



z/OS LDAP

MYTHS, TRUTHS AND PRACTICAL USE CASES

David Z. Rossi

Cybersecurity Architect
dzrossi@us.igm.com

May 12, 2020





Agenda

- Myths
- Truths
- Practical Use Cases



Myths



z/OS LDAP is a Single Sign On Solution - FALSE

SSO Definition -

Single sign-on (SSO) is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems. It is often accomplished by using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on (directory) servers.[1] A simple version of single sign-on can be achieved over IP networks using cookies but only if the sites share a common DNS parent domain.[2]

For clarity, a distinction should be made between Directory Server Authentication and single sign-on: Directory Server Authentication refers to systems requiring authentication for each application but using the same credentials from a directory server, whereas single sign-on refers to systems where a single authentication provides access to multiple applications by passing the authentication token seamlessly to configured applications.

David's Definition - Sign on once, and identity token passed there after so user does not sign in again.

zOS LDAP can be used to enable RACF user IDs to be used in SSO solution but it is not a SSO Solution

zOS has many entry points - There is no one SSO solution for zOS

Examples - Session managers for TN3270 with the use of passtickets

- WAS, CICS, DB2 Network Authorization Services enablement of Kerberos
- WAS with SAML enabled by ISAM or IBM Cloud Identify Verify



z/OS LDAP exposes only RACF user, groups and connections - FALSE

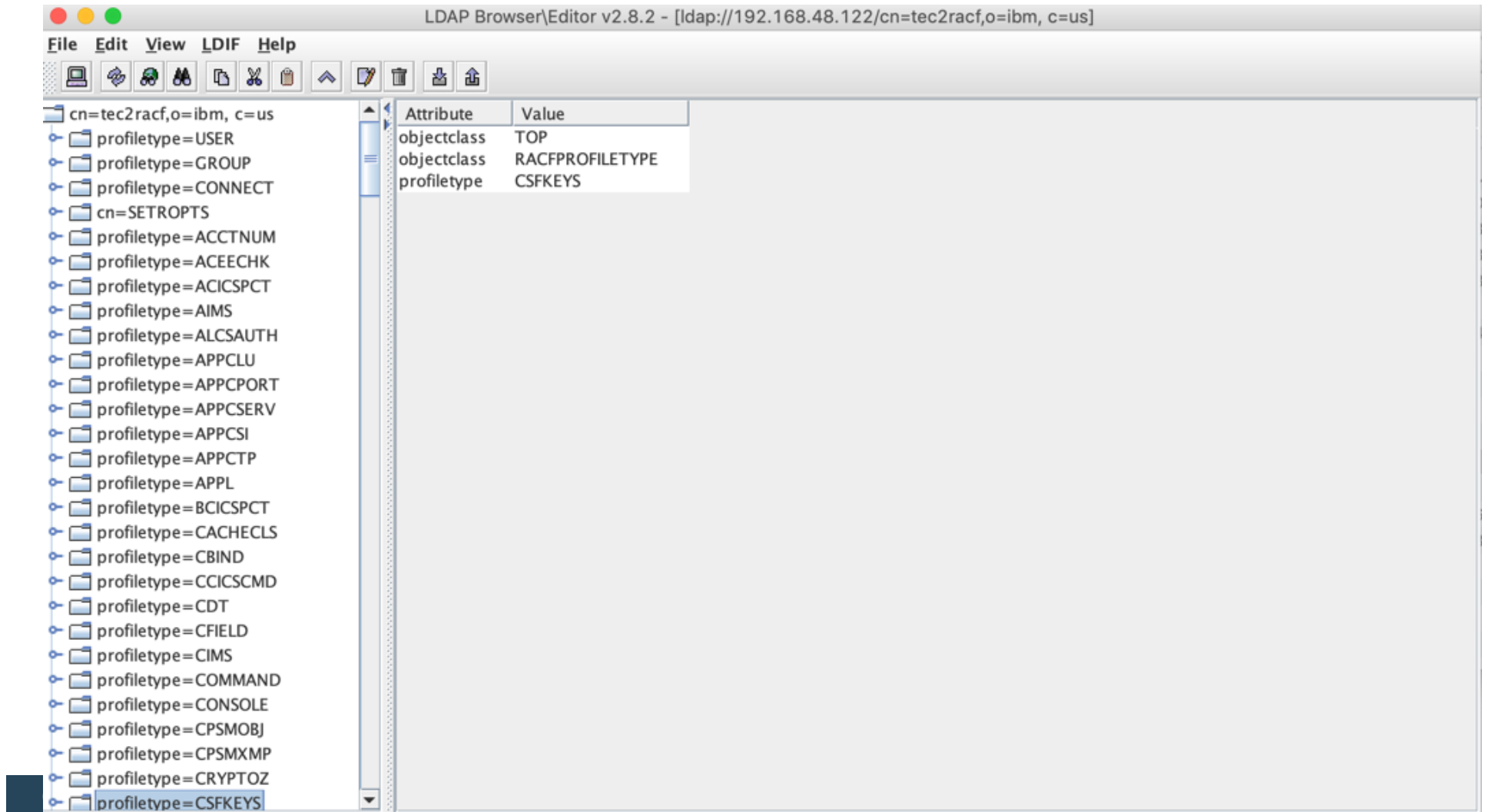
RACF provides definitions of users, groups, classes, and ***general resources**, and access control for resources. The LDAP server can provide LDAP access to this information stored in RACF. Using SDBM, the RACF database backend of the LDAP server, you can accomplish the following tasks:

- Add, modify, and delete RACF users, groups, and general resources. Data set resources are not supported.
- Add, modify, and delete user connections to groups.
- Add and remove users and groups in general resource access lists.
- Modify SETROPTS options that affect classes (for example, RACLIST).
- Retrieve RACF information for users, groups, connections, general resources, and class options.
- Retrieve RACF user password and password phrase envelopes.

*To see resources you must enable in ds.config with this variable `enableresources {on | off}`

Note All RACF Defined Resources will be seen active and not active

z/OS LDAP exposes only RACF user, groups and connections - FALSE



The screenshot shows the LDAP Browser/Editor v2.8.2 interface. The title bar indicates the connection path: [ldap://192.168.48.122/cn=tec2racf,o=ibm,c=us]. The left pane displays a tree view of LDAP entries under the root 'cn=tec2racf,o=ibm,c=us'. The right pane shows the details for the selected entry, 'profiletype=CSFKEYS', in a table format.

Attribute	Value
objectclass	TOP
objectclass	RACFPROFILETYPE
profiletype	CSFKEYS

z/OS LDAP exposes only RACF user, groups and connections - FALSE

The screenshot shows the LDAP Browser/Editor v2.8.2 interface. The title bar indicates the connection path: [ldap://192.168.48.122/cn=tec2racf,o=ibm,c=us]. The menu bar includes File, Edit, View, LDIF, and Help. The toolbar contains various icons for navigation and editing. The left pane shows a tree view of LDAP entries under the profiletype=CSFKEYS container. The right pane displays the attributes and values for the selected entry.

Attribute	Value
objectclass	TOP
objectclass	RACFPROFILETYPE
profiletype	CSFKEYS

Ready. 50 entries returned.

z/OS LDAP exposes only RACF user, groups and connections - FALSE

The screenshot shows the LDAP Browser\Editor v2.8.2 interface. The title bar indicates the connection path: [ldap://192.168.48.122/cn=tec2racf,o=ibm,c=us]. The menu bar includes File, Edit, View, LDIF, and Help. The toolbar contains various icons for navigation and editing. The left pane displays a tree view of profile types under 'profiletype=CSFKEYS'. The right pane shows a table of attributes and their values for the selected profile.

