#SHAREorg

SHARE
Technology · Connections · Results

How-to Access RACF From Distributed Platforms

Saheem Granados
IBM

Wednesday, February 6, 2013
12538

sgranado@us.ibm.com

Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

SHARE in San Francisco 2013

Trademarks

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

- CICS*
- DB2*
- IBM*
- IBM (logo)*
- OS/390*
- RACF*
- Websphere*
- z/OS*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Identrus is a trademark of Identrus, Inc
VeriSign is a trademark of VeriSign, Inc
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

* 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.

Agenda

- Why RACF from Distributed?
- LDAP Primer
- Intro to TDS for z/OS
- RACF Authentication from Distributed
- RACF Authorization from Distributed
- RACF Audit Records from Distributed
- Retrieving RACF Profile Data from Distributed
- Summary
- Additional References

Why RACF from Distributed?

- Heavily invested in RACF for securing z-Specific resources
- Enterprise is becoming more diverse
  - Cost of Securing heterogeneous enterprises can increase if deploying many different security solutions for different platforms
    - New Skills
    - New Software/Hardware
- Centralization of security on z and RACF can be cost effective alternative
  - Leverage existing Security Related procedures/skills
- LDAP facilitates the centralization of enterprise wide security in RACF

What is LDAP?

- Directory – data repository
  - Data stored in Entries managed in a hierarchical fashion, e.g., entries have parent entries
  - Commonly used to store user repository data
    - Also used to store application specific configuration data
  - Each entry contains 1 or more attributes
    - Every entry has a Distinguished Name attribute – unique identifier of the entry
    - Other attributes include password, native ID, etc..
- Lightweight Directory Access Protocol
  - A standard protocol for accessing/managing Directory data over TCP/IP
    - Add, delete, modify entries…
    - Search entries
- Can be key to an enterprises IT security infrastructure
  - Authentication of user
  - Authorization

Directory Server for z/OS

- Tivoli Directory Server is a LDAP server implementation fully optimized for z/OS
  - **Not** a port of distributed TDS server to z/OS
- Supports standard LDAP V3 protocol
- z/OS specific capabilities include
  - Full sysplex support
  - System SSL, ICSF, CTRACE, WLM, ARM, DB2, etc… support
  - LDAP based access to RACF data
    - RACF still responsible for authorization
- LDAP-RACF relationship allows
  - LDAP based remote authentication to be done by RACF
  - Limited LDAP based access to RACF user, resource, and custom profiles
  - LDAP plugin allows for remote RACF audit and authorization services.

Key LDAP Terms

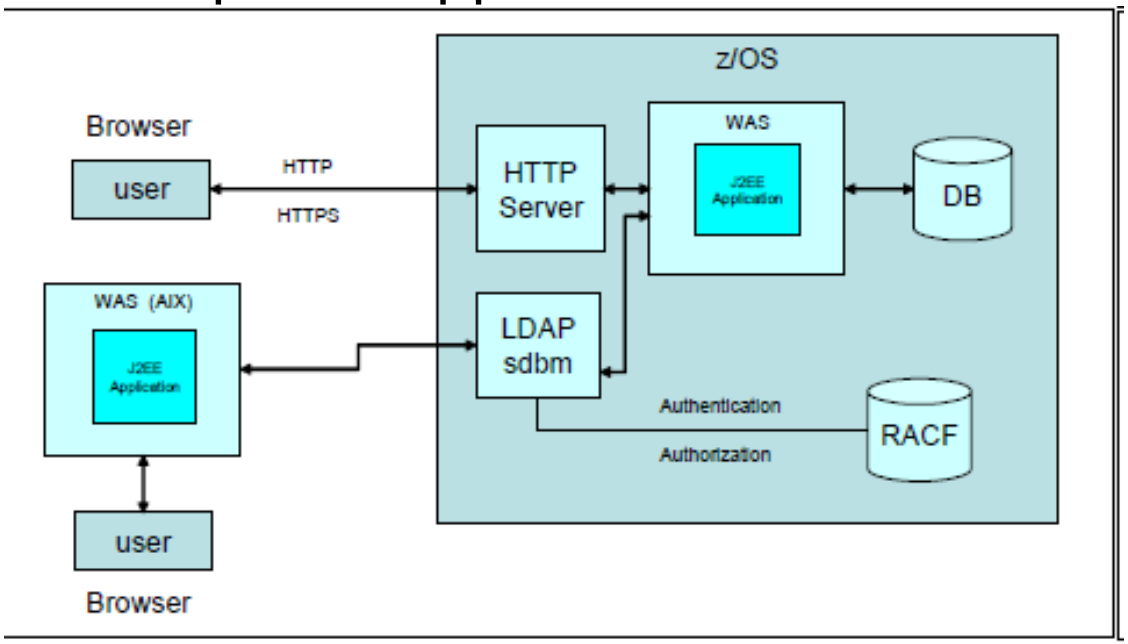
- Distinguished Name (DN) – Attribute in LDAP entry that uniquely identifies any given entry in the directory
  - Made up attribute=value pairs separated by commas
  - Format of DN is recursive, i.e., DN = RDN/Parent's DN
    - RDN consist of attribute-value pairs within the entry
- Bind – LDAP server authenticates a user
  - Distinguished Name/Password or Passphrase
  - Kerberos
  - X.509 Certificate

