DIRMAINT und RACF auf z/VM (V10)

GSE Frühjahrestagung 2006
24.-26. April 2006

Dr. Manfred Gnirss
TMCC Böblingen, Germany
gnirss@de.ibm.com

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

AIX*
CICS*
DB2*
e-business logo*
Enterprise Storage Server*
ESCON*
FICON
FlashCopy*
GDPS*
HyperSwap
IBM*
IBM eServer*
IBM logo*
NetView*
OS/390*
Parallel Sysplex*
S/390*
Sysplex Timer*
Tivoli*
TotalStorage*
z/OS*
z/VM*
zSeries*
System z9*
RACF
Dirmaint

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Intel is a trademark of the Intel Corporation in the United States and other countries.

Java and all Java-related trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

UNIX is a registered trademark of The Open Group in the United States and other countries.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

This presentation and the claims outlined in it were reviewed for compliance with US law. Adaptations of these claims for use in other geographies must be reviewed by the local country counsel for compliance with local laws.

Acknowledgement

My very best thanks to

Alan Altmark and Gary Detro

for their help and contribution to this presentation.

(Some of the material is extracted from IBM Learning Services Course ZV20)

Agenda

- DirMaint
- RACF/VM
- DirMaint and RACF/VM

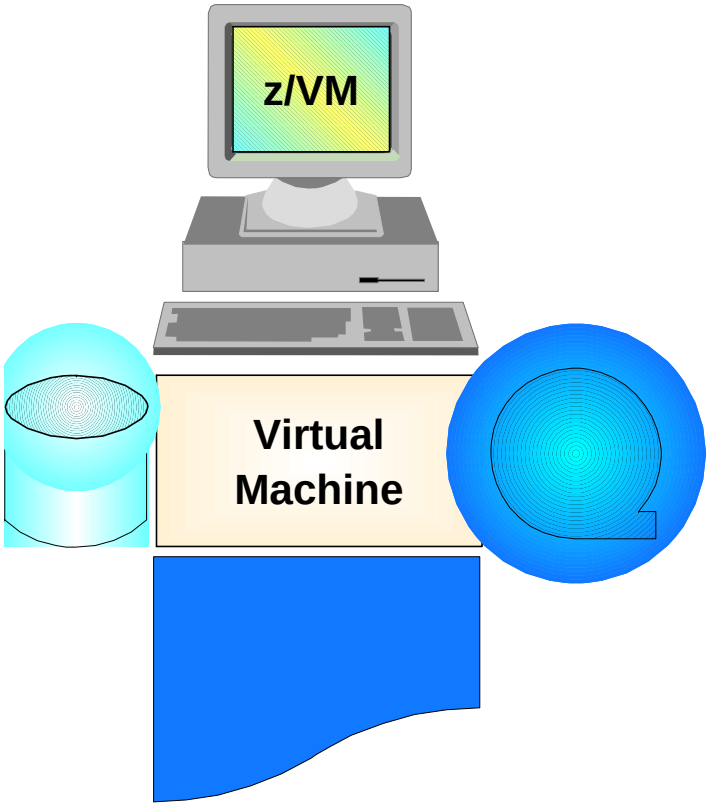
DirMaint Overview

What is DIRMAINT ?

- IBM Directory Maintenance for z/VM and VM/ESA (DirMaint) is a Pre-installed Priced Program Product that helps manage an installation's VM directory
- DirMaint has a corresponding command for every z/VM directory statement, command authorization is controlled by assigning DirMaint commands to privileged command sets.
- DirMaint Release 5.0 supports the z/VM Security strategy
- Access to minidisks is controlled by either passwords or explicit link authorization, as determined by the minidisk owner. Minidisk passwords are now optional for controlling minidisk directory links.
- DirMaint also supports control of minidisk links by an ESM, such as RACF/VM or other vendors external security manager
- Online information for the DirMaint Release 5.0 base feature includes National Language Support (default is American English)
- DirMaint Release 5.0 maintains compatibility with DirMaint Release 4.0 by supporting upward compatability

Directory Maintainance Program - DirMaint

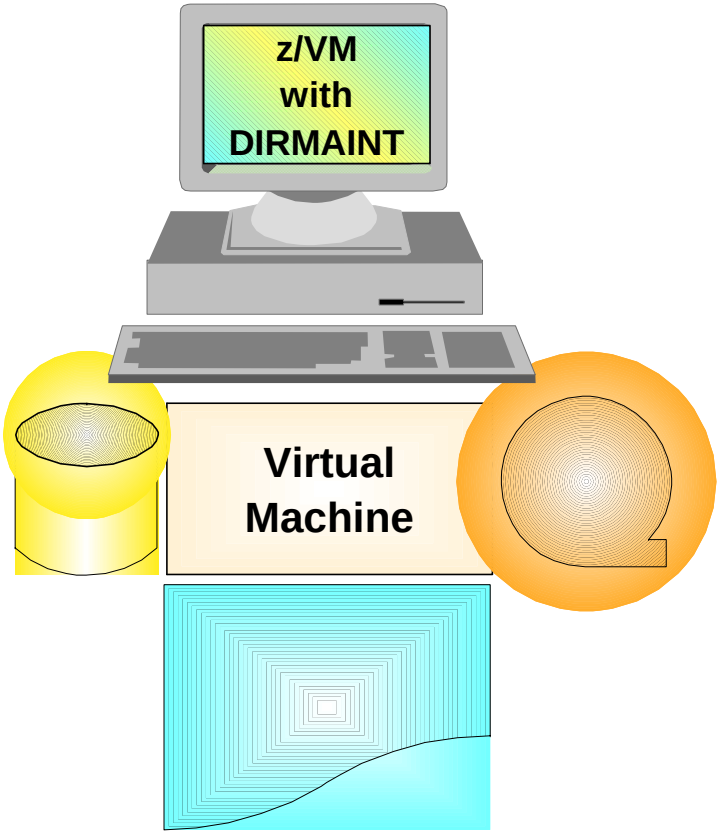
Old/Manual Method



XEDIT USER DIRECT

DIRECTXA USER DIRECT

Automated Method



DIRM FOR GUMBY AMDISK 191

DIRM DIRECT

Why Do I need DirMaint ?

- DirMaint operates as a CMS application in a z/VM operating system for support of the system directory
- DirMaint minimizes the possibility of human error through an automated process of managing the directory
- DirMaint ensures the integrity of the directory
- DirMaint ensures the integrity of mdisk by preventing new minidisk space from being inadvertently allocated over existing extents.
- DirMaint improves overall system efficiency
- A menu/panel is displayed for the complex DirMaint commands
- DirMaint's service processes are simplified by using VMSES/E.
- Online HELP is available for every DirMaint commands and messages.
- The DirMaint service machines run disconnected and unattended

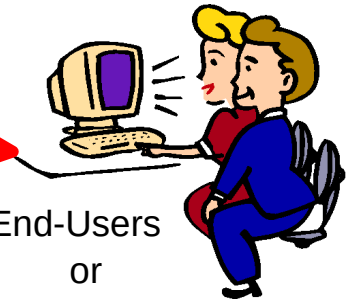
How do you interface with DirMaint

USER DIRECT

Directory 3390 ...
Profile IBMDFLT
User MIKE
User LINUX1
User LINUX2
User LINUX3
:

User LINUX99

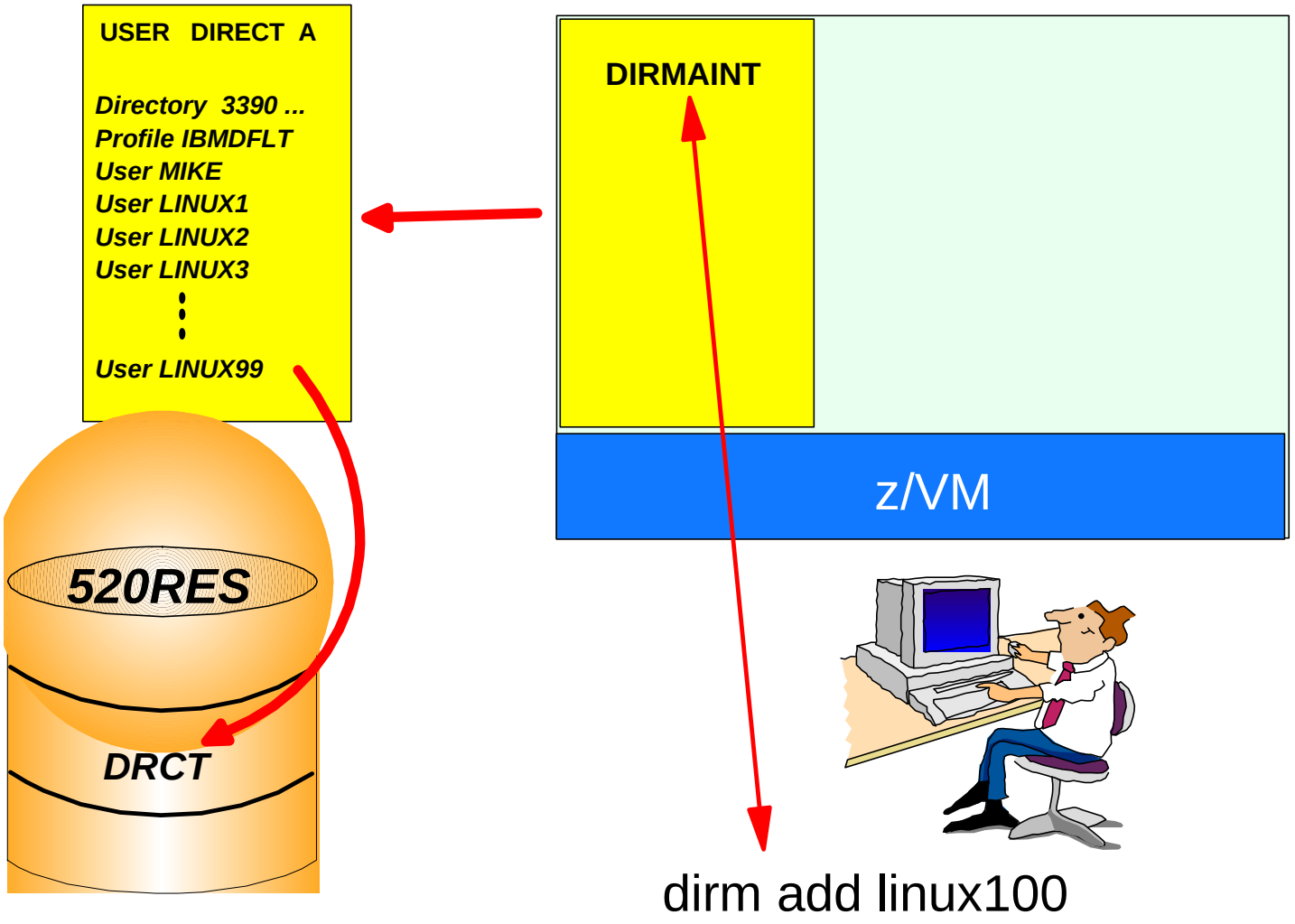
Backup Directory
Admistrator



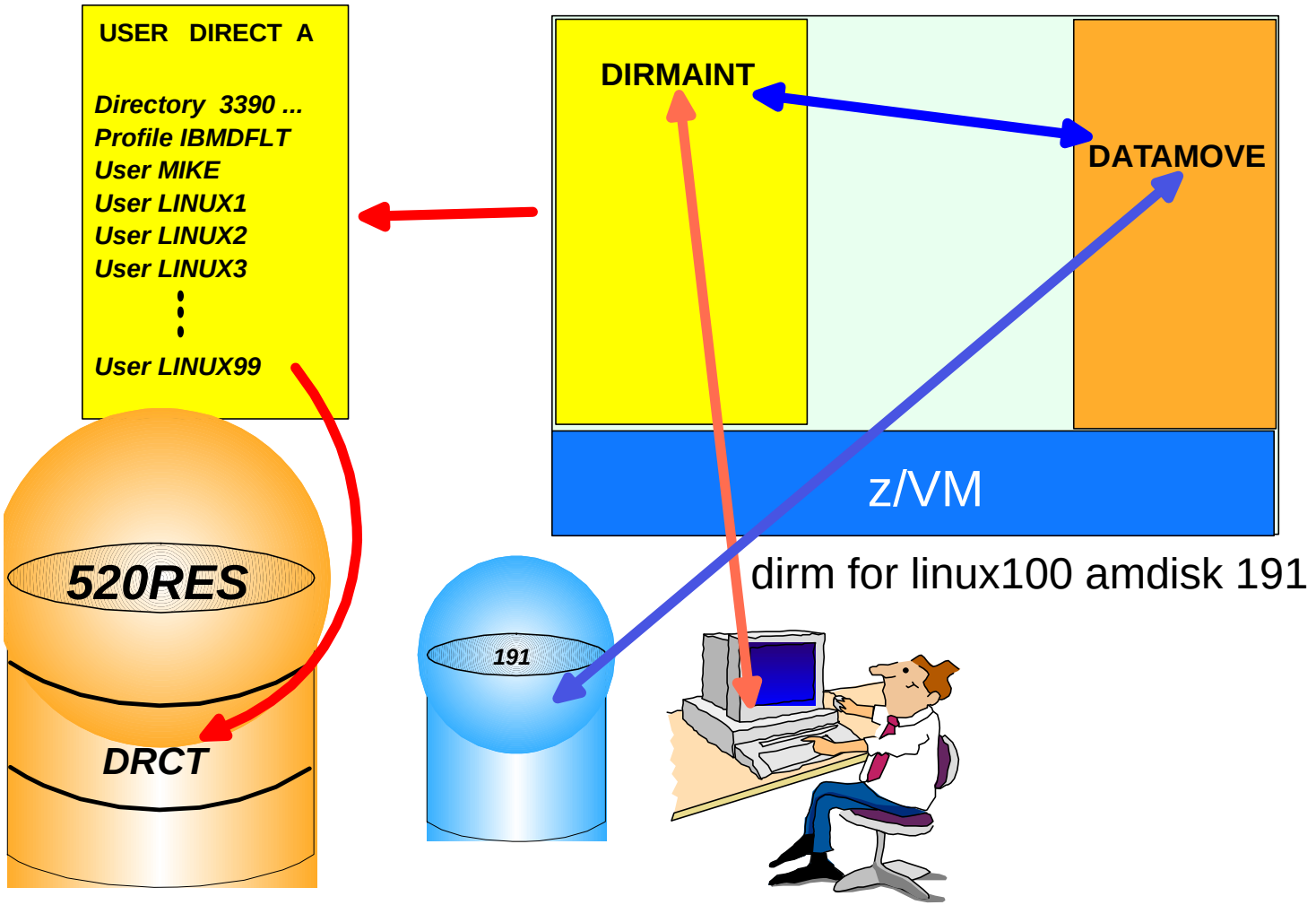
End-Users
or
Linux Admin

Directory Admistrator

How does DirMaint work?

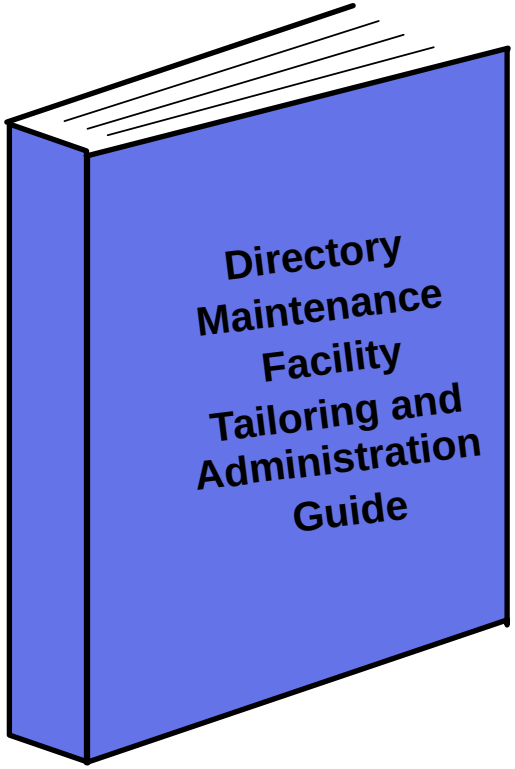


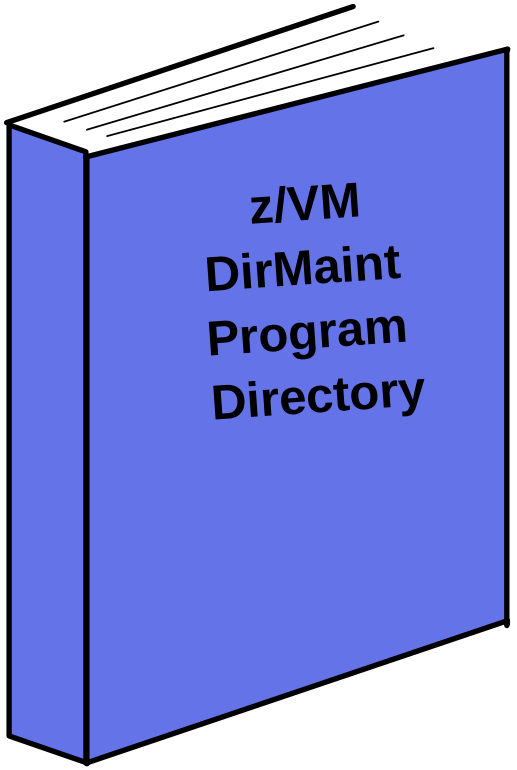
How does DirMaint work? . . .



