z/OS 2.4 IBM Education Assistant (IEA)

Solution (Epic) Name: ITDS Remove 4096 entry limit on users/group for SDBM

Element(s)/Component(s): TDS-LDAP

Agenda

- Trademarks
- Session Objectives
- Overview
- Usage & Invocation
- Session Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.

- Additional Trademarks:
  - None

Session Objectives

- At the end of this presentation, you should have an understanding of …
- The IBM Tivoli Directory Server enhancements for
  - SDBM extended search
- How to use the enhancements

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.*

Usage & Invocation - Special search filters

- Search filters that are processed outside LDAP server
  - Search results are filtered by RACF: no need to load the complete profile to LDAP server
  - Traditional SDBM search and basic extended search only support search filters in table below
  - Other search filters supported by advanced extended search require loading the complete RACF profile to LDAP server for filter evaluation

LDAP Search Filter	**Processing Method**
objectclass=*	processed as no search filter
racfid=any_value	processed by RACF search command
racfuserid=any_value	processed by RACF search command
racfgroupid=any_value	processed by RACF search command
(&(racfuserid=any_value)(racfgroupid=any_value))	processed by RACF search command
profilename=any_value	processed by RACF search command
krbprincipalname=any_value	processed by R_usermap callable service
racflnotesshortname=any_value	processed by R_usermap callable service
racfndsusername=any_value	processed by R_usermap callable service
racfomvsgroupid=number	processed by getgrgid()
racfomvsgroupid;allOMVSids=number *	processed by RACF search command
racfomvsuid=number	processed by getpwuid()
racfomvsuid;allOMVSids=number *	processed by RACF search command

* Sequence "**;allOMVSids**" is presented as the attribute option introduced in LDAP v3

Usage & Invocation – Server configuration

- New server configuration option
  - extendedSearch {off | basic | advanced} in the SDBM section, default is off
  - Control the default SDBM search behavior
  - Overwritable by the SDBM extended search server control
- SDBM extended search server control (OID: 1.3.18.0.2.10.35)
  - Non-critical server control for the LDAP search request
  - Overwrite the server side setting for the current request
  - ASN.1 syntax:

```
sdbmExtendedSearch ::= SEQUENCE {
    level       ExtendedLevel
}

ExtendedLevel ::= ENUMERATED {
    off         (0),
    basic       (1),
    advanced    (2)
}
```

Usage & Invocation - Command line utility

- New option "-X control" in the ldapsearch utility
  - Specify an SDBM extended search server control
  - Only one option can be specified, as they are mutually exclusive

```
usage: ldapsearch [options] filter [attributes...]
where:
    filter        RFC-4515 compliant LDAP search filter
    attributes    whitespace-separated list of attributes to retrieve
        (if no attribute list is given, all are retrieved)
options:
    -?            print this text
    ……
    -x sslFipsMd  set the SSL FIPS mode (supported SSL FIPS modes are Level1, Level2, Level3, and Off)
    -X control    set a server control:
                    sdbm_extended_search_off
                    sdbm_extended_search_basic
                    sdbm_extended_search_advanced
    -z sizeLimit  size limit (in entries) for search
    -Z            use a secure LDAP connection for search
```

Session Summary

- You should have an understanding of …
    - The IBM Tivoli Directory Server enhancements for the SDBM extended search
    - How to use the enhancements

Appendix

- Publications
  - IBM Tivoli Directory Server Administration and Use for z/OS
  - IBM Tivoli Directory Server Client Programming for z/OS