# Tivoli Directory Server v6.3 – Part06 of 06, Best Practices and Ask the Experts.

By : Nilesh Panhale, Shruti Maheshwari, Shital Patil & Nilesh Patel

Tivoli software

# Introduction

## Abstract:

This STE will discuss ‘Best Practices’ for IBM Tivoli Directory Server release 6.3

## Objectives:

We will be covering 23 different topics related to TDS and discuss about the common errors and best practices for the same.

# Agenda

- Useful links
- Previous STEs
- Installation
- Uninstallation
- Configuration
- Migration
- Client utilities
- Web Admin Tool
- Proxy

# Agenda (Contd.)

- Start-up
- Secure Socket Layer (SSL)
- Access Control Lists
- Schema
- Password policy
- Referrals
- Tombstones
- Performance

# Agenda (Contd.)

- Pass Through Authentication
- Persistent Search
- Replication
- Hang / Core
- DB2 settings
- Day to-day tasks, like monitoring, backup
- Logging
- Plug-in

# Useful Links

- ITDS Support Portal:
  http://www-947.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Directory_Server
- ITDS Online documentation:
  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml
- Tivoli Product Lifecycle Site:
  http://www-306.ibm.com/software/sysmgmt/products/support/lifecycle/
- System Requirements:
  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/sysreq.htm
- Google group :
  http://groups.google.com/group/ibm.software.ldap/topics?lnk=gschg&hl=en

# Useful Links (Contd.)

- Support Techical Exchange (STE) Website:
  http://www-01.ibm.com/software/sysmgmt/products/support/supp_tech_exch.html
- Collecting Data For ITDS (Must Gather):
  http://www-01.ibm.com/support/docview.wss?rs=767&uid=swg21268035
- Recommended Fixes for ITDS:
  http://www-01.ibm.com/support/docview.wss?rs=767&uid=swg27009778
- Featured Documents:
  http://www-1.ibm.com/support/docview.wss?uid=swg27009603

# Useful Links (Contd.)

- Fixes by Version:
  http://www-01.ibm.com/support/docview.wss?rs=767&uid=swg21252238
- Tivoli Software Global User Group Community
  http://www.tivoli-ug.org/
- My Notifications:
  https://www-01.ibm.com/software/support/einfo.html
- Download Link from passport advantage
  http://www.ibm.com/support/docview.wss?uid=swg24015906

# Previous STEs

Part 1: Installation and Configuration

https://www-304.ibm.com/support/docview.wss?uid=swg27021610

Part 2: Web Admin Tool , ACL, SSL

http://www-01.ibm.com/support/docview.wss?uid=swg27021610

Part 3: Backup and Restore

http://www-01.ibm.com/software/sysmgmt/products/support/TE/techex_V980536A95841W35.html

# Previous STEs(Contd.)

Part 4: Replication

http://www-01.ibm.com/software/sysmgmt/products/support/TE/techex_W517531B55309Q11.html

Part 5 : Proxy, Performance, Troubleshooting

https://de202.centra.com:443/GP/main/000001b9d4d80000012fb9ce7d638b5f

# Installation and configuration

- Install the prerequisite software if you are installing with the installshield GUI, If you are using the operating system utilities to install, installation might fail if you do not have the prerequisite software installed
- Check the system requirements guide before continuing with the installation

  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/sysreq.htm

- If installation fails, check the ldapinst.log file, uninstall the previously installed components completely and then start the installation process again.
  - C:\Program, \IBM\LDAP\V6.2\var
  - /var/idsldap/V6.2

