

Grants DISPLAY authority to a user's own settings, including the user's account on the CA Support Online website.

ADMIN.SETTINGS.USER.@SELF.@UPDATE

Grants UPDATE authority to a user's own settings, including the user's account on the CA Support Online website.

ADMIN.LMPKEY

Grants full access to the resources on the LMP Keys Browser page.

ADMIN.LMPKEY.UPDTKEYS

Grants access to Update Keys on the LMP Keys Browser page.

ADMIN.LMPKEY.REFRSITE

Grants access to Refresh Site IDs on the LMP Keys Browser page.

CONFIG

Grants full access to the resources on the Configurations tab.

CONFIG.@DISPLAY

Grants display only access to the resources related to SCS.

CONFIG.@ACTION.CREATE

Grants full access to create or update the resources related to SCS.

CONFIG.@ACTION.REMOVE

Grants full access to the resources on the Deployments tab.

CONFIG.@ACTION.IMPL

Grants access to implement configurations on remote systems.

DEPLOY

Grants full access to the resources on the Deployment tab.

DEPLOY.@DISPLAY

Grants read-only authority to information provided on the Deployments tab.

DEPLOY.@SELF

Grants authority to create deployments, assign systems and custom data sets as well as all actions for the deployment if your CA CSM user ID is marked as the owner of that deployment.

DEPLOY.@BUILD

Grants authority to create and update deployments, assign systems and custom data sets as well as previewing the deployment.

DEPLOY.@EXECUTE

Grants authority to perform a snapshot, transmit, deploy, and confirm a deployment.

METHOD

Grants full access to all methodologies.

METHOD.@DISPLAY

Grants read access to all methodologies.

METHOD.@SELF

Grants full access to only those methodologies where you are listed as the owner.

METHOD.@UPDATE

Grants access to create, edit, and remove methodologies from within the Maintain Methodologies page. It also controls the availability of the Edit button next to the methodology within the deployment view.

SC

Grants full access to the resources on the Products tab.

SC.@ACTION

Grants full access to the actions on the Products tab.

SC.@ACTION.UPDTCAT

Grants access to all Update Catalog actions on the Products tab.

SC.@ACTION.SHOWLMP

Grants access to the Show License Keys action in the Actions section on the Products tab.

SC.@ACTION.INSRTPRD

Grants access to the Add Product action in the Actions section on the Products tab.

SC.@ACTION.INSTPKG

Grants access to the Install External Package action in the Actions section on the Products tab.

SC.@HIDE

Grants access to the Hide Product action in the Products tree and to the Show Products button on the Show Hidden Products dialog on the Products tab.

SIS.BASE.@SELF.WORKDD.@UPDATE

Grants access to the action to update work DDDEF settings during product installation.

SMPE.@ACTION

Grants full access to the actions on the SMP/E Environments tab.

SMPE.@ACTION.MIGRATE

Grants access to the action to migrate an SMP/E environment.

SMPE.@ACTION.REMOVECSI.*csidatasetname*

Grants access to Remove SMP/E Environment from CA CSM on the SMP/E Environments, SMP/E Environment Information tab. The permission is for the specified SMP/E environment.

.csidatasetname

Specifies the data set names of the SMP/E environments that the user can remove.

The value can be a full name that matches one SMP/E environment or a prefix that can match multiple SMP/E environment data set names.

SYSREG

Grants full access to the resources on the System Registry tab.

SYSREG.@DISPLAY

Grants display authority to all System Registry values.

Note: Users defined with this access are not allowed to create, delete or update any information on any of the panels.

SYSREG.@ACTION

Grants full access to the actions on the System Registry tab.

SYSREG.@ACTION.CREATE

Grants access to the Create Non-Sysplex System link, the Create Sysplex link, the Create Shared DASD Cluster link and the Create Staging System link. It also enables the Create button from within the display for each primary node of the System Registry tree as well as the Create button within Data Destinations. Create authority also implies Update authority.

SYSREG.@ACTION.REMOVE

Grants access to the Select check box and the Remove item from within the Actions button from within each primary node of the System Registry tree.

Note: If the user does not have this authority, these items are disabled.

SYSREG.@PROFILE

Grants full access to the profile information within each primary node of the system registry. Profile Information is applicable to those CA CSM users within your organization that create or implement configurations. If this access is not granted, the system profile information will not be displayed within the web-based user interface.

Note: Implementations can result in changes on the remote system that, if done incorrectly, could adversely affect the stability of that system. We recommend that you restrict authorization to this profile.

SYSREG.@PROFILE.DISPLAY

From within each system node of the system registry, a user with this access does not have authority to modify any values within a profile. These items are displayed but all Action buttons are disabled.

SYSREG.@PROFILE.UPDATE

From within each system node of the system registry, grants access to create an occurrence of a profile or update any existing values within a profile. If the system registry is secured with the resource rule SYSREG@PROFILE.DISPLAY, this access rule is required to allow updating of any profile information.

SYSREG.@SYSTEM

Grants full access to all systems defined within the System Registry tab.

SYSREG.@SYSTEM.*systemname*

Grants access to the “system name” within the System Registry tab. If a system is created within a CA CSM session and specific system level security is desired, the security administrator must grant access to the newly defined system before it will become visible to the CA CSM user. Security at this level simply controls which defined systems are available to the user. The ability to update or delete information with the defined system is permitted using the SYSREG.@ACTION.CREATE, SYSREG.@ACTION.REMOVE, and SYSREG.@PROFILE.UPDATE resources.

TM.TASK.ARCHIVE

Grants access to Manage History functionality within the Task tab and allows authorized users to create, run, or delete task archive policies.

TM.TASK.@SELF.DELETE

Grants access to delete user's own tasks.

TM.TASK.SYSTEM.DELETE

Grants access to delete any tasks.

SAF Check During SMP/E Processing

All CA CSM features that execute SMP/E commands do it in the security context of the user that is logged in to CA CSM and drives these features. Depending on the CA CSM feature, users must have READ access to different sets of SMP/E SAF facility class resources.

Note: CA CSM executes GIMUNZIP in the security context of the CA CSM application server ID. If SMP/E security is active, the CA CSM application server ID must have READ access to the GIM.PGM.GIMUNZIP resource in the SAF FACILITY class.

SMP/E Environment Migration

If new DDDEFs are added to a migrated SMP/E environment using customer-provided JCL, you must have READ access to the following SMP/E SAF facility class resources:

- GIM.CMD.SET
- GIM.CMD.UCLIN

Base Product Installation

To install products, you must have READ access to the following SMP/E SAF facility class resources:

- GIM.PGM.GIMUNZIP
- GIM.CMD.SET
- GIM.CMD.UCLIN
- GIM.CMD.RECEIVE
- GIM.CMD.APPLY
- GIM.CMD.ACCEPT

If an error occurs when installing a product to an existing SMP/E environment, CA CSM performs UNDO operations to restore the SMP/E environment to its state before starting the installation.

Depending on the level of UNDO operations that CA CSM performs, you must have READ access to the following SMP/E SAF facility class resources:

- GIM.CMD.SET
- GIM.CMD.UCLIN
- GIM.CMD.RESTORE
- GIM.CMD.REJECT

Maintenance Management

You must have READ access to the GIM.CMD.SET SAF facility class resource to manage maintenance.

Other requirements depend on a particular maintenance operation:

- To install maintenance, you must have READ access at least to the following SMP/E SAF facility class resources:
  - GIM.CMD.RECEIVE
  - GIM.CMD.APPLY
- To accept maintenance, you must also have READ access to the GIM.CMD.ACCEPT SAF facility class resource.

- To perform elementary SMP/E commands on one or more maintenance packages, you must have READ access to the following corresponding SAF facility class resources:
  - GIM.CMD.RECEIVE (for RECEIVE operation)
  - GIM.CMD.APPLY (for APPLY operation)
  - GIM.CMD.ACCEPT (for ACCEPT operation)
  - GIM.CMD.RESTORE (for RESTORE operation)
  - GIM.CMD.REJECT (for REJECT operation)

Deployment

SDS relies on the SMP/E GIMZIP program. If you perform a deployment operation, you must have READ access to the GIM.PGM.GIMZIP SAF facility class resource on the CA CSM driving system. Also, you must have READ access to the GIM.PGM.GIMUNZIP SAF facility class resource on the CA CSM remote system.

DBINIT and DBUPDATE Settings

The DBINIT member, *RunTimeMVSHLQPrefix*.SAMPLIB(DBINIT), is used when CA CSM starts for the first time. The CA CSM installer sets the content of this member.

Important! Change the member content only when CA Support requests it. The values set for some keywords may vary between the CA CSM Setup Options file and *RunTimeMVSHLQPrefix*.SAMPLIB(DBINIT) member. Therefore, it is important that you closely follow the instructions from CA Support.

The DBINIT member is allocated to DBINIT DD of the CA CSM startup JCL (*RunTimeMVSHLQPrefix*.JCL(MSMTCSRV)). The DBINIT member is used only when CA CSM is run for the first time.

