IBM DB2 and Transparent LDAP Authentication

IBM Deutschland Research & Development GmbH
SAP DB2 Development Team
08/2009

Author: Hinnerk Gildhoff - hinnerk@de.ibm.com
Co-Author**:** Marcel Csonka – marcel.csonka@de.ibm.com

1. Abstract

This document describes how to use transparent LDAP with DB2. This is a new feature of DB2 9.7 and has been supported since DB2 9.5 FP4.

Older database versions had a different and more complicated approach in using the benefits of LDAP together with DB2 which is described in more detail in the whitepaper "IBM DB2 authentication with OpenLDAP in system landscapes like SAP" [2].

The old approach works with security plug-ins which users needs to install and configure before they can combine the benefits of DB2 and LDAP in their system environments. The communication between DB2 and LDAP is managed by these plug-ins as a broker.

With the new transparent LDAP feature of DB2, we do not need to configure any plug-ins anymore. DB2 can now access and support underlying operating systems that are configured to use LDAP as authentication mechanism for users and their groups. So, DB2 asks the operating system which can get the needed information from the LDAP server and returns it to the database. The database operates not differently from local system authentication. The LDAP authentication works now as a transparent feature in DB2.

In this whitepaper, you learn how to set up LDAP users and groups for DB2 on Linux and how you can use OpenLDAP and DB2 without having to configure security plug-ins. You understand the benefits of transparent LDAP support in DB2 and how you can use this in you own system environment to improve your user management.

2. Table of Contents

3. Disclaimer & Trademarks

The information in this document may concern new products that IBM may or may not announce. Any discussion of OEM products is based upon information which has been publicly available and is subject to change. The specification of some of the features described in this presentation may change before the General Availability date of these products.

REFERENCES IN THIS PUBLICATION TO IBM PRODUCTS, PROGRAMS, OR SERVICES DO NOT IMPLY THAT IBM INTENDS TO MAKE THESE AVAILABLE IN ALL COUNTRIES IN WHICH IBM OPERATES.

IBM MAY HAVE PATENTS OR PENDING PATENT APPLICATIONS COVERING SUBJECT MATTER IN THIS DOCUMENT. THE FURNISHING OF THIS DOCUMENT DOES NOT IMPLY GIVING LICENSE TO THESE PATENTS.

TRADEMARKS

IBM, the IBM logo, ibm.com, and DB2, 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"

SAP and related names like SAP NetWeaver are registered trademarks of SAP AG in Germany and in several other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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

4. Transparent LDAP

LDAP is a Lightweight Directory Access Protocol that describes the communication between LDAP clients and a directory server. It is based on a client/server model, which is generally used together with directory services. The directory server contains object-related information which can be read by different LDAP clients using LDAP queries that fulfill the standard LDAP implementation.

One of the important reasons for using LDAP is the centralized management of logon credentials, which can be queried by any applications supporting the open LDAP standard. Additionally, it is easy to use and to integrate in your existing environment and the LDAP protocol provides great flexibility. With LDAP, it is possible to create a single point of administration across a heterogeneous environment.

In order to get detailed information about LDAP, refer to [1] or other documentations. Intended audience for this paper, are experienced administrators with at least knowledge about how to configure LDAP servers and clients (Otherwise see [2]). We focus on the DB2 SAP users and groups that are needed to leverage LDAP with your SAP system, based on IBM DB2.

4.1 Configure Transparent LDAP for DB2

The first thing to do, create a LDIF file containing all user and group objects in an LDAP like manner. Our base DN is simply an example. If you have an existing LDAP tree in your directory, change the root node appropriately and include the following as an sub tree into your structure.

