Introducción a RACF

Erik Zepeda

Septiembre 2010

Lámina 1 Ing. Erik Zepeda

Agenda

- Seguridad y sus beneficios
- RACF vs Seguridad
  - Revisión de la arquitectura MF (Z Series ZOS)
  - ¿Qué es RACF?
  - Evolución de RACF
  - Protección de recursos
  - Niveles de Seguridad
- Operación y administración del ambiente de seguridad
  - Comandos de TSO
  - Paneles de ISPF
  - Utilerías batch
- Auditoría al RACF
  - Que cuidar

Lámina 2 Ing. Erik Zepeda

Seguridad y sus beneficios

- Confidencialidad, Integridad, Disponibilidad
- Servicios de Seguridad
  - Autenticación
  - Control de Acceso
  - Responsabilidad (Accountability)
  - No repudiación
  - Integridad
  - Confidencialidad
  - Disponibilidad

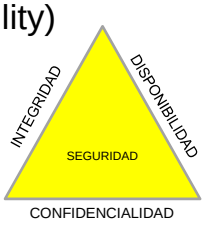


Lámina 3 Ing. Erik Zepeda

Mecanismos a cumplir con la Seguridad

- Identificar a los usuarios que quieren accesar el sistema
- Verificar que los usuarios son quien dicen ser
- Permitir solo a los usuarios autorizados a accesar los recursos protegidos.
- Proporcionar un modo apropiado para administrar la seguridad.
- Registrar los accesos a los recursos protegidos.
- Documentar las violaciones inmediatamente o cuando el usuario requiera un reporte o periódicamente.
- Que pueda ser usado por cualquiera cuyos datos estén siendo protegidos.
- Listar los recursos clave protegidos y el nivel de protección que existe para cada uno.

Lámina 4 Ing. Erik Zepeda

Beneficios a buscar en la seguridad

- Le permite asociar un identificador único a cada usuario potencial cuando el usuario entra al sistema
- Provee un futuro nivel de identificación, tal como una password para verificar que el usuario tiene el identificador apropiado hasta accesar al sistema
- Le da al usuario el nivel apropiado de autoridad para accesar cada recurso protegido.
- Le permite seleccionar el tipo de estructura de seguridad y administración a usar en su instalación.
- Provee otro nivel de responsabilidad de tal forma que usted puede estar viendo quien está usando que recurso.
- Le permite definir los registros que requiere.
- Le permite ver las violaciones donde quiera y en el formato que escoja.
- Fácil de definir y fácil de usar. Esto ayuda a prevenir mecanismos de bypass
- Le permite ver cuales recursos están protegidos

Lámina 5 Ing. Erik Zepeda

RACF vs Seguridad

¿Qué es RACF?
Evolución de RACF
Protección de recursos
Niveles de Seguridad

Lámina 6 Ing. Erik Zepeda

Contenido de esta sección

- Del OS/360 al z/OS – Todo lo que siempre quiso saber sobre los mainframes y tenía miedo de preguntarlo (pero que sea rápido y simple por favor…)
- Nomenclatura

Lámina 7 Ing. Erik Zepeda

Por que los clientes usan Mainframes

- **Capacidad y rendimiento**
  - Muchas aplicaciones comerciales son intensivas en datos, no intensivas en procesador – no son candidatas para plataformas distribuidas
- **Escalabilidad**
  - Ambos horizontalmente (a lo largo de múltiples máquinas) y verticalmente (de una pequeña a un sistema único muy grande
- **Confiabilidad, Disponibilidad, Serviciabilidad, Integridad de Datos y Seguridad**
  - Cinco nueves de disponibilidad, administración madura del sistema
- **Multitareas**
  - Un solo sistema z/OS puede correr cientos de usuarios interactivos, trabajos en lote, y proceso de transacciones, todos al mismo tiempo en la misma imagen de sistema
- **Costos de personal**
  - Debido a la centralización, el costo de soporte por usuario es la más baja de las alternativas

Lámina 8 Ing. Erik Zepeda

Dispositivos periféricos I/O

- Almacenamiento en línea
  - DASD: Direct Access Storage Device
    - Arreglos de discos de SUN, IBM, EMC y HDS
- Almacenamiento fuera de línea
  - Drives de cinta y cartuchos de SUN e IBM
- Almacenamiento casi en línea
  - Librerías de cinta automatizadas de SUN, IBM, Quantum-Adic, Fujitsu
  - Sistemas de cintas virtuales de SUN, IBM, Fujitsu Siemens, Luminex, Bus Tech
- Impresoras
- Comunicaciones y redes
  - TCP/IP vía OSA (Open System Adapter)
  - Unidades de control de red: System Network Architecture

Lámina 9 Ing. Erik Zepeda

z/OS y el almacenamiento

- MVS = «Multiple Virtual Storage»
- IBM diseñó sus mainframes con la idea de que este podría mantener una cantidad muy grande de I/Os agregados descargando a la CPU de esta tarea
- La intención original fue la de compartir datos fácilmente entre múltiples procesos y servidores (sysplex) y soportar el movimiento de datos por medio de políticas
- HSM (Hierarchical Storage Manager) es una pieza clave de la arquitectura de administración del almacenamiento de z/OS. Este realiza migraciones automáticas basadas en políticas y operaciones de recuperación entre diferentes niveles de disco y cinta.

