CA Chorus™

사이트 준비 안내서

버전 03.0.00, 세 번째 버전

ca technologies

CA Technologies 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- CA ACF2™ for z/OS(CA ACF2)
- CA Chorus™
- CA Chorus™ for DB2 Database Management
- CA Chorus™ Infrastructure Management for Networks and Systems
- CA Chorus™ for Security and Compliance Management
- CA Chorus™ for Storage Management
- CA Chorus™ Software Manager(CA CSM)
- CA Common Services for z/OS(CA Common Services for z/OS)
- CA Datacom®/AD(CA Datacom/AD)
- CA Datacom/DB®
- CA Easytrieve
- CA Top Secret® for z/OS(CA Top Secret)

CA 에 문의

기술 지원팀에 문의

온라인 기술 지원 및 지사 목록, 기본 서비스 시간, 전화 번호에 대해서는 http://www.ca.com/worldwide에서 기술 지원팀에 문의하십시오.

설명서 변경 사항

다음 목록에는 두 번째 버전 이후 변경된 내용이 자세히 설명되어 있습니다.

소프트웨어 요구 사항 (페이지 26) - CCS 및 CA CSM 에 대한 FIXCAT 요구 사항을 비롯하여 CA Datacom/AD MUF 를 생성하는 올바른 작업 순서에 대한 설명이 명확해졌습니다.

다음 목록에는 첫 번째 버전 이후 변경된 내용이 자세히 설명되어 있습니다.

예제: IBM RACF 를 사용하는 사용자에게 권한 부여 (페이지 54) - 1 단계의 CA Chorus for DB2 Database Management 참조 정보가 수정되었습니다. 이제 DB2DBA 로 나타납니다.

서버 요구 사항 (페이지 29) - 수정된 힙 값과 모든 전문 분야가 선택된 경우의 새로운 예가 추가되었습니다.

소프트웨어 요구 사항 (페이지 26) - 브라우저 요구 사항이 명확히 설명되고 IBM z/OS 지원 정보가 1.12 이상으로 업데이트되었습니다.

다음 목록은 이전에 *설치 안내서*에 나타났던 내용 중 변경된 사항이 자세히 설명되어 있습니다.

일반 - 이 안내서는 시스템 프로그래머와 보안 관리자가 제품 설치 이전에 완료해야 하는 작업을 알리기 위해 작성되었습니다.

설치 프로세스 작동 방식 (페이지 10) - 이 안내서와 *설치 안내서*를 사용하는 방법을 설명하기 위해 이 항목과 다이어그램이 추가되었습니다.

설치 전 계획 (페이지 13) - 이 신규 안내서와 새로운 HLQ 요구 사항 항목을 설명하기 위해 이 항목이 업데이트되었습니다.

보안 관리자 및 시스템 프로그래머 검사 목록 (페이지 14) - 이 안내서를 사용하기 전에 두 역할의 담당자가 동의해야 할 세부 정보를 간략히 나타내기 위해 이 항목이 추가되었습니다.

보안 ID 재사용 고려 사항 (페이지 20) - 2.0 및 2.5 보안 ID 를 재사용하는 고객을 위해 이 항목이 추가되었습니다.

시스템 요구 사항 (페이지 31) - 힙 메모리 요구 사항이 제거되었습니다.

CA Chorus 서버 요구 사항 (페이지 29) - 힙 메모리 요구 사항이 수정되어 이 신규 항목으로 이동했습니다.

메모리 제한 (페이지 30) - 이 항목이 추가되었습니다.

소프트웨어 요구 사항 (페이지 26)

- CCS 릴리스 14.1 및 CA Datacom/AD 버전 14 요구 사항이 명확히 설명되고, "IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 Release 0 Modification 0 Service **Release 2**(5655-W44)(선택적 JZOS batch launcher 포함)" 부분이 업데이트되었습니다.
- 필요한 PTF 는 RO56614 임을 나타내기 위해 CA CSM 요구 사항이 업데이트되었습니다.
- CA Datacom/AD 유지 관리에 사용하는 FIXCAT 레이블이 추가되었습니다.

대상 라이브러리 (페이지 32)

- CETJDATV, CETJSIDE, CETJZFS1 이 제거되었습니다.
- CETJJCL, CETJTOPN, CETJXML 및 TPV.AETJHFS 의 값이 업데이트되었습니다.

배포 라이브러리 (페이지 33)

- TPV.AETJJAR, AETJDATV 및 TPV.AETJSHSC 가 제거되었습니다.
- AETJJCL, AETJOPTN, AETJXML 및 TPV.AETJHFS 의 값이 업데이트되었습니다.

포트 요구 사항 (페이지 34) - 최대 요구 사항이 17 에서 12 로 업데이트되었습니다.

(선택 사항) SMTP 전자 메일 요구 사항 (페이지 35) - 플랫폼을 구성하는 동안 나중에 사용할 수 있도록 수집할 데이터를 설명하기 위해 이 항목이 추가되었습니다.

USS PARMLIB 요구 사항 (페이지 35) - USS PARMLIB 설정을 검사하는 명령이 추가되었습니다.

설치 관리자 보안 권한 (페이지 37) - FSACCESS 옵션이 정의되었습니다.

CA Chorus 보안 작업 실행 (페이지 38) - 이 항목이 추가되고, 이 작업으로 자동화된 이전 수동 작업 항목은 제거되었습니다.

CA Chorus 에서 작업할 사용자에게 권한을 부여하는 방법 (페이지 43)

- 이 시나리오는 *관리 안내서*에서 이 안내서로 이동했습니다.
- CA Chorus Infrastructure Management for Networks and Systems 및 AUTOREFRESH 리소스를 추가했습니다.
- "사용자 소프트웨어 요구 사항 검토"를 제거했습니다. 이 정보는 소프트웨어 요구 사항 (페이지 26)에 나타납니다.
- "(선택 사항) EXPLAIN 명령을 사용하여 보조 권한 부여 ID 사용을 위한 권한 부여"가 *CA Chorus for DB2 Database Management 사이트 준비 안내서*로 이동했습니다.

z/OS UNIX System Services 리소스에 액세스할 수 있도록 CA Chorus 사용자에게 권한 부여 (페이지 45) - 이러한 설정이 이미 존재하는지 확인할 수 있도록 사전 검사 단계가 추가되었습니다.

CA Chorus 에 대한 CA CSM PassTicket 구성 방법 (페이지 57) - ETJI095*x* 보안 작업에서 다룬 단계를 설명하기 위해 이 시나리오가 업데이트되었습니다.

CA Chorus 에 대한 CA CSM PassTicket 구성 방법 (페이지 57) - 이 시나리오가 추가되었습니다.

예제: IBM RACF 를 사용하는 사용자에게 권한 부여 (페이지 54) - 각 전문 분야 리소스를 CAMFC 에 추가할 수 있도록 새로운 1 단계가 추가되었습니다.

CA Chorus 보안 작업 실행 (페이지 38) - "CA CSM 사용자에 대한 PassTicket" 하위 항목을 추가하도록 이 시나리오가 업데이트되었습니다.

목차

제 1 장: 소개

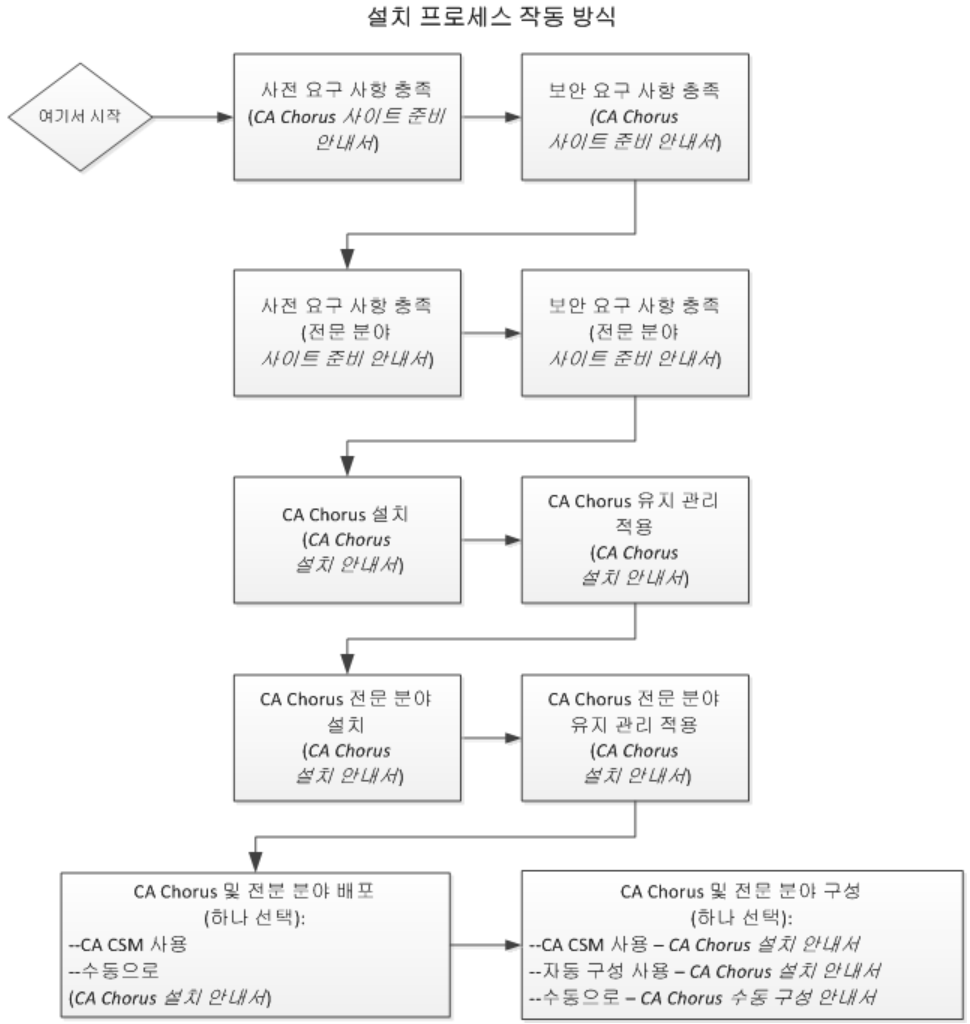
이 섹션은 다음 항목을 포함하고 있습니다.

설치 프로세스 작동 방식

이 안내서에는 시스템 프로그래머 및 보안 관리자가 *설치 안내서*에 설명된 설치, 배포 및 구성 작업을 시작하기 전에 완료할 수 있는 작업이 자세히 설명되어 있습니다. 다음 다이어그램에는 CA Chorus 와 전문 분야의 설치, 배포 및 구성 프로세스에 대한 개략적인 개요와 사용할 안내서가 나와 있습니다.

중요! CA Chorus 및 전문 분야는 CA Chorus Software Manager 를 사용하여 설치해야 합니다.

참고: 전문 분야 *사이트 준비 안내서*의 작업을 나타내는 상자의 경우 설치하는 각 전문 분야마다 해당 단계를 반복해야 합니다.



CA Chorus 및 전문 분야를 설치, 배포 및 구성하려면 다음 단계를 완료하십시오.

1. *CA Chorus 사이트 준비 안내서*에 설명된 대로 소프트웨어, 시스템 포트 및 기타 사전 요구 사항을 충족합니다.
2. CA Chorus *사이트 준비 안내서*에 설명된 대로 보안 요구 사항을 충족합니다.
3. 해당 전문 분야의 *사이트 준비 안내서*에 설명된 대로 소프트웨어, 시스템 포트 및 기타 사전 요구 사항을 충족합니다. 설치하는 각 전문 분야에 대해 이 단계를 반복합니다.
4. 해당 전문 분야의 *사이트 준비 안내서*에 설명된 대로 보안 요구 사항을 충족합니다. 설치하는 각 전문 분야에 대해 이 단계를 반복합니다.
5. *CA Chorus 설치 안내서*에 설명된 대로 CA CSM 을 사용하여 CA Chorus 및 해당 전문 분야를 설치합니다. 이 단계에는 CA Chorus 소프트웨어를 취득(z/OS 시스템으로 전송)하여 SMP/E 를 통해 설치하는 작업이 포함되어 있습니다. 설치 프로세스를 통해 CSI 환경이 생성되고 RECEIVE, APPLY 및 ACCEPT SMP/E 단계가 실행됩니다. 소프트웨어가 적절하게 조정되지 않은 상태입니다.
6. CA CSM 또는 수작업을 통해 CA Chorus 및 전문 분야를 배포합니다. 두 방법 모두 *CA Chorus 설치 안내서*에 자세히 설명되어 있습니다.

   이 단계를 수행하면 대상 라이브러리가 다른 시스템 또는 LPAR 에 복사됩니다.

   중요! CA CSM 에서 배포하는 경우 CA Chorus 및 전문 분야를 동시에 배포해야 합니다. 예를 들어 CA Chorus, DBA 및 Security 를 설치한 후 CA Chorus 및 DBA 만 배포하는 것은 지원되지 않습니다.

   중요! CA CSM Software Configuration Service 를 사용하려면 CA CSM 을 배포해야 합니다.

