

CA Common Services™ for z/OS and OS/390

Getting Started



PRINTED ON
RECYCLED PAPER



Computer Associates™

MAN04133527E

This documentation and related computer software program (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by Computer Associates International, Inc. ("CA") at any time.

This documentation may not be copied, transferred, reproduced, disclosed or duplicated, in whole or in part, without the prior written consent of CA. This documentation is proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of this documentation for their own internal use, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the confidentiality provisions of the license for the software are permitted to have access to such copies.

This right to print copies is limited to the period during which the license for the product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to return to CA the reproduced copies or to certify to CA that same have been 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 the end user or any third party for any loss or damage, direct or indirect, from the use of this documentation, including without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised of such loss or damage.

The use of any product referenced in this documentation and this documentation is governed by the end user's applicable license agreement.

The manufacturer of this documentation is Computer Associates International, Inc.

Provided with "Restricted Rights" as set forth in 48 C.F.R. Section 12.212, 48 C.F.R. Sections 52.227-19(c)(1) and (2) or DFARS Section 252.227-7013(c)(1)(ii) or applicable successor provisions.

© 2002 Computer Associates International, Inc. (CA)

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.



Contents

Chapter 1: Introducing CA Common Services (CCS) for z/OS and OS/390

Overview	1-1
Why Common Services?	1-2
Changing Role of z/OS	1-2
The CCS for z/OS and OS/390 Solution	1-3
End-to-End Management	1-4
Business Process Views	1-5
Comprehensive Unicenter Administration	1-5
Multi-layered Architecture	1-6
Visualization Services	1-6
Services Provided by CCS for z/OS and OS/390	1-11
Getting Started with CCS for z/OS and OS/390	1-14
Getting Help	1-15
Documentation Set	1-15
What Happened to...?	1-17

Chapter 2: System Requirements

Installation Overview	2-1
Hardware and Software Requirements	2-2
Target Libraries	2-2
Comprehensive View of Storage Requirements	2-5
Event Management Requirements	2-8

WorldView Requirements	2-9
CAIRIM/CAISSF Requirements	2-10
CAIENF Requirements	2-12
CAIENF Utilities Requirements	2-16
CAIENF/CICS Requirements	2-17
CAIENF/DB2 Requirements	2-18
CAIENF/CICS SPAWN Requirements	2-19
CAIENF/USS Requirements	2-20
CAICCI Requirements	2-22
CAIVPE Requirements	2-23
CAIVPE Installation Considerations	2-24
CA-MFLINK Requirements	2-24
EARL Service Requirements	2-25
SRAM Service Requirements	2-26
CA-C Runtime Requirements	2-26
ViewPoint Requirements	2-27
CA PROFILE Requirements	2-29
Agent Technology Requirements	2-29
CA-Datacom/TR Requirements	2-31
CA-L-Serv Requirements	2-34
CA-GSS Requirements (System Interfaces).....	2-37
CA-XPS Requirements	2-45
Installation Dependencies	2-46

Chapter 3: Installing CCS for z/OS and OS/390

Installation Steps	3-1
Step 1. Visit the Support Page	3-2
Step 2. Load Installation Sample JCL Library	3-2
Step 3. Download BookManager Files	3-3
Step 4. Download PDF Files	3-3
Step 5. Review System Requirements	3-3
Step 6. Complete the Installation Worksheet	3-4
Step 7. Modify SAMPJCL Member JOBCARD	3-4
Step 8. Modify SAMPJCL Member TNGVARS	3-4

Step 9. Allocate Target and Distribution Libraries	3-5
Step 10. Allocate Private SMP/E Libraries	3-6
Step 11. Set Up Environment to Use SMP DDDEFs	3-6
Step 12. Set Up Event Management and WorldView SMP DDDEFs	3-6
Step 13. Allocate Event Management and WorldView HFS	3-7
Step 14. Create Event Management Directories	3-7
Step 15. Create Event Management and WorldView Profile	3-8
Step 16. Modify SAMPJCL Member AGNTVARS	3-9
Step 17. Create Agent Technologies Install Directory	3-9
Step 18. Initialize SMP/E for Agent Technologies	3-9
Step 19. Agent Technologies Downloads	3-10
Step 20. Event Management and WorldView Downloads	3-10
Step 21. RECEIVE CCS for z/OS and OS/390	3-10
Step 22. Copy and Modify the EARL Option Source Member	3-11
Step 23. Prelink Agent Technologies	3-11
Step 24. Create Userid for Agent Technologies	3-12
Step 25. Allocate Agent Technologies HFS	3-12
Step 26. Update INSTPAX member	3-13
Step 27. Expand Agent Technologies Tarfile	3-13
Step 28. APPLY CCS for z/OS and OS/390	3-14
Step 29. Set Mode Bits for Agent Technologies	3-14
Step 30. Set userid Mode Bit for Agent Technologies	3-15
Step 31. APF Authorize the CAILIB Data Set	3-15
Step 32. Define or Upgrade the CAIENF Database	3-15
Step 33. Allocate CA-Datcom SMP/E and Database Data Sets	3-17
Step 34. Load CA-Datcom SMP/E Libraries	3-17
Step 35. Rename SMP/E DDDEFs	3-17
Step 36. ASSEMBLE/LINK Custom Modules	3-17
Step 37. Customize TNG	3-18
Step 38. Install CA-Datcom SVC	3-18
Step 39. Load CA-Datcom Databases from Tape	3-18
Step 40. Start Up MULTI-USER	3-18
Step 41. Reset HSD File	3-19
Step 42. Back Up CXX AND DATADictionary	3-19
Step 43. Shut Down MULTI-USER	3-19

Step 44. Start Up Datacom/TR with the Trigger Server	3-19
Step 45. Create Links for Event Management	3-20
Step 46. Create Links for WorldView	3-20
Step 47. Shut Down the Trigger Server	3-20
Step 48. Shut Down MULTI-USER	3-20
Step 49. Link-Edit CAICCI 1.1 for TCP/IP	3-21
Step 50. Link-Edit ENF SNMP Monitor	3-22
Step 51. Establish Site Defaults for CA-C Runtime	3-23
Step 52. Allocate the ViewPoint Profile	3-23
Step 53. Allocate GSS ISET VSAM Data Sets	3-24
Step 54. Compile and Load IMOD Files	3-24
Step 55. Copy GSS Option Members to PPOPTION	3-25
Step 56. ACCEPT CCS for z/OS and OS/390	3-25
Step 57. Save All Materials and Output	3-26
Step 58. Post-Installation Steps	3-26

Chapter 4: Post-Installation Tasks

List of Tasks	4-1
What Next?	4-2
Running the Management Services Install Script	4-2
The Repository	4-3
WorldView	4-4
Configuring OS/390 UNIX System Services for WorldView	4-4
Configuring the Web Server	4-5
Installing Java	4-7
Reviewing Security Definitions for WorldView	4-7
Initializing the CCS for z/OS and OS/390 Java Server	4-9
Event Management	4-10
Store and Forward	4-10
Setting Up the Berkeley syslog daemon	4-12
Enable catrapd	4-15
Initialize the Event Management Servers	4-15
Agent Technology Services	4-16
Tailor the Profile, Script, and Configuration Files in the HFS System	4-17

Build the Aws_admin Store Files	4-22
Arrange for Agent Security	4-23
Installing Multiple Systems	4-23
Move the Load Library to LPA	4-25
Start Agent Technology	4-26
CAIRIM Tasks	4-26
Modify the CAIRIM Initialization Parameters	4-26
Customize CAISSF for RACF or RACF-Compatible Products	4-29
Start CAIRIM	4-36
CAIENF Tasks	4-37
Define Structures in the Coupling Facility	4-37
Start CAIENF	4-39
CAIENF/USS Tasks	4-40
CAICCI Tasks	4-40
Configuring and Starting CAICCI	4-40
Loading CAICCI on the Client Platform	4-41

Chapter 5: Customizing CA-GSS

Defining Subsystem IDs	5-2
Copying CA-GSS Procs to System PROCLIB	5-2
Preparing the Started Task PROC	5-3
Installing the IMOD Editor	5-3
Review Enqueue Requirements	5-4
Construct the Parameter List and Update the CA-GSS RUNPARMS	5-4
Modify the ISPF Menu Panel	5-5
IMOD Editor Problems?	5-6
Installing the CA-GSS/ISERVE Operator Control Panel	5-7
Testing the Installation	5-8
Starting CA-GSS	5-8
Testing CA-GSS	5-8
Testing the IMOD Editor	5-9
Stopping CA-GSS	5-9
Recompiling Under TSO	5-10
Customizing Initialization Parameters	5-10

Customizing for Particular Products	5-11
CA-Insight for DB2	5-11
CA-Jobtrac	5-16
CA-OPS/MVS II	5-16
CA-SYSVIEW	5-18
CA-View	5-18
DB2	5-20
IDCAMS	5-22
Installing Optional Features	5-24
GoalNet	5-24
ILOGs	5-27
Logon Facility	5-28
Upgrading ISETs	5-31

Chapter 6: Starting CA-L-Serv

Update External Security for CA-L-Serv	6-1
Who Needs to Update?	6-2
Update Tasks	6-2
Define CA-L-Serv to VTAM	6-9
Tailor Startup Parameters	6-10
Update the Message Table	6-12
Copy and Tailor the Startup Procedure	6-13
Start CA-L-Serv	6-14
Verify the Communications Server Installation	6-15
Communications Server Verification Steps	6-16
Troubleshooting	6-18
Verify the File Server Installation	6-19
File Server Verification Steps	6-20

Chapter 7: Maintaining CCS for z/OS and OS/390

Maintenance Steps	7-1
Step 1. Visit the Support Page	7-1
Step 2. Load Installation SAMPJCL Library	7-2

Step 3. Download BookManager Files	7-3
Step 4. Download PDF Files	7-3
Step 5. Complete the Installation Worksheet.....	7-3
Step 6. Modify SAMPJCL Member JOBCARD	7-3
Step 7. Modify SAMPJCL Member TNGVARS.....	7-4
Step 8. Edit JCL to Exclude Previously Applied SYSMODs	7-4
Step 9. ACCEPT Previous Maintenance of CCS for z/OS and OS/390 Base Functions	7-5
Step 10. Agent Technologies Downloads	7-5
Step 11. Prelink Agent Technologies	7-5
Step 12. Event Management and WorldView Downloads	7-5
Step 13. Set Up Event Management and WorldView SMP DDDEFs	7-6
Step 14. RECEIVE CCS for z/OS and OS/390 Maintenance	7-6
Step 15. APPLY Check CCS for z/OS and OS/390 Maintenance	7-7
Step 16. RESTORE Applicable SYSMODs	7-8
Step 17. APPLY CCS for z/OS and OS/390 Maintenance	7-9
Step 18. Reapply Applicable SYSMODs	7-10
Step 19. Start Up Datacom/TR with Trigger Server	7-10
Step 20. Create Links for Event Management	7-11
Step 21. Create Links for WorldView	7-11
Step 22. Save All Materials and Output	7-11

Appendix A: Installation Checklists

Event Management Common Installation Checklist	A-2
WorldView Installation Checklist	A-4
CAIRIM Installation Checklist	A-5
CAIENF Installation Checklist	A-6
CAISSF Installation Checklist.....	A-7
CAICCI Installation Checklist	A-8
CAIENF/CICS Installation Checklist	A-9
CAIENF/CICS SPAWN Installation Checklist	A-10
CAIENF/DB2 Installation Checklist	A-11
CAIENF/PIGware Installation Checklist	A-12
EARL Service Installation Checklist	A-13

SRAM Service Installation Checklist	A-14
CA-C Runtime Installation Checklist	A-15
CAIVPE Installation Checklist	A-16
ViewPoint Installation Checklist	A-17
CA-MFLINK Installation Checklist	A-18
CA-L-Serv Installation Checklist	A-19
CA-Agent Technologies Installation Checklist	A-20
CA-GSS Installation Checklist	A-21
CA-XPS Installation Checklist	A-22

Appendix B: Installation Worksheet

Installation and Maintenance Worksheet	B-1
--	-----

Introducing CA Common Services (CCS) for z/OS and OS/390

CA Common Services (CCS) is an open, cross-platform enterprise management infrastructure available on over thirty operating system platforms, including z/OS and OS/390.

This guide provides you with the necessary information to successfully install, customize, and maintain CCS for z/OS and OS/390. To aid you with the installation, you will find that installation checklists and an installation worksheet have been provided in the appendixes.

Overview

CCS for z/OS and OS/390 provides common services and enabling technology for Computer Associates systems management solutions, extending these solutions to manage UNIX System Services as well as adding capability to help them manage remote platforms. It also provides a distributed architectural framework on which clients and third-party vendors can create IT management applications that work together smoothly.

Note: References to the z/OS operating system throughout this manual pertain to the supported versions of z/OS and OS/390 operating systems.

Why Common Services?

In recent years, as the IT industry has recognized the need for integrated management of diverse client/server environments, the role of the mainframe as a super server for eBusiness and distributed applications has emerged, revealing the need for a framework on which to base management solutions. Such a framework, implemented on the mainframe, could enable consistent and dependable management of today's—and tomorrow's—varied workloads. The goal of CCS is to provide integrated management of all IT resources, including z/OS resources, using common enabling technology.

Changing Role of z/OS

Traditionally, z/OS has been a workhorse, processing millions of business transactions daily for large corporations. z/OS is well known for its robustness, scalability, reliability, availability, and serviceability.

With the advent of UNIX-based applications, high-performance Web servers, client-server applications, Java applications, Netware and other third-party applications and networking services, the z/OS workload has become more complex. Using a variety of system and application agents, existing Computer Associates z/OS management solutions are now capable of managing a variety of platforms. Not only that, you also have the capability of managing z/OS from other platforms through integration with CA eBusiness solutions.

The implication is a more heterogeneous IT environment composed of various hardware and software platforms and network protocols. This emergent environment requires an infrastructure that provides sophisticated monitoring and administration facilities and enables the integration of UNIX with traditional mainframe resources—allowing your mainframe to participate in a distributed enterprise management structure.

The CCS for z/OS and OS/390 Solution

CCS for z/OS and OS/390 includes distributed services common to all CCS implementations and solutions specific to z/OS. It provides a common GUI, object repository, and event services to create multiple, unified views of resources. It also contains and supersedes components from CA90s, Unicenter TNG Framework for OS/390, Global Subsystem (GSS), and L-Serv enabling infrastructures.

CCS for z/OS and OS/390 combines the comprehensive services and utilities formerly included as part of CA90s Services, which evolved into Unicenter TNG Framework for OS/390, with the rich functionality of CCS to provide state-of-the-art management capabilities and the most effective processing of data across your enterprise. It lets you manage emerging z/OS workloads and enables existing z/OS management applications to provide cross-platform facilities for the distributed enterprise within and beyond z/OS.

This z/OS-hosted enterprise management framework, identical to existing CCS on platforms ranging from Windows to UNIX, expands the choice of what and where to manage. It also contains all the essential components and functionality to enable integrated management of z/OS.

CCS for z/OS and OS/390 includes support for applications based on z/OS UNIX Systems Services. CCS for z/OS and OS/390 also furnishes the Agent Technology infrastructure to run z/OS Agents.

CCS for z/OS and OS/390 enables you to:

- Integrate your mainframe with other distributed platforms.
- Manage emerging z/OS workloads such as Web servers, Java applications, and UNIX applications.
- Use existing CA management applications (CA-1, CA-7, CA-MICS) to manage your distributed, heterogeneous enterprise from your mainframe.

- Achieve enterprise-wide, automated, high-level monitoring and management of critical resources using sophisticated manager/agent technology, together with CA products.
- View all of the resources in the repository using a Web-based Real World Interface. z/OS resources are also accessible from CA products and CCS on other platforms.

End-to-End Management

With CCS for z/OS and OS/390, 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. It enables you to identify resources widely dispersed throughout your enterprise and, in conjunction with manager software (available separately), you can organize, monitor, and manage them from your mainframe.

The unparalleled software technology of CCS for z/OS and OS/390 give you the freedom to run the appropriate hardware platforms and software applications for each aspect of your business and deploy them across many machines, spanning thousands of miles, and over complicated network topologies, while enabling you to manage them as an integrated whole.

CCS for z/OS and OS/390 also enable you to create strategies for managing your enterprise as a whole or to subdivide it into localized or functional domains, each with its own Business Process Views and requirements.

Business Process Views

Business Process Views are user-defined groups of managed objects that represent specific business processes, resource features, geographical locations, organizational structures, or applications. For example, you may create a Business Process View that displays only objects related to the accounting processing, and another for payroll for your company. The manufacturing department might have a view showing the servers and networking devices and segments in various factories and warehouses.

These segments of your enterprise may be composed of software applications running across several servers, including mainframe systems, UNIX and Windows servers, several hundred workstations, several databases, many printers, and various other processes. With CCS for z/OS and OS/390, these usually disparate pieces of software and hardware may be logically and cleanly organized into a Business Process View. Once defined, this view is just a click away.

Comprehensive Unicenter Administration

Using CCS for z/OS and OS/390, you can also administer Unicenter components installed on other platforms. This administrative capability includes all of the functionality of Enterprise Management:

- Workload Management—provides job scheduling, monitoring of job sequence and failure, and determination of resources for jobs.
- Event Management—allows you to monitor and administer different kinds of asynchronous events including SNMP Traps, application events, and system events.
- File Management—comprehensive backup and restore functions for all environments.
- Security Management—additional layer of security on top of native operating system security secures the integrity and confidentiality of your data and programs.

- Problem Management—provides for management of day-to-day problems and questions encountered in the administration of your enterprise.
- Performance Management—manages system performance, including optimization of throughput, collection of performance and usage data, and analysis of usage data.

Thus, the mainframe can act as an administrative client for other CCS and Unicenter platforms.

Multi-layered Architecture

CCS for z/OS and OS/390 is composed of a visualization layer and a z/OS software services layer. The visualization layer provides a Web-based real-world graphical interface, monitoring of application and system events, and browsing tools for comprehensive administration of all your IT resources. The z/OS services layer includes a suite of industry standard integration and distributed processing services to unify software applications.

Visualization Services

CCS for z/OS and OS/390 visualization services enable integrated administration of all IT resources in your enterprise, including network devices, databases, business applications for desktop systems and mainframes, and all servers between. The various components are outlined in the following sections.

The Real World Interface

The WorldView component of CCS for z/OS and OS/390 provides your enterprise with a revolutionary new graphical user interface (GUI)—the Real World Interface. The Real World Interface allows management applications to identify the business resources they manage as well as the relationships between those resources.

The Real World Interface for CCS for z/OS and OS/390 is available from any Web browser. z/OS resources can also be visualized by CCS on other platforms. The z/OS hosted version uses sophisticated Java, HTML, and VRML technology for Web browser access. Web access is optionally secured using the secure sockets layer yet provides for open and extensible management capabilities. From the Web browser interface, the user can launch mainframe and distributed applications, including 3270 sessions, for access to legacy applications.

Browsers and ObjectView

CCS for z/OS and OS/390 offers views of information stored in the Common Object Repository and other data stores, which organize complicated information and allow a simplified, yet comprehensive, look at your IT infrastructure. This information is presented in easy-to-use browsers – Class, Object, Topology, and Link – and through ObjectView.

Class Browser	The Class Browser presents the CCS for z/OS and OS/390 classes and their properties. It provides a comprehensive look at all the classes in the repository.
Topology Browser	The Topology Browser displays the inclusion relationship between objects as they appear on the map. It provides you with a view of the set of relationships between managed objects.
ObjectView	Many of the managed objects in the Common Object Repository represent network devices. ObjectView provides details on the performance of a device, such as the number of devices connected, which interfaces are down, and the number of packets coming in compared with the number going out.

The Common Object Repository

The Common Object Repository is central to all enterprise management functions. The repository stores managed resources, their status and instrumentation data, and the policies that govern them. It also contains icons and graphical representations of managed resources, also referred to as “managed objects,” which may include software applications, hardware, databases, and entities such as accounts receivable, inventory, and manufacturing processes.

The design of managed objects throughout CCS for z/OS and OS/390 is formalized using a Common Object Model, which facilitates the integration of diverse applications and includes search and query capabilities. These capabilities enable management functions to find relevant sets of objects on which to operate.

Building the Common Object Repository and loading it with data that describes your enterprise – also called “populating the repository” – is performed automatically by CCS for z/OS and OS/390 through a remarkable process called Discovery.

Auto Discovery

The Discovery service included with CCS for z/OS and OS/390 automatically detects entities in your IT infrastructure and populates the Common Object Repository with managed objects that represent these entities and their relationships. Once created, these objects can be displayed using the Real World Interface. The entities they represent can be monitored and controlled by the Event Management component of CCS for z/OS and OS/390, as well as by agent managers and third-party management applications.

CCS for z/OS and OS/390 Discovery provides significant advantages over other network discovery applications. This Discovery service allows you to:

- Run multiple instances of Discovery at the same time.
- Discover one single device using Single IP Discovery.
- Define the granularity of Discovery, so that you can discover all resources in the infrastructure or just the ones belonging to a subnetwork.
- Initiate Discovery automatically or manually.
- Specify the types of resources to be discovered.

Event Management

Event Management is a collection of management components that employ a single, easy-to-use Graphical User Interface to monitor and administer different kinds of asynchronous events including SNMP Traps, application events, and system events. Event Management makes it easy for you to collect related messages network-wide for display at a single location or send them to multiple locations, as needed.

CCS for z/OS and OS/390 Event Management augments z/OS automation solutions, such as CA-OPS/MVS II, by providing built-in access to a wide range of distributed events and by allowing actions to be triggered on any CCS equipped platform. CCS for z/OS and OS/390 provides event correlation and event processing and is fully integrated with CCS event management facilities on other platforms. CCS for z/OS and OS/390 also has several SDK functions, including command line and batch interfaces.

You may define specific Event Management policy to:

- Respond to messages
- Suppress messages
- Issue CCS for z/OS and OS/390 commands
- Start other programs or scripts

- Send information to a network management or automation application such as CA-OPS/MVS II
- Forward messages to other managed platforms
- Issue commands to be executed on other platforms
- Interpret the results of any action to decide if additional actions are warranted
- Define or update objects in the Common Object Repository

Event Management can be configured to process messages on individual servers and redirect them to a central server or other servers and, by extension, their consoles. Event Management makes it easy to collect related messages network-wide for display at a single location or send them to multiple locations, as needed.

The Event Console Log GUI window enables you to monitor system events as they occur. All running programs and user processes can direct inquiries and informative messages to this facility. It provides a complete view of processes across the network.

Calendars

The CCS for z/OS and OS/390 calendar object is a common object available for use by any of the Enterprise Management functions, including Event Management.

Calendars make it possible to determine a course of action based on **when** an event occurs. The event not only meets the general criteria; it also meets the date, day, and time criteria established through calendar profiles. The primary function of a calendar can be identified in a naming scheme. CCS for z/OS and OS/390 provides facilities to define as many calendars as you require to meet your needs and to store them for easy reference.

Note: The use of calendars with Event Management is optional.

Agent Technology

CCS for z/OS and OS/390 includes the Agent Technology infrastructure that 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. The Agent Technology infrastructure supports existing prepackaged z/OS agents such as the z/OS System Agent, CA-IDMS Agent, CA-Datacom Agent, DB2 Agent, and CICS Agent, as well as other agents created to CCS specifications.

Agent Technology supports 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 further enhances the ability of z/OS environments to participate in a true heterogeneous network.

Services Provided by CCS for z/OS and OS/390

z/OS services support the sharing of software services among a variety of applications and promote the efficient exchange of information across your disparate hardware platforms and operating systems. The services provided by CCS for z/OS and OS/390 are:

- Management of OS/390 UNIX System Services (CAIENF/USS)—extensions to CCS for z/OS and OS/390 encapsulate and integrate the management of UNIX Systems Services applications on z/OS. This service enables management applications to process system events occurring in the z/OS UNIX System Services subsystem.
- CAIRIM—prepares your operating system environment for all of your CA applications and then 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.

- CAIENF (Base, CICS, and DB2)—provide comprehensive operating system interfacing services to any of the Computer Associates z/OS applications, exploiting technologies such as relational database architectures, 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.
- CAIENF/CICS SPAWN—a communications facility that enables Computer Associates applications to start CICS units of work from outside the CICS region. This facility provides a layer that isolates the application software from CICS release dependencies.
- CAIENF Utilities (formerly PIGware)—a collection of facilities that allows you to use the services provided by CAIENF. Facilities include an online database query editor, a real-time CAIENF event monitor, and a command for performing CAIENF LISTEN and EXTRACT functions. (Information regarding these utilities can be found in the *CA Reference Guide*.)
- CAICCI—provides CA enterprise applications with a wealth of capabilities including common communications, cooperative processing, and database server facilities, as well as distributed database management. Full support for all forms of distributed processing ensures the highest degree of flexibility for the enterprise.
- CA-GSS—a simplified communication interface that allows various CA products to communicate easily, seamlessly, and reliably, thereby providing 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—enables cross-platform scheduling for CA products including CA-7, CA-Scheduler, and CA-Jobtrac.