Lámina 10 Ing. Erik Zepeda

Conceptos importantes Z series

- **Disponibilidad** – Un mainframe tiene casi 100% de disponibilidad. El almacenamiento se debe alinear a este requerimiento
- **Mantenimiento** – El soporte de alto nivel es mandatorio (en sitio en menos de 4 horas en el peor de los casos)
- **Depreciación** – El objetivo es usualmente lograr una depreciación sobre 3 a 5 años, mayormente en cintas y algunas veces en discos
- **Aplicaciones** – en muchos casos, el almacenamiento es independiente de las aplicaciones

Lámina 11 Ing. Erik Zepeda

Términos importantes

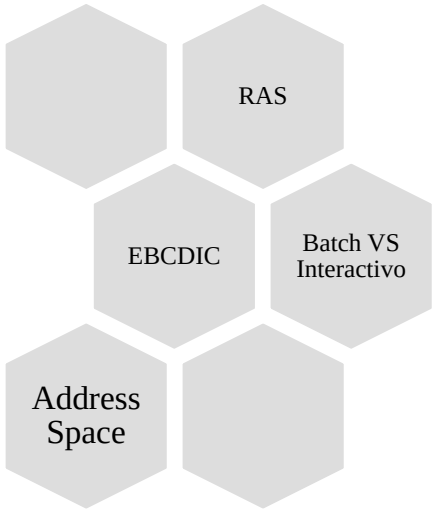


Lámina 12 Ing. Erik Zepeda

Conceptos de almacenamiento

- **DASD** – Direct Access Storage Device
  - UN dispositivo de almacenamiento el cual se puede accesar directamente por el SO por medio de una unidad de control (CU)
  - Equivale a Hard Drive
- **HFS/zFS** – Hierarchical File System
  - Un HFS es una representación de un sistema File System tradicional de Unix (con directorios y archivos). Un HFS es actualmente almacenado en un dataset
- **Data Set** – Espacio de almacenamiento en DASD para almacenar información. Los Datasets pueden ser particionados (con miembros internos) o secuenciales
  - La analogía más cercana es; Particionado = una gaveta con múltiples archivos
  - Archivo secuencial = Archivo
- **DFSMS** – Data Facility Storage Management Subsystem
  - El subsistema responsable de la ubicación de espacio en DASD. Ahora contiene al HSM (Hierarchical Storage Management)
  - La analogía más cercana es cualquier producto de administración del almacenamiento
- **VSAM** – Virtual Storage Access Method
  - Un método de almacenamiento secuencialmente indexado

Lámina 13 Ing. Erik Zepeda

Explorar conceptos de administración

- **JCL** – Job Control Language
  - Código usado para iniciar tareas y definir los recursos requeridos
  - Analogía: Shell script
- **TSO** – Time sharing Option
- **Subsistemas/Started Tasks** – tareas que corren sin requerir la interacción de un usuario
  - Funciones del núcleo del sistema operativo, tales como seguridad, servicios de administración del almacenamiento
  - Analogía: Daemons, cron jobs
- **USS** – Unix System Services
  - UN ambiente Unix Posix certificado corriendo encima de z/OS

Lámina 14 Ing. Erik Zepeda

Explorar los conceptos de Clustering

- **LPAR** – Logical Partition
  - Una división lógica de una máquina la cual actua como una máquina física – cada LPAR corre su propia instancia de SO
  - Analogía: System Partition /Dominio (SUN)
- **Sysplex** – SYStem comPLEX
  - Multiples LPARs las cuales con capaces de compartir recursos para procesar unidades de trabajo y proveer redundancia.
  - Analogía: Un cluster altamente mejorado
- **CF** – Coupling Facility
  - Un dispositivo el cual permite la comunicación entre LPARs en un SysPlex
- **Parallel Sysplex** – Parallel System comPlex
  - Clustering
- **IRD** – Intelligent Resource Director
  - Tecnología que permite la afinación automática de los recursos entre LPARS – como WLM de LPARs
- **ICF** – Integrated Coupling Facility e Integrated Catalog Facility

Lámina 15 Ing. Erik Zepeda

Explorar conceptos varios

- **RACF** – Resource Access Control Facility
  - Un subsistema de seguridad que cumple con el System AUTHORIZATION FACILITY (SAF)
  - Analogía: PAM (Linux) o cualquier otra herramienta de seguridad
- **JES** – Job Entry Subsystem
  - El subsistema que administra el trabajo eb z/OS. Este es un sistema de prioridades de colas
  - Analogía: colas de mensajes
- **ISPF** – Interactive System Panel Facility
  - Un manejador de paneles interactivos (TN3270) interface del TSO
  - Analogía: SMIT para AS400, LinuxConf o Yasr (en Linux)

Lámina 16 Ing. Erik Zepeda

El servidor de seguridad de IBM

- Componentes del servidor de seguridad:
  - DCE Security Server
  - LDAP (Lightweight Directory Access Protocol)
  - z/OS Firewall Technologies
  - Network Authentication Service for z/OS
  - PKI Services
  - RACF (Resource Access Control Facility)

Lámina 17 Ing. Erik Zepeda

RACF vs Seguridad

¿Qué es RACF?

Resource Access Control Facility, también conocido como Z/OS Security Server

- Producto de seguridad IBM para mainframes
- Control Flexible
- Protección de Recursos definidos en su propias instalaciones
- Almacenamiento de información de seguridad para otros productos
- Implementación de seguridad centralizada o descentralizada

Lámina 18 Ing. Erik Zepeda

Seguridad y sus beneficios

- ¿Porqué seguridad en Mainframes?
  - B2B, B2C
  - Normatividad y Regulaciones
  - Altos volúmenes de información
  - Capacidades crecientes de almacenamiento e información
  - ¿Quién pude ver qué?
    - Empleados
    - Clientes
    - Socios comerciales
    - Entidades gubernamentales

