

Users **Centralized** Management

Gestión centralizada para SecureEntry

Antes de empezar	4
Derechos de copia	4
Información general	4
Tipos de instalación de UCM	5
Requerimientos de Software	8
Host	9
Estación de administración de UCM/Estación UCM	9
Oficinas	9
Instalando UCM	10
Plataforma MVS/ESA	10
Configurando el APPC/MVS	11
Creando la Base de Datos UCM	12
Inicializando la Base de Datos UCM	13
Instalando los programas UCM	13
Planificando la distribución	16
Configurando la característica DDF del DB2 para MVS/ESA	17
Configurando Communications Manager/2	17
Configurando el DB2 DDCCS/2 en la estación de UCM	26
Vinculando las funciones de UCM (API)	27
Vinculando la aplicación de consulta de oficinas	29
Vinculando la Herramienta de Recuperación UCM	30
Instalando el emulador de RACF	31
Instalando EDYURACF	31
Migrando desde versiones previas de UCM	34
Plataforma OS/2	35
Prerequisitos de UCM en OS/2	36
Guía rápida de instalación de UCM en OS/2	36
Creando la Base de Datos de UCM	38
Configurando Communications Manager/2	38
Vinculando los programas UCM	47
Inicializando la Base de Datos UCM	47
Planificando la distribución	48
Software adicional de UCM	49
Procesos UCM (Gestión Centralizada de Usuarios)	51
Procesos Online	51
Aplicaciones transaccionales de UCM	52
Aplicación de consulta de oficinas	57
Herramienta de recuperación UCM	58
Procesos desasistidos	59
UCMPCUSF	60
UCMP01	61
UCMP02	62
UCMP03	63
EDYEXLOG	64
EDYQUERY	66
EDYUCDIS	67
EDYUCSRT	68
Transacciones multi-trans	69
Configuración multi-trans	70
Formato del archivo de cliente	71
Información requerida para la palabra clave (keyword) de subsistema	72

UCM	72
SecureEntry	72
Guía de determinación de problemas UCM	74
Mensajes NETBIOS	75
Mensajes EDYSRV	76
Mensajes EDYFREE	78
Apéndice	79
Tabla de traducción ASCII/EBCDIC	79
Archivo UCMLOG. Información, problemas de ejecución y estadísticas	80
¿Cómo puedo mejorar el rendimiento de UCM?	81
NOVEDADES !!	83

Antes de empezar

Antes de instalar UCM, debería vd. leer detalladamente este manual de referencia para asegurarse que comprende la filosofía del producto, así como de que dispone del hardware y software apropiado y prerequisite para el mismo. Así mismo, vd. debería haber leído y comprendido previamente el manual de referencia de SecureEntry/2 donde se detallan las funcionalidades principales del producto.

Además de este manual, sírvase leer el documento *README.DOC* que encontrará en el primer diskette de instalación de SecureEntry/2. En él encontrará descritos los cambios de última hora.

Derechos de Copia

Información general

Tipos de Instalación de UCM

Requerimientos de Software

Derechos de copia

IBM for SecureEntry/UCM Version 4RX
5793-R46 (C) Copyright IBM Corp. 1996-1999
All Rights reserved. US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP
Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM.

Información general

UCM (Gestión Centralizada de Usuarios) es una extensión a SecureEntry que permite la gestión centralizada de los usuarios, grupos y recursos de red, con una única vista lógica de todas las sucursales (oficinas) SecureEntry. Esto se consigue mediante el almacenamiento de toda esta información en el ordenador central de la corporación (Host), de tal manera que cada oficina se convierte efectivamente en una imagen parcial de este repositorio central de datos.

Cuando un usuario UCM se conecta a una de las máquinas administradas por UCM, sus perfiles de seguridad son descargados desde el Host a la red local y dados de alta, si el usuario es desconocido, o modificados si estos han cambiado desde la última vez que el usuario se identificó en conexión. Una vez que se han descargado los perfiles de seguridad correctos (los últimos), estos son activados por SecureEntry para el usuario en su sesión de trabajo.

Como beneficio adicional, UCM aumenta la funcionalidad de SecureEntry con evidentes ventajas de movilidad para los usuarios de la corporación, ya que cualquier usuario podrá conectarse en cualquier máquina de la corporación sin necesidad de registro previo para esa máquina o red local.

Remítase al Manual de administración SecureEntry para obtener más información sobre SecureEntry.

Este manual describe el funcionamiento de UCM. Incluye el proceso de instalación, los procedimientos ejecutables que lo componen, la especificación del formato del archivo de cliente para la carga de la Base de

Datos y una guía de problemas donde se especifican los posibles mensajes y códigos de retorno que pueden aparecer durante la ejecución de los procesos que integran UCM.

*** **NOTA** ***

En los ejemplos de este manual encontrará referencias a datasets con la siguiente nomenclatura:

UCM.Vxxx.

Donde Vxxx identifica la versión actual de UCM.

*** **NOTA** ***

Si usted no ha contratado la solución UCM, entonces la única parte de este documento que le puede resultar de alguna utilidad es la guía de problemas y códigos de retorno, especialmente la que describe los códigos de retorno de NETBIOS para los procesos EDYSRV/EDYFREE. Esto es debido a que estos procesos son una pieza común en para las instalaciones en red local (LAN).

*** **NOTA** ***

En la explicación de cada proceso UCM, vd. encontrará una tabla que indica en qué Sistemas Operativos puede ser ejecutado.

Manual de administración de UCM. Listado de cambios incorporados a la documentación:

(14/02/2000) UCM V4R3. Transacciones seguras a RACF (EDYURACF).

(15/11/1999) UCM V4R3. UCMLLOG y Caché de refresco dinámico de datos.

(18/08/1999) UCM V4R3. Versión OS/2.

(19/06/1999) UCM V4R3. APPC, Transacciones multi-trans.

(28/04/1999) UCM V4R3. Emulación de RACF y Transacciones multi-trans.

Tipos de instalación de UCM

Users Centralized Management (UCM) es una extensión de SecureEntry/2 que vd. puede utilizar para administrar la definición de los usuarios de su corporación de una forma centralizada. UCM está disponible tanto para entornos MVS/ESA (OS/390) como para entornos OS/2. A continuación se exponen una lista con las principales funcionalidades de esta solución:

1. Autenticación centralizada de los usuarios

Al instalar UCM, la autenticación de los usuarios SecureEntry/2 debe ser gestionada de forma centralizada. El subsistema de seguridad principal que vd. puede configurar para autenticar a los usuarios de sus oficinas puede ser uno de los siguientes:

RACF (Resource Access Control Facility) (*disponible en MVS*)

Subsistema de seguridad principal instalado en su corporación (RACF, TOP SECRET, ACF/2...). El acceso a este subsistema puede realizarse de dos formas diferentes:

DIRECTO

Acceso a través de un Service TP del SNA. A menos que vd. tenga la encriptación SNA instalada, este modo permite el acceso no autorizado por terceras partes (pinchando la línea) a la información.

CIFRADO (EDYURACF)

Vd. puede utilizar la funcionalidad de cifrado de UCM para enviar cifrados, a RACF, los datos de los usuarios a través del canal de comunicaciones. En este caso, SecureEntry accede a RACF a través del programa transaccional de UCM EDYURACF residente en el MVS.

EMULACIÓN RACF A TRAVÉS DE UCM (*disponible bajo entornos OS/2 y MVS*)

Vd. puede utilizar UCM como su subsistema de seguridad principal para autenticar los usuarios SecureEntry/2 en tiempo de conexión. Básicamente, esto significa que el repositorio UCM será, también, utilizado para almacenar las passwords de los usuarios. La utilización de este subsistema de seguridad implica el cifrado de los datos de conexión de sus usuarios. En este caso SecureEntry/2 utiliza el programa transaccional de UCM EDYTP.

2. Gestión centralizada de las políticas de seguridad

Con UCM, vd. puede definir las políticas de seguridad activas para sus usuarios, grupos y recursos de red. Estos datos pueden ser gestionados o bien:

A través de UCM (gestión centralizada)

Con UCM, vd. puede gestionar de forma centralizada todas las políticas de seguridad corporativas para sus usuarios, grupos y recursos de red a través de la herramientas de administración de SecureEntry trabajando en modo centralizado. Estas políticas de seguridad y definiciones residirán en el repositorio UCM (Base de datos DB2) de la corporación, siendo utilizados programas transaccionales para la distribución de los datos de usuarios a las oficinas en tiempo de conexión. Estos programas transaccionales podrán funcionar en modo:

TP estándar o

TP multi-trans (*únicamente disponible en MVS*) para incrementar el rendimiento.

Además, para datos de oficinas (datos no específicos de usuarios) vd. puede escoger entre los siguientes métodos de actualización (refresco) de datos de oficinas:

ONLINE

Los datos de oficinas serán actualizados en sus oficinas en el momento que haya preconfigurado (o bien en tiempo de conexión de sus usuarios, o a una hora fija del día,...). Si sus líneas de comunicaciones son lentas, vd. puede seleccionar que esta tarea se realice de forma incremental prefijando el límite máximo de información que puede ser distribuida a cada oficina.

BATCH

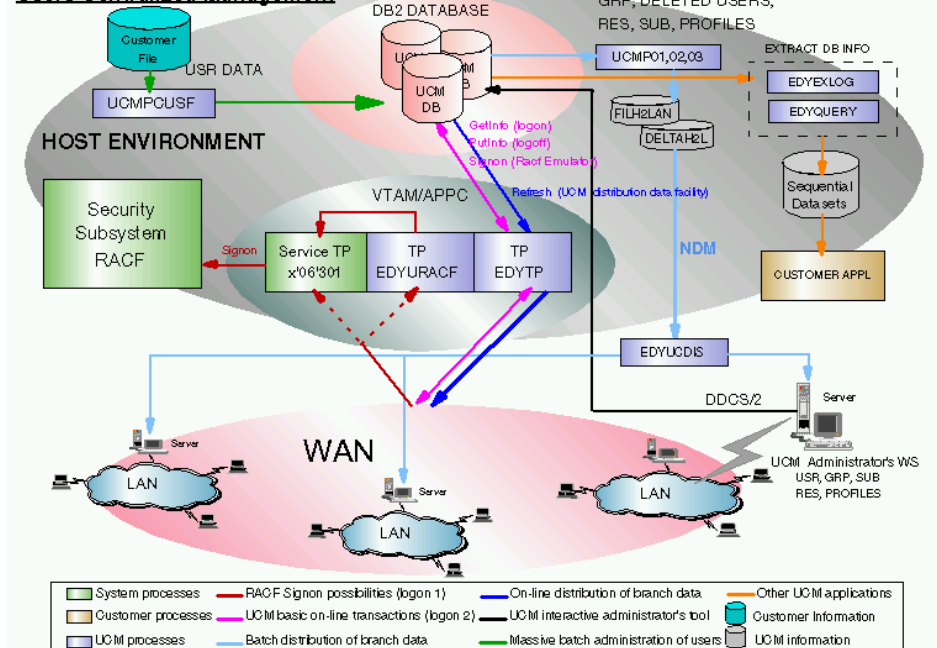
Vd. puede recoger a través de procesos desasistidos de UCM toda la información de oficinas y distribuirla a través de su propio Software a las oficinas. Una vez que la información se encuentra en las oficinas, puede ser actualizada a través de procedimientos desatendidos de SecureEntry/2.

A través de su propio Software

Por si vd. desea UCM únicamente para la autenticación centralizada de sus usuarios pero no para gestionar las políticas de seguridad. En este caso, vd. debe distribuir los perfiles de seguridad a través de sus propios métodos, y utilizar las herramientas de administración de SecureEntry para activarlos en las oficinas.

En la siguiente figura, puede observar las diferentes piezas y procesos que componen UCM. Se muestra, además, el flujo de información (simplificado) que existe entre cada uno de estos componentes.

Users Centralized Management



Antes de abordar la instalación de UCM, debe decidir qué tipo de instalación utilizará su corporación en relación con las posibilidades explicadas sobre estas líneas. Esto implica tomar la decisión de cuál será el subsistema de autenticación de usuarios principal, y si vd. requiere UCM para gestionar centralizadamente el repositorio de políticas de seguridad (recomendado) o no. En caso de utilizar UCM, deberá, además, decidir entre la utilización del método online (recomendado) o batch de distribución de datos de oficinas.

Vd. puede instalar la autenticación de RACF (logon 1 y (opcionalmente) las transacciones básicas de UCM), o la autenticación de UCM (logon 2 y (obligatorio) las transacciones básicas de UCM). Consulte los Programas transaccionales de UCM para obtener más información acerca de estos procesos.

Una vez instalado y configurado el Software de UCM, necesitará definir los Grupos y Recursos a través de la estación administradora de UCM. Una vez definidos, podrá añadir los usuarios SecureEntry/2 en el repositorio central. UCM le ofrece la utilidad UCMPCUSF para abordar esta tarea. Mediante UCMPCUSF, vd. podrá administrar masivamente todos los usuarios, gestionando las altas, bajas y modificaciones de usuarios. Vd., también puede definir sus usuarios a través de las herramientas de administración de SecureEntry/2 (interactivamente o en modo desasistido), ejecutándolas contra el repositorio UCM.

Una vez realizadas todas las definiciones de oficinas, vd. puede descargarlas y actualizarlas en las oficinas a través de dos diferentes caminos:

En modo *Batch*

Vd. puede recoger toda la información de oficina almacenada en UCM a través de los procesos UCMP01, UCMP02 y UCMP03 en entorno Host y actualizarla en las oficinas a través del proceso EDYUCDIS.

Estos procesos UCM recogen la información de oficina y la almacenan en un archivo (dataset en MVS). Vd. debe distribuir este archivo a todas los servidores de oficinas y entonces actualizar las definiciones a través de la utilidad SecureEntry de LAN (EDYUCDIS).

En modo *On-Line*

Si esta función (Funcionalidad de refresco dinámico de datos) está activa, UCM descargará, en el momento especificado en configuración, en todas las estaciones servidoras de oficinas la información de oficina almacenada en el repositorio central. Este proceso se realiza a través del *transaction program* EDYTP.

UCM suministra las aplicaciones EDYEXLOG y EDYQUERY que le permitirán extraer información de la Base de Datos de UCM de manera que luego pueda ser procesada por sus propias aplicaciones.

El Software de UCM está disponible bajo plataformas OS/2 y MVS/ESA, pudiendo realizar la instalación del mismo según las necesidades de su corporación.

UCM bajo entorno MVS/ESA está dirigido a grandes corporaciones con un gran número de usuarios y oficinas. Para estas corporaciones que demandan gran capacidad de procesamiento de datos, fiabilidad y escalabilidad del entorno, UCM Versión para MVS/ESA es la solución idónea. Diríjase al capítulo de Instalando UCM en MVS/ESA para obtener información detallada.

UCM bajo entorno OS/2 está dirigido a corporaciones con un número de usuarios y oficinas limitado, que no disponen de un gran ordenador que centralice el procesamiento de datos o bien para aquellas corporaciones en las que la utilización de UCM en MVS/ESA no está justificado.

Observe que el código UCM OS/2 se distribuye conjuntamente con SecureEntry/2, en modo de evaluación. Para desbloquear dicho código, de modo que no expire, lea atentamente Instalando UCM en plataformas OS/2.

Vd. puede proceder ahora con el capítulo Instalando UCM donde se encuentran detalladas las diferentes tareas que tendrá que abordar en la puesta en marcha del código de UCM.

Requerimientos de Software

Esta sección enumera el software requerido para que la instalación y operación de UCM se realice correctamente. Los requerimientos de software son diferentes según del entorno en el que instalemos: Host, Estación de administración UCM/Estación UCM o las oficinas.

Host

Estación de administración de UCM/Estación UCM

Oficinas

Si vd. está instalando UCM bajo plataforma OS/2 no necesita conocer los requerimientos de software necesarios para Host.

Host

MVS/ESA Version 4 Release 3 (5695-047, 5695-048)

RACF/MVS Version 1 Release 9.2 (5740-XXH) u otro subsistema de seguridad con el mismo nivel. De acuerdo, ahora puede instalar UCM con la funcionalidad de emulación de RACF. Diríjase al manual para administradores de SecureEntry para obtener más información al respecto.

ACF/VTAM Version 3 Release 4 (5685-085)

ACF/NCP Version 4 Release 3 (5668-854)

ACF/SSP Version 4 Release 6 (5665-338)

Librerías de run-time de C/370 or PL/I

DB2 MVS Version 2 Release 3 (5665-DB2)

Estación de administración de UCM/Estación UCM

Si vd. está configurando UCM bajo entorno OS/2, la estación de administración UCM es la misma donde se instala físicamente la Base de Datos de UCM.

OS/2 Warp V3.0 con FixPack XR_W017, o superior, y (opcionalmente) SES OS/2 (Security Enabling Services)

Communications Manager/2

DB2 y DDCCS/2 Single User (DDCCS/2 únicamente si instala UCM en MVS/ESA)

SecureEntry release 3.0

Oficinas

OS/2 Warp V3.0 with FixPack XR_W017, o superior, y (opcionalmente) SES OS/2 (Security Enabling Services)

IBM LAN Server 4.0 o superior

CM/2 en el servidor

SecureEntry release 3.0

Instalando UCM

Esta sección describe las tareas necesarias para la instalación y consecución de un entorno operacional de UCM bajo plataformas MVS/ESA y OS/2.

Se detallan de forma específica estas tareas para cada plataforma donde se desea instalar UCM tal como sigue:

Plataforma MVS/ESA

Plataforma OS/2

Plataforma MVS/ESA

Este capítulo describe las tareas relacionadas con la instalación y la consecución de un entorno de UCM operacional en Host, tal como sigue:

Configurando APPC/MVS

Creando la Base de Datos UCM

Inicializando la Base de Datos UCM

Instalando los programas UCM

Planificando la distribución

Configurando la característica de facilidad de datos distribuidos (DDF) del DB2 para MVS/ESA

También se describen las tareas adicionales que tendrá que ejecutar en el servidor de la oficina y en la estación administradora de UCM cuando utilice UCM.

Configurando Communications Manager/2

Configurando el DB2 DDCS/2 en la estación administradora de UCM

Vinculando las funciones de UCM (API)

Vinculando la Aplicación de consulta de oficinas

Vinculando la Herramienta de Recuperación UCM

Si vd. instala la emulación de RACF, encontrará una sección que describe detalladamente la funcionalidad de la misma y cómo ha de configurarla:

Instalando el emulador de RACF

Si vd. está instalando la autenticación de usuarios a RACF y requiere el cifrado de datos a través del canal de comunicaciones, vd. debe instalar y configurar el TP EDYURACF:

Instalando EDYURACF

Así mismo se describen las tareas que tendrá que realizar si vd. se encuentra migrando desde una versión previa del UCM.

Migrando desde versiones previas de UCM

*** **NOTA** ***

Para obtener una descripción de los procedimientos SecureEntry a seguir durante la instalación de SecureEntry para habilitar la gestión de UCM, remítase al capítulo 'Instalando SecureEntry' del 'Manual de administración SecureEntry'.

Configurando el APPC/MVS

El APPC/MVS es un componente estándar de MVS/ESA. Para configurarlo, vd. ha de seguir los pasos que se describen a continuación:

- Configure el APPC y el ASCH en la parmlib

- Configure el proceso de arranque automático del APPC y su planificador (scheduler)

- Cree los dos archivos VSAM necesitados por el APPC

- Defina un nodo principal y un modo de log (logmode) específico

A continuación se detalla cada uno de los puntos mencionados sobre estas líneas haciendo hincapié en los procedimientos de ayuda que ofrece UCM para configurar cada uno de ellos:

1. Configurando la PARMLIB

La información requerida por el APPC y su planificador, ASCH, está definida en los miembros de la PARMLIB APPCPMxx y ASCHPMxx. Estos miembros pueden ser configurados mediante los miembros del conjunto de datos ('data set members') distribuidos en **UCM.Vxx.JCL(APPCPM00)** y **UCM.Vxx.JCL(ASCHPM00)**.

2. Configurando el arranque automático del APPC y su planificador

Vd. puede incluir los comandos para arrancar el APPC y el ASCH usando el miembro de la PARMLIB SYS1.PARMLIB(COMMAND00) o bien mediante el procedimiento de arranque automático que normalmente utilice en IPL.

Los comandos para arrancar las tareas de APPC/MVS son los siguientes:

```
S APPC, SUB=MSTR, APPC=xx
S ASCH, SUB=MSTR, ASCH=xx
```

Donde xx corresponde al sufijo xx de los miembros de la PARMLIB APPCPMxx y ASCHPMxx

3. Creando los archivos VSAM necesarios

El APPC/MVS guarda la información de los TP (programas transaccionales) y la 'SIDE INFORMATION' (el alias que define la LUNAME, MODENAME y TPNAME) en dos archivos VSAM. En las siguientes secciones se describe como crear estos dos archivos VSAM:

Utilice el IDCAMS para crear el archivo VSAM SIDE INFORMATION

Utilice el miembro data set distribuido a tal efecto: **UCM.Vxx.JCL(ATBSIVSM)** como ejemplo de trabajo para crearlo.

Utilice el IDCAMS para crear el archivo VSAM que guarda la información del TP (programa transaccional)

Utilice a tal efecto el miembro data set distribuido en: **UCM.Vxx.JCL(ATBTPVSM)** como ejemplo de trabajo para crearlo.

4. Definiendo un nodo principal y un logmode específico

Estas definiciones son un ejemplo; Los únicos requerimientos son el nombre de logmode (APPCHOST) y el soporte de sesiones paralelas de LU6.2.

Nodo principal de VTAM

Defina el nodo principal en SYS1.VTAMLST o en la librería apropiada.

```
/* SYS1.VTAMLST APPL DEFINITIONS FOR APPC
*/
APPLAPPC VBUILD TYPE=APPL
*
APPCLU1  APPL  ACBNAME=APPCLU1,
            APPC=YES,
            AUTOSSES=0,
            DDRAINL=NALLOW,
            DLOGMOD=APPCHOST,
            DMINWNL=0,
            DMINWNR=3,
            DRESPL=NALLOW,
            DSESLIM=3,
            EAS=90,
            LMDENT=19,
            MODETAB=TABPCLU,
            PARSESS=YES,
            SECACPT=CONV,
            SRBEXIT=YES,
            VPACING=1
```

Logmode para estaciones OS/2 y APPC

```
LU62P      MODEENT LOGMODE=APPCHOST,
            FMPPROF=X'13',
            TSPROF=X'07',
            PRIPROT=X'B0',
            SECPROT=X'B0',
            COMPROT=X'50B1',
            SSNDPAC=X'00',
            SRCVPAC=X'00',
            RUSIZES=X'8585',
            TYPE=0,
            PSNDPAC=X'00',
            PSERVIC=X'060200000000000000002F00'
```

Creando la Base de Datos UCM

El miembro data set **UCM.Vxx.DB2(CREAUCM)** recoge el conjunto de sentencias SQL necesarias para crear todas las tablas de la Base de Datos UCM.

El miembro data set **UCM.Vxx.DB2(CREASYNR)** recoge todas las sentencias SQL necesarias para crear todos los sinónimos de las tablas de la Base de Datos para resolver las peticiones dinámicas de SQL que se realizan desde las estaciones de UCM. Esto es necesario si el USERID de la estación no coincide con el ID usado cuando se crearon las tablas de la Base de Datos UCM.

A partir de DB2V4, y como posible alternativa al uso de sinónimos, usted puede especificar el parámetro de BIND, para los procesos UCM, **DYNAMICRULES(BIND)**. De este modo el cualificador usado para resolver las sentencias SQL dinámicas será el especificado en el momento del BIND.

Migrando desde versiones previas de UCM: Si está realizando una migración desde una versión previa de UCM, entonces ha de utilizar los siguientes miembros data set en vez de los descritos sobre estas líneas:

UCM.Vxx.DB2(UP40TUCM) y **UCM.Vxx.DB2(UP40SUCM)** para crear las dos nuevas tablas de la versión V4Rx, sus índices y sinónimos.