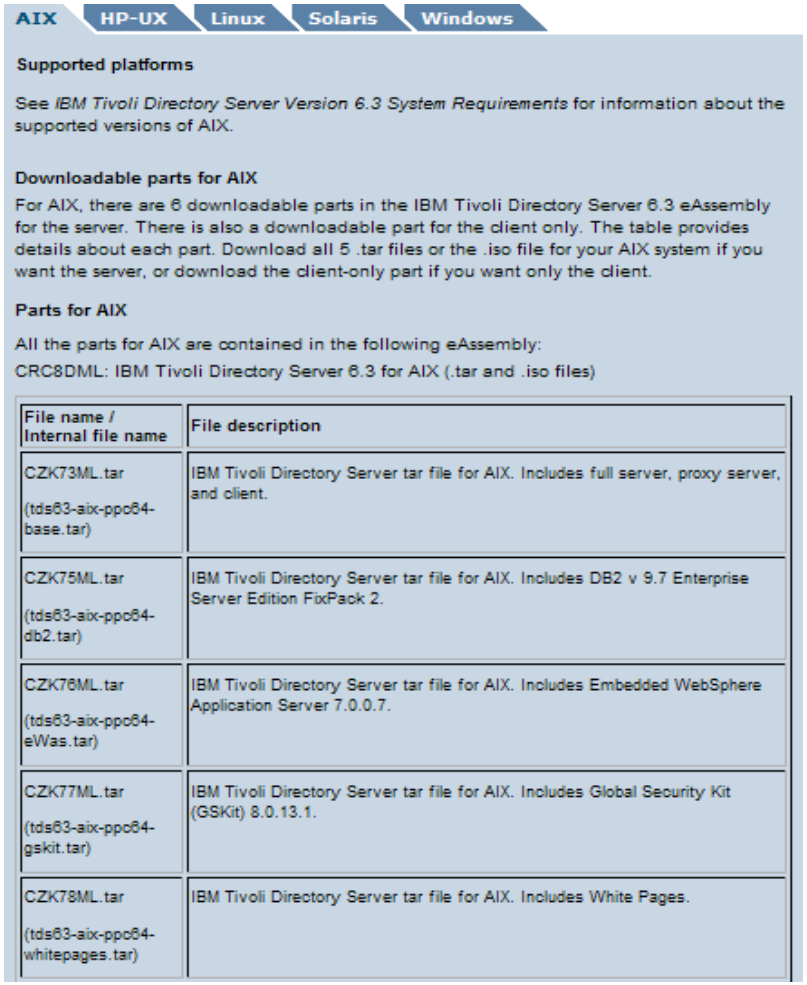
# Installation and configuration(Contd.)

- Chose the correct part number depending on your operating system and architecture

  http://www-01.ibm.com/support/docview.wss?rs=767&uid=swg24027373

- IF you have downloaded standalone TDS installable then the sequence should be

  Install GSKit => DB2 => TDS



AIX | HP-UX | Linux | Solaris | Windows

**Supported platforms**

See *IBM Tivoli Directory Server Version 6.3 System Requirements* for information about the supported versions of AIX.

**Downloadable parts for AIX**

For AIX, there are 6 downloadable parts in the IBM Tivoli Directory Server 6.3 eAssembly for the server. There is also a downloadable part for the client only. The table provides details about each part. Download all 5 .tar files or the .iso file for your AIX system if you want the server, or download the client-only part if you want only the client.

**Parts for AIX**

All the parts for AIX are contained in the following eAssembly:

CRC8DML: IBM Tivoli Directory Server 6.3 for AIX (.tar and .iso files)

| File name / Internal file name | File description |
|---|---|
| CZK73ML.tar (tds63-aix-ppc64-base.tar) | IBM Tivoli Directory Server tar file for AIX. Includes full server, proxy server, and client. |
| CZK75ML.tar (tds63-aix-ppc64-db2.tar) | IBM Tivoli Directory Server tar file for AIX. Includes DB2 v 9.7 Enterprise Server Edition FixPack 2. |
| CZK76ML.tar (tds63-aix-ppc64-eWas.tar) | IBM Tivoli Directory Server tar file for AIX. Includes Embedded WebSphere Application Server 7.0.0.7. |
| CZK77ML.tar (tds63-aix-ppc64-gskit.tar) | IBM Tivoli Directory Server tar file for AIX. Includes Global Security Kit (GSKit) 8.0.13.1. |
| CZK78ML.tar (tds63-aix-ppc64-whitepages.tar) | IBM Tivoli Directory Server tar file for AIX. Includes White Pages. |

# Installation and configuration(Contd.)

Before you continue with the installation, it is a good practice that you create a user and make it a member of the idsldap group.

For AIX

- mkgroup idsldap
- mkuser pgrp=idsldap home=/home/idsldap shell=/bin/ksh idsldap
- passwd idsldap

For Linux/ HP/ Solaris

- groupadd idsldap
- useradd -g idsldap -d /home/idsldap -m -s /bin/ksh idsldap
- passwd idsldap

# Installation and configuration(Contd.)

- Verify that the idsicrt command has run successfully to create the database instance with idscfgdb
- On Windows OS, check the password specifications to avoid messages such as “DB2 install was not successful / cannot create user”
- Stop the Tivoli Directory Server before configuring a suffix
- Run the idslink utility to direct the pointers to the new installation

  For ex idslink -g -i -s myinstance –f

# Uninstallation

- Drop the existing instances before you begin with uninstallati

```
idsidrop -I <instance name>
```

