IBM Directory Server Version 5.1
README Addendum

IBM Directory Server Version 5.1
README Addendum

Note

Before using this information and the product it supports, read the general information under “Notices”, on page 27.

Fifth Edition (April 2003)

This edition applies to version 5, release 1, of the IBM Directory Server and to all subsequent releases and modifications until otherwise indicated in new editions.

Preface

This file contains information about changes and fixes that occurred after the product documentation had been translated. This file is in English only. This file can also be found by selecting **Library** on the IBM® Directory Server Web page, located at http://www.software.ibm.com/network/directory.

Contents

Preface iii

1.0 Must read known problems 1

1.1 New locations for the installation program . . . 1

1.2 Interrupting ldapxcfg database tasks causes an incorrect status for the files 1

1.3 ldapxcfg startup messages are in English. . . . 2

1.4 Web Administration Tool does not save templates created with an object class that has no attributes . . 2

1.5 Port number error in Web Administration help panel 2

1.6 Translated titles might truncate 2

1.7 Default value of LOGFILSIZ needs to be increased 3

1.8 Environment variables removed during migration 3

1.9 DSML file client throws exception 3

1.10 Nondefault log files need valid path 4

1.11 Replication limitations 4

1.12 Default ports for the embedded version of IBM WebSphere® Application Server - Express. 5

1.13 Clarification for ldapsearch -i <*file*> option. . . 5

1.14 On UNIX systems you must configure the database in a location other than /home when /home is an NFS mount 6

1.16 HTTPS for the Embedded Version of WebSphere Application Server Express Version V5.0 8

1.17 Corrections to the Kerberos information in the Administration Guide 9

1.18 /var requirements on UNIX platforms 9

1.19 Before you configure: creating the DB2 database owner 9

2.0 Must read known problems - platform specific 11

2.1 For AIX only 11

2.1.1 Supported levels of the AIX operating system 11

2.1.2 Preventing logouts on AIX 5.x systems when InstallShield GUI is invoked. 11

2.1.3 Locales for InstallShield GUI panels . . . 11

2.1.4 Missing titles from ldapxcfg panels in simplified and traditional Chinese 11

2.1.5 Error code -1 at startup. 11

2.1.6 Migrating DB2 fixpack3 to DB2 fixpack7 . . 12

2.1.7 Applying DB2 8.1 fixpaks on AIX 5.x systems. 12

2.1.8 Enabling Asynchronous IO 12

2.1.9 Configuration program fails on AIX with 0509-136 errors 12

2.1.10 Error on AIX 5.1 when running db2start . 13

2.2 For Windows NT®, Windows 2000 and Windows XP client, only: 14

2.2.1 Setting LANG and LC_ALL system environment variables for nonEnglish InstallShield GUI installation 14

2.2.2 Uninstalling Version 5.1 shows Version 4.1 option 14

2.2.3 Installing and uninstalling DB2 with InstallShield GUI 14

2.2.4 Tomcat Web application does not start with IBM JDK 1.3.1 14

2.2.5 Certain UTF-8 supplementary characters do not display correctly 15

2.3 For Solaris Operating Environment Software only:. 15

2.3.1 Locales for InstallShield GUI panels . . . 15

2.3.2 Command line installation using pkgadd. . 15

2.4 For Linux only: 17

2.4.1 CD-ROM does not eject from Linux machines 17

2.4.2 Java failure when configuring an existing instance and database 17

2.4.3 Incorrect display when installing with the InstallShield GUI on a system set to a Japanese locale 18

2.4.4 InstallShield GUI uninstall does not remove the appsrv directory 18

2.4.5 Linux S/390 client operations fail with SSL using GSKit 6.0 18

2.4.6 DB2 opt file requirements 18

2.4.7 GSKit 6.0.3 is not supported on Intel Linux 18

2.5 For HP-UX only 19

2.5.1 HP-UX 11 client is supported. 19

3.0 General information, hints and tips 21

3.1 Peer-to-peer scenario with Web Administration Tool 21

3.2 Migrating a replicating environment from 3.2.x to 5.1 22

3.3 Support for industry standards 23

3.4 Password Guidelines 24

Passwords for User Entries (InetOrgPerson) stored in the IBM Directory Server using the C or java Software Development Kits 24

LDAP ibmslapd.conf users: 24

Using the IDS Web Administration Tool to modify password attributes: 25

Additional Recommendations: 25

Appendix. Notices 27

Trademarks 28

1.0 Must read known problems

The following information applies cross-platform.

1.1 New locations for the installation program

The location of the installation programs on the CD and in the .zip and .tar files has changed:

On Windows® platforms:

- If you are installing from a CD, on the CD, in the \ids_ismp folder, double-click **setup**.
- If you downloaded the .zip file, go to the directory where you unzipped the .zip file. In the \ids_ismp folder, double-click **setup**.

On AIX®, Solaris, and Intel Linux platforms, for InstallShield GUI installation:

- If you are installing from a CD, on the CD, change to the /ids_ismp directory and type **./setup**. You must type **./setup** on the command line even if ″.″ is in your path. Otherwise, the WebSphere Application Server - Express, V5.0 installation does not work.
- If you downloaded the .tar file, go to the directory where you untarred the file. Change to the /ids_ismp directory and type **./setup**.

On UNIX® platforms (including Linux S/390® and HP-UX), for native installations:

- If you are installing from a CD, on the CD, change to the /ids directory and then follow the instructions in the *IBM Directory Server Version 5.1 Installation and Configuration Guide*.
- If you downloaded the .tar file, go to the directory where you untarred the file. Change to the /ids directory and then follow the instructions in the *IBM Directory Server Version 5.1 Installation and Configuration Guide*.

1.2 Interrupting ldapxcfg database tasks causes an incorrect status for the files

If you are using **ldapxcfg** to configure, unconfigure, import, export, backup, restore, or optimize a database and the process is interrupted by, for example, a segmentation fault, the status of the files is returned incorrectly. When you try to restart the process the message

```
Task is already running.
```

is displayed. This is because the status output for the process is monitored through files in the $LDAPHOME/tmp folder that were not deleted when the process was interrupted.

To restart the interrupted process, you must first manually delete these two files:

```
  /usr/ldap/tmp/ldapcfg.dat
  /usr/ldap/tmp/ldapcfg.stat file to start configuration from starting
```

1.3 ldapxcfg startup messages are in English

Although you might have selected a different locale, when you start the **ldapxcfg** utility the following startup messages are always displayed in English:

```
MenuManager: File 'FILE.pdml.ser' loaded successfully
MenuManager: File 'EDIT.pdml.ser' loaded successfully
MenuManager: File 'VIEW.pdml.ser' loaded successfully
MenuManager: File 'HELP.pdml.ser' loaded successfully
(-) SHOW_TOOLBAR
(+) STATUSBAR
(-) TEXT_BOTTOM
(+) NO_TEXT
(-) TASKPAD
(+) TREE
MenuManager: File 'APP_TOOLBAR.pdml.ser' loaded successfully
CSA Toolkit Version 1 Release 2
(c) Copyright IBM Corporation 2001. All rights reserved.
```

1.4 Web Administration Tool does not save templates created with an object class that has no attributes

You can create object classes for the IBM Directory Server Version 5.1 that have no MAY or MUST attributes. Such object classes can be used to create entries using other auxiliary object classes. However, if you attempt to create a template through the Web Administration Tool using such an object class, you are unable to save the template.

