CONSUL Risk Management bv

Dutch software research and consultancy firm

Established in 1980

First Computer Security audits in 1984

Performance analysis and reporting software

- since 1986
- used by Memorex Telex worldwide
- worldwide distribution contract with BGS
- **CONSUL/SMS DSCAT**
  used and distributed by IBM

Security oriented software

- for research and consultancy since 1983
- **CONSUL/RACF** since 1989
- distributed by IBM in some countries

CONSUL/Collect

Very efficient collector of all relevant MVS data

- VTOC, VVDS, ICF Catalogs

  describe online datasets

- PDS directories for APF and Linklist datasets

  show programs with sensitivity to APF

- hardware Sense and Device Characteristics data

  describe the physical devices in the I/O farm

- RACF control blocks

  describe options actually in use

- other MVS control blocks

  show actual datasets in use for system tasks

  show security-related options actually in use

CONSUL/Collect

- Speed

number of disks	50	122	360
CPU seconds	5.7	9	11
wallclock seconds	27	45	65
MB of data	5	15	20

- Needs APF

access to VVDS

access to ICF Catalogs without an ALTER permit

access to APF and Linklist datasets without READ permit

- Use of APF options secured with a FACILITY profile

auditability

CONSUL/RACF incentives

- Disaster recovery - sync VTOC / RACF
- Reports for group-administrator
- Removing user references
- Show fields not reported by RACF commands
- Ad-hoc programs needed maintenance for 1.8
- More than 100.000 profiles
- Can do 100 times faster than **ICHUT100**
- PADS maintenance required tools
- Conversion to generics

Later incentives

- Audit tool
- Automated security leak detection
- Resource protection coverage
- System library protection
- AC1 module protection
- Worm hole detection
- Identifying obsolete generics
- Warning if close to RACF restrictions
- RACF 1.9: more than 30 new classes

Target user group

Ad-hoc tool for

- Security administrator
- EDP auditor
- Security officer
- Systems programmer

In addition, automated procedures for

- Moving / removing users and groups
- Reports for group-administrators
- Regular detection of security holes
- Creating input for arbitrary postprocessing

Operation

- Fast, parallel read of all databases
  (supports RDS and non-RDS)
- Needs READ permit on databases (or backups)
- Uses templates for access to profiles fields
- Does not modify database directly
- Generates RACF commands in a file
- Can generate all your own reports / extracts in one pass
- Can match profiles with resources
- Resource data collected by **CONSUL/Collect**
  (included in the product)
- Very fast incore operation

  2-30 Mb region
  5-60 seconds CPU
  10-120 seconds elapsed
- Low I/O load on RACF database
- ISPF display of RACF tables

ISPF incore table display

- Database Name Table
- Range Table
- Class Descriptor Table
- All currently active class options
- Router table
- Authorized Caller Table
- Started Procedure Table
- Tutorial panels

Batch Interface

- Steps to run **CONSUL/RACF**:

  1 Get VTOC/VVDS/Catalog data: **Consul/Collect**

  2 Unload RACF database to flat file (optional)

  3 Create reports

- Easy JCL to run on the live database:

```
//LIST     EXEC PGM=CNRACF
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  select class=user, revoke
  list key, pgmrname, ljdate, passdate
```

- Standard cataloged procedures for most functions
- No ISPF based JCL generator (yet)

Main Batch Commands

- `UNLOAD`

  Snapshot of database to be used subsequently

- `SELECT / EXCLUDE`

  Select or restrict to subset of profiles

- `LIST / SORTLIST`

  Make your own report of profiles field contents

- `VERIFY`

  Consistency checks, internally and with resources

- `REPORT`

  Special-purpose reports

- `(RE)MOVE`

  Generate RACF commands to remove user references

Daily Administration

- Remove users and groups
  e.g. REMOVE USER=*id*
  e.g. REMOVE GROUP=*id*

  permits (3 kinds)

  owner fields

  connects

  notify fields

  user-specific profiles (13 classes)