7. CA Chorus 및 전문 분야를 구성합니다. 이 단계에서 사용자 지정된 로드 모듈을 생성하고 CA Chorus 소프트웨어를 실행 가능한 상태로 만듭니다. 다음 방법 중 하나를 사용하여 제품을 구성합니다.

   참고: 가장 효율적인 방법인 처음 두 옵션 중 하나를 사용하여 제품을 구성하는 것이 좋습니다.

   CA CSM

   이 방법을 사용하면 마법사 기반 CA CSM 도구를 사용하여 제품을 구성할 수 있습니다.

   이 방법에 대한 CA Chorus 및 전문 분야 단계는 *설치 안내서*에 수록되어 있습니다.

   자동화된 구성

   이 방법을 사용하여 하나의 배치 작업(ETJICUST) 및 하나의 구성 파일을 편집할 수 있습니다. 그러면 Java 프로그램에 의해 변경 내용이 해당 멤버에 전파됩니다. 그리고 각 작업은 사용자가 수동으로 제출합니다. 이 옵션의 경우 플랫폼과 전문 분야를 동시에 구성하는 것이 좋습니다.

   이 방법에 대한 CA Chorus 및 전문 분야 단계는 *설치 안내서*에 수록되어 있습니다.

   수작업

   이 방법을 사용하여 각 구성 작업을 수동으로 편집하고 실행할 수 있습니다.

   이 방법의 경우 *Manual Configuration Guide*(수동 구성 안내서)를 참조하여 CA Chorus 및 전문 분야를 구성합니다.

제 2 장: 일반 사전 요구 사항 설명

이 장에서는 시스템 프로그래머가 CA Chorus 설치, 배포 및 구성 작업을 시작하기 전에 완료해야 하는 모든 작업이 자세히 설명되어 있습니다.

이 섹션은 다음 항목을 포함하고 있습니다.

설치 전 계획

CA Chorus 설치는 여러 분야의 전문 지식을 갖춘 사람들이 수행해야 하는 세부적인 프로세스입니다. 설치를 시작하기 전에 다음과 같은 팀 구성원들이 참여하는 모임을 갖고 각자의 역할을 검토하는 것이 좋습니다.

- z/OS 를 위한 시스템 프로그래머
- DASD 할당을 위한 저장소 관리자
- 액세스 권한 및 보안 구성을 위한 보안 관리자
- DB2 및/또는 CA Datacom/AD 구성을 위한 데이터베이스 관리자

이 모임에서 다음 항목을 사용하는 것이 좋습니다.

- 보안 관리자 및 시스템 프로그래머 검사 목록 (페이지 14)
- 플랫폼 및 해당 전문 분야의 *사이트 준비 안내서*
- *설치 안내서*
- 해당 보안 작업 ETJI095*x*(여기서 x 는 CA ACF2 의 경우 A 를, CA Top Secret 의 경우 T 를, IBM RACF 의 경우 R 을 나타냄). 이러한 작업은 CA Chorus 제품 페이지*에 있습니다.*

중요! 모든 팀원이 각자 맡은 설치 작업에 대해 명확히 이해할 때까지 설치를 시작하지 마십시오. 이렇게 하지 않으면 설치를 제시간에 완료하는 데 문제가 있을 수 있습니다.

보안 관리자 및 시스템 프로그래머 검사 목록

이 섹션의 각 표에는 설치 세부 정보가 간략하게 정리되어 있습니다. 보안 관리자 및 시스템 프로그래머가 각 표를 함께 검토하는 것이 좋습니다. 검토한 후 두 관리자는 이 안내서와 *설치 안내서*의 작업을 각자 시작하기 전에 특정 세부 정보를 동의하거나 서로 알고 있어야 합니다.

표의 일부 항목에 대해 동의한 값을 지정합니다. 그 외의 항목은 단순히 구현 세부 정보를 조정하면 됩니다.

중요! 이러한 검사 목록의 작업을 완료할 때까지 다른 준비 또는 설치 절차를 시작하지 마십시오. 예를 들어 보안 설정 및 제품 구성에 대한 표에는 값을 지정해야 합니다.

보안 고려 사항

다음 표에서

- 보안 심볼 앞에는 & 또는 %가 옵니다. 이러한 심볼은 보안 관리자가 실행하는 ETJI095*x* 보안 작업에 나타납니다.

  %

  기본값을 나타냅니다.

  &

  값을 결정해야 함을 나타냅니다.

- 음영으로 표시된 셀은 값을 기록할 필요는 없지만 이 안내서의 작업을 시작하기 전에 내용을 검토해야 함을 나타냅니다.

ID 또는 보안 항목	정의	값	심볼
CHORGRP	CA Chorus 관리 그룹(선택 사항) 기본 그룹 이름을 지정합니다.		%CHORGRP
CHORUGRP	CA Chorus 사용자 그룹(선택 사항) 개인 사용자가 아닌 그룹에 리소스를 할당하여 관리 작업을 지원합니다.		&CHORUGRP
CA Chorus Discipline Group	개인 사용자가 아닌 그룹에 리소스를 할당하여 관리 작업을 지원합니다. 사용자는 자신의 업무에 필요한 전문 분야 그룹에 연결됩니다. 실제 명명 표준 및 조직 구조에 따른 이름을 사용하는 것이 좋습니다.		&CHRD*x*GRP (여기서 x 는 전문 분야를 식별함)
CHORADM	관리자(시작된 작업의 소유자): ■ 시작된 작업을 소유합니다. ■ OMVS 세그먼트가 있어야 합니다. ■ 사용자에 대한 PassTicket 생성에 사용됩니다. **참고:** 홈 디렉터리를 CA Chorus USS 설치 디렉터리와 동일한 위치로 하는 것이 좋습니다.		%CHORADM

ID 또는 보안 항목	정의	값	심볼
CHORTHD	보조 사용자: ■ 로그인한 사용자가 없는 경우 백엔드 기능에 액세스할 때 사용자 ID 로만 사용됩니다. 기본적으로는 시작 시 구성 데이터를 가져오는 데 사용됩니다. ■ PassTicket 생성에 사용됩니다. 작업 또는 온라인 액세스에 사용자 ID 가 직접적으로 사용되지는 않습니다. 이 사용자 ID 의 암호에 액세스하는 사용자가 없어야 합니다. RACF 의 경우 암호가 필요합니다. CA ACF2 또는 CA Top Secret 에서는 암호를 사용하지 않습니다. ■ CHORJBOS 는 CHORTHD 에 대해 PassTicket 을 생성할 수 있어야 하며 CHORTHD 에는 적절한 응용 프로그램(APPLID)에 대한 액세스 권한이 부여되어야 합니다. ■ 다음 항목에 대한 권한을 제외하고 CA Chorus 사용자와 동일한 보안 권한이 필요합니다. -- CAMFC -- CETJOPTV CETJEZTR(CA Easytrieve 보고서 실행용) ■ 일부 전문 분야에는 백엔드 제품에 액세스하기 위해 CHORTHD 권한이 필요할 수 있습니다. 자세한 내용은 해당 전문 분야의 *사이트 준비 안내서*를 참조하십시오.		%CHORTHD
Installer ID	설치 관리자의 사용자 ID 에는 HLQ 및 데이터 집합에 대한 업데이트 액세스 권한이 있어야 합니다. 설치 이후 업데이트 권한이 해지될 수 있습니다. 자세한 전체 내용은 설치 관리자 보안 권한 (페이지 37)을 참조하십시오.		&INSTALLER

ID 또는 보안 항목	정의	값	심볼
PassTicket	PassTicket 리소스는 CA Chorus 플랫폼에 필요합니다. 전문 분야에는 추가 PassTicket 정의가 필요합니다. PassTicket 액세스는 그룹에 대해 정의될까요, 아니면 개인에 대해 정의될까요? ■ 그룹은 관리가 더 용이하며, 분산 구성을 더 많이 허용할 수 있습니다. 그룹 권한은 중앙 보안에 유지되며 로컬(그룹) 관리자가 멤버쉽을 관리할 수 있습니다. ■ 일부 사이트에서는 사용자별 액세스 권한이 명시적으로 표시되는 방식을 선호할 수도 있습니다.		
	보안 관리자는 각 응용 프로그램에 대해 KEYMASKED 또는 SESSKEY 값을 선택해야 합니다. 하지만 이들 값은 보호되어야 하므로 여기에 입력하지는 않습니다. 모든 시스템에서 응용 프로그램별로 동일한 값이 사용되어야 합니다.		
	CHORWEBS: 사용자에 대해 PassTicket 이 생성되는 기본 응용 프로그램 ID 입니다. 다른 APPL 을 사용하려면 해당 값을 확인하고 기록해야 합니다.		%CHORWEBS
	CSMAPPLM: "Quick Links"(빠른 링크) 모듈에서 CA CSM 을 시작한 사용자에 대해 PassTicket 이 생성되는 기본 응용 프로그램 ID 입니다. 다른 APPL 을 사용하려면 해당 값을 확인하고 기록해야 합니다. 이러한 단계는 ETJI095*x* 에 위치하지 않습니다. 자세한 내용은 CA CSM PassTicket 을 구성하는 방법 (페이지 57)을 참조하십시오. CA CSM 을 빠른 링크로 추가하지 않는 경우 이 옵션을 무시하십시오.		&CSMAPPLM

ID 또는 보안 항목	정의	값	심볼
CAMFC	CAMFC 는 구체적으로 CA Chorus 를 위한 리소스 클래스입니다. 클래스 이름 및 항목은 고정되어 있습니다. 플랫폼에 대한 항목은 CHORUS.SETTINGS.KNOWLEDGECENTER 하나입니다. Knowledge Center 에서 사용자 문서를 업데이트하거나 유지 관리할 사용자에게는 이 항목이 필요합니다. 이 클래스에 전문 분야별 항목이 하나씩 있습니다. 전문 분야에 대한 그룹에는 전문 분야 항목에 대한 읽기 액세스 권한이 허용되어야 합니다.		
CAWEBSVR Master Facility	CA Top Secret 에만 해당: 사용자를 정의하여 이 Master Facility 에 추가해야 합니다.		
Program Control(APF 허가)	시작된 작업의 STEPLIB 에서 명명된 데이터 집합은 프로그램 제어 하에 있어야 합니다. CA ACF2 또는 CA Top Secret 을 사용하는 사이트의 경우 이러한 라이브러리는 APF 허가를 받아야 합니다.		
	Runtime Environment 용 HLQ 가 있는 라이브러리: ■ CETJPLD: CA Chorus 라이브러리가 포함됩니다. ■ CETJLOAD: CA Chorus 라이브러리가 포함됩니다. ■ CC2DLOAD: TSF(Time Series Facility) 라이브러리가 포함됩니다.		
	CA Datacom/AD 사전 요구 사항을 충족하려면 *datacomad_adthlq*.CAAXLOAD(CA Datacom/AD 로드 라이브러리) 및 *datacomad_adchlq*.CUSLIB(CA Datacom/AD 사용자 지정 라이브러리) 라이브러리가 APF 허가되어야 합니다.		

ID 또는 보안 항목	정의	값	심볼
	(IBM RACF 만 해당) CA Chorus 이외의 라이브러리 CA Chorus 에서 사용되는 라이브러리가 Linklist 에는 있지만 CA Chorus 에서 명시적으로 명명되지 않은 경우라도 프로그램 제어 하에 있어야 합니다. 이러한 라이브러리는 해당 제품이 설치되었지만 시스템 관리자가 해당 구성을 확인해야 하는 경우 프로그램 제어에 추가될 수 있습니다. 시스템 프로그래머는 사이트 관련 이름을 제공해야 합니다. ■ Java v7 m0 라이브러리: &JAVALIB ■ CCS.CAW0LINK: CA CCS 라이브러리 - 릴리스 14.1(릴리스 2.5 CA Chorus 용) ■ TCPIP.SEZALOAD - ■ SYS1.CSSLIB: A C++ 라이브러리(IBM)		

추가 정보:

CA Chorus 보안 작업 실행 (페이지 38)

보안 ID 재사용 고려 사항

버전 3.0 보안 ID 구현에서 변경된 다음 사항을 참고하십시오. 버전 2.0 또는 릴리스 2.5 의 보안 ID 를 재사용하는 경우 다음 개체를 3.0 구현 환경에 추가해야 합니다. 이러한 변경과 관련된 예제 명령을 보려면 해당 ETJI095*x* 작업을 참조하십시오. 이 작업에서 *x* 는 CA ACF2 의 경우 A 를, CA Top Secret 의 경우 T 를, IBM RACF 의 경우 R 을 나타냅니다.

중요! 버전 3.0 에는 외부 CA Datacom/AD MUF(Multi-User Facility)가 필요합니다. 따라서 MUF 를 실행하는 데이터 집합을 알고 있어야 합니다.

CA ACF2

사용자 ID CHORTHD: PassTicket 을 사용하는 로그인의 보조 로그인 ID 입니다.

CAMFC: 새 SETTINGS.AUTOREFRESH 기능에 대한 CA Chorus 플랫폼 리소스입니다.

규칙: CA Datacom/AD 의 사용자 지정 라이브러리 CUSLIB

CA Chorus Software Manager Quick Links(선택 사항)

CA Top Secret

ACID %CHORTHD: PassTicket 을 사용하는 로그인의 보조 로그인 ID 입니다.

