

CA Common Services for z/OS

Installation Guide

Version 14.0



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

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

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

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

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

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

The manufacturer of this Documentation is CA.

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

Copyright © 2011 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references some of the following CA Technologies products:

- CA 1® Tape Management
- CA 7® Workload Automation
- CA 11™ Workload Automation Restart and Tracking
- CA ACF2™
- CA Allocate™ DASD Space and Placement
- CA Audit
- CA Automation Point
- CA Balancing
- CA Bundl®
- CA Database Analyzer™ for DB2 for z/OS
- CA Datacom®/AD
- CA Data Compressor™ for DB2 for z/OS
- CA DB2
- CA Deliver™
- CA Disk™ Backup and Restore
- CA Dispatch™
- CA Easytrieve®
- CA Earl™
- CA Endeavor® Software Change Manager
- CA Fast Check® for DB2 for z/OS
- CA Fast Index® for DB2 for z/OS
- CA Fast Load for DB2 for z/OS
- CA Fast Recover® for DB2 for z/OS
- CA Fast Unload® for DB2 for z/OS
- CA IDMS™
- CA IDMB™/DB
- CA Insight™ Database Performance Monitor for DB2 for z/OS
- CA Index Expert™ for DB2 for z/OS
- CA JARS®

- CA JARS® Resource Accounting
- CA Jobtrac™ Job Management
- CA Log Analyzer™ for DB2 for z/OS
- CA Mainframe Software Manager™ (CA MSM)
- CA Merge/Modify™ for DB2 for z/OS
- CA MIA Tape Sharing
- CA MIC Message Sharing
- CA MICS® Resource Management
- CA MII Data Sharing
- CA MIM™ Resource Sharing
- CA NetMaster® File Transfer Management
- CA NetMaster® Network Automation
- CA NetMaster® Network Management for SNA
- CA NetMaster® Network Management for TCP/IP
- CA NetMaster® Network Operations for TCP/IP
- CA NetSpy™ Network Performance
- CA Network and Systems Management
- CA NSM System Status Manager
- CA OPS/MVS® Event Management and Automation
- CA Partition Expert™ for DB2 for z/OS
- CA Plan Analyzer® for DB2 for z/OS
- CA Quick Copy for DB2 for z/OS
- CA Rapid Reorg® for DB2 for z/OS
- CA RC/Extract™ for DB2 for z/OS
- CA RC/Migrator™ for DB2 for z/OS
- CA RC/Query® for DB2 for z/OS
- CA RC/Secure™ for DB2 for z/OS
- CA RC/Update™ for DB2 for z/OS
- CA Recovery Analyzer™ for DB2 for z/OS
- CA Roscoe®
- CA Scheduler® Job Management
- CA SYSVIEW® Performance Management
- CA Service Desk (Service Desk)

- CA Spool™ Enterprise Print Management
- CA SQL Ease® for DB2 for z/OS
- CA SYSVIEW® Performance Management
- CA TCPAccess™ Communications Server for z/OS
- CA TLMS Tape Management
- CA Top Secret®
- CA TPX™ Session Management for z/OS
- CA Value Pack for DB2
- CA Vantage™ Storage Resource Manager
- CA View®
- CA XCOM™
- CA Workload Control Center

Contact CA Technologies

Contact CA Support

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

- 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

Provide Feedback

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

If you would like 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>.

Contents

Chapter 1: Introduction	13
Audience	13
CA Common Services for z/OS	14
End-to-End Management	14
Business Process Views	15
Comprehensive CA NSM Administration	15
Multilayered Architecture	15
Software Services	17
How the Installation Process Works	23
Chapter 2: Preparing for Installation	25
Component FMIDs	25
Software Requirements	27
Security Requirements	27
Storage Requirements	28
Target Libraries	28
Comprehensive View of Storage Requirements	33
Component Installation Requirements	37
Chapter 3: Installing Your Product Using CA MSM	69
Access CA MSM Using the Web-Based Interface	69
How to Use CA MSM: Scenarios	70
How to Acquire a Product	70
How to Install a Product	71
How to Maintain Existing Products	76
How to Deploy a Product	76
Chapter 4: Installing from Pax Files Using the SAMPJCL Method	79
How to Install a Product Using Pax Enhanced ESD Files	79
How the Pax-Enhanced ESD Download Works	81
ESD Product Download Window	81
USS Environment Setup	84
Allocate and Mount a File System	85
Copy the Product Pax Files into Your USS Directory	86
Download Using Batch JCL	87

Upload Files to Mainframe through a PC	90
Create a Product Directory from the Pax File	91
Sample Job to Execute the Pax Command (Unpackage.txt)	92
Copy Installation Files to z/OS Data Sets	92
How to Install Products Using Native SMP/E JCL	94
Prepare the SMP/E Environment for SAMPJCL Installation	95
Run the Installation Jobs for a SAMPJCL Installation	99
Clean Up the USS Directory	100
Apply Maintenance	101
HOLDDATA	102
CA Common Services Specific Post-Installation Requirement	103
Deploy Products	104
Deploying USS file systems	104
Deploying Agent Technology on Multiple Systems	106
Deploying Event Management on Multiple Systems	109

Chapter 5: Configuring Your Product **111**

Configuration Steps	111
---------------------------	-----

Chapter 6: CAIRIM Configuration **115**

CAIRIM Initialization Parameters	115
Customize CAISSF for RACF or RACF-Compatible Products	117
CAS9SAFC/CAS9RACL for CICS TS	117
Install CAS9RACL	118
Modify and Submit the CAS9CSSF Sample JCL	119
Modify RACF or the RACF-Compatible Product	119
Place the CAISSF Routines in the Common Service Area (CSA)	120
The CAISSF Installation Process	120
Start CAIRIM	121

Chapter 7: CAIENF Configuration **123**

Customize the CAIENF Procedures	124
Symbolics	124
Configure CAIENF Parameter File	126
Configure CAIENF JCL for finding CA product DCMs	127
CA Product DCM compatibility	127
Start CAIENF	128
Prepare for Component Tracing	128
CAIENF/USS Configuration Tasks	129
Customize the ENFSNMPM Procedure	129

Chapter 8: CAICCI Configuration **131**

CAICCI Tasks	131
Configure and Start CAICCI	132
Additional Configuration Tasks for CAICCI	133
Load CAICCI on the Client Platform	146
Peer-to-Peer Communication with Remote Computers	148
Use CA NSM	150
Activate Changes	152
Verify Changes	153
Verify Your Installation	155
Troubleshooting	155
Current Status	155
Activate Tracing	155

Chapter 9: Event Management Configuration **159**

Review and Adjust the Event Management PROFILE	159
Rerun D5II0065 for GUI Tasks on the Deployed System	159
Run the Event Management Configuration Script	159
How to Configure Event Management GUI Tasks	162
Configure the UNIX System Services for Event Management	163
Configure the Web Server	163
Security Definitions for Event Management	165
Initialize the Java Server	166
How to Configure Optional Event Management Tasks	167
Store and Forward	168
Enable catrapd to Receive SNMP Traps	170
Start and Stop the Event Management Processes	171
Install the OPSMVS Exit	171
Set Up the Berkeley syslog daemon	172
Customize emstart and emstop Scripts	174
Startup Procedures	174
Java GUI	175
Timeout Settings	175
Security Requirements	176
Enterprise Management	176
Web Server Configuration	177
Verify Your Installation	179
Verify that Processes are Running	179
Verify the GUI Interface Servers are Active	179
Event Management Maintenance Considerations	181

Chapter 10: Agent Technology Configuration 183

Tailor the Profile, Script, and Configuration Files in the zFS System	183
Edit the profile file: /cai/agent/agentworks.profile	184
Execute the agentworks.profile	186
Edit the script file: /cai/agent/services/tools/install_mibs	186
Edit the config file: /cai/agent/services/config/aws_orb/quick.cfg	187
Edit the config file: /cai/agent/services/config/aws_sadmin/aws_sadmin.cfg	187
Edit the config file: /cai/agent/services/config/aws_snmp/aws_snmp.cfg	188
Tailor the config file: /cai/agent/services/config/awsservices/awsservices.cfg	188
Tailor the ENVFILE from the CNSMOPTV	189
Verify the TCP/IP Network Configuration	189
Build the aws_sadmin Store Files	190
Agent Security	190
Agent Configuration Set Verification	191
Load Library Considerations	191
Start Agent Technology	191
Build and Run the Example Agent (EXAGENT)	192
Compile and Link Online (USS)	192
Compile and Link in Batch Mode (z/OS)	193
Verify Agent Technology Installation	194

Chapter 11: CA Global SubSystem Configuration 197

Complete the GSS Installation	197
How the Post-Configuration Process Works for CA-GSS	198
Define Subsystem IDs	198
Copy CA-GSS Procedures to System PROCLIB	198
Install the IMOD Editor	199
IMOD Editor Problems	201
Install the CA-GSS/ISERVE Operator Control Panel	202
Test the Installation	202
Recompile under TSO	204
Customize CA-GSS	204
Customize CA-GSS for CA Insight Database Performance Monitor for DB2 for z/OS	204
Customize CA Jobtrac Job Management	207
Customize CA-GSS for CA MIM	207
Customize CA-GSS for CA OPS/MVS Event Management and Automation	209
Customize CA SYSVIEW Performance Management	210
Customize CA-GSS for CA View	211
Customize CA-GSS for DB2	212
Customize CA-GSS for IDCAMS	213
Optional Features	214

GoalNet	214
ILOG Files	216

Chapter 12: CA-L-Serv Configuration Tasks **219**

Update External Security for CA-L-Serv	219
Who Needs to Update?	219
How the Update Tasks are accomplished	220
Define CA-L-Serv to VTAM	226
Tailor Startup Parameters	226
Update the Message Table	228
Copy and Customize the Startup Procedure	229
Start CA-L-Serv	230
Verify the Communications Server Installation	230
Troubleshoot: Communications Server IVP is Not Running Successfully	233
Verify the File Server Installation	233

Chapter 13: Other Configurations **237**

CAECIS CA EXAMINE Configuration Tasks	237
Utilize CAECIS	238
CAISDI Configuration Tasks	239
CAICRS Easytrieve Service Configuration Tasks	239
Link Edit the Easytrieve IDMS Interface Module	239
Compile and Link Edit the CA Datacom User Requirements Table (URT)	240
Assemble and Link Edit the Easytrieve Options Table Module	240
Compile and Link Edit the Extended Reporting Options Module	240
CAICRS References	240
Earl Service Configuration Task	241
Verify Earl Service Installation	241
CA MSM Common Services Configuration	241
SRAM Usermod	242
Unicenter Service Desk Installation Configuration	243
Viewpoint Configuration	243

Chapter 14: Install CA Datacom/AD **245**

CA LMP	246
CA Datacom/AD Multi-User Deployment	247
Customize CA Datacom/AD for CAIENF	249
Customize an Existing CA Datacom/AD for CAIENF	249
Customize a New CA Datacom/AD for CAIENF	250
Resolve CA Datacom/AD for CAIENF Customization Issues	252

Customize CA Datacom/AD for Event Management	254
Clone Your CA Datacom/AD Database	258
Central Databases on Multiple Systems	258
Resolve CA Datacom/AD for Event Management Customization Issues	258
Appendix A: Third-Party Software Acknowledgements	261
Apache Software Foundation	261
Index	267

Chapter 1: Introduction

This guide describes how to install and implement CA Common Services for z/OS

CA Common Services is an open, cross-platform enterprise management infrastructure available on many operating system platforms, including z/OS. It provides common services and enabling technology for CA IT management solutions.

This section contains the following topics:

[Audience](#) (see page 13)

[CA Common Services for z/OS](#) (see page 14)

[End-to-End Management](#) (see page 14)

[Business Process Views](#) (see page 15)

[Comprehensive CA NSM Administration](#) (see page 15)

[Multilayered Architecture](#) (see page 15)

[How the Installation Process Works](#) (see page 23)

Audience

Readers of this book must have knowledge in the following areas:

- JCL
- TSO/ISPF
- z/OS environment and installing software in this environment
- z/OS UNIX System Services
- Your organization's IT environment, enterprise structure, and region structure

Consult with the following personnel as required:

- Systems programmer for z/OS and VTAM definitions
- Storage administrator for DASD allocations

CA Common Services for z/OS

CA Common Services for z/OS includes distributed services common to CA implementations and solutions specific to z/OS. CA Common Services for z/OS 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 CA Common Services works on Windows and UNIX platforms. CA Common Services for z/OS also contains the essential components and functionality to enable integrated management of z/OS.

CA Common Services for z/OS includes support for applications based on z/OS UNIX System Services. CA Common Services for z/OS also furnishes the Agent Technology infrastructure to run z/OS Agents.

CA Common Services for z/OS lets 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 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 products.

End-to-End Management

With CA Common Services for z/OS, you can integrate z/OS solutions with management solutions on other platforms to achieve enterprise-wide end-to-end management from any remote location and from a single console.

The software technology of CA Common Services for z/OS lets you run the appropriate hardware platforms and software applications for each aspect of your business and deploy them across many machines while enabling you to manage them as an integrated whole.

Business Process Views

Business Process Views are user-defined groups of managed objects that represent the following:

- Specific business processes
- Resource features
- Geographical locations
- Organizational structures
- Applications

With the CA Network and Systems Management architecture, you can create a Business Process View that displays only those objects related to accounting processing, or a view for payroll. The manufacturing department might have a view showing the servers, networking devices, and segments in various factories and warehouses. Your view options are numerous. With CA Common Services for z/OS and the installation of z/OS Agents, you can include your z/OS systems in CA Network and Systems Management Business Process Views.

Comprehensive CA NSM Administration

Using CA Common Services for z/OS, you can cause CA NSM components installed on other platforms to react to events on the mainframe and conversely have the mainframe react to components on other platforms.

Event Management lets you do the following:

- Monitor and administer different kinds of asynchronous events including SNMP traps, application events, and system events.
- See the z/OS Event Management console from other CA NSM platforms.
- See other platform CA NSM Event Management consoles from the z/OS Event Management Java GUI.

Multilayered Architecture

CA Common Services for z/OS is composed of a software services layer and a management services layer. The software services layer includes a suite of industry standard integration and distributed processing services to unify software applications. The management services layer provides a web-based, real-world graphical interface and monitoring of application and system events.

Each service component has been assigned to one of the following packaging bundles:

- Base
- Optional
- Legacy
- MFNSM (Mainframe CA NSM)

All the components found in the Base Common Services bundle must be installed. The components found in the other three bundles may be required based on your site's needs and are therefore considered optional for the CA Common Services Installation.

The following are the components of each of the packaging bundles.

Base Common Services

CAECIS
CAICCI
CAIENF
CAIRIM
CA Health Checker
CA Master
CA MSM

Optional Common Services

CA Easytrieve
CA-GSS
CA-GREXX
CA-XPS
CAIENF/CICS
CAIENF/CICS Spawn
CAIENF/DB2
CAIENF/USS
CAISDI
Apache Tomcat

Legacy Common Services

CA-C Runtime

CA-L-Serv

CA Earl

SRAM Service

Viewpoint

Mainframe CA NSM Common Services (MFNSM)

Agent Technology

Event Management

Event Management Utilities

Software Services

CA Common Services for z/OS Software Services consist of a number of software components that perform various functions.

Base Common Services

The components included in the Base Common Services packaging bundle are described in this section. All components found in this bundle must be installed.

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.

Four integral parts of CAIRIM are CAISSF, CA LMP, Serviceability, and zIIP Enablement Services.

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 sign-in, 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.

Serviceability

Includes the following functionality that can be taken advantage of by CA products:

- Verify that messages associated with an error or failure provide clear information for use in problem determination.
- Capture necessary documentation (DUMPS, SYSLOG, LOGREC, TRACE DATA).
- Identify ownership of resources (Eyecatchers).
- Simplify identification of preventive and corrective maintenance.

zIIP Enablement Services

zIIP Enablement Services can be exploited by some CA products under some circumstances to have some of the CA product code eligible to run on zIIP processors.

CAIENF (Base)

CAIENF (Base) is a software component that provides comprehensive operating system interfacing services to any of the CA 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 software generated event information to be driven through a standard interface, simplifying multiple product to product interfaces and associated maintenance that would otherwise be necessary.

CAICCI

CAICCI is a software component that 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.

CAECIS

CA Examine Common Inventory Service (CAECIS) is a support services component that provides a tool for CA Support to collect and report on installed instances of CA products at a particular customer site. This service is useful for troubleshooting.

CA Health Checker Common Service

CA Health Checker common service provides a simple and consistent method for CA products to create health checks to run under the IBM Health Checker for z/OS. The IBM Health Checker for z/OS helps you identify potential problems in your z/OS environment by checking system or product parameters and system status against recommended settings. CA z/OS product health checks are automatically activated on the target system when the product is started on a system where the following components are installed and configured:

- CA Health Checker common service
- IBM Health Checker for z/OS

CA Master

The CAMASTER address space is an early IPL, limited function, permanent system address space which provides a set of operating system level services that may be utilized by any CA product. CAMASTER provides the capability for privileged CA components to:

1. Register non-space switch PC function routines that may be used instead of SVC routines, or to provide persistent access to component-specific function routines through the hardware assisted program-call mechanism.
2. Use persistent private storage provided by the CAMASTER address space (through CAMASTER provided space switch PC storage management services or explicit STORAGE OBTAIN using the CAMASTER ALET in AR ASC mode) to eliminate the need for using z/OS common storage resources such as ESQA or ECSA.
3. Provide a CA owned permanent system address space from which to anchor CA product objects, such as public access data spaces, and so forth.

In short, CAMASTER can help CA products reduce their ECSA usage, help them avoid using user SVCs, and help CA products avoid using the IBM *MASTER* address space.

CA MSM Common Services

CA MSM Common Services is a set of services provided by the CA Mainframe Software Manager (CA MSM) component of CA Mainframe 2.0, that enables a customer to take their installed software and deploy it onto systems across the enterprise.

Optional Common Services

The components included in the Optional Common Services packaging bundle are described in this section.

CAIENF/CICS

CAIENF/CICS is a support services component that provides the ability for CICS to participate in event monitoring.

CAIENF/CICS SPAWN

CAIENF/CICS SPAWN is a support services component that provides a communications facility, enabling CA applications to start CICS units of work from outside the CICS region. This facility provides a layer isolating the application software from CICS release dependencies.

CAIENF/DB2

CAIENF/DB2 is a software component that provides the ability for DB2 systems to participate in event monitoring.

CAIENF/USS

CAIENF/USS is a support services component that enables management applications to process system events occurring in the z/OS UNIX System Services subsystem. Management of z/OS UNIX System Services (CAIENF/USS) provides extensions to CA Common Services for z/OS that encapsulate and integrate the management of UNIX System Services applications on z/OS.

CAISDI

CAISDI is a support services component that provides a set of services that opens CA Service Desk requests from the z/OS environment. The requests can be opened directly by CA products or they can be opened on their behalf, depending on the requirements of each specific product using the interface.

CA-GREXX

CA-GREXX is a support services component that provides for implementation of the REXX programming language.

CA-GSS

CA-GSS is a support services component providing a simplified communication interface that lets various CA Technologies products communicate easily, seamlessly, and reliably, allowing quick access to information from various sources. CA-GSS provides connectivity by using a collection of one or more REXX subroutines that are edited, compiled, and executed as a single program.

CA-XPS

CA-XPS is a support services component that enables cross-platform scheduling for CA Technologies products including CA 7, CA Scheduler, and CA Jobtrac Job Management.

Easytrieve Service

Easytrieve Service is a support services component that provides a powerful productivity language for both business and information processing professionals containing easy-to-use information retrieval, sophisticated report writing, and comprehensive application development capabilities. The Easytrieve Service is a limited version of the full-featured CA Easytrieve product, which lets you modify the contents of an Easytrieve application that is provided with another CA Technologies product. If you have CA Easytrieve already installed at your site, you do not need to install the Easytrieve Service from CA Common Services.

Tomcat

Tomcat is the well known open source Web Application Management software from the Apache project. It is distributed with CA Common Services for software installation convenience. This saves the customer from having to download it from the Apache website and allows for sharing of the installed software between CA products. It is also placed under SMP/E control through the CA Common Services installation. For the associated Open Source License Agreement, see the appendix.

Legacy Common Services

The components included in the Legacy Common Services packaging bundle are described in this section.

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.

CA-L-Serv

CA-L-Serv is a support services component providing the CA-L-Serv services that are used by CA Technologies products including CA Endeavor Software Change Manager, CA Bundl, CA Balancing, CA-TPX, and CA MIC Message Sharing. These services include centralized logging and messaging facilities, VSAM file management, cross-system communications, and SQL table management.

Earl Service

Earl Service is a support services component that provides a user-friendly report-definition facility with the power of a comprehensive programming system. Earl Service allows you to modify and print the contents and layout of a pre-defined CA application report using English-like statements.

SRAM Service

SRAM Service is a support services component that allows the activation of several sorts concurrently, simplifying the data and logic flow. The incoming data to the sort can be manipulated as desired by the user program in a high-level language without the need for special exit routines.

Viewpoint

Viewpoint is a support services component that provides an SQL engine for PC-based workstation products. Workstation products can use Viewpoint to query z/OS product databases without knowledge of the underlying database structure.

Mainframe CA NSM Common Services

The management services components included in the Mainframe CA NSM (MFNSM) Common Services packaging bundle enable integrated administration of all IT resources in your enterprise, including network devices, databases, business applications for desktop systems and mainframes. These management services consist of the Agent Technology and Event Management components.

Agent Technology

The Agent Technology infrastructure enables the use of agents for the z/OS environment. The agents report to agent managers, which monitor and report the status of your resources and applications. It works with existing prepackaged z/OS agents such as the z/OS System Agent, CA IDMS, DB2 Agent, and CICS Agent, and other agents created to CA Common Services specifications.

Agent Technology works on a wide range of platforms and is deployable in traditional client/server, internet, and intranet environments. This versatility enables enterprise-wide monitoring and management of z/OS elements and enhances the ability of z/OS environments to participate in a true heterogeneous network.

Event Management

Event Management is a collection of management components that employ a single, easy to use graphical user interface (GUI) to monitor and administer different kinds of asynchronous events including SNMP traps, application events, and system events. Event Management makes it easy to collect related messages network wide for display at a single location or to send them to multiple locations as needed. The GUI included with Event Management on z/OS provides access to the Event Management Console, the management of Message Action records, and the management of calendars.

Note: Message Actions and calendars are Event Management options that require the installation of CA Datacom/AD.

CA Common Services for z/OS Event Management augments z/OS automation solutions such as CA OPS/MVS Event Management and Automation, by providing built-in access to a wide range of distributed events and by allowing actions to be triggered on any CA Common Services equipped platform. CA Common Services for z/OS provides event correlation and event processing and is fully integrated with CA Common Services Event Management facilities on other platforms. CA Common Services for z/OS also has several SDK functions, including command line and batch interfaces.

You can define a specific Event Management policy to do the following:

- Respond to messages.
- Suppress messages.
- Issue CA Common Services for z/OS commands.
- Start other programs or scripts.
- Send information to a network management or automation application such as CA OPS/MVS Event Management and Automation.
- Forward messages to other managed platforms.
- Issue commands to be executed on other platforms.
- Interpret the results of any action to decide whether additional actions are warranted.

Event Management may be configured to process messages on individual servers and redirect the messages to a central server or other servers. Event Management makes it easy to collect related messages network wide for display at a single location or to send to multiple locations as needed.

The Event Console Log provides a view of system events and processes as they occur across the network. All running programs and user processes can direct inquiries and informative messages to the log.

Calendars

Calendars is an Event Management option that makes it possible to determine a course of action based on when an event occurs. Actions can be triggered as events meet the general criteria and the date, day, and time criteria established through calendar profiles. The primary function of a calendar is identified in a naming scheme. CA Common Services for z/OS provides facilities to define and store as many calendars as required to meet your needs.

How the Installation Process Works

The following steps describe the installation process:

1. Prepare for the installation by confirming that your site meets all installation requirements.
2. Acquire the pax files that contain the CA Common Services you need at your site using one of the following methods:

Note: CA Common Services for z/OS Version 14.0 is bundled in four separate pax files, Base, Optional, Legacy, and MFNSM, For the contents of each pax file, see the Introduction chapter. You should install all the CA Common Services components contained in the Base CA Common Service bundle.

- CA MSM

Note: If you do not have CA MSM, you can download it from the Download Center at [the CA Support Online website](#). Follow the installation instructions in the CA Mainframe Software Manager documentation bookshelf on the CA Mainframe Software Manager product page.

- Pax files delivered using Electronic Software Delivery (ESD)

Follow the installation instructions in the CA Mainframe Software Manager documentation bookshelf on the CA Mainframe Software Manager product page.

You can download the CA Common Services pax files from the Download Center at the CA Support Online website.

- Pax files delivered on DVD

3. Install your product. Two methods of installation are supported, CA MSM and a pax enhanced SAMPJCL.

Both installation methods perform the same steps to install Common Services in that both methods allocate the required data sets, set up the SMP/E CSI, and perform SMP/E processing to Receive, Apply and Accept the CA Common Services products.

The difference in the two methods is CA MSM performs most of the work for you while using the SAMPJCL installation method requires you to edit and submit the various members found in the SAMPJCL data set.

4. Apply maintenance, if applicable.
5. Deploy.

Note: There are special considerations prior to deployment for Event Management and Agent Technology.

6. Configure the minimum settings for each CA Common Service that has configuration parameters.

Chapter 2: Preparing for Installation

This section describes what you need to know and do before you install the product.

This section contains the following topics:

[Component FMIDs](#) (see page 25)

[Software Requirements](#) (see page 27)

[Security Requirements](#) (see page 27)

[Storage Requirements](#) (see page 28)

Component FMIDs

Common Services component FMIDs (functional SYSMODS) are required for other components you install. Check your individual product documentation to determine which Common Services components are required.

The Version 14.0 FMIDs associated with each Common Services component are listed in the following table.

The Common Services Components are delivered in 4 bundles (pax files) known as BASE, OPTIONAL, LEGACY and MFNSM. All components found in the BASE pax file must be installed.

Component	FMIDs	Additional Required FMIDs
CA-C Runtime - CA C Language Runtime Facility LEGACY pax file	CAF3E00	None
CAIRIM - CA Resource Initialization Manager BASE pax file	CAS9E00	None
SRAM Service - CA Re-entrant Sorting Tool LEGACY pax file	CASR710	None
CAIENF - CA Event Notification Facility BASE pax file	CAW1E00	CAS9E00 *With CA Datacom/AD - CAF3E00, and CAW4E00
CAIENF/CICS - CA CAIENF CICS Interface OPTIONAL pax file	CAW3E00	CAS9E00 and CAW1E00

Component	FMIDs	Additional Required FMIDs
CAIENF/CICS SPAWN - CA CAIENF CICS-SPAWN Interface OPTIONAL pax file	CAW3E01	CAS9E00, CAW1E00, CAW3E00, and CAW4E00
CAICCI - CA Common Communications Interface with Secure Sockets Layer support BASE pax file	CAW4E00	CAS9E00, CAW1E00, and CEIOE00
CAIENF/DB2 - CA CAIENF DB2 Interface OPTIONAL pax file	CAW5E00	CAS9E00 and CAW1E00
Agent Technology - Mainframe Agent Support Facility MFNSM pax file	CB6DB30	None
CA-L-Serv - Cross System Messaging and File Services LEGACY pax file	CBUJE00	CAS9E00
CA-GSS - Communications interface OPTIONAL pax file	CBYSE00	CCF3E00
CA-GREXX - REXX EXEC environment OPTIONAL pax file	CCF3E00	None
CA-XPS - Cross-platform scheduling common component OPTIONAL pax file	CCF9E00	CAS9E00, CAW1E00, and CAW4E00
CAIENF/USS - CA CAIENF UNIX System Services interface OPTIONAL pax file	CCQ9E00	CAS9E00, CAW1E00, and CEIOE00
CAECIS - CA Examine Common Inventory Service* BASE pax file	CD0E350	None
Event Management - Event Management Facilities MFNSM pax file	CD5IB30	CAS9E00, CAW1E00, and CAW4E00 *With CA Datacom/AD - CAF3E00
Event Management Utilities - Event Management Utilities MFNSM pax file	CD5IB31	CD5IB30

Component	FMIDs	Additional Required FMIDs
Viewpoint - User Interface to CA system solutions LEGACY pax file	CDU4E00	CAS9E00 and CAF3E00
Easytrieve Service - CA productivity and Reporting Language Service OPTIONAL pax file	CDX8E00	None
CAISDI - CA Service Desk Simple Object Access Protocol OPTIONAL pax file	CDYFE00	CAS9E00, CAW1E00, and CAW4E00
CA Health Checker Common Service - CA system health check service BASE pax file	CEF5E00	None
CA Master BASE pax file	CEI0E00	None
CA MSM Common Services BASE pax file	CETN400	CAW4E00
Earl Service - CA Easy Access Report Language Reporting Service LEGACY pax file	CXE6100	None
Apache Tomcat OPTIONAL pax file	CEG1E00	None

* See the CA ENF chapter or the Event Management chapter of the *Best Practices Guide* to make a decision on whether CA Datacom/AD is required or not.

Software Requirements

The following software is required for CA Common Services for z/OS:

- An IBM Supported z/OS version.
- A supported release of one of the security subsystems, either CA Top-Secret, CA ACF2, or IBM RACF.

Security Requirements

Security requirements differ for different CA Common Services and are covered within the sections of this guide that discuss the particular CA Common Service.

Storage Requirements

Verify that the following storage requirements are met.

Target Libraries

As part of the SMP/E process for CA Common Services for z/OS, the following target libraries are updated with product-specific routines. You can determine the space allocation for each target library by reviewing the system requirements for each service you are installing.

There are three sets of target data sets. One set for BASE and OPTIONAL components, one set for LEGACY components, and one set for MFNSM components.

Older releases of CA products using CA Common Services may still refer to the CA Common Services load libraries with low-level qualifiers of CAILIB or CAILOAD and CAIPDSE. In an effort to standardize CA product libraries across the company, CAILIB/CAILOAD and CAIPDSE have been replaced by CAW0LOAD and CAW0PLD.

BASE and OPTIONAL Target Libraries

Note: For these descriptions, the default high-level qualifier for CA libraries is used.

CAI.CAW0CLS0

Common Service CLIST library

CAI.CAW0DCM

The ENF Authorized DCM load library.

CAI.CAW0EXP

Common Service Export Datacom Plan Library.

CAI.CAW0JCL

Common Service JCL Library.

CAI.CAW0LINK

This CA product authorized load library contains service-related executable modules for the BASE Common Services that must be in the system linklist.

CAI.CAW0LOAD

This CA product authorized load library contains service-related executable modules for the BASE and OPTIONAL Common Services. The deployed version of this library can optionally be in the system linklist.

CAI.CAW0LPA

The CA link pack area library contains service-related executable modules that must be in the system LPA list.

CAI.CAW0MAC

The CA Macro library contains the macros used in compiling service-related programs.

CAI.CAW0MSG0

Common Service Message Library.

CAI.CAW0OPTN

The CA product Options library contains sample parm members for CA Common Services for z/OS.

CAI.CAW0OPTV

Common Services variable length Option Library.

CAI.CAW0PLD

The CA product authorized PDSE load library contains service-related executable modules link edited in program format 3.

CAI.CAW0PNLO

Common Service Panel Library.

CAI.CAW0PROC

The CA Procedure library contains sample procedures for invocation of CA Common Services for z/OS and its related utilities.

CAI.CAW0SAMP

Common Service Sample Library.

CAI.CAW0SCRN

The CAIENF Utilities Panel library.

CAI.CAW0SDF

Common Services side decks.

CAI.CAW0SMPI

The CA-GSS Sample IMOD library contains sample REXX source.

CAI.CAW0SYSI

The CA-GSS system IMOD library contains source for internal IMODs used by CA-GSS.

CAI.CAW0XML

The CA MSM XML library.

CAI.CAW0XML0

The XML library for Remote Deployment.

CAI.CEG1ZFS1

The Tomcat zFS file system which holds the Apache Tomcat USS directories with binary executable files and base configuration files.

LEGACY target libraries

Note: For these descriptions, the default High Level Qualifier for CA libraries are used.

CAI.CCSCICS

The CA CICS Load library contains service-related CICS executable modules.

CAI.CCCSCLS0

Common Service CLIST.

CAI.CCCSJCL

Common Service JCL Library.

CAI.CCCSLINK

This CA product authorized load library contains service-related executable modules for the Legacy Common Services that must be in the system linklist.

CAI.CCCSLOAD

This CA product authorized load library contains service-related executable modules for the Legacy Common Services. The deployed version of this library can optionally be in the system linklist.

CAI.CCCSMAC

The CA Macro library contains the macros used in compiling service-related programs.

CAI.CCCSOPTN

The CA product Options library contains sample parm members for CA Common Services for z/OS.

CAI.CCCSPNLO

Common Service Panel Library.

CAI.CCCSPROC

The CA Procedure library contains sample procedures for invocation of CA Common Services for z/OS and its related utilities.

CAI.CCCSSRC

The CA Source library contains the service-related source code.

CAI.VPOINT.CHOICES

The ViewPoint Choices library contains service-related ViewPoint lists.

CAI.VPOINT.DIALOG

The ViewPoint Dialog library contains service-related ViewPoint dialogs.

CAI.VPOINT.HELP

The ViewPoint Help library contains service-related ViewPoint help.

CAI.VPOINT.MESSAGE

The ViewPoint Message library contains service-related ViewPoint messages.

CAI.VPOINT.PANEL

The ViewPoint Panel library contains service-related ViewPoint panels.

CAI.VPOINT.SQL

The ViewPoint SQL library contains service-related ViewPoint SQL statements.

CAI.VPOINT.TEMPLATE

The ViewPoint Template library contains service-related ViewPoint templates.

MFNSM Target Libraries

Note: For these descriptions, the default High Level Qualifier for CA libraries are used.

CAI.CNSMJCL

Common Service JCL Library

CAI.CNSMLOAD

This CA product authorized load library contains service related executable modules for the Mainframe NSM Common Services. The deployed version of this library can optionally be in the system linklist.

CAI.CNSMOPTV

Common Services variable length Option Library.

CAI.CNSMPLD

The CA product authorized PDSE load library contains service related executable modules link edited in program format 3.

CAI.CNSMPROC

The CA Procedure library contains sample procedures for invocation of CA Common Services for z/OS and its related utilities.

CAI.CNSMSDF

Common Services side decks.

CAI.CNSMSRCV

Common Services variable length source library.

CAI.MIBLIB

The Agent Technology MIB source library.

CAI.RO.CB6DZFS

AGENT Technology Read Only zFS.

CAI.RW.CB6DZFS

AGENT Technology Read/Write zFS.

CAI.RO.CD5IZFS

Event Management Read Only zFS.

CAI. RW.CD5IZFS

Event Management Read/Write zFS.

Non-SMP/E Product Specific Data Sets

The following are not SMP/E data sets, but are specific to the named products:

CAI.CAIEVENT

CAISDI Event library.

CAI.CETN400.RW.CAIZFS

The zFS file system used by CA MSM Common Services.

CAI.SAMPIMOD

CA-GSS VSAM IMOD file for the SAMPLE ISET library.

CAI.SYSIMOD

CA-GSS VSAM IMOD file for the INTERNAL ISET library.

CAI.VPOINT.PROFILE

Viewpoint Profile Library.

Comprehensive View of Storage Requirements

The following lists the minimum storage requirements for each component within the target library and does not necessarily represent the actual target library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a BLOCK SIZE of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Component	Tracks	Directory Blocks
CAI.CAWOCLS0	0	CA-GSS	2	2
		CAECIS	1	1
		CAIENF	1	1
		CAIRIM	1	1
CAI.CAW0DCM	6144	CA-XPS	1	1
		CAICCI	1	1
		CAIENF	1	1
		CAIENF/CICS	1	1
		CAIENF/USS	1	1
CAI.CAW0EXP	0	CAIENF	5	1
		CA MSM Common Services	47	1
CAI.CAW0JCL	0	CA-GSS	1	1
		CA-XPS	1	1
		CAECIS	1	1
		CAICCI	1	1
		CAIENF	6	5
		CAIRIM	2	2
		CAISDI	1	1
		EASYTREIVE	2	1
		CA MSM Common Services	1	1
CAI.CAW0LINK	6144	CA-HEALTH-CHECKER	16	3
		CA-MASTER	11	7
		CAICCI	1	1
		CAIENF	1	1
		CAIRIM	8	3

Library Name	Block Size	Component	Tracks	Directory Blocks
CAI.CAW0LOAD	6144	CA-GREXX	6	1
		CA-GSS	108	5
		CA-XPS	6	3
		CAECIS	26	1
		CAICCI	65	5
		CAIENF	31	20
		CAIENF/CICS	11	2
		CAIENF/CICS-SPAWN	6	2
		CAIENF/DB2	5	1
		CAIENF/USS	12	9
		CAIRIM	16	5
		CAISDI	16	3
		EASYTRIEVE	36	27
		CA MSM Common Services	8	2
CAI.CAW0LPA	6144	CAIRIM	1	1
CAI.CAW0MAC	0	CA-GSS	3	1
		CAIRIM	1	1
		CAISDI	2	1
		EASYTRIEVE	4	1
CAI.CAW0MSG0	0	CA-GSS	1	1
		CAECIS	1	1
CAI.CAW0OPTN	0	CA-GSS	6	8
		CA-XPS	2	1
		CAICCI	247	2
		CAIENF	2	2
		CAIRIM	2	3
		CAISDI	3	3
		CA MSM Common Services	1	1
CAI.CAW0OPTV	25600	CAIENF	2	1
		CAISDI	1	1
CAI.CAW0PLD	6144	CAICCI	39	
		CAIENF	15	
		CAISDI	18	
		CA MSM Common Services	171	

Library Name	Block Size	Component	Tracks	Directory Blocks
CAI.CAW0PNLO	0	CA-GSS	20	82
		CAECIS	6	2
CAI.CAW0PROC	0	CAI-GSS	1	1
		CA-XPS	1	1
		CAECIS	1	1
		CAICCI	2	2
		CAIENF	2	2
		CAIRIM	1	2
		CAISDI	1	1
		CA MSM Common Services	1	1
CAI.CAW0SAMP	0	CA-GSS	2	1
		CAIENF	1	1
		CAIRIM	7	2
CAI.CAW0SCRN	4104	CAIENF	8	23
CAI.CAW0SDF	0	CAICCI	1	1
		CAIRIM	1	1
		CA MSM Common Services	4	1
CAI.CAW0SMPI	3600	CA-GSS	3	6
CAI.CAW0SYSI	3600	CA-GSS	65	58
CAI.CAW0XML	32760	CAIRIM	12	1
CAI.CAW0XML0	32760	CA MSM Common Services	245	4
CAI.CCCSCICS	6144	CA-C Runtime	8	4
		Viewpoint	14	1
CAI.CCCSCLSO	0	Viewpoint	1	1
CAI.CCCSJCL	0	CA-C Runtime	1	1
		CA-L-SERV	1	2
		EARL	1	1
		SRAM-Service	1	1
		Viewpoint	2	1
CAI.CCCSLINK	6144	CA-C Runtime	26	9
		SRAM-Service	2	2

Library Name	Block Size	Component	Tracks	Directory Blocks
CAI.CCCSLOAD	6144	CA-L-SERV	20	3
		EARL	19	1
		Viewpoint	91	9
CAI.CCCSMAC	0	CA-CRruntime	1	1
		EARL	2	1
		SRAM-Service	1	1
		Viewpoint	5	1
CAI.CCCSOPTN	0	CA-CRruntime	1	1
		CA-L-SERV	4	4
		EARL	1	1
CAI.CCCSPNLO	0	Viewpoint	2	1
CAI.CCCSPROC	0	CA-L-SERV	1	1
CAI.CCCSSRC	0	EARL	1	1
CAI.CEG1ZFS1	-	Tomcat	50 cyls	-
CAI.CNSMJCL	0	Agent Technology	3	2
		Event Management	6	2
		Event Management/Utilities	1	1
CAI.CNSMLOAD	6144	Agent Technology	103	5
		Event Management	3	1
		Event Management/Utilities	1	1
CAI.CNSMOPTV	25600	Agent Technology	1	1
CAI.CNSMPLD	6144	Event Management/Utilities	11	
CAI.CNSMPROC	0	Agent Technology	1	1
		Event Management	1	1
CAI.CNSMSDF	0	Agent Technology	8	1
		Event Management	1	1
		Event Management/Utilities	1	1
CAI.CNSMSRCV	25600	Agent Technology	2	1
CAI.MIBLIB	25600	Agent Technology	15	1
CAI.RO.CB6DZFS	-	Agent Technology	30 cyls	-
CAI.RO.CD51ZFS	-	Event Management	700 cyls	-
CAI.RW.CB6DZFS	-	Agent Technology	30 cyls	-

Library Name	Block Size	Component	Tracks	Directory Blocks
CAI.RW.CD5IZFS	-	Event Management	200 cyls	-
CAI.VPOINT.CHOICES	4104	ViewPoint	1	1
CAI.VPOINT.DIALOG	8204	ViewPoint	15	5
CAI.VPOINT.HELP	4104	ViewPoint	38	28
CAI.VPOINT.MESSAGE	4104	ViewPoint	6	8
CAI.VPOINT.PANEL	4104	ViewPoint	6	6
CAI.VPOINT.SQL	0	ViewPoint	2	1
CAI.VPOINT.TEMPLATE	0	ViewPoint	1	1

The following are for non-SMP/E Product Specific Data Sets.

Library Name	Block Size	Component	Tracks	Directory Blocks
CAI.CAIEVENT	8000	CAISDI	68	50
CAI.CAITXLIB	32760	Agent Technology Event Management	10 cyls 10 cyls	10 10
CAI.RW.CETNZFS	-	CA MSM Common Services	500 cyls	
CAI.SAMPIMOD	-	CA-GSS	1 cyl	-
CAI.SYSIMOD	-	CA-GSS	4 cyls	-
CAI.VPOINT.PROFILE	0	ViewPoint	5	10

Component Installation Requirements

This section lists the installation requirements and distribution libraries required for each CA Common Services component.

Agent Technology Requirements

Agent Technology has the following installation requirements:

- An IBM supported z/OS version.
- UNIX System Services (also known as OpenEdition or OMVS) in full-function mode and zFS physical file system implemented.
- Any supported version of TCP/IP.
- Any supported version of IBM C/C++ for z/OS if you are using the example agent or writing your own custom agents.
- Disk space: (RO and RW zFSs) approximately 60 cylinders.
- Security definitions permitting a new Agent Technology user to be created.

The following lists the minimum storage requirements for each Agent Technology distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

library Name	Block Size	Tracks	Directory Blocks	Description
CAI.AB6DJCL	0	2	2	JCL library
CAI.AB6DMIB	25600	15	1	MIB library
CAI.AB6DMOD	6144	160	5	Module library
CAI.AB6DOPTV	25600	1	1	Source library
CAI.AB6DPROC	0	1	1	Procedure library
CAI.AB6DSDF	0	8	1	Side Decks
CAI.AB6DSRCV	25600	2	1	Source library
CAI.AB6DZFS	32760	144	1	ZFS Element library

Prepare to Install Agent Technology

Before installing Agent Technology, perform the following tasks to make sure your system is prepared.

1. Note the IP address of each remote system that is to manage z/OS system agents and receive mainframe traps.
2. Verify the TCP/IP procedures for your site:

If the data set prefix of your TCP/IP configuration data sets is not TCPIP (the IBM default) ensure the //SYSTCPD DD statement points at a data set that contains a DATASETPREFIX statement identifying your alternate prefix.

Note the TCP/IP data set name from the //SYSTCPD DD statement.
3. Ensure that the following data sets exist and are cataloged to accompany your other TCP/IP data sets:
 - ETC.SERVICES
 - HOSTS.ADDRINFO
 - HOSTS.SITEINFO
4. Enable Uppercase-Lowercase support on all terminals that will be used during the installation.

CA-C Runtime Requirements

CA-C Runtime works with an IBM supported z/OS version.

CA-C Runtime supports the following products:

- CA Roscoe Interactive Environment (ETSO) all supported releases
- CICS (z/OS) all supported releases
- TSO all supported releases
- IMS/DC all supported releases
- z/VM all supported releases

The following is a list of the minimum storage requirements for each CA-C Runtime distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.AAF3CICS	6144	8	4	CICS load library
CAI.AAF3JCL	0	1	1	JCL library
CAI.AAF3MAC	0	1	1	MACRO library
CAI.AAF3MOD	6144	35	9	Module library
CAI.AAF3OPTN	0	1	1	Option library

CA-GREXX Requirements

CA-GREXX installation requires an IBM supported z/OS version.

The following lists the minimum storage requirements for each CA-GREXX distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.ACF3MOD0	6144	6	3	Module library

CA-GSS (System Interfaces) Requirements

CA-GSS has the following installation requirements:

- An IBM supported z/OS version.
- CA-GSS must be installed into an APF authorized library. The CA-GSS routines can be executed from a STEPLIB concatenation or from a LNKLST concatenation.
- Due to cross-memory communication requirements, CA-GSS makes itself non-swappable.
- Since CA-GSS services multiple applications and tasks, the CA-GSS dispatching priority must be greater than or equal to the highest dispatching priority of any task requesting CA-GSS services.

The following lists the minimum storage requirements for each CA-GSS distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.ABYSCLSO	0	2	2	CLIST library
CAI.ABYSJCL	0	1	1	JCL library
CAI.ABYSMAC	0	3	1	MACRO library
CAI.ABYSMODO	6144	151	100	Module library
CAI.ABYSMMSGO	0	1	1	Message library
CAI.ABYSOPTN	0	6	8	Option library
CAI.ABYSPNLO	0	20	82	Panel library
CAI.ABYSPROC	0	1	1	Procedure library
CAI.ABYSSAMP	0	10	1	Sample library
CAI.ABYSSMPI	3600	5	2	SAMP IMOD library
CAI.ABYSSYSI	3600	100	11	System IMOD library

Permanent VSAM IMOD libraries required for CA-GSS are shown in the following table:

ISET Library Name	Cylinders	Description
CAI.SAMPIMOD	1	SAMPIMOD library

ISET Library Name	Cylinders	Description
CAI.SYSIMOD	4	SYSIMOD library

CA-GSS Memory Requirements

CA-GSS memory can be classified based on its function. The types of memory allocated are:

- System level memory - Allocated once and retained until the CPU is IPLed.
- Primary CA-GSS memory - Allocated only by the primary (or only) CA-GSS Subsystem.
- ISERVE memory - Allocated by each CA-GSS Subsystem that runs on the system, including the primary subsystem.

System Level Memory

CA-GSS requires one system linkage index (LX) to provide for Program Call (PC) routines. This is obtained from the system automatically at initialization. If CA-GSS is restarted, the previously obtained LX is reclaimed.

The first time you start CA-GSS after performing an IPL, CSA and ECSA areas are reserved. These areas are obtained only once during an IPL (unless you restart CA-GSS, in which case a second set of areas is obtained). These areas are retained until the next IPL. The storage required is:

- 40 bytes of CSA for a subsystem anchor
- 23.6 KB of ECSA for common routines and data tables

These areas are used by CA-GSS background tasks and are shared by all address spaces using CA-GSS services.

If you reload CA-GSS (PGM=GSSLOAD,PARM=RELOAD), a new ECSA area is allocated and the old area is retained. This prevents the possibility of freeing an area that is still in use by another address space. If you reload CA-GSS a third time, the original storage is freed and the second load is retained. Only the latest two versions of CA-GSS are retained.