At startup, values from the DBINIT member are stored in the database. Some of the values can be set only once. You cannot change them, or changing the values does not have any effect. You can modify the other values later using the web-based CA CSM interface.

To modify the values that cannot be modified using the web-based interface, you can use the DBUPDATE DD (see page 202). The DBUPDATE DD is processed during CA CSM startup.

Important! Update these values only when CA Support requests it. Otherwise, you may cause data inconsistency.

The contents of DBINIT and DBUPDATE are records that can be either comments starting with # or value settings in the following format:

setting=value

The values are not verified during DBINIT or DBUPDATE processing.

The following settings are available for the Mount Point Manager:

mpmPath

Defines the path to the USS directory that CA CSM uses for work files. This directory must be available when you execute the setup utility.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the Application Root field.

Note: Changing this value does not copy existing data to the new path. Ensure that the new path is valid.

mpmHlq

Defines a prefix that is used for file system allocation.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the Data Set Prefix field.

Limits: 40 characters

Note: If you change this setting, it will be used for newly allocated data sets only.

mpmStorclas

Defines the SMS storage class on the Mount Point Management page of the Settings tab.

The value can be blank.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the Storage Class field.

Note: If you change this setting, it will be used for newly allocated data sets only.

mpmVolser

Defines the volume serial number of the corresponding DASD on the Mount Point Management page of the Settings tab.

The value can be blank. If defined, mpmVolser must be the volume serial number of an online volume.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the VOLSER field.

Note: If you change this setting, it will be used for newly allocated data sets only.

mpmFilesystemType

Specifies the file system type that is used for file system allocation.

Options include:

- HFS
- zFS

Note: We recommend using zFS file systems.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page.

Note: If you change this setting, it will be used for newly allocated data sets only. Existing data sets remain intact.

mpmAutomount

Specifies whether CA CSM mounts all file systems during startup.

Options include:

- true
- false

This value can be changed in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, the Automount check box.

mpmunit

Specifies the type of the DASD on which to place data sets on the Mount Point Management page of the Settings tab.

This value can be changed in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the Unit field.

Note: If you change this setting, it will be used for newly allocated data sets only.

mpmDataClas

Specifies the SMS data class for file system data sets on the Mount Point Management page of the Settings tab.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the Data Class field.

Note: If you change this setting, it will be used for newly allocated data sets only.

mpmMgmtClas

Specifies the SMS management class for file system data sets on the Mount Point Management page of the Settings tab.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the Storage Class field.

Note: If you change this setting, it will be used for newly allocated data sets only.

mpmAllocation

Specifies whether to use SMS when allocating new data sets for file systems on the Mount Point Management page of the Settings tab.

Options include:

- SMS
- NONSMS

If mpmStorclas is defined, mpmAllocation is treated as SMS. Otherwise, it is treated as NONSMS.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the Use SMS or Use Non-SMS fields.

Note: If you change this setting, it will be used for newly allocated data sets only.

The following settings are available for the Software Catalog:

scDatasetPrefix

Specifies a suffix for the data set name, which also has an internally generated counter.

The name has the following format:

`mpmHlq.scDatasetPrefix`*n*

You can change this value in the web-based interface using the Settings tab, on the System Settings, Software Catalog page, in the Data Set Suffix field.

Note: If you change this setting, it will be used for newly allocated data sets only.

scRoot

Defines the root directory of the Software Catalog database where packages from the CA Support Online website are stored on a customer site. The directory is relative to the CA CSM application root, mpmPath.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Software Catalog page, in the Root Directory field.

Note: Ensure that the new path points to a valid Software Catalog root.

scPrimBig

Specifies the default value for primary quantity for data sets implicitly mounted at the product or release level in the USS database.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Software Catalog page, in the Primary Quantity field.

scSecBig

Specifies the default value for secondary quantity for data sets implicitly mounted at the product or release level in the USS database.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Software Catalog page, in the Secondary Quantity field.

The following settings are available for CA DSI Server:

dsiHost

Specifies the host name for CA DSI Server that CA CSM uses internally to provide security features.

This value cannot be changed in the web-based interface, but can be modified using DBUPDATE.

dsiPort

Specifies the port number for CA DSI Server that CA CSM uses internally to provide security features.

This value cannot be changed in the web-based interface, but can be modified using DBUPDATE.

dsiConf

Specifies the path of the CA DSI Server configuration file.

This value cannot be changed in the web-based interface, but can be modified using DBUPDATE.

The following settings are available for the Software Installation Service:

sisGimunzipTempPrefix

Defines the prefix that CA CSM uses to allocate GIMUNZIP output temporary data sets during product installation and maintenance. The name of the resulting data set is *prefix*.*jobname*.*unpacked_file_name*. The created temporary work files are not SMP/E controlled data sets. CA CSM deletes them through the product installation process. These files are used as input relative files for SMP/E processing during the receiving of a product into the SMP/E environment global zone.

You can change this value in the web-based interface using the Settings tab, on the Software Installation page, in the GIMUNZIP Temporary Prefix field (for both System Settings and User Settings).

Limits: 12 through 19 characters (depending on the number of characters used for *jobname*)

Note: If you use the default 6-character *jobname*, you can enter up to 14 characters for the GIMUNZIP temporary prefix.

sisExecutorServerDsnPrefix

Defines the prefix for temporary data sets used by executed programs.

The name of a temporary data set has the following format: *prefix*.R*n*.*ddname* (*n* is the execution request number).

You can change this value in the web-based interface using the Settings tab, on the Software Installation page, in the Temporary Data Set Prefix field (for both System Settings and User Settings).

Default: *userid*.CAMSM.*jobname*

Limits: 24 characters

sisGimunzipTempVolser

Specifies the volume serial number of the DASD to use for the temporary data sets created by GIMUNZIP during installation.

You can change this value in the web-based interface using the Settings tab, on the Software Installation page, in the GIMUNZIP Temporary VOLSER field (for both System Settings and User Settings).

Limits: 1-6 alphanumeric characters or an asterisk (*). If an asterisk is specified, SMS assigns a volume for a new VSAM data set if the automatic class selection (ACS) routines allow it.

sisExecutorOutputStorclas

Specifies the SMS storage class for the data sets that executed programs use for temporary data.

You can change this value in the web-based interface using the Settings tab, on the Software Installation page, in the Storage Class field (for both System Settings and User Settings).

sisExecutorOutputVolser

Specifies the volume serial number of the DASD to use for the data sets that executed programs use for temporary data.

You can change this value in the web-based interface using the Settings tab, on the Software Installation page, in the VOLSER field (for both System Settings and User Settings).

Limits: 1-6 alphanumeric characters

sisExecutorOutputUnit

Specifies the type of the DASD on which to place the data sets that executed programs use for temporary data.

You can change this value in the web-based interface using the Settings tab, on the Software Installation page, in the Unit field (for both System Settings and User Settings).

The following settings are available for the PAS component keys:

PASAdvancedSettingsPDS

Defines the data set where the member containing a sample of FTP proxy advanced settings is located.

Default: *RunTimeMVSHLQPrefix*.SAMPLIB

RunTimeMVSHLQPrefix

Specifies the prefix for CA CSM runtime data sets, which are runtime copies of the target data sets.

This value cannot be changed in the web-based interface, but can be modified using DBUPDATE.

PASAdvancedSettingsMember

Defines the member that contains a sample of FTP proxy advanced settings where you can configure both FTP and HTTP advanced proxy settings.

Default: PASADVOP

This value cannot be changed in the web-based interface, but can be modified using DBUPDATE.

The following setting is available for the Task Management:

sysTaskDeleteOverrideEnabled

Lets all CA CSM users delete completed tasks when the security feature in CA CSM is disabled.

true

Any user can delete any competed task.

false

Users cannot delete completed tasks.

Note: If the security feature is enabled in CA CSM, the task deletion is managed by security resources (see page 189), and the parameter is ignored.

Default: None.

This value cannot be changed in the web-based interface, but can be modified using DBUPDATE.

Modify Values Using the DBUPDATE DD

To modify entry values in the CA CSM database using the DBUPDATE DD, add the DBUPDATE DD to the CA CSM startup JCL (*RunTimeMVSHLQPrefix*.JCL(MSMTCSRV)).

Follow these steps:

1. Create a *RunTimeMVSHLQPrefix*.SAMPLIB(DBUPDATE) member.
2. Add only the settings (see page 195) and their values in the *RunTimeMVSHLQPrefix*.SAMPLIB(DBUPDATE) member that you want to modify.
3. Add the DBUPDATE DD pointing to the *RunTimeMVSHLQPrefix*.SAMPLIB(DBUPDATE) member to the CA CSM startup JCL (*RunTimeMVSHLQPrefix*.JCL(MSMTCSRV)).
4. Restart the CA CSM application server.
5. Comment out the DBUPDATE DD in the *RunTimeMVSHLQPrefix*.JCL(MSMTCSRV).

ASCII Configuration Files

All files in the tomcat/conf folder and all configuration files in tomcat/webapps/MSM folder are stored in ASCII. Therefore, you cannot edit these files in the standard way. This section describes some of the ASCII files and how to edit them.