Lámina 19 Ing. Erik Zepeda

Historia del RACF

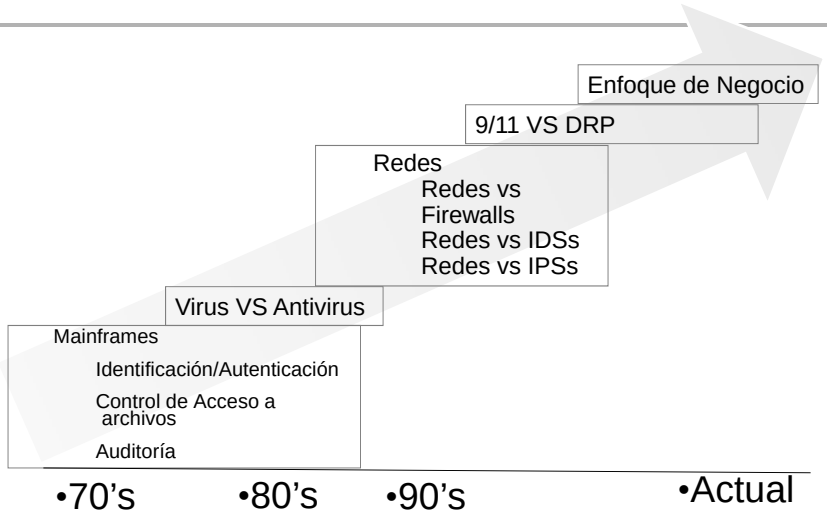


Lámina 20 Ing. Erik Zepeda

Como es que RACF le ayuda con sus necesidades de seguridad

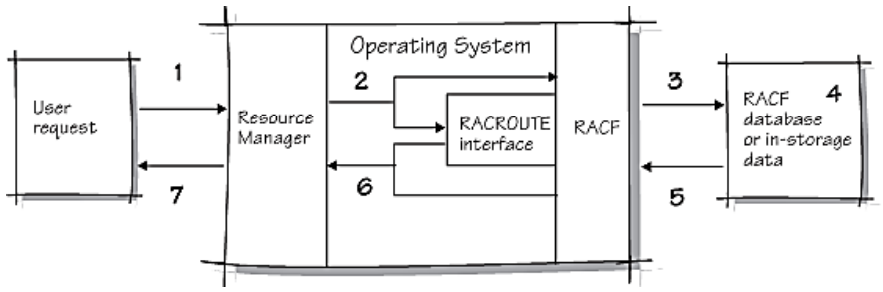
RACF le ayuda a cumplir con sus necesidades de seguridad por medio de proveerle:

- Control de acceso flexible para los recursos protegidos
- Protección de los recursos definidos por la instalación
- Habilidad para almacenar información de otros productos
- Elección de control de perfiles centralizado o descentralizado
- Paneles de acceso por ISPF
- Transparente a los usuarios finales
- Modificación al flujo normal por medio de EXITS escritas en la instalación

Como los requerimientos de seguridad varía en cada instalación de proceso de datos, estos beneficios le permiten cumplir sus objetivos de seguridad únicos

Lámina 21 Ing. Erik Zepeda

Como trabaja RACF con el Z/OS



1. El usuario requiere acceso a un recurso usando un método de acceso (ejemplo TSO/E).
2. El método de acceso manda un requerimiento al RACF para ver si el usuario tiene acceso al recurso.
3. RACF de refiere a la base de datos de RACF o a los registros en memoria y …
4. Revisa el perfil apropiado para el recurso
5. Basado en la información del perfil
6. RACF pasa el estatus del requerimiento al método de acceso.
7. El método de acceso le concede (o niega) el acceso requerido