Key LDAP Terms cont…

- SDBM
  - AN LDAP front-end to RACF Database
    - Data is NOT duplicated in TDS
  - Allows LDAP clients to retrieve profile data (user, group, resource)
  - Allows TDS to have RACF perform authentication
    - TDS sends RACF ID + password/passphrase to RACF to authenticate
- Native Authentication
  - Standard LDAP user entries in TDS + a native user ID attribute
  - TDS calls RACF to authenticate native user ID and password or passphrase

RACF Authentication

- Goal: RACF serves as Authentication Authority
- Use passwords/passphrases, Kerberos, or X.509 Certificates to authenticate
- Consider WebSphere Application Server Environment +SDBM



RACF Authentication cont…

- Setup TDS: ds.conf (SDBM)

```
#---------- GLOBAL ------------
adminDN cn=admin
adminPW secret
listen ldap://:1492
listen ldaps://:1493
audit on
audit all,modify+delete+add+search+connect+disconnect+modifydn+bind+unbind+compare
schemaPath /home/suimgwi/ldap/test/r11db/schema
logfile /home/suimgwi/ldap/test/conf.log
#---------- SDBM ----------------
database sdbm GLDBSD31/GLDBSD64 mysdbm
suffix cn=myracf
enableResources on
```

RACF Authentication cont…

- Ds.conf cont… (TDBM+native Auth)

#---------- TDBM ----------

database tdbm GLDBTD31/GLDBTD64 TDBM1

suffix o=sample

extendedgroupsearching on

pwencryption sha

dbuserid DBUSR101

dsnaoini SUIMGWI.PRIVATE.EZCONFIG(DSNAOINI)

useNativeAuth all

nativeAuthSubtree o=sample

RACF Authentication cont…

- Setup WAS

In the administrative console go to **Security → Global security → User registries → LDAP** and supply the values shown in Table 4-1.

Table 4-1 User registry settings

Property	**Value** (*description*, actual)
Server user ID	*Master Administrators' RACF user ID*
Server user password	*Master Administrators' password*
Type	Custom
Host	*IP address or URL of LPAR where LDAP is listening*
Port	*LDAP listen port as specified in slapd.conf*
Base distinguished name (DN)	*suffix as in slapd.conf (without the quotes)*
Bind distinguished name (DN)	racfid=*BDNracid*,profiletype=user,*suffix*
Bind password	*password of BDNracid*

Table 4-2 Filters for Advanced LDAP user registry settings

property	**value**
User filter	racfid=%v
Group filter	racfid=%v
User ID map	*:racfid
Group ID map	*:racfid
Group member ID map	racfconnectgroupname:racfgroupuserids

ICTX: Remote RACF Authorization/SMF

- ICTX – a TDS for z/OS plug-in that add supports for remote RACF authorization and auditing over LDAP protocol
- Originally shipped with Enterprise Indentity Manager for z/OS as of V1R8.
- Now shipped with TDS for z/OS starting in V2R1
- DS.conf update:
  plugin clientOperation GLDBIC31/GLDBIC64 ICTX_INIT “CN=ICTX”

ICTX: Remote RACF Authorization/SMF cont…

1. Client must bind to TDS for z/OS
   - Native Auth
   - SDBM bind
   - RACF mapping Enabled
     - Kerberos
     - X.509 SASL External bind
2. Client must BER Encode ICTX Request and send to TDS for z/OS
3. Client must BER Decode ICTX Response to check results