Attribute	Value
racfupdateaccesscount	0
racfresourceaudit	FAILURES(READ)
objectclass	TOP
objectclass	RACFRESOURCE
objectclass	EXTENSIBLEOBJECT
profilename	AES.PE.LABUSERXX.NONVSAMDATA.V1.DEC122018
racfcontrolaccesscount	0
racfauthorizationdate	12/12/18
racfaccesscontrol	ID(EKMFSGRP) ACCESS(READ) COUNT(0)
racfaccesscontrol	ID(USERXX) ACCESS(READ) WHEN(CRITERIA(SMS('DSENCRIPTION
racflastchangedate	12/12/18
racfuacc	NONE
racficsfsympacfwrap	YES
racfalteraccesscount	0
racfreadaccesscount	0
racficsfsymexportable	BYANY
racfowner	RACFID=PERES,PROFILETYPE=GROUP,CN=TEC2RACF,O=IBM,C=
racflevel	0
racflastreferencedate	12/12/18
racficsfsympacfret	YES
racficsfasymusage	SECUREEXPORT
racficsfasymusage	HANDSHAKE

z/OS LDAP has only one type of back end - FALSE

Backends

TDBM

The LDAP server provides a backend to store directory information in a Db2 database. TDBM is a general purpose backend that can store any type of directory information.

SDBM

The LDAP server can provide remote LDAP access to the user, group, connection, and general resource profile information stored in RACF. It also supports setting RACF options that affect classes. When creating change log records for changes to RACF data, SDBM is required.

LDBM

The LDAP server provides a file-based backend to store directory information in a z/OS UNIX System Services file system. LDBM is a general-purpose backend that can store any type of directory information.

CDBM

The LDAP server provides the CDBM backend to store configuration information, for example, for advanced replication and password policy. CDBM is file-based, storing its directory information in a UNIX System Services file system.

GDBM

The LDAP server can provide a change log containing information about changes to:

- RACF users, groups, user-group connections, and general resource profiles.
- TDBM, LDBM, and CDBM entries.
- LDAP server schema entry.





Overview of LDAP

What is LDAP?

- Lightweight Directory Access Protocol (LDAP) is a global directory model
- Originally developed as front-end of X.500 (DAP)
- The LDAP protocol runs over TCP
- Global directory model is based on entries

Each entry identified by its DN (distinguished name)

- Often uses cn (common name), ou (organization unit), o (organization)

