CA Chorus™

站点准备指南

版本 03.0.00，第三版

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- 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)

联系技术支持

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：http://www.ca.com/worldwide。

文档更改

下表详细介绍了自第二版以来所做的更改：

软件要求 (p. 22)－澄清了 CCS 和 CA CSM 对 FIXCAT 的要求，并且更正了创建 CA Datacom/AD MUF 的作业顺序。

下表详细介绍了自第一版以来所做的更改：

示例：使用 IBM RACF 授权用户 (p. 45)－更正了步骤 1 中的 CA Chorus for DB2 Database Management 参考。它现在称为 DB2DBA。

服务器要求 (p. 25)－为选择的所有管控领域添加了修订的堆值和新示例。

软件要求 (p. 22)－澄清了浏览器要求并更新了 IBM z/OS 对 1.12 或更高版本的支持。

下表详细介绍了先前在《*安装指南*》中显示的内容的更改：

常规－创建了本指南以介绍系统程序员和安全管理员可以在安装产品前完成的任务。

安装过程的工作原理 (p. 11)－添加了此主题和图表，说明如何使用本指南和《*安装指南*》。

安装前计划 (p. 13)－更新了此主题以介绍这本新指南和新的“HLQ 要求”主题。

安全管理员和系统程序员核查清单 (p. 14)－添加了此主题以详细说明，只有两个角色事先一致同意，才能使用本指南。

安全 ID 重复使用注意事项 (p. 18)－为重复使用 2.0 和 2.5 安全 ID 的客户端添加了此主题。

系统要求 (p. 26)－删除了堆内存要求。

CA Chorus 服务器要求 (p. 25)－修订了堆内存要求并将其移至这个新主题。

内存限制 (p. 26)－添加了此主题。

软件要求 (p. 22)

- 澄清了 CCS 14.1 版和 CA Datacom/AD 版本 14 的要求并且更新了“IBM 64-bit SDK for z/OS、Java Technology Edition、Version 7 Release 0 Modification 0 Service **Release 2** (5655-W44)，包括可选的 JZOS 批处理启动器”。
- 更新了 CA CSM 要求以指出必需的 PTF 为 RO56614。
- 添加了 FIXCAT 标签以用于 CA Datacom/AD 维护。

目标库 (p. 27)

- 删除了 CETJDATV、CETJSIDE 和 CETJZFS1。
- 更新了 CETJJCL、CETJTOPN、CETJXML 以及 TPV.AETJHFS 的值。

分发库 (p. 28)

- 删除了 TPV.AETJJAR、AETJDATV 和 TPV.AETJSHSC。
- 更新了 AETJJCL、AETJOPTN、AETJXML 以及 TPV.AETJHFS 的值。

端口要求 (p. 29)—将最大值要求从 17 更新到 12。

（可选）SMTP 电子邮件要求 (p. 30)—添加了此主题以说明可在平台配置期间收集以供日后使用的数据。

USS Parmlib 要求 (p. 30)—添加了检查此设置的命令。

安装程序安全权限 (p. 31)—定义了 FSACCESS 选项。

运行 CA Chorus 安全作业 (p. 32)—添加了此主题，并且删除了此作业自动完成、先前人工完成的相关主题。

如何授权用户在 CA Chorus 中工作 (p. 37)

- 将此场景从《*管理指南*》移到了本指南中。
- 添加了 CA Chorus Infrastructure Management for Networks and Systems 并自动刷新了资源。
- 删除了“查看用户软件要求”。此信息现显示在“软件要求 (p. 22)”中。
- （可选）使用 EXPLAIN 命令将“授权使用辅助授权 ID”移到了《*CA Chorus for DB2 Database Management 站点准备指南*》中。

授权 CA Chorus 用户访问 z/OS UNIX 系统服务资源 (p. 38)—添加了预先检查步骤以确认这些设置是否已经存在。

如何为 CA Chorus 配置 CA CSM PassTicket (p. 48)—更新了此场景以说明 ETJI095*x* 安全作业所涉及的步骤。

如何为 CA Chorus 配置 CA CSM PassTicket (p. 48)—添加了此场景。

示例：使用 IBM RACF 授权用户 (p. 45)－添加了新的步骤 1，将每个管控领域资源添加到 CAMFC 中。

运行 CA Chorus 安全作业 (p. 32)－更新了此场景以添加“CA CSM 用户的 PassTicket”子主题。

目录

第 1 章： 简介

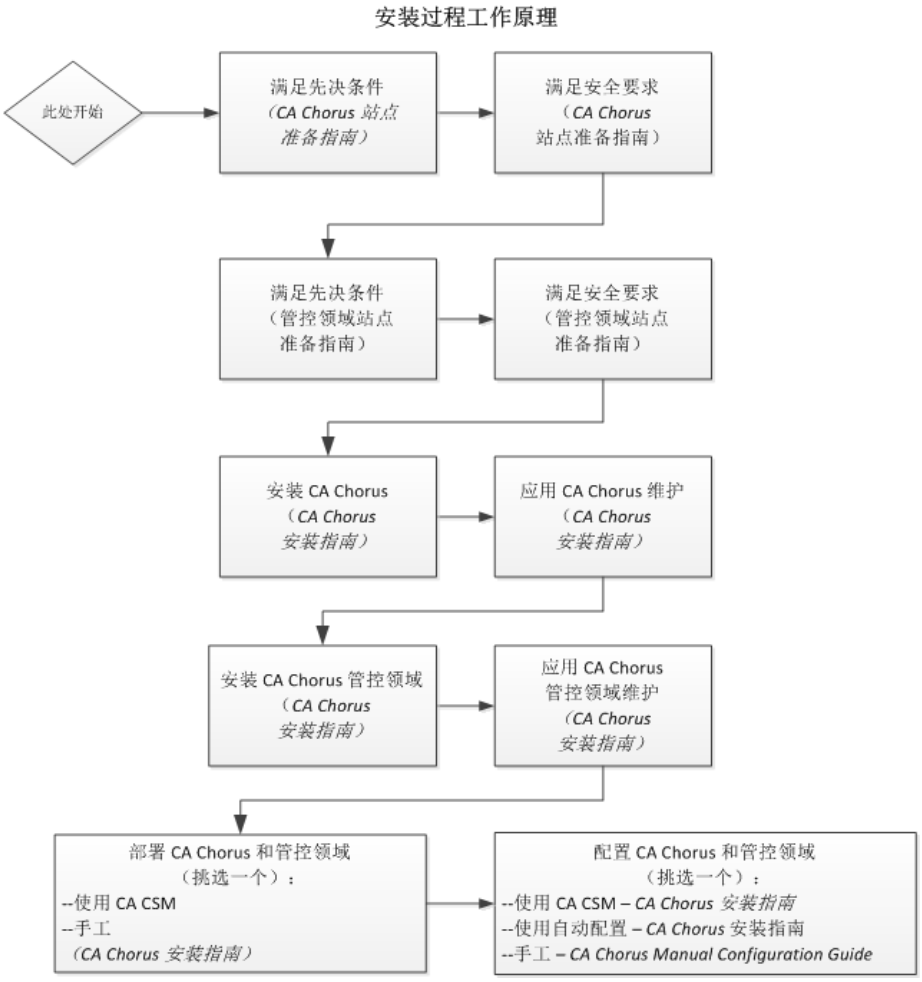
此部分包含以下主题：

安装过程的工作原理

本指南详细说明了系统程序员和安全管理员在开始《*安装指南*》中介绍的安装、部署和配置任务前能够完成的任务。下图提供了有关 CA Chorus 和管控领域安装、部署和配置过程的总体概览，以及您使用的指南。

重要提示！ 您必须使用 CA Chorus Software Manager 来安装 CA Chorus 及其管控领域。

注意：对于指示管控领域《*站点准备指南*》中的工作的框，请针对您要安装的每个管控领域重复此步骤。



要安装、部署和配置您的 CA Chorus 及其管控领域，请完成下列步骤：

1. 满足《*CA Chorus 站点准备指南*》中所述的软件、系统、端口要求以及其他先决条件。
2. 满足《*CA Chorus 站点准备指南*》中所述的安全要求。
3. 满足适用管控领域《*站点准备指南*》中所述的软件、系统、端口要求以及其他先决条件。针对您要安装的每个管控领域重复此步骤。
4. 满足适用管控领域《*站点准备指南*》中所述的安全要求。针对您要安装的每个管控领域重复此步骤。
5. 按照《*CA Chorus 安装指南*》中所述，使用 CA CSM 安装 CA Chorus 及适用管控领域。此步骤涉及获取 CA Chorus 软件（传输到您的 z/OS 系统）以及使用 SMP/E 进行安装。在安装过程中，将创建 CSI 环境并运行 RECEIVE、APPLY 和 ACCEPT SMP/E 步骤。软件是非定制的。
6. 使用 CA CSM 或手工过程部署 CA Chorus 及适用管控领域。《*CA Chorus 安装指南*》详细介绍了这两种方法。