Note: All of the object classes included with the IBM Directory Server Version 5.1 contain MAY and MUST attributes. They can be used to create templates.

1.5 Port number error in Web Administration help panel

If performing **Console administration**, under **Manage console servers**, the **Add** function has an incorrect help. Clicking **Help** from the **Add server** panel displays the **Add, modify or remove a server from the console** help panel. This panel has a link, **Port/Administration port**, that displays the following information:

```
Specify the port numbers or accept the defaults.

If SSL is enabled, the default port number is 389 and the default administration
port is 3538. If SSL is not enabled, the default port number is 636 and the
default administration port is 3539.

If SSL is enabled, make sure you select SSL enabled ports.
```

The correct default port numbers are:

For SSL:
The default port number is 636 and the default administration port is 3539.

For non-SSL:
The default port number is 389 and the default administration port is 3538.

1.6 Translated titles might truncate

In the ldapxcfg utility, titles in the pop-up windows might truncate depending upon the language. If this problem occurs, depending on your display, you can resize the the window accordingly.

1.7 Default value of LOGFILSIZ needs to be increased

If you are adding a very large group (more than 50,000 members) to your 5.1 Directory, and you have migrated your database from a previous release such as Version 4.1, you need to modify the LOGFILSIZ parameter of your DB2® database to be at least 2000. On migrated databases, this value might currently be set to 750 or 1000.

You can verify this value by issuing the following commands. For this example the names of the user, instance, and database are ldapdb2.

For UNIX platforms:

```
su -ldapdb2
db2start
db2 get database config for ldapdb2 | grep LOGFILSIZ
```

If you need to increase this value issue the command:

```
db2 update database config for ldapdb2 using LOGFILSIZ 2000
```

For Windows platforms:

```
db2cmd
set DB2INSTANCE=ldapdb2
db2 get database config for ldapdb2 ><outputfile>
```

Find the value for LOGFILSIZ in the output file. If you need to increase this value issue the command:

```
db2 update database config for ldapdb2 using LOGFILSIZ 2000
```

Note: This value is already set correctly, if you created or configured your database with the IBM Directory Server Version 5.1 configuration tools.

1.8 Environment variables removed during migration

During migration, all commented out instances of ibm-slapdSetEnv in the **slapd32.conf** file are removed. Additionally all instances of the following environment variables in **slapd32.conf** are also removed:

- ibm-slapdSetEnv: ACLCACHE
- ibm-slapdSetEnv: ACLCACHESIZE
- ibm-slapdSetEnv: RDBM_FCACHE_SIZE
- ibm-slapdSetEnv: RDBM_CACHE_BYPASS_LIMIT

The functions of these four environment variables are performed in Version 5.1 by attributes under the DN:

```
cn:Front End, cn=Configuration
```

1.9 DSML file client throws exception

The DSML file client throws the following exception when it is set up to communicate using SSL and the user tries to connect to an LDAP server that does not use SSL.

```
SSL IS ON
javax.naming.CommunicationException: 9.182.21.228:389.  Root exception is javax.
net.ssl.SSLProtocolException: end of file
    at com.ibm.jsse.bd.a(Unknown Source)
    at com.ibm.jsse.b.a(Unknown Source)
    at com.ibm.jsse.b.write(Unknown Source)
    at com.sun.jndi.ldap.Connection.<init>(Connection.java:226)
    at com.sun.jndi.ldap.LdapClient.<init>(LdapClient.java:127)
    at com.sun.jndi.ldap.LdapCtx.connect(LdapCtx.java:2398)
    at com.sun.jndi.ldap.LdapCtx.<init>(LdapCtx.java:258)
    at com.sun.jndi.ldap.LdapCtxFactory.getInitialContext(LdapCtxFactory.java:91)
    at javax.naming.spi.NamingManager.getInitialContext(NamingManager.java:674)
    at javax.naming.InitialContext.getDefaultInitCtx(InitialContext.java:255)
    at javax.naming.InitialContext.init(InitialContext.java:231)
    at javax.naming.InitialContext.<init>(InitialContext.java:207)
    at javax.naming.directory.InitialDirContext.<init>(InitialDirContext.java:92)
    at com.ibm.ldap.dsml.DsmlRequest.processRequests(DsmlRequest.java:767)
    at com.ibm.ldap.dsml.DsmlServer.processDsmlRequest(DsmlServer.java:253)
    at com.ibm.ldap.dsml.DsmlServer.processDsmlRequest(DsmlServer.java:402)
    at com.ibm.ldap.dsml.DsmlServer.processDsmlRequest(DsmlServer.java:373)
    at com.ibm.ldap.dsml.DsmlServer.processDsmlRequest(DsmlServer.java:296)
    at com.ibm.ldap.dsmlClient.DsmlFileClient.main(DsmlFileClient.java:203)
```

The exception is not fatal and the output XML file is generated.

1.10 Nondefault log files need valid path

If you want to store your log files in a nondefault path, you must ensure that the path is valid. Otherwise you need to create the directory before you can configure the log files.

1.11 Replication limitations

This release supports subtree replication. Replication can be configured differently on individual subtrees (for individual replication contexts). This enables a single server to play different roles for different parts of the Directory Information Tree (DIT). For example, one subtree on a server could be a leaf replica (consumer), and another subtree could be a master (supplier) in the topology.

Directory updates, such as those to schema and password policy, do not belong to any replication context. They are replicated to all consumers based on all the replication contexts defined on the server. However, if the server contains one subtree for which it is a master, and another subtree for which it is a replica, the replication role to be assumed for schema or password policy updates cannot be determined. Because of this mixed replication mode in the topology, these types of global updates, schema and password policy, cannot be made. A referral result is returned causing a replication loop among the replicas and masters. Consequently, the client is referred between servers until the maximum referral limit is exceeded. If an administration control is used, an `unwilling  to perform` result is returned.

To avoid this situation, do not assign mixed roles to a single server. Ensure that the server performs the same server role for each of its subtrees. That is, if a server is a master for most of its subtrees, it is a master for all of its subtrees. Conversely, if the server acts as a replica for most of its subtree, it acts as a replica for all of its subtrees.

Another solution, depending on your situation, is to make both of the subtrees peer-masters on each of the servers. The master that received the entry, updates the other peer servers. As peers, the servers receive the entry update but do not replicate it.

1.12 Default ports for the embedded version of IBM WebSphere® Application Server - Express

The **embedded version of IBM WebSphere Application Server - Express** uses four default port settings:

- Http Transport (port 1): 9080
- Http Transport (port 2): 9443
- Bootstrap/rmi port: 2809
- Soap connector port: 8880

If a conflict exists with another application using one or more of these default ports, you can use a text editor to change the default ports to an unused port.