Installation Process

DirMaint Manuals



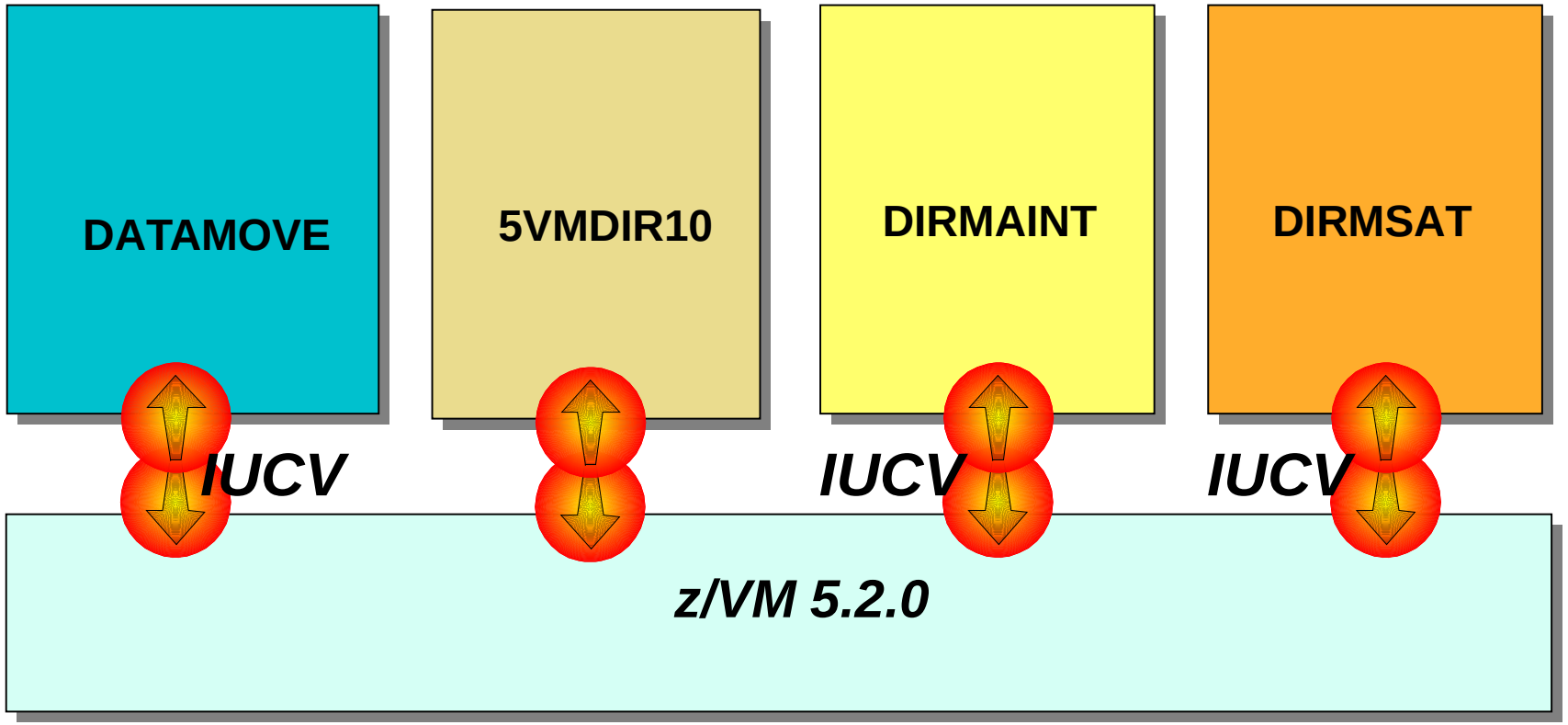


www.vm.ibm.com/pubs

Download in PDF format

Check also: http://www.vm.ibm.com/related/dirmaint/

DirMaint Service Virtual Machines



System Config - Product Statement

```
 SYSTEM   CONFIG   Z1  F 80  Trunc=80 Size=278 Line=264 Col=1 Alt=0
===>
264 /*                 PRODUCT ENABLE/DISABLE INFORMATION
265 /*************************************************************
266
267 PRODUCT PRODID 5684096K STATE ENABLED DESCRIPTION '00/00/00.00:00
268 RSCS Networking Version 3 Release 2 Modification 0'
269
270 PRODUCT PRODID 5VMDIR10 STATE ENABLED DESCRIPTION '00/00/00.00:00
271 DIRECTORY MAINTENANCE FL 510'
272
273 PRODUCT PRODID 5767002P STATE ENABLED DESCRIPTION '00/00/00.00:00
274 RACF for VM/ESA V2'
275
276 PRODUCT PRODID 5VMPTK20 STATE ENABLED DESCRIPTION '00/00/00.00:00
277 PERFORMANCE TOOLKIT FOR VM'
278
279 * * * End of File * * *
```

Query Product Command

```
q product

Product  State    Description
5VMDIR10 Enabled  01/16/06.19:18:45.MAINT    Install/service
DirMaint using minidisk
5VMPTK20 Enabled  01/16/06.16:00:31.MAINT    PERFKIT Minidisk
Install and Service
5684096K Disabled 00/00/00.00:00:00.$BASEDDR RSCS Networking
Version 3 Release 2  Modification 0
5767002P Disabled 00/00/00.00:00:00.$BASEDDR RACF for VM/ESA V2
Ready; T=0.01/0.01 19:22:14
```

Dynamically Enabling DIRMAINT Program Product

```
service dirm enable
VMFSRV2760I SERVICE PROCESSING STARTED
VMFINS2767I READING VMFINS DEFAULTS B FOR ADDITIONAL OPTIONS
VMFINS2760I VMFINS PROCESSING STARTED
VMFINS2602R THE FOLLOWING COMPONENTS CAN BE ENABLED FOR PROD 5VMDIR10 DIRM
            ENTER THE NUMBER OF YOUR CHOICE
(0) BYPASS THIS PRODUCT
(1) :PPF 5VMDIR10 DIRM :PRODID 5VMDIR10%DIRM
      :DESC INSTALL/SERVICE DIRMAINT USING MINIDISK
(2) :PPF SERVP2P DIRM :PRODID 5VMDIR10%DIRM
      :DESC DIRECTORY MAINTENANCE FACILITY FUNCTION LEVEL 510
(3) EXIT
VMFINS2603I PROCESSING PRODUCT :PPF 5VMDIR10 DIRM :PRODID 5VMDIR10%DIRM
VMFINS2603I ENABLING PRODUCT 5VMDIR10%DIRM
VMFINS2771I THE CP SET PRODUCT COMMAND COMPLETED SUCCESSFULLY FOR PRODUCT
            5VMDIR10
                                ●
                                ●
                                ●
VMFBLD2180I THERE ARE 0 BUILD REQUIREMENTS REMAINING
VMFBLD2760I VMFBLD PROCESSING COMPLETED SUCCESSFULLY
VMFSUI2760I VMFSUFIN PROCESSING COMPLETED SUCCESSFULLY FOR PRODUCT 5VMDIR10%DIRM

VMFSUI2760I VMFSUFIN PROCESSING COMPLETED SUCCESSFULLY
VMFSUT2760I VMFSUFTB PROCESSING STARTED
VMFSUT2760I VMFSUFTB PROCESSING COMPLETED SUCCESSFULLY
VMFSRV2760I SERVICE PROCESSING COMPLETED SUCCESSFULLY
```

Installation Process

- Enable the DirMaint product
- Perform Post-installation Tasks
- Place DirMaint Files into Production

DirMaint Files

Important DirMaint Files

- **CONFIG DATADVH**
- **CONFIG99 DATADVH**
- **WHERETO DATADVH**
- **AUTHFOR CONTROL**
- **DATAMOVE DATADVH**
- **EXTENT CONTROL**
- **DEFAULTS DATADVH**
- **RPWLIST DATA**

DirMaint Commands

Some Useful DirMaint Commands

SEND - Request a copy of a DirMaint control file
FILE - Add or replace a DirMaint control file
RLDCode - Cause DirMaint to reload its resident operating procedures
RLDExtn - Cause DirMaint to reload its CONFIG* DATADVH file
Add - Add a new user or profile directory entry
REView - Review a user or profile directory entry
AMDisk - Adds a new minidisk
DEDicate - Add or delete an existing dedicate statements
DMDisk - Removes a minidisk
LOGONBY - Allows users to use their own password to logon to different IDs
MDisk - Change the access mode and passwords for minidisks
STorage - Change logon storage size
SETOptn - Add, change or delete CP options
CLAss - Change the CP class for a directory entry
SPEcial - Add or delete an existing special statement
TMDisk - Transfer ownership of a minidisk from one userid to another

DirMaint HELP MENU

```
      ADVH MENU        Menu Help Information
 *DVHAMENG CHngid     DLink      INVen      NICDEF     QLog       SHARE
 *DVHUCENG CHVaddr    DMDisk     IOPriori   NOPdata    Qry        SHUTDOWN
 *UDVH     CLAss      DROPBy     IPL        NOTAPE     QUery      SPEcial
 ?         CLONEDisk  DROPFor    IUCV       OFFline    REPlace    SPOOL
 :ADVH     CMDisk     DROPScif   Link       ONline     REView     STAG
:HELP     CMS        DSECuser   LOADDEV    OPtion     RLDCode    STATus
 ACCount   CONsole    DUMP       LOCK       POOL       RLDData    STDEvopt
 ACIgroup  CP         D8ONECMD   LOGmsg     POSIXFSRo  RLDExtn    STorage
 ACNTAdd   CPU        ELink      LOGONBY    POSIXGLIs  RMDisk     SUPGLIST
 ACNTDel   CRYpto     ENable     MACHine    POSIXGROu  SATellite  SYSaffin
 Add       DASDOPT    EXECDrop   MAIL       POSIXINFo  SCAn       Term
 AMDisk    DATamove   EXECLoad   MAXSPool   POSIXIUPg  SCReen     TESTpw
 APPCpass  DATEForma  EXTNchk    MAXstorag  POSIXIWDi  SECuser    TMDisk
 AUTHBy    DEDicate   FILE       MAXstore   POSIXOPT   SEND       UNLock
 AUTHFor   DEFAULTs   FREExt     MDAUDit    PRIORity   SETAcnt    USEDext
 AUTHLink  DEFINESTa  Get        MDisk      PRIOset    SETClass   USER
 AUTHScif  DIRECT     GETCONsol  MDPW       PRIVclass  SETCPU     USERMAP
 AUTOlog   DIRECTORy  GLOBALOpt  MINIOPT    PURGE      SETMach    USEROPtn
 BACKUP    DIREDIT    GLObalv    MMDisk     PW         SETOptn    WORKUNIT
 BATch     DIRMAP     HELP       NAMEsave   PW?        SETPRiori  XAUtolog
 CHECK     DISAble    HISTory    NEEDPASS   PWGen      SETpw      XCONfig
 CHKsum    DISTrib    INClude    NEWS       PWMON      SETSTAG    XSTORE
```

DIRM CLONEDISK

```
----------------------DirMaint CLONEdisk--------------------------
To add a new minidisk to a user definition, fill in the following:
  Minidisk Address ===> 191
  Source Owner ID  ===> gumby
  Source Address   ===> 191
Optionally, fill in one of the following rows for a new allocation:
  Explicit Start ===>              Volser ===>
               AUTOV               Volser ===> gen150
               AUTOG               Grpname===>
               AUTOR               Region ===>
               DEVNO   Real Device Number ===>
Optionally, for a new allocation, also fill in:
  Link Mode ===> mr
  PWS  Read ===>       Write ===>        Multi ===>        (passwords)



5741-A05 (c) Copyright IBM Corporation 1979, 2004.
   1= Help     2= Prefix Operands      3= Quit     5=Submit       12=Cursor
```