Lámina 22 Ing. Erik Zepeda

System Authorization Facility SAF

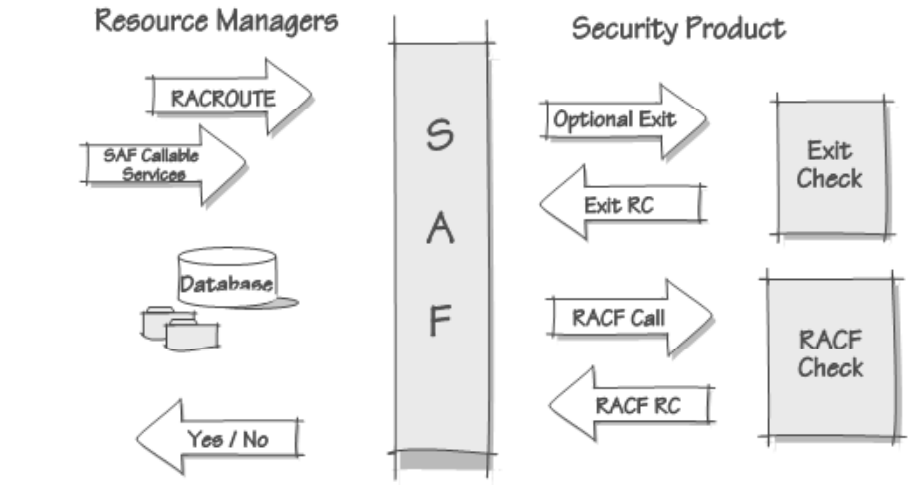


Lámina 23 Ing. Erik Zepeda

Ambiente básico de discos compartidos

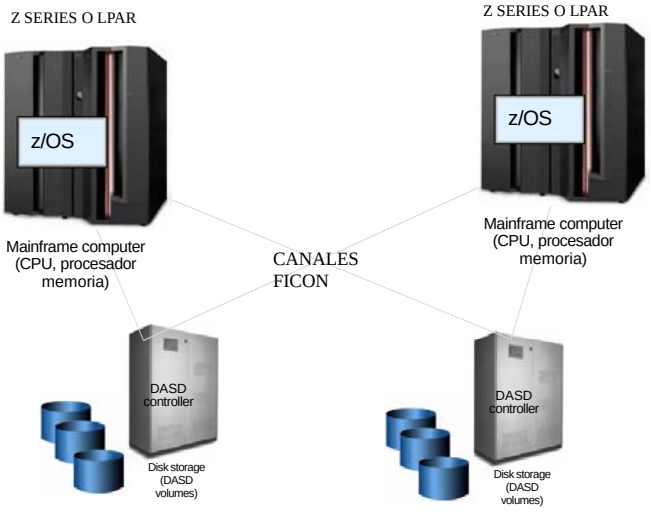


Lámina 24 Ing. Erik Zepeda

Parallel Sysplex

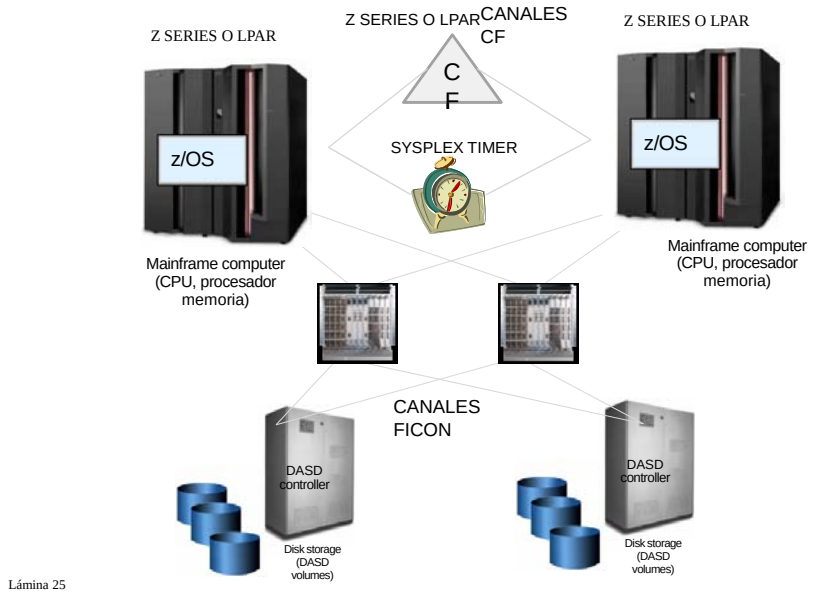


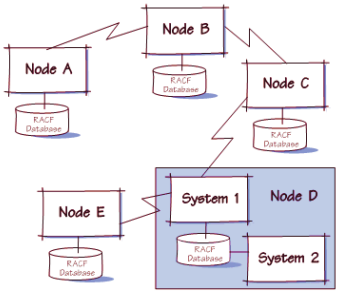
Lámina 25 Ing. Erik Zepeda

RRSF (RACF Remote Sharing Facility)

- Si se tienen muchos sistemas que utilizan una base de datos RACF pueden existir problemas de conexión
- RACF propagará comandos a través de un sysplex
- RACF puede usar al *Coupling Facility* de un *Parallel Sysplex* para mejorar el desempeño en las búsquedas de los perfiles y las autorizaciones
- RRSF puede utilizarse para mantener las bases de datos RACF distribuidas en línea

Lámina 26 Ing. Erik Zepeda

Nodos RRSF Remote Sharing Facility



Funciones

- Sincronización de passwords
- Dirección del comando
- Dirección automática del comando
- Dirección automática de las actualizaciones de las aplicaciones

Beneficios

- Usabilidad
- Administración del sistema
- Disponibilidad
- Tiempo

Lámina 27 Ing. Erik Zepeda

Como realiza RACF sus funciones

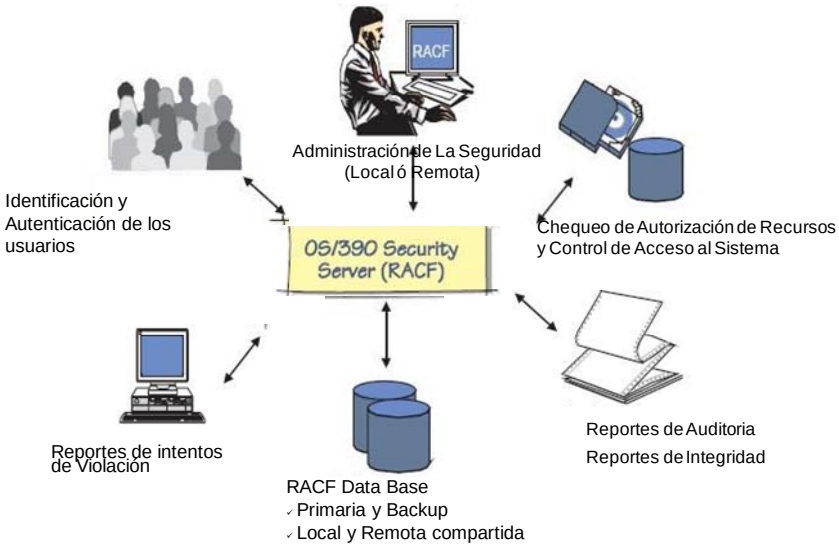


Lámina 28 Ing. Erik Zepeda

Como realiza RACF sus funciones …

Para lograr esta metas, RACF le da la habilidad de:

- Identifica y autenticar usuarios
- Autorizar a los usuarios a accesar los recursos protegidos
- Registrar y reportar varios intentos no autorizados de acceso a los recursos protegidos
- Control de los medios de acceso a los recursos
- Permite a las aplicaciones el uso de macros de RACF

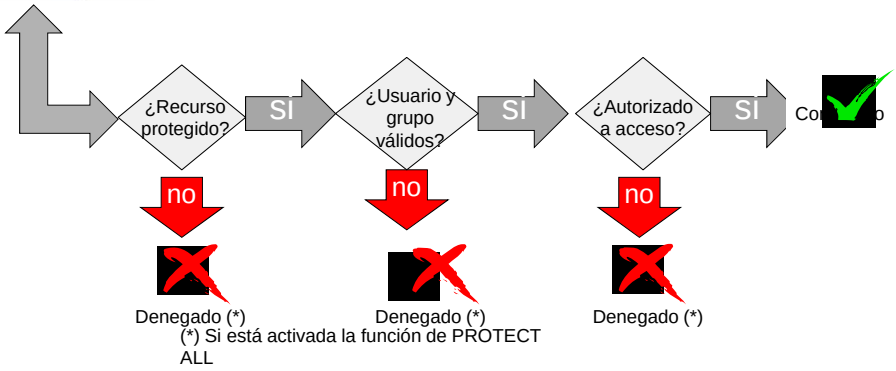
Lámina 29 Ing. Erik Zepeda

Perfiles discretos y genéricos

- Facilidad para definir un grupo de recursos que tienen elementos de su nombre en común
- Facilita la administración
- Un perfil discreto define un recurso por su nombre completo
- Un perfil genérico define a un grupo de recursos
- Se da preferencia a las definiciones más específicas y después a las más genéricas
- Se permiten uno o más de los siguientes caracteres genéricos:
  - Signo de porciento (%) Un solo carácter
  - Asterisco sencillo (*) Un calificador en el nombre de l archivo
  - Doble asterisco (**) Uno o más calificadores en el nombre del archivo
  - Ampersand (&) Usado para variables del sistema operativo
- Debe estar activa la función de enhanced generic profile en los parámetros de operación de RACF