- CA-L-SERV—provides the CA-L-Serv services that are used by CA products including Endeavor, CA-Bundl, CA-OPS/MVS II, CA-Balancing, CA-TPX, and CA-Multi-image Console. These services include centralized logging and messaging facilities, VSAM file management, cross-system communications, and SQL table management.
- CAISSF—provides an external security mechanism for controlling and monitoring access to all system and application resource processes. CAISSF is already well integrated into many CA enterprise applications, and is used by other CCS for z/OS and OS/390 services as well. It provides security services for user signon, resource access control, process use control, and recording and monitoring of violation activity.
- CA LMP—an integral part of CAIRIM that provides a standardized and automated approach to the tracking of licensed software.
- SRAM Service—allows the activation of several sorts concurrently, thereby 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.
- EARL Service—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 predefined CA application report using English-like statements.
- CAIVPE—an inter-product facility used by other CA applications running under CA-Roscoe, TSO, or CICS. It contains monitor-specific code and allows Computer Associates applications to run independent of the environment.
- CA-C Runtime—a 'C' runtime facility that insulates programs from system and release dependencies.

Getting Started with CCS for z/OS and OS/390

The following table outlines the recommended approach for learning about CCS for z/OS and OS/390.

Tasks ...	How to Perform Them ...
Determine the Hardware and Software requirements for CCS for z/OS and OS/390	Before you begin installation, review the Hardware and Software Requirements section in the chapter “System Requirements” of this guide. It provides the necessary information for ensuring that your hardware and software configurations accommodate CCS for z/OS and OS/390.
Install CA Common Services for z/OS and OS/390	Review the instructions in the chapter “Installing CCS for z/OS and OS/390” of this guide for information about what to expect during installation. Here you will find guidance on proceeding through the installation instructions.
Finish Up the Install	Carry out the appropriate post-installation tasks for the components you installed.
Customize Your Configuration	Customize many aspects of CCS for z/OS and OS/390 to meet your needs. See the CCS for z/OS and OS/390 <i>Administrator Guide</i> , and the online <i>CA Procedures Guide</i> , <i>CA Reference Guide</i> , and the online GUI help system for the detailed information you need.
Define Your Enterprise Management Policies	<p>A policy represents a set of rules that outline how and when Enterprise Management tasks are to be performed. Use the CCS for z/OS and OS/390 GUI, commands, and configuration files to define your policies.</p> <p>See the CCS for z/OS and OS/390 <i>Administrator Guide</i>, and the online <i>CA Procedures Guide</i>, <i>CA Reference Guide</i>, and the online GUI help system for the detailed information you need.</p>

Getting Help

CCS for z/OS and OS/390 visualization services have an online help system to assist you in using the various components. The online help system is linked to the online *CA Procedures Guide* to take advantage of the full functionality and unique features of CCS for z/OS and OS/390.

For further technical assistance with this product, please contact Computer Associates technical support 24 hours a day, 7 days a week at <http://esupport.ca.com>.

Documentation Set

Documentation provided with CCS for z/OS and OS/390 includes the following items:

- *CA Common Services for z/OS and OS/390 Getting Started (BookManager and PDF)*—Provides a description of the product, details the hardware and software requirements, and provides installation instructions and considerations.
- *CA Common Services for z/OS and OS/390 Administrator Guide (BookManager and PDF)*—Provides descriptive information regarding the CCS for z/OS and OS/390 components and details regarding usage and operation.
- *CA Message Guide (BookManager and Web Browser-based online help)*—Provides information regarding error messages that may occur during the operation of CCS for z/OS and OS/390.
- *CA Procedures Guide (Web Browser-based online help)*—Provides step-by-step procedures regarding CCS for z/OS and OS/390 visualization components.
- *CA Reference Guide (Web Browser-based online help)*—Provides all of the commands, control options, and utilities used with CCS for z/OS and OS/390. This includes control options for CAICCI, CAIENF, CAS9DB, CAIRIM, CAIENF Utilities (formerly known as PIGware), CA-GSS, and CA-L-Serv.

- *Working With Agents (BookManager and PDF)*—Provides comprehensive information regarding Agent Technology, including how to configure agents and agent managers.
- *CA-Activator Implementation and User Guide (BookManager)*
- *ViewPoint User Guide (BookManager)*
- *CA-EARL Systems Programmer Guide (BookManager)*
- *CA-EARL Reference Guide (BookManager)*
- *CA-EARL User Guide (BookManager)*
- *CA-EARL Examples Guide (BookManager)*
- *CA-Datacom/DB Database Administrator Guide (BookManager)*
- *CA-Datacom/DB DBUTLTY Reference Guide (BookManager)*
- *CA-Datacom/DB Message Guide (Volume 1 and 2) (BookManager)*
- *CA-Datacom Server User Guide (BookManager)*

Generally, all commands, control options, and utilities are documented in the online *CA Reference Guide*. However, for added convenience, we have also placed the control options for the Common Services (former CA90s components, CA-L-Serv, and CA-GSS) in the *CA Common Services for z/OS and OS/390 Administrator Guide*.

What Happened to...?

Since CCS for z/OS and OS/390 combines former CA90s Services with CCS, certain items from the former CA90s Services documentation set have been restructured, as shown in the following table:

To find information formerly in:	Look here
<i>CAICCI User Guide</i> general information	CA Common Services for z/OS and OS/390 <i>Administrator Guide</i>
<i>CAICCI User Guide</i> commands messages	<i>CA Reference Guide</i> <i>CA Message Guide</i>
<i>PIGware Reference Guide</i>	<i>CA Reference Guide</i> , CAIENF Utilities section
<i>CA90s Services Installation Guide</i>	CA Common Services for z/OS and OS/390 <i>Getting Started</i>
<i>CA90s Services Reference Guide</i>	CA Common Services for z/OS and OS/390 <i>Administrator Guide</i>

The CA-L-Serv and CA-GSS documentation sets have been restructured also, to reflect their incorporation into CCS for z/OS and OS/390.

To find information formerly in:	Look here
<i>CA-L-Serv Installation Guide</i>	CA Common Services for z/OS and OS/390 <i>Getting Started</i>
<i>CA-L-Serv User Guide</i>	CA Common Services for z/OS and OS/390 <i>Administrator Guide</i>
<i>CA-L-Serv Message Reference</i>	<i>CA Message Guide</i>
<i>CA-L-Serv Command Reference</i>	<i>CA Reference Guide</i>
<i>CA-GSS for MVS Installation Guide</i>	CA Common Services for z/OS and OS/390 <i>Getting Started</i>
<i>CA-GSS for MVS Function Reference</i>	<i>CA Reference Guide</i>

To find information formerly in:	Look here
<i>CA-GSS for MVS Technical Reference</i>	<i>CA Common Services for z/OS and OS/390 Administrator Guide</i> <i>CA Reference Guide</i>
<i>CA-GSS for MVS Messages and Codes</i>	<i>CA Message Guide</i>
<i>CA-GSS for MVS Operations Guide</i>	<i>CA Reference Guide</i>
<i>CA-GSS for MVS IMOD Guide</i>	<i>CA Common Services for z/OS and OS/390 Administrator Guide</i>

System Requirements

This chapter details the hardware and software required to install and run CCS for z/OS and OS/390 and includes installation considerations where applicable.

It also provides information regarding installation dependencies among the different components that comprise CCS for z/OS and OS/390. It is recommended that only required components be installed. To determine which components may require other Computer Associates z/OS products, see the installation requirements documentation for the individual products.

Installation Overview

Installing CCS for z/OS and OS/390 involves the following phases:

- Review system requirements
- Fill out the Installation Worksheet
- Generate and submit the JCL
- Perform applicable post-installation tasks

Hardware and Software Requirements

The hardware and software requirements are discussed in this section.

Target Libraries

As part of the SMP process for CCS for z/OS and OS/390, the CAI target libraries named in the following table are updated with specific routines. You can determine the space allocation for each target library by reviewing the system requirements for each service you are installing.

Note: For these descriptions, the default names for the Computer Associates libraries have been used.

Library	Contents
CAI.CAILIB	The CAI Common Authorized Load library contains service-related executable modules.
CAI.PPOPTION	The CAI Product Options library contains sample parm members for CCS for z/OS and OS/390.
CAI.CAIPROC	The CAI Procedure library contains sample procedures for invocation of CCS for z/OS and OS/390 and its related utilities.
CAI.SAMPJCL	The SAMPJCL library contains the sample JCL necessary to install and maintain CCS for z/OS and OS/390.
CAI.CAIPDSE	The PDSE library contains load modules link edited in program format 3.
CAI.CAISRC	The Source library contains the source programs used for executing service-related utilities under TSO.
CAI.CAIMAC	The Macro library contains the macros used in compiling service-related programs.
CAI.CAICICS	The CICS Load library contains service-related CICS executable modules.

Library	Contents
CAI.CAICLIB	The CLIST library contains service-related CLISTs.
CAI.CAIISPL	The ISPF Load library contains service-related ISPF executable modules.
CAI.CAIISPM	The ISPF Message library contains service-related ISPF messages.
CAI.CAIISPP	The ISPF Panel library contains service-related ISPF panels.
CAI.CAIISPS	The ISPF Skeleton library contains service-related ISPF skeletons.
CAI.CAIISPT	The ISPF Table library contains service-related ISPF tables.
CAI.CAISYSI	The CA-GSS system IMOD library contains source for internal IMODs used by CA-GSS.
CAI.CAISAMPI	The CA-GSS Sample IMOD library contains sample REXX source.
CAI.CAEDIT	The CAIENF Utilities Editor library.
CAI.CASCRN	The CAIENF Utilities Panel library.
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.CHOICES	The ViewPoint Choices library contains service-related ViewPoint lists.
CAI.VPOINT.MESSAGE	The ViewPoint Message library contains service-related ViewPoint messages.
CAI.VPOINT.PANEL	The ViewPoint Panel library contains service-related ViewPoint panels.

Library	Contents
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.
CAI.EXP	The Agent Technology Export decks library.
CAI.HFS	The Agent Technology POSIX files.
CAI.INDOBJ	The Agent Technology Pre-linked object library.
CAI.LISTLIB.PRELINK	The Agent Technology Pre-linked listing library.
CAI.LOADLIB	The Agent Technology Program library.
CAI.MIBLIB	The Agent Technology MIB source library.
CAI.OBJ	The Agent Technology Object Library for the user.
CAI.OBJLIB	The Agent Technology Object library.
CAI.TARFILE	The Agent Technology TAR backup file.

Comprehensive View of Storage Requirements

The following table lists the minimum storage requirements for each target library, broken down by component. Later in the chapter, the distribution library requirements are presented one component at a time.

Library Name	Block Size	Component	Blocks	Dir Blks
CAI.CAILIB	6144	Event Mgt.	5	1
		CAIRIM	19	2
		CAIENF	685	24
		CAIENF Utilities	73	2
		CAIENF/USS	45	10
		CAICCI	260	3
		CAIVPE	196	5
		CA-MFLINK	7	1
		EARL Service	85	5
		SRAM Service	30	5
		CA-C Runtime	685	24
		ViewPoint	854	50
		CA PROFILE	5	1
		CA-Datacom/TR	3000	90
		CA-L-Serv	1675	30
		CA-GSS	720	6
		CA-XPS	5	1

Library Name	Block Size	Component	Blocks	Dir Blks
CAI.PPOPTION	3120	CAIRIM	3	1
		CAIENF	6	1
		CAIENF Utilities	13	2
		CAICCI	315	1
		EARL Service	10	1
		ViewPoint	13	10
		CA-L-Serv	575	10
		CA-GSS	81	4
CAI.CAISRC	3120	CAIRIM	58	1
		CAIENF	1	5
		CAIVPE	3	2
		EARL Service	60	2
		CA-C Runtime	1	5
		ViewPoint	13	10
		CA-L-Serv	65	5
		CA-GSS	3	1
CAI.CAIMAC	3120	CAIRIM	13	1
		CAIVPE	3	2
		EARL Service	60	2
		CA-C Runtime	80	2
		ViewPoint	52	5
		CA-Datacom/TR	1500	10
		CA-GSS	13	1

Library Name	Block Size	Component	Blocks	Dir Blks
CAI.CAIPROC	3120	CAIRIM	5	1
		CAIENF	10	1
		EARL Service	350	40
		CA-C Runtime	10	1
		CA-L-Serv	20	5
CAI.CAICLIB	3120	CAIENF Utilities	10	2
		ViewPoint	13	10
		CA-GSS	26	1
CAI.CAIISPP	3120	CAIENF Utilities	15	1
		ViewPoint	52	75
		CA-GSS	270	20
CAI.CAICICS	6144	CA-C Runtime	85	30
CAI.CAIPDSE	6144	Event Mgt.	100	5
CAI.CAEDIT	6144	CAIENF Utilities	15	5
CAI.CASCRN	4104	CAIENF Utilities	100	25
CAI.CAIISPM	3120	CA-GSS	6	1
CAI.VPOINT.DIALOG	8204	ViewPoint	215	300
CAI.VPOINT.HELP	4104	ViewPoint	770	1200
CAI.VPOINT.CHOICES	4104	ViewPoint	60	60
CAI.VPOINT.MESSAGE	4104	ViewPoint	60	60
CAI.VPOINT.PANEL	4104	ViewPoint	370	300
CAI.VPOINT.SQL	3120	ViewPoint	39	30
CAI.VPOINT.TEMPLATE	3120	ViewPoint	26	10
CAI.CAISAMPI	3600	CA-GSS	39	2
CAI.CAISYSI	3600	CA-GSS	810	11

Library Name	Block Size	Component	Blocks	Dir Blks
CAI.EXP	3200	Agent Tech.	5	5
CAI.HFS	-	Agent Tech.	9000	-
CAI.INDOBJ	3200	Agent Tech.	400	20
CAI.LISTLIB.PRELINK	3200	Agent Tech.	25	10
CAI.LOADLIB	6144	Agent Tech.	400	10
CAI.MIBLIB	25600	Agent Tech.	270	5
CAI.OBJ	3200	Agent Tech.	85	5
CAI.OBJLIB	3200	Agent Tech.	300	10
CAI.TARFILE	32760	Agent Tech.	5	0

Event Management Requirements

Event Management has the following installation requirements:

- OS/390 Version 2.5 and above
- 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
- Disk space: (HFS) - approximately 200 cylinders

Library Storage Requirements

The distribution libraries required for Event Management are:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.TN22.CTN22LLD	6144	1500	5	Distribution Load Library
CAI.TN22.CTN22SLD	32760	30	10	Distribution Source Library
CAI.TN22.CTN22BLD	6144	20	10	Distribution Binary Library

WorldView Requirements

WorldView has the following installation requirements:

- OS/390 Version 2.5 and above
- IBM Domino GO Webserver 4.6 or above, with 5.0 recommended
- Java runtime environment 1.1.6 or above
- BPXPRMxx setting MAXASSIZE > 128MB
- BPXPRMxx setting MAXPROCUSER > 100
- BPXPRMxx setting MAXCPU TIME > 5000
- Disk space: (HFS) - approximately 1200 cylinders
- Security definitions for these resources in class CAIUNI:

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

Library Storage Requirements

The distribution libraries required for WorldView are:

Library Name	Block Size	Number of Cyls	Directories	Description
CAI.TN22.CTN22HTM	32760	60	800	Distribution HTML Library
CAI.TN22.CTN22JVA	32760	30	200	Distribution Java Library
CAI.TN22.CTN22MSC	32760	90	50	Distribution Miscellaneous Library
CAI.TN22.CTN22GIF	32760	30	250	Distribution GIF Library
CAI.TN22.CTN22SCR	32760	13	10	Distribution Script Library

Note: The WorldView storage requirements are given for cylinders, not blocks.

CAIRIM/CAISSF Requirements

The CAIRIM service, S910, comprises both CAIRIM and CAISSF services.

Note: See the chapter “Resource Initialization Manager” in the CCS for z/OS and OS/390 *Administrator Guide* for detailed information regarding non-CA security product support of CAISSF.

CAIRIM has the following installation requirements:

- 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 routines can be executed from a STEPLIB concatenation or from a LNKLST concatenation. CAIRIM is normally installed into the common CAI.CAILIB.

- 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.

If SMF is not currently active on your system, see the section on member SMFPRMxx in the IBM *OS/390 Initialization and Tuning Reference* (SC28-1752) for more information.

- CAIRIM requires approximately 12K of ECSA and 4K 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 22K of ECSA.
 - CAISSF requires approximately 1K of CSA for the security into the routine, and approximately 2K to 4K 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. There is no need to select an SVC entry for the CA LMP SVC, as it will use the first available unused SVC slot it finds.

CAIRIM does not use LPA or ELPA.

Library Storage Requirements

The distribution libraries required for CAIRIM are:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.S910.CS910LLD	6144	34	4	Distribution Load Library
CAI.S910.CS910SLD	3120	81	1	Distribution Source Library

Note: The previous space calculations were generated using a 3380 device type. Space requirements should be increased or decreased based on the device type in which you are allocating CCS for z/OS and OS/390 libraries.

CAIENF Requirements

CAIENF has the following installation requirements:

- CAIENF supports operating system levels of OS/390 V2R5 and above.
- CAIENF must be installed into an APF authorized library. LINKLIST is not required; however, it 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 CCS for z/OS and OS/390 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. See the chapter “Event Notification Facility” in the *CCS for z/OS and OS/390 Administrator Guide* and the *CA Reference Guide* for information on tailoring CAIENF control options.

- When running within a sysplex, multiple CAIENFs can be connected to form an ENFplex. At least one coupling facility and one structure are required to enable this option. For information regarding setting up an ENFplex, see the chapter “Event Notification Facility” in the CCS for z/OS and OS/390 *Administrator Guide*.
- A database must be allocated and initialized for CAIENF use. The amount of disk space required by CAIENF for its database depends on several factors. A rough estimate of the space requirements can be given according to this formula:

$$\text{Space in cylinders} = (A * B / C) + 10$$

A = Total number of **logged** events per day.

B = Desired retention period in days.

C = Device constant:

For 3380, use 3000

For 3390, use 3600

See the “Event Notification Facility” chapter of the CCS for z/OS and OS/390 *Administrator Guide* for detailed information on allocating and initializing the database for CAIENF use.

- 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, 90K 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. As an estimate, the CAIENF address space requires approximately three to four megabytes 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 about 4K in each application address space, although this amount varies depending on application structure.

Library Storage Requirements

The distribution libraries required for CAIENF are:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.W110.CW110LLD	6144	3500	175	Distribution Load Library
CAI.W110.CW110SLD	3120	130	1	Distribution Source Library

Note: The above space calculations were generated using a 3380 device type. Space requirements should be increased or decreased based on the device type in which you are allocating CCS for z/OS and OS/390 libraries.

The space allocation for target and distribution libraries includes the space required by CAIENF/CICS, CAIENF/DB2, part of CAIENF Utilities, and CAICCI.

CAIENF Installation Considerations for CA-ACF2 Users

Note: This section applies to CA-ACF2 users only.

You must create two logon IDs (LIDs) for CAIENF:

- LID for the started task
- LID for use with any batch job that runs the CAIENF database utility CAS9DB

If your data center uses the restricted command list facility of CA-ACF2, the LID created for use with the batch jobs must have a command list of CAS9ACMD, which is supplied with CAIENF in the CAIENF load libraries.

Any batch job that executes CAS9DB should be submitted to run under the special LID. This is done using either of the following methods:

- By coding USER= and PASSWORD= parameters on the jobcard, or
- By inserting the following CA-ACF2 control statements immediately after the jobcard:

```
//*LOGONID special_lid
//*PASSWORD special_lid_password
```

Note: After the desired jobs have run, it is suggested that you remove or comment out this data to prevent unauthorized use of the LID.

Examples

The following examples show what your JCL might look like if your special LID is defined as CAS9LID and the password is defined as CAS9PASS, using the two methods described above:

Method 1:

```
//JOBNAME JOB (ACCOUNTING INFO),
//          USER=CAS9LID,PASSWORD=CAS9PASS,
//          CLASS=...
//STEP1    EXEC   PGM=CAS9DB.....
```

Method 2:

```
//JOBNAME JOB (ACCOUNTING INFO),
//          CLASS=...
//*LOGONID CAS9LID
//*PASSWORD CAS9PASS
//STEP1    EXEC   PGM=CAS9DB.....
```

Note: These are examples only. It is suggested that you choose a LID and a password that are different from those used above.

CAIENF Utilities Requirements

CAIENF utilities (formerly known as PIGware) have the following installation requirements:

- Requires the CA-C Runtime (CF33100) and cBASE MAPPER (CF62300) SMP functions to be installed.
- Requires the CAIENF SMP functions CW11000 and CW21000 to be installed. All system requirements for CAIENF must be met.
- If using the CAIENF Utilities ENFC facility, CAIENF/Extract (CW11001) and CAICCI (CW41100) must be installed. All system requirements for CAIENF/Extract and CAICCI must be met.
- Supports OS/390 V2R5 and above, with TSO/E Release 1.3 and up.

Library Storage Requirements

The distribution libraries required for CAIENF Utilities are:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.W110.CW110ELD	6144	15	5	Distribution Editor Library
CAI.W110.CW110PLD	4104	100	25	Distribution Panel Library

Note: The above space allocations were generated using a 3380 device type. Space requirements should be increased or decreased based on the device type in which you are allocating CCS for z/OS and OS/390 libraries.

CAIENF/CICS Requirements

CAIENF/CICS has the following installation requirements:

- CAIENF/CICS supports all CICS releases from CICS R1.7.0 and above.
- 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 CCS for z/OS and OS/390 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. See the CAIENF/CICS Control Options in the *CA Reference Guide* for more information.
- A database must be allocated and initialized for CAIENF use. An update to the database is required which tells CAIENF that the CAIENF/CICS interface is to be installed. See the section CAIENF/CICS and CAIENF/DB2 Operation in the chapter “Event Notification Facility” in the CCS for z/OS and OS/390 *Administrator Guide* for more information.
- 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 per 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 40K of CSA or CICS Private Area, depending on where they are loaded.

When a CICS Region is started, CAIENF/CICS checks for the existence of a DDNAME of CENFLIB. If this DDNAME is defined, then 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.

- Space allocation for the target and distribution libraries can be found in the section on CAIENF Requirements in this chapter.

CAIENF/DB2 Requirements

CAIENF/DB2 has the following installation requirements:

- CAIENF/DB2 supports all DB2 releases from DB2 R2.3 and above.
- A database must be allocated and initialized for CAIENF use. See the section CAIENF/CICS and CAIENF/DB2 Operation in the chapter “Event Notification Facility” in the *CCS for z/OS and OS/390 Administrator Guide* for more information.
- The load module DSNXAUTH cannot be loaded into LPA or an abend will occur when CAIENF/DB2 is initialized. CAIENF/DB2 requires DSNXAUTH to be loaded into the private area so intercepts can be managed by subsystem (not all subsystems will 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 20K 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.
- Space allocation for the target and distribution libraries can be found in the section on CAIENF Requirements in this chapter.

CAIENF/CICS SPAWN Requirements

CAIENF/CICS SPAWN has the following installation requirements:

- CAIENF/CICS SPAWN supports all CICS releases from CICS R2.1.2 and above.
- CAIENF/CICS SPAWN supports various control options that can be tailored to meet the individual data center requirements. See the section CAIENF/CICS SPAWN Control Options in the *CA Reference Guide* for more information.
- CAICCI is required software and needs to be installed prior to the installation of CAIENF/CICS SPAWN.
- A database must be allocated and initialized for CAIENF use. See the section CAIENF/CICS SPAWN Communications Facility in the chapter “Event Notification Facility” in the *CCS for z/OS and OS/390 Administrator Guide* for more information.

- The primary function of CAIENF/CICS SPAWN is to let Computer Associates 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, then 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.

- Space allocation for the target and distribution libraries can be found in the section on CAIENF Requirements in this chapter.

CAIENF/USS Requirements

CAIENF/USS has the following installation requirements:

- OS/390 V2R5 or higher, with OS/390 UNIX System Services active in full-function mode. Consult your IBM documentation for information on configuring OS/390 UNIX System Services.
- The ENF address space must run with root privileges under OS/390 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.

Consult your security product documentation for more information.

- For best performance, CAIENF/USS requires that you define a new object to VLF (Virtual Look-aside Facility) as follows:
 - Add an entry to the COFVLFxx member of SYS1.PARMLIB (where xx is the VLF identifier assigned by your systems programmer).