Http Transport port 1
Find the line containing the port number 9080 in the following files and replace the 9080 with the port number that you want:

```
$BOBCAT_HOME\config\cells\DefaultNode\nodes\DefaultNode\servers\server1\server.xml
$BOBCAT_HOME\config\cells\DefaultNode\virtualhosts.xml
```

Http Transport port 2
Find the line containing the port number 9443 in the following files and replace the 9443 with the port number that you want:

```
$BOBCAT_HOME\config\cells\DefaultNode\nodes\DefaultNode\servers\server1\server.xml
$BOBCAT_HOME\config\cells\DefaultNode\virtualhosts.xml
```

Bootstrap/rmi port
Find the line containing the port number 2809 in the following file and replace the 2809 with the port number that you want:

```
$BOBCAT_HOME\config\cells\DefaultNode\nodes\DefaultNode\serverindex.html
```

Soap connector port
Find the line contain ing the port number 8880 in the following file and replace the 8880 with the port number that you want:

```
$BOBCAT_HOME\config\cells\DefaultNode\nodes\DefaultNode\serverindex.html
```

1.13 Clarification for ldapsearch -i <*file*> option

The -i < *file*> option replaces the -f< *file*> option in this release. The -f option is still supported, although it is deprecated.

In the command, **ldapsearch -V3 -v -b ″o=ibm,c=us″ -D ″cn=admin″ -w ldap -i filter.input %s dn**, the **filter.input** file might contain the following filter information:

```
(cn=*Z)
(cn=*Z*)
(cn=Z*)
(cn=*Z*)
(cn~=A)
(cn>=A)
(cn<=B)
```

Note: Each filter must be specified on a separate line.

The command performs a search of the subtree **o=ibm,c=us** for each of the filters beginning with **cn=*Z**. When that search is completed, the search begins for the next filter **cn=*Z*** and so forth until the search for the last filter **cn<=B** is completed.

1.14 On UNIX systems you must configure the database in a location other than /home when /home is an NFS mount

If you use NFS automount, you must configure everything manually to create the database in a location other than /home. Performing manual configuration in this situation also avoids the problem of the **ldapcfg** command trying to write to /home.

Notes:

1. The following steps assume that you want to set up a database like the default ldapdb2 database, that is the instance owner is ldapdb2, DB2 instance is ldapdb2, and database name is ldapdb2.
2. It is strongly recommended to save a copy of any system file before editing it.

1. Create a group named dbsysadm for the database administrators:

   ```
   groupadd [-g <gid>] dbsysadm
   ```

   Note: The **groupadd** command on some Linux distributions requires that the group ID number (gid) be specified using the **-g** <*gid*> syntax. Type

   ```
   cat /etc/group
   ```

   to find an available group ID number. Red Hat automatically assigns the next available gid if the **-g** option is not specified.
2. Add users root and ldap to the dbsysadm group:

   ```
   usermod -G dbsysadm root
   usermod -G dbsysadm ldap
   ```
3. Create a user account (ldapdb2) for the DB2 instance:

   ```
   useradd -g dbsysadm -m ldapdb2
   ```
4. Set the password for the user account (ldapdb2):

   ```
   passwd ldapdb2
   ```

   Enter the new password when prompted. Record your password for future reference.
5. Create the database instance:

   ```
   <LDAPHOME>/db2/instance/db2icrt -u ldapdb2 ldapdb2
   ```

   where <*LDAPHOME*> is:
   - AIX, Linux operating systems- /usr/ldap
   - Solaris operating systems - /opt/IBMldaps
   - HP-UX operating systems- /usr/IBMldap
6. Before performing this step save a copy of /etc/services.

   Update /etc/services to include a line for local loopback:

   ```
   echo "ldapdb2svc      3700/tcp" >> /etc/services
   echo "ldapdb2svci     3701/tcp" >> /etc/services
   ```
7. Log in as the database user id:

   ```
   su - ldapdb2
   ```
8. Start the database manager:

   ```
   db2start
   ```
9. Create the database under the instance:

   ```
   db2 create db ldapdb2 on <location> using codeset UTF-8 territory US
   ```

Note: If you omit the `using codeset UTF-8 territory US` the database is created in the local code page. However, using the local code page does affect performance. The database requires at least 80Mb of free space available on the filesystem. Use **df -k** to verify this before creating the database.

10. Enable multi-page file allocation:

    ```
    db2empfa ldapdb2
    ```

    Note: This is a performance enhancement, and cannot be undone after being run.

11. Update some of the DB2 tuning variables:

    ```
    db2 update db cfg for <databasename> using <parm> <newvalue>
    DB2 Parameter Minimum value allowed
    APPLHEAPSZ 2048
    PCKCACHESZ 360
    SORTHEAP   256
    ```

    For example:

    ```
    db2 update db cfg for ldapdb2 using APPLHEAPSZ 1280
    ```

    Note: At this point, the database is created. However, for IBM Directory Server Version 4.1, the use of a local loopback database connection is required. To enable local loopback perform the following steps:

    a. Update the database for local loopback connections:

       ```
       db2 update dbm cfg using SVCENAME ldapdb2svc
       db2 catalog tcpip node ldapdb2n remote localhost server ldapdb2svc
       db2 catalog db ldapdb2 as ldapdb2b at node ldapdb2n authentication client
       db2set DB2COMM=TCPIP
       ```

    b. Restart the database manager:

       ```
       db2stop
       db2start
       ```

12. The database is fully configured, you can update the configuration file to use this database. In *<LDAPHOME>*etc/slapd32.conf, in the following stanza:

    ```
    dn: cn=Directory,cn=RDBM Backends,cn=IBM SecureWay,cn=Schemas,cn=Configuration
    objectclass: top
    objectclass: ibm-slapdRdbmBackend
    cn: Directory
    ibm-slapdPlugin:  database /bin/libback-rdbm.dll rdbm_backend_init
    ibm-slapdDbConnections:  15
    ibm-slapdSuffix:  cn=localhost
    ibm-slapdReadOnly:  FALSE
    ```

    Add the following lines:

    ```
    ibm-slapdDbInstance: ldapdb2
    ibm-slapdDbAlias: ldapdb2b
    ibm-slapdDbUserId: ldapdb2
    ibm-slapdDbUserPw: <user pw>
    ibm-slapdDbLocation: <user defined location>
    ```

    The resulting stanza is:

    ```
    dn: cn=Directory,cn=RDBM Backends,cn=IBM SecureWay,cn=Schemas,cn=Configuration
    objectclass: top
    objectclass: ibm-slapdRdbmBackend
    cn: Directory
    ibm-slapdPlugin:  database /bin/libback-rdbm.dll rdbm_backend_init
    ibm-slapdDbInstance: ldapdb2
    ibm-slapdDbAlias: ldapdb2b
    ibm-slapdDbUserId: ldapdb2
    ```

```
ibm-slapdDbUserPw: <user pw>
ibm-slapdDbLocation: <user defined location>
ibm-slapdDbConnections:  15
ibm-slapdSuffix:  cn=localhost
ibm-slapdReadOnly:  FALSE
```

13. If you used a UTF-8 datastore as described in step 9 on page 6, in the stanza: dn: cn=Front End, cn=Configuration, you must uncomment the line:

    ```
    #ibm-slapdSetEnv: DB2CP=1208
    ```

The database is ready for the Directory server to use. The first startup takes longer because the server must create its own tablespaces and bufferpools. For further reading and documentation, see the *IBM(R) Directory Server Version 4.1 Tuning Guide*.