Primary CA-GSS Memory

The CA-GSS primary subsystem requires the following storage. All storage estimates are for the base configuration and reflect only storage explicitly used by CA-GSS. Storage used by other CA Technologies products, the operating system, VTAM, and other entities is not included.

- 3 MB (minimum) private storage. Except for I/O buffers and interfaces to some external routines, this storage resides above 16 MB line.
- 160 bytes of CSA for a subsystem anchor and related storage.
- 120 KB of ECSA. This storage is used for buffers, communication, and PC routines. This storage is released, recovered, or reused upon CA-GSS termination or restart.

ISERVE Memory

Each executing copy of ISERVE (including the primary) requires:

- 120 bytes of CSA
- 95.4 KB of ECSA
- 3 MB of private area storage above the 16 MB line

All CA-GSS programs are re-entrant, AMODE 31, and RMODE ANY.

ISERVE-acquired ECSA is retained at termination but released during the next initialization of an ISERVE with an identical subsystem ID. This ensures that cross-memory ISERVE users are not impacted.

The ISERVE CSA usage includes 40 bytes used for a subsystem anchor block. Whether pre-defined by the installation or dynamically obtained, this block is retained until the next IPL and is reclaimed upon each ISERVE restart.

Each CA Technologies product that is used in conjunction with ISERVE using REXX ADDRESS commands may require additional CSA or ECSA. Check the appropriate documentation for each installed product to determine any additional storage requirements.

The amount of private storage ISERVE requires depends on the options you choose and the amount of traffic on your system. The recommended starting point is 4 MB.

Resource Consumption

Depending on installation-controlled tracing options, significant SPOOL space may be used. Spooled log files may be closed and spun at any time by operator command.

During operation, CA-GSS performs minimal I/O. Therefore, the location of data sets is generally not a concern.

CPU utilization should not be significant. While it is possible to cause excessive CPU consumption by making incorrect or inappropriate requests to CA-GSS, internal resource-limiting techniques minimize this possibility.

System Security

IMODs executing in a CA-GSS address space can access and update a variety of data sets and data areas. To prevent unauthorized activity, CA-GSS supports system security software that is compatible with the IBM System Authorization Facility (SAF).

In z/OS, each task operates under control of an Accessor Environment Element (ACEE), which controls access to all resources. SAF-compatible security software maintains the ACEE based on a user ID and ensures that the necessary checks are provided.

CA-GSS ensures that an appropriate ACEE is in place for each executing IMOD and that all services invoked on behalf of the IMOD execute under the scope of that ACEE.

User IDs

CA-GSS needs two valid user IDs for proper security enforcement:

- The primary user ID assigned by the system to the CA-GSS started task or job
- A user ID to use as a default ID for service requests that have no associated user ID or for which CA-GSS cannot determine the associated user ID

You must define this user ID to your security software and define it to CA-GSS through the SECURITY initialization parameter. Since this is the default user ID, it should be limited in scope.

Note: For more information about CA-GSS initialization parameters, see the *Reference Guide*.

CAGSS User ID

Many installations routinely do not assign a specific user ID to started tasks. You should assign one, at least for CA-GSS.

CA-GSS executes under its own user ID during initialization and when performing some housekeeping functions.

IMODs execute under authority of the CA-GSS user ID when performing initialization and housekeeping functions and when no other valid user ID can be determined.

IMOD User IDs

When an IMOD task is created, CA-GSS assigns it a valid user ID and obtains an ACEE for it.

In most cases, the user ID is taken from the task that triggered the IMOD task. For example, a request from a TSO user (IMOD editor or SRVCALL() function) is assigned the TSO user ID.

In some cases, CA-GSS cannot determine which user ID to use. For example, this can happen if a started task that has no user ID issues a WTO that, in turn, triggers an IMOD. In these cases, CA-GSS assigns the CA-GSS default user ID to the IMOD task.

Note: If no default user ID was defined at CA-GSS initialization, the IMOD task executes under the scope of the primary user ID of the CA-GSS address space.

How CA-GSS Chooses a User ID for an IMOD

The following table contains additional information about how CA-GSS determines which user ID an IMOD executes under:

Type of IMOD	How CA-GSS Determines the User ID
IMODs that support operator commands	If you have defined a user ID through the COMMAND parameter in the PARMLIB data set, CA-GSS uses it. Otherwise, CA-GSS uses its default user ID.
IMODs triggered by WTOs	If you have defined a user ID through the WTO parameter in the PARMLIB data set, CA-GSS uses it. If not, CA-GSS tries to determine and use the user ID of the WTO issuer. As a last resort, CA-GSS uses its default user ID. Note: During execution, an IMOD task may switch user IDs by supplying a new user ID and its associated password to the SECURITY() function.

Type of IMOD	How CA-GSS Determines the User ID
WTO-triggered IMODs with ASID numbers matching those on the MONITOR command	CA-GSS tries to determine and use the user ID of the WTO issuer. Otherwise, CA-GSS uses its default user ID.
IMODs supporting the Logon Facility	If a user ID and password are provided, CA-GSS uses them. Otherwise, CA-GSS uses its default user ID.
Server IMOD	CA-GSS uses the user ID of the IMOD that started it.
ADDRESS environments and subtasks	CA-GSS uses the user ID of the IMOD that invokes them. Note: If a subtask is reassigned to another IMOD, the user ID changes.

CA-L-Serv Requirements

CA-L-Serv works with an IBM supported z/OS version.

The following lists the minimum storage requirements for each CA-L-Serv distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.ABUJCL	0	1	2	JCL Library
CAI.ABUJMOD	6144	64	23	Module Library
CAI.ABUJOPTN	0	4	4	Options Library
CAI.ABUJPROC	0	1	1	Procedure Library

XCF Communications Considerations

If you plan to use XCF communication between systems, ensure that you have installed CAIRIM (CAS9E00) and that the load library is accessible to CA-L-Serv.

Running the CAS9 procedure is not necessary to the execution of CA-L-Serv.

CA-L-Serv does not require an LMP key.

z/OS Requirements

CA-L-Serv must reside in an authorized load library.

Since CA-L-Serv is installed into a different load library from the rest of Common Services, note the following information:

- Both the CA-L-Serv and Common Services running load libraries must be APF-authorized.
- Users of the XCF component of the Communications Server must ensure that CA-L-Serv has access to the Common Services CAWLOAD data set.
- The Common Services CAWLOAD data set must be accessible to CA-L-Serv from the LINKLIST or the STEPLIB concatenation in the CA-L-Serv startup procedures.

Virtual Storage Requirements

CA-L-Serv requires the following amounts of virtual storage:

Type of Storage	Minimum Virtual Storage
CSA	3 KB of CSA and 2 KB of extended CSA
ESQA	Requirements vary from 4 KB to over 500 KB depending on the size and number of VSAM buffer pools

CSA storage is not released when CA-L-Serv is shut down but will be reused when CA-L-Serv is restarted (provided REUSE=YES is specified in the startup procedure).

ESQA storage is used by VSAM and concerns only users of the File Server.

CA-L-Serv SQL Dictionary

The SQL Server requires the following VSAM database:

Database	Description
SQL dictionary	Contains the definitions of the SQL tables that are managed by the SQL Server.

Storage requirements for the SQL dictionary vary depending on the requirements of your site.

Note: This file is necessary only for users of the SQL Server.

CA-XPS Requirements

CA-XPS (Cross-Platform Scheduling Common Component) provides CA 7, CA Scheduler, and CA Jobtrac Job Management with the capability to accept scheduling requests from other platforms. In some documentation it is referred to as the XPS ROUTER.

For CA 7 or CA Scheduler, the CA-XPS code executes in the CA 7 or CA Scheduler address space. For CA Jobtrac Job Management, the CA-XPS code executes in the CA-GSS address space.

For information about implementing cross-platform scheduling using CA-XPS, see one of the following guides:

- *CA NSM CA 7 Interfaces Guide*
- *CA NSM CA Scheduler Interfaces Guide*
- *CA Jobtrac Job Management Installation and Maintenance Guide*

The following lists the minimum storage requirements for each CA-XPS distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.ACF9JCL	0	1	1	JCL Library
CAI.ACF9MOD0	6144	20	3	Module Library
CAI.ACF9OPTN	0	1	1	Option Library
CAI.ACF9PROC	0	1	1	Procedure Library

CAECIS Requirements

The CA Examine Common Inventory Service works with an IBM supported z/OS version.

The following lists the minimum storage requirements for each CAECIS distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.ADOECLSO	0	1	1	CLIST library
CAI.ADOEJCL	0	1	1	JCL library
CAI.ADOEMOD	6144	40	15	Module library
CAI.ADOEMSGO	0	1	1	Message library
CAI.ADOEPNLO	0	4	2	Panel library
CAI.ADOEPROC	0	1	1	Procedure library

CAICCI Requirements

CAICCI has the following installation requirements:

- An IBM supported z/OS version.
- CAICCI must be installed into an APF authorized library. This library must be the same library that was used for the CAIENF service installation.
- CAICCI supports various control options, which may be tailored to meet the individual data center requirements.

- CAICCI requires 172 KB of ECSA for modules and global control blocks. For each concurrent host program, CAICCI requires an additional 304 bytes of ECSA. The amount of ECSA required varies depending on the individual data center configuration and general activity. An estimate may be achieved by the following formula:

$$172\text{K bytes} + (\text{Number of concurrent host-related programs using CAICCI}) * (308 \text{ bytes}) + 328 * (\text{Number of sessions in a multi-CPU environment})$$

Determine the number of concurrent host-related (application) programs using CAICCI from the ENF STATUS,CCIR operator command, which displays the general status of the CAICCI resources.

Message CAS9701I displays the number of pending receivers (programs using CAICCI).

- In a multi-CPU environment, add 258 KB for each CPU defined.
- The ID associated with the CCITCP, CCITCPGW, CCISSL, and/or CCISSLGW started tasks must have a valid security OMVS segment defined.

The following lists the minimum storage requirements for each CAICCI distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Tracks	Directory Blocks	Description
AAW4JCL	0	1	1	JCL library
AAW4MOD	6144	150	9	Module library
AAW4OPTN	0	246	2	Option library
AAW4PROC	0	2	2	JCL procedure library
AAW4SDF	0	1	1	Side deck file

CAIENF Requirements

CAIENF has the following installation requirements and considerations:

- An IBM supported z/OS version.
- The ID associated with the ENF started task must have a valid security OMVS segment defined.
- CAIENF must be installed into an APF authorized library. LINKLIST is not required but is recommended, to prevent STEPLIB problems.

- CAIENF runs as a started task. A procedure containing the CAIENF started task JCL must be defined in any PROCLIB data set. The sample provided on the CA Common Services for z/OS tape can be tailored to the requirements of the data center.

CAIENF supports various control options that can be tailored to meet the requirements of the individual data center.

Note: For information about tailoring CAIENF control options, see the *Administration Guide*.

- CAIENF requires common storage for modules and global control blocks. The amount of CSA required varies depending on the configuration of the individual data center; however, 90 KB can be used as a rough estimate.

Approximately 50% of the CSA required by CAIENF is allocated in ECSA. The amount of storage that the CAIENF address space requires varies depending on overall system load, recording options, and database service times. The CAIENF address space requires approximately 3-4 MB of private area modules and work areas, as well as an average of 256 bytes for each queued event request. The number of queued event requests can be determined from the ENF STATUS operator command. CAIENF also requires approximately 4 KB in each application address space, although this amount varies depending on application structure.

- CAIENF dynamically installs SVC 159 for ENF/CICS communication purposes. No SVC number selection is required.
- ACF2 users must create a logon ID (LID) for the CAIENF started task.
- To enable CAIENF DCM modules for handling events, the DCM modules must be specified with a DCM statement in the ENF configuration member ENFPARM. For DCM statement specification details, see the *Reference Guide*, section CAIENF Control Options.

Note: With the switch to CA Datacom/AD, the ENFDB DD statement is no longer needed in the ENF started task JCL.

The following lists the minimum storage requirements for each CAIENF distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.AAW1CLS0	0	1	1	CLIST Library
CAI.AAW1EXP	0	5	1	EXPORT Library
CAI.AAW1JCL	0	5	5	JCL Library

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.AAW1LOAD	6144	1	1	Load Library
CAI.AAW1MOD	6144	100	26	Module Library
CAI.AAW1OPTN	0	1	2	Option Library
CAI.AAW1OPTV	25600	2	1	Variable Length Option Library
CAI.AAW1PROC	0	2	2	Procedure Library
CAI.AAW1SAMP	0	1	1	Sample Library
CAI.AAW1SCRN	4104	8	23	Screen

CAIENF/CICS Requirements

CAIENF/CICS has the following installation requirements:

- CAIENF/CICS works with all releases of CICS TS generally supported by IBM.
- CAIENF/CICS has a subtask that runs within the CAIENF address space. The primary function of the subtask is to keep track of all CICS regions and to handle operator commands. A procedure containing the CAIENF started task JCL must be defined in any PROCLIB data set. The sample provided on the CA Common Services for z/OS tape may be tailored to your data center requirements.
- CAIENF/CICS supports various control options that can be tailored to meet the individual data center requirements.
- The CAS9DCM2 DCM module must be processed by ENF with a DCM(CAS9DCM2) ENF parameter in the ENFPARMS file. No database is required but the DCM must be installed.
- The primary function of the CAIENF/CICS Interface is to provide one common service for handling CICS release dependencies. This alleviates the effects of new CICS releases on CA CICS solutions.
- The CAIENF/CICS Interface consists of a different set of load modules for each CICS release. These modules are loaded into CSA when CAIENF is started. Optionally, the appropriate load module may be loaded into the CICS Private Area. Each module uses approximately 40 KB of CSA or CICS Private Area, depending on where it is loaded.

- When a CICS Region is started, CAIENF/CICS checks for the existence of a DDNAME of CENFLIB. If this DDNAME is defined, CAIENF/CICS loads the appropriate modules into the CICS Private Area. If the DDNAME of CENFLIB is not defined, CAIENF/CICS tries to load the modules from STEPLIB. If the modules are found in STEPLIB, they are loaded into the CICS Private Area. Lastly, CAIENF/CICS attempts to find the modules in CSA.
- To use this feature to apply maintenance on the global CAIENF/CICS modules, enter the ENF REFRESH(CAS9Cxx) control option, where xx is the release of CICS.

The following lists the minimum storage requirements for each CAIENF/CICS distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.AAW3MOD	6144	30	34	Module Library

CAIENF/CICS SPAWN Requirements

CAIENF/CICS SPAWN has the following installation requirements:

- CAIENF/CICS SPAWN works with all releases of CICS TS generally supported by IBM.
- CAIENF/CICS SPAWN supports various control options that can be tailored to meet the individual data center requirements.
- CAICCI is required software and needs to be installed prior to the installation of CAIENF/CICS SPAWN.

Note: For more information about CAIENF/CICS SPAWN, see the *Administration Guide*.

The primary function of CAIENF/CICS SPAWN is to let CA solutions start CICS units of work from outside the CICS region. The facility provides a layer that isolates the application software from the CICS release. CAICCI is the proprietary communications vehicle that enables this facility.

When a CICS region is started, CAIENF/CICS SPAWN checks for the existence of a DDNAME of CENFLIB. If this DDNAME is defined, CAIENF/CICS SPAWN loads the appropriate modules into the CICS Private Area. If the DDNAME of CENFLIB is not defined, CAIENF/CICS SPAWN tries to load the modules from STEPLIB. If the modules are found in STEPLIB, they are loaded into the CICS Private Area. Lastly, CAIENF/CICS SPAWN attempts to find the modules in CSA.

The following lists the minimum storage requirements for each CAIENF/CICS SPAWN distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.AAW3MOD	6144	12	12	Module Library

CAIENF/DB2 Requirements

CAIENF/DB2 has the following installation requirements:

- CAIENF/DB2 supports all DB2 releases from DB2 R2.3.
- The load module DSNXAUTH cannot be loaded into LPA; if loaded, an ABEND will occur when CAIENF/DB2 is initialized. CAIENF/DB2 requires DSNXAUTH to be loaded into the private area so that intercepts can be managed by subsystem (not all subsystems require the intercept).
- The primary function of the CAIENF/DB2 interface is to handle release dependencies between different levels of DB2. This anticipates and prevents the need for changes to CA DB2 solutions that are otherwise necessary with each new release of DB2.

- CAIENF/DB2 uses approximately 20 KB of CSA for its own load modules. Additional storage, for units of work data, is obtained from extended CSA whenever possible, although some work storage is obtained from the individual user private area. The amount of extended CSA used is a function of the size and workload of the individual DB2 system.
- When a DB2 subsystem is started, CAIENF/DB2 gets control and queries CAIENF based applications for required exit points. Only those exit points actually required are installed. If no exit points are required, only the primary CAIENF/DB2 anchor is installed in the system. This anchor is not accessed again until the DB2 subsystem is terminated.

Note: For more information about CAIENF/DB2, see the *Administration Guide*.

The following lists the minimum storage requirements for each CAIENF/DB2 distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.AAW5MOD	6144	10	4	CAIENF/DB2 Module Library

CAIENF/USS Requirements

CAIENF/USS has the following installation requirements:

- An IBM supported z/OS version.
- The ENF address space must run with root privileges under UNIX System Services. The security ID associated with the ENF started task requires:
 - A superuser ID (UID 0), or permission to the IBM Facility resource BPX.SUPERUSER.
 - A valid group ID (GID), home directory, and shell program.
 - Permission to the IBM Facility resource BPX.DAEMON, if you have defined this resource in your installation.

Note: For more information, see your security product documentation.

- Products that use the CAIENF/USS component also have a Data Control Module (DCM). The CAIENF/USS DCM and all product-specific DCMs must be specified with a DCM statement in the ENFPARMS parameter configuration member. For DCM statement specification details, see the *Reference Guide*, section CAIENF Control Options.
- To enable CAIENF/USS event intercepts, the ENF/USS DCM, CARRDCM0, must be specified with a DCM statement in the ENF configuration member ENFPARM.
- For best performance, CAIENF/USS requires that you define a new object to VLF (Virtual Lookaside Facility).

Define a New Object to VLF

Defining a new object to the Virtual Lookaside Facility (VLF) may help improve the performance of certain CA Common Services for z/OS components.

To define a new object to VLF, add an entry to the COFVLFxx member of SYS1.PARMLIB, where xx is the VLF identifier assigned by your systems programmer.

Example: Define a New Object to VLF

```
CLASS NAME(CAENFU) /* ENF/USS pathname lookup cache*/
EMAJ(PATHCACHE) /* Required major name*/
MAXVIRT(512) /* 512 = 2MB*/
```

The class name (CAENFU) and major name (PATHCACHE) must be entered exactly as shown.

MAXVIRT in the range of 512 to 1024 (representing 2 MB to 4 MB of virtual storage) should suffice for most sites; however, you may want to change MAXVIRT according to the following formula:

$$\text{MAXVIRT} = \text{MAXFILEPROC} * \text{MAXPROCSYS} * 16$$

MAXFILEPROC and MAXPROC are UNIX System Services configuration parameters found in SYS1.PARMLIB(BPXPRMxx).

The following lists the minimum storage requirements for each CAIENF/USS distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.ACQ9MOD	6144	10	16	Module Library

CAIRIM Requirements

The CAIRIM service includes CA LMP, Serviceability, and CAISSF services.

Note: For information about non-CA security product support of CAISSF, see the *Administration Guide*.

CAIRIM has the following installation requirements:

- An IBM supported z/OS version.
- CAIRIM runs on any z/OS processor with no special setup or modification required.
- CAIRIM must be installed into an APF authorized library.
- The CAIRIM SMF recording must be active in the system for any SMF event or data-handling solution routines. The CAIRIM SMF Interceptor component does not require any particular SMF records. If desired, you can suppress all SMF record types as long as the SMF parameters specify that SMF is active.

In some cases, a particular CA solution requires that certain SMF records be recorded. This recording is strictly for historical analysis and reporting, not for solution operation or initialization.

- CAIRIM requires approximately 12 KB of ECSA and 4 KB of CSA. Additional CSA requirements for resident modules vary with each service or product. Consult the installation documentation for your solution for additional solution-specific information.
- CA LMP requires approximately 22 KB of ECSA.

- CAISSF requires approximately 1 KB of CSA for the security routine and approximately 2 KB to 4 KB for the respective security translator.
- CAIRIM uses a small amount of SQA for creating CDE entries — approximately 30 bytes per module.
- CA LMP uses an SVC that is dynamically installed during CAIRIM initialization. You do not need to select an SVC entry for the CA LMP SVC, as it will use the first available unused SVC slot it finds.
- CAIRIM has a CAILPA data set, which is required for Serviceability. The CAILPA data set needs to be added to the system 'SYS1.PARMLIB' LPALSTxx member. The ELPA usage is approximately 3.5K.

The following lists the minimum storage requirements for each CAIRIM Utilities distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.AAS9CLS0	0	1	1	CLIST Library
CAI.AAS9JCL	0	1	1	JCL Library
CAI.AAS9MOD	6144	25	7	Module Library
CAI.AAS9OPTN	0	1	3	Option Library
CAI.AAS9PROC	0	1	2	JCL Procedure Library
CAI.AAS9SAMP	0	7	2	SAMP Library
CAI.AAS9SDF	0	1	1	Side Deck Library
CAI.AAS9XML	32760	12	1	Source Library

CAISDI Requirements

CAISDI consists of the following components: soap, med, and els. In the past, these components were installed separately. Now, they are installed as one product.

CAISDI has the following installation requirements:

- An IBM supported z/OS version.
- Use a region size of 4 MB or larger.
- CAISDI/med uses approximately 24 KB of the extended common service area (ECSA) for loading common storage resident services and intercepts.

Certain types of service calls use approximately 100 KB of ECSA while the service call is outstanding; however, CAISDI makes extensive use of cross-memory services to avoid the need for common storage areas.

- CAISDI/els uses varying amounts of CSA depending on which products use this component.

The CAISDI/els Interface Controller reports the ECSA usage for each product separately.

- CAI.CAW0OPTN contains the CAISDI initialization statements for all CAISDI components. If the parameter data set is to be shared by multiple z/OS systems, it must reside on a shared DASD volume.
- CAI.CAIEVENT contains the event definitions for the CAISDI/els component. The event members are provided by the CA Technologies products that use this interface.
- CAISDI provides the interface to CA Service Desk over a network connection using TCP/IP. Be sure TCP/IP is up and running on at least one z/OS system. The CAISDI/soap client will be installed there.
- The userid associated with running the CAISDI/soap Client address space must have the UNIX System Services profile defined to UID 0 or be a SUPERUSER (BPX.SUPERUSER).
- Verify that CA Service Desk is installed and properly configured.
- Some products generate Service Desk Request Description content in HTML format.

By default, CA Service Desk renders embedded HTML directives in the request description field. This capability can be deactivated. To render the request text properly, your CA Service Desk server must support HTML rendering. Contact your CA Service Desk administrator and ask that this task be performed.

This task involves customizing the detail_cr.html form to add keeptags and keeplinks support.

Note: For more information about the installation and configuration of CA Service Desk, see the *CA Service Desk Installation Guide*.

The following lists the minimum storage requirements for each CAISDI distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.ADYFJCL	0	1	1	Macro Library
CAI.ADYFMAC	0	2	1	Macro Library
CAI.ADYFMOD	6144	50	12	Module Library
CAI.ADYFOPTN	0	2	3	Option Library
CAI.ADYFOPTV	25600	1	1	Option V Library
CAI.ADYFPROC	0	1	1	Procedure Library

Earl Service Requirements

Earl Service has the following installation requirements:

- An IBM supported z/OS version.
- Earl Service requires CA Sort for z/OS, IBM DF/Sort, or a compatible product with the module name SORT.

The following lists the minimum storage requirements for each Earl Service distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI. AAXEJCL	0	1	1	JCL Library
CAI. AAXEMAC	0	2	1	Macro Library
CAI. AAXEMOD	6144	17	3	Module Library
CAI. AAXESRC	0	1	1	Source Library

Easytrieve Service Requirements

Easytrieve Service has the following installation requirements:

- An IBM supported z/OS version.
- Easytrieve Service requires CA Sort for z/OS, IBM DF/Sort, or a compatible product with the module name SORT.
- The Easytrieve Service provided in CA Common Services is not the full-featured Easytrieve product.
- SMP/E prevents installation of CA Common Services Easytrieve into the same CSI where the full-featured Easytrieve product is already installed.
- New data set naming standards have been implemented starting with the CA Common Services r12 version of Easytrieve 6.4.

If you have the full-featured Easytrieve r6.4 product or any lower version of Easytrieve already installed at your site, install the Easytrieve Service provided with this release of CA Common Services into an SMP CSI where Easytrieve is not already installed. This release of Easytrieve must be installed into SMP Distribution and Target libraries that are different from your existing Easytrieve installation. This is necessary because the module names are the same for the two products.

If after installing the Easytrieve supplied with this release of CA Common Services, you have both a full-featured Easytrieve and a CA Common Services Easytrieve product installed, continue to use your full-featured Easytrieve for production jobs and CA Common Services Easytrieve for jobs provided by the other CA Technologies products that use the Easytrieve Service. This is necessary because the Easytrieve Service provided in CA Common Services is not the full-featured Easytrieve product, and this may affect your production Easytrieve jobs. Also, your production jobs may encounter some of the issues that can exist when moving from the 24-bit version of Easytrieve, (pre-r6.4), to the 31-bit version, (r6.4).

The following lists the minimum storage requirements for each Easytrieve distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.ADX8JCL	0	1	1	JCL Library
CAI.ADX8MAC	0	4	1	Macro Library
CAI.ADX8MOD	6144	51	27	Module Library

Event Management Requirements

Event Management has the following installation requirements:

- An IBM supported z/OS version, including full-function OMVS and zFS physical file system implemented.
- The user ID for the OMVS address space must have UPDATE access to the zFS data sets if the data sets are protected by external security.
- The user ID used to install Event Management must have superuser authority and read access to the following resources:

BPX.FILEATTR.APF

BPX.FILEATTR.PROGCTL

BPX.SERVER

- IBM HTTP Server
- Java runtime environment at the JDK 1.4, 1.5, or 1.6 level

Important! z/OS includes the Java environment with the web server so that both are installed together. If you have not previously used Java on z/OS, you can order a copy on tape from IBM. Be certain to install all necessary prerequisites and follow the installation documentation exactly. You should verify that you can run some of the IBM-provided Java sample programs before attempting to start Event Management.

- BPXPRMxx setting MAXASSIZE > 128 MB
- BPXPRMxx setting MAXPROCUSER > 100
- BPXPRMxx setting MAXCPU TIME = 86400
- Disk space: (RO and RW zFS) approximately 900 cylinders total

Note: Temporary HFS space is also required. Ensure that the temporary HFS file has at least 50 MB space available.

- Security definitions for these resources in class CAIUNI are shown in the following table for using the optional Java GUI:

Define Resource	Permitting Access To
EMSRVC.APPMAP	Enterprise Management
EMSRVC.MSG RECORD	Messages
EMSRVC.MSG ACTION	Message actions
EMSRVC.CALENDAR	Calendars
EMSRVC.CONLOG	The Console
EMSRVC.CONLOG ANNOTATION	Console message annotation

The following lists the minimum storage requirements for each Event Management distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.AD5IJCL	0	5	1	JCL Library
CAI.AD5MOD	6144	5	1	Module Library
CAI.AD5IPROC	0	6	1	Proc Library
CAI.AD5ISDF	0	4	1	Side Deck File
CAI.AD5IZFS	32760	7000	3	ZFS element types

Event Management Utilities Requirements

The following lists the minimum storage requirements for each Event Management Utility library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.AD5IJCL	0	1	1	JCL Library
CAI.AD5IMOD	6144	1	1	Module Library
CAI.AD5ISDF	0	1	1	Side Deck File

CA Health Checker Common Service Requirements

The CA Health Checker common service works with any IBM supported z/OS version.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.AEF5MOD	6144	65	75	Module Library

The CA Health Checker common service requires no customization. Its only requirement is that its load modules are available in the System Linklist.

CA MSM Common Services Requirements

The CA MSM Common Services works with any IBM supported z/OS version.

The following lists the minimum storage requirements for each distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.AETNEXP	0	47	1	CA Datacom Export
CAI.AETNJCL	0	1	1	JCL Library
CAI.AETNMOD	6144	180	-	PDSE Module Library
CAI.AETNOPTN	0	1	1	Option Library
CAI.AETNPROC	0	1	1	Procedure Library
CAI.AETNSDF	0	4	1	Side Deck Library
CAI.AETNXML0	32760	245	4	XML Library

SRAM Service Requirements

The SRAM Service works with an IBM supported z/OS version.

The following lists the minimum storage requirements for each SRAM distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.AASRJCL	0	1	1	JCL Library
CAI.AASRMAC	0	1	1	Macro Library

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.AASRMOD	6144	3	2	Module Library
CAI.AASROPTN	0	2	1	Option Library*

*Used for installation of USERMOD(ASR0001)

ViewPoint Requirements

ViewPoint works with an IBM supported z/OS version.

The following lists the minimum storage requirements for each Viewpoint Utilities distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation. Data set allocation JCL and (MSM) XML contains a block size of 0 for FB data sets with a LRECL of 80. This change was made in order to follow both IBM's SMP/E packaging standards, and CA's packaging standards. Specifying BLKSIZE=0 will allow your system to choose the most efficient block size for these data sets.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.ADU4CICS	6144	14	1	CICS Load Library
CAI.ADU4DLD	8204	14	5	Dialog Library
CAI.ADU4JCL	0	1	1	JCL Library
CAI.ADU4MLD	0	4	1	Macro Library
CAI.ADU4MOD	6144	92	9	Module Library
CAI.ADU4PANL	4104	42	41	Panel Library
CAI.ADU4TLD	0	3	2	Template Library

Apache Tomcat Requirements

Tomcat works with any IBM supported z/OS version.

The IBM Java JDK is required at v1.6 or higher. The 64-bit versions of the Java SDK are also supported at v1.6 and higher.

The following lists the minimum storage requirements for each Tomcat distribution library and does not necessarily represent the actual distribution library allocation that is provided during the installation.

Library Name	Block Size	Tracks	Directory Blocks	Description
CAI.TPV.AEG1JAR	6144	112	1	JAR File Library
CAI.TPV.AEG1SHSC	255	1	1	SMP Apply Shell Script Library

Chapter 3: Installing Your Product Using CA MSM

These topics provide information to get you started managing your product using CA MSM. You can use the online help included in CA MSM to get additional information.

Before using these topics, you must already have CA MSM installed at your site. If you do not have CA MSM installed, you can download it from the Download Center at [the CA Support Online website](#), which also contains links to the complete documentation for CA MSM.

Note: The information in this section applies to the latest version of CA MSM. If you are using an earlier version, see the appropriate bookshelf on the CA Mainframe Software Manager product page.

Access CA MSM Using the Web-Based Interface

You access CA MSM using the web-based interface. You must have at least *one* of the following web browsers: Microsoft Internet Explorer 6.0, 7.0, or 8.0, or Mozilla Firefox 3.5.

You need the URL of CA MSM from the CA MSM administrator.

To access CA MSM using the web-based interface

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

The login page appears.

Note: If the Notice and Consent Banner appears, read the information provided, and click the link to confirm it.

2. Enter your z/OS login user name and password, and click the Log In button.

The initial page appears. If you log in for the first time, you are prompted to define your account on [the CA Support Online website](#).

Note: For more information about the interface, click the Help link at the top right corner of the page.

3. Click New.

You are prompted for the credentials to use on [the CA Support Online website](#).

Important! The account to which the credentials apply *must* have the Product Display Options set to BRANDED PRODUCTS. You can view and update your account preferences by logging into [the CA Support Online website](#) and clicking My Account. If you do not have the correct setting, you are not able to use CA MSM to download product information and packages.

4. 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.

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

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

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

How to Use CA MSM: Scenarios

In the scenarios that follow, imagine that your organization recently deployed CA MSM to simplify the installation of CA Technologies products and unify their management. You have also licensed a new CA Technologies product. In addition, you have a number of existing CSIs from previously installed products.

- The first scenario shows how you can use CA MSM to acquire the product.
- The second scenario shows how you can use CA MSM to install the product.
- The third scenario shows how you can use CA MSM to maintain products already installed in your environment.
- The fourth scenario shows how you can use CA MSM to deploy the product to your target systems.

How to Acquire a Product

The *Product Acquisition Service (PAS)* facilitates the acquisition of mainframe products and the service for those products, such as program temporary fixes (PTFs). The PAS retrieves information about the products to which your site is entitled and records these entitlements in a software inventory maintained on your driving system.

You can use the PAS component of CA MSM to acquire a CA Technologies product.

To do this, complete the following tasks:

1. Set up a CA Support Online account.

To use CA MSM to acquire or download a product, you must have a CA Support Online account. If you do not have an account, you can create one on [the CA Support Online website](#).

2. Determine the CA MSM URL for your site.

To access CA MSM, you require its URL. You can get the URL from your site's CA MSM administrator and log in using your z/OS credentials. When you log in for the first time, you are prompted to create a CA MSM account with your credentials for [the CA Support Online website](#). This account enables you to download product packages.

3. Log in to CA MSM and go to the Software Catalog tab to locate the product that you want to manage.

After you log in to CA MSM, you can see the products to which your organization is entitled on the Software Catalog tab.

If you cannot find the product you want to acquire, update the catalog. CA MSM refreshes the catalog through [the CA Support Online website](#) using the site IDs associated with your credentials for [the CA Support Online website](#).

4. Download the product installation packages.

After you find your product in the catalog, you can download the product installation packages.

CA MSM downloads (acquires) the packages (including any maintenance packages) from the CA FTP site.

The product is now ready for you to install or maintain.

How to Install a Product

The *Software Installation Service (SIS)* facilitates the installation and maintenance of mainframe products in the software inventory of the driving system, including browsing downloaded software packages, managing SMP/E consolidated software inventories (CSIs) on the driving system, and automating installation tasks.

You can use the SIS component of CA MSM to install a CA Technologies product.

To do this, complete the following tasks:

1. Initiate product installation and review product information.
2. Select an installation type.
3. Review installation prerequisites if any are presented.

4. Do *one* of the following to select a CSI:
 - Create a new CSI:
 - a. Set up the global zone.
 - b. Create a target zone.
 - c. Create a distribution zone.
 - Use an existing CSI from your working set:
 - a. Update the global zone.
 - b. Set up the target zone: either create a new target zone or use an existing target zone.
 - c. Set up the distribution zone: either create a new distribution zone or use an existing distribution zone.

Note: If you install a product or any of its components into an existing target or distribution zone, the installation process deletes older versions from the zone and the associated target and distribution data sets. We recommend that you use new target and distribution zones for this installation so that you can apply maintenance to your current release if necessary.
5. Review the installation summary and start the installation.

Agent Technology and Event Management Post-Installation

After performing the installation for Agent Technology and Event Management, perform the following post-installation tasks. These tasks must be completed before deployment.

These post-installation procedures assume that the zFS data sets are mounted at their installation mountpoints.

Agent Technology Post-Installation

To complete the Agent Technology installation

1. Create a user ID for Agent Technology.

The Agent Technology jobs should be run using one user ID, usually called AWADMIN with group name AWGROUP. This user ID should have a UNIX System Services segment defined so that the following conditions are met:

Note: The user ID should not be UID(0).

- The home directory is the same as the installation path for Agent Technology.
- The z/OS shell is specified as the default shell. Generally, this is /bin/sh.

The user ID for Agent Technology is created.

After installation is completed, other user IDs can be cloned for use on production systems, depending on your site's security policies.

CNSMJCL member B6DI0015 can create this user ID. The job provides control statements for RACF, CA ACF2, and CA Top Secret.

Update the statements for your security package and delete the remainder.

Important! The User ID used to run this job must have the authority to issue the commands.

2. Set Agent Technology directory group ownership and Set User ID mode bit for Agent Technology.

Certain programs in Agent Technology need to run with UID(0).

Edit CNSMJCL member B6DI0065 to set the user ID bit for these programs.

This job must be run with the UID that owns the Agent Technology zFS files.

3. Enable Agent Technology command line EXEC.

Optionally, you may set the environment variable to enable all OMVS users to execute Agent Technology programs from the command line. This job updates /etc/profile.

Use CNSMJCL member B6DI0068.

Event Management Post-Installation

To complete the Event Management installation

1. Create additional Event Management directories.
 - a. Modify and submit CNSMJCL member D5II0040.
 - b. Check the results of this job by reviewing the STDOUT and STDERR zFS files referenced in the EXPAND step. Do not rely on the job's return codes as evidence of successful completion.
2. Create the Event Management profile.
 - a. If you are installing Event Management on a system where Event Management has been previously installed, prior to submitting the job associated with this step, you must remove (not simply comment out) the Event Management updates in the /etc/profile file. If they exist, the updates can be found at the end of the file and are clearly marked.
 - b. Modify and submit CNSMJCL member D5II0050. Running Event Management depends on the setting of various environment variables.

Modify the following variables to match your installation standards:

- STEPLIB and CA_DBHLQ

If you plan to use either the Calendars or Message Actions option, you are required to install CA Datacom/AD after your CA Common Services components installation and Configuration are completed. If you do not know the CA Datacom/AD data set names or data set high level qualifier at this time, you can edit the profile file directly with this information after your CA Datacom/AD installation is completed.

STEPLIB must reference your CA Datacom/AD and CA Common Services load libraries in the following order:

```
STEPLIB=$STEPLIB:CAI.DATACOM.CUSLIB
STEPLIB=$STEPLIB:CAI.DATACOM.SMPE.CAAXLOAD
STEPLIB=$STEPLIB:CAI.CAW0LOAD
STEPLIB=$STEPLIB:CAI.CNSMLOAD
```

CA_DBHLQ must reference your CA Datacom/AD high level qualifier. The value to be used is the custom data set prefix. The value for CA_DBHLQ should not have the trailing dot. This high level qualifier is the same one used in the STEPLIB for CUSLIB.

If you are not going to use the Calendars or Message Actions option, delete the CA Datacom/AD references.

If you are not going to use the Calendars or Message Actions option, STEPLIB should reference your CA Common Services load libraries only. Delete the STEPLIB statements that reference the CA Datacom/AD data sets. The CA Common Services load libraries are:

```
STEPLIB=$STEPLIB:CAI.CAW0LOAD  
STEPLIB=$STEPLIB:CAI.CNSMLOAD
```

Also delete the CA_DBHLQ statement.

- CA_OPR_ZOSDB indicates whether the CA Datacom/AD database will be used. The default value is N (no). If you are going to use Calendars or Message Actions change the value of this environment variable to Y(yes).
- INSTALLSAF indicates whether Store and Forward should be active. The default is Y (yes).
- UPDATE_ETC indicates whether /etc/profile should be updated to set the environment variables required to run Event Management commands. The default is N (no).

If you select Y (yes) and Event Management was previously installed on this system, then /etc/profile will not be updated and you must review the contents of /etc/profile to decide if the current CAIGLBL0000 value defined is correct and preferable for all users.

If you select N (no), the tngprofile file in the CAIGLBL0000 directory will be updated with the appropriate profile settings that can be used later at logon.

3. Create links for Event Management.

CNSMJCL member D5I10065 creates the links required for Event Management and runs the Event Management component installation scripts. This is a long-running job.

Check the results of this job by reviewing the STDOUT and STDERR zFS files referenced in the EXPAND step. Do not rely on the job's return codes for evidence of successful completion.

Important! JAVA_HOME must be initialized first, or this step will not complete properly.

How to Maintain Existing Products

If you have existing CSIs, you can bring those CSIs into CA MSM so that you can maintain all your installed products in a unified way from a single web-based interface.

You can use the PAS and SIS to maintain a CA Technologies product.

To do this, complete the following tasks:

1. Migrate the CSI to CA MSM to maintain an existing CSI in CA MSM.

During the migration, CA MSM stores information about the CSI in the database.

2. Download the latest maintenance for the installed product releases from the Software Catalog tab.

If you cannot find a release (for example, because the release is old), you can add the release to the catalog manually and then update the release to download the maintenance.

3. Apply the maintenance.

Note: You can also install maintenance to a particular CSI from the SMP/E Environments tab.

After the maintenance process completes, the product is ready for you to deploy. You may have to perform other steps manually outside of CA MSM before beginning the deployment process.

How to Deploy a Product

The *Software Deployment Service (SDS)* facilitates the deployment of mainframe products from the software inventory of the driving system to the target system, including deploying installed products that are policy driven with a set of appropriate transport mechanisms across a known topology.

You can use the SDS component of CA MSM to deploy a CA Technologies product that you have already acquired and installed.

To do this complete the following tasks:

1. Set up the system registry:
 - a. Determine the systems you have at your enterprise.
 - b. Set up remote credentials for those systems.
 - c. Set up the target systems (Non-Sysplex, Sysplex or Monoplex, Shared DASD Cluster, and Staging), and validate them.
 - d. Add FTP information, including data destination information, to each system registry entry.
2. Set up methodologies.
3. Create the deployment, which includes completing each step in the New Deployment wizard.

After creating the deployment, you can save it and change it later by adding and editing systems, products, custom data sets, and methodologies, or you can deploy directly from the wizard.

Note: If you must deploy other products to the previously defined systems using the same methodologies, you must create a separate deployment.

4. Deploy the product, which includes taking a snapshot, transmitting to target, and deploying (unpacking) to your mainframe environment.

After the deployment process completes, the product is ready for you to configure. You may have to perform other steps manually outside of CA MSM before beginning the configuration process.

CA Common Services Deployment

The CA Common Services deployment process provides multiple options in the deployment product list. You can either select a group of components or a single component. Individual product selection for BASE components is not available because all the BASE components must be installed and deployed.

Important! After performing the installation for Agent Technology and Event Management, perform the tasks described in the section [Agent Technology and Event Management Post-Installation](#) (see page 72). The Agent Technology and Event Management Post-Installation must be done before their deployments.

To select a group of components, you must have all the components installed in your selected CSI otherwise the selection is blocked.

The deployment process only deploys SMP/E target data sets associated with the FMIDs defined to the product ID.

You can add non-SMP/E target data sets to be allocated and copied on the target system under the Custom Data Sets section.

To add custom data sets, click on the ADD DATASET button then input the data set information.

Chapter 4: Installing from Pax Files Using the SAMPJCL Method

This section contains the following topics:

[How to Install a Product Using Pax Enhanced ESD Files](#) (see page 79)

[Allocate and Mount a File System](#) (see page 85)

[Copy the Product Pax Files into Your USS Directory](#) (see page 86)

[Create a Product Directory from the Pax File](#) (see page 91)

[Copy Installation Files to z/OS Data Sets](#) (see page 92)

[How to Install Products Using Native SMP/E JCL](#) (see page 94)

[Prepare the SMP/E Environment for SAMPJCL Installation](#) (see page 95)

[Run the Installation Jobs for a SAMPJCL Installation](#) (see page 99)

[Clean Up the USS Directory](#) (see page 100)

[Apply Maintenance](#) (see page 101)

[CA Common Services Specific Post-Installation Requirement](#) (see page 103)

[Deploy Products](#) (see page 104)

How to Install a Product Using Pax Enhanced ESD Files

This section describes the Pax-Enhanced ESD process. We recommend that you read this overview and follow the entire procedure the first time you complete a Pax-Enhanced installation. Experienced UNIX users may find the *Pax-Enhanced ESD Quick Reference Guide* or this overview sufficient for subsequent installations.

Important! Downloading pax files for the SMP/E installation as part of the Pax-Enhanced ESD process requires write authority to the UNIX System Services (USS) directories used for the process.

If your site limits the access to z/OS UNIX System Services and you do not have the authority, provide a list of the MVS data sets to an authorized individual to perform steps 1 through 4. USS is not required for the actual SMP/E RECEIVE of a product. However, the remaining installation steps may require USS, based upon the products you are installing. If you are installing a product that requires USS such as Agent Technology, Event Management or the version of Tomcat shipped with CA Common Services, you must have USS authority to perform the installation.

To install files using Pax Enhanced ESD files, use the following process:

1. Allocate and mount the file system. This process requires a USS directory to receive the pax file and to perform the unpack steps. We recommend that you allocate and mount a file system dedicated to Pax-Enhanced ESD Installations and create a directory in this file system. Ensure that all users who will be working with pax files have write authority to the directory.

2. Copy the product pax files into your USS directory and choose one of the following options:
 - Download a zip file from CA Support Online to your PC, unzip the file, and then upload the product pax files to your USS directory.
 - FTP the pax files from CA Support Online directly to your USS directory.
 - Load the DVD into your PC and Upload the pax files to your USS directory

Note: Perform the following steps for each pax file that you upload to your USS directory.

CA Common Services software components are packaged using four pax files.

To determine which pax files to download, see the Introduction chapter.

3. Create a product directory from the pax file. Set the current working directory to the directory containing the pax file, and create a new directory in your USS directory by entering the following command:
`pax -rvf pax-file-name`
4. Copy Installation Files to z/OS Data Sets. Use the SMP/E GIMUNZIP utility to create z/OS installation data sets. The file UNZIPJCL in the directory created by the pax command in Step 3 contains a sample job to GIMUNZIP the installation package. Edit and submit the UNZIPJCL job.
5. Perform the product installation. Consult product-specific documentation, including AREADME files and installation notes to complete the product installation.
6. (Optional) Clean up the USS directory. Delete the pax file, the directory created by the pax command, all of the files in it, and the SMP/E RELFILES, SMPMCS, and HOLDDATA data sets.
7. Apply Maintenance.
8. Deploy Products.
9. Configure.

How the Pax-Enhanced ESD Download Works

Important! To download pax files for the SMP/E installation as part of the Pax-Enhanced ESD process, you must have write authority to the UNIX System Services (USS) directories used for the ESD process and available USS file space before you start the procedures in this guide.

Use the following process to download files using Pax-Enhanced ESD:

1. Log in to <https://support.ca.com/>, and click Download Center.
The CA Support Online web page appears.
2. Under Download Center, select Products from the first drop-down list, and specify the product, release, and genlevel (if applicable), and click Go.
The CA Product Download window appears.
3. Download an entire CA Technologies product software package or individual pax files to your PC or mainframe. If you download a zip file, you must unzip it before continuing.

For both options, [The ESD Product Download Window](#) (see page 81) topic explains how the download interface works.

Note: For traditional installation downloads, see the *Traditional ESD User Guide*. Go to <https://support.ca.com/>, log in, and click Download Center. A link to the guide appears under the Download Help heading.

4. Perform the steps to install the product based on the product-specific steps.
The product is installed on the mainframe.

ESD Product Download Window

CA Technologies product ESD packages can be downloaded multiple ways. Your choices depend on the size of the individual files and the number of files you want to download. You can download the complete product with all components or you can select individual pax and documentation files for your product or component.

The following illustration shows sample product files. It lists all components of the product. You can use the Download Cart by checking one or more components that you need or check the box for Add All to cart. If you prefer to immediately download a component, click the Download link.