- Remove the installation directory manually after uninstallation is complete
- Clean up any registry entries that might have been made by the installation process, on Windows use **regedit** to remove the LDAP entry in the registry as below

```
HKEY_LOCAL_MACHINE\SOFTWARE\IBM\IDSLDAP\6.2
```

- On AIX

```
lslpp -l |grep -i idsl,
```

if any packages are left then

```
installp -u <packagename>
```

- On Linux

```
rpm -qa | grep -i idslrpm -ev packagenames
rpm -ev --noscripts packagenames
```

- On Solaris

```
pkginfo | grep -i idsl
pkgrm packagenames
```

# Migration

- Idsimigr utility is prefered over instance administration tool as it ignores few attributes that are not required
- Take backup of the schema, configuration, and key stash files before migration, even if, the user has not dropped the instances.
- When migrating from 6.0 or later version to 6.2
  - If the instance already exists then do not specify the path of backup directory, if it has been dropped then you need to specify the path

# Migration (Contd.)

- Verify that the DB2 environment variables point to the correct DB2 version which is being used by the latest Directory Server
  - PATH
  - CLASSPATH
  - INCLUDE
  - LIB
  - DB2INSTANCE

# Client utilities

- If a null DN is specified, or a 0 length DN is specified, you receive unauthenticated access unless you are using an external bind (SASL) such as Kerberos
- When specifying a DN and password make sure it falls under any suffix in the directory else a referral is returned.
- Specify the user password with the object along with the correct DN and password for the result to be returned
- To display syntax help with any client utility / command type
  - <command name> -?
  - For ex. ldapmodify -?

# Web Admin Tool

- Ensure that the application server on which the WAT is installed is started .
- When using the Web Admin Tool, do not open additional login panels from the **File** options of the browser. Only one instance of the WAT can function on a single browser instance.
- Avoid changing the password using command line when you are already logged into the Web Admin Tool .
- The **Back** and **Forward** buttons on Internet browsers cannot be used to navigate the Web Administration Tool

# Web Admin Tool (Contd.)

- If Internet Explorer's cache is set to never check for new pages, webadmin can return stale pages from the cache. So it should be changed from "Never" to "Automatically" or "Every visit to the page”.
- Avoid using the latest version of Web Administration Tool to administer an older version of the directory server instance, as some of the panels may not be visible
- Suffix does not show up in the Web Admin tool .

https://www-304.ibm.com/support/docview.wss?rs=767&uid=swg21412674&dc=DB560&wv=1

# Proxy Server

- While configuring the proxy server initially start it in the configuration only mode
- Do not perform a null based serarch on the Tivoli Directory Proxy Server, as it is not supported
- For the proxy server to start in normal mode, check whether it is able to connect to all of its backend servers
- Ensure that the schema is same across Proxy and Backend servers
- To update schema, update using local admin user or user with schema admin privileges, update on back-end servers and proxy separately

# Start up

- Always issue the command ibmslapd –I <instance name> -n to start the server .
- Ensure ulimit settings are correct by executing the command ulimit –a.

  http://www-01.ibm.com/support/docview.wss?uid=swg21206894&wv=1
- Try to start ibmslapd with root privileges .
- If Db2 admin user password expires ,the server will start in configuration only mode or will not start at all . Reset it as per the link below :

  https://www-304.ibm.com/support/docview.wss?uid=swg21297067&wv=1

# Start up (Contd.)

- db2nodes.cfg needs to be updated if the hostname is modified.
- TDS startup might fail if the hostname cannot be resolved. Correct the hostname and IP address in the /etc/hosts file.
- ibmslapd fails to start after idsdbrestore
  https://www-304.ibm.com/support/docview.wss?rs=767&uid=swg21423555&dc=DB560
- ibmslapd fails to start from services panel.
  https://www-304.ibm.com/support/docview.wss?rs=767&uid=swg21431177&dc=DB560

# Start up (Contd.)

- ibmslapd does not start if there is undefined attribute in ibmslapd.conf
  https://www-304.ibm.com/support/docview.wss?rs=767&uid=swg21222536&wv=1
- ibmslapd server process won't start when ibmslapd.conf is truncated
  https://www-304.ibm.com/support/docview.wss?rs=767&uid=swg21221726&wv=1
- ibmslapd does not start up after migration because of an existing table in DB2
  https://www-304.ibm.com/support/docview.wss?rs=767&&uid=swg21375531&wv=1

# Secure Socket Layer (SSL)

- GSKit should be installed before the client or base server “max_crypto” packages are installed.
- Run the following command to verify that SSL is set up correctly.

```
ldapsearch -Z -K <keyfile> -P <keyfilepw> -b
suffix objectclass=*
```

- Key label in .kdb file and ibmslapd.conf file should match.
- The key database certificate should be created before setting up SSL

# Secure Socket Layer (Contd.)

- Do not use the default key name/path for the SSL key database file
- Collecting a GSKIT Trace

  https://www-304.ibm.com/support/docview.wss?rs=767&uid=swg21283690&dc=DB560

- Value for the timeout of the SSL handshake transaction can be configured using SSL_TIMEOUT_MILLISEC environment variable.