Lámina 30 Ing. Erik Zepeda

Verificación de perfiles RACF



(*) Si está activada la función de PROTECT ALL

Lámina 31 Ing. Erik Zepeda

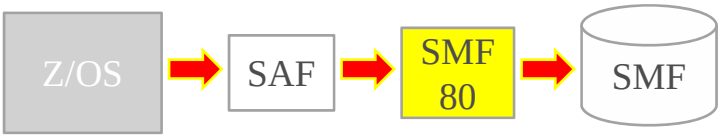
Almacenamiento y reporte

- RACF mantiene información estadística
- RACF escribe un log de seguridad cuando detecta lo siguiente:
  - Intentos no autorizados de acceso al sistema
  - Acceso a recursos
    - Esto depende de los parámetros del recurso
    - Por ejemplo AUDIT(ALL(UPDATE)) almacenará todas las actualizaciones el recurso
  - Ejecución de comandos

Lámina 32 Ing. Erik Zepeda

Almacenamiento y reportes

RACF registra eventos del sistema, permitiendo el monitoreo de usuarios y sus actividades; reporta los intentos de ejecutar acciones no autorizadas



- RACF corta los registros de SMF para pos proceso y provee un Report Writer
- Interfaces XML para reporteo
- El reporte describe los intentos para accesar los recursos RACF-protegidos por userID, de accesos exitosos, ó violaciones a la seguridad
- Record Type 80 (50) — Security Product Processing
- Record Type 81 (51) — RACF Initialization
- Record Type 82 (52) — CUSP Record
- Record Type 82 (52) — ICSF Record
- Record Type 82 (52) — PCF Record
- Record Type 83 (53) — RACF Audit Record For Data Sets

Lámina 33 Ing. Erik Zepeda

- **System Management facility**
  - System management facilities (SMF) recolecta y almacena información del sistema y de trabajos que puede usarse en:
- Facturación de usuarios
- Reportes de confiabilidad
- Análisis de la configuración
- Planificación de trabajos
- Evaluación de la actividad de conjuntos de datos
- Perfilando el uso de recursos del sistema
- Manteniendo la seguridad del sistema

Lámina 34 Ing. Erik Zepeda

Guardar registros de eventos en SMF

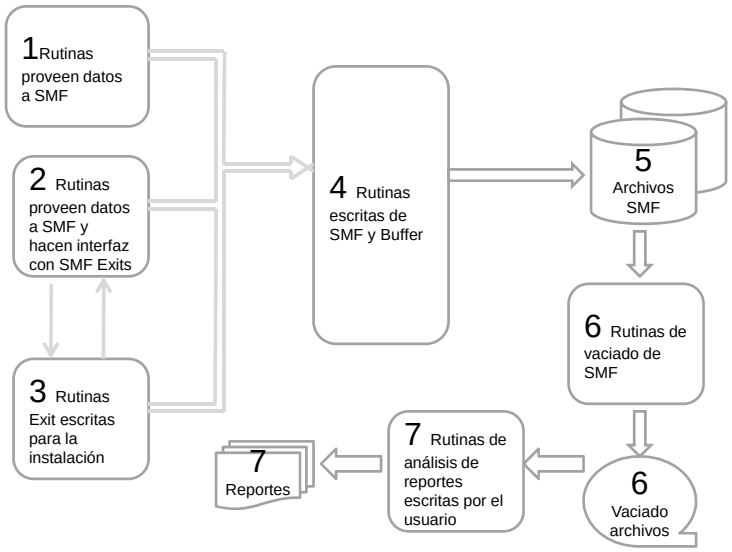


Lámina 35 Ing. Erik Zepeda

Funciones de RACF

Protección de los Data Sets	Protección de los recursos	Convención de nombres
Organización	Nombres de los grupos	Transparencia
Puesta a punto del RACF	Recuperación	Detección de violaciones
Subsistemas	Redes	Compartir datos

Lámina 36 Ing. Erik Zepeda

Role Based Access Control (RBAC)

- RBAC es una forma de restringir el acceso al sistema a usuarios autorizados
  - RBAC Inicia la distinción entre una cuenta de usuario y la función asignada a esa cuenta
  - Cada cuenta tiene una función definida por un administrador
  - Esta distinción permite el cambio a hacer seguimiento de la actividad de login
- Hay tres partes principales en las cuentas basadas en RBAC
  - **Nombre de la cuenta** – Nombre de Login y password
  - **Función (Role)** – Concede o niega el acceso a cambiar de permisos a algunas actividades
  - **Descripción** – Parámetro opcional para añadir más detalles sobre la cuenta

Lámina 37 Ing. Erik Zepeda

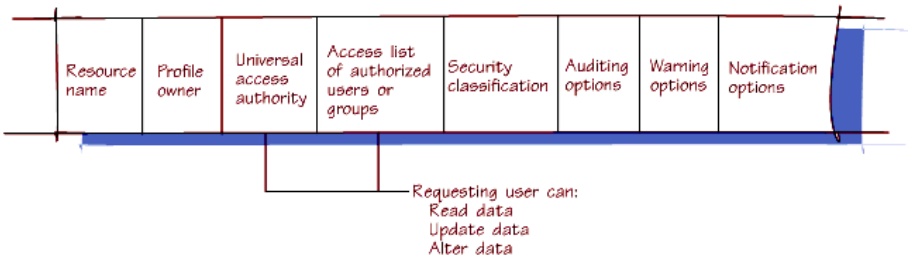
Estructura RACF

- Userid
- Group
  - Todos los userids pertenecen al menos a un grupo
  - Las estructuras de grupo son utilizadas para acceso a recursos
- Resource
  - Resource classes
- Class descriptor table – usada para customizar las clases de recursos a proteger