CA Earl - MVS

- » [Pax Enhanced Electronic Software Delivery \(ESD\) Guide](#)
- » [Pax Enhanced Electronic Software Delivery \(ESD\) Quick Reference Guide](#)
- » [Traditional Electronic Software Delivery \(ESD\) Guide](#)
- » [Learn more about Using pkzip with your Downloaded Mainframe Products](#)
- » [Learn more about downloading components of CA product](#)

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

[View Download Cart](#)

Add All to cart

Product Components				Add to cart	Download
CA COMMON SERVICES PROD PKG 11SP08AW000.pax.Z	11.0 /SP08	03/31/2010	407MB	<input type="checkbox"/>	Download
CA EARL PRODUCT PACKAGE 610106AEO00.pax.Z	6.1 /0106	03/31/2010	1MB	<input type="checkbox"/>	Download
EARL PIPPACK AEO61010600.pdf	6.1 /0106	03/31/2010	93KB	<input type="checkbox"/>	Download
EARL INSTALL GUIDE MANUAL I2J2ED610NE.pdf	6.1 /0000	03/31/2010	361KB	<input type="checkbox"/>	Download
CA COMMON SERVICES COVER LTR QI92742.pdf	11.0 /SP08	03/31/2010	46KB	<input type="checkbox"/>	Download

Clicking the link for an individual component takes you to the Download Method page.

Download Method

Please choose a download method to complete your download request. [Learn More](#)

HTTP via Download Manager
This is the CA recommended method for download. The Download Manager allows you to download your files faster and more efficiently.
[Download](#)

HTTP via Internet Browser
If Download Manager cannot be used or fails to start you may access your file(s) via your internet browser.
[View File Link\(s\)](#)

FTP
This method allows you to download your file(s) via FTP from CA's content delivery network or via native FTP servers.
Note: Processing is required and an email notification will be sent when your request is ready for downloading.
[FTP Request](#)

Depending on the size and quantity of product files ordered, the Download Method screen could also have these options:

Note: For mainframe downloads using this HTTP method, click the Learn More link.

Download Method

Please choose a download method to complete your download request. [Learn More](#)

HTTP via Download Manager
This is the CA recommended method for download. The Download Manager allows you to download your files faster and more efficiently.
[Download](#)

Create a Zip File
This method allows you to bundle your download files into one or more zip files of up to 3.5 GB each. These zip files can then be downloaded via HTTP or FTP.
Note: Processing is required and an email notification will be sent when your request is ready for downloading.
[Create Zip](#)

The HTTP method lets you start downloading immediately. The FTP method takes you to the Review Orders page that displays your order, first in a Pending status changing to Ready when your order has been processed.

Preferred FTP uses the new content delivery network (CDN). Alternate FTP uses the CA Technologies New York-based FTP servers.

The Create a Zip File option first creates the zip, and when ready, offers the options shown by the Zip Download Request examples in the next screen.

Review Download Requests

Below is a list of the FTP and large HTTP downloads that have been requested by your site. When status is set to 'Ready' a link will appear.

- For FTP requests, click on the FTP link to view the path information for your download. For more information view our [FTP Help document](#)
- For HTTP requests, click on the HTTP link to initiate your download.
- To view the details of your request, click on the desired order number.

Today's Downloads

Order #	Status	Description	Date Placed	Download Options
10000961	Ready	FTP Download Request	04/30/2010	Preferred FTP ▼ Alternate FTP ▼

Previous 6 day Download History

Order #	Status	Description	Date Placed	Download Options
10000949	Ready	ZIP Download Request	04/29/2010	HTTP via DLM Preferred FTP ▼ Alternate FTP ▼
10000948	Ready	ZIP Download Request	04/29/2010	HTTP via DLM Preferred FTP ▼ Alternate FTP ▼

USS Environment Setup

You need a UNIX System Services (USS) directory and a file system with adequate space to perform the following tasks:

- Receive product pax files from CA Support Online.
- Perform utility functions to unpack the pax file into MVS data sets that you can use to complete the product installation.

We recommend that you allocate and mount a file system dedicated to Pax-Enhanced ESD. The amount of space that you need for the file system depends on the following variables:

- The size of the pax files that you intend to download.
- Whether you plan to keep the pax files after unpacking them. We do not recommend this practice.

We recommend that you use one directory for downloading and unpacking pax files. Reusing the same directory minimizes USS setup. You need to complete the USS setup only one time. You reuse the same directory for subsequent downloads. Alternatively, you can create a new directory for each pax download.

Important! Downloading pax files for the SMP/E installation as part of the Pax-Enhanced ESD process requires write authority to the UNIX System Services (USS) directories used for the ESD process. In the file system that contains the ESD directories, you also need free space approximately 3.5 times the pax file size to download the pax file and unpack its contents. For example, to download and unpack a 14 MB pax file, you need approximately 49 MB of free space in the file system hosting your ESD directory.

Allocate and Mount a File System

You can use the zSeries File System (zFS) or hierarchical file system (HFS) for Pax-Enhanced ESD downloads.

This procedure details how to perform the following tasks:

- Allocate an HFS file system
- Create a new mount point in an existing maintenance directory
- Mount the file system on the newly created mount point
- Optionally permit write access to anyone in the same group as the person who created the directory

Important! USS commands are case-sensitive.

To allocate and mount the file system

1. Allocate the HFS. For example:

```
//ALCHFS EXEC PGM=IEFBRI4
//CAESD DD DSN=yourHFS dataset name,
// DISP=(NEW,CATLG,DELETE),UNIT=3390,
// DSNTYPE=HFS,SPACE=(CYL,(primary,secondary,1))
```

The HFS is allocated.

2. Create a mount point for the file system. This example shows how to create a /CA/CAESD directory in an existing directory, /u/maint. From the TSO OMVS shell, enter the following commands:

```
cd /u/maint/  
mkdir CA  
cd CA  
mkdir CAESD
```

Note: This document refers to this structure as *yourUSSESDdirectory*.

The mount point is created.

3. Mount the file system. For example, from TSO, enter the following command:

```
MOUNT FILESYSTEM('yourHFS dataset name')  
      MOUNTPOINT('yourUSSESDdirectory')  
      TYPE(HFS)  MODE(RDWR)
```

The file system is mounted.

4. (Optional) Set security permissions for the directory. You can use the chmod command to let other users access the ESD directory and its files. For example, to allow write access to the ESD directory for other users in your USS group, from the TSO OMVS shell, enter the following command:

```
chmod -R 775 /yourUSSESDdirectory/
```

Write access is granted.

Note: For more information about the chmod command, see the IBM *z/OS UNIX System Services User Guide (SA22-7802)*.

Copy the Product Pax Files into Your USS Directory

To begin the CA product installation procedure, copy the product's pax files into the USS directory you set up. Since CA Common Services software components are packaged using four pax files, it may be easier to copy all the pax files you require to the USS directory now versus coming back to this procedure later.

Use one of the following methods:

- Download the product pax files directly from the CA Support Online FTP server to your z/OS system.
- Download the product pax files from the CA Support Online FTP server to your PC, and upload it to your z/OS system.
- Download the product files from CA Support Online to your PC. If your download included a zip file, unzip the file, and upload the unzipped pax files to your z/OS system.
- Upload the pax files found on the DVD to your z/OS system.

This section includes a sample batch job to download a product pax file from the CA Support Online FTP server directly to a USS directory on your z/OS system and sample commands to upload a pax file from your PC to a USS directory on your z/OS system.

Important! The FTP procedures may vary due to your local firewall and other security settings. Consult your local network administrators to determine the appropriate FTP procedure to use at your site.

Ensure that sufficient free space is available in the USS file system you are using for Pax-Enhanced ESD to hold the product pax file. If you do not have sufficient free space, error messages similar to the following appear:

```
EZA1490I Error writing to data set  
EZA2606W File I/O error 133
```

When the download finishes, the pax file size in your USS directory should match the value in the Size column for the corresponding pax file on the CA Technologies Products Download window.

Download Using Batch JCL

Use this process to download a pax file from the CA Support Product Downloads window by running batch JCL on the mainframe. Use the sample JCL attached to the PDF file as CAtoMainframe.txt to perform the download.

Important! To simplify the Pax-Enhanced ESD process, the PDF version of this guide includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon in the lower left corner of the PDF reader. This opens a window displaying attachments. Double-click the file to view the sample JCL.

Note: We recommend that you follow the preferred method as described on CA Support Online. This procedure is our preferred download method; however, we do include the procedure to download to the mainframe through a PC in the next section.

Follow these steps:

1. Supply a valid JOB statement.
The job points to your profile.
2. Replace *yourTCPIP.PROFILE.dataset* with the name of the TCP/IP profile data set for your system. Consult your local network administrators, if necessary.
The job points to your email address.
3. Replace *YourEmailAddress* with your email address.
The job points to your email address.
4. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.
The job points to your USS directory.

5. Locate the product component to download on the CA Support Product Download window.

You have identified the product component to download.

6. Click Download for the applicable file.

Note: For multiple downloads, add files to a cart.

The Download Method window opens.

7. Click FTP Request.

The Review Download Requests window displays any files that you have requested to download.

Note: We send you an email when the file is ready to download or a link appears in this window when the file is available.

8. Select one of the following methods:

Preferred FTP

Uses CA Technologies worldwide content delivery network (CDN). If you are not able to download using the Preferred FTP method, check the security restrictions for all servers that company employees can download from that are outside of your corporate network.

Host Name: ftp://ftpdnloads.ca.com

Alternate FTP

Uses the original download servers that are based on Long Island, New York.

Host Name: ftp://scftpd.ca.com for product files and download cart files and ftp://ftp.ca.com for individual solution files.

Both methods display the host, user name, password, and FTP location, which you then can copy into the sample JCL.

Note: For details regarding FTP, see the FTP Help document link in the Review Download Requests window and the Learn More link available in the Download Methods window.

9. Submit the job.

Important! If your FTP commands are incorrect, it is possible for this job to fail and still return a zero condition code. Read the messages in the job DDNAME SYSPRINT to verify the FTP succeeded.

After running the JCL, the pax file resides in the mainframe USS directory that you supplied.

Example: CAtomainframe.txt, JCL

The following text appears in the attached CAtomainframe.txt JCL file:

```
//GETPAX JOB (ACCOUNTNO),'FTP GET ESD PACKAGE',
//          MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
/* This sample job can be used to download a pax file directly from *
/* CA Support Online to a USS directory on your z/OS system.      *
/*                                                                *
/* This job must be customized as follows:                        *
/* 1. Supply a valid JOB statement.                               *
/* 2. Replace "yourTCPIP.PROFILE.dataset" with the name of the TCPIP *
/*    profile data set for your system.                           *
/* 3. Replace "Host" based on the type of download method.       *
/* 4. Replace "YourEmailAddress" with your email address.        *
/* 5. Replace "yourUSSESDdirectory" with the name of the USS     *
/*    directory used on your system for ESD downloads.           *
/* 6. Replace "FTP Location" with the complete path              *
/*    and name of the pax file obtained from the FTP location   *
/*    of the product download page.                              *
//*****
//GETPAX EXEC PGM=FTP,REGION=0K
//SYSTCPD DD DSN=yourTCPIP.PROFILE.dataset,DISP=SHR
//SYSPRINT DD SYSOUT=*
//OUTPUT DD SYSOUT=*
//INPUT DD *
Host
anonymous YourEmailAddress
lcd yourUSSESDdirectory
binary
get FTP location
quit
```

Upload Files to Mainframe through a PC

If you download pax or zip files from CA Support Online to your PC or if you are using a DVD, use this procedure to upload the pax file from your PC to your z/OS USS directory.

To upload files to the mainframe through a PC

1. Follow the procedures in How the Pax-Enhanced ESD Download Works to download the product pax or zip file to your PC. If you download a zip file, first unzip the file to use the product pax files.

The pax or zip file resides on your PC.

2. Open a Windows command prompt.

The command prompt appears.

3. Customize and enter the FTP commands with the following changes:
 - a. Replace *mainframe* with the z/OS system's IP address or DNS name.
 - b. Replace *userid* with your z/OS user ID.
 - c. Replace *password* with your z/OS password.
 - d. Replace *C:\PC\folder\for\thePAXfile* with the location of the pax file on your PC.
 - e. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.
 - f. Replace *paxfile.pax.Z* with the name of the pax file to upload.

The pax file is transferred to the mainframe.

Example: FTP Commands

This list is a sample of FTP commands to upload the pax file from your PC to your USS Pax-Enhanced ESD directory:

```
ftp mainframe
userid
password
bin
lcd C:\PC\folder\for\thePAXfile
cd /yourUSSESDdirectory/
put paxfile.pax.Z
quit
exit
```

Create a Product Directory from the Pax File

Use the sample job attached to the PDF file as `Unpackage.txt` to extract the product pax file into a product installation directory. Since CA Common Services software components are packaged using four pax files, it may be easier to perform this procedure for all the pax files you require now versus coming back to this procedure later. You should create a separate directory for each pax file.

Important! To simplify the Pax-Enhanced ESD process, the PDF version of this guide includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon in the lower left corner of the PDF reader. This opens a window displaying attachments. Double-click the file to view the sample JCL.

To create a product installation directory using the `Unpackage.txt` sample job

1. Supply a valid JOB statement.
2. Replace *yourUSSESDdirectory* with the name of the USS directory that you used for ESD downloads.

The job points to your specific directory.

3. Replace *paxfile.pax.Z* with the name of the pax file.

The job points to your specific pax file.

4. Submit the job.

The job runs and creates the product directory.

Note: After making the changes noted in the job, if the `PARM=` statement exceeds 71 characters, uncomment and use the second form of `UNPAXDIR` instead. This sample job uses an X in column 72 to continue the `PARM=` parameters to a second line.

Sample Job to Execute the Pax Command (Unpackage.txt)

The following text appears in the attached Unpackage.txt JCL file:

```
//ESDUNPAX JOB (ACCOUNTNO),'UNPAX ESD PACKAGE ',
// MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
/* This sample job can be used to invoke the pax command to create *
/* the product-specific installation directory. *
/* *
/* This job must be customized as follows: *
/* 1. Supply a valid JOB statement. *
/* 2. Replace "yourUSSESDdirectory" with the name of the USS *
/* directory used on your system for ESD downloads. *
/* 3. Replace "paxfile.pax.Z" with the name of the pax file. *
/* NOTE: If you continue the PARM= statement on a second line, make *
/* sure the 'X' continuation character is in column 72. *
//*****
//UNPAXDIR EXEC PGM=BXPBATCH,
// PARM='sh cd /yourUSSESDdirectory/; pax -rvf paxfile.pax.Z'
/*UNPAXDIR EXEC PGM=BXPBATCH,
/* PARM='sh cd /yourUSSESDdirectory/; pax X
/* -rvf paxfile.pax.Z'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
```

Copy Installation Files to z/OS Data Sets

Use this procedure to invoke the SMP/E GIMUNZIP utility to create MVS data sets from the files in the product-specific directory. Since CA Common Services software components are packaged using four pax files, it may be easier to perform this procedure for all the pax files you require now versus coming back to this procedure later. Each pax file contains its own UNZIPJCL file.

To copy the Pax-Enhanced ESD installation files to z/OS data sets

1. Locate and read the product readme file or installation notes, if applicable, which resides in the product-specific directory that the pax command created. This file contains product-specific details you need to complete the installation procedure.

You have identified product-specific installation details.

2. Use ISPF EDIT or TSO ISHELL to edit the UNZIPJCL sample job. You can perform this step in one of the following ways:
 - Use ISPF EDIT. Specify the full path name of the UNZIPJCL file.
 - Use TSO ISHELL. Navigate to the UNZIPJCL file and use the E line command to edit the file.

The job is edited.

3. Change the SMPDIR DD PATH to the product-specific directory created by the pax command.

Your view is of the product-specific directory.

4. If ICSF is not active, perform the following steps:
 - a. Change the SMPJHOME DD PATH to your Java runtime directory. This directory varies from system to system.
 - b. Perform one of the following steps:
 - Change the SMPCPATH DD PATH to your SMP/E Java application classes directory, usually /usr/lpp/smp/classes/.
 - Change HASH=YES to HASH=NO on the GIMUNZIP parameter.

One of the following occurs: ICSF is active or you are using Java.

5. Change all occurrences of *YourHLQ* to the high-level qualifier (HLQ) for z/OS data sets used by the installation process. We suggest that you use the same HLQ for each expanded CA Common Services pax file. Using the same HLQ will allow you to perform one installation for all CA Common Services components. Each CA Common Services pax file has its own UNZIPJCL file. If you use a different HLQ for *YourHLQ* value in each UNZIPJCL file, at a minimum, you would have to perform multiple SMP/E receives to bring the unzipped files into your SMP/E installation environment. Do not use the same value for *YourHLQ* as you will use for the SMP/E RELFILES.

All occurrences of *YourHLQ* are set to your high-level qualifier for z/OS data sets.

6. Submit the UNZIPJCL job.

The UNZIPJCL job should complete with a zero return code. Messages GIM69158I and GIM48101I in the output and IKJ56228I in the JES log are acceptable.

GIMUNZIP creates z/OS data sets with the high-level qualifier you specified in the UNZIPJCL job. You use these data sets to perform the product installation. The pax file and product-specific directory are no longer needed at this point.

Note: For more information, see the IBM Reference Manual, *SMP/E for z/OS Reference (SA22-7772)*.

How to Install Products Using Native SMP/E JCL

The following steps describe the process to install products using native SMP/E JCL:

1. Allocate product data sets and SMP/E data sets.
2. Create SMP/E CSI.
3. Receive base functions.

Complete the SMP/E RECEIVE using files on DASD that the UNZIPJCL job created. Consult the product sample JCL library that contains a sample job customized to receive the product from DASD. Specifically, you must specify the following values:

- DASD data set names for SMPPTFIN and SMPHOLD (if applicable)
 - The HLQ that you used in the UNZIPJCL job on the RFPREFIX parameter on the RECEIVE command.
4. Apply base functions.
 5. Accept base functions.
 6. Apply Maintenance.

Prepare the SMP/E Environment for SAMPJCL Installation

The members in this procedure prepare the SMP/E data sets, initialize the zones, and create the DDDEFS for CA Common Services for z/OS. External DDDEF data sets are required.

Prior to beginning this procedure, if you are installing Agent Technology, Event Management or the version of Tomcat shipped with CA Common Services, establishing a USS hierarchical file system is required as part of the product installation. If you are installing CA MSM Common Services, USS is a required feature of the product.

Since the CA Common Services software components are packaged using four pax files, it may be easier to install all the components at once versus repeating this procedure for each Common Services component or pax file.

The BASE pax file contains the SAMPJCL data set to install all the CA Common Services components. If you prefer performing multiple installations, make copies of the BASE SAMPJCL data set for each installation before you edit any of the members.

For information about the members, see the comments in the JCL.

All CA Common Services components must be installed into the same SMP/E CSI.

All the CA Common Services components found in the BASE pax file must be installed.

To prepare the SMP/E environment for your product

1. Customize the ISPF Edit macro, AW0SEEDIT found in the SAMPJCL data set unzipped from the BASE pax file with your site-specific information then copy it to your SYSPROC location.

To customize member AW0SEEDIT, replace the right-most parameters for each ISREDIT CHANGE macro command with your site specific information.

Each time you edit an installation member, type AW0SEEDIT on the TSO command line, and press Enter to replace the defaults with your specifications.

The macro is ready to customize the SAMPJCL members.

Important! All CA Common Services components **must** be installed into the same CSI and zones. If you decide to perform multiple installations for each CA Common Services component or pax file, the “change to” values specified for GLOBALHLQ and CAIT0HLQ must be the same for each installation.

Note: Update the SREDIT Change command for DASDHLQ by replacing CAI to the same value you specified as *yourHLQ* in the UNZIPJCL file for the pax file. This value is used in the SMP/E receive processing.

If you are installing CA Common Services components from multiple pax files and you specified a different value for *yourHLQ* in each pax file’s UNZIPJCL, you must perform the SMP/E receive for each *yourHLQ* you used.

Update ISREDIT CHANGE ALL DASDHLQ CAI

To ISREDIT CHANGE ALL DASDHLQ *yourHLQ*

The following steps include instructions to execute the AW0SEEDIT macro each time you open a new SAMPJCL member. To edit all SAMPJCL members simultaneously, read and follow the instructions in the AWOEDALL member

2. Open the SAMPJCL member AW01ALL in an edit session and execute the AW0SEEDIT macro from the command line.

3. Submit AW01ALL.

The job produces the following results:

- The target and distribution data sets for the BASE and OPTIONAL CA Common Services components are created.
- Unique SMPPTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

4. Complete the following sub-steps for each pax file that contains components you wish to install.

xxx represents the following 3-character codes:

CCS - LEGACY components

NSM - MFNSM components

- a. Open the SAMPJCL member xxx1ALL in an edit session and execute the AW0SEDIT macro from the command line.

xxx1ALL is customized.

- b. Submit xxx1ALL.

These jobs produce the following results:

- The target and distribution data sets for LEGACY and MFNSM CA Common Services components are created.

5. If you are installing Agent Technology, Event Management or the version of Tomcat shipped with CA Common Services, complete the following sub-steps for each of these products you are installing:

Note: All instances of ccc in this step represent the following three-character component codes based on the FMID.

B6D - MFNSM - Agent Technology

D5I - MFNSM - Event Management

EG1 - OPTIONAL - Tomcat

- a. Open the SAMPJCL member ccc1ALLU in an edit session and execute the AW0SEDIT macro from the command line.

ccc1ALLU is customized.

- b. Submit ccc1ALLU.

This job allocates your zFS data sets.

- c. Open the SAMPJCL member ccc2MKD in an edit session and execute the AW0SEDIT macro from the command line.

ccc2MKD is customized.

- d. Submit ccc2MKD.

This job creates all directories and mounts the file system.

6. All CA Common Services components must be installed into the same SMP/E CSI. This JCL creates the CSI for all CA Common Services components. Open the SAMPJCL member AW02CSI in an edit session and execute the AW0SEEDIT macro from the command line.

AW02CSI is customized.

7. Submit AW02CSI.

This job produces the following results:

- The CSI data set is defined.
- Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.
- The SMPPTS and SMPLOG data sets are allocated.
- The global, target, and distribution zones are initialized.
- The DDDEFs for the required SMP/E data sets are created.

8. Complete the following sub-steps for each pax file that contains components you wish to install: xxx represents the following 3-character codes.

- AW0 – BASE and OPTIONAL component DDDEFs
- CCS - LEGACY components DDDEFs
- NSM - MFNSM components DDDEFs

- a. Open the SAMPJCL member xxx2CSID in an edit session and execute the AW0SEEDIT macro from the command line.

xxx2CSID is customized.

- b. Submit xxx2CSID.

These jobs produce the following results:

- The DDDEF entries for Common Services component data sets are created.

9. If you are installing Agent Technology, Event Management or the version of Tomcat shipped with CA Common Services, complete the following sub-steps for each of these products you are installing:

- a. Open the SAMPJCL member ccc3CSIU in an edit session and execute the AW0SEEDIT macro from the command line.

ccc3CSIU is customized.

Note: All instances of ccc in this section indicate a three-character component code based on the FMID.

- b. Submit ccc3CSIU.

This job customizes the CSI by adding the DDDEFs associated with the USS target paths.

Run the Installation Jobs for a SAMPJCL Installation

Submit and run these SAMPJCL members in sequence. Do not proceed with any job until the previous job has completed successfully.

Each of the following members contains all the FMIDs associated with CA Common Services. Delete any FMIDs or steps associated with an FMID you do not want to install in each of the members.

To run the installation jobs

1. Open the SAMPJCL member AW03RECD in an edit session and execute the AW0SEEDIT macro from the command line.

AW03RECD is customized.

If you specified a different value for *yourHLQ* in each pax file's UNZIPJCL, you must customize and submit this JCL for each *yourHLQ* you used.

2. Submit the SAMPJCL member AW03RECD to receive SMP/E base functions.
CA Common Services for z/OS is received and now resides in the global zone.
3. Open the SAMPJCL member AW04APP in an edit session and execute the AW0SEEDIT macro from the command line.
AW04APP is customized.
4. Submit the SAMPJCL member AW04APP to apply SMP/E base functions.
Your product is applied and now resides in the target libraries.
5. Open the SAMPJCL member AW05ACC in an edit session and execute the AW0SEEDIT macro from the command line.
AW05ACC is customized.
6. Submit the SAMPJCL member AW05ACC to accept SMP/E base functions.
Your product is accepted and now resides in the distribution libraries.
7. Apply Maintenance.
8. Deploy products.

Clean Up the USS Directory

Important! This procedure is optional. Do not use this procedure until you complete the entire installation process.

To free file system disk space for subsequent downloads after downloading and processing the pax files for your CA Technologies product, we recommend removing the files from your USS directory and deleting unnecessary MVS data sets. You can delete the following items:

- Pax file
- Product-specific directory created by the pax command and all of the files in it
- SMP/E RELFILEs, SMPMCS, and HOLDDATA MVS data sets

These data sets have the HLQ that you assigned in the UNZIPJCL job.

Note: Retain non-SMP/E installation data sets such as *yourhlq*.INSTALL.NOTES for future reference.

Follow these steps:

1. Navigate to your Pax-Enhanced ESD USS directory.

Your view is of the applicable USS directory.

2. Delete the pax file by entering the following command:

```
rm paxfile
```

paxfile

Specifies the name of the CA Technologies pax file that you downloaded.

The pax file is deleted.

3. Delete the product-specific directory by entering the following command:

```
rm -r product-specific-directory
```

product-specific-directory

Specifies the product-specific directory created by the pax command.

The product-specific directory is deleted.

Note: You can also use TSO ISHELL to navigate to the pax file and product-specific directory, and delete them using the D line command.

Apply Maintenance

Prior to performing any maintenance, review the chapters concerning component configuration for any maintenance considerations.

CA Support Online may have maintenance and HOLDDATA that have been published since the installation data was created. In addition to maintenance found on CA Support Online, there may be maintenance already received into your SMP/E environment during the installation step associated with SAMPJCL member, AW03RECD.

To apply maintenance

1. Check CA Support Online and download any PTFs and HOLDDATA published since this release was created. Also, browse the SMP/E data set SMPPTS created during the installation process for maintenance that was RECEIVED but not APPLIED or ACCEPTED during the installation process.
2. Transfer the CA Support Online downloaded files to two separate FB 80 sequential data sets. Use one data set to contain the PTFs and the other to contain the HOLDDATA.

The PTFs and HOLDDATA become accessible to the SAMPJCL maintenance members.

3. The AW0SEEDIT macro was customized in the installation steps. Verify that you still have the values from the install.
4. Open the SAMPJCL member AW06RECP in an edit session and execute the AW0SEEDIT macro from the command line.
AW06RECP is customized with your JOB statement, CSI location, and zone names.
5. Customize the AW06RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.
6. Submit AW06RECP.

The PTFs and HOLDDATA are received.

7. Open the SAMPJCL member AW07APYP in an edit session and execute the AW0SEEDIT macro from the command line.
AW07APYP is customized.
8. Submit AW07APYP.

The PTFs are applied.

9. (Optional) Open the SAMPJCL member AW08ACCP in an edit session and execute the AW0SEEDIT macro from the command line.

AW08ACCP is customized.

10. (Optional) Submit AW08ACCP.

The PTFs are accepted.

Note: You do not have to submit the job at this time. You can accept the PTFs according to your site's policy.

Note: We recommend that you check for available maintenance; however, you may find that none is available.

HOLDDATA

When you apply maintenance, you typically encounter SMP/E HOLDDATA. We use HOLDDATA to notify your SMP/E system of SYSMODs that have errors or special conditions. We support system and external HOLDDATA.

System HOLDDATA

System HOLDDATA indicates data that is an in-stream part of the SYSMOD instructing you of special conditions. Examples of system HOLDDATA are as follows:

ACTION

Indicates that you must perform special processing before or after you apply this SYSMOD.

DEP

Indicates a dependency for this SYSMOD that you must externally verify.

DELETE

Deletes the SYSMOD load module. You cannot reverse this type of SYSMOD with the SMP/E RESTORE command.

DOC

Indicates a documentation change with this SYSMOD.

EC

Indicates that this SYSMOD requires a hardware engineering change. An EC hold SYSMOD usually does not affect the product unless the EC is present on the hardware device.

Code a bypass operand on your APPLY command to install SYSMODs that have internal holds. Only code the bypass operand after you have performed the required action, or if you are performing the action after the APPLY, if that is appropriate.

External HOLDDATA

External HOLDDATA is not part of the PTF. It resides in a separate file. It is commonly used for SYSMODs that have been distributed and later are discovered to cause problems.

Download the external HOLDDATA from CA Support Online to a DASD file, and allocate the file to the SMPHOLD DD statement. To take care of the external HOLDDATA, receive it into your SMP/E environment. If you use the jobs supplied by CA, SMP/E receives the HOLDDATA.

If a SYSMOD has an unresolved hold error, SMP/E does not install it unless you add a bypass to your APPLY command. You can bypass an error hold in situations that are not applicable to you. Error holds that are not applicable to you can include a problem that happens only with a hardware device that you do not have or in a product feature that you do not use.

When you issue the SYSMOD that resolves the hold, the resolving SYSMOD supersedes the hold error. This action lets you apply the original SYSMOD in conjunction with the fixing SYSMOD.

A special HOLDDATA class called ERREL exists. We have determined that the problem fixed by the SYSMOD is more important than the one that it causes. We recommend that you apply these SYSMODs.

To reliably manage external HOLDDATA, allow SMP/E to manage it automatically. The only manual task is running a REPORT ERRSYSMODS. This report identifies any held SYSMODs already applied to your system. If the resolving SYSMOD is in RECEIVE status, SMP/E identifies the SYSMOD to apply to correct the situation.

CA Common Services Specific Post-Installation Requirement

After performing the installation for Agent Technology and Event Management, perform the tasks found in the chapter [Agent Technology and Event Management Post-Installation](#) (see page 72). The Agent Technology and Event Management Post-Installation must be done before their deployments.

Deploy Products

You should deploy all SMP/E target data sets created during the SMP/E installation process by making copies of them (at least once) available on the targeted system where the CA Common Services components are to execute.

If the component is to execute on multiple systems, at a minimum, you must make the copies available through shared DASD on the targeted system. However, in some cases you may want to make multiple copies of some or all of the SMP/E target data sets for configuration purposes.

Most CA Common Services SMP/E target data sets can be identified by their lowest level qualifier which begins with the letter C followed by a 3-character pax file identifier, AWO, CCS, or NSM. Review the chapter concerning the storage requirements for a complete list of SMP/E target data sets.

Important! Before deploying the SMP/E target data sets, confirm that the targeted system meets the system requirements for the products you are deploying.

If you installed Agent Technology, Event Management or the version of Tomcat shipped with CA Common Services, see the section in this chapter concerning the deployment of USS zfs data sets.

After deploying the SMP/E target data sets, go to the chapter, [Configuring Your Product](#) (see page 111).

Deploying USS file systems

To deploy a product that uses USS

- Use the SMP/E CSI and its SMP/E target USS environment to track software changes only.
- For Agent Technology and Event Management, you must perform post-installation steps before you can deploy the SMP/E target data sets.
- Create copies of the USS zfs data sets on the installation or another machine to be used by the executing CA Common Services component.

Use the following procedure to copy your USS zFS data sets. This procedure assumes that the CA Common Services component that uses USS has been successfully installed on the installation z/OS image.

1. Make copies of the CA Common Services BASE load libraries, CAWOLINK, CAW0LOAD, CAW0LPA and CAW0PLD available on the targeted system.

If you are deploying Agent Technology or Event Management, copies of the MFNSM load libraries, CNSMLOAD and CNSMPLD as well as the CNSMJCL, CNSMOPTV, and CNSMPROC must also be available.

2. Create backup copies of your SMP/E USS z/FS data sets. The USS z/FS data sets are linear VSAM. Use IDCAMS REPRO to back up the data sets.

Before creating the backup do the following:

- Confirm that there are no CA Common Services components using the USS file system being backed up.
 - For Agent Technology, confirm that all post-installation tasks have been completed.
 - For Event Management, confirm that all post-installation tasks have been completed.
3. Tailor and submit the SAMPJCL member on the targeted system to allocate and format the zFS data sets.
 - For Agent Technology use B6D1ALLU
 - For Event Management use D5I1ALLU
 - For Tomcat use EG11ALLU
 4. Tailor and submit the SAMPJCL member on the targeted system to create the mount points and mount the zFS data sets created in the previous step in READ/WRITE mode.

The READ/WRITE mount is to perform configuration.

Only the mount point directories need to be created on the targeted system.

Delete any steps that create additional directories.

- For Agent Technology use B6D 2MKD
 - For Event Management use D5I2MKD
 - For Tomcat use EG12MKD
5. Restore the backups created in Step 2 into the newly allocated zFS data sets on the targeted systems.
 6. Update your BPXPRMxx member on the targeted system with the MOUNT directories for the new zFS data sets.
 - Mount zfs data sets with RO in their DSName as read only.
 - Mount zfs data sets with RW in their DSName as read/write.

Deploying Agent Technology on Multiple Systems

If you are installing multiple systems, you have two choices for Agent Technology:

- Do a complete installation on each system. This provides separate CSIs for tracking each system independently.
- Track the software using the existing CSI and simply install copies on the other machines.

If you employ the second option, make use of the Agent Technology Read-Only zFS which was created, formatted and mounted by SAMPJCL jobs B6D1ALLU and B6D2MKD. The Read-Only zFS contains all executable programs and can be shared among multiple systems. Thus, only the Read-Write zFS (which is relatively small) needs to be copied to the second and successive systems in order to run the Agent Technology services. This zFS structure also simplifies product maintenance procedures because nearly all updates need to be applied to the shared Read-Only zFS only.

Copy Your Agent Technology Installation

Use the following procedure to copy your Agent Technology services installation onto a second z/OS image. This procedure assumes that Agent Technology services have been successfully installed and tested on at least one z/OS image.

To copy your Agent Technology installation

1. Confirm that the target system meets the minimal system requirements for z/OS Agent Technology.
2. Backup your existing Agent Technology zFSs on the source LPAR. This backup should be taken when the Agent Technology services are down, after the `aws_admin` Store has been properly initialized and the Agent MIBs have been loaded. The zFS files are VSAM linear data sets. Use IDCAMS REPRO to back up the data sets.
3. Make the Agent Technology CNSMLOAD, CNSMJCL, CNSMOPTV, and MIBLIB partitioned data sets accessible on the target system, either through shared DASD or by copying the files.
4. Tailor and submit CNSMJCL(B6DI0015) on the target system to define the user ID AWADMIN and group AWGROUP to the security system, if required.
5. Tailor and submit SAMPJCL(B6D1ALLU) to allocate and format only the Read-Write zFS on the target system. Be sure to remove the steps that allocate and format the Read-Only zFS (jobsteps DEFINRO and FMTR0).
6. Restore the backup file of the Read-Write zFS from Step 2 into the newly allocated Read-Write zFS on the target LPAR
7. Tailor and submit SAMPJCL(B6D2MKD) to create the mount points for the zFS files and mount the RW zFS just created and formatted. Remove the step that mounts the RO zFS.
8. Make the Read-Only zFS, which was created by the initial installation, available to the target system in read-only mode.
9. Update your BPXPRMxx member on the target system to add the MOUNT directories for the new zFSs.
10. Perform the following configuration tasks on the target LPAR:
 - a. Modify your `agentworks.profile` script in the root Agent Technology directory to reflect the new environment.
Pay particular attention to the environment variables:
 - `AWORKS_MVS_PREFIX` designates the prefix for your Agent Technology z/OS files.
 - `AGENTWORKS_DIR` designates the Agent Technology home directory.
 - `RESOLVER_CONFIG` designates the DSN for the `TCPIP.DATA` file. This reference must correlate to the DSN specified by the `SYSTCPD DD` statement for the TCP stack running on the new system. A member name must be included if the data set is a PDS.

- b. Modify member ENVFILE in your CNSMOPTV. If you share your CNSMOPTV between multiple z/OS images, you may need to create a new unique member for the new system. This is the case only if you need to modify the contents on the ENVFILE member for the new LPAR. When modifying or creating this file, pay particular attention to AGENTWORKS_DIR, which designates the Agent Technology root directory.
 - c. Modify all scripts, configuration files, and JCL members as necessary for the target LPAR.
 - Scripts--Aside from the changes to the agentworks.profile script mentioned previously, you may also need to modify your install_mibs script located in the \$AGENTWORKS_DIR/services/tools directory to include or exclude agents that either will or will not be running on the target system.
 - Configuration Files--The file most likely to require change is the aws_sadmin.cfg file. This file, located in the /cai/agent/services/config/aws_sadmin directory, contains the trap destinations where traps will be sent, as well as SNMP community strings.
 - JCL--If JCL changes are required, such as to reference a different ENVFILE, you should create a unique copy of the JCL for the new system.
 - d. The process of copying and restoring the Read-Write zFS to a new system image also copies the aws_sadmin Store files. This is not appropriate for your target systems unless you are running the same releases of agents across all your systems. If you are running different releases, you need to run the procedures found in the previous section titled Build the aws_sadmin Store files.
 - e. Within UNIX System Services, after the agentworks.profile script has been invoked, run the awftest tcpip utility. This utility verifies that the TCPIP stack has been properly configured. Do not attempt to start your Agent Technology services until this utility runs without error.
11. Start your Agent Technology services on the target LPAR.

Deploying Event Management on Multiple Systems

If you want to run Event Management on multiple systems, you have two choices:

- Do a complete installation on each system. This provides separate CSIs for tracking each system independently.
- Track the software using the existing CSI and simply copy the installation target data sets to the other machines.

Install Event Management on another system after completing all the installation and configuration steps on the first system.

To deploy Event Management on multiple systems

1. If you are using Calendars or Message Actions, see the *CA Datacom/AD Installation Guide*. Start the repository address space and JAVA GUI before using Event management on your target system.

Initialize the Repository before the Event Management components start, or you may get startup error messages.

The Repository address space should be started as a long running batch job or as a started task. The caiopr daemon starts without the Repository address space running, but the Calendar daemon does not.

2. Ensure that the mount points for the READ ONLY and READ/WRITE zFS are identical on the source and target systems.
3. Check the System Requirements on the target system.
4. Back up the READ/WRITE Event Management zFS files, if you have not already done so.
5. Make the BASE CAW0LOAD and CAW0PLD, and the MFNSM CNSMLOAD, CNSMPLD, CNSMPROC and CNSMJCL partitioned data sets accessible, either through shared DASD or by copying the data sets.
6. Allocate new Read/Write zFS data sets on the target system and restore the READ/WRITE Event Management zFS backups into the newly created zFS data sets. Mount the READ ONLY zFS and READ/WRITE zFS.

Review the bullets carefully to determine proper mount criteria. Remember to update your BPXPRMxx member on the target system to add MOUNT directories for the READ/WRITE zFS (MODE RDWR) and the READ ONLY zFS (MODE READ).

- If you want to use the Java GUI with the target system, the READ ONLY zFS must be mounted as READ/WRITE, and the READ/WRITE zFS must be mounted as READ/WRITE. Then run the batch *yourdeployHLQ.CNSMJCL* job D5I10065 on that system.

- The READ ONLY zFS may be mounted as READ ONLY or READ/WRITE, and the READ/WRITE zFS should be mounted as READ/WRITE. Run the batch *yourdeployHLQ.CNSMJCL* job D51FWMIG on the target system. This creates the required directories for this system. Check STDOUT and STDERR for the results. If the READ ONLY zFS was mounted READ ONLY, the STDERR file will contain informational messages which can be ignored. Prior to running this script, ensure that all Event Management tasks are shut down.
7. Ensure that you are using the correct CAIGLBL0000 and STEPLIB by reviewing the Modification made by CA Common Services in /etc/profile. If necessary, remove the sections that do not contain the correct CAIGLBL0000 and STEPLIB. These could be left over from a previous installation.
 8. Copy your started tasks or batch job to the new system if you are starting the Repository address space. Review your JCL/PROC to ensure that the correct data sets and libraries are specified.
 9. Create a security account for the Java and Web servers with these attributes if you use the JAVA GUI.
 - UID zero - The user identity that runs the Java server and the web server must be defined with real UID zero. You cannot assign a non-zero UID and permit the user access to the BPX.SUPERUSER resource.
 - Any valid group ID (GID)
 - Any valid home directory (the directory where you install for z/OS is a good choice)
 - Any valid shell program, typically /bin/sh
 - READ permission to IBM FACILITY resources BPX.SUPERUSER, BPX.DAEMON, and BPX.SERVER, if you implement any of these features; optionally, surrogate permission to any users that are to be signed on without password checking by the server
 10. Copy your started tasks or batch jobs for the web server and Java server to the new system if you use the JAVA GUI.
 11. Access the Event Management GUI by starting a web browser session with a URL of this form: `http://<host_name>:<port_number>` where *host_name* is the name or IP address of the host running the web server, and *port_number* is the number you assigned in the httpd.conf file. It is highly recommended that a hostname be used rather than a hardcoded IP address. If you accept the default port of 80, you can omit the port number.

Chapter 5: Configuring Your Product

This section describes the minimum configuration tasks needed before CA Common Services for z/OS can be started, customized, and used in your environment.

You should configure the CA Common Services components using the deployed data sets.

Configuration Steps

For information concerning APF authorizing data sets and adding data sets to the LINK list and LPA, See IBM's *z/OS MVS Initialization and Tuning Reference* manual.

To configure your system before starting CA Commons Services for z/OS

1. APF Authorize Data Sets
 - a. Determine if your site is using SYS1.PARMLIB member IEAAPFxx or PROGxx to specify the APFlist.
 - b. Add the following data sets that apply to the SYS1.PARMLIB APF list member your site is using:
 - *YourdeployHLQ.CAW0LOAD* – BASE component Installation
 - *YourdeployHLQ.CCCSLOAD* – LEGACY component Installation
 - *YourdeployHLQ.CNSMLOAD* – MFNSM component Installation
 - *YourdeployHLQ.CAW0PLD* – BASE component Installation
 - *YourdeployHLQ.CNSMPLD* – MFNSM component Installation
 - *YourdeployHLQ.CAW0DCM* – BASE component Installation - CAIENF
 - *YourdeployHLQ.CAW0LINK* – BASE component Installation

Important! Failure to APF authorize these data sets can result in the incorrect completion of later jobs in the configuration process or the failure to start address spaces.

2. LINK LIST Data Sets

- a. Determine if your site is using SYS1.PARMLIB member LNKLSTxx or PROGxx to specify the LNKLST concatenation.
- b. Add the following data sets that apply to the SYS1.PARMLIB LINK list member your site is using:
 - YourdeployHLQ.CAW0LINK – BASE component Installation
 - YourdeployHLQ.CCCSLINK – LEGACY component Installation
 - YourdeployHLQ.CNSMLOAD - MFNSM component installation

3. Add CAW0LPA to the LPA library list

- Add data set YourdeployHLQ.CAW0LPA to your SYS1.PARMLIB LPALSTxx member

4. Perform Component Configuration Steps. See the following Configuration chapters for specific tasks to perform for CA Common Services components:

- [CAIRIM Configuration Tasks](#) (see page 115)
- [CAIENF Configuration Tasks](#) (see page 123)
- [CAICCI Configuration Tasks](#) (see page 131)
- [Event Management Configuration Tasks](#) (see page 159)
- [Agent Technology Configuration Tasks](#) (see page 183)
- [CA Global SubSystem Configuration Tasks](#) (see page 197)
- [CA-L-Serv Configuration Tasks](#) (see page 219)
- [Other Configuration Tasks](#) (see page 237)

5. Save All Materials and Outputs.

This is an important step so that you will have information available for maintenance and upgrade purposes.

6. Perform CA Datacom/AD Installation.

- If you previously installed the version of CA Datacom/AD being shipped with this release of CA Common Services, you do not need to re-install CA Datacom/AD. However, you may still need to perform CA Datacom/AD customization for CAIENF and/or Event Management. See chapter [Install CA Datacom/AD](#) (see page 245).

Installation of CA Datacom/AD is optional for ENF and Event Management but certain ENF and Event Management options require the use of the CA Datacom/AD database.

For ENF, CA Datacom/AD is required to record events.

If you are not sure that you record events at your site, you can check your ENFParms file and see if RECORD(YES) is specified. In addition, you can check your previous ENF release database to see if any event types have a record count above zero. To check the previous database, use the CAS9DB LIST DETAIL report. The following CAS9DB JCL can be used if the previous release of ENF is up and running:

```
//CAS9DB EXEC PGM=CAS9DB,REGION=4M
//STEPLIB DD DISP=SHR,DSN=yourHLQ.CAW0LOAD <=Update
//DBOUT DD SYSOUT=*
//DBIN DD *
LIST DB(*) DETAIL
/*
```

- For Event Management, CA Datacom/AD is required with the Calendars or Message Actions option. If you will use Calendars or Message Actions, you must set the environment variable CA_OPR_ZOSDB to Y in the PROFILE file in the Event Management zFS installation directory. This should have been done in the Event Management configuration step associated with CNSMJCL member D5I10050. If it was not, the environment variable can be set at any time before starting Event Management.
- Since CA Datacom/AD requires CA Common Services, you must complete the CA Common Services Configuration procedures for the CA Common Services components before installing CA Datacom/AD.

CA Datacom/AD requires the following CA Common Services Components:

- CA C-Runtime
 - CAICCI
 - CAIRIM which includes CA LMP and CAISSF
- Use the version of CA Datacom/AD distributed with the CA Common Services installation and follow the instructions in chapter [Install CA Datacom/AD](#) (see page 245).

Note: For the installation of CA Datacom/AD, see the *CA Datacom/AD for z/OS r12 Installation and Maintenance Guide*.

Chapter 6: CAIRIM Configuration

After installing CA Common Services for z/OS, configuration tasks for CAIRIM may include modifying the initialization parameters, customizing CAISSF for RACF products, and starting CAIRIM. Use your deployed data sets when performing these tasks.

This section contains the following topics:

[CAIRIM Initialization Parameters](#) (see page 115)

[Customize CAISSF for RACF or RACF-Compatible Products](#) (see page 117)

[Start CAIRIM](#) (see page 121)

CAIRIM Initialization Parameters

You may need to modify the CAIRIM initialization parameters. This task is required if you are installing CAIRIM and intend to execute the CAS9 procedure. If you are installing CAIRIM on behalf of another service, without intending to run CAIRIM, you do not need to perform this task.

Each solution initialized by CAIRIM is defined through an entry in the CAIRIM parmlib member (found in *YourdeployHLQ.CAW0OPTN*), described as the member CARIMPRM in our sample proc. Your solution-specific installation documentation provides you with the specific CAIRIM parm definition (if required by the CA solution) for the solution and services you are installing. Any requirements for the ordering of statements are included in the instructions supplied with your CA solution.

Two general rules are followed by all CA software solutions that can be run using CAIRIM:

- **Rule 1**--Services must be initialized before products. For example, if CA Scheduler uses ADAPTER and OMS, both ADAPTER and OMS initialization statements must precede the CA Scheduler initialization statement.
- **Rule 2**--If a previously installed CA solution has already included one or more services also used by a subsequent solution, the statements already present are used and additional statements are not added for the services.

The following parameter structure for initialization statements is used for all software solution and service definitions:

```
PRODUCT(desc) VERSION(vers) LOADLIB(dsn) INIT(name) PARM(parm)
```

Important! CAIRIM control statements cannot go beyond column 72. Control statements can be continued on the next line by placing a dash (-) at the end of the line, but a keyword and its operands that are contained within parentheses must be on the same line.

Example

```
PRODUCT(desc) VERSION(vers) LOADLIB(dsn) -
INIT(name) PARM(parm)
```

Parameter	Required?	Description
<i>desc</i>	Required	Solution or service description (up to 20 characters). This parameter is specified once for each product to be installed.
<i>vers</i>	Required	Four-character identifier, consisting of a two-character solution or service code plus a two-character version code.
<i>dsn</i>	Optional	Data set name for solution or service load modules. If the modules are in LINKLIST or the CAIRIM procedure STEPLIB, then the LOADLIB parameter need not be specified.
<i>name</i>	Optional	Name of initialization routine. By default, the name of the initialization module is the version information plus 'INIT'. Thus for solution KO42, the initialization module would be KO42INIT. The INIT parameter needs to be specified only if the default module name is not appropriate.
<i>parm</i>	Optional	Special parameter to be passed to the initialization routine. This parameter is used for any custom solution function such as re-initialization or deactivation. Up to 32 characters can be passed in the PARM field.