Edit an ASCII File

Some text files are stored on USS in ASCII. If you attempt to open the file as EBCDIC, it may appear to be binary.

The ASCII requirement is due to Java, which only runs in ASCII. USS (OMVS) can run code that is ASCII and EBCDIC.

Note: OEDIT and ISHELL are for EBCDIC and cannot be used to edit ASCII files.

You can edit a file in ASCII mode using one of the following methods:

- Use a third-party utility that allows direct editing of ASCII files from USS.
- Edit the ASCII file locally with a text editor:
  1. Download the file to your computer using FTP in binary mode, so that the encoding is not changed during the transfer.
  2. Edit the file on your computer with a text editor.
  3. Upload the file back in binary using FTP.

- Edit the ASCII file with the ISPF UI Tool within USS:

  1. Select UTILITIES from the ISPF primary option menu.

     The Utility Selection Panel opens.

  2. Select Udlist.

     The z/OS UNIX Directory List Utility opens.

  3. Type the pathname, then use normal USS commands to step down the path to the required directory.

  4. Make yourself a superuser and enter the EA command on the appropriate file.

The file is in a readable form, and you can update it.

context.xml Parameters

You can edit values in the context.xml file. The context.xml file is an ASCII file and you must use special handling when editing this file. (see page 202)

Important! If you change the value for ServerName, you must also change the corresponding value in the SAMPLIB(SRVLIB) member. In the SAMPLIB(SRVLIB) member, the ServerName value corresponds to SERVERNAME.

If you change the value for ApplicationID, you must also change the corresponding value in the SAMPLIB(SRVLIB) member and in the SAMPLIB(SRVSLIB) member. In both the SAMPLIB(SRVLIB) member and the SAMPLIB(SRVSLIB) member, the ApplicationID value corresponds to APPLID.

The following is a sample from context.xml:

```
url="jdbc:datacom:/ServerName=SRVMUF,SystemID=A31SENF, ApplicationID=SRVMUF,
HostPort=1202,ConnectType=CCI, HostName=AA01,UserID=SWMGRQA"
```

The URL string consists of the following parameters:

ServerName

Defines the CA Datacom/MSM server used by the CA CSM application server.

SystemID

Defines the CA-ENF CAICCI SYSID on the system used by the CA CSM application server.

ApplicationID

Defines the CA Datacom/MSM server name.

HostPort

Defines the CA CCITCP or CCISSL port number configured on your system, for example, 1202.

ConnectType

Defines the type of connection between the CA CSM application server (see page 229) and the CA Datacom/MSM server. ConnectType is always CCI.

HostName

Defines the name or IP address of the host system on your system.

UserID

Defines the user ID used by CA CSM to access the database.

Job Allocation Details

This section provides details about the z/OS and USS files and folders that are created after CA CSM is installed.

The following jobs are submitted based upon whether you are performing a CA CSM installation or an upgrade. The job name has the format CSM*axxyy*.

a

Indicates a new installation (N) or an upgrade (U).

xx

Indicates the version number that you are upgrading from or has a value of 51 for a new installation.

yy

Indicates the sequence number of the job.

This section contains the following topics:

- CSMaxx02 (see page 205) (new installation and upgrade)
- CSMaxx06 (see page 207) (new installation and upgrade)
- CSMaxx09 (see page 208) (new installation and upgrade)
- CSMUxx01 (see page 209) (upgrade only)

CSMaxx02

The following table lists the data sets and USS files that are created when this job runs.

Note: The total primary quantity of cylinders is 922 of 3390 DASD space.

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<CSIHLQ>.SMPCSI.CSI	NA	NA	NA	VSAM KSDS	NA	NA	NA
<CSIHLQ>.SMPCSI.CSI.DATA	CYLS	15		VSAM KSDS	NA	NA	NA
<CSIHLQ>.SMPCSI.CSI.INDEX	CYLS	5		VSAM KSDS	NA	NA	NA
<CSIHLQ>.SMPLOG	CYLS	6	5	PS	VB	510	6233
<CSIHLQ>.SMPLOGA	CYLS	6	5	PS	VB	510	6233
<CSIHLQ>.SMPLTS	CYLS	6	5	PO	U	0	6144
<CSIHLQ>.SMPMTS	CYLS	6	5	PO	FB	80	3120
<CSIHLQ>.SMPPTS	CYLS	102	100	PO	FB	80	27920
<CSIHLQ>.SMPSCDS	CYLS	10	5	PO	FB	80	3120
<CSIHLQ>.SMPSTS	CYLS	6	5	PO	FB	80	3120
<DatabaseHLQ>.MSM.ADCXX.BKP	CYLS	5	1	PS	VB	4088	4096
<DatabaseHLQ>.MSM.DB002.BKP	CYLS	10	2	PS	VB	20480	27998
<DatabaseHLQ>.MSM.DB015.BKP	CYLS	4	2	PS	VB	20480	27998
<DatabaseHLQ>.MSM.JNL4000.BKP	CYLS	4	2	PS	VB	20480	27998
<DatabaseHLQ>.MSM.PCY4000.BKP	CYLS	4	2	PS	VB	20480	27998
<DatabaseHLQ>.MSM.SRG4000.BKP	CYLS	4	2	PS	VB	20480	27998
<DlibHLQ>.AAAXDATV	CYLS	88	1	PO	VB	31996	32000
<DlibHLQ>.AAAXHFS	CYLS	3	1	PO	VB	1028	6144
<DlibHLQ>.AAAXMAC	CYLS	15	1	PO	FB	80	32720
<DlibHLQ>.AAAXMOD0	CYLS	45	1	PO	U	0	6144
<DlibHLQ>.AAAXSAMP	CYLS	26	1	PO	FB	80	32720
<DlibHLQ>.AABDXML	CYLS	5	1	PO	VB	512	32760
<DlibHLQ>.AEG1JAR	CYLS	10	2	PO-E	VB	1028	6144

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<DlibHLQ>.AEG1SHSC	CYLS	1	1	PO-E	VB	255	27998
<DlibHLQ>.AEGPHFS	CYLS	35	10	PO-E	VB	1028	6144
<DlibHLQ>.AEGPJAR	CYLS	127	10	PO-E	VB	1028	6144
<DlibHLQ>.AEGPJCL	CYLS	2	1	PO-E	FB	80	32720
<DlibHLQ>.AEGPPROC	CYLS	1	1	PO-E	FB	80	32720
<DlibHLQ>.AEGPSAMP	CYLS	1	1	PO-E	FB	80	32720
<MSMPATH>/CEG1JAR	NA						
<MSMPATH>/CEG1SHSC	NA						
<MSMPATH>/CEGPHFS	NA						
<MSMPATH>/CEGPJAR	NA						
<MSMPATH>/datacom/dbsrv	NA						
<MSMPATH>/dsi	NA						
<RunTimeMVSHLQPrefix>.CAAXLOAD	CYLS	50	5	PO	U	0	27998
<RunTimeMVSHLQPrefix>.CAAXLOAD.BO1	CYLS	50	5	PO	U	0	27998
<RunTimeMVSHLQPrefix>.CAAXLOAD.BO2	CYLS	50	5	PO	U	0	27998
<RunTimeMVSHLQPrefix>.CAAXMAC	TRKS	227	15	PO	FB	80	32720
<RunTimeMVSHLQPrefix>.CAAXSAMP	CYLS	26	1	PO	FB	80	32720
<RunTimeMVSHLQPrefix>.CUSLIB	CYLS	8	1	PO	U	0	6144
<RunTimeMVSHLQPrefix>.CUSMAC	TRKS	37	15	PO	FB	80	3120
<RunTimeMVSHLQPrefix>.DEPLOYIN	TRKS	2	1	PS	FB	80	27920
<RunTimeMVSHLQPrefix>.JCL	TRKS	20	20	PO	FB	80	27920
<RunTimeMVSHLQPrefix>.PROCLIB	TRKS	16	15	PO	FB	80	27920
<RunTimeMVSHLQPrefix>.SYSPRINT	TRKS	19	5	PS	VB	510	3120
<RunTimeUSSPath>/dsi	NA						
<RunTimeUSSPath>/tomcat	NA						
<TargetHLQ>.CAAXDATV	CYLS	88	1	PO	VB	31996	32000
<TargetHLQ>.CAAXLOAD	CYLS	20	5	PO	U	0	27998
<TargetHLQ>.CAAXLPA	TRKS	12	6	PO	U	0	27998
<TargetHLQ>.CAAXMAC	CYLS	15	1	PO	FB	80	32720

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<TargetHLQ>.CAAXSAMP	CYLS	26	1	PO	FB	80	32720
<TargetHLQ>.CABDXML	TRKS	5	5	PO	VB	512	32720
<TargetHLQ>.CUSLIB	CYLS	8	1	PO	U	0	6144
<TargetHLQ>.CUSMAC	TRKS	37	15	PO	FB	80	3120
<TargetHLQ>.CEGPJCL	CYLS	2	1	PO-E	FB	80	32720
<TargetHLQ>.CEGPPROC	CYLS	1	1	PO-E	FB	80	32720
<TargetHLQ>.CEGPSAMP	CYLS	1	1	PO-E	FB	80	32720

CSMaxx06

The following table lists the data sets that are created when this job runs.