   此步骤将目标库复制到另一个系统或 LPAR。

   重要提示！对于使用 CA CSM 进行的部署，必须同时部署 CA Chorus 和管控领域。例如，不支持安装 CA Chorus、DBA 和 Security 后仅部署 CA Chorus 和 DBA。

   重要提示！为了使用 CA CSM 软件配置服务，必须进行 CA CSM 部署。
7. 配置 CA Chorus 和管控领域。此步骤会创建自定义的加载模块，使 CA Chorus 软件进入可执行状态。使用下列方法之一配置产品：

   注意：建议您使用前两个选项之一作为最有效的方法来配置您的产品。

   CA CSM

   通过此方法，您可以使用基于向导的 CA CSM 工具来配置产品。

   《*安装指南*》包括此方法的 CA Chorus 和管控领域步骤。

   自动化配置

   通过此方法，您可以编辑一个批处理作业 (ETJICUST) 和一个配置文件。接着一个 Java 程序会将您的更改传播到适用的成员。然后您可以手工提交每个作业。对于此选项，建议您同时配置平台和管控领域。

   《*安装指南*》包括此方法的 CA Chorus 和管控领域步骤。

   手工

   通过此方法，您可以手工编辑和运行每个配置作业。

   如果采用此方法，请按照《*Manual Configuration Guide*》中的描述配置 CA Chorus 及其管控领域。

第 2 章： 满足常规先决条件

本章详细介绍了系统程序员在开始 CA Chorus 的安装、部署和配置任务前必须完成的所有任务。

此部分包含以下主题：

安装前计划

CA Chorus 安装是一个详细的过程，需要在若干个领域具有专业经验的人员。建议您在安装开始之前会见以下每个团队成员并复查每个人的角色：

- 负责 z/OS 的系统程序员
- 负责 DASD 分配的存储管理员
- 负责访问权限和安全配置的安全管理员
- 负责 DB2 和/或 CA Datacom/AD 配置的数据库管理员

对于此次会见，建议您使用以下项：

- 安全管理员和系统程序员核查清单 (p. 14)
- 平台和适用管控领域《*站点准备指南*》
- *安装指南*
- 适用的安全作业 ETJI095*x*，其中 x 等于 A 时表示 CA ACF2，等于 T 时表示 CA Top Secret，等于 R 时表示 IBM RACF。这些作业位于 CA Chorus 产品页面上。

重要提示！ 在所有团队成员都清楚了解其安装责任后，再开始安装。否则会影响安装的及时完成。

安全管理员和系统程序员核查清单

本部分的每个表详细介绍了高级安装详细信息。建议安全管理员和系统程序员一起检查每张表。检查之后，在任何人开始本指南和《*安装指南*》中的工作之前，管理员必须同意特定详细信息，或者必须了解其他信息。

对于表中的某些条目，指定所同意的值。对于其他条目，简单地协调实施详细信息。

重要提示！ 完成这些清单中的工作以后，再开始任何准备或安装过程。例如，进行安全设置和产品配置时需要这些表中的值。

安全注意事项

在下表中：

- 安全符号以 & 或 % 开头。这些符号在安全管理员运行的 ETJI095*x* 安全作业中显示。

  %

  表示默认值。

  &

  表示您必须确定值。

- 带阴影的单元格表示不需要记录值，但是在开始执行本指南中的工作之前需要查看此内容。

ID 或 安全实体	定义	值	符号
CHORGRP	CA Chorus 管理组（可选） 指定默认组名称。		%CHORGRP
CHORUGRP	CA Chorus 用户组（可选） 通过将资源分配给组而不是个人用户来帮助进行管理。		&CHORUGRP
CA Chorus 管控领域组	通过将资源分配给组而不是个人用户来帮助进行管理。 用户将连接到其作业功能需要的管控领域组。 建议使用遵循站点命名标准和组织的名称。		&CHRD*x*GRP （其中 x 标识管控领域）

ID 或 安全实体	定义	值	符号
CHORADM	管理（启动任务所有者）： ■ 拥有启动任务。 ■ 必须有 OMVS 分段。 ■ 用于为用户生成 PassTicket。 **注意：**建议主目录为 CA Chorus USS 安装所在的位置。		%CHORADM
CHORTHD	辅助用户： ■ 仅用作用户 ID，在没有用户登录的情况下访问后端功能。在启动期间主要用来获取配置数据。 ■ 用于生成 PassTicket。用户 ID 从不直接用于作业或在线访问。无人可以访问此用户 ID 的密码。对于 RACF，密码是必需的。CA ACF2 或 CA Top Secret 不使用密码。 ■ CHORJBOS 必须能够为 CHORTHD 生成 PassTicket，并且必须授权 CHORTHD 访问适当的应用程序 (APPLID)。 ■ 需要与 CA Chorus 用户相同的安全权限，下列项除外： -- CAMFC -- CETJOPTV CETJEZTR，以便 CA Easytrieve 报告执行 ■ 有些管控领域可能需要 CHORTHD 授权才能访问后端产品。有关详细信息，请参阅适用管控领域《*站点准备指南*》。		%CHORTHD
安装程序 ID	安装程序的用户 ID 必须具有对新 HLQ 和数据集的更新访问权限。在安装之后，可以撤回更新权限。 有关完整的详细信息，请参阅“安装程序安全权限 (p. 31)”。		&INSTALLER
PassTicket	CA Chorus 平台需要 PassTicket 资源。管控领域需要其他 PassTicket 定义。 PassTicket 访问权限将针对组还是针对个人定义？ ■ 组更容易管理，并且可能允许更加分散。通过安全中心保持组授权，但是本地（组）管理员会控制成员资格。 ■ 有些站点可能更希望按用户明确显示访问权限。		

ID 或 安全实体	定义	值	符号
	安全管理员必须为每个应用程序选择 KEYMASKED 或 SESSKEY 值。但由于必须保护该值，因此不会在此处输入值。同样的值必须用于所有系统上的应用程序。		
	CHORWEBS：为用户生成 PassTicket 的默认应用程序 ID。如果您打算使用其他 APPL，请确认并记录该值。		%CHORWEBS
	CSMAPPLM：为从快速链接模块启动 CA CSM 的用户生成 PassTicket 的默认应用程序 ID。如果您打算使用其他 APPL，请确认并记录该值。这些步骤不在 ETJI095*x* 中。请参阅“如何配置 CA CSM PassTicket (p. 48)”。 如果未添加 CA CSM 作为快速链接，则忽略此选项。		&CSMAPPLM
CAMFC	CAMFC 是专门针对 CA Chorus 的资源类。类和条目的名称被修复。平台有一个条目－CHORUS.SETTINGS.KNOWLEDGECENTER：只有将更新或维护知识中心内用户文档的用户才需要此条目。 每个管控领域在此类中都有一个条目。应当允许管控领域组对管控领域的条目进行读取访问。		
CAWEBSVR 主工具	仅 CA Top Secret：您必须定义用户，并将其添加到此主工具。		
程序控制（APF 授权）	启动任务的 steplib 中指定的数据集必须受程序控制。对于使用 CA ACF2 或 CA Top Secret 的站点，这些库必须经过 APF 授权。		
	带有 HLQ for Runtime Environment 的库： ■ CETJPLD：包括 CA Chorus 库。 ■ CETJLOAD：包括 CA Chorus 库。 ■ CC2DLOAD：包括 Time Series Facility (TSF) 库。		
	作为满足 CA Datacom/AD 先决条件的一部分，下列库应当经过 APF 授权：*datacomad_adthlq*.CAAXLOAD（CA Datacom/AD 加载库）和 *datacomad_adchlq*.CUSLIB（CA Datacom/AD 自定义库）。		

ID 或 安全实体	定义	值	符号
	（仅 IBM RACF）非 CA Chorus 库 CA Chorus 所使用的库必须受程序控制，即使他们是在链接列表中，并且未在 CA Chorus 中明确指定。在其产品被安装时，这些库可能已添加到程序控制中，但是现在，系统管理员必须验证此配置。 系统程序员必须提供站点特定的名称。 ■ Java v7 m0 库：&JAVALIB ■ CCS.CAW0LINK：CA CCS 库 - 版本 14.1（对于版本 2.5 CA Chorus） ■ TCPIP.SEZALOAD - ■ SYS1.CSSLIB：来自 IBM 的 C++ 库		

更多信息：

运行 CA Chorus 安全作业 (p. 32)

安全 ID 重复使用注意事项

请注意版本 3.0 安全 ID 实施的以下更改。如果您在版本 2.0 或版本 2.5 中重复使用安全 ID，则将以下对象添加到 3.0 实施中。要查看与这些更改有关的示例命令，请参阅适用的 ETJI095*x* 作业。在此作业中，*x* 等于 A 时表示 CA ACF2，等于 T 时表示 CA Top Secret，等于 R 时表示 IBM RACF。