1.16 HTTPS for the Embedded Version of WebSphere Application Server Express Version V5.0

The Embedded Version of WAS Express, V5.0 comes with HTTPS setup by default on port 9443. To use HTTPS, you need to change your login URL to the following:

```
https://<hostname>:9443/IDSWebApp/IDSjsp/Login.jsp
```

For non-HTTPS connections, conitnue to use the URL:

```
http://<hostname>:9080/IDSWebApp/IDSjsp/Login.jsp
```

Additionally, if you want to change the application server's SSL certificate, you create new key and trust store database files for the WebSphere Application Server Express to use. By default, the key and trust store database files are separate and are located in the *<WASHOME>*/etc directory. These files are named **DummyServerKeyFile.jks** and **DummyServerTrustFile.jks** respectively.

After you have created your new jks files, you can change the key and trust store database files that WAS uses by modifying the following items (highlighted in **bold**) in the *<WASHOME>*/config/cells/DefaultNode/security.xml file to use your new file names, passwords, and file formats:

```
<repertoire xmi:id="SSLConfig_1" alias="DefaultSSLSettings">
  <setting xmi:id="DefaultSSLSettings"
     keyFileName="${USER_INSTALL_ROOT}/etc/DummyServerKeyFile.jks"
     keyFilePassword="WebAS" keyFileFormat="JKS"
     trustFileName="${USER_INSTALL_ROOT}/etc/DummyServerTrustFile.jks"
     trustFilePassword="WebAS" trustFileFormat="JKS"
     clientAuthentication="false" securityLevel="HIGH"
     enableCryptoHardwareSupport="false">
      <cryptoHardware xmi:id="CryptoHardwareToken_1" tokenType=""
         libraryFile="" password=""/>
      <properties xmi:id="Property_4" name="com.ibm.ssl.protocol" value="SSLv3"/>
      <properties xmi:id="Property_5" name="com.ibm.ssl.contextProvider"
         value="IBMJSSE"/>
  </setting>
</repertoire>
```

1.17 Corrections to the Kerberos information in the Administration Guide

To manage Kerberos settings using the Web Administration Tool, in the navigation area you need to select **Server administration**, expand **Manage security properties** and select the **Kerberos** tab. Follow the directions in the Administration Guide. However, when you enter the Alternate administrator ID (Step 5), you must ensure that this ID is a valid ID in your Kerberos realm.

In the Replication chapter, under ″Creating credentials″ in the section ″If you selected Kerberos authentication:″ there is an error in the example. The corrected text is: ″For example, if the supplier is named master.our.org.com and the realm is SOME.REALM, the DN is **ibm-Kn=ldap/master.our.org.com@SOME.REALM**.″

In this same chapter under the topic ″Adding the supplier information to the replica″ note that in Step 1, you need to expand **Server management** in the navigation area before you can click **Manage replication properties**. Also note that in Step 5, the Kerberos bind DN example is missing a hyphen. The correct DN is ibm-kn=ldap/<*yourservername@yourrealm*>.

1.18 /var requirements on UNIX platforms

Before you install on UNIX platforms, be sure that you have adequate space in the /var directory. A minimum of 100 MB of free space in /var is recommended.

1.19 Before you configure: creating the DB2 database owner

Note: The information for UNIX platforms has been changed slightly from the information in the *Installation and Configuration Guide*.

Before you configure the database, you must create a user ID for the user who will own the DB2 database. The user ID you specify will own the database instance where the DB2 database will exist, and the DB2 instance will be in the user’s home directory. The user ID can be no longer than 8 characters. In addition:

- On Windows platforms, the user must be a member of the Administrators group.
- On UNIX platforms:
  - The user must have a home directory and must be the owner of the home directory.
  - The group ownership of the user’s home directory should be the DB2 group created when DB2 was installed. On AIX and Solaris, this group is usually named **dbsysadm**. On Linux for S/390, this group is usually named **db2iadm**. For example, in the case of a user named **ldapdb2**, the user ID home directory should be owned by ldapdb2:dbsysadm on AIX and Solaris or by ldapdb2:db2iadm on Linux for S/390.

    There might be some groups that do not work correctly as the user’s primary group when configuring the database. For example, if the user’s primary group on Linux is **users**, problems might occur. Use **other** on Linux if you want to be sure that the primary group will work.
  - The user **root** must be a member of the user’s primary group. If **root** is not a member of this group, add **root** as a member of the group.
  - For best results, the user’s login shell should be the Korn shell script (/usr/bin/ksh).

- The user’s password must be set correctly and ready to use. For example, the password cannot be expired or waiting for a first-time validation of any kind. (The best way to verify that the password is correctly set is to telnet to the same computer and successfully log in with that user ID and password.)
- When configuring the database, it is not necessary, but only customary, to specify the home directory of the user ID as the database location. However, if you specify some other location, the user’s home directory still must have 3 to 4 MB of space available. This is because DB2 creates links and adds files into the home directory of the instance owner (that is, the User) even though the database itself is elsewhere.

2.0 Must read known problems - platform specific

This information applies to the following operating systems:

2.1 For AIX only

The following information applies only to the AIX operating system.

2.1.1 Supported levels of the AIX operating system

The IBM Directory Server Version 5.1 is supported on the following levels of the AIX operating system:

- On the AIX operating system Release 4.3.3 and on higher maintenance levels of AIX Release 4.3
- On the AIX operating system Release 5.1L and on higher maintenance levels of AIX Release 5.1
- On the AIX operating system Release 5.2A and on higher maintenance levels of AIX Release 5.2

Note: If you are using SSL with Release 5.2A, you need to install the fix for APAR IYIY33524.

2.1.2 Preventing logouts on AIX 5.x systems when InstallShield GUI is invoked

Before installing or uninstalling the IBM Directory Server Version 5.1 using the InstallShield GUI on AIX 5.x systems, be sure you issue the following command:

```
xset fp default
```

This command prevents logouts from occurring when InstallShield GUI is invoked.

2.1.3 Locales for InstallShield GUI panels

For the READMEs to display correctly in the InstallShield GUI panels the following languages need to use the correct locales:

Table 1.

Language	**Locale**
Japanese	Ja_JP
Traditional Chinese	Zh_TW

2.1.4 Missing titles from ldapxcfg panels in simplified and traditional Chinese

On the AIX 5.1 operating system, the ldapxcfg panels for simplified and traditional Chinese are missing titles. This situation is corrected by AIX 5.1 maintenance level 3 (5100–03).

2.1.5 Error code -1 at startup

If DB2 is not already started, you might see the following message when starting the server:

```
Error code -1 from odbc string:" SQLConnect " ldapdb2b.
```

This occurs because the IBM Directory Server is trying to connect to DB2, before DB2 is started. If you see the message:

```
SQL1063N  DB2START processing was successful.
```

you can ignore the previous error message because the Directory Server has started DB2 and subsequently connected to it.