Vd. ha de tener en cuenta, sin embargo, que el tamaño de esta Base de Datos ha sido decidido pensando en un entorno de TEST. Cuando esta Base de Datos sea utilizada para producción debe ser reconsiderado el tamaño pensando en el número estimado de usuarios así como en el número de grupos, recursos y enlaces entre los mismos que contendrá.

Puede ejecutar las sentencias SQL desde el SPUFI, usando un JCL o desde la estación administradora de UCM utilizando el DDCCS/2.

Inicializando la Base de Datos UCM

El miembro data set distribuido en: **UCM.Vxx.DB2(UCMSETUP)** recoge las sentencias SQL necesarias para inicializar la tabla T_KEYWORD de la Base de Datos UCM con todas las palabras clave por defecto de la versión V4Rx.

Migrando desde versiones previas de UCM (solo): Si está realizando una migración desde una versión previa de UCM deberá utilizar los siguientes miembros data set (en vez de los descritos sobre estas líneas): **UCM.Vxx.DB2(UP40KUCM)**, para inicializar la tabla (existente) de la Base de Datos UCM T_KEYWORD con las nuevas palabras clave requeridas por la versión V4Rx.

Instalando los programas UCM

Para que todos los procesos UCM, desasistidos y 'ONLINE', se ejecuten correctamente, vd. debe instalar los programas UCM y funciones (APIs) en el MVS/ESA. Los miembros data set que contienen los archivos ejecutables y de vinculación (BIND) a la Base de Datos deben seguir la nomenclatura del cliente, realizando los cambios necesarios en las STEPLIBs de los JCLs que son requeridos para ellos.

Para instalar los programas de UCM, vd. debe ejecutar las siguientes tareas:

Defina los datasets necesarios para el UCM (observe el siguiente JCL)

```
//ALLOCDTS JOB ( ),MSGLEVEL=(1,1),CLASS=W,MSGCLASS=X
//*****
//*
//* JCL para crear los datasets necesarios *
//* para el UCM *
//* *
//*****
//STEP1 EXEC PGM=IEFBR14
//LOADDD DD DSN=UCM.Vxx.LOADLIB,
// DISP=(NEW,CATLG),
// UNIT=SYSDA,VOL=SER=RM2005,
// SPACE=(6144,(640,320,10),,CONTIG,ROUND),
// DCB=(RECFM=U,BLKSIZE=6144)
//JCLDD DD DSN=UCM.Vxx.JCL,
// DISP=(NEW,CATLG),
// UNIT=SYSDA,VOL=SER=RM2005,
// SPACE=(6160,(25,10,5),,CONTIG,ROUND),
// DCB=(RECFM=FB,LRECL=80,BLKSIZE=6160)
//BNDDD DD DSN=UCM.Vxx.BND,
// DISP=(NEW,CATLG),
// UNIT=SYSDA,VOL=SER=RM2005,
// SPACE=(6160,(25,10,5),,CONTIG,ROUND),
// DCB=(RECFM=FB,LRECL=80,BLKSIZE=6160)
//OBJDD DD DSN=UCM.Vxx.OBJ,
// DISP=(NEW,CATLG),
// UNIT=SYSDA,VOL=SER=RM2005,
// SPACE=(6160,(25,10,5),,CONTIG,ROUND),
// DCB=(RECFM=FB,LRECL=80,BLKSIZE=6160)
//DB2DD DD DSN=UCM.Vxx.DB2,
// DISP=(NEW,CATLG),
// UNIT=SYSDA,VOL=SER=RM2005,
// SPACE=(6160,(25,10,5),,CONTIG,ROUND),
// DCB=(RECFM=FB,LRECL=80,BLKSIZE=6160)
//*
//* *****
//* Data set de ejemplo de un archivo de parámetros del proceso *
//* EDYEXLOG *
//* *****
```

```
//PARAMS      DD DSN=UCM.Vxx.EDYEXLOG.PARAMS,
//              DISP=(NEW,CATLG),
//              UNIT=SYSDA,VOL=SER=RM2005,
//              SPACE=(CYL,(2,1)),
//              DCB=(RECFM=FB,LRECL=80,BLKSIZE=800,DSORG=PS)
//
// * *****
// * Este data set es opcional. Contiene un miembro data set con *
// * la tabla de traducción de ASCII a EBCDIC. *
// * Si es omitida, se utilizará una tabla de traducción por *
// * defecto *
// * *****
//TABLESDD     DD DSN=UCM.Vxx.TABLES,
//              DISP=(NEW,CATLG),
//              UNIT=SYSDA,VOL=SER=RM2005,
//              SPACE=(CYL,(2,1)),
//              DCB=(RECFM=FB,LRECL=256,BLKSIZE=2560)
//
// *
```

Copie los datasets de UCM desde el cartucho de instalación (observe el siguiente JCL)

```
//TAPEDISK JOB ( ),MSGLEVEL=(1,1),CLASS=W,MSGCLASS=X
//*****
// * *
// * JCL para copiar los datasets de UCM desde *
// * el cartucho de instalación *
// * *
//*****
//STEP1       EXEC PGM=IEBCOPY
//SYSUT3      DD UNIT=SYSDA,SPACE=(CYL,(5,5))
//SYSUT4      DD UNIT=SYSDA,SPACE=(CYL,(5,5))
//LOADDS      DD DSN=UCM.Vxx.LOADLIB,DISP=SHR
//LOADTP      DD DSN=UCM.Vxx.LOADLIB,
//              DISP=(,PASS),LABEL=(1,SL),
//              UNIT=TAP01,VOL=SER=UCMTAP,
//              DCB=(RECFM=U,BLKSIZE=6144)
//JCLDS       DD DSN=UCM.Vxx.JCL,DISP=SHR
//JCLTP       DD DSN=UCMTAPE.UCM.JCL,
//              DISP=(,PASS),LABEL=(2,SL),
//              UNIT=TAP01,VOL=SER=UCMTAP,
//              DCB=(RECFM=FB,LRECL=80,BLKSIZE=6160)
//BNDDS       DD DSN=UCM.Vxx.BND,DISP=SHR
//BNDDTP      DD DSN=UCM.Vxx.BND,
//              DISP=(,PASS),LABEL=(3,SL),
//              UNIT=TAP01,VOL=SER=UCMTAP,
//              DCB=(RECFM=FB,LRECL=80,BLKSIZE=6160)
//OBJDS       DD DSN=UCM.Vxx.OBJ,DISP=SHR
//OBJTP       DD DSN=UCM.Vxx.OBJ,
//              DISP=(,PASS),LABEL=(4,SL),
//              UNIT=TAP01,VOL=SER=UCMTAP,
//              DCB=(RECFM=FB,LRECL=80,BLKSIZE=6160)
//DB2DS       DD DSN=UCM.Vxx.DB2,DISP=SHR
//DB2TP       DD DSN=UCM.Vxx.DB2,
//              DISP=(,PASS),LABEL=(5,SL),
//              UNIT=TAP01,VOL=SER=UCMTAP,
//              DCB=(RECFM=FB,LRECL=80,BLKSIZE=6160)
//PARDS       DD DSN=UCM.Vxx.EDYEXLOG.PARAMS,DISP=SHR
//PARTP       DD DSN=UCM.Vxx.EDYEXLOG.PARAMS,
//              DISP=(,PASS),LABEL=(6,SL),
//              UNIT=TAP02,VOL=SER=UCMTAP,
//              DCB=(RECFM=FB,LRECL=80,BLKSIZE=800)
//TABDS       DD DSN=UCM.Vxx.TABLES,DISP=SHR
//TABTP       DD DSN=UCM.Vxx.TABLES,
//              DISP=(NEW,PASS),LABEL=(7,SL),
//              UNIT=TAP02,VOL=SER=UCMTAP,
//              DCB=(RECFM=FB,LRECL=256,BLKSIZE=2560)
//
// *
//SYSPRINT    DD SYSOUT=*
```

```

COPY  INDD=LOADTP , OUTDD=LOADDS
COPY  INDD=JCLTP , OUTDD=JCLDS
COPY  INDD=BNFTP , OUTDD=BNDDS
COPY  INDD=OBJTP , OUTDD=OBJDS
COPY  INDD=DBFTP , OUTDD=DB2DS
COPY  INDD=PARTP , OUTDD=PARDS
COPY  INDD=TABTP , OUTDD=TABDS

```

/*

Reservando datasets adicionales

El miembro data set **UCM.Vxx.JCL(ALLOC DT2)** distribuido contiene las sentencias para ubicar los datasets adicionales.

UCMLOG

El data set UCMLOG es utilizado para almacenar un LOG en el entorno de MVS. Es utilizado entre otros por el proceso UCMPUSF encargado de cargar la Base de Datos.

FILH2LAN

El data set FILH2LAN ha sido creado para contener la información que va a ser distribuida a las oficinas. Esta DD es referenciada por el proceso UCMP03. Si vd. utiliza los procesos desasistidos en vez de los ONLINE para distribuir la información a las oficinas, tendrá que crearlo.

DELTAH2L

DELTAH2L ha sido creado para contener la información que va ser distribuida a las oficinas. Este dataset puede ser referenciado en los procesos UCMP01 y UCMP03 en vez del FILH2LAN, si vd. desea mantener dos versiones separadas (la información completa o únicamente el delta).

SEQLOG

SEQLOG ha sido creado para recibir la salida del proceso EDYEXLOG.

UCMQUERY

UCMQUERY ha sido creado para recibir la salida del proceso EDYQUERY.

Ejecute la vinculación (BIND) de los programas

El miembro data set **UCM.Vxx.JCL(BIND)** es un ejemplo de trabajo de los JCL para ejecutar la vinculación, usando los miembros de la librería distribuida UCM.Vxx.BIND:

UCMPUSF

UCMP01

UCMP02

UCMP03

PUTGETUS

UCMREFSH

EDYEXLOG

EDYQUERY

Defina el TP EDYTP en el correspondiente VSAM de APPC utilizando el programa ATBSDFMU con el parámetro TPADD. Como ejemplo, se distribuye el miembro **UCM.Vxx.JCL(TPPROF)**, que debe adaptarse a la nomenclatura de su instalación.

Consulte la sección del Programa transaccional EDYTP para conocer cuáles son los parámetros que debe añadir en el JCL de ejecución del TP según las funcionalidades que desee activar.

Utilice los miembro dataset distribuido en **UCM.Vxx.JCL(ATBTPVSM)** y **UCM.Vxx.JCL(ATBSIVSM)** como ejemplos de trabajo para definir los VSAM necesarios para contener la información de APPC. Utilizar únicamente en el caso de primera instalación de APPC.

Copie y adapte a la nomenclatura del cliente los procesos JCLs desasistidos distribuidos en el data set **UCM.Vxx.JCL**:

UCMPCUSF

UCMP01

UCMP02

UCMP03

EDYEXLOG

EDYQUERY

Planificando la distribución

Para distribuir la información acerca de recursos, grupos y enlaces (links) entre grupos y recursos a los diferentes subsistemas (SecureEntry y LAN Server), recomendamos que utilice el sistema de distribución ONLINE de la versión UCM V4Rx.

Como alternativa al proceso de distribución ONLINE, UCM mantiene el método antiguo, en el cual mediante procesos desasistidos puede recoger esta información y distribuirla mediante el método de distribución que actualmente utilice en su instalación.

Procesos ONLINE de UCM V4Rx

Mediante la herramienta de administración de UCM, vd. puede activar el refresco de información de oficina (Refresco de oficina en línea). A través de esta herramienta puede seleccionar de una lista de posibilidades cuándo desea que los cambios se actualicen en sus oficinas.

El proceso EDYSRV.EXE que se ejecuta en el entorno de LAN, es el encargado de actualizar estos cambios en cada oficina de la corporación.

Si vd. desea tener más información acerca del funcionamiento de este proceso puede leer el capítulo de Actualización en línea de las oficinas en el Manual de administración SecureEntry.

Procesos desasistidos de UCM

UCM le ofrece los procesos UCMP01, UCMP02 y UCMP03 para recoger la información de la Base de Datos. Estos procesos están descritos con todo detalle en Procesos UCM (Gestión Centralizada de Usuarios).

Si vd. utiliza estos procesos, tendrá que diseñar dos planes de distribución de la información:

PLAN1

Ejecute el proceso UCMP03 para recoger toda la información necesaria para crear un objeto que le servirá para inicializar una nueva oficina. Distribuya este objeto a la nueva oficina. Ejecute el proceso desasistido EDYUCDIS.EXE en el servidor de la oficina usando el objeto distribuido como parámetro de entrada al proceso. Este, le inicializará todas las estaciones de la oficina.

PLAN2

Ejecute el proceso UCMP01 para recoger toda la información modificada para crear un objeto que le servirá para modificar la información de la oficina. Distribuya este objeto a la oficina. Ejecute el proceso desasistido EDYUCDIS.EXE en el servidor de la oficina usando como parámetro de entrada el objeto distribuido. Este, le modificará la información de todas las estaciones de la oficina.

La información acerca de usuarios es distribuida desde el Host a la oficina a través de un canal de comunicaciones UCM. Esta distribución se realiza en ONLINE en tiempo de conexión y desconexión.

Configurando la característica DDF del DB2 para MVS/ESA

El acceso al DB2 para MVS/ESA desde la estación de UCM está basado en la arquitectura distribuida de Bases de Datos relacionales (DRDA). La característica DDF del DB2 para MVS/ESA debe ser configurada para activar este tipo de acceso.

Si el DDF no está configurado, diríjase a la Guía de Instalación del DBS para MVS/ESA para obtener información de cómo puede ser configurado.

Configurando Communications Manager/2

La instalación de UCM requiere la configuración de las comunicaciones con objeto de habilitar al producto DRDA el acceso a la Base de Datos de UCM desde la estación administradora de UCM y para activar el canal de comunicaciones utilizado para la autenticación de usuarios de forma centralizada en el Host.

Vd. debe actualizar la configuración de Communications Manager/2 tanto en las estaciones servidoras de perfiles de SecureEntry (controladores de dominio de sus oficinas) como en la estación que vd. debe dedicar como punto central de administración de UCM.

Bajo estas líneas hallará una guía paso a paso con los requerimientos de configuración para cada tipo de estación:

- Estación de administración de UCM.

- Estaciones servidoras.

Estación de administración de UCM

Esta sección consiste en una lista paso por paso de las definiciones adicionales que ha de especificar para actualizar la configuración del CM/2 en la estación administradora de UCM.

Estas definiciones engloban las definiciones requeridas para configurar una estación servidora de oficina:

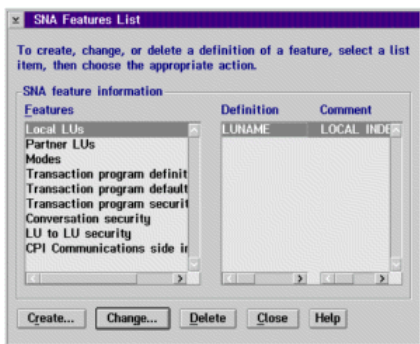
1. En el panel de configuración del Communications Manager List, seleccione la opción de **SNA features**.



2. Usted necesita una LU (6.2) local independiente para establecer las conexiones APPC entre la estación administradora de UCM y el HOST.

Esta LU puede ser una LU independiente definida en el Host con una LOCAL ADDRESS=0, o utilizar el CP.

Si vd. crea una LU independiente, ésta debería ser configurada como la LU 6.2 por defecto. Si necesita utilizar una que no sea la de defecto, vd. deberá hacer uso, entonces, de la variable de entorno de SecureEntry/2 **SGM_FORCE_LUALIAS**.



3. En este ejemplo, se ha definido la LU independiente LUNAME con el alias LOCALLU, estableciéndose como la LU por defecto. El nombre de LU, si no es utilizado el CP, debe ser provisto por su administrador de red SNA. El alias de la LU puede ser cualquiera que vd. escoja.

Local LU

LU name: LUNAME

Alias: LOCALLU

NAU address:

☒ Independent LU

☐ Dependent LU NAU: [] { 1 - 254 }

Host link: HOST0001

Optional LU model name: []

☒ Use this local LU as your default local LU alias

Optional comment: LOCAL INDEPENDENT LU 6.2

OK Cancel Help

4. Defina la LU asociada (partner) que actúa como puerta de acceso al APPC/MVS. Esta LU deberá estar, a su vez, definida en el Host como una LU 6.2 con soporte para sesiones paralelas, APPC=YES, y logmode APPCHOST, tal y como se describe en el apartado **Configurando el APPC/MVS**.

Esta es la puerta de acceso al APPC/MVS. Escriba el nombre completo de LU y el alias que debe ser EDYALIAS. En el ejemplo el identificador de la red es NETID y el nombre de la LU asociada (definida en el APPC/MVS) es APPCLU1. El alias de esta definición es (por requerimiento) EDYALIAS.

Partner LU

Fully qualified LU name: NETID . APPCLU1

Alias: EDYALIAS

☐ Conversation security verification

Dependent partner LU:

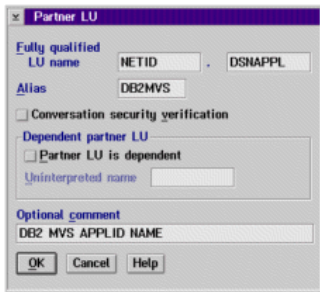
☐ Partner LU is dependent

Uninterpreted name: []

Optional comment: LU 6.2 DEFINED IN APPC/MVS

OK Cancel Help

5. Defina una segunda LU asociada. Esta es la definición correspondiente de DB2 para soportar DRDA, para de este modo activar el acceso de la Aplicación administradora de SecureEntry a la Base de Datos Central de UCM. Defina la LU correspondiente (su pareja), definida en el Host como un subsistema DB2 APPL, y especifique un alias, a su elección, para ser usado en las definiciones CPI.



Partner LU

Fully qualified LU name: NETID . DSNAPPL

Alias: DB2MVS

☐ Conversation security verification

Dependent partner LU

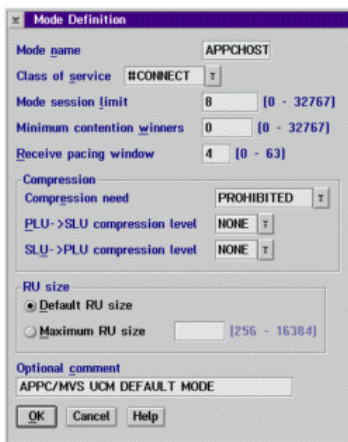
☐ Partner LU is dependent

Uninterpreted name:

Optional comment: DB2 MVS APPLID NAME

OK Cancel Help

6. Añada el Modo de Definición (Mode Definition) con los parámetros estándar. El único requerimiento específico es el Nombre de Modo (Mode name), el cual debe ser APPCHOST.



Mode Definition

Mode name: APPCHOST

Class of service: #CONNECT

Mode session limit: 0 [0 - 32767]

Minimum contention winners: 0 [0 - 32767]

Receive pacing window: 4 [0 - 63]

Compression

Compression need: PROHIBITED

PLU->SLU compression level: NONE

SLU->PLU compression level: NONE

RU size

☒ Default RU size

☐ Maximum RU size: [256 - 16384]

Optional comment: APPC/MVS UCM DEFAULT MODE

OK Cancel Help

7. Defina un segundo Modo de Definición para esta estación. El único parámetro requerido en este paso es el Nombre de Modo, ya que el logmode por defecto para el DB2 en MVS/ESA es IBMRDB. Si vd. desea cambiar este nombre póngase en contacto con su administrador de sistema de DB2 en Host. Los parámetros especificados en este modo son negociados durante el establecimiento de la sesión.

Mode Definition

Mode name: IEMRDEI

Class of service: #CONNECT

Mode session limit: 8 [0 - 32767]

Minimum contention winners: 0 [0 - 32767]

Receive pacing window: 4 [0 - 63]

Compression:

Compression need: PROHIBITED

PLU->SLU compression level: NONE

SLU->PLU compression level: NONE

RU size:

☒ Default RU size

☐ Maximum RU size: [256 - 16384]

Optional comment:

DOCS DB2 STANDARD MODE

OK Cancel Help

8. El CPI (Communications Side Information) incluye los nombres de LU y los nombres de TP a los que vd. tendrá acceso a través del subsistema de comunicaciones CPI.

Vd. debe definir el CPI EDYCCHST (requerimiento). Éste se utilizará como el canal de comunicaciones UCM entre la estación administradora de las oficinas y la parte de la aplicación UCM que reside en Host.

Como alias de la *partner* LU debe seleccionar EDYALIAS (punto 4). El nombre de TP que debe especificar es el nombre con el que haya definido el TP UCM en el HOST, por ejemplo, EDYTP. El modo que debe establecer es APPCHOST (punto 6). El tipo de seguridad será programa, de este modo, al iniciarse la petición de conexión APPC, se enviará un identificador de usuario (userID) y una password para ser autenticados en el Host a través de RACF mediante una exit de seguridad del APPC/MVS.

CPI Communications Side Information

Symbolic destination name: EDYCCHST

Partner LU:

☐ Fully qualified name

☒ Alias: EDYALIAS

Partner TP:

☐ Service TP

TP name: EDYTP

Security type:

☐ Same ☐ None ☒ Program

Mode name: APPCHOST

Optional comment:

UCM COMMUNICATION CHANNEL CPI

Continue... Cancel Help

9. Pulse el botón **Continue...** y especifique el Identificador de un usuario (userID) definido en RACF, cuya contraseña no ha de expirar, que posee los privilegios (grants) necesarios para acceder a la Base de Datos UCM. La autoridad de este userID será utilizada por la aplicación UCM para recoger y actualizar información de las oficinas en la Base de Datos UCM.

CPI Communications Program Security

Enter your user ID, and then type your password twice for confirmation. Select OK.

User ID: UCMUSER

Password: *****

Retype the password: *****

OK Cancel Help

- Defina un segundo CPI. Llámelo por ejemplo, DB2CPI. Esta definición se correlaciona con las definiciones del Director de Bases de Datos DB2 que enlaza el alias de UCM en DB2 con la localización del nodo de DB2.

Como nombre de TP debe especificar X'07'6DB , éste es el nombre del TP que reside en el DB2 de MVS, y que permite la conexión remota. El tipo de seguridad que debe seleccionar es Same. El logmode que debe especificar es el que definió como IBMRDB (punto 7).

CPI Communications Side Information

Symbolic destination name: DB2CPI

Partner LU:

- ☐ Fully qualified name
- ☒ Alias: DB2MVS

Partner TP:

- ☒ Service TP
- TP name: X'07'6DB

Security type: ☒ Same ☐ None ☐ Program

Mode name: IBMRDB

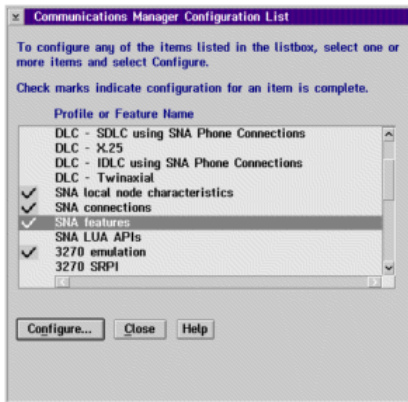
Optional comment: DB2 DDOS CPI

OK Cancel Help

Estaciones servidoras

Esta sección consiste en una lista paso por paso de las definiciones adicionales que ha de especificar para actualizar la configuración del CM/2 en las estaciones servidoras de sus oficinas.

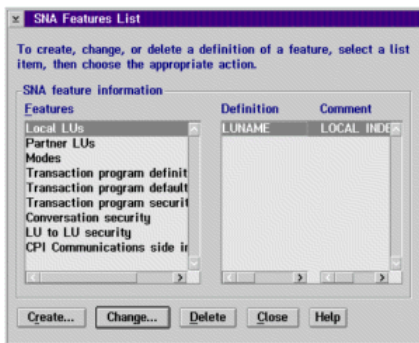
- En el panel de configuración del Communications Manager List, seleccione la opción de **SNA features**.



2. Usted necesita una LU (6.2) local independiente para establecer las conexiones APPC entre la estación servidora de oficinas y el HOST.

Esta LU puede ser una LU independiente definida en el Host con una LOCAL ADDRESS=0, o utilizar el CP.