  Setting the SSL_TIMEOUT_MILLISEC environment variable
  http://www-01.ibm.com/support/docview.wss?uid=swg21233758

# Access Control Lists

- When there a large number of setting to be done for a particular subject, setting up the ACLs using the Web Admin Tool is much easy
- Verifying ACLs for an entry :

```
idsldapsearch -p <port #> -D <admin DN> -w <admin DN password> -b "your base DN" -s base "objectclass=*" aclentry aclpropagate aclsource entryowner ownerpropagate ownersource ibm-filterAclEntry ibm-filterAclInherit ibm-effectiveAcl
```

# Access Control Lists(Contd.)

- When +ibmaci is present in search, the server returns all operational attributes to which the client is authorized.

```
idsldapsearch -p <port> -D <admin DN> -w <admin DN
password> -b "your base DN" -s base "objectclass=*"
+ibmaci
```

- Granular ACLs can be set for particular attributes rather than the complete security class.

```
aclEntry: role:cn=System
Admins,o=IBM:object:grant:a:at.attribute2:grant:rsc
:critical:grant:rsc
```

# Schema

- It is not recommended to manually edit the V3.* files.
- Creating indexing rule for an attribute greatly improves the response time to searches with filters which include those attributes.
- Schema replication needs to be explicitly setup on cn=ibmpolicies to have the changes under cn=schema replicated.

# Schema(Contd.)

- Partially configured replication under cn=ibmpolicies might cause the schema modification to fail if the server ID is modified
- Errors can be encountered if the format of backed-up schema files is incorrect.
- If the schema defines too many attributes, Transaction log is full kind of error messsages are displayed .

# Password policy

- Password Policy cannot be enforced for the password of the console administrator .
- This feature is not available in configuration only mode although level of password encryption can be changed .
- Password policy entry has to be created before it can be associated with a user or a group entry as an individual or a group password policy.
- The administrative password policy applies to all these users except the DB2 user.

# Password policy(Contd.)

- Do NOT assign global password policy to a user as an individual or a group password policy
- In a distributed environment, all members of a group have to be defined in same backend server.
- The administration password policy is set using the command line only. Web administration tool does not support administration password policy

# Referrals

- A referral specifies the URL of an alternate LDAP server.
- Referrals are not recommended in a proxy environment.
- On the Linux, Solaris, and HP-UX platforms, if a client hangs while chasing referrals, ensure that the environment variable LDAP_LOCK_REC has been set in your system environment.
- The default referral LDAP URL does not include the DN portion. It includes only the ldap:// identifier and the hostname:port

# Tombstones

- This feature supported with TDS 6.2 and above versions.
- This feature is supported only in the primary RDBM backend of the directory server.
- Tombstones are not supported in configuration, schema, or change log backend.
- Tombstone feature is disabled by default.

# Performance

- Configure LDAP caches to improve directory servers performance .
- Use the Instance Administration Tool, **idsperftune**, and **idsdbmaint** for performance tuning
- Obtain server status and statistical information to assess and improve directory server performance.
- Control LDAP Client functions .
- Perform regular runstats and reorg of tables and indexes .

# Pass Through Authentication(PTA)

- Pass-through servers need to be running.
- For attribute mapping, always use an attribute which has unique values.
- One user entry should not map to multiple PTA servers.
- One instance can have multiple PTA servers.
- Schema has to be defined on PTA server.
- Configuring PTA to an AD catalog .

https://www- 304.ibm.com/support/docview.wss?rs=767&uid=swg21393633&wv=1

# Persistent Search : A search that never stops

- The Persistent Search operation is memory- and connection-intensive for the LDAP server
- If you are using this feature make sure you have set value of attribute `ibm-slapdMaxPersistentSearches` to not more than 2000
- Enforce ACL to make sure that users can retrieve only those entries or parts of entries that they have access to
- The search size and time limits applicable for non-administrative users will be applicable for persistent search
- Check information on how to set client to use persistent search can be found in Programming Ref Guide of TDS 6.3

# Replication

- All master-replica servers should be Cryptographically Synchronized.
- Server ids for master and replica servers should be unique.
- Customized schema files should be synchronized on all master and replica servers.
- Replication topology should be modified after making any changes in the IP address or hostname of OS.
- Bind Password should be synchronized in the topology and ibmslapd.conf file.

