

IBM Tivoli Directory Server



# Installation and Configuration Guide

*Version 6.0*



IBM Tivoli Directory Server



# Installation and Configuration Guide

*Version 6.0*

**Note**

Before using this information and the product it supports, read the general information under Appendix R, "Notices," on page 269.

**First Edition (April 2005)**

This edition applies to version 6, release 0, of IBM Tivoli Directory Server and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 1998, 2005. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

|  |           |
|--|-----------|
| <b>Preface</b> . . . . .                     | <b>ix</b> |
| Who should read this book . . . . .          | ix        |
| Publications . . . . .                       | ix        |
| IBM Tivoli Directory Server library. . . . . | ix        |
| Related publications . . . . .               | x         |
| Accessing publications online. . . . .       | x         |
| Ordering publications . . . . .              | x         |
| Accessibility . . . . .                      | x         |
| Tivoli technical training . . . . .          | xi        |
| Support information . . . . .                | xi        |
| Conventions used in this book . . . . .      | xi        |
| Typeface conventions . . . . .               | xi        |
| Operating system differences. . . . .        | xi        |

|  |          |
|--|----------|
| <b>Chapter 1. Quick installation path for a server</b> . . . . . | <b>1</b> |
|--|----------|

|  |          |
|--|----------|
| <b>Chapter 2. Installation, instance creation, configuration, and migration overview</b> . . . . . | <b>3</b> |
|--|----------|

|  |   |
|--|---|
| Before you begin: zip, tar, and iso files. . . . .                       | 3 |
| Migration from a previous release . . . . .                              | 3 |
| Installation . . . . .   | 4 |
| Client SDK . . . . .   | 4 |
| Java client . . . . .  | 4 |
| Server . . . . .   | 4 |
| Web Administration Tool . . . . .  | 5 |
| The embedded version of WebSphere Application Server - Express . . . . . | 5 |
| DB2 . . . . .  | 6 |
| Global Security Kit (GSKit) . . . . .                                    | 6 |
| Instance creation and database configuration . . . . .                   | 6 |
| Database configuration and server setup . . . . .                        | 7 |

|  |          |
|--|----------|
| <b>Chapter 3. System requirements and supported software versions.</b> . . . . . | <b>9</b> |
|--|----------|

|   |    |
|---|----|
| Requirements that are common to all operating systems . . . . .       | 9  |
| Requirements on Windows operating systems . . . . .                   | 10 |
| Requirements on AIX operating systems . . . . .                       | 11 |
| Requirements on xSeries Linux operating systems . . . . .             | 13 |
| Requirements on zSeries Linux operating systems . . . . .             | 15 |
| Requirements on iSeries and pSeries Linux operating systems . . . . . | 17 |
| Requirements on Solaris operating systems . . . . .                   | 19 |
| Requirements on HP-UX operating systems . . . . .                     | 21 |

|  |           |
|--|-----------|
| <b>Chapter 4. Migration from previous releases</b> . . . . . | <b>23</b> |
|--|-----------|

|  |    |
|--|----|
| About the client . . . . .                   | 23 |
| Location of migration utilities . . . . .    | 24 |
| Migration from SecureWay Directory . . . . . | 24 |
| High-level migration steps . . . . .         | 28 |

|   |    |
|---|----|
| Migration from IBM Directory Server 4.1 or 5.1 on non-AIX systems or IBM Tivoli Directory Server 5.2 on all systems . . . . . | 29 |
| Migration from IBM Directory Server version 4.1 or 5.1 on AIX systems . . . . .   | 31 |
| Database tasks before, during, and after migration . . . . .  | 33 |
| Preparing the database before migration. . . . .  | 33 |
| Replacing or installing a new version of DB2 . . . . .  | 35 |
| Migrating your database instances and databases . . . . .   | 36 |
| The command-line migration utility (idsimigr). . . . .  | 40 |
| Migrating the Web Administration Tool and upgrading the embedded version of WebSphere Application Server - Express. . . . .   | 43 |
| Migrating the embedded version of WebSphere Application Server - Express and the Web Administration Tool . . . . .            | 43 |

|   |           |
|---|-----------|
| <b>Chapter 5. Installing language packs using the InstallShield GUI</b> . . . . . | <b>45</b> |
|---|-----------|

|  |           |
|--|-----------|
| <b>Chapter 6. Installing IBM Tivoli Directory Server using the InstallShield GUI</b> . . . . . | <b>47</b> |
|--|-----------|

|  |    |
|--|----|
| Before you install . . . . .   | 47 |
| Creating user IDs . . . . .  | 48 |
| Installing IBM Tivoli Directory Server on a Windows platform . . . . .               | 48 |
| Installing IBM Tivoli Directory Server on an AIX, Linux, or Solaris system . . . . . | 52 |

|  |           |
|--|-----------|
| <b>Chapter 7. Considerations on AIX, Linux, Solaris, and HP-UX systems</b> . . . . . | <b>55</b> |
|--|-----------|

|   |    |
|---|----|
| The idsldap user and group . . . . .                                    | 55 |
| Installation path on AIX, Linux, Solaris, and HP-UX platforms . . . . . | 56 |
| Using commands to set and remove links . . . . .                        | 57 |
| Using idslink to set links . . . . .                                    | 57 |
| Using idsrmlink to remove links . . . . .                               | 62 |

|  |           |
|--|-----------|
| <b>Chapter 8. Installing IBM Tivoli Directory Server using AIX utilities</b> . . . . . | <b>65</b> |
|--|-----------|

|  |    |
|--|----|
| Before installing on a node within an RS/6000 SP environment . . . . . | 66 |
| Packages, filesets, and prerequisites . . . . .                        | 66 |
| SMIT installation . . . . .  | 69 |
| Command line installation using installp . . . . .                     | 72 |
| Installing GSKit . . . . .   | 74 |
| Setting system variables for GSKit. . . . .                            | 75 |
| Removing GSKit. . . . .  | 75 |

|   |           |
|---|-----------|
| <b>Chapter 9. Installing IBM Tivoli Directory Server using Linux utilities.</b> . . . . . | <b>77</b> |
|---|-----------|

|  |    |
|--|----|
| Installing IBM Tivoli Directory Server . . . . . | 77 |
|--|----|

|                               |    |
|-------------------------------|----|
| Packages . . . . .            | 77 |
| Installing features . . . . . | 79 |
| Installing GSKit . . . . .    | 80 |
| Removing GSKit. . . . .       | 81 |

**Chapter 10. Installing IBM Tivoli Directory Server using Solaris utilities . 83**

|  |    |
|--|----|
| Before you install . . . . .                     | 83 |
| Setting kernel parameters. . . . .               | 83 |
| Installing IBM Tivoli Directory Server . . . . . | 84 |
| Package dependencies . . . . .                   | 85 |
| AdminTool installation . . . . .                 | 86 |
| Command line installation using pkgadd . . . . . | 87 |
| Installing GSKit . . . . .                       | 90 |
| Removing GSKit. . . . .                          | 90 |

**Chapter 11. Installing IBM Tivoli Directory Server using HP-UX utilities . 91**

|  |    |
|--|----|
| Before you install . . . . .                         | 91 |
| Setting the kernel configuration parameters. . . . . | 92 |
| Mounting and unmounting the CD . . . . .             | 93 |
| Installing IBM Tivoli Directory Server . . . . .     | 94 |
| Package dependencies . . . . .                       | 94 |
| Installing using swinstall . . . . .                 | 96 |
| Installing GSKit . . . . .                           | 97 |
| Removing GSKit. . . . .                              | 97 |

**Chapter 12. Installing and uninstalling silently on Windows platforms . . . . . 99**

|   |     |
|---|-----|
| Silent installation . . . . .   | 99  |
| Installing the server or client silently . . . . .                              | 100 |
| Installing language packs silently. . . . .                                     | 101 |
| Verifying the silent installation . . . . .                                     | 102 |
| Options files for silent installation of servers and language packs . . . . .   | 103 |
| Silent uninstallation . . . . .   | 105 |
| Options files for silent uninstallation of servers and language packs . . . . . | 106 |
| Installing GSKit on Windows operating systems . . . . .                         | 107 |
| Removing GSKit . . . . .  | 108 |

**Chapter 13. Creating and administering instances. . . . . 109**

|   |     |
|---|-----|
| Using the Instance Administration Tool to work with instances . . . . . | 109 |
| Starting the Instance Administration Tool . . . . .                     | 109 |
| Creating an instance . . . . .  | 110 |
| Changing the TCP/IP settings for an instance . . . . .                  | 114 |
| Viewing information about an instance . . . . .                         | 115 |
| Deleting an instance . . . . .  | 115 |
| Using commands to work with instances . . . . .                         | 115 |
| Using idsicrt to create an instance . . . . .                           | 116 |
| Using idssethost to set IP addresses . . . . .                          | 119 |
| Using idssetport to set ports . . . . .                                 | 120 |
| Using idsilist to view instance details . . . . .                       | 122 |
| Using idsidrop to remove a directory server instance . . . . .          | 123 |

**Chapter 14. Configuration . . . . . 125**

|   |     |
|---|-----|
| Using the IBM Tivoli Directory Server Configuration Tool (idsxcfg) . . . . .  | 125 |
| Managing the administrator DN for a directory server instance . . . . .       | 126 |
| Managing the administrator password for a directory server instance. . . . .  | 127 |
| Configuring the database for a directory server instance . . . . .            | 127 |
| Unconfiguring the database for a directory server instance . . . . .          | 128 |
| Enabling or disabling the change log for a directory server instance. . . . . | 129 |
| Managing suffixes . . . . .   | 130 |
| Managing schema files . . . . .   | 131 |
| Importing and exporting LDIF data . . . . .                                   | 132 |
| Backing up, restoring, and optimizing the database . . . . .                  | 134 |
| Using command-line utilities for configuration . . . . .                      | 136 |
| Using idsdnpw to set the administrator DN and password. . . . .               | 136 |
| Using idsfcgdb to configure the database . . . . .                            | 138 |
| Using idsucfgdb to unconfigure the database . . . . .                         | 140 |
| Using idsfcgchglg to configure the change log . . . . .                       | 141 |
| Using idsucfgchglg to unconfigure the change log . . . . .                    | 142 |
| Using idsfcgsuf to add a suffix . . . . .                                     | 143 |
| Using idsucfgsuf to remove a suffix . . . . .                                 | 144 |
| Using idsfcgsch to add a schema file . . . . .                                | 146 |
| Using idsucfgsch to unconfigure a schema file . . . . .                       | 146 |
| Importing or exporting data . . . . .   | 148 |
| Backing up, restoring, and optimizing the database . . . . .                  | 148 |

**Chapter 15. After you install and configure . . . . . 149**

|  |     |
|--|-----|
| Starting the directory server instance . . . . .                             | 149 |
| Starting the application server to use the Web Administration Tool . . . . . | 149 |
| Starting the Web Administration Tool . . . . .                               | 149 |
| Stopping the application server . . . . .                                    | 150 |

**Chapter 16. Uninstalling IBM Tivoli Directory Server . . . . . 151**

|  |     |
|--|-----|
| Uninstalling IBM Tivoli Directory Server using the InstallShield GUI . . . . . | 151 |
| Uninstalling language packs using the InstallShield GUI . . . . .              | 152 |
| Uninstalling using operating system utilities . . . . .                        | 153 |
| AIX operating system . . . . .   | 153 |
| Linux operating system . . . . .   | 154 |
| Solaris operating system. . . . .  | 155 |
| HP-UX . . . . .  | 156 |

**Appendix A. Directory structure of unzipped and untarred files . . . . . 157**

|  |     |
|--|-----|
| The top level directory . . . . .                            | 157 |
| Server InstallShield GUI installation files . . . . .        | 157 |
| Server operating system utility installation files . . . . . | 159 |
| Client InstallShield GUI installation files . . . . .        | 163 |
| Client operating system utility installation files . . . . . | 165 |

**Appendix B. Disk space requirements for installable features . . . . . 167**

Windows disk space requirements . . . . . 167  
AIX disk space requirements . . . . . 167  
Linux disk space requirements . . . . . 168  
Solaris disk space requirements . . . . . 168  
HP-UX disk space requirements . . . . . 168

**Appendix C. Database configuration planning . . . . . 171**

**Appendix D. Setting up users and groups: directory server instance owner, database instance owner, and database owner . . . . . 173**

Naming rules . . . . . 173  
Additional restrictions for users and groups . . . 174  
Creating instance owners: examples . . . . . 175

**Appendix E. Synchronizing two-way cryptography between server instances . . . . . 177**

**Appendix F. Directory server instances . . . . . 179**

Directory server instance content on Windows systems . . . . . 179  
Directory server instance content on AIX, Linux, Solaris, and HP-UX systems . . . . . 180