Si vd. crea una LU independiente, ésta debería ser configurada como la LU 6.2 por defecto. Si necesita utilizar una que no sea la de defecto, vd. deberá hacer uso, entonces, de la variable de entorno de SecureEntry/2 **SGM_FORCE_LUALIAS**.



3. En este ejemplo, se ha definido la LU independiente LUNAME con el alias LOCALLU, estableciéndose como la LU por defecto. El nombre de LU, si no se utiliza el CP, debe ser provisto por su administrador de red SNA. El alias de la LU puede ser cualquiera que vd. escoja.

Local LU

LU name: LUNAME

Alias: LOCALLU

NAU address:

☒ Independent LU

☐ Dependent LU NAU: [] { 1 - 254 }

Host link: HOST0001

Optional LU model name: []

☒ Use this local LU as your default local LU alias

Optional comment: LOCAL INDEPENDENT LU 6.2

OK Cancel Help

4. Defina la LU asociada (partner) que actúa como puerta de acceso al APPC/MVS. Esta LU deberá estar, a su vez, definida en el Host como una LU 6.2 con soporte para sesiones paralelas, APPC=YES, y logmode APPCHOST, tal y como se describe en el apartado **Configurando el APPC/MVS**.

Esta es la puerta de acceso al APPC/MVS. Escriba el nombre completo de LU y el alias que debe ser EDYALIAS. En el ejemplo el identificador de la red es NETID y el nombre de la LU asociada (definida en el APPC/MVS) es APPCLU1. El alias de esta definición es (por requerimiento) EDYALIAS.

Partner LU

Fully qualified LU name: NETID . APPCLU1

Alias: EDYALIAS

☐ Conversation security verification

Dependent partner LU:

☐ Partner LU is dependent

Uninterpreted name: []

Optional comment: LU 6.2 DEFINED IN APPC/MVS

OK Cancel Help

5. Añada el Modo de Definición (Mode Definition) con los parámetros estándar. El único requerimiento específico es el Nombre de Modo (Mode name), el cual debe ser APPCHOST.

Mode Definition

Mode name: APPCHOST

Class of service: #CONNECT

Mode session limit: 8 [0 - 32767]

Minimum contention winners: 0 [0 - 32767]

Receive pacing window: 4 [0 - 63]

Compression:

Compression need: PROHIBITED

PLU->SLU compression level: NONE

SLU->PLU compression level: NONE

RU size:

☒ Default RU size

☐ Maximum RU size: [256 - 16384]

Optional comment:

APPC/MVS UCM DEFAULT MODE

OK Cancel Help

6. El CPI (Communications Side Information) incluye los nombres de LU y los nombres de TP a los que vd. tendrá acceso a través del subsistema de comunicaciones CPI.

Vd. debe definir el CPI EDYCCHST (requerimiento). Éste se utilizará como el canal de comunicaciones UCM entre la estación servidora de las oficinas y la parte de la aplicación UCM que reside en Host.

Como alias de la *partner* LU debe seleccionar EDYALIAS (punto 4). El nombre de TP que debe especificar es el nombre con el que haya definido el TP UCM en el HOST, por ejemplo, EDYTP. El modo que debe establecer es APPCHOST (punto 5). El tipo de seguridad será programa, de este modo, al iniciarse la petición de conexión APPC, se enviará un identificador de usuario y una password para ser autenticados en el Host a través de RACF mediante una exit de seguridad del APPC/MVS.

CPI Communications Side Information

Symbolic destination name: EDYCCHST

Partner LU:

☐ Fully qualified name

☒ Alias: EDYALIAS

Partner TP:

☐ Service TP

TP name: EDYTP

Security type:

☐ Same ☐ None ☒ Program

Mode name: APPCHOST

Optional comment:

UCM COMMUNICATION CHANNEL CPI

Continue... Cancel Help

7. Pulse el botón **Continue...** y especifique el Identificador de un usuario (userID) definido en RACF, cuya contraseña no ha de expirar, que posee los privilegios (grants) necesarios para acceder a la Base de Datos UCM. La autoridad de este userID será utilizada por la aplicación UCM para recoger y actualizar información de las oficinas en la Base de Datos UCM.

☒ **CPI Communications Program Security**

Enter your user ID, and then type your password twice for confirmation. Select OK.

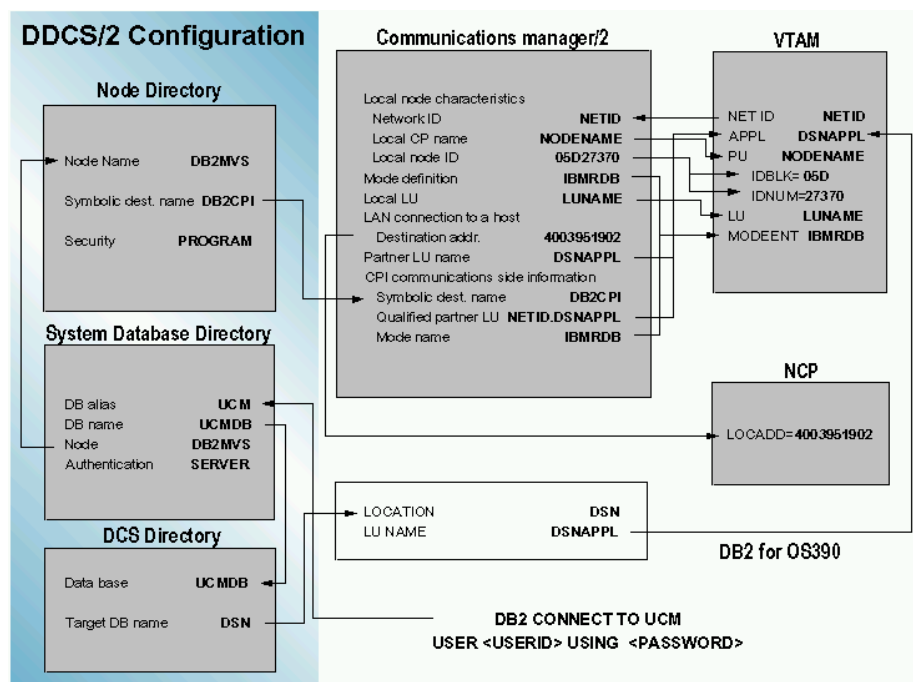
User ID

Password

Retype the password

Configurando el DB2 DDCS/2 en la estación de UCM

Para configurar la estación de administración UCM, vd. debe configurar el DB2 local instalado en la estación de tal manera que haga referencia a la configuración de *Communications Manager/2* y a los datos configurados en su Host tal y como se muestra en la siguiente figura:



Vd. puede definir el acceso a la Base de Datos de UCM manualmente a través de las herramientas gráficas o bien desde una sesión OS/2 tal y como se detalla a continuación:

Catalogue el nodo APPC que especifica el nombre de destino simbólico que vd. ha definido en el CM/2.

DB2 CATALOG APPC NODE **DB2MVS** REMOTE **DB2CPI** SECURITY PROGRAM/SAME/NONE

Catalogue la Base de Datos UCM correlacionándola con la definición anterior

DB2 CATALOG DB UCMDDB AS UCM AT NODE **DB2MVS** AUTHENTICATION SERVER

Catalogue la información de la Base de Datos UCM en remoto

DB2 CATALOG DCS DB UCMDDB AS **DSN**

Donde **DSN** es el nombre del Subsistema de DB2 MVS/ESA exportado por DDF. DDF MVS/ESA permite que el subsistema DB2 de MVS/ESA sea conocido por otros sistemas con el nombre especificado en el parámetro **LOCATION** en el arranque de DDF y **LU NAME** es el nombre de la LU 6.2 a través de la cual será accedido el DB2.

Debe vd. vincular las Aplicaciones y Utilidades del DDCS/2. para habilitar el acceso remoto a UCM una vez realizada la configuración del DDCS/2. Encontrará la información necesaria para realizar esta tarea en el manual *DDCS User's Guide*.

Vinculando las funciones de UCM (API)

Para administrar la Base de Datos UCM desde la estación administradora de UCM, vd. puede utilizar las funciones (APIs) de UCM. Ya que en el desarrollo de estas funciones ha sido utilizado SQL embebido, deben ser vinculadas (bind) contra cada Base de Datos en Host con la cual vayan a interactuar.

Los planes de acceso están contenidos en los *archivos de vinculación*, los cuales fueron creados durante la precompilación. Vincular significa precisamente el procesamiento de estos archivos por el servidor de DRDA.

Para vincular las funciones (API) de UCM, debería asegurarse que tiene asignada la autoridad suficiente en el sistema de gestión de Bases de Datos en MVS:

```
SYSADM    o
SYSCTRL   o
BINDADD y CREATE IN COLLECTION NULLID y/o BIND
```

Una vez hecho esto, escriba las siguientes sentencias desde una sesión de OS/2:

```
DB2START
DB2 CONNECT TO dbalias USER userid USING password
DB2 BIND @EDYUCM.LST QUALIFIER ucmsqid
DB2 CONNECT RESET
DB2STOP
```

Donde *dbalias* es el alias de Base de Datos de Host definido en el DDCS/2 y *userid* es el identificador de usuario con los privilegios (grants) apropiados para vincular los programas. *ucmsqid* corresponde al prefijo definido sobre la Base de Datos UCM.

Note que vd. puede realizar el mismo proceso utilizando el comando EDYUCBND, que se encuentra dentro del directorio INSTALL de SecureEntry. Invóquelo sin parámetros para ver la sintaxis del mismo.

El proceso de los archivos de vinculación en diferentes paquetes proporciona la granularidad necesaria para dar los diferentes privilegios de ejecución a niveles de usuarios o grupos.

Si vd. ejecuta una conexión con un usuario con privilegio SYSADM, podrá ejecutar cualquier paquete de la API de UCM. Los usuarios normales deberían tener privilegio de ejecución sobre las funciones (o paquetes), dependiendo de las tareas que estarán autorizados a realizar.

Estos son los planes de administración previstos:

Acceso básico

El usuario solo puede ver la información de la Base de Datos.

Acceso de usuario

El usuario puede ver y cambiar la información de la Base de Datos siempre y cuando esté relacionada con el usuario.

Acceso de Grupos y recursos

El usuario puede ver la información de la Base de Datos y cambiar la información que está relacionada con grupos y recursos.

Acceso completo

El usuario puede realizar cualquier tarea sobre la Base de Datos.

Para simplificar la tarea de asignar privilegios (grant), se ofrece una utilidad de línea de comando que es capaz de otorgar estos privilegios sobre los paquetes de sentencias de ejecución para un usuario o grupo:

```
EDYUCM GRANT /G:id /F:nombrearchivo [/D:Base Datos][/P:prefijo][ /CONTINUE]
```

id

Identificador de usuario o identificador de grupo al cual van a ser concedidos los privilegios.

nombrearchivo

Nombre del archivo que contiene la lista de paquetes sobre los cuales los privilegios van a ser concedidos.

Base Datos

Alias de la Base de Datos. Por defecto es **UCM**.

prefijo

Nombre de prefijo para el paquete. Si el parámetro es omitido, el prefijo del paquete debe ser especificado en el nombre de archivo, de forma *prefijo.nombre_paquete*.

CONTINUE

Especifica que el comando sea ejecutado para cada entrada del archivo, a pesar de que ocurra algún error durante el proceso. Si se omite el parámetro, el comando es completado únicamente si no ocurre ningún error.

Estos son los archivos provistos para cada tipo de acceso:

EDYBASIC.LST

Acceso básico

EDYUSER.LST

Acceso de usuario

EDYGROUP.LST

Acceso de grupo y recurso

EDYALL.LST

Acceso completo

Para revocar el privilegio de ejecución para un usuario o grupo, se ofrece la siguiente utilidad:

```
EDYUCM REVOKE /G:id /F:nombreachivo [/D:Base Datos][ /P:prefijo ][/CONTINUE]
```

id

Identificador de usuario o grupo para el cual el privilegio va a ser revocado.

nombreachivo

Nombre del archivo que contiene la lista de paquetes sobre los cuales el privilegio va ser revocado.

Base Datos

Alias de la Base de Datos Por defecto es **UCM**.

prefijo

Nombre de prefijo para el paquete. Si se omite el parámetro, el prefijo del paquete debe ser especificado en el nombre de archivo, de la forma prefijo.nombre_paquete.

CONTINUE

Especifica que el comando sea ejecutado para cada entrada del archivo, a pesar de que ocurra algún error durante el proceso. Si se omite el parámetro, el comando será completado únicamente cuando no ocurra ningún error.

El siguiente ejemplo, muestra como se concede el nivel de autorización mínima al usuario USER0112.

```
edyucm grant /G:USER0112 /F:EDYBASIC.LST
```

Este otro ejemplo concede autorización completa al grupo ADMINS sobre la Base de Datos UCM; el prefijo para las tablas de la Base de Datos UCM (UCMPROD) se especifica explícitamente:

```
edyucm grant /G:ADMINS /F:EDYALL.LST /P:UCMPROD
```

Vinculando la aplicación de consulta de oficinas

EDYQRYBR es una aplicación que le permite consultar el nivel de actualización de sus oficinas desde el entorno de LAN en la estación administradora de UCM.

Ya que en el desarrollo de esta aplicación ha sido utilizado SQL embebido, debe vincularla con cada Base de Datos en Host contra las que la aplicación vaya a interactuar.

Los planes de acceso a la Base de Datos están contenidos en los *archivos de vinculación*, los cuales fueron creados durante la precompilación. La vinculación significa precisamente el procesamiento de estos archivos por el servidor de DRDA.

Para vincular la aplicación EDYQRYBR, debería asegurarse de que tiene asignada la suficiente autoridad en el sistema de gestión de Bases de Datos en MVS:

```
SYSADM    y
SYSCTRL   y
BINDADD y CREATE IN COLLECTION NULLID y/o BIND
```

Entonces, desde una sesión de OS/2 entre las siguientes sentencias:

```
DB2START
DB2 CONNECT TO dbalias USER userid USING password
DB2 BIND @EDYQRYBR.LST QUALIFIER ucmsqid
DB2 CONNECT RESET
DB2STOP
```

Donde *dbalias* es el alias de la Base de Datos en Host definido en el DDCS/2 y *userid* es el identificador de usuario con los apropiados privilegios concedidos para realizar la tarea de vinculación de programas. *ucmsqid* corresponde al prefijo definido sobre la Base de Datos UCM.

Note que vd. puede realizar el mismo proceso mediante el comando EDYUCBND, ubicado dentro del directorio INSTALL en el SecureEntry. Invóquelo sin parámetros para ver su sintaxis.

El archivo **EDYQRYBR.LST** ubicado en el directorio INSTALL, puede ser utilizado para vincular el programa.

Tal como se explicó en el capítulo anterior, vd. puede utilizar el comando EDYUCM para realizar la tarea de concesión de los privilegios adecuados al programa. Para hacer esto, puede utilizar el archivo **EDYQUERY.LST** ubicado dentro del directorio INSTALL del SecureEntry.

Vinculando la Herramienta de Recuperación UCM

Esta herramienta ha sido realizada para corregir y compactar las tablas de cambios de la Base de Datos UCM cuando es detectado un error en el proceso Actualización en línea de oficinas.

Ya que en el desarrollo de esta aplicación ha sido utilizado SQL embebido, debe vincularla con cada Base de Datos en Host contra las que la aplicación vaya a interactuar.

Los planes de acceso a la Base de Datos están contenidos en los *archivos de vinculación*, los cuales fueron creados durante la precompilación. La vinculación significa precisamente el procesamiento de estos archivos por el servidor de DRDA.

Para vincular la aplicación EDYRVUCM debería asegurarse de que tiene asignada la suficiente autoridad en el sistema de gestión de Bases de Datos en MVS:

```
SYSADM    o
SYSCTRL   o
BINDADD y CREATE IN COLLECTION NULLID y/o BIND
```

Entonces, desde una sesión de OS/2 entre las siguientes sentencias:

```
DB2START
DB2 CONNECT TO dbalias USER userid USING password
DB2 BIND @EDYRVUCM.LST QUALIFIER ucmsqid
DB2 CONNECT RESET
DB2STOP
```

Donde *dbalias* es el alias de la Base de Datos en Host definido en el DDCS/2 y *userid* es el identificador de usuario con los apropiados privilegios concedidos para realizar la tarea de vinculación de programas. *ucmsqid* corresponde al prefijo definido sobre la Base de Datos UCM.

Note, que vd. puede realizar el mismo proceso mediante el comando EDYUCBND, ubicado dentro del directorio INSTALL en el SecureEntry. Invóquelo sin parámetros para ver su sintaxis.

El archivo **EDYRVUCM.LST** ubicado en el directorio INSTALL, puede ser utilizado para vincular el programa.

Tal como se explicó en el capítulo anterior, vd. puede utilizar el comando EDYUCM para realizar la tarea de concesión de los privilegios adecuados al programa. Para hacer esto, puede utilizar el archivo **EDYRCVRY.LST** ubicado dentro del directorio INSTALL del SecureEntry.

Instalando el emulador de RACF

Si tiene la intención de instalar la funcionalidad de emulación de RACF, puede hacerlo a través de la herramienta de instalación de SecureEntry. Diríjase a la guía de administración SecureEntry para obtener más información al respecto.

Si escoge esta opción de instalación de SecureEntry, debe especificar la **DD UCMINSTT** en los siguientes procesos ejecutables:

1. UCMPCUSF
2. EDYTP

Esta **DD** debe apuntar al miembro data set que contiene la información relativa al nombre de la corporación, el conjunto de caracteres permitidos y las longitudes máxima y mínima permitidas para las passwords de su corporación. Estos datos son necesarios para el correcto funcionamiento de la emulación SecureEntry de RACF.

En este archivo puede especificar los siguientes parámetros (claves):

INSTITUTION = Nombre de la corporación. Ha de ser la misma que utilice en la instalación de SecureEntry en las LAN's.

MINPASSWORDLEN = Longitud mínima permitida para las passwords. Ha de ser la misma que la especificada en la instalación de SecureEntry.

MAXPASSWORDLEN = Longitud máxima permitida para las passwords. Ha de ser la misma que la especificada en la instalación de SecureEntry.

AVAILABLECODES = Conjunto de caracteres permitidos que pueden componer sus passwords. Ha de ser la misma que la especificada en la instalación de SecureEntry.

UCMSUBSRACFKEY = Clave de descricción para autenticación de usuarios en RACF a través de EDYURACF.

El **NOMBRE DE LA CORPORACIÓN** que escoja ha de ser el mismo que el que especifique para sus oficinas en la herramienta de instalación SecureEntry.

Puede utilizar el miembro data set **UCM.Vxx.TABLES(INSTITUT)** que se distribuye con UCM como ejemplo de trabajo para crear un archivo que contenga la información necesaria para la emulación de RACF.

Si es usted usuario de la Emulación de RACF que UCM provee a sus clientes, verá incrementada la velocidad de conexión de sus usuarios debido a las mejoras de rendimiento efectuadas para minimizar el número de transacciones que un usuario provoca en tiempo de conexión a la estación contra el HOST. Al mismo tiempo que se valida/autentica la contraseña de un usuario se verifica si se ha de realizar la segunda transacción a UCM para obtener los cambios producidos sobre los datos del usuario. De no haber cambios, no se realiza esta segunda transacción.

ATENCIÓN: actualmente no es posible migrar de validación contra RACF a la emulación SecureEntry de RACF. Si desea hacerlo, por favor, póngase en contacto con el equipo de SecureEntry.

Instalando EDYURACF

EDYURACF es un *Transaction Program* diseñado para atender las peticiones de autenticación de usuarios que se desencadenan desde las oficinas, descifrando los datos que le llegan por la línea de comunicaciones y luego estableciendo una conversación APPC con RACF (o producto de seguridad instalado) para verificar la autenticidad del usuario.

Para habilitar el uso de esta funcionalidad, vd. deberá seguir una serie de pasos concretos de configuración tanto en las estaciones servidoras de sus oficinas como en el entorno MVS/ESA:

Servidores de Oficinas (incluyendo la estación de administración de UCM)

Haga lo siguiente:

1. Cuando vd. instale SecureEntry en un servidor, y haya especificado que desea cifrado de comunicaciones para la autenticación de usuarios, SecureEntry copiará la DLL **EDYURACF.DLL** ubicada en el directorio **SecureEntryPath\INSTALL** al directorio **SecureEntryPath\DLL**. Al hacer esto, la instalación SecureEntry estará activando implícitamente el cifrado de datos a través del canal de comunicaciones.

Si desea utilizar una clave maestra de cifrado de datos diferente del NOMBRE DE INSTITUCIÓN especificado durante la instalación de SecureEntry, vd. debe añadir la clave **UCMSUBSRACFKEY** en el archivo **EDYUCFPW.DSC** ubicado en el directorio **SecureEntryPath\INSTALL**.

2. Añada la siguiente definición en su configuración del Communications Manager/2:

Debe vd. definir el CPI (Communications Side Information) EDYURACF. Esta definición se utilizará para establecer el canal de comunicaciones entre sus estaciones servidoras y el TP EDYURACF residente en el APPC/MVS. El alias de la LU asociada (*partner LU*) será **EDYALIAS**.

Bajo estas líneas se muestra un ejemplo de la definición del CPI EDYURACF:

CPI Communications Side Information

Symbolic destination name: EDYURACF

Partner LU

☐ Fully qualified name

☒ Alias: EDYALIAS

Partner TP

☐ Service TP

TP name: EDYURACF

Security type

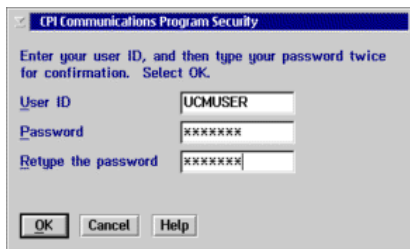
☐ Same ☐ None ☒ Program

Mode name: APPCHOST

Optional comment: RACF COMMUNICATION CHANNEL CPI

Continue... Cancel Help

El tipo de seguridad deberá ser **Program**, y en *CPI Communications program security* deberá definir un usuario que cuya contraseña no expire en RACF tal y como se muestra en el siguiente ejemplo:



Si desea más información de cómo definir la LU asociada EDYALIAS o el LOGMODE APPHOST diríjase al apartado de Configuración del Communications Manager/2 puntos **4 y 6**.

Entorno MVS/ESA

Bajo el entorno del MVS/ESA, vd. debe configurar un nuevo TP llamado EDYURACF con los siguientes requerimientos:

El TP EDYURACF debe residir en una **librería APF** debido a que establece una sesión de comunicaciones con otra LU 6.2.

Defina el TP EDYURACF en el correspondiente VSAM de APPC utilizando ATBSDFMU con el parámetro TPADD. Como ejemplo, se distribuye el miembro UCM.Vxx.JCL(TPPROF), que debe adaptarse a la nomenclatura de su instalación.

EDYURACF utiliza una clave de descifrado que debe ser especificada para que pueda entender los datos que le son enviados desde las oficinas. Esta clave puede ser especificada de dos formas diferentes tal y como se explica a continuación:

1. Mediante parámetro de carga del proceso */I:clave_de_descifrado*.
2. Mediante definición de la **DD UCMINSTT** en el JCL de ejecución del proceso EDYURACF en APPC.

Para obtener información adicional de la clave de cifrado/descifrado, diríjase a la sección Programa transaccional EDYURACF.

Debe configurar la CPI Side Information en el APPC con nombre **EDYSECSI** que debe hacer referencia a una partner LU 6.2 existente en APPC/MVS (puede ser la misma LU 6.2 origen) y en el campo de TP hay que configurar el **Service TP del SNA x'06'301**. El MODE NAME debe ser **APPCHOST**. En la siguiente figura se muestra la configuración de estos datos a través de los paneles del ISPF/PDF:

```

Add Side Information

Type information. Then Enter.

To system file . . SYS1.APPCSI_____

Symbolic Destination
Name . . . . . EDYSECSI

TP Name "X'06'301_____

Mode Name APPCHOST          SNA Session Connecting Local LU to Partner LU
Partner LU APPCLU1_____ Identifier of the Remote TP Residence

PF01 = Help      PF03 = Exit      PF12 = Cancel
Command ==>

```

Como alternativa a los paneles del ISPF/PDF, puede utilizar el programa utilidad ATBSDFMU para añadir la CPI Side Information en su Sistema utilizando la clave **SIADD**.

