

# IBM Tivoli Directory Server for z/OS

Saheem Granados, CISSP

IBM

sgranado@us.ibm.com

Tuesday, March 13, 2012

10429



Visit [www.SHARE-SEC.com](http://www.SHARE-SEC.com)  
for more information on  
the SHARE Security &  
Compliance Project

# 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

- LDAP Primer
- Intro to TDS for z/OS
- About the lab.

# 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 type 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 optimizations include
  - Full sysplex support
  - System SSL, ICSF, CTRACE, WLM, ARM, DB2, etc... support
  - LDAP based access to RACF data
- 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 allow for remote RACF audit and authorization services.

# About the lab

- Introduction material that expands on Primer/Intro
- Walk through a complete LDAP server configuration setup
  - Includes DB2 setup
- Run some tests to verify configuration
- Optionally setup SSL if time permits
- User IDs SHARA01-20.
  - Passwords: “firstpw”

# References

- z/OS Hot Topics Newsletter [http://www-03.ibm.com/systems/z/os/zos/bkserv/hot\\_topics.html](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!”
- 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\\_coverage.html](http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp?topic=/com.ibm.iea.zos/plugin_coverage.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