Password prompt support

IBM Education Assistance for z/OS V2R4

Name: password prompt support
Element/Component: TDS-LDAP

© 2019 IBM Corporation

Agenda

- Overview
- Impacts and Attributes
- Mainline
- Errors & Recovery
- Diagnostic Aids
- Appendix

© 2019 IBM Corporation

Overview

Problem Statement, High Level Objective, Benefits

© 2019 IBM Corporation

Overview

- Problem Statement / Need Addressed
  - Customers complain about password exposure when using z/OS LDAP utilities to connect to the LDAP server.
  - Because the password is specified in the plain text form, a mechanism to prevent the characters from being displayed on the console is necessary.
- Solution
  - Use a predefined character as the reserved value for the password related command line options to indicate the password should be input in a special way that is not visible on the console.
- Benefit / Value
  - Avoid sensitive data being displayed on the console.

© 2019 IBM Corporation

Main Changes

- The “password prompt support” provides a new way to prevent passwords in the plain text form to be exposed for LDAP command line utilities.
  - The question mark “?” can be used to represent the password that is used to bind to the z/OS LDAP server.
  - z/OS LDAP command line utilities detect if “?” is specified in the bind password option, and prompts customer to input password which is not displayed from the console.
  - New function include in the following z/OS LDAP utilities:

    Server utilities:
    - *db2pwden*
    - *ldapdiff*

    client utilities:
    - *ldapadd*
    - *ldapcompare*
    - *ldapdelete*
    - *ldapmodify*
    - *ldapmodrdn*
    - *ldapsearch*

© 2019 IBM Corporation

Main Changes

- Modules

Module updated	Description
GLDCMPR	ldapcompare utility
GLDDLET	ldapdelete utility
GLDMDFY	ldapmodify utility
GLDMRDN	Ldapmodrdn utility
SDELETE	sdelete.c
GLDDB2PW	db2pwden.c

- Files

File	Path	Update
ldapcompare.c	ldap/apps/src/client/	Add “getpass()” at “-w” option
ldapdelete.c		
ldapmdfy390.c		
ldapmodify.c		
ldapmodrdn.c		
sdelete.c		
db2pwden.c	ldap/apps/src/server/	
LdapDiff.java	ldap/ported/src/boosterpack/com/ibm/ldap/bp/ldapdiff/	

© 2019 IBM Corporation

Impacts and Attributes

© 2019 IBM Corporation

Interactions & Dependencies

- Software Dependencies
  - ldapdiff utility need java 6.0 or later.
- Hardware Dependencies
  - No
- Exploiters
  - No

© 2019 IBM Corporation

Mainline

Flows, Modules, Macros

© 2019 IBM Corporation

Mainline

- The question mark “?” used to avoid password is displayed in Plaintext
  - ”?” can be specified at bind password option “-w”
  - non-echoed prompt will appear with words ”Enter current password ==>”
  - Ldap use the function: getpass() — Read a string of characters without echo

```
[SUIMGUC@DCEIMGUC.ttyp0000 ~ #] ldap_utility -D C=CN -w "?"
Enter current password ==>
```

```
-w passwd     bind password or '?' for non-echoed prompt
```

© 2019 IBM Corporation

Diagnostic Aids

Traces, IPCS, Formatters

© 2019 IBM Corporation

Test Case / Recreate Examples

- Examples
  - Old way:

    ldapmodify –p 239 -D admin –w password -f modify.ldif
  - New way*:*

    ldapmodify –p 239 -D admin –w “? “ -f modify.ldif

  After issuing the command, the console will prompt you to input the password:

  ”Enter current password ==> "

  But no character is displayed when you type.
  - The ldapdiff utility is a little different:

  you need “?” twice because this utility used for two servers comparing:

  ldapdiff -sh 1.2.3.4 -sD cn=admin -sw “?” -ch 1.2.3.5 -cD cn=admin -cw “?” -F –a

  And the console will prompt twice:

  "Enter current sw password ==> "

  "Enter current cw password ==> "

© 2019 IBM Corporation

Appendix

Publications, wikis, references, websites, terminology, etc.

© 2019 IBM Corporation

Publications

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