DIRM FOR CMS1 CLONEDISK

CLONEDISK - Output

```
DVHXMT1191I Your CLONEDISK request has been sent for processing.
Ready; T=0.11/0.12 08:48:48
 DVHREQ2288I Your CLONEDISK request for CMS1 at * has been accepted.
 DVHSCU3541I Work unit 14084849 has been built and queued for processing.
 DVHSHN3541I Processing work unit 14084849 as MAINT from ZVML76,
 DVHSHN3541I notifying MAINT at ZVML76, request 60 for CMS1 sysaffin *;
 DVHSHN3541I to: CLONEDISK 0191 GUMBY 0191 AUTOV GEN150 MR PWS XXX XXX
 DVHSHN3541I XXX
 DVHBIU3450I The source for directory entry CMS1 has been updated.
 DVHBIU3450I The source for directory entry DATAMOVE has been updated.
 DVHBIU3450I The source for directory entry DATAMOVE has been updated.
 DVHBIU3450I The source for directory entry DATAMOVE has been updated.
 DVHBIU3450I The source for directory entry CMS1 has been updated.
 DVHDRC3428I Changes made to directory entry CMS1 have just been placed
 DVHDRC3428I online.
 DVHDRC3428I Changes made to directory entry DATAMOVE have just been
 DVHDRC3428I placed online.
 DVHBIU3450I The source for directory entry DATAMOVE has been updated.
 DVHRLA3891I Your DMVCTL request has been relayed for processing.
 DVHREQ2289I Your CLONEDISK request for CMS1 at * has completed; with
 DVHREQ2289I RC = 0.
```

Password Expiration and Characteristics

- How often do they have to be changed ?
- Should you receive a warning when it is about to expire ?
- What happens when your password expires ?
- Format of the Password ?
  - Minimum length of passwords
  - Alpha-numeric requirements for passwords
- Exclude certain virtual machines form password expiration ?

CONFIG99 DATADVH

```
 CONFIG99   DATADVH  A2  V 80  Trunc=80 Size=1324
====>
 00477     PW_INTERVAL_FOR_GEN= 160 180
 00478     PW_INTERVAL_FOR_PRIV= 70 90
 00479     PW_INTERVAL_FOR_SET= 180
 00480     PW_WARN_MODE= AUTOMATIC
 00481     PW_LOCK_MODE= AUTOMATIC
 00482     PW_NOTICE_PRT_CLASS= A
 00483     PW_NOTICE_RDR_CLASS= A
 00484     PW_MIN_LENGTH=   5
 00485     PW_MONITOR=    SYSADMIN
 00486     PW_REUSE_HASHING_EXIT=         DVHHASH  MODULE
 00487     PW_REUSE_INTERVAL=  365 DAYS
```

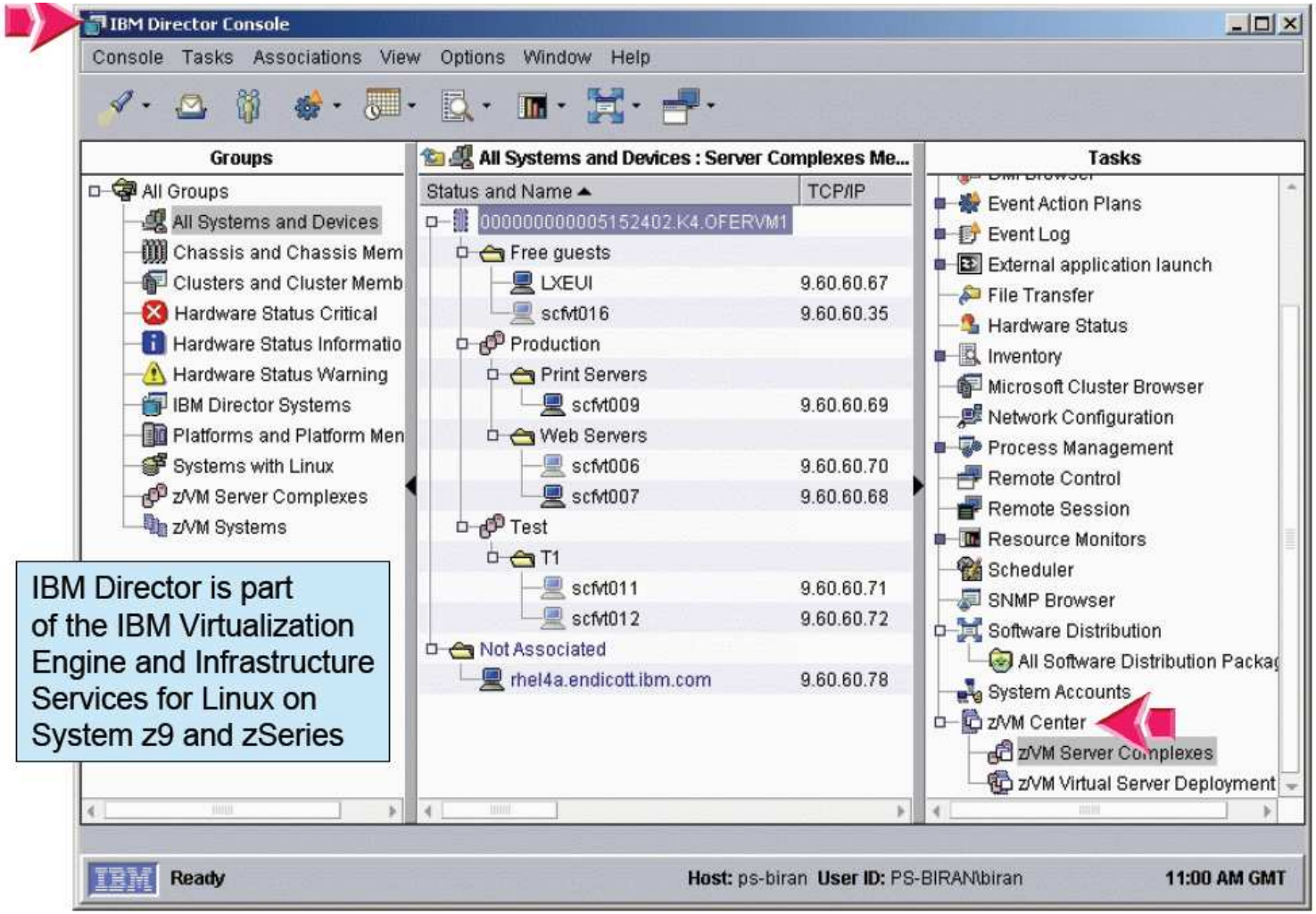
Now set the PW with an expiration date

```
dirm for gumby setpw  billbob vpw billbob  60 days
DVHXMT1191I Your SETPW request has been sent for processing.
Ready; T=0.05/0.05 11:07:55

DVHREQ2288I Your SETPW request for GUMBY at * has been accepted.
DVHBIU3450I The source for directory entry GUMBY has been updated.
DVHBIU3423I The next ONLINE will take place via Diagnose 84.
DVHBIU3428I Changes made to directory entry GUMBY have been placed
DVHBIU3428I online.
DVHREQ2289I Your SETPW request for GUMBY at * has completed; with RC =
0.
```

Misc.

IBM Director



- „Prereq“ for using IBM Director in z/VM environment is DirMaint
- More details: Visit session V11 IBM Virtualization Engine and IBM Director

DirMaint Summary

- For simplified and productive user management (directory management)
- Multiple administrators – different roles possible.
- Directory management possible via commands
  - Scripting
  - Delegation on command level is possible
  - Can be used by tools (self-written, z/VM-APIs, IBM Director, Levanta) – remote
- Dirmaint is not a security tool! Don‘t misunderstand, only security like tool (see password expiration)

Resource Access Control Facility

RACF/VM

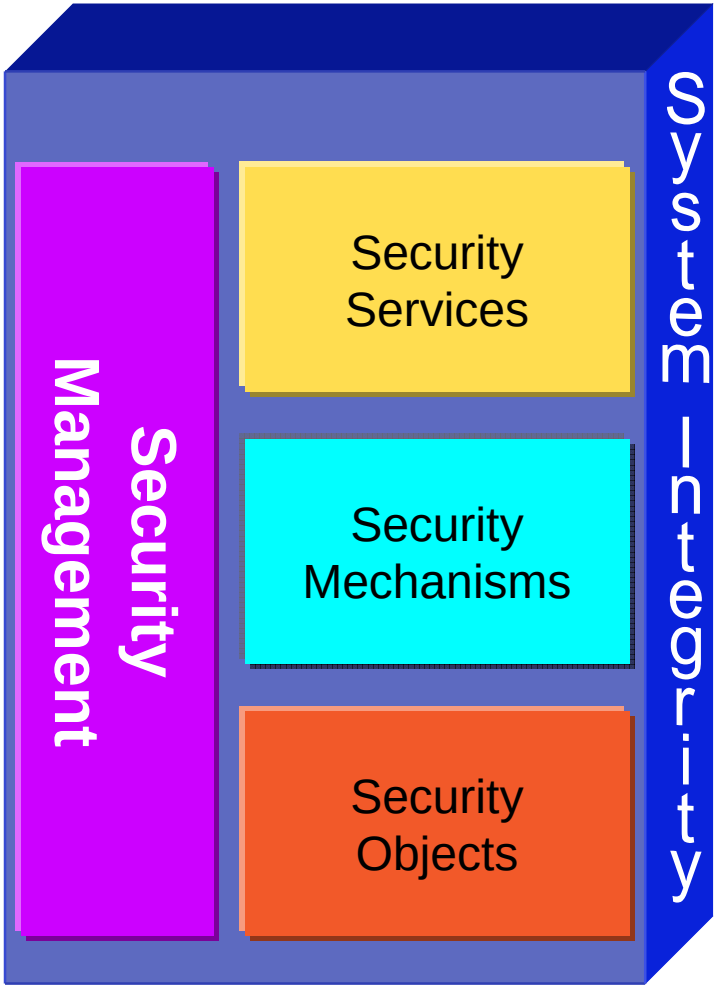
What is RACF?