2.1.6 Migrating DB2 fixpack3 to DB2 fixpack7

When migrating from DB2 FP 3 to DB2 FP 7 on the AIX operating system, be sure to complete all of the ″After Installation″ steps in the FixpakReadme.txt file that is packaged with DB2 FP7. These steps include:

- Update Instances
- Enabling scalar functions (if applicable)
- Rebinding bind files

Also, perform the ″Special Notes″ section steps, if they are applicable to your installation.

2.1.7 Applying DB2 8.1 fixpaks on AIX 5.x systems

If you are using a AIX 5.x operating system and you have obtained DB2 Version 8.1 from the IBM Directory Server Version 5.1 package, you must use the **installp** utility to apply future DB2 fixpaks. The GUI installer that is provided with the fixpak does not work in this case.

2.1.8 Enabling Asynchronous IO

On AIX, if you are using DB2 8.1, you must enable Asynchronous IO before you begin configuration. To enable Asynchronous IO, type the following at a command prompt:

```
smitty aio
```

2.1.9 Configuration program fails on AIX with 0509-136 errors

Because of an AIX library change, **ldapcfg** and **ldapxcfg** sometimes fail with 0509-136 errors while configuring the DB2 database on AIX 5.1 or 5.2.

To avoid this error, do the following at the AIX level:

1. Run `smitty chgaio`.
2. Set **STATE to be configured at system restart** to **available**.
3. Press Enter.
4. Restart the system.

The following is a sample of the output of **ldapcfg** when the failure occurs:

```
Starting database manager for instance: 'ldapdb2'.
exec(): 0509-036 Cannot load program db2start because of the
following errors:
 0509-130 Symbol resolution failed for
/usr/lib/threads/libc.a(aio.o) because:
 0509-136   Symbol kaio_rdwr (number 0) is not exported from
     dependent module /unix.
 0509-136   Symbol listio (number 1) is not exported from
     dependent module /unix.
 0509-136   Symbol acancel (number 2) is not exported from
     dependent module /unix.
 0509-136   Symbol iosuspend (number 3) is not exported from
     dependent module /unix.
 0509-136   Symbol aio_nwait (number 4) is not exported from
     dependent module /unix.
 0509-130 Symbol resolution failed for
/usr/opt/db2_08_01/lib/libdb2e.a(shr.o) because:
 0509-136   Symbol aio_nwait (number 416) is not exported from
     dependent module /usr/lib/threads/libc.a(aio.o).
 0509-192 Examine .loader section symbols with the
   'dump -Tv' command.
 Failed to start database manager for instance: 'ldapdb2'.
 Creating database: 'ldapdb2'.
exec(): 0509-036 Cannot load program db2start because of the
following errors:
 0509-130 Symbol resolution failed for
/usr/lib/threads/libc.a(aio.o) because:
 0509-136   Symbol kaio_rdwr (number 0) is not exported from
     dependent module /unix.
 0509-136   Symbol listio (number 1) is not exported from
     dependent module /unix.
 0509-136   Symbol acancel (number 2) is not exported from
     dependent module /unix.
 0509-136   Symbol iosuspend (number 3) is not exported from
     dependent module /unix.
 0509-136   Symbol aio_nwait (number 4) is not exported from
     dependent module /unix.
 0509-130 Symbol resolution failed for
/usr/opt/db2_08_01/lib/libdb2e.a(shr.o) because:
 0509-136   Symbol aio_nwait (number 416) is not exported from
     dependent module /usr/lib/threads/libc.a(aio.o).
 0509-192 Examine .loader section symbols with the
   'dump -Tv' command.
 Failed to create database: 'ldapdb2'.
 Removing database: 'ldapdb2'
```

2.1.10 Error on AIX 5.1 when running db2start

The following error might occur when you try to run **db2start**:.

```
0509-130 Symbol resolution failed for /usr/lib/threads/libc.a(aio.o)
because:
         0509-136   Symbol kaio_rdwr (number 0) is not exported from
                    dependent module /unix.
         0509-136   Symbol listio (number 1) is not exported from
                    dependent module /unix.
         0509-136   Symbol acancel (number 2) is not exported from
                    dependent module /unix.
         0509-136   Symbol iosuspend (number 3) is not exported from
                    dependent module /unix.
         0509-136   Symbol aio_nwait (number 4) is not exported from
                    dependent module /unix.
         0509-192 Examine .loader section symbols with the
                  'dump -Tv' command.
```

If this occurs on AIX 5.1, you have Asynchronous I/O turned off.

To turn on Asynchronous I/O:

1. Run **smitty chgaio** and set **STATE to be configured at system restart** from **defined** to **available**.
2. Press Enter.
3. Do **one** of the following:
   - Restart your system.
   - Run **smitty aio** and move the cursor to **Configure defined Asynchronous I/O**. Then press Enter.

The **db2start** command now works.

2.2 For Windows NT®, Windows 2000 and Windows XP client, only:

The following information applies only to theWindows NT and Windows 2000 platforms.

2.2.1 Setting LANG and LC_ALL system environment variables for nonEnglish InstallShield GUI installation

For the InstallShield GUI installation to bring up the same language that the operating system is using, two variables need to be set in the system environment

- LANG = <*locale*>
- LC_ALL = <*locale*>

where <*locale*> is the locale that the operating system is using.

Go to http://www.microsoft.com/globaldev/ for a list of Microsoft® locale values.

2.2.2 Uninstalling Version 5.1 shows Version 4.1 option

If you have migrated from IBM Directory Server Version 4.1 to Version 5.1, and you are performing an InstallShield GUI uninstall, the **DMT 4.1 and Java™ 1.3** feature is listed as an uninstallable selection. Although this is no longer supported in Version 5.1 this feature continues to be listed until you select and remove it using the InstallShield GUI uninstall process.

2.2.3 Installing and uninstalling DB2 with InstallShield GUI

If you installed DB2 version 7.2 for Windows with the InstallShield GUI V4.1, you must use the InstallShield GUI to uninstall DB2. Click **Start -> Settings -> Control Panel -> Add/Remove Programs -> IBM Directory Server** and select the DB2 feature.

If instead you use the DB2 uninstall for version 7.2 without using InstallShield GUI (**Start -> Settings -> Control Panel -> Add/Remove Programs -> DB2**), and later install DB2 V 8.1 with InstallShield GUI for version 5.1, the new uninstall features panel for the 5.1 InstallShield GUI shows DB2 V7.2, not DB2 V8.1. This occurs even though DB2 V8.1 is the actual version installed.

Note: If you select DB2 V7.2 during an InstallShield GUI uninstall in this situation, the InstallShield GUI does uninstall DB2 V8.1.