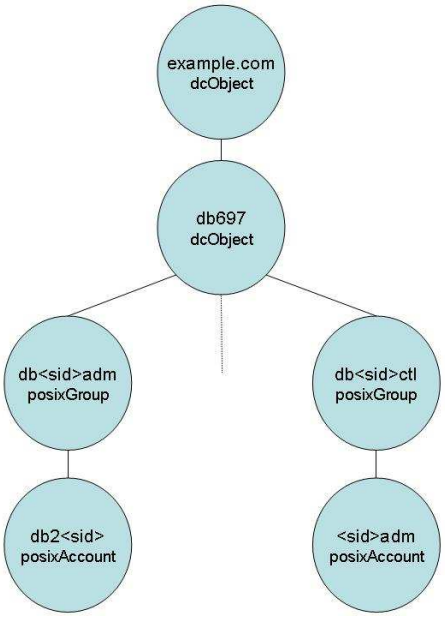

Figure 1 - DB2 LDIF Tree

It is possible to use a remote or a local LDAP server. Ensure that your LDAP server is up and running and that it is working correctly. The following LDIF file represents the structure described in Figure 1 with the SAP example identifier *HM1*. Use this file with your own SID to add the new objects to your LDAP server:

```
# base dn:          example.com
dn:                 dc=example,dc=com
dc:                 example
o:                  example
objectClass:        organization
objectClass:        dcObject
# pc box db
dn:                 dc=db697,dc=example,dc=com
dc:                 db697
o:                  db697
objectClass:        organization
objectClass:        dcObject

#
# Group: db<sid>adm
#
dn:                       cn=dbhm1adm,dc=db697,dc=example,dc=com
cn:                       dbhm1adm
objectClass:              top
objectClass:              posixGroup
gidNumber:                400
objectClass:              groupOfNames
member:                   uid=db2hm1,cn=dbhm1adm,dc=db697,dc=example,dc=com
memberUid:                db2hm1
#
# User: db2<sid>
#
dn:                       uid=db2hm1,cn=dbhm1adm,dc=db697,dc=example,dc=com
cn:                       db2hm1
sn:                       db2hm1
uid:                      db2hm1
objectClass:              top
objectClass:              inetOrgPerson
objectClass:              posixAccount
uidNumber:                400
gidNumber:                400
loginShell:               /bin/csh
homeDirectory:            /db2/db2hm1
#
# Group: db<sid>ctl
#
dn:                       cn=dbhm1ctl,dc=db697,dc=example,dc=com
cn:                       dbhm1ctl
objectClass:              top
objectClass:              posixGroup
gidNumber:                404
objectClass:              groupOfNames
member:                   uid=hm1adm,cn=dbhm1adm,dc=db697,dc=example,dc=com
```

```
memberUid:              hm1adm
#
# User: <sid>adm
#
dn:                uid=hm1adm,cn=dbhm1ctl,dc=db697,dc=example,dc=com
cn:                hm1adm
sn:                hm1adm
uid:               hm1adm
objectClass:       top
objectClass:       inetOrgPerson
objectClass:       posixAccount
uidNumber:         404
gidNumber:         404
loginShell:        /bin/csh
homeDirectory:     /home/hm1adm
```

Save this in a text file, for example, /data/ldap/db2_97.ldif and execute the following command to add these entries to your LDAP server:

```
ldapadd r- -D "cn=Manager,dc=example,dc=com" -W -f /data/ldap/db2_97.ldif
```

After successful registration of the DB2 users and the respective groups at the LDAP server, logon to the server where you want to install the database. As mentioned before, this could be your local LDAP server host or a different server. You only need to configure your LDAP client accordingly.

Next, ensure that all home directories for the new users exist with the right permissions, especially for the database administrator user. In our case, this is db2hm1. The SAP installation tool does not create these directories because we use an existing user in the db2 setup process. So, ensure that these directories exist with at least two files needed for user environment specifications (.profile and .login). If this is not the case, create the directories and the files as specified below. DB2 saves data in these directories and adds a few lines to the profile files enabling the database administrator, for example, to access the db2 library.

```
rwxr-xr-x   hm1adm:hm1adm     /home/hm1adm
-rw-r--r--  hm1adm:hm1adm     /home/hm1adm/.profile
-rw-r--r--  hm1adm:hm1adm     /home/hm1adm/.login
rwxr-xr-x   db2hm1:db2hm1     /db2/db2hm1
-rw-r--r--  db2hm1:db2hm1     /db2/db2hm1/.profile
-rw-r--r--  db2hm1:db2hm1     /db2/db2hm1/.login
```

Before you continue with the SAP/DB2 installation, validate the current system environment. You need to check whether the LDAP server is accessible, users and groups are registered at the directory server and, if the usage of LDAP is enabled.

In order to test if the LDAP server is accessible and whether all required users are included, it is recommended that you use the ldapsearch command. If open LDAP tools are installed (see [2]) and the LDAP server is up and running, the following command returns all users listed in the LDAP directory:

```
# ldapsearch –x
```

Now check if your operating system is using LDAP as authentication mechanism. These commands should return your local and your new configure LDAP user and groups:

```
# getent passwd
# getent group
```

After validation was successful, start the SAP installation tool (SAPinst). SAPinst will determine existing users automatically without further interaction, as seen in Figure 2. You just have to enter the current password of the LDAP users. That is all. The SAP and DB2 installation supports now your LDAP user and groups.