Remote RACF Authorization

- TDS issues RACROUTE REQUEST=AUTH SAF
- RACF Required Defines:
  RDEFINE FACILITY IRR.LDAP.REMOTE.AUTH UACC(NONE)
  PERMIT IRR.LDAP.REMOTE.AUTH CLASS(FACILITY) ID(*BINDUSER*)
  ACCESS(UPDATE))
  SETROPTS RACLIST(FACILITY) REFRESH
- BER Encoding/Decoding
  - Client must have code that encodes parameters in BER Encoded block
  - Client must have code that decoded BER encoded response

Remote RACF Authorization

- Authorization Request ASN.1

```
requestValue ::= SEQUENCE {
        requestVersion INTEGER,
        itemList SEQUENCE of
                item SEQUENCE {
                        itemVersion INTEGER,
                        itemTag INTEGER,
                        userOrGroup OCTET STRING,
                        resource OCTET STRING,
                        class OCTET STRING,
                        access INTEGER,
                        logString OCTET STRING
                }
        }
}
```

Remote RACF Authorization

- Authorization Response ASN.1

```
responseValue ::= SEQUENCE {
        responseVersion INTEGER,
        responseCode INTEGER,
        itemList SEQUENCE of
                item SEQUENCE {
                        itemVersion INTEGER,
                        itemTag INTEGER,
                        majorCode INTEGER,
                        minorCode1 INTEGER,
                        minorCode2 INTEGER,
                        minorCode3 INTEGER
                }
        }
}
```

Simple Remote RACF Authorization

1. User requests a distributed Application to access a resource in the enterprise
   - Resource may have a profile in RACF or
   - Application may need to map resource to an existing profile name in RACF (could use LDAP to manage mappings)
2. Distributed Application binds to TDS for z/OS, using user's credentials.
3. Distributed Application encodes the ICTX Authorization Request and sends to TDS for z/OS
4. Distributed Application decodes response
5. If success, the application grants access

Remote RACF Audit

- TDS issues r_auditx (IRRSAX00) SAF callable service
- **SMF Record Type 83 subtype 4 records**
  - Unload using the IRRADU00 utility
  - RACF controls determine if record written
- RACF Required Defines:
  RDEFINE FACILITY IRR.RAUDITX UACC(NONE)
  PERMIT IRR.RAUDITX CLASSS(FACILITY) ID(LDAPSRV) ACCESS(READ))
  SETROPTS RACLIST(FACILITY) REFRESH
- BER Encoding/Decoding
  - Client must have code that encodes parameters in BER Encoded block
  - Client must have code that decoded BER encoded response

Remote RACF Audit

- Audit Request ASN.1

```
requestValue ::= SEQUENCE {
        requestVersion INTEGER,
        itemList SEQUENCE of
                item SEQUENCE {
                        itemVersion INTEGER,
                        itemTag INTEGER,
                        linkValue OCTET STRING SIZE(8),
                        violation BOOLEAN,
                        event INTEGER,
                        qualifier INTEGER,
                        class OCTET STRING,
                        resource OCTET STRING,
                        logString OCTET STRING,
                        dataFieldList SEQUENCE of
                        dataField SEQUENCE {
                        type INTEGER,
                        value OCTET STRING
                }
        }
}
```

Remote RACF Audit

- Audit Response ASN.1

```
responseValue ::= SEQUENCE {
        responseVersion INTEGER,
        responseCode INTEGER,
        itemList SEQUENCE of
                item SEQUENCE {
                        itemVersion INTEGER,
                        itemTag INTEGER,
                        majorCode INTEGER,
                        minorCode1 INTEGER,
                        minorCode2 INTEGER,
                        minorCode3 INTEGER
                }
        }
}
```