Lámina 38 Ing. Erik Zepeda

Protegiendo un data set

- Un perfil de data set se crea y almacena en la base de datos
- Este proporcionará al usuario o grupos un nivel de acceso
- Adicionalmente, se crea un nivel de acceso universal
- El perfil puede ser específico o genérico, con o sin wild cards



Niveles de protección

- RACF trabaja en una estructura jerárquica
  - ALLOC permite la creación y destrucción de data sets
  - CONTROL permite VSAM repro
  - WRITE permite actualización de datos
  - READ permite leer datos
  - NONE ningún acceso
- El mayor permiso implica todos los listados

Lámina 40 Ing. Erik Zepeda

Control de Acceso

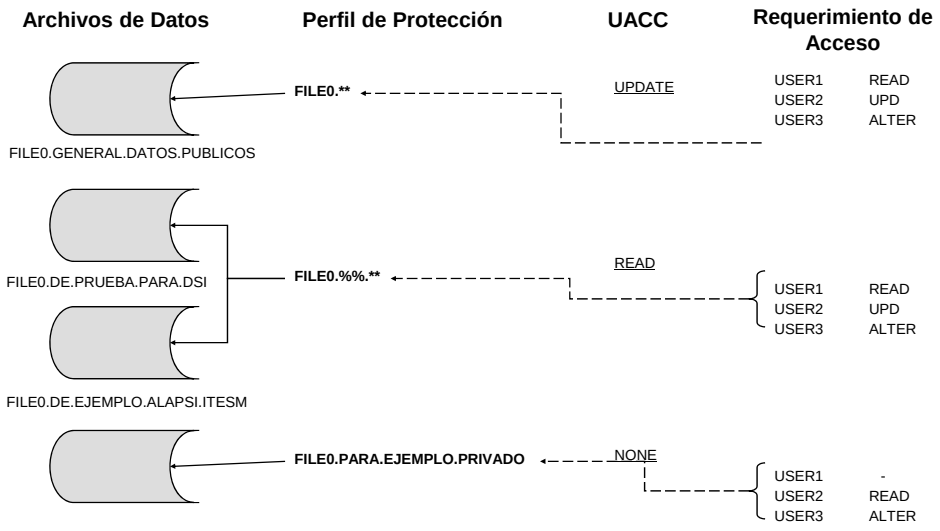


Lámina 41 Ing. Erik Zepeda

Protegiendo recursos generales

- Muchos recursos de sistema pueden estar protegidos
  - Volúmenes DASD
  - Cintas
  - Programas (módulos de carga)
  - Recursos de aplicaciones (tales como recursos para IMS, CICS y DB2)
  - Terminales
  - Recursos definidos por la instalación
  - Transacciones CICS o IMS
  - Data sets
  - Comandos de sistema
  - Recursos de aplicación entre otros
- Los recursos son protegidos con perfiles. Un perfil contiene información descriptiva sobre un usuario, un grupo, o un recurso. RACF usa la información en un perfil para controlar el uso de los recursos protegidos. Cuando usted intenta usar un recurso protegido, RACF revisa su perfil de usuario, así como el perfil del recurso, para decidir si le permite hace uso del recurso

Lámina 42 Ing. Erik Zepeda

Definición de usuarios

Usuarios y Grupos

- Identificación y Autenticación
  - 8 caracteres para identificadores
  - 8 caracteres para contraseñas
  - 8 caracteres para grupos

Atributos para usuarios

- AUDITOR
- OPERATIONS
- SPECIAL
- CLAUTH
- REVOKE

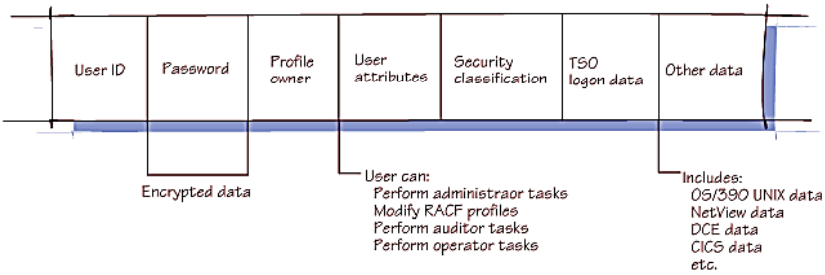


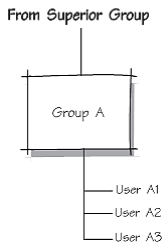
Lámina 43 Ing. Erik Zepeda

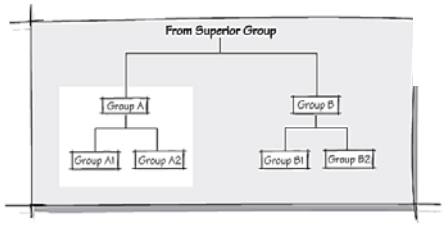
Conexión de usuarios y grupos

Grupos

Atributos de usuarios sobre grupos

- –USE
- –CREATE
- –CONNECT
- –JOIN





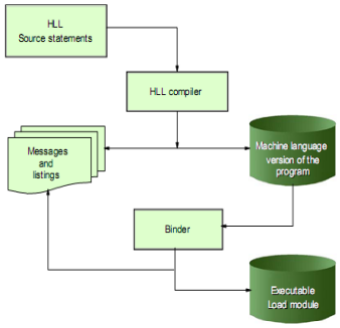
Estableciendo la estructura de grupos de RACF

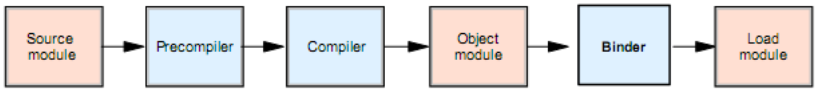
Usted debe mapear sus grupos a la estructura de su organización y ordenarlos jerárquicamente de tal forma que cada grupo es un subgrupo de algún otro grupo. El grupo SYS1 está predefinido como el grupo de mayor jerarquía. Usted debe documentar la estructura de grupos resultante como parte de su plan de implementación.