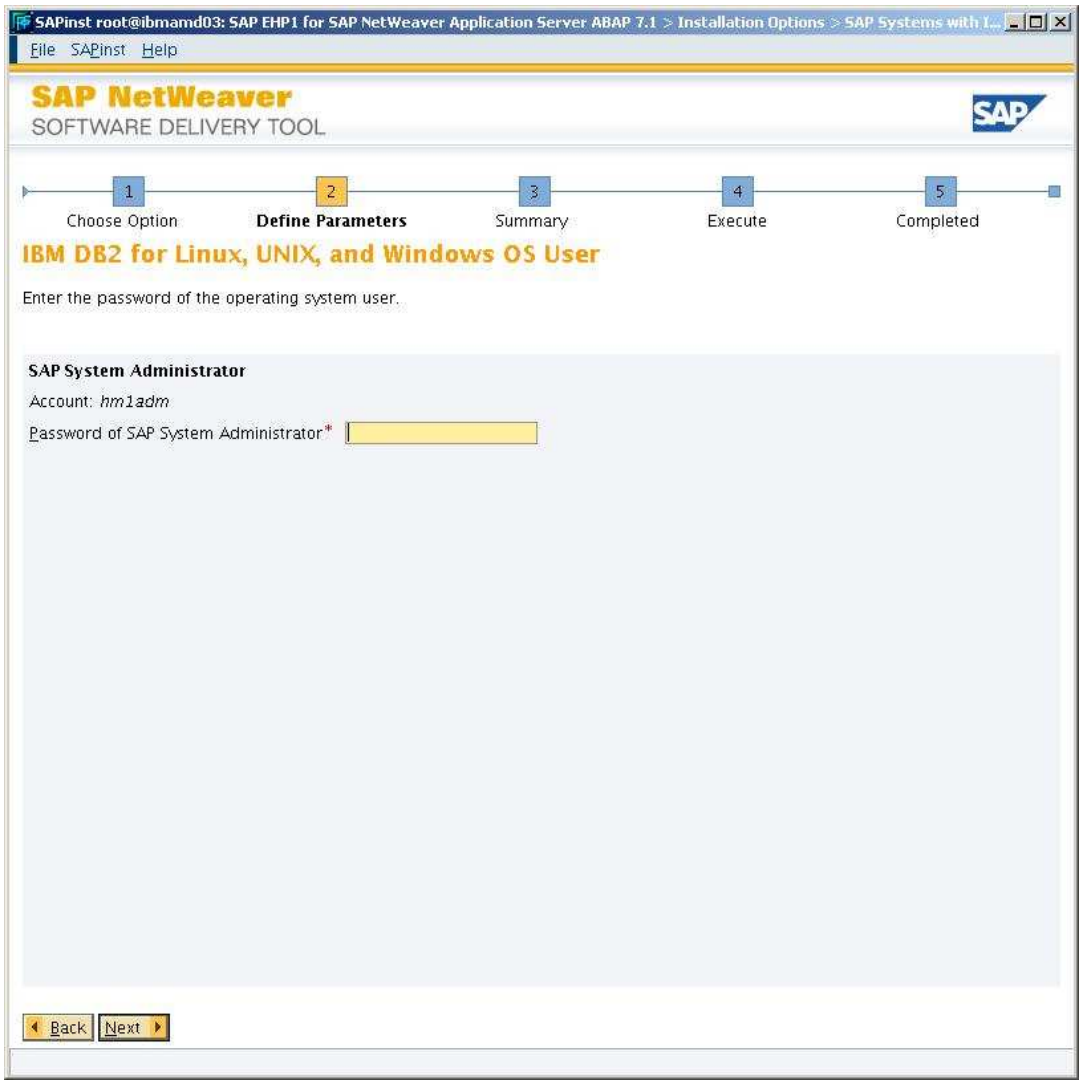

Figure 2 - Use existing LDAP user as <sapsid>adm

After your installation finished successfully, change to your new database administrator `db2hm1` and check if you have the required authorities to perform your daily administrative tasks. As you will see, everything will work as before with local user authentication.

As a conclusion we see, that the usage of LDAP with DB2 V9.5 FP4 and DB2 9.7 is much more easy than before. The installation process of DB2 for SAP did not change and no special DB2 configuration is needed anymore. The only requirement is a base knowledge with LDAP for setting up the LDAP environment and adding the DB users and groups as described above. All the other underlying communication is fully transparent to the user.

5. List of Abbreviations

LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
DN	Distinguished Name
DBA	Database Administrator
SID	SAP System Identifier

6. Table of Figures

7. List Of Literature

[1] Understanding LDAP – Design and Implementation, June 2004,

http://www.redbooks.ibm.com/abstracts/sg244986.html

[2] IBM DB2 authentication with OpenLDAP in system landscapes like SAP

https://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/e098bb76-f50a-2c10-bf8e-ae421e82e9f9