重要提示！版本 3.0 需要外部的 CA Datacom/AD Multi-User Facility (MUF)。因此，要识别运行您的 MUF 的数据集。

CA ACF2

用户 ID CHORTHD：使用 PassTicket 进行登录的辅助登录 ID。

CAMFC：新的 SETTINGS.AUTOREFRESH 功能的 CA Chorus 平台资源。

规则：CA Datacom/AD 自定义库 CUSLIB。

CA Chorus Software Manager 快速链接（可选）

CA Top Secret

ACID %CHORTHD：使用 PassTicket 进行登录的辅助登录 ID。

配置文件 %CHORUPF： CA Chorus 用户的配置文件（可选）

CAMFC：新的 SETTINGS.AUTOREFRESH 功能的 CA Chorus 平台资源。

数据集： CA Datacom/AD 自定义库 CUSLIB。

CA Chorus Software Manager 快速链接（可选）

IBM RACF

用户 ID %CHORTHD：使用 PassTicket 进行登录的辅助登录 ID。

组 %CHORUGRP： CA Chorus 用户的组（可选）

CAMFC：新的 SETTINGS.AUTOREFRESH 功能的 CA Chorus 平台资源。

数据集： CA Datacom/AD 自定义库 CUSLIB。

特定库的常规数据集配置文件

CA Chorus Software Manager 快速链接（可选）

更多信息：

运行 CA Chorus 安全作业 (p. 32)

数据集注意事项

在下表中：

- 安全符号以 & 或 % 开头。这些符号在安全管理员运行的 ETJI095*x* 安全作业 (p. 32)中显示。

  %

  表示默认值。

  &

  表示您必须确定值。

- 带阴影的单元格表示不需要记录值，但是在开始执行本指南中的工作之前需要查看此内容。

数据集	注意事项	值	符号
现有	在允许 CA Chorus ID 访问之前，如果数据集事先没有在安全产品中定义，可能还需要定义组和配置文件。		
	TCP/IP 启动任务的 SYSTCPD DD 语句中指定的数据集或库成员必须提供给 CHORADM（只读）。此数据集随系统而变化。		&TCPDATA
	Java v7 库必须提供给 CHORADM 和 CHORUGRP（只读）		&JAVALIB
	UNIX 系统服务 (USS) Java 主目录必须可供 CHORADM 读取。 这可能还需要将 FSACCESS 读到已挂接的文件系统中（如果启用了 FSACCESS）。		@JAVA_HOME **注意：**您不需要此安全值，但是您可能需要挂接到它的数据集。
CA Chorus 安装数据集	团队必须同意安装 HLQ for CA Chorus。 **注意：**安装 HLQ 不同于运行时环境。两者可能都需要进行定义。但没有为这些条目提供默认值。 示例 JCL 提供用于搭建运行时环境的命令：		
	HLQ：安装环境		无
	HLQ：运行时环境		$CAI @RT_HLQ

数据集	注意事项	值	符号
运行时数据集	其他 HLQ for CA Chorus		
	HLQ for VSAM 数据集。如果站点标准指出 VSAM 文件应有特别的分配要求，可以将另一个 HLQ 分配给 VSAM 数据集。		$TSF
	数据库文件的 HLQ。您可能想要区别 CA Chorus 使用的 CA Datacom/AD 数据文件。在为 CA Chorus 特别创建的 MUF 中使用这些文件。		$ADHLQ
CA Datacom/AD 安装数据集	为了供 CA Chorus 使用，需要以下运行时 HLQ。有关详细信息，请参阅《*CA Datacom/AD Installation Guide*》。		
	CA Datacom/AD 系统库，包括 CAAXLOAD。记录 HLQ。		&ADTHLQ
	CA Chorus 实例特定的库 (CUSLIB)。记录 HLQ。		&ADCHLQ

启动任务注意事项

在下表中：

- 安全符号以 & 或 % 开头。这些符号在安全管理员运行的 ETJI095*x* 安全作业 (p. 32)中显示。

  %

  表示默认值。

  &

  表示您必须确定值。

带阴影的单元格表示不需要记录值，但是在开始执行本指南中的工作之前需要查看此内容。

注意：管控领域可能还要求执行作业或其关联产品的启动任务。这些项在各自的产品指南中介绍。

项目	定义	值	符号
启动任务	CA Chorus 有多个启动任务和一个生成的任务。您可以根据您的站点标准和首选项，为其命名。默认名称如下：		

项目	定义	值	符号
	CHORJBOS：JBoss 服务器 承载 CA Chorus 应用程序。JBoss 是跨平台运行的、基于 Java 的开源应用程序服务器。JBoss 可在任何支持 Java 的操作系统上使用。		CHORJBOS
	CA Datacom/AD Multi User facility (MUF) MUF 是系统的管理器，并且充当数据的操作系统。它接收来自应用程序的请求，并确定请求的处理方式。它协调必须为请求执行的活动。您构建新的和专用的 MUF 作为安装 CA Chorus 的先决条件。 记录您创建的 MUF 名称。		&AD_MUF_STCID
	MUF 所有者：拥有 MUF 启动任务的用户 ID。		&AD_MUF_OWNER
	CHORTSF：Time Series Facility (TSF) TSF 使您可以在线图中查看性能数据。		%CHORTSF
	CHORTSFR：Time Series Facility 中继任务 通过 TSF 数据中继，可以将远程 LPAR 上收集的数据发送到 TSF。		%CHORTSFR
	CHORJBOS 为 CA DSI 安全验证生成其他任务。 如果您想让此任务与为 CHORJBOS 选择的任务不同名，请向 CA Chorus 管理用户 ID 授予 BPX.SUPERUSER 和 BPX.DAEMON 工具的读取访问权限。		

软件要求

CA Chorus 需要以下软件：

- CA Technologies 软件－需要以下软件：
  - 带有 CAIRIM 和 CAMASTER 服务组件的 CA Common Services for z/OS (CCS) 版本 14.1，以及 CA Easytrieve 版本 11.6。
  - 应用具有下列 FIXCAT 标签的所有 CCS 维护：CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.V3.0。

    CCS

    服务组件随 CCS 一起交付和安装。如果站点上安装了其他 CA Technologies 产品，则可能已安装这些服务及其他服务。如果尚未安装这些服务，请立即安装。有关安装和配置这些组件的详细信息，请参阅 CCS 文档。

    重要提示！ CAMASTER 地址空间必须正在运行。如果它正在运行，以下消息将作为消息 IPL 部分的一部分包含在 z/OS 系统日志中：
    CAMS101I CAMASTER INITIALIZATION COMPLETE.
    CAMASTER 是不得取消的启动任务，它会向各个 CA 产品和 CCS 提供系统服务和存储资源。CAMASTER 使用的 CPU 最少，并且无法停止或重新启动。

    注意： 作为满足 CCS 先决条件的一部分，CAW0LOAD 加载库必须经过 APF 授权。

    CA Easytrieve

    在 CCS 版本 14.1 之前，CA Easytrieve 作为 Easytrieve Service CDX8E00 交付。自 CCS 版本 14.1 开始，CA Easytrieve 作为独立的 Pax 安装交付。可以在 CCS 模式或完全功能模式下单独安装 CA Easytrieve，而无需多次安装 CA Easytrieve。CCS 14.1 的程序包中随附了 CA Easytrieve Release 11.6。如果您已安装 CA Easytrieve 11.6，则不需要安装随 CCS 14.1 一起分发的副本，因为他们是相同的。如果您尚未安装 CA Easytrieve Release 11.6，请遵循《*CA Easytrieve Release 11.6 Installation Guide*》的附录 B 中列出的说明。

- CA Chorus Software Manager (CA CSM) 版本 5.1 (RO56614)：必须使用 CA CSM 安装 CA Chorus。
- 应用具有下列 FIXCAT 标签的所有 CA Datacom/AD 维护：CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.V3.0。

  重要提示！ 确认 CA CSM 配置了系统设置，可使用特定于产品的文件系统。使用 CA CSM 中的“Settings”选项卡验证此设置。单击“Software Installation”，滚动至右面板中的“SIS Base Install-File System”，然后验证是否已选择“Product Specific File System”对应的项目符号。

  重要提示！ CA Chorus 仅支持 zFS 文件系统。HFS 文件系统不受支持。

- CA Datacom/AD 版本 14

  注意： CA Chorus 不支持 CA Datacom/DB。如果您安装了 CA Datacom/DB，请安装 CA Datacom/AD，并且在安装 CA Chorus 时参考这些库。