- Each entry is a collection of attributes

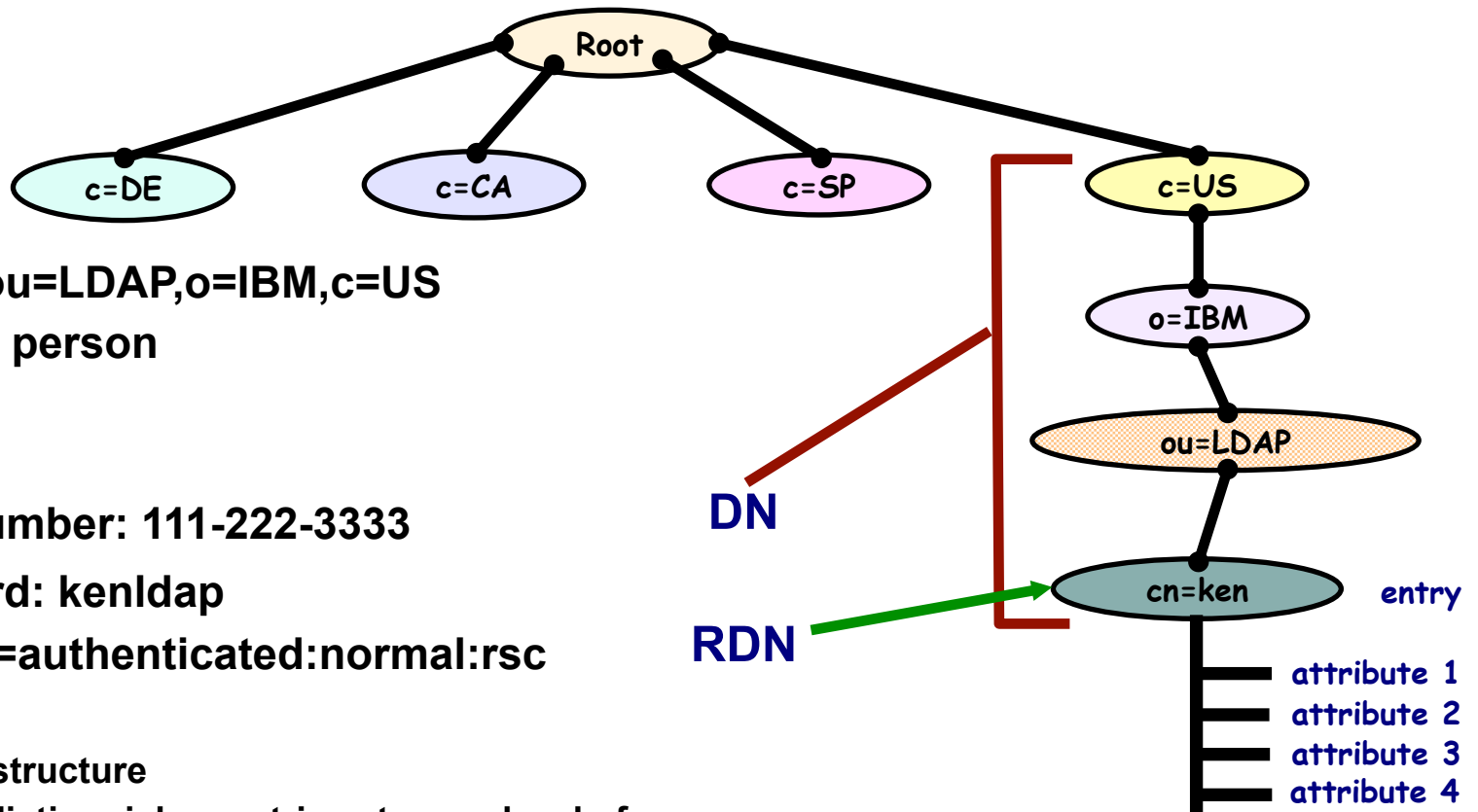
Each attribute has a type and values

Attributes are grouped into object classes

- Determine mandatory and optional attributes for an entry

DN: cn=ken,ou=LDAP,o=IBM,c=US

LDAP Directory Structure



dn: cn=ken,ou=LDAP,o=IBM,c=US

objectclass: person

cn: ken

sn: morgan

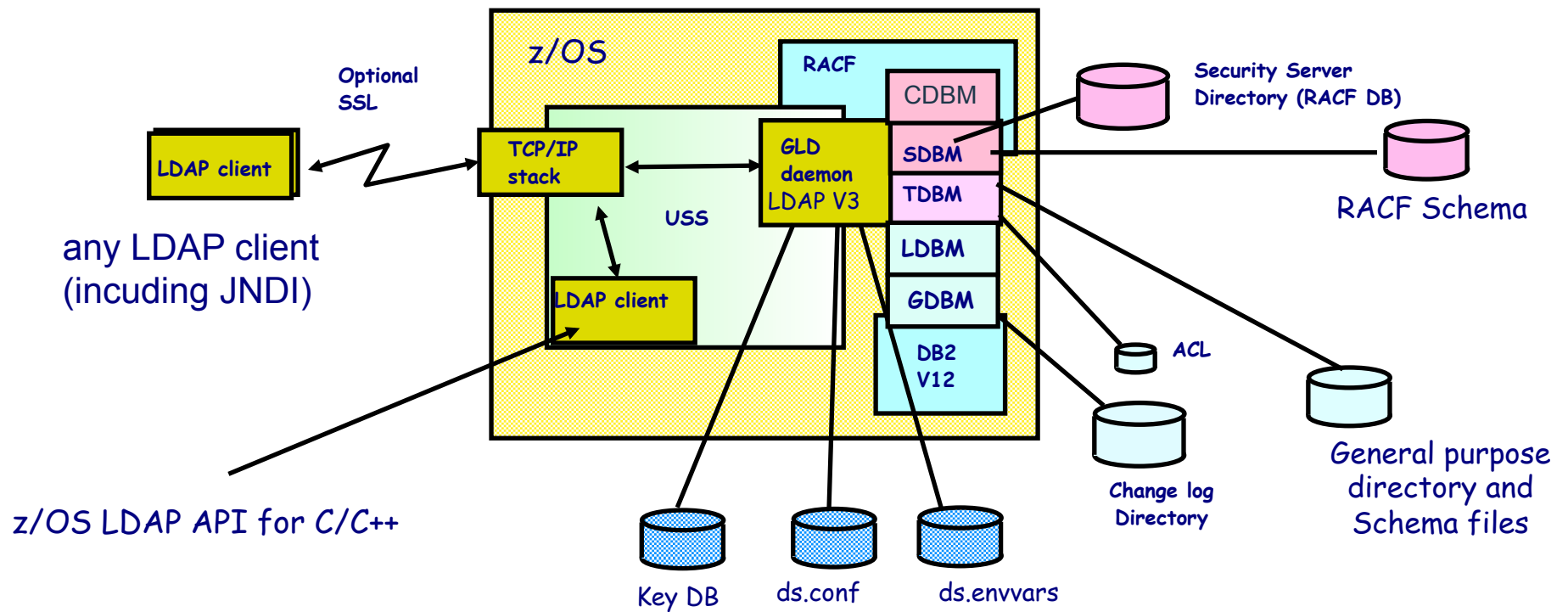
telephonenumber: 111-222-3333

userpassword: kenldap

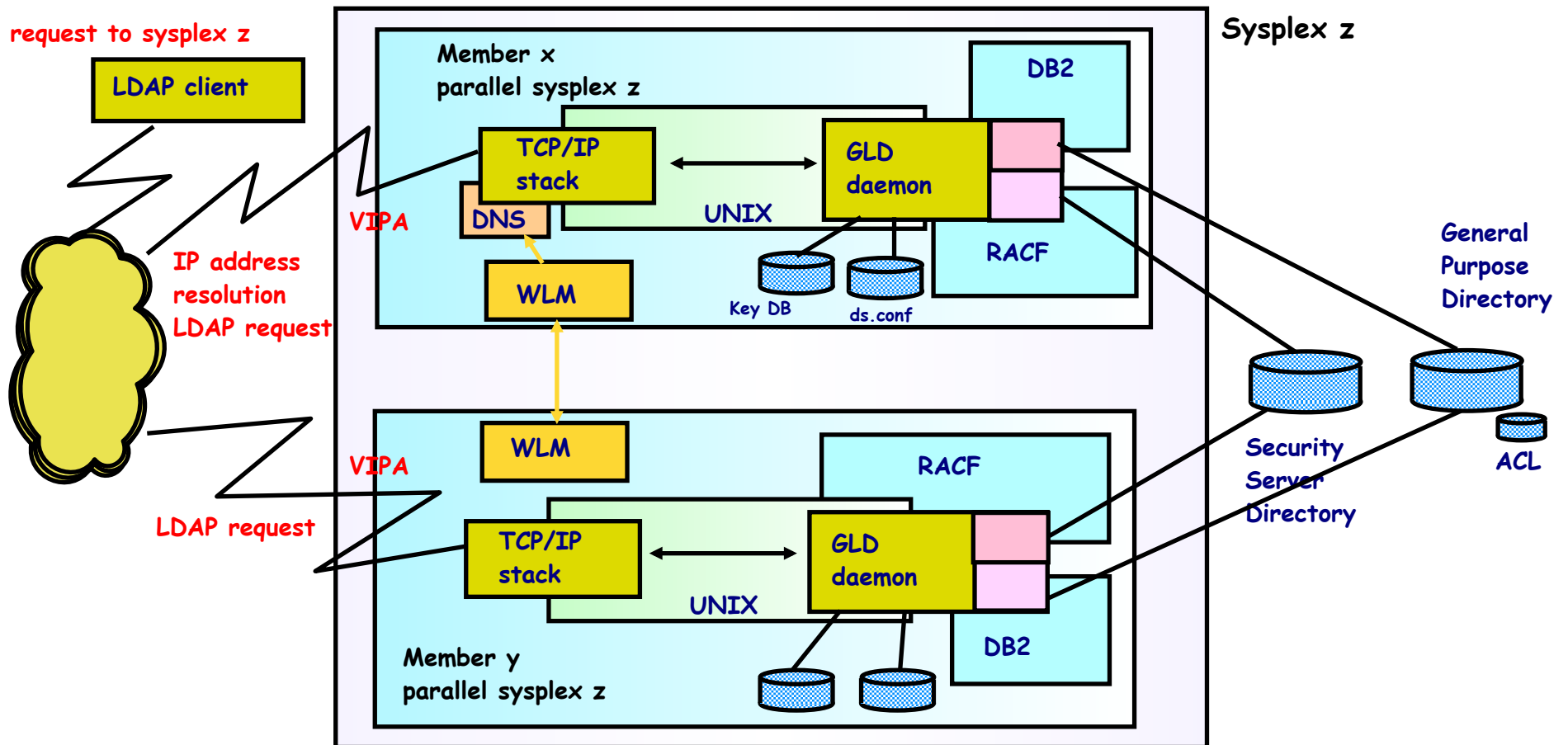
acentry: cn=authenticated:normal:rsc

- Hierarchical structure
- Relative DN distinguishes entries at same level of hierarchy
- Attributes are protected by Access Control Lists (ACL)