Note: The LOADLIB parameter causes the tasklib for the indicated install program to be switched to that data set, which must be APF-authorized. Therefore, if LOADLIB is used, the INIT program and associated CAIRIM program modules must be either in LINKLIST or in the library described by the LOADLIB statement. If the INIT program and associated CAIRIM program modules are only in a CAIRIM STEPLIB, an ABEND S806 occurs.

Customize CAISSF for RACF or RACF-Compatible Products

This task is required if you plan to use CAISSF with RACF or RACF-compatible security software. If you are using CA Top Secret or CA ACF2, you can skip this task.

Customizing CAISSF for RACF may include the following activities:

- Modify CAS9SAFC/CAS9RACL for CICS TS
- Modify and Submit the CAS9CSSF Sample JCL
- Modify RACF or the RACF-Compatible Product
- Optionally Place the CAISSF Routines in CSA
- APF Authorize the CAISSF Load Library

The Standard Security Facility (CAISSF) is a sub-service of the CAIRIM service (FMID CAS9E00). Following the completion of this task, the Standard Security Facility for RACF and RACF-compatible products is installed and ready for use for each CA solution.

The security interface provided for RACF and RACF-compatible products, CAS9SAFC, is shipped in both object and source format. The source for CAS9SAFC resides in the CA Common Source library, *YourdeployHLQ.CAW0SAMP*.

Note: The security translators for CA ACF2 and CA Top Secret, CAS9ACF2 and CAS9TS42 respectively, are provided on the installation tapes of these CA solutions. Accordingly, support for these security translators, if needed, should be obtained through support for the appropriate CA solution. For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact CA Support.

The translator for RACF and RACF-compatible solutions may not require modification.

CAS9SAFC/CAS9RACL for CICS TS

If the product for which you are installing CAISSF does not require RESOURCE ACCESS processing, you can skip this task.

The CAS9SAFC translator for RACF and RACF-compatible products, as shipped, executes in a TSO, BATCH, CICS, CA Roscoe Interactive Environment, or any single-user address environment. The following modifications are required for CICS.

The CAS9RACL PLT application is required for products using the RESOURCE ACCESS function. The PLT program, CAS9RACL, RACLISTs all classnames found in the table CASRTBL. Even though the CAS9SAFC translator is invoked to issue the RESOURCE ACCESS check (using the RACF macro FRACHECK), it cannot issue a RACLIST to bring the associated classname profiles in storage because CICS runs unauthorized. To RACLIST the required classnames for RESOURCE ACCESS processing, you need to define the CAS9LRAC, CAS9RACL, and DFHSIP programs to RACF through the RACF authorized callers table

Note: If there are changes to any classname profiles CAS9RACL has RACLISTed, the CICS region must be recycled.

Install CAS9RACL

To install CAS9RACL

1. Edit the source member, CAS9RACL, in the CA Common Source Library, *YourdeployHLQ.CAW0SAMP*.
2. Locate the table identified by label RACLTBL.
3. Add the required CA solution classnames to this table as defined by your solution-specific documentation.
4. Modify and Submit member CAS9CSSF in the *YourdeployHLQ.CAW0JCL* data set.
CAS9RACL is installed when you submit CAS9CSSF. Read the JCL comments in CAS9CSSF for instructions on which steps should be executed to install CAS9RACL.
5. Add programs DFHSIP, CAS9LRAC, and CAS9RACL to the RACF authorized callers table, ICHAUTAB, for the RACLIST privilege only.
6. Define the CAS9LRAC program to your current startup and shutdown PLT for CICS using the following entry:

```
DFHPLT TYPE=ENTRY, PROGRAM=CAS9LRAC
```

Add the same entry to your PLT shutdown member, so all classes RACLISTed during CICS startup are deleted at shutdown.

Sample PLT members S910PLT and S910PLTS are furnished in *YourdeployHLQ.CAW0OPTN* for reference.

7. Define the CAS9LRAC program to your current PPT for CICS using the following entry:

```
DFHPPT TYPE=ENTRY, PGMLANG=ASSEMBLER, PROGRAM=CAS9LRAC
```

A sample PPT member, S910PPT, is furnished in *YourdeployHLQ.CAW0OPTN* for reference.

8. Make program CAS9LRAC accessible through DFHRPL and CAS9RACL accessible through STEPLIB or LNKSTxx of your CICS job control.

CAS9RACL is installed.

Modify and Submit the CAS9CSSF Sample JCL

Modify and submit the sample JCL in the member CAS9CSSF, which is located in the library *YourdeployHLQ.CAW0JCL*.

If you uncommented the corresponding JCL statement containing the exec statement for the procedure, member CAS9RACL is installed when you submit CAS9CSSF.

Modify RACF or the RACF-Compatible Product

The product for which you are installing CAISSF has product-specific classnames that need to be installed into RACF or the RACF-compatible product. You should refer to your product-specific documentation for information on the required classnames. The product classnames must be added to the RACF class descriptor table, ICHRRCDE, and to the RACF SAF router table, ICHRFRTB.

The following examples display what you need to code. The examples use classname CACMD. These are only examples. The product that is using CAISSF may not require this classname.

Note: Control statements can be continued on the next line when a dash (-) is placed at the end of the line to be continued.

Example 1: Class Descriptor Table Entry for CACMD

```
CACMD  ICHERCDE  CLASS=CA@MD,      -
                {GROUP=DFTGRP, }  -
                MAXLNTH=8,        -
                FIRST=ALPHANUM,   -
                OTHER=ANY,        -
                OPER=NO,          -
                DFTUACC=NONE,     -
                ID=CLASS_NUMBER,  -
                POSIT=19-255
```

Example 2: SAF Router Table Entry for CACMD

```
CACMD  ICHRFRTB  CLASS=CA@MD,  -
                ACTION=RACF
```

Place the CAISSF Routines in the Common Service Area (CSA)

If desired, the CAISSF routines (CAS9SEC) and the security translator (CAS9SAFC for RACF, CAS9TS42 for CA Top Secret) may be optionally placed in CSA.

Note: CA ACF2, by installation default, requires its translator, CAS9ACF2, to reside in PLPA. Therefore, external security does not load this routine.

Placing CAISSF routines in CSA provides the following advantages:

- Ensures the latest versions of the CAISSF routines are loaded and executed
- Allows one set of CAISSF routines to be used across all address spaces for CA solutions that require CAISSF
- Gives the ability to reinitialize CAISSF routines through execution of CAIRIM, if maintenance is applied
- Gives the ability to delete CAISSF routines through execution of CAIRIM (if desired)

The CAISSF Installation Process

While installing the CAISSF routines, the system performs the following actions:

- The installation of the CAISSF routines into CSA is accomplished through execution of CAIRIM (the CAS9 procedure). A CAIRIM initialization routine, CAS9INIT, loads the CAISSF routines into CSA.
- Before executing the CAS9 procedure, add the following CAIRIM input initialization control statement to member CARIMPRM in the *YourdeployHLQ.CAW0OPTN* data set.

```
PRODUCT(CAIRIM) VERSION(CAS9) INIT(CAS9INIT)
```

- Later, when you start the CAS9 procedure, CAIRIM attaches the CAISSF initialization routine. This in turn loads the CAISSF routines into CSA if they are present in the CAS9 STEPLIB or a link-listed data set.

Note: If you do not use the optional installation of the CAISSF routines into CSA, the first APF-authorized caller of CAISSF unconditionally causes the CAISSF routines to be loaded into CSA. If you do not use the CAS9 procedure (CAIRIM) to install the CAISSF routines, you lose the ability to delete or refresh the CAISSF routines. If you do not use the optional placement of the CAISSF routines in CSA, the CAS9 procedure (CAIRIM) does not need to be executed.

Start CAIRIM

Copy the CAS9 proc from *YourdeployHLQ.CAW0PROC* to a valid system procedure library if it is to be invoked as a started task.

Important! If you are currently running a lower version of CAIRIM, an IPL is necessary before starting CAIRIM using the new libraries.

Important! If CAIRIM and DATACOM are already running when you start CAIRIM, you might receive an error message similar to the following:

```
SVC NUMBER SELECTED IS ALREADY IN USE. SVC 254 IS AVAILABLE FOR USE.
```

The result is Datacom error: Init error: CA-DATACOM. This problem will disappear after the next system IPL, so you can ignore this error until the next IPL.

Note: For more information about starting CAIRIM, see the *Administration Guide*.

Chapter 7: CAIENF Configuration

After installing CA Common Services for z/OS components, configuration tasks for CAIENF may include the following:

Note: Use your deployed data sets when performing these tasks.

- Customizing the CAIENF procedure
- Starting CAIENF
- Customizing the ENFSNMPM procedure
- CAIENF/USS configuration steps
- Customizing CA Datacom/AD for CAIENF

In addition, if you have other CA Technologies products that use CAIENF, see the individual product documentation for any related setup requirements, such as DCMs or control options.

This section contains the following topics:

[Customize the CAIENF Procedures](#) (see page 124)

[Configure CAIENF Parameter File](#) (see page 126)

[Configure CAIENF JCL for finding CA product DCMs](#) (see page 127)

[Start CAIENF](#) (see page 128)

[Prepare for Component Tracing](#) (see page 128)

[CAIENF/USS Configuration Tasks](#) (see page 129)

[Customize the ENFSNMPM Procedure](#) (see page 129)

Customize the CAIENF Procedures

This task is required if you are installing CAIENF, CAIENF/CICS, CAIENF/DB2, CAIENF Utilities, or CAICCI.

To customize the CAIENF procedures

1. Customize the CAIENF procedures for the CAIENF, CAIENF/CICS, and CAIENF/DB2 services.

The CAIENF procedures are found in the *Yourdeploy*HLQ.CAWOPROC library. Each procedure runs as a started task in its own address space.

CAWOPROC contains three CAIENF procedures; ENF, ENFXMUF, and ENFIMUF. Select the procedure that applies to your site's requirements.

ENF - Use the JCL found in this procedure when you do not wish to record events or install CA Datacom/AD.

ENFXMUF - Use the JCL found in this procedure when you wish to record events. CA Datacom/AD is installed and the MUF is external (runs in its own address space) to ENF.

ENFIMUF - Use the JCL found in this procedure when you wish to record events. CA Datacom/AD is installed and the MUF is internal (runs under the ENF address space) to ENF.

2. Access each procedure and edit it to conform to user solution standards.

Symbolics

Below are the symbolics used in the ENF procedure. Modify each symbolic as necessary.

Symbolic	Description	Default
CAW0LOAD	CAIENF Load Library	'CAI.CAW0LOAD'
CAW0DCM	CAIENF DCM Library	'CAI.CAW0DCM'
CAW0OPTN	CAIENF Options Library	'CAI.CAW0OPTN'
ENFPARM	The member defined in the OPTLIB data set containing CAIENF control options.	'ENFPARM'
ENFCMDS	The member defined in the OPTLIB data set containing auto commands.	'ENFCMDS'
OUTC	SYSOUT class specifications	'*'
optional	Dependent upon the CA solution installed. See the CA solution-specific documentation for more information.	n/a

Symbolic	Description	Default
CCIPARM	CAICCI initialization parameter member	CCIPARM
SPNPARAM	CAICCI Spawn initialization parameter member	SPNPARAM
SYSTCPD	TCP/IP DATA DATA SET	'TCPIP.TCPIP.DATA'

CAW0LOAD, CAW0DCM, CAW0OPTN

Update the default value with your deployed data set High Level Qualifier.

ENFPARM DD

ENFPARM is used to identify DCMs required for event processing as well as specify CAIENF control options that are processed during CAIENF startup. In addition to the ENFPARMs, CAIENF uses parameters obtained from the operator start command and from the EXEC JCL statement. The ENFPARM DD statement should point to a file that contains any number of 80-byte CAIENF commands.

For more information on configuring DCM statements, see the *Administration Guide*.

Note: Commands entered by the EXEC JCL statement or the z/OS start command, override entries found in the parameter file.

ENFCMDS

Used to specify z/OS operator commands that are to be executed after CAIENF initialization. Enter commands in ENFCMDS exactly as you would on the operator console.

ENFCMDS DD statement

Describes a data set containing a list of z/OS operator commands to be issued after CAIENF has successfully initialized. The default procedure describes the ENFCMDS member of *YourdeployHLQ.CAW0OPTN*.

ENFCMDS file

Coded as one z/OS command per line, exactly as it would be issued from the operator console. This file recognizes comments to be any line with an asterisk (*) in column 1.

For example, the following would be a valid command for starting CA Scheduler:

```
Col 1
  v
  * Executes the CA Scheduler procedure
  START CASCHD
```

Commands within the ENFCMDS file are issued only during initial CAIENF startup. If the CAIENF Started Task is restarted for any reason, the auto-commands in the ENFCMDS file are not issued.

An optional ENFDUMP DD statement can be coded to override CAIENF dynamic allocation for dump processing.

Typically, each time the CAIENF command DUMP is entered, a SYSOUT data set is dynamically allocated according to the SYSOUT control option. If desired, the ENFDUMP DD statement can be specified to force dumps and other diagnostic data to be recorded on a DASD or tape data set. This data set, if coded, must have a blocksize that is some multiple of 133 and a record format of FBA.

Configure CAIENF Parameter File

The CAIENF parameters allow you to customize and control various aspects of the way CAIENF will perform its functions. Some of these parameter settings need to be done based on the requirements of the CA products that you will be running on the system. CA product CAIENF parameter requirements are covered in the software requirements sections in the specific CA product documentation.

Each CAIENF parameter is documented in *CA Common Services for z/OS Reference Guide*, in the CAIENF Chapter, in the Control Options section.

If any of the CA products that are running on the system perform CAIENF event recovery, these products will have instructions that require CAIENF event recording to be enabled (RECORD(YES) parameter). If event recording needs to be enabled, then ENF must be run with a CA Datacom/AD database. See the chapter [Install CA Datacom/AD](#) (see page 245) on preparing a CA Datacom/AD MUF and database for use with CAIENF. If event recording is not required, then the ENF parameter NODB can be set. NODB will instruct ENF to start without trying to establish a connection to a CA Datacom/AD MUF.

If you are upgrading from a CA Common Services for z/OS release prior to release 12.0, you can use a tool called ENFUTIL to help create the CAIENF control options that replace old CAS9DB functions that existed for CAIENF on releases prior to release 12.0. The ENFUTIL utility has been provided to create the DCM and EVENT control option statements starting with CAIENF release 12.0. This utility uses a CA Common Services release 11 DB detail listing as input. For Special DCM and EVENT Utility details, see the *Reference Guide*.

The ENFUTIL output file will be a list of CAIENF DCM and EVENT control options statements that will match the settings that used to be stored on the CAIENF database on CAIENF releases prior to release 12.0. These statements can then simply be placed at the back of the CAIENF parms file.

Configure CAIENF JCL for finding CA product DCMs

The CAIENF procedure includes a DD name //CAIDCM. The CAIDCM DD needs to be configured such that it is a concatenation of CA Common Services and CA product load libraries that contain required CAIENF DCM load modules. The first load library in the concatenation should always be the CA Common Services for z/OS CAW0DCM load library.

Example

```
//CAIDCM DD DISP=SHR,DSN=&CAW0DCM
//      DD DISP=SHR,DSN=ISLPROD.SCHEDULR.R11000.CAILOAD
//      DD DISP=SHR,DSN=SYSISL.CPM30.SP04A.CAIPDSE
//      DD DISP=SHR,DSN=BSTPROD.CA13.R1106.DISPATCH.LINKLIB
```

CA Product DCM compatibility

CA Products that deliver CAIENF DCM load modules must have DCM statements defined in the CAIENF control options for the DCMs to take effect. DCMs can do the following:

- Define events to CAIENF
- Define applications that CAIENF needs to start after CAIENF initialization is complete
- Define both events and applications.

DCMs that define events must be compatible with CAIENF Release 12.0 and above. See the *CA Common Services for z/OS Readme* document, in the Apply Necessary Fixes section, for a list of CA product PTFs that are required for CAIENF Release 12.0 and above compatibility. If your DCM supplying CA product is in the Readme list and you are running a release of the product higher than the one indicated in the Readme table, the base product level has the compatibility already built in.

Start CAIENF

If a CAIENF procedure is to be invoked as a started task, it must be copied to a valid system procedure library. The ID associated with the ENF started task must have a valid security OMVS segment defined.

Three sample procedures are provided for CAIENF. They are ENF, ENFXMUF, and ENFIMUF.

The JCL associated with the ENF procedure contains no references to CA Datacom/AD database data sets and should be used in conjunction with the CAIENF control option, NODB. At this point in the configuration of CAIENF, only the ENF procedure is valid to start CAIENF.

The other two procedures ENFXMUF and ENFIMUF, are only valid after the installation of CA Datacom/AD and the configuration of CA Datacom/AD for CAIENF.

If you already installed the release of CA Datacom/AD being shipped with this version of CA Common Services from a prior version of CAIENF, then you need to import this releases version of the CAIENF plan into your existing CA Datacom/AD environment. Make sure to follow the directions in [Customize an Existing CA Datacom/AD for CAIENF](#) (see page 249).

Important! If you are currently running a lower service level of CAIENF, an IPL is necessary before bringing up CAIENF using the new libraries.

Prepare for Component Tracing

By default the CAIENF address space initializes Component Tracing using component name CAIENF. The environment is initialized but tracing must be activated by an MVS TRACE CT command.

The ENF Parm ENFCT can be used to activate and customize the Component Tracing environment including the component name. The Component Tracing parmlib member name can be specified in the ENFCT command to activate tracing. See the *Reference Guide* for instruction on configuring the parmlib member. Typically you would only enable component tracing for ENF at the request of CA Technical Support.

Note: If the external writer proc name is specified in the parmlib member, then the external writer must be configured prior to starting ENF. See the sample ENFXWTR proc in the *Reference Guide*.

CAIENF/USS Configuration Tasks

Two configuration tasks are associated with CAIENF/USS, the first required and the second optional.

To perform the CAIENF/USS tasks

1. Define a security OMVS segment for the user ID assigned to the proc to allow the ENF proc to work.

You can define a new user ID or use a pre-existing one such as the one used for TCP/IP or UNIX System Services.

2. (optional) Update the COFVLFxx member used for the system to add a class for CAIENF/USS to use. For example:

```
CLASS  NAME(CAENFU)
        EMAJ(PATHCACHE)
        MAXVIRT(512)
```

Customize the ENFSNMPM Procedure

This task is required if you will use the ENF SNMP Monitor.

The ENF SNMP Monitor runs as a started task in its own address space. It runs after the primary ENF address space has been brought up. The proc to start the ENF SNMP Monitor is delivered in the *YourdeployHLQ.CAWOPROC* Library as member ENFSNMPM. This procedure should be customized according to user solution standards.

To customize the ENFSNMPM procedure

1. Copy the SNMPVARS member of CAWOOPTV data set to the ENVVAR dsn that will be used by the started task and customize it as needed.

If the ENFSNMPM Monitor will be used with CA Audit, the library containing the eTrust DLLs must be APF authorized as well as the *YourdeployHLQ.CAWOPLD* in which the executable for CAW1SNMP resides. For this reason, these libraries should be invoked through STEPLIB in the proc instead of from the linklist.

If the DLL's exist in a linklisted library and a non-APF authorized STEPLIB, the system will use the linklisted copies, which can cause misleading results when testing.

2. Use the delivered CAWOPROC ENFSNMPM proc as a sample to customize. The previous release of CA Common Services for z/OS used sample procs CAW1SNMP for IPv4 only and CAV6SNMP for IPv6 or IPv4. This release only delivers one proc, ENFSNMPM which can support both IPv4 or IPv6.

3. Add a DCM ENF Parm statement for the CAS9DCM4 data collector in order to use the ENF SNMP Monitor. CAS9DCM4 is delivered in *YourdeployHLQ.CAW0DCM*.
4. Define a security OMVS segment for the user ID associated with the ENF SNMP Monitor started task because it uses TCP/IP. You can define a new user ID to the security package or you can use an existing user ID that already has an OMVS segment definition.
5. Define a TSS ACID with a valid OMVS segment for the ENFSNMPPM procedure. For example, for TSS users:

```
TSS ADD(stc) PROCNAME(ENFSNMPPM) ACID(omvs)
```

where you call your procedure ENFSNMPPM as delivered, you run it as a started task, and OMVS is the proper ACID to use in your environment.

If you do not do this properly, you may get a U4093 ABEND with a reason code of x'90'.

Note: With IPv6 support, you may supply the nodename or IP address in many different ways.

IPv4 IP address examples

141.202.65.31

141.202.66.11

Nodename examples

USILCA11

TCPIP11V

USI286ME.CA.COM

IPv6 IP address examples

::1

fd00:7a06:0a20:0100:0000:0000:0000:0011..1086

0000:0000:0000:0000:0000:ffff:c0a8:060b..1088

Chapter 8: CAICCI Configuration

After installing CA Common Services for z/OS, configuration tasks for CAICCI are needed in order to best implement and maintain CAICCI.

Note: Use your deployed data sets when performing these tasks.

This section contains the following topics:

[CAICCI Tasks](#) (see page 131)

[Peer-to-Peer Communication with Remote Computers](#) (see page 148)

[Verify Your Installation](#) (see page 155)

[Troubleshooting](#) (see page 155)

CAICCI Tasks

Configuration tasks for CAICCI may include:

- Configure and start CAICCI
- Additional Configuration Tasks for CAICCI Version 14.0
- Load CAICCI on the client platform

Configure and Start CAICCI

To configure and start CAICCI

1. Define a valid security OMVS segment to the ID associated with the CCITCP, CCITCPGW, CCISSL and/or CCISSLGW started tasks.
2. Define the following DCM statement in the CAIENF parameter file if not already done in section [Configure CAIENF Parameter File](#) (see page 126).

DCM(CAS9DCM3)

3. Review and update the default CAICCI options that are stored in the data set *YourdeployHLQ.CAW0OPTN* member CCIPARM.
 - Determine if additional or new options may be required for the CA solution you are installing along with the options you have tailored for CAICCI. In particular, any CA solution that utilizes the CAICCI SPAWN facility will provide an associated spawn parameter that must be appended to the SPNPARAM DD statement within the ENF PROC. See your solution-specific documentation for further information.
 - Add the LOGGER command to the CCIPARM, if the CA solution requires Assured Delivery.

Note: For more information about Assured Delivery, see the *Administration Guide*.

- As of Version 14.0, CAICCI supports the use of 64-bit (above the bar) storage. There is the potential for CA solutions to drive CAICCI to allocate and use 64-bit storage for queuing and application buffers. Therefore, the system MEMLIMIT which sets the number of usable virtual pages above the bar for a single address space should be set to a non-zero value such as 2Gigabytes. Specific CA solutions that utilize 64-bit storage will identify their particular MEMLIMIT requirement.

MEMLIMIT can be set in any of the following ways:

- On the JOB or EXEC statement (See *z/OS MVS JCL Reference*)
- Through the MEMLIMIT parameter in the SMFPRMxx parmlib member (See *z/OS MVS Initialization and Tuning Reference*)
- Through the SET SMF or SETSMF commands (See *z/OS System Commands*)
- Through the IEFUSI installation exit (See *z/OS MVS Installation Exits*)

Additional Configuration Tasks for CAICCI

This section describes optional configuration steps that you can perform to complete the installation of CAICCI. Most of these steps are only required if you wish to make use of SSL CAICCI connections between systems. SSL stands for Secured Sockets Layer Protocol. SSL provides CAICCI with a means of sending data utilizing standard encryption algorithms. SSL combined with the proper use of digital certificates, can ensure that data is sent with a high level of encryption and that the receiving node is who it claims to be. You can run the SSL TCPIP protocol without turning on SSL across any of the links. With no SSL links, the TCPSSL and TCPSSLGW protocols behave in exactly the same manner as the TCPIP and TCPIP GW protocols.

Note: For more information about CAICCI link protocols, see the *Administration Guide*.

The Sample Certificates in this section, CCIP12 and CCIRTARM, are an End User certificate and the Root certificate that signs (authenticates) it. The PC also has these same sample End User and Root certificates installed (cci.pem and cciroot.pem). By having these sample certificates residing on the mainframe and PC platforms, it will enable the mainframe server CCISSL to authenticate its PC clients. Likewise, using these same certificates, the mainframe gateway server CCISSLGW can authenticate its remote peer servers. You should generate your own SSL certificates and substitute them for the sample certificates that are provided.

Utilize SSL Communication Links

You can utilize SSL links in your environment. Use FTP or IND\$FILE (binary transfer) to perform mainframe to PC downloads.

To utilize SSL links

1. Download CCIPCS32 and/or CCIPCS64 - See section [Load CAICCI on the Client Platform](#) (see page 146).
2. Copy CCISSL - You need to know the location of your key database (keyring) and stored(stashed) password file.
3. Copy CCISSLGW - You need to know the location of your key database (keyring) and stored(stashed) password file.
4. Copy CCIRTARM
5. Copy CCIP12

Note: See your external security manual for instructions on how to create and add certificate keys to an external keyring if you prefer not to use IBM's Key Database.

Copy CCISSL

The CCISSL file contains the JCL cataloged procedure for executing module CAS9PDGM.

To copy CCISSL

1. Copy member CCISSL from the CAW0PROC data set to a site-specific user proclib from which CCISSL will execute.
2. Edit CCISSL to specify the following:
 - Your data set naming convention for IBM and CA directories
 - The location of your key database (keyring) and stored (stashed) password file
 - Various parameter options (PARM=)

PARM

```
PORT=&PORT,US=&UNSECON,CLAUTH=&CLAUTH,CERT=&CERT,KEYRING=&KEYRING,  
SV=&SSLVERS,CI=&CIPHERS,SSLT=&SSLTRCFN,SSLD=&SSLDUMP,CBDLL=&CBDLL,  
TO=&TIMEOUT'
```

where

PORT= specifies the Listen Port (Default: 1202)

TCP= specifies the single TCP/IP stack name that CCISSL will use. The default is all active TCP/IP stack names.

UNSECON= specifies one of the following:

- NEVER - (default) A connecting CCIPC not supporting and enabled for SSL is denied a connection.
- ALLOW - All connections will be unsecured unless the connecting CCIPC supports and REQUIRES an SSL connection.
- NONSSL – A connecting CCIPC not supporting SSL (pre version 1.1.7) is allowed to connect unsecured. A connecting CCIPC supporting and enabled for SSL will connect secured.
- ONLY - Only unsecured connections are allowed. A connecting CCIPC supporting and requiring SSL is denied a connection This option disables SSL support for this CCIPC server. (CCITCP is CCISSL permanently set to this value.)

CLAUTH= specifies one of the following:

- N (default) - Do not authenticate Client Certificates.
- Y - Do authenticate Client Certificates.
- Pass - Client certificates are not authenticated but are still requested for user exit validation.

CERT= specifies the Server Certificate Label Name:

- '*' - Use a Certificate whose label is CCIPC. If not found, use a Certificate whose label is local to the CAICCI Sysid. If not found, use a Certificate whose label is CAICCI.
- 'label' - Use a Certificate whose name is label.
- "(null)" - Use the SystemSSL default Certificate.

Note: Embedded blanks within Certificate Label Names are not supported.

KEYRING= specifies the name of an external security keyring (Used instead of an HFS key database)

SSLVERS= specifies the version of System SSL that CCISL should use to request SSL services.

- 1 - Version 1 (OS/390 version)
- 2 - Version 2 (z/OS 1.2 version)
- "(null)" - Use highest available version (default)

PROT= specifies which security protocol(s) should be enabled:

- SSL - Only SSL Version 3 (default)
- TLS - Only TLS Version 1
- SSL/TLS or TLS/SSL or S/T or T/S or BOTH - Both SSL Version 3 and TLS Version 1 are enabled.

CIPHERS= specifies one or more SSL (Version 3) ciphers, in the order of usage preference, for CAICCI packet encryption in the form XXYYZZ...

- '01' - NULL MD5
- '02' - NULL SHA
- '03' - RC4 MD5 Export
- '04' - RC4 MD5 US
- '05' - RC4 SHA US
- '06' - RC2 MD5 Export
- '09' - DES SHA Export
- '0A' - 3DES SHA US
- '2F' - 128-bit AES SHA US
- '35' - 256-bit AES SHA US
- IBM - Use System SSL default list: (i.e., 0504352F0A090306020100)
- 3DES - Use System SSL default list putting 3DES at top of list: (i.e.,0A0504352F090306020100) (default)
- AES128 or AES-128 - Use System SSL default list putting 128-bit AES at top of list: (i.e., 2F0504350A090306020100)

- AES or AES256 or AES-256 - Use System SSL default list putting 256-bit AES at top of list: (i.e., 3505042F0A090306020100)

SSLTRCFN= specifies the name of the HFS file where System SSL can write trace entries. (Specifying the file name turns on tracing.)

SSLDUMP= specifies whether SSL packets should be dumped to the Trace File (TRCPRINT):

- No (default)
- Yes

CBDLL= specifies the module name of the dll containing the user exit routine for validating client (and server) certificates.

TIMEOUT= specifies the number of seconds that a connection may remain idle before it is disconnected by CCISSL (or CCITCP).

3. APF-authorize the libraries found in the STEPLIB concatenation which are the CAW0PLD Library containing the CAS9PDGM module, the system SSL Library, and the C and C++ runtime libraries.

This proc must be assigned a user ID that has:

- A UNIX System Services segment.
- Read-write authority to the key database.

Copy CCISSLGW

CCISLWG contains the JCL catalogued procedure for executing module CAS9PDPM.

To copy CCISSLGW

1. Copy member CCISSLGW from the CAW0PROC data set to a site-specific user proclib from which CCISSLGW will execute.
2. Edit CCISSLGW to specify the following:
 - Your data set naming convention for IBM and CA directories.
 - The location of your key database (keyring) and stored (stashed) password file.
 - Various parameter options (PARM=).

```
PORT=&PORT , TCP=&TCP , US=&UNSECON , RMAUTH=&RMAUTH , CERT=&CERT ,
KEYRING=&KEYRING , SV=&SSLVERS , CI=&CIPHERS , SSLT=&SSLTRCFN , SSL
D=&SSLDUMP , CBDLL=&CBDLL '
```

where

PORT= specifies the Listen Port (Default: 1202)

TCP= specifies the single TCP/IP stack name that CCISSLGW will use. The default is all active TCP/IP stack names.

UNSECON= specifies one of the following:

- NEVER - (default) A remote CCI not supporting and enabled for SSL is denied a connection.
- ALLOW - All connections will be unsecured unless the remote CCI supports and REQUIRES an SSL connection.
- NONSSL – A remote CCI not supporting SSL are allowed to connect unsecured. A remote CCI supporting and enabled for SSL will connect secured.
- ONLY - Only unsecured connections are allowed. A remote CCI supporting and requiring SSL is denied a connection. This option disables SSL support for this gateway server. (CCITCPGW is CCISSLGW permanently set to this value.)

RMAUTH= specifies one of the following:

- N - Do not authenticate Remote Certificates.
- (default) - Do authenticate Remote Certificates.
- Pass - Remote certificates are not authenticated but are still requested for user exit validation.

CERT= specifies the Server Certificate Label Name:

- '*' - Use a Certificate whose label is CCIGW. If not found, use a Certificate whose label is local to the CAICCI Sysid. If not found, use a Certificate whose label is CCI.

- 'label' - Use a Certificate whose name is label.
- "(null)" - Use the SystemSSL default Certificate.

Note: Embedded blanks within Certificate Label Names are not supported.

KEYRING= specifies the name of an external security keyring (Used instead of an HFS key database)

SSLVERS= specifies the version of System SSL that CCISLWG should use to request SSL services.

- 1 - Version 1 (OS/390 version)
- 2 - Version 2 (z/OS 1.2 version)
- "(null)" - Use highest available version (default)

PROT= specifies which security protocol(s) should be enabled:

- SSL - Only SSL Version 3 (default)
- TLS - Only TLS Version 1
- SSL/TLS or TLS/SSL or S/T or T/S or BOTH - Both SSL Version 3 and TLS Version 1 are enabled.

CIPHERS= specifies one or more SSL (Version 3) ciphers, in the order of usage preference, for CAICCI packet encryption in the form XXYYZZ...

- '01' - NULL MD5
- '02' - NULL SHA
- '03' - RC4 MD5 Export
- '04' - RC4 MD5 US
- '05' - RC4 SHA US
- '06' - RC2 MD5 Export
- '09' - DES SHA Export
- '0A' - 3DES SHA US
- '2F' - 128-bit AES SHA US
- '35' - 256-bit AES SHA US
- IBM - Use System SSL default list: (such as, 0504352F0A090306020100)
- 3DES - Use System SSL default list putting 3DES at top of list: (such as, 0A0504352F090306020100) (default)
- AES128 or AES-128 - Use System SSL default list putting 128-bit AES at top of list: (such as, 2F0504350A090306020100)
- AES or AES256 or AES-256 - Use System SSL default list putting 256-bit AES at top of list: (such as, 3505042F0A090306020100)

SSLTRCFN= specifies the name of the HFS file where System SSL can write trace entries. (Specifying the file name turns on tracing.)

SSLDUMP= specifies whether SSL packets should be dumped to the Trace File (TRCPRINT):

- No (default)
- Yes

CBDLL= specifies the module name of the dll containing the user exit routine for validating client (and server) certificates.

3. APF-authorize the libraries found in the STEPLIB concatenation which are the CAW0PLD Library containing the CAS9PDPM module, the system SSL Library, and the C and C++ runtime libraries.

This proc must be assigned a user ID that has:

- UNIX System Services segment.
- Read-write authority to the key database.

Copy CCIRTARM

Keep the following items in mind before you copy CCIRTARM.

- When using CCISSL, CCIRTARM comes into play if CCISSL has been configured to request and authenticate client certificates.
- This option is turned off, by default.
- CCIRTARM is the sample Certificate Authority certificate used by mainframe server CCISSL to authenticate its PC clients that are using the sample key/certificate cci.pem as their End User certificate.
- File cci.pem is copied into directory C:\CA_APPS\ during CCIPC/SSL installation.
- If this option is turned on (CLAUTH=Y within the CCISSL proc PARM or the TCPSSL PROTOCOL statement), then CCIRTARM is required to authenticate the cci.pem certificate coming down from the PC client.

If you are using an HFS key database, CCIRTARM must be imported as a CA certificate within the SSL key database on the mainframe using the gskkyman utility.

If you are using a z/OS key database, CCIRTARM must be imported as a CA certificate to the z/OS key database using security software such as Top Secret, ACF2, or RACF.

Note: For more information about importing certificate keys and the gskkyman utility, see the *IBM System SSL Programming Guide and Reference (SC24-5877)*.

- When using CCISSLGW, CCIRTARM is used to authenticate certificates from remote hosts when the remote host initiates the connection, thereby functioning as the client side of the SSL session. Although CCISSLGW and its remote hosts are ultimately peer-to-peer connections, the driver of the connection request determines their initial client/server identities for SSL session establishment. Since either the local or remote host can initiate the connection, either side could be the client end of the SSL session. Therefore, CCIRTARM is required to reside on all hosts that will connect over SSL.
- The controlling proc PARM option (RMAUTH=Y) is turned on by default.

If you have configured CCISSL to request and authenticate client certificates or you are running CCISSLGW, do the following:

To copy CCIRTARM

1. Copy CCIRTARM from the CAW0OPTN data set using ASCII (text) transfer to an HFS file on your mainframe where CCISSL or CCISSLGW will be executing.
2. Store the file on an HFS as ccirt.arm. For example, issue the TSO command `OPUT YourdeployHLQ.CAW0OPTN(CCIRTARM) '/etc/ccirt.arm' TEXT`
3. If you are using an HFS key database, use the System SSL utility (gskkyman) to import the certificate authority of the PC ccirt.arm (CCIRTARM) as a CA certificate in the SSL key database for client authentication.

If you are using a z/OS key database, consult your security software documentation or your security administrator for the import process.

Copy CCIP12

Keep the following items in mind before you copy CCIRTARM.

- This is a sample exported key and certificate (a PKCS#12 file) that can be imported into IBM's System SSL key database to be used by CCISSL and CCISSLGW as their End User certificate.
- This key/certificate is only to allow the CCISSL and CCISSLGW servers to run out of the box.
- As discussed previously, an authenticating CA (Certificate Authority) certificate must also be present on the remote client side of the SSL connection (the PC or other machines, such as mainframes or UNIX) for the server certificate to be accepted as valid by the client.
- The PC install already has this authenticating CA certificate within its Certificate Authority file (ccirroot.pem in directory C:\CA_APPSW), so using CCIP12 will allow an SSL connection by the PC.

- Having CCIRTARM imported into the key database or keyring as a Certificate Authority certificate will also allow an SSL connection from any PCs or remote CAICCI hosts that are using the sample cci.pem or CCIP12 certificates as their End User certificates.
- You can and probably will prefer to generate your own SSL certificates. Ensure that a copy of the Certificate Authority that has signed your generated certificate is within the cciroot.pem file in directory C:\CA_APPSW and also in your mainframe key database.

To copy CCIP12

1. Copy CCIP12 from the CAW0OPTN data set using binary transfer to an HFS file on your mainframe where CCISSL or CCISSLGW will be executing.
2. Store the file on the HFS as cci.p12. For example, issue the TSO command: OPUT *YourdeployHLQ.CAW0OPTN(CCIP12) '/etc/cci.p12'* BINARY
3. If you are using an HFS key database, use the System SSL utility (gskkyman) to import the key/certificate file CCIP12 into the SSL key database.

If you are using a z/OS key database, consult your security software documentation or your security administrator for the import process.

Start CCISSL

To start CCISSL

If CCISSL will be taking the place of CCITCP, cancel the CCITCP address first by issuing the following MVS console command:

```
C CCITCP
```

You can also configure CCISSL to run on an alternate port number and thereby run both CCITCP and CCISSL.

Automate CCISSL

You can automate the starting and stopping of CCISSL with the initiation and termination of the ENF/CAICCI address space.

To automate CCISSL

1. Copy member PRTCPSSL from the CAWOOPTN data set to your mainframe where CCISSL will be executing. This member contains the CAICCI PROTOCOL statement that drives ENF/CAICCI to start the CCISSL proc with specified runtime options.
2. Edit this file to change the fourth argument of the PROTOCOL statement, which specifies the sysid of your mainframe. The default value is MyMainFrameCCISysid.
3. Define SSL options and values by the proc PARM field. However, you can also specify one or more SSL parameters, separated by semicolons (;) with the PROTOCOL statement:

```
PROTOCOL(TCPSSL,Port;SSLKeyword1=SSLValue1;  
SSLKeyword2=SSLValue2;...,1,MyMainFrameCCISysid,16384)
```

where *Port* is the port number on which CCISSL will listen for connections. If the port number is to be specified, it must be the first network parameter.

4. Add or concatenate the contents of this file to the existing data set pointed to by the ENFPARMS DD statement within your ENF proc.

Start and Stop CCISSL from the Console

You can start and stop CCISSL using console commands. If you select this method instead of automatic initiation, the PARM=options hard-coded in the CCISSL proc will be in effect.

To start and stop CCISSL from the console

1. Enter the command:

```
S CCISSL
```

If CCISSL initializes successfully, it will display the following messages:

```
CAS9850I - CCI/SSL Version 12 Active  
CAS9850I - CCI TCP/IP Host Name = myTCP/Iphostname  
CAS9850I - CCI TCP/IP SSL Server Ready. Port = myPort  
CAS9850I - Addr = myIpAddr
```

CCISSL is now ready to accept connect requests on the specified port number (myPort). Successful and unsuccessful connections will be displayed along with any diagnostic messages.

2. Enter the command:

```
P CCISSL
```

To stop CCISSL from the console.

Start and Stop CCISSLGW

If you require the Secure Sockets Layer for your CAICCI host-to-host connections, you must use the CCISSLGW procedure.

The ID associated with the CCISSLGW started task must have a valid security OMVS segment defined.

Automate CCISSLGW

You can automate the starting and stopping of CCISSLGW with the initiation and termination of the ENF/CAICCI address space.

To automate CCISSLGW

1. Copy member PRTCPSSL from the CAW0OPTN data set to your mainframe where CCISSLGW will be executing.

This member contains the CAICCI PROTOCOL statement that drives ENF/CAICCI to start the CCISSLGW proc with specified runtime options.
2. Edit this file to change the fourth argument of the PROTOCOL statement, which specifies the sysid of your mainframe. The default value is MyMainFrameCCISysid.
3. Specify one or more SSL parameters, separated by semicolons (;) through the PROTOCOL statement. The second argument, which allows the specification of optional network parameters, can also be used to pass SSL-related information. SSL options and values can be defined by the proc PARM field.

```
PROTOCOL (TCPSSLGW,Port;SSLKeyword1=SSLValue1;  
SSLKeyword2=SSLValue2;...,1,MyMainFrameCCISysid,16384)
```

4. Add or concatenate the contents of this file to the existing data set pointed to by the ENFPARMS DD statement within your ENF proc.

Create and Populate the HFS Key Database

CAICCI includes optional SSL support under TCP/IP. Connections between mainframes, PCs, UNIX and Linux boxes may be secured using CAICCI with SSL implemented. A key database that contains security certificates is used to secure these SSL connections.

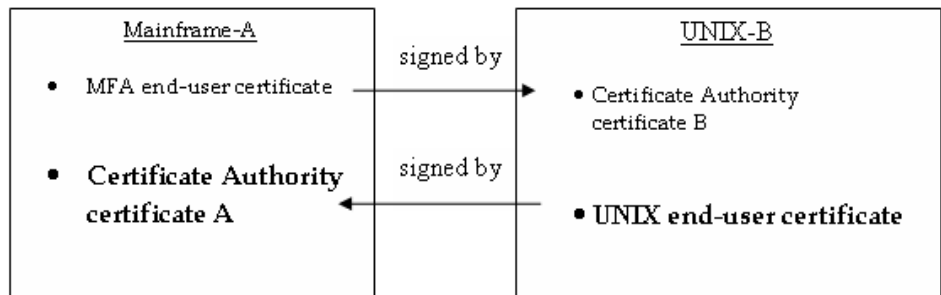
For client-server connections, mainframe started task CCISSL is used. The CAICCI-PC Configurator controls whether SSL will be used and how to locate the security certificates on the PC.

For peer-to-peer connections, mainframe started task CCISSLGW is used. Certificates can be stored on an HFS or in a security package's keyring. Supported security packages are CA Top Secret, CA ACF2 and RACF.

Security Certificates

On each node using SSL, two certificates are required: an end-user certificate and a Certificate Authority certificate that signs or verifies the end-user certificate on another node. CAICCI is delivered with two default certificates that can be installed on each node. For security in a production environment, the client node should generate its own certificates after the basic installation with default certificates has been tested.

For example, in a 2-node environment, there would be a total of four certificates as shown in the following diagram:



The key database is an ordinary file that may be saved anywhere within the HFS, such as:

```
/etc/cci/keyring/cci.kdb
```

You can have multiple key databases defined, or you can modify the CCISL and CCISLGW procs to reference your key database file instead. The procs require the specification of your key database pathname, certificate name, and a stored (stashed) password file pathname.

To create and populate the HFS key database

1. Create the directory where you want to place the HFS key database, such as /etc/cci/keyring.
2. Change (cd) into that directory and run gskkyman to do the remaining steps.

You will probably have to set the STEPLIB environment variable to point to GSK.SGSKLOAD (z/OS prior to 1.6) or SYS1.SIEALNKE (z/OS 1.6) to run this program. This can be done by updating the profile member (export STEPLIB=\$STEPLIB:GSK.SGSKLOAD or export STEPLIB=\$STEPLIB:SYS1.SIEALNKE) or issuing the export command for the session only.

3. Select Create new database from the gskkyman Database Menu.
4. Name the database cci.kdb.

5. Make the password cci, and do not let the password expire.
6. Enter the database record length (use the default).
7. Choose Store database password to store the encrypted database password into cci.sth.
8. Store the Root certificate from the ccirt.arm (CCIRTARM) file, in the key database required for client authentication, by following these gskkyman instructions:
 - Choose Import a Certificate from the gskkyman Key Management menu.
 - Enter ccirt.arm for the certificate file name (include the full pathname if it is not in the current directory).
 - Enter CCIROOT as its label. Use uppercase, as the label is case sensitive.

The sample Root certificate is stored in the key database. When client authentication is requested, CCISSL can now validate the PC client's incoming certificate. CCISSLGW can now authenticate a peer host that is initiating the connection to it.

9. Import the Certificate and Private Key from cci.p12 (CCIP12).
 - Choose Import a certificate and a private key from the gskkyman Key Management menu.
 - Enter cci.p12 for the import file name.
 - Enter cacci for the import file password.
 - Enter CAICCI as its label. Use uppercase, as the label is case sensitive.

The CAICCI End User certificate is imported into the key database and is available to CCISSL and CCISSLGW. When a PC connects to CCISSL or a remote host initiates a connection to CCISSLGW, these local servers respond with this End User certificate to identify them. The PC or remote host must have the corresponding Root Certificate (cciroot.pem or CCIRTARM) installed to correctly authenticate their identities.

If these servers are already running, you must recycle them, or a certificate error message is displayed.

Load CAICCI on the Client Platform

If you installed CAICCI and you plan to use mainframe to PC communication with client server products such as CA Datacom/AD and CA IDMS, you must install CAICCI/PC by downloading CAW0OPTN member CCIPCS32 and/or CCIPCS64.

CAICCI/PC is distributed on the CA Common Services for z/OS installation tape. It supports SSL and the TCP/IPv4 and TCP/IPv6 protocols.

CAICCI/PC can be installed from the mainframe using either TCPIP (FTP) or LU2 if the PC is connected to the mainframe with a 3270 emulator that supports the IND\$FILE file transfer protocol. No other software is required. Other file transfer applications, such as CA XCOM or Unicenter Software Delivery, may also be used to perform mass distributions of the required CAICCI/PC files. For specific instructions, see the documentation for that product.

Note: CAICCI/PC cannot be installed on a LAN server and shared by multiple users. A copy of CAICCI/PC must be installed on each PC.

To install CAICCI/PC to your PC

1. Remove any previous version of CAICCI-PC by using the CAINDREG program located in the C:\CA_APPSW directory.
2. Download CAW0OPTN member CCIPCS32 and/or CCIPCS64 to your PC using TCP/IP (FTP) or LU2.

If you have a 32-bit PC, you should only download the 32-bit version CCIPCS32. If you have a 64-bit PC, or you may need both versions depending on the applications that will be used. The choice of which package to use should be determined by the client-server product that will run on the PC. You can install both packages on a 64-bit PC if you have a mix of client-server products that require both.

To Download with TCP/IP (FTP)

Your PC must be connected through TCP/IP in order to use FTP to download the CAICCI/PC files from a z/OS host.

From your PC's Command Prompt:

- Change the directory to the directory that will receive the transferred file.
- Enter the ftp command with the IP address or name of the remote host.
- Logon to the remote host by entering your userid and password when prompted.
- Specify binary transfer.