  - 需要完整的 CA Datacom/AD 安装和配置。请参阅《*CA Datacom/AD Installation Guide*》。
  - 应用具有下列 FIXCAT 标签的所有 CA Datacom/AD 维护：CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.V3.0。
  - 安装包括 CA Datacom 服务器在内的所有 CA Datacom/AD 组件（从 CA CSM 安装向导中，选择“Base Install”和“USS Client for DBSRV”、FMID CAYTE02）。CA Datacom 服务器包括在 UNIX 系统服务 (USS) 下运行的 JDBC 组件。
  - 新的和空的 CA Datacom/AD MUF：您必须运行以下成员以构建 CA Datacom/AD MUF。记录您在安装期间为使用而定义的 MUF 名称。有关创建 MUF 的具体步骤，请参阅《*CA Datacom/AD Installation Guide*》中的 INSTJCL 成员主题。

    注意： 作为 CA Datacom/AD 先决条件的一部分，以下库应当经过 APF 授权：*datacomad_adthlq*.CAAXLOAD（CA Datacom/AD 加载库）和 *datacomad_adchlq*.CUSLIB（CA Datacom/AD 自定义库）。

    AXCUS00： 构建、填充和批量编辑 JCL 安装数据集。

    AXCUS01： 包括 CA Datacom/AD MUF 的所有自定义。

    AXAPFADD： 包括 CA SYSVIEW 示例以动态地将库添加到列出的 APF。

    AXRIM01： 安装 PC CALLS。

    AXNEW01： 分配并填充 MUF 需要的数据集。

    AD14STRT： 用于启动 MUF 的示例 JCL。

    AXIVP01： 示例安装验证 JOB。

    注意： 您可以共享目标运行时库，但是无法共享 MUF。

- IBM 软件—在安装 CA Chorus 的系统中必须具备以下软件：
  - IBM z/OS 1.12 或更高版本
  - 对 zFS 文件系统的 IBM z/OS UNIX 系统服务 (USS) 支持
  - IBM z/OS 系统记录器
  - IBM 64-bit SDK for z/OS、Java Technology Edition、Version 7 Release 0 Modification 0 Service Release 2 (5655-W44)，包括可选的 JZOS 批处理启动器

    注意：IBM 31-bit SDK for z/OS、Java Technology Edition 和 Version 7 Release 0 Modification 0 (5655-W43) 是在 CA Chorus 中生成批处理报告所必需的。此功能使用 CCS 的 CA Easytrieve 服务组件。
- 每个用户所需的 PC 软件：
  - Adobe Flash Player 9.0.124 或更高版本
  - 在版本 3.0 的发行版中，CA Chorus 支持 Microsoft Windows Internet Explorer 9 和 Mozilla Firefox 13 至 19。当新浏览器发布时，我们将对其进行验证并在 CA Chorus 产品页面上的“Recommended Reading”下发布兼容性。

  注意：CA Chorus 要求最低屏幕分辨率为 1024 x 768。如果您的屏幕分辨率不符合此要求，请使用全屏模式（在大多数浏览器中按 F11 键）以在显示中包括滚动条。

CA Chorus 服务器要求

CA Chorus 需要 2450 MB 的堆内存，同时要求每个管控领域满足下列其他堆要求：

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

如果您选择所有管控领域，则至少需要将 3150 MB 的实际存储分配给正在运行 CA Chorus 服务器的 LPAR。此值是默认值。

要修改堆内存大小，请参阅 *chorus_runtime_hlq*.CETJOPTN 的 ENVETJ 成员中的 Java 堆大小（Java SDK 选项）设置。对于堆范围，-Xms 是开始值，-Xmx 是结束值。

示例

具有所有管控领域的 CA Chorus 需要：2450 MB + 200 MB + 200 MB + 200 MB + 100 MB = 3150 MB。

具有存储和安全管控领域的 CA Chorus 需要：2450 MB + 200 MB + 100 MB = 2750 MB。

内存限制

z/OS 设置了内存限制，这些限制基于为作业指定的 REGION= 和 MEMLIMIT= 参数的值。但可以使用多个安装出口来覆盖这些限制，如 IEFUJV、IEFUSI、IEALIMIT、JES2 Exit 6 或 JES3 Exit IATUX03。在提出 GETMAIN 请求时，它必须满足可用限制。也就是说，必须提供满足限制条件的连续可用空间，否则请求失败。

CA Chorus 旨在以 REGION=0M（默认值）运行。IBM 定义此方案意味着“没有限制”。因此，如果 z/OS 默认值不被覆盖，则低于线、高于线但低于条以及高于条的所有内存都可供分配。其他值的 REGION 会导致低于条的内存存在限制，导致默认情况下没有高于条的内存。要在这些情况下获得高于条的内存，必须将 MEMLIMIT 指定为非零值。

安装过程中可以在 SYS1.PARMLIB 的 SMFPRMxx 成员中指定 MEMLIMIT 的默认值。如果没有指定默认值，z/OS 默认值为 MEMLIMIT(00000M)，高于条的内存将不可用，除非指定 REGION=0M（如上所述）。也可以在 JCL 的 JOB 或 EXEC 语句中指定 MEMLIMIT=nnnnnM。JCL 中的值始终覆盖 SMFPRMxx 成员中的默认值。IEFUSI 出口是可用于覆盖 MEMLIMIT 的唯一值。要找到活动的默认值，可通过输入以下控制台命令显示活动的 SMF 选项：

```
D SMF,O
```

系统要求

确认您的站点满足以下系统要求：

处理器

CA Chorus 在 z/OS 中使用 JavaVM 环境。因此，*强烈*建议您使用专业处理器以便获得最好的性能，并更好地使用资源。

磁盘

- 运行 CA Chorus 部署大约需要 11050 个柱面。
- 安装大约需要 5300 个柱面。
- 保留 Pax 安装文件的 zFS 大约需要 1500 个柱面。

  注意：安装完成后，可以删除 Pax 文件以释放空间。
- 必须能够在 DASD 上进行辅助空间分配。

注意：有关 Time Series Facility 的安装后磁盘空间建议，请参阅《*管理指南*》。

目标库

下表显示了 CA Chorus 目标库的数据集空间要求（按磁轨数）：

数据集名称	磁轨数
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

数据集名称	磁轨数
CETJPROC	10
CETJSAMP	20
CETJVSMI	1425
CETJXML	750
CETJZFS0（zFS 目录）	60000

注意：CA CSM 会创建挂接点（如果之前不存在）并自动挂接新文件系统。

分发库

下表显示了 CA Chorus 分发库的数据集空间要求（按磁轨数）：

数据集名称	磁轨数
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

数据集名称	磁轨数
AETJVSMI	1425
AETJXML	750
AETJZFS	9750
TPV.AETJHFS	14850

CA CSM 临时存储要求

在 CA CSM 安装期间，“User Settings”下指定的选项需要满足以下存储要求：

- User Unpax Temporary Directory 目录上挂载的 zFS 上大约需要 1000 个柱面。
- 为 GIMUNZIP Temporary Prefix 创建的数据集大约需要 700 个柱面。
- 为 Temporary Data Set Prefix 创建的数据集大约需要 300 个柱面。

注意：CA CSM 大约需要 2000 个柱面才能创建其临时部署文件系统，以便执行 CA Chorus 部署。有关这些设置的详细信息，请参阅 CA CSM 产品文档。

端口要求

对于 CA Chorus 的 JBoss 服务器和 Time Series Facility (TSF) 组件，需要满足以下端口需求：

- 12 个连续端口用于 CA DSI 服务器和 JBoss 服务器。JBoss 端口包括一个 DSI 双向（连接和侦听）端口以及 11 个服务器（侦听）端口。
- 三个单向端口用于 TSF。

  注意：如果正在远程 LPAR 上使用 TSF 实例，则该实例另外还需要二个单向端口。

在后面的安装过程中，在 JBoss 服务器和 TSF 配置期间配置这些端口。

要确认您打算使用的端口是否可用，请咨询您的网络管理团队。

（可选）SMTP 电子邮件要求

在位于 CA Chorus 界面内的调查器中，您可以指定电子邮件操作，以便在满足性能策略时通知您。

例如，您可以在调查器中创建策略，即当指定时间间隔内有 *x* 位用户尝试登录产品均失败时通知您。如果您已经为该产品配置了 SMTP，则在满足策略条件时可以收到电子邮件。执行此操作可以实现此类通知的自动化。