Simple Remote RACF Audit

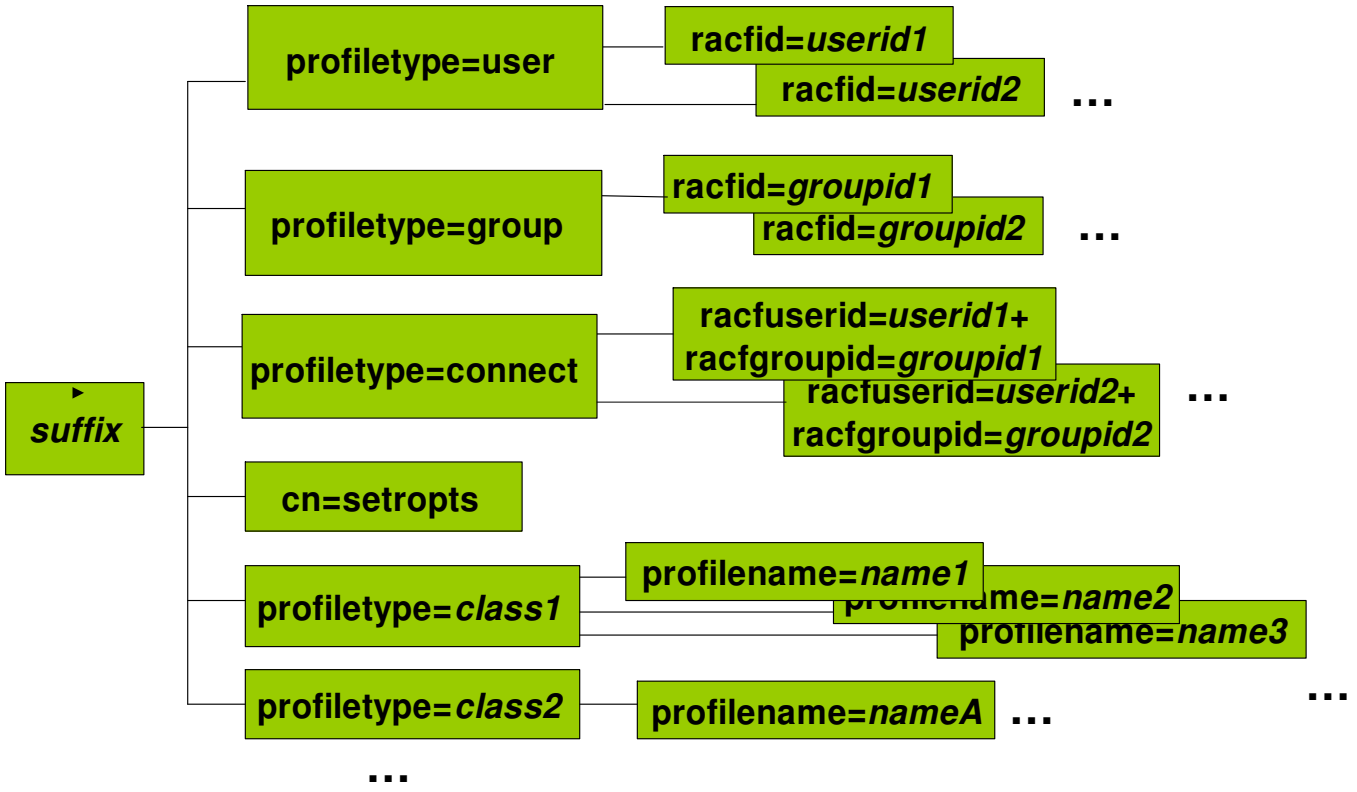
1. Administrator defines profiles for different operations in an application
2. Distributed Application binds to TDS for z/OS
   - May have a single/long living TDS connection for remote audit
3. Distributed Application encodes the ICTX Audit Request and sends to TDS for z/OS
4. Distributed Application decodes response
5. If RACF controls set correctly, audit record will be written

SDBM: RACF Data and LDAP

- Add, modify, delete RACF users, groups, and general resources
- Add, modify, and delete user connections to groups
- Add and remove users and groups in general resource profiles
- Modify SETROPTS options that affect classes
- Retrieve RACF information for users, groups, connections, general resources, and class options
- Retrieve RACF user password and password phrase envelopes