Migrando desde versiones previas de UCM

Si usted posee una versión previa de UCM, puede actualizar su software a la versión V4Rx de UCM.

La Versión 4 de UCM ofrece nuevas herramientas para actualizar la información de grupos y recursos en sus oficinas a través de los procesos EDYSRV y EDYTP.

Esta opción resulta muy útil para realizar el refresco dinámico de sus datos de oficina de tal manera que puede vd. configurar cuando se va a realizar esta actualización dependiendo de sus necesidades o requerimientos. Si utiliza esta nueva funcionalidad de UCM, ya no tendrá que utilizar los procesos desasistidos UCMP01, UCMP02, UCMP03 y EDYUCDIS para distribuir los cambios a sus oficinas.

Si planea actualizar el nivel de UCM a la versión 4, también tendrá que actualizar el nivel de SecureEntry al 190 o superior.

Para actualizar el nivel de UCM en el entorno de Host ha de seguir los siguientes pasos:

Cree las nuevas tablas de la versión UCM V4Rx.

El miembro data set **UCM.Vxx.DB2(UP40TUCM)**, que se distribuye en el cartucho de instalación, contiene las sentencias de SQL necesarias para crear las dos nuevas tablas de la versión V4Rx, así como sus índices.

Puede ejecutar las sentencias de SQL desde el SPUFI, utilizando JCL, o desde la estación administradora de UCM, utilizando DDCS/2.

Cree los nuevos sinónimos para las tablas.

El miembro data set **UCM.Vxx.DB2(UP40SUCM)** contiene las sentencias SQL para crear los dos nuevos sinónimos para las tablas que creó en el paso anterior.

Puede ejecutar las sentencias SQL desde el SPUFI, utilizando JCL, o desde la estación administradora de UCM, utilizando el DDCS/2.

Cargue la tabla T_KEYWORD.

El miembro data set **UCM.Vxx.DB2(UP40KUCM)** contiene las sentencias SQL para cargar sobre la tabla T_KEYWORD las nuevas palabras clave que la versión V4Rx de UCM necesita para comenzar a funcionar.

Instalando la distribución de UCM V4Rx.

Este es el mismo paso que para una instalación nueva. Para tener el UCM actualizado a último nivel, recomendamos que se instalen todos los módulos distribuidos.

Siga las instrucciones que encontrará en Instalando los programas UCM.

Plataforma OS/2

La instalación de UCM bajo plataforma OS/2 no es de ningún modo compatible con la instalación y configuración de un entorno operacional de UCM bajo plataforma MVS/ESA.

Bajo entorno OS/2 se propone una instalación y configuración de UCM en la estación que luego se utilizará para administrar la Base de Datos de UCM. Si usted desea separar la administración de la Base de Datos de UCM de su implementación física deberá configurar DB2 y CM/2 para poder atender peticiones remotas.

La instalación de UCM bajo entorno OS/2 presupone aceptar funcionalidades específicas comentadas en:

Prerequisitos de UCM en OS/2

La herramienta de instalación de SecureEntry/2 instala los módulos ejecutables necesarios para establecer UCM operacional bajo entorno OS/2.

Paso a paso del proceso de instalación:

Guía rápida de instalación de UCM en OS/2

Descripción detallada de los diversos procedimientos de instalación:

Configurando Communications Manager/2

Creando la Base de Datos de UCM

Vinculando los programas UCM

También se describen las tareas adicionales que tendrá que ejecutar en el servidor de la oficina y en la estación administradora de UCM (ésta también es la estación donde se instala físicamente UCM) cuando utilice UCM.

Inicializando la Base de Datos UCM

Planificando la distribución

Así mismo, se detallan ejemplos de procesos que explotan la Base de Datos de UCM, configuraciones de Communications Manager/2 para la *Estación de Administración de UCM* y para la *Estación Servidora de Perfiles* de una oficina.

Software adicional de UCM

NOTA IMPORTANTE

El código de administración centralizada UCM/2 se distribuye conjuntamente con SecureEntry/2. No obstante, y al tratarse de un paquete que se debe contratar por separado, dicho código se suministra en régimen de evaluación. Así pues, el mismo expira automáticamente a los 6 meses de la fecha de generación del paquete SecureEntry/2 bajo el que se halle instalado. Si vd. decide contratar dicho código, entonces podrá

eliminar este mecanismo de protección por medio de una contraseña que nuestro equipo le proporcionará.
Teclee :

```
EDYTPPRD -P: contraseña
```

desde la vía de acceso SecureEntry, directorio *INSTALL*, y su copia de UCM/2 pasará a ser considerada de producción, sin fecha alguna de expiración.

Prerequisitos de UCM en OS/2

Nótese que la instalación de UCM bajo entorno OS/2 supone la utilización obligatoria de la funcionalidad de Emulación de RACF. En este caso, el nombre de institución es obtenido de la configuración estándar de SecureEntry/2 que se encuentra en el archivo *SENTRY.CNF* ubicado en el directorio *\SGMSHELL\INSTALL*, u obtenido por parámetro de carga del programa transaccional *EDYTP*. Este dato es utilizado para realizar el cifrado de datos de usuarios en la Base de Datos de UCM.

Además, vd. deberá instalar las tablas de translación ASCII/EBCDIC ubicadas en el directorio *\SGMSHELL\INSTALL*. Estas tablas son utilizadas por el código de UCM para traducir los datos entrantes a la convención de página de códigos soportada por el Host. Ya que bajo este entorno la página de datos del Host es también la ASCII, ambas tablas deberían contener el código ASCII para que no se realice ningún tipo de translación de datos. Vd. encontrará estas tablas para ser utilizadas con UCM OS/2 en el directorio *SecureEntryPath\INSTALL\UCMOS2*. Proceda a copiarlas al directorio *SecureEntryPath\INSTALL*. **Esto debe ser realizado en la estación administradora de UCM y en todas las estaciones servidoras de oficinas.**

Guía rápida de instalación de UCM en OS/2

Este capítulo contiene una enumeración paso a paso del proceso de instalación y configuración de UCM bajo entorno OS/2 en los diferentes escenarios:

Estación de Host/Administración de UCM

Bajo entorno OS/2, la estación de administración de UCM es la misma donde reside físicamente la Base de Datos de UCM.

La instalación de la Base de Datos de UCM y de la administración centralizada debe realizarse tal y como se expone en los siguientes pasos:

1. Configure el Communications Manager/2.
2. Instale SecureEntry 3.0 con las funcionalidades de administración centralizada UCM y emulación de RACF. Recuerde, además, especificar que esta estación es un servidor de perfiles.
3. Edite el archivo **EDYSTART.CMD** y añada las siguientes líneas al inicio del archivo:

```
Edylkmsg "Arrancando el DB2"  
Logon <ID de usuario> /P:Contraseña /L  
Db2start
```

Donde :

Id de usuario: debe ser el identificador de usuario con privilegios suficientes para arrancar el DB2. Se recomienda que sea el mismo usuario que el definido en CM/2 para autenticar las transacciones del proceso *EDYTP*.

4. Copie en el directorio `\SGMSHELL\INSTALL`, las tablas de traducción ASCII/EBCDIC `EDYA2E.DAT` y `EDYE2A.DAT` ubicadas en el directorio `\SGMSHELL\INSTALL\UCMOS2`.
5. Reinicialice la máquina y conéctese con un usuario con privilegios de administrador. Esta conexión se realizará en estado de emergencia.
6. Cree la Base de Datos de UCM mediante la utilidad `CREAUCM.CMD` (Sección: Creando la Base de Datos de UCM).
7. Inicialice la Base de Datos de UCM mediante la utilidad `UCMSETUP.CMD` (Sección: Inicializando la Base de Datos UCM).
8. Vincule la API y el software de administración de UCM mediante la utilidad `BINDUCM.CMD` (Sección: Vinculando los programas UCM) ubicada en el directorio `\SGMSHELL\INSTALL\UCMOS2`.
9. Ejecute el programa **INSTSUB.EXE**, con el objeto de añadir la información básica de los subsistemas de seguridad soportados. Vd. puede encontrar esta utilidad en el directorio `\SGMSHELL\INSTALL`.
10. Abra la carpeta **SecureEntry: Herramientas de Administración**. Haga una nueva copia del objeto **Administración de usuarios y grupos** y renómbrela como **Administración de usuarios y grupos UCM**. Abra la libreta de propiedades de este nuevo objeto y cambie `EDYSNADM.EXE` por `UCMADM.CMD` como nombre de programa a invocar. Ponga como parámetro `EDYSNADM.EXE`.
11. Asegúrese de que en el archivo `EDYSTART.CMD` se encuentra la sentencia apropiada para arrancar el Communications Manager/2 (Normalmente 'start cmstart', tal y como fue configurado por la instalación de SecureEntry/2).
12. Ejecute el objeto *Administración de usuarios y grupos UCM* que fue creado anteriormente y defina en UCM un usuario con privilegios de administrador.
13. Shutdown de la máquina y vuelva a reinicializarla conectándose con el nuevo usuario definido en UCM.
14. Defina en la Base de Datos de UCM los grupos, perfiles de seguridad para grupos y recursos que vd. desea añadir en sus oficinas. Una vez que haya realizado estas definiciones, vd. estará en condiciones de implementar Planes de distribución de estos datos a sus oficinas.
15. Finalmente, lea detenidamente la sección Software adicional de UCM donde podrá encontrar ejemplos de uso de procesos UCM.

Estaciones controladoras de dominio en oficinas

Para instalar y configurar las estaciones servidoras siga los siguientes pasos:

1. Configure el Communications Manager/2.
2. Instale SecureEntry 3.0 con las funcionalidades de administración centralizada UCM y emulación de RACF. Recuerde además especificar que esta estación es un servidor de perfiles.
3. Copie en el directorio `\SGMSHELL\INSTALL`, las tablas de traducción ASCII/EBCDIC `EDYA2E.DAT` y `EDYE2A.DAT` ubicadas en el directorio `\SGMSHELL\INSTALL\UCMOS2`.
4. Asegúrese de que en el archivo `EDYSTART.CMD` se encuentra la sentencia apropiada para arrancar el Communications Manager/2 (Normalmente 'start cmstart', tal y como fue configurado por la instalación de SecureEntry/2).

5. Reinicialice la máquina y conectese con un usuario definido en UCM.

Estaciones clientes en oficinas

Para instalar y configurar las estaciones cliente simplemente debe instalar SecureEntry 3.0 con las funcionalidades de administración centralizada UCM y emulación de RACF. Recuerde además especificar que esta estación es una estación cliente. Una vez finalizada la instalación, reinicialice la máquina y conectese con un usuario definido en UCM.

Creando la Base de Datos de UCM

En el directorio `\$GMSHELL\INSTALL\UCMOS2`, vd. encontrará la utilidad REXX `CREAUCM.CMD` que le permitirá de forma fácil crear la Base de Datos de UCM bajo entorno OS/2.

La sintaxis de esta utilidad es la siguiente:

```
CREAUCM [NOMBRE_DB] | [?]
```

Donde

NOMBRE_DB: Nombre de la Base de Datos UCM.
UCM por defecto.

? : Visualiza la ayuda de la utilidad

Esta utilidad ha sido desarrollada de forma genérica como ayuda para crear la Base de Datos. Si usted desea crear la Base de Datos de UCM con otros parámetros debe editar la utilidad y adecuarla a sus necesidades.

Configurando Communications Manager/2

Usted debe actualizar la configuración del Communications Manager/2 en las estaciones servidoras de las oficinas y en la estación de administración de UCM, tal como se detalla en los siguientes apartados:

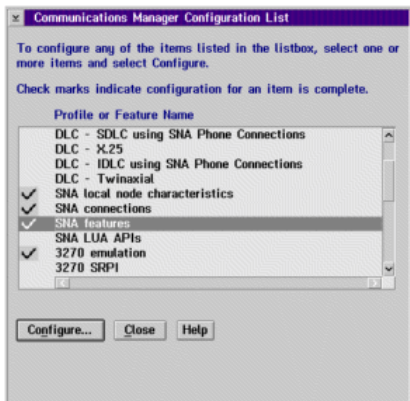
Estación administradora de UCM.

Estaciones servidoras.

Estación de administración de UCM

Esta sección consiste en una lista paso a paso de las definiciones adicionales que ha de especificar para actualizar la configuración del CM/2 en la estación de administración de UCM. Bajo entorno OS/2 la estación de administración de UCM es también la estación Host donde reside UCM.

1. En el panel de configuración del Communications Manager List, seleccione la opción de **SNA features**.

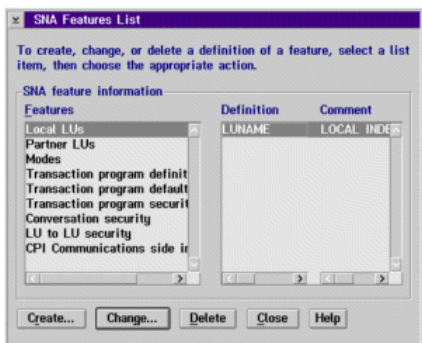


2. Necesita definir una LU (6.2) local independiente por defecto para establecer las conexiones APPC entre la estación administradora y la estación donde reside el repositorio UCM (la propia estación de administración).

Si en su configuración ya posee definida una LU 6.2 local independiente y por defecto, entonces puede saltar al siguiente paso de la configuración.

Si desea utilizar una LU 6.2 local configurada como no la de por defecto, entonces deberá utilizar la variable de entorno de SecureEntry/2 **SGM_FORCE_LUALIAS**, documentada en la **Guía para Administradores de SecureEntry/2**.

Esta LU 6.2 será referenciada por las estaciones servidoras de perfiles como la LU 6.2 *asociada* (partner) para establecer el canal de comunicaciones UCM.



3. En el siguiente ejemplo, la LU LUNAME ha sido definida como una LU 6.2 local independiente con alias LOCALLU.

Local LU

LU name: LUNAME

Alias: LOCALLU

NAU address:

☒ Independent LU

☐ Dependent LU NAU: [] { 1 - 254 }

Host link: HOST0001

Optional LU model name: []

☒ Use this local LU as your default local LU alias

Optional comment: LOCAL INDEPENDENT LU 6.2

OK Cancel Help

El nombre de la LU deberá serle suministrado por su administrador de red SNA. Vd. puede definir el alias de la LU según los criterios de su corporación.

En la sección de Software adicional de UCM encontrará dos ejemplos de configuraciones de CM/2 para activar una estación servidora y la estación UCM. Estos ejemplos difieren de la configuración propuesta en que se trata de una configuración de CM/2 para establecer una comunicación entre dos **Nodos tipo END node**, sin la intervención de ningún **Network Node**.

4. Debe definir una segunda LU (6.2) local independiente. Esta LU será utilizada como *partner* LU en las conexiones APPC entre la estación administradora y la propia estación administradora.

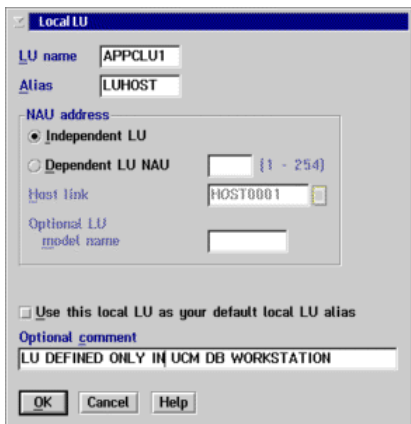
SNA Features List

To create, change, or delete a definition of a feature, select a list item, then choose the appropriate action.

SNA feature information	Definition	Comment
Local LUs	APPCLU1	LU FOR UCM
Partner LUs	LUNAME	LOCAL INDEF
Modes		
Transaction program definitions		
Transaction program defaults		
Transaction program security		
Conversation security		
LU-to-LU security		
CPI Communications side information		

Create... Change... Delete Close Help

5. Si no dispone de esta segunda LU debe crearla. Tanto el nombre para esta LU como el alias puede establecerlos usted mismo. En este ejemplo, el nombre de LU es APPCLU1 y el alias LUHOST.



Local LU

LU name: APPCLU1

Alias: LUHOST

NAU address:

- ☒ Independent LU
- ☐ Dependent LU NAU: [] { 1 - 254 }

Host link: HOST0001

Optional LU model name: []

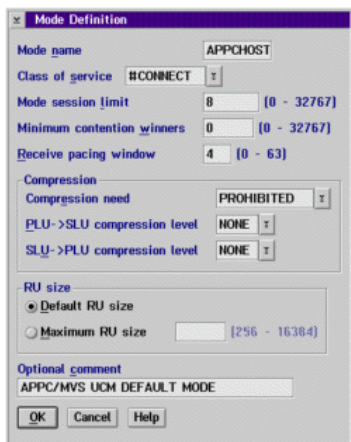
☐ Use this local LU as your default local LU alias

Optional comment: LU DEFINED ONLY IN UCM DB WORKSTATION

OK Cancel Help

Este nombre de LU será utilizado en la definición de la CPI (Communications Side Information) **EDYCCHST**.

- Añada el Modo de Definición (Mode Definition) con los parámetros estándar. El único requerimiento específico es el Nombre de Modo (Mode name), el cual debe ser APPCHOST.



Mode Definition

Mode name: APPCHOST

Class of service: #CONNECT

Mode session limit: 8 { 0 - 32767 }

Minimum contention winners: 0 { 0 - 32767 }

Receive pacing window: 4 { 0 - 63 }

Compression:

- Compression need: PROHIBITED
- PLU->SLU compression level: NONE
- SLU->PLU compression level: NONE

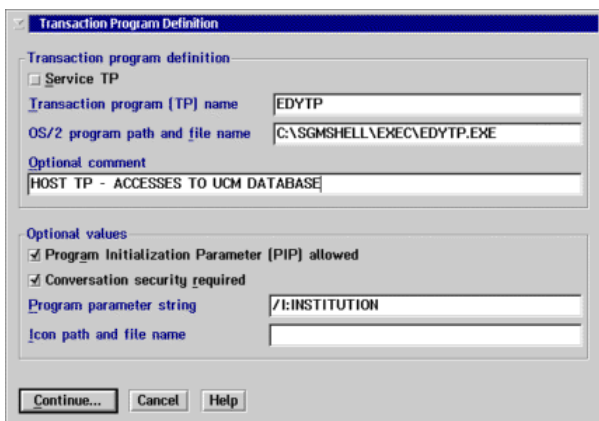
RU size:

- ☒ Default RU size
- ☐ Maximum RU size: [] { 256 - 16384 }

Optional comment: APPC/MVS UCM DEFAULT MODE

OK Cancel Help

- Defina el transaction program (TP) EDYTTP tal y como se especifica en el siguiente panel de configuración:



Transaction Program Definition

Transaction program definition

☐ Service TP

Transaction program (TP) name: EDYTP

OS/2 program path and file name: C:\SGMSHELL\EXEC\EDYTP.EXE

Optional comment: HOST TP - ACCESSES TO UCM DATABASE

Optional values

☒ Program Initialization Parameter (PIP) allowed

☒ Conversation security required

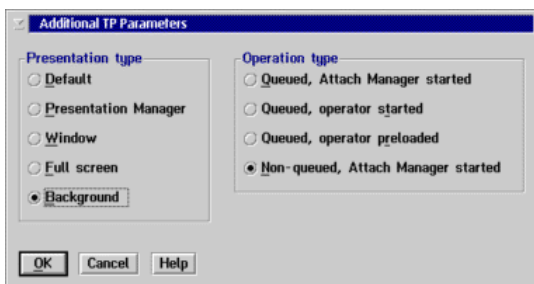
Program parameter string: /I:INSTITUTION

Icon path and file name:

Continue... Cancel Help

En Valores Opcionales, marque los dos botones y en los parámetros del programa especifique el nombre de su institución (Parámetro /I:NOMBRE_DE_INSTITUCION) que ha de coincidir con el especificado en el archivo SENTRY.CNF ubicado en \SGMSHELL\INSTALL.

Presione el botón **Continue** y defina en Parámetros adicionales del TP el **Presentation type** y el **Operation type** tal y como se muestra en la siguiente figura:



Additional TP Parameters

Presentation type

☐ Default

☐ Presentation Manager

☐ Window

☐ Full screen

☒ Background

Operation type

☐ Queued, Attach Manager started

☐ Queued, operator started

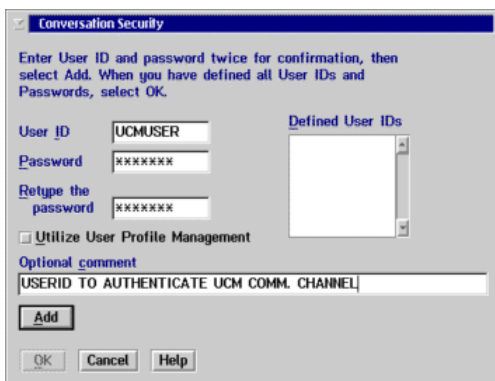
☐ Queued, operator preloaded

☒ Non-queued, Attach Manager started

OK Cancel Help

8. En **Conversation Security** especifique el identificador de usuario (userID), y la contraseña del usuario utilizado para validar las peticiones de comunicaciones. Al especificar que las peticiones entrantes deben suministrar un UserID y una Password, el **Attach Manager** de CM/2 validará la seguridad suministrada antes de ejecutar el proceso EDYTP. Si el UserID y Password no coinciden con uno de los usuarios válidos almacenados en el Communications Manager/2, la petición será rechazada.

En el siguiente ejemplo puede observar la definición del usuario UCMUSER:



Conversation Security

Enter User ID and password twice for confirmation, then select Add. When you have defined all User IDs and Passwords, select OK.

User ID: UCMUSER

Password: *****

Retype the password: *****

☐ Utilize User Profile Management

Optional comment: USERID TO AUTHENTICATE UCM COMM. CHANNEL

Add

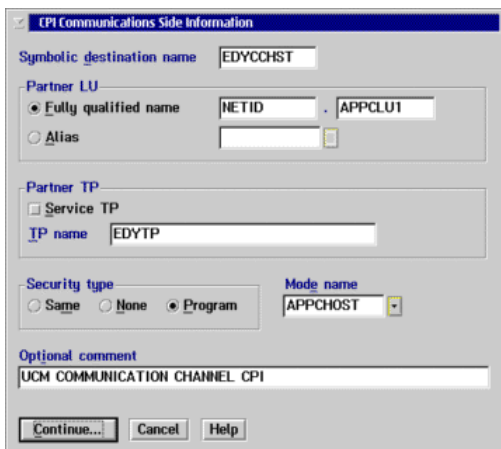
OK Cancel Help

Este es el usuario que se define en la CPI (Communication Side Information) **EDYCHST** al seleccionar que el tipo de seguridad requerida es *Program*.

Recuerde que la definición de este usuario es *case-sensitive*. Si la password que otorga a este usuario es en mayúsculas, en la CPI **EDYCHST** deberá especificar la password del usuario en mayúsculas.

9. El CPI (Communications Side Information) incluye los nombres de LU y los nombres de TP a los que vd. tendrá acceso a través del subsistema de comunicaciones CPI.

UCM requiere que vd. defina el CPI **EDYCHST**. Esta definición contiene todos los datos necesarios para establecer la sesión de comunicaciones entre la estación servidor de perfiles y el TP que reside en la estación Host de UCM (en este caso ambos son la misma estación).



CPI Communications Side Information

Symbolic destination name: EDYCHST

Partner LU

☒ Fully qualified name: NETID . APPCLU1

☐ Alias

Partner TP

☐ Service TP

TP name: EDYTP

Security type

☐ Same ☐ None ☒ Program

Mode name: APPCHOST

Optional comment: UCM COMMUNICATION CHANNEL CPI

Continue... Cancel Help

En el ejemplo que se muestra sobre estas líneas, el *Nombre del TP* es **EDYTP** (definido en el punto 7), el *LOGMODE* utilizado para establecer las características de la sesión es **APPCHOST** (definido en el punto 6) y la *Partner LU* utilizada es **NETID.APPCLU1** (definida en el punto 5) donde **NETID** es el nombre de la red.