如果希望站点使用此功能，请标识以下信息。稍后配置 CA Chorus 时会使用此信息：

SMTPHOST

SMTP 邮件服务器的名称/IP 地址。

SMTPPORT

SMTP 邮件服务器的端口号（1024 到 65535）。

USS Parmlib 要求

在 z/OS parmlib 成员 BPXPRM*xx* 中，CA Chorus 需要 MAXFILEPROC(64000)。

要验证设置，请从 MVS 控制台输入以下命令：

```
D OMVS,OPTIONS
```

第 3 章： 满足安全要求

此部分包含以下主题：

安装程序安全权限

在开始安装过程*之前*，确认 CA Chorus 安装程序用户 ID 已定义以下安全权限：

- 对于 UNIX 系统服务：
  - 操纵 zFS 数据集的能力。此能力需要对 FSACCESS 类中相应实体的更新授权。
    - FSACCESS 使您可以安全访问 ZFS 文件系统容器（即数据集）。资源名称为 ZFS 文件系统名称。
    - 例如，如果您定义了名为 OMVS.ZFS.WEBSRV.TOOLS 的 ZFS 文件系统，然后创建了目录 U1 和 U2 并在其中包含文件，那么当用户尝试访问 ZFS 文件系统下目录 U1 或 U2 中的文件时，将针对 FSACCESS 类资源 OMVS.ZFS.WEBSRV.TOOLS 进行资源检查。有关详细信息，请参阅适用的安全产品文档。
  - 有效的 OMVS 定义。
  - 超级用户授权。
  - 对 FACILITY 类中下列资源的读取访问权限：
    - BPX.SUPERUSER
    - BPX.FILEATTR.APF
    - BPX.FILEATTR.PROGCTL
    - BPX.FILEATTR.SHARELIB
    - BPX.SERVER
    - UNIXPRIV 资源类中的 SUPERUSER.FILESYS.PFSCTL 配置文件

- 对于 z/OS：
  - 从 CA Chorus 安装数据集和库进行创建、更新和执行的授权。
  - 执行命令以处理外部安全管理器（CA ACF2、CA Top Secret 或 IBM RACF）数据库的授权。

在 CA Chorus 配置过程期间定义必须通过外部安全产品执行的 APF 授权和其他安全要求，如《*安装指南*》中所述。由于您需要访问安装程序包中的各个作业和成员，因此需在安装期间完成这些任务。

运行 CA Chorus 安全作业

ETJI095*x* 安全作业可简化您满足诸多安全要求的方式。安全作业标识为如下格式：ETJI095*x*，x 等于 A 时表示 CA ACF2，等于 T 时表示 CA Top Secret，等于 R 时表示 IBM RACF。这些作业位于 CA Chorus 产品页面上。

以下列表详细介绍了作业需要满足的安全要求。

重要提示！ 在您继续执行*本主题末尾*的几个步骤前，请先查看以下概念材料。

（仅 CA Top Secret）主工具

如果您使用的是 CA Top Secret，请定义主工具并将其与 CA Chorus 启动任务关联。将 CAWEBSVR 用作主工具。通过主工具（MASTFAC 关键字），用户可以访问 CAWEBSVR 工具。在工具可用作主工具之前，必须将该工具作为系统工具矩阵中的用户工具定义到 CA Top Secret 中。

重要提示！ 只需执行此任务一次。如果您已将 CAWEBSVR 添加到工具矩阵中且已激活定义，则不重复执行此任务。

然后向 CA Top Secret 工具 CAWEBSVR 授予权限，以便每个用户 ACID 都可以访问 CA Chorus。

管理员用户 ID 和组 ID

使用已定义 UNIX 系统服务 (USS) 段的用户 ID（默认情况下为 CHORADM）运行 CA Chorus，以便满足以下条件：

- 用户 ID 具有一个*非* UID(0) 的有效 UID。
- shell 指定为默认 shell，通常为 /bin/sh。
- 用户 ID 具有一个有效的 OMVS 组。

注意：建议主目录与 CA Chorus 安装路径相同。

运行 ETJI095*x* 作业时，创建了以下安全用户 ID。如果不使用默认值，则更改安全作业中 CHORADM 和 CHORGRP 的所有匹配项。

CHORADM

用于运行 CA Chorus 的启动任务用户 ID。

CHORGRP

默认组名称。此组可创建所有相关安全对象间的关系。

CHORTHD

与应用程序相关的 PassTicket 请求的用户 ID。

注意：唯一 USS UID 和 GID（用户 ID 和组 ID）必须用于 CA Chorus 启动任务用户 ID。选择数值上匹配的 UID 和 GID 以方便跟踪。

重要提示！ 所有用户（包括安装员）必须具有该成员中指定的组的访问权限。默认组为 CHORGRP。

启动任务

运行 ETJI095*x* 作业时，定义了以下启动任务。显示默认值。如果不要对启动任务使用默认名称，则在安全作业中更改名称。

注意：我们建议所有 CA Chorus 任务都作为带有 REGION=0M 的启动任务运行。如果您的站点限制了 REGION=0M 参数，我们建议您使用允许的最大区域大小运行。

your_muf_name

与 CA Datacom/AD MUF for CA Chorus 关联的启动任务名称。此名称取决于先前分配给 MUF 的名称。

CHORTSF

与 Time Series Facility (TSF) 关联的启动任务名称。

CHORTSFR

与远程 TSF 配置关联的启动任务名称。只有在定义了 TSF 数据中继后，才可以创建该启动任务。

CHORJBOS

与 JBoss 服务器关联的启动任务名称。

资源类

CA Chorus 在使用安全产品定义的 CAMFC 类中定义安全资源。然后根据需要将用户权限分配给特定于管控领域的资源。有关所需用户权限的详细信息，请参阅特定于管控领域的安装指南。

一般用户的 PassTicket

用户要访问 CA Chorus 及其支持的管控领域所使用的 z/OS 组件和产品，需要具有 PassTicket。*PassTicket* 是临时编码并加密的用户密码替代项，可用于访问特定应用程序。PassTicket 必须在生成之后的 10 分钟内使用。

使用 PassTicket 使 z/OS 组件和产品能够验证用户 ID，而无需通过网络发送 z/OS 密码。相反，在用户使用有效的 z/OS 用户 ID 和密码初次登录之后验证用户。当用户选择用于访问 z/OS 组件的功能时，将发生以下过程：

- CA Chorus Web 服务调用 z/OS 安全产品，以生成用于访问授权的 PassTicket。
- PassTicket 随用户请求一起发送给组件，该组件可能位于不同的 z/OS 系统。

  在处理请求之前，组件调用 z/OS 安全产品，以使用 PassTicket 作为密码替代项来验证用户。

CA Chorus 服务器会生成 PassTicket，它们允许用户访问 CA Chorus 管控领域使用的各种后端产品。当用户访问组件时，将生成 PassTicket 以验证请求。

CA Chorus PassTicket 配置包括以下系统：

- 运行 JBoss 服务器和同一系统中的 CA Chorus 管控领域所需的后端产品（如 CA Detector、CA Compliance Manager、CA Vantage SRM 和 CA NetMaster NM for TCP/IP）的 z/OS 系统。此类型的系统是 CA Chorus 服务器系统。
- 只运行 CA Chorus 管控领域所需的产品和组件的其他 z/OS 系统。此类型的系统称为 CA Chorus 远程系统。

CA Chorus 服务器系统可为 CA Chorus 用户提供入口点。然后，用户可以访问已授权其在 z/OS 系统的网络中使用的所有 CA Chorus 远程系统。

必须在承载 CA Chorus 所用组件的每个 z/OS 系统上进行安全产品的 PassTicket 配置。在 z/OS 安全产品中配置 PassTicket，以允许生成和验证 CA Chorus 管控领域所需的连接。如果站点满足以下条件，则无需在远程系统上执行其他安全设置：

- z/OS 配置中的安全产品正在使用共享安全数据库。
- 您要添加一个或多个远程系统，只需进行 CA Chorus 服务器系统设置。

如果必需产品和组件存在于不共享安全数据库的远程系统中，则需在远程系统中进行其他安全设置。

CA CSM 用户的 PassTicket

CA Chorus 使用 PassTicket 安全来允许用户从快速链接模块启动 CA CSM，而无需其他用户登录。使用 Passticket 的所有系统对于网络中的所有节点必须具有相同的应用程序名称和会话密钥。注意以下要求：

- 如果 CA Chorus 实例和 CA CSM 实例位于*不同*计算机上，则在运行此作业后，完成“如何为 CA Chorus 配置 CA CSM Passticket (p. 48)”中的适用步骤。
- 如果 CA Chorus 实例和 CA CSM 实例位于*相同*计算机上，则在运行此作业后，CA CSM passticket 配置会完成，但有一个异常。如果使用的是 CA ACF2，则完成“示例：使用 CA ACF2 将 PassTicket 配置为从 CA Chorus 连接到 CA CSM (p. 49)”中的 CA Chorus 服务器端和 CA CSM 端步骤。

遵循这些步骤:

1. 检索适用于外部安全管理器的 ETJI095*x* 作业。这些作业位于 CA Chorus 产品页面上。
2. 全面查看成员 ETJI095*x*。
3. 根据成员注释编辑作业。
4. 提交该成员。