LDAP Server on z/OS



LDAP for z/OS Parallel Sysplex Support





LDAP Authentication

Authentication with an LDAP Server

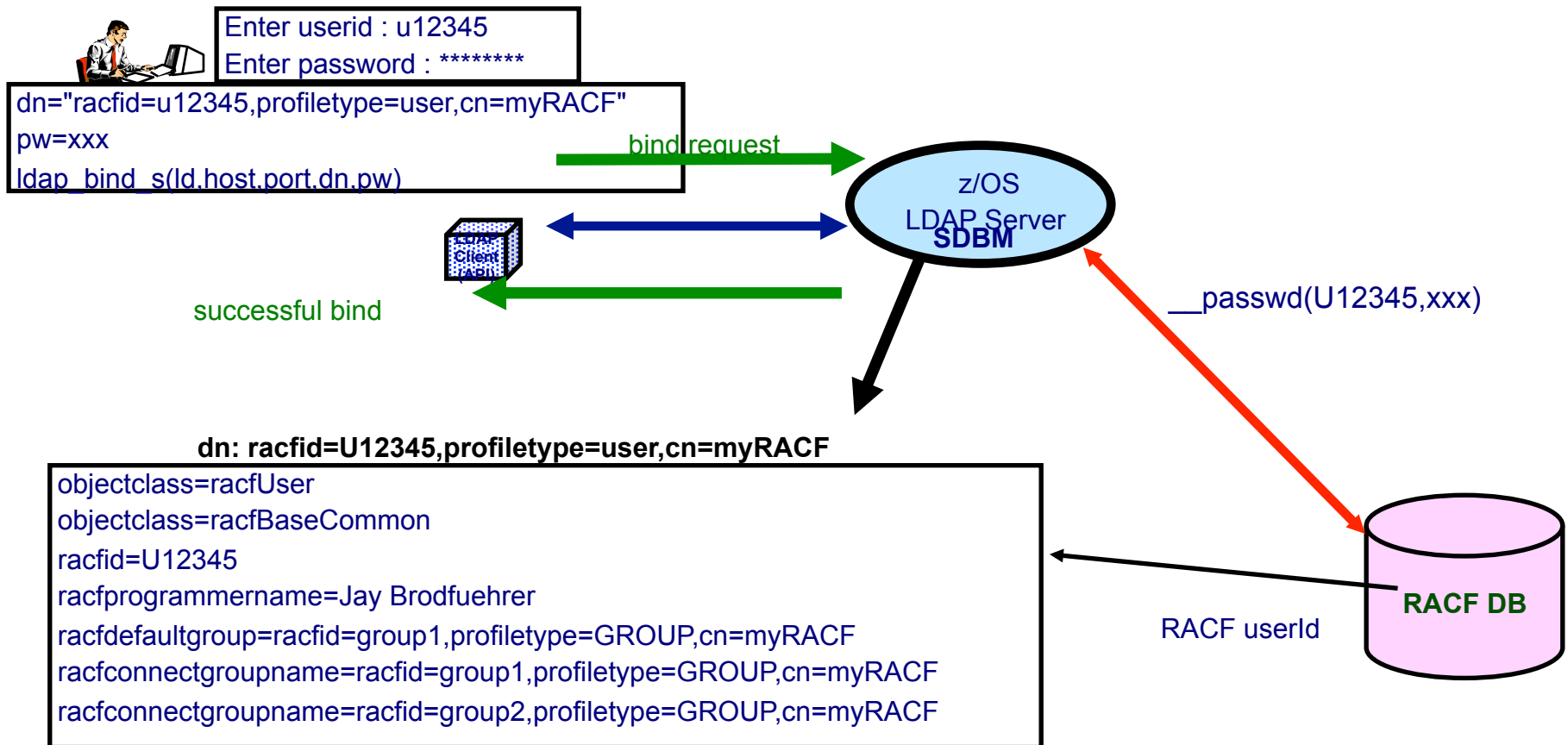
- **LDAP is a stateful protocol**

- Session starts when client "binds" to server
- Session can be unauthenticated (anonymous bind)
- Authentication is performed during bind
 - Check password or certificate
 - Determine groups to which user belongs (for authorization checking)

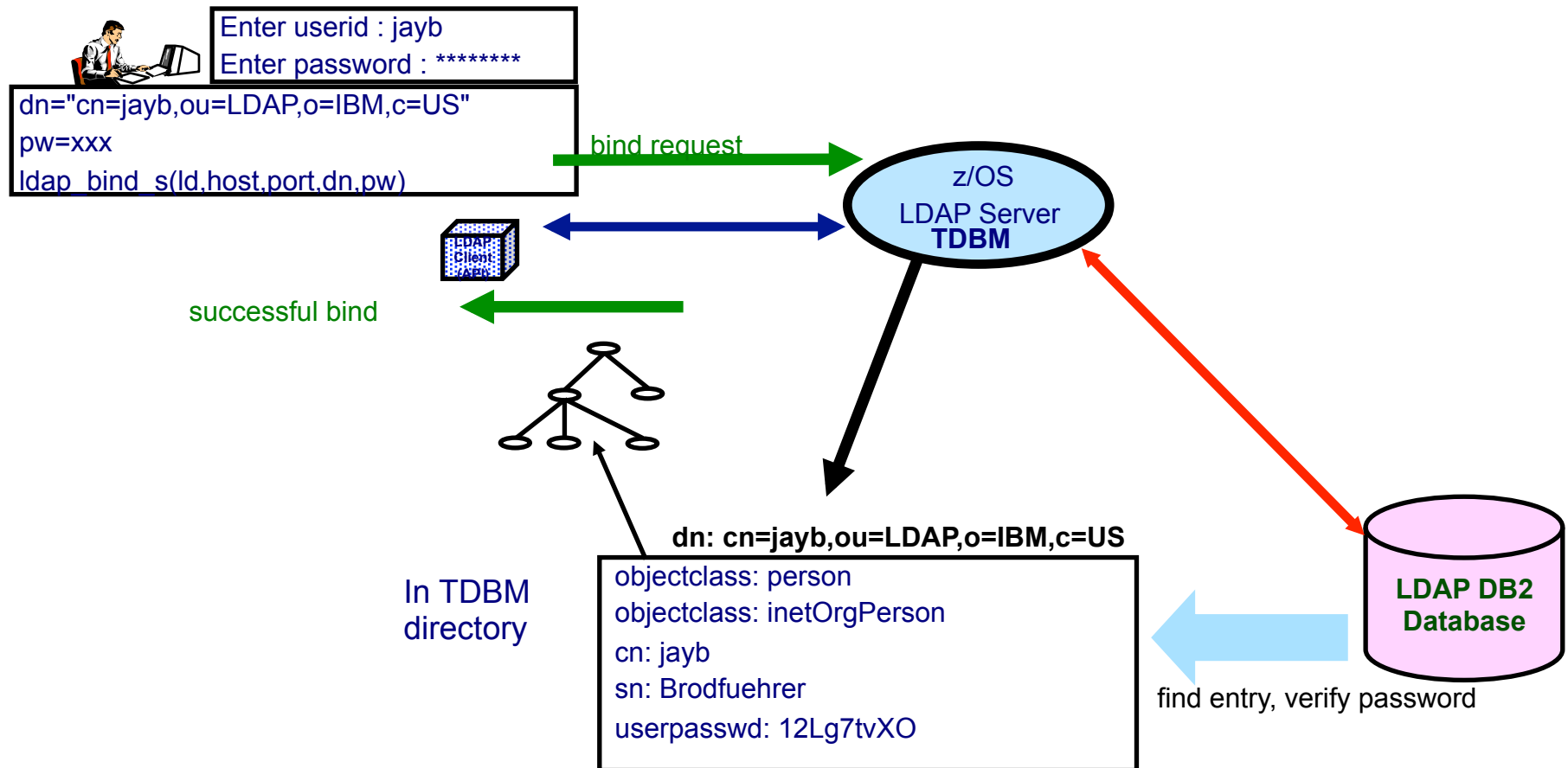
- **LDAP supports different authentication protocols**

- **Simple bind: Distinguished Name and password**
 - Session can optionally be protected with SSL
 - Passwords can be stored in LDAP directory, optionally one-way (MD5, SHA-1, crypt) or two-way (TDES) encrypted, or stored in RACF
- **Certificate bind: X.509 digital certificate over SSL**
 - Distinguished name in certificate must conform with distinguished name of person authenticating
- **Kerberos bind: Kerberos principal sends ticket for LDAP server**
 - Attribute: `ibm-kn = principal @ realm`
- **CRAM-MD5, DIGEST-MD5 binds: DN/userid and password**
 - Client hashes password using MD5 encryption

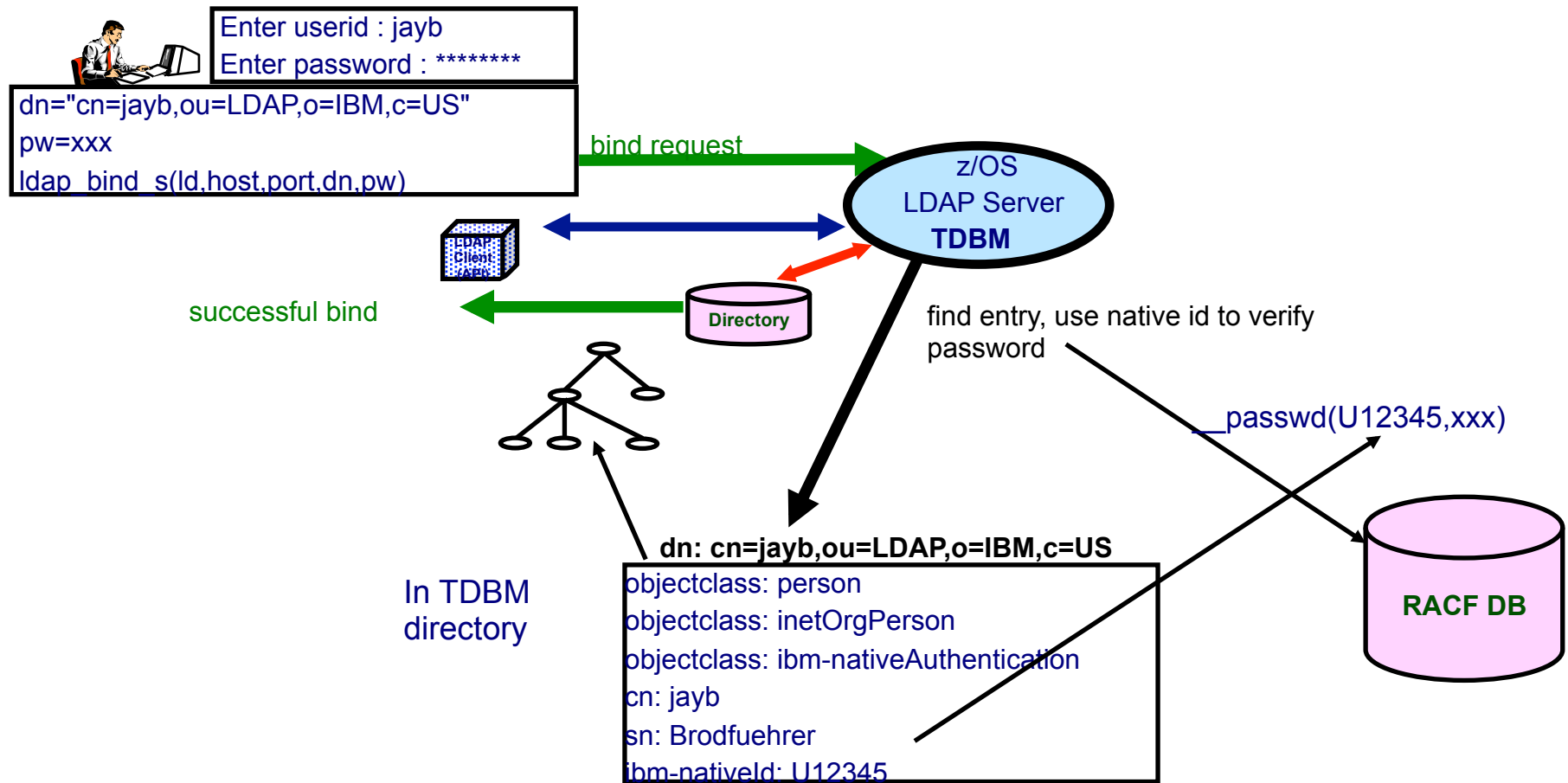
LDAP Authentication with SDBM (RACF)