PROFILE %CHORUPF: CA Chorus 사용자 프로필(선택 사항)

CAMFC: 새 SETTINGS.AUTOREFRESH 기능에 대한 CA Chorus 플랫폼 리소스입니다.

데이터 집합: CA Datacom/AD 의 사용자 지정 라이브러리 CUSLIB

CA Chorus Software Manager Quick Links(선택 사항)

IBM RACF

USERID %CHORTHD: PassTicket 을 사용하는 로그인의 보조 로그인 ID 입니다.

GROUP %CHORUGRP: CA Chorus 사용자용 그룹(선택 사항)

CAMFC: 새 SETTINGS.AUTOREFRESH 기능에 대한 CA Chorus 플랫폼 리소스입니다.

데이터 집합: CA Datacom/AD 의 사용자 지정 라이브러리 CUSLIB

특정 라이브러리용 일반 데이터 집합 프로필

CA Chorus Software Manager Quick Links(선택 사항)

추가 정보:

CA Chorus 보안 작업 실행 (페이지 38)

데이터 집합 고려 사항

다음 표에서

- 보안 심볼 앞에는 & 또는 %가 옵니다. 이러한 심볼은 보안 관리자가 실행하는 ETJI095*x* 보안 작업 (페이지 38)에 나타납니다.

  %

  기본값을 나타냅니다.

  &

  값을 결정해야 함을 나타냅니다.
- 음영으로 표시된 셀은 값을 기록할 필요는 없지만 이 안내서의 작업을 시작하기 전에 내용을 검토해야 함을 나타냅니다.

데이터 집합	고려 사항	값	심볼
기존 데이터 집합	이전에 데이터 집합이 보안 제품에 정의되지 않은 경우 CA Chorus ID 를 기준으로 액세스 권한을 허용하기 전에 그룹 및 프로필을 정의해야 할 수도 있습니다.		
	TCP/IP 시작된 작업의 SYSTCPD DD 문에 명명된 라이브러리의 데이터 집합이나 멤버는 CHORADM(읽기 전용)에 사용할 수 있어야 합니다. 이 데이터 집합은 시스템별로 다릅니다.		&TCPDATA
	Java v7 라이브러리를 CHORADM 및 CHORUGRP(읽기 전용)가 사용할 수 있어야 합니다.		&JAVALIB

데이터 집합	고려 사항	값	심볼
	USS(UNIX System Service)의 Java 홈 디렉터리를 CHORADM 이 읽을 수 있어야 합니다. 또한 FSACCESS 가 사용되는 경우 마운트된 파일 시스템에 대한 읽기 FSACCESS 도 필요할 수 있습니다.		@JAVA_HOME **참고:** 보안상의 이유로 이 값이 필요하지 않지만 여기에 마운트되는 데이터 집합은 필요할 수 있습니다.
CA Chorus 설치 데이터 집합	팀원들은 CA Chorus 설치의 HLQ 에 동의해야 합니다. **참고**: 설치 HLQ 은 런타임 환경과 다릅니다. 둘 모두를 정의해야 할 수 있습니다. 이들 항목에 대한 기본값은 제공되지 않습니다. 예제 JCL 에서는 런타임 환경을 설정하는 명령이 제공됩니다.		
	HLQ: 설치 환경		없음
	HLQ: 런타임 환경		$CAI @RT_HLQ
런타임 데이터 집합	CA Chorus 의 추가 HLQ		
	VSAM 데이터 집합의 HLQ 입니다. 사이트 표준에 따라 VSAM 파일에 특정 할당 요구 사항이 필요한 경우 VSAM 데이터 집합에 다른 HLQ 를 할당할 수 있습니다.		$TSF
	데이터베이스 파일의 HLQ 입니다. CA Chorus 에 사용되는 CA Datacom/AD 데이터 파일을 구분하려 할 수 있습니다. 이러한 파일은 구체적으로 CA Chorus 를 위해 생성된 MUF 에 사용됩니다.		$ADHLQ

데이터 집합	고려 사항	값	심볼
CA Datacom/AD 설치 데이터 집합	CA Chorus 에 사용하는 경우 다음 런타임 HLQ 가 필요합니다. 자세한 내용은 *CA Datacom/AD Installation Guide*(CA Datacom/AD 설치 안내서)를 참조하십시오.		
	CAAXLOAD 를 포함하여 CA Datacom/AD 시스템 라이브러리입니다. HLQ 를 기록하십시오.		&ADTHLQ
	CA Chorus 인스턴스 관련 라이브러리(CUSLIB)입니다. HLQ 를 기록하십시오.		&ADCHLQ

시작된 작업 고려 사항

다음 표에서

- 보안 심볼 앞에는 & 또는 %가 옵니다. 이러한 심볼은 보안 관리자가 실행하는 ETJI095*x* 보안 작업 (페이지 38)에 나타납니다.

  %

  기본값을 나타냅니다.

  &

  값을 결정해야 함을 나타냅니다.

음영으로 표시된 셀은 값을 기록할 필요는 없지만 이 안내서의 작업을 시작하기 전에 내용을 검토해야 함을 나타냅니다.

참고: 또한 전문 분야를 사용하려면 관련 제품의 작업 또는 시작된 작업이 실행되고 있어야 합니다. 이러한 항목은 각 제품 안내서에 설명되어 있습니다.

항목	정의	값	심볼
시작된 작업	CA Chorus 에는 여러 시작된 작업과 하나의 생성된 작업이 있습니다. 사이트 표준과 기본 설정에 따라 이들의 이름을 지정할 수 있습니다. 기본 이름은 다음과 같습니다.		
	CHORJBOS: JBoss 서버 CA Chorus 응용 프로그램을 호스팅합니다. JBoss 는 다양한 플랫폼에서 운영되는 오픈 소스 Java 기반 응용 프로그램 서버입니다. JBoss 는 Java 를 지원하는 모든 운영 체제에서 작동합니다.		CHORJBOS
	CA Datacom/AD MUF(Multi-User Facility) MUF 는 시스템 관리 프로그램이며 기능적으로 데이터에 대해 운영 체제 역할을 합니다. MUF 는 응용 프로그램의 요청을 수신하고 이를 처리하는 방식을 결정합니다. MUF 는 요청을 처리하기 위해 수행해야 할 작업을 조정합니다. CA Chorus 설치에 필요한 사전 요구 사항에 따라 새로운 전용 MUF 를 제작할 수 있습니다. 생성한 MUF 이름을 기록하십시오.		&AD_MUF_STCID

항목	정의	값	심볼
	MUF OWNER: MUF 시작된 작업을 소유한 사용자 ID 입니다.		&AD_MUF_OWNER
	CHORTSF: TSF(Time Series Facility) TSF 를 사용하면 꺾은선 그래프로 성능 데이터를 볼 수 있습니다.		%CHORTSF
	CHORTSFR: Time Series Facility 릴레이 작업 TSF 데이터 릴레이를 사용하면 원격 LPAR 에서 수집된 데이터를 TSF 에 보낼 수 있습니다.		%CHORTSFR
	CHORJBOS 는 CA DSI 보안 확인에 대한 별도의 작업을 생성합니다. 이 작업의 이름을 CHORJBOS 에 대해 선택한 작업 이름과 다르게 하려면 CA Chorus 관리 사용자 ID 에 BPX.SUPERUSER 및 BPX.DAEMON 기능에 대한 읽기 액세스 권한을 부여해야 합니다.		

소프트웨어 요구 사항

CA Chorus 에 대해 다음과 같은 소프트웨어가 필요합니다.

- CA Technologies 소프트웨어 - 다음과 같은 소프트웨어가 필요합니다.
  - CAIRIM 및 CAMASTER 서비스 구성 요소가 설치된 CCS(CA Common Services for z/OS) 릴리스 14.1 및 CA Easytrieve 릴리스 11.6
  - FIXCAT 레이블이 CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.V3.0 인 모든 CCS 유지 관리를 적용합니다.

    CCS

    서비스 구성 요소는 CCS 와 함께 제공 및 설치됩니다. 사이트에 다른 CA Technologies 제품이 설치된 경우 이러한 서비스가 설치되어 있을 수 있습니다. 이러한 서비스가 설치되지 않은 경우 지금 설치하십시오. 이러한 구성 요소의 설치 및 구성에 대한 자세한 내용은 CCS 설명서를 참조하십시오.

    중요! CAMASTER 주소 공간이 실행 중이어야 합니다. 실행 중인 경우 z/OS syslog 에 IPL 메시지의 일부로 다음 메시지가 나타납니다.
    CAMS101I CAMASTER INITIALIZATION COMPLETE.
    CAMASTER 는 취소할 수 없는 시작된 작업으로, 다양한 CA 제품 및 CCS 에 시스템 서비스 및 저장소 리소스를 제공합니다. CAMASTER 는 최소 CPU 를 사용하며, 중지 또는 다시 시작할 수 없습니다.

    참고: CCS 사전 요구 사항을 충족하기 위해 CAW0LOAD 로드 라이브러리에 APF 허가를 받아야 합니다.

    CA Easytrieve

    CCS 릴리스 14.1 이전에 CA Easytrieve 는 Easytrieve Service CDX8E00 으로 제공되었습니다. CCS 릴리스 14.1 부터 CA Easytrieve 는 독립 실행형 pax 설치 형태로 제공됩니다. 한 번의 CA Easytrieve 설치로 CCS 모드로 운영되거나 CA Easytrieve 를 여러 번 설치할 필요 없이 전체 기능 모드로 운영될 수 있습니다. CCS 14.1 의 패키지에는 CA Easytrieve 릴리스 11.6 이 제공됩니다. CA Easytrieve 11.6 을 설치한 경우 CCS 14.1 로 배포된 복사본을 설치할 필요가 없습니다. 둘이 동일하기 때문입니다. CA Easytrieve 릴리스 11.6 을 설치하지 않은 경우 *CA Easytrieve Release 11.6 Installation Guide*(CA Easytrieve 릴리스 11.6 설치 안내서)의 부록 B 에 나열된 지침을 따르십시오.

- CA CSM(CA Chorus Software Manager) 릴리스 5.1(RO56614): CA Chorus 를 설치하는 데 CA CSM 을 사용해야 합니다.
- FIXCAT 레이블이 CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.V3.0 인 모든 CA Datacom/AD 유지 관리를 적용합니다.

  중요! CA CSM 이 시스템 설정에서 제품별 파일 시스템을 사용하도록 구성되어 있는지 확인하십시오. 이 설정은 CA CSM 의 "Settings"(설정) 탭에서 확인할 수 있습니다. "Software Installation"(소프트웨어 설치)을 클릭하고 오른쪽 창에서 "SIS Base Install -File system"(SIS 기본 설치 - 파일 시스템)으로 스크롤한 후 "Product Specific File System"(제품별 파일 시스템)의 글머리 기호가 선택되어 있는지 확인합니다.

  중요! CA Chorus 에서는 zFS 파일 시스템만 지원되고 HFS 파일 시스템은 지원되지 않습니다.

- CA Datacom/AD 버전 14

  참고: CA Chorus 는 CA Datacom/DB 를 지원하지 않습니다. CA Datacom/DB 가 설치되어 있으면 CA Datacom/AD 를 설치한 후 CA Chorus 를 설치할 때 해당 라이브러리를 참조하십시오.

  - 전체 CA Datacom/AD 설치 및 구성이 필요합니다. 자세한 내용은 *CA Datacom/AD Installation Guide*(CA Datacom/AD 설치 안내서)를 참조하십시오.
  - FIXCAT 레이블이 CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.V3.0 인 모든 CA Datacom/AD 유지 관리를 적용합니다.
  - CA CSM 설치 마법사에서 "Base Install + USS Client for DBSRV"(기본 설치 + DBSRV, FMID CAYTE02 용 USS 클라이언트)를 선택하여 CA Datacom Server 를 포함한 모든 CA Datacom/AD 구성 요소를 설치하십시오. CA Datacom Server 에는 USS(UNIX System Services)에서 실행되는 JDBC 가 포함됩니다.
  - 새롭거나 비어 있는 CA Datacom/AD MUF: CA Datacom/AD MUF 를 구축할 다음 멤버를 실행해야 합니다. 설치하는 동안 사용할 수 있도록 정의한 MUF 이름을 기록하십시오. MUF 를 생성하는 정확한 단계는 *CA Datacom/AD Installation Guide*(CA Datacom/AD 설치 안내서)의 INSTJCL 멤버 항목을 참조하십시오.

    참고: CA Datacom/AD 사전 요구 사항에 따라 *datacomad_adthlq*.CAAXLOAD(CA Datacom/AD 로드 라이브러리) 및 *datacomad_adchlq*.CUSLIB(CA Datacom/AD 사용자 지정 라이브러리) 라이브러리가 APF 허가되어야 합니다.

    AXCUS00: 설치 JCL 데이터 집합을 작성하고 채우고 대량 편집합니다.

    AXCUS01: CA Datacom/AD MUF의 모든 사용자 지정을 포함합니다.

    AXAPFADD: APF에 나열할 라이브러리를 동적으로 추가하는 CA SYSVIEW 예가 포함되어 있습니다.

    AXRIM01: PC CALLS를 설치합니다.