   满足指明的安全要求。
5. （仅 CA Top Secret）将以下行添加到适用的 CA Top Secret 参数文件 (PARMFILE) 中：

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

   xx

   用户工具编号。请使用您系统上的任一可用的用户工具编号。

更多信息：

安全注意事项 (p. 14)
安全 ID 重复使用注意事项 (p. 18)

如何授权用户在 CA Chorus 中工作

安全管理员管理针对产品的所有用户访问请求。对于 CA Chorus，安全管理员必须执行以下任务：

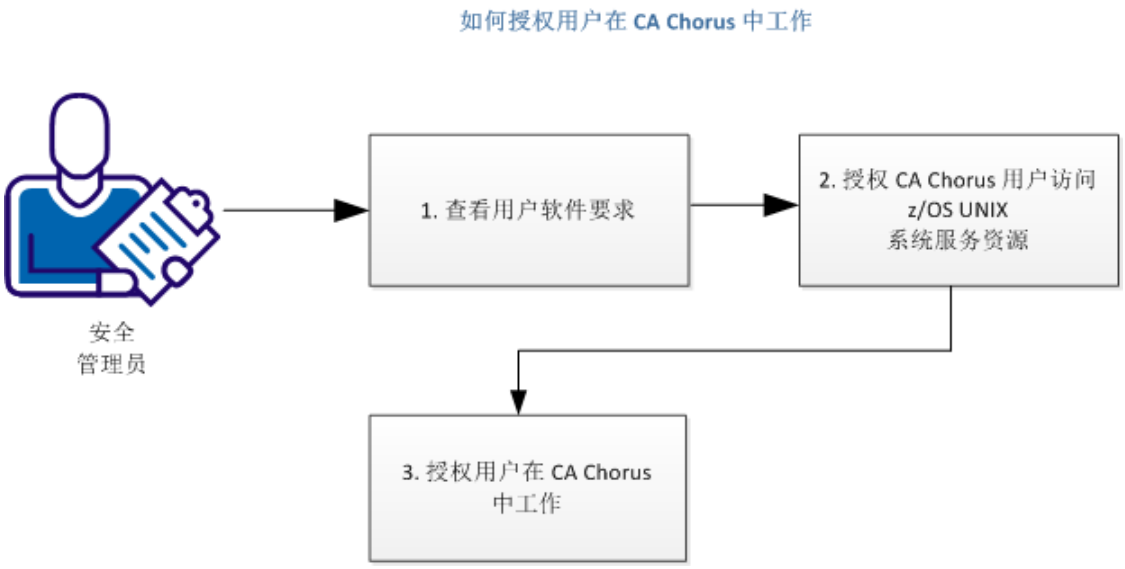
- 授权并确认每个用户 UNIX 系统服务 (USS) 环境。
- 授权用户在 CA Chorus 及其支持的管控领域中工作。

注意：CA Chorus 在 CAMFC 类中定义安全资源。您可以删除 CAMFC 资源类和用户访问权限，以限制访问并阻止特定用户登录产品。

要执行这些授权，安全管理员需使用 CA ACF2、CA Top Secret 或 IBM RACF。

下图介绍授权用户在 CA Chorus 及其支持的管控领域中工作需要完成的任务：

注意：您可以按任意顺序完成任务，但是建议您按此图中显示的顺序执行任务。



完成以下任务，以授权用户在 CA Chorus 中工作：

1. 查看用户软件要求。 (p. 38)
2. 授权 CA Chorus 用户访问 z/OS UNIX 系统服务资源。 (p. 38)
3. 授权用户在 CA Chorus 中工作。 (p. 40)

查看用户软件要求

- 每个用户所需的 PC 软件：
  - Adobe Flash Player 9.0.124 或更高版本
  - 在版本 3.0 的发行版中，CA Chorus 支持 Microsoft Windows Internet Explorer 9 和 Mozilla Firefox 13 至 19。当新浏览器发布时，我们将对其进行验证并在 CA Chorus 产品页面上的“Recommended Reading”下发布兼容性。

注意：CA Chorus 要求最低屏幕分辨率为 1024 x 768。如果您的屏幕分辨率不符合此要求，请使用全屏模式（在大多数浏览器中按 F11 键）以在显示中包括滚动条。

授权 CA Chorus 用户访问 USS 资源

CA Chorus 组件和管控领域使用 z/OS TCP/IP 通信服务和 z/OS UNIX 系统服务 (USS)。同时为每个用户定义 OMVS 段，以便他们在 CA Chorus 中工作时可以访问 z/OS USS 资源。使用 CA ACF2、CA Top Secret 或 IBM RACF 可启用此访问权限。

要授权 CA Chorus 用户访问 z/OS USS 资源，请为每个用户定义包含以下选项的 OMVS 段：

- 默认 shell 程序指定值（PROGRAM 或 OMVSPGM）
- 数字型 z/OS USS 用户 ID (UID)

  注意：您的站点上可能存在用于分配 OMVS UID 编号的策略。如果不存在，则使用唯一编号。
- 数字型 z/OS USS 组 ID (GID)

遵循这些步骤:

1. 确认用户是否可以访问 OMVS 段：

   - CA ACF2：

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

   - CA Top Secret：

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

   - IBM RACF：

     ```
     LISTUSER userid OMVS NORACF
     ```

   如果用户不具有此访问权限，则转到下一步。

2. 创建与每个用户 ID (UID) 关联的主目录。

   例如，要为 UID*nnn* 设置名为 /u/name 的目录，请在 OMVS UNIX shell 中发出以下命令：

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

3. 确认所有者和目录访问权限：

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

   显示以下示例结果：

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

   粗体区域显示存在正确的所有者和读取/写入访问权限。

4. 使用安全产品定义 OMVS 段：

   注意：执行这些命令前，必须存在有效的组记录。

   - 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)
     ```

以下语法变量适用于所有这三个安全产品：

userid

标识用户 ID。

path_name

标识与每个用户 ID 关联的主目录。

uid

标识用户标识 (UID) 号。

ggggg

标识 OMVS 组。

5. 确认 OMVS 段的内容。

   - CA ACF2：

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

   - CA Top Secret：

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

   - IBM RACF：

     ```
     LISTUSER userid OMVS NORACF
     ```

用户现在具有定义的 OMVS 段并且可以访问 USS，这是用户在 CA Chorus 中工作所必需的。

授权用户在 CA Chorus 中工作

您可以添加或删除对 CA Chorus 支持的管控领域的访问权限。这些权限确保用户可以访问他们需要的管控领域和功能。CA Chorus 会为所有所需权限使用 CHORUS 的资源名称高级限定符。CA Chorus 检查用户是否对适用资源具有读取访问权限。此外，您可以修改管理知识中心内容和使用自动刷新选项的权限。要执行此操作，请根据 CA ACF2、CA Top Secret 或 IBM RACF 中的功能，授权用户在 CA Chorus 中工作。

- 使用 CA ACF2 授权用户 (p. 41)
- 使用 CA Top Secret 授权用户 (p. 43)
- 使用 IBM RACF 授权用户 (p. 45)

注意：知识中心是 CA Chorus 中所有文档的存储库。知识中心内容可以包括 CA 产品文档、用户生成的文档、Chicago-Soft MVS/Quick-Ref、网站以及与第三方文档的链接。

示例：使用 CA ACF2 授权用户

使用此过程可标识能够登录 CA Chorus 并使用特定管控领域的用户。此外，您可以授权用户执行以下任务：

- 为知识中心内容建立索引。通过为内容建立索引，用户可向此存储库添加文档或从中删除文档。
- 使用自动刷新选项。每当后端数据更改时，此选项就会刷新 CA Chorus UI 中显示的数据。

注意：此过程中的命令用作示例。有关使用这些命令的详细信息，请参阅 *《CA ACF2 管理指南》*。

要定义用户访问权限，请输入以下命令：

```
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

标识允许用户访问的 CA Chorus 资源。

ROLE.DB2DBA

控制对 CA Chorus for DB2 Database Management 功能的访问。CA Chorus Infrastructure Management for Networks and Systems 提供 CA Insight 数据，但是该管控领域不需要此资源。

ROLE.INFRASTRUCTURE

控制对 CA Chorus Infrastructure Management for Networks and Systems 功能的访问。

ROLE.SECURITY

控制对 CA Chorus for Security and Compliance Management 功能的访问（UI 和批处理）。

ROLE.SDK*instance*

控制对 SDK 的访问。CA Chorus 可以支持多个 SDK。与系统管理员和应用程序开发人员合作，以定义和共享此名称。建议应用程序开发人员使用此名称来构建支持 SDK 所必需的文件。有关更多详细信息，请参阅《*软件开发包用户指南*》。

实例

为 SDK 标识此资源的字母数字字符串。

ROLE.STORAGE

控制对 CA Chorus for Storage Management 功能的访问。

SETTINGS.KNOWLEDGECENTER

指示用户可以为知识中心内容建立索引。

SETTINGS.AUTOREFRESH

指示用户可以使用自动刷新选项。

uid-of-userid1*、*uid_of_userid2...uid_of_useridn

标识请求访问的 CA Chorus 用户的 UID。

READ

指示用户具有读取访问权限。

用户可以访问指定资源，也可以登录 CA Chorus 并在其中工作。

示例

下列命令授予用户 ABC1 以下能力：

- 登录到 CA Chorus。
- 使用 CA Chorus for DB2 Database Management 的功能。
- 修改知识中心的文档。
- 使用自动刷新选项。