En Security Type debe seleccionar la opción **Program** para que el establecimiento de la sesión de comunicaciones sea autenticado por un usuario y password predefinidos. Para definir el usuario que debe ser validado en el Host, pulse el botón de **Continue...** y rellene los campos del nuevo diálogo que se le muestra en la pantalla.

Especifique como usuario el Id de usuario definido en el punto 8 de esta sección. Recuerde que tanto el Id de usuario como la contraseña del mismo deben ser tecleados tal y como se hizo en el punto 8. Esto es debido a que estos campos son *case-sensitive*

Bajo estas líneas aparece el diálogo de ejemplo para el usuario UCMUSER:

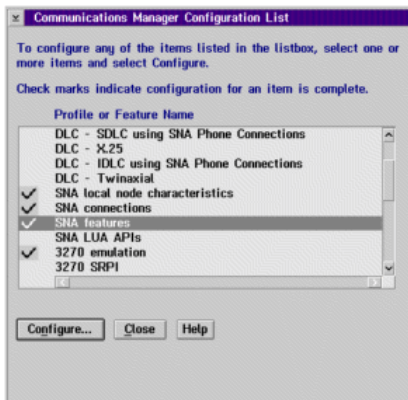


Vd. dispone de un ejemplo de configuración (archivo de respuestas) de la Estación UCM en el directorio *SecureEntryPath\INSTALL\UCMOS2*. Vd. puede activar la configuración que se muestra en este ejemplo siguiendo las instrucciones que encontrará en el capítulo de Software adicional de UCM.

Estaciones servidoras

Esta sección consiste en una lista paso a paso de las definiciones adicionales que ha de especificar para actualizar la configuración del CM/2 en las estaciones servidoras de las oficinas.

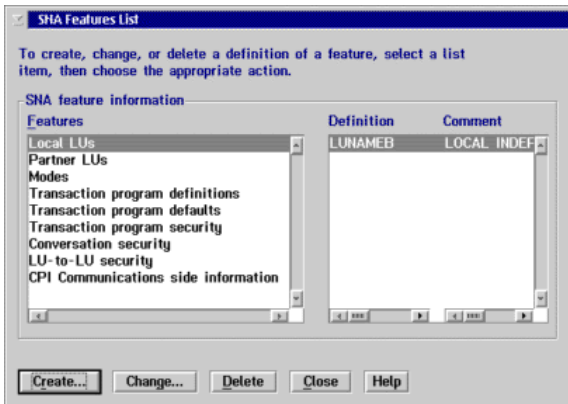
1. En el panel de configuración del Communications Manager List, seleccione la opción de **SNA features**.



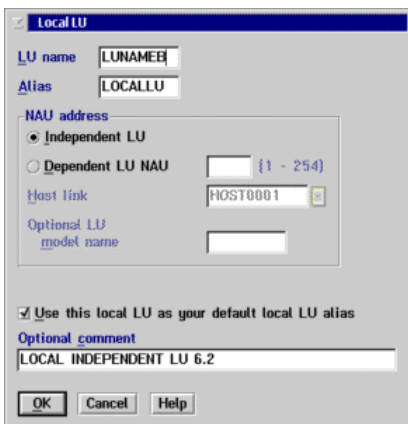
2. Necesita definir una LU (6.2) local independiente por defecto para establecer las conexiones APPC entre la estación servidora y la estación donde reside el repositorio UCM.

Si en su configuración ya posee definida una LU 6.2 local independiente y por defecto, entonces puede, si lo desea, saltar al siguiente paso de la configuración.

Si desea utilizar una LU 6.2 local configurada como que no es la de por defecto, entonces deberá utilizar la variable de entorno de SecureEntry/2 **SGM_FORCE_LUALIAS**, documentada en la **Guía para Administradores de SecureEntry/2**.



3. En este ejemplo, se define la LU LUNAMEB con alias LOCALLU. Recuerde que debe establecer esta LU como su LU 6.2 por defecto.



Su administrador de red deberá proporcionarle el nombre de LU 6.2 que debe utilizar. El alias de esta LU puede establecerlo según su propio criterio.

En la sección de Software adicional de UCM encontrará dos ejemplos de configuraciones de CM/2 para activar una estación servidora y la estación UCM. Estos ejemplos difieren de la configuración propuesta en que se trata de una configuración de CM/2 para establecer una comunicación entre dos **Nodos tipo END node**, sin la intervención de ningún **Network Node**.

4. Añada el Modo de Definición (Mode Definition) con los parámetros estándar. El único requerimiento específico es el Nombre de Modo (Mode name), el cual debe ser APPCHOST.

The screenshot shows the 'Mode Definition' dialog box. The 'Mode name' field is set to 'APPCHOST'. The 'Class of service' is set to '#CONNECT'. The 'Mode session limit' is set to '8'. The 'Minimum contention winners' is set to '0'. The 'Receive pacing window' is set to '4'. The 'Compression' section has 'Compression need' set to 'PROHIBITED', 'PLU->SLU compression level' set to 'NONE', and 'SLU->PLU compression level' set to 'NONE'. The 'RU size' section has 'Default RU size' selected. The 'Optional comment' field contains 'APPC/MVS UCM DEFAULT MODE'. The 'OK', 'Cancel', and 'Help' buttons are at the bottom.

5. El CPI (Communications Side Information) incluye los nombres de LU y los nombres de TP a los que vd. tendrá acceso a través del subsistema de comunicaciones CPI.

UCM requiere que vd. defina el CPI con nombre EDYCCHST. Esta definición contiene todos los datos necesarios para establecer la sesión de comunicaciones entre la estación servidor de perfiles y el TP que reside en la estación Host de UCM.

The screenshot shows the 'CPI Communications Side Information' dialog box. The 'Symbolic destination name' field is set to 'EDYCCHST'. The 'Partner LU' section has 'Fully qualified name' selected, with 'NETID' and 'LUNAME' fields. The 'Partner TP' section has 'Service TP' checked, and the 'IP name' field is set to 'EDYTP'. The 'Security type' section has 'Program' selected. The 'Mode name' dropdown is set to 'APPCHOST'. The 'Optional comment' field contains 'UCM COMMUNICATION CHANNEL CPI'. The 'Continue...', 'Cancel', and 'Help' buttons are at the bottom.

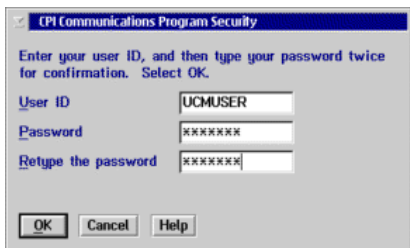
En el ejemplo que se muestra sobre estas líneas, el *Nombre del TP* es EDYTP, el *LOGMODE* utilizado para establecer las características de la sesión es APPCHOST (definido en el punto 4) y la *Partner LU* utilizada es NETID.LUNAME (que es la LU 6.2 por defecto definida en la **Estación de Administración de UCM**) donde NETID es el nombre de la red.

En Security Type debe seleccionar la opción **Program** para que el establecimiento de la sesión de comunicaciones sea autenticado por un usuario y password predefinidos. Para definir el usuario que

debe ser validado en el Host, pulse el botón de **Continue...** y rellene los campos del nuevo diálogo que se le muestra en la pantalla.

Introduzca el mismo UserId que fue definido en el punto 8 de la configuración de la Estación de administración de UCM. Recuerde que tanto el campo UserId como el de Password son *case-sensitive*, y deberán ser tecleados tal y como se definieron en el Host UCM (Estación de administración UCM).

Bajo estas líneas aparece el diálogo de ejemplo para el usuario UCMUSER que fue especificado como el Id de Usuario necesario para autenticar las transacciones entrantes en el TP EDYTP.



Vd. dispone de un ejemplo de configuración de una estación servidora de perfiles en el directorio *SecureEntryPath\INSTALL\UCMOS2*. Puede activar la configuración en una estación siguiendo las instrucciones que encontrará en el capítulo Software adicional de UCM.

Vinculando los programas UCM

SecureEntry/2 distribuye en los diskettes de instalación el software de UCM bajo entorno OS/2. Sin embargo, antes de poderlos utilizar, vd. deberá realizar la vinculación DB2 asociada a estos procesos.

Para ello, SecureEntry/2 distribuye la utilidad BINDUCM.CMD ubicada en el directorio *SecureEntryPath\INSTALL\UCMOS2* encargada de realizar la vinculación de todos los programas DB2 de UCM para OS/2.

La sintaxis de utilización de esta utilidad es la expuesta a continuación:

```
BINDUCM [DBNAME]
```

Donde

DBNAME: Nombre de la Base de Datos de UCM en OS/2. Por defecto 'UCM'

Observe que tras ejecutar esta utilidad, vd. tendrá acceso a UCM a través de la administración de grupos y usuarios UCM.

Recuerde que cada vez que aplique el servicio de mantenimiento de SecureEntry/2 sobre esta máquina, vd. deberá volver a ejecutar el procedimiento de vinculación de los programas UCM.

Iniciando la Base de Datos UCM

En el directorio *\SGMSHELL\INSTALL\UCMOS2*, vd. encontrará la utilidad UCMSETUP.CMD que recoge las sentencias SQL necesarias para inicializar la tabla T_KEYWORD (diccionario de datos) de la Base de Datos UCM con todas las palabras clave por defecto de la versión V4Rx.

La sintaxis de utilización de esta utilidad es la siguiente:

UCMSETUP [NOMBRE_DB]

Donde

NOMBRE_DB: Nombre de la Base de Datos UCM.
'UCM' por defecto.

Adicionalmente, en el directorio \SGMSHELL\INSTALL existe la utilidad EDYKWD.CMD que le permite añadir a la tabla T_KEYWORD todas aquellas definiciones de nuevos componentes de seguridad no provistos originalmente con UCM. Vd. puede diferir la ejecución de esta utilidad al momento en que configure la función de administración de UCM.

Una vez que haya configurado CM/2 y haya inicializado la Base de Datos de UCM, vd. debe ejecutar el proceso **INSTSUB.EXE** ubicado en el directorio \SGMSHELL\INSTALL para añadir en UCM la información básica de subsistemas (SecureEntry/2 y UCM). Una vez ejecutada esta utilidad de forma satisfactoria, estará en disposición de interactuar con UCM.

Planificando la distribución

Para distribuir la información acerca de recursos, grupos y enlaces (links) entre grupos y recursos a los diferentes subsistemas (SecureEntry y LAN Server), UCM para OS/2 ofrece las mismas herramientas de las que ya se disponía en MVS/ESA.

Vd. puede utilizar el método on-line de distribución de datos basado en políticas de refresco, de tal manera que los datos UCM de oficinas sean automáticamente distribuidos a los servidores de oficina. Vd. podrá seleccionar la política de refresco que mejor se adapte a sus requerimientos y expectativas a través de la herramienta interactiva de administración de UCM.

Como alternativa al método de distribución de datos comentado sobre estas líneas, vd. puede utilizar las mismas herramientas batch que ya estaban disponibles en el entorno MVS/ESA. Note, sin embargo, que si vd. utiliza estas utilidades será su responsabilidad el distribuir los paquetes de cambios y ejecutar el proceso adecuado en los servidores de oficina para actualizar esta información.

La utilidad UCMP03 le permitirá recoger una imagen de los datos de oficina almacenados en la Base de Datos de UCM. Esta imagen, puede ser utilizada para inicializar nuevas oficinas con todos los datos necesarios evitando que sean distribuidos de forma online a través del canal de comunicaciones. De esta manera, vd. evitará sobrecargar las líneas de comunicaciones con la imagen completa de la Base de Datos de UCM.

Las utilidades UCMP01 y UCMP02 le permitirán recoger de la Base de Datos de UCM los cambios realizados sobre la imagen de oficina almacenada en UCM.

Resumiendo, vd. puede utilizar los siguientes métodos de distribución de datos de oficina:

Procesos ONLINE de UCM V4Rx

Mediante la herramienta de administración de UCM, vd. puede activar el refresco de información de oficina (Refresco de oficina en línea). A través de esta herramienta puede seleccionar de una lista de posibilidades cuándo desea que los cambios se actualicen en sus oficinas.

El proceso EDYSRV.EXE que se ejecuta en el entorno de LAN, es el encargado de actualizar estos cambios en cada oficina de la corporación.

Si vd. desea tener más información acerca del funcionamiento de este proceso puede leer el capítulo de Actualización en línea de las oficinas en el Manual de administración SecureEntry.

Procesos desasistidos de UCM

UCM le ofrece los procesos UCMP01, UCMP02 y UCMP03 para recoger la información de la Base de Datos UCM. Estos procesos están descritos con todo detalle en Procesos UCM (Gestión Centralizada de Usuarios).

Si vd. utiliza estos procesos, tendrá que diseñar dos planes de distribución de la información:

PLAN1

Ejecute el proceso UCMP03 para recoger toda la información necesaria para crear un objeto que le servirá para inicializar una nueva oficina. Distribuya este objeto a la nueva oficina. Ejecute el proceso desasistido EDYUCDIS.EXE en el servidor de la oficina usando el objeto distribuido como parámetro de entrada al proceso. Este, le inicializará todas las estaciones de la oficina.

PLAN2

Ejecute el proceso UCMP01 o UCMP02 para recoger toda la información modificada para crear un objeto que le servirá para modificar la información de la oficina. Distribuya este objeto a la oficina. Ejecute el proceso desasistido EDYUCDIS.EXE en el servidor de la oficina usando como parámetro de entrada el objeto distribuido. Este, le modificará la información de todas las estaciones de la oficina.

La información acerca de usuarios es distribuida desde el Host a la oficina a través de un canal de comunicaciones UCM. Esta distribución se realiza en ONLINE en tiempo de conexión y desconexión.

Software adicional de UCM

En este capítulo encontrará las referencias a procedimientos de ejecución de programas UCM/2 que SecureEntry/2 instala como ejemplos junto con el Software:

Procedimientos batch de explotación de UCM

Tablas de traducción ASCII/EBCDIC

Ejemplo de configuración de Communications Manager/2

Procedimientos batch de explotación de UCM

A continuación se detalla los procedimientos de explotación/actualización de la Base de Datos de UCM que podrá utilizar como ejemplos para desarrollar los suyos propios:

BATCHUCF.CMD

Utilidad que permite encadenar el programa **EDYUCSRT.EXE** que ordena un Archivo de Cliente junto con la ejecución del programa **UCMPCUSF.EXE**

BATCHLOG.CMD

Ejemplo de utilización del programa EDYEXLOG.EXE para extraer datos de la tabla de anotaciones de UCM.

Vd. puede encontrar estos ejemplos en el directorio *SecureEntryPath\API\UCMOS2*.

Tablas de traducción ASCII/EBCDIC

UCM para OS/2 también le proporciona las tablas de traducción ASCII/EBCDIC *EDYA2E.DAT* y *EBCDIC/ASCII EDYE2A.DAT* que necesitará para configurar/installar un entorno de UCM bajo OS/2 totalmente operacional.

Estas tablas se encuentran en el directorio *SecureEntryPath\INSTALL\UCMOS2* y **deben ser copiadas** en el directorio *SecureEntryPath\INSTALL* tanto en la **estación administradora de UCM** como en los **servidores de perfiles** de las oficinas.

Ejemplo de configuración de Communications Manager/2

En *SecureEntryPath\INSTALL\UCMOS2* encontrará un ejemplo completo de configuración de **Communications Manager/2** para una Estación de administración UCM y para una Estación Servidora en un ambiente de LAN Token Ring a través del adaptador 0.

Estas configuraciones han sido diseñadas para ser activadas en una red propia sin intervención de su administrador de red SNA, estableciendo directamente los canales de comunicaciones e informando a la estación cliente (servidor de oficina) de todos los datos que necesita conocer de la estación servidora (Estación UCM).

UCMHSTWS.RSP

Archivo de respuestas para generar la configuración de la **Estacion de Administración de UCM**. Debe adaptar a su instalación de SecureEntry/2 la siguiente clave:

PARM_STRING

Encontrará esta clave en la sección de definición del TP EDYTP. Esta es la clave de institución que EDYTP necesita para descifrar la información de usuarios en tiempo de conexión. El nombre de institución debe coincidir con el nombre de institución especificado en la instalación de SecureEntry/2.

UCMCLTWS.RSP

Archivo de respuestas para generar la configuración de la **Estación servidora de perfiles**. Vd. deberá adaptar las siguientes claves a los valores de su instalación:

DESTINATION_ADDRESS

Vd. encontrará esta clave en la sección de **LOGICAL_LINK** que es donde se define el LINK **HOSTLINK** desde la Estación servidora de perfiles a la Estación de administración de UCM.

El valor de esta clave debe ser la dirección del Nodo Token Ring de la Estación de Administración UCM.

Desde *SecureEntryPath\INSTALL\UCMOS2* ejecute la utilidad CMSETUP.EXE tal y como se muestra a continuación para generar la configuración de Communications Manager/2 para ambos nodos:

```
CmSetup /r UcmHstWs.Rsp -> En la Estación UCM
```

```
CmSetup /r UcmCltWs.Rsp -> En la Estación servidora de perfiles
```

Note que estos archivos de respuestas han sido generados con **Access Feature versión 5.10**.

Procesos UCM (Gestión Centralizada de Usuarios)

UCM le permite crear y mantener un repositorio corporativo sobre el Host, donde la información consolidada de la corporación es almacenada. La información generada por las actividades de los administradores del sistema así como los cambios que se produzcan en las oficinas es utilizada para modificar el repositorio de la corporación. También puede utilizar su organización de Bases de Datos para alimentar este repositorio. Para poder realizar esto, ha de generar un archivo de cliente. El formato de este archivo de cliente se describe con detalle en Formato del archivo de cliente.

Para alcanzar la meta de una administración segura y una gestión de usuarios a nivel corporativo, UCM implementa una serie de procesos: ONLINE y desasistidos.

Procesos Online

Procesos desasistidos

Procesos Online

Los procesos Online han sido implementados para resolver las siguientes situaciones que pueden implicar una interacción con el repositorio de la corporación. Por ejemplo: cualquier información que pudiera ser necesitada para ser modificada o eliminada, o cualquier información que pudiera ser necesitada para ser recuperada o distribuida.

Cuando el administrador del sistema lleva a cabo las tareas de mantenimiento, se producen cambios sobre el repositorio de la corporación. Estos son directamente realizados desde la estación administradora de UCM mediante el uso de la arquitectura relacional de Bases de Datos distribuidas (DRDA).

Cuando un usuario se conecta a una estación, se desencadena una transacción de autenticación del usuario gestionada por el Software de UCM.

Cuando el subsistema central de seguridad utilizado para la autenticación de usuarios es el RACF (o producto similar), la transacción de autenticación puede ser gestionada o bien a través de un **Service TP del SNA** o a través de **UCM** mediante el programa transaccional EDYURACF.

Sin embargo, cuando vd. utiliza como repositorio central de seguridad para autenticar los usuarios SecureEntry/2 a UCM, el proceso encargado de gestionar las transacciones de autenticación es siempre el programa transaccional EDYTP.

Ambos programas transaccionales de UCM utilizan un método seguro para comunicar los datos de conexión de los usuarios a través del canal de comunicaciones. Cuando los datos son recogidos por los programas transaccionales, se utiliza un algoritmo de descifrado para descifrar los datos.

Cuando un usuario se conecta a una estación, los procesos de UCM buscan los cambios del usuario en el repositorio de la corporación. Si se encuentra algún cambio, los datos del usuario son enviados a la oficina para modificar sus perfiles de usuario antes de que este realice la conexión. Este es un proceso automático que ayuda a definir o modificar dinámicamente la información de los usuarios en las oficinas.

Cuando el administrador del sistema lleva a cabo las tareas de mantenimiento de definiciones de grupos y recursos, se producen cambios en el repositorio de la corporación. Estos cambios pueden ser descargados al entorno de LAN de las oficinas mediante el modo de distribución online. El administrador del sistema puede activar el sistema de Actualización en línea de oficinas tal como se describe en la Guía de administración SecureEntry. Este procedimiento descarga los cambios sobre las definiciones de grupos y recursos desde la Base de Datos Central de UCM al entorno de LAN de las oficinas.

El administrador de sistema puede consultar el nivel de actualización de las oficinas mediante la Aplicación de consulta de oficinas. A través de esta herramienta podrá localizar aquellas oficinas que están teniendo problemas en la actualización de los datos de oficina y aplicar los mecanismos necesarios para corregirlos.

El administrador de sistema puede activar la facilidad de anotación de operaciones de UCM a través de la herramienta de administración SecureEntry. Una vez activada esta facilidad, se almacenan las operaciones de ALTAS, BAJAS y MODIFICACIONES que se realizan contra el subsistema SENT (SecureEntry). Estos datos pueden ser gestionados por el proceso desasistido EDYEXLOG.

Cuando el proceso de Actualización en línea de oficinas falla a causa de una definición errónea en las tablas de cambios, vd. puede ejecutar la herramienta de recuperación EDYRVUCM para corregir el error. Esta herramienta le ayudará a corregir el error en las tablas de cambios de la Base de Datos UCM. Si desea obtener más información acerca de esta herramienta puede leer el capítulo *Herramienta de recuperación UCM* en este manual.

Aplicaciones transaccionales de UCM

UCM provee dos aplicaciones transaccionales para atender en *on-line* las peticiones de las oficinas:

Programa transaccional EDYTP

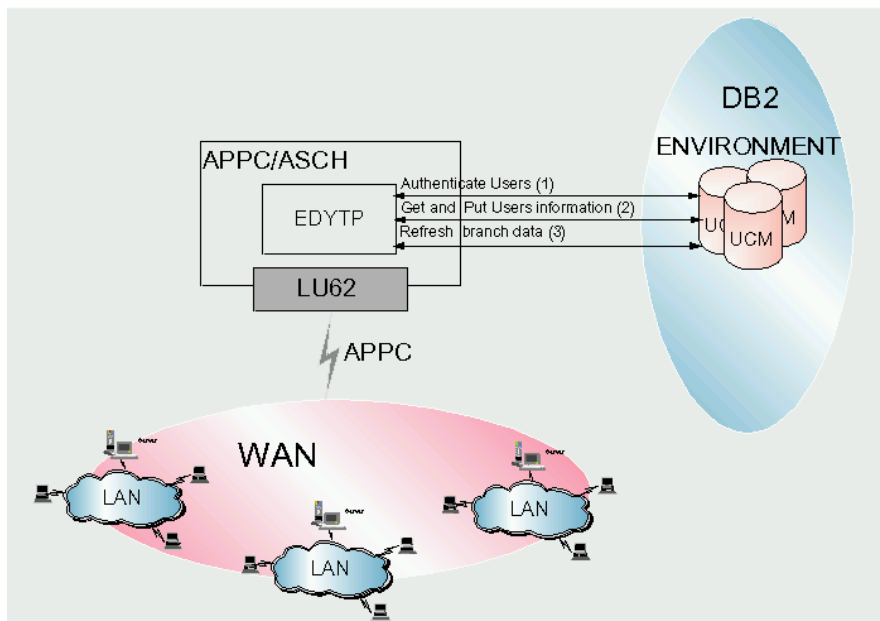
Programa transaccional EDYURACF

Programa transaccional EDYTP

MVS/ESA	OS/2	UNIX
X	X	

EDYTP es el proceso encargado de gestionar las peticiones on-line que se producen en tiempo de conexión de los usuarios. Este programa recoge y actualiza información de usuarios de/en la Base de Datos de UCM cuando es necesitada. Además, el proceso EDYTP es capaz de gestionar información de oficinas, distribuyendo por sus propios medios las definiciones de oficinas a todas sus sucursales.

Bajo estas líneas puede observar una figura que muestra las transacciones básicas que UCM puede gestionar:



El *Transaction Program* EDYTP de UCM aporta las siguientes funcionalidades:

1. Autenticación y validación de usuarios a través del Emulador de RACF

En versiones anteriores, el uso de UCM había estado siempre ligado al uso de la autenticación de usuarios mediante RACF. Ahora puede configurar UCM para que gestione la autenticación de usuarios SecureEntry/2 en tiempo de conexión.

La emulación de RACF se caracteriza por lo siguiente:

- Almacenamiento de passwords en formato cifrado.

- Los datos de conexión de los usuarios viajan cifrados por la línea de comunicaciones.