**Appendix G. Migrating a replicating environment from SecureWay Directory 3.2.2 . . . . . 181**

**Appendix H. Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express . . . . . 183**

Manually installing and configuring the embedded version of WebSphere Application Server - Express. 183  
    Installing the embedded version of WebSphere Application Server - Express . . . . . 183  
    Installing the Web Administration Tool into the embedded version of WebSphere Application Server - Express . . . . . 184  
Uninstalling the Web Administration Tool from the embedded version of WebSphere Application Server - Express . . . . . 184  
Default ports for the embedded version of WebSphere Application Server - Express . . . . 185  
Using HTTPS for the embedded version of WebSphere Application Server - Express Version 5.1.1 . . . . . 186

**Appendix I. Installing the Web Administration Tool into WebSphere . 187**

**Appendix J. ASCII characters from 33 to 126. . . . . 189**

**Appendix K. Information for bundlers 191**

How to install silently . . . . . 191  
Environment variable for silent installation with native packages . . . . . 191  
Installing corequisite products silently . . . . . 192  
Starting the instance administration tool in migration mode . . . . . 192  
Additional information about GSKit. . . . . 192

**Appendix L. Installing and configuring DSML. . . . . 193**

**Appendix M. Loading a sample database . . . . . 195**

**Appendix N. UTF-8 support . . . . . 197**

Why choose anything other than UTF-8? . . . . 197  
Server utilities . . . . . 197  
    Examples. . . . . 197  
Supported IANA character sets . . . . . 198

**Appendix O. Setting up GSKit to support CMS key databases . . . . . 201**

**Appendix P. IBM Tivoli Directory Server configuration schema . . . . . 203**

Directory Information Tree . . . . . 203  
    cn=Configuration . . . . . 204  
    cn=Admin . . . . . 204  
    cn=AdminGroup . . . . . 205  
    cn=Front End . . . . . 205  
    cn=Connection Management . . . . . 206  
    cn=Event Notification . . . . . 206  
    cn=Kerberos . . . . . 207  
    cn=Master Server . . . . . 207  
    cn=Referral . . . . . 207  
    cn=Schemas . . . . . 208  
    cn=IBM Directory . . . . . 208  
    cn=Config Backends . . . . . 209  
    cn=ConfigDB . . . . . 209  
    cn=RDBM Backends . . . . . 209  
    cn=Directory . . . . . 210  
    cn=Change Log. . . . . 211  
    cn=LDCF Backends . . . . . 212  
    cn=SchemaDB . . . . . 212  
    cn=Proxy Backends . . . . . 212  
    cn=Proxy DB . . . . . 213  
    cn=Replication . . . . . 213  
    cn=Log Management . . . . . 214  
    cn=Default . . . . . 214  
    cn=ibmslapd . . . . . 214  
    cn=Audit . . . . . 215  
    cn=Bulkload. . . . . 216  
    cn=DB2CLI . . . . . 216  
    cn=Tools . . . . . 217

|   |     |   |     |
|---|-----|---|-----|
| cn=Replication . . . . .                    | 217 | ibm-slapdLdapCrlPort . . . . .                | 240 |
| cn=Admin . . . . .                          | 218 | ibm-slapdLdapCrlUser . . . . .                | 240 |
| cn=admin audit . . . . .                    | 218 | ibm-slapdLog . . . . .                        | 241 |
| cn=pwdPolicy Admin . . . . .                | 219 | ibm-slapdLogArchivePath . . . . .             | 241 |
| cn=SSL . . . . .                            | 219 | ibm-slapdLogMaxArchives . . . . .             | 241 |
| cn=CRL . . . . .                            | 220 | ibm-slapdLogOptions . . . . .                 | 241 |
| cn=Transaction . . . . .                    | 220 | ibm-slapdLogSizeThreshold . . . . .           | 242 |
| cn=Digest . . . . .                         | 221 | ibm-slapdMasterDN . . . . .                   | 242 |
| Attributes . . . . .                        | 221 | ibm-slapdMasterPW . . . . .                   | 242 |
| cn . . . . .                                | 224 | ibm-slapdMasterReferral . . . . .             | 243 |
| ibm-ReplicationOnHold . . . . .             | 224 | ibm-slapdMaxEventsPerConnection . . . . .     | 243 |
| ibm-slapdACLCache . . . . .                 | 225 | ibm-slapdMaxEventsTotal . . . . .             | 243 |
| ibm-slapdACLCacheSize . . . . .             | 225 | ibm-slapdMaxNumOfTransactions . . . . .       | 244 |
| ibm-slapdAdminDN . . . . .                  | 225 | ibm-slapdMaxOpPerTransaction . . . . .        | 244 |
| ibm-slapdAdminGroupEnabled . . . . .        | 226 | ibm-slapdMaxPendingChangesDisplayed . . . . . | 244 |
| ibm-slapdAdminPW . . . . .                  | 226 | ibm-slapdMaxTimeLimitOfTransactions . . . . . | 245 |
| ibm-slapdAllowAnon . . . . .                | 226 | ibm-slapdPagedResAllowNonAdmin . . . . .      | 245 |
| ibm-slapdAllReapingThreshold . . . . .      | 226 | ibm-slapdPagedResLmt . . . . .                | 245 |
| ibm-slapdAnonReapingThreshold . . . . .     | 227 | ibm-slapdPageSizeLmt . . . . .                | 246 |
| ibm-slapdBoundReapingThreshold . . . . .    | 227 | ibm-slapdPlugin . . . . .                     | 246 |
| ibm-slapdBulkloadErrors . . . . .           | 227 | ibm-slapdPort . . . . .                       | 247 |
| ibm-slapdCachedAttribute . . . . .          | 227 | ibm-slapdProxyBackendServerDn . . . . .       | 247 |
| ibm-slapdCachedAttributeSize . . . . .      | 228 | ibm-slapdProxyBindMethod . . . . .            | 247 |
| ibm-slapdChangeLogMaxAge . . . . .          | 228 | ibm-slapdProxyConnectionPoolSize . . . . .    | 248 |
| ibm-slapdChangeLogMaxEntries . . . . .      | 228 | ibm-slapdProxyDigestRealm . . . . .           | 248 |
| ibm-slapdCLIErrors . . . . .                | 229 | ibm-slapdProxyDigestUserName . . . . .        | 248 |
| ibm-slapdConcurrentRW . . . . .             | 229 | ibm-slapdProxyDn . . . . .                    | 249 |
| ibm-slapdCryptoSync . . . . .               | 229 | ibm-slapdProxyNumPartitions . . . . .         | 249 |
| ibm-slapdDB2CP . . . . .                    | 230 | ibm-slapdProxyPartitionBase . . . . .         | 249 |
| ibm-slapdDBAlias . . . . .                  | 230 | ibm-slapdProxyPartitionIndex . . . . .        | 249 |
| ibm-slapdConfigPwdPolicyOn . . . . .        | 230 | ibm-slapdProxyPw . . . . .                    | 250 |
| ibm-slapdDbConnections . . . . .            | 230 | ibm-slapdProxyTargetURL . . . . .             | 250 |
| ibm-slapdDbInstance . . . . .               | 231 | ibm-slapdPWEncryption . . . . .               | 250 |
| ibm-slapdDbLocation . . . . .               | 231 | ibm-slapdReadOnly . . . . .                   | 250 |
| ibm-slapdDbName . . . . .                   | 231 | ibm-slapdReferral . . . . .                   | 251 |
| ibm-slapdDbUserID . . . . .                 | 231 | ibm-slapdReplConflictMaxEntrySize . . . . .   | 251 |
| ibm-slapdDbUserPW . . . . .                 | 232 | ibm-slapdReplContextCacheSize . . . . .       | 251 |
| ibm-slapdDerefAliases . . . . .             | 232 | ibm-slapdReplDbConns . . . . .                | 252 |
| ibm-slapdDigestAdminUser . . . . .          | 232 | ibm-slapdReplMaxErrors . . . . .              | 252 |
| ibm-slapdDigestAttr . . . . .               | 233 | ibm-slapdReplicaSubtree . . . . .             | 252 |
| ibm-slapdDigestRealm . . . . .              | 233 | ibm-slapdSchemaAdditions . . . . .            | 252 |
| ibm-slapdDistributedDynamicGroups . . . . . | 233 | ibm-slapdSchemaCheck . . . . .                | 253 |
| ibm-slapdEnableEventNotification . . . . .  | 234 | ibm-slapdSecurePort . . . . .                 | 253 |
| ibm-slapdEntryCacheSize . . . . .           | 234 | ibm-slapdSecurity . . . . .                   | 253 |
| ibm-slapdESizeThreshold . . . . .           | 234 | ibm-slapdServerBackend . . . . .              | 254 |
| ibm-slapdEThreadActivate . . . . .          | 235 | ibm-slapdServerId . . . . .                   | 254 |
| ibm-slapdEThreadEnable . . . . .            | 235 | ibm-slapdSetenv . . . . .                     | 254 |
| ibm-slapdETimeThreshold . . . . .           | 235 | ibm-slapdSizeLimit . . . . .                  | 254 |
| ibm-slapdFilterCacheBypassLimit . . . . .   | 235 | ibm-slapdSortKeyLimit . . . . .               | 255 |
| ibm-slapdFilterCacheSize . . . . .          | 236 | ibm-slapdSortSrchAllowNonAdmin . . . . .      | 255 |
| ibm-slapdIdleTimeOut . . . . .              | 236 | ibm-slapdSslAuth . . . . .                    | 256 |
| ibm-slapdIncludeSchema . . . . .            | 236 | ibm-slapdSslCertificate . . . . .             | 256 |
| ibm-slapdIpAddress . . . . .                | 237 | ibm-slapdSslCipherSpec . . . . .              | 257 |
| ibm-slapdKrbAdminDN . . . . .               | 237 | ibm-slapdSslFIPsModeEnabled . . . . .         | 257 |
| ibm-slapdKrbEnable . . . . .                | 238 | ibm-slapdSslFIPsProcessingMode . . . . .      | 257 |
| ibm-slapdKrbIdentityMap . . . . .           | 238 | ibm-slapdSslKeyDatabase . . . . .             | 258 |
| ibm-slapdKrbKeyTab . . . . .                | 238 | ibm-slapdSslKeyDatabasePW . . . . .           | 258 |
| ibm-slapdKrbRealm . . . . .                 | 239 | ibm-slapdSslKeyRingFile . . . . .             | 258 |
| ibm-slapdLanguageTagsEnabled . . . . .      | 239 | ibm-slapdSslKeyRingFilePW . . . . .           | 259 |
| ibm-slapdLdapCrlHost . . . . .              | 239 | ibm-slapdStartupTraceEnabled . . . . .        | 259 |
| ibm-slapdLdapCrlPassword . . . . .          | 239 | ibm-slapdSuffix . . . . .                     | 259 |



|   |            |
|---|------------|
| ibm-slapdSupportedWebAdmVersion . . . . .       | 260        |
| ibm-slapdTimeLimit . . . . .                    | 260        |
| ibm-slapdTraceMessageLevel . . . . .            | 260        |
| ibm-slapdTraceMessageLog. . . . .               | 261        |
| ibm-slapdTransactionEnable . . . . .            | 261        |
| ibm-slapdUseProcessIdPw . . . . .               | 261        |
| ibm-slapdVersion . . . . .                      | 261        |
| ibm-slapdWriteTimeout . . . . .                 | 262        |
| ids-instanceDesc . . . . .                      | 262        |
| ids-instanceLocation . . . . .                  | 262        |
| ids-instanceVersion . . . . .                   | 263        |
| objectClass . . . . .                           | 263        |
| <b>Appendix Q. Support information. . . . .</b> | <b>265</b> |
| Searching knowledge bases. . . . .              | 265        |

|  |            |
|--|------------|
| Search the information center on your local system or network. . . . . | 265        |
| Search the Internet . . . . .  | 265        |
| Obtaining fixes . . . . .  | 265        |
| Contacting IBM Software Support . . . . .                              | 266        |
| Determine the business impact of your problem                          | 267        |
| Describe your problem and gather background information . . . . .      | 267        |
| Submit your problem to IBM Software Support                            | 267        |
| <b>Appendix R. Notices . . . . .</b>                                   | <b>269</b> |
| Trademarks . . . . .   | 270        |

|                        |            |
|------------------------|------------|
| <b>Index . . . . .</b> | <b>273</b> |
|------------------------|------------|



---

## Preface

This book describes how to install, configure, and uninstall IBM Tivoli Directory Server version 6.0. IBM Tivoli Directory Server 6.0 is supported on Windows, AIX, Linux (xSeries, zSeries, pSeries, and iSeries), Solaris, and Hewlett-Packard UNIX (HP-UX) operating systems. For detailed information about supported operating system versions, as well as other required software and hardware, see Chapter 3, “System requirements and supported software versions,” on page 9.

