Saheem Granados,CISSP® (sgranado@us.ibm.com) – IBM Software Engineer
August 2011

# Don't Judge an LDAP Server By Its Name

## SHARE Orlando

## August 2011

## S9545

# Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Source If Applicable

# Agenda

- Re-introduce IBM Tivoli Directory Server (TDS) for z/OS®
- Highlight Key TDS for z/OS Optimizations
  - WLM
  - ICSF
  - RACF
  - SMF
  - Sysplex
  - DB2
  - ARM
  - System SSL
  - Network Authentication Service (Kerberos)
- Review TDS for z/OS Architecture
- What's new with TDS for z/OS?
  - z/OS V1.10
    - Plug-in
    - AES encryption using ICSF
    - SSL certificate mapping
    - Operations Monitor support
    - RACF custom profiles

# Agenda (cont...)

- z/OS V1.11
  - Advanced Replication
  - WLM support
  - RACF resource profiles
- z/OS V1.12
  - Filtered Access control
  - Password Policy
  - Activity Log updates
  - Salted SHA support
- z/OS V1.13
  - Administrator Roles
  - 64 bit TDBM
  - Paged/Sorted Search
  - SHA-2 Support
  - Group Specific size/time limits

- List References to Publications

# LDAP on z/OS

- LDAP Client C APIs first introduced with OS/390 V2R4
- LDAP Server first introduced on OS/390 V2R5 as “SecureWay Security Server LDAP Server” (ISS adopted as unofficial acronym)
  - Port from distributed code base
- OS/390 V2R10 first major shift from distributed code base with introduction of TDBM
- z/OS V1R6 new LDAP Client C APIs introduced
  - 64 bit support
  - Rewritten & Optimized for z/OS
- z/OS V1R8 new LDAP Server introduced
  - Rewritten & Optimized for z/OS (more later....)
  - New Name: IBM Tivoli Directory Server for z/OS (TDS adopted as unofficial acronym)
- z/OS V1R8 – z/OS V1R10: both TDS and ISS shipped as part of z/OS
  - z/OS V1R10 was LAST release with ISS

# TDS on z/OS

- Despite Tivoli and no LDAP in name, TDS for z/OS is:
  - Base component of z/OS, i.e., not a priced feature
  - Supports LDAP V3
  - New code base, fully optimized for z/OS

- TDS and System z Optimizations classified by Key System Traits
  - Reliability
  - Availability
  - Serviceability
  - Scalability
  - Security

- Reliability & Serviceability
  - Same extensive test cycle and service process as all base components
  - Dynamic trace and z/OS Component Trace to help ffdc and use of IPCS CTRACE routines to process trace data

# TDS on z/OS

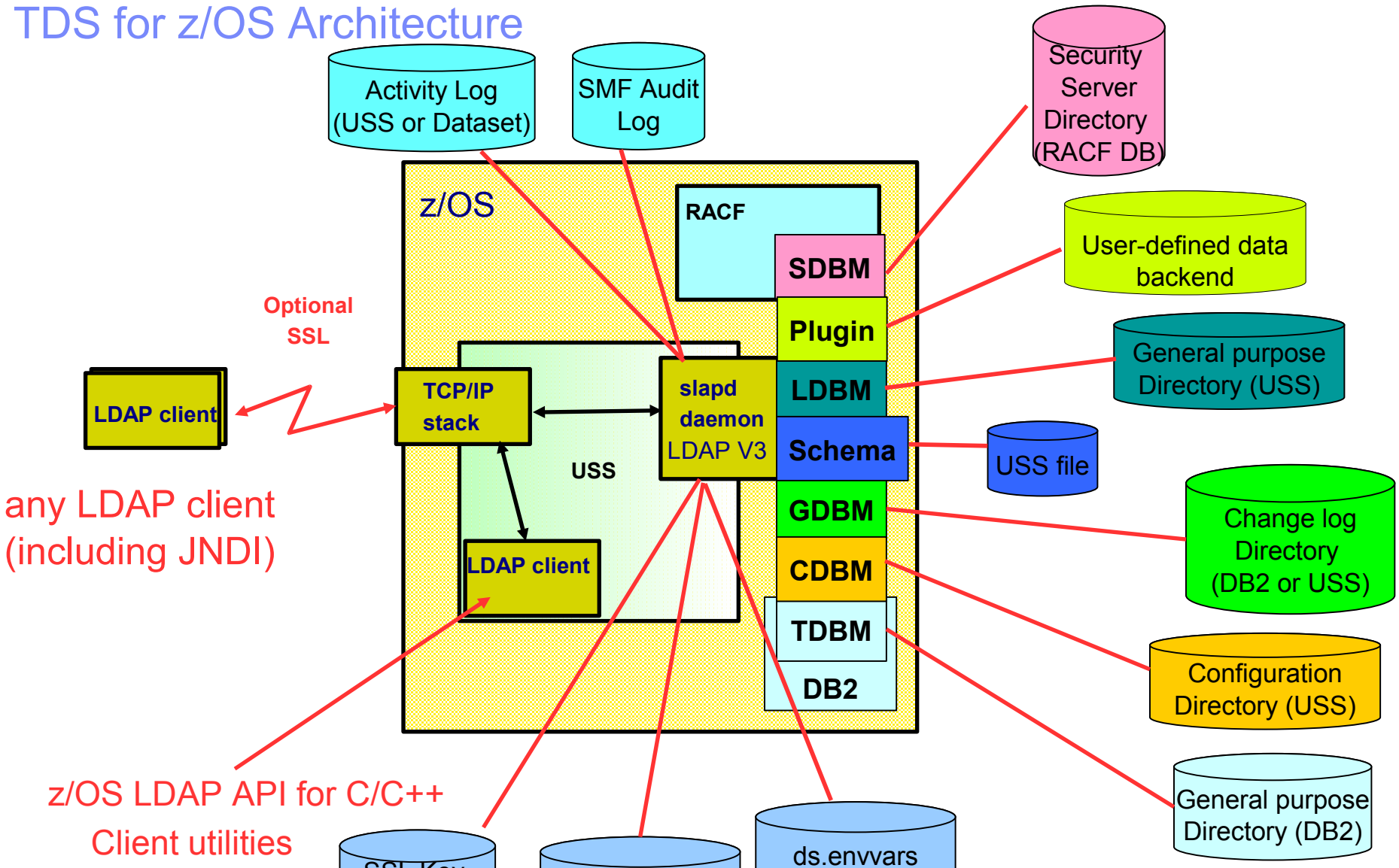
- Availability
  - Supports Parallel Sysplex Clustering Technology to allow clustering of many server instances
    - VIPA/DVIPA helps ensure client requests can be handled even if server instances are down
  - Supports Workload Manager to help ensure overall System z availability/performance requirements met
  - Supports Automatic Restart Manager to help recover server instances in case of abend
- Scalability
  - DB2 support (data sharing and partitioning support)
  - 64 bit mode
  - Rewrite resulted in better performance/CPU utilization
- Security
  - Tight RACF co-existence/relationship
    - LDAP access to RACF users, groups, user-group connections, general resource profiles, SETROPTS settings
    - LDAP authentication against RACF database
  - Leverage System SSL for SSL communication
  - Leverage ICSF for crypto for hashing and encryption
  - Supports Integrated Security Services Network Authentication Service for Kerberos authentication
  - Cuts SMF Audit Records