- Soporte de Passwords con longitud comprendida entre 4 y 14 caracteres alfanuméricos.

- Expiración automática de passwords después de un período de tiempo establecido.

- Límite de reintentos fallidos de logon configurable antes de deshabilitar la cuenta del usuario.

- Sincronización de perfiles de seguridad de los usuarios en tiempo de logon/logoff.

En el momento de conexión de los usuarios se lanza una transacción al Host para actualizar (si es necesario) los perfiles del usuario en la LAN antes de que le sea permitido trabajar en su estación.

EDYTP es el proceso encargado de recoger los perfiles de seguridad asociados a un usuario en el Host y enviarlos (cuando es necesario) a la oficina donde el usuario está realizando la conexión. Cuando llegan nuevos perfiles a la LAN, estos son activados antes de que termine el proceso de logon. Si el usuario no existe, sus definiciones son añadidas en la LAN. Si el usuario ya existe, su definición de LAN es actualizada siempre y cuando sea necesario.

En tiempo de desconexión aquellos perfiles de SecureEntry habilitados para poder ser cambiados por el usuario, y que lo hayan hecho durante una sesión normal de trabajo, son recogidos de la LAN y

enviados a UCM para ser actualizados en la Base de Datos de UCM. El proceso EDYTP recibe estos datos actualizándolos correctamente en la Base de Datos de UCM.

Esta funcionalidad permite la movilidad de usuarios de una oficina a otra. Por tanto, vd. no tiene la necesidad de replicar todas sus bases de datos de usuarios en cada oficina. Como valor añadido, el usuario siempre tendrá la sensación de estar trabajando físicamente en la misma estación.

2. Actualización de imagen única de oficina (Refresco dinámico de datos)

EDYTP es capaz de recoger automáticamente las definiciones de datos de oficinas y distribuirla a todas sus sucursales (oficinas), replicando estos datos como una 'imagen única de oficina'.

La información que compone la imagen única de oficina en la Base de Datos de UCM es la siguiente:

- Subsistemas

- Grupos

- Recursos

- Grupo-recurso, enlaces

- Usuarios a eliminar

- Grupo-grupo, enlaces

- Nivel de las oficinas

A través del *programa transaccional* EDYTP y mediante la selección de una **política de refresco** apropiada (utilizando la herramienta interactiva de gestión de usuarios y grupos), vd. será capaz de activar la distribución on-line de datos de oficina para su corporación de tal manera que la replicación de datos de oficina ocurra en el momento que vd. desee. Las políticas de refresco están completamente documentadas en la *Guía para Administradores de SecureEntry/2*.

Adicionalmente, UCM ofrece un conjunto de procesos desasistidos para extraer de la Base de Datos de UCM toda la información necesaria para ser actualizada en las oficinas de su corporación. Estos procesos construyen la imagen única de oficina y la almacenan en un archivo que debe ser distribuido a todas sus oficinas mediante procesos desasistidos (provistos por su corporación). Este archivo debe ser procesado por un programa SecureEntry/2 (EDYUCDIS.EXE) en entorno LAN con objeto de actualizar las definiciones de oficina. Estos procesos son: UCMP01, UCMP02 y UCMP03. **Estos procesos representan una alternativa para actualizar las definiciones de oficinas sin utilizar la funcionalidad on-line de UCM.**

El proceso transaccional EDYTP puede modificar su comportamiento/rendimiento según los parámetros que se especifiquen en el momento de carga del mismo tal y como se detalla a continuación:

/I:INSTITUTIONNAME

Parámetro de carga para informar al proceso EDYTP del nombre de institución en la cual está siendo ejecutado. Este nombre ha de coincidir con el de instalación del producto **SecureEntry**. Esta información es utilizada en las transacciones de **Emulación de RACF** para descifrar los datos que son utilizados para autenticar la validez de los usuarios en tiempo de conexión.

De no ser especificado, estando configurada en SecureEntry la Emulación de RACF, este dato es leído por el proceso EDYTP del miembro dataset **UCM.Vxx.TABLES(INSTITUT)** en tiempo de ejecución.

/O:nm (Disponible únicamente en MVS)

A través de este parámetro vd. puede activar o desactivar la salida por SYSOUT (Si la tiene redirigida a DUMMY el parámetro no tiene efecto), o la funcionalidad de almacenamiento de datos en el LOG de UCM (**DD UCMLOG**). Tanto *n* como *m* pueden tomar los valores **0** y **1**.

n, indica si se desea salida por SYSOUT.

m, indica si se desea salida por UCMLOG.

Valor **cero** es que no se desea activar esta funcionalidad y **uno** es que se desea la funcionalidad que aporta cada opción.

Por defecto, si no se especifica parámetro de carga ambas opciones quedan deshabilitadas (valor cero).

Note, que si instala UCM bajo entorno OS/2 este parámetro no posee ninguna efectividad. En este caso el proceso EDYTP escribe directamente sobre el registro de rastreo estándar de SecureEntry/2.

En caso de que el TP EDYTP haya sido configurado en modo multi-trans, a pesar de haber desactivado la salida al LOG de UCM, se almacenarán en este (si existe la DD UCMLOG) las estadísticas de utilización del TP y los errores graves.

/C:n (Disponible únicamente en MVS)

Donde n indica el tamaño de la caché primaria. Rango aceptado: 10..100

Cuando el TP EDYTP trabaja en modo multi-trans, reserva un buffer para almacenamiento intermedio de datos el cual contiene datos sobre los cambios pedidos por los diferentes niveles de actualización de sus oficinas. Este parámetro puede ser utilizado para especificar el número de diferentes niveles de información que pueden ser almacenados en este buffer. Incrementarlo, si es necesario, puede mejorar los tiempos de respuesta para las transacciones on-line de distribución de datos, pero también le exigirá una mayor cantidad de recursos de memoria.

Si vd. se encuentra instalando UCM en MVS/ESA, se distribuye el miembro dataset **UCM.Vxx.JCL(DATOS)** como ejemplo de los datos de ejecución del proceso EDYTP. Si usted desea activar cualquiera de los parámetros debe editar el miembro y adecuarlo a sus necesidades. A continuación se muestra un ejemplo donde se pasa como parámetros el nombre de la corporación, se indica que se desea salida a UCMLOG y se amplía la memoria caché:

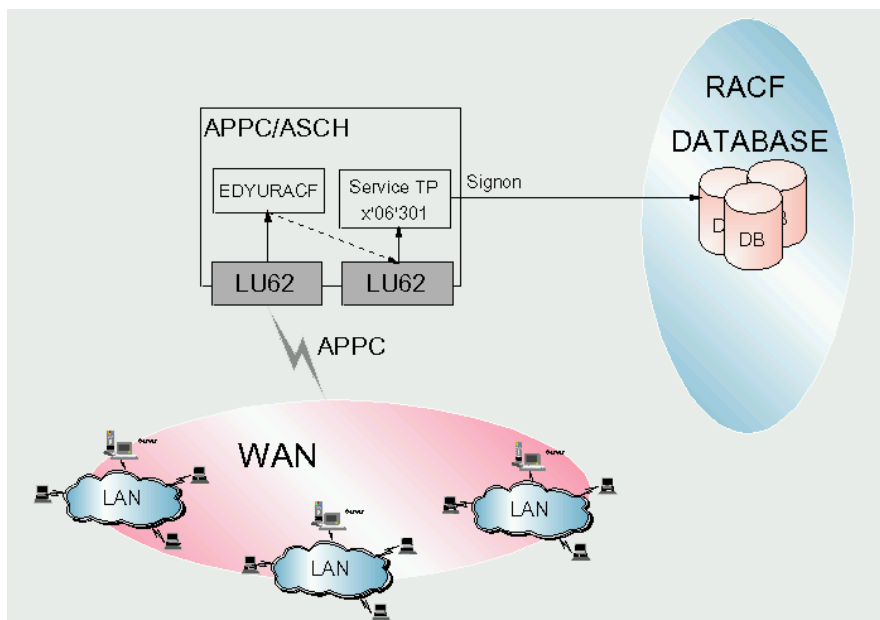
```
DSN SYSTEM(DSN)
RUN PROGRAM (EDYTP) -
  PARMS ('/I:BANCOB' '/O:01' '/C:14') -
  PLAN (PUTGETUS)
END
```

Programa transaccional EDYURACF

MVS/ESA	OS/2	UNIX
X		

En caso de que vd. utilice la funcionalidad de autenticación de passwords de usuarios a través de RACF, y que escoja el cifrado de datos a través del canal de comunicaciones vd. deberá instalar y configurar el *programa transaccional* EDYURACF.

EDYURACF es un proceso APPC/MVS capaz de recibir los datos de conexión de los usuarios, descifrarlos y validarlos contra el RACF tal y como se muestra en la siguiente figura:



Vd. debe configurar la clave que utilizará el proceso transaccional EDYURACF para descifrar los datos que recibe por la línea de comunicaciones. Esta configuración puede ser realizada por parámetro de carga del proceso o a través de la **DD UCMINSTT**:

Parámetros de carga

El programa transaccional EDYURACF puede recibir los siguientes parámetros de carga:

/I:clave_de_descifrado

Mediante la definición de este parámetro, vd. estará informando al proceso EDYURACF de cuál es la clave de descifrado que ha de utilizar para descifrar los datos que son recibidos por la línea de comunicaciones. El valor de esta clave ha de ser el mismo que el utilizado en los servidores de oficinas para cifrar los datos.

/O

Mediante el uso de este parámetro, vd. indica al programa transaccional EDYURACF que inhabilite la salida por SYSOUT (si vd. la tiene redirigida a DUMMY este parámetro no tiene efecto). Habitualmente, la salida por SYSOUT es utilizada para tareas de reconocimiento de problemas (debug).

DD UCMINSTT

Vd. puede utilizar el miembro dataset apuntado por la DD UCMINSTT para definir el valor de la clave de descifrado. En caso de no especificar el parámetro de carga /I, el programa EDYURACF busca la clave *UCMSUBSRACFKEY* = *clave_de_descifrado* en este miembro dataset, y si no la encuentra busca entonces el valor de la clave *INSTITUTION* para utilizarla como clave de descifrado.

Note que en las estaciones servidoras de oficinas vd. deberá definir la clave de cifrado *UCMSUBSRACFKEY* en el archivo **EDYUCFPW.DSC** ubicado en el directorio *SecureEntryPath\INSTALL*. Si vd. no especifica

esta clave, se utilizará el *NOMBRE DE INSTITUCIÓN* especificado en instalación de SecureEntry para cifrar los datos a enviar por el canal de comunicaciones.

Recuerde que las claves de cifrado/descifrado han de ser las mismas en ambos entornos: en el Host y en las estaciones servidoras de oficinas.

Nota!!

Para clientes que ya tuviesen instalado el programa transaccional EDYURACF, pueden especificar como clave de cifrado el valor **V30SCRAMBLING** que obliga al TP EDYURACF a utilizar el método original de descifrado. Este valor ha de ser especificado en la clave **UCMSUBSRACFKEY** tanto en entorno MVS/ESA como en las Estaciones servidoras de las oficinas.

Diríjase a la sección Instalando EDYURACF para obtener más información de los requerimientos y pasos necesarios para instalar este proceso transaccional.

Aplicación de consulta de oficinas

MVS/ESA	OS/2	UNIX
	X	

EDYQRYBR es un programa que le permitirá consultar los niveles de actualización de las oficinas de la corporación y almacenar la consulta en un archivo de salida de información.

Este proceso ha sido diseñado para ser usado por el administrador de sistema. Con EDYQRYBR podrá ver el nivel de actualización de sus oficinas y por tanto identificar las oficinas que pudieran tener problemas de actualización de la información, o verificar que todas están en el nivel correcto.

Nótese que esta es una aplicación que realiza una consulta directa al repositorio central de UCM y extrae los niveles actuales de todas las oficinas pertenecientes a la corporación. El nivel asignado a una oficina depende del método de Actualización en línea de oficinas que esté haciendo servir actualmente en cada servidor de sus oficinas.

Cuando un servidor de una oficina actualiza la información de la oficina obtenida del repositorio central de UCM, descarga todos los cambios habidos sobre la Base de Datos hasta el momento actual, y además refresca el indicador de nivel de la oficina en el repositorio de UCM al valor del anterior nivel al que se encontraba la misma. Una vez que los cambios de la Base de Datos son aplicados correctamente en el servidor de la oficina, el nuevo nivel de esta oficina se reportará al repositorio de UCM en el siguiente intento de actualización de nivel. Entonces, tenemos que el nivel de actualización de las oficinas que sean consultados del repositorio de UCM siempre será menor o igual al nivel de actualización real de las mismas.

La sintaxis para ejecutar el programa es la que se detalla a continuación:

```
EDYQRYBR [COMANDOS:[/R:<rango>] | [/T:<timestamp>]] |  
        [/O:<archivo de salida>]
```

Donde

```
<rango>           : n..m  
<timestamp>      : yyyy-mm-dd-hh.mm.ss  
<archivo de salida>: salida del programa
```

significa

```
rango: n..m: Rango de oficinas a consultar (n <= m)  
timestamp: yyyy-mm-dd-hh.mm.ss  
           año-mes-día-hora.minutos.segundos  
EDYQRYBR consulta oficinas con nivel menor
```

o igual al especificado

- Si no se especifica un comando, EDYQRYBR consulta el nivel de todas las oficinas
- Si el parámetro /O no se especifica, el archivo EDYQRYFL.DAT será utilizado como salida por defecto

El ejemplo que exponemos a continuación consulta el nivel de las oficinas comprendidas en el rango de identificación de la 5 a la 50, y almacena el resultado en el archivo de salida C:\FILES\MYQUERY.DAT:

Sintaxis

```
EDYQRYBR /R:5..50 /O:C:\FILES\MYQUERY.DAT
```

Herramienta de recuperación UCM

MVS/ESA	OS/2	UNIX
	X	

EDYRVUCM es una aplicación que se ejecuta en la máquina administradora de UCM. Esta herramienta le ayudará a compactar y corregir los errores de las tablas de cambios de la Base de Datos UCM.

Cuando vd. añade sobre la Base de Datos una definición incorrecta de un grupo o recurso, esta definición se almacena tanto en las tablas principales como en las tablas de cambios de la Base de Datos. El proceso de actualización en línea de oficinas consulta las tablas de cambios para descargar los cambios en el entorno de LAN de las oficinas. Cuando el proceso EDYSRV intenta actualizar una definición incorrecta en el repositorio de LAN Server, recibe un error que provoca que el nivel de la oficina no sea actualizado al último nivel de la Base de Datos.

La siguiente vez que se activa este proceso de actualización descarga los mismos datos desde la Base de Datos produciéndose otra vez el mismo error.

Si el administrador de sistema corrige el error en la definición del objeto, el error queda eliminado de las tablas principales pero no de las tablas de cambios. Esto se debe a que las tablas de cambios son un repositorio histórico de los cambios que se producen sobre la Base de Datos UCM ordenadas por timestamp. Entonces, en estas tablas tendríamos el alta de la definición errónea y la modificación de esta misma definición para corregir el error.

Con el proceso EDYRVUCM ahora puede eliminar de las tablas de cambios aquellas definiciones que habiéndose realizado erróneamente, se hayan modificado o eliminado para corregir el error.

El mecanismo que vd. debería seguir para determinar y corregir el error que no le permite que sus oficinas alcancen el último nivel de la Base de Datos es el que se describe bajo estas líneas:

1. Primero, ha de determinar qué objeto de la Base de Datos le está causando los problemas: Subsistemas, Grupos, Recursos, enlaces entre Grupos/Recursos o los enlaces entre Grupos/Grupos.

Para hacer esto, vd. puede consultar el archivo EDYADMIN.LOG ubicado dentro del directorio NOUSER en la instalación de SecureEntry, o bien examinando el archivo UCMLOG en el entorno de HOST, donde encontrará el error de la última actualización que realizó su oficina. Recomendamos que examine el primero, puesto que en él encontrará todos los errores que se produjeron en tiempo de actualización de la oficina.

Una vez localizados los errores de LAN Server que provocan que la actualización acabe en error, puede corregirlos mediante la herramienta de administración UCM.

2. Una vez hecho esto, ya puede ejecutar el proceso EDYRVUCM en la estación de administración UCM con los parámetros apropiados. Esto es, con el tipo de objeto que le provoca el error y con el valor límite de comienzo para la corrección de la(s) tabla(s) de cambio(s).

El límite de comienzo, nivel, es el timestamp que el proceso EDYRVUCM utilizará para consultar filas de la Base de Datos con timestamp mayor al especificado. Usted puede especificar dos valores: Nivel mínimo o nivel máximo.

El nivel mínimo provoca que EDYRVUCM comience a corregir los errores para las filas de las tablas de cambios con timestamp mayor que el timestamp de la oficina a menor nivel.

El nivel máximo provoca que EDYRVUCM comience a corregir errores para las filas de las tablas de cambios con timestamp mayor que el timestamp de la oficina a mayor nivel.

Normalmente el error o errores están ubicados en las tablas de cambios con timestamp mayor que la oficina a mayor nivel.

La sintaxis de carga de este programa es la siguiente:

```
EDYRVUCM [</O:objeto> & </L:nivel> & [/T]] | [/H]
```

Donde

/O[BJECT]: Es el tipo de objeto a ser comprimido y corregido por el proceso EDYRVUCM. Le indica la tabla de cambio que ha de procesar.

/L[EVEL]: Es el límite inferior a partir del cual comenzará a corregir filas de las tablas de cambios.

/T[EST]: Es opcional. Fuerza al proceso EDYRVUCM a funcionar en modo test. En este modo no se realiza ninguna acción física sobre las tablas de cambios, únicamente se informa al administrador de las estadísticas de procesamiento en caso de funcionar en modo producción (sin este parámetro). Con este modo es obligatorio especificar los parámetros anteriores.

/H[ELP]: Imprime la pantalla de ayuda del proceso.

Procesos desasistidos

UCM proporciona los siguientes procesos desasistidos para activar el mantenimiento del repositorio de la corporación sobre una base periódica.

Procesos que funcionan en entorno de Host (Host MVS o Host OS/2):

UCMPCUSF.

UCMP01.

UCMP02.

UCMP03.

EDYEXLOG.

EDYQUERY.

EDYUCSRT.

Procesos que funcionan en entorno de LAN:

EDYUCDIS.

UCMPCUSF

MVS/ESA	OS/2	UNIX
X	X	

Este proceso lee el archivo de cliente, el repositorio UCM y modifica este último con la información de salida una vez procesadas las dos entradas. Con este proceso, vd. puede realizar las siguientes operaciones sobre la Base de Datos de UCM:

ADD

La información que contiene el archivo de cliente que no esté presente en el repositorio UCM es añadida a la Base de Datos. El parámetro de procesamiento para este tipo de operación es **A**.

MODIFY

La información que contiene el archivo de cliente que exista en el repositorio de UCM, pero que tenga un valor diferente, es modificada con los valores encontrados en el archivo de cliente. El parámetro de procesamiento para este tipo de operación es **M**.

DELETE

La información que contiene el repositorio de UCM que no está presente en el archivo de cliente, es eliminada de la Base de Datos. El parámetro de procesamiento para este tipo de operación es **D**.

FORCE

Si la operación de DELETE ha eliminado más del 10 por ciento de los usuarios de la Base de Datos, realiza un ROLLBACK para dar marcha atrás a los cambios. Si usted desea eliminar todos estos usuarios, debe utilizar el parámetro FORCE. El parámetro de procesamiento para esta operación es **D F**.

La columna USERID en el archivo de cliente debe estar ordenada ascendentemente. Además, sin alterar esta ordenación, la columna de SUBSISTEMA debe estar ordenada descendentemente.

Este es un ejemplo del correspondiente JCL. Se distribuye como un miembro data set en

UCM.Vxx.JCL(UCMPCUSF):

```
//STEPSORT EXEC PGM=ICEMAN
//SYSOUT DD SYSOUT=*
//SORTIN DD DSN=UCM.CUSTOMER.FILE,DISP=SHR
//SORTOUT DD DSN= &&CUST,DISP=(NEW,PASS),UNIT=VIO,
// SPACE=(CYL,(1,1)),DCB=(LRECL=1024,RECFM=FB,BLKSIZE=0)
//SORTWK01 DD UNIT=SYSDA,SPACE=(CYL,(10,10))
//SORTWK02 DD UNIT=SYSDA,SPACE=(CYL,(10,10))
//SYSIN DD*
SORT FIELDS=(1,10,PD,A,11,4,PD,D)
/*
/*=====
/* (DSN COMMAND) CUSTOMER FILE
/*=====
//DB2TSO EXEC PGM=IKJEFT01
//STEPLIB DD DSN=UCM.LOADLIB,DISP=SHR
```

```
//SYSUDUMP DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSTSPRT DD SYSOUT=*
//UCMLOG DD DSN=UCM.UCMLOG,DISP=SHR
//CUSTOMF DD DSN=&&CUSTF,DISP=(OLD,DELETE)
//SYSTSIN DD*
DSN SYSTEM(DSN)
RUN PROGRAM (UCMPCUSF) -
    PARM('A') -
    PLAN (UCMPCUSF)
END
/*
//
```

Si vd., está instalando UCM en plataforma OS/2, el programa UCMPCUSF.EXE distribuido para esta plataforma espera encontrar en su directorio de trabajo un archivo CUSTOMER.SRT ordenado según los criterios mencionados anteriormente. Vd. puede utilizar la utilidad EDYUCSRT.EXE para ordenar el Archivo de Cliente antes de ser enviado a procesar por el proceso UCMPCUSF.

UCMP01

MVS/ESA	OS/2	UNIX
X	X	

Este proceso recoge información acerca de los cambios de la Base de Datos UCM (tablas de cambios).

- Subsistemas
- Grupos
- Recursos
- Grupo-recurso, enlaces
- Usuarios a eliminar
- Grupo-grupo, enlaces
- Nivel de las oficinas

Esta información es almacenada en un archivo binario que debería ser distribuido a las oficinas. El proceso UCMP01 recoge toda la información de las tablas de cambios de la Base de Datos UCM y pone el flag de transmitido a **Yes**. Usted puede utilizar este proceso para modificar la información de una oficina que ha sido previamente instalada y que requiere los últimos cambios (delta de información).

Para ejecutar este proceso, debe especificar el parámetro de borrado forzado (Force_Delete). Este parámetro puede tener uno de los siguientes valores:

Force_Delete=Y

La información procesada y transmitida será eliminada de la tablas de cambios.

Force_Delete=N

La información no será eliminada.

Este es un ejemplo del JCL correspondiente. Se distribuye como un miembro data set en **UCM.Vxx.JCL(UCMP01)**:

```
//DB2TSO EXEC PGM=IKJEFT01
//STEPLIB DD DSN=UCM.LOADLIB,DISP=SHR
```

```
//SYSUDUMP DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSTSPRT DD SYSOUT=*
//FILH2LAN DD DSN=UCM.DELTAH2L,DISP=OLD
//SYSTSIN DD*
DSN SYSTEM(DSN)
RUN PROGRAM (UCMP01)-
  PLAN (UCMP01)-
  PARM ( 'N' )
END
/*
```

Bajo entorno OS/2 el proceso crea un archivo con nombre DELTAH2L.BIN en el directorio de ejecución del proceso.

UCMP02

MVS/ESA	OS/2	UNIX
X	X	

Este proceso recoge la información acerca de los cambios de la Base de Datos UCM (tablas de cambios).

- Subsistemas
- Grupos
- Recursos
- Grupo-recurso, enlaces
- Usuarios a eliminar
- Grupo-grupo, enlaces
- Nivel de las oficinas

Esta información es almacenada en un archivo binario que debería ser distribuido a las oficinas. El proceso UCMP02 recoge toda la información de las tablas de cambios de la Base de Datos de UCM, incluso la que ya ha sido transmitida y construye un archivo con todos los cambios. Usted puede utilizar este proceso para actualizar la información de una oficina que haya sido previamente instalada y que requiera todos los cambios (n delta de información).

Este proceso no necesita parámetros para ser ejecutado.