- Enter the change directory command with the *YourdeployHLQ.CAW0OPTN* data set in quotation marks as the remote directory location. CAI is the HLQ used to install CA Common Services.
- Enter the get command with the name of the member (either CCIPCS32 or CCIPCS64) to be transferred from the remote directory to the current local directory as either CCIPCS32.EXE or CCIPCS64.EXE. If you are downloading both the 32 bit version and the 64 bit version, you need to use individual get commands as illustrated in the following example:

The following is a sample FTP session:

```
C:>ftp myIPname
User:
Password:
. . .
binary
. . .
cd 'cai.CAW0OPTN'
get ccipcs32 ccipcs32.exe
get ccipcs64 ccipcs64.exe

quit
```

To download using LU 2

Note: The steps below are for CCIPCS32 (32 bit version). If you need CCIPCS64 (64-bit version), use the same method, substituting the name CCIPCS64 wherever CCIPCS32 appears.

- Create a new directory on the PC.
- Click the button that invokes your terminal emulator file transfer facility.
- Select Receive from Host.
- For the Host file name, enter '*YourdeployHLQ.CAW0OPTN(CCIPCS32)*' or '*CAI.CAIOPTN(CCIPCS64)*', for the Host Type, enter TSO.
- For the PC file name, enter the PC drive and newly created directory followed by CCIPCS32.exe. or CCIPCS64.exe, such as:

c:\ccinst\CCIPCS32.exe

or

c:\ccinst\CCIPCS64.exe
- Ensure that the transfer type is BINARY.
- Start the transfer.

3. When the file download is complete, go into the new directory you created and double-click the CCIPCS32.exe icon or the CCIPCS64.exe icon to begin the self-extraction process.
CAICCI/PC installation begins.
4. When the installation completes, review the readme file created during this process for a description of the new certificate files, installation considerations, and a copy of the OpenSSL/SSLey licenses.

For more information about CAICCI on the PC, see the *Administration Guide*.

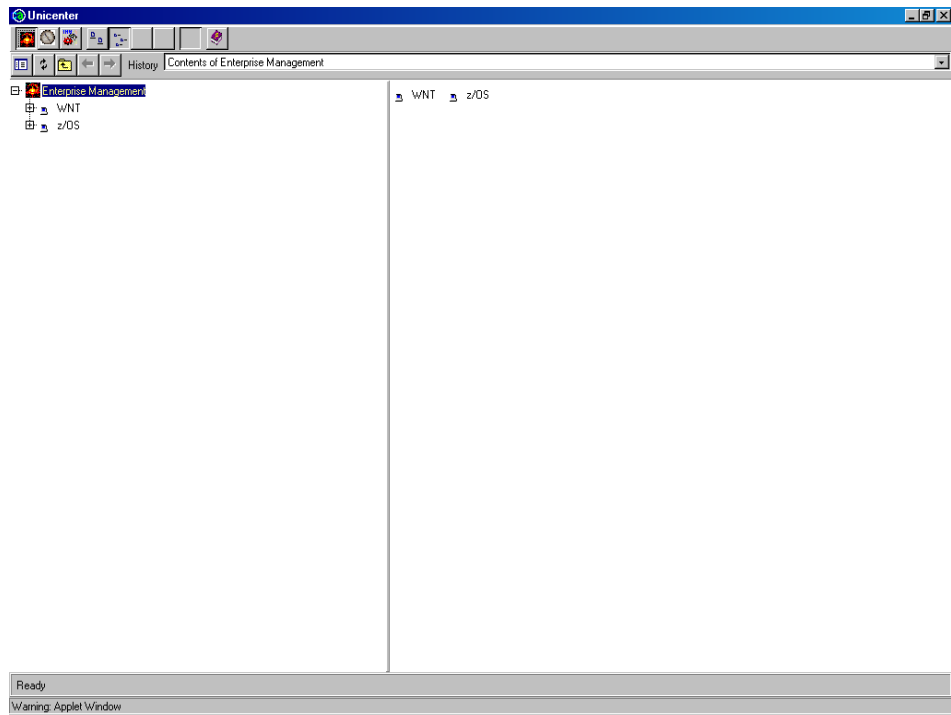
Peer-to-Peer Communication with Remote Computers

Peer-to-peer communications can occur among mainframes running CCISLWG or among distributed CA NSM computers and mainframes. In both cases the mainframe task CCISLWG facilitates the communication.

A single instance of the CA NSM Java GUI can be used to work with multiple CA Common Services or CA NSM computers. For example, even though the Workload component of CA NSM is not delivered as part of CA Common Services on z/OS, it is still available from the GUI. The main requirement is that the computers be connected by CAICCI. All of the remote computer CA NSM applications are visible in the GUI. You are prompted for a user ID and password for remote computers to ensure security.

To limit the computers that are displayed, you can create a file `/cai/nsmem/emsvvc/data/nodelist` that lists the CAICCI SYSIDs of each computer you want to display. A sample file called `nodelist.sample` is provided in that directory. Limiting the number of computers displayed reduces response time.

Here is an example of the GUI with multiple computers displayed:



Use CA NSM

To use CA NSM

1. Open the EM Connection Manager on your remote CA NSM distributed computer and make the following selections:
 - a. For Machine Name, choose the CAICCI SYSID as the name of the server.
 - b. For Platform, choose IBM zOS.
 - c. Check the Edit CAICCI Fields check box.
 - d. Click Add New to add the server to the list.

EM Connection Manager

You may now add additional machines to your administration configuration by specifying their platform and Unicenter version below.

Machine Name: MyMachineName

Platform: IBM zOS, NSM 11.x

Language: English

Check here to also include servers that are managed by the machines you selected. Edit CCI Fields Only Event Agent

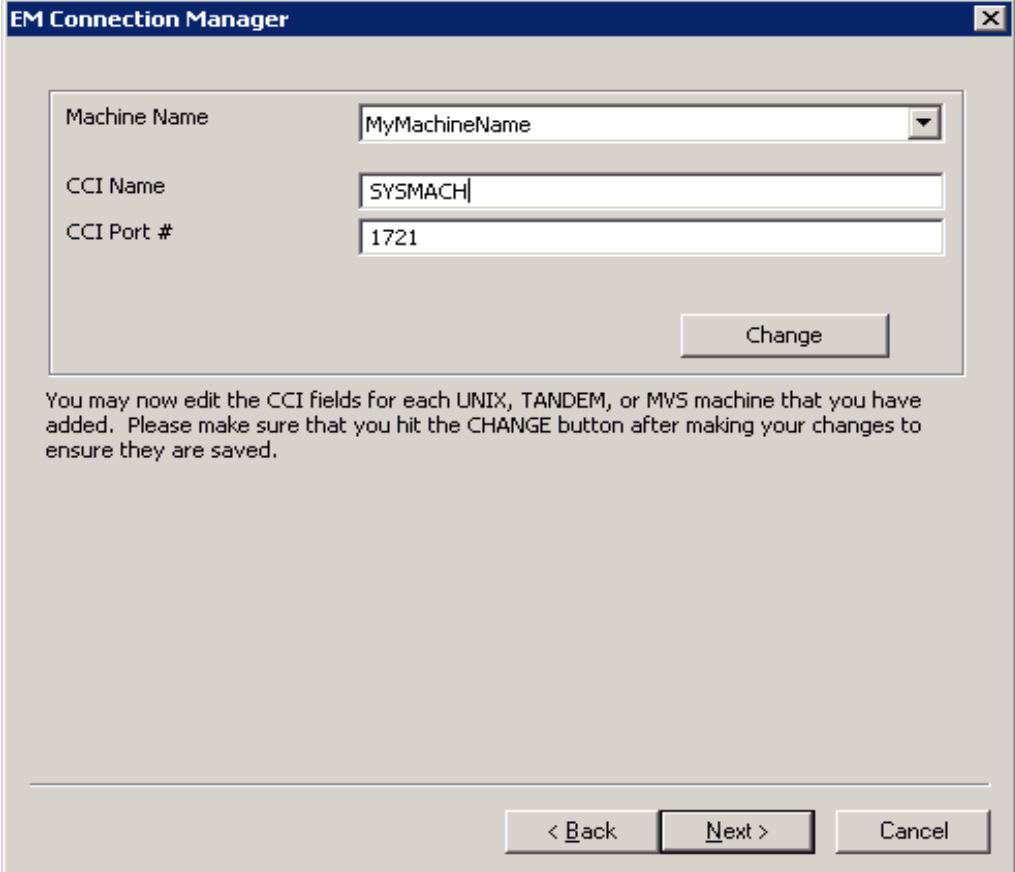
Modify Add Remove

Machine Name	Platform	Language
MyMachineName	IBM zOS, NSM 11.x	English

< Back Next > Cancel

2. Click Next to update the CAICCI fields to conform to the mainframe settings.
3. Ensure that the value specified for the CAICCI Port # matches what is being used by the CCISSLGW started task on the mainframe.

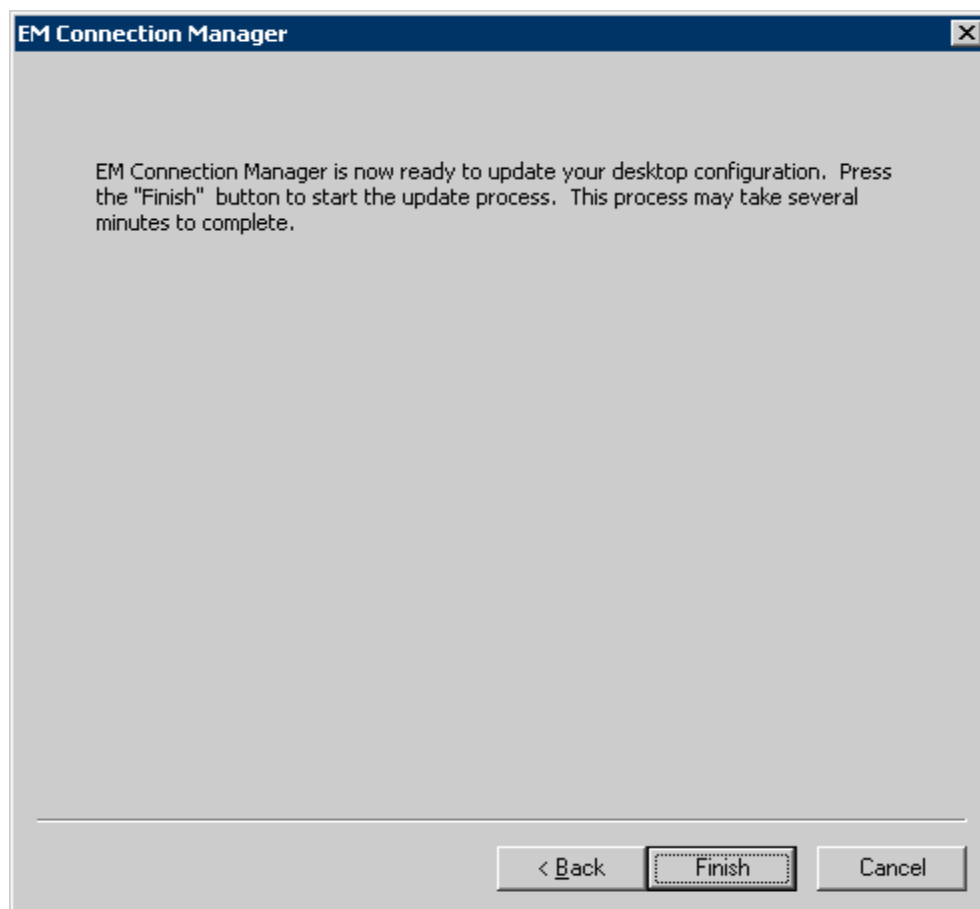
To check for the correct Port #, the CCISSLGW started task JOBL0G can be inspected on the z/OS system. The Alias field should remain blank since aliases are only required when the CAICCI sysid is longer than 8 characters. CAICCI sysids on z/OS cannot be greater than 8 characters.



The image shows a dialog box titled "EM Connection Manager" with a close button in the top right corner. Inside the dialog, there are three input fields: "Machine Name" with a dropdown menu showing "MyMachineName", "CCI Name" with a text box containing "SYSMACH", and "CCI Port #" with a text box containing "1721". A "Change" button is located below these fields. Below the "Change" button, there is a paragraph of text: "You may now edit the CCI fields for each UNIX, TANDEM, or MVS machine that you have added. Please make sure that you hit the CHANGE button after making your changes to ensure they are saved." At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

4. Click Next to display the final screen.
5. Click Finish and wait for the successful update message box.

Equation 1: This is the confirmation screen to finish updating your desktop configuration in the EM Connection Manager.



Activate Changes

To activate CA NSM changes, you must recycle the CAICCI remote component by issuing the following commands from the remote CA NSM distributed computer:

```
ccicntrl stop rmt  
ccicntrl start rmt
```

Verify Changes

To verify that the changes made to CA NSM are working, issue the following command on your remote CA NSM distributed computer:

```
ccii
```

The z/OS sysid will appear in this list. It may take a minute to get the connection, so wait before issuing the command. If it does not appear, check the following:

- Is the CCISSLGW task active on z/OS?

Yes—Check the SYSPRINT for a connection message from the NT machine. For example, the following is a sample ccirmttd.rc file on a Windows machine:

```
LOCAL = BARNA03W2K BARNA03W2K 32768 startup ALIAS=BARNA03W
REMOTE = 141.202.204.93 a93s 32768 startup PORT=7000
REMOTE = 141.202.36.71 a71senf 32768 startup PORT=7000
REMOTE = usilca11 a11senf 32768 startup PORT=7000
REMOTE = 141.202.204.97 a97s 4096 startup PORT=7000
```

Using this example, you can expect to see the following message on mainframe hostname usilca11:

```
CAS9603I - CAICCI A11SENF CONNECTED TO CAICCI BARNA03W
```

No—Check that the CAICCI PARMs contains a protocol statement:

```
PROTOCOL(TCPIP)GW
```

```
PROTOCOL(TCPSSLGW)
```

- Look at the ccirmttd.rc file in your NT NSM/caiusr directory. There should be an entry for the z/OS machine. The entry should look like this:

```
REMOTE = hostname ccisysid 32768 startup PORT=portnumber
```

where *hostname* specifies the TCP/IP name or ipaddress for the z/OS machine, *ccisysid* specifies the SYSID of the z/OS machine, and *portnumber* specifies the port number from the CAS9850I message.

Correct any mistakes and recycle CAICCI remote again.

You can obtain these z/OS machine values by inspecting the CCISSLGW started task JOBLLOG, and by issuing the following z/OS console command:

```
ENF DISPLAY,SYSID
```

- Are there any active receivers on z/OS? Issue the following console command to see what local receivers are available:

F ENF,DISPLAY,RECEIVER

Example display:

```
CAS9626I - CAICCI SUBSYSTEM IS OPERATIONAL
CAS9701I - CCI # RCVRS(00000009) LOCAL(00000009) REMOTE(00000000)
CAS9700I - ++++++
CAS9702I - CCI RESOURCE RECEIVER(#A93S CA-TOP-SECRET )
CAS9703I - CCI RESOURCE SENDER( )
CAS9704I - CCI RESOURCE OWN(A93S ) RCVI(00000001) SND(00000000) T(L)
CAS9707I - CCI RESOURCE ROUT(Y) DOLRI(2003.300) TOLRI(09:16:51.62) D(N)
CAS9708I - CCI RESOURCE QUE(Y) DOLSI(2003.300) TOLSI(09:16:51.62)
CAS9700I - ++++++
CAS9702I - CCI RESOURCE RECEIVER(@A93S W410_SPAWN_SERVER )
CAS9703I - CCI RESOURCE SENDER(@A93S SPAWN_INQY_SERVICES )
CAS9704I - CCI RESOURCE OWN(A93S ) RCVI(00000003) SND(00000002) T(L)
CAS9707I - CCI RESOURCE ROUT(Y) DOLRI(2003.300) TOLRI(12:54:18.47) D(N)
CAS9708I - CCI RESOURCE QUE(N) DOLSI(2003.300) TOLSI(12:52:11.72)
CAS9700I - ++++++
CAS9702I - CCI Resource Receiver(#USI273ME CA_STARUNIX_SERVER )
CAS9703I - CCI Resource Sender( )
CAS9704I - CCI Resource Own(USI273ME) RcvI(00000001) Snd(00000000) T(L)
CAS9707I - CCI Resource Rout(Y) DOLRI(2003.300) TOLRI(16:11:40.36) D(N)
CAS9708I - CCI Resource Que(Y) DOLSI(2003.300) TOLSI(16:11:40.36)
CAS9700I - ++++++
CAS9702I - CCI RESOURCE RECEIVER(#A93S CAI_OPR_DAEMON )
CAS9703I - CCI RESOURCE SENDER( )
CAS9704I - CCI RESOURCE OWN(A93S ) RCVI(00000002) SND(00000001) T(L)
CAS9707I - CCI RESOURCE ROUT(Y) DOLRI(2003.300) TOLRI(15:33:10.06) D(N)
CAS9708I - CCI RESOURCE QUE(Y) DOLSI(2003.300) TOLSI(15:33:10.03)
```

Important! Check for CAI_OPR_DAEMON and CA_STARUNIX_SERVER on the list of receivers. For Event Management running on z/OS to fully communicate with a CA NSM running on a distributed platform, these two receivers must be present.

Verify Your Installation

For client-server connections, mainframe started task CCISSL is used.

For peer-to-peer connections, mainframe started task CCISSLGW is used.

To verify that CAICCI is started correctly

1. Start the ENF procedure, which starts a subtask for CAICCI when the following statement is specified in the CCIPARM part of the ENFPARMS concatenation:

```
SYSID(xxxxxxxx)
```

2. Once ENF is initialized, issue the following console command:

```
ENF STATUS
```

3. In the output, look for the following message:

```
CAS9626I – CAICCI Subsystem is operational
```

If the message is not present, check that the DCM statement for CAICCI, CAS9DCM3, was defined in the CAIENF parameter file and that your CCIPARM was updated to include a valid SYSID.

4. Verify that the CCISSL and CCISSLGW started tasks are available in a system proc library. Verify that these started tasks have been properly set up in your security environment. CCISSL and CCISSLGW, plus ENF, require a security OMVS segment.
 - For CCISSL, verify that PGM= in the proc JCL is set to PGM=CAS9PDGM.
 - For CCISSLGW, verify that PGM= in the proc is set to PGM=CAS9PDPM.

Troubleshooting

This section describes how to determine the current status of a connection and how to activate tracing.

Current Status

There are several commands that can be issued to determine the current status of a connection between machines and the applications that are visible between them.

```
ENF CCI(DISPLAY,RESOURCE)
ENF CCI(DISPLAY,LINK)
```

Activate Tracing

Depending on the application there are several ways to turn tracing on.

CCITCPGW

Issue the following command to turn on tracing dynamically:

```
F CCISSLGW,T,SYSPRINT (for SSL)
```

```
F CCITCPGW,T,SYSPRINT (for non-SSL)
```

To deactivate the trace, specify:

```
F CCISSLGW,NOTRACE (for SSL)
```

```
F CCITCPGW,NOTRACE (for non-SSL)
```

Note: To start tracing immediately at CCISSLGW startup, add a TRCPRIINT DD statement to the started task JCL. Deactivation is the same as noted previously.

Local CAICCI

For the local CAICCI trace, issue the following commands:

```
ENF CCI(LINT)
```

```
ENF CCI(PRINTT)
```

CAICCI Spawn

Some applications will also require the use of CAICCI Spawn. Any product that uses this feature will contain installation instructions to update the CCISPNPM member in the *YourdeployHLQ.CAW0OPTN* member.

To turn tracing on for CAICCI Spawn, add a SPNDEBUG DD statement to the ENF procedure.

Prepare for Component Tracing

By default, CAICCI initializes Component Tracing using component name CACCI. The environment is initialized but tracing must be activated by an MVS TRACE CT command.

The ENF Parm CCICT can be used to activate and customize the Component Tracing environment including the component name. The Component Tracing parmlib member name can be specified in the CCICT command to activate tracing. For instruction on configuring the parmlib member, see the *Reference Guide* .

Note: If the external writer proc name is specified in the parmlib member, then the external writer must be configured prior to starting ENF/CCI. See the sample CCIXWTR proc in the *Reference Guide*.

CAICCI/PC - Using a Workstation Product

On the client side, you can enable tracing using the check box on the Trace tab of the CAICCI Configurator. The trace output goes to the file specified. To disable the trace, uncheck the box.

On the z/OS side, issue the following command to turn tracing on:

```
F CCISSL,T,SYSPRINT (for SSL)
```

```
F CCITCP,T,SYSPRINT (for non-SSL)
```

To deactivate the trace, specify:

```
F CCISSL,NOTRACE (for SSL)
```

```
F CCITCP,NOTRACE (for non-SSL)
```

CA TCPaccess Communications Server for z/OS Considerations

Started tasks CCISSL and CCISSLGW support CA TCPaccess Communications Server for z/OS using OE sockets, as well as IBM TCP/IP.

Connection Initiation Considerations

CAICCI tends to function better when connections are only initiated from one side of a potential connection. CAICCI may potentially be set up such that all nodes will try to connect to all other defined nodes. This would generally cause an excessive amount of connection attempts within the network. The general recommendation is for distributed platforms such as Windows and UNIX machines to initiate connections to mainframes and for mainframes not to initiate connections to distributed platforms. This can easily be achieved by simply not coding CONNECT statements in CCIPARMS for distributed nodes. Windows and UNIX REMOTE statements, by default, try to establish connections to the listed node.

For mainframe-to-mainframe connections, the recommendation is to code a CONNECT statement only on one (1) of the systems involved in a connection. The system that is more test oriented (more likely to go down) should be the system that has the CONNECT statement coded. If the systems are complete equals, then just choose one to be the one with the CONNECT statement. When there are many nodes involved, all requiring connections to each other, simply number each of the nodes, then have each node have a connect statement to all higher numbered nodes.

CA Workload Control Center

This section provides an example using CA Workload Control Center.

If you are having a problem connecting with the mainframe-scheduling engine, check the CAICCI connection.

To find an application on the mainframe

1. Ensure that the two CAICCI are connected. You can do this by entering the following DOS command:

```
rmtcntrl status
```

The output should show the current status of the connection.

2. If the computer does not appear in the list, you must check the ccirmt.d.rc file.
3. If the computer is on the list as INACT RETRY, check on the mainframe to see if the CCITCPGW or CCISLGW task is active.
 - a. If it is not active, issue the following console command to start it:

```
ENF PROTOCOL(TCPIPGW) (for non-SSL)  
ENF PROTOCOL(TCPSSLGW) (for SSL)
```

- b. If it is active, check to see if the IP address for the local PC is listed as trying to connect. If it is not, recycle CAICCI on the local computer by issuing the following commands:

```
CCICNTRL STOP RMT  
CCICNTRL START RMT
```

4. After you recycle CAICCI, retry the rmtcntrl status command. If the output from this command shows ACTIVE for the mainframe machine, you must verify that the application is available.

In the case of UEJM the application receiver name is SUBMITC Server. To see if that application is available to CAICCI, issue the following DOS command:

```
CCII sysid
```

where *sysid* is the mainframe SYSID.

5. If you do not see the receiver name in the list, the application is not available. Check to see if the application task is running. In the case of UEJM, that would be the CPS started task.

Chapter 9: Event Management Configuration

After installing and deploying CA Common Services for z/OS components, several configuration tasks are needed in order to implement and maintain the deployed Event Management.

This section contains the following topics:

- [Review and Adjust the Event Management PROFILE](#) (see page 159)
- [Rerun D5II0065 for GUI Tasks on the Deployed System](#) (see page 159)
- [Run the Event Management Configuration Script](#) (see page 159)
- [How to Configure Event Management GUI Tasks](#) (see page 162)
- [How to Configure Optional Event Management Tasks](#) (see page 167)
- [Startup Procedures](#) (see page 174)
- [Java GUI](#) (see page 175)
- [Verify Your Installation](#) (see page 179)
- [Event Management Maintenance Considerations](#) (see page 181)

Review and Adjust the Event Management PROFILE

On the deployed system, review the contents of the /cai/nsmem/PROFILE file with special attention to accurate settings for CAIGLBL0000, STEPLIB, and any TCP/IP environment variables that may have been added (such as RESOLVER_CONFIG and _BPXK_SETIBMOPT_TRANSPORT). Make any necessary adjustments for this deployed system.

Rerun D5II0065 for GUI Tasks on the Deployed System

If you want to use the Java GUI on the deployed system, the CNSMJCL member D5II0065 must be run on this system to pick up any environmental changes. Be sure that the variables used in the job reflect the correct values for this system.

Run the Event Management Configuration Script

Include Event Management zFS in BPXPRMxx by updating your system BPXPRMxx member to include the new mount points for Event Management.

Adding the new mount points to your BPXPRMxx member allows the mounts to occur automatically when your system is IPLed.

If you selected Event Management for installation, run the configuration script to customize certain files to your specific system. The configuration script, `fwsetup`, can be found in the designated Event Management directory (`/cai/nsmem` by default).

Note: Messages and prompts differ depending on whether you are running the script for the first time, rerunning the script, or re-installing. Steps that do not run under all circumstances are appropriately identified.

To run the Event Management configuration script

1. Go into OMVS on your system and change to the Event Management directory.

```
cd /cai/nsmem
```

2. Invoke the script with the following command:

```
. fwsetup
```

Note: `fwsetup` executes many tasks. Be patient during the execution of `fwsetup`. The text prompt will not automatically be seen on the screen. To see the text prompt, press PF10 to refresh the screen when the status of the session changes from RUNNING to INPUT. You can press the refresh key any number of times. If you see the text prompts, type your response and press Enter, or press Enter to accept the default. Follow these steps until you see CA Common Services installation has completed.

Important! Do Not Press Enter unless you are responding to a prompt or accepting the default to a prompt. If you press enter, you bypass the text prompt and will not be able to choose a value for your response. Instead, you will be accepting the default value.

The following messages display:

```
Installing CA Common Services...
```

```
Installing Event Management component...
```

3. Choose to activate Store and Forward or not.

In the event that other Event Management nodes cannot be reached, the Event Management Store and Forward facility can save failed events for forwarding at a later time.

```
Store and Forward (default: y)
```

4. Choose whether to create a rules file to restrict the use of certain message actions or allow all users to issue them.

Default behavior allows UNIXCMD and UNIXSH message actions to be submitted to this node (assuming there is a CAICCI connection) by all users. Event Management allows these two message actions to be restricted. The rules for these message actions are maintained through a utility called `caevtsec`. For more information on `caevtsec`, see the *Administration Guide*.

- For first time installations:

If the script does not find an existing rules file, you must decide if you want to create one.

Would you like to restrict the UNIXCMD and UNIXSH message actions for this host?

These actions were not restricted in Unicenter release 1.5. (y/n) (default: n)

After you answer, the following message appears:

Installing Star Server component...

- When re-installing and rerunning the script:

The script asks if you want to create a new rules file or use the existing one.

A version of the Event Security rules file has been detected on your system.

Answering y will preserve the original rules file (from the previous installation or upgrade) and will remove the restrictions of UNIXCMD and UNIXSH message actions for this host.

Answering n (default) will assume the restrictions previously enacted.

Would you like to recreate Event Security rules file? (y/n) (default: n)

If you choose to create a new rules file, the script informs you that the rules have been updated and the original rules file has been saved.

The original rules file has been preserved as
/cai/nsmem/opr/config/<nodename>/actnode.prf.sav

5. Set environment variables.

To use Event Management, certain environment variables need to be set, including PATH and LIBPATH.

You can have the system file `etc/profile` automatically set the Event Management environment variables in the `/cai/nsmem/PROFILE` file when a user logs on.

- If the environment variable `UPDATE_ETC` in the `PROFILE` file is set to Y (yes), `/etc/profile` is updated to run the `PROFILE` file automatically. Your EM environment variables are then set automatically when a user logs on .
- If the environment variable `UPDATE_ETC` in the `PROFILE` file is set to N (no), `/etc/profile` is not updated and all users have to manually set the EM environment variables.
- If the environment variable `UPDATE_ETC` was not set in the `PROFILE` file either during installation or subsequently, you are asked whether you wish to update `/etc/profile`.

For first time installations you have the option to update `/etc/profile` to set variables automatically when users logon.

Do you want to update `/etc/profile`? (y/n)

- If you choose y (yes), `/etc/profile` is updated to set environment variables for all users when they logon.

- If you choose n (no), you must run the `tngprofile` script before attempting to issue any commands

When re-installing or rerunning the `fwsetup` script, if it is detected that `/etc/profile` has been previously updated to run the `PROFILE` file, you may receive the following messages and the option to update `/etc/profile` is bypassed.

WARNING! `/etc/profile` has been previously updated. Please check the contents of `/etc/profile` to be sure the entry is valid for the current installation. If not, remove the update and re-run this `fwsetup` script.

WARNING! `/etc/csh.login` has been previously updated. Please check the contents of the file to be sure the entry is valid for the current installation. If not, remove the update and re-run this `fwsetup` script.

6. The following message appears:
CA Common Services installation has completed.
7. Verify that `fwsetup` has completed successfully.
 - If you indicated y to update `/etc/profile`, in that file you should see the updates inserted for Event Management.
 - Confirm that the `/cai/nsmem/RW/config/` directory contains a subdirectory with the same name as the nodename for the system.

How to Configure Event Management GUI Tasks

The following tasks are required if you plan to run the Event Management GUI elements:

1. Configure the UNIX System Services environment.
2. Configure and start the web server.
3. Install a compatible Java environment.
4. Review Security Definitions for Event Management.
5. Initialize the Event Management Java server.

These tasks are described in the following sections.

Configure the UNIX System Services for Event Management

Event Management requires USS to be configured and running in full function mode.

To review your BPXPARM member

1. Verify that you have the following USS configurable options set to at least the minimum values indicated:

Option	Minimum Value
MAXPROCSYS	200
MAXASSIZE	128MB
MAXTHREADTASKS	200
MAXPROCUSER	100
MAXCPUPTIME	86400

2. During Event Management startup, three POSIX shared memory segments are created; your IPCSHMNIDS parameter must reflect this requirement.
3. For best performance, ensure that temporary files are allocated to a TFS file system. Approximately 32 MB of temporary space are required for a typical Event Management installation.
4. Be sure the BPXPRM member starts zFS. There should be an entry for FILESYSTYPE TYPE(ZFS).

Configure the Web Server

The Event Management GUI requires a z/OS HTTP server. Any z/OS web server may be used if it provides compatible HTTP, Java, and CGI scripting capabilities. The web server must run on the same host where the Event Management Java server resides.

If you already run a web server on z/OS, you may elect to add the CA Common Services for z/OS definitions to your existing server. In most cases, however, you should run a secondary web server dedicated to servicing requests for CA Common Services for z/OS.

When configuring the web server, you will need to update or create an HTTPD configuration file. During Event Management installation, a sample is created in \$CAIGLBL0000/browser/httpd.conf, where \$CAIGLBL0000 is the path you choose to install into. Verify the settings found in this file.

The following settings are required:

```
Exec          /scripts/*
Exec          /tngfw/scripts/*
Exec          /tng/scripts/*
Exec          /ubi/scripts/*
Exec          /ubifw/scripts/*
Pass          /tngfw/*
Pass          /tng/*
Pass          /browser/*
Pass          /UBIImages/*
Pass          /ubiimages/*
Pass          /ubi/*
Pass          /ubifw/*
Pass          /*
Pass          *
```

See file \$CAIGLBL0000/browser/httpd.conf.sample for a complete list of required Exec and Pass parameters.

If you are running a web server dedicated to CA Common Services for z/OS, you will also need to specify these configuration options:

Statement	Purpose
Welcome tngfw.html	Defines the initial CA Common Services for z/OS page.
Port <i>nnnn</i>	Assigns the server to the specified TCP/IP port.

The Event Management HTML files are shipped in EBCDIC format. Typically, your z/OS web server should be configured to process HTML files in EBCDIC format. You should have an HTTPD configuration statement similar to the following:

```
AddType .html text/html ebcdic 1.0
```

The Event Management GUI performs user authentication and security validations as sensitive resources are accessed; however, you may also want to review web server security options. Certain CGI scripts required by CA Common Services for z/OS require superuser privileges, and the web server must be configured to run the scripts in the \$CAIGLBL0000/browser/scripts using UID 0. Other than this requirement, you are free to deploy any of the security features outlined in your web server documentation, including SSL, SAF, and Certificate-based authentication.

The scripts in `$CAIGLBL0000/browser/scripts` require certain environmental variables to be set. For best performance, you can define these variables in an LE envvar file, which is used to start the web server. After Event Management installation, a sample environment variable file can be found in `$CAIGLBL0000/browser/httpd.envvars`. Review this file and specify it on the `PARM=` field of the JCL used to start the web server.

The web server can be run as a started task or as a batch job. CNSMPROC member NSMWEBSV can be used as a model. Be sure to set the path statement on the DD card associated with the `CEE_ENVFILE` environment variable to your `/cai/nsmem/browser/httpd.envvars` file and use your `/cai/nsmem/browser/httpd.conf` configuration file.

Security Definitions for Event Management

The Event Management server maintains a secure environment by authenticating users as they connect to the system, verifying that individual users are permitted to access sensitive functions, and supporting delegation. All transactions triggered on the mainframe automatically inherit the security context of the individual signed-on user, rather than the server. The Event Management server implements these security interfaces by integrating with your external security product. CA ACF2, CA Top Secret, and IBM's RACF are all fully supported.

To perform its security functions, the Event Management server requires specific security permissions that may vary depending on which security product you have, the release of z/OS you run, and the details of the security policy you have in effect.

Create a security account for the Java and Web servers with these attributes:

- UID 0. The user identity that runs the Java server and the web server must be defined with real UID 0; you cannot assign a non-zero UID and permit the user access to the BPX.SUPERUSER resource.
- Any valid group ID (GID).
- Any valid home directory (the directory where you install CA Common Services for z/OS is a good choice).
- Any valid shell program, typically /bin/sh.
- READ permission to IBM FACILITY resources BPX.SUPERUSER, BPX.DAEMON, and BPX.SERVER, if you implement any of these features.
- Optional surrogate permission to any users that are to be signed on without password checking by the server.

In addition, all of the Event Management executable programs and DLL libraries must be marked as program-controlled, and certain executable programs must also be marked as APF-authorized. If you install Event Management into zFS directories, the installation process marks the appropriate files using the UNIX extattr command. RACF users installing into PDSE libraries also need to mark all of the Event Management modules and libraries as PADS-protected.

See the documentation for your security product for details about how to implement these functions.

Initialize the Java Server

The CA Common Services for z/OS Event Management Java server is run using the w2startup script located in \$CAIGLBL0000/browser/scripts. This script launches the Event Management Java server; it may need configuration, depending on the directory names you select when installing Java.

- \$CAIGLBL0000/browser/classes must be added to your Java CLASSPATH.
- Event Management and Java executable programs must be included in your PATH.
- Event Management and Java Library (DLL) directories must be included in your LIBPATH.

These variables are set in the file \$CAIGLBL0000/browser/httpd.envvars.

The w2startup script can be run as a UNIX command or as a batch job using BPXBATCH syntax. The sample member NSMJSERV in CNSMPROC can be run as a batch job or started task. You should run it as a started task in production. Process CaemRts and processes CAEMRTA are also started by w2startup. Check the status of this job by referring to STDOUT and STDERR zFS files for the job. Do **not** rely on the job return codes for evidence of successful completion.

Once the server is started, you can access the Event Management GUI by starting a web browser session with a URL of this form:

```
http://hostname:port
```

where *hostname* is the name or IP address of the host running the web server, and *port* is the port number you assigned in the `httpd.conf` file. It is highly recommended to use a hostname rather than a hardcoded IP address. If you accept the default port of 80, you can omit the port number.

To limit the nodes reported on by the GUI, copy the file `$CAIGLBL0000/emsvc/data/nodelist.sample` to `$CAIGLBL0000/emsvc/data/nodelist`, and edit that file to include only the node names on which you intend to report. This will improve performance when viewing the GUI.

To terminate the Java server, you can run CNSMPROC member NSMJSTOP; or from USS, run the `w2kill` script found in `$CAIGLBL0000/browser/scripts`. The script leaves processes `CaemRtS` and `CAEMRTA` (5 instances) running, allowing any remote CA NSM machines to access the Event Management GUI on z/OS.

Check the status of this job by referring to `STDOUT` and `STDERR` zFS files for the job. Do not rely on the job's return codes for evidence of successful completion. If you wish to shut down `CaemRts` and the `CAEMRTA` processes, run CNSMPROC member NSMSHRTS.

How to Configure Optional Event Management Tasks

The following tasks associated with Event Management may be required, depending on your environment:

- Activate Store and Forward
- Set up the Berkeley syslog daemon (required)
- Enable `catrapd`
- Initialize the Event Management servers
- Install the OPSMVS Exit
- Customize `emstart` and `emstop` Scripts
- Install Multiple Systems - Event Management

If you are installing multiple systems, you have a choice of installation methods.

If you have installed CAICCI, you must also configure and start CAICCI, as described in the [CAICCI Configuration Tasks](#) (see page 131) chapter.

Note: For more information about starting Event Management, see the *Administration Guide*.

Store and Forward

The Store and Forward feature (SAF) guarantees message delivery through the storage and eventual forwarding of messages that cannot be immediately delivered to target nodes (because of network problems, because the Event Manager is not running, and so on). Store and Forward is enabled during installation by setting and exporting the environment variable `INSTALLSAF=Y` in the `$/CAIGLBL0000/PROFILE` file.

When Store and Forward is activated, the Event Management guaranteed message delivery feature is activated. With this feature activated, any messages that cannot be delivered in real time will be stored for automatic delivery at some later time when the destination applications are once again reachable. (Undeliverable messages are stored in a file located, by default, in the directory `$/CAIGLBL0000/opr/saf`. Once all messages in this file have been sent, the file is automatically erased.)

Limiting SAF Eligibility

By default, when Store and Forward is activated, all nodes are eligible for this feature. If you wish to limit SAF eligibility to specific nodes, you must create a configuration file that lists those node names (and optionally, the directory path for the SAF files). Subsequently, only those nodes listed are targeted for SAF. If the SAF configuration file exists but is empty, no nodes are eligible for SAF.

Use a text editor to create a `SAF.CFG` file that meets your particular needs, using the following sample `SAF.CFG` template provided:

```
# Node                Directory
#
UGGP12                Dynamo
UGIPP4                Pluto
UXTTP1                Mercury
UURET5                Neptune
```

Create an SAF Configuration File

You should create an SAF configuration file to tell the system which target nodes are eligible for storing messages. If an SAF configuration file does not exist, all target nodes are eligible for storing messages.

To create an SAF configuration file

1. Copy the sample SAF.CFG file you created to the `$CAIGLBL0000/opr/saf` directory.
2. Edit the SAF.CFG file as follows:
 - In the first position of each data line, specify the machine name (node) to be eligible for SAF. This name can be up to 15 alphanumeric characters.
 - In the second position of each data line, specify the directory under SAF root by which the identified log file of the machine (node) is to be accessed from this machine.
3. Save the edited file with the name `SAF.CFG` or choose a unique file name.

Change the SAF Interval

When a file exists that contains stored messages, the SAF daemon will try periodically to re-send the messages based on a defined interval. You can alter the interval of time (in seconds) between each SAF re-try.

To change the SAF interval

1. Edit the file `$CAIGLBL0000/opr/scripts/envsetlocal`.

If the file does not exist, create it.

2. Add the following lines to this file:

```
CA_OPR_SAF_SCAN_INT=xx
export CA_OPR_SAF_SCAN_INT
```

where `xx` represents the new scan interval in seconds.

If you are using SAF between other platforms and z/OS, consult the appropriate documentation for configuration information.

Enable Store and Forward for Another Task

This task lets you store and forward `cawto`, `wto`, or both messages from another task such as `OPSMVS`.

Add the following environment variables to the `OPSMVS` or other task's environment variable file:

```
export CA_OPR_SAF=Y
export CA_OPR_SAF_ROOT=$CAIGLBL0000/opr/saf
```

Enable catrapd to Receive SNMP Traps

Unicenter NSM has the ability to send and receive SNMP traps. Any received traps will appear on the Event Management console.

To receive traps, the daemon `catrapd` must be running. By default, the process listens on port 161. Your TCP/IP procedure has a PROFILE DD that contains reserved port numbers.

Enable `catrapd` if you want to route SNMP messages from other consoles by making port 161 available if possible.

To enable `catrapd` using the default port

Modify the TCPIP profile (the data set used in DD statement PROFILE in your TCPIP proc) to ensure that:

- Port 161 is not reserved for OSNMPD (the SNMP Agent)
- AUTOLOG does not start OSNMPD

To enable `catrapd` using a different port

Add the following two lines to the envset script in the `$CAIGLBL0000/snmp/scripts` directory if port 161 cannot be used:

```
CAICATD0001=nnn  
export CAICATD0001
```

Note: `CAICATD0001=nnn` is the port number to listen on, replace *nnn* with the actual port number.

You can use the `catrap` program to send a trap. The syntax for the command is described in the *Reference Guide*.

Start and Stop the Event Management Processes

A CA Common Services for z/OS Event Management server is started using the CNSMPROC member NSMEMSTR. It can be run as a batch job or a started task. You should run it as a started task in production. This job starts four daemons (caiopr, logdr, ca_calendar and stardaemon) associated with Event Management by invoking the emstart script. The catrapd daemon is not started by default. Edit the script `/cai/nsmem/opr/scripts/emstart` by uncommenting the 'unicntrl start snmp' command if you wish to start the catrapd daemon. Customize the script so that you start only those components that you want to use. Comment out the components that you do not want to use.

The Event Management daemons are stopped using CNSMPROC member NSMEMSTP by invoking the emstop script. NSMEMSTP can be run as a batch job or a started task. You should run it as a started task in production. Edit the script `/cai/nsmem/opr/scripts/emstop` so that it stops the same processes that are started by the emstart script.

Check the status of this job by referring to STDOUT and STDERR HFS files for the job. Do **not** rely on the job's return codes for evidence of successful completion.

The user ID assigned to these jobs should be assigned UID 0 and have access to BPX.DAEMON, BPX.SUPERUSER, and BPX.SERVER facilities.

Install the OPSMVS Exit

If you want to use Event Management to handle OPSUSS messages, you must run OPS job INSTUSEX to install the OPS exit for Event Management.

Note: For more information, see the *CA OPS/MVS Event Management and Automation Installation Guide*.

Set Up the Berkeley syslog daemon

Event Management takes advantage of the powerful messaging facilities provided by the Berkeley syslog daemon that may be used to:

- Select from several priorities, levels, and facilities of messages
- Route messages by level or priority to different devices
- Route messages by level or priority to different hosts
- Receive messages from other hosts for local display

The Berkeley syslog daemon configuration options are usually specified in the file `/etc/syslogd.conf` in the following format:

selectoraction

- **selector** identifies the type of message.
- **action** is the location where the selector is sent.

Note: For more information about the Berkeley syslog daemon, see the *IBM z/OS Communications Server IP Configuration Guide*.

Sample syslogd Configuration File

The following is a sample syslogd configuration file with Enterprise Management installed in a single-host configuration:

```
# @(#) $Revision: 66.1 $
#
# syslogd configuration file
#
# See syslogd(1M) for information about the format of this file
#
mail.debug      /usr/spool/mqueue/syslog
*.info,mail.none /usr/adm/syslog
*.alert        /dev/Event
*.alert        root
*.emerg        *
*.info         /cai/nsmem/opr/config/abcfred/pipe/oprpipexxx
```

Note: If CAIGLBL0000 is `/cai/nsmem`, and the current node name is `abcfred`, the preceding entry routes the `*.info` to Event Management. The entry for `*.info` is automatically added during the startup of the `caiopr` process.

Reroute Messages to a Remote Host

Event Management on z/OS can accept syslog messages from any remote system running a compatible BSD syslog service.

To instruct the syslog daemon to route all messages to a remote machine, edit the syslogd configuration file and insert the remote hostname in the action part of the line, prefixing the hostname with a single at sign (@).

Note: The syslog daemon makes use of DNS (Domain Name Services) and relies on proper definition of the hostname and IP address of the receiving host.

Example: The following syslogd configuration illustrates an entry on the local node that routes all messages with a priority of info and above to the remote host known as titan:

```
# @(#) $Revision: 66.1 $
#
# syslogd configuration file

# See syslogd(1M) for information about the format of this file

mail.debug      /usr/spool/mqueue/syslog
*.info,mail.none /usr/adm/syslog
*.alert         /dev/Event
*.alert         root
*.emerg        *
*.info         /cai/nsmem/oprconfig/abcfred/pipe/oprpipexxxx
*.info         @titan
```

Note: The syslogd configuration file contains tabs as field delimiters in addition to spaces. Typically, the first and second columns are separated by tabs as well as spaces. Do not use blanks alone to delimit fields, as this will cause the syslog daemon to ignore the line in question or give improper results.

To send messages to additional hosts, simply add more lines as needed. If you want to limit the messages to certain priorities or facilities, do so with the first part of the command line. For more information on selecting and routing messages, see the man pages for syslogd.

Activate the Changes

For the syslogd configuration updates to take effect, you must stop the syslog daemon and restart it from the root ID.

To activate the changes

1. Stop the syslog daemon by entering the following command:

```
kill -15 `cat /etc/syslog.pid`
```

2. Restart the syslog daemon by entering the following command:

```
/usr/sbin/syslogd -f /etc/syslogd.conf
```

where /etc/syslogd.conf is the name of the syslogd configuration file.

Customize emstart and emstop Scripts

The emstart and emstop scripts are located in the following directory:

```
/cai/nsmem/opr/scripts
```

emstart and emstop are the startup and stop scripts for Event Management. Customize the scripts so that you start only those components that you want to use. Comment out the components that you do not want to use.

Startup Procedures

The CNSMPROC member NSMEMSTR is used to start Event Management. By default, this starts the caiopr, logdr, stardaemon, ca_calendar, newdaylog, and caidoc processes. CNSMPROC member NSMEMSTP should be used to stop Event Management in an orderly fashion. Both of these jobs run scripts that are in the /cai/nsmem/opr/scripts directory. The scripts can be edited to include only the components you need to run.

Note the following startup considerations:

- All processes must be started with UID(0), and CAICCI must be active before they are started. To ensure that CAICCI is completely initialized, you can start Event Management as part of the CAIENF autocmds.
- The stardaemon does not require any additional services.

- The caiopr daemon has the option of using the repository. If the definition of message actions and calendars, or both, are desired, the repository is needed, and must be started prior to Event Management. You must ensure that the STEPLIB environment variable and the CA_OPR_ZOSDB environment variable, in the PROFILE file, is set correctly prior to starting caiopr.

If you are using CA OPS/MVS Event Management and Automation exclusively to handle the processing of messages, the repository is not required. The startup of caiopr may receive some warning messages concerning the connection to the repository and that the messages cannot be reloaded, but caiopr will continue processing normally and the messages can be ignored.

- The user ID assigned to Event Management must be UID(0). This is required to be able to switch a user from the Event Management user ID to the user ID of the client signed on. This prevents the client from being able to issue commands they would normally not be allowed to enter for the CA NSM console.
- If the SNMP trap listener, catrapd, needs to be started, you must locate the following line in the /cai/nsmem/opr/scripts/emstart file and remove the pound sign (#) from the beginning of the line:

```
#unicntrl start snmp
```

When finished, the line should appear as follows:

```
unicntrl start snmp
```

Java GUI

This section describes Java GUI considerations.

Timeout Settings

The following settings control how long the GUI waits for a response:

`TIMEOUT=300`

Instructs CAICCI to wait 300 seconds. This value is set near the end of the /cai/nsmem/browser/scripts/w2startup file.