LDAP TDBM Authentication



LDAP Native Authentication



z/OS LDAP Server Native Authentication

- **Disadvantage of Authentication in RACF:**

- SDBM backend required
- Nonstandard Distinguished Name (racfid, profiletype)
- Fixed schema: only RACF information is available, cannot add attributes to contain additional information

- **Native Authentication uses TDBM backend**

- Standard Distinguished Name (e.g. cn, ou, o)
- Any schema supported by LDAP V3 for person entry can be used
 - Any information supported by the schema can be retrieved
 - Use TDBM groups and group membership in ACLs
- Authentication (password verification) performed by RACF
 - Password for entry is in security server (not in TDBM)
 - No need for administration or synchronization of multiple password registries
 - RACF authentication triggered by attribute **ibm-nativeId** in TDBM entry
- Can limit native authentication to specific TDBM subtrees or entries - some entries use RACF, others have passwords in entry



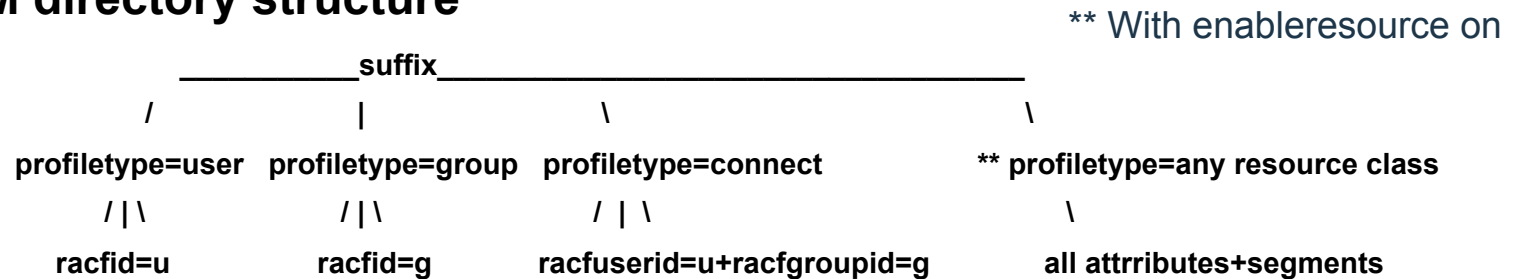
Accessing RACF via LDAP

SDBM Support of RACF

Use LDAP to add, modify, delete, display RACF users, groups, and user-group connection - remote admin

Equivalent to RACF commands: ADDUSER, ALTUSER, DELUSER, LISTUSER, ADDGROUP, ALTGROUP, DELGROUP, LISTGRP, CONNECT, REMOVE

SDBM directory structure



example DN: racfid=kmorgan,profiletype=user,cn=myRacf

Hard coded schema definitions

Limited search capabilities - predefined by SDBM

All data accessed via RACF

No RACF Data in LDAP

Authorization controled by RACF, based on bound userid

Changing the RACF Password

- Idapmodify can be used to change RACF password

Via SDBM:

- `dn: racfid=G12345,profiletype=user,cn=myRACF`
`changetype: modify`
`replace: racfPassword`
`racfPassword: new_password`

Via TDBM with native authentication

- `dn: cn=jayb,ou=LDAP,o=ibm,c=us`
`changetype: modify`
`delete: userPassword`
`userPassword: old_password`
-
`add: userPassword`
`userPassword: new_password`
-

- **Note:** `replace: userPassword` cannot be used - not supported

- LDAP SDBM or native authentication bind can be used to change a password (even if expired)

Specify *old_password* / *new_password*



Access Control in TDBM

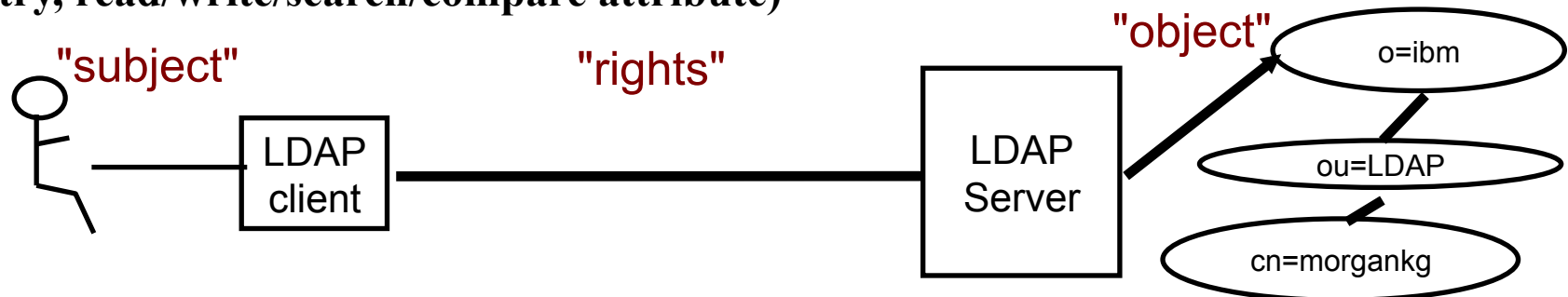
Access Control Checking

Does subject have the right to perform the requested operation on an object?