---

## Who should read this book

This book is intended for system administrators.

---

## Publications

Read the descriptions of the IBM Tivoli Directory Server library, the prerequisite publications, and the related publications to determine which publications you might find helpful. After you determine the publications you need, see “Accessing publications online” on page x for information about accessing publications online.

### IBM Tivoli Directory Server library

The publications in the IBM Tivoli Directory Server library are:

*IBM Tivoli Directory Server Version 6.0 Release Notes*

Contains information about the new features in the IBM Tivoli Directory Server Version 6.0 release, as well as last-minute updates.

*IBM Tivoli Directory Server Version 6.0 Installation and Configuration Guide*

Contains complete information for installing, configuring, and uninstalling IBM Tivoli Directory Server. Includes information about migrating from a previous version of IBM Tivoli Directory Server or SecureWay Directory.

*IBM Tivoli Directory Server Version 6.0 Administration Guide*

Contains instructions for performing administrator tasks through the Web Administration Tool and the command line.

*IBM Tivoli Directory Server Version 6.0 Performance Tuning Guide*

Contains information about tuning your server for better performance.

*IBM Tivoli Directory Server Version 6.0 Server Plug-ins Reference*

Contains information about writing server plug-ins.

*IBM Tivoli Directory Server Version 6.0 C-Client SDK Programming Reference*

Contains information about writing Lightweight Directory Access Protocol (LDAP) client applications.

*IBM Tivoli Directory Server Version 6.0 Problem Determination Guide*

Contains information about possible problems and corrective actions that can be tried before contacting IBM Software Support.

*IBM Tivoli Directory Server Version 6.0 Messages Guide*

Contains a list of all informational, warning, and error messages associated with IBM Tivoli Directory Server 6.0.

## Related publications

Information related to IBM Tivoli Directory Server is available in the following publications:

- IBM Tivoli Directory Server Version 6.0 uses the JNDI client from Sun Microsystems. For information about the JNDI client, refer to the *Java Naming and Directory Interface™ 1.2.1 Specification* on the Sun Microsystems Web site at <http://java.sun.com/products/jndi/1.2/javadoc/index.html>.
- The Tivoli Software Library provides a variety of Tivoli publications such as white papers, datasheets, demonstrations, redbooks, and announcement letters. The Tivoli Software Library is available on the Web at: <http://publib.boulder.ibm.com/tividd/td/tdprodlist.html>
- The *Tivoli Software Glossary* includes definitions for many of the technical terms related to Tivoli software. The *Tivoli Software Glossary* is available at <http://publib.boulder.ibm.com/tividd/glossary/tivologlossarymst.htm>

## Accessing publications online

The publications for this product are available online in Portable Document Format (PDF) or Hypertext Markup Language (HTML) format, or both in the Tivoli software library: <http://publib.boulder.ibm.com/tividd/td/tdprodlist.html>

To locate product publications in the library, click the **Product manuals** link on the left side of the library page. Then, locate and click the name of the product on the Tivoli software information center page.

Product publications include release notes, installation guides, user's guides, administrator's guides, and developer's references.

**Note:** To ensure proper printing of PDF publications, select the **Fit to page** check box in the Adobe Acrobat Print window (which is available when you click **File** → **Print**).

## Ordering publications

You can order many Tivoli publications online at the following Web site:

<http://www.elink.ibm.link.ibm.com/public/applications/publications/cgibin/pbi.cgi>

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, see the following Web site for a list of telephone numbers:

<http://www.ibm.com/software/tivoli/order-lit/>

---

## Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You also can use the keyboard instead of the mouse to operate all features of the graphical user interface.

---

## Tivoli technical training

For Tivoli technical training information, refer to the IBM Tivoli Education Web site: <http://www.ibm.com/software/tivoli/education>.

---

## Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

- Searching knowledge bases: You can search across a large collection of known problems and workarounds, Technotes, and other information.
- Obtaining fixes: You can locate the latest fixes that are already available for your product.
- Contacting IBM Software Support: If you still cannot solve your problem, and you need to work with someone from IBM, you can use a variety of ways to contact IBM Software Support.

For more information about these three ways of resolving problems, see Appendix Q, "Support information," on page 265.

---

## Conventions used in this book

This reference uses several conventions for special terms and actions and for operating system-dependent commands and paths.

### Typeface conventions

The following typeface conventions are used in this reference:

**Bold** Lowercase commands or mixed case commands that are difficult to distinguish from surrounding text, keywords, parameters, options, names of Java classes, and objects are in **bold**.

*Italic* Variables, titles of publications, and special words or phrases that are emphasized are in *italic*.

<*Italic*>

Variables are set off with < > and are in <*italic*>.

Monospace

Code examples, command lines, screen output, file and directory names that are difficult to distinguish from surrounding text, system messages, text that the user must type, and values for arguments or command options are in monospace.

### Operating system differences

This book uses the UNIX convention for specifying environment variables and for directory notation. When you are using the Windows command line, replace *\$variable* with *%variable%* for environment variables and replace each forward slash (/) with a backslash (\) in directory paths. If you are using the bash shell on a Windows system, you can use the UNIX conventions.



---

## Chapter 1. Quick installation path for a server

To follow the simplest path through installation of a server, use the checklist in this chapter. If you are migrating from a previous release, do not use this checklist. See Chapter 4, “Migration from previous releases,” on page 23 for instructions.

- 1. Decide what kind of server or servers you want to install on this computer. See Chapter 2, “Installation, instance creation, configuration, and migration overview,” on page 3 for information.
- 2. Be sure that you have the minimum required hardware and software. See Chapter 3, “System requirements and supported software versions,” on page 9 for information. The chapter contains a section for each supported operating system.

Also see the *IBM Tivoli Directory Server Version 6.0 Server Release Notes* for last-minute information. (See “Accessing publications online” on page x for information about accessing online publications.)

- 3. Plan the organization of your database if you want a full server. See Appendix C, “Database configuration planning,” on page 171 for information.
- 4. For each directory server instance that will be on this computer, create the user ID that will own that directory server instance. (You can wait until after installation, but you must create the user ID before you create the directory server instance.)  
See Appendix D, “Setting up users and groups: directory server instance owner, database instance owner, and database owner,” on page 173 for information.
- 5. If you want to use a language other than English, install the language pack for your language. See Chapter 5, “Installing language packs using the InstallShield GUI,” on page 45 for instructions.

**Note:** You can install a language pack after installing IBM® Tivoli® Directory Server, but the Instance Administration Tool and Configuration Tool panels, as well as server messages, will display in English until you install a language pack.

- 6. Install IBM Tivoli Directory Server using the InstallShield GUI, if available for your operating system platform. You can use the InstallShield GUI on Windows®, AIX®, xSeries®, zSeries®, iSeries™, and pSeries™ Linux®, and Solaris operating systems. (There is no InstallShield GUI installation available for HP-UX.)

For Windows platforms, see “Installing IBM Tivoli Directory Server on a Windows platform” on page 48.

For AIX, Linux, and Solaris platforms, see “Installing IBM Tivoli Directory Server on an AIX, Linux, or Solaris system” on page 52.

**Note:** To install IBM Tivoli Directory Server using utilities for your operating system instead of the InstallShield GUI, see the chapter for your operating system. These chapters are:

- Chapter 8, “Installing IBM Tivoli Directory Server using AIX utilities,” on page 65

- Chapter 9, “Installing IBM Tivoli Directory Server using Linux utilities,” on page 77
  - Chapter 10, “Installing IBM Tivoli Directory Server using Solaris utilities,” on page 83
  - Chapter 11, “Installing IBM Tivoli Directory Server using HP-UX utilities,” on page 91
- \_\_\_ 7. On Windows, if the system restarts, log on as the user you were logged on as during installation.
  - \_\_\_ 8. After the Instance Administration Tool starts, create a directory server instance if you do not already have one. While you are creating the instance, set the administrator DN and password. If you installed the full server and you do not want this directory server instance to be a proxy server, also configure the database while you are creating the instance. See Chapter 13, “Creating and administering instances,” on page 109 for instructions.

**Note:** If you used operating system utilities to install, you must start the Instance Administration Tool from the command line, using the **idsxinst** command.

- \_\_\_ 9. Optionally, if you installed the full server, verify the installation and configuration by loading the sample database.  
See Appendix M, “Loading a sample database,” on page 195 for information.  
(You will need to add a suffix for this task. Instructions are included in the procedure for loading a sample database.)
- \_\_\_ 10. Start the directory server instance and, if you installed the Web Administration Tool, start it.  
See Chapter 15, “After you install and configure,” on page 149 for information.
- \_\_\_ 11. See the *IBM Tivoli Directory Server Version 6.0 Administration Guide* for information about setting up and using the server and the Web Administration Tool.



---

## Chapter 2. Installation, instance creation, configuration, and migration overview

This chapter briefly describes migration, installation, instance creation, and configuration for IBM Tivoli Directory Server version 6.0.

---

### Before you begin: zip, tar, and iso files

The IBM Tivoli Directory Server product is available in three file formats: zip, tar, and iso.

If you downloaded a zip file, use a product such as PKZIP to unzip the file after you download it to your computer. Be sure to unzip the file into a path that has no spaces in the name.

If you downloaded a tar, or Tape ARchive, untar it after you download it.

The iso version of the product is used to burn an installation CD-ROM that can then be used in the installation process. The iso file is an image that must be processed through a CD-ROM burner program to create the CD-ROM. When you create the CD-ROM, be sure that you do not make a data CD of the iso file. Select the option that unencapsulates the data from the iso file and burns the files on the CD-ROM.

For information about the directory structure after you unzip or untar the file on different operating systems, see Appendix A, "Directory structure of unzipped and untarred files," on page 157.

After you process the downloaded file, you can install IBM Tivoli Directory Server using the installation instructions in the appropriate installation chapter.

---

### Migration from a previous release

If you have a previous version of the IBM Directory, migration is necessary to preserve any changes that you have made to the schema definitions and to preserve your directory server configuration. Previous versions include the following:

- SecureWay<sup>®</sup> Directory Version 3.1.1.5, 3.2, 3.2.1, or 3.2.2  
**Attention:** If you have SecureWay Directory Version 3.1.1.5, 3.2, or 3.2.1 currently installed and you want to migrate your data, you must upgrade to level 3.2.2 before you install IBM Tivoli Directory Server 6.0. You can download SecureWay Directory version 3.2.2 from:  
<http://www.ibm.com/software/sysmgmt/products/support/IBMDirectoryServer.html>. See the SecureWay Directory version 3.2.2 documentation for information about migrating from a previous version.
- IBM Directory Server 4.1, 5.1, or 5.1 for Linux iSeries and pSeries
- IBM Tivoli Directory Server 5.2

In addition, it might be necessary to upgrade your operating system and your DB2<sup>®</sup> version. For example, on AIX, the server is supported only on 64-bit versions; therefore you might need to install a 64-bit version of AIX and DB2.

If you want to migrate your data, see Chapter 4, “Migration from previous releases,” on page 23 before you begin the installation process for IBM Tivoli Directory Server 6.0.

---

## Installation

When you install IBM Tivoli Directory Server on a computer, you can install one or more features that allow the computer to function as a client, a proxy server, a full server, or a console for managing servers. In addition, if you want a server to display messages in a language other than English, you must also install a language pack.

IBM Tivoli Directory Server 6.0 has several ways of installing. You can install using an InstallShield graphical user interface (GUI) or use platform-specific installation methods such as the command line or installation tools for the operating system. Instructions for using the InstallShield GUI are found in Chapter 6, “Installing IBM Tivoli Directory Server using the InstallShield GUI,” on page 47.

For information about platform-specific installation methods, see the installation chapter for the operating system on which you are installing. For example, see Chapter 8, “Installing IBM Tivoli Directory Server using AIX utilities,” on page 65.

**Note:** On Hewlett-Packard UNIX<sup>®</sup> (HP-UX), the InstallShield GUI is not available, and you must use operating system utilities to install.

Before you install, see Chapter 3, “System requirements and supported software versions,” on page 9 for hardware and software requirements.

To help you decide what you want to install, the following sections describe the choices on the InstallShield GUI main panel.

### Client SDK

The client Software Development Kit (SDK) provides the tools required to develop C-language LDAP applications. The following are provided:

- Client libraries that provide a set of C-language APIs
- C header files for building and compiling LDAP applications
- Sample programs in source form
- Executable versions of the sample programs

The client can be installed alone, and it must be installed when you install a server. IBM Tivoli Directory Server 6.0 clients can coexist on the same computer with another client that is version 4.1, 5.1, or 5.2.