Note: The total primary quantity of cylinders is 2,445 of 3390 DASD space.

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<dbHLQ>.A011007	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.A021007	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.AUD4000	CYLS	500	350	PS	F	27992	27992
<dbHLQ>.CBS1006	CYLS	15	15	PS	F	4096	4096
<dbHLQ>.CXX	CYLS	35	10	PS	F	4096	4096
<dbHLQ>.DD1002	CYLS	60	15	PS	F	4096	4096
<dbHLQ>.DDD015	CYLS	15	15	PS	F	4096	4096
<dbHLQ>.DDDIXX	CYLS	15	15	PS	F	4096	4096
<dbHLQ>.DEL1020	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.FXX	CYLS	90	15	PS	F	32760	32760
<dbHLQ>.INV4000	CYLS	400	100	PS	F	8192	8192
<dbHLQ>.IXX002	CYLS	45	15	PS	F	4096	4096
<dbHLQ>.IXX006	CYLS	15	15	PS	F	4096	4096
<dbHLQ>.IXX015	CYLS	15	15	PS	F	4096	4096
<dbHLQ>.IXX016	CYLS	5	5	PS	F	4096	4096
<dbHLQ>.IXX017	CYLS	5	5	PS	F	4096	4096

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<dbHLQ>.IXX1000	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.IXX1006	CYLS	15	15	PS	F	4096	4096
<dbHLQ>.IXX1007	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.IXX1018	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.IXX1019	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.IXX1020	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.IXX4000	CYLS	120	30	PS	F	4096	4096
<dbHLQ>.JNL4000	CYLS	120	30	PS	F	8192	8192
<dbHLQ>.LXX	CYLS	90	15	PS	U	32760	32760
<dbHLQ>.MSG015	CYLS	15	15	PS	F	4096	4096
<dbHLQ>.PXX	CYLS	90	15	PS	U	0	0
<dbHLQ>.PCY4000	CYLS	35	15	PS	F	4096	4096
<dbHLQ>.SCS4000	CYLS	130	60	PS	F	8192	8192
<dbHLQ>.SDS4000	CYLS	90	30	PS	F	8192	8192
<dbHLQ>.SIT015	CYLS	5	5	PS	F	4096	4096
<dbHLQ>.SNP1019	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.SQ1016	CYLS	5	5	PS	F	4096	4096
<dbHLQ>.SRG4000	CYLS	60	15	PS	F	8192	8192
<dbHLQ>.STA1018	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.SYS1000	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.TTM017	CYLS	5	5	PS	F	4096	4096
<dbHLQ>.XML4000	CYLS	300	300	PS	F	27992	27992

CSMaxx09

The following table lists the data sets that are created when this job runs.

Note: The total primary quantity of cylinders is 460 of 3390 DASD space.

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<dbHLQ>.MSM.CXX.INSBKUP	CYLS	35	10	PS	VB	4088	4096

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<dbHLQ>.MSM.DB002.INSBKUP	CYLS	60	15	PS	VB	4069	27998
<dbHLQ>.MSM.DB015.INSBKUP	CYLS	15	15	PS	VB	2309	27998
<dbHLQ>.MSM.DB4000.INSBKUP	CYLS	350	300	PS	VB	27988	27992

CSMUxx01

The following table lists the data sets that are created when this job runs.

This is the first job to run.

The contents of this job is specific to the version that you are upgrading from.

Primary quantity space allocation reflects what is defined in the associated z/OS job stream and should be sufficient. However, the total quantity will be adjusted to the actual quantity required based upon your current environment usage.

The following is required if you are upgrading from CA MSM V5.0 to CA CSM Release 5.1:

Note: The total primary quantity of cylinders is 1,060 of 3390 DASD space.

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<depDbHLQ>.CXX.BACKUP	CYLS	35	10	PS	VB	4088	27998
<depDbHLQ>.DB4000.BACKUP	CYLS	350	300	PS	VB	27988	27992
<depDbHLQ>.DDDBBU.BACKUP	CYLS	60	10	PS	VB	4069	27998
<depDbHLQ>.DDDDBU.BACKUP	CYLS	15	15	PS	VB	2309	27988
<depDbHLQ>.PR.BEXCLINV	CYLS	200	200	PS	VB	27988	27992
<depDbHLQ>.PR.BEXCLJNL	CYLS	200	200	PS	VB	27988	27992
<depDbHLQ>.PR.BEXCLPCY	CYLS	200	200	PS	VB	27988	27992

The following is required if you are upgrading from CA MSM R4.1 to CA CSM Release 5.1:

Note: The total primary quantity of cylinders is 985 of 3390 DASD space.

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<depDbHLQ>.CXX.BACKUP	CYLS	35	10	PS	VB	4088	27998
<depDbHLQ>.DB4000.BACKUP	CYLS	350	300	PS	VB	27988	27992
<depDbHLQ>.DDDBBU.BACKUP	CYLS	60	10	PS	VB	4069	27998
<depDbHLQ>.DDDDBU.BACKUP	CYLS	15	15	PS	VB	2309	27988
<depDbHLQ>.PR.BEXCLSCS	CYLS	130	60	PS	VB	2371	27998
<depDbHLQ>.PR.BEXCLSDS	CYLS	50	25	PS	VB	5778	27998
<depDbHLQ>.PR.ESCSDUF	CYLS	50	25	PS	FB	64	25600
<depDbHLQ>.PR.ESDSC13	CYLS	50	25	PS	FB	12	24000
<depDbHLQ>.PR.ESDSC24	CYLS	50	25	PS	FB	1349	26980
<depDbHLQ>.PR.ESDSSYS	CYLS	15	15	PS	FB	1043	26075
<depDbHLQ>.PR.ESRGSR1	CYLS	15	15	PS	FB	517	32571
<depDbHLQ>.PR.NSCSDUF	CYLS	50	25	PS	FB	82	24600
<depDbHLQ>.PR.NSDSC13	CYLS	50	25	PS	FB	20	26000
<depDbHLQ>.PR.NSDSC24	CYLS	50	25	PS	FB	1370	27400
<depDbHLQ>.PR.NSDSSYS	CYLS	15	15	PS	FB	1060	26500

The following is required if you are upgrading from CA MSM V4.0 to CA CSM Release 5.1:

Note: The total primary quantity of cylinders is 1,105 of 3390 DASD space.

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<depDbHLQ>.CXX.BACKUP	CYLS	35	10	PS	VB	20480	27998
<depDbHLQ>.DB4000.BACKUP	CYLS	350	300	PS	VB	20480	27998
<depDbHLQ>.DDDBBU.BACKUP	CYLS	60	15	PS	VB	20480	27998
<depDbHLQ>.DDDDBU.BACKUP	CYLS	15	15	PS	VB	20480	27998
<depDbHLQ>.PR.BEXCLSCS	CYLS	130	60	PS	VB	2371	27998

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<depDbHLQ>.PR.BEXCLSDS	CYLS	50	25	PS	VB	5779	27998
<depDbHLQ>.PR.ESCSCNP	CYLS	30	15	PS	FB	801	24030
<depDbHLQ>.PR.ESCSDUF	CYLS	50	25	PS	FB	64	25600
<depDbHLQ>.PR.ESDSC13	CYLS	50	25	PS	FB	12	24000
<depDbHLQ>.PR.ESDSC23	CYLS	30	15	PS	FB	632	25280
<depDbHLQ>.PR.ESDSC24	CYLS	50	25	PS	FB	1250	27500
<depDbHLQ>.PR.ESDSSYS	CYLS	15	15	PS	FB	1043	26075
<depDbHLQ>.PR.ESRGSR1	CYLS	15	15	PS	FB	517	32571
<depDbHLQ>.PR.NSCSCNP	CYLS	30	15	PS	FB	806	24180
<depDbHLQ>.PR.NSDSDUF	CYLS	50	25	PS	FB	82	24600
<depDbHLQ>.PR.NSDSC13	CYLS	50	25	PS	FB	20	26000
<depDbHLQ>.PR.NSDSC23	CYLS	30	15	PS	FB	634	25360
<depDbHLQ>.PR.NSDSC24	CYLS	50	25	PS	FB	1370	27400
<depDbHLQ>.PR.NSDSSYS	CYLS	15	15	PS	FB	1060	26500

The following is required if you are upgrading from CA MSM r3.1 to CA CSM Release 5.1:

Note: The total primary quantity of cylinders is 1,110.