Este es un ejemplo del JCL correspondiente. Se distribuye en el miembro data set **UCM.Vxx.JCL(UCMP02):**

```
//DB2TSO EXEC PGM=IKJEFT01
//STEPLIB DD DSN=UCM.LOADLIB,DISP=SHR
//SYSUDUMP DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSTSPRT DD SYSOUT=*
//FILH2LAN DD DSN=UCM.DELTAH2L,DISP=OLD
//SYSTSIN DD*
DSN SYSTEM(DSN)
RUN PROGRAM (UCMP02)-
  PLAN (UCMP02)
END
/*
```

Bajo entorno OS/2 el proceso crea un archivo con nombre DELTAH2L.BIN en el directorio de ejecución del proceso.

UCMP03

MVS/ESA	OS/2	UNIX
X	X	

Este proceso genera una imagen de los datos de oficina recogiendo la información necesaria para inicializar las oficinas. Esta imagen es almacenada en una archivo binario.

El proceso actúa sobre las tablas principales de UCM recogiendo la información de:

- Subsistemas
- Grupos
- Recursos
- Grupo-recurso, enlaces
- Grupo-grupo, enlaces
- Nivel de las oficinas

Este archivo puede ser utilizado para inicializar una nueva oficina a través del programa *EDYUCDIS.EXE*.

Este proceso no necesita parámetros para ser ejecutado.

Bajo entorno OS/2, el proceso genera un archivo con nombre *FILH2LAN.BIN* ubicado en el directorio de ejecución del programa.

Para aquellos clientes que instalen UCM bajo entorno MVS/ESA, este es un ejemplo del JCL correspondiente. Se distribuye en el miembro data set **UCM.Vxx.JCL(UCMP03)**:

```
//DB2TSO EXEC PGM=IKJEFT01
//STEPLIB DD DSN=UCM.LOADLIB,DISP=SHR
//SYSUDUMP DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSTSPRT DD SYSOUT=*
//FILH2LAN DD DSN=UCM.FILH2LAN,DISP=OLD
//SYSTSIN DD*
DSN SYSTEM(DSN)
RUN PROGRAM (UCMP03)-
PLAN (UCMP03)
END
/*
```

EDYEXLOG

MVS/ESA	OS/2	UNIX
X	X	

Este proceso recoge información de la tabla de anotación de UCM. Esta tabla contiene información acerca de las operaciones de altas, bajas y modificaciones ejecutadas sobre el subsistema SENT (SecureEntry). Las operaciones anotadas aquí se encuentran descritas en las siguientes líneas:

```

ADD      -> Operaciones de altas
UPDATE   -> Operaciones de modificaciones
DELETE   -> Operaciones de bajas

```

Esta información se almacena en un archivo de texto que puede ser gestionado por el cliente. Usted podría utilizar este proceso para conocer las operaciones ejecutadas sobre la Base de Datos UCM. Cada línea del archivo describe una operación y los objetos implicados en la misma.

EDYEXLOG extrae de la Base de Datos de UCM las anotaciones en el orden en que las encuentra en la tabla de anotaciones de UCM. Si vd. desea que la salida del proceso sea un archivo ordenado por el timestamp de las operaciones, debe indicarlo por argumento de carga del proceso. EDYEXLOG acepta el parámetro de carga /S:<Y|N> donde:

```

/S:Y -> Salida ordenada por timestamp
/S:N -> Salida no ordenada. (Defecto)

```

Si vd. desea ordenar la salida por timestamp de las operaciones, debe tener en cuenta que el consumo de recursos de memoria crecerá rápidamente dependiendo del volumen de datos a procesar.

El proceso EDYEXLOG lee un archivo de parámetros **DD:PARAMS**. Cada registro de este archivo determina una operación a ser ejecutada por el proceso EDYEXLOG. La sintaxis del archivo **DD:PARAMS** se encuentra descrita bajo estas líneas:

```

[EXTRACT:<operación> [OBJECT:<tipoobjeto>]] | [DELETE] |
[PURGE] | [ROWSPROCESSED:<YES|NO>]

```

Donde

- EXTRACT:<operación> [OBJECT:<tipoobjeto>]
Información a ser extraída de la Base de Datos UCM y almacenada en el archivo de salida del proceso. El tipo de objeto a ser extraído es un parámetro opcional en esta línea.
- DELETE
EDYEXLOG eliminará todas las filas procesadas de la tabla de anotaciones de UCM.
- PURGE
EDYEXLOG eliminará todas las filas de la tabla de anotaciones de UCM que se encuentren por debajo del valor límite de proceso encontrado al inicializar el procedimiento.
- ROWSPROCESSED
EDYEXLOG extraerá de la tabla de anotaciones todas las filas procesadas en ejecuciones anteriores si vd. indica el valor YES. Vd. puede activar/desactivar la funcionalidad según le convenga. Por defecto, EDYEXLOG asume el valor NO.

Cuando EDYEXLOG arranca, guarda el timestamp mayor de la tabla de anotaciones. Este valor se utilizará como el valor límite para todas las operaciones de extracción de información que a partir de ese momento se realicen. La salida del proceso EDYEXLOG se almacenará en el archivo apuntado por la **DD:SEQLOG**.

El proceso EDYEXLOG almacena aquellos registros que coinciden con el criterio de búsqueda especificado en el archivo apuntado por la **DD:SEQLOG** con el siguiente formato por cada registro:

Offset	Longitud	Descripción	Valores
0	1	Tipo operación	'A'->ADD, 'U'->UPDATE, 'D'->DELETE

1	2	Tipo objeto	'U'->USER, 'G'->GROUP, 'R'->RESOURCE, 'UG'->USERGROUP, 'RU'->RESOURCEUSER, 'RG'->RESOURCEGROUP, 'GG'->GROUPGROUP
3	20	Identificador de objeto	Valor dependiente de la operación
23	20	Identificador de objeto	Valor dependiente de la operación
43	26	Timestamp operación	Timestamp del momento en que produjo la operación

Si vd. se encuentra instalando UCM para OS/2, el proceso EDYEXLOG espera encontrar el archivo de parámetros **PARAMS.OPR** en el directorio de ejecución. Una vez procesadas las instrucciones de extracción de datos, EDYEXLOG genera en el mismo directorio el archivo de salida **SEQLOG.OUT**.

Ejemplos de uso:

Bajo estas líneas tenemos dos ejemplos del archivo apuntado por la DD:PARAMS, que también pueden ser aplicados para aquellos clientes que instalen UCM bajo entorno OS/2.

En este primer ejemplo, extraemos todas las operaciones de la tabla de anotaciones del tipo de objeto *Usuario*. Una vez hecho esto, todas las filas de esta tabla con el timestamp menor que el valor límite que encuentre al iniciar el proceso serán eliminadas:

```
EXTRACT:ALL OBJECT:U
PURGE
```

El mismo ejemplo, pero realizando la extracción operación a operación:

```
EXTRACT:ADD OBJECT:U
EXTRACT:UPDATE OBJECT:U
EXTRACT:DELETE OBJECT:U
PURGE
```

En este segundo ejemplo, extraemos todas las operaciones de Alta realizadas sobre los tipos objeto: *Usuario*, *Grupo*, y *enlaces Usuario/Grupo*. Se desea extraer de la Base de Datos de UCM todas las operaciones de Altas de Usuarios a pesar de haber sido tratadas anteriormente. Todas las filas que se procesen serán eliminadas de la tabla de anotaciones:

```
ROWSPROCESSED:YES
EXTRACT:ADD OBJECT:U
ROWSPROCESSED:NO
EXTRACT:ADD OBJECT:G
EXTRACT:ADD OBJECT:USERG
DELETE
```

Para instalaciones en MVS/ESA, se muestra, también, un ejemplo del JCL correspondiente. Este es distribuido como miembro data set en **UCM.Vxx.JCL(EDYEXLOG)**:

```
//DB2TSO EXEC PGM=IKJEFT01
//STEPLIB DD DSN=UCM.LOADLIB,DISP=SHR
// DD DSN=DSN230.DSNLOAD,DISP=SHR
// DD DSN=SYS1.EDC.V2R2M0.SEDCLINK,DISP=SHR
// DD DSN=SYS1.PLI.V2R3M0.SIBMLINK,DISP=SHR
//SYSUDUMP DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSTSPT DD SYSOUT=*
```

```
//PARAMS DD DSN=UCM.EDYEXLOG.PARAMS,DISP=OLD
//UCMLOG DD DSN=UCM.UCMLOG,DISP=OLD
//SEQLOG DD DSN=UCM.SEQLOG,DISP=OLD
//SYSTSIN DD *
DSN SYSTEM(DSN)
RUN PROGRAM (EDYEXLOG) -
PLAN (EDYEXLOG)
END
/*
```

EDYQUERY

MVS/ESA	OS/2	UNIX
X		

Este proceso consulta el valor de una palabra clave de la Base de Datos de UCM para un objeto dado y lo almacena en el archivo apuntado por la DD:UCMQUERY, o lo muestra por la salida estándar del sistema.

Aquellos clientes que posean instalado UCM bajo entorno OS/2, pueden encontrar la funcionalidad que ofrece este programa en la herramienta de administración batch de SecureEntry/2.

Cuando sea necesario, EDYQUERY puede realizar una traducción de ASCII a EBCDIC utilizando la tabla de traducción por defecto del UCM, o utilizando una tabla de traducción opcional provista por el cliente.

Sintaxis

Para ejecutar EDYQUERY, es necesario especificar el tipo de objeto y el identificador de la palabra clave que se desea consultar en el siguiente formato:

```
PARM('tipoobjeto=objetoID [Subsistema.]palabraclave /C') -
```

Donde

```
tipoobjeto: User | USERGroup | Group | GROUPGroup |
Resource | RESOURCEGroup | RESOURCEUser

[Subsistema.]palabraclave: Identificador de la palabra clave
                             Puede ir precedido del subsistema de referencia

/C: Realiza una traducción de la salida de ASCII a
    EBCDIC.
```

Ejemplos de uso:

```
PARM('G=SGCAS01 TREE_LOCK /C') -
PARM('U=USER0112 UCM.BRANCH') -
```

A continuación se muestra un ejemplo del JCL correspondiente. Este se distribuye como miembro data set en UCM.Vxx.JCL(EDYQUERY):

```
//UCMQUERY JOB (0),'RUN',CLASS=A,MSGCLASS=X,MSGLEVEL=(1,1),
//          USER=UCMUSR
//*****
//* Sample JCL to run EDYQUERY (DB2)                                UCM V4Rx *
//*                                                                           *
//* Si el miembro data set EDYA2E no existe, EDYQUERY utilizará        *
//* la tabla de traducción por defecto de ASCII a EBCDIC                *
//* de UCM.                                                              *
//*****
//DB2TSO    EXEC PGM=IKJEFT01
//STEPLIB   DD DSN=UCM.Vxx.LOADLIB,DISP=SHR
//          DD DSN=SYS1.DSN310.SDSNLOAD,DISP=SHR
```

```
//          DD DSN=EDC220.SEDCLINK,DISP=SHR
//          DD DSN=PLI230.SIBMLINK,DISP=SHR
//SYSUDUMP DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSTSPRT DD SYSOUT=*
//EDYA2E   DD DSN=UCM.Vxx.TABLES(EDYA2E),DISP=SHR
//UCMQUERY DD DSN=UCM.UCMQUERY,DISP=OLD
//UCMLOG   DD DSN=UCM.UCMLOG,DISP=OLD
//SYSTSIN  DD *
DSN SYSTEM(DSN)
RUN PROGRAM (EDYQUERY) -
      PARM('G=SGCAS01 TREE_LOCK /C') -
      PLAN (EDYQUERY)
END
/*
//
```

El miembro data set **EDYA2E** es la tabla opcional de traducción de ASCII a EBCDIC. Si existe, anula la tabla por defecto que posee el UCM codificada en este módulo. Para una descripción del formato de la tabla opcional de traducción diríjase al capítulo de Tabla de Traducción.

EDYUCDIS

MVS/ESA	OS/2	UNIX
	X	

EDYUCDIS es un programa que lee el archivo creado en el entorno de Host por los procesos UCMP01, UCMP02 o UCMP03 y actualiza en el servidor de la oficina la información siguiente:

- Alias de LAN Server
- Asignaciones en conexión
- Grupos (SecureEntry y LAN Server)
- Componentes de Seguridad
- Nivel de la oficina
- ...

Si vd. arranca este programa sin parámetros, obtendrá la ayuda Online. Utilice la siguiente sintaxis para ejecutar el programa:

Vía de acceso EDYUCDIS Vía de acceso nombreobjeto nivel_de_mensajes

La sentencia siguiente es un ejemplo de uso del programa EDYUCDIS:

```
C:\SGMSHELL\EXEC\EDYUCDIS.EXE C:\DISTRIBU\FILEH2L.BIN 0
```

EDYUCDIS ha sido modificado para actualizar el nivel de las oficinas. Si vd. activa el procedimiento de actualización en línea de oficinas después de haber ejecutado este proceso, únicamente se descargarán del repositorio central de UCM los últimos cambios realizados sobre la Base de Datos.

EDYUCSRT

MVS/ESA	OS/2	UNIX
	X	

EDYUCSRT es una utilidad orientada a aquellos clientes que instalen UCM bajo entorno OS/2.

Este programa recibe como entrada un archivo de cliente creado por la corporación y genera como salida un archivo de cliente ordenado que puede ser utilizado como entrada del programa UCMPCUSF.

Si vd. arranca este programa sin parámetros obtendrá la ayuda Online. Utilice la siguiente sintaxis para ejecutar el programa:

```
Vía de acceso EDYUCSRT /I:Archivo de entrada /O:Archivo de salida
```

Note, que si no especifica un archivo de salida, el programa crea el archivo de salida *CUSTOMER.SRT* en el directorio desde el cual se ejecuta la utilidad.

Adicionalmente, el programa UCMPCUSF espera encontrar un archivo *CUSTOMER.SRT* en el directorio desde el cual es ejecutado.

La sentencia siguiente es un ejemplo de uso del programa EDYUCSRT:

```
C:\SGMSHELL\EXEC\EDYUCSRT /I:C:\DATA\CUSTOMER.BIN
```

En este ejemplo, el programa recibe un archivo de cliente desordenado y como salida crea el archivo de cliente *CUSTOMER.SRT* ordenado y que ya puede ser utilizado como entrada del programa UCMPCUSF.

Transacciones multi-trans

Si vd. ha instalado y configurado un UCM operacional bajo plataforma OS/2 puede omitir la lectura de este capítulo.

Vd. puede configurar las aplicaciones transaccionales de UCM como procesos APPC multi-trans.

Dependiendo de la carga de transacciones que deba soportar su Sistema en las horas punta de conexión de sus usuarios, puede interesarle esta opción de funcionamiento de los TP's de UCM.

Se recomienda el uso de la configuración multi-trans en aquellas instalaciones que cumplan las siguientes características:

- Número de usuarios elevado (>3000).

- Intervalo de conexión de usuarios se encuentra en una estrecha franja horaria (aprox. 30 minutos).

- Problemas de carga de CPU en la instalación.

En modalidad estándar el proceso es cargado por el ASCH en cada transacción que se recibe de las oficinas. Una vez que la transacción APPC es procesada, el programa transaccional retorna la respuesta al cliente y se descarga de memoria.

Las transacciones en línea de UCM (las de conexión y desconexión) son transacciones ligeras con lo que la mayor parte del consumo de CPU se gasta en la carga y descarga de este proceso, así como en la adquisición de los recursos que necesita para funcionar.

Si usted configura el proceso transaccional para funcionar en modalidad multi-trans, éste modificará su comportamiento de la siguiente forma:

- La primera transacción que llega al APPC provoca la carga en memoria y adquisición de los recursos de ejecución necesarios para el proceso transaccional. Una vez procesada la primera transacción, se retorna la respuesta al peticionario y el proceso permanece en memoria a la espera de nuevas transacciones entrantes.

- Las transacciones siguientes encuentran el proceso transaccional cargado en memoria con lo que el APPC/ASCH únicamente ha de comunicarle la transacción entrante. El proceso procesa la transacción y retorna la respuesta al peticionario (cliente).

- Este comportamiento no requiere el ciclo de carga y descarga del proceso transaccional, con lo que se economizan los recursos que de otra forma se dedicarían a estas tareas. Este ahorro de recursos impacta notablemente en un aumento de la velocidad de tratamiento de las transacciones.

- El proceso transaccional es automáticamente descargado de memoria por el APPC después de un intervalo fijo de tiempo en el que no recibe más transacciones (aproximadamente 5 minutos).

- En modalidad multi-trans, el consumo de CPU por transacción disminuye drásticamente en las horas punta de conexión de sus usuarios comparándolo con el mismo proceso funcionando en modalidad estándar.

Como ejemplo de las mejoras de rendimiento de los procesos transaccionales en modo multi-trans tenemos que para una instalación con 3500 usuarios se obtiene que el consumo medio de CPU representa aproximadamente el 5% (en conexiones/desconexiones de usuarios) del que se produciría si estuviese funcionando en modalidad transaccional estándar.

En caso de que el proceso transaccional EDYTP sea configurado en este modo de ejecución se activarán, si vd. lo desea, diversas mejoras de rendimiento pensadas para cuando está funcionando en modo multi-trans como son:

Caché de datos para refresco dinámico de oficinas

Estadísticas de utilización de las diversas transacciones del proceso

Consulte los parámetros de carga del proceso EDYTP para obtener más información.

Al igual que el proceso EDYTP, el TP EDYURACF puede ser configurado en modo multi-trans aumentando considerablemente su rendimiento.

El hecho de configurar un proceso transaccional del APPC como un proceso multi-trans, debería ser consecuencia del resultado de un estudio previo de la carga de su Sistema para poder identificar las causas que le motivan a realizar este cambio en la configuración de su Sistema.

La configuración por defecto que UCM presenta como ejemplo para sus clientes es una instalación y configuración de los procesos transaccionales en el APPC de HOST como TP's estándar. Si usted desea que en su instalación estos procesos funcionen en modo multi-trans, ha de cambiar la configuración de los perfiles de los TP's.

Para cambiar la configuración de los procesos transaccionales a modalidad multi-trans, lea detenidamente la sección de Configuración multi-trans

Configuración multi-trans

Vd. puede configurar el los *transactions programs* **EDYTP** y **EDYURACF** para que funcionen en modalidad multi-trans tal y como se detalla a continuación:

Definición de un usuario RACF con suficientes privilegios para poder ejecutar el proceso EDYTP/EDYURACF. Este usuario será el encargado de proporcionar el entorno de seguridad que necesita el *caparazón* (shell) multi-trans. De hecho, el usuario que vd. debe definir puede ser el mismo usuario que utilizó para autenticar el canal de comunicaciones UCM entre las estaciones servidoras y el APPC/MVS tal y como fue descrito en los puntos 8 y 9 de la configuración del Communications Manager/2 en la Estación administradora de UCM.

Usted, ha de definir que el proceso EDYTP/EDYURACF es un proceso multi-trans y el usuario que proporciona el entorno de seguridad en el perfil del TP EDYTP/EDYURACF en el APPC.

Para ello puede utilizar el programa utilidad ATBSDFMU con la clave TPMODIFY para modificar la definición del TP. Vd. debe modificar los siguientes valores:

Cambiar de TPSCHED_TYPE(STANDARD) a TPSCHED_TYPE(MULTI_TRANS)

Añadir GENERIC_ID(UCMUSER).

Opcionalmente, si usted configura el EDYTP como un proceso multi-trans, le sugerimos que utilice una clase de ejecución de APPC específica. Los parámetros de configuración de la clase de ejecución válidos en modalidad estándar siguen siendo válidos en modalidad multi-trans. Por tanto, usted puede especificar el número de iniciadores de APPC mínimos/máximos para el EDYTP, como los objetivos de tiempo de respuesta para las transacciones de UCM.

Formato del archivo de cliente

El archivo que ha de crear con la información de sus Bases de Datos existentes ha de seguir el formato que se detalla en este capítulo:

El archivo de cliente es una Base de Datos secuencial que tiene el siguiente DSORG:

FB,LRECL=1024,BLKSIZE=0 (bloques secuenciales de 1024 bytes en el caso de OS/2). Los registros de la Base de Datos están compuestos por las siguientes columnas:

UsuarioID

Nombre de Usuario. Esta columna tiene una longitud de 10 caracteres.

SubsistemaID

Identificador de Subsistema. El subsistema debe ser previamente definido en la Base de Datos UCM. Esta columna tiene una longitud de 4 caracteres. Los subsistemas actualmente disponibles son:

SENT (SecureEntry)

UCM (Gestión Centralizada de Usuarios)

GrupoID

Grupo al que pertenece el usuario en el subsistema especificado. El grupo debe haber sido previamente definido en la Base de Datos UCM. Esta columna tiene una longitud de 10 caracteres.

RecursoID

Identificador de Recurso. El recurso debe haber sido previamente definido en la Base de Datos UCM. Esta columna tiene una longitud de 20 caracteres.

Keyword

Cada subsistema requiere sus propias palabras clave (keywords). Esta columna tiene una longitud de 20 caracteres.

TipoValor

Los tipos de valores posibles son los siguientes:

E (Valor en formato EBCDIC)

A (Valor en formato ASCII)

B (Valor en formato Binario)

Esta columna tiene una longitud de 1 carácter.

Longitud

Es un Short que representa la longitud del dato. Esta columna tiene una longitud de 2 caracteres.

Valor

Valor de la palabra clave (keyword). Esta columna puede tener hasta una longitud máxima de 954 caracteres.

Cada subsistema de seguridad soportado por SecureEntry/2 y UCM necesitan que sea definida cierta información para cada usuario UCM:

Información requerida para la palabra clave (keyword) de subsistema

Información requerida para la palabra clave (keyword) de subsistema

Esta sección muestra qué palabras clave (keywords) han de ser especificadas para cada uno de los subsistemas soportados (UCM y SecureEntry), y cómo especificarlas.

Información requerida para la palabra clave (keyword) de UCM

Información requerida para la palabra clave (keyword) de SecureEntry

UCM

La única palabra clave (keyword) requerida para el subsistema UCM es BRANCH. Su valor asigna un usuario a una oficina.

UserId	SubsistemaId	GrupoId	RecursoId	Keyword	TipoValor	Longitud	Valor
U12345678	UCM	NULL	NULL	BRANCH	E	8	filial1
U00000001	UCM	NULL	NULL	BRANCH	E	8	filial2

Cada usuario que defina en la Base de Datos de UCM ha de tener especificada esta palabra clave (keyword) obligatoriamente. Vd. puede utilizar este dato en sus oficinas para eliminar de una oficina en concreto todos aquellos usuarios que no pertenezcan a la misma.

A través del proceso EDYERASE.CMD documentada en el manual para Administradores de SecureEntry/2, vd. podrá eliminar las definiciones no deseadas de cada oficina de su corporación.

SecureEntry

En el subsistema SecureEntry, vd. puede suministrar información para el LAN Server a través de la palabra clave (keyword) LAN_DATA. Esta keyword puede tener las siguientes sub-keywords:

Sub-keyword	Valores permitidos	Defecto
PASSWORD	Una contraseña válida	No contraseña
PRIV_USER	GUEST, USER, and ADMIN	USER
HOME_DIR	Directorio	No Directorio
MAX_STORAGE	Número de KB (-1 para ilimitado)	-1
DESCRIPTION	Una cadena de texto de hasta 48 caracteres	Vacío
CONNECTION	0, 1	1 (permitida)
SCRIPT_PATH	Nombre del archivo script	Ninguno
FULL_NAME	Una cadena de texto de hasta 48 caracteres	Vacio
USER_EXPIRE	dd-mm-yyyy o NEVER	NEVER
HOURL_START	[0-23]	0
HOURL_END	[1-24]	24

Para obtener información adicional acerca de estas LAN_DATA sub-keywords, dirjase al manual de administración de LAN Server 4.0.