### Java client

The Java client includes a Java runtime version 1.4.2 and Java utilities. The Java client is required if you are installing a server.

### Server

In this release of IBM Tivoli Directory Server, you can install two types of servers: the full server and the proxy server. You can install both types of servers on one computer and create one or more instances of the types of servers you have installed. These are called directory server instances. Each directory server instance can function as either a proxy server or a full server, but not both.

An IBM Tivoli Directory Server 6.0 server requires that the version 6.0 client and the Java client also be installed. In addition, the server can coexist on the same computer with another client that is version 4.1, 5.1, or 5.2.

### **Proxy server**

The *proxy* server is an LDAP server that acts as a front-end to the directory. It authenticates the client with respect to the entire directory and routes requests to certain other directory servers. This improves performance and provides a unified view of the directory to the client. The proxy server can also be used at the front-end of a server cluster or a distributed directory for providing failover and load balancing.

The proxy server is configured with information that allows it to connect to each of the servers for which it is the proxy server. It routes each request to one or more target servers. The proxy server can load balance among target servers that are equally capable of handling an operation; it performs transparent failover to alternate servers if a server is busy or down.

To install a proxy server, you do not need to have DB2 installed on the computer.

This book contains information about installing a proxy server and creating and configuring a proxy server instance. For information about configuring a proxy server instance as a proxy for other directory server instances, see the *IBM Tivoli Directory Server version 6.0 Administration Guide*.

### **Full server**

When you install the *full* server package, you install both the proxy server and the directory server. The directory server is an LDAP server; it is configured with a database instance, and it processes client requests that require accessing entries stored in the database. DB2 is required for a full server.

## **Web Administration Tool**

You can use the Web Administration Tool to administer LDAP servers, which can be of the following types:

- IBM Tivoli Directory Server 6.0
- IBM Tivoli Directory Server 5.2
- IBM Directory Server 5.1
- IBM Directory Server 4.1
- IBM SecureWay Directory 3.2.2
- i5/OS
- z/OS™ R4

**Note:** For z/OS R4, only the following setups are supported:

- A single TDBM backend
- A single SDBM backend
- One TDBM and SDBM backend

## **The embedded version of WebSphere Application Server - Express**

An application server is required to run the Web Administration Tool. The embedded version of WebSphere® Application Server - Express, version 5.1.1, is provided with IBM Tivoli Directory Server.

## DB2

IBM DB2 is required for the full server package because directory entries are stored in a DB2 database. IBM DB2 Enterprise Server Edition (ESE) 8 Fix Pack 8 refresh is included with IBM Tivoli Directory Server for all operating systems except HP-UX. (This version of DB2 is also called version 8.1 Fix Pack 8, or version 8.2 Fix Pack 1.) DB2 Enterprise Server Edition (ESE) 8 Fix Pack 2 refresh is included with IBM Tivoli Directory Server for HP-UX. However, versions other than the version provided are supported. See Chapter 3, “System requirements and supported software versions,” on page 9 to find out which versions of DB2 are supported for your operating system.

**Note:** Remote databases are **not** supported.

## Global Security Kit (GSKit)

Secure Sockets Layer (SSL) Global Security Kit (GSKit) is an optional software package that is required only if Secure Sockets Layer Security or Transport Layer Security (TLS) is required.

IBM Tivoli Directory Server alone does not provide the capability for SSL connections from IBM Tivoli Directory Server clients. You can enable the SSL feature by installing the IBM GSKit package. The GSKit package includes SSL support and associated RSA Security, Inc. technology.

OpenSSL is included in GSKit and may be used for cryptographic operations (as per the OpenSSL license requirements).

The IBM Tivoli Directory Server server can work without the GSKit installed. In this case the server accepts only non-secure connections from directory clients. Similarly, the IBM Tivoli Directory Server client can work without the GSKit installed. Install GSKit on both the server and the client if you want to use secure connections.

Version 7.0.3.3 of GSKit is provided with IBM Tivoli Directory Server 6.0.

---

## Instance creation and database configuration

After you install a server, you must perform the following configuration tasks before you can use the server:

- Create user IDs for the directory server instance owner and, for some installations, the database instance owner and the database owner. See Appendix D, “Setting up users and groups: directory server instance owner, database instance owner, and database owner,” on page 173 for detailed information about these user IDs.
- Create a directory server instance.
- Set the IBM Tivoli Directory Server administrator distinguished name (DN) and password for the directory server instance. This operation can be compared to defining the root user ID and password on a UNIX system.
- If the directory server instance is not a proxy server, configure the database; you do not need a database for a proxy server instance.

To create a directory server instance, you can use either the Instance Administration Tool (**idsxinst**), which has a GUI, or the **idsicrt** command-line utility. When you create a directory server instance, a database instance is also created if the full server package is installed on the computer. By default, the

directory server instance and the database instance have the same name. The name must match the name of an existing user on the system that meets certain qualifications, described in Appendix D, “Setting up users and groups: directory server instance owner, database instance owner, and database owner,” on page 173.

You can have multiple directory server instances on one computer, and they can be a mixture of proxy server and full server instances. The files for each directory server instance are stored in a path that includes the directory server instance name.

After successful installation of a server, if you used the InstallShield GUI to install, the Instance Administration Tool runs. If you did not use the InstallShield GUI to install, you must start the Instance Administration Tool manually or use the **idsicrt** command-line utility.

You can also use the Instance Administration Tool for the following tasks:

- Migrating server schema and configuration files from a previous release to an IBM Tivoli Directory Server 6.0 instance
- Editing the TCP/IP settings for an instance
- Viewing all instances on the computer
- Viewing details about a particular instance
- Deleting an instance

If you prefer to use the command line, all the tasks in the list can be done with the following command-line utilities:

- **idsimigr** migrates the schema and configuration files from a previous release to IBM Tivoli Directory Server versions of these files.
- **idssethost** sets the IP addresses the directory server instance binds to.
- **idssetport** sets the ports the directory server instance binds to.
- **idsilist** lists the directory server instances on the computer and can list detailed information about each instance.
- **idsidrop** removes a directory server instance.

---

## Database configuration and server setup

If you do not set the administrator DN and password or configure the database through the Instance Administration Tool, you can use the Configuration Tool (**idsxcfg**) for these and other tasks. (You must create a directory server instance before you can use the Configuration Tool.)

The Configuration Tool has a GUI, and it can be used for the following tasks:

- Setting or changing the IBM Tivoli Directory Server administrator DN and password
- Configuring and unconfiguring the database for a full server instance
- Enabling and disabling the changelog
- Adding or removing suffixes
- Adding schema files to or removing schema files from the list of schema files to be loaded at startup
- Importing and exporting LDAP Data Interchange Format (LDIF) data
- Backing up, restoring, and optimizing the database

If you prefer to use the command line, all the tasks in the list can be done with the following command-line utilities.

- **idsdnpw** sets the administrator DN and password for a directory server instance.
- **idscfgdb** configures the database for a directory server instance. (The database is created when you create the directory server instance.)
- **idsucfgdb** unconfigures the database for a directory server instance.
- **idscfgchlg** configures the change log for a directory server instance.
- **idsucfgchlg** unconfigures the change log for a directory server instance.
- **idscfgsuf** configures a suffix for a directory server instance.
- **idsucfgsuf** unconfigures a suffix for a directory server instance.
- **idscfgsch** configures a schema file for a directory server instance.
- **idsucfgsch** unconfigures a schema file for a directory server instance.
- **idsldif2db** or **idsbulkload** imports LDIF data.
- **idsdb2ldif** exports LDIF data.
- **idsdbback** backs up the database.
- **idsdbrestore** restores the database.
- **idsrunstats** optimizes the database.

**Note:** For proxy server instances, only the following tasks are available:

- Managing the administrator DN and password in the Configuration Tool (**idsdnpw** command-line utility)
- Managing schema files in the Configuration Tool (**idscfgsch** and **idsucfgsch** command-line utilities)

---

## Chapter 3. System requirements and supported software versions

To install and use IBM Tivoli Directory Server and its related software, your computer must meet the minimum system requirements described in this chapter.

See the *IBM Tivoli Directory Server Version 6.0 Release Notes* for any updated information about supported versions of the operating system and database requirements. (See “Accessing publications online” on page x for information about accessing online publications.)

---

### Requirements that are common to all operating systems

The following are required on all supported operating systems:

#### For the client:

##### Memory

A minimum of 128 MB RAM is required. For better results, use 256 MB or more.

#### For the server:

(These recommendations are based on a directory with 100,000 inetOrgPerson objects, where each entry is approximately 10 KB. Requirements will vary based on your directory and performance responsiveness requirements.):

##### Memory

The following amounts of RAM are recommended for each directory server instance:

- At least 512 MB for each directory server instance. This includes both proxy servers and full servers.

**Note:** If you are running DB2 8.1 on Solaris 9, at least 640 MB of memory is required.

- At least 256 MB for each database instance. (This is not required for a proxy server.)
- At least 256 MB for running the Web Administration Tool and the embedded version of WebSphere Application Server - Express on the same computer.

Add these memory requirements together if you have a full server, the Web Administration Tool, and the embedded version of WebSphere Application Server - Express on the same computer.

##### Disk space

For a full server, IBM Tivoli Directory Server (including the client, the server, and the database) requires about 2 GB of disk space. This might increase based on the number of entries and the size of each entry for your installation.

For information about disk space required for each installable feature for each operating system, see Appendix B, “Disk space requirements for installable features,” on page 167.



The following sections show system requirements for specific supported operating systems.

## Requirements on Windows operating systems

The following table shows the versions of Windows on which IBM Tivoli Directory Server 6.0 is supported.

| Intel 32-bit Windows   |   |
|--|---|
| Operating system version   | 32-bit Directory Server components      |
| Windows 2000 Professional<br>Windows 2000 Server<br>Windows 2000 Advanced Server | Client, Server, Web Administration Tool |
| Windows XP Professional  | Client                                  |
| Windows Server 2003 Standard,<br>Windows Server 2003 Enterprise                  | Client, Server, Web Administration Tool |

The following table shows the supported versions of related software. Versions that are provided with IBM Tivoli Directory Server 6.0 are marked with an asterisk (\*).

| Intel 32-bit Windows   |   |  |  |  |
|--|---|--|--|--|
| Version  | Browser   | IBM Network Authentication System (NAS) (Kerberos) | embedded version of WebSphere Application Server - Express or WebSphere Application Server | DB2 Universal Database Enterprise Server Edition (ESE)   |
| Windows 2000 Professional<br>Windows 2000 Server<br>Windows 2000 Advanced Server<br>Windows Server 2003 Standard<br>Windows Server 2003 Enterprise | Internet Explorer 5.5+, 6.x; Mozilla 1.6, 1.7, 1.75 (Firefox 1.0) | NAS client 1.4.0.2 for Windows *                   | 5.1.1 * (embedded version is provided), 6.0  | 8 Fix Pack 1<br>8 Fix Pack 2<br>8 Fix Pack 3<br>8 Fix Pack 4<br>8 Fix Pack 5<br>8 Fix Pack 6a<br>8 Fix Pack 6b<br>8 Fix Pack 8 refresh * |
| Windows XP Professional  | Internet Explorer 5.5+, 6.x; Mozilla 1.6, 1.7, 1.75 (Firefox 1.0) | NAS client 1.4.0.2 for Windows *                   | N/A  | N/A  |

### Notes:

1. Not all Fix Pack levels of DB2 are supported. Check the list carefully to be sure that the Fix Pack level you are using is supported.
2. The Web browser is required on the computer from which you will use the Web Administration Tool. (This might or might not be the computer where the Web Administration Tool is installed).
3. The application server is required on the computer where the Web Administration Tool is installed. The application server is not required for the client or the server.

In addition:

### Other software



- GSKit 7.0.3.3 is provided and is the only supported version of GSKit. To use GSKit, the IBM JDK 1.4.2 or an equivalent JDK is required.
- Java 1.4.2 (runtime only) is provided.
- If you acquire IBM Tivoli Directory Server through Passport Advantage, it includes a copy of IBM Tivoli Directory Integrator 6.0 with Fix Pack 1 for limited use with IBM Tivoli Directory Server 6.0. (Installation instructions are included with the package.)
- It is important that you install any operating system requirements that are necessary for the version of DB2 that you are using. For DB2 requirements, go to the following Web address:  
<http://www.ibm.com/software/data/db2/udb/sysreqs.html>

**Other hardware**

Before installing, be sure that you have at least 100 MB of free space in the directory specified by the TEMP environment variable or the directory you want to use as a temporary directory.