"subject" - the "bound" LDAP client identity: DN of requestor + DNs of groups to which requestor belongs

"object" - the entries or the attributes of the entries involved in the operation

"rights" - the access required to perform the requested operation (add/delete entry, read/write/search/compare attribute)



Access Control Implementation

TDBM uses an Access Control List (ACL) to control access to an entry
Specifies DNs of bound users and groups that can access the entry

Can control access to individual attributes or to classes of attributes
(normal, sensitive, critical, restricted and system)
Attribute's access class defined in the schema

Use LDAP modify operation to set ACL and search operation to display ACL info

examples:

acentry: cn=Jayb,o=Your Company:normal:rwsc:sensitive:rsc

acentry: racfid=morgankg,profiletype=user,cn=myRacf:object:ad

acentry: group:cn=mgrs,o=Your Company:at:userpassword:rwsc

acentry:group:racfid=g1,profiletype=group,cn=myRacf:normal:rwsc

Can propagate an entry's ACL to the subtree below it



Special aclEntry "pseudo-DNs"

cn=anybody

Applies when no other specific ACL value applies

cn=authenticated

Applies when the requestor has authenticated to the directory but no other specific ACL value applies

Meant to allow more access than cn=anybody ACL value

cn=this

Applies when the requestor has authenticated with the same DN as the entry being accessed
Used to grant individuals access to their own entry

Example:

aclentry: cn=anybody:normal:rsc

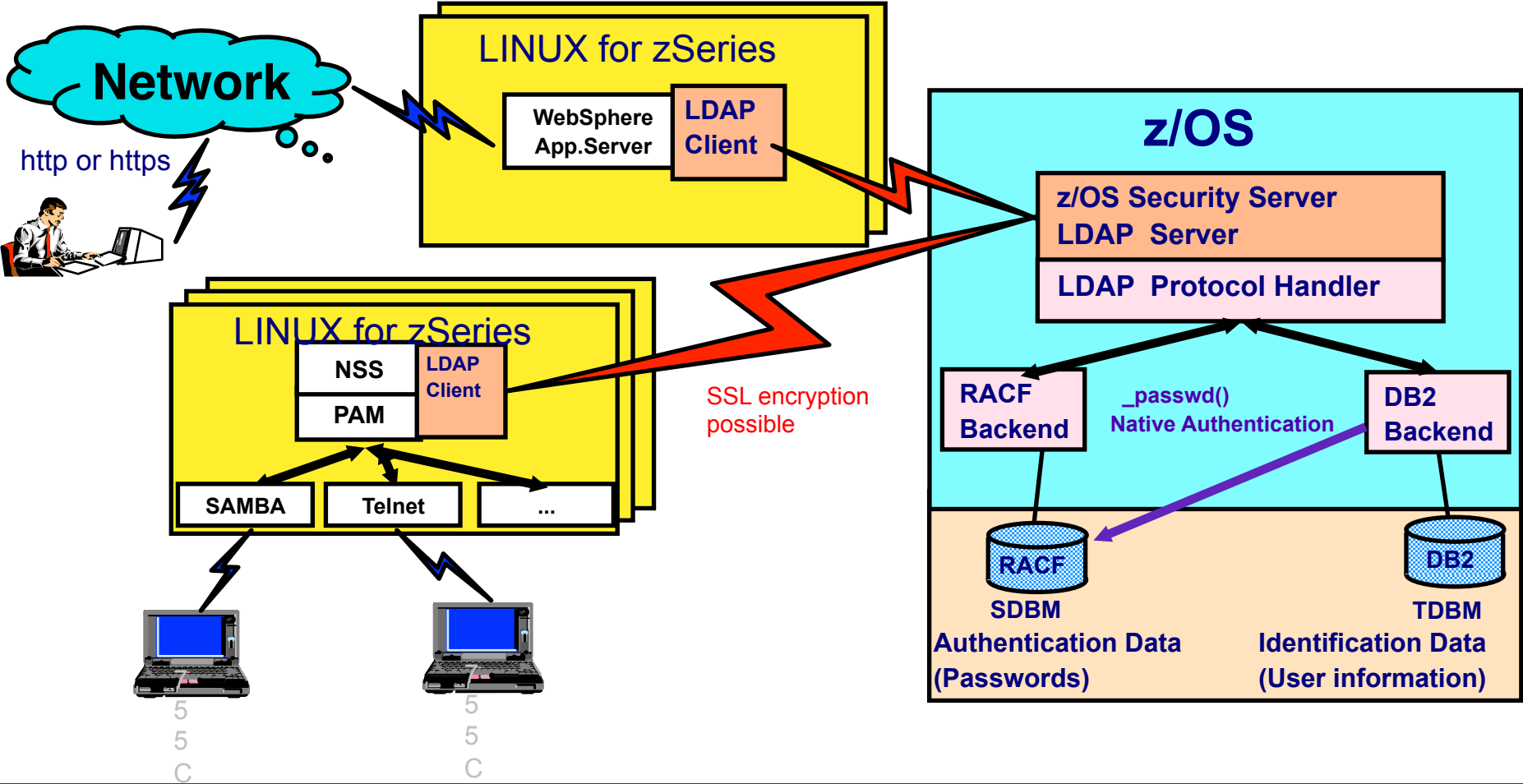
aclentry: cn=authenticated:normal:rsc:sensitive:rs

aclentry: cn=this:normal:rscw:sensitive:rscw:critical:rsc



The Big Picture

User Information and Authentication in LDAP





**New Function in z/OS V2R4
LDAP**



Overview

- **Problem Statement / Need Addressed**
 - SDBM backend uses R_admin callable service to issue the RACF search command, and is subject to the R_admin 4096-line output limitation.
 - SDBM backend search results can be incomplete if the RACF database contains over 4096 user/group/general resource profiles.
 - SDBM backend only supports a few search filters and the search capability is limited.
- **Solution**
 - The R_admin extract next profile function can be used to iteratively retrieve the rest of the profiles not returned from the RACF search command.
 - The SDBM extended search is introduced to support all the LDAP-compliant search filters.
- **Benefit / Value**
 - Search capability enhancement simplifies RACF profile management and makes the SDBM search behavior more similar to that of other backends.

Usage & Invocation - SDBM extended search

- Enhanced search capability
 - Complete search result, no 4096-line limitation
 - Common LDAP search filter support
- Performance consideration
 - **Basic mode** supports limited search filters, with performance equivalent to the traditional SDBM search that disables the extended search (**Off mode**)
 - **Advanced mode** has performance impact because common LDAP search filter support requires loading complete profiles from RACF

SDBM Extended Search			
Mode	Search Capability		
	4096-Line Limitation	Search Filter Support	Search Result
Off	Yes	Limited	Profile entry DN or complete profile entry *
Basic	No	Limited	Profile entry DN or complete profile entry *
Advanced	No	All	Complete profile entry

* Complete profile entry is returned only when the search target exactly matches a certain entry, e.g. the search base DN is set to a leaf level entry, or the search scope is set to base.

Davidson-MacBook-Pro-10:~ davidrossi\$ ldapsearch -h 192.168.48.122 -D racfid=dzrossi,profiletype=user,
cn=tec2racf,o=ibm,c=us -w password -b profiletype=user,cn=tec2racf,o=ibm,c=us "objectclass=*" -

extendedSearch off

```
# USER05, USER, tec2racf, ibm, us  
dn: racfid=USER05,profiletype=USER,cn=tec2racf,o=ibm,c=us
```