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<DatabaseHLQ>.MSM.CXX.BACKUP	CYLS	35	10	PS	VB	20480	27998
<DatabaseHLQ>.MSM.DB4000.BACKUP	CYLS	350	300	PS	VB	20480	27998
<DatabaseHLQ>.MSM.DDDBBU.BACKUP	CYLS	60	15	PS	VB	20480	27998
<DatabaseHLQ>.MSM.DDDDBBU.BACKUP	CYLS	15	15	PS	VB	20480	27998
<DatabaseHLQ>.MSM.PR.BEXCLSDS	CYLS	50	25	PS	VB	20480	27998
<DatabaseHLQ>.MSM.PR.ESDSC13	CYLS	30	15	PS	FB	8	27992
<DatabaseHLQ>.MSM.PR.ESDSC14	CYLS	30	15	PS	FB	8	27992
<DatabaseHLQ>.MSM.PR.ESDSC15	CYLS	30	15	PS	FB	8	27992
<DatabaseHLQ>.MSM.PR.ESDSC16	CYLS	30	15	PS	FB	8	27992
<DatabaseHLQ>.MSM.PR.ESDSC23	CYLS	30	15	PS	FB	630	27720

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<DatabaseHLQ>.MSM.PR.ESDSC24	CYLS	50	25	PS	FB	1250	27500
<DatabaseHLQ>.MSM.PR.ESDSDAS	CYLS	30	15	PS	FB	329	27965
<DatabaseHLQ>.MSM.PR.ESDSSYS	CYLS	15	15	PS	FB	770	27720
<DatabaseHLQ>.MSM.PR.NSDSC13	CYLS	50	15	PS	FB	20	26000
<DatabaseHLQ>.MSM.PR.NSDSC14	CYLS	30	15	PS	FB	13	27989
<DatabaseHLQ>.MSM.PR.NSDSC15	CYLS	30	15	PS	FB	13	27989
<DatabaseHLQ>.MSM.PR.NSDSC16	CYLS	30	15	PS	FB	13	27989
<DatabaseHLQ>.MSM.PR.NSDSC23	CYLS	30	15	PS	FB	634	25360
<DatabaseHLQ>.MSM.PR.NSDSC24	CYLS	50	25	PS	FB	1370	27400
<DatabaseHLQ>.MSM.PR.NSDSDAS	CYLS	30	15	PS	FB	331	27804
<DatabaseHLQ>.MSM.PR.NSDSSYS	CYLS	15	15	PS	FB	1060	26500

Appendix B: Troubleshooting

This appendix provides Frequently Asked Questions and troubleshooting information to help you identify and resolve issues that you may encounter when using CA CSM. The appendix does not include CA CSM error messages.

Note: For a complete list of CA CSM messages, see the *Message Reference Guide*.

Accept or Restore Maintenance in SMP/E Fails

Symptom:

When I try to accept or restore maintenance in an SMP/E environment, the task fails, and the SPMOUT output reports error messages.

- For accepting maintenance, the error messages can be:

  GIM51702S ** THE ACCEPT COMMAND WAS NOT PROCESSED BECAUSE NO RELATED ZONE WAS SPECIFIED IN THE ZONE DEFINITION ENTRY.

  GIM50801S ** ZONE *zone_name* WAS NOT USED BECAUSE IT IS NOT DEFINED BY A ZONEINDEX SUBENTRY IN THE GLOBAL ZONE.

- For restoring maintenance, the error messages can be:

  GIM51702S ** THE RESTORE COMMAND WAS NOT PROCESSED BECAUSE NO RELATED ZONE WAS SPECIFIED IN THE ZONE DEFINITION ENTRY.

  GIM50801S ** ZONE *zone_name* WAS NOT USED BECAUSE IT IS NOT DEFINED BY A ZONEINDEX SUBENTRY IN THE GLOBAL ZONE.

Reason:

Depending on the action you are performing, the reason is one of the following:

- If you accept maintenance, the SMP/E environment is missing the target zone that is related to the affected distribution zone, or the related target zone does not exist.
- If you restore maintenance, the SMP/E environment is missing the distribution zone that is related to the affected target zone, or the related distribution zone does not exist.

Solution:

- Submit a batch job with a step similar to the following example to either add the missing target zone that is related to the affected distribution zone, or define the existing target zone:

```
SET
   BOUNDARY(distribution_zone_name) .
UCLIN .
ADD DLIBZONE(distribution_zone_name)
  RELATED(target_zone_name) .
ENDUCL .
```

- Submit a batch job with a step similar to the following example to either add the missing distribution zone that is related to the affected target zone, or define the existing distribution zone:

```
SET
   BOUNDARY(target_zone_name) .
UCLIN .
ADD TARGETZONE(target_zone_name)
  RELATED(distribution_zone_name) .
ENDUCL .
```

CA CSM Address Space Functions Incorrectly

Symptom:

The SCS address space does not function correctly, and I see messages similar to the following sample in the log:

```
MSMC0501E SQL PREPARE VERSIONSTMT for task MSMCJTSK failed, SQLCODE=-124,
SQLSTATE=51002, RETCODE=,
                            IRETCODE=X'0000'
MSMC0503E SQL error message: PLAN CASWMGT.MSMCFSQL_050_001 DOES NOT EXIST
MSMC0501E SQL ROLLBACK for task MSMCJTSK failed, SQLCODE=-124, SQLSTATE=51002,
RETCODE=, IRETCODE=X'0000'
MSMC0503E SQL error message: PLAN CASWMGT.MSMCFSQL_050_001 DOES NOT EXIST


MSMC0501E SQL PREPARE_DEPUNIT for task MSMCIENG failed, SQLCODE=-124, SQLSTATE=51002,
RETCODE=, IRETCODE=X'0000'
MSMC0501E SQL ROLLBACK for task MSMCIENG failed, SQLCODE=-124, SQLSTATE=51002,
RETCODE=, IRETCODE=X'0000'
```

Additionally, you can see the messages similar to these messages:

```
MSMC0401E EVTINIT for task MSMCIES0 failed, RETCODE=X'00000020'
MSMC0401E EVTINIT for task MSMCIENG failed, RETCODE=X'00000020'
MSMC0401E EVTINIT for task MSMCCEVH failed, RETCODE=X'00000020'
```

Reason:

The SQL plans in the CA Datacom/MSM database are not up-to-date.

Solution:

Update and synchronize the SQL plans in the CA Datacom/MSM database.

More information:

SQL Plan Updates (see page 88)

CA CSM Application Server Error in MSMLOG File

Symptom:

I see the following error message in the CA CSM application server MSMLOG file:

```
WARNING: Error reading /dev/urandom
Throwable occurred: java.io.FileNotFoundException: /dev/urandom (EDC5157I An
internal error has occurred.)
 at java.io.FileInputStream.<init>(FileInputStream.java:112)
```

Reason:

This message only appears when both of the following conditions are met:

- You have installed PTF RO21996 on CA CSM r2.0 (FMID CEG1200).
- The IBM Integrated Cryptographic Service Facility (ICSF) has not been started on the z/OS system where the CA CSM application server session is running.

Solution:

The appearance of this message in no way affects the performance of CA CSM, and CA CSM will continue to function. If you want to verify that dev/urandom is running and is compatible with CA CSM, use the following command:

```
$ cat </dev/urandom | head -c12 | od -X
```

The command has to return random data without any error. For example:

```
0000000000          60621BCF        8AAD1F12        8944D619
0000000014
```

If the device is not working, a warning message appears. For example:

```
FSUM7343 cannot open "/dev/urandom" for input: EDC5157I An internal error
has occurred.
0000000000
```

If you see this error message, reconfigure your /dev/random device in order that the command can successfully read from this device.

Note: For more information about the /dev/random device, see the IBM *z/OS V1R10.0 UNIX System Services Planning* (GA22-7800-14).

CA CSM Application Server Error on Startup in MSMLOG File

Symptom:

CA CSM application server fails during startup, and I see the following error message in the MSMLOG file:

```
SEVERE: StandardServer.await: create[22150]:
Throwable occurred: java.net.BindException: EDC8116I Address not available.
             at java.net.PlainSocketImpl.socketBind(Native Method)
             at java.net.PlainSocketImpl.bind(PlainSocketImpl.java:384)
             at java.net.ServerSocket.bind(ServerSocket.java:331)
```

Reason:

The localhost Domain Name System (DNS) entry was not defined in your local DNS.

Solution:

Your network administrator must define a DNS entry for localhost.

CA CSM Application Server Timeout

Symptom:

When I select to display a list of maintenance packages, the following message appears:

```
Reading maintenance packages from Software Catalog
```

Then, the following error message is displayed:

```
The call failed on the server; see server log for details
```

I can see the following messages in the MSMTC job log:

```
SEVERE: Exception while dispatching incoming RPC call
Throwable occurred: java.net.SocketTimeoutException: Read timed out
at java.net.SocketInputStream.read(SocketInputStream.java:140)
```

This issue only appears when I work in CA CSM in Microsoft Internet Explorer.

Reason:

CA CSM fails to display a large amount of data.

Solution:

Take the following steps, as necessary:

1. Verify the number of table rows to display. This number is defined in the Table Rows field on the User Settings, User Preferences page, under the Settings tab. If the number of rows is 250, set it to a lower value, for example, 50 or 100.
2. If for any reason you need to keep the number of table rows set to 250, update the CA CSM application server timeout parameter.

   In the server.xml file that is located in the tomcat/conf directory, find the following line:

   ```
   connectionTimeout="20000"
   ```

   This parameter defines how long (in milliseconds) the TCP/IP stack waits for incoming packets. Set this parameter to a greater value (for example, 180000). Then, restart the CA CSM application server for the changes to take effect.