2.2.4 Tomcat Web application does not start with IBM JDK 1.3.1

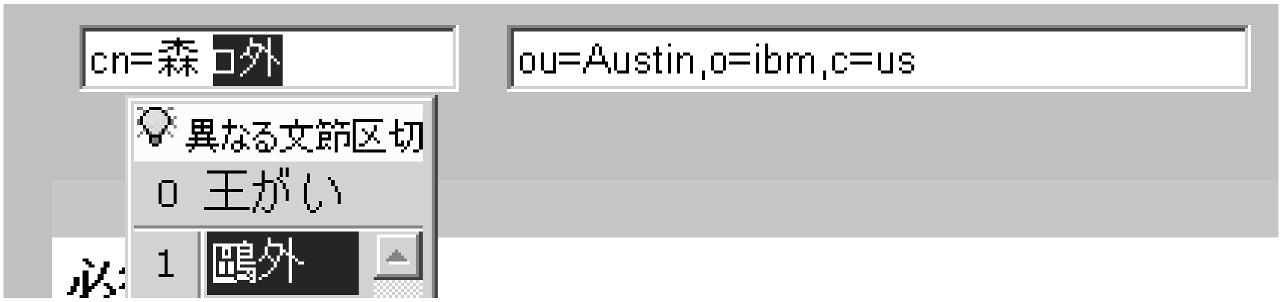
If you are using the IBM JDK 1.3.1, you might not be able to start the Tomcat Web application. This is a known limitation.

If you must use Tomcat, you have two alternatives:

- Obtain a copy of Sun 1.3.1 Service release 4 (1.3.1_4).
- Use the IBM JDK 1.3.0 Service release 13a.

2.2.5 Certain UTF-8 supplementary characters do not display correctly

IBM Directory Server supports UTF-8 (Unicode Transformation Format, 8-bit form) to use Unicode characters, which contains MS932 (Shift JIS) characters plus supplementary characters not defined in MS932. Supplementary characters might be displayed as square box in Internet Explorer running on Windows NT and Windows 2000. See Figure 1.



cn=森 □外

ou=Austin,o=ibm,c=us

Figure 1. Unicode Code Point U+9DD7 displayed as a square

If this occurs, install one of the East Asian language kits. Depending on your environment, install the Japanese, Korean, Simplified Chinese or Traditional Chinese language kit which is included in your Windows NT and Windows 2000 CDs. For example, Unicode code point U+9DD7 is one of the supplementary characters in the Japanese environment. With the correct language kit installed, the supplementary character is displayed correctly. See Figure 2.

○ cn=森 鷗外 person 02/11/18 02/11/18 CN=ROOT

Figure 2. U+9DD7 displayed correctly

Note: This problem is not observed in Windows XP.

2.3 For Solaris Operating Environment Software only:

The following information applies only to the Solaris Operating Environment Software.

2.3.1 Locales for InstallShield GUI panels

For the READMEs to display correctly in Japanese in the InstallShield GUI panels the locale needs to be set to **ja**.

2.3.2 Command line installation using pkgadd

To install the IBM Directory Server Version 5.1 from a command prompt:

1. Go to the ids subdirectory of the directory where you mounted the CD-ROM or where you untarred the tar file.
2. At the command prompt, install the packages you want by typing the following command for each package:

   ```
   pkgadd -d pkgfilename
   ```

where *pkgfilename* is the file name of the package you want to install. Do not use the system default of **ALL**. The system does not sequence the packages correctly and the installation fails.

The packages shown in the following table are available. If you are installing the server, you must install the client package first, and then the server package. You can then install the documentation, the messages, and the Web Administration Tool in any order.

Table 2. IBM Directory Server packages for Solaris

Package	**Package name**	**File name**
IBM Directory Client	IBMldapc	ldap.client_rted.pkg
IBM Directory Server	IBMldaps	ldap.server_rted.pkg
IBM Directory documentation	IBMldi*xxx*	ldap.man.*xx_XX*.pkg
IBM Directory messages	IBMldm*xxx*	ldap.msg.*xx_XX*.pkg
IBM Directory Webadmin	IBMldapw	ldap.webadmin_rted.pkg

xxx and *xx_XX* are specific language identifiers.

Note: The English messages are automatically installed with the IBMldaps (server) package. There is no separate package for English messages.

Examples:

- To install the client package, type:
  ```
  pkgadd -d ldap.client_rted.pkg
  ```
- To install the server package, type:
  ```
  pkgadd -d ldap.server_rted.pkg
  ```
- To install the documentation package, type:
  ```
  pkgadd -d ldap.man.xx_XX.pkg
  ```
- To install the message package, type:
  ```
  pkgadd -d ldap.msg.xx_XX.pkg
  ```
- To install the Web Administration Tool package, type:
  ```
  pkgadd -d ldap.webadmin_rted.pkg
  ```

3. During installation, you are asked if you want to use `/opt` as the base directory. If space permits, use `/opt` as the base installation directory. To accept `/opt` as the base directory, press Enter.

   Notes:

   a. With the installation of client and server packages, the system prompts you with the query, `This package contains scripts which will be executed with super-user permission during the process of installing the package. Continue with installation?` These scripts create the IBM Directory Server Version 5.1 user ID. Type `y` to continue.

   b. If you are installing the server package, you also see the prompt, `Do you want to install these as setuid and/or setgid files?` The programs need to be able to start daemons, run DB2 commands, and create the IBM Directory Server Version 5.1 DB2 instance user ID and group, so they occasionally need to run as root. Type `y` to continue.

4. When the installation is completed, type `q` to return to the command prompt.

2.4 For Linux only:

The following information applies only to the Linux operating systems.

2.4.1 CD-ROM does not eject from Linux machines

When installing the server from a CD-ROM using the native RPM installation method on a Linux machine, the CD-ROM fails to eject. To eject the CD-ROM, you must either reboot your system or stop the ibmdiradm process.

To stop the ibmdiradm process issue the following command to obtain the PID number of the ibmdiradm process:

```
ps -ef |grep ibmdiradm
```

This command returns output similar to this example:

```
ldap      7048     1  0 10:26 pts/1    00:00:00 /usr/bin/ibmdiradm
ldap      7049  7048  0 10:26 pts/1    00:00:00 /usr/bin/ibmdiradm
ldap      7050  7049  0 10:26 pts/1    00:00:00 /usr/bin/ibmdiradm
ldap      7051  7049  0 10:26 pts/1    00:00:00 /usr/bin/ibmdiradm
ldap      7052  7049  0 10:26 pts/1    00:00:00 /usr/bin/ibmdiradm
ldap      7053  7049  0 10:26 pts/1    00:00:00 /usr/bin/ibmdiradm
ldap      7054  7049  0 10:26 pts/1    00:00:00 /usr/bin/ibmdiradm
ldap      7055  7049  0 10:26 pts/1    00:00:00 /usr/bin/ibmdiradm
ldap      7056  7049  0 10:26 pts/1    00:00:00 /usr/bin/ibmdiradm
ldap      7057  7049  0 10:26 pts/1    00:00:00 /usr/bin/ibmdiradm
ldap      7058  7049  0 10:26 pts/1    00:00:00 /usr/bin/ibmdiradm
ldap      7059  7049  0 10:26 pts/1    00:00:00 /usr/bin/ibmdiradm
ldap      7060  7049  0 10:26 pts/1    00:00:00 /usr/bin/ibmdiradm
```

In this example the PID for ibmdiradm is 7048. To stop the ibmdiradm process, issue the following command:

```
kill -9 <PID>
```

In this example, 7084 is the PID, so the command is:

```
kill -9 7084
```

After ejecting the CD-ROM, restart the ibmdiradm process by issuing the command:

```
ibmdiradm
```

Note: This problem does not occur if you use the InstallShield GUI installation method.