UsuarioId	SubsistemaId	GrupoId	RecursoId	Keyword	TipoValor	Longitud	Valor
U12345678	SENT	NULL	NULL	LAN_DATA	E	hex 7EH	Sub-keywords
U12345678	SENT	Group1	NULL	NULL	NULL	NULL	NULL
U12345678	SENT	Group2	NULL	NULL	NULL	NULL	NULL

Donde Sub-keywords son:

```

HOUR_START=8\0
HOUR_END=20\0
PRIV_USER=USER\0
FULL_NAME=John Smith\0
CONNECTION=0\0
USER_EXPIRE=31-12-2000\0
DESCRIPTION=Cualquier texto\0

```

La sintaxis para las sub-keywords especificadas es la siguiente:

```
KEYWORD=valor\0
```

Si vd. no especifica una sub-keyword, se asume el valor por defecto.

En el archivo de cliente, NULL o \0 representan ceros binarios. El campo Longitud debe ser la suma de la longitud del valor, los campos separadores (Valor NULL), y dos caracteres NULL después del último carácter.

Guía de determinación de problemas UCM

El acceso a la Base de Datos UCM puede retornar los siguientes mensajes, que también pueden ser visualizados cuando utilice la aplicación de administración en la estación de UCM o como entradas en el archivo UCMLOG en el entorno MVS.

Código	Descripción	Acción de Usuario
UCAP 0I: Retorno OK.	Código de retorno OK.	Nada requerido.
UCAP 1I: (info_string)	Cadena informativa.	Nada requerido.
UCAP 2W: keyword (objeto) tiene un tamaño no válido.	Se ha intentado realizar una operación de modificación en la que no se han especificado palabras clave (keywords).	Repita la operación especificando una o más keywords a ser modificadas.
UCAP 3E: Tipo de objeto no válido: (objeto)	Se ha intentado realizar una operación con un tipo de objeto no válido.	Reintente con un tipo de objeto válido.
UCAP 4E: Operación no válida: (operación)	Se ha intentado una operación no válida.	Reintente con un tipo de operación válida.
UCAP 5W: Parámetros incorrectos: (parámetros)	Se ha intentado una operación con parámetros incorrectos.	Corrija los parámetros y reintente.
UCAP 6E: Objeto (objeto) ya existe.	Se ha realizado una operación de Alta de un objeto que ya existe.	Corrija la operación.
UCAP 7E: Objeto (objeto) no existe.	Una operación que requiere un objeto, y no lo ha encontrado.	Cree el objeto o cambie la operación.
UCAP 8E: Keywords obligatorias esperadas: (keywords).	Faltan las palabras clave (keywords) obligatorias en la operación demandada.	Corrija la operación.
UCAP 9E: Keywords no esperadas: (keywords).	Keywords (palabras clave) encontradas en la operación no eran esperadas.	Corrija la operación.
UCAP 10E: Keyword (keyword) no existe.	Una operación que requiere una palabra clave (keyword) que no ha sido encontrada.	Corrija la operación.
UCAP 11E: Keyword (keyword) existe.	Una palabra clave (keyword) que ya existe.	Corrija la operación.
UCAP 12E: Keyword (keyword) es incorrecta.	Una palabra clave (keyword) de la operación ha sido dada como incorrecta.	Corrija la operación.
UCAP 13E: No están todas las keywords del (objeto)	Faltan palabras clave (keywords) en la operación.	Corrija la operación.
UCAP 14I: Demasiadas filas seleccionadas. Número de filas: (filas).	Demasiada información ha sido consultada.	Concrete la operación de consulta.
UCAP 15I: No hay filas seleccionadas en el (objeto)	No hay información disponible de este objeto.	Nada requerido.
UCAP 16E: Eliminación del	La eliminación del usuario	Cambie la operación.

usuario en el (subsistema) subsistema no permitida.	requerido en un subsistema ha sido intentado.	
UCAP 17E: Eliminación del subsistema (subsistema) no permitida.	Se ha intentado eliminar un subsistema.	Cambie la operación.
UCAP 18E: No existe valor de defecto: (keyword).	Para esta palabra clave (keyword), en la tabla t_keyword, no existe un valor por defecto.	Ponga un valor a la keyword.
UCME errno E: (error string)	Una función de reserva interna ha fallado.	Revise la memoria del sistema.
UCSQ sqlcode E: (sql string)	Una sentencia de SQL ha fallado.	Revise el código de SQL en la Guía de Determinación de Problemas DB/2.

Además, UCM escribe información en un archivo de anotaciones, EDYUCM.LOG, el cual puede ser encontrado en cada servidor de una oficina. Las entradas en este archivo de anotaciones tienen el siguiente formato:

```
Mensaje de información
12/11/96 12:04:30 (Comp) [I] Texto

Aviso o mensaje de error
12/11/96 12:04:30 (Comp) [[W]|[ERR]] Texto
                                (Comp) rc=+código de retorno

Mensaje de error
12/11/96 12:04:30 (Comp) [ERR] Texto
                                (Comp) rc=+código de retorno
                                Componente finalizado.
```

Donde *Comp* puede ser NETBIOS, EDYSRV, y EDYFREE

Vd. puede leer también la siguiente lista de mensajes:

- Mensajes NETBIOS
- Mensajes EDYSRV
- Mensajes EDYFREE

Mensajes NETBIOS

Código	Descripción	Acción de Usuario
NETBIOS [I] Reinicialización Netbios. Utilizando número de adaptador (adapternum).		
NETBIOS [I] Nombre de Netbios		

(servername) añadido.		
NETBIOS [W] Los recursos reservados son S=(sessionsnumber), C=(commandsnumber), N=(namesnumber). NETBIOS rc=+56		
NETBIOS [ERR] [Listening Receiving Sending Hanging] NETBIOS rc=+(netbios return code) Componente finalizado.	Un error fatal ha causado que el EDYSRV se descargue.	Revise el código de retorno de Netbios.
NETBIOS [ERR] Los recursos reservados son S=(sessionsnumber), C=(commandsnumber), N=(namesnumber). NETBIOS rc=+56 Componente finalizado.	La insuficiencia de recursos Netbios ha causado que el EDYSRV se descargue.	Revise los recursos Netbios.
NETBIOS [ERR] Recursos demandados de Netbios, no disponibles. NETBIOS rc=+56 Componente finalizado	EDYSRV se ha descargado debido a la insuficiencia de recursos Netbios.	Revise los recursos Netbios.
NETBIOS [ERR] Número máximo de aplicaciones excedido. NETBIOS rc=+54 Componente finalizado.	EDYSRV se ha descargado debido a la insuficiencia de recursos Netbios.	Revise los recursos Netbios.
NETBIOS [ERR] El nombre Netbios (servername) no es único. NETBIOS rc=+(netbios return code) Componente finalizado.	EDYSRV se ha descargado debido a que existe un nombre de Netbios duplicado.	Revise el código de retorno de Netbios.

Mensajes EDYSRV

Código	Descripción	Acción de Usuario
EDYSRV [I] Componente descargado después de una petición de FREE.		
EDYSRV [ERR] Número de sesiones no válido. Componente finalizado.	No se ha especificado un número de sesiones en el parámetro de carga.	Reintente con un número de sesiones válido.
EDYSRV [ERR] Número de adaptador no válido. Componente finalizado.	El número de adaptador especificado en el parámetro de carga es no válido.	Reintente con un número de adaptador válido.
EDYSRV [ERR] Nombre de servidor no válido. Componente finalizado.	El nombre de servidor especificado en el parámetro de carga es no válido.	Reintente con un nombre de servidor válido.
EDYSRV [ERR] Parámetro de	Uno de los parámetros de carga	Reintente con parámetros de

carga no válido. Componente finalizado.	especificados es no válido.	carga válidos.
EDYSRV [ERR] Error cargando ACSNETB.DLL. Componente finalizado.	La librería de run-time de Netbios no ha podido ser cargada.	Revise que el Netbios se encuentre correctamente instalado.
EDYSRV [ERR] Memoria disponible insuficiente. Componente finalizado.	No hay suficiente memoria disponible.	Revise la memoria de sistema.
EDYSRV [ERR] La contraseña no es correcta en LS. EDYSRV rc=+1	Contraseña incorrecta en LS.	Revise la contraseña.
EDYSRV [ERR] La contraseña no es correcta en RACF. EDYSRV rc=+1	Contraseña no válida en RACF.	Revise la contraseña.
EDYSRV [ERR] La contraseña ha expirado. EDYSRV rc=+2	La contraseña ha expirado en LS.	Cambie la contraseña.
EDYSRV [ERR] La contraseña ha expirado. EDYSRV rc=+2	La contraseña ha expirado en RACF.	Cambie la contraseña.
EDYSRV [ERR] Parámetro de contraseña no válido. EDYSRV rc=+3	Contraseña no válida en LS.	Cambie la contraseña.
EDYSRV [ERR] EDYSRV rc=+4	El proceso de conexión o desconexión UCM ha sobrepasado el tiempo de espera.	Revise las comunicaciones y reintente.
EDYSRV [ERR] El usuario no ha sido encontrado en LS (UsuarioID). EDYSRV rc=+7	El usuario especificado no está definido en LS.	Defina el UsuarioId y reintente.
EDYSRV [ERR] Usuario (UsuarioId) no ha sido encontrado en RACF. EDYSRV rc=+7	El usuario especificado no ha sido definido en RACF.	Defina el usuario y reintente.
EDYSRV [ERR] EDYSRV rc=+7	Usuario no está definido en UCM.	Defina el UsuarioId y reintente.
EDYSRV [ERR] La nueva contraseña es incorrecta en RACF. EDYSRV rc=+9	Contraseña no válida en RACF.	Cambie la contraseña y reintente.
EDYSRV [ERR] El usuario no tiene permiso para conectarse en este momento. EDYSRV rc=+10	El usuario posee una restricción de tiempo para conectarse.	Espere para conectarse.
EDYSRV [ERR] Error de Seguridad General en RACF. Ret_code: 7 EDYSRV rc=+11	Un usuario no autorizado a intentado conectarse a RACF.	Reintente con un usuario autorizado.
EDYSRV [ERR] EDYSRV rc=+12	Cuenta de usuario deshabilitada en LS.	Habilite la cuenta.
EDYSRV [ERR] EDYSRV rc=+13	Cuenta de usuario expirada en LS.	Actualice la cuenta.

EDYSRV [ERR] Código de operación no válido. EDYSRV rc=+61	Se ha especificado a EDYSRV un código de operación no soportado.	Corrija el código de operación y reintente.
EDYSRV [ERR] EDYSRV rc=+61	Error interno de EDYSRV.	Descargue el proceso EDYSRV y vuélvalo a cargar.
EDYSRV [ERR] Memoria insuficiente para procesar la petición. EDYSRV rc=+61	Error interno de EDYSRV.	Revise la memoria de sistema.
EDYSRV [ERR] La creación de una tarea ha fallado. EDYSRV rc=+61	Error interno de EDYSRV.	Revise los recursos del sistema.
EDYSRV [ERR] Ha fallado LAN Server. Ret_code: (RetCode). EDYSRV rc=+62	Una operación de LAN Server ha fallado.	Revise el código de retorno de LAN Server.
EDYSRV [ERR] Error de Seguridad General de RACF. Ret_code: 6. EDYSRV rc=+63	Un formato de datos incorrecto ha sido enviado a RACF.	Revise el formato de los datos y la configuración RACF.
EDYSRV [ERR] EDYSRV rc=+64	Error general de UCM en el proceso de conexión o desconexión.	Revise las comunicaciones. Arranque los trazes de SecureEntry.
EDYSRV [ERR] Error de memoria en la Base de Datos UCM. EDYSRV rc=+65	Error interno del EDYTP. Error general en refresco dinamico de oficinas.	Revise la memoria asignada al proceso EDYTP en el entorno de Host y reintente. Revise las comunicaciones. Arranque los trazes de SecureEntry.
EDYSRV [ERR] EDYSRV rc=+66	Error general de UCM en el proceso refresco de perfiles para WSOD	Revise las comunicaciones. Arranque los trazes de SecureEntry.
EDYSRV [ERR] EDYSRV rc=+67	Refresco de perfiles para WSOD no encontró perfiles que refrescar.	Ninguna

Mensajes EDYFREE

Código	Descripción	Acción de Usuario action
EDYFREE [I] EDYFREE ha sido invocado.		

Este capítulo se ha dedicado a comentar los complementos de UCM que por sí solos no tienen el suficiente peso como para agruparlos en una sección principal.

Tabla de traducción ASCII/EBCDIC

Archivo de problemas UCM

¿Cómo puedo mejorar el rendimiento de UCM?

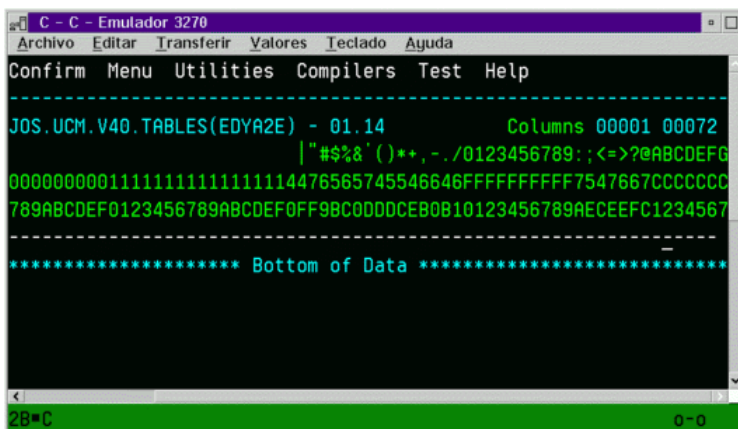
Tabla de traducción ASCII/EBCDIC

Tal y como SecureEntry V3.0 hace, UCM le permite codificar una tabla de traducción alternativa ASCII/EBCDIC que anule la que UCM integra y hace servir, por defecto, en sus módulos cuando es necesario.

Formato de la tabla ASCII/EBCDIC

Esta tabla es un miembro data set con un único registro de 256 bytes de longitud, utilizados para realizar la conversión. La posición de cada byte, de la 0 a la 255 (0 a FF hexadecimal), representa el carácter ASCII. El valor codificado en cada posición representa el carácter EBCDIC equivalente.

Ejemplo:



En el ejemplo que se distribuye **UCM.Vxx.TABLES(EDYA2E)**, la columna 65 (en un rango de 0..255) tiene el carácter EBCDIC A. Esto significa que el carácter ASCII A (decimal 65, hexadecimal 41) será convertido al EBCDIC A (hexadecimal C1).

Los registros comentados están permitidos. Estos, deben tener un carácter * en la columna 0 y un carácter * en la columna 255 (siempre en un rango de 0..255).

UCM suministra un miembro data set de ejemplo en **UCM.Vxx.TABLES(EDYA2E)** como guía para aquellos usuarios que tengan que utilizar su propia tabla de conversión. En la distribución del archivo EDYA2E, la tabla ha sido codificada igual que la tabla por defecto utilizada por los módulos de UCM. Así, si usted no necesita hacerle ningún cambio, no existe ninguna razón para utilizar esta tabla de ejemplo.

Archivo UCMLLOG. Información, problemas de ejecución y estadísticas

Bajo entorno MVS/ESA, la mayoría de los procesos UCM escriben información en el dataset apuntado por **DD:UCMLLOG**.

Los procesos UCM pueden escribir tres tipos de información en el dataset de anotaciones de UCM (UCMLLOG):

- Informativa
Información sobre ejecución normal de los procesos UCM, que le informan acerca de las operaciones realizadas contra la Base de Datos UCM.
- Errores
Información sobre errores que provocan el mal funcionamiento de alguno de los procesos UCM. Cuando estos errores están relacionados con DB2 se escribe el valor completo de la estructura SQLCA.
- Estadística
Información estadística de los datos tratados por los procesos UCM. Es especialmente útil en el proceso APPC EDYTP para conocer el número de transacciones que su red de oficinas está ejecutando contra este proceso y como utilidad para detectar posibles cuellos de botella.

Cuando el TP EDYTP se encuentra configurado en modalidad multi-trans, se utiliza este dataset para almacenar las estadísticas de las transacciones tratadas por cada instancia de ejecución del proceso. Vd. puede diferenciar las estadísticas de cada instancia del proceso EDYTP a través de un ID único por ejecución.

ID=XXXXXXXX-JJJ-hh:mm:ss

Donde

XXXXXXXX = Número hexadecimal de 8 dígitos
JJJ = Día Juliano de ejecución
hh:mm:ss = Hora, minuto y segundo de inicio de ejecución

Una vez que EDYTP es descargado de memoria por el APPC se almacenan en este dataset las estadísticas que hacen referencia a la utilización de cada tipo de transacción tratadas por el proceso:

```
-EDYTP (ID=47BB0698-316-04:30:17): ----- MULTI-TRANS RESULTS -----  
-EDYTP (ID=47BB0698-316-04:30:17): SIGNON TX OK                      = 1234  
-EDYTP (ID=47BB0698-316-04:30:17): SIGNON TX NOK                   = 0  
-EDYTP (ID=47BB0698-316-04:30:17): UCM LOGON TX OK                  = 622  
-EDYTP (ID=47BB0698-316-04:30:17): UCM LOGON TX NOK                = 0  
-EDYTP (ID=47BB0698-316-04:30:17): UCM LOGOFF TX OK                = 13  
-EDYTP (ID=47BB0698-316-04:30:17): UCM LOGOFF TX NOK               = 0  
-EDYTP (ID=47BB0698-316-04:30:17): GET BRANCHID TX OK              = 4
```



```

-EDYTP (ID=47BB0698-316-04:30:17): GET BRANCHID TX NOK           = 0
-EDYTP (ID=47BB0698-316-04:30:17): REFRESH TX OK                 = 259
-EDYTP (ID=47BB0698-316-04:30:17): REFRESH TX NOK                 = 0
-EDYTP (ID=47BB0698-316-04:30:17): REFRESH AVERAGE (SECONDS) = 0.023166
-EDYTP (ID=47BB0698-316-04:30:17): REFRESH GETS DB2 DATA        = 4
-EDYTP (ID=47BB0698-316-04:30:17): PRIMARY REFRESH CACHE
-EDYTP (ID=47BB0698-316-04:30:17): LEVEL <1999-11-10-22.07.13.253638>. BRANCHES WITH
THIS LEVEL <233>. BUF. SIZE <2158>
-EDYTP (ID=47BB0698-316-04:30:17): LEVEL <1999-11-09-22.08.46.201035>. BRANCHES WITH
THIS LEVEL <12>. BUF. SIZE <4254>
-EDYTP (ID=47BB0698-316-04:30:17): LEVEL <1999-04-12-12.45.17.137138>. BRANCHES WITH
THIS LEVEL <10>. BUF. SIZE <50102>
-EDYTP (ID=47BB0698-316-04:30:17): LEVEL <1999-11-08-22.07.35.579767>. BRANCHES WITH
THIS LEVEL <1>. BUF. SIZE <5564>
-EDYTP (ID=47BB0698-316-04:30:17): SECONDARY REFRESH CACHE
-EDYTP (ID=47BB0698-316-04:30:17): TOTAL TX PROCESSED = 2128
-EDYTP (ID=47BB0698-316-04:30:17): FINISHING NORMALLY

```

Donde

- Por cada tipo de transacción que es capaz de tratar el proceso EDYTP se exponen las transacciones finalizadas correctamente y las finalizadas insatisfactoriamente.
- Para las transacciones de refresco (distribución de datos de oficina) EDYTP muestra el número de veces que falló la obtención de datos de la memoria caché (causando accesos DB2) y cuántos buffers diferentes fueron almacenados en memoria. Por cada buffer almacenado muestra cuantas oficinas pidieron su información.
- Finalmente, se informa del número total de transacciones que trató la instancia del EDYTP.

Bajo entorno OS/2, los procesos UCM almacenan la información de errores en las trazas estándar de SecureEntry/2. Ya que el modo de ejecución multi-trans solo está disponible en MVS/ESA, no se muestra información estadística bajo entorno OS/2.

¿Cómo puedo mejorar el rendimiento de UCM?

Si vd. posee UCM bajo entorno MVS/ESA instalado y desea mejorar el tiempo de respuesta de UCM en sus transacciones lea detenidamente esta sección:

Active la funcionalidad multi-trans para el TP EDYTP.

Si vd. está utilizando la funcionalidad de distribución de datos on-line, configúrelo en modo 'HORA DETERMINADA DEL DIA'. Esta política de refresco distribuye mejor los recursos que sus oficinas requieren del Host. Intente escoger una hora con una baja carga de CPU en el Host.

Si vd. posee activada la funcionalidad de distribución de datos de oficina, amplíe la ventana de tiempo durante la cual los diferentes EDYSRV de sus oficinas se despertarán para ejecutar la transacción. Con esto disminuirá las probabilidades de que todas sus oficinas intenten refrescarse al mismo tiempo.

Vd. puede modificar la cantidad de extensiones de la memoria caché primaria. Esta memoria es utilizada para almacenar datos a ser enviados a las oficinas evitando innecesarios accesos a DB2 para recuperarlos.

Si todavía no tiene instalado UCM, piense en la posibilidad de utilizar la emulación de RACF que UCM ofrece. A través de esta funcionalidad conseguirá decrementar el número de transacciones realizadas en tiempo de conexión de sus usuarios.

Si vd. tiene activada la funcionalidad de salida de ejecución (SYSPRINT) del proceso EDYTP, desactívela por parámetro de carga del proceso EDYTP. Este tipo de salida es utilizada normalmente para tareas de rastreo de problemas (debug).

Si vd. tiene activada la funcionalidad de UCMLOG puede anularla por parámetro de carga del proceso EDYTP. Únicamente se utilizará UCMLOG en caso de producirse errores o para escribir las estadísticas del proceso si vd. lo tiene configurado en modo multi-trans.

Si vd. posee activada en su instalación, la Emulación de RACF, informe al proceso EDYTP del nombre de institución por parámetro de carga.

Si vd. tiene configurado la autenticación de usuarios a través del TP de UCM EDYURACF, puede mejorar el rendimiento del mismo a través de los siguientes consejos:

Active la funcionalidad multi-trans para el TP EDYURACF.

Si vd. tiene activa la funcionalidad de salida por cola de ejecución (SYSPRINT) del proceso EDYURACF, desactívela por parámetro de carga. Este tipo de salida es utilizada habitualmente para tareas de seguimiento de problemas (debug).

Informe de la clave de descifrado de los datos por parámetro de carga del proceso.

Es posible que a pesar de seguir los consejos descritos sobre estas líneas, no consiga aumentar el rendimiento de los procesos UCM. Es posible que deba entonces revisar parámetros de configuración del Sistema MVS:

Revise la prioridad de ejecución asignada al APPC/ASCH en las horas punta de transacciones APPC.

Revise el número de iniciadores mínimos y máximos para la clase de ejecución de los TP's.

Revise el objetivo de tiempo de respuesta asignado para la clase de ejecución de los TP's.

Consulte con sus administradores de VTAM/APPC

NOVEDADES !!

Este capítulo pretende ser una guía rápida para usuarios que provengan de versiones anteriores de SecureEntry-UCM y que quieran ponerse al día. Es una enumeración de las nuevas funcionalidades añadidas al producto, en orden cronológico descendente (de más reciente a menos reciente), con enlaces a los puntos apropiados de la documentación donde se describen en mayor detalle. Sin embargo, para una referencia completa de la resolución de problemas (parches) y nuevas funcionalidades, se recomienda leer el archivo README suministrado dentro del primer diskette de instalación, ya que la lista que sigue a continuación sólo incluye las nuevas funcionalidades que se consideran más importantes para el producto.

Nuevo *transaction program* EDYURACF para autenticación de usuarios contra RACF.

Nueva funcionalidad de UCM bajo plataforma OS/2.

Soporte de conexiones en línea de UCM en modalidad multi-trans.

Nueva funcionalidad de Emulación de RACF.

Una nueva utilidad EDYRVUCM para compactar y corregir las tablas de cambios de la Base de Datos UCM.

Una nueva utilidad EDYQRYBR para consultar los niveles de actualización de todas sus oficinas.

Nuevo capítulo acerca de Migrando desde una versión previa de UCM.

Nueva facilidad de anotación de operaciones UCM descrita en los procesos EDYEXLOG y EDYQUERY.

Nuevas tablas de traducción de ASCII a EBCDIC (opcional) en Tabla de traducción para el proceso EDYQUERY.

Nuevo método de actualización dinámica de los cambios en las definiciones de grupos y recursos descrito en Procesos Online