Lámina 44 Ing. Erik Zepeda

Fuente, objecto, y módulo de carga

- Un programa fuente puede ser dividido en unidades lógicas – o *módulos* – que realizan funciones específicas
- Cada módulo es ensamblado o compilado por alguno de los traductores de lenguaje.
- La entrada a un traductor de lenguaje es un *módulo fuente*
- La salida de un traductor de leguajes es un *módulo objeto*
- Los módulos objetos deben ser procesados por el linkeditor antes de que se puedan ejecutar.
- La salida del linkeditor es un *módulo de carga*.





Los programas de usuario, llamados aplicaciones, implementan el proceso que el usuario quiere que el sistema ejecute. Sin embargo los programas de usuario no deben interferir con o substituir sus funciones con el sistema operativo. Esto obviamente disminuirá la confianza del usuario hacia el sistema si otra entidad puede realizar funciones de administración del sistema.

Lámina 45 Ing. Erik Zepeda

Llaves protección de memoria

- Usadas para prevenir cambios no autorizados en la memoria
- Necesario contar con una llave para cambiar
- Llave por cada 4K de memoria
- Numeradas del 0 al 15
  - La llave reside en el PWS (Program Status Word)

- Las tareas autorizadas ejecutan programas autorizados permiten el acceso a funciones de sistema sensitivas
- Los programas autorizados pueden solamente utilizar funciones estándar para eliminar problemas de integridad

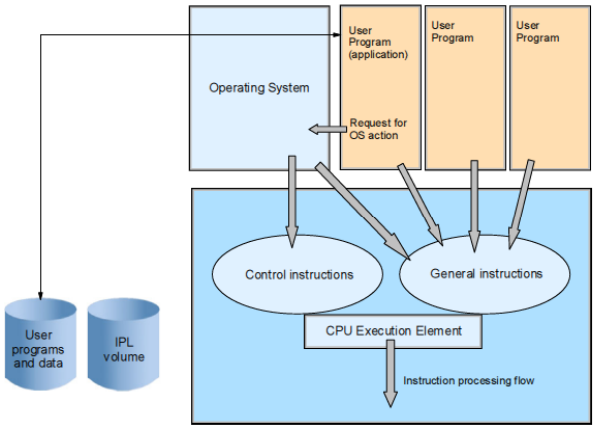


Lámina 46 Ing. Erik Zepeda

Estados del sistema operativo y la APF

- Estados del sistema
  - Supervisor (system) state
    - trabajo realizado por el sistema
  - Problem program (user) state
    - trabajo realizado por el usuario
  - El sistema se encuentra en un estado o en otro
- Authorized Program Facility (APF)
  - no es un estado, sino una característica especial
  - un programa APF autorizado debe residir en una librería designada por APF que se encuentra en SYS1.PARMLIB
  - El programa debe estar linkeditado con código 01 en dicha librería

Lámina 47 Ing. Erik Zepeda

Authorized Program Facility

APF

Autorizando programas especiales del sistema

Dentro del sistema operativo z/OS, existe una función que permite a la plataforma identificar programas especiales del sistema, así como programas de usuario que se les permite usar funciones sensitivas de seguridad. Esta función es conocida como Authorized Program Facility (APF). Esta función es única del sistema operativo de los System z y una de las mayores funciones de seguridad que le da al System z una ventaja sobre otros sistemas operativos. Windows y Unix no tienen una función equivalente.

Bibliotecas autorizadas

•SYS1.LINKLIB
•SYS1.LPALIB
•SYS1.SCVLIB

+

La lista de bibliotecas definidas por la instalación

Lámina 48 Ing. Erik Zepeda

Bibliotecas Autorizadas

- Una tarea está autorizada cuando la ejecución de un programa tiene las siguientes características:
  - Se ejecutan en estado supervisor
  - Se ejecuta en PSW llave 0 a 7
  - Todos los programas previos en la misma tarea fueron programas APF
  - El módulo fue cargado desde una biblioteca APF
- **Privilegios de un programa autorizado**

UN programa autorizado en la APF puede:

- Puede ponerse a si mismo en modo estado supervisor o con llave del sistema
- Puede modificar los bloques de control del sistema
- Puede ejecutar instrucciones privilegiadas (después de ponerse en estado supervisor)
- Puede apagar el logeo para cubrir sus rastros

Lámina 49 Ing. Erik Zepeda

Bibliotecas APF

- Las bibliotecas autorizadas se definen por la listas APF en SYS1.PARMLIB
- SYS1.LINKLIB, SYS1.SVCLIB y SYS1.LPALIB son autorizadas automáticamente
- La instalación de bibliotecas son definidas en PROGxx
- Por omisión todas las bibliotecas en la lista de enlace se autorizan pero muchas instalaciones establecen el parámetro LNKAUTH=APFTAB, de forma que esto ya no ocurre y solamente aquellas bibliotecas en la lista son las autorizadas

Lámina 50 Ing. Erik Zepeda

Bibliotecas autorizadas

•Bibliotecas autorizadas
- SYS1.LINKLIB
- SYS1,LPALIB
- SYS1.SVCLIB

Lista de bibliotecas de la instalación

Los programas del sistema Usualmente:
- Residen en bibliotecas autorizadas APF
- Se ejecutan en estado supervisor
- Usan llave de almacenamiento 0 a 7

Bibliotecas No autorizadas

Los programas de aplicaciones usualmente:
- Residen en bibliotecas no autorizadas
- Se ejecutan en estado problema
- Usan llave almacenada 8