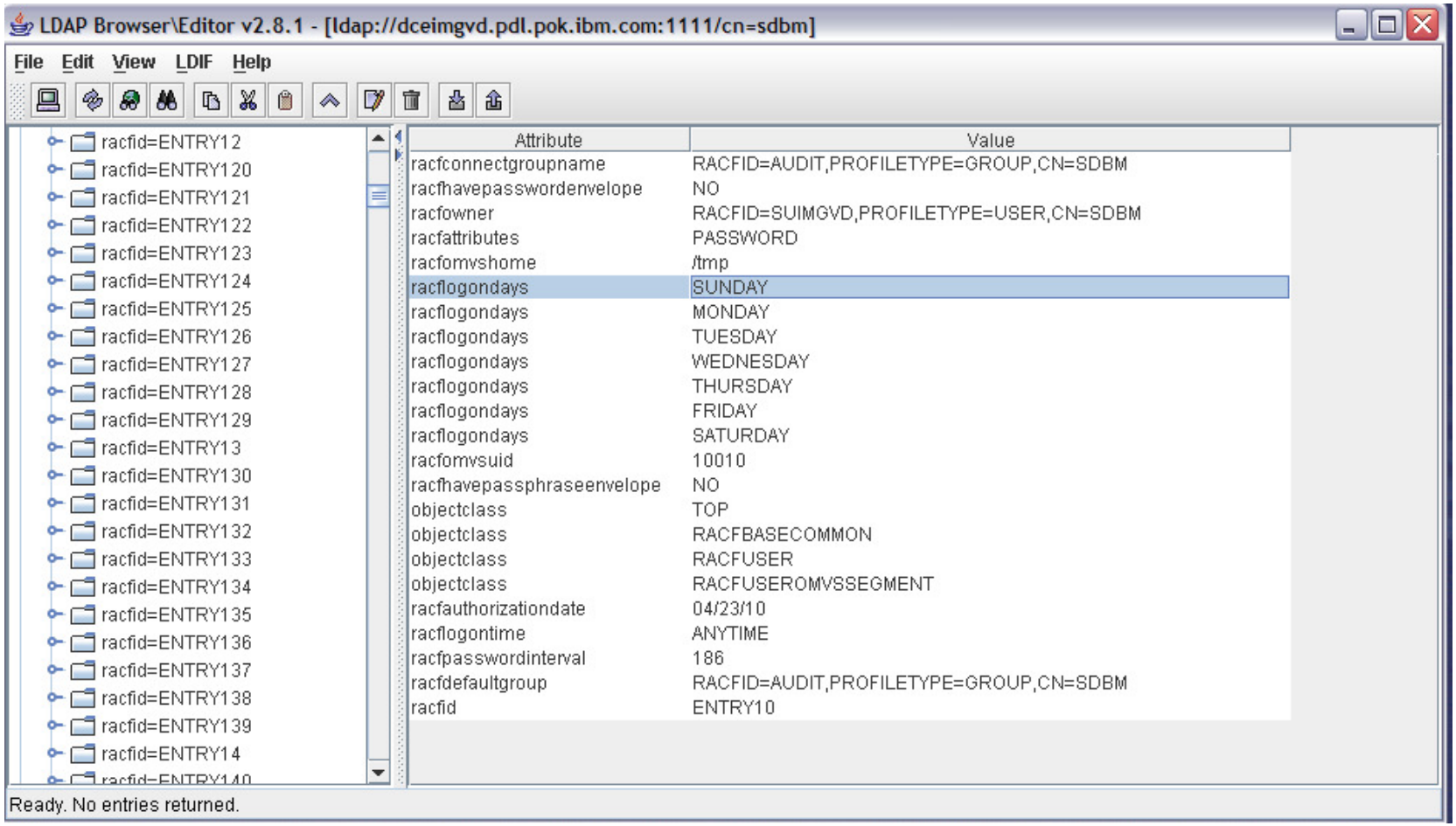
SDBM: RACF Data and LDAP

SDBM Backend Directory Hierarchy



Example DN: racfid=jon,profiletype=user,cn=sdbm

SDBM: RACF Data and LDAP



Common SDBM Commands

- Add a RACF user entry
- Create a file, u1234.ldif, containing an entry to be added:

```
dn: racfid=u1234,profiletype=user,cn=sdbm
objectclass: racfUser
objectclass: racfUserOmvsSegment
racfid: u1234
racfdefaultgroup: group1
racfowner: radmin
racfattributes: special
racfomvsuid: 1234
racfomvshome: /home/u1234
```

- Invoke the ldapadd utility:
  - ldapadd -D “racfid=radmin,profiletype=user,cn=sdbm” -w radminpw -f u1234.ldif
- SDBM executes under the context of bound (radmin) user:
  - ADDUSER u1234 OWNER(radmin) DFLTGRP(group1) SPECIAL OMVS(UID(1234) HOME(/home/u1234))

Common SDBM Commands

- Display a RACF user-group connection:
  - ldapsearch -L -D “racfid=radmin,profiletype=user,cn=sdbm” -w radminpw -b “racfuserid=u1234+racfgroupid=group1,profiletype=connect,cn=sdbm” “objectclass=*”
- SDBM executes under the context of bound (radmin) user: LISTUSER U1234 and returns group info for GROUP1