---

## Requirements on AIX operating systems

The following table shows the versions of AIX on which IBM Tivoli Directory Server 6.0 is supported.

| AIX on pSeries (64-bit/32-bit)   |   |   |                                   |
|--|---|---|-----------------------------------|
| Operating system version   | 64-bit Directory Server components      | 32-bit Directory Server components                  | 32-bit on 64-bit operating system |
| AIX 5.1 (Maintenance Level 7 or higher maintenance level for client or server) | Client, Server, Web Administration Tool | Client (operating system utility installation only) | N/A                               |
| AIX 5.2 (Maintenance Level 5 or higher maintenance level for client or server) | Client, Server, Web Administration Tool | Client (operating system utility installation only) | N/A                               |
| AIX 5.3 (Maintenance Level 1 or higher maintenance level for client or server) | Client, Server, Web Administration Tool | Client (operating system utility installation only) | N/A                               |

**Note:** If you installed maintenance levels and have nothing else to install (such as locale-specific requirements), after you apply all the services that you need for your system, restart your system to enable the changes.

The following table shows the supported versions of related software. Versions that are provided with IBM Tivoli Directory Server 6.0 are marked with an asterisk (\*).

| AIX on pSeries (64-bit/32-bit)  |                                      |  |  |   |
|---|--------------------------------------|--|--|---|
| Version   | Browser                              | IBM Network Authentication System (NAS) (Kerberos) | embedded version of WebSphere Application Server - Express or WebSphere Application Server | DB2 Universal Database Enterprise Server Edition (ESE)  |
| AIX 5.1 (Maintenance Level 7 or higher maintenance level)<br>AIX 5.2 (Maintenance Level 5 or higher maintenance level)<br>AIX 5.3 (Maintenance Level 1 or higher maintenance level) | Mozilla 1.6, 1.7, 1.75 (Firefox 1.0) | NAS client 1.4 for AIX                             | 5.1.1 * (embedded version is provided), 6.0  | 8 Fix Pack 3<br>8 Fix Pack 4<br>8 Fix Pack 5<br>8 Fix Pack 6a<br>8 Fix Pack 6b<br>8 Fix Pack 7a<br>8 Fix Pack 8 refresh * |

**Notes:**

1. Not all Fix Pack levels of DB2 are supported. Check the list carefully to be sure that the Fix Pack level you are using is supported.
2. For maintenance levels of AIX, go to the following Web address:  
<http://www.ibm.com/servers/eserver/support/pseries/aixfixes.html>.
3. The Web browser is required on the computer from which you will use the Web Administration Tool. (This might or might not be the computer where the Web Administration Tool is installed).
4. The application server is required on the computer where the Web Administration Tool is installed. The application server is not required for the client or the server.
5. On AIX 5.3, IBM NAS (Kerberos) 1.4 is provided on the AIX operating system CDs.
6. IBM Tivoli Directory Server 6.0 is designed and tested to be used on 64-bit hardware and running on a 64-bit kernel for optimal performance. IBM Tivoli Directory Server 6.0 supports running on AIX operating systems with the IBM Tivoli Directory Server 6.0 64-bit binaries on a 32-bit kernel on 64-bit hardware. You can install the 64-bit binaries on a 32-bit kernel on 64-bit hardware only by using operating system utilities such as **installp** or SMIT. Installation through the InstallShield GUI is not supported and will not work on a 32-bit kernel..

In addition:

**Other software**

- The Korn shell is required.
- GSKit 7.0.3.3 is provided and is the only supported version of GSKit. To use GSKit, the IBM JDK 1.4.2 or an equivalent JDK is required.
- On AIX 5.1, 5.2, and 5.3 the xIC.aix50rte 6.0.0.0 or later fileset is required for GSKit 7.0.3.3.
- Java 1.4.2 (runtime only) is provided.
- If you acquire IBM Tivoli Directory Server through Passport Advantage, it includes a copy of IBM Tivoli Directory Integrator 6.0 with Fix Pack 1 for limited use with IBM Tivoli Directory Server 6.0. (Installation instructions are included with the package.)
- It is important that you install any operating system requirements that are necessary for the version of DB2 that you are using. For DB2

requirements, go to the following Web address:  
<http://www.ibm.com/software/data/db2/udb/sysreqs.html>

- For the server or 64-bit client, you must be running a 64-bit kernel. To verify that you have the 64 bit kernel (/usr/lib/boot/unix\_64) installed and running, run the following command:

```
bootinfo -K
```

**Note:** If the hardware is 32-bit, then you can only have a 32-bit kernel; you cannot have a 64-bit kernel. If the hardware is 64-bit, then you can have either a 32 or 64-bit kernel

#### Other hardware

- If you plan to use the InstallShield GUI to install, be sure that you have at least 100 MB of free space in the /var directory and one of the following:

- At least 100 MB in the /tmp directory if installing only the client
- At least 400 MB in the /tmp directory if installing a server

- For a server or 64-bit client, you must be running on 64-bit hardware. To verify that your AIX hardware is 64-bit, run the following command:

```
bootinfo -y
```

If the command returns 32, your hardware is 32-bit.

In addition, if you type the command `lsattr -El proc0`, the output of the command returns the type of processor for your server. If you have any of the following, you have 64-bit hardware: RS64 I, II, III, IV, POWER3, POWER3 II, POWER4, or PowerPC\_POWER5 (for AIX 5.2 and 5.3).

**Other** For a server, be sure that asynchronous I/O is turned on.

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.

---

## Requirements on xSeries Linux operating systems

The following table shows the versions of xSeries Linux on which IBM Tivoli Directory Server 6.0 is supported.

| xSeries Linux (32-bit)   |  |
|--|--|
| Operating system version   | 32-bit Directory Server components   |
| Red Hat Enterprise Linux AS 3.0, Update 1, 2, 3, or 4<br>Red Hat Enterprise Linux ES 3.0, Update 1, 2, 3, or 4<br>SuSE Linux Enterprise Server 9 | Client, Server, Web Administration Tool  |
| SuSE Linux Enterprise Server 8   | Client, Full server, Web Administration Tool. (You must install the proxy server if you install the full server. However, using the proxy server as a proxy server is not supported on this operating system.) |

The following table shows the supported versions of related software. Versions that are provided with IBM Tivoli Directory Server 6.0 are marked with an asterisk (\*).

| xSeries Linux (32-bit)   |                                      |  |  |   |
|--|--------------------------------------|--|--|---|
| Version  | Browser                              | IBM Network Authentication System (NAS) (Kerberos) | embedded version of WebSphere Application Server - Express or WebSphere Application Server | DB2 Universal Database Enterprise Server Edition (ESE)                                    |
| Red Hat Enterprise Linux AS 3.0, Update 1, 2, 3, or 4<br>Red Hat Enterprise Linux ES 3.0, Update 1, 2, 3, or 4 | Mozilla 1.6, 1.7, 1.75 (Firefox 1.0) | N/A  | 5.1.1 * (embedded version is provided), 6.0  | 8 Fix Pack 5<br>8 Fix Pack 6a<br>8 Fix Pack 6b<br>8 Fix Pack 7a<br>8 Fix Pack 8 refresh * |
| SuSE Linux Enterprise Server 8   | Mozilla 1.6, 1.7, 1.75 (Firefox 1.0) | N/A  | 5.1.1 * (embedded version is provided), 6.0  | 8 Fix Pack 5<br>8 Fix Pack 6a<br>8 Fix Pack 6b<br>8 Fix Pack 7a<br>8 Fix Pack 8 refresh * |
| SuSE Linux Enterprise Server 9   | Mozilla 1.6, 1.7, 1.75 (Firefox 1.0) | N/A  | 5.1.1 * (embedded version is provided), 6.0  | 8 Fix Pack 8 refresh *  |

**Notes:**

1. Not all Fix Pack levels of DB2 are supported. Check the list carefully to be sure that the Fix Pack level you are using is supported.
2. The Web browser is required on the computer from which you will use the Web Administration Tool. (This might or might not be the computer where the Web Administration Tool is installed).
3. The application server is required on the computer where the Web Administration Tool is installed. The application server is not required for the client or the server.

In addition:

**Other software**

- The Korn shell, provided in the pdksh rpm package for your version of Linux, is required. Install the most recent version for your operating system.
- If you want to install the client or a server on Red Hat versions of Linux, you must install the following packages, which are included with the operating system, before you install IBM Tivoli Directory Server:
  - compat-gcc
  - compat-gcc-c++
  - compat-libstdc++
  - compat-libstdc++-devel
  - glibc-devel
  - glibc-headers
  - glibc-kernheaders

If you want to install the Java client or a server on Red Hat Enterprise Linux AS 3.0, you must install the following packages before you install IBM Tivoli Directory Server:

- compat-gcc-7.3-2.96.128.i386.rpm

- compat-libstdc++-7.3-2.96.128.i386.rpm
- compat-libstdc++-devel-7.3-2.96.128.i386.rpm
- compat-gcc-c++-7.3-2.96.128.i386.rpm

**Note:** You might need to upgrade to the latest patch level of these packages. See the Red Hat support site at <http://rhn.redhat.com> for patches for Red Hat Enterprise Linux.

- GSKit 7.0.3.3 is provided and is the only supported version of GSKit. To use GSKit, the IBM JDK 1.4.2 or an equivalent JDK is required.
- Java 1.4.2 (runtime only) is provided.
- If you acquire IBM Tivoli Directory Server through Passport Advantage, it includes a copy of IBM Tivoli Directory Integrator 6.0 with Fix Pack 1 for limited use with IBM Tivoli Directory Server 6.0. (Installation instructions are included with the package.)
- It is important that you install any operating system requirements that are necessary for the version of DB2 that you are using. For DB2 requirements, go to the following Web address:  
<http://www.ibm.com/software/data/db2/udb/sysreqs.html>
- If you want to use the **idsupport** tool to gather device information for problem determination, you must install the procinfo package.

#### Other hardware

- If you plan to use the InstallShield GUI to install, be sure that you have at least 100 MB of free space in the /var directory and one of the following:
  - At least 100 MB in the /tmp directory (or the directory you want to use as a temporary directory) if installing only the client
  - At least 400 MB in the /tmp directory (or the directory you want to use as a temporary directory) if installing a server

## Requirements on zSeries Linux operating systems

The following table shows the versions of zSeries Linux on which IBM Tivoli Directory Server 6.0 is supported.

| zSeries Linux (31-bit and 64-bit)   |   |  |
|---|---|--|
| Operating system version  | 64-bit Directory Server components                  | 31-bit Directory Server components   |
| <b>zSeries Linux (31-bit) operating system version</b>  |   |  |
| Red Hat Enterprise Linux AS 3.0, Update 1, 2, 3, or 4<br>SuSE Linux Enterprise Server 9                                   | N/A   | Client, Server, Web Administration Tool  |
| SuSE Linux Enterprise Server 8  |   | Client, Full server, Web Administration Tool. (You must install the proxy server if you install the full server. However, using the proxy server as a proxy server is not supported on this operating system.) |
| <b>zSeries Linux (64-bit) operating system version</b>  |   |  |
| Red Hat Enterprise Linux AS 3.0, Update 1, 2, 3, or 4<br>SuSE Linux Enterprise Server 8<br>SuSE Linux Enterprise Server 9 | Client (operating system utility installation only) | N/A  |

The following table shows the supported versions of related software. Versions that are provided with IBM Tivoli Directory Server 6.0 are marked with an asterisk (\*).

| <b>zSeries Linux</b>                                   |                |   |   |   |
|--|----------------|---|---|---|
| <b>Version</b>   | <b>Browser</b> | <b>IBM Network Authentication System (NAS) (Kerberos)</b> | <b>embedded version of WebSphere Application Server - Express or WebSphere Application Server</b> | <b>DB2 Universal Database Enterprise Server Edition (ESE)</b>                             |
| <b>zSeries Linux (31-bit) operating system version</b> |                |   |   |   |
| Red Hat Enterprise Linux AS 3.0, Update 1, 2, 3, or 4  | None           | N/A   | 5.1.1 * (embedded version is provided), 6.0   | 8 Fix Pack 5<br>8 Fix Pack 6a<br>8 Fix Pack 6b<br>8 Fix Pack 7a<br>8 Fix Pack 8 refresh * |
| SuSE Linux Enterprise Server 8                         | None           | N/A   | 5.1.1 * (embedded version is provided), 6.0   | 8 Fix Pack 5<br>8 Fix Pack 6a<br>8 Fix Pack 6b<br>8 Fix Pack 7a<br>8 Fix Pack 8 refresh * |
| SuSE Linux Enterprise Server 9                         | None           | N/A   | 5.1.1 * (embedded version is provided), 6.0   | 8 Fix Pack 8 refresh *  |

**Notes:**

1. Not all Fix Pack levels of DB2 are supported. Check the list carefully to be sure that the Fix Pack level you are using is supported.
2. No Web browsers are supported for the Web Administration Tool on computers running zSeries Linux operating systems. (This means that you must use the Web Administration Tool from a browser on a different computer, using a supported operating system).
3. The application server is required on the computer where the Web Administration Tool is installed. The application server is not required for the client or the server.