- IBM Resource Access Control Facility for z/VM (RACF/VM) is a Pre-installed Priced Program Product that provides system and data security
- RACF Version 1 Release 10 is a product that works together with the existing system features of z/VM to provide improved data security for your installation.
- RACF enhances the security and auditability features of the z/VM operating system.
- RACF helps meet the need for security by providing:
  - Flexible control of access to protected resources (mdisk and sfs)
  - Protection of installation-defined resources (ftp, vswitches, etc.)
  - Choice of centralized or decentralized control of profiles
  - Transparency to end users

RACF Security Architecture

- System security
  - Identification & Authentication
    - –Identify users, ensure accountability
  - Access Control
    - –Limiting / controlling access to information
  - Auditing
    - –Verification of security policy enforcement
  - System Integrity
    - –Security mechanisms cannot be compromised
- Application security
  - A way for applications to extend the controls present in the operating system

Based on ISO 7498-2



User Identification and Authentication

- Password management
  - Only user knows the password
  - User can change his or her own password
  - Security administrator or hacker cannot read the password
    - One-way DES encryption
  - Security administrator *can* reset the password (temporary)

User Identification and Authentication

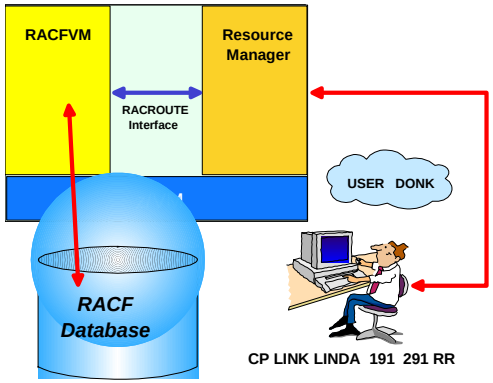
- Password policies
  - Required change interval and expiration warnings
  - Content and length
  - Re-use
  - Encryption
  - Exits are available to control generation and validation of passwords
- User policies
  - Automatic suspension of inactive users
  - Automatic revocation of users due to invalid password count
  - Notification of last system access

User attributes

- Extraordinary system-wide privileges
  - SPECIAL – All privileged RACF commands
  - AUDITOR – monitor system security
  - OPERATIONS – full resource access
- Extraordinary user privileges
  - Group SPECIAL – applies only to members of the user's group and the resources those users own.
  - Group AUDITOR - monitors security for the group
  - Group OPERATIONS – access to resources owned by the the group or the users in that group
  - Group authorities - USE, CREATE, CONNECT, and JOIN

Authorization

- Access rights are based on VM user ID
- CP tells RACF “UserA is LINKing UserB’s 191 minidisk. OK?”
- RACF responds:
  - Yes: READ
  - No
  - Don’t know; figure it out for yourself - a.k.a “defer”