    AXNEW01: MUF에 필요한 데이터 집합을 할당하고 채웁니다.

    AD14STRT: MUF를 시작하는 예제 JCL입니다.

    AXIVP01: 설치 확인 JOB 예제입니다.

    참고: 대상 런타임 라이브러리를 공유할 수 있지만 MUF 를 공유할 수는 없습니다.

- IBM 소프트웨어 - CA Chorus 를 설치한 시스템에서 다음과 같은 소프트웨어를 사용할 수 있어야 합니다.
  - IBM z/OS 1.12 이상
  - zFS 파일 시스템에 대한 IBM z/OS USS(UNIX System Services) 지원
  - IBM z/OS 시스템 로거
  - IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 Release 0 Modification 0 Service Release 2(5655-W44)(선택적 JZOS batch launcher 포함)

    참고: IBM 31-bit SDK for z/OS, Java Technology Edition, Version 7 Release 0 Modification 0(5655-W43)은 CA Chorus 에서 배치 보고서를 생성하는 데 필요합니다. 이 기능은 CCS 의 CA Easytrieve Service 구성 요소를 사용합니다.
- 각 사용자에게 필요한 PC 소프트웨어:
  - Adobe Flash Player 9.0.124 이상
  - 버전 3.0 의 경우 CA Chorus 는 Microsoft Windows Internet Explorer 9 및 Mozilla Firefox 13~19 을 지원합니다. 새 브라우저가 출시되는 경우 CA 는 해당 브라우저의 유효성을 검사하고 CA Chorus 제품 페이지의 "Recommended Reading"(권장 자료)에 호환성 여부를 게시합니다.

  참고: CA Chorus 를 사용하려면 화면 해상도가 최소 1024x768 이어야 합니다. 화면 해상도가 이 요구 사항을 충족하지 않는 경우 전체 화면 모드(대부분의 브라우저에서 F11 키로 실행)를 사용하여 화면에 스크롤 막대를 포함해야 합니다.

CA Chorus 서버 요구 사항

CA Chorus 에는 2450 MB 의 힙 메모리가 필요하며 각 전문 분야에 대해 다음 추가 힙 요구 사항이 필요합니다.

- CA Chorus for DB2 Database Management 에 200 MB
- CA Chorus Infrastructure Management for Networks and Systems 에 200 MB
- CA Chorus for Security and Compliance Management 에 100 MB
- CA Chorus for Storage Management 에 200 MB

모든 전문 분야를 선택하는 경우 최소 3150 MB 의 실제 저장소를 CA Chorus 서버가 실행되는 LPAR 에 할당해야 합니다. 이 값이 기본값입니다.

힙 메모리 크기를 수정하려면 *chorus_runtime_hlq*.CETJOPTN 의 ENVETJ 멤버에서 Java 힙 크기(Java SDK 옵션) 설정을 확인하십시오. 힙이 범위로 지정된 경우 -Xms 가 시작 값이며 -Xmx 가 끝 값입니다.

예제

모든 전문 분야가 설치된 CA Chorus 의 경우: 2450 MB + 200 MB + 200 MB + 200 MB + 100 MB = 3150 MB 필요

저장소 및 보안 전문 분야가 설치된 CA Chorus 의 경우: 2450 MB + 200 MB + 100 MB = 2750 MB 필요

메모리 제한

z/OS 는 작업에 지정된 REGION= 및 MEMLIMIT= 매개 변수의 값에 따라 메모리 제한을 설정합니다. 하지만 IEFUJV, IEFUSI, IEALIMIT, JES2 Exit 6, JES3 Exit IATUX03 등 여러 설치 종료 작업이 제한을 재정의하는 데 사용될 수 있습니다. GETMAIN 요청이 발생하는 경우 해당 요청은 사용 가능한 제한 내에서 충족되어야 합니다. 즉, 제한 내에서 인접한 여유 공간을 사용할 수 있어야 하며, 사용할 수 없는 경우 요청이 실패합니다.

CA Chorus 는 REGION=0M 으로 실행되도록 설계되었으며 이 값이 기본값으로 배포되어 있습니다. IBM 은 이 시나리오를 "제한이 없음"의 의미로 정의합니다. 따라서 z/OS 기본값을 재정의하지 않는 경우 제한값 아래와 제한값 위를 제외하고 행 아래 및 행 위의 모든 메모리를 할당할 수 있습니다. REGION 에 다른 값을 지정하면 제한값 아래의 메모리로 제한되고 제한값 위에 존재하지 않는 메모리가 기본값이 됩니다. 이러한 경우 제한값 위의 메모리를 사용하려면 MEMLIMIT 에 영(0)이 아닌 값을 지정해야 합니다.

설치 시 SYS1.PARMLIB 의 SMFPRMxx 멤버에서 MEMLIMIT 의 기본값을 지정할 수 있습니다. 기본값이 지정되지 않은 경우 z/OS 기본값은 MEMLIMIT(00000M)이고 제한값 위의 메모리는 이전 설명처럼 REGION=0M 이 지정되지 않는 한 사용할 수 없습니다. 또한 MEMLIMIT=nnnnnM 이 JCL 의 JOB 또는 EXEC 문에 지정될 수 있습니다. JCL 의 값은 항상 SMFPRMxx 멤버의 기본값을 재정의합니다. IEFUSI exit 가 MEMLIMIT 를 재정의하는 데 사용할 수 있는 유일한 항목입니다. 현재 기본값을 찾으려면 다음 콘솔 명령을 입력하여 활성 SMF 옵션을 표시합니다.

```
D SMF,O
```

시스템 요구 사항

사이트가 다음과 같은 시스템 요구 사항을 충족하는지 확인하십시오.

프로세서

CA Chorus 는 z/OS 에서 JavaVM 환경을 사용합니다. 따라서 최상의 성능과 더 효과적인 리소스 사용을 위해 전문 프로세서를 사용할 것을 *강력히* 권장합니다.

디스크

- CA Chorus 배포를 실행하는 데 약 11050 실린더가 필요합니다.
- 설치하는 데 약 5300 실린더가 필요합니다.
- pax 설치 파일이 저장될 zFS 에 약 1500 실린더가 필요합니다.

  참고: 설치가 완료되면 pax 파일을 삭제하여 공간을 확보할 수 있습니다.
- DASD 에 공간을 추가적으로 할당할 수 있어야 합니다.

참고: Time Series Facility 의 설치 후 디스크 공간 권장 사항은 *관리 안내서*를 참조하십시오.

대상 라이브러리

다음 표에서는 CA Chorus 대상 라이브러리의 트랙별 데이터 집합 공간 요구 사항을 보여 줍니다.

데이터 집합 이름	트랙
CC2DEXEC	3000
CC2DLINK	15
CC2DLMD0	5
CC2DLOAD	750
CC2DLPA	4
CC2DMAC	20
CC2DSAMP	330
CC2DVSMI	2250
CETJDATA	15
CETJEXEC	600
CETJEZTR	10
CETJJCL	75
CETJLMDR	75
CETJLOAD	75
CETJMAC	20
CETJOPTN	30
CETJOPTV	5
CETJPLD	2250
CETJPROC	10
CETJSAMP	20
CETJVSMI	1425
CETJXML	750

데이터 집합 이름	트랙
CETJZFS0(zFS 디렉터리)	60000

참고: CA CSM 은 이전에 마운트 포인트가 존재하지 않은 경우 마운트 포인트를 생성하고 자동으로 새 파일 시스템을 마운트합니다.

배포 라이브러리

다음 표에서는 CA Chorus 배포 라이브러리의 트랙별 데이터 집합 공간 요구 사항을 보여 줍니다.

데이터 집합 이름	트랙
AC2DEXEC	3000
AC2DLOAD	750
AC2DMAC	20
AC2DMOD	750
AC2DSAMP	330
AC2DVSMI	2250
AETJDATA	15
AETJEXEC	600
AETJEZTR	10
AETJJCL	75
AETJLOAD	75
AETJMAC	20
AETJMODE	15
AETJMODR	75
AETJOPTN	30
AETJOPTV	5
AETJPLD	2250
AETJPROC	10
AETJSAMP	20

데이터 집합 이름	트랙
AETJVSMI	1425
AETJXML	750
AETJZFS	9750
TPV.AETJHFS	14850

CA CSM 임시 저장소 요구 사항

사용자 설정에 지정된 옵션을 사용하기 위해서는 CA CSM 설치 과정 중에 다음과 같은 저장소 요구 사항을 충족해야 합니다.

- User Unpax Temporary Directory 로 사용되는 디렉터리에 마운트된 zFS 에 약 1000 실린더 필요
- GIMUNZIP Temporary Prefix 를 위해 생성된 데이터 집합에 약 700 실린더 필요
- Temporary Data Set Prefix 를 위해 생성된 데이터 집합에 약 300 실린더 필요

참고: CA CSM 에는 CA Chorus 배포를 처리하기 위한 임시 배포 파일 시스템을 생성하는 데 약 2000 실린더가 필요합니다. 이러한 설정에 대한 자세한 내용은 CA CSM 제품 설명서를 참조하십시오.

포트 요구 사항

CA Chorus 는 JBoss 서버 및 TSF(Time Series Facility) 구성 요소를 위한 다음 포트 요구 사항을 충족해야 합니다.

- CA DSI Server 및 JBoss 서버용 연속 포트 12 개. JBoss 포트는 DSI 양방향(연결 및 수신 대기) 포트 하나와 서버(수신 대기) 포트 11 개로 구성됩니다.
- TSF 용 단방향 포트 3 개.

  참고: TSF 인스턴스가 원격 LPAR 에 사용되는 경우 TSF 인스턴스에 단방향 포트가 2 개 더 필요합니다.

이러한 포트는 나중에 JBoss 서버 및 TSF 구성을 설치하는 과정에서 구성됩니다.

사용하려는 포트를 사용할 수 있는지 확인하려면 네트워크 관리 팀에 문의하십시오.

(선택 사항) SMTP 전자 메일 요구 사항

CA Chorus 인터페이스 내에 위치한 Investigator 에서 전자 메일 작업을 지정하여 성능 정책이 충족되는 경우 알림을 받을 수 있습니다.

예를 들어 지정한 시간 간격으로 제품 로그인 시도를 *x* 명의 사용자가 실패하면 알림을 받도록 Investigator 의 정책을 생성할 수 있습니다. 제품에 SMTP 를 구성한 경우 정책 조건이 충족된 전자 메일을 받을 수 있습니다. 그러면 이러한 유형의 알림이 자동화됩니다.

사이트에서 이러한 기능을 사용하려면 다음 정보를 파악해야 합니다. 그리고 나중에 CA Chorus 를 구성할 때 이 정보를 사용합니다.

SMTPHOST

SMTP 메일 서버의 이름 및 IP 주소입니다.

SMTPPORT

SMTP 메일 서버의 포트 번호(1024~65535)입니다.

USS Parmlib 요구 사항

z/OS parmlib 멤버 BPXPRM*xx* 에서는 CA Chorus 에 MAXFILEPROC(64000)가 필요합니다.

설정을 확인하려면 MVS 콘솔에서 다음 명령을 입력합니다.

```
D OMVS,OPTIONS
```

제 3 장: 보안 요구 사항 설명

이 섹션은 다음 항목을 포함하고 있습니다.

설치 관리자 보안 권한

설치 프로세스를 시작하기 *전에* CA Chorus 설치 관리자 사용자 ID 에 다음과 같은 보안 권한이 정의되어 있는지 확인하십시오.

- UNIX System Services 에 대해:
  - zFS 데이터 집합을 조작할 수 있는 권한. 이 권한에는 FSACCESS 클래스 내의 적절한 항목에 대한 UPDATE 권한이 필요합니다.
    - FSACCESS 를 통해 ZFS 파일 시스템 컨테이너(즉, 데이터 집합)에 대한 액세스 권한을 보호할 수 있습니다. 리소스 이름은 ZFS 파일 시스템 이름입니다.
    - 예를 들어 이름이 OMVS.ZFS.WEBSRV.TOOLS 인 ZFS 파일 시스템을 정의하고 디렉터리에 파일을 포함하여 U1 및 U2 디렉터리를 생성하면 사용자가 ZFS 파일 시스템의 U1 및 U2 디렉터리에 있는 파일에 액세스할 때 FSACCESS 클래스의 OMVS.ZFS.WEBSRV.TOOLS 리소스에 대한 리소스 검사가 수행됩니다. 자세한 내용은 해당 보안 제품의 설명서를 참조하십시오.
  - 유효한 OMVS 정의
  - Superuser 권한
  - FACILITY 클래스의 다음 리소스에 대한 READ 액세스 권한:
    - BPX.SUPERUSER
    - BPX.FILEATTR.APF
    - BPX.FILEATTR.PROGCTL
    - BPX.FILEATTR.SHARELIB

  - BPX.SERVER
  - UNIXPRIV 리소스 클래스의 SUPERUSER.FILESYS.PFSCTL 프로필
- z/OS:
  - CA Chorus 설치 데이터 집합과 라이브러리에서 생성, 업데이트 및 실행할 수 있는 권한
  - 외부 보안 관리자(CA ACF2, CA Top Secret 또는 IBM RACF) 데이터베이스를 조작하는 명령을 실행하는 권한

*설치 안내서*에 설명된 대로 외부 보안 제품을 통해 수행해야 하는 APF 허가 및 기타 보안 요구 사항은 CA Chorus 구성 프로세스 중에 정의됩니다. 설치 패키지의 다양한 작업과 멤버에 액세스해야 하므로 설치하는 동안 해당 작업을 완료해야 합니다.