`persistentservertimeout`

A registry setting that is set by using the Java TIMEOUT command. The command by itself displays the number of seconds the GUI waits for a response. Passing a parameter changes the setting to whatever is passed.

If you consistently get timeout messages, you should increase these settings by updating the TIMEOUT parm to a higher value.

Security Requirements

Built-in security checks protect the defined resources from being modified by unknown sources. You must define these resources to the security system to protect them. All the resources are defined to a single class CAIUNI. The following describes each resource:

EMSRVC.MSGRECORD

Controls access to define/modify message records.

EMSRVC.MSGACTION

Controls access to define/modify message action records.

EMSRVC.CALENDAR

Controls access to define/modify calendars.

EMSRVC.CONLOG

Controls access to the CA NSM Console log.

EMSRVC.ANNOTATION

Controls access to the CA NSM Console log annotation feature.

To allow access to any of these resources, READ access is required.

Enterprise Management

The Enterprise Management icon displays all the machines that can be found running CA NSM or CA Common Services.

Run a CAICCI inquiry to find the receiver EMSRVC_ROUTER_U.

For each machine that is found, an attempt to obtain the APPMAP is made. If the map cannot be loaded, the machine is left off the list.

To limit the list to only a selected few, you can create a file nodelist in the /cai/nsmem/emsvrc/data directory. A nodelist.sample file can be used as an example. To select a node to be on the list, enter the CAICCI SYSID for that machine. The local machine also needs to be in the list.

Web Server Configuration

The installation process creates a configuration file containing all the information required to run the Java GUI. However, there are many options that affect the behavior of the web server; we discuss only some of them here.

For more information about web servers, see the IBM manual *IBM HTTP Server* for your operating system release.

If a web server is already running, you can support multiple applications from the one server or change the port number for one of them.

To change the port number, edit the configuration file and modify the Port operand.

To merge CA Common Services into an existing web server, you must add the following to your configuration file:

```
ServerRoot /cai/nsmem/browser  this should contain the install path for Event
Management
HostName   yourhostname       this should be the host name of your computer
Port      80                   The port to connect to: Default 80.

#
# The default Framework configuration specifies no security inside the
# Web server since authentication is performed in our Java server once
# The user connects to the system. The NOSEC definition (below) allows
# Access to occur under the web server's security context (as opposed
# To under any specific individual's context).
#
Protection NOSEC {
    ServerId      TNGFW_Server
    AuthType      Basic
    PasswdFile    %%SAF%%
    UserID        %%SERVER%%
    Mask          Anonymous
}
Protect        /scripts/*      NOSEC %%SERVER%%
Protect        /tngfw/scripts/* NOSEC %%SERVER%%
Protect        /tngfw/*        NOSEC %%SERVER%%
Protect        /tng/*          NOSEC %%SERVER%%
Protect        /browser/*      NOSEC %%SERVER%%
#
# The following directives specify the location of the Framework
# directories. If you are integrating Framework into an existing
# web server, these statements must be included in your existing
# HTTPD configuration file.
#
Exec          /scripts/*        /cai/nsmem/browser/scripts/*
Exec          /tngfw/scripts/*   /cai/nsmem/browser/scripts/*
Exec          /tng/scripts/*     /cai/nsmem/browser/scripts/*
Exec          /ubi/scripts/*     /cai/nsmem/browser/scripts/*
Exec          /ubifw/scripts/*   /cai/nsmem/browser/scripts/*
Pass          /tngfw/*           /cai/nsmem/browser/*
Pass          /tng/*             /cai/nsmem/browser/*
Pass          /browser/*         /cai/nsmem/browser/*
Pass          /UBIImages/*       /cai/nsmem/browser/images/*
Pass          /ubiimages/*       /cai/nsmem/browser/images/*
Pass          /ubi/*             /cai/nsmem/browser/*
Pass          /ubifw/*           /cai/nsmem/browser/*
Pass          /*                 /cai/nsmem/browser/*
Pass          *                  /cai/nsmem/browser/*
#
Logging:
#      -- Uncomment the following lines to enable logging --
```

```
# AgentLog      logs/Agent
# AccessLog     logs/httpd-log
# CgiErrorLog   logs/cgi-errors
# ErrorLog      logs/httpd-errors
# TraceLog      logs/jttrace
```

You will find a complete list of the statements in file `/cai/nsmem/browser/httpd.conf`. You may copy and paste them into your existing web server configuration file.

Verify Your Installation

Event Management consists of the following:

- Processes that make up the functional components such as message handling, calendars, and remote servers.
- GUI interface, which includes the ability to add messages to act on and the actions to take, the creation of calendars, and the viewing of the event console.

Not all sites will require both parts of this verification process.

Verify that Processes are Running

You can use the CNSMPROC member NSMEMSTR to start the functional component. After starting this job, issue the following command:

```
D OMVS,A=ALL
```

The `caiopr`, `newdaylog`, `caidoc` and `logdr` processes minimally should be running. Depending on your needs `ca_calendar`, `stardaemon`, `oprsafd` and `catrapd` may also be running.

Verify the GUI Interface Servers are Active

The GUI interface requires that the `httpd` server is active and the Java backend server be up and running. You can also use CNSMPROC member NSMWEBSV to start the `httpd` server if you do not already have one started. For more information about setting up a new server or merging into an existing one, see the [Java GUI](#) (see page 175) section.

Start the Java Server

You can use the CNSMPROC member NSMJSERV to start the Java server. The following message appears on the system console to signify the startup is complete:

```
CAXX506I – TNG Root Processes Initialized
```

OMVS processes CaemRtS, CAEMRTA(5 instances), logonserver.exe, EMserver.exe, and w2Tree should be running at this point.

Connect to the GUI

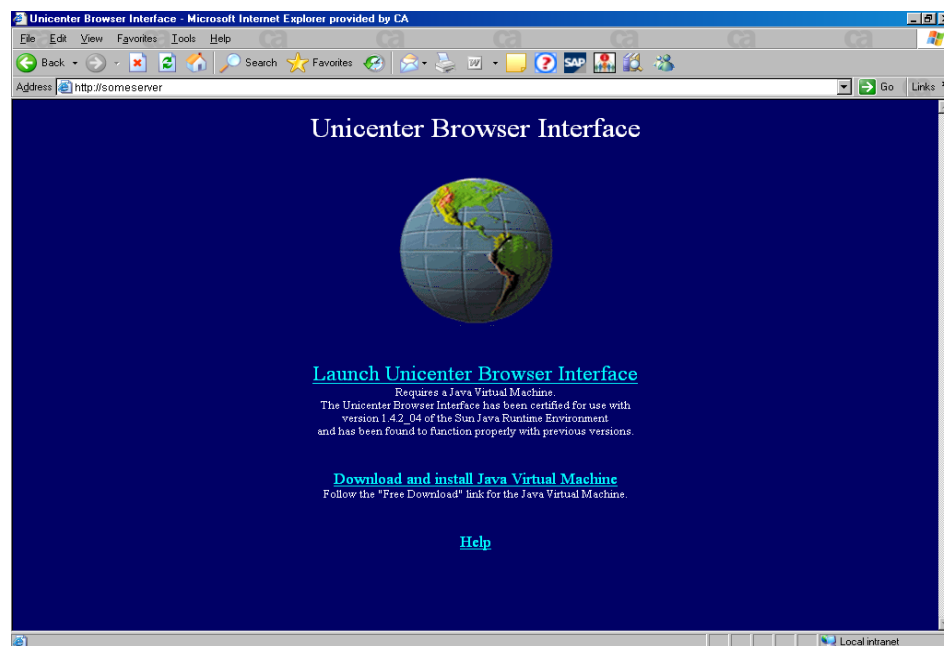
To connect to the GUI

1. Start your browser and use the following URL to display the welcome page:

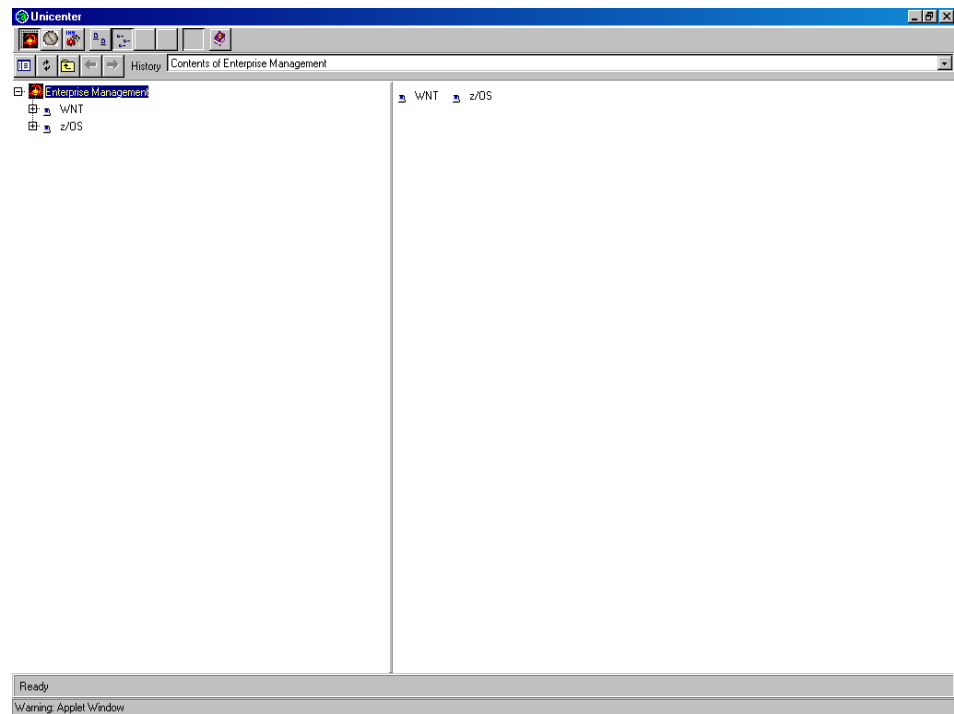
`http://hostname:port`

The welcome page appears.

2. Select [Click Here](#) to launch CA NSM Browser Interface.



3. Enter a mainframe user ID and password.
4. Click OK to display the main CA NSM GUI.



Event Management Maintenance Considerations

Event Management and Event Management utilities are installed into several different SMP/E target libraries:

- The traditional PDS and PDSE data sets like CNSMLOAD and CNSMPLD load libraries.
- Two USS zFS data sets:
 - Read-only zfs aggregate that contains the executables, scripts, HTML, and Java class files.
 - Read-write zfs aggregate that contains the system specific information such as Event Management log files, temporary files, and configuration files for that system.

When a new service pack becomes available, to perform maintenance without disrupting the running system

Important! Never use the SMP/E target libraries as your executable code. Always deploy the SMP/E target libraries at least once and run off the deployed data sets.

1. Confirm that no CA Common Services components are executing from the SMP/E environment.
2. Confirm the SMP/E DDDEFS are correct and have not been altered from the original installation.
3. Confirm that the SMP/E Target USS zfs data sets are mounted at the same point used during the SMP/E installation and are mounted for RW.
4. RECEIVE and APPLY the maintenance as usual to the SMP/E targets.
5. Run the pre-maintenance script CNSMJCL (EMPREMT) against your running libraries to save your production configuration. The script must be edited to point to the production mount point.
6. Re-deploy the SMP/E target data sets to the production system using a different HLQ and mount point. Temporarily mount both zFS files RW.
7. Run the post-maintenance script (EMPOSTMT) to restore the configuration. This script must point to the newly deployed USS zfs data set mount point.
8. Once the EMPOSTMT script has completed, you should be able to:
 - a. Unmount the newly deployed zfs data sets
 - b. Shut down the running product
 - c. Unmount the running product zfs data sets
 - d. Swap in all the newly deployed data sets as production

The SYS1.PARMLIB(BPXPRMxx) member should not require any changes, since the deployed zFS should be mounted at the same mount point as was previously used.

Chapter 10: Agent Technology Configuration

After installing and deploying CA Common Services for z/OS, several tasks remain before the deployed Agent Technology is ready to start.

Include Agent Technology zFS files in BPXPRMxx by updating your system BPXPRMxx member to include the mount points for the deployed Agent Technology.

Adding the new mount points to your BPXPRMxx member allows the mounts to occur automatically when your system is IPLed.

This section contains the following topics:

[Tailor the Profile, Script, and Configuration Files in the zFS System](#) (see page 183)

[Build the aws_sadmin Store Files](#) (see page 190)

[Agent Security](#) (see page 190)

[Agent Configuration Set Verification](#) (see page 191)

[Load Library Considerations](#) (see page 191)

[Start Agent Technology](#) (see page 191)

[Build and Run the Example Agent \(EXAGENT\)](#) (see page 192)

[Verify Agent Technology Installation](#) (see page 194)

Tailor the Profile, Script, and Configuration Files in the zFS System

Before starting Agent Technology you must tailor the following files in the zFS system.

File	Type	Purpose
agentworks.profile	Profile file	Contains the environment variables needed to run CA Common Services for z/OS Agent Technology.
install_mibs	Script file	Loads the management information bases that you expect to use on your system.
quick.cfg	Config file	Describes the protocols that can be used for communication between the Distributed Services Bus and its partners (such as aws_sadmin and the agents).
aws_sadmin.cfg	Config file	Identifies each remote system that is to receive mainframe traps.

File	Type	Purpose
aws_snmp.cfg	Config file	Describes some UDP parameters that can be used by the aws_admin service and by the SNMP tools.

Edit the profile file: /cai/agent/agentworks.profile

The following environment variables should be set to the values that reflect your installation:

Environment Variable	Description
AWORKS_MVS_PREFIX	The data set high-level prefix used for the Agent Technology data sets. This must be the same value assigned to the CAI variable in running the installation script.
AGENTWORKS_DIR	The full path name that defines the directory where Agent Technology files are installed in the zFS system. This must be the same value assigned to the AWORKDIR variable in running the installation script.
RESOLVER_CONFIG	The name of the TCP/IP configuration information data set. This must be the same value assigned to the SYSTCPD DD data set in your TCPIP procedure. A member name must be included if the data set is a PDS.
_BPXK_SETIBMOPT_TRANSPORT	This establishes Agent Technology with an explicit affinity to a specific TCP/IP stack transport Job Name.
AWS_STARTER_REQUEST	The TCP/IP port number used internally to submit requests to the awsservices process. The default is 9990.
AWS_STARTER_CONTROL	The TCP/IP port number that allows the awsservices process to control the services with agents still active. The default is 9991.
TZ	Your time zone. The default is EST5EDT.
AW_MAX_LOGSIZE_K	The maximum size of the various log files. The default is MAX, the maximum size allowed by your file system. Possible values are integer values representing the file size in KB (for example, 10000 for a maximum size of 10 MB).

Environment Variable	Description
AW_AUTO_START	If the awsservices process is not running, this variable controls whether another service or agent that was started from a shell using the start command option is allowed to start awsservices implicitly. The default value is ON.

The following four environment variables control the collection of statistical information by the `aws_sadmin` process. This information is held in the `awsAdmin` MIB, which can be viewed using the MIB Browser tool. Benchmark tests have shown that as much as 40% of the CPU time spent by `aws_sadmin` is consumed by the updating of these statistics.

Environment Variable	Description
AW_ADMIN_STAT_AGENT	Controls the statistics maintained in table <code>awsAdminAgentTable</code> . When set to OFF, the <code>awsAdminAgentResponseAvg</code> variable returns the value 0. The default value is ON.
AW_ADMIN_STAT_SNMP	Controls all the variables within group <code>awsAdminSnmpGroup</code> . When set to OFF, all variables from the group always return the value 0. When set to NOTOTAL, only the <code>awsAdminSnmpInRequestsTotal</code> variable is not incremented. This variable represents the total of all GET, GETNEXT, and SET requests. The default value is ON.
AW_ADMIN_STAT_PERF	Controls all the variables within group <code>awsAdminPerfGroup</code> . When set to OFF, all variables from the group return the value 0. The default value is ON.
AW_ADMIN_STAT_SOURCE	Controls all entries within table <code>awsAdminSourceTable</code> . When set to OFF, this table shows empty. The default value is ON.

Execute the agentworks.profile

Prior to executing an Agent Technology utility, you must first execute the agentworks.profile file explicitly to assign the correct values to the variables that describe your current environment.

Note: The agentworks.profile file is executed automatically by all the scripts that are delivered with the Agent Technology component.

To execute the agentworks.profile

1. Start a shell session under USS.
2. Set your current directory to the directory that contains the directory defined by the AGENTWORKS_DIR environment variable.

```
cd /cai/agent
```

3. Invoke the agentworks.profile script.

```
. agentworks.profile
```

Note: Do not omit the space after the initial period.

An Agent Technology utility is now ready to be executed.

Edit the script file: /cai/agent/services/tools/install_mibs

Make the ldmib entries match your chosen MIBs, and select MIB alternatives.

To edit the script file

1. Review and tailor the ldmib entries to match the MIBs you expect to use on your system. The awsAdmin MIB is required.
2. Choose one of the following alternatives for MIBs that are no longer delivered in the MIBLIB:
 - Copy the corresponding MIB from the Agent's specific library to the standard MIBLIB and activate the existing ldmib entry in the install_mibs script. Since the standard Agent Technology MIBLIB is an SMP/E target library, it is advisable to keep track of its contents using SMP/E. The CNSMJCL Library contains a sample job, AWADDMIB to facilitate copying your Agent's MIB and adding it as a USERMOD to the SMP/E environment.
 - Keep the corresponding MIB in the Agent's specific library, and edit the ldmib entry in the install_mibs script to make it point to the correct data set.

Edit the config file: `/cai/agent/services/config/aws_orb/quick.cfg`

The `quick.cfg` configuration file describes the various protocols that can be used for communication between the Distributed Services Bus and its different partners. It contains a full description of the different parameters, and is delivered with default values that should usually satisfy all environments.

Edit the config file: `/cai/agent/services/config/aws_sadmin/aws_sadmin.cfg`

This configuration file identifies each remote system that receives mainframe traps.

To edit the `aws_sadmin.cfg` file

1. Specify an `SNMP_TRAP` entry with the corresponding machine name or IP address and port number 162 or 6162, depending on the port number used by the remote system's trap listener.
2. Substitute the sample values with your own machine name or IP address in the default file. It is preferable to use the machine name.

```
SNMP_TRAP xyzwin2k3.ca.com|162 # traps to NSM manager Machine
```

or

```
SNMP_TRAP 172.24.138.21|6162 # traps to another NSM manager Machine
```

Note: This file also lists SNMP community names and their attributes, which are not usually changed. Any line in this file that starts with a pound sign (#) is a comment and is ignored by the runtime system.

The following trap destinations are *not* the same:

Correct

```
SNMP_TRAP 172.24.138.21|6162 # non-padded IP Address
```

Wrong

```
SNMP_TRAP 172.24.138.021|6162 # Padded IP Address
```

Note: Zero-padding of IP addresses is not allowed. IP addresses should be specified exactly as they are returned from the TCP/IP stack (when queried using the `IPCONFIG` command in DOS under Windows, for example).

A Tab character (`X'05'`) is used as the delimiter between the `SNMP_TRAP` and `SNMP_COMMUNITY` keywords and their associated values and following comments. The Tab character usually appears as a period in the ISH and UNIX System Services editor.

Edit the config file: `/cai/agent/services/config/aws_snmp/aws_snmp.cfg`

The `aws_snmp.cfg` configuration file describes some parameters that can be used to tailor the `aws_admin` service or the SNMP tools. It contains a full description of the different parameters.

The following parameters are supported:

- `IP_TO_BIND`-allows the `aws_admin` service to bind to a specific IP address. By default the SNMP Listener socket (default Port 6665) will listen on all TCP/IP stacks.

Note: Users running in a multi-homed environment may not want to see their mainframe agents on multiple TCP/IP nodes. To restrict the discovery of your mainframe agents to 'only' the default TCP/IP stack, change the `IP_TO_BIND` parameter to 127.0.0.1 (loopback designation).

- `SNMP_PORTS`-controls which ports will be used by `aws_admin` or the other SNMP tools such as `awget`, `awnext`, and so on when generating SNMP requests.

Tailor the config file: `/cai/agent/services/config/awsservices/awsservices.cfg`

The `awsservices.cfg` configuration file contains various services and agents that can be activated within Agent Technology.

Starting with CA NSM r3.0, the default `awsservices.cfg` file delivered with Agent Technology contains only entries for the `aws_orb` and `aws_admin` services.

New entries are usually created automatically in the `awsservices.cfg` file during the standard installation of agents, such as the MQSeries agent.

If you are upgrading from a previous release of Agent Technology and will not be re-installing agents, use the `install_agents` script file currently delivered in your `/agent/services/tools` directory. This script file can be used to add or remove entries in the `awsservices.cfg` file for any agents or services currently supported on z/OS.

To add or remove entries in the `awsservices.cfg` file

1. Perform the procedure to [Execute the agentworks.profile](#). (see page 186)
2. Enter the `install_agents` command with no parameter to get a full description of the different parameters supported.

Example: If you know you will run the `exagent` example agent, enter the following command:

```
install_agents install exagent
```

Tailor the ENVFILE from the CNSMOPTV

Tailor the CNSMOPTV (ENVFILE) to fit your standards. The variables that can be customized are AGENTWORKS_DIR, TZ, AW_MAX_LOGSIZE, AWS_STARTER_REQUEST, and AWS_STARTER_CONTROL. For more information, see the section titled [Edit the profile file: /cai/agent/agentworks.profile](#) (see page 184).

Verify the TCP/IP Network Configuration

Verify that the TCP/IP network configuration is compatible with the Agent Technology components.

To verify the TCP/IP network configuration

1. Submit the AWFTEST job from CNSMJCL.
2. View the output, and verify that correct values have been returned for functions such as gethostname(), gethostid(), and so on.
3. If the AWFTEST job does not run successfully, review your TCPIP procedure to verify that the TCPDATA variable was correctly customized. This must be the same data set assigned to the SYSTCPD DD.

If you are using a PDS for this data set, verify that the member name has been included. If this does not solve the problem, consult your network administrators for assistance before proceeding.

Build the aws_sadmin Store Files

To complete the installation of Agent Technology, build the aws_sadmin store files.

To build the aws_sadmin store files

1. Run the CLEANADM job from CNSMJCL to allocate the aws_sadmin store files.
Processing error messages from this job are placed in the clean_sadmin.out file in the /cai/agent/services/tools directory.
2. Review the contents of the clean_sadmin.out file to ensure the utility ran correctly.
3. Verify that the /cai/agent/services/tools/install_mibs script file has been customized to include an Idmib entry for each agent you plan to use.
4. Submit the INSTMIBS job from the CNSMJCL to load the aws_sadmin store files with the appropriate MIBs for your system. This job starts the install_mibs script file referred to in the previous step.

The output of the job is placed in the install_mibs.out file in the /cai/agent/services/tools directory.

5. Review the contents of the install_mibs.out file to ensure the utility ran correctly.

Important! A zero return code from the BPXBATCH steps in either the CLEANADM or INSTMIBS job does not indicate a successful completion of the script being invoked. You must check the output in the .out files to determine successful completion. If you encounter error messages in the .out files, refer to the CA Common Services CA Support website which provides tips for identifying and fixing common Agent Technology configuration problems.

The installation of Agent Technology on your machine is now complete.

Note: This is a good time to make a backup copy of your new zFS.

Agent Security

Arrange with your security administrator for your site to create or update the user IDs that will be running agents. They must all have access to UNIX System Services and be members of the group that owns the Agent Technology files.

Agent Configuration Set Verification

If you are installing on multiple systems or upgrading from a previous release of Agent Technology and use configuration sets with your agents, the configuration sets must be loaded at this time. These configuration sets could be those distributed with an agent or those you have written yourself. In particular, the agent for CA NSM System Status Manager CA-OPS/MVS Option will not run without the configuration set that is delivered with CA OPS/MVS Event Management and Automation. Review the documentation for the agents you are running to see whether this is applicable and for the procedure to reload the configuration set if required.

Note: For more information about the *ldconfig* utility that loads configuration sets, see the *Reference Guide*.

Load Library Considerations

All Agent Technology modules used by batch jobs and agents now reside in the CNSMLOAD.

Important! Review the JCL for all jobs that run agents, and modify the STEPLIB DD statement to remove any reference to CAILOAD or CAILIB, adding references to both CAW0LOAD and CNSMLOAD.

Note: If you have defined CAW0LOAD and CNSMLOAD to the system LNKLST, no STEPLIB reference is required in jobs that run agents.

Start Agent Technology

To start Agent Technology

1. Modify and start AWSTART in CNSMPROC.
2. Issue online commands (shell scripts) to perform the same tasks.

Note: For more information about batch jobs and their corresponding shell scripts, see the *Reference Guide*.

Build and Run the Example Agent (EXAGENT)

This task is optional. An example agent has been developed to help you verify that your Agent Technology services are functioning properly. This agent also serves as a model for coding your own agents. The source code for the example agent is distributed with the Agent Technology services within:

- Member EXAGENT installed in CNSMSRCV
- File `exagent.c` in directory `/$AGENTWORKS_DIR/agents/samples/exagent`

The function of the agent is to traverse the structure of a directory within the UNIX System Services zFS.

Compile and link the example agent on site before attempting to start the agent. You can compile and link either online within USS or through a batch job submission in z/OS. Select the environment you are more comfortable with, online or batch.

Compile and Link Online (USS)

You can compile and link online within USS.

To run the example agent online

1. Perform the procedure to [Execute the agentworks.profile](#) (see page 186)
2. Position yourself within the example agent directory:

```
cd /$AGENTWORKS_DIR/agents/samples/exagent
```

3. Invoke the command:

```
make install
```

This command compiles and links the example agent and copies the executable into the `agents/bin` directory.

4. Start the example agent, by invoking the command:

```
exagent start
```

Compile and Link in Batch Mode (z/OS)

You can compile and link through a batch job submission.

To run the example agent in batch mode

1. Tailor and submit member EDCCPL within your Common Services runtime JCL Library (CNSMJCL).

This job compiles, prelinks, and links the example agent and assembles the default user runtime options module, creating module EXAGENT in the Common Services Load Library.

2. Tailor and submit member EXAGNT within your Common Services runtime JCL Library (CNSMJCL).

This job starts the example agent.

The links performed include the default user options for the example agent to provide the runtime options for IBM's Language Environment (LE). In some cases, users may wish to tailor the LE parameters to meet certain site-specific requirements. If so, edit the EDCCPL jobstep that assembles the user options table CEEUOPT.

The job streams named above can also be used as sample JCL decks for the compilation, linkage, and submission of user-built agents.

Note: For more information about the development and deployment of these agents, see the *CA NSM Inside Systems Management* and *Inside Systems Monitoring* guides.

Verify Agent Technology Installation

Once your Agent Technology z/OS services have successfully started, perform these steps.

To verify that the Agent Technology services are running properly

1. Check on the state of the AT Services. To do this, within OMVS:

a. Issue the following command:

```
. agentworks.profile
```

Note: Do not enclose this command in quotes and do not forget the period and space before the actual invocation of the agentworks.profile script.

b. Issue the following command:

```
awservices list
```

The first two lines of the report produced should read:

```
RUNNING   aws_orb:aws_orb  
RUNNING   aws_sadmin:aws_sadmin
```

Note: You may see several other services and agents, or both, listed in the report with a status of Stopped. This is normal.

2. Check the status of the AT services ports. To do this, within OMVS:

a. Issue the following command:

```
onetstat
```

b. The report produced should list all of the AT ports (see the Overview section earlier in this chapter) and show them in the appropriate status, as follows:

```
Listen - For all TCP/IP socket ports  
UDP - For the SNMP listener port (normally 6665)
```

3. Ensure all of the Agent/Services MIBS have been loaded into the Object Store. To do this, within OMVS:

a. Issue the following command:

```
. agentworks.profile
```

b. Issue the following command:

```
agentctrl -m
```

The report produced must show the awsAdmin MIB, as well as at least one other Agent MIB. For example:

```
<awsAdmin>      is registered
<caiDatacom>    is registered
<caiDb2mvs>     is registered
<caiIDMS>       is registered
<caiSysAgtzOS>  is registered
<caiSysAgtCics> is registered
<caiSysAgtMqs>  is registered
<caiSysAgtMvs>  is registered
```

4. If you encounter problems, review the Services log files within the AT zFS (under directory \$AGENTWORKS_DIR/services/var/log) to help diagnose the problem. These files are overwritten each time the AT services are started.

Chapter 11: CA Global SubSystem Configuration

After installing CA Common Services for z/OS, configuration tasks are needed for the CA Global SubSystem (CA-GSS).

Note: Use your deployed data sets when performing these tasks.

This section contains the following topics:

[Complete the GSS Installation](#) (see page 197)

[How the Post-Configuration Process Works for CA-GSS](#) (see page 198)

[Define Subsystem IDs](#) (see page 198)

[Copy CA-GSS Procedures to System PROCLIB](#) (see page 198)

[Install the IMOD Editor](#) (see page 199)

[Install the CA-GSS/ISERVE Operator Control Panel](#) (see page 202)

[Test the Installation](#) (see page 202)

[Customize CA-GSS](#) (see page 204)

[Optional Features](#) (see page 214)

Complete the GSS Installation

To complete the GSS installation

1. Allocate the GSS VSAM data sets.

Edit and Submit CAW0JCL member BYSI0010 to allocate the VSAM IMOD files for the INTERNAL and SAMPLE ISETs.

2. Load the GSS IMOD files.

Edit and Submit CAW0JCL member BYSI0020 to load the GSS IMOD files.

Note: The STEPLIB data sets must be APF authorized prior to running this step.

How the Post-Configuration Process Works for CA-GSS

To complete the installation of CA-GSS and prepare it for use, perform the following configuration tasks:

- Define Subsystem IDs.
- Copy CA-GSS Procs to System PROCLIB.
- Install the IMOD Editor.
- Install the ISERVE Operator Control Panel.
- Test the Installation.
- Configuration.

Define Subsystem IDs

Specify your ISERVE subsystem ID using the SSNAME parameter in the CA-GSS CAW0OPTN RUNPARM member. For documentation purposes, specify the CA-GSS subsystem ID (GOAL) and your ISERVE subsystem ID (ISRV) in your SYS1.PARMLIB data set.

Note: If you do not add the subsystem IDs to your SYS1.PARMLIB data set, they will be dynamically added to the subsystem name table when CA-GSS is started.

Copy CA-GSS Procedures to System PROCLIB

The CA-GSS procedures are distributed in the CAW0PROC Library. These procedures must be moved to a system PROCLIB to make them available as a started task. The following table lists the CAW0PROC members to be copied and gives the suggested name for each.

CAW0PROC name	PROCLIB name	Description
BYSGSSA	GSSA	Primary CA-GSS started task.
BYSGSSP	GSSP	CA-GSS Passive area utility.

To copy the procs to system PROCLIB

1. Update the CAW0PROC members to ensure they are properly customized.
Change data set names and JCL statements as appropriate for your installation.
Select values for the lowercase parameters
2. Copy the members to your system PROCLIB.

If you plan to run multiple CA-GSS subsystems, a sample proc, BYSISRV, for running secondary GSS subsystems is included in the CAW0PROC Library.

Note: For more information about running multiple CA-GSS subsystems, see the *Administration Guide*.

Install the IMOD Editor

The IMOD editor is an ISPF-based facility that lets you write, edit, compile, and test IMODs. Installation of the editor requires the following:

- Accessibility to the CA-GSS Load Library, CAW0LOAD by the TSO user. This is accomplished through the system LINK LIST or by providing the appropriate STEPLIB statement.
- Accessibility from the CA-GSS ISPF-related libraries (panel, message, and CLIST) to the TSO user. This is accomplished through dynamic allocation when the CA-GSS editor program (SRVEDIT) is called.
- Construction of a parameter list, based on information provided to the CA-GSS address space in the ISETS member of the CAW0OPTN data set.
- Addition of appropriate ISPF menu entries to permit invocation of the IMOD editor from an ISPF panel, if desired.

To install the IMOD editor

1. Review enqueue requirements.
 - CA-GSS observes strict enqueue compliance to ensure that ISETs can be shared across multiple systems without risk of corruption. To ensure proper handling of enqueues, you must notify your enqueue management software about the CA-GSS enqueues.
 - During update operations, an exclusive enqueue is obtained for qname IPGMGREX and rname *F.dsn*, where *dsn* is the 44-byte cluster name, right padded with blanks.
 - During edit operations, an exclusive enqueue is obtained for qname IPGMGREX and rname *P.imod.dsn*, where *imod* is the 16-byte IMOD name, right padded with blanks, and *dsn* is the 44-byte cluster name, right padded with blanks.
 - All enqueues have a scope of SYSTEMS.
2. Construct the parameter list and update the CA-GSS RUNPARMS.

The entry panel of the IMOD editor lists all ISETs (IMOD data sets) that are available for use. Each entry in this list includes the ISET name, a description, and the subsystem ID of the ISERVE address space, if any, which is linked with the ISET.

Consider the following:

- Only one data set may be referred to by a particular ISET name, although multiple ISET names may refer to a single data set.
- If dynamic reloading or execution of IMODs is to be permitted, the ISET and DSNAME references must be identical to those appearing on the ISET statements defined to the CA-GSS address space. You can ensure that the references will be identical by using the CAW0OPTN RUNPARM, ISETS, and EDITPARM members.
- If UNIT=VIO is not valid for data set allocation in your data center, you must include a VIOUNIT parameter before the IMOD compiler can be executed.
- The parameter list is referenced through the member name value that you specify on the EDITOR MEMBER statement. You should specify the EDITPARM member of the CAW0OPTN data set for this value.
- A sample parameter list is provided in the ISETS member of the CAW0OPTN data set. You can customize this member, adding ISET definitions appropriate for your own environment. You must select values for the lowercase parameters. The EDITPARM member referenced by the EDITOR MEMBER statement contains an INCLUDE statement for the ISETS member. This ensures that the CA-GSS task and the SRVEDIT program reference identical ISET lists.

Note: For more information about the format of ISET initialization parameter statements, see the *Reference Guide*.

3. Modify the ISPF menu panel.

You can invoke the IMOD editor by issuing the GSSEDIT command, or you can invoke the IMOD editor from an ISPF menu panel. The GSSEDIT command is a REXX EXEC that is contained in the distribution CLIST data set.

To invoke the IMOD editor from ISPF, locate the appropriate ISPF menu panel and add the following menu items to the panel and in the PROC section:

```
ISRV, 'PGM(SRVEDIT) NEWAPPL(nnnn) NOCHECK'
```

where *nnnn* is an arbitrary four-character ISPF application ID (such as ISRV).

Important! Use caution when modifying the ISPF primary menu panel. An error can prevent you from using ISPF. Always keep a backup member and a tested procedure that is independent of ISPF.

IMOD Editor Problems

If you select the IMOD editor and receive an ISPF error message referring to ISPPROF, verify that you have enough space in the ISPPROF data set.

If you cannot reload or execute an IMOD from the IMOD editor, do the following:

- Press PF1 (or enter HELP) to display the long error message, which identifies the cause of the failure.
- Make sure that CA-GSS is executing. This requires that the GSSMAIN program be running.

Secondary ISERVEs may also be running, using the SRVSYS program.

Make sure that the ISERVE and DSNAME references are identical to those appearing on the ISET statements defined to the CA-GSS address space. You can ensure that the references are identical by using the CAWOOPTN RUNPARM, ISETS, and EDITPARM members.

Install the CA-GSS/ISERVE Operator Control Panel

CA-GSS provides an ISPF-based control facility called the CA-GSS/ISERVE Operator Control Panel that you can use to execute CA-GSS commands from a terminal (rather than requiring access to a z/OS operator console.) These commands, which let you operate and monitor the CA-GSS address space, can be directed to any CA-GSS address space operating on the user's z/OS system. GoalNet permits commands to be issued to any GoalNet participant.

Results of these commands are displayed on the panel in full-screen mode so that you can scroll up and down through them. The results are not rolled off the screen, except when replaced with another command.

To install the CA-GSS/ISERVE operator control panel, invoke the CA-GSS/ISERVE Operator Control Panel by issuing the GSSOPER command, or you can invoke it from an ISPF menu panel.

To invoke the panel from ISPF, add the following menu item to the panel and the PROC section for the appropriate ISPF panel:

```
ISRVO, 'PGM(SRVOPER) NEWAPPL(mmm) NOCHECK'
```

where *mmm* is an arbitrary four-character ISPF application ID (such as OSRV).

Important! Use caution when modifying the ISPF primary menu panel. An error can prevent you from using ISPF. Always keep a backup member and a tested procedure that is independent of ISPF.

Test the Installation

At this point, the basic installation process is complete. Before proceeding with final configuration, you may wish to verify that CA-GSS has been installed correctly.

To verify the installation of CA-GSS

1. Start CA-GSS.

Enter the following command from the operator console:

```
START GSSA
```

Initialization should proceed rapidly; when it is complete, the following message is displayed:

```
SRV220 Version 02.08.mm: Initialization Complete (ssid)
```

mm represents the current maintenance level of CA-GSS, and *ssid* represents the subsystem ID you selected for ISERVE.

2. Test CA-GSS.

- Invoke the CA-GSS/ISERVE Control Panel by issuing the following command from an ISPF panel:

```
TSO EX 'CAI.CAW0CLS0(GSS0PER)'
```

- Execute the Installation Verification Program (IVP) by issuing the following command from the CA-GSS/ISERVE Control Panel:

```
IVP [PRINT [TO userid [AT node]]]
```

If you omit the text in brackets, output is produced on the console, verifying the operation of CA-GSS. Optionally, you can specify that a more complete report be printed. If the PRINT option is specified, you can also specify the user ID and node where the printed listing is to be routed.

- Use the PF3 key to return to your ISPF panel.

3. Test the IMOD Editor.

- Invoke the IMOD editor by issuing the following command from an ISPF panel:

```
TSO EX 'CAI.CAW0CLS0(GSSEDT)'
```

- Select the SAMPLIB ISET by specifying S next to its name. Then select the \$\$\$VERSION member by specifying S next to its name.

- Verify that the correct version of CA-GSS is specified in the \$\$\$VERSION member. (It should be 0208*mm*.)

When the version is correct, use the PF3 key to go back to the SAMPLIB ISET display.

- Compile the \$\$\$VERSION member by specifying G next to its name.

To verify that the compile worked, look for an IMOD LOADED message in the upper right corner of the panel.

- Use the PF3 key to back out of your ISPF session.

4. Stop CA-GSS.

Terminate CA-GSS properly by entering one of the following commands from an operator console:

```
STOP GSSA  
P GSSA  
F GSSA, STOP
```

If CA-GSS does not terminate within a few seconds, enter the following command:

```
F GSSA, STOP FORCE
```

If CA-GSS still does not terminate, cancel the address space and inspect the JESLOG and ISRVLOG listings for diagnostic messages.

Recompile under TSO

You may want to recompile IMODs while under TSO.

To recompile IMODs while under TSO

1. Select an ISET and enter the IMOD selection panel.
2. Enter the TOGGLE command to display the current compiler version for each IMOD.
3. Enter a C (compile) command on each line that shows an IMOD in need of recompiling.
4. Press ENTER to recompile all IMODs identified with a C.

The IMODS are recompiled.

Customize CA-GSS

When you initially install CA-GSS, you may need to modify certain initialization parameters, including but not limited to product-specific parameters. However, you probably do not need to customize every CA-GSS initialization parameter. For more information about CA-GSS initialization parameters and to determine which ones you need to customize, see the *Administration Guide*.

The following sections describe product-specific configuration steps.

Customize CA-GSS for CA Insight Database Performance Monitor for DB2 for z/OS

CA Insight Database Performance Monitor for DB2 for z/OS uses CA-GSS for various logging, access, and auditing capabilities. REXX-based IMODs are used for all CA Insight Database Performance Monitor for DB2 for z/OS functions that access CA-GSS.

Look at your CA Insight Database Performance Monitor for DB2 for z/OS documentation to determine whether this product supplies IMOD libraries (ISETs). If ISETs are supplied, you need to load them into DASD.

You can use the CA-GSSIMOD member of CA Insight Database Performance Monitor for DB2 for z/OS libraries to load ISETs. Before you submit the JCL in this member, make sure the unit and volser number match those on your CA Insight Database Performance Monitor for DB2 for z/OS tape.

To customize CA Insight Database Performance Monitor for DB2 for z/OS

1. Allocate ILOGs.

ILOGs are VSAM linear data sets that CA-GSS uses to record information about a subsystem. Each ILOG is composed of two *subfiles* (data sets)-one primary, and one backup that is used when the primary becomes full.

For each DB2 subsystem that CA-GSS will be monitoring, you need to allocate two data sets. To do this, modify and submit an SRVMAINT job that contains one or more ALLOC_ILOG commands. Each ALLOC_ILOG statement allocates a pair of VSAM linear data sets. Another way of allocating these data sets is to modify and submit the BYSIALI member of the CAW0JCL data set.

Make these changes for your allocation job:

- Provide the volser of the DASD volume on which the ILOG files should reside.
- Make sure there is one DEFINE step for each of your DB2 subsystems.
- Provide data set names. You may choose to use the naming convention LOGnn#0 for primary subfiles and LOGnn#1 for backup subfiles, where *nn* represents a DB2 subsystem. For example, here are the files for a set of three DB2 subsystems:

Subsystem	Primary	Secondary
01	LOG01#0	LOG01#1
02	LOG02#0	LOG02#1
03	LOG03#0	LOG03#1

- If you are using the BYSIALI method, do not change the values for either the LINEAR or SHAREOPTIONS parameters.

2. Identify ILOGs to CA Insight Database Performance Monitor for DB2 for z/OS.

Identify your ILOG data sets to CA-GSS through the INSIGHT member of the CAW0OPTN data set.

Each ILOG statement identifies one ILOG file and one subfile. An ILOG statement contains this information:

- A unique ILOG number that is not being used by any other application
- The dsname of a data set that you allocated for ILOG use
- The subfile for the ILOG

3. Modify your GSSA system PROCLIB member by adding the following DD statement:

```
//DB2SSID DD DSN=CAI.CAW0OPTN(DB2SSID),DISP=SHR
```

This DD statement points to the DB2SSID member of the CAW0OPTN data set.

CA-GSS reads the DB2SSID member at initialization time to determine what DB2 address spaces it should monitor and which ILOGs it should use to record information about those address spaces.

4. Identify DB2 subsystems to CA-GSS.

In the DB2SSID member referenced in your GSSA system CA-GSS PROCLIB member, you need to define an ILOG statement for each DB2 subsystem that CA-GSS will be monitoring.

The ILOG numbers in this member must match the ILOG numbers in the INSIGHT member of the CAW0OPTN data set (which was discussed in step 2).

5. Modify CA-GSS parameters.

As needed, modify the CA-GSS initialization parameters that affect the CA-GSS support. Examples of these parameters are contained in the DBDEL member of the CAW0OPTN data set.

The following parameters may need to be modified:

- **COMMAND**-Defines the INSIGHT console command to CA-GSS.

CA Insight Database Performance Monitor for DB2 for z/OS distributes a set of IMODs with a name prefix of \$DBGL_. These IMODs process operator console commands to provide additional functions to the operator.

ILOG-Defines an ILOG file. Specify this parameter once for each ILOG that you have defined.
- **ISET**-Identifies an ISET (IMOD Library) that is included on the distribution tape of CA Insight Database Performance Monitor for DB2 for z/OS.
- **PRODUCT**-Activates the CA-GSS support for CA Insight Database Performance Monitor for DB2 for z/OS.
- This parameter does not conflict with other specifications of the **PRODUCT** parameters.
- **WTO**-Executes a particular IMOD whenever a WTO that you identify is issued.
- Use the **WTO** parameter to execute the **IDB2_IDB2309E** IMOD in response to the **IDB2309** message (which indicates the **FLASHBACK** file needs to be backed up).

You will need to modify the IMOD to meet the requirement of your installation.

6. Provide an IMOD for logging.

When you are logging large volumes of data, you need to provide a \$USER_ILOG_FULL IMOD so that CA-GSS can automatically switch or reset ILOGs that become full.

Note: For more information about this special-purpose IMOD, see the *Reference Guide*.

7. Activate GoalNet.

If you are using CA Insight Database Performance Monitor for DB2 for z/OS and you are operating in a multi-CPU environment, with or without shared DASD, you may want to activate GoalNet so that CA Insight Database Performance Monitor for DB2 for z/OS can gather information from multiple systems and can consolidate displays.

In order to use the CA Insight Database Performance Monitor for DB2 for z/OS System Condition Monitor on external systems, you must install CA-GSS on all CPUs. CA Insight Database Performance Monitor for DB2 for z/OS is required on the systems where information is to be displayed.

Customize CA Jobtrac Job Management

CA Jobtrac Job Management uses CA-GSS facilities to extend its capabilities and to provide you with fully customizable support for job scheduling. In addition, CA Jobtrac Job Management information is made available to other CA-GSS client software, including that provided by you.

CAW0OPTN member JOBTRAC contains sample configuration parameters.

Note: For more information about configuration details, see the *CA Jobtrac Job Management* documentation.

Customize CA-GSS for CA MIM

CA MIM has a Tape Preferencing Control Facility (TPCF) that provides information on tape device allocation for devices shared among multiple CPUs. This information is available to REXX IMODs through ADDRESS TPCF and the \$SRV_TPCF service routine.

GSS provides the potential, with its REXX IMOD functionality, to setup integrations between the following CA products:

- CA Sysview
- CA OPS/MVS
- CA Jobtrac
- CA View

There may also be other integration paths available between these and other products and if you decide to do product integration, you should consult the product documentation for alternative methods or check with CA Technical Support. The GSS method of integration may have been superseded by more advanced techniques.

Make sure that the MIMAPI1 API module is available. This module resides in the CA MIM Load Library. This library must be in the APF list.

Note: For more information about the API module for CA MIM, see the CA NSM *CA-MIA Systems Programmer Guide*.

To customize CA-GSS for CA MIM

1. Modify the JCL.

If the CA MIM MIMAPI1 load module is not in a LINKLIST Library, include the library that contains the load module as a STEPLIB in the CA-GSS PROC.

2. Modify CA-GSS parameters.

As needed, modify the CA-GSS initialization parameters that affect CA-GSS' CA MIM support. Examples of these parameters are contained in the MIM member of the CAWOOPTN data set.

Most parameters in the MIM member are commented out. To activate one of them, replace its leading asterisk (*) with a blank.

You can copy the contents of the MIM member to your RUNPARM member, or you can simply provide an INCLUDE MIM statement.

With respect to the ADDRESS parameter, note the following:

The ADDRESS environment is provided on the CA MIM distribution tape as a load module available to REXX IMODs.

- CA-distributed IMODs expect the address names TPCF. If you use another name, provide the ALTNAME parameter to define TPCF.
- The load module name reflects the name as shipped on the CA MIM tape. Make sure that this load module resides in an APF-authorized library that is accessible to CA-GSS.

For more information, see [Optional Features](#) (see page 214).

Customize CA-GSS for CA OPS/MVS Event Management and Automation

CA OPS/MVS Event Management and Automation uses CA-GSS facilities to access other CA Technologies products and makes its facilities available to other products through CA-GSS facilities.

GSS provides the potential, with its REXX IMOD functionality, to setup integrations between the following CA products:

- CA Sysview
- CA OPS/MVS
- CA Jobtrac
- CA View

There may also be other integration paths available between these and other products and if you decide to do product integration, you should consult the product documentation for alternative methods or check with CA Technical Support. The GSS method of integration may have been superseded by more advanced techniques.