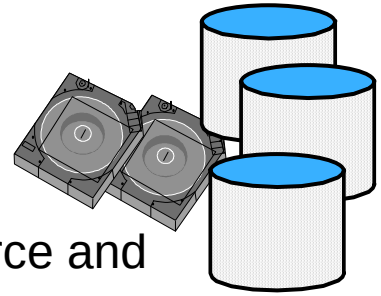


Elements of RACF

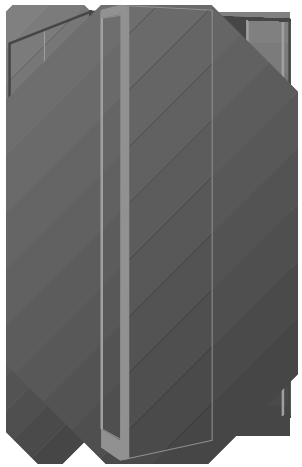
Users

User identification and authentication

Resources

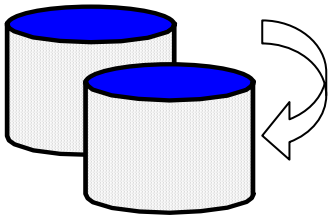


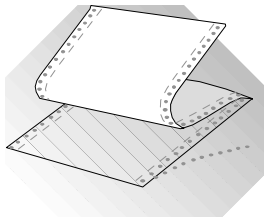
Resource and System access controls



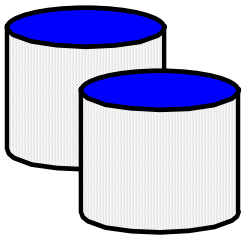
Security administration

Audit trail





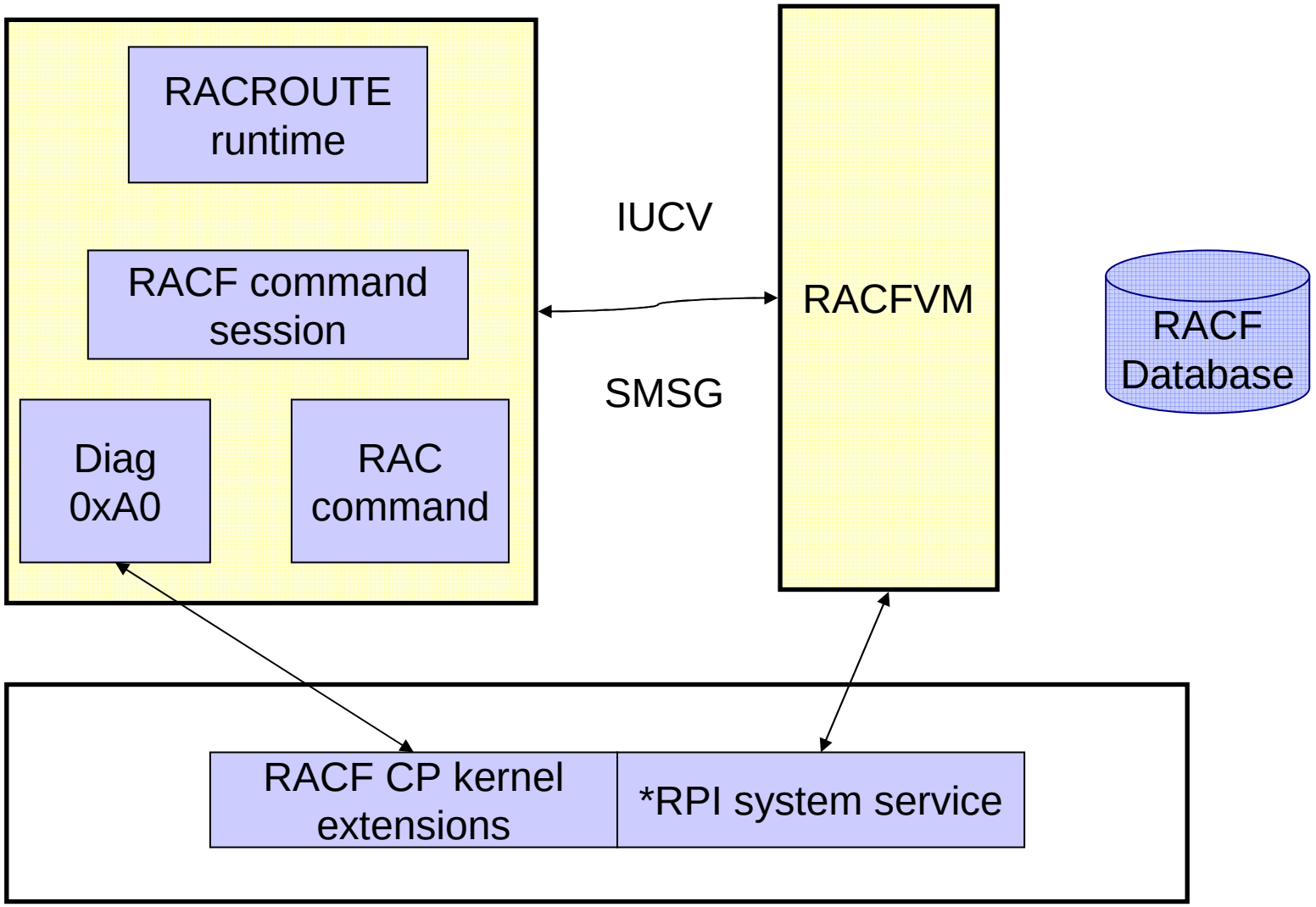
Audit and Integrity reports



RACF database
- Primary and secondary
- Local sharing

Security console
- Violation reporting
- OPERATOR

RACF for z/VM Structure

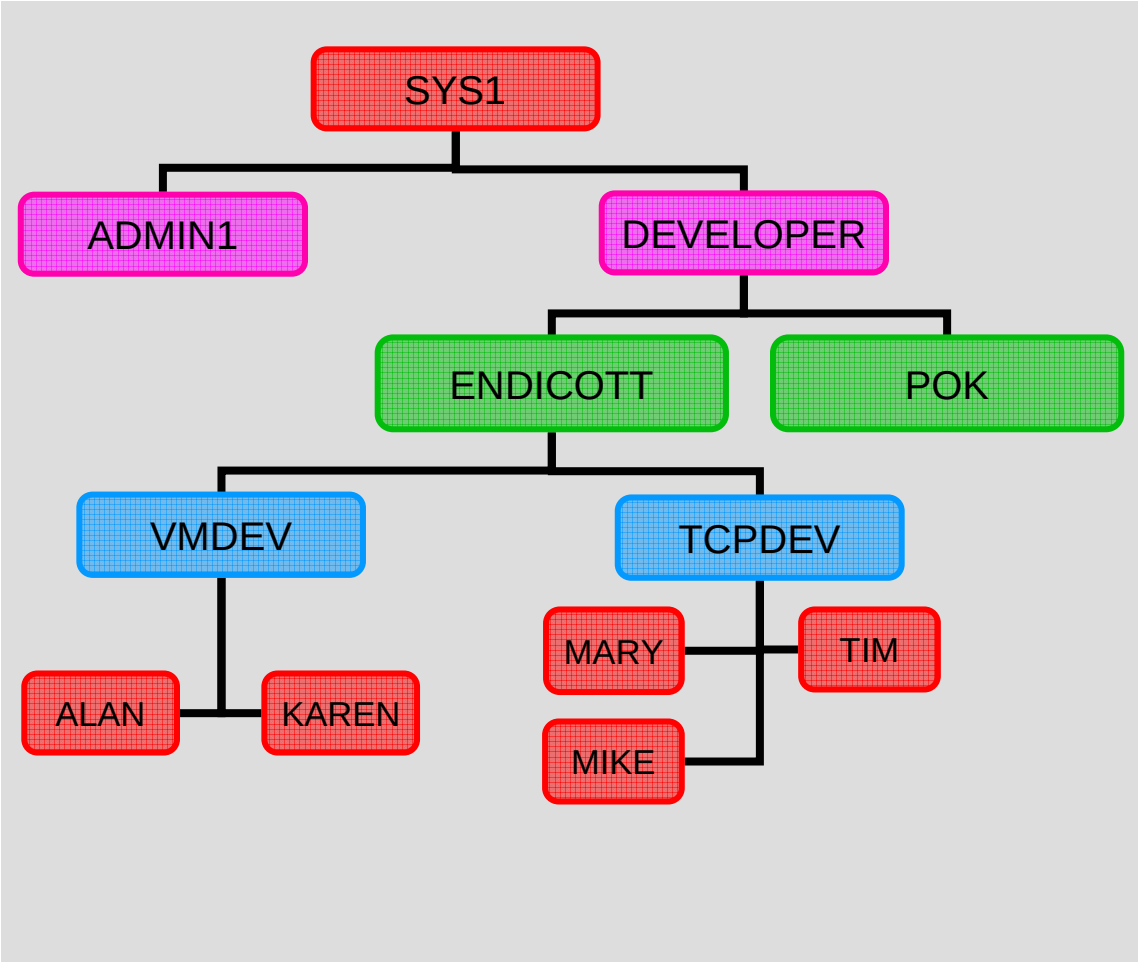


Features and Functions

- Protected system access
  - One-way DES password encryption
  - Where and when controls
  - Intrusion detection and defense
- Resource access control lists
- Groups
- Separation of duties: security admin, operations, auditor
- Multi-level security (MLS)
- Real-time violation notification
- Audit reporting tools
- Integrity verification tool (DSMON)
- Synergy with z/OS

RACF Groups

- Represents a group of users
- Users can belong to more than one group (one at a time)
- Groups have access rights
- Resources can be owned by a group
- Delegate group management - reduce administration effort



RACF Administrative Commands

Function	User	Group	Resource
Create	ADDUSER	ADDGROUP	RDEFINE
Change	ALTUSER	ALTGROUP	RALTER
Delete	DELUSER	DELGROUP	RDELETE
Display	LISTUSER	LISTGROUP	RLIST

- PASSWORD
  - Change pw or change interval
- PERMIT
  - Modify resource ACL
- SEARCH
  - Scan RACF database
- CONNECT
  - Associate user with a group
- REMOVE
  - Undo Connect
- SETROPTS
  - Control RACF processing
- SETEVENT
  - Modify VM events that are to be audited or controlled
- SETRACF
  - Turn RACF on or off
- RVARY
  - Deactivate RACF database

Resource Profiles

- Profiles describe resources
  - One for each resource or collection of similar resources
  - Owner
  - Auditing
  - “Universal” (default) access rights
  - Access list
  - Security classification
  - Notification settings
  - Statistics

Example – protecting a minidisk – Access Rights

- `RDEFINE VMMDISK BRUCE.191 UACC(NONE)`
- `PERMIT BRUCE.191 CLASS(VMMDISK) ID(ALAN) ACCESS(READ)`
- `RDEFINE VMMDISK MAINT.190 UACC(READ)`
- `SETROPTS CLASSACT(VMMDISK) RACLIST(VMMDISK)`

RACF audit trail

- Any CP command, diagnose, or system function can be audited
- Only LOGON, XAUTOLOG, and AUTOLOG are audited by default
- Two audit log files
  - Automatic swap
  - Facility is available to dump inactive log to permanent storage and clear it
  - Can (should) configure RACF to fail requests if both logs are full

RACF control of CP functions

- A subset of CP functions are controllable
  - APPCVM CONNECT with password
  - Links to minidisks (whether by command or by user directory)
  - STORE HOST
  - COUPLE (Guest LAN and VSWITCH)
  - TAG and TRANSFER
  - TRSOURCE
  - Use of restricted DCSS (diag 0x64) or NSS (IPL)
  - Diagnose 0xA0, 0xD4, 0xE4, 0x280
  - LOGON, XAUTOLOG, AUTOLOG (mandatory)
- If a function is not controlled, authorization is determined by CP

RACF control of CP functions

- Controlled by profiles in the VMXEVENT class
- The member list of a VMXEVENT profile specifies which CP functions are audited and which are controlled
- SETEVENT LIST shows which functions are being audited and controlled
- SETEVENT REFRESH is used to alter the settings
  - May select another VMXEVENT profile
- VMXEVENT profiles can be defined at an individual user level to override system-wide settings

Control of z/VM Commands and Diagnoses…

- When a function is controlled using VMXEVENT, CP calls RACF to authorize a request when that function is used
- At this point, RACF protection is handled by:
  - Defining RACF profiles which provide the security definition of the protected resource
  - Activating the appropriate RACF class

RACF classes which control CP events

VMMDISK	Minidisk access via LINK command
VMRDR	Ability to send files to unit record devices of a user via TRANSFER, SPOOL, etc commands
VMNODE	Ability to send files to RSCS nodes using the TAG command
VMBATCH	Ability to work on behalf of another user using Diagnose 0xD4
VMSEGMT	Use of a restricted named saved segment (NSS) or discontinous saved segment (DCSS)
VMCMD	Various CP commands: STORE, XAUTOLOG, TRSOURCE, etc
VMLAN	Authorization to couple to a Guest LAN or Virtual Switch

RACF classes which control CP events . . .

VMXEVENT	CP events that can be controlled or audited
VMMAC	Used with MLS support (SECLABELs)
VMPOSIX	OpenExtensions
SECLABEL	Information sensitivity and partitioning (MLS)
TERMINAL	Local, SNA, or telnet terminals
SFSCMD	Shared File System server operator commands
FACILITY	Use of RACROUTE macro
SURROGAT	LOGON BY
TAPEVOL	Tapes (if supported by tape management system)

Logon controls

- RACF is called whenever a user enters the system via LOGON, AUTOLOG, or XAUTOLOG
  - This is unconditional – cannot disable in the VMXEVENT profile
- Passwords are one-way encrypted in the RACF database
- Undefined users cannot logon
- Can control which terminals a user can log on to using the TERMINAL class
  - Telnet IP addresses can be mapped into terminal names
    - 9.12.248.3 = 090CF803

Support for shared user IDs (LOGON BY)

- Define **LOGONBY.*userid*** in SURROGAT class and permit surrogate users with READ access
- Users specify LOGON <shared> BY <surrogate>, specifying their own password
- Audit trail identifies shared and surrogate user IDs for subsequent authorizations
- Shared users cannot be logged onto directly by default.
  - Can be allowed by permitting user to its own SURROGAT class profile

RACF Monitoring

- Immediate notification of abnormal security events
  - Sent to system operator console
    - As defined in CSTCONS table
  - Optionally sent to resource owner
- Types of messages
  - Unsuccessful system accesses
  - Unsuccessful attempts to access resources
  - Failed RACF commands due to insufficient authority
- Messages include who caused the failure and what they were trying to do

RACF Journaling

- Logging of
  - Database status
  - Failed attempts to access the system
  - Resource access (optional)
    - Successes, failures, or both
      - READ, UPDATE, ALTER, CONTROL
  - Access granted with a warning
  - “Failsoft” decisions made by the system operator
- Options can be set by profile owners or auditors

RACF Journaling

- Auditor controls
  - Users
  - SPECIAL users
  - Resources
  - Resource classes
  - RACF command violations

Misc.

z/VM V5 Common Criteria certification

- **New z/VM V5.1 Certification Achieved**
  On October 26, 2005, the German Federal Office of Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) issued its certification that z/VM V5.1 conforms to the requirements of the Controlled Access Protection Profile (CAPP) and the Labeled Security Protection Profile (LSPP), both at Evaluation Assurance Level 3+. **IBM intends to evaluate z/VM V5.2 with the RACF for z/VM** optional feature for conformance to the Controlled Access Protection Profile (CAPP) and Labeled Security Protection Profile (LSPP) of the Common Criteria standard for IT security, ISO/IEC 15408, **at Evaluation Assurance Level 4 (EAL4).**