2.4.2 Java failure when configuring an existing instance and database

If you are using Intel Linux SuSe 7.3, SuSe 8.0, or Red Hat Advanced Server 2.1, with DB2 v8.1 and you are configuring an existing instance and database, a Java failure might occur after the configuration is completed. This failure, however, can be ignored. The instance and database are successfully configured. For example, if you issued the the command:

```
ldapcfg -a <myuserID> -w <mypassword> -d <mydatabase> -l /home/<myuserID>
```

the following message might be displayed after the completion of the configuration process:

```
IBM Directory Server Configuration complete.
Unexpected exception has occurred:
ReportedExceptionCode = b, at ExceptionAddress = 74736574
```

```
        ACCESS_VIOLATION occured outside Interpreter and JITed code
        ExecMode = EXECMODE_BYTECODE
        stackpointer=0xbffc7370
Writing Java core file ....
Written Java core to /var/ldap/javacore9151.1035571351.txt
Abort
```

2.4.3 Incorrect display when installing with the InstallShield GUI on a system set to a Japanese locale

On Linux Redhat 7.3, if you are using the InstallShield GUI to install on a system with the locale set for Japanese, the list of languages displays as question marks. Use the linux utility (RPM) instead of the InstallShield GUI for installation to avoid this behavior. See the *IBM Directory Server Version 5.1 Installation and Configuration Guide*, Chapter 7, for the installation information.

2.4.4 InstallShield GUI uninstall does not remove the appsrv directory

On Linux systems, when uninstalling the **embedded version of IBM WebSphere Application Server - Express** using the InstallShield GUI, the /usr/ldap/appsrv directory is not removed. You are not able to reinstall the **embedded version of IBM WebSphere Application Server - Express** using the InstallShield GUI until the appsrv directory is removed.

To remove this directory manually, issue the command:

```
rm -rf /usr/ldap/appsrv
```

2.4.5 Linux S/390 client operations fail with SSL using GSKit 6.0

To perform client functions on SuSE 7.0 and Red Hat 7.2 on Linux for S/390 with kernel level 2.4.x, you must download and install the compat-libstdc++-2.10.0-1.s390.rpm package. This package contains compatibility Standard C++ libraries that allow older binaries (created with old versions of compilers) to execute.

You also need to set the following environment variable:

```
export LD_PRELOAD=/usr/lib/libstdc++-libc6.2-2.so.3
```

Notes:

1. You must specify the absolute path of the library.
2. When this variable is set, you are not able to start or stop the server from this window. You must use a separate window that does not have the LD_PRELOAD variable set if you want to start or stop the server.

2.4.6 DB2 opt file requirements

The InstallShield GUI does not verify the amount of space in the /opt directory. Before installing DB2 V8.1 on Linux using the InstallShield GUI, ensure that you have at least 329MB of free space in the /opt directory.

2.4.7 GSKit 6.0.3 is not supported on Intel Linux

GSKit 6.0.3 is not being supported on Intel Linux for this release. GSKit 5.0.4.58 is included in the packages for the Intel Linux distributions. Consequently, the rpm file name (gsk5bas-5.0-4.58.i386.rpm) is different than the one documented in the *IBM Directory Server Version 5.1 Installation and Configuration Guide*. Ensure that you use the correct file names when installing GSKit.

2.5 For HP-UX only

This information applies to the HP-UX operating system only.

2.5.1 HP-UX 11 client is supported

In addition to supporting the directory server and client on the HP-UX 11i operating system, the IBM Directory Server Version 5.1 client is also supported on the HP-UX 11 operating system.

3.0 General information, hints and tips

This information applies to the AIX, Windows NT, Windows 2000, the Solaris Operating Environment Software, and Linux platforms.

3.1 Peer-to-peer scenario with Web Administration Tool

This procedure was used to set up an environment with two peer-masters and two replicas (server1, server2, server3, and server4). All steps were performed from the master machine.

1. Follow the directions in the *IBM Directory Server Version 5.1: Administration Guide* to set up a master (server1).
2. Create a set of credentials to use for your replication topology. You can locate these either in the replicated subtree or in **cn=replication,cn=localhost**. For this scenario use a simple bind.

   Note: Because this topology is being set up from the master machine the **cn=replication,cn=localhost** location is not available when you set up the replicas under the peer server. It is most important that you use the same DN and password when you add the credentials to the subtree.
3. From your master machine use the Web Administration Tool to connect to each of the other three servers and start each of the servers.
4. Follow the directions in the *IBM Directory Server Version 5.1: Administration Guide* to set up three replicas under the master. **Do not** populate the replicas or add any supplier information at this time.
5. Select the replica (server2) that you want to promote to a peer-master and click **Move**.
6. Select **Replication topology** to promote the replica to a master. Click **Move**. The peer topology is now:
   - server1 (master-peer)
     - server2 (replica)
     - server3 (replica)
     - server4 (replica)
   - server2 (master-peer)
7. Add server1, server3, and server4 as replicas under server2 so that the topology looks like:
   - server1 (master-peer)
     - server2 (replica)
     - server3 (replica)
     - server4 (replica)
   - server2 (master-peer)
     - server1 (replica)
     - server3 (replica)
     - server4 (replica)
8. Copy the subtree information from the original master (server1) by issuing the command:

   ```
   db2ldif -o <master.ldif> -s <subtreename>
   ```

9. Copy <*master.ldif*> to server2, server3, and server4.
10. Stop server2, server3, and server4.
11. On each of the three servers (server2, server3, and server4) issue the following command:

    ```
    ldif2db -r no -i <master.ldif>
    ```

    This command has populated each server with the subtree data that was on the master and a complete copy of the topology.
12. Add the supplier information for each of the replicas. This includes server1 in its role as a replica to server2.

    Connect the Web Administration Tool to each of the replicas and at each of the replicas perform the following:

    a. Click **Manage replication properties** in the navigation area.
    b. Under the **Supplier information** field, select **Default credentials and referral**.
    c. Click **Edit**.
    d. For server3 and server4 enter a referral LDAP URL to one of the peer-master servers. For example,

       ```
       ldap://server1.<mylocation>.<mycompany>.com
       ```
    e. Enter the replication bindDN for the credentials you created in step 2.
    f. Enter and confirm the credential password.
    g. Click **OK**.
    h. You must restart the replicas for the changes to take effect.
13. Replicas are created with replication in the suspended state, you must resume replication on each of the replicas. This must be performed at each of the peer-master servers (server1 and server2):

    a. Click **Manage queues**.
    b. Select the replica and click **Suspend/resume**.
    c. Repeat this process for each of the other two replicas in the queue.

    After this has been completed for each of the six replicas (three under each peer-master), the topology is ready to begin replication.

This procedure can be followed for any peer topology setup. Remember not to populate or add supplier information to any of the replicas until after you have completed designing your topology on the original master.

3.2 Migrating a replicating environment from 3.2.x to 5.1

When migrating from 3.2.x to 5.1, you need to unconfigure the database. Before unconfiguring the database, you might want to ensure that all replication changes have been completed.