Example

```
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 2MB to 4MB of virtual storage) should suffice for most sites; however, you may want to change MAXVIRT according to the following formula:

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

where:

MAXFILEPROC and MAXPROC are OS/390 UNIX Services configuration parameters found in SYS1.PARMLIB(BPXPRMxx).

Note: See the *OS/390 Initialization and Tuning Reference (SC28-1752)* for more information about defining VLF objects.

- Your base CAIENF component needs to be at a service level of 9901 or higher. If you do not have this version of CAIENF installed, then CAIENF/USS will not initialize, and CA products which depend on CAIENF/USS will not function properly.
- The CAIENF DCM module CARRDCM0 must be installed using the CAS9DB utility.

Note: Products which use the CAIENF/USS component will also have a DCM (data collection module). The CAIENF/USS DCM and all product-specific DCMs must be installed to ensure correct operation. See your CA product documentation for details.

Library Storage Requirements

The distribution library required for CAIENF/USS is:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.RR10.CRR10LLD	32760	40	20	Distribution Load Library

CAICCI Requirements

CAICCI has the following installation requirements:

- CAICCI supports OS/390 V2R5 and above. If you use SNA connections, VTAM at release 2.1.1 and above is required. If you use TCP/IP with CAICCI, TCP/IP 2.1 or higher is required.
- 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. See the section CAICCI Control Options in the *CA Reference Guide* for information on tailoring CAICCI control options.
- A CAIENF database must be allocated and initialized. An update to the CAIENF database is required which tells CAIENF that CAICCI is to be installed. See the section Configuring the CAIENF Database in the chapter "Event Notification Facility" in the *CCS for z/OS and OS/390 Administrator Guide* for information on allocating and initializing a CAIENF database.

- CAICCI requires 172K 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. However, a rough estimate may be achieved by the following formula:

172K bytes + (Number of concurrent host-related programs using CAICCI) *

(308 bytes) + 328 * (Number of sessions in a multi-CPU environment)

One way of determining the number of concurrent host-related (application) programs using CAICCI is 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).

- Space allocation for the distribution libraries can be found in the section on CAIENF Requirements in this chapter.
- In a multi-CPU environment, add 258 bytes for each CPU defined.

CAIVPE Requirements

CAIVPE is used with other CA solutions. The prerequisite system requirements of these solutions meet or exceed the requirements for CAIVPE with respect to the environments and operating systems supported by CAIVPE.

Library Storage Requirements

The distribution libraries required for CAIVPE 4.2 are:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.WU42.CWU42LLD	6144	280	49	Distribution Load Library
CAI.WU42.CWU42MLD	3120	2	5	Distribution Macro Library
CAI.WU42.CWU42SLD	3120	50	50	Distribution Source Library

Note: The space calculations for the distribution libraries were generated using a 3380 device type. Space requirements should be increased or decreased based on the device type in which you are allocating CCS for z/OS and OS/390 Libraries.

CAIVPE Installation Considerations

CAIVPE is an interproduct component used by other CA solutions, such as CA-eMAIL+, CA-IDEAL, and others.

CA-MFLINK Requirements

CA-MFLINK provides mainframe services that support mainframe-to-PC communications for other CA solutions. CA-MFLINK has the following installation requirements:

- CAIVPE Release 4.2.
- CA-MFLINK is used with other CA solutions. The prerequisite system requirements of these solutions meet or exceed the requirements for CA-MFLINK with respect to the environments and operating systems supported by CA-MFLINK.

Library Storage Requirements

The distribution library required for CA-MFLINK is:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.PC42.CPC42LLD	6144	7	1	Distribution Load Library

EARL Service Requirements

The EARL Service has the following installation requirements:

- EARL supports all OS/390 and above operating systems.
- EARL requires CA-Sort, IBM DF/Sort, or a compatible product with the module name SORT.

Library Storage Requirements

The distribution libraries required for EARL are as follows:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.EO61.CEO61LLD	6144	73	3	Distribution Load Library
CAI.EO61.CEO61MLD	3120	21	1	Distribution Macro Library
CAI.EO61.CEO61SLD	3120	12	1	Distribution Source Library

Note: The above space calculations were generated using a 3380 device type. Space requirements should be increased or decreased based on the device type in which you are allocating CCS for z/OS and OS/390 libraries.

SRAM Service Requirements

The SRAM Service supports OS/390 2.5 and above operating systems.

Library Storage Requirements

The distribution library for SRAM Release 7.0 is:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.SR70.CSR70LLD	6144	15	5	Distribution Load Library

Note: The above space calculations were generated using a 3380 device type. Space requirements should be increased or decreased based on the device type in which you are allocating CCS for z/OS and OS/390 libraries.

CA-C Runtime Requirements

CA-C Runtime is supported by the following operating systems:

- CA-Roscoe (ETSO) All releases
- CICS (MVS) Releases 1.7 and higher
- CICS (DOS) Releases 1.5, 1.6, 1.7, and 2.3
- DOS/VSE Release 3.5 at all SP levels
- OS/390 2.5 and higher
- TSO Release 1.3 and higher
- IMS/DC Release 1.3 and higher
- VM/SP-VM/XA Release 1.3 and higher

Library Storage Requirements

The distribution libraries required for CA-C Runtime Release 3.1 are:

Library Name	Block Size	Number of Blocks	Directories	Description
CAIF331.CF331LLD	6144	170	15	Distribution Load Library
CAIF331.CF331SLD	3120	10	2	Distribution Source Library
CAIF331.CF331MLD	3120	1	1	Distribution Macro Library

Note: The above space calculations were generated using a 3380 device type. Space requirements should be increased or decreased based on the device type in which you are allocating CCS for z/OS and OS/390 libraries.

ViewPoint Requirements

ViewPoint 2.0 is supported by the following operating system:

- OS/390 V2R5 and above

Library Storage Requirements

The profile library required for ViewPoint is:

Library Name	Block Size	Number of Blocks	Directories	Description
userid.VPOINT. PROFILE	3120	50	10	ViewPoint Profile and customization library

The distribution libraries required for the ViewPoint base are:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.VPNT.CWC20DLD	8204	190	30	ViewPoint Base Dialog Library
CAI.VPNT.CWC20LLD	6144	250	10	ViewPoint Base Load Library
CAI.VPNT.CWC20PLD	4104	300	90	ViewPoint Base Panel Library
CAI.VPNT.CWC20TLD	3120	30	10	ViewPoint Base Template Library

The distribution libraries required for ViewPoint cBASE are:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.COMN.CIF23LLD	6144	70	10	COMN Load Library
CAI.COMN.CIF23MLD	3120	20	5	COMN Macro Library
CAI.SACX.CAG23LLD	6144	182	20	SACX Load Library
CAI.SACX.CAG23PLD	4104	80	10	SACX Panel Library
CAI.SCAM.CF623LLD	6144	35	2	SCAM Load Library
CAI.SCAM.CF623MLD	3120	13	1	SCAM Macro Library
CAI.SDBS.CSP23LLD	6144	42	5	SDBS Load Library
CAI.SDBS.CSP23MLD	3120	39	5	SDBS Macro Library
CAI.SHLP.CBS23LLD	6144	14	2	SHLP Load Library
CAI.SHLP.CBS23MLD	3120	13	1	SHLP Macro Library
CAI.STMP.CTB23LLD	6144	42	2	STMP Load Library
CAI.STMP.CTB23MLD	3120	13	1	STMP Macro Library

CA PROFILE Requirements

The distribution library required for CA PROFILE is:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.PROFILE.CPP10LLD	6144	15	10	Distribution Load Library

Agent Technology Requirements

The following software is required to run CCS Agent Technology for z/OS and OS/390 on your system:

- OS/390 Release Version 2 Release 5 and above
- OS/390 UNIX System Services (also known as OpenEdition) in full-function mode
- TCP/IP Version 3 Release 2 and above
- IBM C/C++ for OS/390 V2R4M0 or higher if you are using the example agent or writing your own custom agents
- Language Environment for OS/390 V1R7M0 and above. Agent Technology must be installed on a system with a release of LE that is compatible with the LE version your target system runs.
- Security definitions permitting a new Agent Technology user to be created.

TCP/IP Requirements

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.
 - Ensure that the following data sets exist and are cataloged to accompany your other TCP/IP data sets:


```
ETC.SERVICES
HOSTS.ADDRINFO
HOSTS.SITEINFO
```
3. Note the TCP/IP data set name from the //SYSTCPD DD statement.
4. Enable “uplow” support on all terminals that will be used during the installation.

Library Storage Requirements

The distribution libraries required for Agent Technology are:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.DISTLOAD	6144	1050	10	Backup load library
CAI.DISTSRC	25600	375	5	Backup source library

CA-Datacom/TR Requirements

CA-Datacom/TR has the following prerequisite requirements:

- OS/390 Version 2.5 and above
- Approximately 500K of ECSA

SVC (Supervisor Call)

During CCS for z/OS and OS/390 installation, you need to allocate an unused SVC number to be used by CA-Datacom/TR. If you are already a CA-Datacom client, it is possible that the existing CA-Datacom SVC may also be used to support CA-Datacom/TR. However, since the CA-Datacom/TR environment may be maintained at a different release than the existing CA-Datacom environment, we strongly recommend the assignment of a different SVC for CA-Datacom/TR.

The SVC must be established prior to starting the Multi User Facility (MUF). The base module for the SVC operation is provided in the TR libraries. When you install CCS for z/OS and OS/390, CAIRIM is utilized to load this SVC code into the selected z/OS SVC number. This CAIRIM job needs to be re-executed after each system IPL to re-establish the CA-Datacom/TR SVC. More information on the SVC is provided in the *CA-Datacom/DB Database Administrator* guide. The default selections for SVC and SUBID are SVC 246 and SUBID 0.

Library Storage Requirements

The minimum storage requirements for the permanent libraries required to run CA-Datcom/TR are:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.CAILIB	6144	3000	90	Common Load Library
CAI.CAIMAC	3120	1500	10	Common Macro Library
CAI.CXX	4096	1200	0	CA-Datcom/TR Directory
CAI.PXX	4096	2000	0	Statistics and Diagnostics Area
CAI.LXX	8192	3000	0	Logging Area
CAI.IXX001	3860	30	0	Index for Sample Database
CAI.PAY001	4096	15	0	Sample Data Area
CAI.PMF001	4096	15	0	Sample Data Area
CAI.DEM001	4096	30	0	Sample Data Area
CAI.IXX002	3860	2400	0	Datadictionary Index
CAI.ALL002	4096	7200	0	Datadictionary Area
CAI.IXX006	3860	720	0	CBS/SAAT Index
CAI.IXX015	3860	350	0	Data Definition Directory Index
CAI.DDD015	4096	775	0	Data Definition Data Area
CAI.SIT015	4096	175	0	DDD Schema Information Data Area
CAI.MSG015	4096	110	0	DDD Message Data Area
CAI.IXX016	3860	34	0	SQL Default Index
CAI.SQ1016	4096	82	0	Data Default Data Area
CAI.IXX017	3860	15	0	SQL Temporary Table Manager Index Area

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.TTM017	4096	1050	0	SQL Temporary Table Manager Data Area
CAI.IXX1000	3860	15	0	Dynamic System Tables Index Area
CAI.SYS1000	4096	15	0	Dynamic System Tables Data Area
CAI.IXX1008	300	50	0	Discovery Trigger Table Index Area
CAI.TA01008	130	60	0	Discovery Trigger Table Data Area 0 (base)
CAI.TA11008 to CAI.TA91008	130	60	0	Discovery Trigger Table Data Areas 1-9
CAI.IXX1009	750	50	0	Discovery Non-Trigger Table Index Area
CAI.TN01009	130	60	0	Discovery Non-Trigger Table Data Area
CAI.TN11009 to CAI.TN91009	130	60	0	Discovery Non-Trigger Table Data Areas 1-9
CAI.IXX1010	75	25	0	Discovery In-flight Table Index Area
CAI.IF01010	110	50	0	Discovery In-flight Table Data Area
CAI.IXX1011	175	50	0	Event Management Table Index Area
CAI.EM01011	375	50	0	Event Management Table Data Area

The distribution libraries required by CA-Datcom/TR are:

Library Name	Block Size	Number of Blocks	Dirs.	Description
CAI.CUSLIB	6144	500	5	Customized Executable Modules
CAI.CAD90LLD	6144	700	50	Distribution Load Library
CAI.CAD90MLD	3120	400	50	Distribution Macro Library
CAI.CAD90SLD	3120	20	10	Distribution Source Library
CAI.CBD90LLD	6144	700	40	Distribution Load Library
CAI.CBD90MLD	3120	700	5	Distribution Macro Library
CAI.CVE90LLD	6144	500	5	Distribution Load Library
CAI.CVE90MLD	3120	250	5	Distribution Macro Library
CAI.CVT30LLD	6144	70	5	Distribution Load Library
CAI.CVT30MLD	3120	25	5	Distribution Macro Library

CA-L-Serv Requirements

CA-L-Serv supports OS/390 2.5 and above releases.

Prior Installations of CA-L-Serv

The current CA-L-Serv comprises the following sysmod:

CHJ3500: CA-L-Serv

If SMP was previously used to install older releases or an older genlevel of L-Serv, L-Comm, or XPErtware (alternate product names) prior to this installation, you should consider using a different SMP environment.

Optionally, you may execute the SMP clean-up jobs provided in the CA-L-Serv SAMPJCL library to delete any SMP objects created by the prior installation of the above products.

XCF Communications Considerations

If you plan to use XCF communication between systems, ensure that you have installed CAIRIM (CS91000) at genlevel 9706 or higher 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

1. CA-L-Serv must reside in an authorized load library.
2. If CA-L-Serv and Common Services (formerly CA90s) reside in different load libraries (because each had been previously installed), note the following information:
 - Both CAILIBs 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 CAILIB.
 - The Common Services CAILIB must be accessible to CA-L-Serv from either 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	3K of CSA and 2K of extended CSA
ESQA	Requirements vary from 4K to over 500K depending on the size and number of VSAM buffer pools

Notes:

1. 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).
2. ESQA storage is used by VSAM and concerns only users of the File Server.

Library Storage Requirements

The distribution libraries required for CA-L-Serv are:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.HJ35.CHJ35LLD	6144	1675	45	CAI load library
CAI.HJ35.CHJ35SLD	3120	225	5	CAI source library

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 will vary depending on the requirements of your site.

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

CA-GSS Requirements (System Interfaces)

CA-GSS has the following installation requirements:

- CA-GSS runs on any OS/390 R2V5 and above processor. All releases of OS/390 R2V5 and above are supported.
- 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 if so desired. CA-GSS is installed into the common CAI.CAILIB.
- Due to cross-memory communication requirements, CA-GSS makes itself non-swappable.
- Since CA-GSS services multiple applications and tasks, CA-GSS' dispatching priority must be greater than or equal to the highest dispatching priority for any tasks requesting CA-GSS services.

Memory Requirements

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

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

The types of memory are described in more detail in the following sections.

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
- 23.6K 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 Computer Associates products, the operating system, VTAM, or other entities is not included.

- 3MB (minimum) private storage. Except for I/O buffers and interfaces to some external routines, this storage will all reside above 16 megabytes.
- 160 bytes of CSA for a subsystem anchor and related storage.
- 120K 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.

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

ISERVE Memory

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

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

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. This block, whether predefined by the installation or dynamically obtained, is retained until the next IPL. It is, however, reclaimed upon each ISERVE restart.

Each Computer Associates 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 upon the options you choose and the amount of traffic on your system. The recommended starting point is 4 megabytes.

Resource Consumption

Depending upon installation-controlled tracing options, significant SPOOL space may be used. However, 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 will minimize this possibility.

Library Storage Requirements

The distribution libraries required for CA-GSS are:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.JD41.CJD41LLD	6144	60	5	Distribution GREXX Object Library
CAI.YS28.CYS28CLD	3120	30	1	Distribution CA-GSS CLIST Library
CAI.YS28.CYS28LLD	6144	3000	100	Distribution CA-GSS Object Library
CAI.YS28.CYS28MLD	3120	10	1	Distribution CA-GSS Message Library
CAI.YS28.CYS28OPT	3120	85	4	Distribution CA-GSS Option Library
CAI.YS28.CYS28PLD	3120	270	20	Distribution CA-GSS Panel Library
CAI.YS28.CYS28SAI	3600	40	2	Distribution CA-GSS Sample IMOD Library
CAI.YS28.CYS28SYI	3600	810	11	Distribution CA-GSS System IMOD Library

Permanent VSAM ISET libraries required for CA-GSS are:

ISET Library Name	Cyls	Description
CAI. SAMPIMOD	1	Distribution GREXX Object Library
CAI. SYSIMOD	4	Distribution CA-GSS CLIST Library

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 upon 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 either 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 *very* limited in scope. See the *CA Reference Guide* for detailed information on CA-GSS initialization parameters.

CA-GSS' User ID

Many installations routinely do not assign a specific user ID to started tasks. Computer Associates highly recommends that you do 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 what user ID to use. For example, this can happen if a started task which 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

Here is additional information on how CA-GSS determines what user ID an IMOD executes under:

Type of IMOD	How CA-GSS Determines the User ID
IMODs that support operator commands	<ol style="list-style-type: none"> 1. If you have defined a user ID through the COMMAND parameter in the PARMLIB data set, CA-GSS uses it. 2. Otherwise, CA-GSS uses its default user ID.
IMODS triggered by WTOs	<ol style="list-style-type: none"> 1. If you have defined a user ID through the WTO parameter in the PARMLIB data set, CA-GSS uses it. 2. If not, CA-GSS tries to determine and use the user ID of the WTO issuer. 3. As a last resort, CA-GSS uses its default user ID. <p>Note: During execution, an IMOD task may switch user IDs by supplying a new user ID and its associated password to the SECURITY() function.</p>
WTO-triggered IMODs with ASID numbers matching those on the MONITOR command	<ol style="list-style-type: none"> 1. CA-GSS tries to determine and use the user ID of the WTO issuer. 2. Otherwise, CA-GSS uses its default user ID.
IMODs supporting the Logon Facility	<ol style="list-style-type: none"> 1. If a user ID and password are provided, CA-GSS uses them. 2. Otherwise, CA-GSS uses its default user ID.

Type of IMOD	How CA-GSS Determines the 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-XPS Requirements

CA-XPS (Cross-Platform Scheduling Common Component) provides CA-7, CA-Scheduler, and CA-Jobtrac 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, the CA-XPS code executes in the CA-GSS address space.

For information on implementing cross-platform scheduling using CA-XPS, please see one of the following publications:

- *CA-7 Interfaces Guide*
- *CA-Scheduler Interfaces Guide*
- *CA-Jobtrac Installation and Maintenance Guide*

Library Storage Requirements

The distribution library required for CA-XPS is:

Library Name	Block Size	Number of Blocks	Directories	Description
CAI.CJE10LLD	6144	32	4	Distribution Load Library

Installation Dependencies

The CCS for z/OS and OS/390 tape contains a wide array of FMIDs (functional sysmods). You may or may not need all of them installed. The need for a particular component depends on what CA products are installed or will be installed. Check your individual product documentation to determine which ones are required.

The FMIDs that should be RECEIVED (and later applied and accepted), as they pertain to each of the installable components, are listed in the following tables.

Component	FMIDs	Also Need FMIDs
Event Management - Event Management for OS/390 and z/OS.	CTN2221	CS91000, CW11000, CF33100, CW21000, CW41100, CWU4200, and CTN2220
Event Management Common	CTN2220	none
CAIRIM - The CA Resource Initialization Manager.	CS91000	none
CAIENF - The CA Event Notification Facility.	CW11000	CS91000 and CW21000
CAIENF/DB	CW21000	none
CAIENF/Extract - The CA Event Notification Extract Facility.	CW11001	CS91000, CW11000, CW21000, and CW41100
CAIENF Utilities - The CA tools package for CAIENF.	CW11002	CW11000, CW21000, CF33100, and CF62300
If using the ENFC facility		CW11001 and CW41100
CAIENF/CICS - The CA CICS Interface.	CW31000	CS91000, CW11000, and CW21000
CAIENF/CICS SPAWN - The CA CICS Interface.	CW31001	CS91000, CW11000, CW21000, CW41100, and CW31000

Component	FMIDs	Also Need FMIDs
CAICCI - The CA Common Communications Interface.	CW41100	CS91000, CW11000, and CW21000
CAIENF/USS - The CA UNIX Systems Services interface.	CRR1000	CS91000, CW11000, and CW2100
CAIENF/DB2 - The CA DB2 Interface. This service consists of a series of programs that contain DB2 release dependencies.	CW51000	CS91000, CW11000, and CW21000
CA-C Runtime - The CA C Language Runtime Facility.	CF33100	none
EARL Service - The CA Easy Access Report Language Reporting Service.	CXE6100	none
SRAM Service - The CA Sort Reentrant Access Method Service, Release 7.0.	CSR7000	none
CAIVPE - The CA Interproduct Service for CAIVPE 4.2.	CWU4200	none
CA-MFLINK - Communication link enabling mainframe-to-PC communications.	CPC4200	CWU4200
CA PROFILE - The CA Common Profile Program. The CPP1000 function should be RECEIVED regardless of which Common Services you are installing.	CPP1000	none
ViewPoint - User Interface to CA system solutions.	CWC2000	CIF2300, CAG2300, CSP2300, CF62300, CTB2300, CBS2300, and CF33100

Component	FMIDs	Also Need FMIDs
cBASE COMMON - Subsystems common to CA solutions used for variable initialization, database access, and so on.	CIF2300	CS91000 and CF33100
cBASEX - The runtime driver for CA-solution cBASE dialogs.	CAG2300	CS91000, CF33100, CIF2300, CTB2300, CBS2300, CF62300, and CSP2300
WorldView - The Real World Interface and GUI for Enterprise Management.	CTN2223	CTN2220 and CTN2221
Agent Technology - Support for various Agents.	CID2200	none
CA-SQI - Software that supports various CA solutions in conjunction with CA-Datcom/TR.	CSP2300	CF33100
CA-TEMPLATE - Software that supports various CA solutions.	CTB2300	CF33100
CA-MAPPER - Software that supports various CA solutions.	CF62300	CF33100
CA-HELP - Software that supports various CA solutions.	CBS2300	CF33100
CA-GSS - Communications interface used by various CA solutions.	CYS2800	CJD4100
CA-L-Serv - Services used by various CA solutions.	CHJ3500	CS91000
CA-XPS - Cross-platform scheduling common component	CJE1000	CW11000, CW21000, and CW41100
CA-GREXX - A REXX execution environment used by various CA solutions.	CJD4100	none

Note: FMID CPP1000, CA-PROFILE, is not unique to the CCS for z/OS and OS/390 tape. It consists of a series of programs that generate documentation that is used for problem determination.

If any of the Common Services have been previously installed, you must perform one of the following actions. Both actions require that the services be ACCEPTed.

- Install cumulative maintenance against the function.
- Reinstall the function.

If the services are not being reinstalled, remove them from the RECEIVE SELECT list.

Installing CCS for z/OS and OS/390

Now that you have reviewed the system requirements and determined which components to install, you are ready to proceed with the installation. Installation checklists and worksheet are provided in appendixes.

Installation Steps

The following installation information is included in this guide:

- All the steps of a complete install are listed here.
- The Installation Checklist appendix discusses each component separately, with a list of the steps required to install that component.
- The Worksheet appendix provides a general worksheet to keep track of the different values used in the install.

Step 1. Visit the Support Page

Note: This step is required for all components

The Support page contains any additional information that will aid in installing and running CCS for z/OS and OS/390. In addition to any new maintenance that may be available, each component has an FAQ and other technical information. The URL is <http://esupport.ca.com/>. Select CCS for z/OS and OS/390 from the product list.

Step 2. Load Installation Sample JCL Library

Note: This step is required for all components.

CCS for z/OS and OS/390 installs through SMP/E. The solution tape received with this package contains all the necessary data to install and execute CCS for z/OS and OS/390. It is a standard label 3480 IDRC tape. Prior to installing the solution, you should load the sample JCL library from tape. This is the ninth file, DSN=CAI.SAMPJCL, on the tape, and it is in IEBCOPY unload format. Use the following JCL as a model to load the sample JCL library to DASD.

Note: The CCS for z/OS and OS/390 CAI.SAMPJCL data set contains both installation and maintenance JCL members.