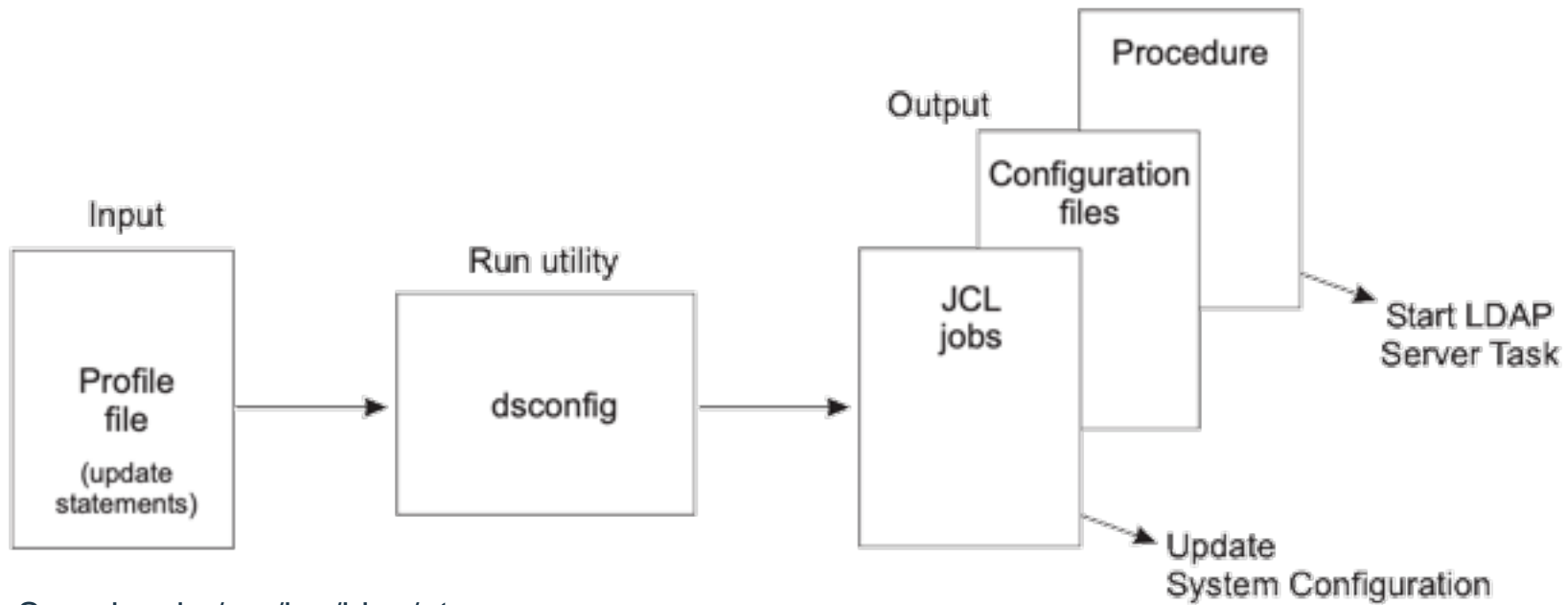
extendedSearch advanced

```
# USER05, USER, tec2racf, ibm, us  
dn: racfid=USER05,profiletype=USER,cn=tec2racf,o=ibm,c=us  
racfid: USER05  
racfauthorizationdate: 01/09/19  
racfowner: RACFID=PEUSER,PROFILETYPE=GROUP,CN=TEC2RACF,0=IBM,C=US  
racfpasswordinterval: 90  
racfpasswordchangedate: 03/24/20  
racfprogrammername: PELAB USER05  
racfdefaultgroup: RACFID=PEUSER,PROFILETYPE=GROUP,CN=TEC2RACF,0=IBM,C=US  
racflastaccess: 03/24/20/14:28:09  
racflogondays: SUNDAY  
racflogondays: MONDAY  
racflogondays: TUESDAY  
racflogondays: WEDNESDAY  
racflogondays: THURSDAY  
racflogondays: FRIDAY  
racflogondays: SATURDAY  
racflogontime: ANYTIME  
racfconnectgroupname: RACFID=PEUSER,PROFILETYPE=GROUP,CN=TEC2RACF,0=IBM,C=US  
racfhavepasswordenvelope: NO  
racfhavepassphraseenvelope: NO  
racfmfapwfallback: NOPWFALLBACK  
racfattributes: PASSWORD  
safaccountnumber: D999  
safdefaultcommand: : IA==  
safholdclass: H  
safjobclass: A  
safdefaultloginproc: IKJACCNT  
saflogonsize: 1048000  
safmessageclass: H  
safmaximumregionsize: 0  
safdefaultsysoutclass: 0  
safuserdata: 0000  
objectclass: TOP  
objectclass: RACFBASECOMMON  
objectclass: RACFUSER  
objectclass: SAFTSOSEGMENT
```



DS CONFIG

Setup made easy with DSCONFIG



Samples in /usr/lpp/ldap/etc

IBM Tivoli Directory Server Administration and Use for z/OS – chapter 4

[https://www-01.ibm.com/servers/resourceLink/svc00100.nsf/pages/zOSV2R4sc236788/\\$file/glpa200_v2r4.pdf](https://www-01.ibm.com/servers/resourceLink/svc00100.nsf/pages/zOSV2R4sc236788/$file/glpa200_v2r4.pdf)



Setup made easy with ds config

1) Create or add to existing .profile
export STEPLIB=SYS1.SIEALNKE:QSTEPLIB
export PATH=/usr/lpp/ldap/sbin:\$PATH
export NLSPATH=/usr/lpp/ldap/1ib/nls/msg/%L/%N:\$NLSPATH
export LANG=En_US.UTF-8

2) Copy over ds.profile from /usr/lpp/ldap/etc to your working directory. Edit ds.profile

3) Run ds utility - dsconfig -I ds.profile This will create the following jobs.

GLD.CNFOUT

APF
DSCONFIG
DSENVVAR
GLDSRV
PRGMCTRL
PROG00
RACF

IBM Tivoli Directory Server Administration and Use for z/OS - chapter 4

[https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R4sc236788/\\$file/glpa200_v2r4.pdf](https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R4sc236788/$file/glpa200_v2r4.pdf)



Practical Use Cases

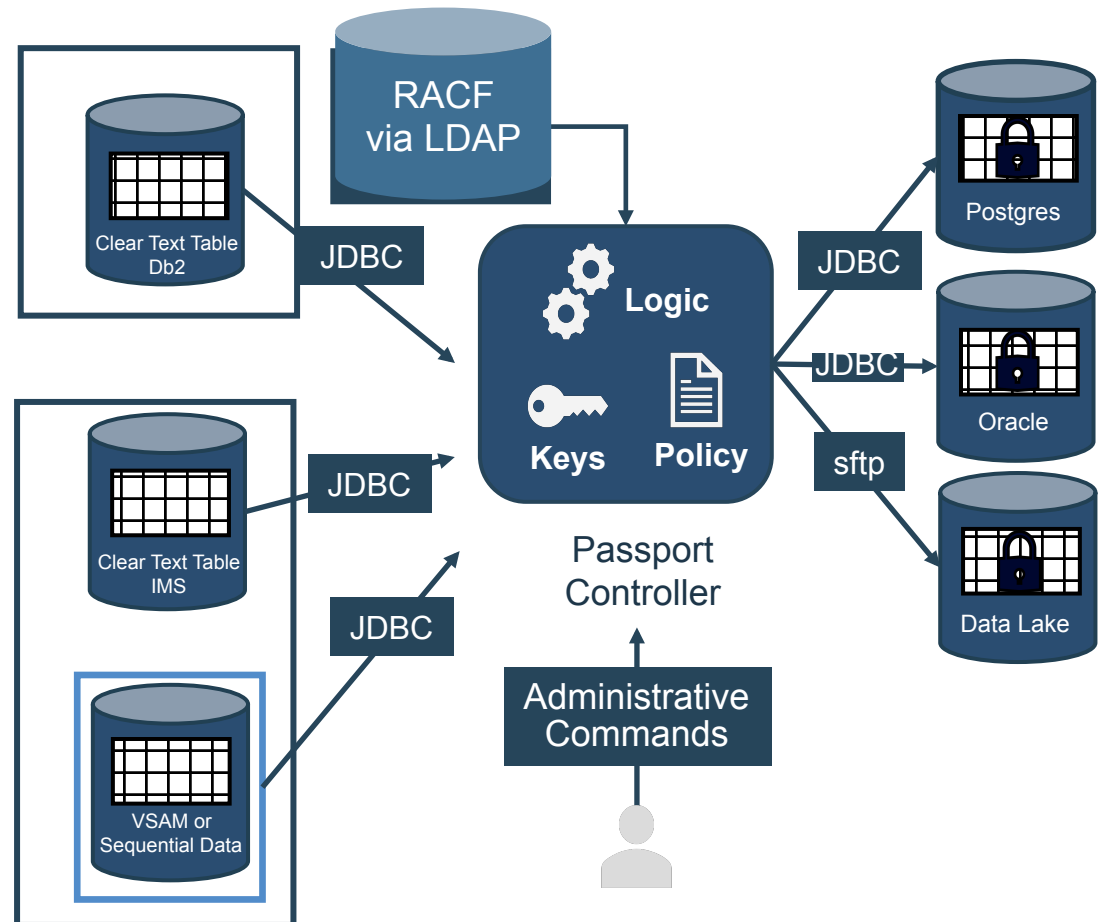


Distributed Identity Management

Data Privacy Passports (DPP)