In addition:

**Other software**

- The Korn shell, provided in the pdksh rpm package for your version of Linux, is required. Install the most recent version for your operating system.
- On 31-bit versions only, GSKit 7.0.3.3 is provided and is the only supported version of GSKit. To use GSKit, the IBM JDK 1.4.2 or an equivalent JDK is required.
- Java 1.4.2 (runtime only) is provided on 31-bit versions only.
- If you want to install the client or a server on Red Hat versions of Linux, you must install the following packages, which are included with the operating system, before you install IBM Tivoli Directory Server:
  - compat-gcc
  - compat-gcc-c++
  - compat-libstdc++
  - compat-libstdc++
  - glibc-devel

glibc-headers  
glibc-kernheaders

**Note:** You might need to upgrade to the latest patch level of these packages. See the Red Hat support site at <http://rhn.redhat.com> for patches for Red Hat Enterprise Linux.

- On 31-bit versions only, if you acquire IBM Tivoli Directory Server through Passport Advantage, it includes a copy of IBM Tivoli Directory Integrator 6.0 with Fix Pack 1 for limited use with IBM Tivoli Directory Server 6.0. (Installation instructions are included with the package.)
- It is important that you install any operating system requirements that are necessary for the version of DB2 that you are using. For DB2 requirements, go to the following Web address:  
<http://www.ibm.com/software/data/db2/udb/sysreqs.html>
- If you want to use the **idsupport** tool to gather device information for problem determination, you must install the procinfo package.

#### Other hardware

- If you plan to use the InstallShield GUI to install, be sure that you have at least 100 MB of free space in the /var directory and one of the following:
  - At least 100 MB in the /tmp directory (or the directory you want to use as a temporary directory) if installing only the client
  - At least 400 MB in the /tmp directory (or the directory you want to use as a temporary directory) if installing a server

---

## Requirements on iSeries and pSeries Linux operating systems

The following table shows the versions of iSeries and pSeries Linux on which IBM Tivoli Directory Server 6.0 is supported.

| iSeries and pSeries Linux (64-bit)                    |   |   |  |
|---|---|---|--|
| Operating system version                              | 64-bit Directory Server components                  | 32-bit Directory Server components      | 32-bit on 64-bit operating system  |
| Red Hat Enterprise Linux AS 3.0, Update 1, 2, 3, or 4 | Client (operating system utility installation only) | Client, Server, Web Administration Tool | Client, Server, Web Administration Tool  |
| SuSE Linux Enterprise Server 8                        | N/A   | Client, Server, Web Administration Tool | Client, Full server, Web Administration Tool. (You must install the proxy server if you install the full server. However, using the proxy server as a proxy server is not supported on this operating system.) |
| SuSE Linux Enterprise Server 9                        | Client (operating system utility installation only) | Client, Server, Web Administration Tool | Client, Server, Web Administration Tool  |

The following table shows the supported versions of related software. Versions that are provided with IBM Tivoli Directory Server 6.0 are marked with an asterisk (\*).



| iSeries and pSeries Linux (64-bit)                    |         |  |  |   |
|---|---------|--|--|---|
| Version   | Browser | IBM Network Authentication System (NAS) (Kerberos) | embedded version of WebSphere Application Server - Express or WebSphere Application Server | DB2 Universal Database Enterprise Server Edition (ESE)                                    |
| Red Hat Enterprise Linux AS 3.0, Update 1, 2, 3, or 4 | None    | N/A  | 5.1.1 * (embedded version is provided), 6.0  | 8 Fix Pack 5<br>8 Fix Pack 6a<br>8 Fix Pack 6b<br>8 Fix Pack 7a<br>8 Fix Pack 8 refresh * |
| SuSE Linux Enterprise Server 8                        | None    | N/A  | 5.1.1 * (embedded version is provided), 6.0  | 8 Fix Pack 5<br>8 Fix Pack 6a<br>8 Fix Pack 6b<br>8 Fix Pack 7a<br>8 Fix Pack 8 refresh * |
| SuSE Linux Enterprise Server 9                        | None    | N/A  | 5.1.1 * (embedded version is provided), 6.0  | 8 Fix Pack 8 refresh *  |

**Notes:**

1. Not all Fix Pack levels of DB2 are supported. Check the list carefully to be sure that the Fix Pack level you are using is supported.
2. No Web browsers are supported for the Web Administration Tool on computers running iSeries and pSeries Linux operating systems. (This means that you must use the Web Administration Tool from a browser on a different computer, using a supported operating system).
3. The application server is required on the computer where the Web Administration Tool is installed. The application server is not required for the client or the server.

In addition:

**Other software**

- The Korn shell, provided in the pdksh rpm package for your version of Linux, is required. Install the most recent version for your operating system.
- GSKit 7.0.3.3 is provided and is the only supported version of GSKit. To use GSKit, the IBM JDK 1.4.2 or an equivalent JDK is required.
- Java 1.4.2 (runtime only) is provided.
- If you want to install the client or a server on Red Hat versions of Linux, you must install the following packages, which are included with the operating system, before you install IBM Tivoli Directory Server:
  - compat-gcc
  - compat-gcc-c++
  - compat-libstdc++
  - compat-libstdc++
  - glibc-devel
  - glibc-headers
  - glibc-kernheaders

**Note:** You might need to upgrade to the latest patch level of these packages. See the Red Hat support site at <http://rhn.redhat.com> for patches for Red Hat Enterprise Linux.



- If you acquire IBM Tivoli Directory Server through Passport Advantage, it includes a copy of IBM Tivoli Directory Integrator 6.0 with Fix Pack 1 for limited use with IBM Tivoli Directory Server 6.0. (Installation instructions are included with the package.)
- It is important that you install any operating system requirements that are necessary for the version of DB2 that you are using. For DB2 requirements, go to the following Web address:  
<http://www.ibm.com/software/data/db2/udb/sysreqs.html>
- If you want to use the **idssupport** tool to gather device information for problem determination, you must install the procinfo package.

#### Other hardware

- If you plan to use the InstallShield GUI to install, be sure that you have at least 100 MB of free space in the /var directory and one of the following:
  - At least 100 MB in the /tmp directory (or the directory you want to use as a temporary directory) if installing only the client
  - At least 400 MB in the /tmp directory (or the directory you want to use as a temporary directory) if installing a server

---

## Requirements on Solaris operating systems

The following table shows the versions of Solaris on which IBM Tivoli Directory Server 6.0 is supported.

**Note:** Trusted Solaris is not supported.

| Solaris (64-bit)         |   |   |   |
|--------------------------|---|---|---|
| Operating system version | 64-bit Directory Server components                  | 32-bit Directory Server components      | 32-bit on 64-bit operating system       |
| Solaris 8                | Client (operating system utility installation only) | Client, Server, Web Administration Tool | Client, Server, Web Administration Tool |
| Solaris 9                | Client (operating system utility installation only) | Client, Server, Web Administration Tool | Client, Server, Web Administration Tool |

The following table shows the supported versions of related software. Versions that are provided with IBM Tivoli Directory Server 6.0 are marked with an asterisk (\*).

| Solaris (64-bit) |                                      |  |  |   |
|------------------|--------------------------------------|--|--|---|
| Version          | Browser                              | IBM Network Authentication System (NAS) (Kerberos) | embedded version of WebSphere Application Server - Express or WebSphere Application Server | DB2 Universal Database Enterprise Server Edition (ESE)  |
| Solaris 8        | Mozilla 1.6, 1.7, 1.75 (Firefox 1.0) | N/A  | 5.1.1 * (embedded version is provided), 6.0  | 8 Fix Pack 1<br>8 Fix Pack 2<br>8 Fix Pack 3<br>8 Fix Pack 4<br>8 Fix Pack 5<br>8 Fix Pack 6a<br>8 Fix Pack 6b<br>8 Fix Pack 7a<br>8 Fix Pack 8 refresh * |
| Solaris 9        | Mozilla 1.6, 1.7, 1.75 (Firefox 1.0) | N/A  | 5.1.1 * (embedded version is provided), 6.0  | 8 Fix Pack 1<br>8 Fix Pack 2<br>8 Fix Pack 3<br>8 Fix Pack 4<br>8 Fix Pack 5<br>8 Fix Pack 6a<br>8 Fix Pack 6b<br>8 Fix Pack 7a<br>8 Fix Pack 8 refresh * |

**Notes:**

1. Not all Fix Pack levels of DB2 are supported. Check the list carefully to be sure that the Fix Pack level you are using is supported.
2. The Web browser is required on the computer from which you will use the Web Administration Tool. (This might or might not be the computer where the Web Administration Tool is installed).
3. The application server is required on the computer where the Web Administration Tool is installed. The application server is not required for the client or the server.

In addition:

**Other software**

- The Korn shell is required.
- GSKit 7.0.3.3 is provided and is the only supported version of GSKit. To use GSKit, the following are required:
  - On Solaris 8, the following patches are required: 108434-14, 111327- 05, 108991, 108993- 31, 108528-29, 113648-03, 116602- 01,111317-05, 111023-03, 115827- 01
  - On Solaris 9, the following patch is required for the gsk runtime: 111711-08.
  - The IBM JDK 1.4.2 or an equivalent JDK is required. Patches are required for the Java™ 2 Runtime Environment, v 1.4.2.  
To obtain patches, see the SunSolve support Web site at:  
<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE>.  
Also see <http://java.sun.com/j2se/1.3/font-requirements.html> for information about which font packages should be on your system.
- Java 1.4.2 (runtime only) is provided.

- If you acquire IBM Tivoli Directory Server through Passport Advantage, it includes a copy of IBM Tivoli Directory Integrator 6.0 with Fix Pack 1 for limited use with IBM Tivoli Directory Server 6.0. (Installation instructions are included with the package.)
- Ensure that the code page conversion routines (en\_US.UTF-8 1.0) are installed.
- It is important that you install any operating system requirements that are necessary for the version of DB2 that you are using. For DB2 requirements, go to the following Web address:  
<http://www.ibm.com/software/data/db2/udb/sysreqs.html>

#### Other hardware

- If you plan to use the InstallShield GUI to install, be sure that you have at least 100 MB of free space in the /var directory and one of the following:
  - At least 100 MB in the /tmp directory (or the directory you want to use as a temporary directory) if installing only the client
  - At least 400 MB in the /tmp directory (or the directory you want to use as a temporary directory) if installing a server

## Requirements on HP-UX operating systems

The following table shows the versions of HP-UX on which IBM Tivoli Directory Server 6.0 is supported.

| HP-UX PA-RISC (64-bit)   |                                    |   |   |
|--------------------------|------------------------------------|---|---|
| Operating system version | 64-bit Directory Server components | 32-bit Directory Server components      | 32-bit on 64-bit operating system       |
| HP-UX 11i                | None                               | Client, Server, Web Administration Tool | Client, Server, Web Administration Tool |

The following table shows the supported versions of related software. Versions that are provided with IBM Tivoli Directory Server 6.0 are marked with an asterisk (\*).

| HP-UX PA-RISC |                                      |  |  |  |
|---------------|--------------------------------------|--|--|--|
| Version       | Browser                              | IBM Network Authentication System (NAS) (Kerberos) | embedded version of WebSphere Application Server - Express or WebSphere Application Server | DB2 Universal Database Enterprise Server Edition (ESE)   |
| HP-UX 11i     | Mozilla 1.6, 1.7, 1.75 (Firefox 1.0) | N/A  | 5.1.1 * (embedded version is provided), 6.0  | 8 Fix Pack 1<br>8 Fix Pack 2 refresh *<br>8 Fix Pack 3<br>8 Fix Pack 4<br>8 Fix Pack 5<br>8 Fix Pack 6a<br>8 Fix Pack 6b |

#### Notes:

1. Not all Fix Pack levels of DB2 are supported. Check the list carefully to be sure that the Fix Pack level you are using is supported.

2. The Web browser is required on the computer from which you will use the Web Administration Tool. (This might or might not be the computer where the Web Administration Tool is installed).
3. The application server is required on the computer where the Web Administration Tool is installed. The application server is not required for the client or the server.