Stop the master server and issue the following command to ensure that all changes have been replicated. This example assumes that the name of the user, instance and database are ldapdb2.

For UNIX platforms:

```
su -ldapdb2 -c "db2 connect to ldapdb2;
    select count (id) from ldapdb2.change"
```

Note: If not issuing this command as the root, you need to provide the database instance owner password.

For Windows platforms:

```
db2cmd
```

In the new DB2 command window issue the following commands:

```
set DB2INSTANCE=ldapdb2
db2 connect to ldapdb2
select count (id) from ldapdb2.change
```

If the count is **0**, then all changes have been replicated and the replica and master are synchronized. You can proceed with regular migration (exporting the database to an LDIF file, migrating and so on). Otherwise you might want to restart the master in read only mode and wait for all of the updates to be replicated. . This is important if you have a topology that is heterogeneous, for example, 3.2.x replicas and 4.1 replicas with a 5.1 master.

If you are moving your whole enterprise to 5.1 from 3.2.x, you can:

1. Create an LDIF file using **db2ldif** on the master.
2. Unconfigure the database on all the servers.
3. Install the IBM Directory Server Version 5.1 on each server.
4. Perform the migration procedure.
5. Use the **ldif2db** or **bulkload** command to load the master's data on to the replicas. This ensures that the replicas are synchronized with the master.
6. Start the master and the replicas.
7. Use the Web Administration Tool **Replication management ->Manage queues** to resume replication or issue the following command:

```
ldapexop -h <hostname> -D <binddn> -w <password>
        -op controlrepl -action resume -rc <contextDN>
```

3.3 Support for industry standards

The following standards were implemented in this release:

- RFC 1274 The COSINE and Internet X.500 Schema
- RFC 1777 Lightweight Directory Access Protocol (V2)
- RFC 1778 String Representation of Standard Attribute Syntaxes
- RFC 1779 String Representation of Distinguished Names
- RFC 1823 LDAP Application Program Interface (V2)
- RFC 2052 A DNS RR for Specifying the Location of Services (DNS SRV)
- RFC 2219 Use of DNS Aliases for Network Services
- RFC 2222 Simple Authentication and Security Layer (SASL)
- RFC 2247 Using Domains in LDAP/X.500 Distinguished Names
- RFC 2251 Lightweight Directory Access Protocol (V3)
- RFC 2252 Lightweight Directory Access Protocol (V3): Attribute Syntax Definitions
- RFC 2253 Lightweight Directory Access Protocol (V3): UTF-8 String Representation of Distinguished Names
- RFC 2254 The String Representation of LDAP Search Filters
- RFC 2255 The LDAP URL Format
- RFC 2256 A Summary of the X.500(96) User Schema for use with LDAPv3
- RFC 2696 LDAP Control Extension for Simple Paged Results Manipulation
- RFC 2849 The LDAP Data Interchange Format (LDIF) - Technical Specification

- RFC 2891 LDAP Control Extension for Server Side Sorting of Search Results
- The Open Group schema for liPerson and liOrganization (NAC/LIPS)
- RFC 2307 An Approach for Using LDAP as a Network Information Service. (IBM Directory Server 5.1 ships with the schema defined in this RFC and supports clients that need to use an LDAP server to authenticate.)

3.4 Password Guidelines

The following section provides details of the supported values of the IBM Directory Server (IDS) password attribute for user entries in the IBM Directory Server, as well as the accounts used to administer the LDAP environment. It also provides guidelines of what characters to avoid to reduce confusion attempting to run using the Directory Server command line tools and C-API interfaces.

The Directory Server has two types of user accounts:

- Administration accounts (LDAP Administrator (cn=root), or the LDAP DB2 user) that are stored in the /etc/ibmslapd.conf file.
- User Entries (iNetOrgPerson) that have a password attribute used with Directory Server C and java (JNDI) APIs. These are the interfaces that applications, such as Policy Director and WebSphere use. While the Directory Server supports a wide variety of values for password entries, you need to review the application documentation to confirm what guidelines or restrictions apply.

The following provides details and recommendations of the supported password values using the IBM Directory Server 5.1 release.

Passwords for User Entries (InetOrgPerson) stored in the IBM Directory Server using the C or java Software Development Kits

Using the 5.1 release, the following characters are supported for the userPassword attribute field to be stored in the Directory Server using the C and java APIs. Applications, such as Policy Director, WebSphere, and so on, that are using the Directory Server might have additional restrictions on password values. Please review these specific product documentation for additional information.

- All upper and lower case English alpha and numeric characters.
- All other ASCII English characters are supported.
- Double-byte characters are supported for languages specified in the IBM Directory Server Version 5.1 Release Notes documentation.
- Passwords are case sensitive. (For example, if the password = TeSt, using a password of TEST or test fails. Only the exact case, TeSt, works.)

LDAP ibmslapd.conf users:

Using the 5.1 release, the following are the supported passwords for users that are in the *<LDAP_DIR>*/etc/ibmslapd.conf file.

- All upper and lower case English alpha and numeric characters.
- All other ASCII single-byte characters are supported.
- Passwords are case sensitive. (For example, if the password = TeSt, using a password of TEST or test fails. Only the exact case, TeSt, works.)

Notes:

1. The Users in the ibmslapd.conf file can include the following:
   - LDAP Administrator (cn=root)

   - Master ID for Replication (cn=MASTER)
   - LDAP DB2 users for LDAP DB entry and change log databases (LDAPDB2)
2. Double-byte characters in the administrator passwords are not supported.

Using the IDS Web Administration Tool to modify password attributes:

Using the Web Administration Tool in the 5.1 release, the following characters are supported for adding/modifying the password attribute field:

- All upper and lower case English alpha and numeric characters.
- All other ASCII single-byte characters are supported.
- Passwords are case sensitive. (For example, if the password = TeSt, using a password of TEST or test fails. Only the exact case, TeSt, works.)

Notes:

1. Double-byte characters are not supported for the administrator password.
2. Double-byte characters are supported for the user password.

Additional Recommendations:

It is recommended that you avoid using the following characters because the operating shell might interpret these ″special″ characters:

```
 `
 '
 \
 "
 |
```

For example, Using the 5.1 Web Administration Tool to assign a user password attribute to the value:

```
 "\"test\'
```

requires the following password from the command line to be used:

```
-w\"\\\"test\'
```

Here is an example search:

```
ldapsearch -b" " -sbase  -Dcn=newEntry,o=ibm,c=us   -w\"\\\"test\' objectclass=*
```

Note: This password works in the Web Administration Tool/java application using the original password without the escape character. In the previous example, the Web Administration Tool bind password is the same as the one that was entered when assigning the password in the Web Administration Tool:

```
 "\"test\'
```

Appendix. Notices

This information was developed for products and services offered in the U.S.A. IBM might not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the information. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this information at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of 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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

```
AIX     DB2      IBM    S/390    WebSphere
```

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

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

UNIX is a registered trademark in the United States and/or other countries licensed exclusively through X/Open Company Limited.

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

Printed in U.S.A.