```
//LOAD      EXEC PGM=IEBCOPY
//SYSPRINT DD  SYSOUT=*
//SYSUT1    DD  DISP=OLD,
//          DSN=CAI.SAMPJCL,
//          UNIT=TAPE,                <=== generic 3490 tape
//          VOL=SER=W0rrsp,
//          LABEL=(9,SL),
//          DCB=DCB=4
//SYSUT2    DD  DISP=(NEW,CATLG,DELETE),
//          DSN=CAI.SAMPJCL,          <=== your DSN
//          UNIT=SYSDA,               <=== your generic DASD
//          VOL=SER=.....,           <=== permanent DASD volser
//          SPACE=(3120,(800,25,50)), <=== minimum space required
//          DCB=(LRECL=80,BLKSIZE=3120,RECFM=FB)
//SYSUT3    DD  UNIT=SYSDA,SPACE=(CYL,(3,3))
//SYSUT4    DD  UNIT=SYSDA,SPACE=(CYL,(3,3))
//SYSIN     DD  *
            COPY      INDD=((SYSUT1,R)),OUTDD=SYSUT2
//
```

Once this job has ended, your library contains all of the JCL needed to complete the installation of CCS for z/OS and OS/390. In order to satisfy your data center needs, certain tailoring of JCL is necessary while executing the steps on the following pages. See the Installation Worksheet completed in Step 5 to obtain values for the various JCL parameters.

Step 3. Download BookManager Files

Note: This step is optional.

To download the documentation provided in BookManager format, use SAMPJCL member W010BMGR.

Step 4. Download PDF Files

Note: This step is optional.

The documentation is also provided in PDF format. To download the PDF files, use SAMPJCL member PDFDOWNL.

Step 5. Review System Requirements

Note: This step is required for all components.

Be sure that you have reviewed the system requirements to ensure that all the requirements are met before installing CCS for z/OS and OS/390. See the chapter “System Requirements” in this manual for more information. Be sure to check the section Installation Dependencies as well; you may need to install or maintain additional services.

Step 6. Complete the Installation Worksheet

Note: This step is required for all components.

A CCS for z/OS and OS/390 installation worksheet is provided in an appendix to this guide. It is designed to simplify modifying the supplied JCL.

Answer each question on the worksheet, filling in the blanks with the appropriate information. Default values are noted, so if the default value is acceptable, leave the item blank on the worksheet. However, you must supply appropriate volume serial numbers.

Once you have completed the worksheet, you can use it as a reference while performing the remaining installation steps.

Step 7. Modify SAMPJCL Member JOBCARD

Note: This step is required for all components.

Edit the member JOBCARD to conform to your installation standards. Modify the JCLLIB statement to point to your SAMPJCL data set. This member will then be used for the remaining jobs. If you need to add SETUP cards for tape mounts, you may want to create a separate member for those jobs.

Step 8. Modify SAMPJCL Member TNGVARS

Note: This step is required for all components.

Edit the member TNGVARS to conform to your installation standards. This member will be included as part of the JOBCARD member updated in the previous step. The member TNGVARS will set variables that will be used in the remaining members.

Use the worksheet that was filled in previously to make any changes.

Step 9. Allocate Target and Distribution Libraries

Note: This step is required for all components.

SAMPJCL member W010ALC allocates the target libraries required by CCS for z/OS and OS/390 and the service-specific distribution libraries during installation and maintenance. However, many CA solutions have common services and common libraries that may have already been installed. Therefore, careful analysis must be done not to allocate duplicate libraries.

Edit the JCL to conform to your installation standards and the previously completed worksheet. However, never change any of the DD names or the last qualifier of the data set names.

All space allocations are given in blocks to allow for compatibility between DASD types. The allocations given are the minimum required for installing CCS for z/OS and OS/390. You may want to adjust these values for your installation device types, and to allow enough free space for maintenance (the more free space you allocate, the less often it is compressed during maintenance). For common libraries already present, be sure there is sufficient space for CCS for z/OS and OS/390.

Note: Depending on which CCS for z/OS and OS/390 components you selectively choose to install (and not to install), some distribution libraries may not be required. Allocate only those distribution libraries that pertain to the CCS for z/OS and OS/390 you are installing. The distribution libraries for each service are listed separately in the chapter “System Requirements” under each service heading.

Step 10. Allocate Private SMP/E Libraries

Note: This step is required for all components.

***Important!** If you have already created an SMP environment, you may need to allocate the SMPLTS data set. This data set is required for Agent Technologies and Event Management.*

SAMPJCL member CAINITE5 may be used to allocate and initialize private SMP data sets for all CA solutions. This is recommended to keep Computer Associates solutions as distinct entities from other SMP data sets. This member also sets up CAI global, target, and distribution zones for CA solutions.

Step 11. Set Up Environment to Use SMP DDDEFs

Note: This step is required for all components.

The CCS for z/OS and OS/390 SMP environment uses SMP DDDEFs. SAMPJCL member W010DDEF is provided for this purpose. Edit this job so that the DDDEFs match the data set allocations from Step 9 and Step 10.

Step 12. Set Up Event Management and WorldView SMP DDDEFs

Note: This step is required for Event Management and WorldView.

The Event Management and WorldView SMP environment uses SMP DDDEFs instead of DD statements. SAMPJCL member TNGDDDEF is provided to update the CSI with the correct data set names. Edit this job so that the DDDEFs match the data set allocations in the W010ALC job from Step 7 and the install path you plan to use for the PATH DDDEFs.

Step 13. Allocate Event Management and WorldView HFS

Note: This step is required for Event Management and WorldView.

To allocate a new HFS for Event Management and WorldView, member TNGHFS can be used. You may use an existing HFS if desired; however, using a separate HFS will ease the change to an upgraded version.

Important! *The HFS needs to be mounted read/write before continuing further. SAMPJCL member HFSMOUNT can be used to mount the HFS.*

This is a good time to update your BPXPRMxx member to also include the mount point, so subsequent IPLs will mount the HFS automatically.

Step 14. Create Event Management Directories

Note: This step is required for Event Management and WorldView.

This step creates the directories used to install Event Management and WorldView components. SAMPJCL member TNGMKDIR is used to create the directories.

The output from this job is an HFS file in the STDOUT DD statement.

Step 15. Create Event Management and WorldView Profile

Note: This step is required for Event Management and WorldView.

The running of Event Management and WorldView depends on the setting of various environment variables. SAMPJCL member TNGPROF creates a profile member in the install directory to set these variables. Modify the variables to match your installation standards.

- TNGNAMESERVERIPADDRESS - The IP address for the DNS used on the install machine. Issue a nslookup command and use the Address that is associated with the Server name for your DNS.
- TNGHOSTNAME - The IP hostname for the install system.
- TNGHOSTIPADDRESS - The IP address for the install system.
- TNGDEFAULTROUTE - Is the device name that TCPIP uses. To obtain the device name, issue a netstat -r command and look for the entry that contains either default or defaultnet, depending on which level of the OS you are running. The interface column contains the device name.
- TNGDEFAULTGATEWAY - Is the gateway address. Using the same output from the netstat -r command, use the Gateway that matched the device used for TNGDEFAULTROUTE.
- INSTALLSAF - Indicate, by specifying yes or no, if Store and Forward should be active.
- UPDATE_ETC - Indicate, by specifying yes or no, if /etc/profile should be updated to set the environment variables required to run TNG commands.

Step 16. Modify SAMPJCL Member AGNTVARS

Note: This step is required for Agent Technologies.

Edit the member AGNTVARS to conform to your installation standards. This member will be included as part of the JOBCARD member updated in Step 7. The member will set variables that will be used in the remaining members.

Use the worksheet that was filled in previously to make any changes.

Step 17. Create Agent Technologies Install Directory

Note: This step is required for Agent Technologies.

If the directory already exists, you can skip this step.

Edit the SAMPJCL member AINSTJ01 to create the directory that will be used to install Agent Technologies. If you will be using a separate HFS for Agent Technologies, this HFS can also be used as the mount point.

Step 18. Initialize SMP/E for Agent Technologies

Note: This step is required for Agent Technologies.

Agent Technologies requires different link-edit parameters than the other components. To allow for this, SAMPJCL member AINSTJ02 will create a new SMP OPTIONS member. This will be referred to when the APPLY and ACCEPT steps are run.

Step 19. Agent Technologies Downloads

Note: This step is required for Agent Technologies.

This step downloads files from the tape that are used by Agent Technologies.

SAMPJCL member AINSTJ03 is provided to download these files.

Step 20. Event Management and WorldView Downloads

Note: This step is required for Event Management and WorldView.

This step downloads files from the tape that are used by Event Management and WorldView. SAMPJCL member TNGDOWNL is provided to download these files.

Step 21. RECEIVE CCS for z/OS and OS/390

Note: This step is required for All components.

SAMPJCL member W010REC RECEIVES all of the service FMIDs (functional sysmods) of CCS for z/OS and OS/390. Edit the JCL to conform to your installation standards and the previously completed worksheet. Select only the sysmods that are required.

If other CA solutions have been installed, some of these functions may already have been received. If this is the case, SMP may re-receive the sysmods. Therefore, you should be aware that not all sysmods RECEIVED are later ACCEPTed. Failing sysmods should be removed and the job resubmitted.

Step 22. Copy and Modify the EARL Option Source Member

Note: This step is required for EARL.

SAMPJCL member XE61COPY copies the EARL Service option source from file 40 of the CCS for z/OS and OS/390 tape to the OPTLIB data set. Modify the sample JCL to conform with the standards of your data center and the CCS for z/OS and OS/390 installation worksheet.

It may be necessary to modify the EARL Reporting Service options source member EARLOPT in the CAI.PPOPTION data set. If modifications are necessary, they must be made to this member before the SMP APPLY step is executed.

If modifications need to be made after the APPLY has been executed, see SAMPJCL member XE61OPT. Submit this job to assemble and re-link the customized CA-EARL options member.

For complete information pertaining to the EARL default options, see the *CA-EARL Systems Programmer Guide*.

Step 23. Prelink Agent Technologies

Note: This step is required for Agent Technologies.

To resolve the LE requirements, a prelink must be run. The output for this job is used as input for the APPLY step. SAMPJCL member AINSTJ04 is used to complete the prelink.

Step 24. Create Userid for Agent Technologies

Note: This step is required for Agent Technologies.

The Agent Technologies jobs should be run using one user ID. This user ID should have an OMVS segment defined so that the home directory is the same as the install path for Agent Technologies. SAMPJCL member AINSTJ05 will create this user ID if desired. The job provides ACF2, RACF, and CA-Top Secret control statements.

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

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

Step 25. Allocate Agent Technologies HFS

Note: This step is required for Agent Technologies.

To allocate a new HFS for Agent Technologies, member AINSTJ06 can be used. You may use an existing HFS if desired; however, using a separate HFS will facilitate an upgrade by allowing you to swap HFS files.

***Important!** The HFS needs to be mounted read/write before continuing further. SAMPJCL member HFSMOUNT can be used to mount the HFS.*

This is a good time to update your BPXPRMxx member to include the mount point so subsequent IPLs will mount the HFS automatically.

Step 26. Update INSTPAX member

Note: This step is required for Agent Technologies.

Update SAMPJCL member INSTPAX. Change AWORKDIR to the install path for Agent Technologies.

Step 27. Expand Agent Technologies Tarfile

Note: This step is required for Agent Technologies.

The Agent Technology directory structure is created by expanding a tarfile. The file was downloaded earlier by member AINSTJ03. The expand will also create several HFS files. To expand the tarfile, use member AINSTJ07. Edit the agentworks.profile member to match your installation:

Change to your MVS HLQ:

```
AWORKS_MVS_PREVIX=CAI
```

Change to your install path:

```
AGENTWORKS_DIR=/cai/agent
```

Change to your TCPIP SYSTCPD file:

```
RESOLVER_CONFIG='/' tcpip.tcpip.data'
```

Step 28. APPLY CCS for z/OS and OS/390

Note: This step is required for all components.

SAMPJCL member W010APP applies all the services (functional sysmods) of CCS for z/OS and OS/390 to the Target libraries. Edit the JCL to conform to your installation standards and the previously completed worksheet. Select only the sysmods that are required.

If other CA solutions have been installed, some of these functions may already have been applied. If this is the case, a non-zero return code occurs. Remove any failing sysmods and resubmit the job. SMP/E users have the option of specifying REDO on the APPLY command statement to re-APPLY the function only if in the previous step the function had been reinstalled.

Modify the APPLY SELECT list accordingly. Submit the job and verify that the APPLY processing ran successfully.

If SMP APPLY completes with a return code greater than 4, perform the following tasks:

1. Review the output carefully before continuing.
2. Correct the problem.
3. Resubmit the job.

Note: A return code of 8 from the linkage editor is normal when APPLYing a new function and can be disregarded.

Step 29. Set Mode Bits for Agent Technologies

This step is required for: Agent Technologies

To allow updates to the Agent Technologies files by the other agents, the file mode bits need to be set. SAMPJCL member AINSTJ09 is used to do this.

Step 30. Set userid Mode Bit for Agent Technologies

Note: This step is required for Agent Technologies.

Certain programs in Agent Technologies need to run with the owner of the Agent Technology files. SAMPJCL member AINST10 is used to set the user ID bit.

Step 31. APF Authorize the CAILIB Data Set

Note: This step is required for CAIRIM, CAIENF and CA-GSS.

Some of the later steps require the CAILIB to be APF authorized. Failure to do so will result in the job not completing correctly or abending.

Step 32. Define or Upgrade the CAIENF Database

Note: This step is required for CAIENF.

To define the CAIENF database, you must begin by calculating its space requirements. The amount of disk space required by CAIENF for its database depends on several factors. A rough estimate of the space requirements can be calculated using the following formula:

$$\text{Space in cylinders} = (A * B / C) + 10$$

Where:

A = Total number of logged events per day

B = Desired retention period in days

C = Device constant:

For 3380, use 3000

For 3390, use 3600

Determine the values for A, B, and C as they pertain to your data center, and calculate the number of cylinders needed. Keep in mind, when determining the value for A, only events that are defined to be logged are written to the CAIENF database.

SAMPJCL member ENFDBINT allocates and initializes the CAIENF database. Modify member ENFDBINT as required for your data center. Install only the DCM modules for the components being installed.

The following SHARE operand indicates whether the same DB is to be used across systems. If recording is required, the DB should not be shared.

* Initialize the DB

```
INIT DB(ENFDB) SHARE(NO | YES)
```

* Install the base DCM module - Required

```
INST DB(ENFDB) ID(CAS9DCM0)
```

Notes:

1. If you are upgrading an existing DB, comment out the above two statements.
2. If ENF is active, you must change the DB(ENFDB) to DB(*) to protect the integrity of the DB. The ENFDB DD statement should also be commented out.
3. The CAILIB also needs to be APF authorized to prevent a S047 abend.

Step 33. Allocate CA-Datcom SMP/E and Database Data Sets

Note: This step is required for Event Management and WorldView.

SAMPJCL member TRINS02 will allocate the libraries required for Datcom/TR.

Datcom/TR is used as the repository for CCS for z/OS and OS/390.

Step 34. Load CA-Datcom SMP/E Libraries

Note: This step is required for Event Management and WorldView.

SAMPJCL member TRINS03 will create the SMP/E environment for Datcom/TR. This is used as the repository for CCS for z/OS and OS/390.

Step 35. Rename SMP/E DDDEFs

Note: This step is required for Event Management and WorldView.

The CSI that was downloaded needs to be changed to point to your libraries. SAMPJCL member TRINS04 will change the DDDEFs to make this happen.

Step 36. ASSEMBLE/LINK Custom Modules

Note: This step is required for Event Management and WorldView.

SAMPJCL member TRINS05 will cause the creation of several modules. The job will assemble and link several modules into the CA-Datcom/TR CUSLIB library.

Step 37. Customize TNG

Note: This step is required for WorldView.

The CA-Datcom CUSMAC library member TNGPARM contains the startup options for the trigger server. Update the LIBPATH environment variable to include the installation path used for WorldView.

Step 38. Install CA-Datcom SVC

Note: This step is required for Event Management and WorldView.

Datcom/TR requires that its SVC be installed before it can be used. SAMPJCL member TRINS06 uses CAIRIM to install the SVC.

Step 39. Load CA-Datcom Databases from Tape

Note: This step is required for Event Management and WorldView.

SAMPJCL member TRINS07 is used to pre-load the Database files with all the required tables and initialization records.

Step 40. Start Up MULTI-USER

Note: This step is required for Event Management and WorldView.

SAMPJCL member TRINS08 will start Datcom/TR. It needs to be up for the next job to complete successfully.

Step 41. Reset HSD File

Note: This step is required for Event Management and WorldView.

The next job will perform some housekeeping chores to allow the database to be used after the load. SAMPJCL member TRINS09 is used to perform this task.

Step 42. Back Up CXX AND DATADICTONARY

Note: This step is required for Event Management and WorldView.

SAMPJCL member TRINS10 will be used to create a backup of the database file for future use.

Step 43. Shut Down MULTI-USER

Note: This step is required for WorldView.

SAMPJCL member TRINS11 is used to shut down Datacom/TR.

Step 44. Start Up Datacom/TR with the Trigger Server

Note: This step is required for WorldView.

Task 44a. Start Up CAIENF and CAICCI

If CAIENF and CAICCI are not already active on the system, you must first start CAIENF. CAICCI runs as a subsystem within the CAIENF address space. Follow the CAIENF and CAICCI Post-Installation tasks for instructions on how to customize CAIENF and CAICCI and then to finally start CAIENF.

Task 44b. Start Up Datacom/TR with the Trigger Server

If WorldView is being installed, the next job requires that the trigger server be active. SAMPJCL member TRINSTRG will start Datacom/TR with the trigger server.

Step 45. Create Links for Event Management

This step is required for: Event Management

SAMPJCL member TNGBLDEM will create the links required for Event Management.

Step 46. Create Links for WorldView

Note: This step is required for WorldView.

SAMPJCL member TNGBLDWV will create the links required for WorldView.

Step 47. Shut Down the Trigger Server

Note: This step is required for Event Management and WorldView.

SAMPJCL member TRGSTOP will shut down the trigger server.

Step 48. Shut Down MULTI-USER

Note: This step is required for WorldView.

SAMPJCL member TRINS11 is used to shut down Datacom/TR.

Step 49. Link-Edit CAICCI 1.1 for TCP/IP

Note: This step is required for CAICCI.

This task is required if you are installing, or have installed, CAICCI Release 1.1 using TCP/IP as one of your communications protocols.

Task 49a. For IBM TCP/IP Users with LE/370 Runtime

The CAICCI support of TCP/IP is provided as four modules: CAS9CTGU, CAS9CTSU, CAS9CTLU, and CAS9CTPU. These modules make up the TCP/IP feature and are packaged as part of the CAICCI 1.1 FMID. The JCL needed to link the load modules is found in member W010LINK in CAI.SAMPJCL.

If you have already installed IBM TCP/IP for z/OS and can link the CAICCI TCP/IP modules into an existing APF authorized or LNKLST data set, you are ready to run the CAICCI TCP/IP feature; no IPL is required following the installation.

Task 49b. For IBM TCP/IP Users that Do Not Have LE/370 Runtime

A SAS C supported version of the TCP/IP server modules for CAICCI is provided.

SAMPJCL member W010SASL can be used to download the SAS C file.

Task 49c. For CA-TCP/Access TCP/IP V3.1 and V4.1 Users Only

The CAICCI support of TCP/IP is provided by four modules: CAS5I3GM, CAS5I3SM, CAS5I3PM, and CAS5I3LM. These modules make up the TCP/IP feature and are packaged as part of the CAICCI Release 1.1 FMID.

If you have already installed CA-TCP/Access TCP/IP for z/OS into an existing APF authorized or LNKLST data set, you are ready to run the CAICCI TCP/IP feature; no IPL is required following the installation.

Task 49d. Configure the CCITCP Started Task

The CAICCI implementation of TCP/IP uses a discrete z/OS address space to run a multi-user TCP/IP server for PC-to-HOST connectivity. Choose the proper CAIPROC member based on your TCPIP vendor and C Runtime choice.

- The JCL needed to run the CAICCI TCP/IP server using IBM TCP/IP with LE/370 Runtime is found in CAI.CAIPROC member CCITCP.
- The JCL needed to run the CAICCI TCP/IP server using IBM TCP/IP with the SAS C Runtime in lieu of the IBM C Runtime is found in CAI.CAIPROC member CCITCPS.
- The JCL needed to run the CAICCI TCP/IP server using CA-TCP/Access TCP/IP V3.1 and V4.1 is found in CAI.CAIPROC member CCITCPI3.

Step 50. Link-Edit ENF SNMP Monitor

Note: This step is required for CAIENF.

This task is required if you are installing the ENF SNMP Monitor using TCP/IP as one of your communications protocols. The link-edit job used will depend on the C Runtime being used.

- For IBM TCP/IP users that have C/370 or LE/370 Runtime installed:

The SNMP support of TCP/IP is provided as one object module, CAS9TRAI, and one load module, CAS9TRAP. The JCL needed to link the load module is found in SAMPJCL member SNMPLINK.

- For IBM TCP/IP users that do not have IBM C/370 and LE/370 Runtime:

The SNMP support of TCP/IP is provided as one object module, CAS9TRPS, and one load module, CAS9TRAP. The module, CAS9TRPS, has been prelinked with the SAS C and sockets library. To complete the build, an additional linkedit is required. The JCL needed is found in SAMPJCL member SNMPSASL. Edit the member to conform to your site standards and submit the JCL.

The module requires access to the SAS C Runtime library using a STEPLIB concatenation or LINKLST. If your site does not have the SAS C Runtime library release 6.0 or greater installed, a copy may be obtained from the CCS for z/OS and OS/390 tape. The JCL needed to load the SAS C Runtime library is found in SAMPJCL member W010SASL.

Step 51. Establish Site Defaults for CA-C Runtime

Note: This step is required for CA-C.

Add the PCT entries required for CA-C Runtime. These entries are defined in SAMPJCL member F331PCTR, which is the CICS RDO JCL for defining the CA-C/Runtime 3.1 tasks.

Add the PPT entries required for CA-C Runtime. These entries are defined in SAMPJCL member F331PPTR, which is the CICS RDO JCL for defining the CA-C/Runtime 3.1 tasks.

Step 52. Allocate the ViewPoint Profile

Note: This step is required for ViewPoint.

SAMPJCL member WC20PROF allocates the ViewPoint profile library. Edit this JCL to conform to the standard of your installation using the previously completed worksheet.

The WC20PROF member can be shared with other CA products, and additional parameters may be added to it. See the individual product documentation for details. Before running this step, make sure no other products use this data set, because this step may cause undesirable results.

Once you have made any necessary additions/changes to the member WC20PROF, submit the member to allocate and initialize the ViewPoint database.

If the job completes with a return code greater than 0, then:

1. Review the output carefully before continuing.
2. Correct the problem.
3. Resubmit the job.

Note: The member WC20PROF must be used to create a profile library for each user who will have the ability to save their ViewPoint session customization options across multiple ViewPoint sessions.

For users of Katakana terminals who need all uppercase characters, edit member CACCENV and add KATAKANA=UPPER. If this is not done, the default is mixed case.

Step 53. Allocate GSS ISET VSAM Data Sets

Note: This step is required for CA-GSS.

SAMPJCL member YS28IALV will allocate the IMOD files for the internal and sample ISETs.

Step 54. Compile and Load IMOD Files

Note: This step is required for CA-GSS.

SAMPJCL member YS28ILOD will compile and then load the IMOD files.

The STEPLIB must be APF authorized prior to running this step.

Step 55. Copy GSS Option Members to PPOPTION

Note: This step is required for CA-GSS.

SAMPJCL member YS28IOPT is used to copy the options members from the SMP target library CAISRC to the PPOPTION data set. This will prevent any future SMP maintenance from overlaying the customized versions.

Step 56. ACCEPT CCS for z/OS and OS/390

Note: This step is required for all components.

SAMPJCL member W010ACC accepts all the services (functional sysmods) of CCS for z/OS and OS/390 to the distribution libraries.

Edit the JCL to conform to your installation standards and the previously completed worksheet.

If other CA solutions have been installed, some of these functions may have already been accepted. If this is the case, a non-zero return code occurs. Remove the failing sysmods and resubmit the job. SMP/E users have the option of specifying the operand REDO on the ACCEPT command statement and should expect an SMP return code of 8, which in this case is permissible.

Modify the ACCEPT SELECT list accordingly. Submit the job and verify that the ACCEPT processing ran successfully. If the SMP ACCEPT completes with a return code greater than 4, then:

1. Review the output carefully before continuing
2. Correct the problem
3. Resubmit the job

Step 57. Save All Materials and Output

Note: This step is required for all components.

Be sure to save all of your installation materials and all output from the installation process. This material is essential for timely and accurate Computer Associates maintenance and support of the solution.

Step 58. Post-Installation Steps

Note: This step is required for all components.

Follow the post install steps from the chapter “Post-Installation Tasks” in this manual.

Post-Installation Tasks

This chapter details the post installation tasks that need to be performed before you begin using CCS for z/OS and OS/390.

List of Tasks

Before CCS for z/OS and OS/390 is ready for use, you may need to perform certain post-installation tasks. Check the following list to determine which tasks are relevant to your installation.

Management Services

- Running the Management Services install script
- Repository tasks
- WorldView tasks
- Event Management tasks
- Agent Technology tasks

Common Services

- CAIRIM tasks
- CAIENF tasks
- CAICCI tasks, including loading CAICCI on the client platform

This chapter provides guidance for performing these tasks. In some cases, tasks to be performed at installation coincide with tasks to be performed on an ongoing basis. In those instances, we may refer you to the *CA Common Services for z/OS and OS/390 Administrator Guide* or other appropriate guides for detailed instructions.

Post-installation tasks for CA-GSS and CA-L-Serv are described in the following two chapters.

What Next?

Once you have performed the necessary post-installation tasks, see the appropriate chapter of the CCS for z/OS and OS/390 *Administrator Guide* for detailed instructions on starting the various services.

Running the Management Services Install Script

If you selected any of the Management Services components for installation, run the install script to customize certain files to your specific system. The install script, `fwsetup`, can be found in the directory you specified in the first Event Management Worksheet panel (`/cai/tngfw` by default).

The Repository

The Repository address space needs to be started either as a long running batch job or as a started task. The Repository must be initialized before any Event Management or Worldview component starts.

Prior to starting the Repository address space, the CAIRIM proc must be run to load the SVC. This is done in three steps:

- Alter the CARIMPRM entry as in the following example:

```
PRODUCT(TNGREPOS) VERSION(DB90) INIT(DBRIMPR)
PARM(D246,DBSVCPR,TYP=3)
```
- Add an additional DD statement, DBLIB, to the CAIRIM proc (normally the CAS9 procedure). This DD statement must concatenate the CUSLIB and CAILIB data sets where the repository has been installed.
- Define the OMVS segment of the security record of the user ID assigned to the job. This user ID requires UID 0.
- If CAICCI was installed but is not currently active, you must also configure and start CAICCI, as described in the CAICCI Tasks section later in this chapter.

An easy way to synchronize the startup is to have CAIRIM start the Repository by adding an entry to the AUTOCMDS file used by CAS9, such as 'S TR90STRT'. The SAMPJCL file contains several jobs used to start and stop the Repository address space. TR90STRT is used to start the address space. If WorldView is being started, use SAMPJCL member TRINSTRG; this will start the trigger server as well. TRGSTOP is used to stop the trigger server if active; this job must run before the Repository will shut down. TR90STOP is used to stop the Repository address space.

For detailed instructions on running CAIRIM and starting the Repository address space, see the "Resource Initialization Manager" and "CA-Datcom/TR" chapters of the CCS for z/OS and OS/390 *Administrator Guide*, respectively.

WorldView

Perform these steps before running WorldView:

- Configure the USS environment by adjusting various BPXPRMxx parameters.
- Configure and start a web server.
- Install a compatible Java environment, if you have not done so already.
- Establish security and authorization for certain components.
- Initialize the WorldView Java server.

These tasks are described in the following sections.

For detailed instructions on running WorldView, see the chapter “WorldView” in the *CCS for z/OS and OS/390 Administrator Guide*.

Configuring OS/390 UNIX System Services for WorldView

WorldView requires OS/390 USS to be configured and running in full function mode. Verify that you have the following USS configurable options set to the recommended minimum values:

Option	Value
MAXPROCSYS	200
MAXASSIZE	128MB
MAXTHREADTASKS	200
MAXPROCUSER	100
MAXCPUPTIME	5000

In addition to the above, during WorldView startup, three POSIX shared memory segments are created, and your IPCSHMNIDS parameter must reflect this requirement.

For best performance, you should ensure that temporary files are allocated to a TFS file system. Approximately 32MB of temporary space is required for a typical WorldView installation.

Consult your IBM documentation for detailed information about setting up USS parameters.

Configuring the Web Server

The WorldView GUI requires an OS/390 HTTP server such as the IBM Lotus Domino GO Webserver. If you use the IBM web server, release 4.6 or above is required, and release 5.0 is strongly recommended. Other compatible OS/390 web servers may also be used if they provide compatible HTTP, Java, and CGI scripting capabilities. The web server must run on the same host where the WorldView Java server resides (see the following).

If you already run a web server on OS/390, you may elect to add the CCS for z/OS and OS/390 definitions to your existing server. In most cases, however, it is recommended that you run a secondary web server dedicated to servicing requests for CCS for z/OS and OS/390.

When configuring the web server, you will need to update or create an HTTPD configuration file. During WorldView 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:

<code>Exec /scripts/*</code>	<code>\$/CAIGLBL000/browser/scripts/*</code>
<code>Exec /tngfw/scripts/*</code>	<code>\$/CAIGLBL000/browser/scripts/*</code>
<code>Pass /tngfw/*</code>	<code>\$/CAIGLBL000/browser/*</code>
<code>Pass /tng/*</code>	<code>\$/CAIGLBL000/browser/*</code>
<code>Pass /browser/*</code>	<code>\$/CAIGLBL000/browser/*</code>

If you are running a web server dedicated to CCS for z/OS and OS/390, you will also need to specify these configuration options:

Statement	Purpose
Welcome tngfw.html	Defines the initial CCS for z/OS and OS/390 page.
Port <i>nnnn</i>	Assigns the server to the specified TCP/IP port.

The WorldView HTML files are shipped in EBCDIC format. Normally, 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 WorldView 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 CCS for z/OS and OS/390 require superuser privileges, and the web server must be configured to run the scripts in the \$CAIGLBL000/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 \$CAIGLBL000/browser/scripts require certain environment 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 WorldView installation, a sample environment variable file can be found in \$CAIGLBL000/browser/httpd.envvars. You should 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. SAMPJCL member WEBSERV can be used as a model to start from. Be sure to set the CEE_ENVFILE environment variable to /cai/tngfw/browser/httpd.envvars and to use the /cai/tngfw/browser/httpd.conf configuration file.

Installing Java

The WorldView application on z/OS includes a Java-based server that processes requests from GUI clients. In order to run CCS for z/OS and OS/390, WorldView requires a Java runtime environment at the JDK 1.1.6 or higher level.

Recent releases of OS/390 include the Java environment with the web server so that both are installed together. If you are running an older OS/390 release and have not previously used Java on OS/390, you can order a copy on tape from IBM or download the most recent version from the IBM web site (<http://www.s390.ibm.com>). 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 WorldView.

Reviewing Security Definitions for WorldView

The WorldView 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 WorldView 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.

In order to perform its security functions, the WorldView server requires specific security permissions that may vary depending on which security product you have, the release of OS/390 or z/OS you run, and the details of the security policy you have in effect.

CA recommends that you 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 to the BPX.SUPERUSER resource.
- Any valid group ID (GID).
- Any valid home directory (the directory where you install CCS for z/OS and OS/390 is a good choice).
- Any valid shell program, normally `"/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.

In addition, all of the WorldView 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 WorldView into HFS directories, the installation process marks the appropriate files using the UNIX `"extattr"` command. RACF users installing into PDSE libraries will also need to mark all of the WorldView modules and libraries as PADS-protected.

Please consult the documentation for your security product for details on how to implement these functions.

Initializing the CCS for z/OS and OS/390 Java Server

The CCS for z/OS and OS/390 WorldView Java server is run using the w2startup script located in \$CAIGLBL0000/browser/scripts. This script launches the WorldView Java server; it may need customization, depending on the directory names you select when installing Java.

- \$CAIGLBL0000/browser/classes must be added to your Java CLASSPATH.
- Both the WorldView and Java executable programs must be included in your PATH.
- Both the WorldView and Java library (DLL) directories must be included in your LIBPATH.

These variables are set in file \$CAIGLBL0000/browser/httpd.envvars.

The w2startup script can be run as a UNIX command or as a batch job using BPXBATCH syntax. A sample batch job can be found in the SAMPJCL library in member TNGSERV. A separate job TNGRTS also needs to be started. This job uses the same environment variables as the Java server.

Once the server is started, you can access the WorldView GUI by starting a web browser session with a URL of this form:

<http://hostname:port/tngfw>

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. If you accept the default port of 80, you can omit the port number.

To terminate the Java server you can run SAMPJCL job TNGSTOP or from USS run the w2kill script found in \$CAIGLBL0000/browser/scripts. The script will leave process CaemRtS running, allowing any remote Unicenter machines to access z/OS.

Event Management

The following tasks associated with Event Management may be required, depending on your environment:

- Activate Store and Forward
- Set up the Berkeley syslog daemon
- Enable catrapd
- Initialize the Event Management servers

If you have installed CAICCI, you must also configure and start CAICCI, as described in the CAICCI Tasks section later in this chapter.

For detailed instructions on starting Event Management, see the chapter “Event Management” in the *CCS for z/OS and OS/390 Administrator 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).

When Store and Forward is activated, the Event Management guaranteed message delivery feature will be 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/logs`. Once all messages in this file have been sent, the file is automatically erased.)

Activating SAF

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 will be targeted for SAF. If the SAF configuration file exists but is empty, no nodes will be eligible for SAF.

Use the text editor of your choice 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                Diabolo
```

Creating an SAF Configuration File

The following outline summarizes the steps you should follow 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. You can either save the edited file with the name **SAF.CFG** or choose a unique file name.

Changing 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 do so, proceed as follows:

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.

Setting 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` and are specified in the following format:

selector action

where:

selector identifies the type of message.

action is the location where the selector is sent.

Additional documentation on the Berkeley syslog daemon is provided in the *IBM OS/390 eNetwork Communications Server: IP Configuration* guide (SC31-8513).

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         /a/tng/opr/config/abcfred/pipe/oprpipexxxx
```

Note: If CAIGLBL0000 is /a/tng, and the current node name is abcfred, then the entry above routes the *.info to Event Management. The entry for *.info is automatically added during the startup of the caiopr process.

Rerouting 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.

For example, the following syslogd configuration on node mars illustrates an entry 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          /a/tng/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.

Placing Changes into Effect

In order for the syslogd configuration updates to take effect, you must stop the syslog daemon and restart it from the root ID.

1. To stop the syslog daemon, enter:

```
kill -15 `cat /etc/syslog.pid`
```

2. Restart the syslog daemon by entering:

```
/usr/sbin/syslogd -f syslogd configuration file
```

Enable catrapd

To enable catrapd, which is necessary if you want to route SNMP messages from other consoles, you must make port 162 available. To do so, modify the TCPIP profile (the data set used in DD statement PROFILE in your TCPIP proc) to ensure that:

- Port 162 is not reserved for SNMPQE (the SNMP Query Engine)
- AUTOLOG does not start SNMPQE

If port 162 cannot be used, add following two lines to the envset script in the \$CAIGLBL0000/snmp/scripts directory:

```
CAICATD0001=nnn
export CAICATD0001
```

Note: CAICATD001=*nnn* is the port number to listen on, replace *nnn* with the actual port number.

Initialize the Event Management Servers

A CCS for z/OS and OS/390 Event Management server is started using the SAMPJCL member TNGPROC. This job starts three daemons associated with Event Management: caiopr, stardaemon, and ca_calendar.

Ensure that the following environment variables are set correctly:

Variable	Description
SYSTYPE	The type of system you are running on: z/OS.
CAIGLBL0000	The path used to install the product.
PATH	The search path used to find programs and scripts.

Variable	Description
LIBPATH	The search path used to find DLL modules.
STEPLIB	Should contain the libraries used to install the repository and the library that CAIVPE was installed into.

The remaining variables are dependent on the install path variable CAIGLBL0000 and should not need any modification:

- CA_DB
- CA_CAIMESSAGE
- CAI_OPR_CONFIG
- CAI_CONLOG

The user ID assigned to this job should be assigned UID 0 and have access to the BPX.DAEMON FACILITY.

Agent Technology Services

If you are installing the Agent Technology component, several tasks remain before the Agent Technology services are ready to start.

After performing the necessary tasks, start Agent Technology using the detailed instructions you will find in the chapter “Agent Technology” of the CCS for z/OS and OS/390 *Administrator Guide*.

Tailor the Profile, Script, and Configuration Files in the HFS System

In this step you will edit and tailor the following HFS files:

File	Type	Purpose
agentworks. profile	Profile file	Contains the environment variables needed to run CCS for z/OS and OS/390 Agent Technology.
install_mibs	Script file	Loads the MIBs that you expect to use on your system.
awservices.cfg	Config file	Describes the services and agents that can be activated within CCS for z/OS and OS/390 Agent Technology.
aws_orb.cfg	Config file	Describes the protocols that can be used for communication between the Distributed Services Bus and its different partners (aws_sadmin, the agents, and so on.).
aws_sadmin.cfg	Config file	Identifies each remote system that is to receive mainframe traps (see the System Requirements for Agent Technology).

Edit the profile file: `/agent/agentworks.profile`

The following environment variables should be set to the values that reflect your installation:

<code>AWORKS_MVS_PREFIX</code>	The data set high-level prefix used for Agent Technology data sets. This must be the same value assigned to the <code>PREFIX</code> variable in running the installation script.
<code>AGENTWORKS_DIR</code>	The full path name that defines the directory where Agent Technology files are installed in the HFS system. This must be the same value assigned to the <code>AWORKDIR</code> variable in running the installation script.
<code>RESOLVER_CONFIG</code>	The name of the TCP/IP configuration information data set. This must be the same value assigned to the <code>TCPDATA</code> variable in running the installation script.
<code>AWS_STARTER_REQUEST</code>	The TCP/IP port number used internally to submit requests to the <code>awservices</code> process. The default is 9990.
<code>AWS_STARTER_CONTROL</code>	The TCP/IP port number that allows the <code>awservices</code> 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 kilobytes (for example, 10000 for a maximum size of 10 megabytes).

Note: The `agentworks.profile` file is executed automatically by all the scripts that are delivered with the Agent Technology component. If you want to execute an Agent Technology utility, you will need to first execute this profile explicitly to assign the correct values to the variables that describe your current environment. To do this, set your current directory to the directory that contains this profile (that is, the directory defined by the `AGENTWORKS_DIR` environment variable), and enter the following command:

```
. agentworks.profile
```

Note: Be sure you enter a dot followed by a blank character and the name of the profile file.

Edit the script file: `/agent/services/tools/install_mibs`

Review and tailor the `ldmib` entries to match those MIBs you expect to use on your system. Please note that the `awsAdmin` MIB is always required if you want to use the MIBMUX facility. The documentation that comes with your agent will specify whether MIBMUX is required.

Edit the config file: `/agent/services/config/awsservices/awsservices.cfg`

This configuration file describes the various services and agents that can be potentially activated within Agent Technology. This configuration file has the following content:

- The two first lines in the file describe the common services `aws_orb` and `aws_admin`.
- The default SNMP port on which `aws_admin` listens for SNMP requests is set to 6665, but it can be set to any free value you want.
- The other input lines describe all the agents that are currently supported. Do not change these lines.
- If you plan to develop your own agent, then you will need to add a new line in this file to describe the new agent. Follow this procedure:
 - Be sure the services are stopped.
 - Edit the `awsservices.cfg` file.
 - Duplicate the last line from the file and edit it by substituting the three occurrences of the current agent program name with your own agent program name, and adapting the 3rd and 4th fields (the agent description and agent version).
 - Save the file and restart the services.

Edit the config file: `/agent/services/config/aws_orb/quick.cfg`

This file describes the various protocols that can be used for the communication between the Distributed Services Bus and its different partners. The file is delivered with default values that should normally satisfy all environments.

This configuration file has the following structure:

- The first line defines the name of the pipe that has to be used between the Distributed Services Bus and its partners that are running on the same system.
- The other lines define the TCP/IP port numbers that have to be used between the Distributed Services Bus and its partners that run on different systems. The default port is 7770 for all platforms that run Agent Technology version 2.0 or 2.1 and 7774 for all platforms that run with version 2.2.

Edit the config file: `/agent/services/config/aws_sadmin/aws_sadmin.cfg`

This configuration file identifies each remote system that is to receive mainframe traps. For each remote system, specify an `SNMP_TRAP` entry with the corresponding IP address and port number 162 or 6162, depending on the port number used by the trap listener. In the default file, substitute the 141.202.001.001 values with your own IP address.

```
SNMP_TRAP 141.202.138.21|6162 # traps to TNG DSM Machine
```

Note: This file also lists SNMP community names and their attributes, which are not normally changed. Any line in this file that starts with a # sign is a comment and is ignored by the runtime system.

The following trap destinations are NOT the same:

```
SNMP_TRAP 141.202.138.21|6162 # non-padded IP Address  
                                specification (Correct)
```

```
SNMP_TRAP 141.202.138.021|6162 # Padded IP Address  
                                specification (Wrong)
```

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).

Tailor the ENVFILE from the SRCLIB

The variables that can be customized are AGENTWORKS_DIR, TZ, AW_MAX_LOGSIZE, AWS_STARTER_REQUEST, and AWS_STARTER_CONTROL. Refer to the earlier description of editing the profile file for definitions of these variables.

Verify the TCP/IP Network Configuration

To verify that the TCP/IP network configuration is compatible with the Agent Technology components, submit the AWFTEST job from SAMPJCL. View the output, and verify that correct values have been returned for all the functions (gethostname(), gethostid(), and so on). If the AWFTEST job does not run successfully, you should review the TNGVARS member in SAMPJCL to verify that the TCPDATA variable was correctly customized. 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, please consult with your network administrators for assistance before proceeding.

Build the Aws_sadmin Store Files

Allocate the aws_sadmin store files by running the CLEANADM job from SAMPJCL. The output of the job is placed in the clean_sadmin.out file in the /services/tools directory.

Verify that the /services/tools/install_mibs script file has been customized to include an "ldmib" entry for each agent you plan to use.

Submit the INSTMIBS job from the SAMPJCL 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 paragraph. The output of the job is placed in the `install.mibs.out` file in the `/services/tools` directory.

The installation of Agent Technology on your machine is now complete. This is a good time to make a backup copy of your new HFS.

Arrange for Agent Security

Arrange with your the security administrator for your site to create or update the user IDs that will be running agents. They must all have access to OMVS and be members of the group that owns the Agent Technology files.

Installing Multiple Systems

If you are installing multiple systems, you have two choices:

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

To employ the second option, you must perform the following steps. The effort involved is directly related to how similar the systems are:

1. If you have not already backed up the AGENT HFS, do so now.
2. On the target system, check the System Requirements.
3. Make the LOADLIB, SAMPJCL, and SRCLIB partitioned data sets accessible, either through shared DASD or by copying the data sets.
4. Restore the AGENT HFS backup into the newly created HFS.

5. Update your BPXPRMxx member on the target system to add the MOUNT directive for the new HFS.
6. Perform the following Pre and Post Installation Tasks on the target LPAR:
 - Create, if necessary, the AT security UIDs and GIDs on the new system.
 - Modify your agentworks.profile script in the root AT directory to reflect the new environment. Pay particular attention to:
 - AWORKS_MVS_PREFIX - Designates the prefix for your AT z/OS files
 - AGENTWORKS_DIR - Designates the AT root directory
 - RESOLVER_CONFIG - Designates the DSN for the TCP/IP.DATA file. This reference must correlate to the DSN specified by the SYSTCPD DD statement for the TCP stack running on the new system.
 - Modify member ENVFILE in your AT SRCLIB. If you share your AT SRCLIB between multiple z/OS images then you may need to create a new and unique member for the new system. This will only be the case if you need to modify the contents on the ENVFILE member for the new LPAR. When modifying or creating this file pay attention to the AGENTWORKS_DIR, which designates the AT root directory

- 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 above) you may also need to modify your `install.mibs` script (located in the `AT-Root/services/tools` directory) to include or exclude agents that either will or will-not be running on the target system.
 - Configuration Files - Will probably be ok. The file most likely to require change is the `aws_admin.cfg` file. This file contains the trap destinations where traps will be sent, as well as the SNMP community strings and is located in the `services/config/aws_admin` directory.
 - JCL - If JCL changes are required (to reference a different `ENVFILE`) then you should create a unique copy of the `AT JCLLIB` for the new system.
- Run the `'awftest tcpip'` utility within OMVS, after the `'agentworks.profile'` script has been invoked. You will need to be in the `services/tools` directory prior to invoking this command. This utility will verify that the TCPIP stack has been properly configured. Do not attempt to start your AT services until this utility runs error free.

7. Startup your AT services on the target LPAR.

Move the Load Library to LPA

Optionally, you can move the Agent Technology load library data set to the link pack area (LPA) to optimize the performance of your system.

Start Agent Technology

You now can start, stop, or control Agent Technology using one of these methods:

- Running batch jobs from the SAMPJCL library
- Issuing online commands (that is, shell scripts) to perform the same tasks.

See the online *CA Reference Guide* for more information about batch jobs and their corresponding shell scripts.

CAIRIM Tasks

Post-installation tasks for CAIRIM may include modifying the initialization parameters, customizing CAISSF for RACF products, and starting CAIRIM.

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 CAI.PPOPTION), 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 Computer Associates solution) for the solution and services you are installing. Any requirements for the ordering of statements is included in the instructions supplied with your Computer Associates solution.

Two general rules are followed by all Computer Associates 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 Computer Associates 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)
```

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.

Parameter	Required?	Description
<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 reinitialization or deactivation. Up to 32 characters can be passed in the PARM field.

Notes:

1. 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 will result.
2. Coding the special keyword 'CONSOLE' in column 1 of any control statement causes CAIRIM to obtain all remaining input through operator prompts (WTOR). The command syntax when entering commands from the console is exactly as for coding statements in a data set. This feature can be useful for debugging purposes, or for creating alternate CAIRIM parameter files for use in adding and reinitializing solutions after the initial CAIRIM execution.

3. Control statements can be continued on the next line when a dash, "-", is placed in column 72 of the first line, as shown in the following example.

Col 1	Col 72
v	v
PRODUCT(CA-PRODUCT) VERSION(PC50) INIT(PCVMINIT)	-
PARM(INITIALIZE)	

PC50 in the above example represents the two-character product code and the release number.

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/CAS9SIA2 for CICS 1.7 and 2.1
- Modify CAS9SAFC/CAS9RACL for CICS 3.x and up
- 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 subservice of the CAIRIM service (FMID CS91000). Following the completion of this task, the Standard Security Facility for RACF and RACF-compatible products is installed and ready for use for each Computer Associates 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, CAI.CAISRC.

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, Computer Associates Technical Support for these security translators, if needed, should be obtained through support for the appropriate CA solution.

If the translator for RACF and RACF-compatible solutions does not require modification, skip to the section Modify RACF or the RACF-Compatible Product.

Modify CAS9SAFC/CAS9SIA2 for CICS 1.7 and 2.1

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

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

The CAS9SIA2 SIMOD application is required for products using the RESOURCE ACCESS function. The SIMOD 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 it runs unauthorized. When the A2 SIMOD program is executed at CICS startup, CICS is running authorized. Then, all classname profiles can be RACLISTed. Following SIMOD A2 processing, CICS runs unauthorized.

Note: If classname profiles that have been RACLISTed are updated after CICS startup, CICS must be recycled to pick up these changes.

To install CAS9SIA2, perform the following modifications:

1. Edit source member CAS9SIA2 in the CA Common Source Library, CAI.CAISRC.
2. Locate the table identified by label CASRTBL.
3. Add the required CA solution classnames to this table as defined by your solution-specific documentation.
4. Locate sample JCL member CAS9CSSF in the sample data set created during installation. Uncomment the JCL statement containing the exec statement for the CAS9SIA2 procedure.
5. Update the CICS procedure to include the SIMOD application, DFHSIA2. An example of the SIMOD parameter follows:

```
SIMOD=' (A1 ,A2 ,B1 ,C1 ,D1 ,E1 ,F1 ,G1 ,H1 , I1 , J1) '
```

DFHSIA2 is placed here (A2) in the SIMOD list.

Modify CAS9SAFC/CAS9RACL for CICS 3.x and up

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

The CAS9SAFC translator for RACF and RACF-compatible products, as shipped, executes in a TSO, BATCH, CICS, CA-Roscoe, 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 recycled.

To install CAS9RACL, perform the following modifications:

1. Edit the source member, CAS9RACL, in the CA Common Source Library, CAI.CAISRC.
2. Locate the table identified by label RACLTLBL.
3. Add the required CA solution classnames to this table as defined by your solution-specific documentation
4. Locate the sample JCL member CAS9CSSF in the sample data set created during installation. Uncomment the JCL statement containing the exec statement for the CAS9RACL program.
5. Add programs DFHSIP, CAS9LRAC, and CAS9RACL to the RACF authorized callers table, ICHAUTAB, for the RACLIST privilege only. See the *IBM System Programming Library: Resource Access Control Facility (RACF)* guide for additional information on adding and implementing the RACF authorized callers table.

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 RACLSTed during CICS startup are deleted at shutdown.

Sample PLT members S910PLT and S910PLTS are furnished in the CA Common Macro Library 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 the CA Common Macro Library for reference.

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

Modify and Submit the CAS9CSSF Sample JCL

Modify and submit the sample JCL in the member CAS9CSSF, which is located in the library CAI.SAMPJCL.

Member CAS9SIA2 or CAS9RACL is installed when you submit CAS9CSSF, if you uncommented the corresponding JCL statement containing the exec statement for the procedure.

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 in column 72 of the line to be continued.