# TDS vs ISS

- TDS fully supports 64 bit
  - ISS did not.
- TDS supports a file based backing store (LDBM), in addition to DB2 (TDBM)
  - ISS only supported DB2 (TDBM)
- TDS fully supports WLM, Sysplex, CTRACE, ARM
  - ISS did not
- TDS supports plug-ins
  - ISS did not

- Migration instructions available for moving from ISS->TDS
  - Recommended to unload LDAP data from ISS and reload to TDS

# TDS for z/OS Architecture



# What's new with TDS for z/OS V1R10?

- Passphrase support
  - Supports native/RACF passphrases for LDAP authentication
- Plug-in
  - TDS allows custom user exit code to be introduced
  - 3 basic entry points: Pre, Post, Client
    - Pre: user exit called prior to TDS processing operation
    - Post: user exit called after TDS processes operation
    - Client: user exit called instead of TDS processing operation
  - APIs available to plug-ins
- AES encryption using ICSF
  - TDS can use AES with keys in CKDS for encrypting passwords stored in TDS
- SSL certificate mapping
  - Allows SDBM operations after certificate/SASL/native auth binds to LDAP
- Operations Monitor support
  - Helps monitor real time traffic to detect DOS attacks, performance issues
- RACF custom profiles
  - SDBM can now set and use RACF custom fields

# What's new with TDS for z/OS V1R11?

- Advanced Replication (original replication model is still supported. Refer to Basic Replication)
  - Distributed TDS replication model implement in TDS for z/OS
  - Additional Replication Topologies available
    - Peer-Peer
    - Gateway
    - Forwader
    - Master-replica
  - Additional tools/extended operations to manage replication environment
  - Server's role, i.e., master, peer, replica, forwarder, for a given topology is determined at a subtree level (as opposed to a backend basis)
  - Peer-peer supports conflict resolution
  - Filtered/partial replication
  - Scheduling
- WLM support
  - TDS interfaces with WLM's health service to indicate a health value
  - Useful for TCP/IP to route client requests
- RACF resource profiles
  - Allow SDBM access of RACF resource profiles and SETROPTS settings

# What's new with TDS for z/OS V1R12?

- Filtered Access control
  - Access control can be extended to take into account dynamic characteristics of the user
    - Time of access
    - Day of access
    - Encrypted connection
    - Bind mechanism
    - Client's IP
  - aclEntry/entryOwner values now can be extended with filters that are checked against the client's dynamic characteristics
  - Standard values are "logically" combined with filtered ACL values using set arithmetic, i.e. UNION, INTERSECT, REPLACE
- Password Policy
  - Establish/enforce password rules for passwords stored in TDS
- Activity Log updates
  - Allow for activity log roll-over
  - Allow for IP filtering of activity log entries
- Salted SHA support
  - Support Salted SHA hashing of passwords stored in TDS

# What's new with TDS for z/OS V1R13?

- Administrator Roles
  - Supports an Administrator Group
    - Addresses the issue of having more than one administrator share the same credentials
  - Also, addresses “all admins are not created equally”
- 64 bit TDBM
  - Support 64bit TDBM
- Paged/Sorted Search
  - Support Paged/Sorted results for LDAP search commands
- SHA-2 Support
  - Support SHA-2 hashing of passwords stored in TDS
- Group Specific size/time limits
  - Establish size/time limits via group membership
    - In the past, admin had no limits, and all other clients were governed by value in ds.conf

# QUESTIONS?

# LDAP Related References & Publications

- 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!”
- 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