In addition:

**Other software**

- The Korn shell is required.
- GSKit 7.0.3.3 is provided and is the only supported version of GSKit. To use GSKit on HP-UX 11i, patch PHSS\_26945 is required for the gsk runtime.
- Java 1.4.2 (runtime only) is provided. The following operating system patches are required.
  1. Quality pack: GOLDBASE11i December 2003
  2. Additional patches that are not part of the quality pack. These, or anything that supersedes them:
    - PHKL\_25468
    - PHKL\_25842
    - PHNE\_29887
    - PHCO\_29960
    - PHSS\_30049
- If you acquire IBM Tivoli Directory Server through Passport Advantage, it includes a copy of IBM Tivoli Directory Integrator 6.0 with Fix Pack 1 for limited use with IBM Tivoli Directory Server 6.0. (Installation instructions are included with the package.)
- For the server, be sure to set the current kernel configuration parameters. See “Setting the kernel configuration parameters” on page 92 for the required parameters.
- It is important that you install any operating system requirements that are necessary for the version of DB2 that you are using. For DB2 requirements, go to the following Web address:  
<http://www.ibm.com/software/data/db2/udb/sysreqs.html>

---

## Chapter 4. Migration from previous releases

*Migration* refers to the process of installing IBM Tivoli Directory Server version 6.0 to replace an earlier version while preserving the data, changes that were made to the schema definitions, and directory server configuration from the earlier version. Use the procedures in this chapter when you are migrating an existing directory server on the same physical computer from a version of SecureWay Directory, IBM Directory Server, or IBM Tivoli Directory Server.

If you have only a client installed, see “About the client” for important information about Java applications.

If you are migrating from SecureWay Directory, see “Migration from SecureWay Directory” on page 24.

If you are migrating from IBM Directory Server 4.1, 5.1, 5.1 for Linux iSeries and pSeries, or IBM Tivoli Directory Server 5.2, see one of the following sections:

- For non-AIX systems or AIX systems with IBM Tivoli Directory Server 5.2, see “Migration from IBM Directory Server 4.1 or 5.1 on non-AIX systems or IBM Tivoli Directory Server 5.2 on all systems” on page 29.
- For AIX systems with versions other than IBM Tivoli Directory Server 5.2, see “Migration from IBM Directory Server version 4.1 or 5.1 on AIX systems” on page 31.

---

### About the client

If you have only a client installed, migration is generally not necessary. However, if you are migrating from a release prior to IBM Directory Server 4.1 and you have Java applications that use the IBM JNDI JAR files, the JAR files will be removed during installation; therefore, save them before you install IBM Tivoli Directory Server 6.0.

To save the files:

- Save files, including any subdirectories, in the *installpath*\jre\bin directory to a temporary directory that you choose.
- Save files, including any subdirectories, in the *installpath*\jre\lib directory to a temporary directory that you choose.

JNDI-related files are:

- Ibmjcefw.jar
- Ibmjceprovider.jar
- IBMjgssprovider.jar
- Local\_policy.jar
- US\_export\_policy.jar
- Krb5.ini
- Ibmjndi.jar
- Ibmjndi.zip

Starting with IBM Directory Server 4.1, IBM JNDI is not supported. IBM Directory Server 4.1, 5.1, and 5.1 for Linux iSeries and pSeries, IBM Tivoli Directory Server

5.2, and IBM Tivoli Directory Server 6.0 include the Sun Microsystems JNDI. See the Sun documentation for information about the Sun JNDI. There might be some functional differences between IBM and Sun implementations that require changes to existing JNDI applications. IBM JNDI applications might still run, but for reliable results, begin using the Sun JNDI immediately.

---

## Location of migration utilities

There are two migration utilities used in the migration procedures in this chapter: **migbkup** and **idswmigr**. You can find these utilities in one of the following locations:

### For Windows systems:

If you created a CD: the \tools subdirectory on the CD

If you downloaded a .zip file, the itdsV60\tools subdirectory of the directory where you unzipped the file

### For AIX, Linux, Solaris, and HP-UX systems:

If you created a CD for InstallShield GUI installation: the /tools subdirectory on the CD

If you created a CD for installation with operating system utilities: the /tools subdirectory on the CD

If you downloaded a .tar file for InstallShield GUI installation: the itdsV60ismp/tools subdirectory of the directory where you untarred the file

If you downloaded a .tar file for installation with operating system utilities: the itdsV60/tools subdirectory of the directory where you untarred the file

---

## Migration from SecureWay Directory

The version of SecureWay Directory you are migrating must be 3.2.2 or higher. If you have a SecureWay Directory version that is less than 3.2.2 currently installed, you must upgrade to version 3.2.2 before installing IBM Tivoli Directory Server 6.0. You can download SecureWay Directory version 3.2.2 from the IBM Directory Web page: <http://www.ibm.com/software/sysmgmt/products/support/IBMDirectoryServer.html>

To migrate from the 3.2.2 version of SecureWay Directory, use the following procedure:

### Pre-installation steps:

1. If you have not done so already:
  - a. Export the database using **db2ldif**:  
`db2ldif -o ldiffile`

where *ldiffile* specifies the LDIF output file to contain the directory entries in LDIF format.

For more information about the **db2ldif** command, read the **db2ldif** documentation in the *SecureWay Administration Guide* for version 3.2.2 before exporting the database. Databases must not be unconfigured or dropped unless they have been backed up using the 3.2.2 version of **db2ldif**. Failure to comply with this results in a complete loss of data.

Data contained in the SecureWay Directory 3.2.2 database is not compatible with IBM Tivoli Directory Server 6.0 unless it is exported using the 3.2.2 version of **db2ldif** and imported through the **idsbulkload** utility provided with IBM Tivoli Directory Server 6.0.

**Attention:** Do not use the **DB2BACKUP** command to export your data. If you do not export using **db2ldif** before unconfiguring and removing the database, you will lose your data.

- b. Unconfigure and remove the database by typing the following at a command prompt:

```
ldapucfg -d
```

Type **y** to confirm the removal. Default LDAP databases and instances are automatically removed from the system when the command successfully completes. (If your database instance name and your database name are both **ldapdb2**, you have a default database configured.)

If you use a custom database, you must manually remove the DB2 database from the system.

**Notes:**

- 1) The server will not start if you do not migrate the database.
  - 2) The changes in the changelog database are not compatible with the new data format and cannot be used, and you must also reconfigure the change log.
  - 3) The audit log settings are not migrated. After you install IBM Tivoli Directory Server, you can respecify the settings for the audit log.
2. Back up the configuration files and schema files by using the **migbkup** utility. (See “Location of migration utilities” on page 24 for the location of the **migbkup** utility.) Type the following at a command prompt:

- For Windows systems:

```
migbkup.bat <install_location> <backup_directory> [jndi]
```

- For AIX, Linux, and Solaris systems:

```
migbkup.ksh <install_location> <backup_directory> [jndi]
```

This utility backs up the `slapd32.conf` file and some schema files from the `install_location\etc` directory to a temporary directory, specified by `<backup_directory>`. `<install_location>` is the directory where SecureWay Directory is installed. Use the **jndi** option only if you have JNDI-related files that you want the utility to back up.

For example:

- On a Windows system, to back up files from SecureWay Directory, installed in the `C:\Program Files\IBM\LDAP` directory, to a directory named `d:\ldap\savefiles`, where there are no JNDI-related files, type the following:

```
migbkup.bat "C:\Program Files\IBM\LDAP" d:\ldap\savefiles
```

Be sure to enclose the path in quotation marks if there is a space in the path.

- On a Linux system, to back up files from SecureWay Directory, installed in the `/usr/ldap` directory, to a directory named `/usr/savefiles`, where there are JNDI-related files that you want to save, type the following:

```
migbkup.ksh /usr/ldap /usr/savefiles jndi
```

The backed-up files are:

- `slapd32.conf`
- `V3.ibm.at`

- V3.ibm.oc
- V3.system.at
- V3.system.oc
- V3.user.at
- V3.user.oc
- V3.modifiedschema

If you have additional schema files that you used in your previous release, copy them manually to the `<backup_directory>` also. When you migrate the configuration and schema files during instance creation, these files will not be migrated, but they will be copied to the new directory server instance location for use by the directory server instance.

The following JNDI-related files are backed up if they exist and you specified the **jndi** option on the **migbkup** command:

- Files and subdirectories in the `<install_location>/jre/bin` subdirectory
- Files and subdirectories in the `<install_location>/jre/lib` subdirectory
- Ibmjcefw.jar
- Ibmjceprovider.jar
- IBMjgssprovider.jar
- Local\_policy.jar
- US\_export\_policy.jar
- Krb5.ini
- Ibmjndi.jar
- Ibmjndi.zip

**Note:** Starting with IBM Directory Server 4.1, IBM JNDI is not supported. IBM Directory Server 4.1, 5.1, and 5.1 for Linux iSeries and pSeries, IBM Tivoli Directory Server 5.2, and IBM Tivoli Directory Server 6.0 include the Sun Microsystems JNDI. See the Sun documentation for information about the Sun JNDI. There might be some functional differences between IBM and Sun implementations that require changes to existing JNDI applications. IBM JNDI applications might still run, but for reliable results, begin using the Sun JNDI immediately.

3. Uninstall SecureWay Directory Version 3.2.2, using the *IBM SecureWay Directory Version 3.2.2 Installation and Configuration Guide* for your operating system.

**Note:** If you have a version of DB2 that is not supported for IBM Tivoli Directory Server 6.0, you must upgrade to a supported version of DB2. (Be sure that you have exported the database first.) Alternatively, you can remove DB2 after you have exported the database and install the version of DB2 provided with IBM Tivoli Directory Server. On AIX systems, you *must* upgrade to a 64-bit version of DB2. See Chapter 3, “System requirements and supported software versions,” on page 9 for information about supported DB2 versions.

#### Installation steps:

4. If you want to use IBM Tivoli Directory Server 6.0 in a language other than English, install the language pack for your language. See Chapter 5, “Installing language packs using the InstallShield GUI,” on page 45 for instructions.
5. Install IBM Tivoli Directory Server 6.0. To install using the InstallShield GUI, see Chapter 6, “Installing IBM Tivoli Directory Server using the InstallShield



GUI,” on page 47 for instructions. To install using operating system utilities for AIX, Linux, or Solaris platforms, see one of the following chapters:

- For AIX operating systems: Chapter 8, “Installing IBM Tivoli Directory Server using AIX utilities,” on page 65.
- For Linux operating systems: Chapter 9, “Installing IBM Tivoli Directory Server using Linux utilities,” on page 77.
- For Solaris operating systems: Chapter 10, “Installing IBM Tivoli Directory Server using Solaris utilities,” on page 83.

**Post-installation steps:**

6. After installation, you must create a directory server instance and a database instance and configure the database. (The administrator DN and password are preserved from the configuration files you backed up.) You must perform these server setup tasks before you import the data you exported in step 1 on page 24. Use one of the following sets of instructions to perform these:

- If you installed using the InstallShield GUI, the Instance Administration Tool starts automatically. (On Windows systems, your computer might restart before the Instance Administration Tool starts.) In the Instance Administration Tool, do the following:
  - a. On the first window, click **Create**.
  - b. On the Create a new directory server instance window, click **Migrate from a pre-6.0 version of directory server**. Then type the path where you backed up the configuration and schema files. Click **Next**.

The Instance Administration Tool prompts you for input to create a directory server instance and a database instance, using your migrated information. Use the Instance Administration Tool also to configure the database. See Chapter 13, “Creating and administering instances,” on page 109 for instructions for using the Instance Administration Tool for these tasks.

- If you did not use the InstallShield GUI to install, use one of the following:
  - To start the Instance Administration Tool, type the following at a command prompt:

```
idsxinst
```

In the Instance Administration Tool, do the following:

- a. On the first window, click **Create**.
- b. On the Create a new directory server instance window, click **Migrate from a pre-6.0 version of directory server**. Then type the path where you backed up the configuration and schema files. Click **Next**.

The Instance Administration Tool prompts you for input to create a directory server instance and a database instance, using your migrated information. Use the Instance Administration Tool also to configure the database. See Chapter 13, “Creating and administering instances,” on page 109 for instructions for using the Instance Administration Tool for these tasks.

- Use the **idsimigr** for command-line migration. See “The command-line migration utility (idsimigr)” on page 40 for information about using the migration utility to migrate your configuration and schema files. After you have migrated, use either the Configuration Tool (see “Using the IBM Tivoli Directory Server Configuration Tool (idsxcfg)” on page 125) or the **idscfgdb** command (see “Using idscfgdb to configure the database” on page 138) to configure the database.