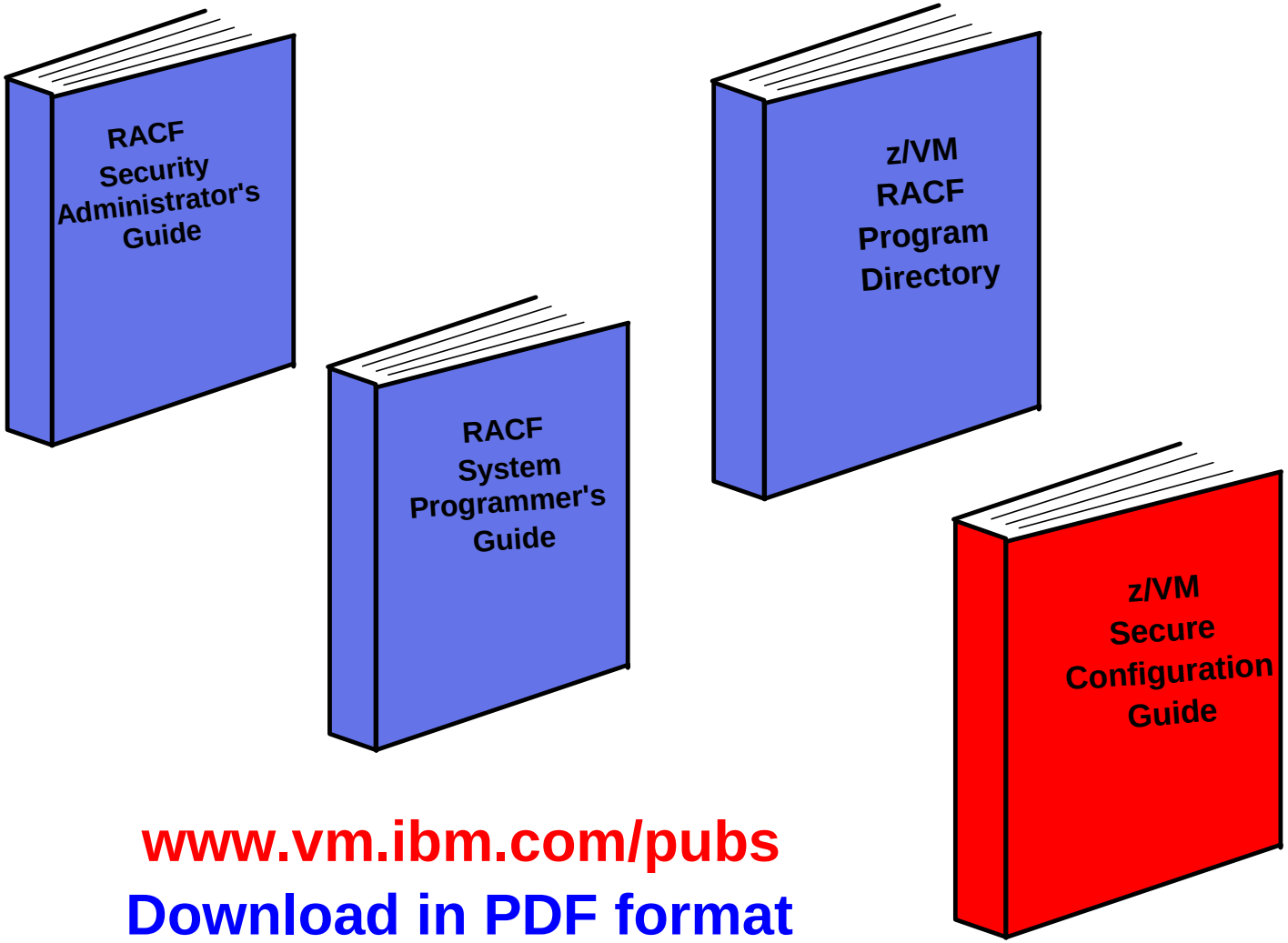
- http://www-03.ibm.com/systems/z/security/ccs_certification.html

Sharing RACF Databases

- If you intend to share a RACF database between different systems, please see RACF System Programmer‘s Guide in chap. 5 „Sharing a RACF database“ for details.
  - You need at least one full-pack minidisk

Installation

RACF Manuals for z/VM



www.vm.ibm.com/pubs

Download in PDF format

Check also: http://www-03.ibm.com/servers/eserver/zseries/zos/racf/

RACF Installation Overview

- Plan your installation
- Allocate resources
- Install / Enable the RACF product
- Perform post-installation tasks
  - Information about file tailoring and initial activation of the program is presented in 6.9, “Task 7. Create PROFILE EXEC and SMF CONTROL Files for the RACF Service Machines” on page 46 through 6.27, “Task 25. Set Up the RACF ISPF Panels (Optional)” on page 85.
- Place RACF files into production
  - Once the product files have been tailored and the operation of RACF is satisfactory, copy the product files from the test BUILD disk(s) to the production BUILD disk(s).

RACF Installation Overview . . .

After building a new CPLOAD Module with active RACF modules
(keep a backup version of the „old“ CPLOAD/Nucleus module)

- IPL the CP System with RACF with NOAUTOLOG option

```
STAND ALONE PROGRAM LOADER: z/VM VERSION 5 RELEASE 2.0

DEVICE NUMBER:   0440       MINIDISK OFFSET:   00000000   EXTENT:  2

MODULE NAME:     CPLOAD     LOAD ORIGIN:       1000

--------------------------------IPL PARAMETERS--------------------------

---------------------------------COMMENTS-------------------------------

------------------------------------------------------------------------

9= FILELIST  10= LOAD  11= TOGGLE EXTENT/OFFSET
```

```
 14:17:57 z/VM  V5 R2.0  SERVICE LEVEL 0401 (64-BIT)
 14:17:58 SYSTEM NUCLEUS CREATED ON 2005-12-19 AT 13:48:53, LOADED FROM 520RES
14:17:58
14:17:58 ************************************************************
14:17:58 * LICENSED MATERIALS - PROPERTY OF IBM*                      *
14:17:58 *                                                           *
14:17:58 * 5741-A05 (C) COPYRIGHT IBM CORP. 1983, 2004. ALL RIGHTS    *
14:17:58 * RESERVED. US GOVERNMENT USERS RESTRICTED RIGHTS - USE,     *
14:17:58 * DUPLICATION OR DISCLOSURE RESTRICTED BY GSA ADP SCHEDULE   *
14:17:58 * CONTRACT WITH IBM CORP.                                    *
14:17:58 *                                                           *
14:17:58 * * TRADEMARK OF INTERNATIONAL BUSINESS MACHINES.           *
14:17:58 ************************************************************
14:17:58
14:17:58 HCPZCO6718I Using parm disk 2 on volume 520RES (device 0440).
14:17:58 HCPZCO6718I Parm disk resides on cylinders 84 through 128.
14:17:58 Start ((Warm|Force|COLD|CLEAN) (DRain) (DIsable)  (NODIRect)
14:17:58       (NOAUTOlog)) or (SHUTDOWN)

warm drain noautolog
                                                    CP READ   DETRO
```

- Start the RACMAINT virtual machine
  xautolog racmaint
- Logon with IBMUSER (this is the only possible userid to use)

RACF Installation Overview . . .

As IBMUSER link and access of some resources
to run exec RPIBLDDS to „initialize“ the RACF database

```
LOGON IBMUSER
RPIMGR042I PASSWORD EXPIRED

To change your password - enter: nnn/nnn  where nnn = new password
or, enter LOGOFF to cancel
   xxxxxxx/xxxxxx
ICH70001I IBMUSER  LAST ACCESS AT **:**:** ON ****, **** **,****
HCPRPW004I Password changed
RPIMGR031E RESOURCE MAINT.190 SPECIFIED BY LINK COMMAND NOT FOUND
RPIMGR031E RESOURCE MAINT.19E SPECIFIED BY LINK COMMAND NOT FOUND
RPIMGR031E RESOURCE 5767002P.29E SPECIFIED BY LINK COMMAND NOT FOUND
RPIMGR031E RESOURCE 5767002P.505 SPECIFIED BY LINK COMMAND NOT FOUND
RPIMGR031E RESOURCE 5767002P.191 SPECIFIED BY LINK COMMAND NOT FOUND
RPIMGR031E RESOURCE IBMUSER.191 SPECIFIED BY LINK COMMAND NOT FOUND
z/VM Version 5 Release 1.0, Service Level 0401 (64-bit),
built on IBM Virtualization Technology
There is no logmsg data
FILES:   NO RDR,   NO PRT,   NO PUN
LOGON AT 14:31:08 EST WEDNESDAY 01/19/05
DMSACC724I 19E replaces Y (19E)
DMSACP723I Y (19E) R/O
```

```
rpibldds  rpidirct
Processing batch file RPIDIRCT SYSUT1 using "RAC" command interface
 => RDEFINE VMCMD RACF UACC(READ)
 => RDEFINE VMCMD RAC UACC(READ)
 => ADDGROUP SYSTEM
 => ALTGROUP SYSTEM OVM(GID(0))
 => ADDGROUP STAFF
 => ALTGROUP STAFF OVM(GID(1))
 => ADDGROUP GADM
 => ALTGROUP GADM OVM(GID(4))
 => ADDGROUP MAIL
 => ALTGROUP MAIL OVM(GID(6))
 => ADDGROUP SECURITY
*
*
 => ADDUSER MAINT DFLTGRP(SYS1) UACC(NONE) PASSWORD(DETRO)
 => RDEFINE VMBATCH MAINT OWNER(MAINT) UACC(NONE)
 => PERMIT MAINT CLASS(VMBATCH) ACCESS(ALTER) RESET
 => RDEFINE VMRDR MAINT UACC(NONE) OWNER(MAINT)
 => PERMIT MAINT CLASS(VMRDR) ID(MAINT) ACCESS(ALTER) RESET
 => CONNECT MAINT GROUP(SYSTEM)
 => ALTUSER MAINT OVM(UID(0))
 => RDEFINE VMMDISK MAINT.CF1 OWNER(MAINT) UACC(NONE)
 => PERMIT MAINT.CF1 CLASS(VMMDISK) RESET ID(MAINT) AC(ALTER)
 => RDEFINE VMMDISK MAINT.CF2 OWNER(MAINT) UACC(NONE)
 => PERMIT MAINT.CF2 CLASS(VMMDISK) RESET ID(MAINT) AC(ALTER)
 => RDEFINE VMMDISK MAINT.CF3 OWNER(MAINT) UACC(NONE)
 => PERMIT MAINT.CF3 CLASS(VMMDISK) RESET ID(MAINT) AC(ALTER)
```

RACF Installation Overview . . .