   Note: The server.xml file is stored in ASCII.

More information:

Edit an ASCII File (see page 202)

CA CSM Fails to Start with SAF Security Enabled

Symptom:

CA CSM fails with SAF security enabled. SafError with RC=13 or RC=15 is displayed in the job log. The log displays error messages similar to the following example:

```
FATAL (main) 2012-06-13 14:12:37,056
(SafManagerImpl.java:434):SafManager–initialize
DSI():Return code from DDSI_java_open is higher than zero.RC=13
FATAL (main) 2012-06-13 14:12:37,067 (SystemManager.java:491):
com.ca.mf20.zos.services.saf.errors.SafError: null
```

```
Additional Diagnostic Data:
Error during DSI java open. RC=13
Path to 'dsi.conf': /u/users/msmr51/msmruntime/dsi/dsi.conf
BEGINNING OF 'dsi.conf':
This is the DSI Server component configuration file
host localhost
port 22130
TLSKeyringFile /u/users/msmdev/dsi/cert/CA_SelfSigned_Server.kdb
TLSKeyringStash /u/users/msmdev/dsi/cert/CA_SelfSigned_Server.sth
TLSKeyLabel "Cert for SelfSigned Server"
TLSVerifyClient ON
END OF 'dsi.conf'

DSI parameters from table USERCONFIG in database:
Required parameters are marked with (*):
KEY:            DEFAULT_VALUE:  VALUE
*dsiPort:       22130:          22130
*dsiHost:       localhost:      localhost
*dsiConf:       N/A:            /u/users/msmr51/msmruntime/dsi/dsi.conf
>dsiKdb:        N/A:            Uninitialized
>dsiSth:        N/A:            Uninitialized
>dsiLabel:      N/A:            Uninitialized
>dsiVerPeer:    N/A:            false
```

Solution:

Take the following steps as necessary:

- Verify whether the localhost entry is defined in your DNS. Issue the following USS command:

  ```
  oping localhost
  ```

  If the command returns the error message (EZZ3111I Unknown host 'localhost'), the localhost entry is not defined. In this case, perform one of the following actions:

  - Ask your network administrator to define the localhost entry in your DNS.
  - In the USERCONFIG database table and in dsi.conf, set the dsiHost entry to 127.0.0.1 (see page 202).

- Verify whether the host and the port parameters in the dsi.conf file are the same as dsiHost and dsiPort parameters in the USERCONFIG database table. If the host/dsiHost and port/dsiPort parameters differ, update either the dsi.conf file or the database entries (see page 202). The content of the dsi.conf file, the CA DSI Server parameters in the USERCONFIG database table, and the path to the dsi.conf file are displayed in the error message.

- Verify whether the CA DSI Server port (port/dsiPort) is free. Issue the following USS command:

  `onetstat -P port_number`

  For example:

  `onetstat –P 22130`

  If the command returns an empty table, the port is free.

- Verify whether the CA DSI Server port is reserved for CA CSM. Issue the following USS command:

  `onetstat -o`

  The command displays the list of reserved ports. If the CA DSI Server port is not listed, we recommend that you reserve the CA DSI Server port.

CA CSM Fails with Exception

Symptom:

CA CSM fails with an exception, for example:

```
MSM0008E - System startup failed - please see error output for further information.
Fatal error that has stopped the startup was: or
g.apache.tomcat.dbcp.dbcp.SQLNestedException: Cannot create
PoolableConnectionFactory (IO error sending or receiving native data:
ca.datacom.db.DBIOException: CCICONV FAILURE:  No receiver online in
Session(connect)).

MSM0010E - CA CSM startup failed.

FATAL (main) 2011-01-12 15:05:15,098 (SystemManager.java:333): java.lang.Error:
org.apache.tomcat.dbcp.dbcp.SQLNestedException: Cannot create
PoolableConnectionFactory (IO error sending or receiving native data:
ca.datacom.db.DBIOException: CCICONV FAILURE:  No receiver online in
Session(connect))
```

Reason:

The ServerName for the CA Datacom/MSM server or ApplicationID in both the SAMPLIB(SRVLIB) member and the context.xml file do not match.

Solution:

Change the ServerName or the ApplicationID (see page 203) in either context.xml or SAMPLIB(SRVLIB) so that they match.

Delete Task Button Disabled on the Tasks Tab

Symptom:

I cannot delete a task from the Tasks tab, and the Delete Task button is disabled.

Reason:

You do not have access to delete tasks.

Solution:

Check whether the security feature in CA CSM is enabled, and perform one of the following actions:

- If the security feature is enabled, verify that the following resource profiles are created:

  TM.TASK.@SELF.DELETE

  Grants access to delete a user's own tasks.

  TM.TASK.SYSTEM.DELETE

  Grants access to delete any tasks.

- If the security feature is disabled, verify that the following option is specified in the CA CSM options file:

  `sysTaskDeleteOverrideEnabled=Y`

  sysTaskDeleteOverrideEnabled

  Specifies whether to let CA CSM users delete tasks.

  Y

  Any user can delete any competed task.

  N

  Users cannot delete completed tasks.

  Default: N

Deployment SMPOUT Reports GIMUNZIP Message

Symptom:

I get message GIM69158I in the SMPOUT report for my deployment task.

Reason:

The message is displayed when the user executing the deployment does not have UNIX SUPERUSER attributes or authorities that are assigned to them. GIMUNZIP behavior on the target system is affected by the presence of the SUPERUSER attribute.

Solution:

This message is informational.

Note: For more information about the specific return or reason codes that are associated with the message, see the *IBM SMP/E Messages and Codes*.

Dynamic Allocation Errors for Temporary and RELFILE Data Sets

Symptom:

I get a dynamic allocation error for temporary and RELFILE data sets.

Reason:

The HLQ option was set to a value that you are not authorized to use.

Solution:

Change the HLQ option to a value that you are authorized to use.

Dynamic Allocation for the MACLIB Library Fails During Software Installation

Symptom:

When creating an SMP/E environment during product installation, I see the following error in the message log:

```
Dynamic allocation of input data set member SYS1.MACLIB(GIMZPOOL) failed. DD: ZP3 RC:
4 Error code: 0x1708 Info code: 0x2.
```

Reason:

CA CSM cannot locate the default MACLIB library, SYS1.MACLIB. For example, the library was renamed.

Solution:

Define a new Java runtime option maclib.dsn variable in the SAMPLIB(MSMLIB) member. Verify that the new data set name does not exceed 38 characters.

Example:

```
IJO="$IJO -Dmaclib.dsn=CUSTOM.MACLIB"
```

False Product Update Succeeded Status

Symptom:

CA CSM completes a product update with a Succeeded status, but the software catalog has not been updated.

Note: This issue does not occur when HTTPS downloads are active.

Reason:

Pax and ESD product files are occasionally unavailable for immediate download. When this situation occurs, CA CSM initiates a Request Product PrePackage process. This process makes these files available on the web page and sends an email to you when that process is completed. Because of internal changes on the CA Support Online website, CA CSM no longer initiates a Request Product PrePackage process unless you have installed CA CSM Build 442, PTF 5EGP442 or later.

Solution:

Ensure that you have installed CA CSM Build 442, PTF 5EGP442 or later.

GIM54701S ** ALLOCATION FAILED FOR SMPJHOME

Symptom:

When applying a maintenance package, I see the following SMP/E error message:

```
GIM54701S ** ALLOCATION FAILED FOR SMPJHOME - IKJ56228I PATH
/sys/java31bt/v6r0m0/usr/lpp/java/J6.0 NOT IN CATALOG OR CATALOG CAN NOT BE ACCESSED.
```

Note: Your Java home path may be different from the Java home path in the previous message as CA CSM does not specify a mandatory path.

Reason:

The SMPJHOME DDDEF is not set correctly in the SMP/E environment where you applied a maintenance package.

Solution:

Change the SMPJHOME DDDEF in the SMP/E environment.

- If the SMPJHOME DDDEF is not set correctly in the CA CSM SMP/E environment, use the UCLIN statement to correct the SMPJHOME DDDEF in the CA CSM SMP/E environment. (see page 112)
- If the SMPJHOME DDDEF is not set correctly in another SMP/E environment, use the UCLIN statement to correct the SMPJHOME DDDEF in all zones in the SMP/E environment. (see page 112)

I/O Errors in SMP/E Generated Data Sets

Symptom:

When I try to install a product or manage a maintenance package, the task is missing one or more steps with task output. These steps can be of the following types: SMPLIST, SMPPRINT, SYSPRINT, or SYSTERM. I see the following error message in the MSMTC job log:

```
Errno2: -1070137335, ErrorCode: 0, FeedbackFdbk: 0, FeedbackFtncd: 0,
FeedbackRc: 0, LastOp: 3, ErrnoMsg: EDC5066I A read system error was detected.
```

Reason:

CA CSM failed to read one of temporary data sets with task output that it created, and interrupted further reading.