Example 1: Class Descriptor Table Entry for CACMD

```
Col 72
CACMD  ICHERCDE  CLASS=CACMD,      -
                {GROUP=DFTGRP,}      -
                MAXLNHG=8,           -
                FIRST=ALPHANUM,      -
                OTHER=ANY,           -
                OPER=NO,             -
                DFTUACC=NONE,        -
                id=CLASS_NUMBER,     -
                POSIT=19-255        -
```

Example 2: SAF Router Table Entry for CACMD

```
Col 72
CACMD  ICHRFRTB  CLASS=CACMD,      -
                ACTION=RACF          -
```

Additional information on the class descriptor table and the RACF SAF router table can be found in the *IBM System Programming Library: Resource Access Control Facility (RACF) guide*.

Optionally Place the CAISSF Routines in 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 confers 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 installation of the CAISSF routines into CSA is accomplished through execution of CAIRIM (the CAS9 procedure). A CAIRIM initialization routine, S910INIT, loads the CAISSF routines into CSA.

Before executing the CAS9 procedure, add the following CAIRIM input initialization control statement to member CARIMPRM in the CAI.PPOPTION data set.

```
PRODUCT(CAIRIM) VERSION(S910) INIT(S910INIT)
```

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.

See the chapter “Resource Initialization Manager” in the CCS for z/OS and OS/390 *Administrator Guide* for additional information on the S910INIT initialization routine.

Note:

1. If you choose not to use 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.
2. 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.
3. If you have chosen **not** to use optional placement of the CAISSF routines in CSA, the CAS9 procedure (CAIRIM) does **not** need to be executed.

APF Authorize the CAISSF Load Library

To finalize the overall installation of CAISSF for RACF and RACF-compatible products, the library in which the CAISSF routines (CAS9SEC) and the security translator (CAS9SAFC) reside must be APF-authorized.

Note: If CAIRIM was installed only to obtain CAISSF, the CAS9 procedure for CAIRIM does not have to be executed for CAISSF.

Start CAIRIM

If the CAS9 proc is to be invoked as a started task, it must be copied to a valid system procedure library.

See the chapter “Resource Initialization Manager” in the CCS for z/OS and OS/390 *Administrator Guide* for detailed instructions on starting CAIRIM.

CAIENF Tasks

Post-installation tasks for CAIENF may include:

- Defining structures
- Starting CAIENF

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

Define Structures in the Coupling Facility

This task is required only if you are running within a sysplex and plan to define an ENFplex. It consists of the following steps:

- Execute the CAS9ESTR utility
- Execute the IBM IXCMIAPU utility
- Define the ENFplex

You will need to repeat the steps in this task once for each structure you are defining.

Execute the CAS9ESTR Utility

Executing the CAS9ESTR utility provides you with an estimated structure size. Modify the estimated size as needed before using it in the next step.

Note: Sample JCL for the CAS9ESTR utility is in the member named CAS9ESTR.

The CAS9ESTR utility can be run in either batch or TSO. However, the following rules apply:

- The user executing the utility must be defined to the CAIENF database with the CAS9DB ADDU command.
- The utility must be executed on a system where CAIENF is running.

When executed from TSO, output will look like this:

```
CAS9ESTR
CAIENF requires a structure of 54 4096 byte records be defined
The above assumes you are not logging.
If you are logging you should add 8 4096 byte records per system
READY
```

If cross-system logging is being used, insert the size recommendations obtained from the CAS9ESTR output into the following mathematical equation:

$$a + (b * c) = \text{total 4096-byte records}$$

Replace a with the first size listed in the CAS9ESTR output (in the example shown above it is 54). Replace b with the number of systems to be connected. Replace c with the second size listed in the CAS9ESTR output (in the earlier example it is 8). If you are connecting three systems, your equation will look like this:

$$54 + (3 * 8) = 78 \text{ total 4096-byte records}$$

If you do not plan to use cross-system logging, omit the equation and use the first size listed in the output as your total (in the output shown earlier it would be 54).

Execute the IBM IXCMIAPU Utility

Executing the IXCMIAPU utility defines a structure within the Coupling Facility. Use the estimated size obtained in the previous step as input. See the IBM guide *Setting Up a Sysplex* for information on how to execute this utility and the JCL you will need.

Define the ENFplex

This task is required if you plan to connect multiple CAIENFs in an ENFplex.

To define an ENFplex, you must add the structure name to each CAIENF system that will be a member of the ENFplex. The structure name is added to each system ENFPARMS DD using the STRNAME control option. Each ENFPARMS DD can contain only one STRNAME control option. See the “CCS for z/OS and OS/390 Administrator Guide for information on the STRNAME control option and a complete description of defining an ENFplex.

Note: Multiple ENFplexes cannot share event information.

After adding the STRNAME control option to each ENFPARMS DD, you must perform a rolling recycle using the REINIT option of the CAIENF STCs on all of the systems in the ENFplex. The first system to connect to the structure determines what information is placed in the structure. All systems connecting after this point will use the information contained in the structure, rather than what is on their respective databases.

Note: Even though a structure will be used, each CAIENF STC must still retain an ENFDB DD card pointing to a valid CAIENF database.

Start CAIENF

If the ENF proc is to be invoked as a started task, it must be copied to a valid system Procedure library.

See the chapter “Event Notification Facility” in the CCS for z/OS and OS/390 Administrator Guide for additional information about starting CAIENF.

CAIENF/USS Tasks

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

- To allow the ENF proc to work with OMVS, you need to define an OMVS segment for the user ID assigned to the proc. You can define a new user ID or use a pre-existing one such as the one used for TCP/IP or OMVS.
- Update the COFVLFxx member used for the system to add a class for CAIENF/USS to use. A sample follows:

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

CAICCI Tasks

Post-installation tasks for CAICCI may include:

- Configuring and starting CAICCI
- Loading CAICCI on the client platform

Configuring and Starting CAICCI

This task is required if you are installing CAICCI.

Default CAICCI options are stored in the data set PPOPTION member CCIPARM. You will need to review and update these options depending on the particular network configuration in use at your installation.

See the chapter "Common Communications Interface" in the CCS for z/OS and OS/390 *Administrator Guide* for details.

In addition to the options you have tailored for CAICCI, additional or new options may be required for the Computer Associates solution you are installing. In particular, any Computer Associates solution that utilizes the CAICCI SPAWN facility will provide an associated spawn parameter that must be appended to the SPNPARM DD statement within the ENF PROC. See your solution-specific documentation for further information.

If the Computer Associates solution requires Assured Delivery, you must add the LOGGER command to the CCIPARM.

See the CCS for z/OS and OS/390 *Administrator Guide* for more information on assured delivery.

Loading CAICCI on the Client Platform

If you have installed CAICCI and you plan to use mainframe-to-PC communication with client-server products such as CA-Datcom and CA-IDMS, follow the steps listed here.

CAICCI/PC is distributed on the CCS for z/OS and OS/390 installation tape. The CAL.PPOPTION data set contains the member CCIPCW32.

Downloading with TCP/IP

If your PC is connected through TCP/IP, you can use FTP to download the CAICCI/PC files from a z/OS host. Make sure to specify binary transfer. Here is a sample FTP session:

```
C:>ftp <mainframe>
User:
Password:
. . .
binary
. . .
cd 'cai.poption'
get ccipcw32 ccipcw32.exe
quit
```

If you are using LU2 communications and a supported emulator is installed on your PC, you can download the CAICCI/PC file using the instructions in the section Downloading with LU2, which follows.

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.

Downloading with LU 2

CAICCI/PC may be installed from the mainframe if the PC is connected to the mainframe using a 3270 emulator that supports the IND\$FILE file transfer protocol. No other software is required.

The following steps will create a directory and download the necessary files:

1. Create a new directory on the PC.
2. Select Receive from Host from your terminal emulator file transfer facility. For the Host file name, enter 'CAL.PPOPTION(CCIPCW32)'. For the PC file name, enter the PC drive and directory created in step 1, followed by CCIPCW32.EXE. For example:

```
c:\ccinst\ccipcw32.exe
```

Ensure that the transfer type is BINARY. Press Enter.

3. Go into the directory created in step 1 when the file download is complete and double-click the CCIPC223.EXE icon to begin the self-extraction process.

After loading CAICCI on the PC, you need to configure it for that PC. See the chapter "Windows to Mainframe - Common Communications Interface" in the CCS for z/OS and OS/390 *Administrator Guide*.

Other file transfer applications, such as CA-XCOM or Unicenter Software Delivery Option, may also be used to perform mass distributions of the required CAICCI/PC files. See the documentation for that product.

Customizing CA-GSS

To complete the installation of CA-GSS and prepare it for use, you need to perform the following post-installation tasks:

- Define subsystem IDs
- Copy PROCs to the System PROCLIB
- Prepare the Started Task PROC
- Install the IMOD Editor
- Install the ISERVE Operator Control Panel

Then you will probably want to test the installation

Depending on the presence of other products, you may need to perform various customization tasks, including the following:

- Customize CA-GSS initialization parameters
- Customize CA-GSS for particular products
- Install optional features
- Upgrade ISETs

Defining Subsystem IDs

Specify your ISERVE subsystem ID using the SSNAME parameter in the CA-GSS RUNPARM member. For documentation purposes, we recommend that you 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.

Copying CA-GSS Procs to System PROCLIB

The CA-GSS procs are distributed in the SAMPJCL library. These must be moved to a system PROCLIB to make them available to be run as a started task.

The following table lists the SAMPJCL member names to be copied and gives the suggested proc name for each. Please review the SAMPJCL members to ensure they are properly customized. Then copy the members to your system PROCLIB.

SAMPJCL name	Proclib name	Description
YS28GSSA	GSSA	Primary CA-GSS started task
YS28GSSP	GSSP	CA-GSS Passive area utility

IF you plan to run multiple CA-GSS subsystems, a sample proc, YS28ISRV, for running secondary GSS subsystems is included in the SAMPJCL library. See the CCS for z/OS and OS/390 *Administrator Guide* for information on running multiple CA-GSS subsystems.

Preparing the Started Task PROC

The GSSA PROC is used to initialize the CA-GSS address space. Copy the SAMPJCL data set member YS28GSSA to your started-task procedure library. Change data set names and JCL statements as appropriate for your installation. You must select values for the lowercase parameters.

Installing 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 of the CA-GSS LINKLIB by the TSO user. This may be done through the LNKLST or by providing the appropriate STEPLIB statement.
- Accessibility of 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 PPOPTION 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, perform the following tasks.

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 need to notify your enqueue-management software about the CA-GSS enqueues.

Note:

1. 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.
2. 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.
3. All enqueues have a scope of SYSTEMS.

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 sample RUNPARAM, ISETS, and EDITPARAM members.

- If UNIT=VIO is not valid for data set allocation in your data center, you must include a VIUNIT 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. We recommend that you specify the EDITPARM member of the PPOPTION data set for this value.
- A sample parameter list is provided in the ISETS member of the PPOPTION 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.
- For the format of ISET initialization parameter statements, see the online *CA Reference*.

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(#####) NOCHECK'
```

Replace ##### with 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:

1. Press PF1 (or enter HELP) to display the long error message, which identifies the cause of the failure.
2. 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.

3. 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 will be identical by using the sample RUNPARM, ISETS, and EDITPARM members.

Installing 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 z/OS system of the user. 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.

You can 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 it from ISPF, add the following menu item to the panel and the PROC section for the appropriate ISPF panel:

```
ISRVO, 'PGM(SRVOPER) NEWAPPL(mmmm) NOCHECK'
```

Replace *mmmm* with 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.

Testing the Installation

At this point, the basic installation process is complete. Before proceeding with final customization, you may wish to verify that CA-GSS has been installed correctly. You can test it by using an operator console to start CA-GSS, issue a command to CA-GSS, and then stop CA-GSS.

Starting CA-GSS

From the operator console, enter the following command:

```
START GSSA
```

Initialization should proceed rapidly; when it is complete, the following message is displayed:

```
SRV220 Version 02.08.mmm: Initialization Complete (ssid)
```

where *mmm* represents the current maintenance level of CA-GSS and *ssid* represents the subsystem ID you selected for ISERVE.

Testing CA-GSS

Follow these steps to test CA-GSS:

1. Invoke the CA-GSS/ISERVE Control Panel by issuing this command from an ISPF panel:

```
TSO EX 'CAI.CAICLIB(GSSOPER)
```

2. Execute the Installation Verification Program (IVP) by issuing this command from the CA-GSS/ISERVE Control Panel:

```
F GSSA,IVP [PRINT [TO userid [AT node]]]
```

If you omit the text in brackets, output will be 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.

3. Use the PF3 key to return to your ISPF panel.

Testing the IMOD Editor

Follow these steps to test the IMOD Editor:

1. Invoke the IMOD editor by issuing this command from an ISPF panel:

```
TSO EX 'CAI.CAICLIB(GSSEEDIT)'
```

2. Select the CAICLIB ISET by specifying S next to its name.

Then select the \$\$\$VERSION member by specifying S next to its name.

3. In the \$\$\$VERSION member, verify that the correct version of CA-GSS is specified. (It should be 0208*mm*.)

When the version is correct, use the PF3 key to go back to the CAICLIB ISET display.

4. 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.

5. Use the PF3 key to back out of your ISPF session.

Stopping CA-GSS

To terminate CA-GSS properly, enter 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.

Recompiling Under TSO

If you want to recompile IMODs while under TSO, select an ISET and enter the IMOD selection panel. In this panel, enter the TOGGLE command to display the current compiler version for each IMOD. You may then enter a C (compile) command on each line that shows an IMOD in need of recompiling. Press ENTER to recompile all IMODs identified with a C.

Customizing Initialization Parameters

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. Product-specific parameters are described in the next section.

See the CA-GSS chapter in the CCS for z/OS and OS/390 *Administrator Guide* for an overview of CA-GSS initialization parameters and to determine which ones you need to customize now. For a detailed description of any CA-GSS initialization parameter, see the online *CA Reference Guide* or the CCS for z/OS and OS/390 *Administrator Guide*.

Customizing for Particular Products

If you are using any of the following products, you may need to customize CA-GSS for those products:

- CA-Insight for DB2
- CA-Jobtrac
- CA-OPS/MVS II
- CA-SYSVIEW
- CA-View
- DB2
- IDCAMS

These customization tasks are described in the following sections.

CA-Insight for DB2

CA-Insight for DB2 uses CA-GSS for various logging, access, and auditing capabilities. REXX-based IMODs are used for all CA-Insight for DB2 functions that access CA-GSS.

Before You Begin

Look at your CA-Insight for DB2 documentation to see whether this product supplies IMOD libraries (ISETs). If so, you need to load these ISETs to DASD.

You can use the CA-GSSIMOD member of CA-Insight for the DB2 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 for DB2 tape.

Customization Steps

Perform the following steps to customize CA-GSS for CA-Insight for DB2.

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, Computer Associates recommends that you 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 **YS28IALI** member of the **SAMPJCL** 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. Computer Associates recommends that you use the naming convention LOG nn #0 for primary subfiles and LOG nn #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 YS28IALI method, do not change the values for either the LINEAR or SHAREOPTIONS parameters.

For detailed information on the SRVMAINT job or the ALLOC_ILOG command, see the CCS for z/OS and OS/390 *Administrator Guide* and the *CA Reference Guide*.

2. Identify ILOGs to CA-Insight for DB2.

Identify your ILOG data sets to CA-GSS through the INSIGHT member of the PPOPTION 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 the CA-GSS PROC(YS28GSSA).

Add the following DD statement to your CA-GSS PROC:

```
//DB2SSID DD DSN=CAI.PPOPTION(DB2SSID),DISP=SHR
```

This DD statement points to the DB2SSID member of the PPOPTION 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 CA-GSS' PROC, 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 PPOPTION 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 PPOPTION data set.

A list of the parameters you may need to modify is provided in the following table. For a complete description of any CA-GSS initialization parameter, see the *CA Reference Guide*.

Parameter	Description
COMMAND	<p>Defines the INSIGHT console command to CA-GSS.</p> <p>CA-Insight for DB2 distributes a set of IMODs with a name prefix of \$DBGL_. These IMODs process operator console commands to provide additional functions to the operator.</p>
ILOG	<p>Defines an ILOG file. Specify this parameter once for each ILOG that you have defined.</p>

Parameter	Description
ISET	Identifies an ISET (IMOD library) that is included on the distribution tape of CA-Insight for DB2.
PRODUCT	<p>Activates the CA-GSS support for CA-Insight for DB2.</p> <p>This parameter does not conflict with other specifications of the PRODUCT parameters.</p>
WTO	<p>Executes a particular IMOD whenever a WTO that you identify is issued.</p> <p>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).</p> <p>You will need to modify the IMOD to meet the requirement of your installation.</p>

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.

For information about this special-purpose IMOD, see the *CA Reference Guide*.

7. Activate GoalNet.

If you are using CA-Insight for DB2 and you are operating in a multi-CPU environment, with or without shared DASD, you may want to activate GoalNet so that CA-Insight for DB2 can gather information from multiple systems and can consolidate displays.

In order to use the CA-Insight for DB2 System Condition Monitor on external systems, you must install CA-GSS on all CPUs. CA-Insight for DB2 is required on the systems where information is to be displayed.

CA-Jobtrac

CA-Jobtrac uses CA-GSS facilities to extend its capabilities and to provide you with fully customizable support for job scheduling. In addition, CA-Jobtrac information is made available to other CA-GSS client software, including that provided by you.

PPOPTION member JOBTRAC contains sample customization parameters. See the *CA-Jobtrac* documentation for customization details.

CA-OPS/MVS II

CA-OPS/MVS II uses CA-GSS facilities to access other Computer Associates products and makes its facilities available to other products through CA-GSS facilities.

Before You Begin

Before you begin the customization steps:

- Make sure that the CA-OPS/MVS II OPGLEVMG communication module is available. This module resides in the CA-OPS/MVS II load library. This library must be in the APF list.
- Provide a CA-OPS/MVS II security rule so that CA-GSS can issue z/OS commands through the OPER ADDRESS environment.

Customization Steps

Perform the following steps to customize CA-GSS for CA-OPS/MVS II.

1. Modify the PROC(YS28GSSA).

If the OPGLEVMG load module is not in a LINKLIST library, include its library as a STEPLIB in the CA-GSS PROC(YS28GSSA).

2. Modify CA-GSS parameters.

As needed, modify the CA-GSS initialization parameters that affect CA-GSS' CA-OPS/MVS II support. Examples of these parameters are contained in the OPSMVS member of the PPOPTION data set.

Note:

- 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.
- A summary description of each parameter you may need to modify is provided in the following table. For a complete description of any CA-GSS initialization parameter, see the *CA Reference Guide*.

Parameter	Description
SSID	Identifies the CA-OPS/MVS II system that should process associated ADDRESS and function requests.
ADDRESS	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 II OPGLEVMG load module.
- If you want to make the OPSVALUE() function available, you also need to provide the appropriate ADDRESS parameter.
- Computer Associates-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 II tape. Make sure that this load module resides in an APF-authorized library that is accessible to CA-GSS.

CA-SYSVIEW

Unicenter CA-SYSVIEW provides facilities that may be used by IMODs and by other Computer Associates products through the use of IMODs.

See the Unicenter CA-SYSVIEW Realtime Performance Management documentation for customization details.

CA-View

CA-View provides facilities that may be used by IMODs and by other Computer Associates products through the use of IMODs.

Before You Begin

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.

Customization Steps

Perform the following steps to customize CA-GSS for CA-VIEW.

1. Modify the PROC(YS28GSSA).

If the SARINTF load module is not in a LINKLIST library, include its library as a STEPLIB in the CA-GSS PROC(YS28GSSA).

2. Modify CA-GSS parameters.

As needed, modify the CA-GSS initialization parameters that affect CA-GSS' CA-View support. Examples of these parameters are contained in the VIEW member of the PPOPTION data set.

Note:

- 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 so your RUNPARM member, or you can simply provide an INCLUDE VIEW statement.
- A summary description of each parameter you may need to modify is provided in the following table. For a complete description of any CA-GSS initialization parameter, see the *CA Reference Guide*.

Parameter	Description
ADDRESS	Makes the ADDRESS environment provided on the CA-View distribution tape as a load module available to REXX IMODs.
VIEW	Provides parameters to the initialization IMOD that CA-View provides. You can specify the VIEW parameter multiple times.

With respect to the ADDRESS parameter, note the following:

- Computer Associates-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.

DB2

If you are running the IBM DB2 database software, an IMOD can retrieve data by executing dynamic SQL statements.

Before You Begin

Make sure that the DSNALI and DSNHLI2 communication modules of DB2 are available. These modules must reside in an APF-authorized LINKLIB data set.

Customization Steps

Perform the following steps to customize CA-GSS for DB2.

1. Modify the PROC(YS28GSSA).

If the DSNALI and DSNHLI2 load modules are not in a LINKLIST library, include their library as a STEPLIB in the CA-GSS PROC(YS28GSSA).

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 PPOPTION data set. Note that:

- 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.
- A summary description of each parameter you may need to modify is provided in the following table. For a complete description of any CA-GSS initialization parameter, see the *CA Reference Guide*.

Parameter	Description
ADDRESS	Loads the DB2 DSNALI and DSNHLI2 modules during CA-GSS/ISERVE initialization and makes them available for processing the DB2() REXX function.
DB2PLAN	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.
SSID	<p>Identifies the DB2 address space that CA-GSS should communicate with. Each CA-GSS can communicate with only one DB2 address space.</p> <p>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.</p> <p>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.</p>

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, Computer Associates distributes the SRVDB2P program in source format. This program, along with sample JCL, can be found in the SAMPJCL member YS28DB2P.

4. Bind the plan.

Before you execute dynamic SQL using the DB2() function, you must bind the plan (created in step 3 and specified in the DB2PLAN initialization parameter) to the target DB2 address space.

IDCAMS

CA-GSS/ISERVE makes the facilities provided by the IBM Access Method Services (IDCAMS) available to IMODs.

Before You Begin

Make sure 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.

Customization Steps

Perform the following steps to customize CA-GSS for IDCAMS.

1. Modify the PROC(YS28GSSA).

If the IDCAMS load module is not in a LINKLIST library, include its library as a STEPLIB in the CA-GSS PROC(YS28GSSA).

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 PPOPTION data set.

Note that:

- 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.
- A summary description of the parameter you may need to modify is provided in the following table. For a complete description of any CA-GSS initialization parameter, see the *CA Reference Guide*.

Parameter	Description
ADDRESS	Makes the ADDRESS environment provided through the IDCAMS load module available to REXX IMODs. Computer Associates-provided IMODs expect the address name IDCAMS. If you use another name, use the ALTNAME parameter to define the name IDCAMS.

Installing 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 Computer Associates products and user-written IMODs.

Use GoalNet if you want to use VTAM to enable communications between multiple copies of MVS 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 for DB2 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

GoalNet is an LU 6.2-based communications protocol that is used by CA-GSS to permit cross-system communication by Computer Associates products and user-written IMODs. 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.

PPOPTION Member: GOALNET

A sample GoalNet definition is provided in the GOALNET member of the PPOPTION data set. Computer Associates recommends that you examine this member before creating your own GoalNet definitions.

See the CCS for z/OS and OS/390 *Administrator Guide* for more information on GOALNET.

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 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.

SAMPJCL Member: GOALNETT

A sample logmode table is provided in the GOALNETT member of the SAMPJCL data set. Computer Associates highly recommends that you use this table exactly as provided.

An assembled and link-edited version of the provided logmode table is distributed in the CAILIB 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, Computer Associates highly recommends that you 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.

SAMPJCL Member: YS28VTAM

The YS28VTAM member of the SAMPJCL data set contains sample definitions for both GoalNet and Logon Facility applications. Only the minimum parameters are shown.

CA strongly recommends that you not make changes or additions to these parameters unless you fully understand VTAM requirements.

ILOGs

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.

Allocating ILOG Files

There are two ways to allocate ILOG files:

- Computer Associates recommends that you 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.

A sample statement:

```
ALLOC_ILOG NAME CLUSTER VOLSER xxxxxx CYL 1 1
```

For more information on this method, see the CCS for z/OS and OS/390 *Administrator Guide*.

- Another way of allocating these data sets is to modify and submit the YS28IALI member of the SAMPJCL 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 Computer Associates 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 Computer Associates 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.

Logon Facility Definition Steps

Perform the following steps 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 YS28VTAM member of the SAMPJCL data set. (This member is also used to define GoalNet.)

2. Provide applications.

You must determine each application, by name, that is 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, Computer Associates provides an application IMOD (\$SRVV) that provides a CA-GSS operator interface.

For detailed information on writing application IMODs, see the CCS for z/OS and OS/390 *Administrator 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 PPOPTION 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 simply provide an INCLUDE LOGON statement.

- A summary description of each parameter you may need to modify is provided in the following table. For a complete description of any CA-GSS initialization parameter, see the *CA Reference Guide*.

Parameter	Description
LOGON LUNAME	Replace <i>luname</i> with an application ID that has been defined to VTAM.
LOGON LUNAME <i>luname</i> <i>password</i>	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	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.
LOGON APPLICATION OPERator \$SRV	

Note the special use of case when specifying the application name. 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.

Upgrading ISETs

If you have any ISETs that were not distributed on the CCS for z/OS and OS/390 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 YS28UPGR member of the SAMPJCL data set contains sample JCL and control statements for upgrading ISETs. Complete information on the SRVMAINT program may be found in the section on batch maintenance of ISETs in the *CA Common Services for z/OS and OS/390 Administrator Guide*.

Starting CA-L-Serv

Before starting CA-L-Serv, you may need to update external security and define CA-L-Serv to VTAM, and you will need to tailor the CA-L-Serv startup parameters, update the message table, and tailor the startup procedure. After starting CA-L-Serv, you may want to verify the communications server and file server installation.

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.

Update Tasks

The security enhancements generally require the security administrator to accomplish the following:

1. Create a new resource class: \$LSRVDSN
2. Define CA-L-Serv data sets to the new resource class
3. Permit access to users through the new resource class
4. Create a user ID for the CA-L-Serv started task
5. Permit the CA-L-Serv user ID access to the data sets

Usage Notes

1. Security definitions previously implemented for Endeavor or other products need not be altered. The security checks made by these products will still function in exactly the same manner.
2. 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.

3. Permitting users using 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).
4. 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.
5. The CA-L-Serv utility program, LDMAMS, can be executed only under a user ID that has CONTROL access to the data sets.

Important! Endeavor users must grant access to the new resource class to the 'true' user ID, not the 'alternate' user ID. When Endeavor 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.

CA-Top Secret Environments

The following are sample definitions for users running under CA-Top Secret.

These sample definitions are provided to help illustrate the above description. The actual implementation in your environment may differ from these templates.

1. Define the new resource class to the CA-Top Secret Resource Descriptor Table (RDT). For example:

```
TSS ADD(RDT) RESCLASS($LSRVDSN) RESCODE('X'02')
ATTR(LONG,DEFPROT) ACLST(CONTROL) DEFACC(NONE)
```

See the *CA-Top Secret Reference Guide* for additional information regarding the command syntax and features.

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)
```

CA-ACF2 Environments

The following are sample definitions for users running under CA-ACF2.