CA Chorus 보안 작업 실행

ETJI095*x* 보안 작업은 여러 보안 요구 사항을 충족하는 방식을 간소화합니다. 보안 작업은 ETJI095*x* 로 식별되고 여기서 x 는 CA ACF2 의 경우 A 를, CA Top Secret 의 경우 T 를, IBM RACF 의 경우 R 을 나타냅니다. 이러한 작업은 CA Chorus 제품 페이지*에 있습니다.*

다음 목록에는 작업이 충족해야 할 보안 요구 사항이 자세히 설명되어 있습니다.

중요! *이 항목의 뒷부분*에 있는 단계를 진행하기 전에 다음 개념서를 검토하십시오.

(CA Top Secret 에만 해당) Master Facility

CA Top Secret 을 사용하는 경우에는 Master Facility(마스터 기능)를 정의하여 CA Chorus 시작된 작업에 연결해야 합니다. CAWEBSVR 를 Master Facility 로 사용합니다. Master Facility(MASTFAC 키워드)는 사용자가 CAWEBSVR 기능에 액세스하는 데 사용됩니다. 기능을 Master Facility 로 사용하려면 먼저 시스템 기능 매트릭스의 CA Top Secret 에 사용자 기능으로 정의해야 합니다.

중요! 이 작업은 한 번만 수행하십시오. 기능 매트릭스에 CAWEBSVR 을 추가하여 정의를 활성화한 경우 이 작업을 반복해서는 안 됩니다.

CA Chorus 에 액세스하는 모든 ACID 사용자에 대해 CA Top Secret 기능 CAWEBSVR 에 사용 권한을 추가합니다.

관리자 ID 및 그룹 ID

다음과 같은 조건을 충족하도록 정의된 USS(UNIX System Services) 세그먼트가 있는 사용자 ID 하나(기본값: CHORADM)를 사용하여 CA Chorus 를 실행합니다.

- 사용자 ID 가 UID(0)이 *아닌* 유효한 UID 를 가지고 있습니다.
- 셸이 기본 셸(일반적으로 /bin/sh)로 지정되어 있습니다.
- 사용자 ID 가 유효한 OMVS 그룹을 가지고 있습니다.

참고: 홈 디렉터리를 CA Chorus 설치 디렉터리와 동일한 위치로 하는 것이 좋습니다.

ETJI095*x* 작업을 실행할 때 다음 보안 사용자 ID 가 생성됩니다. 기본값을 사용하지 않는 경우 보안 작업에서 모든 CHORADM 및 CHORGRP 항목을 변경해야 합니다.

CHORADM

CA Chorus 를 실행하는 데 사용되는 시작된 작업 사용자 ID 입니다.

CHORGRP

기본 그룹 이름입니다. 이 그룹은 모든 관련 보안 개체 간의 관계를 생성합니다.

CHORTHD

응용 프로그램과 관련된 PassTicket 요청의 사용자 ID 입니다.

참고: CA Chorus 시작된 작업 사용자 ID 에는 고유한 USS UID 와 GID(사용자 ID 와 그룹 ID 번호)를 사용해야 합니다. 숫자가 일치하는 UID 와 GID 를 선택하면 추적하기 쉽습니다.

중요! 설치하는 사용자를 포함한 모든 사용자는 이 멤버에 지정된 그룹에 액세스할 수 있어야 합니다. 기본값은 CHORGRP 입니다.

시작된 작업

다음 시작된 작업은 ETJI095*x* 작업을 실행할 때 정의됩니다. 기본값이 표시됩니다. 시작된 작업에 기본 이름을 사용하지 않는 경우 보안 작업에서 이름을 변경합니다.

참고: 모든 CA Chorus 작업은 REGION=0M 으로 설정하여 시작된 작업으로 실행하는 것이 좋습니다. 사이트에서 REGION=0M 매개 변수의 사용을 제한하는 경우에는 허용되는 최대 영역 크기를 사용하여 실행하는 것이 좋습니다.

your_muf_name

CA Chorus 용 CA Datacom/AD MUF 에 연결된 시작된 작업 이름입니다. 이름은 이전에 MUF 에 할당한 이름에 따라 달라집니다.

CHORTSF

TSF(Time Series Facility)와 관련된 시작된 작업 이름입니다.

CHORTSFR

원격 TSF 구성과 관련된 시작된 작업 이름입니다. 이 시작된 작업은 TSF 데이터 릴레이를 정의한 경우에만 생성됩니다.

CHORJBOS

원격 JBoss 서버와 관련된 시작된 작업 이름입니다.

리소스 클래스

CA Chorus 는 CAMFC 클래스의 보안 리소스를 정의하고, 해당 클래스는 보안 제품을 사용하여 정의합니다. 그런 다음 필요에 따라 전문 분야 관련 리소스에 대한 권한을 사용자에게 할당합니다. 참고: 필요한 사용자 권한에 대한 자세한 내용은 전문 분야별 설치 안내서를 참조하십시오.

일반 사용자를 위한 PassTicket

PassTicket 은 사용자가 CA Chorus 및 지원되는 전문 분야가 사용하는 z/OS 구성 요소 및 제품에 액세스하기 위해 필요합니다. *PassTicket* 은 임시로 인코딩되고 암호화된 사용자 암호의 대용물로서 특정 응용 프로그램에 액세스하기 위해 사용할 수 있습니다. PassTicket 은 생성된 후 10 분 이내에 사용해야 합니다.

PassTicket 을 사용하면 z/OS 구성 요소 및 제품이 네트워크를 통해 z/OS 암호를 전송하지 않고도 사용자 ID 를 인증할 수 있습니다. 대신, 사용자는 올바른 z/OS 사용자 ID 와 암호를 사용하여 처음 로그인한 이후에 인증됩니다. 다음 프로세스는 사용자가 z/OS 구성 요소에 액세스하는 기능을 선택할 때 발생합니다.

- CA Chorus 웹 서비스가 액세스 권한 부여를 위해 PassTicket 을 생성하기 위해 z/OS 보안 제품을 호출합니다.
- PassTicket 이 사용자 요청과 함께 (주로 다른 z/OS 시스템에 있는) 구성 요소로 전달됩니다.

  요청을 처리하기 전에 PassTicket 을 암호 대용물로 사용하여 사용자를 인증하기 위해 구성 요소가 z/OS 보안 제품을 호출합니다.

CA Chorus 서버는 CA Chorus 전문 분야가 사용하는 여러 백엔드 제품에 사용자가 액세스하도록 허용하는 PassTicket 을 생성합니다. 사용자가 구성 요소에 액세스할 때 요청의 유효성을 검사하기 위해 PassTicket 이 생성됩니다.

CA Chorus PassTicket 구성은 다음 시스템을 포함합니다.

- 동일한 시스템에서 CA Chorus 전문 분야에 필요한 JBoss 서버 및 백엔드 제품(CA Detector, CA Compliance Manager, CA Vantage SRM, CA NetMaster NM for TCP/IP 등)을 실행하는 하나의 z/OS 시스템. 이 유형의 시스템은 CA Chorus 서버 시스템입니다.
- CA Chorus 전문 분야에 필요한 제품 및 구성 요소만 실행하는 추가 z/OS 시스템. 이 유형의 시스템은 CA Chorus 원격 시스템이라고 합니다.

CA Chorus 서버 시스템은 모든 CA Chorus 사용자에게 진입점을 제공합니다. 그런 다음 사용자들은 z/OS 시스템의 네트워크에서 사용하도록 허가된 모든 CA Chorus 원격 시스템에 액세스할 수 있습니다.

보안 제품에 대한 PassTicket 구성은 CA Chorus 에서 사용하는 구성 요소를 호스팅하는 각 z/OS 시스템에서 수행되어야 합니다. CA Chorus 전문 분야에 필요한 연결을 생성하고 검사할 수 있도록 z/OS 보안 제품에서 PassTicket 을 구성하십시오. 사이트가 다음과 같은 조건을 충족하는 경우 원격 시스템에서 추가적인 보안 설정이 필요 없습니다.

- z/OS 구성의 보안 제품이 공유 보안 데이터베이스를 사용하고 있습니다.
- 하나 이상의 원격 시스템을 추가하길 원하며, CA Chorus 서버 시스템 설정만 필요합니다.

보안 데이터베이스를 공유하지 않는 원격 시스템에 필수 제품 및 구성 요소가 있는 경우 원격 시스템에서 추가 보안 설정이 필요합니다.

CA CSM 사용자를 위한 PassTicket

CA Chorus 에서 사용하는 PassTicket 보안을 통해 또 다른 사용자 로그인 없이 "Quick Links"(빠른 링크)에서 CA CSM 을 시작할 수 있습니다. Passticket 을 사용하는 모든 시스템은 네트워크에 있는 모든 노드에 대해 동일한 응용 프로그램 이름과 세션 키를 가져야 합니다. 다음 요구 사항에 유의하십시오.

- CA Chorus 인스턴스와 CA CSM 인스턴스가 *서로 다른* 시스템에 상주하는 경우 이 작업을 실행한 후 CA Chorus 에 대한 CA CSM PassTicket 구성 방법 (페이지 57)에서 적용되는 단계를 완료해야 합니다.
- CA Chorus 인스턴스와 CA CSM 인스턴스가 *동일한* 컴퓨터에 상주하는 경우 이 작업을 수행하면 CA CSM PassTicket 구성이 완료됩니다. 단, 한 가지 예외가 있습니다. CA ACF2 를 사용하는 경우 예제: CA ACF2 를 사용하여 CA Chorus 에서 CA CSM 으로 연결할 수 있도록 PassTicket 구성 (페이지 60)에 있는 하나의 CA Chorus 서버 측 및 CA CSM 측 단계를 완료해야 합니다.

다음 단계를 수행하십시오.

1. 외부 보안 관리자에 적용하는 ETJI095*x* 작업을 검색합니다. 이러한 작업은 CA Chorus 제품 페이지 *에 있습니다.*
2. ETJI095*x* 멤버를 전체적으로 검토합니다.
3. 멤버 주석에 따라 작업을 편집합니다.
4. 멤버를 제출합니다.

   명시된 보안 요구 사항이 충족됩니다.
5. (CA Top Secret 만 해당) 해당 CA Top Secret 매개 변수 파일(PARMFILE)에 다음 행을 추가합니다.

   ```
   FACILITY(USERxx=NAME=CAWEBSVR)
   FACILITY(CAWEBSVR=PGM=********)
   FACILITY(CAWEBSVR=ACTIVE,SHRPRF,MULTIUSER,AUTHINIT)
   ```

   xx

   사용자 기능 번호입니다. 시스템의 이용 가능한 사용자 기능 번호를 사용합니다.

추가 정보:

보안 고려 사항 (페이지 15)
보안 ID 재사용 고려 사항 (페이지 20)

CA Chorus 에서 작업할 사용자에게 권한을 부여하는 방법

보안 관리자는 제품에 대한 모든 사용자 액세스 요청을 관리합니다. CA Chorus 의 경우 보안 관리자는 다음 작업을 수행해야 합니다.

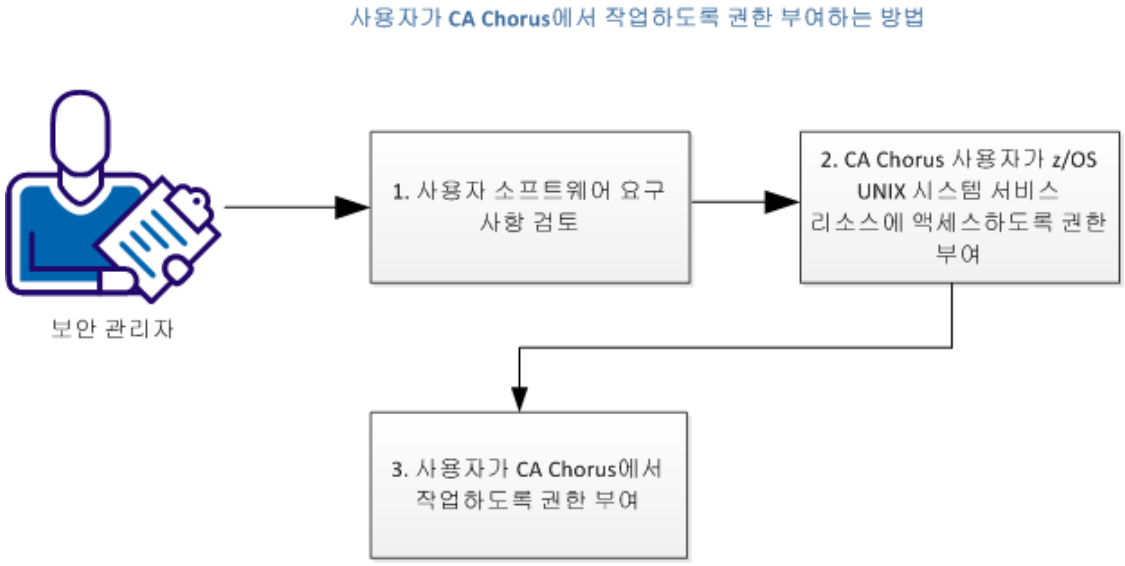
- 각 사용자 USS(UNIX System Services) 환경에 권한을 부여하고 확인합니다.
- CA Chorus 및 지원되는 관련 전문 분야에서 작업할 수 있도록 사용자에게 권한을 부여합니다.