To customize CA-GSS for CA OPS/MVS Event Management and Automation

1. Make sure that the CA OPS/MVS Event Management and Automation OPGLEVMG communication module is available. This module resides in the CA OPS/MVS Event Management and Automation Load Library. This library must be in the APF list.
2. Provide appropriate CA OPS/MVS Event Management and Automation security rules so that CA-GSS can utilize CA OPS/MVS Event Management and Automation facilities. For example, provide an OPSCMD security rule to allow z/OS commands to be issued through the GSS OPER ADDRESS environment.

3. Modify your GSSA system PROCLIB member.

- If the CA OPS/MVS Event Management and Automation OPGLEVMG load module is not in a LINKLIST Library, include its library as a STEPLIB in your GSSA system PROCLIB member.
- As needed, modify the CA-GSS initialization parameters that affect CA-GSS' CA OPS/MVS Event Management and Automation support. Examples of these parameters are contained in the OPSMVS member of the CAW0OPTN data set.

Most parameters in the OPSMVS member are commented out. To activate one of them, replace its leading asterisk (*) with a blank.

You can copy the contents of the OPSMVS member to your RUNPARM member, or you can simply provide an INCLUDE OPSMVS statement.

The SSID parameter identifies the CA OPS/MVS Event Management and Automation system that should process associated ADDRESS and function requests.

The ADDRESS parameter makes up to four ADDRESS environments and a function call available to REXX IMODs.

With respect to the ADDRESS parameter, note the following:

- These ADDRESS environments and a function call are provided in the CA OPS/MVS Event Management and Automation OPGLEVMG load module.
- If you want to make the OPSVALUE() function available, you also need to provide the appropriate ADDRESS parameter.
- CA-distributed IMODs expect the address names OPER, OPSREQ, AOF, OSF, and OPSVALUE. If you use other names, provide ALTNAME parameters to define OPER, OPSREQ, AOF, OSF, and OPSVALUE.
- The load module name reflects the name as shipped on the CA OPS/MVS Event Management and Automation tape. Make sure that this load module resides in an APF-authorized library that is accessible to CA-GSS.

Customize CA SYSVIEW Performance Management

CA-SYSVIEW provides facilities that may be used by IMODs and by other CA Technologies products through the use of IMODs.

For more information about configuration details, see the *CA SYSVIEW Performance Management* documentation.

Customize CA-GSS for CA View

CA View provides facilities that may be used by IMODs and by other CA Technologies products through the use of IMODs.

Make sure that the CA View SARINTF communication module is available. This module is on the CA View tape and must be moved to an APF-authorized LINKLIB data set.

To configure CA-GSS for CA View

1. Modify your GSSA system PROCLIB member.

If the CA View SARINTF load module is not in a LINKLIST Library, include its library as a STEPLIB in your GSSA system PROCLIB member.

2. Modify CA-GSS parameters. As needed, modify the CA-GSS initialization parameters that affect CA-GSS support of CA View. Examples of these parameters are contained in the VIEW member of the CAW0OPTN data set.
 - Most parameters in the VIEW member are commented out. To activate one of them, replace its leading asterisk (*) with a blank.
 - You can copy the contents of the VIEW member to your RUNPARM member, or you can simply provide an INCLUDE VIEW statement.
 - For more information about any CA-GSS initialization parameter, see the *Reference Guide*.
 - The ADDRESS parameter makes the ADDRESS environment provided on the CA-View distribution tape as a load module available to REXX IMODs.
 - With respect to the ADDRESS parameter, note the following:
 - CA-distributed IMODs rely on the address name XPVIEW. If you choose another name, use the ALTNAME parameter to define XPVIEW.
 - The name of the load module reflects the name as shipped on the CA View distribution tape. Make sure that this load module resides in an APF-authorized library that is accessible to CA-GSS.
 - The VIEW parameter provides parameters to the initialization IMOD that CA View provides. You can specify the VIEW parameter multiple times.

Customize CA-GSS for DB2

If you are running the IBM DB2 database software, an IMOD can retrieve data by executing dynamic SQL statements.

Make sure that the DSNALI and DSNHLI2 communication modules of DB2 are available. These modules must reside in an APF-authorized LINKLIB data set.

To configure CA-GSS for DB2

1. Modify your GSSA system PROCLIB member.

If the DB2 DSNALI and DSNHLI2 load modules are not in a LINKLIST Library, include their library as a STEPLIB in the GSSA system PROCLIB member.

2. Modify CA-GSS parameters. As needed, modify the CA-GSS initialization parameters that affect CA-GSS' DB2 support. Examples of these parameters are contained in the DB2 member of the CAW0OPTN data set.

- Most parameters in the DB2 member are commented out. To activate one of them, replace its leading asterisk (*) with a blank.
- You can copy the contents of the DB2 member to your RUNPARM member, or you can simply provide an INCLUDE DB2 statement.
 - The ADDRESS parameter loads the DB2 DSNALI and DSNHLI2 modules during CA-GSS/ISERVE initialization and makes them available for processing the DB2() REXX function.
 - The DB2PLAN parameter identifies the plan that will be bound to the DB2 where your SQL statements will be processed. The default name is GSSPLAN. If you use a different plan, specify the name through the DB2PLAN parameter.
 - The SSID parameter identifies the DB2 address space that CA-GSS should communicate with. Each CA-GSS can communicate with only one DB2 address space.

The default value is DSN.

If your DB2 address space uses a different subsystem ID, or you want CA-GSS to communicate with a different address space, use the SSID parameter to properly identify the address space.

If you want to process dynamic SQL in multiple DB2 address spaces, you can provide secondary ISERVE address spaces, one for each DB2. GoalNet can then be used to direct processing requests to the appropriate ISERVE address space.

3. Create the SRVDB2P load module.

Since dynamic SQL programs are highly dependent upon DB2 release level, program name, and date and time of program assembly, CA-GSS distributes the SRVDB2P program in source format. This program, along with sample JCL, can be found in the CAW0JCL member BYSDB2P.

4. Bind the plan.

Before you execute dynamic SQL using the DB2() function, you must bind the plan (created in step 2 and specified in the DB2PLAN initialization parameter) to the target DB2 address space.

Customize CA-GSS for IDCAMS

CA-GSS/ISERVE makes the facilities provided by the IBM Access Method Services (IDCAMS) available to IMODs.

Ensure that the IDCAMS load module is available. This module must reside in an APF-authorized LINKLIB data set and be accessible to CA-GSS/ISERVE.

To customize CA-GSS for IDCAMS

1. Modify your GSSA system PROCLIB member.

If the IDCAMS load module is not in a LINKLIST Library, include its library as a STEPLIB in the CA-GSS PROC(BYSGSSA).

2. Modify CA-GSS parameters.

As needed, modify the CA-GSS initialization parameters that affect CA-GSS' IDCAMS support. Examples of these parameters are contained in the IDCAMS member of the CAW0OPTN data set.

Most parameters in the IDCAMS member are commented out. To activate one of them, replace its leading asterisk (*) with a blank.

You can copy the contents of the IDCAMS member to your RUNPARM member, or you can simply provide an INCLUDE IDCAMS statement.

- The ADDRESS parameter makes the ADDRESS environment provided through the IDCAMS load module available to REXX IMODs.
- CA-provided IMODs expect the address name IDCAMS. If you use another name, use the ALTNAME parameter to define the name IDCAMS.

Optional Features

Consider whether you need to use the following optional CA-GSS features:

GoalNet

GoalNet is an LU 6.2-based communications protocol that CA-GSS uses to permit cross-system communication by CA Technologies products and user-written IMODs.

Use GoalNet if you want to use VTAM to enable communications between multiple copies of z/OS or multiple copies of CA-GSS on the local system.

ILOGs

ILOG files are VSAM linear data sets (LDS) that are used to record WTO text and other events of interest.

You need to use ILOGs if you are using CA Insight Database Performance Monitor for DB2 for z/OS or if you have written your own IMOD applications for capturing and processing data.

Logon Facility

The Logon Facility provides access to the CA-GSS/ISERVE Control Panel from VTAM applications.

You may want to use the Logon Facility if you want to display and control CA-GSS from VTAM applications.

GoalNet

Each ISERVE that participates in GoalNet is called a node. Each GoalNet node requires a single VTAM ACB and establishes a bi-directional link with every other node in GoalNet.

GoalNet is a peer-to-peer implementation. Each node maintains its own membership in the network.

Defining GoalNet

GoalNet is defined by parameters specified using the PARMLIB DD statement included in a CA-GSS address space. All address spaces in the network can use a common set of parameters.

GOALNET Parameter

Specify the GOALNET parameter once for each CA-GSS address space that is to participate in the network. CA-GSS recognizes its own node by the GOALNETLOCAL parameter. Only nodes defined by the GOALNET parameter may be communicated with.

CAWOOPTN Member: GOALNET

A sample GoalNet definition is provided in the GOALNET member of the CAWOOPTN data set. Examine this member before creating your own GoalNet definitions.

Note: For more information about GOALNET, see the *Reference Guide* and the *Administration Guide*.

Sample LOGMODE Table

Under the IBM implementation of LU 6.2 (APPC), each conversation is based on a *logmode*. A logmode is a set of parameters that define how the conversation is to be conducted. Although a certain amount of negotiation is performed between two nodes to arrive at a compatible subset of logmode parameters, all GoalNet participants should use identical logmode parameters.

A special logmode, SNASVCMG, is used by the underlying IBM code to establish a conversation for the purpose of establishing the other conversations. SNASVCMG must not be changed from its IBM-provided values.

Logmode definitions are combined into a *logmode* table. Each application ID then specifies one logmode table from which all logmode entries will be selected. Both the logmode table and the default logmode are specified in the application ID definition. These values can be modified by the VTAM operator command.

The logmode table must be assembled, using VTAM-supplied MACRO libraries, and link-edited into your SYS1.VTAMLIB data set or its equivalent. Do not modify the supplied values unless you are sure that you know what you are doing. The SNASVCMG logmode is provided by IBM and is used by their internal protocols when sessions are established. If you modify the SNASVCMG logmode, GoalNet will probably not work.

CAWOOPTN Member: BYSMTAB

A sample logmode table is provided in the BYSMTAB member of the CAWOOPTN data set. Use this table exactly as provided.

An assembled and link-edited version of the provided logmode table is distributed in the CAWOLOAD data set under the name GOALNETT. It was assembled using VTAM MACROs at Version 3, Release 4. If you are certain that this module is compatible with your current VTAM release, you may copy it. Otherwise, assemble and link-edit the provided table source code, using your own macro libraries.

Define GoalNet to VTAM

Each ISERVE that participates in GoalNet as a node requires a VTAM application ID (ACB). This ACB must be configured for LU 6.2 communications (APPC=YES). The node uses the ACB to establish conversations with other GoalNet nodes. Each conversation requires one VTAM session. During z/OS to z/OS operations, the conversation remains allocated for the duration of the communication. For operations where the target node is not executing under z/OS, the conversation terminates as soon as the request has been made to the remote node. If results need to be returned, a different conversation is allocated.

CAWOOPTN Member: BYSVTAM

The BYSVTAM member of the CAWOOPTN data set contains sample definitions for both GoalNet and Logon Facility applications. Only the minimum parameters are shown.

Important! Do not make changes or additions to these parameters unless you fully understand VTAM requirements.

ILOG Files

ILOG files are VSAM linear data sets (LDS) that are used to record WTO text and other events of interest.

You can allocate up to 100 ILOGs per ISERVE address space, and you can provide up to 10 subfiles per ILOG. Each subfile is one VSAM LDS. During operation, when a subfile is filled, recording switches to the next subfile.

Modify and submit an SRVMaint job that contains one or more ALLOC_ILOG commands. Each ALLOC_ILOG statement allocates a pair of VSAM linear data sets. If you modify this job, do not modify the LINEAR and SHAREOPTIONS parameters.

Example Statement

```
ALLOC_ILOG NAME CLUSTER VOLSER xxxxxx CYL 1 1
```

Another way of allocating these data sets is to modify and submit the BYSIALI member of the CAWOJCL data set.

Logon Facility

CA-GSS provides an LU 2 gateway to VTAM. This permits terminal users to connect with CA-GSS and establish a session under control of an IMOD task. Several CA Technologies products provide session-control IMODs to communicate with software executing on personal computers. In addition, your installation may develop applications to permit terminal users to interact with CA-GSS and, through address environments, with other CA Technologies products.

Security

During the logon procedure, each user may be required to specify a user ID and password. If your installation is using RACF (or other SAF-compatible) security software, the user session executes under the authority of the user ID.

ISET Upgrades

If you have any ISETs that were not distributed on the CA Common Services for z/OS tape, it is possible that the IMODs contained in them were compiled under a different version of CA-GSS.

In general, minor differences in compiler and interpreter versions will not create problems. However, to eliminate the potential for error, CA-GSS automatically recompiles back-leveled (or up-leveled) IMODs during initialization. This recompiling is done in memory but is not saved back to the ISET on DASD.

The CA-GSS SRVMAINT program provides an UPGRADE command that causes the recompiling of all IMODs in an ISET or all IMODs that are not at the current release level.

The BYSUPGR member of the CAWOJCL data set contains sample JCL and control statements for upgrading ISETs.

Note: For more information about the SRVMAINT program, see the *Administration Guide*.

Define the Logon Facility

To ensure that each application is acceptable at logon, you can define the Logon Facility.

To define the logon facility

1. Define the network.

Before you activate the Logon Facility, you need to define a VTAM application ID. Ask your VTAM systems programmer to provide an LU name capable of accepting logons from terminals. A definition that takes all defaults is generally satisfactory.

For sample VTAM definitions, see the BYSVTAM member of the CAWOOPTN data set. (This member is also used to define GoalNet.)

2. Provide applications.

You must determine each application, by name, to be acceptable for logon. In addition, you must provide an IMOD for each application that is capable of accepting input from the terminal, processing it, and providing a 3270 data stream for display. As an example, CA provides an application IMOD (\$SRVV) that provides a CA-GSS operator interface.

Note: For more information about writing application IMODs, see the *Administration Guide*.

3. Modify CA-GSS parameters.

As needed, modify the CA-GSS initialization parameters that affect the Logon Facility. Examples of these parameters are contained in the LOGON member of the CAW0OPTN data set. Note that:

- Most parameters in the LOGON member are commented out. To activate one of them, replace its leading asterisk (*) with a blank.
- You can copy the contents of the LOGON member to your RUNPARM member, or you can provide an INCLUDE LOGON statement.
- A summary description of each parameter you may need to modify is provided in the following table.

Parameter	Description
LOGON LUNAME LOGON LUNAME luname password	Replace <i>luname</i> with an application ID that has been defined to VTAM. This is the name by which terminal users will request a session with CA-GSS. If your installation requires VTAM passwords, you must also specify the correct value. If a password is not required, remove <i>password</i> and leave the field blank. This parameter is required.
LOGON APPLICATION LOGON APPLICATION OPERator \$SRVV	Each application that may be used with the Logon Facility must be defined during initialization (or later, by using the LOGON DEFINE command). You must assign a name to the application, an IMOD that provides the processing support for the application, and an optional argument string that should be passed to the IMOD.

Note: The application name is case sensitive as shown. To select the application, users must specify all leading uppercase letters. However, they can omit trailing lowercase letters. Except for this special treatment of the application name, all other fields are case-insensitive. For example, the application name 'USERS' matches the strings 'user' and 'users'. However, it will not match the strings 'use' or 'userid'.

The OPERATOR application is provided with CA-GSS (IMOD \$SRVV) and may be activated to provide a VTAM-based CA-GSS/ISERVE Control Panel.

Chapter 12: CA-L-Serv Configuration Tasks

After installing CA Common Services for z/OS, configuration tasks and procedures must be performed before starting CA-L-Serv.

Note: Use your deployed datasets when performing these tasks.

This section contains the following topics:

[Update External Security for CA-L-Serv](#) (see page 219)

[Define CA-L-Serv to VTAM](#) (see page 226)

[Tailor Startup Parameters](#) (see page 226)

[Update the Message Table](#) (see page 228)

[Copy and Customize the Startup Procedure](#) (see page 229)

[Start CA-L-Serv](#) (see page 230)

[Verify the Communications Server Installation](#) (see page 230)

[Verify the File Server Installation](#) (see page 233)

Update External Security for CA-L-Serv

If you do not plan to use CA-L-Serv to manage data sets, you can skip this section.

CA-L-Serv 3.5 introduced two major security enhancements:

- Before a requester is allowed to open a data set using CA-L-Serv, external security is invoked to verify that the user has the required level of authority to have CA-L-Serv open the data set on the behalf of the user. This is done by checking the user access against the data set using the new \$LSRVDSN resource class.
- Before CA-L-Serv is allowed to open a data set that has been placed under its control by an ADDFILE command, external security is invoked to verify that the CA-L-Serv user ID has the required authority to open the data set.

Who Needs to Update?

If you have installed CA-L-Serv for the first time or if you are upgrading from CA-L-Serv level 9501 or older, your security system will need updating in order to:

- Create a specific user ID for the CA-L-Serv started task and grant this user ID sufficient access to managed data sets.
- Create a resource class for data sets placed under the management of the File Server and grant users sufficient access to the new resource class.

How the Update Tasks are accomplished

The security enhancements generally require the security administrator to accomplish the following:

- Create a new resource class: \$LSRVDSN.
- Define CA-L-Serv data sets to the new resource class.
- Permit access to users through the new resource class.
- Create a user ID for the CA-L-Serv started task.
- Permit the CA-L-Serv user ID access to the data sets.

Usage Notes

Please note the following:

- Security definitions previously implemented for CA Endeavor Software Change Manager or other products need not be altered. The security checks made by these products will still function in exactly the same manner.
- For administrators who do not wish to discriminate between CA-L-Serv data sets, defining a resource named 'ALL' in class \$LSRVDSN and giving users or groups CONTROL access to this resource provides a convenient means of controlling access to CA-L-Serv data sets without having to make extensive new security definitions.
- Allowing users to use the \$LSRVDSN class gives them access to the data sets only through CA-L-Serv. It does not provide any access to the data sets through any other program (such as IDCAMS REPRO).
- Privileged users who already have CONTROL access to the data sets managed by CA-L-Serv will be able to access data sets using CA-L-Serv in the same manner as outside CA-L-Serv. No additional definitions are necessary for these privileged users.
- The CA-L-Serv utility program, LDMAMS, can be executed only under a user ID that has CONTROL access to the data sets.

Important! CA Endeavor Software Change Manager users must grant access to the new resource class to the 'true' user ID, not the 'alternate' user ID. When CA Endeavor Software Change Manager invokes CA-L-Serv, the 'true' user ID is in control, not the 'alternate' user ID.

The following sections describe implementation of external security for CA-L-Serv in three different environments.

Implement Security with CA Top Secret

The following sample definitions are for users running under CA Top Secret. The actual implementation in your environment may differ from these templates.

To implement security with CA Top Secret

1. Define the new resource class to the CA Top Secret Resource Descriptor Table (RDT). For example:

```
TSS ADD(RDT) RESCLASS($LSRVDSN) RESCODE(02) ATTR(LONG,DEFPROT)
      ACLST(CONTROL) DEFACC(CONTROL)
```

Note: For more information about the command syntax and features, see the *CA Top Secret Reference Guide*.

2. Protect your data sets using the \$LSRVDSN resource class.

One approach is to issue commands to define the data sets that are under the control of CA-L-Serv:

```
TSS ADDTO(owner_acid) $LSRVDSN(prefix1)
TSS ADDTO(owner_acid) $LSRVDSN(prefix2)
```

An alternative approach is to define a pseudo data set named 'ALL' that stands for all the data sets under CA-L-Serv control:

```
TSS ADDTO(owner_acid) $LSRVDSN(all)
```

3. Permit the users access to the CA-L-Serv data sets.

Once the resources are protected, issue PERMIT commands to permit users access to these data sets using the \$LSRVDSN resource class:

```
TSS PERMIT(user_acid1) $LSRVDSN(dsname1) ACCESS(CONTROL)
TSS PERMIT(user_acid1) $LSRVDSN(dsname2) ACCESS(CONTROL)
TSS PERMIT(user_acid2) $LSRVDSN(dsname1) ACCESS(CONTROL)
```

This can also be achieved using a generic prefix:

```
TSS PERMIT(user_acid) $LSRVDSN(prefix.) ACCESS(CONTROL)
```

Optionally, users may be permitted access to the 'ALL' resource:

```
TSS PERMIT(user_acid1) $LSRVDSN(all) ACCESS(CONTROL)
TSS PERMIT(user_acid2) $LSRVDSN(all) ACCESS(CONTROL)
```

4. Define CA-L-Serv to CA Top Secret.

A user ID must be created for CA-L-Serv so it has access to its data sets. To do this, specify:

```
TSS CREATE(lserv_acid) TY(USER) DEPT(deptname) FAC(STC) -  
      NAME('name') PASS(NOPW,0) NOSUBCHK
```

5. Permit CA-L-Serv access to data sets.

CA-L-Serv must be given authority to access its data sets using the PERMIT command:

```
TSS PERMIT(lserv_acid) DSN(dsname1) ACCESS(CONTROL)  
TSS PERMIT(lserv_acid) DSN(dsname2) ACCESS(CONTROL)
```

This permission can also be achieved using a generic prefix:

```
TSS PERMIT(lserv_acid) DSN(prefix.) ACCESS(CONTROL)
```

Implement Security with CA ACF2

The following are sample definitions for users running under CA ACF2. The actual implementation in your environment may differ from these templates.

- CLASMAP the new \$LSRVDSN resource class to resource type LSV.

For example:

```
SET CONTROL(GS0)  
INSERT CLASMAP.LSRV2 ENTITYLN(44) -  
      RESOURCE($LSRVDSN) RSRCTYPE(LSV)
```

Issue a MODIFY command from the console:

```
F ACF2,REFRESH(CLASMAP)
```

- Protect your data sets using the \$LSRVDSN resource class.

Create resource rules for the data sets that are under the control of CA-L-Serv:

```
SET RESOURCE(LSV)
COMPILE
.$KEY(prefix1) TYPE(LSV)
.UID(*****userid1) SERVICE(DELETE) ALLOW
.UID(*****userid2) SERVICE(DELETE) ALLOW
.<blank character>
STORE
```

Optionally, you can define a pseudo data set of 'ALL' to represent all the data sets under CA-L-Serv control:

```
SET RESOURCE(LSV)
COMPILE
.$KEY(ALL) TYPE(LSV)
.UID(*****userid1) SERVICE(DELETE) ALLOW
.UID(*****userid2) SERVICE(DELETE) ALLOW
.<blank character>
STORE
```

- Create or modify access rules for relevant data sets to give CA-L-Serv the required access.

```
SET RULE
COMPILE
.$KEY(prefix1)
.$MODE(ABORT)
.qualifier.qualifier UID(*****LSERV) WRITE(A)
.<blank character>
STORE
```

```
COMPILE
.$KEY(prefix2)
.$MODE(ABORT)
.qualifier.qualifier UID(*****LSERV) WRITE(A)
.<blank character>
STORE
```

Implement Security with RACF

The following are sample definitions for users running under RACF. The actual implementation in your environment may differ from these templates.

- Add an entry for the new resource class to the Class Descriptor Table. The Class Descriptor Table ICHRRCD E must then be assembled and linked into SYS1.LPALIB. For example:

```
LSERVDSN ICHERCDE CLASS=$LSRVDSN,           X
          ID=(valid installation value),      X
          MAXLNTH=44,                          X
          FIRST=ALPHA,                          X
          OTHER=ANY,                            X
          POSIT=(valid installation value),    X
          OPER=NO,                              X
          RACLIST=ALLOWED,                     X
          DFTUACC=NONE
```

Consult the RACF bibliography for the correct values for ID and POSIT. You *must* consider both IBM and site restrictions.

Important! Changes to the Class Descriptor Table require an IPL to take effect.

- Update the link to the RACF Router Table.

The CA-L-Serv interface uses the RACROUTE macro. Therefore, the RACF Router Table (ICHRFR01) must also be updated and linked into a link listed library. For example:

```
ICHRFR01 CLASS=$LSRVDSN,           X
          ACTION=RACF
```

- Activate the \$LSRVDSN class.

Following an IPL with the new Class Descriptor Table, enter the following command:

```
SETROPTS CLASSACT($LSRVDSN)
```

- Define the data sets to RACF using the \$LSRVDSN class.

You can issue commands to define the data sets that are under the control of CA-L-Serv:

```
RDEF $LSRVDSN dsname1 UACC(NONE) OWNER(ownerid)
RDEF $LSRVDSN dsname2 UACC(NONE) OWNER(ownerid)
RDEF $LSRVDSN dsname3 UACC(NONE) OWNER(ownerid) (etc.. )
```

Optionally, you can define a resource of 'ALL' to represent all the data sets under CA-L-Serv control:

```
RDEF $LSRVDSN all UACC(NONE) OWNER(ownerid)
```

- Permit the users access to the CA-L-Serv data sets.

Once data sets are defined as resources, issue commands to permit users access to these data sets using the \$LSRVDSN resource class:

```
PERMIT dsname1 ID(userid1) AC(CONTROL) CLASS($LSRVDSN)
PERMIT dsname2 ID(userid1) AC(CONTROL) CLASS($LSRVDSN) ...
```

Optionally, you can permit CA-L-Serv users access to the 'ALL' resource:

```
PERMIT all      ID(userid1) AC(CONTROL) CLASS($LSRVDSN)
PERMIT all      ID(userid2) AC(CONTROL) CLASS($LSRVDSN)
PERMIT all      ID(userid3) AC(CONTROL) CLASS($LSRVDSN)
```

- Define CA-L-Serv to RACF.

Create a user ID for CA-L-Serv providing access to its data sets. To do this, type:

```
AU lsrv-id DFLTGRP(systask) PASSWORD(xxxxxxxx)
```

In this example, a user ID of *lsrv-id* and a group of *systask* are chosen. These are arbitrary names; any name of up to seven characters is valid.

- Add CA-L-Serv to the RACF Started Procedures Table.

There must be an entry for CA-L-Serv in the RACF Started Procedures Table (ICHRIN03). This can be accomplished in either of the following ways:

- Establish a separate entry for the CA-L-Serv started task.
- For example:

LSERV	DC	CL8'LSERV'	CA-L-Serv proc name
	DC	CL8'LSERVID'	CA-L-Serv userid
	DC	CL8'SYSTASK'	CA-L-Serv group
	DC	XL1'00'	unused
	DC	XL7'00'	unused

In addition, it is necessary to add 1 to the number of entries in the table. This table must be assembled and linked into SYS1.LPALIB, and an IPL must be performed.

- If a generic entry exists in the table, you may set up the CA-L-Serv procname and user ID to conform to that entry.
- Give CA-L-Serv authority to access its data sets using the PERMIT command:

```
PERMIT 'data set name' ID(LSERVID) ACCESS(CONTROL)
```

Define CA-L-Serv to VTAM

This procedure is necessary only if you plan to use VTAM to support communication between copies of CA-L-Serv executing on different systems.

To define CA-L-Serve to VTAM

1. Create a major node member in your SYS1.VTAMLST data set using the CCCSOPTN member SAMPACB as a template.
2. Specify an APPL statement for each local instance of CA-L-Serv that will use VTAM to communicate with other instances of CA-L-Serv executing on other z/OS images.
3. Identify the new major node to VTAM by adding the member name to the ATCCONxx member of your SYS1.VTAMLST. This will ensure that the corresponding APPL is activated when you start VTAM.
4. Define the cross-domain resources to VTAM by adding the corresponding CDRSC definitions to your SYS1.VTAMLST data set.

Notes: The SAMPACB definition provided in the *YourdeployHLQ.CCCSOPTN* data set may be used for either LU 0 or LU 6.2 communication.

5. Your new definitions can be activated without having to restart VTAM by issuing V NET,ACT,ID=.... commands against the newly-defined resources.

Tailor Startup Parameters

The installation of CA-L-Serv places the sample startup command member LSVPARM into the target CCCSOPTN data set. A sample CA-L-Serv startup parameter member follows, with an explanation for each line of the parameter.

```
OPTION  SVCDUMP(YES)                (1)
ADDLOG  MSGLOG  SYSOUT(X)           (2)
ADDLOG  SQLLOG  SYSOUT(X)
*
IFSYS  SYSA                          (3)
      ATTACH  COMMSERVER  ACBNAME=COMMSYSA,  (4)
                        CONTYPE=LU0,
                        LOG=MSGLOG
      ACTIVATE  COMMSYSB                (5)
      ACTIVATE  COMMSYSC
```

```

ATTACH FILESERVER SERVETYPE=HOST (6)
ADDPPOOL 01 (4096,32) (8192,16) (7)
ADDFILE FILE1 XXXXXXX.FILE1.VSAM,POOL(1) (8)
ADDFILE FILE2 XXXXXXX.FILE2.VSAM,POOL(1)
ADDFILE LDMSQL XXXXXXX.LSERV.SQLDICT, (9)
        BUFND=5 BUFNI=5
ATTACH SQLSERVER LOGID=SQLLOG AUDIT=ALL (9)
ENDIF (3)
*IFSYS SYSB (3)
    ATTACH COMMSERVER ACBNAME=COMMSYSB,
        CONTYPE=LU0,
        LOG=MSGLOG
    ACTIVATE COMMSYSA CONTYPE=LU0
    ATTACH FILESERVER SERVETYPE=REMOTE (*)
ENDIF (3)
*IFSYS SYSC (3)
    ATTACH COMMSERVER ACBNAME=COMMSYSC etc.
(...)
    ATTACH FILESERVER SERVETYPE=REMOTE (*)
ENDIF (3)

```

Footnotes:

(1) This command enables the CA-L-Serv recovery code to schedule dumps when exception conditions are encountered.

Since CA-L-Serv does not take duplicate dumps when identical ABENDs recur, this option should not be altered.

(2) The ADDLOG command defines message logs for the various components of CA-L-Serv.

(3) The IFSYS/ENDIF statements cause CA-L-Serv to skip all embedded commands until a match is found on the system sysid. This provides a convenient means of maintaining startup parameters for related CA-L-Serv regions executing on different z/OS images within a single LDMPARM member.

(4) The various services are attached as z/OS subtasks using the ATTACH command. Consult the documentation for your client application to determine which services are necessary to its successful execution.

Delete statements that are not relevant to your environment. For instance, all communications server commands are not necessary if you run on a single system.

(5) The ACTIVATE command enables communication between CA-L-Serv regions sharing the same subsystem name executing on different systems.

Note: This command is valid only for VTAM communication. Comment it out or delete it for any systems that use XCF communication.

(6) This File Server is identified as the HOST. It has physical access to the data sets and will service requests from both local regions executing on SYSA and remote callers executing on SYSB and SYSC.

Note: All other File Servers in the complex have a SERVERTYPE of REMOTE (*). In a single CPU context, specify SERVERTYPE=LOCAL.

(7) The ADDPOOL command causes CA-L-Serv to invoke VSAM in order to create a pool of shared buffers.

(8) The ADDFILE command causes CA-L-Serv to dynamically allocate a data set, enabling CA-L-Serv to process I/O requests.

(9) If you plan to use the SQL Server, you need to allocate the SQL dictionary (DDname=SQLDICT) before activating this component.

Note: A functionally equivalent setup in three separate members (LSVPARAM1, LSVPARAM2, and LSVPARAM3) is also provided in the *YourdeployHLQ.CCCSOPTN* data set.

Update the Message Table

The installation of CA-L-Serv places the LSERVMSG message member into the target CAI.CCCSOPTN Library. The new message member may need to be copied to an active CA-L-Serv PARMLIB so that it can be accessed when CA-L-Serv is started.

Customize the following JCL to meet the requirements of your data center:

```
//LOAD      EXEC PGM=IEBCOPY,REGION=256K
//SYSPRINT DD  SYSOUT=A
//I1        DD  DISP=SHR,
//          DSN=CAI.CCCSOPTN           <=== your Deployed DSN
//01        DD  DISP=SHR,
//          DSN=CAI.LDMCMND           <=== your Deployed DSN
//SYSUT3    DD  UNIT=SYSDA,
//          SPACE=(CYL,(5,5))
//SYSUT4    DD  UNIT=SYSDA,
//          SPACE=(CYL,(5,5))
//SYSIN     DD  *
            COPY 0=01,I=((I1,R))
            SELECT M=LSERVMSG
```

If the CA-L-Serv parameter data set already contains an older version of the LSERVMSG member, rename it before submitting this JCL.

Copy and Customize the Startup Procedure

The installation of CA-L-Serv places the startup procedure, LSVPROC, into the target procedure library *YourdeployHLQ.CCCSPROC*. Copy the procedure to SYS1.PROCLIB or any of the system procedure libraries so that it can be accessed when CA-L-Serv is started.

The following template is provided:

```
//LSVPROC PROC PLIB='CAI.CCCSOPTN', (1)/* CA-L-Serv PARMLIB */
// AUTHLIB='CAI.CCCSLOAD', (2)/* CA-L-Serv LOADLIB */
// MEMB=LDM Parm, (3)/* CA-L-Serv parm member*/
// JCL='CAI.CCCSJCL', (4)/* CA-L-Serv jcl lib */
// REUSE=YES, (5)/* Reuse CSA */
// SSN=LSRV (6)/* Subsystem name */
//*
//***** CA-L-Serv *****
//*
//* Use this procedure to start up L-Serv using a console command
//*
//*****
//*
//LSERV EXEC PGM=LDMMAIN,REGION=8M,DPRTY=(15,15),TIME=1440,
// PARM=('ME=&MEMB','REU=&REUSE','SSNM=&SSN')
//*
//STEPLIB DD DSN=&AUTHLIB,DISP=SHR
//LDMCMND DD DSN=&PLIB,DISP=SHR
//SYSPRINT DD SYSOUT=A
//SYSTEM DD SYSOUT=A
//SYSUDUMP DD SYSOUT=A
//INTRDR DD SYSOUT=(A,INTRDR)
//ERRORLOG DD SYSOUT=A
//JCLLIB DD DSN=&JCL,DISP=SHR
```

To customize the startup procedure

1. Update the LDMCMND DD to reflect the name chosen for the CA-L-Serv parameter data set.
2. Update the STEPLIB DD to reflect the name chosen for the CA-L-Serv Load Library.
3. Specify the LDMPARM member of the LDMCMND PARMLIB that will be read by CA-L-Serv when it initializes.
4. Update the JCLLIB DD to reflect the name chosen for the CA-L-Serv JCL Library.
5. Specify REUSE=YES unless directed otherwise by CA Support.
6. Specify a unique subsystem name.

Important! Do not define CA-L-Serv z/OS subsystems using the active IEFSSNxx member of SYS1.PARMLIB because doing so prevents CA-L-Serve and the associated products from initializing successfully.

Start CA-L-Serv

Start CA-L-Serv from a z/OS console using the START command.

- If you choose to have identical z/OS subsystem and procedure names, direct the execution to the Job Entry Subsystem expressly by specifying START */svproc*,SUB=JESx, thereby preventing CA-L-Serv from executing under the z/OS Master Scheduler.
- A syntax error in the parms can cause CA-L-Serv to terminate. Be sure to investigate and correct the cause of any errors before restarting, rather than restarting automatically, because each automatic restart allocates additional system resources.

Verify the Communications Server Installation

If you do not plan to use CA-L-Serv on multiple systems or if you will not use the CA-L-Serv Communications Server, you may skip this section.

The Installation Verification Procedure for the Communications Server ensures that CA-L-Serv tasks running on different systems are able to establish communication and exchange messages.

The following procedure may be repeated between every pair of systems that will use CA-L-Serv to establish communication.

To verify the Communications Server installation

1. Tailor the JCL members HJ35IVC1 and HJ35IVC2.

Customize the following templates available in members HJ35IVC1 and HJ35IVC2, which the installation placed in the CCCSJCL data set.

Receiving job:

```
//HJ35IVC1 JOB (JOBACNT) (1)
//MAMS0001 EXEC PGM=LDMAMS
//STEPLIB DD DISP=SHR,DSN=CAI.CCCSLOAD (2)
//SSN$xxxx DD DUMMY (3)
//SYSPRINT DD SYSOUT=X
//SYSIN DD *
  COMMTEST (4)
  RECEIVE
  END
/*
```

Sending job:

```
//HJ35IVC2 JOB (JOBACNT) (1)
//MAMS0001 EXEC PGM=LDMAMS
//STEPLIB DD DISP=SHR,DSN=CAI.CCCSLOAD (2)
//SSN$xxxx DD DUMMY (3)
//SYSPRINT DD SYSOUT=X
//SYSIN DD *
  COMMTEST (4)
  WAIT APPL(HJ35IVC1)
  SEND
  END
/*
```

Footnotes:

- (1) Provide a valid job card.
- (2) Change to the CA-L-Serv target library.
- (3) Replace xxxx by the z/OS subsystem name that you specified in your CA-L-Serv start procedure.
- (4) The SYSIN statements in both jobs are self-explanatory.

Important! The two jobs must have different job names.

2. Start CA-L-Serv on both systems.

Start CA-L-Serv on the two z/OS systems that will run the test.

Important! You must ATTACH both the Communications Server and the File Server to run this test successfully.

3. Submit HJ35IVC1.

Submit this job on the first of the two systems. This job will emulate a client application that will receive a message from his partner on the second z/OS system. HJ35IVC1 will wait until it receives data from the sending system.

4. Submit HJ35IVC2.

Submit this job on the second of the two z/OS systems. The job sends 512 bytes of data to job HJ35IVC1 running on the other system. Both jobs should end immediately after this job is submitted.

5. Verify the results.

- Browse the spooled output of job HJ35IVC1. You should see the following messages:

```
COMMTEST
LDM0829I CommServer initialization returned RC=0000 Reason=0000
RECEIVE
LDM0832I Receive complete: APPL=HJ35IVC2 QUAL=COMMTEST Length=512
END
LDM0829I CommServer LCOMSHUT returned RC=0000 Reason=0000
```

- Browse the spooled output of job HJ35IVC2. You should see the following:

```
COMMTEST
LDM0829I CommServer initialization returned RC=0000 Reason=0000
WAIT APPL(HJ35IVC1)
SEND
LDM0829I CommServer send returned RC=0000 Reason=0000
END
LDM0829I CommServer LCOMSHUT returned RC=0000 Reason=0000
```

Any return code higher than 0 from both jobs indicates a problem.

The Communications Server installation is verified.

Troubleshoot: Communications Server IVP is Not Running Successfully

Symptom:

There are multiple reasons why the Communications Server IVP might not run successfully. Identifying these problems at an early stage is precisely the purpose of the IVP.

Solution:

Do the following:

- Review the output of jobs HJ35IVC1 and HJ35IVC2.
- Review the message logs of CA-L-Serv on both systems and look for messages with corresponding timestamps.
- Verify that the file server and the communications server are active on both systems. The DISPLAY ACTIVE command lists the currently active servers.
- Verify that the subsystem name specified on the SSN\$xxxx DD DUMMY statement in both IVP jobs matches the subsystem name specified in the CA-L-Serv procedure (LSVPROC).
- If you are using VTAM communication, issue 'DISPLAY NET,ID=' commands to verify the state of your APPL and CDRSC definitions.
- If you are using XCF, issue 'D XCF,G' commands to verify the status of the XCF group created by the communications server. The group initialized by CA-L-Serv at start-up is LSRVxxxx where xxxx is the subsystem name specified in the CA-L-Serv procedure (LSVPROC).

If you are still experiencing problems after checking the above, retain the relevant diagnostic information and contact CA Support.

Verify the File Server Installation

If you do not plan to use CA-L-Serv to manage data sets, you can skip this section.

The Installation Verification Procedure for the File Server ensures that an application running on the same system as CA-L-Serv is able to access data sets managed by the File Server.

The installation of CA-L-Serv places installation verification JCL members HJ35IVF1 and HJ35IVF2 in the target source library CCCSJCL.

The File Server IVP uses the LDMAMS utility to perform a simple maintenance task against a managed data set.

Note: You may choose to back up one of your client product data sets rather than the VSAMTEST file used in this procedure.

To verify the file server installation

1. Initialize the VSAM test file and allocate a work file.

Customize and run job HJ35IVF1 that the installation copied into the CCCSJCL data set. This job will allocate and initialize the CAI.VSAMTEST VSAM data set as well as a sequential work file.

```
//HJ35IVF1 JOB (JOBACCNT) (1)
//IEFBR14 EXEC PGM=IEFBR14 (2)
//BACKUP DD DISP=(,CATLG,DELETE),DSN=CAI.VSAMTEST.BACKUP,(3)
// VOL=SER=XXXXXX,UNIT=SYSDA, (4)
// DCB=(LRECL=80,BLKSIZE=3120,RECFM=FB),
// SPACE=(3120,(1,1))
//*
//DEFCL EXEC PGM=IDCAMS (5)
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
DEFINE CLUSTER (
NAME (CAI.VSAMTEST) - (6)
VOLUMES (XXXXXX) -
TRACKS (1 0) - (7)
RECORDSIZE (80 80) - (8)
KEYS (10 00) - (9)
FREESPACE (10 10) -
SHR (2 3) -
REUSE - (10)
INDEXED -
) -
```

```

          DATA  (
                NAME          (CAI.VSAMTEST.DATA) - (6)
                CISZ          (8192) -
                ) -
          INDEX  (
                NAME          (CAI.VSAMTEST.INDEX) - (6)
                CISZ          (2048) -
                )
//*
//REPRO    EXEC PGM=IDCAMS
//SYSPRINT DD  SYSOUT=A
//SYSIN    DD  *
          REPRO INFILE(INFILE) ODS(CAI.VSAMTEST)          (11)
//INFILE   DD  *
0000000000          (12)
0000000001
0000000002
(etc..)

```

Footnotes:

- (1) Provide a valid job statement.
- (2) Allocate a work file.
- (3) Provide a valid dsname for work file.
- (4) Provide a valid volser and unit name.
- (5) Allocate and initialize VSAM test file.
- (6) Provide a valid dsname and volser.
- (7) Space allocation.
- (8) Eighty-byte records.
- (9) The key field is ten bytes long and starts at offset +0.
- (10) Specify REUSE if you wish to perform other LDMAMS functions such as restores or compress.
- (11) Initialize the VSAMTEST file.
- (12) Provide several initialization records, making sure there are no duplicate keys and that they are in sequence.

If you choose to back up a pre-existing data set, you can skip most of this step.

2. Start CA-L-Serv.

Verify that your startup deck contains an ATTACH FILESERVER statement and start CA-L-Serv. You can issue the following command to verify that the file server has successfully initialized:

```
DISPLAY TASK(FILESERVER) ALL
```

3. Place the VSAM test file under the management of the File Server.

To place your test VSAM data set under the management of CA-L-Serv, issue the following command from a z/OS console:

```
ADDFILE dname test.file.dsname
```

4. Tailor the HJ35IVF2 JCL to the requirements of your site.

Customize the following JCL to meet the requirements of your data center:

```
//HJ35IVF2 JOB (JOBACCNT) (1)
//MAMS0000 EXEC PGM=LDMAMS
//STEPLIB DD DISP=SHR,DSN=CAI.CCCSLOAD (2)
//BACKUP DD DISP=SHR,DSN=VSAMTEST.BACKUP (3)
//SSN$xxxx DD DUMMY (4)
//SYSPRINT DD SYSOUT=XA
//SYSIN DD *
REPRO INFILE(VSAMTEST) OUTFILE(BACKUP) (5)
```

Footnotes:

- (1) Provide a valid job statement.
- (2) Change to the CA-L-Serv target library.
- (3) Indicate the dsname of your test sequential data set.
- (4) Replace xxxx with the z/OS subsystem name you specified in your CA-L-Serv start procedure.
- (5) The syntax is similar to the IBM IDCAMS statement.

Note: Do not allocate the VSAM file in the LDMAMS job step. This is unnecessary and would cause the job to fail.

5. Submit job HJ35IVF2 and review the SYSPRINT data set.

You should see the following messages:

```
REPRO INFILE(VSAMTEST) OUTFILE(BACKUP)
```

```
LDM0810I nn records copied from VSAMTEST to BACKUP - REPRO
operation complete
```

Chapter 13: Other Configurations

After installing and deploying CA Common Services for z/OS, there may be some additional post-deployment tasks to perform before you begin using CA Common Services for z/OS.

Note: Use your deployed data sets when performing these tasks.

This section contains the following topics:

[CAECIS CA EXAMINE Configuration Tasks](#) (see page 237)

[CAISDI Configuration Tasks](#) (see page 239)

[CAICRS Easytrieve Service Configuration Tasks](#) (see page 239)

[CAICRS References](#) (see page 240)

[Earl Service Configuration Task](#) (see page 241)

[CA MSM Common Services Configuration](#) (see page 241)

[SRAM Usermod](#) (see page 242)

[Unicenter Service Desk Installation Configuration](#) (see page 243)

[Viewpoint Configuration](#) (see page 243)

CAECIS CA EXAMINE Configuration Tasks

The CA Common Inventory Services (CAECIS) program, CAISERVX, is used to gather basic environmental diagnostic and product information that can be useful to CA support personnel when responding to a product question or problem. Running this utility produces valuable information about your executing environment. This can help the CA support technician more quickly focus on the specific problem.

Information reported by the CAISERVX program provides a general snapshot of your executing environment, including:

- Operating system release
- Job entry subsystem (JES) information
- System Residence (SYSRES) information
- IPL-related information including:
 - Time/date of system IPL
 - CPU model/serial number(s)
 - IPL LOADPARM value
 - Architecture mode

- CAIRIM-related information, including:
 - Products initialized using CAIRIM
 - CAIRIM-installed SMF intercepts
 - CAIRIM-installed subsystem names
- CAIENF started task status
- System Link library (LINKLIST) data sets in use
- Link Pack Area library (LPA) data sets in use
- APF-authorized libraries in use
- Inventory information of installed CA mainframe management solutions

Utilize CAECIS

CAECIS is installed when you install CA Common Services.

To utilize CAECIS

1. Identify the specific z/OS system experiencing the problem with your CA Technologies product. The batch job to execute CAISERVX will need to be run on this system.
2. Use the CAISERVX execution JCL found in *YourdeployHLQ.CAW0JCL*.
3. Copy the JOBCARD member found in SAMPJCL at the beginning of the member created in the previous step.
4. Modify the JOB statement as appropriate to meet installation requirements. Adjust the TIME and CLASS values as appropriate. CAISERVX will process all system linklist data sets, so ensure that the JOB statement parameters accommodate this.
5. Modify the JCLLIB statement as appropriate to reference the CAW0PROC data sets created during your CA Common Services deployment.
6. Ensure that your z/OS user ID has the appropriate security authority to:
 - Use z/OS Time Sharing Option (TSO) services.
 - Read all system linklist (LNKLSTxx) and link pack area (LPA) libraries.
 - Submit the job; a return code of zero is expected.
7. Save the output and supply to CA Support as necessary.

As distributed, the CAISERVX procedure will write the utility output to the CAECIS DD statement, by default, and allocate it to a SYSOUT data set. If desired, you can alter the CAISERVX procedure to direct the utility output to a physical data set. Read the instructions within the CAISERVX procedure in CAW0PROC.

CAISDI Configuration Tasks

Implementing CAISDI gives you access to the three new components; soap, med and els.

To implement the CAISDI tasks

1. Configure TCP/IP on your z/OS system.
2. Install CA Service Desk on a server that can be accessed through the network from your z/OS system.
3. Configure CAICCI on your z/OS system if you have not already done so.
4. Configure the CAISDI components for your environment.

Note: For information about configuring CAISDI/soap, CAISDI/med, and CAISDI/els, see the *CA Service Desk Integration Guide*.