- The data is protected at the point of extraction and is enforced at the point of consumption
- Move data from IBM Z to distributed as Trusted Data Objects – Start with SQL data sources on IBM Z
- Passport Controller deployed in an SSC LPAR
- Policy for enforcement can be changed dynamically to revoke to entitle users to data
- Create a single protected table to provide multiple views of data

Runs on IBM z15



Data Privacy Passports – External Identity Management

Access Management is about Users, Groups and Connects

- RACF id
- RACF password
- RACF group
- RACF connect

```
ldapsearch -h 129.40.130.17 -D racfid=usrda,profiletype=user,cn=RACF,o=IBM,c=in -w datapass -b  
racfid=usrda,profiletype=user,cn=RACF,o=IBM,c=in "objectclass=*" racfconnectgroupname
```

```
# extended LDIF  
#  
# LDAPv3  
# base <racfid=usrda,profiletype=user,cn=RACF,o=IBM,c=in> with scope subtree  
# filter: objectclass=**  
# requesting: racfconnectgroupname  
#  
# USRDA, USER, RACF, ibm, in  
dn: racfid=USRDA,profiletype=USER,cn=RACF,o=ibm,c=in  
racfconnectgroupname: RACFID=DPPDA,PROFILETYPE=GROUP,CN=RACF,O=IBM,C=IN  
racfconnectgroupname: RACFID=0MK1,PROFILETYPE=GROUP,CN=RACF,O=IBM,C=IN  
racfconnectgroupname: RACFID=0MK2,PROFILETYPE=GROUP,CN=RACF,O=IBM,C=IN  
racfconnectgroupname: RACFID=SMK1,PROFILETYPE=GROUP,CN=RACF,O=IBM,C=IN  
racfconnectgroupname: RACFID=SMK2,PROFILETYPE=GROUP,CN=RACF,O=IBM,C=IN  
  
# search result  
search: 2  
result: 0 Success  
  
# numResponses: 2  
# numEntries: 1
```



User Behavior Analytics

Dashboard

Search for User Next Refresh: 00:40 Reset Layout

Monitored Users
7.8K

High Risk Users
0

0% of monitored users

Users Discovered from Events
87

1% of monitored users

Users Imported from Directory
7.7K

99% of monitored users

Active Analytics

- UBA Rules
- Machine Learning

Status of Machine Learning Models

Authentication Activity	<div style="width: 100%; height: 10px; background-color: green;"></div>	
Suspicious Activity	<div style="width: 100%; height: 10px; background-color: gray;"></div>	
Data Downloaded	<div style="width: 100%; height: 10px; background-color: gray;"></div>	
Activity Distribution	<div style="width: 100%; height: 10px; background-color: green;"></div>	
Defined Peer Group	<div style="width: 100%; height: 10px; background-color: green;"></div>	
Learned Peer Group	<div style="width: 100%; height: 10px; background-color: green;"></div>	

Monitored Users

	Recent risk	Risk score ↓	
U070003 USS TEAM	10	22.1	
U040016 USS TEAM	10	17.13	
U050030 USS TEAM	0	15.68	
C2PSUSER	0	12.19	
U040009 USS TEAM	0	12	

Recent Offenses

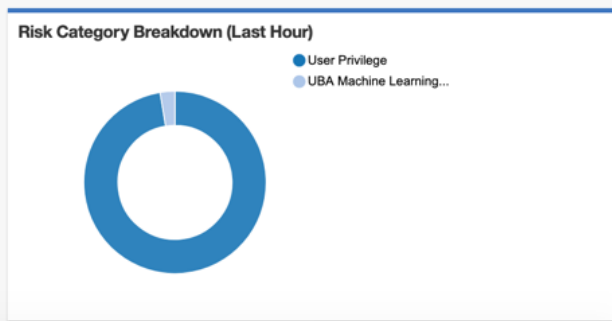
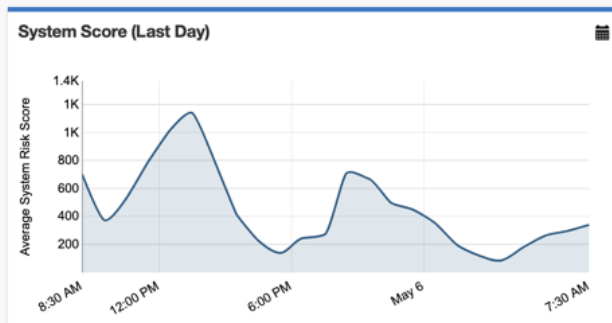
Offense # 81 updated about 23 hours ago
User: SIRC
 Description: UACC Set To Read On A Data Set Profile containing Change_UACC
 Event Count: 2 Flow Count: 0 **Magnitude: 3/10**

Offense # 71 updated 12 days ago
User: PPETERS
 Description: UACC Set To Read On A Data Set Profile preceded by System Authority Was Granted containing Change_UACC
 Event Count: 6 Flow Count: 0 **Magnitude: 4/10**

Offense # 70 updated 16 days ago
User: WASADM
 Description: UACC Set To Read On A Data Set Profile containing Change_UACC
 Event Count: 4 Flow Count: 0 **Magnitude: 3/10**

Offense # 69 updated about a month ago
User: CSTLSEC
 Description: System Authority Was Granted containing Grant_Privilege_System
 Event Count: 2 Flow Count: 0 **Magnitude: 3/10**

Offense # 68 updated 2 months ago
User: PPETERS
 Description: System Authority Was Granted preceded by UACC Set To Read On A Data Set Profile containing Change_UACC





- ✔ LDAP server configuration
- 2 Other import settings
- 3 Summary

LDAP server configuration

Enter the LDAP server information to retrieve user data. Before going to the next step, click Test Connection.

Protocol	LDAP Server Host * ⓘ	Port *
ldap://	9.12.20.114	2389
Username (Bind DN)		
racfid=dzrossi,profiletype=user,sysplex=plex1		
Password		
.....		
⌵ Advanced Settings		
Base DN ⓘ		
profiletype=user,sysplex=plex1		
Filter ⓘ		
objectclass=*		
Certificate ⓘ		
Click to upload the certificate file for the root certificate authority. File size is limited to 10 KB.		
<input type="checkbox"/> Paged results		
✔ Test Connection Number of attributes: 20		

Attribute	Samples
dn	racfid=\$IZUSVR,profiletype=USER,sysple... more
racfattributes	PROTECTED more
racfauthorizationdate	02/14/17 more
racfconnectgroupname	RACFID=CFZUSRGP,PROFILETYPE=GR...
racfdefaultgroup	RACFID=ZOSMF\$90,PROFILETYPE=GR... more
racfhavepassphraseenvelope	NO
racfhavepasswordevelope	NO
racfid	\$IZUSVR more
racfinstallationdata	2019 -- HUANG XIAO CHEN -- ZOSMF
racflastaccess	07/04/18/22:25:56
racflogondays	SUNDAY MONDAY TUESDAY WEDNESD...
racflogontime	ANYTIME

IBM QRadar

Dashboard Offenses Log Activity Netw

Dashboard > User Def

DZROSSI

Job title: DAVE ROSSI
 Department: 2017 -- DAVE ROSSI -- C
 Group membership: RACFID=POKTSI

Overall Risk Score Risk
 0 ↘ 0

Advanced Actions ▾

Recent Offenses
 No recent Sense Offens

Peers in Group membership : RACFID=POKTSO,PROFILETYPE=GROUP,SYSPLEX=PLEX1 ✕

Filter users...

	Recent risk	Risk score ↓	
DODARO1 LISA DODARO	0	0.07	
DZROSSI DAVE ROSSI	0	0.07	
PPETERS8 PHIL PETERS	0	0.07	
TSO8CHAR FRED LATES	0	0	
BARTOE2 RYAN BARTOE	0	0	
FATZ PETER FATZINGER	0	0	






Other Uses cases



THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