Solution:

Follow these steps:

1. Include the following parameter in the SAMPLIB(MSMLIB) data set member:

   ```
   IJO="$IJO -DWriteEmptyRecordMVS=true"
   ```

2. Restart the CA CSM application server.

MSMTC Fails with RC=100

Symptom:

The MSMTC job fails with RC=100 (MAXCC=100) after the job is started.

For example:

```
04.30.18 JOB00480 $HASP165 MSMTC    ENDED AT SYSSERV1  MAXCC=100 CN(INTERNAL)
```

The STDMSG output contains the following message:

```
JVMJZBL2007E Stack trace follows:
java.lang.NoClassDefFoundError: org.apache.catalina.startup.Bootstrap
Caused by: java.lang.ClassNotFoundException: org.apache.catalina.startup.Bootstrap
```

Note: The STDMSG output may not be a part of MSMTC JOBLOG. The following statement in RunTimeMVSHLQPrefix.JCL(MSMTCSRV) manages it:

```
//   ARGS='start 1>stdout 2>stdERR',   <-- Args to Java class
```

If ARGS='', STDMSG is created.

Reason:

The first step of the MSMTC job is to start the CA CSM application server (see page 229) that is located in RunTimeUSSPath/tomcat.

When RunTimeUSSPath is empty, this step fails with RC=100. A possible reason for RunTimeUSSPath being empty is that the file system belonging to this folder is not mounted.

Solution:

- Mount the file system to RunTimeUSSPath and verify that other file systems are properly mounted.
- Contact CA Support.

No Ticket Error Message When Accessing CA CSM

Symptom:

When I try to access CA CSM using a web browser, I get multiple error messages including the No Ticket error message. The access attempt fails.

Reason:

Cookies are not allowed in your web browser.

Solution:

Allow cookies in your web browser.

If your site standards restrict using cookies, add the CA CSM access URL to trusted sites.

Note: For more information about how to allow cookies and how to add a URL to trusted sites, see user documentation for your web browser.

Product List Update Fails

Symptom:

When I update the product list, I receive a message similar to the following sample:

```
IO Error was detected during PAS processing.
Additional Diagnostic Data:
IO Exception Error.(UnknownHostException) Error encountered while
accessing the following URL:
https://supportservices.ca.com/support
supportservices.ca.com
Please review your http proxy settings and validate that your system has network
connectivity to the above URL.
```

Solution:

Verify that the CA CSM application server is using the correct TCP/IP stack. If necessary, uncomment the SYSTCPD DD card in the CA CSM application server startup job (MSMTCSRV) or the application server started task.

```
//SYSTCPD DD DSN=VTAM.TCPIP.TCPIP.DATA,
//           DISP=SHR
```

SMP/E APPLY or ACCEPT Processing Fails

Symptom:

SMP/E APPLY or ACCEPT processing fails due to a target or distribution library running out of free directory blocks.

Reason:

A product (for example, PDSMAN) was installed and configured in a way that PDS directory blocks occupy more space than by default. This particular PDS data set ran out of free directory blocks.

Solution:

Change the PDS directory block increase percentage.

Follow these steps:

1. Shut down the MSMTC address space using the command:

   ```
   P MSMTC
   ```

2. In the STDENV startup script, specify the variable for msm.pds.dirblk.percentage in the data set that the STDENV DDNAME points to in the MSMTC STC procedure. Alternatively you can increase the value of the variable:

   ```
   IJO="$IJO –Dmsm.pds.dirblk.percentage=25”
   ```

3. Start the MSMTC address space using the command:

   ```
   S MSMTC
   ```

4. Retry the task that failed.

SMP/E Environment Does Not Appear on the Tree

Symptom:

I cannot see an SMP/E environment on the tree on the left side of SMP/E environments on the SMP/E Environments tab. Other users can see this SMP/E environment on the tree.

Reason:

Your user ID does not have privileges to access the SMP/E environment.

Solution:

- Verify whether you have access to the HLQ of the SMP/E environment CSI data set.
- Access the SMP/E environment outside of CA CSM. Analyze a message that you receive from the security system that your site uses.

  For example, if you are using CA Top Secret for z/OS, you see the following message:

  ```
  TSS7221E Dataset Not Accessible
  ```

  Contact your security administrator to get access rights to the SMP/E environment.

SMP/E Environment Migration Fails at the SMP/E Environment Functions Step of the SMP/E Environment Migration Wizard

Symptom:

Migration of an SMP/E environment fails on the SMP/E Environment Functions step of the wizard, and I receive one of the following messages:

- I see the following message on the SMP/E Environment Migration wizard:

  ```
  MMR0005S - An error occurred during dlopen(libGIMAPI03040026.so): CEE3501S The module libGIMAPI03040026.so was not found. MMI0084S - Initialization of CAGIMAPI address space failed.
  ```

- I see one of the following messages in the MSMTC job log:

  ```
  .1299171650. CGIMAPIExtractor_ForkStub: Exception occurred during Initialize() processing: mcCagimapiHandshake
  ```

  ```
  .1299171650. CGIMAPIExtractor_ForkStub: Exception text: Initialization of CAGIMAPI address space failed.
  ```

  ```
  An exception has occurred during native_initialize(): MMI0101S - A serious error has occurred while initializing GIMAPI Extractor.
  ```

```
ERROR (http-17310-5) 2011-03-03 14:49:43,895
(DataExtractionDriver_Jni.java:305): Initialization of
DataExtractionDriver_Jni has failed.

INFO  (http-17310-5) 2011-03-03 14:49:43,896 (BufferedMessageReader.java:206):
A new message was read and enqueued in the message log: MMR0005S - An error occurred
during dlopen(libGIMAPI03040026.so): CEE3501S The module libGIMAPI03040026.so
was not found.  at ./CGIMAPIExtractionLibrary.C:51

INFO  (http-17310-5) 2011-03-03 14:49:43,896 (BufferedMessageReader.java:206):
A new message was read and enqueued in the message log: MMI0084S - Initialization
of CAGIMAPI address space failed. At ./CGIMAPIExtractor_ForkStub.C:430
```

Reason:

CA CSM cannot load the shared object files (DLL), because the files do not have the required attributes. All of the files need the following attributes:

```
+p, +s, +r, +x
```

The libcci.so file also needs this attribute:

```
+a
```

Solution:

Check the SO files and DLL files for the correct attributes and privileges. Add the required attributes and privileges to files that are lacking them.

1. Check the attributes and privileges of all the SO files and DLL files in the …/tomcat/lib directory using the command:

   ```
   ls –E  *.so *.dll
   ```

   Results similar to the following example appear:

   ```
   -rwxr-xr-x  aps-  1 USERID  GROUPID   233472 Aug 17  2010 libcci.so
   ```

2. Fix attributes of shared object files using the command:

   ```
   extattr attribute filename
   ```

   For example, to add the +a attribute to the libcci.so file, type:

   ```
   extattr +a libcci.so
   ```

3. Fix access privileges using the command:

   ```
   chmod attribute filename
   ```

   For example, to add the +r attribute to the libcci.so file, type:

   ```
   chmod +r libcci.so
   ```

Glossary

aggregated package

An *aggregated package* is a file that comprises several single maintenance packages (nested packages).

automatic ID

The *automatic ID* is the value of the MSMID variable. This is part of the snapshot and is unique for every deployment.

CA CSM application server

The *CA CSM application server* is the CA CSM Tomcat region that supports the CA CSM application code.

CA Datacom/MSM server

The *CA Datacom/MSM server* is a server that lets workstation-based applications use the CA Datacom/MSM database.

CA Recommended Service (CA RS)

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, download (manually or automatically) all CA RS files that list published maintenance for that CA RS level.

CAICCI system ID

The *CAICCI system ID* is a unique name for a system that is part of a CAICCI network. If you do not specify one, CA CSM obtains it using a validate action.

configuration category

A *configuration category* is a group of variables for a configuration. The top root level is a category that encompasses all categories and variables.

configurations

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

confirm

Confirms that the deployment is complete. This is the final action by the user. A deployment is not completed until it is confirmed. After it is confirmed the deployment moves to the Confirmed deployment list.

contact system

The *contact system* defines which system the deployment is unpackaged on. That is, which system CAICCI is spawned to run the unpackaging.

custom data set

A *custom data set* is a data set that contains either a z/OS data set or USS path.

data destination

A *data destination* must be defined for every system. The data destination is how you tell CA CSM which technique to use to transport the deployment data to the remote system. Data destinations are assigned to non-sysplex systems, sysplexes, and shared DASD clusters. Data destinations are named objects, and thus can be assigned to multiple entities in the system registry and have their own independent maintenance dialogs.

data set name mask

A d*ata 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.

deploy

The *deploy* functionality combines the snapshot, transmit, and deploy actions into one action, letting you copy your CA CSM product onto systems across your enterprise. For example, you can send one or many products to one or many systems by copying it to a shared DASD or through FTP.

deployment

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.

directory path

The root d*irectory path* is the base directory to which the FTP server is allowed access. The FTP server will be allowed to create files to or read files from this directory and any of its subdirectories. The directory path is a USS path name, it consists of one or more directory leaves separated by forward slashes, and has a maximum input length of 255 characters including slashes. When the directory path is translated, it has a maximum length of 255 characters.