5. Configure the CA Technologies products that will be using the CAISDI interface.

CAICRS Easytrieve Service Configuration Tasks

After installing CA Common Services for z/OS, configuration tasks for Easytrieve might be needed for your installation.

Link Edit the Easytrieve IDMS Interface Module

This step is required for the Easytrieve Service with CA Common Services for z/OS only if you have IDMS installed.

Other CA products that use the Easytrieve Service might require this.

CAW0JCL member EZTIDMS link edits various IDMS routines into a module required for IDMS access by Easytrieve.

To link edit the Easytrieve IDMS interface module

- Modify the sample JCL to conform to the standards of your data center and the CA Common Services for z/OS installation worksheet.

Compile and Link Edit the CA Datacom User Requirements Table (URT)

This step is required for the Easytrieve Service only if a CA product distributes an Easytrieve report that uses CA Datacom. If that is the case, instructions are provided with that product regarding if and how to run this step.

CAWOJCL member EZTDCOM creates the URTs which support CA Datacom application programming requirements. Each URT is linked with a copy of EZCSDRVR, creating a new module with the name of urtname (user defined).

Assemble and Link Edit the Easytrieve Options Table Module

This step is required for the Easytrieve Service only if a CA product distributes an Easytrieve report that requires specific Easytrieve options settings. If that is the case, instructions are provided with that product regarding what those settings should be.

CAWOJCL member EZTOPTB updates the Easytrieve Options Table settings.

To assemble and link edit the Easytrieve options table module

- Modify the sample JCL to conform to the standards of your data center and the CA Common Services for z/OS installation worksheet, then change the option setting as necessary.

Compile and Link Edit the Extended Reporting Options Module

This step is required for the Easytrieve Service only if a CA product distributes an Easytrieve report that uses the Extended Reporting feature of Easytrieve. If that is the case, instructions are provided with that product regarding if and how to run this step.

CAWOJCL member EZTXRPT compiles and links the Extended Reporting module. The Extended Reporting Module defines the types of printers and the font codes that are supported by Easytrieve.

CAICRS References

For more information about how to interface CA SYSVIEW with the Easytrieve Common Service component, see the *CA SYSVIEW Performance Management User Guide*.

For more information about how to interface CA MIM with the Easytrieve Common Service component, see the *CA MIM Resource Sharing for z/OS Release Notes*.

For more information about how to interface CA NSM CA JARS with the Easytrieve Common Service component, see the *CA JARS Resource Accounting User Guide*.

Earl Service Configuration Task

The CA Earl Service has an optional configuration task.

Modify the default EARLOPT option settings by following the instructions in CCCSJCL member AXEI0040. This member distributes USERMOD UXE6101, which updates the Earl option's module EARLOPT under SMP/E control.

Note: For more information about the Earl Service default options, see the *CA Earl Systems Programmer Guide*.

Important! Be sure to retain a copy of this USERMOD to save your customized option settings.

Important! Use care when changing the defaults. The supplied defaults were chosen to help you derive the most benefit from the Earl Service. Changing these defaults may cause undesirable results at execution time.

Verify Earl Service Installation

To verify that Earl Service is installed correctly, modify CCCSJCL member AXEI0050 according to comments found in the JCL and Submit.

CA MSM Common Services Configuration

To configure CA MSM Common Services, follow these steps:

1. Define and format the CA MSM Common Services zFS aggregate. Edit and submit CAWOJCL member ETNI0100.
2. Create the mount point and mount the zFS file. Edit and submit CAWOJCL member ETNI0200
3. Update your BPXPARM member in SYS1.PARMLIB to include the new MOUNT point.
4. See the *CA Mainframe Software Manager Release Notes* and the *CA Mainframe Software Manager Administration Guide* for any additional configuration steps and component information.

SRAM Usermod

SRAM uses four-character years in dates. If the data to be sorted includes two-character years, dates after the year 2000 may be sorted before some dates in the 1900's. You can use CCCSJCL member ASRIOPTN to solve this problem.

USERMOD(ASR0001) is available to customize SRAM to handle 2-digit year sort key types. The following lists the key types:

Key	Type	Size
Y2C	Character Year	2 Bytes
Y2Z	Zoned Year	2 Bytes
Y2P	Packed Year	2 Bytes
Y2S	Character Year	2 Bytes
Y2D	Decimal Year	1 Byte
Y2B	Binary Year	1 Byte

The usermod defines the century value attached to the 2-digit year based on the generated Y2K windowing rules.

Either a fixed or a sliding Y2K window may be defined. In the SRAMCNFG member of the CCCSOPTN data set, the CAISRAM macro is invoked with the keyword parameter Y2PAST=. A fixed window is defined by specifying a 4-digit year. A sliding window is defined by specifying a 2-digit year.

```
CAISRAM Y2PAST=1967 fixed
```

```
CAISRAM Y2PAST=88 sliding
```

In the fixed window mode, dates greater than or equal to the 2-digit year are converted to the specified century and dates less than the 2-digit year are converted to the following century.

In the sliding window mode the dates are converted relative to the current date returned from the system by the TIME macro.

An assembled SRAMCNFG is distributed with a default fixed format value of Y2PAST=1967. This means a 2-digit date, $xx < 67$ is converted to 20xx and $xx \geq 67$ is converted to 19xx.

If the provided default does not fit your installation's needs modify the Y2PAST value and submit this job to receive, apply and accept this usermod.

Unicenter Service Desk Installation Configuration

To complete the Unicenter Service Desk Installation, submit CAW0JCL member SD10ALC to create the Event Library, CAI.CAIEVENT, for the Unicenter Service Desk Interface/Event Library Support (CAISDI/els).

The Event Library is the repository for all Product Control and Event Control members. The control members are furnished by the CA products that will use this interface. Those members are typically copied into the Event Library as an installation or Configuration step for those products. The CAISDI/els component can manage multiple Event Libraries, so any given product may provide its own Event Library. The CAISDI/els component does not place any members of its own into the Event Library.

Viewpoint Configuration

To complete the Viewpoint Installation, submit CCCSJCL member DU4I0010 to update the Viewpoint profile library after you have made any necessary additions and changes to the member. The DU4I0010 member can be shared with other CA products and additional parameters may be added to it.

Before running this step, make sure that no other products are already using the Viewpoint profile data set or this step may cause undesirable results.

Note: For users of Katakana terminals who need all uppercase characters, edit member CACCENV and add KATAKANA=UPPER. The default is mixed case.

Chapter 14: Install CA Datacom/AD

After installing and performing the configuration tasks for CA Common Services for z/OS components, you can optionally install CA Datacom/AD.

The installation of CA Datacom/AD requires the installation of certain CA Common Services for z/OS components. CA Common Services is shipped in 4 bundles or PAX files. You should install all components bundled in the BASE PAX file which contains all the DATACOM/AD requirements except for CA-C Runtime which is found in the LEGACY PAX file. If you wish to install Datacom/AD and you have not installed all the required CA Common Services components, please do so before proceeding to the CA Datacom/AD installation.

- Components CAIRIM, CAICCI, CAIENF, and CAISSF are required. They are installed into the CAWOLINK and CAWLOAD data sets.
- Component CA-C Runtime is required for CA Dataquery. It is installed into the CCCSLINK data set.

See the *CA Datacom/AD Installation and Maintenance Guide* for installation instructions concerning the CA Datacom/AD release shipped with this version of CA Common Services.

After performing the installation, you should return to this chapter to customize CAIENF and Event Management.

Note: CA Datacom/AD r12.0 must have PTF RO18150 applied in order to function correctly with CAIENF.

For new and existing customers of CA Datacom/AD, each system running CAIENF requires a unique MUF used only for CAIENF and Event Management data handling.

The CAIENF event data is unique to each system. Sharing a CA Datacom/AD MUF with other CA products is not practical for the following reasons:

- Other CA products generally share data across systems using a cross system MUF.
- Maintenance and backup might be a problem.

We recommend using the ENFIMUF setup for running a CA Datacom/AD MUF within the CAIENF address space discussed later in this chapter.

This section contains the following topics:

[CA LMP](#) (see page 246)

[CA Datacom/AD Multi-User Deployment](#) (see page 247)

[Customize CA Datacom/AD for CAIENF](#) (see page 249)

[Customize CA Datacom/AD for Event Management](#) (see page 254)

CA LMP

When CA Datacom/AD is installed, a library with the low-level qualifier of CAAXSAMP is created. Within that data set is member DBDATIN2, which is used at CA Datacom MUF startup.

Change the statement in member DBDATIN2 that reads

```
DATAKOM    AD
```

to

```
DATAKOM    MSM
```

This change causes the CA Datacom/AD MUF LMP check to be bypassed during startup. Some CA Datacom/AD functionality will be lost, but that will not affect ENF and Event Management. If the CAAXSAMP data set being used by ENF or Event Management is being shared with other products that use CA Datacom/AD, be sure to make a copy of this data set first before making the statement update. In such a case, have ENF or Event Management use its own updated CAAXSAMP data set.

CA Datacom/AD Multi-User Deployment

After CA Datacom/AD has been successfully installed on one LPAR, you can establish fully operational CA Datacom/AD environments on any number of additional LPAR images.

If you used CA MSM to install Datacom/AD, you may be able to deploy Datacom/AD using CA MSM or you can use the IBM ADRDSSU utility to backup all needed data sets from the initially installed LPAR and restore them on a different LPAR. This procedure has eight steps with one JCL member associated with each step. Each JCL member contains a description of its function as well as specific instructions on the changes to be made prior to submitting it for execution.

The source LPAR is the LPAR where the initial CA Datacom/AD new installation was performed. The target LPAR is the LPAR where an additional CA Datacom/AD multi-user environment is to be established.

Each MUF on each LPAR should have a unique MUF name. The LPAR system name can be used in the MUF name to make it easier to identify the origin of CA Datacom/AD messages and reports generated within a SYSPLEX.

The JCL necessary to execute this deployment procedure is found in member DEPLOY in the CAW0JCL library. Running this job creates a new deployment JCL library containing all the needed members.

Important! After creating the deployment JCL library, member AXDEPIPJ contains an IPOUPDTE process that can be used to perform all necessary edits to the CA Datacom/AD Deployment members described below, and must be run to perform the needed customization. You should copy this member to another library then customize and submit it from that library to keep from losing changes when the deployment JCL library is updated.

To establish a fully operational CA Datacom/AD Multi-User Facility (MUF) on a target LPAR

1. Edit member DEPLOY in CAW0JCL. Change the JOB card to match your installation standards. Modify the SYSUT2 card in the IEBUPDTE step, changing the DSN from DEPLOY.JCL to a name that matches the SRC.DATACOM high level qualifier. The low order qualifier should be DEPLJCL to avoid having to make significant changes to the rest of the jobs in the process. Modify the UNIT and VOL=SER to match your installation standards and submit the job.
2. Copy member AXDEPIPJ from the deployment JCL library just created into another library to preserve your changes. Modify each of the parameters after the SYSIN card except the last, \$/<./< . | Change the value found within the angle brackets (<<) to match the value you specified in the deployment work sheet. Submit this job.

In this example, you would change the second occurrence of SRC.SMPE.DATACOM
 SRC . SMPE . DATACOM<SRC . SMPE . DATACOM<

Important! Do not delete or update the last entry \$/./<

3. Use AXDEP01 to backup all required CA Datacom/AD data sets from the Source LPAR.
4. Use AXDEP02 to restore all required CA Datacom/AD data sets to the target LPAR. The data set names used on the target LPAR can be the same or different from those on the source LPAR.
5. Use AXDEP03 to add the PROCS used by CA Datacom/AD customized to meet target LPAR needs.

This step creates the DBDATIN1 MUF startup option SYSIN member. The DBDATIN1 member has an entry called MUF that contains a MUFNAME parameter. The value used for MUFNAME should be different from any currently deployed or yet to be deployed MUF.

6. Use AXDEP04 to assemble the DBSYSID macro and link edit the DBSIDPR module to be installed by CAIRIM on the target LPAR. The DBSYSID macro contains a MUF_TARGET_LIST parameter. The value used must be the same as the value used for MUFNAME in step 5.

APF authorize the following target system data sets before running this job:

- The CA Common Services CAW0LOAD
 - The CA Datacom/AD CAAXLOAD
 - The CA Datacom/AD CUSLIB
7. Use AXDEP05 to initialize and load the CA Datacom/AD CXX data set for use on the target LPAR. The initialization process contains a MUFNAME parameter. The value used must be the same as the value used in steps 5 and 6.
 8. Use AXDEP06 to execute a PROC to start the CA Datacom/AD MUF on the target LPAR.
 9. Use AXDEP07 to change the internal data set references to the target LPAR names. These internal data set references are contained in the CXX data sets that were initialized and loaded in step 7.
 10. Use AXDEP08 to execute a PROC to stop the CA Datacom/AD MUF on the target LPAR.

Customize CA Datacom/AD for CAIENF

After installing CA Datacom/AD or deploying CA Datacom/AD on another LPAR image, you can optionally customize CA Datacom/AD for CAIENF.

If you want CAIENF to record events, you must have installed the version of CA Datacom/AD shipped with this version of CA Common Services and you must perform the steps in this procedure.

After completing the CA Datacom/AD installation, there are two CA Datacom/AD load libraries, CAAXLOAD and CUSLIB that are used to customize CA Datacom/AD for CAIENF and must be APF authorized.

CA Datacom/AD MUF Considerations

Important! Before you perform any CA Datacom/AD customization procedures for CAIENF, consider the following:

- A CA Datacom/AD Multi-User Facility (MUF) must be running on the system where the JCL associated with the procedure will execute.
- A CA Datacom/AD MUF can execute in its own address space or under the CAIENF address space.
- To customize CA Datacom/AD for CAIENF or resolve CA Datacom/AD for CAIENF customization issues, the CA Datacom/AD MUF must be running with its own address space and CAIENF must be down or started in a separate address space from the CA Datacom/AD MUF with the control option NODB.
- Save your Datacom/AD MUF startup JCL even if you decide to use an ENF internal MUF (see ENFIMUF below). There will be database maintenance occasions when you need to bring up the MUF while ENF is down.

Customize an Existing CA Datacom/AD for CAIENF

Important! Before starting this procedure read the section titled, *CA Datacom/AD MUF Considerations*.

To customize an existing CA Datacom/AD for CAIENF

If you already installed the release of CA Datacom/AD being shipped with this version of CA Common Services for z/OS from a prior version of CAIENF, then you will need to import this release's version of the CAIENF plan into your existing CA Datacom/AD environment.

Important! Do not perform the following until you are ready to implement this release's version of CAIENF.

1. Shutdown older version of CAIENF.
2. If not already started, start DATACOM/AD external to CAIENF.
3. IMPORT the New CAIENF plan into DATACOM/AD by editing and submitting CAW0JCL member AW1IMPRT.
4. IPL the system.
5. Start the new release of CAIENF.

Customize a New CA Datacom/AD for CAIENF

To customize a new CA Datacom/AD for CAIENF

1. Modify and submit member, AW1ID001 to install the CAIENF database definitions into CA Datacom/AD and allocate the CAIENF database data sets.

- Specify CA Datacom/AD data set prefix
- Specify CAIENF database data set volume
- Specify the unit type for the volume specified
- Specify space for the CAIENF database index, IXX700

Approximate 3390 CYL Index space

$$A = (30 \times \text{\#total recorded events}) / 3036$$

$$B = A + (A \times .05) / 12$$

$$\text{Cyls} = (B / 15) + 1$$

- Specify space for the CAIENF database data area, ENF700

Approximate 3390 CYL Area space

$$\text{Cyls} = \text{\#total number of events} / 3600$$

Approximate 3380 CYL Area space

$$\text{Cyls} = \text{\#total number of events} / 3000$$

Note: If AW1ID001 does not complete successfully, see Resolve CA Datacom/AD for CAIENF Customization Issues.

If you are upgrading from CA Common Services r11, in order to obtain the total number of events count, your current running CA Common Services for z/OS ENF r11 can be used to help. Run the CAS9DB LIST DETAIL report shortly before your ARCHIVE (BACKUP) time, preferably the day after your three busiest days of the week. The LIST DETAIL report provides the total number of records that are currently recorded for each event type on the ENF r11 database. You can then simply add them up. The following is the CAS9DB LIST DETAIL JCL:

```
//CAS9DB EXEC PGM=CAS9DB,REGION=4M
//DBOUT DD SYSOUT=*
//DBIN DD *
LIST DB(*) DETAIL
/*
```

Make sure ENF r11 is up and running to use the above JCL as is.

2. Update the CAIENF procedure.

CAWOPROC contains three CAIENF procedures; ENF, ENFXMUF, and ENFIMUF. Select the procedure that applies to your site's requirements.

ENF - Use the JCL found in this procedure when you do not wish to record events or install CA Datacom/AD.

ENFXMUF - Use the JCL found in this procedure when you wish to record events. CA Datacom/AD is installed and the MUF is external (runs in its own address space) to ENF.

ENFIMUF - Use the JCL found in this procedure when you wish to record events. CA Datacom/AD is installed and the MUF is internal (runs under the ENF address space) to ENF.

For ENFXMUF and ENFIMUF:

- Set the parameter values for ADSHLQ and ADHLQ to the CA Datacom/AD CAAXLOAD and CUSLIB data set name prefixes.
- Update the ENF input parameters referenced by DD ENFPARMS to include control option statements RECORD(YES) and EVENT(event-name,RECORD). There should be an EVENT control option statement for each EVENT to be recorded.

The Control Options that pertain to the recording of events are:

```
NODB
RECORD(NO|YES)
DCM(dcm-name)
EVENT(event-name,RECORD) |
EVENT(event-name,NOREC)
```

- If the CA Datacom/AD MUF is to execute under the ENF address space, update the ENF input parameters referenced by DD ENFPARMS to include control option IMUF

Note: For more information on these control options, see the *Reference Guide* and the *Administration Guide*.

3. Start or Re-start ENF.

ENF dynamically creates EVENT tables to record events and ENF system tables to record miscellaneous supportive data.

The EVENT tables are created when ENF initializes with RECORD(YES) specified.

If RECORD(YES) is specified and the DATACOM/AD MUF is not available, ENF will shutdown.

Resolve CA Datacom/AD for CAIENF Customization Issues

There may be instances where problems are encountered customizing CA Datacom/AD for CAIENF. For example, a data set name or space allocation may be specified incorrectly or the CAIENF database installation CAW0JCL member AW1ID001 receives an error.

In many cases, the CAIENF database installation CAW0JCL member AW1ID001 can be resubmitted after resolving the issue that caused the error by editing the JCL to begin at the job step encountering the error.

However in some cases, it may be more desirable to delete a partially or completely installed CAIENF database.

To delete a partially or completely installed CAIENF database

1. Before starting this procedure, see *CA Datacom/AD MUF Considerations* in [Customize CA Datacom/AD for CAIENF](#) (see page 249).
2. Submit CAW0JCL member AW1AD001 to obtain a list of existing CAIENF database tables.

If no rows are found, proceed to step 4 to delete the CAIENF database.

3. Edit and execute CAW0JCL member CASQL004 to drop all CAIENF tables.

This step is only required if the listing for job AW1AD001 indicated rows were found.

EVENT tables are dynamically installed at CAIENF startup when the RECORD(YES) ENFPARM control option has been specified.

Important! Never drop an EVENT table while CAIENF is actively recording events. For more information, see *CA Datacom/AD MUF Considerations* in [Customize CA Datacom/AD for CAIENF](#) (see page 249).

Note: The DROP TABLE statement renders the table obsolete, which removes all versions and statuses of the table from the data dictionary databases, deletes the Directory definition, and deletes the data.

If CASQL004 returns an error, execute CAW0JCL member CADB001 to close all CAIENF tables then resubmit CASQL004.

Note: An error is returned if the database table information remained cached by the CA Datacom/AD address space.

4. Edit and submit CAW0JCL member CADB003 to delete the CAIENF database definitions from CA Datacom/AD.
 - Update the JCL SET statement for ADHLQ with the data set high level qualifier used during the CA Datacom/AD installation for CUSLIB.
 - Update the JCL SET statement for ADSHLQ with the data set high level qualifier used during the CA Datacom/AD installation for CAAXLOAD.

Important! Drop all the ENF tables before deleting the CAIENF database.

Note: If the CAIENF database was partially installed, one or more database components may not exist and CADB003 will indicate errors for the missing components. You may safely ignore such errors.

5. Edit and submit CAWOJCL member CADB004 to delete the CA Datacom/AD directory definitions for CAIENF.

This job should only be run when the step to define and initialize the CA Datacom/AD CAIENF database data sets found in CAWOJCL member AW1ID001 successfully initialized and updated the Datacom/AD CXX file with the CAIENF ENF0700 and IX0700 data set information.

- Update the JCL SET statement for ADHLQ with the data set high level qualifier used during the CA Datacom/AD installation for CUSLIB.
- Update the JCL SET statement for ADSHLQ with the data set high level qualifier used during the CA Datacom/AD installation for CAAXLOAD.

6. Edit and submit CAWOJCL member CADB005 to delete the CAIENF database data sets.

This job should only be run when the step to define and initialize the CA Datacom/AD CAIENF database data sets found in CAWOJCL member AW1ID001 successfully allocated the CAIENF ENF0700 and IXX0700 data sets.

- Update the JCL SET statement for ADHLQ with the data set high level qualifier used during the CA Datacom/AD installation for CUSLIB.

7. Re-install the CAIENF database using CAWOJCL member AW1ID001.

Customize CA Datacom/AD for Event Management

The following steps are optional for Event Management.

If you decide to use Calendars or Message Actions with Event Management, you must have CA Datacom/AD installed and perform these steps.

Calendars and Message Actions are typically not required for sites using CA OPS/MVS Event Management and Automation interfacing with Event Management, but may be helpful for sites that are not using CA OPS/MVS Event Management and Automation to process events.

After completing the CA Datacom/AD installation, you will have two CA Datacom/AD load libraries, CAAXLOAD, CUSLIB and a parameter library, CUSMAC. These libraries are required to complete the CA Datacom/AD setup for Event Management.

If you have a DATACOM/TR repository used for release 3.0 of Event Management, you may want to extract the table information from the old repository and load the information into the new DATACOM/AD repository. For information on the optional steps to extract and load your existing table information, see the latter portion of the following procedure.

To customize the CA Datacom/AD for Event Management

1. Update MUF DATAPOOL parameter.

Change the CA Datacom/AD startup and tuning parameter member for the MUF by altering the DATAPOOL buffers.

Depending upon how you are running the MUF, refer to the CAIENF or CA Datacom/AD MUF startup procedure JCL SYSIN DD statement to determine the data set and member name containing the startup and tuning parameters.

Change

```
DATAPOOL      8K,2000,16K,2      DATA BUFFER SIZE,# OF BUFFERS
```

to

```
DATAPOOL      12K,2000,16K,2     DATA BUFFER SIZE,# OF BUFFERS
```

2. Start or Recycle CA Datacom/AD.

Note: Before performing the following steps, the CA Datacom/AD MUF must be active with the previous changes in effect.

3. Create DB Definitions.

Modify and Submit CNSMJCL member D5IRTV01.

4. Verify Definitions and Initialize Database.

Modify and Submit CNSMJCL member D5IRTV02.

5. Define the SQL tables.

Modify and Submit CNSMJCL member D5IRTV03.

Note: If the D5IRTV jobs in steps 3, 4, and 5 do not complete successfully, see [Resolve CA Datacom/AD for Event Management Customization Issues](#) (see page 258).

6. (Optional) If you are a previous CA Datacom/TR user (from CA Common Services r11) and would like to migrate your CA Datacom/TR data to CA Datacom/AD, perform this step. In past releases, Event Management maintained message action records and calendars in the CA Datacom/TR database.
 - With EM 3.0 Datacom R9 active, produce a CA Datacom/AD utility report of the Event Management database using CNSMJCL member D5IDBUTL.
 - Using the Datacom R9 utility report, update CNSMJCL member D5IDBEXT with the three character TABLE NAME for each OCCURRENCE of the Event Management Table Names shown in the JCL member D5IDBEXT.

Example - Datacom utility report:

TABLE NAME - C27
OCCURRENCE - CADB-OPRA_CTL

Change JCL member D5IDBEXT:

```
EXTRACT AREA=EM0,DBID=1011,DDNAME=DDOCTL, TABLE=C27, CADB-OPRA-CTL BLKSIZE=10236
```

- Extract Datacom/TR data for migration to CA Datacom/AD.
Modify and Submit CNSMJCL Member D5IDBEXT.
- Load extracted Datacom/TR Data into CA Datacom/AD.
Modify and submit CNSMJCL member D5IDBLD to load the extracted data into CA Datacom/AD.
Restart CA Datacom/AD if currently started.

7. Confirm your Event Management Profile.

During the Common Services Installation step (Create the Event Management Profile) entries were made pertaining to CA Datacom/AD.

Ensure that the `/cai/nsmem/PROFILE` file is edited to specify `CA_OPR_ZOSDB=Y`.

This allows the usage of Calendars and Message Actions with Event Management. If you did not know the CA Datacom/AD data set names or data set high level qualifier at the time of the installation, you can edit the `/cai/nsmem/PROFILE` file directly with this information now. Refer back to the installation step for information on how to edit this file.

The STEPLIB environment variable in `/cai/nsmem/PROFILE` must point to the correct CA Datacom/AD libraries.

If you are migrating from a CA Datacom/TR or creating a new CA Datacom/AD database, make sure the STEPLIB variable points to the correct CAAXLOAD and CUSLIB data sets.

Once the `/cai/nsmem/PROFILE` file updates are complete, rerun CNSMJCL member D5I10065. This ensures that any information required for the use of the CA Datacom/AD databases is updated in the proper Event Management component scripts.

If you optionally updated the system `/etc/profile` file to have the EM environment variables set when a user logs on, you will have to rerun script `fwsetup` to reflect the CA Datacom/AD libraries in the STEPLIB variable. For more information, see section [Run the Event Management Post-Installation Script](#) (see page 159).

8. Start MUF.

The CA Datacom/AD MUF can run in its own address space or under the CAIENF address space.

If you are using Calendars or Message Actions, you should initialize the MUF before the Event Management components start. If the MUF is not initialized, expect startup error messages. The `caiopr` daemon starts without the MUF running, but the Calendar daemon does not.

9. Start Event Management Daemons.

You can access your new database by starting the Event Management Daemons using CNSMPROC member NSMEMSTR.

Clone Your CA Datacom/AD Database

To clone your CA Datacom/AD database on another system

1. Back up the Event Management CA Datacom/AD database you wish to clone using the CNSMJCL member D5IDBBAK.

Note: This job can run anytime after the CA Datacom/AD customization for Event Management has been completed to back up the database records added after the initialization.

2. Set up the CA Datacom/AD environment on the target system by performing the procedure To Customize the CA Datacom/AD for Event Management.
3. Use the CNSMJCL member D5IDBRST to restore the backup file created in step 1 into the new Event Management CA Datacom/AD database.

Central Databases on Multiple Systems

To use a central database on multiple systems, the environment variable `CAI_OPR_REMOTEDB=ccisysid` should be exported on each remote system. Add this export statement to the `/cai/nsmem/PROFILE` file on each remote system.

This causes Event Management code to send message record queries to the database engine on the `ccisysid` node and receive a response from that node. The multiple systems involved can be distributed systems running CA NSM 3.0. For example, Event Management running on z/OS could use a distributed Microsoft SQL server database as its message record repository.

Resolve CA Datacom/AD for Event Management Customization Issues

You might encounter problems customizing CA Datacom/AD for Event Management. For example, a data set name or space allocation might be specified incorrectly or the database installation CNSMJCL members D5IRTV0* might receive an error.

In many cases after resolving the error, the database installation CNSMJCL members D5IRTV0* that caused the error can be resubmitted after editing the JCL to begin at the job step that caused the error.

In some cases, you might need to delete a partially or completely installed Event Management database.

Important! Before starting this procedure, see *CA Datacom/AD MUF Considerations in Customize CA Datacom/AD for CAIENF* (see page 249).

To delete a partially or completely installed Event Management database, modify and submit in order the following CNSMJCL members:

- D5IDBU02
- D5IDBU04
- D5IDBU05
- D5IDBU06
- D5IDBU07

Appendix A: Third-Party Software Acknowledgements

This section contains the following topics:

[Apache Software Foundation](#) (see page 261)

Apache Software Foundation

This product includes software developed by the Apache Software Foundation, including Tomcat 6.0.29, CGLIB-NODEP 2.1.3, Commons Codec 1.3, Commons Collections 3.2.1, Commons Configuration 1.6, Commons DBCP 1.2.2, Commons HttpClient 3.1, Commons IO 1.4, Commons Language 2.4, Commons Logging 1.1.1, Commons Net 2.0, Commons Pool 1.3, Log4j 1.2.15, Xalan-J 2.1.7, XML Resolver, Google (including Google Web Toolkit 1.7.1 and GWT-Log 2.6.2), and the Spring Framework Project (<http://www.springframework.org>). The Apache software is distributed in accordance with the following license agreement:

Apache License
Version 2.0, January 2004
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of

this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
 - (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
 - (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
 - (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
 - (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify,

defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Index

A

- Access CA MSM Using the Web-Based Interface • 69
- ACEE CA-GSS security • 44
- Activate Changes • 152
- Activate the Changes • 174
- Activate Tracing • 155
- Additional Configuration Tasks for CAICCI • 133
- Agent Configuration Set Verification • 191
- Agent Security • 190
- Agent Technology • 22
 - description • 22
 - installing multiple systems • 106
 - post-installation tasks • 183, 190, 191, 192
 - pre-installation tasks • 39
 - system requirements • 38
 - TCP/IP requirements • 39
 - user-defined agents • 193
- Agent Technology and Event Management Post-Installation • 72
- Agent Technology Configuration • 183
- Agent Technology Post-Installation • 73
- Agent Technology Requirements • 38
- Allocate and Mount a File System • 85
- ALTNAME parameter, CA-VIEW support • 211
- Apache Software Foundation • 261
- Apache Tomcat Requirements • 67
- Apply Maintenance • 101
- APPMAP • 176
- Assemble and Link Edit the Easytrieve Options Table Module • 240
- Audience • 13
- Automate CCISSL • 142
- Automate CCISSLGW • 143

B

- backend Java server • 179
- BASE and OPTIONAL Target Libraries • 28
- Base Common Services • 17
- Berkeley Syslog Daemon
 - overview • 172
 - rerouting messages • 173
- browser interface • 180
- Build and Run the Example Agent (EXAGENT) • 192
- Build the aws_admin Store Files • 190

- Business Process View, description • 15
- Business Process Views • 15

C

- CA Common Services Deployment • 77
- CA Common Services for z/OS • 14
- CA Common Services Specific Post-Installation Requirement • 103
- CA Datacom/AD Multi-User Deployment • 247
- CA Global SubSystem Configuration • 197
- CA Health Checker Common Service • 18
- CA Health Checker Common Service Requirements • 64
- CA LMP • 246
- CA Master • 19
- CA MSM Common Services • 19
- CA MSM Common Services Configuration • 241
- CA MSM Common Services Requirements • 65
- CA Product DCM compatibility • 127
- CA TCPAccess Communications Server for z/OS Considerations • 157
- CA Technologies Product References • 3
- CA Workload Control Center • 158
- ca_calendar • 179
- CA_STARUNIX_SERVER • 153
- CA-C Runtime • 21
- CA-C Runtime Requirements • 39
- CA-C Runtime system requirements • 39
- CAECIS • 18
- CAECIS CA EXAMINE Configuration Tasks • 237
- CAECIS Requirements • 49
- CaemRts process • 180
- CA-GREXX • 20
- CA-GREXX Requirements • 40
- CAGSS
 - copying procs • 198
 - customizing initialization parameters • 204
 - defining subsystem IDs • 198
 - enqueue requirements • 199
 - installing IMOD editor • 199
 - installing ISEERVE Operator Control Panel • 202
 - logon facility • 216
 - memory requirements • 42
 - optional features • 214
 - preparing started task • 198

- starting • 202
- stopping • 202
- testing the installation • 202
- CA-GSS • 20
- CA-GSS (System Interfaces) Requirements • 41
- CA-GSS Memory Requirements • 42
- CAGSS User ID • 45
- CAI_OPR_DAEMON • 153
- CAICCI • 18
 - checking connections • 158
 - downloading • 146
 - implementation considerations • 131
 - installing on client • 146
 - local trace • 156
 - modules • 146
 - recycling • 158
 - remote machine • 148
 - Secured Socket Layer for r2.1 • 133
 - startup procedures • 174
 - SYSID • 150
 - timeout value • 175
 - transferring files from mainframe • 146
 - verifying your installation • 155
- CAICCI Configuration • 131
- CAICCI Requirements • 49
- CAICCI Spawn • 156
- CAICCI Tasks • 131
- CAICCI/PC • 157
- CAICCI/PC - Using a Workstation Product • 157
- CAICRS Easytrieve Service Configuration Tasks • 239
- CAICRS References • 240
- caidoc • 179
- CAIENF (Base) • 18
- CAIENF autocmds • 174
- CAIENF Configuration • 123
- CAIENF database • 155
- CAIENF Requirements • 50
- CAIENF system requirements • 50
- CAIENF/CICS • 19
- CAIENF/CICS Requirements • 52
- CAIENF/CICS SPAWN • 19
- CAIENF/CICS SPAWN Requirements • 53
- CAIENF/CICS SPAWN system requirements • 53
- CAIENF/CICS system requirements • 52
- CAIENF/DB2 • 19
- CAIENF/DB2 Requirements • 54
- CAIENF/USS • 20
- CAIENF/USS Configuration Tasks • 129
- CAIENF/USS Requirements • 55
- CAIENF/USS system requirements • 55
- caiopr • 174, 179
- CAIRIM • 17
- CAIRIM Configuration • 115
- CAIRIM Initialization Parameters • 115
- CAIRIM Requirements • 57
- CAISDI • 20
- CAISDI Configuration Tasks • 239
- CAISDI Requirements • 59
- CAISSF
 - for RACF and compatibles • 117
- caiusr directory • 153
- Calendars • 23
- CA-L-Serv • 21
 - eTrust CA ACF2 security • 222
 - eTrust CA Top Secret security • 221
 - LU 0 and LU 6.2 communication • 226
 - message member • 228
 - RACF security • 224
 - security enhancements • 219
 - SQL dictionary • 47
 - starting • 230
 - startup parameters • 226
 - startup procedure • 229
 - system requirements • 46
- CA-L-Serv Configuration Tasks • 219
- CA-L-Serv Requirements • 46
- CA-L-Serv SQL Dictionary • 47
- CAS9CSSF • 117
- CAS9DCM3 module • 155
- CAS9SAFC • 117
- CAS9SAFC/CAS9RACL for CICS TS • 117
- catrapd • 174, 179
- CAW0OPTN Member
 - BYSMTAB • 215
 - BYSVTAM • 216
 - GOALNET • 215
- CA-XPS • 20
- CA-XPS Requirements • 48
- CA-XPS system requirements • 48
- CCI connection initiation considerations • 157
- ccicntrl command • 152
- CCII command • 158
- ccii commands • 153
- CCIPARMS • 155
- ccirmtd.rc file • 153
- CCISL parameter options • 134
- CCITCP • 155, 157
- CCITCPGW • 155, 156, 157

CCITCPGW task • 153, 156
Central Databases on Multiple Systems • 258
Change the SAF Interval • 169
Clean Up the USS Directory • 100
Clone Your CA Datacom/AD Database • 258
communication server considerations • 157
Compile and Link Edit the CA Datacom User Requirements Table (URT) • 240
Compile and Link Edit the Extended Reporting Options Module • 240
Compile and Link in Batch Mode (z/OS) • 193
Compile and Link Online (USS) • 192
Complete the GSS Installation • 197
Component FMIDs • 25
Component Installation Requirements • 37
Comprehensive CA NSM Administration • 15
Comprehensive View of Storage Requirements • 33
configuration file • 177
Configuration Steps • 111
Configure and Start CAICCI • 132
Configure CAIENF JCL for finding CA product DCMs • 127
Configure CAIENF Parameter File • 126
Configure the UNIX System Services for Event Management • 163
Configure the Web Server • 163
Configuring Your Product • 111
Connect to the GUI • 180
connection initiation considerations • 157
Connection Initiation Considerations • 157
connection manager selections • 150
connection message • 153
console commands • 153
Contact CA Technologies • 5
Copy and Customize the Startup Procedure • 229
Copy CA-GSS Procedures to System PROCLIB • 198
Copy CCIP12 • 140
Copy CCIRTARM • 139
Copy CCISSL • 134
Copy CCISSLGW • 137
Copy Installation Files to z/OS Data Sets • 92
Copy the Product Pax Files into Your USS Directory • 86
Copy Your Agent Technology Installation • 107
Create a Product Directory from the Pax File • 91
Create an SAF Configuration File • 169
Create and Populate the HFS Key Database • 143
Current Status • 155
Customize a New CA Datacom/AD for CAIENF • 250

Customize an Existing CA Datacom/AD for CAIENF • 249
Customize CA Datacom/AD for CAIENF • 249
Customize CA Datacom/AD for Event Management • 254
Customize CA Jobtrac Job Management • 207
Customize CA SYSVIEW Performance Management • 210
Customize CA-GSS • 204
Customize CA-GSS for CA Insight Database Performance Monitor for DB2 for z/OS • 204
Customize CA-GSS for CA MIM • 207
Customize CA-GSS for CA OPS/MVS Event Management and Automation • 209
Customize CA-GSS for CA View • 211
Customize CA-GSS for DB2 • 212
Customize CA-GSS for IDCAMS • 213
Customize CAISSF for RACF or RACF-Compatible Products • 117
Customize emstart and emstop Scripts • 174
Customize the CAIENF Procedures • 124
Customize the ENFSNMPM Procedure • 129
customizing the emstart and emstop scripts • 174

D

data directory • 176
DB2, customizing CA-GSS • 212
DDDEFs • 181
Define a New Object to VLF • 56
Define CA-L-Serv to VTAM • 226
Define GoalNet to VTAM • 216
Define Subsystem IDs • 198
Define the Logon Facility • 217
Defining GoalNet • 214
Deploy Products • 104
Deploying Agent Technology on Multiple Systems • 106
Deploying Event Management on Multiple Systems • 109
Deploying USS file systems • 104
Download Using Batch JCL • 87

E

Earl Service • 21
Earl Service Configuration Task • 241
Earl Service Requirements • 61
Easytrieve Service • 20
Easytrieve Service Requirements • 61

edit CCI fields • 150
Edit the config file
 /cai/agent/services/config/aws_orb/quick.cfg • 187
 /cai/agent/services/config/aws_sadmin/aws_sadmin.cfg • 187
 /cai/agent/services/config/aws_snmp/aws_snmp.cfg • 188
Edit the profile file
 /cai/agent/agentworks.profile • 184
Edit the script file
 /cai/agent/services/tools/install_mibs • 186
Emserver • 180
EMSRVC_ROUTER_U • 176
emstart file • 174
emstart script • 174
emstop script • 174
Enable catrapd to Receive SNMP Traps • 170
Enable Store and Forward for Another Task • 169
End-to-End Management • 14
ENFPARMS • 155
Enterprise Management • 176
Enterprise Management icon • 176
ESD Product Download Window • 81
eTrust CA ACF2 security for CA-L-Serv • 222
eTrust CA Top Secret security for CA-L-Serv • 221
Event Management • 22
Event Management Post-Installation • 74
Event Management Configuration • 159
Event Management Maintenance Considerations • 181
Event Management Requirements • 63
Event Management Utilities Requirements • 64
Example
 CAtoMainframe.txt, JCL • 89
 FTP Commands • 90
Execute the agentworks.profile • 186
exit, OPSMVS • 171
External HOLDDATA • 103

F

F CCITCP command • 157
F CCITCPGW command • 156

G

GoalNet • 214
GOALNET Parameter • 214

H

HOLDDATA • 102
How CA-GSS Chooses a User ID for an IMOD • 45
How the Installation Process Works • 23
How the Pax-Enhanced ESD Download Works • 81
How the Post-Configuration Process Works for CA-GSS • 198
How the Update Tasks are accomplished • 220
How to Acquire a Product • 70
How to Configure Event Management GUI Tasks • 162
How to Configure Optional Event Management Tasks • 167
How to Deploy a Product • 76
How to Install a Product • 71
How to Install a Product Using Pax Enhanced ESD Files • 79
How to Install Products Using Native SMP/E JCL • 94
How to Maintain Existing Products • 76
How to Use CA MSM Scenarios • 70
httpd.conf file • 177

I

IDCAMS load module (for IDCAMS) • 213
IDCAMS, customizing CA-GSS • 213
ILOG Files • 216
IMOD editor • 201
IMOD Editor Problems • 201
IMOD User IDs • 45
Implement Security with CA ACF2 • 222
Implement Security with CA Top Secret • 221
Implement Security with RACF • 224
Initialize the Java Server • 166
Install CA Datacom/AD • 245
Install CAS9RACL • 118
Install the CA-GSS/ISERVE Operator Control Panel • 202
Install the IMOD Editor • 199
Install the OPSMVS Exit • 171
Installing from Pax Files Using the SAMPJCL Method • 79
Installing Your Product Using CA MSM • 69
Introduction • 13
ISERVE CA-GSS requirements • 43
ISERVE Memory • 43
ISET Upgrades • 217
ISETs, upgrading • 217

J

Java GUI • 175

L

Legacy Common Services • 21
LEGACY target libraries • 30
Limiting SAF Eligibility • 168
Link Edit the Easytrieve IDMS Interface Module • 239
Load CAICCI on the Client Platform • 146
Load Library Considerations • 191
Local CAICCI • 156
local CAICCI tracing • 156
Logon Facility • 216
logonsrvr • 180

M

machine name • 150
Mainframe CA NSM Common Services • 22
maintenance considerations • 181
MFNSM Target Libraries • 31
Modify and Submit the CAS9CSSF Sample JCL • 119
Modify RACF or the RACF-Compatible Product • 119
modules in CAICCI • 146
Multilayered Architecture • 15
multiple application support • 177
Multiple system install • 106

N

newdaylog • 179
nodelist file • 148
nodelist.sample file • 176
Non-SMP/E Product Specific Data Sets • 32
NSMJSERV CAW0PROC member • 180
NSMWEBSV CAW0PROC member • 179

O

oprsafd • 179
OPSMVS exit • 171
Optional Common Services • 19
Optional Features • 214
Other Configurations • 237

P

Peer-to-Peer Communication with Remote
Computers • 148
persistentsrvtimeout registry setting • 175

Place the CAISSF Routines in the Common Service
Area (CSA) • 120
platform • 150
port numbers • 150, 153, 177
Prepare for Component Tracing • 128, 156
Prepare the SMP/E Environment for SAMPJCL
Installation • 95
Prepare to Install Agent Technology • 39
Preparing for Installation • 25
Primary CA-GSS Memory • 43
protocol statement • 153

R

RACF security for CA-L-Serv • 224
read-only HFS file • 181
read-write HFS file • 181
receiver, EMSRVC_ROUTER_U • 176
Recompile under TSO • 204
recycle CAICCI • 158
recycling CCI remote components • 152
remote machines • 148
Reroute Messages to a Remote Host • 173
Rerun D5II0065 for GUI Tasks on the Deployed
System • 159
Resolve CA Datacom/AD for CAIENF Customization
Issues • 252
Resolve CA Datacom/AD for Event Management
Customization Issues • 258
Resource Consumption • 44
Review and Adjust the Event Management PROFILE
• 159
rmtcntrl status • 158
Run the Event Management Configuration Script •
159
Run the Installation Jobs for a SAMPJCL Installation •
99

S

Sample Job to Execute the Pax Command
(Unpackage.txt) • 92
Sample LOGMODE Table • 215
Sample syslogd Configuration File • 172
scripts, emstart and emstop • 174
Secured Socket Layer Protocol • 133
Security • 217
Security Definitions for Event Management • 165
security environment • 155
Security Requirements • 27, 176

- security system for CA-L-Serv • 219
- Set Up the Berkeley syslog daemon • 172
- SMP/E environment • 181
- Software Requirements • 27
- Software Services • 17
- SPNDEBUG DD statement • 156
- SPNPARM member • 156
- SQL dictionary, CA-L-Serv • 47
- SRAM Service • 21
- SRAM Service Requirements • 65
- SRAM system requirements • 65
- SRAM Usermod • 242
- SRVMAINT program • 204, 216
- stardaeon • 174, 179
- Start Agent Technology • 191
- Start and Stop CCISSL from the Console • 142
- Start and Stop CCISSLGW • 143
- Start and Stop the Event Management Processes • 171
- Start CAIENF • 128
- Start CAIRIM • 121
- Start CA-L-Serv • 230
- Start CCISSL • 141
- Start the Java Server • 180
- startup procedures • 174
- Startup Procedures • 174
- status • 155
- STEPLIB environment variable • 174
- Storage Requirements • 28
- Store and Forward • 168
- Symbolics • 124
- SYSID • 150
- syslogd configuration file • 172
- SYSPRINT • 153
- System HOLDDATA • 102
- System Level Memory • 42
- System Security • 44

T

- Tailor Startup Parameters • 226
- Tailor the config file
 - /cai/agent/services/config/awsservices/awsservice.s.cfg • 188
- Tailor the ENVFILE from the CNSMOPTV • 189
- Tailor the Profile, Script, and Configuration Files in the zFS System • 183
- Target Libraries • 28
- Test the Installation • 202

- The CAISSF Installation Process • 120
- Third-Party Software Acknowledgements • 261
- timeout GUI settings • 175
- Timeout Settings • 175
- TNGEMSTR sampjcl member • 174, 179
- Tomcat • 21
- tracing • 155
- TRCPRINT DD statement • 156
- Troubleshoot
 - Communications Server IVP is Not Running Successfully • 233
- troubleshooting • 155
- Troubleshooting • 155

U

- UEJM tracing example • 158
- UID(0) • 174
- Unicenter CA-Insight for DB2, customizing CA-GSS • 204
- Unicenter CA-Jobtrac, customizing CA-GSS • 207
- Unicenter CA-OPS/MVS integration • 174
- Unicenter CASYSVIEW, customizing CA-GSS • 210
- Unicenter CA-View, customizing CA-GSS • 211
- Unicenter Service Desk HTML rendering task • 59
- Unicenter Service Desk Installation Configuration • 243
- Unicenter TCPaccess communication server considerations • 157
- Update External Security for CA-L-Serv • 219
- Update the Message Table • 228
- Upload Files to Mainframe through a PC • 90
- Usage Notes • 220
- Use CA NSM • 150
- User IDs • 44
- user-defined agents • 193
- USS Environment Setup • 84
- Utilize CAECIS • 238
- Utilize SSL Communication Links • 133

V

- Verify Agent Technology Installation • 194
- Verify Changes • 153
- Verify Earl Service Installation • 241
- Verify that Processes are Running • 179
- Verify the Communications Server Installation • 230
- Verify the File Server Installation • 233
- Verify the GUI Interface Servers are Active • 179
- Verify the TCP/IP Network Configuration • 189

Verify Your Installation • 155, 179
VIEW parameter, CA-VIEW support • 211
Viewpoint • 21
Viewpoint Configuration • 243
ViewPoint Requirements • 66
ViewPoint system requirements • 66
Virtual Storage Requirements • 47
VTAM, defining CA-L-Serv to • 226

W

w2startup.batch file • 175
W2Tree • 180
web server configuration • 177
Web Server Configuration • 177
welcome page • 180
Who Needs to Update? • 219

X

XCF Communications Considerations • 46

Z

z/OS Requirements • 47