# Replication contd..

- Enable or disable replication conflict resolution as per the requirement.

  Disabling replication conflict resolution

  http://www-01.ibm.com/support/docview.wss?uid=swg21236775

- For the schema replication or password policy replication, replication for subtree cn=ibmpolicies should be configured.
- Replication queues should be monitored continuously.
- Make sure to set `IBMSLAPD_REPL_UPDATE_EXTRA_SECS` large data is being replicated which takes more that 60 seconds to replicate

# Replication contd..

- Set Ulimits appropriately to avoid Master hang
- Never stop multithreaded supplier abruptly
- If using WAT to configure replication, make sure you resume the replication
- Make full use of Scheduled Replication considering the load on the system at different times
- replication events are scheduled too closely together

# Hang / Core

- Set Ulimits as recommended.
- For hang problem, you can run any ldap operation like ldapsearch, ldapadd or ldapmodify to verify whether it is server hang problem or some other issue.
- Server should be up to date with the latest Fix Pack.
- After a hang, always connect to the database and perform a simple select operation on database like the following :

```
db2 "select * from ldap_entry"
```

- Thread dump and audit log should be checked to debug hang or core issues.

# DB2 Settings

- When the password for DB2 user is modified, TDS configuration file must be updated to reflect the change.
- After the installation of DB2 Fix Pack, it is very important to go through the post install procedure.
  http://www-01.ibm.com/support/docview.wss?uid=swg21217323
- Fixing an "SQL0964C Transaction log for database is full" error
  http://www-01.ibm.com/support/docview.wss?uid=swg21121437

# DB2 Settings contd..

- Locate transaction logs on dedicated disks
- Use the `AUTOCONFIGURE` command to obtain good initial configuration settings
- Keep track of changes in configuration and environment settings
- Only tune things that can explain the symptoms you are seeing. Don't change the tire if the engine won't start
- If required increase the database connection in conf file

# DB2 Settings contd..

- The db2look command can be used to see reports of all the system statistic settings in the database

```
db2look -m -d ldapdb2 -u ldapdb2 -o output_file
```

where,

*ldapdb2* is the database name,

*output_file* is the file name with location for storing the results

- Use `db2 force applications all` command prior to the `db2stop`

# Day to Day Tasks

- Regular backup of database and directory data.
- Backup of Schema files.
- Monitor File Size, CPU usage, replication queues.
- In distributed directory environment schema should be synchronized.
- Keep the Server, Client and the GSkit up to date.
- Tuning should be done as per the data load(reorg and indexing).

# Logging Utilities

- **Pre operation audit log**
  - IBMSLAPD_PREOP_AUDIT=YES
- **idslogmgmt tool**
  - TDI required.
  - Setting on TDS side.
- **lostandfound.log**
- **ibmslapd.log**
- **db2diag.log**
- **db2cli.log**

# Plug-in

- When writing a plug-in, follow the steps and procedure mentioned in the Plug-in reference guide.
  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBMDS.doc/plugin.htm
- To compile the code, make file as mentioned in this technote can be used
  http://www-01.ibm.com/support/docview.wss?uid=swg21308436
- Server plug-ins extend the capabilities of your Directory Server. They are dynamically loaded into the LDAP server's address space when it is started
- A server plug-in can return a message to the client as well. However, make sure that the server returns only one message.

# Plug-in(Contd.)

- Custom codes for plug-ins are not supported, however any issues with the TDS code base in relation to the plug-ins are supported
- TDS 6.3 supports the following types of server plug-ins :
  - Database plug-in
  - Pre-operation plug-in
  - Post-operation plug-in
  - Extended operation plug-in
  - Audit plug-in
  - DN partitioning plug-ins

# Plug-in(Contd.)

- Plug-ins must be written using reentrant system calls.
- Global mutex issues in the plug-in.
- Multiple pre- or post-operations are called in the order they appear in the configuration file.

# Self help for any known issues

- Search error code in technotes
  http://www-01.ibm.com/support/search.wss?rs=767&tc=SSVJJU&dc=DB520+DB560&dtm
- Search error code in the APAR site
  http://www-01.ibm.com/support/search.wss?rs=767&tc=SSVJJU&dc=DB550+D100&dtm


Thank
You