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a protocol for transfer of files from one computer to another over the network.

FIXCAT

FIXCAT (fix category) associates a maintenance package to one or more categories of PTFs (for example, installation, function, z/OS version, or communication).

FTP port

An *FTP port* is the point of connection through which files are transferred. The default is 21.

gen level

A *gen level* is the innermost level in the product list in the left pane under the release level of a product. Selecting a gen level in the left pane displays the available base installation packages and other product components in the right pane. Gen levels are preceded with the following icon: 

More information:

product (see page 232)
release (see page 233)

GIMUNZIP volume

The *GIMUNZIP volume* is a data destination setting in CA CSM that specifies the GIMUNZIP volume to direct GIMUNZIP to use GIMUNZIP control files to unpack the data sets onto the specified volume. Use this setting when your environmental setup requires that the libraries that are deployed and copied by CA CSM are directed to a particular volume on your target system.

GIMZIP

GIMZIP is an IBM utility that creates portable packages of software with a suffix of *z*.

landing directory

The *landing directory* is where the data is temporarily placed during a deployment.

managed product USS file system

A *managed product USS file system* is a collection of USS file systems that are used by SMP/E environment under the control of CA CSM. CA CSM creates managed product USS file systems during a base installation and optionally during migration of an SMP/E environment.

methodology

A *methodology* is the process by which data sets are named on the target system. It provides the *how* of a deployment. It is a named object with a description that is assigned to an individual deployment.

monoplex

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.

MSM Common Services

The *MSM Common Services* (CETN500) is a contributed component of CA Common Services for z/OS that consists of the Software Deployment Service (SDS) and the Software Configuration Service (SCS).

MSMCAUX

MSMCAUX is the JCL procedure that is used to start the auxiliary address space. CA Common Services for z/OS that CA CSM uses includes a sample procedure in the member MSMCAUX of the CCS CAIPROC (CCShlq.CAIPROC) library. You must copy this procedure to a system PROCLIB that z/OS START commands use and modify it to suit your installation environment. The MSMCAUX sample member describes the changes that are required. Do not start the MSMCAUX procedure manually. The MSMCAUX procedure is started by the SCS address space (MSMCPROC).

MSMCPROC

MSMCPROC is the JCL procedure that is used to start the SCS address space. CA Common Services for z/OS that CA CSM uses includes a sample procedure in the member MSMCPROC of the CCS CAIPROC (CCShlq.CAIPROC) library. You must copy this procedure to a system PROCLIB that the z/OS START commands use and modify it to suit your installation environment. The MSMCPROC sample member describes the changes that are required.

MSMTC/MSMTCSRV

MSMTC/MSMTCSRV is the job stream or started task associated with the CA CSM application server (see page 229).

non-sysplex

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

optional variable

An *optional variable* does not require a value. Some optional variables must be confirmed.

policy

A *policy* in CA CSM represents a combination of (1) metadata input that identifies the component parts of a product, and (2) user-supplied input that identifies the deployment criteria, such as where it will go and what will it be called.

preview

Preview identifies the deployment by name and briefly states the products, systems, means of transport, target libraries including source, target and resolution, as well as SMP/E environment and snapshot information.

product

A *product* is a level in the product list in the left pane under the vendor. Selecting a product in the left pane displays product releases in the right pane. Products are preceded with the following icon: 

More information:

gen level (see page 231)
release (see page 233)

Product Acquisition Service (PAS)

The *Product Acquisition Service (PAS)* facilitates the acquisition of mainframe products and the service for those products, such as program temporary fixes (PTFs). PAS retrieves information about products to which your site is entitled. Then it records these entitlements in a software inventory that is maintained on your driving system.

profile/profile occurrence

A *profile* is a grouping of variables that belong to a subsystem or a component. A *profile occurrence* is a version of that profile that has been tailored for a specific system. You can have multiple profile occurrences for the same profile on one system.

release

A *release* is the level in the product list in the left pane under the product. Selecting a release in the left pane displays maintenance packages in the right pane. Releases are preceded with the following icon: 

More information:

gen level (see page 231)
product (see page 232)

resolved variable

A *resolved variable* contains a value and has been confirmed (if required). You can modify a variable that has been resolved.

resource

A *resource* is a physical or virtual component of a system. Resources include data sets, parameter settings, libraries, files, and operator commands. Dummy resources are temporary resources used during the configuration build or implementation process, or that serve as place holders for tracking purposes.

SCS address space

The *SCS address space* is a specially defined location where the system registry and commands for interrogating output and console traffic reside within the operating system. The SCS address space provides the services and processing necessary to implement configurations across your targeted z/OS systems. Each target system that is expected to support SCS processing must execute an SCS address space.

SCS address space port

An *SCS address space port* is the point of connection through which the client communicates with the address space. The default is 49152.

shared DASD clusters

A *shared DASD clusters* system is a set of systems that shared DASD and it can be composed of sysplex and/or non-sysplex systems. Staging system cannot be part of a shared DASD cluster.

snapshot

A *snapshot* is a copy of the set of target libraries that CA CSM makes using the IBM utility GIMZIP. CA CSM uses GIMZIP to create a compressed archive of these libraries, including a list of applied maintenance. The SMP/E environment is locked during this archive creation process to verify the integrity of the archived data.

Software Configuration Service (SCS)

The *Software Configuration Service (SCS)* facilitates the mainframe product configuration from the software inventory of the driving system to targeted z/OS operating systems.

Software Deployment Service (SDS)

The *Software Deployment Service (SDS)* facilitates the mainframe product deployment from the software inventory of the driving system to the target system. This facilitation includes deploying installed products that are policy-driven with a set of appropriate transport mechanisms across a known topology.

Software Installation Service (SIS)

The *Software Installation Service (SIS)* facilitates the installation and maintenance of mainframe products in the software inventory of the driving system. This facilitation includes browsing downloaded software packages, managing SMP/E consolidated software inventories on the driving system, and automating installation tasks.

staging system

A *staging system* is a virtual system that 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 can be useful in testing your deployments, and learning deployment in general. It can also be used if your target systems are outside a firewall. For example, deploy to a staging system and then manually copy the deployment to tape.

storage classes

storage classes apply only to SMS-managed data sets and objects. They allow you to define different levels of performance and availability services for your data sets. Using them, you can separate the level of service needed by a data set or object from its physical characteristics. Storage classes can supply such information as attributes for dynamic cache management, sequential data set striping, and concurrent copy.
It is the association of a storage class with a data set or object which causes the data set or object to be SMS-managed. Because of this, such functions as dynamic cache management and sequential data set striping apply only to SMS managed data sets. Data sets may be SMS-managed or non-SMS managed. Objects must be SMS-managed.

symbolic substitution

symbolic substitution, or translation, is a process performed by CA CSM to resolve the mask values specified in the data set name mask and Directory Path, into real names based upon the contents of the symbolic variables at translation time. A CA CSM symbol is defined in the list of symbols. Each symbol begins with an ampersand (&) and ends with a period (.). For example the symbol &LYYMMDD., would be completely replaced with its value at translation time, including the ampersand and trailing period. The trailing period is important and is considered part of the symbolic name.

sysplex

A *sysplex* (SYStem comPLEX) is the IBM mainframe system complex which is a single logic 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.

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.

task output browser

The *task output browser* displays the details of finished tasks.

topology

The enterprise system *topology* can include shared DASD environments, networked environments, and z/OS systems.

transmit

The *transmit* functionality lets you copy a product onto systems across the enterprise through FTP, in preparation for a subsequent deployment.

Uniform Resource Identifier (URI)

A *Uniform Resource Identifier (URI)* is a string of characters used to identify a name or a resource on the Internet. Such identification enables interaction with representations of the resource over a network (typically the World Wide Web) using specific protocols. Schemes specifying a concrete syntax and associated protocols define each URI.
For a shared DASD cluster or sysplex, the URI must be the URI of the Contact System.

UNIX System Services (USS) files

For *UNIX System Services* (*USS*) *files* for z/OS systems, there are three types of files system: HFS (Hierarchical File Systems), zFS (zSeries File Systems), and NFS (Network File Systems). USS files are any one, or combination, of these file systems, and start with the root directory, which is denoted by a single forward slash (/).

validation

The *validation* process is started by the user when they select the Validate button in the Actions drop down for a sysplex system, non-sysplex system, and shared DASD cluster on that system's System Registry Page (staging systems are not validated). This starts a background security procedure using the CAICCI validation services to validate this system.

VOLSER

A *VOLSER* is the Volume Serial Number that places the data on an explicit volume.

working set

A *working set* is a selected group of SMP/E environments with which you want to work. Future displayed information will be based on the working set. For example, maintenance information is shown for the working set. The information is not shown for environments outside the set.

zFS candidate volumes

You can use a *zFS candidate volume* when your environmental setup dictates that zFS container data sets are directed to the specified volume.

Index

M

N

O

P

R

S

T

U

V

W

X