These sample definitions are provided to help illustrate the above discussion. The actual implementation in your environment may differ from these templates.

1. CLASMAP the new \$LSRVDSN resource class to resource type LSV.

For example:

```
SET CONTROL(GSO)

INSERT CLASMAP.LSRV2 ENTITYLN(44)-
      RESOURCE($LSRVDSN) RSRCTYPE(LSV)
```

Issue a MODIFY command from the console:

```
F ACF2,REFRESH(CLASMAP)
```

2. 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
```

3. 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
```

RACF Environments

The following are sample definitions for users running under RACF.

These sample definitions are provided to help illustrate the above discussion. The actual implementation in your environment may differ from these templates.

1. Add an entry for the new resource class to the Class Descriptor Table. The Class Descriptor Table ICHRRCDE 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.

2. 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
```

3. Activate the \$LSRVDSN class.

Following an IPL with the new Class Descriptor Table, enter the following command:

```
SETROPTS CLASSACT($LSRVDSN)
```

4. 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)
```

5. 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 may choose to 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)
```

6. Define CA-L-Serv to RACF.

Create a user ID for CA-L-Serv giving it 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.

7. 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 may 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.

8. 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 step is necessary only if you plan to use VTAM to support communication between copies of CA-L-Serv executing on different systems. If you do not plan to use VTAM for cross-system communication, you can skip this section.

1. Create a major node member in your SYS1.VTAMLST data set using the PPOPTION 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. See the installation manual for the IBM ACF/VTAM product for further information on Cross-Domain Resource information.

Notes:

1. The SAMPACB definition provided in the CALPPOPTION data set may be used for either LU 0 or LU 6.2 communication.
2. 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 PPOPTION data set. A brief discussion of some features of the sample CA-L-Serv startup parameter member follows. See the CCS for z/OS and OS/390 *Administrator Guide* and the *CA Reference Guide* for additional information on CA-L-Serv operation and command syntax.

```

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 SERVERTYPE=HOST (6)
    ADDPOOL 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 SERVERTYPE=REMOTE (*)
ENDIF (3)
*
IFSYS SYSC (3)
    ATTACH COMMSERVER ACBNAME=COMMSYSC etc.
    (...)
    ATTACH FILESERVER SERVERTYPE=REMOTE (*)
ENDIF (3)

```

- (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. See the *IBM Using Data Sets* manual for a detailed discussion of shared VSAM resources.

- (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. See the CCS for z/OS and OS/390 *Administrator Guide* for full details on SQL Server operation with CA-L-Serv.

Note: A functionally equivalent setup in three separate members (LSVPARAM1, LSVPARAM2, and LSVPARAM3) is also provided in the CALPPOPTION data set.

Update the Message Table

The installation of CA-L-Serv places the LSERVMSG message member into the target CALPPOPTION 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.PPOPTION           <=== your DSN
//O1        DD  DISP=SHR,
//          DSN=CAI.LDMCMND           <=== your 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
```

Note: If the CA-L-Serv parameter data set already contains an older version of the LSERVMSG member, you may want to rename it before submitting this JCL.

Copy and Tailor the Startup Procedure

The installation of CA-L-Serv places the startup procedure, LSVPROC, into the target procedure library CAI.CAIPROC. 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.PPOPTION', (1)/* CA-L-Serv PARMLIB */
// AUTHLIB='CAI.CAILIB', (2)/* CA-L-Serv LOADLIB */
// MEMB=LDMPPARM, (3)/* CA-L-Serv parm member*/
// JCL='CAI.CAISRC', (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
```

Customize this procedure to meet the needs of your installation.

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. Always specify REUSE=YES unless directed otherwise by technical support.
6. Specify a unique subsystem name.

Start CA-L-Serv

Start CA-L-Serv from a z/OS console using the MVS START command.

Notes:

1. If you choose to have identical z/OS subsystem and procedure names, direct the execution to the Job Entry Subsystem expressly by specifying `START lsvproc,SUB=JESx`, thereby preventing CA-L-Serv from executing under the z/OS Master Scheduler.
2. Be aware that 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 installation of CA-L-Serv places the installation verification JCLs HJ35IVC1 and HJ35IVC2 in the target source library CAISRC.

The Communications Server IVP comprises the following steps:

- Tailor the JCLs to the requirements of your site
- Start CA-L-Serv on the two systems
- Submit job HJ35IVC1
- Submit job HJ35IVC2
- Verify the results

Tips for troubleshooting the Communications Server IVP follow.

This process may be repeated between every pair of systems that will use CA-L-Serv to establish communication.

Communications Server Verification Steps

Perform the following steps to verify the Communications Server installation.

1. Tailor the JCLs.

Customize the following templates available in members HJ35IVC1 and HJ35IVC2, which the installation placed in the CAI.CAISRC data set:

Receiving job:

```
//HJ35IVC1 JOB (JOBACCNT) (1)
//MAMS0001 EXEC PGM=LDMAMS
//STEPLIB DD DISP=SHR,DSN=CAI.CAILIB (2)
//SSN$xxxx DD DUMMY (3)
//SYSPRINT DD SYSOUT=X
//SYSIN DD *
  COMMTEST (4)
  RECEIVE
  END
/*
```

Sending job:

```
//HJ35IVC2 JOB (JOBACCNT) (1)
//MAMS0001 EXEC PGM=LDMAMS
//STEPLIB DD DISP=SHR,DSN=CAI.CAILIB (2)
//SSN$xxxx DD DUMMY (3)
//SYSPRINT DD SYSOUT=X
//SYSIN DD *
  COMMTEST (4)
  WAIT APPL(HJ35IVC1)
  SEND
  END
/*
```

- (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. HP35IVC1 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. If this is the case you can proceed to the Troubleshooting section.

Troubleshooting

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.

Here are some of the aspects you can verify before calling Computer Associates Support:

1. Review the output of jobs HJ35IVC1 and HJ35IVC2 and see the *CA Message Guide* for an explanation of any error messages or return codes.
2. Review the message logs of CA-L-Serv on both systems and look for messages with corresponding timestamps.
3. Verify that the file server and the communications server are active on both systems. The DISPLAY ACTIVE command lists the currently active servers.
4. 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).
5. If you are using VTAM communication, issue 'DISPLAY NET,ID=' commands to verify the state of your APPL and CDRSC definitions.
6. 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 call Computer Associates technical 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 JCLs HJ35IVF1 and HJ35IVF2 in the target source library CAISRC.

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.

The File Server IVP comprises the following steps:

- Initialize the VSAM test file and allocate a work file
- Start CA-L-Serv
- Place the VSAM test file under the management of the File Server
- Tailor the J35IVF2 JCL to the requirements of your site
- Submit job HJ35IVF2 and verify the results

File Server Verification Steps

Perform the following steps 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 CAI.CAISRC 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..)
```

(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. See the CCS for z/OS and OS/390 *Administrator Guide* for additional information.
- (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 task.

2. Verify initialization and 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 ddname test.file.dsname
```

See the *CA Reference Guide* and the CCS for z/OS and OS/390 *Administrator Guide* for a full description of the ADDFILE command.

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 (JOBACNT) (1)
//MAMS0000 EXEC PGM=LDMAMS
//STEPLIB DD DISP=SHR,DSN=CAI.CAILIB (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)
```

- (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. See the *CA Reference Guide* for a full description of the syntax of LDMAMS statements.

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 verify the results.

Submit job H35IVF2 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
```

Maintaining CCS for z/OS and OS/390

Maintenance Steps

Follow the steps in the order in which they appear.

Step 1. Visit the Support Page

The Support page contains any additional information that will aid in the installation and running of the CCS for z/OS and OS/390. In addition to any new maintenance that may be available, each component has a FAQ and other technical information. The URL is <http://esupport.ca.com>.

Step 2. Load Installation SAMPJCL Library

CCS for z/OS and OS/390 installs and is maintained through SMP/E. The solution tape received with this package contains all the necessary data to install, maintain, and execute CCS for z/OS and OS/390. It is a standard label 3480 IDRC tape. Prior to installing the solution, you should load the SAMPJCL library from tape. This is the ninth file, DSN=CAI.SAMPJCL, on the tape and it is in IEBCOPY unload format. Use the following JCL as a model to load the SAMPJCL library to DASD.

Note: The CCS for z/OS and OS/390 CAI.SAMPJCL data set contains both installation and maintenance JCL members.