Lámina 51 Ing. Erik Zepeda

Un ejemplo de una lista de APF

```
BROWSE SYS1.PARMLIB(PROGTT) -    01.01              Line 00000000 Col 001
080
Command
===>
           Scroll ===> PAGE
************************** Top of Data ********************************
APF FORMAT(DYNAMIC)
APF ADD
    DSNAME(SYS1.VTAMLIB)
    VOLUME(******)
APF ADD
    DSNAME(SYS1.SICELINK)
    VOLUME(******)
APF ADD
    DSNAME(SYS1.LOCAL.VTAMLIB)
    VOLUME(TOTCAT)
APF ADD
    DSNAME(ISP.SISPLOAD)
    VOLUME(*MCAT*)
************************** Bottom of Data *****************************
```

Lámina 52 Ing. Erik Zepeda

Operación y administración del ambiente de seguridad

Comandos de TSO
Paneles de ISPF
Utilerías batch

Lámina 53 Ing. Erik Zepeda

Comandos de TSO

- Las operaciones básicas de todo ambiente de administración son:
  - Alta
  - Baja
  - Cambio
- Los recursos a administrar son:
  - Usuarios y sus grupos
  - Archivos y sus grupos
  - Otros recursos y sus grupos
- Los atributos a manejar
  - Atributos de usuarios y grupos: Special, operations, auditors, dfltgrp
  - Atributos de los recursos: UACC, AUDIT,
- Los parámetros generales de administración
  - Administración, auditoría y operación centralizada o descentralizada
  - Base de datos replicadas, distribuidas remotamente
  - Perfiles en memoria
  - Reglas de actualización de passwords, históricos

Lámina 54 Ing. Erik Zepeda

Comandos en TSO

- Todos tienen una ayuda con el comando HELP de TSO
  - Ejemplo: H LU
- Si lo da en ISPF debe prefijarlo con el comando TSO, ejemplo
  - TSO LU IBMUSER
- Si está en la opción 6 del menú principal de ISPF no necesita el comando TSO
  - LU IBMUSER
- Los comandos más usados son:
  - LU user
  - ALU user PASSWORD(password)
  - ALU user RESTORE
  - LD
- Se pueden programar con REXX o CLIST para automatizar la administración

Lámina 55 Ing. Erik Zepeda

Sintaxis de los comandos de RACF

1. CARACTERES EN MAYUSCULAS o PALABRAS deben ser codificadas como aparecen en los diagramas de sintaxis pero no tienen que estar en mayúsculas.
2. Letras en minúsculas o palabras representan variables para las cuales usted debe suministrar un valor.
3. Paréntesis ( ) debe ser introducido exactamente como aparece en el diagrama de sintaxis
4. Una elipsis … (tres puntos consecutivos) indican que usted puede introducir el artículo precedente más de una ves.
5. Un solo artículo entre corchetes [ ] indica que el artículo encerrado es opcional. No especifique los corchetes en su comando.
6. Artículos apilados en corchetes [ ] indican que los artículos encerrados son opcionales. Usted puede seleccionar más de uno. No especifique los corchetes en su comando.
7. Artículos apilados en llaves { } indican que el artículo encerrado son alternativas. Usted debe especificar uno de los artículos. No especifique las llaves en su comando.
   Nota: Cuando seleccione un corchete que contiene llaves, usted debe especificar una de las alternativas encerradas en las llaves.
8. Artículos separados por una barra vertical | indica que usted puede especificar solo uno de los artículos. No especifique la barra vertical en su comando.
9. Un operando subrayado indica el valor por omisión cuando no se especifica un valor alterno.
10. **NEGRITAS** indican información que debe ser dada para un comando
11. Apostrofes sencillos ‘ ‘ indican que la información debe ser encerrada en apostrofes sencillos.

Lámina 56 Ing. Erik Zepeda

Comandos de RACF en Batch

El siguiente ejemplo muestra como comandos de RACF en TSO en el background como un job batch:

```
//jobname JOB ...
//STEP1 EXEC PGM=IKJEFT01,DYNAMNBR=20
//SYSTSPRT DD SYSOUT=A
//SYSTSIN DD *
ADDGROUP PROJECTA
ADDUSER (PAJ5 ESH25)
ADDSD 'PROJECTA.XYZ.DATA'
PERMIT 'PROJECTA.XYZ.DATA' ID(PAJ5)
  ACCESS(UPDATE)
/*
```

Lámina 57 Ing. Erik Zepeda

Usando páneles de ISPF con RACF

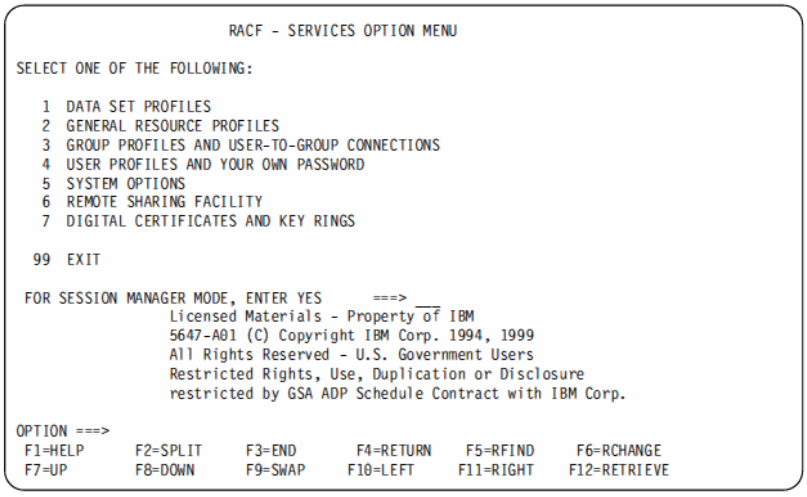


Lámina 58 Ing. Erik Zepeda

Resumen

- La seguridad es importante en los negocios que usar a IT para guardar y administrar su información
- Los ataques y la seguridad están actualizándose constantemente
- La seguridad en los MF está garantizada por el Security Server
- RACF es el componente más importante en el Security Server
- La seguridad es cuestión de personas, no de sw y hw.
- La administración de la seguridad debe hacerse por un equipo interdisciplinario de profesionales bien entrenados y certificados
- Como todo en IT la seguridad debe estarse reaprendiendo constantemente

Lámina 59 Ing. Erik Zepeda