- Define Security Administrator and Maintenance User IDs
- Logoff IBMUSER
- Revoke IBMUSER virtual machine (with SYSADMIN)

```
rac altuser sysadmin special
Ready; T=0.01/0.01 14:43:35

rac altuser maint special operations
Ready; T=0.01/0.01 14:43:48

rac altuser bldseg special operations
Ready; T=0.01/0.01 14:44:01


cp logoff
CONNECT= 14:30:00 VIRTCPU= 000:00.49 TOTCPU= 000:00.57
LOGOFF AT 21:44:58 EST THURSDAY 02/03/05

Press enter or clear key to continue
```

```
id
SYSADMIN  AT ZVML76   VIA TCPIP    01/19/05 14:44:14 EST
Ready; T=0.01/0.01 14:44:14
link 5676002p 29e 29e rr
access 29e d
Ready; T=001/0.01  15:52:01
q disk
LABEL  VDEV M  STAT   CYL TYPE BLKSZ   FILES
SAD191 191  A   R/W     1 3390 4096       0
RAC29E 29E  D   R/O     2 3390 4096      52
MNT190 190  S   R/O   100 3390 4096     690
MNT19E 19E  Y/S R/O   250 3390 4096    1038
Ready; T=0.01/0.01 15:51:12


rac altuser ibmuser revoke
Ready; T=0.01/0.01 15:54:38

rac altuser ibmuser nooperations nospecial
Ready; T=0.01/0.01 14:52:24
```

RACF Installation Overview . . .

- Set RACF Options - CLASSACT
- Set RACF Options - Passwords

```
rac setropts classact(vmmdisk)
Ready; T=0.01/0.01 16:32:54

rac setropts classact(vmrdr)
Ready; T=0.01/0.01 16:33:02

rac setropts classact(vmbatch)
Ready; T=0.01/0.01 16:33:11

rac setropts classact(vmsegmt)
Ready; T=0.01/0.01 16:33:40
```

```
Password Rules:

RAC SETROPTS PASSWORD(INTERVAL(90))
Ready; T=0.01/0.01 16:02:06

SETROPTS INACTIVE(30)
Ready; T=0.01/0.01 16:03:16

SETROPTS PASSWORD(REVOKE(4))
Ready; T=0.01/0.01 16:02:06

SETROPTS PASSWORD(HISTORY(6))
Ready; T=0.01/0.01 16:02:06

SETROPTS PASSWORD(RULE1(LENGTH(6:8) ALPHA(1) NUMERIC (2)
ALPHaNUM (3:8))
Ready; T=0.01/0.01 16:02:06
```

RACF Installation Overview . . .

- Place RACF into production using exec PUT2PROD
- Update AUTOLOG1 Profile to start automatically RACF after IPL
- Shutdown – ReIPL (and you are ready...)

```
link autolog1 191 11 mr
Ready; T=0.01/0.01 17:57:25
ac 11 k
Ready; T=0.01/0.01 17:57:30
link autolog2 191 12 mr
Ready; T=0.01/0.01 17:57:35
ac 12 l
Ready; T=0.01/0.01 17:57:39
copy profile exec k = = l (oldd replace

x profile exec k
 PROFILE  EXEC     K2  V 130  Trunc=130
====>
    0 * * * Top of File * * *
    1 /*************************/
    2 /*  Autolog1 Profile Exec  */
    3 /*************************/
    4 XAUTOLOG RACFVM
    5 * * * End of File * * *
```

```
shutdown reipl
            ●
            ●
            ●
DMSACP060E File not found; filemode D(192) will not be accessed
RACFVM  : RACFVM CMS XA Rel 14 03/19/2002
RACFVM  : DMSACP723I B (305) R/O
RACFVM  : DASD 0591 DETACHED
RACFVM  : DASD 0505 DETACHED
RACFVM  : DASD 0590 DETACHED
RACFVM  : RACF is defined to the Z/VM system and the current product,
RACFVM  : status is ENABLED
RACFVM  :
RACFVM  :       RACF
RACFVM  :  Support for VM
RACFVM  :  Version 1.10.0
RACFVM  :
RACFVM  :  Licensed Materials - Property of IBM
RACFVM  :  5740-XXH
RACFVM  :  (C) Copyright IBM CORP. 1981, 1996  All Right
```

Summary RACF/VM

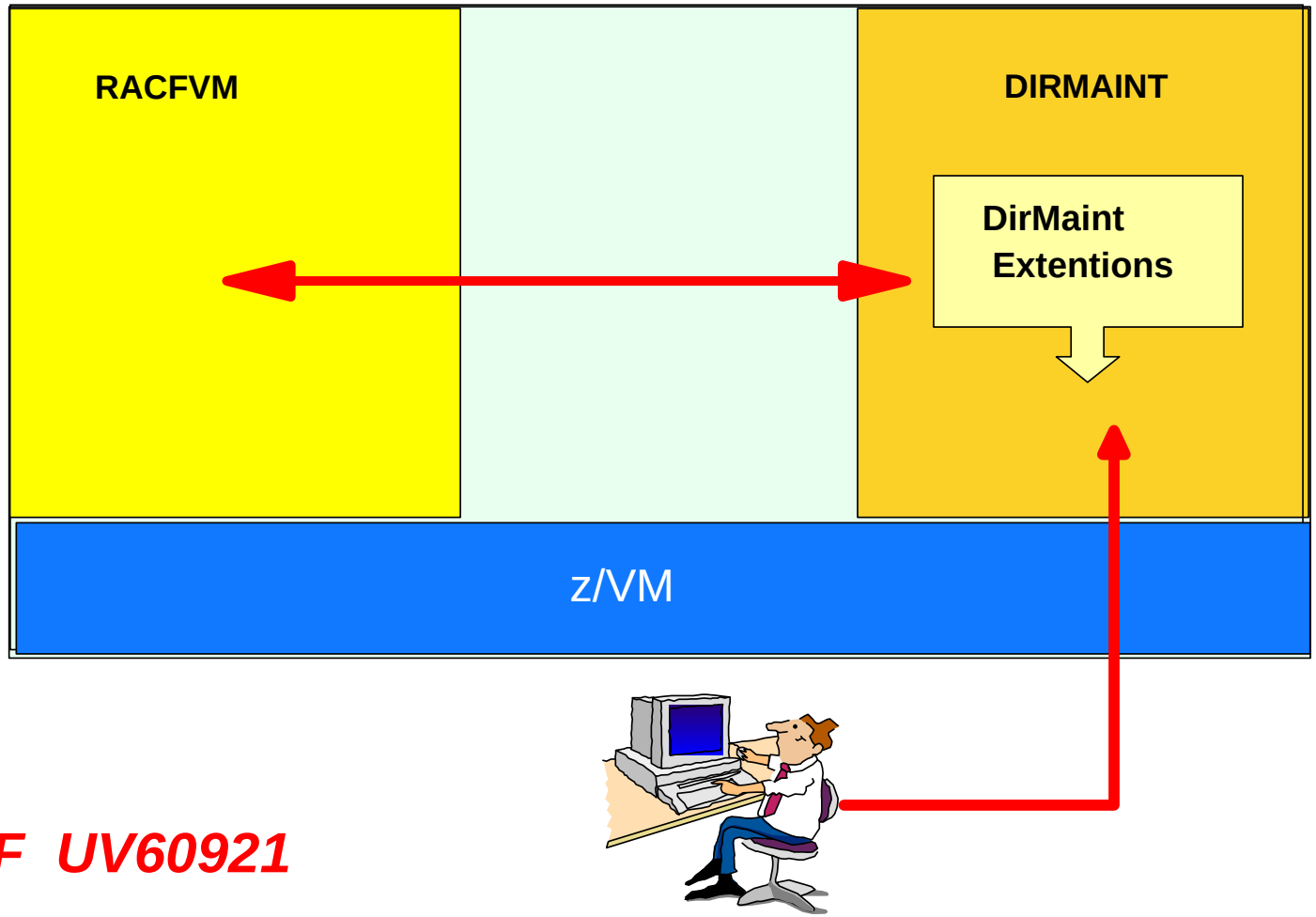
- RACF for z/VM enhances security for z/VM by:
  - Providing fine-grained access controls of VM resources used by users and guests
    - Permits the sharing of VM UserIDs with accountability
  - Auditing capability of VM events – CP commands, diagnoses, access of resources, and authentication
  - Separates the disciplines of security Administrator, Auditor and operations staff
  - Passwords are encrypted, not stored in clear-text.
- Utilities which enable the examination of audit data and security database rules for reporting and data mining
- Depends upon the base system integrity provided by both the z/VM operating system and the zSeries

Combination of Dirmaint and RACF/VM

DirMaint and RACF/VM

How Does RACF and DirMaint work together?

RACF & DirMaint z/VM 5.2.0



PTF UV60921

Simplified User Administration Support

Coordination of DirMaint and RACF Changes

- **z/VM V5.2 can integrate the directory management functions of DirMaintwith the security management functions of RACF**
  - DirMaintcan be configured to notify RACF whenever important changes are made to user definitions and the resources they own
- **Functions that are coordinated by DirMaintwith RACF include:**
  - User creation, deletion, and changes
  - Password management
  - POSIX segment management
  - Access Control Interface (ACI) group management
  - Profile creation and deletion for selected VM functions
- **Benefits:**
  - Reduces the administration effort and skills needed to deploy and manage users and their resources when DirMaint and RACF are used together
  - Eliminates the need to manually define and manage z/VM resources in RACF
  - Helps reduce the chance of incomplete or incorrect RACF configuration data

Wrap-up

Questions ?

Resources and References

- RACF for VM publication library
  - Especially the Security Administrator's Guide
    http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/Shelves/ICHVM07
- IBM Technical Paper - z/VM Security and Integrity
  http://www.ibm.com/servers/eserver/zseries/library/techpapers/gm130145.html
- Security Evaluations for IBM Products
  http://www.ibm.com/security/standards/st_evaluations.shtml
- IBM Security Solutions
  http://www.ibm.com/security
- IBM Global Services – Security and Privacy Services
  http://www.ibm.com/services/security/