참고: CA Chorus 는 CAMFC 클래스에 보안 리소스를 정의합니다. 액세스를 제한하고 특정 사용자가 제품에 로그인하지 못하도록 CAMFC 리소스 클래스와 사용자 액세스 권한을 제거할 수 있습니다.

이러한 권한 부여 작업을 수행하기 위해 보안 관리자는 CA ACF2, CA Top Secret 또는 IBM RACF 를 사용합니다.

다음 그림은 CA Chorus 및 지원되는 관련 전문 분야에서 작업할 수 있도록 사용자에게 권한을 부여하는 작업을 보여 줍니다.

참고: 작업은 순서에 상관없이 완료할 수 있지만 이 다이어그램에 표시된 순서대로 작업을 수행하는 것이 좋습니다.



CA Chorus 에서 작업할 수 있도록 사용자에게 권한을 부여하려면 다음 작업을 완료하십시오.

1. 사용자 소프트웨어 요구 사항을 검토합니다. (페이지 45)
2. z/OS UNIX System Services 리소스에 액세스할 수 있도록 CA Chorus 사용자에게 권한을 부여합니다. (페이지 45)
3. CA Chorus 에서 작업할 사용자에게 권한을 부여합니다. (페이지 48)

사용자 소프트웨어 요구 사항 검토

- 각 사용자에게 필요한 PC 소프트웨어:
  - Adobe Flash Player 9.0.124 이상
  - 버전 3.0 의 경우 CA Chorus 는 Microsoft Windows Internet Explorer 9 및 Mozilla Firefox 13~19 을 지원합니다. 새 브라우저가 출시되는 경우 CA 는 해당 브라우저의 유효성을 검사하고 CA Chorus 제품 페이지의 "Recommended Reading"(권장 자료)에 호환성 여부를 게시합니다.

참고: CA Chorus 를 사용하려면 화면 해상도가 최소 1024x768 이어야 합니다. 화면 해상도가 이 요구 사항을 충족하지 않는 경우 전체 화면 모드(대부분의 브라우저에서 F11 키로 실행)를 사용하여 화면에 스크롤 막대를 포함해야 합니다.

USS 리소스에 액세스할 수 있도록 CA Chorus 사용자에게 권한 부여

CA Chorus 구성 요소 및 전문 분야는 z/OS TCP/IP 통신 서비스 및 z/OS USS(UNIX System Services)를 사용합니다. CA Chorus 에서 작업할 때 z/OS USS 리소스에 액세스할 수 있도록 각 사용자의 OMVS 세그먼트를 정의합니다. CA ACF2, CA Top Secret 또는 IBM RACF 를 사용하여 이 액세스를 활성화합니다.

z/OS USS 에 액세스할 수 있도록 CA Chorus 사용자에게 권한을 부여하려면 각 사용자에 대해 다음 옵션을 포함하는 OMVS 세그먼트를 정의합니다.

- 기본 셸 프로그램 사양(PROGRAM 또는 OMVSPGM)
- 숫자로 구성된 z/OS USS UID(사용자 ID)

  참고: 사용자의 사이트에 OMVS UID 번호를 할당하는 정책이 존재할 수 있습니다. 존재하지 않는 경우 고유 번호를 사용하십시오.
- 숫자로 구성된 z/OS USS GID(그룹 ID)

다음 단계를 수행하십시오.

1. 사용자에게 OMVS 세그먼트에 대한 액세스 권한이 있는지 확인합니다.

   - CA ACF2:

     `LIST *userid* profile(all) section(all)`

   - CA Top Secret:

     `TSS LIST(*userid*) DATA(ALL)`

   - IBM RACF:

     `LISTUSER *userid* OMVS NORACF`

   사용자에게 이 액세스 권한이 없는 경우 다음 단계로 이동합니다.

2. 각 UID(사용자 ID)에 연결할 홈 디렉터리를 생성합니다.

   예를 들어 UID*nnn* 에 대해 /u/name 이름의 디렉터리를 설정하려면 OMVS UNIX 셸에서 다음 명령을 실행합니다.

   ```
   mkdir /u/name
   chown nnn /u/name
   chmod 775 /u/name
   ```

3. 디렉터리에 대한 소유자 및 액세스 권한을 확인합니다.

   ```
   ls -ld /u/name
   ```

   다음과 같은 예제 결과가 나타납니다.

   ```
   drwxrwxr-x   2 user  group  8192 Sep  31 14:58 /u/name
   ```

   굵은 글꼴 영역은 올바른 소유자 및 읽기/쓰기 액세스 권한이 존재한다는 것을 보여 줍니다.

4. 보안 제품을 사용하여 OMVS 세그먼트를 정의합니다.

   참고: 이러한 명령을 실행하기 전에 유효한 그룹 레코드가 존재해야 합니다.

   - CA ACF2:

     ```
     CHANGE userid UID(uid) HOME(path_name) OMVSPGM(/bin/sh)
     GROUP(ggggg)
     ```

   - CA Top Secret:

     ```
     TSS ADD(userid) HOME(path_name) OMVSPGM(/bin/sh) UID(uid)
     GROUP(ggggg) DFLTGRP(ggggg)
     ```

   - IBM RACF:

     ```
     ALU userid OMVS(UID(uid) HOME(path_name) PROGRAM(/bin/sh))
     GROUP(ggggg) DFLTGRP(ggggg)
     ```

세 가지 보안 제품 모두에 다음 구문 변수가 적용됩니다.

userid

사용자 ID를 나타냅니다.

path_name

각 UID(사용자 ID)에 연결하는 홈 디렉터리를 나타냅니다.

uid

UID(사용자 식별) 번호를 나타냅니다.

ggggg

OMVS 그룹을 나타냅니다.

5. OMVS 세그먼트의 내용을 확인합니다.
   - CA ACF2:

     `LIST *userid* profile(all) section(all)`
   - CA Top Secret:

     `TSS LIST(*userid*) DATA(ALL)`
   - IBM RACF:

     `LISTUSER *userid* OMVS NORACF`

OMVS 세그먼트를 정의한 사용자는 이제 CA Chorus 에서 작업하는 데 필요한 USS 에 액세스할 수 있습니다.

CA Chorus 에서 작업할 사용자에게 권한 부여

CA Chorus 지원 전문 분야에 대한 액세스 권한을 추가 또는 제거할 수 있습니다. 사용자는 이러한 사용 권한을 통해 필요한 전문 분야 및 기능에 액세스할 수 있습니다. CA Chorus 에서는 필요한 모든 사용 권한에 리소스 이름 상위 수준 한정자인 CHORUS 를 사용합니다. CA Chorus 에서는 사용자에게 적용 가능한 리소스에 대한 READ 액세스 권한이 있는지 확인합니다. 또한 Knowledge Center 의 내용을 관리하는 권한과 자동 새로 고침 옵션을 사용하는 권한을 수정할 수 있습니다. 이를 수행하려면 CA ACF2, CA Top Secret 또는 IBM RACF 의 기능에 따라 CA Chorus 에서 작업하는 사용자에게 권한을 부여하면 됩니다.

- CA ACF2 를 사용하는 사용자에게 권한 부여 (페이지 48)
- CA Top Secret 를 사용하는 사용자에게 권한 부여 (페이지 51)
- IBM RACF 를 사용하는 사용자에게 권한 부여 (페이지 54)

참고: Knowledge Center 는 CA Chorus 의 모든 설명서가 있는 리포지토리입니다. Knowledge Center 에는 CA 제품 설명서, 사용자가 생성한 설명서, Chicago-Soft MVS/Quick-Ref, 웹 사이트, 타사 설명서에 대한 링크 등의 내용이 포함될 수 있습니다.

예제: CA ACF2 를 사용하는 사용자에게 권한 부여

CA Chorus 에 로그인하고 특정 전문 분야를 사용할 수 있는 사용자를 식별하려면 다음 절차를 사용하십시오. 또한 다음 작업을 수행할 수 있도록 사용자에게 권한을 부여할 수 있습니다.

- Knowledge Center 의 내용을 인덱싱합니다. 내용을 인덱싱하면 사용자가 Knowledge Center 리포지토리에서 설명서를 추가 또는 제거할 수 있습니다.
- 자동 새로 고침 옵션을 사용합니다. 이 옵션을 사용하면 백엔드 데이터가 변경될 때마다 CA Chorus UI 에 나타나는 데이터가 새로 고쳐집니다.

참고: 이 절차의 명령은 예제입니다. 이러한 명령의 자세한 사용 방법은 *CA ACF2 Administration Guide(CA ACF2 관리 안내서)*를 참조하십시오.

사용자 액세스 권한을 정의하려면 다음 명령을 입력합니다.

```
SET RESOURCE(MFC)
RECKEY CHORUS ADD(resource-name UID(uid-of-userid1) SERVICE(READ)
ALLOW)
RECKEY CHORUS ADD(resource-name UID(uid-of-userid2) SERVICE(READ)
ALLOW)
...
RECKEY CHORUS ADD(resource-name UID(uid-of-useridn) SERVICE(READ)
ALLOW)
```

resource-name

사용자에게 액세스가 허용된 CA Chorus 리소스를 식별합니다.

ROLE.DB2DBA

CA Chorus for DB2 Database Management 기능에 대한 액세스 권한을 제어합니다. CA Chorus Infrastructure Management for Networks and Systems 는 CA Insight 의 데이터를 제공하지만 이 전문 분야에는 리소스가 필요하지 않습니다.

ROLE.INFRASTRUCTURE

CA Chorus Infrastructure Management for Networks and Systems 기능에 대한 액세스 권한을 제어합니다.

ROLE.SECURITY

CA Chorus for Security and Compliance Management 기능(UI 및 배치)에 대한 액세스 권한을 제어합니다.

ROLE.SDK*instance*

SDK 에 대한 액세스 권한을 제어합니다. CA Chorus 는 여러 SDK 를 지원할 수 있습니다. 이 이름을 정의하여 공유하려면 시스템 관리자 및 응용 프로그램 관리자와 함께 작업하십시오. 응용 프로그램 개발자는 이 이름을 사용하여 SDK 를 지원하는 데 필요한 파일을 빌드하는 것이 좋습니다. 자세한 내용은 *Software Development Kit 사용자 안내서*를 참조하십시오.

instance

SDK용 인스턴스 리소스를 식별하는 영숫자 문자열입니다.

ROLE.STORAGE

CA Chorus for Storage Management 기능에 대한 액세스 권한을 제어합니다.

SETTINGS.KNOWLEDGECENTER

사용자가 Knowledge Center 의 내용을 인덱싱할 수 있음을 나타냅니다.

SETTINGS.AUTOREFRESH

사용자가 자동 새로 고침 옵션을 사용할 수 있음을 나타냅니다.

uid-of-userid1, uid_of_userid2, ..., uid_of_useridn

액세스를 요청하는 CA Chorus 사용자의 UID 를 나타냅니다.

READ

사용자가 READ 액세스 권한을 갖고 있음을 나타냅니다.

사용자는 지정한 리소스에 대한 액세스 권한을 보유하며 CA Chorus 에 로그인하여 작업할 수 있습니다.

예제

다음 명령은 사용자 ABC1 에게 다음을 수행할 수 있는 권한을 부여합니다.

- CA Chorus 에 로그인합니다.
- CA Chorus for DB2 Database Management 의 기능을 사용합니다.
- Knowledge Center 의 설명서를 수정합니다.
- 자동 새로 고침 옵션을 사용합니다.

```
SET RESOURCE(MFC)
RECKEY CHORUS ADD(ROLE.DB2DBA UID(*************ABC1) SERVICE(READ)
ALLOW)
RECKEY CHORUS ADD(SETTINGS.KNOWLEDGECENTER UID(*************ABC1)
SERVICE(READ) ALLOW)
RECKEY CHORUS ADD(SETTINGS.AUTOREFRESH UID(*************ABC1)
SERVICE(READ) ALLOW)
```

예제: CA Top Secret 를 사용하는 사용자에게 권한 부여

CA Chorus 에 로그인할 수 있는 사용자를 식별하려면 다음 절차를 사용하십시오. 또한 다음 작업을 수행할 수 있도록 사용자에게 권한을 부여할 수 있습니다.

- Knowledge Center 의 내용을 인덱싱합니다. 내용을 인덱싱하면 사용자가 Knowledge Center 리포지토리에서 설명서를 추가 또는 제거할 수 있습니다.
- 자동 새로 고침 옵션을 사용합니다. 이 옵션을 사용하면 백엔드 데이터가 변경될 때마다 CA Chorus UI 에 나타나는 데이터가 새로 고쳐집니다.

참고: 이 절차의 명령은 예제입니다. 이러한 명령에 대한 자세한 내용은 *CA Top Secret Command Functions Guide*(CA Top Secret 명령 기능 안내서)와 *CA Top Secret Control Options Guide*(CA Top Secret 제어 옵션 안내서)를 참조하십시오.