Common SDBM Commands: Search Results

dn:
racfuserid=U1234+racfgroupid=GROUP1,profiletype=CONNECT,cn=sdbm
racfuserid: U1234
racfgroupid: GROUP1
racfconnectauthdate: 02/08/10
racfconnectowner: RACFID=RADMIN,PROFILETYPE=USER,CN=SDBM
racfconnectgroupauthority: USE
racfconnectgroupuacc: NONE
racfconnectcount: 0
objectclass: TOP
objectclass: RACFBASECOMMON
objectclass: RACFCONNECT

Common SDBM Commands

- Refresh the FACILITY class
- Create file, refresh.ldif, containing the modification to the cn=setropts entry:

```
dn: cn=setropts,cn=sdbm
changetype: modify
replace: racfsetroptsattributes
racfsetroptsattributes: REFRESH
-
replace: racfraclist
racfraclist: profiletype=FACILITY,cn=sdbm
```

- Invoke the ldapmodify utility:
  - ldapmodify -D “racfid=radmin,profiletype=user,cn=sdbm”-w radminpw -f refresh.ldif
- SDBM executes under the context of bound (radmin) user:
  - SETROPTS REFRESH RACLIST(FACILITY)

Common SDBM Commands

- The ldapmodify utility can be used to change RACF password or password phrase
- Via SDBM backend:

  dn: racfid=u1234,profiletype=user,cn=sdbm
  replace: racfPassword
  racfPassword: anewpw

- Via LDBM or TDBM with native authentication:

  dn: cn=jon,o=ibm,c=us
  delete: userPassword
  userPassword: racfpw
  -
  add: userPassword
  userPassword: mynewpw

- Note: replace: userPassword is not supported when changing the RACF password with native authentication

SDBM Limitations

- SDBM uses the **R_admin** "run command" interface to implement many RACF related operations
  - Output for search related operations have limits
    - R_admin limits output to 4096 records
- LDAP wildcard searching not fully supported for SDBM
- LDAP attribute names are pre-defined and cannot be changed
  - racfPassword for password cannot be customized
- SDBM subtree searching does not return all attributes
  - Must do subtree search to retrieve DNs then a base level search for each DN to retrieve all the attributes

Conclusion

- TDS for z/OS+RACF allows for consolidation of IT security on System z, regardless of platform
  - Existing skills and procedures can continue to be used
- Distributed Applications can
  - Use RACF to perform all authentication
  - Use RACF to perform all authorization
  - Use RACF for centralized Auditing facility
  - New as of V2R1: Use ICSF and System z crypto hardware, to manage/use cryptographic objects and keys

References

- z/OS Hot Topics Newsletter http://www-03.ibm.com/systems/z/os/zos/bkserv/hot_topics.html
  - #22, March 2010: "We've got your back(bone)"
  - #25, August 2011: "Don't judge an LDAP server by its name!"
  - #26, August 2012: "z/OS LDAP Plug-ins: Endless Opportunities"
- z/OS Publications http://www-03.ibm.com/systems/z/os/zos/bkserv/
  - IBM Tivoli Directory Server Client Programming for z/OS
  - IBM Tivoli Directory Server Messages and Codes for z/OS
  - **IBM Tivoli Directory Server Plug-in Reference for z/OS**
  - IBM Tivoli Directory Server Administration and Use for z/OS
- IBM Education Assistant http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp?topic=/com.ibm.iea.zos/plugin_coverpage.html
  - V1R11 – Security
    - Accessing RACF Resource Profiles through the IBM Tivoli Directory Server for z/OS
    - Introduction to configuring advanced replication in the IBM Tivoli Directory Server for z/OS
  - V1R12 – Security
    - Password policy in the IBM Tivoli Directory Server for z/OS

Complete your sessions evaluation online at SHARE.org/SanFranciscoEval

References (cont…)

- IBM Redbooks: IBM Tivoli Directory Server for z/OS
  - http://www.redbooks.ibm.com/abstracts/sg247849.html
- IBM Redbooks: WebSphere Application Server on z/OS and Security Integration
  - http://www.redbooks.ibm.com/redpapers/pdfs/redp4161.pdf

#SHAREorg

SHARE
Technology · Connections · Results

How-to Access RACF From Distributed Platforms

Saheem Granados
IBM

Wednesday, February 6, 2013
12538

sgranado@us.ibm.com

Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

SHARE in San Francisco 2013