```
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)
```

示例：使用 CA Top Secret 授权用户

使用此过程可标识能够登录 CA Chorus 的用户。此外，您可以授权用户执行以下任务：

- 为知识中心内容建立索引。通过为内容建立索引，用户可向此存储库添加文档或从中删除文档。
- 使用自动刷新选项。每当后端数据更改时，此选项就会刷新 CA Chorus UI 中显示的数据。

注意：此过程中的命令用作示例。有关使用这些命令的详细信息，请参阅《*CA Top Secret Command Functions Guide*》和《*CA Top Secret Control Options Guide*》。

设置用户授权时，请考虑以下几点：

- 单个级别超过 8 字节的较长实体名称不适合使用星号掩码。建议使用浮点掩码。
- 由于您可以影响多个调用，而不仅仅是管控领域登录本身，因此在使用前缀权限时请注意。

要定义用户访问权限，请输入以下命令：

```
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

标识允许用户访问的 CA Chorus 资源。

CHORUS.ROLE.DB2DBA

控制对 CA Chorus for DB2 Database Management 功能的访问。CA Chorus Infrastructure Management for Networks and Systems 提供 CA Insight 数据，但是该管控领域不需要此资源。

CHORUS.ROLE.INFRASTRUCTURE

控制对 CA Chorus Infrastructure Management for Networks and Systems 功能的访问。

CHORUS.ROLE.SECURITY

控制对 CA Chorus for Security and Compliance Management 功能的访问（UI 和批处理）。

CHORUS.ROLE.STORAGE

控制对 CA Chorus for Storage Management 功能的访问。

CHORUS.ROLE.SDK*instance*

控制对 SDK 的访问。CA Chorus 可以支持多个 SDK。与系统管理员和应用程序开发人员合作，以定义和共享此名称。建议应用程序开发人员使用此名称来构建支持 SDK 所必需的文件。有关更多详细信息，请参阅《*软件开发包用户指南*》。

实例

为 SDK 标识此资源的字母数字字符串。

重要提示！ 为 SDK 实例使用*唯*一名称。请注意类似名称的 SDK 实例，因为您可能会错误地应用权限。例如，CHORUS.ROLE.SDKROLE1 和 CHORUS.ROLE.SDKROLE123 可能会具有相同的权限。因为相同的屏蔽限制同时适用于字母和数字。

CHORUS.SETTINGS.KNOWLEDGECENTER

指示用户可以为知识中心内容建立索引。

CHORUS.SETTINGS.AUTOREFRESH

指示用户可以使用自动刷新选项。

acid1*、*acid2...acidn

标识请求访问的 CA Chorus 用户的 ACID。ACID 可以是用户或配置文件。

READ

指示用户具有读取访问权限。

用户可以访问指定资源，也可以登录 CA Chorus 并在其中工作。

示例

下列命令授予用户 ABC1 以下能力：

- 登录到 CA Chorus。
- 使用 CA Chorus for DB2 Database Management 的功能。
- 修改知识中心的文档。
- 使用自动刷新选项。

```
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)
```

示例：使用 IBM RACF 授权用户

使用此过程可标识能够登录 CA Chorus 的用户。此外，您可以授权用户执行以下任务：

- 为知识中心内容建立索引。通过为内容建立索引，用户可向此存储库添加文档或从中删除文档。
- 使用自动刷新选项。每当后端数据更改时，此选项就会刷新 CA Chorus UI 中显示的数据。

注意：以下命令用作示例。有关使用这些命令的详细信息，请参阅 IBM RACF 产品文档。

遵循这些步骤:

1. 将每个管控领域资源添加到 CAMFC 中：

   注意：对于基于功能的资源（例如，自动刷新），不需要此步骤。您只需要执行此步骤一次。如果您已向 CAMFC 定义该资源，请转到步骤 2。

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

   discipline

   DB2DBA

   INFRASTRUCTURE

   SECURITY

   STORAGE

   注意：有关每个管控领域资源的详细解释，请参阅步骤 2。

   将向 CAMFC 分配适用的管控领域资源。现在您可以授予用户访问管控领域的权限。

2. 通过输入以下命令允许用户访问特定资源：

   ```
   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

   标识允许用户访问的 CA Chorus 资源。

   CHORUS.ROLE.DB2DBA

   控制对 CA Chorus for DB2 Database Management 功能的访问。CA Chorus Infrastructure Management for Networks and Systems 提供 CA Insight 数据，但是该管控领域不需要此资源。

   CHORUS.ROLE.INFRASTRUCTURE

   控制对 CA Chorus Infrastructure Management for Networks and Systems 功能的访问。

   CHORUS.ROLE.SECURITY

   控制对 CA Chorus for Security and Compliance Management 功能的访问（UI 和批处理）。

CHORUS.ROLE.STORAGE

控制对 CA Chorus for Storage Management 功能的访问。

CHORUS.ROLE.SDK*instance*

控制对 SDK 角色的访问。CA Chorus 可以支持多个 SDK。与系统管理员和应用程序开发人员合作，以定义和共享此名称。建议应用程序开发人员使用此名称来构建支持 SDK 所必需的文件。有关更多详细信息，请参阅《*软件开发包用户指南*》。

实例

为 SDK 标识此资源的字母数字字符串。

CHORUS.SETTINGS.KNOWLEDGECENTER

指示用户可以为知识中心内容建立索引。

CHORUS.SETTINGS.AUTOREFRESH

指示用户可以使用自动刷新选项。

uid-of-userid1*、*uid_of_userid2...uid_of_useridn

标识请求访问的 CA Chorus 用户的 UID。

READ

指示用户具有读取访问权限。

3. 激活对 CAMFC 资源所做的更改：

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

更改已激活。

用户可以访问指定资源，也可以登录 CA Chorus 并在其中工作。

示例

下列命令授予用户 ABC1 以下能力：

- 登录到 CA Chorus。
- 使用 CA Chorus for Security and Compliance Management 的功能。
- 修改知识中心的文档。
- 使用自动刷新选项。