사용자 권한을 설정할 때 다음 사항을 고려해야 합니다.

- 단일 수준이 8 바이트 이상으로 긴 항목 이름은 별표 마스크를 사용하기에 적합하지 않습니다. 부동 소수점 마스크를 사용하는 것이 좋습니다.
- 전문 분야 로그인 자체만이 아닌 여러 호출에 영향을 줄 수 있으므로 접두사가 붙은 사용 권한을 사용할 때 주의해야 합니다.

사용자 액세스 권한을 정의하려면 다음 명령을 입력합니다.

```
TSS PERMIT(acid1) CAMFC(resource-name) ACCESS(READ)
TSS PERMIT(acid2) CAMFC(resource-name) ACCESS(READ)
...
TSS PERMIT(acidn) CAMFC(resource-name) ACCESS(READ)
```

resource-name

사용자에게 액세스가 허용된 CA Chorus 리소스를 식별합니다.

CHORUS.ROLE.DB2DBA

CA Chorus for DB2 Database Management 기능에 대한 액세스 권한을 제어합니다. CA Chorus Infrastructure Management for Networks and Systems 는 CA Insight 의 데이터를 제공하지만 이 전문 분야에는 리소스가 필요하지 않습니다.

CHORUS.ROLE.INFRASTRUCTURE

CA Chorus Infrastructure Management for Networks and Systems 기능에 대한 액세스 권한을 제어합니다.

CHORUS.ROLE.SECURITY

CA Chorus for Security and Compliance Management 기능(UI 및 배치)에 대한 액세스 권한을 제어합니다.

CHORUS.ROLE.STORAGE

CA Chorus for Storage Management 기능에 대한 액세스 권한을 제어합니다.

CHORUS.ROLE.SDK*instance*

SDK 에 대한 액세스 권한을 제어합니다. CA Chorus 는 여러 SDK 를 지원할 수 있습니다. 이 이름을 정의하여 공유하려면 시스템 관리자 및 응용 프로그램 관리자와 함께 작업하십시오. 응용 프로그램 개발자는 이 이름을 사용하여 SDK 를 지원하는 데 필요한 파일을 빌드하는 것이 좋습니다. 자세한 내용은 *Software Development Kit 사용자 안내서*를 참조하십시오.

instance

SDK용 인스턴스 리소스를 식별하는 영숫자 문자열입니다.

중요! SDK 인스턴스에 *고유* 이름을 사용하십시오. 실수로 사용 권한을 적용할 수 있으므로 이름이 유사한 SDK 인스턴스에 주의해야 합니다. 예를 들어 CHORUS.ROLE.SDKROLE1 및 CHORUS.ROLE.SDKROLE123 에 동일한 사용 권한이 있을 수 있습니다. 문자 및 숫자 모두에 동일한 마스킹 제한이 적용됩니다.

CHORUS.SETTINGS.KNOWLEDGECENTER

사용자가 Knowledge Center 의 내용을 인덱싱할 수 있음을 나타냅니다.

CHORUS.SETTINGS.AUTOREFRESH

사용자가 자동 새로 고침 옵션을 사용할 수 있음을 나타냅니다.

acid1, acid2, ..., acidn

액세스를 요청하는 CA Chorus 사용자의 ACID 를 나타냅니다. ACID 는 사용자 또는 프로필일 수 있습니다.

READ

사용자가 READ 액세스 권한을 갖고 있음을 나타냅니다.

사용자는 지정한 리소스에 대한 액세스 권한을 보유하며 CA Chorus 에 로그인하여 작업할 수 있습니다.

예제

다음 명령은 사용자 ABC1 에게 다음을 수행할 수 있는 권한을 부여합니다.

- CA Chorus 에 로그인합니다.
- CA Chorus for DB2 Database Management 의 기능을 사용합니다.
- Knowledge Center 의 설명서를 수정합니다.
- 자동 새로 고침 옵션을 사용합니다.

```
TSS PERMIT(ABC1) CAMFC(CHORUS.ROLE.DB2DBA) ACCESS(READ)
TSS PERMIT(ABC1) CAMFC(CHORUS.SETTINGS.KNOWLEDGECENTER)
ACCESS(READ)
TSS PERMIT(ABC1) CAMFC(CHORUS.SETTINGS.AUTOREFRESH) ACCESS(READ)
```

예제: IBM RACF 를 사용하는 사용자에게 권한 부여

CA Chorus 에 로그인할 수 있는 사용자를 식별하려면 다음 절차를 사용하십시오. 또한 다음 작업을 수행할 수 있도록 사용자에게 권한을 부여할 수 있습니다.

- Knowledge Center 의 내용을 인덱싱합니다. 내용을 인덱싱하면 사용자가 Knowledge Center 리포지토리에서 설명서를 추가 또는 제거할 수 있습니다.
- 자동 새로 고침 옵션을 사용합니다. 이 옵션을 사용하면 백엔드 데이터가 변경될 때마다 CA Chorus UI 에 나타나는 데이터가 새로 고쳐집니다.

참고: 다음 명령은 예제입니다. 명령 사용에 대한 자세한 내용은 IBM RACF 제품 설명서를 참조하십시오.

다음 단계를 수행하십시오.

1. 각 전문 분야 리소스를 CAMFC 에 추가합니다.

   참고: 이 단계는 기능 기반 리소스(예: 자동 새로 고침)에는 필요하지 않습니다. 이 단계는 한 번만 수행하면 됩니다. CAMFC 에 리소스를 이미 정의한 경우 2 단계로 이동합니다.

   ```
   RDEFINE CAMFC CHORUS.ROLE.discipline UACC(NONE)
   ```

   discipline

   DB2DBA

   INFRASTRUCTURE

   SECURITY

   STORAGE

   참고: 각 전문 분야 리소스에 대한 자세한 설명을 보려면 2 단계를 참조하십시오.

   해당되는 전문 분야 리소스가 CAMFC 에 할당됩니다. 이제 사용자에게 전문 분야에 대한 액세스 권한을 부여할 수 있습니다.

2. 다음 명령을 입력하여 특정 리소스에 대한 사용자 액세스를 허용합니다.

   ```
   PERMIT resource-name ID(uid-of-userid1) AC(READ) CLASS(CAMFC)
   PERMIT resource-name ID(uid-of-userid2) AC(READ) CLASS(CAMFC)
   ...
   PERMIT resource-name ID(uid-of-useridn) AC(READ) CLASS(CAMFC)
   ```

   resource-name

   사용자에게 액세스가 허용된 CA Chorus 리소스를 식별합니다.

   CHORUS.ROLE.DB2DBA

   CA Chorus for DB2 Database Management 기능에 대한 액세스 권한을 제어합니다. CA Chorus Infrastructure Management for Networks and Systems는 CA Insight의 데이터를 제공하지만 이 전문 분야에는 리소스가 필요하지 않습니다.

   CHORUS.ROLE.INFRASTRUCTURE

   CA Chorus Infrastructure Management for Networks and Systems 기능에 대한 액세스 권한을 제어합니다.

   CHORUS.ROLE.SECURITY

   CA Chorus for Security and Compliance Management 기능(UI 및 배치)에 대한 액세스 권한을 제어합니다.

CHORUS.ROLE.STORAGE

CA Chorus for Storage Management 기능에 대한 액세스 권한을 제어합니다.

CHORUS.ROLE.SDK*instance*

SDK 역할에 대한 액세스 권한을 제어합니다. CA Chorus는 여러 SDK를 지원할 수 있습니다. 이 이름을 정의하여 공유하려면 시스템 관리자 및 응용 프로그램 관리자와 함께 작업하십시오. 응용 프로그램 개발자는 이 이름을 사용하여 SDK를 지원하는 데 필요한 파일을 빌드하는 것이 좋습니다. 자세한 내용은 *Software Development Kit 사용자 안내서*를 참조하십시오.

instance

SDK용 인스턴스 리소스를 식별하는 영숫자 문자열입니다.

CHORUS.SETTINGS.KNOWLEDGECENTER

사용자가 Knowledge Center의 내용을 인덱싱할 수 있음을 나타냅니다.

CHORUS.SETTINGS.AUTOREFRESH

사용자가 자동 새로 고침 옵션을 사용할 수 있음을 나타냅니다.

uid-of-userid1, uid_of_userid2, ..., uid_of_useridn

액세스를 요청하는 CA Chorus 사용자의 UID 를 나타냅니다.

READ

사용자가 READ 액세스 권한을 갖고 있음을 나타냅니다.

3. CAMFC 리소스에 대해 변경한 내용을 적용합니다.

   ```
   SETROPTS RACLIST(CAMFC) REFRESH
   ```

   변경 내용이 적용됩니다.

사용자는 지정한 리소스에 대한 액세스 권한을 보유하며 CA Chorus 에 로그인하여 작업할 수 있습니다.

예제

다음 명령은 사용자 ABC1 에게 다음을 수행할 수 있는 권한을 부여합니다.

- CA Chorus 에 로그인합니다.
- CA Chorus for Security and Compliance Management 의 기능을 사용합니다.
- Knowledge Center 의 설명서를 수정합니다.
- 자동 새로 고침 옵션을 사용합니다.

```
PERMIT CHORUS.ROLE.SECURITY ID(ABC1) AC(READ) CLASS(CAMFC)
PERMIT CHORUS.SETTINGS.KNOWLEDGECENTER ID(ABC1) AC(READ)
CLASS(CAMFC)
PERMIT CHORUS.SETTINGS.AUTOREFRESH ID(ABC1) AC(READ) CLASS(CAMFC)
SETROPTS RACLIST(CAMFC) REFRESH
```

(선택 사항) CA Chorus 에 대한 CA CSM PassTicket 구성 방법

CA Chorus 에서 사용하는 PassTicket 보안을 통해 추가 사용자 로그인 없이 "Quick Links"(빠른 링크)에서 CA CSM 을 시작할 수 있습니다. Passticket 을 사용하는 모든 시스템은 네트워크에 있는 모든 노드에 대해 동일한 응용 프로그램 이름과 세션 키를 가져야 합니다.

이 시나리오에서는 보안 관리자 및 시스템 관리자가 추가 사용자 로그인 없이 CA CSM 을 사용할 수 있도록 PassTicket 을 구성하는 방법을 보여 줍니다.

중요! 이 시나리오의 절차는 ETJI095*x* 보안 작업을 실행하고 있다는 것을 전제로 합니다. 아직 실행하지 않았다면 해당 단계를 먼저 완료해야 합니다.

PassTicket 은 임시로 인코딩되고 암호화된 사용자 암호의 대용물로서 특정 응용 프로그램에 액세스하기 위해 사용할 수 있습니다. PassTicket 은 생성된 후 몇 분 이내에 사용해야 합니다. PassTicket 을 사용하면 z/OS 구성 요소 및 제품이 네트워크를 통해 z/OS 암호를 전송하지 않고도 사용자 ID 를 인증할 수 있습니다. 대신, 사용자는 올바른 z/OS 사용자 ID 와 암호를 사용하여 처음 로그인한 이후에 인증됩니다. 다음 프로세스는 사용자가 z/OS 구성 요소에 액세스하는 기능을 선택할 때 발생합니다.

- CA Chorus 웹 서비스가 액세스 권한 부여를 위해 PassTicket 을 생성하기 위해 z/OS 보안 제품을 호출합니다.
- PassTicket 이 사용자 요청과 함께 (주로 다른 z/OS 시스템에 있는) 구성 요소로 전달됩니다.
- 요청을 처리하기 전에 PassTicket 을 암호 대용물로 사용하여 사용자를 인증하기 위해 구성 요소가 z/OS 보안 제품을 호출합니다.

참고: CA ACF2, CA Top Secret 및 IBM RACF 를 사용하여 CA CSM 에 연결하도록 PassTicket 을 구성하는 예가 제공됩니다. 이러한 예는 참조용으로 제공됩니다. CA ACF2 명령 사용에 대한 자세한 내용은 *CA ACF2 Administration Guide*(CA ACF2 관리 안내서)를 참조하십시오. CA Top Secret 사용에 대한 자세한 내용은 *CA Top Secret Command Functions Guide*(CA Top Secret 명령 기능 안내서)를 참조하십시오. IBM RACF 에 대한 자세한 내용은 IBM 설명서를 참조하십시오.

CA Chorus 에서 CA CSM 을 시작하여 사용하려면 다음 작업을 완료해야 합니다.

1. PassTicket 을 사용하도록 보안 시스템을 구성합니다. 다음 옵션 중 *하나*를 선택합니다.
   - CA ACF2 를 사용하여 CA Chorus 에서 CA CSM 으로 연결할 수 있도록 PassTicket 구성 (페이지 60)
   - CA Top Secret 를 사용하여 CA Chorus 에서 CA CSM 으로 연결할 수 있도록 PassTicket 구성 (페이지 62)
   - IBM RACF 를 사용하여 CA Chorus 에서 CA CSM 으로 연결할 수 있도록 PassTicket 구성 (페이지 63)
2. CA CSM 시작 매개 변수를 업데이트합니다 (페이지 66).

중요! CA Chorus 에서 사용하는 것과 동일한 CA CSM Applid 를 사용하는지 확인하십시오.