- Transfer notify (user on holiday)
  e.g. MOVE NOTIFY=*id*, NEWNOTIFY=*id*

- Move user to different department
  e.g. MOVE USER=*id*, TOGROUP=*new*

- Remove from some groups only
  e.g. MOVE USER=*id*, FROMGROUP=(*g1*, *g2*)

- Remove redundant profiles

Dataset profile reports

- Reports meant for central and group administrators

- List access to dataset profiles outside group
  e.g. REPORT OUTOFGROUP

- Same if segregating user and dataset groups
  e.g. REPORT NONDEFAULT

- Find differences with less-specific generic
  e.g. REPORT NONREDUNDANT

- List all profiles
  e.g. REPORT REDUNDANT

- Scope can be limited with SELECT / EXCLUDE
  e.g. SELECT QUAL=SYS1

Accuracy of access control

- Access control system uses a database
  - profiles separate from object definitions
- No referential integrity
  - between resources and profiles
  - between profiles
  - access lists to subjects
    e.g. new user with reused userid
    still has access
- Access exposure through aliasing
  - access by two profiles
    e.g. by incorrect catalog/directories
    e.g. by different access paths
- Relation terminal name - physical location
  e.g. beware of terminal servers and gateways
- Tools exist to identify exposures
  - **CONSUL/RACF** for RACF
  - Security Toolkit for VMS

Verifying Accuracy

- Referential integrity profile -> resource
  e.g. `VERIFY NOTEMPTY`
  e.g. `VERIFY ONVOLUME`
  e.g. `VERIFY PROGRAM`
- Referential integrity resource -> profile
  e.g. `VERIFY PROTECTALL`
- Referential integrity profile -> profile
  e.g. `VERIFY PADS`
  e.g. `VERIFY CONNECT`
- Referential integrity access lists -> subject
  e.g. `VERIFY PERMIT`
- Commands are generated to remedy most situations

Audit Tool

- System dataset protection
  e.g. `REPORT SENSITIVE`
- Modules authorized to bypass RACF
  e.g. `REPORT AC1`
- Worm holes
  e.g. `REPORT SCOPE=*, ACCESS=UPDATE`
- Group administrator scope
  e.g. `REPORT SCOPE=`*id*
- Database accuracy
- Report on profiles (CICS, IMS, FACILITY, ...)
- Ad-hoc extracts for postprocessing
- Non-APF operation possible
  (without APF no VSAM resource data available)

PADS and program control

- List profiles with conditional access lists

  `SELECT CLASS=DATASET, PADS`
- List program profiles

  `SELECT CLASS=PROGRAM`
- Check program referential integrity

  `VERIFY PADS`
- Check program profile dataset existence

  `VERIFY PROGRAM`
- Check program protection AC1 modules

  `REPORT AC1`

Systems Programming and Operations

- List any field from profile, select on any field:

  SMS characteristics, e.g.
  `RESOWNER, STORCLAS, MGMTCLAS`

  verify conformance with SMS installation guidelines

  USER fields, i.e. `USRNM, USRDATA, USRFLG`

  report on products such as CMA-SPOOL

- Combine `DATASET` profiles and actual VTOC entries

  report on protection of JES328X

Summary

- Fast extraction of data from RACF database
- Arbitrary reports based on template field names
- Commands for administrator and auditor
- Match with dataset resources, even VSAM
- Uses MVS security related data
- Functionality grows fast
- Customization possible for Dutch customers

Future enhancements?

- Execution by group-administrators
- Archived resource match (HSM, DMS)
- Tape resource match (CA1, CA-TLMS)
- CICS resource match
- VM resource match
- Terminal resource match
- ISPF table interface to database
- Security label support
- Partially shared DASD
- Simulate SETROPTS options to study effect
- Generate commands to regenerate / restore profiles
- DASD space usage of datasets by profile
- Remove user resources before profile
- Systemwide diagnose
- Combine with SMF audit trail