```
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
```

（可选）如何为 CA Chorus 配置 CA CSM Passticket

CA Chorus 使用 PassTicket 安全来允许用户从快速链接模块启动 CA CSM，而无需其他用户登录。使用 Passticket 的所有系统对于网络中的所有节点必须具有相同的应用程序名称和会话密钥。

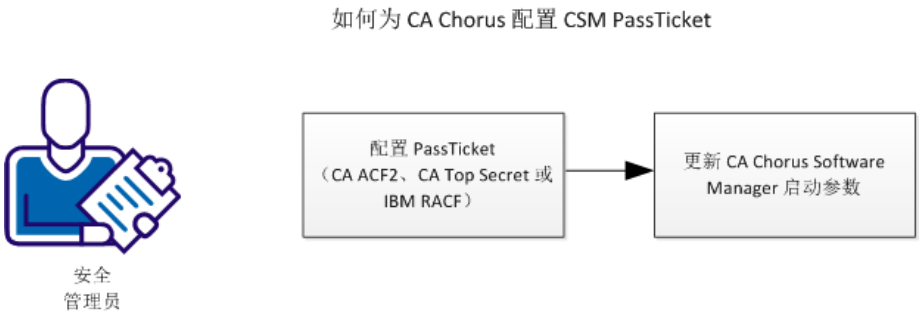
此方案显示了安全管理员和系统管理员如何将 PassTicket 配置为允许用户使用 CA CSM，而无需其他用户登录。

重要提示！ 此方案中的过程假定您已运行 ETJI095*x* 安全作业。如果您尚未运行，请先完成此步骤。

PassTicket 是临时编码并加密的用户密码替代项，可用于访问特定应用程序。PassTicket 必须在生成之后的几分钟内使用。使用 PassTicket 使 z/OS 组件和产品能够验证用户 ID，而无需通过网络发送 z/OS 密码。相反，在用户使用有效的 z/OS 用户 ID 和密码初次登录之后验证用户。当用户选择用于访问 z/OS 组件的功能时，将发生以下过程：

- CA Chorus Web 服务调用 z/OS 安全产品，以生成用于访问授权的 PassTicket。
- PassTicket 随用户请求一起发送给组件，该组件可能位于不同的 z/OS 系统。
- 在处理请求之前，组件调用 z/OS 安全产品，以使用 PassTicket 作为密码替代项来验证用户。

注意：提供了使用 CA ACF2、CA Top Secret 和 IBM RACF 将 PassTicket 配置为连接到 CA CSM 的示例。这些示例作为准则提供。有关使用 CA ACF2 命令的详细信息，请参阅《*CA ACF2 管理指南*》。有关使用 CA Top Secret 的详细信息，请参阅《*CA Top Secret Command Functions Guide*》。有关使用 IBM RACF 的详细信息，请参阅 IBM 文档。



要从 CA Chorus 启动并使用 CA CSM，请完成以下任务：

1. 将安全系统配置为使用 PassTicket。选择以下选项之一：
   - 使用 CA ACF2 将 PassTicket 配置为从 CA Chorus 连接到 CA CSM (p. 49)
   - 使用 CA Top Secret 将 PassTicket 配置为从 CA Chorus 连接到 CA CSM (p. 51)
   - 使用 IBM RACF 将 PassTicket 配置为从 CA Chorus 连接到 CA CSM (p. 52)
2. 更新 CA CSM 启动参数 (p. 55)。

重要提示！ 确认您使用的 CA CSM applid 与 CA Chorus 中使用的相同。

示例：使用 CA ACF2 将 PassTicket 配置为从 CA Chorus 连接到 CA CSM

此示例显示了安全管理员在运行 ETJI095*x* 安全作业之后，如何将 PassTicket 配置为从 CA Chorus 连接到 CA CSM。

注意：此过程中的命令用作示例。有关使用这些命令的详细信息，请参阅 *《CA ACF2 for z/OS 管理指南》*。

此过程要求您在 CA Chorus 服务器和 CA CSM 服务器上设置安全。以下过程突出显示您工作的位置，以及您将焦点转移到新服务器上的时间。请注意适用于这两个服务器的以下定义：

applid

定义用于 CA Chorus 快速链接模块的 PassTicket 验证的应用程序 ID。将 *applid* 替换为 CA CSM applid。有关 CA CSM 配置详细信息，请参阅“更新 CA CSM 启动参数 (p. 55)”。

默认：CSMAPPLM

MULT-USE

允许您多次重用同一 PassTicket。

SSKEY

采用 16 个随机十六进制数字（不同于示例中显示的值）的格式为应用程序定义加密密钥。

注意：示例演示了 16 个十六进制数字组成的完整密钥 SESSKEY 值（创建一个 8 字节或 64 位密钥）。每个应用程序密钥在配置中的所有系统上都必须相同，并且值必须保密且安全。

CA Chorus 服务器端步骤

1. 允许各个用户访问 CA CSM：

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

chorus_userid

需要通过快速链接模块访问 CA CSM 的用户。

将在 CA Chorus 服务器端配置 PassTicket。

（可选）CA CSM 服务器端步骤

注意：如果您插入 GSO CLASMAP 记录来将 APPL 类的类型代码更改为 APL，请在以下命令中针对 TYPE 使用 APL 而不是 SAF。

重要提示！如果 CA Chorus 和 CA CSM 位于不同计算机上，则必需执行步骤 1 和 2。步骤 3 在所有情况下都必需执行。

1. 定义 CA CSM 连接应用程序会话密钥：

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

2. 允许 CA CSM 启动任务用户 ID 代表 CA CSM 用户生成并评估 PassTicket：

```
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

指定 CA CSM 应用程序服务器启动任务用户 ID。此 ID 必须能够为任何用户生成 PassTicket。

默认：MSMSERV

3. 允许各个用户访问 CA CSM：

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

将在 CA CSM 服务器端配置 PassTicket。

要完成 PassTicket 设置，请转至“更新 CA CSM 启动参数 (p. 55)”。

示例：使用 CA Top Secret 将 PassTicket 配置为从 CA Chorus 连接到 CA CSM

此示例显示了安全管理员在运行 ETJI095*x* 安全作业之后，如何将 PassTicket 配置为从 CA Chorus 连接到 CA CSM。

注意：此过程假定已定义 PTKTDATA 类和 IRRPTAUTH 资源所有权。

此过程要求您在 CA Chorus 服务器和 CA CSM 服务器上设置安全。以下过程突出显示您工作的位置，以及您将焦点转移到新服务器上的时间。请注意适用于这两个服务器的以下定义：

applid

定义用于 CA Chorus 快速链接模块的 PassTicket 验证的应用程序 ID。将 *applid* 替换为 CA CSM applid。有关 CA CSM 配置详细信息，请参阅“更新 CA CSM 启动参数 (p. 55)”。

默认：CSMAPPLM

department

标识先前存在的部门。该应用程序将定义到此部门。此所有权允许部门管理员（或更高级别的人员）为 PassTicket 生成和验证定义权限。

SESSKEY

采用 16 个随机十六进制数字（不同于示例中显示的值）的格式为应用程序定义加密密钥。

注意：示例演示了 16 个十六进制数字组成的完整密钥 SESSKEY 值（创建一个 8 字节或 64 位密钥）。每个应用程序密钥在配置中的所有系统上都必须相同，并且值必须保密且安全。

SIGNMULTI

允许您多次重复使用同一 PassTicket。

CA Chorus 服务器端步骤

运行 ETJI095*x* 作业时，为此服务器配置 passticket。

（可选）CA CSM 服务器端步骤

重要提示！ 如果 CA Chorus 和 CA CSM 位于不同计算机上，请完成以下过程。

1. 定义 CA CSM 连接应用程序会话密钥：

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

2. 允许 CA CSM 启动任务用户 ID 代表 CA CSM 用户生成并评估 PassTicket：

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

   csm_stc_userid

   指定 CA CSM 应用程序服务器启动任务用户 ID。此 ID 必须能够为任何用户生成 PassTicket。

3. 将 applid 添加到适当的部门：

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

4. 允许各个用户访问 CA CSM：

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

   将在 CA CSM 服务器端配置 PassTicket。

   要完成 PassTicket 设置，请转至“更新 CA CSM 启动参数 (p. 55)”。

示例：使用 IBM RACF 将 PassTicket 配置为从 CA Chorus 连接到 CA CSM

此示例显示了安全管理员在运行 ETJI095*x* 安全作业之后，如何将 PassTicket 配置为从 CA Chorus 连接到 CA CSM。

注意：在开始此过程之前，请验证是否已定义 PassTicket 资源 (IRRPTAUTH) 的 PTKTDATA 类和所有权。

此过程要求您在 CA Chorus 服务器和 CA CSM 服务器上设置安全。以下过程突出显示您工作的位置，以及您将焦点转移到新服务器上的时间。请注意适用于这两个服务器的以下定义：

applid

定义用于 CA Chorus 快速链接模块的 PassTicket 验证的应用程序 ID。将 *applid* 替换为 CA CSM applid。有关 CA CSM 配置详细信息，请参阅“更新 CA CSM 启动参数 (p. 55)”。

默认：CSMAPPLM

KEYMASKED

使用与示例语法中不同的值定义应用程序的加密密钥。

注意：示例语法演示了 16 个十六进制数字组成的完整密钥值（创建 8 字节或 64 位密钥）。每个应用程序密钥在配置中的所有系统上都必须相同，并且值必须保密且安全。

APPLDATA(‘NO REPLAY PROTECTION’)

允许您多次使用同一 PassTicket。

CA Chorus 服务器端步骤

运行 ETJI095*x* 作业时，为此服务器配置 passticket。

（可选）CA CSM 服务器端步骤

重要提示！ 如果 CA Chorus 和 CA CSM 位于不同计算机上，请完成以下过程。

1. 定义 CA CSM 连接应用程序会话密钥：

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

2. 允许 CA CSM 启动任务用户 ID 代表 CA CSM 用户生成并评估 PassTicket：

```
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

   指定 CA CSM 应用程序服务器启动任务用户 ID。此 ID 必须能够为任何用户生成 PassTicket。

   默认： MSMSERV

3. 允许各个用户访问 CA CSM：

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

4. 刷新 PTKTDATA 类并激活 APPL 类：

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

   将在 CA CSM 服务器端配置 PassTicket。

   要完成 PassTicket 设置，请转至“更新 CA CSM 启动参数 (p. 55)”。

更新 CA CSM 启动参数

此过程显示了系统管理员如何以创建的 CA CSM 应用程序 ID 来启动 CA CSM 应用程序服务器。

遵循这些步骤:

1. 在 SAMPLIB(MSMLIB) 成员中添加以下语句以指定 CA CSM 应用程序 ID：

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

   applid

   定义用于 PassTicket 验证的 CA CSM 应用程序 ID，以验证与服务器的连接。

   默认： CSMAPPLM

2. 重新启动 CA CSM 应用程序服务器。

   这些更改将生效。

用户现在可以从快速链接模块访问 CA CSM。