예제: CA ACF2 를 사용하여 CA Chorus 에서 CA CSM 으로 연결할 수 있도록 PassTicket 구성

이 예제에서는 보안 관리자가 ETJI095*x* 보안 작업을 실행한 후 CA Chorus 에서 CA CSM 으로 연결할 수 있도록 PassTicket 을 구성하는 방법을 보여 줍니다.

참고: 이 절차의 명령은 예제입니다. 이러한 명령 사용에 대한 자세한 내용은 *CA ACF2 for z/OS Administration Guide*(CA ACF2 for z/OS 관리 안내서)를 참조하십시오.

이 절차에서는 CA Chorus 서버 및 CA CSM 서버에 보안을 설정해야 합니다. 다음 절차에는 작업 위치, 새 서버로 초점을 전환해야 하는 시점 등이 강조 설명되어 있습니다. 참고로, 다음 정의는 두 서버 모두에 적용됩니다.

applid

CA Chorus 의 "Quick Links"(빠른 링크) 모듈에 대한 PassTicket 유효성 검사에 사용되는 응용 프로그램 ID 를 정의합니다. *applid* 를 사용 중인 CA CSM applid 로 대체합니다. CA CSM 구성에 대한 자세한 내용은 CA CSM 시작 매개 변수 업데이트 (페이지 66)를 참조하십시오.

기본값: CSMAPPLM

MULT-USE

동일한 PassTicket 을 여러 번 다시 사용할 수 있게 해 줍니다.

SSKEY

예에 표시된 값과는 다른 응용 프로그램 암호화 키를 임의의 16 진수 16 자리 형식으로 정의합니다.

참고: 이 예에서는 16 진수 16 자리(8 바이트 또는 64 비트 키 생성)의 전체 키 SESSKEY 값을 보여 줍니다. 각 응용 프로그램 키는 구성에 포함된 모든 시스템에서 동일해야 하며 값은 "비밀"로 안전하게 유지해야 합니다.

CA Chorus 서버 측 단계

1. 개별 사용자가 CA CSM 에 액세스할 수 있도록 허용합니다.

```
SET RESOURCE(SAF)
RECKEY applid ADD(UID(chorus_userid) SERVICE(READ) ALLOW)
F ACF2,REBUILD(SAF)
```

chorus_userid

"Quick Links"(빠른 링크) 모듈을 통해 CA CSM 에 액세스해야 하는 사용자입니다.

CA Chorus 서버 측에서 PassTicket 이 구성됩니다.

(선택 사항) CA CSM 서버 측 단계

참고: APPL 클래스에 대한 유형 코드를 APL 로 변경하기 위해 GSO CLASMAP 레코드를 삽입한 경우 다음 명령에서 TYPE 에 SAF 대신 APL 을 사용하십시오.

중요! CA Chorus 및 CA CSM 이 동일한 컴퓨터에 위치하지 않은 경우 1 단계와 2 단계를 수행해야 합니다. 3 단계는 모든 상황에 적용되어야 합니다.

1. CA CSM 연결 응용 프로그램 세션 키를 정의합니다.

```
SET PROFILE(PTKTDATA) DIV(SSIGNON)
INSERT applid SSKEY(0123456789ABCDEF) MULT-USE
F ACF2,REBUILD(PTK),CLASS(P)
```

2. CA CSM 시작된 작업 사용자 ID 가 CA CSM 사용자를 위해 PassTicket 을 생성하고 평가할 수 있도록 허용합니다.

```
SET RESOURCE(PTK)
RECKEY IRRPTAUTH ADD(applid.- UID(uid-of-csm_stc_userid)
SERVICE(UPDATE,READ) ALLOW)
F ACF2,REBUILD(PTK)
```

uid_csm_stc_userid

CA CSM 응용 프로그램 서버의 시작된 작업 사용자 ID 를 지정합니다. 이 ID 는 모든 사용자에 대해 PassTicket 을 생성할 수 있어야 합니다.

기본값: MSMSERV

3. 개별 사용자가 CA CSM 에 액세스할 수 있도록 허용합니다.

```
SET RESOURCE(SAF)
RECKEY applid ADD(UID(uid-csm_userid) SERVICE(READ) ALLOW)
F ACF2,REBUILD(SAF)
```

CA CSM 서버 측에서 PassTicket 이 구성됩니다.

PassTicket 설정을 완료하려면 CA CSM 시작 매개 변수 업데이트 (페이지 66)로 이동합니다.

예제: CA Top Secret 를 사용하여 CA Chorus 에서 CA CSM 으로 연결할 수 있도록 PassTicket 구성

이 예제에서는 보안 관리자가 ETJI095*x* 보안 작업을 실행한 후 CA Chorus 에서 CA CSM 으로 연결할 수 있도록 PassTicket 을 구성하는 방법을 보여 줍니다.

참고: 이 절차는 PTKTDATA 클래스 및 IRRPTAUTH 리소스 소유권이 정의되었다고 가정합니다.

이 절차에서는 CA Chorus 서버 및 CA CSM 서버에 보안을 설정해야 합니다. 다음 절차에는 작업 위치, 새 서버로 초점을 전환해야 하는 시점 등이 강조 설명되어 있습니다. 참고로, 다음 정의는 두 서버 모두에 적용됩니다.

applid

CA Chorus 의 "Quick Links"(빠른 링크) 모듈에 대한 PassTicket 유효성 검사에 사용되는 응용 프로그램 ID 를 정의합니다. *applid* 를 사용 중인 CA CSM applid 로 대체합니다. CA CSM 구성에 대한 자세한 내용은 CA CSM 시작 매개 변수 업데이트 (페이지 66)를 참조하십시오.

기본값: CSMAPPLM

department

기존 부서를 나타냅니다. 응용 프로그램은 이 부서에 정의됩니다. 이 소유권이 있으면 부서 관리자나 그 이상의 권한을 가진 사용자는 PassTicket 생성 및 유효성 검증을 정의할 수 있습니다.

SESSKEY

예에 표시된 값과는 다른 응용 프로그램 암호화 키를 임의의 16 진수 16 자리 형식으로 정의합니다.

참고: 이 예에서는 16 진수 16 자리(8 바이트 또는 64 비트 키 생성)의 전체 키 SESSKEY 값을 보여 줍니다. 각 응용 프로그램 키는 구성에 포함된 모든 시스템에서 동일해야 하며 값은 "비밀"로 안전하게 유지해야 합니다.

SIGNMULTI

동일한 PassTicket 을 여러 번 다시 사용할 수 있게 허용합니다.

CA Chorus 서버 측 단계

ETJI095*x* 작업을 실행한 경우 이 서버에 대해 PassTicket 이 이미 구성되어 있습니다.

(선택 사항) CA CSM 서버 측 단계

중요! CA Chorus 및 CA CSM 이 동일한 컴퓨터에 위치하지 않은 경우 이 절차를 완료해야 합니다.

1. CA CSM 연결 응용 프로그램 세션 키를 정의합니다.

   ```
   TSS ADDTO(NDT) PSTKAPPL(applid) SESSKEY(0123456789ABCDEF) SIGNMULTI
   ```

2. CA CSM 시작된 작업 사용자 ID 가 CA CSM 사용자를 위해 PassTicket 을 생성하고 평가할 수 있도록 허용합니다.

   ```
   TSS PERMIT(csm_stc_userid) PTKTDATA(IRRPTAUTH.applid.) ACCESS(READ,UPDATE)
   ```

   csm_stc_userid

   CA CSM 응용 프로그램 서버의 시작된 작업 사용자 ID 를 지정합니다. 이 ID 는 모든 사용자에 대해 PassTicket 을 생성할 수 있어야 합니다.

3. 해당 department 에 Applid 를 추가합니다.

   ```
   TSS ADDTO(department) APPLICATION(applid)
   ```

4. 개별 사용자가 CA CSM 에 액세스할 수 있도록 허용합니다.

   ```
   TSS PERMIT(csm_stc_userid) APPL(applid)
   ```

   CA CSM 서버 측에서 PassTicket 이 구성됩니다.

   PassTicket 설정을 완료하려면 CA CSM 시작 매개 변수 업데이트 (페이지 66)로 이동합니다.

예제: IBM RACF 를 사용하여 CA Chorus 에서 CA CSM 으로 연결할 수 있도록 PassTicket 구성

이 예제에서는 보안 관리자가 ETJI095*x* 보안 작업을 실행한 후 CA Chorus 에서 CA CSM 으로 연결할 수 있도록 PassTicket 을 구성하는 방법을 보여 줍니다.

참고: 이 절차를 시작하기 전에 PTKTDATA 클래스와 PassTicket 리소스(IRRPTAUTH)에 대한 소유권이 이미 정의되어 있는지 확인해야 합니다.

이 절차에서는 CA Chorus 서버 및 CA CSM 서버에 보안을 설정해야 합니다. 다음 절차에는 작업 위치, 새 서버로 초점을 전환해야 하는 시점 등이 강조 설명되어 있습니다. 참고로, 다음 정의는 두 서버 모두에 적용됩니다.

applid

CA Chorus 의 "Quick Links"(빠른 링크) 모듈에 대한 PassTicket 유효성 검사에 사용되는 응용 프로그램 ID 를 정의합니다. *applid* 를 사용 중인 CA CSM applid 로 대체합니다. CA CSM 구성에 대한 자세한 내용은 CA CSM 시작 매개 변수 업데이트 (페이지 66)를 참조하십시오.

기본값: CSMAPPLM

KEYMASKED

샘플 구문에 있는 것과 다른 값을 사용하여 응용 프로그램의 암호화 키를 정의합니다.

참고: 샘플 구문에서는 16 진수 16 개로 구성되어 8 바이트 즉, 64 비트 키를 생성하는 전체 키 값을 보여 줍니다. 각 응용 프로그램 키는 구성에 포함된 모든 시스템에서 동일해야 하며 값은 "비밀"로 안전하게 유지해야 합니다.

APPLDATA('NO REPLAY PROTECTION')

동일한 PassTicket 을 여러 번 사용할 수 있게 해 줍니다.

CA Chorus 서버 측 단계

ETJI095*x* 작업을 실행한 경우 이 서버에 대해 PassTicket 이 이미 구성되어 있습니다.

(선택 사항) CA CSM 서버 측 단계

중요! CA Chorus 및 CA CSM 이 동일한 컴퓨터에 위치하지 않은 경우 이 절차를 완료해야 합니다.

1. CA CSM 연결 응용 프로그램 세션 키를 정의합니다.

   ```
   SETROPTS CLASSACT(PTKTDATA) RACLIST(PTKTDATA)
   RDEFINE PTKTDATA applid SSIGNON(KEYMASKED(FEDCBA9876543210)) APPLDATA('NO
   REPLAY PROTECTION')
   ```

2. CA CSM 시작된 작업 사용자 ID 가 CA CSM 사용자를 위해 PassTicket 을 생성하고 평가할 수 있도록 허용합니다.

   ```
   SETROPTS GENERIC(PTKTDATA)
   RDEFINE PTKTDATA IRRPTAUTH.applid.* CLASS(PTKTDATA) UACC(NONE)
   PERMIT IRRPTAUTH.applid.* CLASS(PTKTDATA) ID(csm_stc_userid)
   ACCESS(READ,UPDATE)
   ```

   csm_stc_userid

   CA CSM 응용 프로그램 서버의 시작된 작업 사용자 ID 를 지정합니다. 이 ID 는 모든 사용자에 대해 PassTicket 을 생성할 수 있어야 합니다.

   기본값: MSMSERV

3. 개별 사용자가 CA CSM 에 액세스할 수 있도록 허용합니다.

   ```
   RDEFINE APPL applid UACC(NONE)
   PERMIT applid CLASS(APPL) ID(csm_stc_userid) ACCESS(READ)
   SETROPTS CLASSACT(APPL)
   ```

4. PTKTDATA 클래스를 새로 고치고 APPL 클래스를 활성화합니다.

   ```
   SETROPTS RACLIST(PTKTDATA) REFRESH
   SETROPTS CLASSACT(APPL)
   ```

   CA CSM 서버 측에서 PassTicket 이 구성됩니다.

   PassTicket 설정을 완료하려면 CA CSM 시작 매개 변수 업데이트 (페이지 66)로 이동합니다.

CA CSM 시작 매개 변수 업데이트

다음 절차에서는 시스템 관리자가 생성된 CA CSM 응용 프로그램 ID 로 CA CSM 응용 프로그램 서버를 시작하는 방법을 보여 줍니다.

다음 단계를 수행하십시오.

1. CA CSM 응용 프로그램 ID 를 지정하도록 SAMPLIB(MSMLIB) 멤버에 다음 문을 추가합니다.

   ```
   IJO="$IJO -DmsmApplid=applid"
   ```

   applid

   서버에 대한 연결을 인증하기 위해 PassTicket 유효성 검사에 사용되는 CA CSM 응용 프로그램 ID 를 정의합니다.

   기본값: CSMAPPLM

2. CA CSM 응용 프로그램 서버를 다시 시작합니다.

   변경 사항이 적용됩니다.

사용자는 이제 "Quick Links"(빠른 링크) 모듈에서 CA CSM 에 액세스할 수 있습니다.