```
//LOAD      EXEC PGM=IEBCOPY
//SYSPRINT DD   SYSOUT=*
//SYSUT1   DD   DISP=OLD,
//          DSN=CAI.SAMPJCL,
//          UNIT=TAPE,                <=== generic 3490 tape
//          VOL=SER=W0rrsp,
//          LABEL=(9,SL),
//          DCB=DEN=4
//SYSUT2   DD   DISP=(NEW,CATLG,DELETE),
//          DSN=CAI.SAMPJCL,          <=== your DSN
//          UNIT=SYSDA,              <=== your generic DASD
//          VOL=SER=.....,          <=== permanent DASD volser
//          SPACE=(3120,(800,25,50)), <=== minimum space required
//          DCB=(LRECL=80, BLKSIZE=3120, RECFM=FB)
//SYSUT3   DD   UNIT=SYSDA, SPACE=(CYL,(3,3))
//SYSUT4   DD   UNIT=SYSDA, SPACE=(CYL,(3,3))
//SYSIN    DD   *
           COPY      INDD=((SYSUT1,R)),OUTDD=SYSUT2
//
```

Once this job has ended, your library contains all of the JCL needed to complete the installation of CCS for z/OS and OS/390.

In order to satisfy your data center needs, certain tailoring of JCL is necessary while executing the steps on the following pages. See the Installation Worksheet completed in Step 5 to obtain values for the various JCL parameters.

Step 3. Download BookManager Files

The documentation is provided in BookManager format. To download the documentation in this format, use member W010BMGR.

Step 4. Download PDF Files

The documentation is also provided in PDF format. To download the PDF files, use member PDFDOWNL.

Step 5. Complete the Installation Worksheet

A CCS for z/OS and OS/390 installation worksheet is provided in an appendix to this guide. It is designed to simplify modifying the supplied JCL.

Answer each question on the worksheet, filling in the blanks with the appropriate information. Default values are noted, so if the default value is acceptable, leave the item blank on the worksheet. However, you must supply appropriate volume serial numbers.

Once you have completed the worksheet, you can use it as a reference while performing the remaining installation steps.

Step 6. Modify SAMPJCL Member JOBCARD

Edit the member JOBCARD to conform to your installation standards. There is a JCLLIB statement that should be modified to point to your SAMPJCL data set. This member will then be used for the remaining jobs. If you need to add SETUP cards for tape mounts you may want to create a separate member for those jobs.

Step 7. Modify SAMPJCL Member TNGVARS

Edit the member TNGVARS to conform to your installation standards. This member will be included as part of the JOBCARD member updated in the previous step. The member will set variables that will be used in the remaining members.

Use the worksheet that was filled in previously to make any changes.

Step 8. Edit JCL to Exclude Previously Applied SYSMODs

Be advised that the PTF tapes are cumulative (that is, these tapes contain all the latest replacement SMP elements since the base release). Therefore, you may have already applied some of the PTFs to your libraries.

You have two choices for performing maintenance:

- Process all the PTFs present regardless of whether some of them have already been received, applied, and accepted, thus reinstalling all maintenance since base level. Here, SMP/E users have to specify REDO on the APPLY and ACCEPT statements.
- Process only the subset of PTFs necessary to bring you to the current level.

Note: If you are not sure whether previous cycles are complete, please process all previous maintenance.

If you have chosen to process only the PTFs necessary to bring you to the current level, edit the JCL members to either comment out or delete the PTF IDs belonging to previously completed maintenance cycles. The JCL members to be edited can be identified by their function name.

Step 9. ACCEPT Previous Maintenance of CCS for z/OS and OS/390 Base Functions

All previous CCS for z/OS and OS/390 maintenance, if any, should be accepted, using the ACCEPT command, prior to the installation of any new maintenance. If CCS for z/OS and OS/390 maintenance has never been applied, ensure the base functions for any of the CCS for z/OS and OS/390 components you have installed have been accepted. This ensures that the current level of code from which you are running can be restored if problems are incurred following application of the new maintenance.

***Important!** Do not under any circumstances accept an SMP usermod that has been applied on top of the CCS for z/OS and OS/390 base level or CCS for z/OS and OS/390 maintenance level. Only base functions, PTFs, and APARs should be accepted.*

Step 10. Agent Technologies Downloads

This step downloads from the tape files that are used by Agent Technologies. SAMPJCL member AINSTJ03 is provided to download these files.

Step 11. Prelink Agent Technologies

To resolve the LE requirements, a prelink must be run. The output for this job is used as input for the apply step. Member AINSTJ04 is used to complete the prelink.

Step 12. Event Management and WorldView Downloads

This step downloads from the tape files that are used by Event Management and WorldView. SAMPJCL member TNGDOWNL is provided to download these files.

Step 13. Set Up Event Management and WorldView SMP DDDEFs

SAMPJCL member TNGDDDEF is provided to update the SMP CSI with the correct data set names in use by Event Management and WorldView. Edit the job to reflect the data set allocations and the install path in use at your site. There have been changes to the order of certain definitions, which require this job to be rerun for maintenance.

Step 14. RECEIVE CCS for z/OS and OS/390 Maintenance

Maintenance JCL member W010MREC RECEIVES all the PTFs corresponding to CCS for z/OS and OS/390 maintenance.

Allocate an SMPHOLD data set (if such a data set has not previously been allocated) by executing the SAMPJCL member W010MHLD.

Edit member W010MREC to conform to your installation standards. Delete any DD statements within the SMPCNTL DD statement that correspond to CCS for z/OS and OS/390 components not currently installed. SMP does not RECEIVE PTFs for CCS for z/OS and OS/390 components that are not present in your SMP environment.

Edit all JCL as necessary. Submit the job and verify that RECEIVE processing ran successfully. If the SMP RECEIVE completed with a return code greater than 4, then do the following:

1. Review the output carefully before continuing
2. Correct the problem
3. Resubmit the job

SMP Update: The SMP LIST command has been added to SMP RECEIVE processing, to list any HOLDDATA that may be present in maintenance to be received. This HOLDDATA should be carefully viewed before executing SMP APPLY for any HELD SYSMODs, because this data contains information pertaining to particular products and how this update to CCS for z/OS and OS/390 affects them.

If SYSMODs are HELD, their respective HOLDDATA should be carefully scrutinized and action taken as necessary prior to the SMP APPLY. For additional information regarding HELD SYSMODs, see the IBM System Modification Program Extended (SMPE) Reference.

Step 15. APPLY Check CCS for z/OS and OS/390 Maintenance

Maintenance SAMPJCL member W010MAPC APPLY checks all the PTFs corresponding to the services specified within the SMP_CNTL DD statement. The purpose of this step is to identify SMP USERMODS and APARS that prevent PTF application, and identify any PTFs already applied.

Computer Associates requires the removal of any SYSMOD preventing PTF application. To allow PTF application, perform SMP RESTORE processing on the SYSMODs identified during SMP APPLY check processing.

If other CA solutions have been installed, some of these PTFs may have already been APPLY checked. Even if this is the case, it is always good practice to run SMP APPLY check processing immediately prior to an SMP APPLY.

Edit member W010MAPC to conform to your installation standards. Delete any DD statements within the SMP_CNTL DD statement that correspond to CCS for z/OS and OS/390 components not currently installed.

Edit all JCL as necessary. Submit the job and verify that APPLY check processing ran successfully. If the SMP APPLY check completed with a return code greater than 4, then do the following:

1. Review the output carefully before continuing
2. Correct the problem
3. Resubmit the job

Notes:

1. SMP APPLY check processing performs preliminary validation on SYSMODS individually. Carefully review the SMP generated reports, noting any possible regression of SYSMODS.
2. SMP APPLY processing may fail because of HELD SYSMODs. See the SMP RECEIVE output for details regarding the HELD SYSMOD. If action has been taken on the HELD SYSMOD and it is to be applied, add the following to the APPLYCHECK control statement:
`BYPASS(HOLDSYSTEM, HOLDERROR, HOLDUSER)`

Step 16. RESTORE Applicable SYSMODs

Maintenance SAMPJCL member W010MRES contains the control statements for SMP RESTORE processing. This step RESTOREs SMP USERMODS and APARS (SYSMODS) identified by APPLY check processing, to allow for PTF application. If you do not have any SYSMODs to RESTORE, you can continue to the next step.

Edit all JCL as necessary. Submit the job and verify that RESTORE processing ran successfully. If the SMP RESTORE completed with a return code greater than 4, then:

1. Review the output carefully before continuing
2. Correct the problem
3. Submit the job

We suggest the SMP APPLY check be executed again to verify that no additional SYSMODs inhibit the application of the new maintenance.

Step 17. APPLY CCS for z/OS and OS/390 Maintenance

Maintenance JCL member W010MAPP APPLYS all PTFs corresponding to CCS for z/OS and OS/390 maintenance.

Edit member W010MAPP to conform to your installation standards. Delete any DD statements within the SMP_CNTL DD statement that correspond to CCS for z/OS and OS/390 components not currently installed.

Edit all JCL as necessary. Submit the job and verify APPLY processing ran successfully. If the SMP APPLY completed with a return code greater than 4, do the following:

1. Review the output carefully before continuing
2. Correct the problem
3. Resubmit the job

PTFs in HOLD: SMP APPLY processing may fail because of HELD SYSMODs, PTFs placed in HOLD status by RECEIVE processing. Prior to running APPLY processing, review the output from the RECEIVE processing for any HOLDDATA entries. Scrutinize the entries carefully, and take action as necessary.

Once the entries have been resolved, use of the BYPASS(HOLDSYSTEM,HOLDERERROR,HOLDUSER) may be added to the APPLY SELECT statement to APPLY any held PTFs.

Step 18. Reapply Applicable SYSMODs

Review all the usermods and APARS RESTORED by Step 15 (RESTORE Applicable SYSMODs). If no applicable SYSMODs were restored, skip to the next step.

SYSMODs identified by APPLY check processing may be at a higher level than the PTFs contained on the CCS for z/OS and OS/390 tape. APARS can be cross-checked using SMP. If the current status of an APAR in question is SUP, then the SYSMOD for that APAR does not need to be reapplied.

Edit member W010MRAP to conform to your installation standards.

Edit all JCL as necessary. Submit the job and verify APPLY processing ran successfully. If the SMP APPLY completed with a return code greater than 4, then do the following:

1. Review the output carefully before continuing
2. Correct the problem
3. Resubmit the job

Note: SMP can handle only one update per element per APPLY select statement. It may be necessary in reAPPLYing applicable SYSMODS to use multiple APPLY select sentences.

Step 19. Start Up Datacom/TR with Trigger Server

This step is required for: WorldView

Task 19a. Start Up CAIENF and CAICCI

If CAIENF and CAICCI are not already active on the system, you must first start CAIENF. CAICCI runs as a subsystem within the CAIENF address space. Follow the CAIENF and CAICCI Post-Installation tasks for instructions on how to customize CAIENF and CAICCI and then to finally start CAIENF.

Task 19b. Start Up Datacom/TR with the Trigger Server

If WorldView is being installed, the next job requires that the trigger server be active. SAMPJCL member TRINSTRG will start Datacom/TR with the trigger server.

Step 20. Create Links for Event Management

This step is required for: Event Management

SAMPJCL member TNGBLDEM will create the links required for Event Management.

Step 21. Create Links for WorldView

This step is required for: WorldView

SAMPJCL member TNGBLDWV will create the links required for WorldView.

Step 22. Save All Materials and Output

Be sure to save all of your maintenance materials and all output from the maintenance process. This material is essential for timely and accurate Computer Associates maintenance and support of the product.

Installation Checklists

This appendix contains a checklist of the steps involved in installing each component of CCS for z/OS and OS/390. You will find a checklist for each of the following components:

Event Management Common	EARL Service
WorldView	SRAM Service
CAIRIM	CA-C Runtime
CAIENF	CAIVPE
CAISSF	ViewPoint
CAICCI	CA-MFLINK
CAIENF/CICS	CA-L-Serv
CAIENF/CICS SPAWN	CA-Agent Technologies
CAIENF/DB2	CA-GSS
CAIENF/PIGware	CA-XPS

Event Management Common Installation Checklist



Step

Step 1. Visit Support page.

Step 2. Load installation SAMPJCL library.

Step 3. Download BookManager files.

Step 4. Download PDF files.

Step 5. Review System Requirements.

Step 6. Complete the Installation worksheet.

Step 7. Modify sample JOBCARD.

Step 8. Modify TNGVARS member.

Step 9. Allocate target and distribution libraries.

Step 10. Allocate private SMP/E libraries.

Step 11. Customize the SMP DDDEFS.

Step 12. Customize the EM DDDEFS.

Step 13. Allocate Event Management and WorldView HFS file.

Step 14. Create the required directories.

Step 15. Create Event Management and WorldView Profile.

Step 20. Event Management and WorldView downloads.

Step 21. RECEIVE CCS for z/OS and OS/390.

Step 28. APPLY CCS for z/OS and OS/390.

✓ **Step**

Step 34. Allocate CA-Datcom/TR SMP/E and Database Data Sets.

Step 35. Load CA-Datcom/TR SMP/E Libraries.

Step 36. Rename DDDEFs for CA-Datcom/TR.

Step 37. Assemble/Link Custom Modules.

Step 38. Customize TNG.

Step 39. Install CA-Datcom/TR SVC.

Step 40. Load CA-Datcom/TR Databases from tape.

Step 41. Start Up Multi-User.

Step 42. Reset HSD file.

Step 43. Back Up CXX and DataDictionary.

Step 44. Create links for Event Management.

Step 49. Shut down Multi-User.

Step 57. ACCEPT CCS for z/OS and OS/390.

Step 58. Save all materials and output.

Step 59. Post-Installation steps.

WorldView Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFS.
	Step 12. Customize the EM DDDEFS.
	Step 13. Allocate Event Management and WorldView HFS file.
	Step 14. Create the required directories.
	Step 15. Create Event Management and WorldView Profile.
	Step 20. Event Management and WorldView downloads.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 28. APPLY CCS for z/OS and OS/390.
	Step 45. Start Up Multi-User with Trigger Server.
	Step 47. Create links for WorldView.
	Step 48. Shut down Trigger Server.
	Step 49. Shut down Multi-User.
	Step 57. ACCEPT CCS for z/OS and OS/390.

✓ Step

Step 58. Save all materials and output.

Step 59. Post-Installation steps.

CAIRIM Installation Checklist

✓ Step

Step 1. Visit Support page.

Step 2. Load installation SAMPJCL library.

Step 3. Download BookManager files.

Step 4. Download PDF files.

Step 5. Review System Requirements.

Step 6. Complete the Installation worksheet.

Step 7. Modify sample JOBCARD.

Step 8. Modify TNGVARS member.

Step 9. Allocate target and distribution libraries.

Step 10. Allocate private SMP/E libraries.

Step 11. Customize the SMP DDDEFS.

Step 21. RECEIVE CCS for z/OS and OS/390.

Step 28. APPLY CCS for z/OS and OS/390.

Step 32. APF Authorize the CAILIB Data Set.

Step 57. ACCEPT CCS for z/OS and OS/390.

Step 58. Save all materials and output.

Step 59. Post-Installation steps.

CAIENF Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFs.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 28. APPLY CCS for z/OS and OS/390.
	Step 32. APF Authorize the CAILIB Data Set.
	Step 33. Define or upgrade the CAIENF Database.
	Step 57. ACCEPT CCS for z/OS and OS/390.
	Step 58. Save all materials and output.
	Step 59. Post-Installation steps.

CAISSF Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFs.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 28. APPLY CCS for z/OS and OS/390.
	Step 57. ACCEPT CCS for z/OS and OS/390.
	Step 58. Save all materials and output.
	Step 59. Post-Installation steps.

CAICCI Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFs.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 28. APPLY CCS for z/OS and OS/390.
	Step 33. Define or upgrade the CAIENF Database.
	Step 50. Link-edit CAICCI Release 1.1 for TCP/IP.
	Step 57. ACCEPT CCS for z/OS and OS/390.
	Step 58. Save all materials and output.
	Step 59. Post-Installation steps.

CAIENF/CICS Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFS.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 28. APPLY CCS for z/OS and OS/390.
	Step 33. Define or upgrade the CAIENF Database.
	Step 57. ACCEPT CCS for z/OS and OS/390.
	Step 58. Save all materials and output.
	Step 59. Post-Installation steps.

CAIENF/CICS SPAWN Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFs.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 28. APPLY CCS for z/OS and OS/390.
	Step 33. Define or upgrade the CAIENF Database.
	Step 57. ACCEPT CCS for z/OS and OS/390.
	Step 58. Save all materials and output.
	Step 59. Post-Installation steps.

CAIENF/DB2 Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFS.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 28. APPLY CCS for z/OS and OS/390.
	Step 33. Define or upgrade the CAIENF Database.
	Step 57. ACCEPT CCS for z/OS and OS/390.
	Step 58. Save all materials and output.
	Step 59. Post-Installation steps.

CAIENF/PIGware Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFs.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 28. APPLY CCS for z/OS and OS/390.
	Step 33. Define or upgrade the CAIENF Database.
	Step 57. ACCEPT CCS for z/OS and OS/390.
	Step 58. Save all materials and output.
	Step 59. Post-Installation steps.

EARL Service Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFS.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 22. Copy and modify the EARL option source member.
	Step 28. APPLY CCS for z/OS and OS/390.
	Step 57. ACCEPT CCS for z/OS and OS/390.
	Step 58. Save all materials and output.
	Step 59. Post-Installation steps.

SRAM Service Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFs.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 28. APPLY CCS for z/OS and OS/390.
	Step 57. ACCEPT CCS for z/OS and OS/390.
	Step 58. Save all materials and output.
	Step 59. Post-Installation steps.

CA-C Runtime Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFs.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 28. APPLY CCS for z/OS and OS/390
	Step 54. Establish Site Defaults for CA-C Runtime.
	Step 57. ACCEPT CCS for z/OS and OS/390.
	Step 58. Save all materials and output.
	Step 59. Post-Installation steps.

CAIVPE Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFs.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 28. APPLY CCS for z/OS and OS/390.
	Step 57. ACCEPT CCS for z/OS and OS/390.
	Step 58. Save all materials and output.
	Step 59. Post-Installation steps.

ViewPoint Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFS.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 28. APPLY CCS for z/OS and OS/390.
	Step 53. Allocate the ViewPoint Profile.
	Step 57. ACCEPT CCS for z/OS and OS/390.
	Step 58. Save all materials and output.
	Step 59. Post-Installation steps.

CA-MFLINK Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFs.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 28. APPLY CCS for z/OS and OS/390.
	Step 57. ACCEPT CCS for z/OS and OS/390.
	Step 58. Save all materials and output.
	Step 59. Post-Installation steps.

CA-L-Serv Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFs.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 28. APPLY CCS for z/OS and OS/390.
	Step 57. ACCEPT CCS for z/OS and OS/390.
	Step 58. Save all materials and output.
	Step 59. Post-Installation steps.

CA-Agent Technologies Installation Checklist

✓	Step
	Step 1. Visit Support page.
	Step 2. Load installation SAMPJCL library.
	Step 3. Download BookManager files.
	Step 4. Download PDF files.
	Step 5. Review System Requirements.
	Step 6. Complete the Installation worksheet.
	Step 7. Modify sample JOBCARD.
	Step 8. Modify TNGVARS member.
	Step 9. Allocate target and distribution libraries.
	Step 10. Allocate private SMP/E libraries.
	Step 11. Customize the SMP DDDEFS.
	Step 16. Modify AGENTVARS.
	Step 17. Create Agent Technologies install directory.
	Step 18. Initialize SMP/E for Agent Technologies.
	Step 19. Download Agent Technologies Libraries.
	Step 21. RECEIVE CCS for z/OS and OS/390.
	Step 23. Prelink CA-Agent Technologies modules.
	Step 24. Create Userid for Agent Technologies.
	Step 25. Allocate CA-Agent Technologies HFS.
	Step 26. Update INSTPAX member.
	Step 27. Expand Agent Technologies tarfile.
	Step 28. APPLY CCS for z/OS and OS/390.
	Step 29. Set mode bits for CA-Agent Technologies.
	Step 30. Set UID bits for CA-Agent Technologies.

✓ Step

Step 31. Initialize Agent Technologies files.

Step 57. ACCEPT CCS for z/OS and OS/390.

Step 58. Save all materials and output.

Step 59. Post-Installation steps.

CA-GSS Installation Checklist

✓ Step

Step 1. Visit Support page.

Step 2. Load installation SAMPJCL library.

Step 3. Download BookManager files.

Step 4. Download PDF files.

Step 5. Review System Requirements.

Step 6. Complete the Installation worksheet.

Step 7. Modify sample JOBCARD.

Step 8. Modify TNGVARS member.

Step 9. Allocate target and distribution libraries.

Step 10. Allocate private SMP/E libraries.

Step 11. Customize the SMP DDDEFs.

Step 21. RECEIVE CCS for z/OS and OS/390.

Step 28. APPLY CCS for z/OS and OS/390.

Step 32. APF Authorize the CAILIB Data Set.

Step 54. Allocate GSS ISET VSAM Data Sets.

Step 55. Compile and load IMOD files.

✓ **Step**

Step 56. Copy GSS option members to PPOPTION Data Set.

Step 57. ACCEPT CCS for z/OS and OS/390.

Step 58. Save all materials and output.

Step 59. Post-Installation steps.

CA-XPS Installation Checklist

✓ **Step**

Step 1. Visit Support page.

Step 2. Load installation SAMPJCL library.

Step 3. Download BookManager files.

Step 4. Download PDF files.

Step 5. Review System Requirements.

Step 6. Complete the Installation worksheet.

Step 7. Modify sample JOBCARD.

Step 8. Modify TNGVARS member.

Step 9. Allocate target and distribution libraries.

Step 10. Allocate private SMP/E libraries.

Step 11. Customize the SMP DDDEFs.

Step 21. RECEIVE CCS for z/OS and OS/390.

Step 28. APPLY CCS for z/OS and OS/390.

Step 57. ACCEPT CCS for z/OS and OS/390.

Step 58. Save all materials and output.

Step 59. Post-Installation steps.

Installation Worksheet

The installation and maintenance worksheet is designed to simplify modifying the supplied JCL. Answer each question on the worksheet, filling in the blanks with the appropriate information. Default values are noted. If the default value is acceptable, leave the item blank on the worksheet. However, you must supply appropriate volume serial numbers.

Installation and Maintenance Worksheet

Note: Since you may be using this worksheet at first for installation and then again in the future for maintenance, we suggest you store the completed copy in a binder so it will be readily available for future reference.

#	Item and Default Value	Name	Your Value
1	What is your installation generic unit name for permanent DASD volumes? Default: PERMDA=SYSDA	PERMDA=	_____
2	What is your installation generic unit name for temporary work DASD volumes? Default: WORKDA=SYSDA	WORKDA=	_____
3	What is your installation generic unit name for a 6250 BPI tape drive? Default: TAPE=TAPE	TAPE=	_____

#	Item and Default Value	Name	Your Value
4	What is your installation standard SYSOUT class for CA solution installs and SMP output? Default: SYSOUT=!*1	SYSOUT=	_____
5	Which DASD pack do you plan to use for the CCS for z/OS and OS/390 target libraries? Default: TGTVOL=	TGTVOL=	_____
6	Which DASD pack do you plan to use for the CCS for z/OS and OS/390 distribution libraries? Default: DLIBVOL=	DLIBVOL=	_____
7	What is the high-level qualifier for all data sets? Default: PREFIX='CAI.'	PREFIX=	_____
8	What VOLSER do you plan to assign to the SMP libraries for your installation of CA solutions? (If these libraries do not already exist, they will be cataloged and made permanent data sets). Default: SMPVOL=	SMPVOL=	_____
9	What is the high level qualifier for the current LE/370 libraries? Default: LE37PREF=CEE.	LE37PREF=	_____
10	What is the library name for the current Callable Systems Services libraries? Default: CSSLIB=SYS1.CSSLIB	CSSLIB=	_____

#	Item and Default Value	Name	Your Value
11	What is the library name for the TCPIP proc SYSTCPD DD statement? If your proc uses a member, be sure to include that as well. Default: TCPDATA='TCPIP.TCPIP.DATA'	TCPDATA=	_____
12	What is the hlq name for the TCPIP data sets? These are the libraries where the TCPIP code and objects used for links reside. Default: TCPIP='TCPIP.'	TCPIP=	_____
13	Some of the data sets need to be allocated as type PDSE. These libraries can be either SMS or NON-SMS managed depending on your operating system. If you wish to use NON-SMS then change the 'XXXXXX' to a valid volume name. If you want to use SMS then change the 'VOL=SER=XXXXXX' to 'STORCLSS=storage class'. Default: PDSE='VOL=SER=XXXXXX'	PDSE=	_____
14	What is the VOLSER for the current tape? Default: TAPVOL=W02201	TAPVOL=	_____
15	What is the prefix used for your CICS data set names? Default: INDEX=CICS	INDEX=	_____
16	Which MVS Utility will be used to perform assemblies? Default: ASMBLR=ASMA90	ASMBLR=	_____
17	What is the name of the System macro library? Default: SYS1.MACLIB	SYSMAC=	_____

#	Item and Default Value	Name	Your Value
18	What data set names do you want to assign to the SMP libraries for your installation of CCS for z/OS and OS/390? Supply the DSName for the CDS (Control Data Set). SMP/E, supply the DSName for the CSI (Consolidated Software Inventory) file. (Skip this step if these data sets currently exist.)		
18a	Default: ()		
	SMP CDS=CAI.SMPCDS	SMPCDS=	_____
	SMPACDS=CAI.SMPACDS	SMPACDS=	_____
	SMPCRQ=CAI.SMPCRQ	SMPCRQ=	_____
	SMPACRQ=CAI.SMPACRQ	SMPACRQ=	_____
	SMPSCDS=CAI.SMPSCDS	SMPSCDS=	_____
	SMPMTS=CAI.SMPMTS	SMPMTS=	_____
	SMPPTS=CAI.SMPPTS	SMPPTS=	_____
	SMPSTS=CAI.SMPSTS	SMPSTS=	_____
	SMPHOLD=CAI.SMPHOLD	SMPHOLD=	_____
18b	Default: ()		
	SMPCSI=CAI.SMPCSI.CSI	SMPCSI=	_____
	SMPSCDS=CAI.SMPSCDS	SMPSCDS=	_____
	SMPMTS=CAI.SMPMTS	SMPMTS=	_____
	SMPPTS=CAI.SMPPTS	SMPPTS=	_____
	SMPSTS=CAI.SMPSTS	SMPSTS=	_____
18c	CSI Zones (SMP/E)		
	GLOBAL=GLOBAL	GLOBAL=	_____
	TARGET ZONE=CAITGT		
	DIST. ZONE=CAIDLIB		

Note: The next eight items refer to Event Management. If you are not installing Event Management, skip to item 28.

#	Item and Default Value	Name	Your Value
19	What is the HLQ for the CA-Datcom/TR libraries? This name must be different from the one used for the rest of the product. Default: TRHLQ='CAI.TNGRES'	TRHLQ=	_____
20	What is the volser or storage class to use for the CA-Datcom/TR target libraries? To use a volume change DASD01 to the correct volume. If you want to use a storage class change: VOL=SER=DASD01 to STORCLAS=your storage class. Default: TRVOLT='VOL=SER=DASD01'	TRVOLT=	_____
21	What is the volser or storage class to use for the CA-Datcom/TR SMP/E libraries? To use a volume change DASD01 to the correct volume. If you want to use a storage class change: VOL=SER=DASD01 to STORCLAS=your storage class. Default: TRVOLS='VOL=SER=DASD01'	TRVOLS=	_____
22	What is the volser or storage class to use for the CA-Datcom/TR dlib libraries? To use a volume change DASD01 to the correct volume. If you want to use a storage class, change: VOL=SER=DASD01 to STORCLAS=your storage class. Default: TRVOLD='VOL=SER=DASD01'	TRVOLD=	_____

#	Item and Default Value	Name	Your Value
23	<p>What is the volser or storage class to use for the CA-Datcom/TR DB libraries? To use a volume change DASD01 to the correct volume. If you want to use a storage class, change: VOL=SER=DASD01 to</p> <p>STORCLAS=your storage class.</p> <p>Default: TRVOLF='VOL=SER=DASD01'</p>	TRVOLF=	_____
24	<p>What is the unit to use for the CA-Datcom/TR target libraries?</p> <p>Default: TRUNIT='SYSDA'</p>	TRUNIT=	_____
25	<p>What is the unit to use for the CA-Datcom/TR SMP/E libraries?</p> <p>Default: TRUNIS='SYSDA'</p>	TRUNIS=	_____
26	<p>What is the unit to use for the CA-Datcom/TR dlib libraries?</p> <p>Default: TRUNID='SYSDA'</p>	TRUNID=	_____
27	<p>What is the unit to use for the CA-Datcom/TR DB libraries?</p> <p>Default: TRUNIF='SYSDA'</p>	TRUNIF=	_____
28	<p>What is the install path for Agent Technologies? (Agent Technology only)</p> <p>Default: AWORKDIR=/cai/agent</p>	AWORKDIR=	_____
29	<p>If installing the EARL Reporting Service, do you plan to use IMS DB support? If so, what is the name of your system IMS resident LOADLIB?</p> <p>Default: DFSRESLB=IMS.VS.DFSRESLB</p>	DFSRESLB=	_____

Note: The remaining items in this worksheet pertain to the ViewPoint service, and are required only if you are going to install that service.

#	Item and Default Value	Name	Your Value
30	Which DASD volume do you plan to use for the &pname1 profile libraries? No default	PVOL=	_____
31	What second-level qualifier do you plan to use for the &pname1 profile libraries? Default: SLQ='VPOINT'	SLQ=	_____

Index

A

- ACEE CA-GSS security, 2-42
- ADDRESS parameter
 - IDCAMS support, 5-23
- Agent Technology
 - description, 1-11
 - installing multiple systems, 4-23
 - post-installation tasks, 4-25
 - pre-installation tasks, 2-30
 - system requirements, 2-29
 - TCP/IP requirements, 2-30
- ALTNAME parameter
 - CA-VIEW support, 5-20

B

- Berkeley Syslog Daemon
 - overview, 4-12
 - rerouting messages, 4-13
- Browsers
 - Class Browser, 1-7
 - ObjectView, 1-7
 - Topology Browser, 1-7
- Business Process View, description, 1-5

C

- CA Common Services for z/OS and OS/390.
See CCS for z/OS and OS/390
- CA LMP
 - FMID, 2-46
 - SVC slot, 2-11
- CA PROFILE
 - system requirements, 2-29
- CA-ACF2
 - CAIENF installation considerations, 2-14
 - logon Ids for CAIENF, 2-14
- CA-ACF2 security for CA-L-Serv, 6-5
- CA-C Runtime
 - system requirements, 2-26
- CA-Datcom/TR
 - system requirements, 2-31
- CA-GSS
 - ACEE security, 2-42
 - copying procs, 5-2
 - customizing initialization parameters, 5-10
 - defining GOALNET, 5-24
 - defining ILOGs, 5-27
 - defining subsystem IDs, 5-2
 - enqueue requirements, 5-4
 - IMOD user ID, 2-43
 - installing IMOD editor, 5-3

-
- installing ISERVE Operator Control Panel, 5-7
 - ISERVE requirements, 2-39
 - logon facility, 5-28
 - memory requirements, 2-38
 - optional features, 5-24
 - preparing started task, 5-3
 - starting, 5-8
 - stopping, 5-9
 - system requirements, 2-37
 - testing, 5-8
 - testing IMOD editor, 5-9
 - testing the installation, 5-8
 - user ID, 2-43
- CAICCI
- downloading, 4-41, 4-42
 - installing
 - on client, 4-41
 - installing from z/OS, 4-42
 - modules, 4-41
 - system requirements, 2-22
 - transferring files from mainframe, 4-41, 4-42
- CAIENF, 2-14
- CA-ACF2 user installation considerations, 2-14
 - space requirements formula, 2-13
 - system requirements, 2-12
- CAIENF utilities
- storage requirements, 2-16
 - system requirements, 2-16
- CAIENF/CICS, 2-46
- system requirements, 2-17
- CAIENF/CICS SPAWN
- system requirements, 2-19
- CAIENF/DB2
- system requirements, 2-18
- CAIENF/USS
- system requirements, 2-20
- CA-Insight for DB2, customizing CA-GSS, 5-11
- CAIRIM
- system requirements, 2-10
- CAISSF
- for RACF and compatibles, 4-29
 - system requirements, 2-10
- CAIVPE
- installation considerations, 2-24
 - system requirements, 2-23
- CA-Jobtrac, customizing CA-GSS, 5-16
- Calendars, 1-10
- CA-L-Serv
- CA-ACF2 security, 6-5
 - CA-Top Secret security, 6-3
 - LU 0 and LU 6.2 communication, 6-9
 - message member, 6-12
 - RACF security, 6-6
 - security
 - enhancements, 6-1
 - SQL dictionary, 2-37
 - starting, 6-14
 - startup parameters, 6-10
 - startup procedure, 6-13
 - system requirements, 2-34
- CA-L-Serv Communications Server
- verifying installation, 6-15
- CA-L-Serv File Server
- verifying installation, 6-19
- CA-MFLINK
- system requirements, 2-24
- CA-OPS/MVS II, customizing CA-GSS, 5-16
- CAS9CSSF, 4-29
- CAS9DB, 2-14
- CAS9SAFC, 4-29
- CAS9SIA2, 4-29
- CA-Top Secret security for CA-L-Serv, 6-3
- CA-View, customizing CA-GSS, 5-18
- CA-XPS

system requirements, 2-45

CCIPCDOS.EXE, 4-41

CCIPCWIN.EXE, 4-41

CCS for z/OS and OS/390

agent technology, 1-11

architecture, 1-6

description, 1-3

installation worksheet, B-1

maintenance steps, 7-1

overview, 1-1

visualization services, 1-6

checklist

list of components, A-1

Class Browser, 1-7

Common Object Repository, 1-8

ObjectView, 1-7

common services, 1-11

CSA requirements

CAICCI, 2-22

CAIENF, 2-13

CAIENF/DB2, 2-18

CSIs for multiple system installs, 4-23

D

Date

controls, calendar, 1-10

DB2, customizing CA-GSS, 5-20

defining

CA-L-Serv to VTAM, 6-9

ENFplex, 4-37

GoalNet to VTAM, 5-27

subsystem Ids for CA-GSS, 5-2

dependencies, installation, 2-46

Discovery

discovering network devices, 1-8

Downloading installation files, 4-42

E

EARL

system requirements, 2-25

End-to-end management, 1-4

ENFplex

defining, 4-37

Event Management

Berkeley syslog daemon, 4-12

description, 1-9

distribution libraries, 2-9

installation requirements, 2-8

rerouting messages, 4-13

store and forward (SAF), 4-10

tasks

establish date and time controls,
1-10

F

FMIDs (functional sysmods), 2-46

functions

OPSVVALUE(), 5-18

G

GOALNET, CA-GSS option, 5-24

H

Help, how to access, 1-15

I

IDCAMS load module (for IDCAMS), 5-22

IDCAMS, customizing CA-GSS, 5-22

ILOGs, CA-GSS options, 5-27

IMOD editor, 5-6

initialization parameters, 5-18

installation

- CA-GSS ISERVE Operator Control Panel, 5-7
- CA-GSS, upgrading ISETs, 5-31
- CAICCI from z/OS, 4-42
- CAIENF/CICS, 2-17
- CA-L-Serv sysmods, 2-34
- checklist, list of components, A-1
- Customize CAISSF for RACF or RACF-Compatible Products, 4-29
- dependencies, 2-46
- installing multiple systems, 4-23
- phases, 2-1
- post-installation tasks, 4-1, 4-25
- pre-installation tasks for Agent Technology, 2-30
- steps, 3-1
- storage requirements, 2-5
- system requirements, 2-2
- worksheet, B-1
- XCF communication, 2-35

installation requirements

- CAIRIM/CAISSF, 2-10
- Event Management, 2-8
- Worldview, 2-9

installation verification

- CA-L-Serv Communications Server, 6-15
- CA-L-Serv File Server, 6-19

ISERVE

- CA-GSS requirements, 2-39

ISETs, upgrading, 5-31

L

learning about the product, 1-14

LMP, 2-11, 2-46

M

maintenance

- worksheet, B-1

maintenance steps, 7-1

modules in CAICCI, 4-41

Multiple system install, 4-23

O

ObjectView

- definition, 1-7

OPSVVALUE() function, 5-18

P

PIGware, 2-16

PIGware, See CAIENF utilities, 2-16

post-installation

- agent security, 4-23
- Agent Technology Services, 4-16
- Berkeley Syslog Daemon, 4-12
- CAICCI, 4-40
- CAIENF, 4-37
- CAIENF/USS, 4-40
- CAIRIM, 4-26
- enable catrapd, 4-15
- Event Management, 4-10
- Event Management server, 4-15

- initializing Java server, 4-9
- installing Java, 4-7
- Management Services, 4-2
- OS/390 USS, 4-4
- Repository, 4-3
- store and forward, 4-10
- web server, 4-5
- WorldView, 4-4
- WorldView security, 4-7

post-installation tasks, 4-1, 4-25

R

RACF security for CA-L-Serv, 6-6

S

SAF.CFG file, 4-11

security

- system for CA-L-Serv, 6-2

SQL dictionary

- CA-L-Serv, 2-37

SRAM

- system requirements, 2-26

SRVMaint program, 5-12, 5-28

Standard Security Facility

- CAS9SAFC, 4-29

- CAS9SIA2, 4-29

starting

- CA-GSS, 5-8

starting CA-L-Serv, 6-14

Store and Forward (SAF)

- activating, 4-10

- changing the interval, 4-11

- creating configuration file, 4-11

SVC for CA LMP, 2-11

syslogd configuration file, 4-13

system requirements

- Agent Technology, 2-29

- CA PROFILE, 2-29

- CA-C Runtime, 2-26

- CA-Datacom/TR, 2-31

- CA-GSS, 2-37

- CAICCI, 2-22

- CAIENF, 2-12

- CAIENF/CICS, 2-17

- CAIENF/CICS SPAWN, 2-19

- CAIENF/DB2, 2-18

- CAIENF/PIGware, 2-16

- CAIENF/USS, 2-20

- CAIRIM/CAISSF, 2-10

- CAIVPE, 2-23

- CA-L-Serv, 2-34

- CA-MFLINK, 2-24

- CA-XPS, 2-45

- EARL, 2-25

- SRAM, 2-26

- target libraries, 2-2

- ViewPoint, 2-27

T

technical support on the web, 1-15

testing

- CA-GSS, 5-8

- CA-GSS IMOD editor, 5-9

V

VIEW parameter, CA-VIEW support, 5-20

ViewPoint

- system requirements, 2-27

VTAM, defining CA-L-Serv to, 6-9

W

worksheet

for manual installation, B-1

WorldView

Class Browser, 1-7

distribution libraries, 2-10

installation requirements, 2-9

ObjectView, 1-7

Real World Interface, 1-6

security definitions, 2-9

Z

z/OS common services, 1-11