**Notes:**

- a. If you want a change log database, be sure the change log is enabled through the Configuration Tool or by using the **idscfgchglg** utility.
  - b. If you want to use the audit log, you can enable the audit log through the Web Administration Tool or the **idslapmodify** command. See the *IBM Tivoli Directory Server 6.0 Administration Guide* for information.
7. Use the **idsbulkload** utility to import the **idsdb2ldif** exported data, as follows:
- ```
idsbulkload -i ldiffile -I instancename -c -d
```

where *ldiffile* is the name of the input file containing the LDIF data to be loaded into the directory. You created this file in step 1 on page 24. *instancename* is the name of the directory server instance.

**Note:** Read the **idsbulkload** documentation in the *IBM Tivoli Directory Server Version 6.0 Administration Guide* for information about command-line settings that provide additional levels of function.

8. When you start the directory server instance, your DB2 table data is migrated.

---

## High-level migration steps

The information in “Migration from IBM Directory Server 4.1 or 5.1 on non-AIX systems or IBM Tivoli Directory Server 5.2 on all systems” on page 29 and “Migration from IBM Directory Server version 4.1 or 5.1 on AIX systems” on page 31 guides you through the migration process in detailed steps.

You can use the information in this section to understand the order in which you must migrate the database, upgrade DB2 if necessary, upgrade the operating system if necessary, and migrate to IBM Tivoli Directory Server 6.0 from your previous release. A summary of the steps follows.

The migration process is:

1. Prepare the database for migration by backing up and stopping the database.
2. Back up the configuration and schema files for your previous version of IBM Directory Server or IBM Tivoli Directory Server.
3. Uninstall your previous version of IBM Directory Server or IBM Tivoli Directory Server.
4. Upgrade your operating system if necessary.
5. Upgrade your DB2 version if necessary.
6. Install IBM Tivoli Directory Server 6.0.
7. Migrate the database instance and the database.
8. Create a migrated IBM Tivoli Directory Server instance with the information from your previous version.

Use the information in “Migration from IBM Directory Server 4.1 or 5.1 on non-AIX systems or IBM Tivoli Directory Server 5.2 on all systems” on page 29 or “Migration from IBM Directory Server version 4.1 or 5.1 on AIX systems” on page 31 to carry out these steps.

---

## Migration from IBM Directory Server 4.1 or 5.1 on non-AIX systems or IBM Tivoli Directory Server 5.2 on all systems

If you are upgrading from the 4.1 or 5.1 version of IBM Directory Server on a non-AIX system or from IBM Tivoli Directory Server 5.2 on any operating system, use the procedure in this section.

### Pre-installation steps:

1. If you plan to install a newer version of DB2, back up the database and stop the database processes, using the information in “Preparing the database before migration” on page 33.
2. Back up the configuration files and schema files by using the **migbkup** utility. (See “Location of migration utilities” on page 24 for the location of the **migbkup** utility.) Type the following at a command prompt:

- For Windows systems:

```
migbkup.bat install_location backup_directory
```

- For AIX, Linux, Solaris, and HP-UX systems:

```
migbkup.ksh install_location backup_directory
```

This utility backs up the server configuration file (slapd32.conf or ibmslapd.conf) and some schema files from the *install\_location*\etc directory to a temporary directory, specified by *<backup\_directory>*. *<install\_location>* is the directory where IBM Directory Server or IBM Tivoli Directory Server is installed.

For example:

- On a Windows system, to back up files from IBM Directory Server, installed in the C:\Program Files\IBM\LDAP directory, to a directory named d:\ldap\savefiles, type the following:

```
migbkup.bat "C:\Program Files\IBM\LDAP" d:\ldap\savefiles
```

Be sure to enclose the path in quotation marks if there is a space in the path.

- On a Linux system, to back up files from IBM Tivoli Directory Server, installed in the /usr/ldap directory, to a directory named /usr/savefiles, type the following:

```
migbkup.ksh /usr/ldap /usr/savefiles
```

The backed-up files are:

- slapd32.conf or ibmslapd.conf
- V3.ibm.at
- V3.ibm.oc
- V3.system.at
- V3.system.oc
- V3.user.at
- V3.user.oc
- V3.modifiedschema

If you have additional schema files that you used in your previous release, copy them manually to the *backup\_directory* also. When you migrate the configuration and schema files during instance creation, these files will not be migrated, but they will be copied to the new directory server instance location for use by the directory server instance.

3. Uninstall the IBM Directory Server or IBM Tivoli Directory Server features you want to uninstall, using the *Installation and Configuration Guide* for that version.

Do **not** uninstall DB2 even if you are installing a newer version of DB2. See Chapter 3, “System requirements and supported software versions,” on page 9 to determine whether you must install a newer, supported version of DB2.

You can leave the client on the computer if you like; an IBM Directory Server 4.1 or 5.1 client or an IBM Tivoli Directory Server 5.2 client can coexist with IBM Tivoli Directory Server 6.0.

If you have the Web Administration Tool from IBM Directory Server 5.1 or IBM Tivoli Directory Server 5.2 and you want to migrate it, uninstall the Web Administration Tool, but leave the embedded version of WebSphere Application Server - Express with the Web Administration Tool installed into it. (To do this through the InstallShield GUI, select **Web Administration Tool**, but do not select **embedded version of WebSphere Application Server - Express** to be uninstalled.)

#### Installation steps:

4. If you are installing a new version of DB2, install it, using the information in “Replacing or installing a new version of DB2” on page 35.
5. If you want to use IBM Tivoli Directory Server in a language other than English, install the language pack for your language. See Chapter 5, “Installing language packs using the InstallShield GUI,” on page 45 for instructions.
6. Install IBM Tivoli Directory Server 6.0. To install using the InstallShield GUI (not available for HP-UX systems), see Chapter 6, “Installing IBM Tivoli Directory Server using the InstallShield GUI,” on page 47 for instructions. To install using operating system utilities for AIX, Linux, Solaris, and HP-UX platforms, see one of the following chapters:
  - For AIX operating systems: Chapter 8, “Installing IBM Tivoli Directory Server using AIX utilities,” on page 65.
  - For Linux operating systems: Chapter 9, “Installing IBM Tivoli Directory Server using Linux utilities,” on page 77.
  - For Solaris operating systems: Chapter 10, “Installing IBM Tivoli Directory Server using Solaris utilities,” on page 83.
  - For HP-UX operating systems: Chapter 11, “Installing IBM Tivoli Directory Server using HP-UX utilities,” on page 91.

#### Post-installation steps:

7. Migrate your database instance and database, using the information in “Migrating your database instances and databases” on page 36.
8. After installation, you must create a directory server instance. (The administrator DN and password and the database configuration are preserved from the configuration files you backed up.) You must perform this server setup task before you can use the directory server instance. Use one of the following sets of instructions:
  - If you installed using the InstallShield GUI, the Instance Administration Tool starts automatically. (On Windows systems, your computer might restart before the Instance Administration Tool starts.) In the Instance Administration Tool, do the following:
    - a. On the first window, click **Create**.
    - b. On the Create a new directory server instance window, click **Migrate from a pre-6.0 version of directory server**. Then type the path where you backed up the configuration and schema files. Click **Next**.

The Instance Administration Tool prompts you for input to create a directory server instance, using your migrated information. (You do not need to

configure the database if you preserved your data by following all the steps in the procedure.) See Chapter 13, “Creating and administering instances,” on page 109 for instructions.

- If you did not use the InstallShield GUI to install, use one of the following:

- To start the Instance Administration Tool, type the following at a command prompt:

```
idsxinst
```

In the Instance Administration Tool, do the following:

- a. On the first window, click **Create**.
- b. On the Create a new directory server instance window, click **Migrate from a pre-6.0 version of directory server**. Then type the path where you backed up the configuration and schema files. Click **Next**.

The Instance Administration Tool prompts you for input to create a directory server instance, using your migrated information. (You do not need to configure the database if you preserved your data by following all the steps in the procedure.) See Chapter 13, “Creating and administering instances,” on page 109 for instructions.

- Use the **idsimigr** command for command-line migration. See “The command-line migration utility (idsimigr)” on page 40 for information about using the migration utility to migrate your configuration and schema files.

**Note:** If you are migrating from IBM Directory Server 4.1, the audit log settings are not migrated. If you are migrating from IBM Directory Server 5.1 or 5.2, these settings might not be migrated accurately. After you install IBM Tivoli Directory Server, you can check and respecify the settings for the audit log. If you want to use the audit log, you can enable the audit log or modify the audit log settings through the Web Administration Tool or the **idsldapmodify** command. See the *IBM Tivoli Directory Server 6.0 Administration Guide* for information.

When you start the directory server instance, your DB2 table data is migrated.

---

## Migration from IBM Directory Server version 4.1 or 5.1 on AIX systems

This section describes migration from IBM Directory Server 4.1 or 5.1 on AIX. These instructions include directions for migrating DB2 Workgroup Server Edition 8.1, 32-bit, or DB2 Enterprise Server Edition 7.2, 32-bit, to DB2 Enterprise Server Edition 8 Fix Pack 8 refresh, 64-bit.

**Note:** If you have the Web Administration Tool installed from IBM Directory Server 5.1, see “Migrating the Web Administration Tool and upgrading the embedded version of WebSphere Application Server - Express” on page 43 for information.

To migrate from IBM Directory Server 4.1 or 5.1 on AIX:

### Pre-installation steps:

1. Back up the database and stop the database processes, using the information in “Preparing the database before migration” on page 33.
2. Back up the configuration files and schema files by using the **migbkup** utility. (See “Location of migration utilities” on page 24 for the location of the **migbkup** utility.) Type the following at a command prompt:

```
migbkup.ksh install_location backup_directory
```

This utility backs up the slapd32.conf or ibmslapd.conf file and some schema files from the *install\_location*\etc directory to a temporary directory, specified by *backup\_directory*. *install\_location* is the directory where IBM Directory Server is installed.

For example, to back up files from IBM Directory Server, installed in the /usr/ldap directory, to a directory named /usr/savefiles, type the following:

```
migbkup.ksh /usr/ldap /usr/savefiles
```

The backed-up files are:

- slapd32.conf or ibmslapd.conf
- V3.ibm.at
- V3.ibm.oc
- V3.system.at
- V3.system.oc
- V3.user.at
- V3.user.oc
- V3.modifiedschema

If you have additional schema files that you used in your previous release, copy them manually to the *<backup\_directory>* also. When you migrate the configuration and schema files during instance creation, these files will not be migrated, but they will be copied to the new directory server instance location for use by the directory server instance.

3. If you installed IBM Directory Server using the InstallShield GUI, uninstall using the InstallShield GUI. If you installed using operating system utilities such as SMIT, use operating system utilities to uninstall.
4. Upgrade the operating system to the 64-bit version of AIX 5.1, 5.2, or 5.3, using the AIX documentation.
5. Replace DB2 with the newer version, using the instructions in “Replacing or installing a new version of DB2” on page 35.

#### **Installation steps:**

6. Install IBM Tivoli Directory Server 6.0 using the InstallShield GUI or SMIT. See “Installing IBM Tivoli Directory Server on an AIX, Linux, or Solaris system” on page 52 or “SMIT installation” on page 69 for information.
7. If you want to use IBM Tivoli Directory Server in a language other than English, install the language pack for your language. See Chapter 5, “Installing language packs using the InstallShield GUI,” on page 45 or “SMIT installation” on page 69 for instructions.

#### **Post-installation steps:**

**Note:** If you installed using the InstallShield GUI, the Instance Administration Tool starts automatically. Ignore this tool for the moment. Instructions for using the Instance Administration Tool are in step 9.

8. Use the information in “Migrating your database instances and databases” on page 36 to migrate the database and update the database instance to a 64-bit width.
9. After installation, you must create a directory server instance. (The administrator DN and password and the database configuration are preserved



from the configuration files you backed up.) You must perform this server setup task before you can use the directory server instance. Use one of the following sets of instructions:

- If you installed using the InstallShield GUI, the Instance Administration Tool starts automatically. In the Instance Administration Tool, do the following:
  - a. On the first window, click **Create**.
  - b. On the Create a new directory server instance window, click **Migrate from a pre-6.0 version of directory server**. Then type the path where you backed up the configuration and schema files. Click **Next**.

The Instance Administration Tool prompts you for input to create a directory server instance, using your migrated information. (You do not need to configure the database if you preserved your data by following all the steps in the procedure.) See Chapter 13, “Creating and administering instances,” on page 109 for instructions.

- If you did not use the InstallShield GUI to install, use one of the following:
  - To start the Instance Administration Tool, type the following at a command prompt:

```
idsxinst
```

In the Instance Administration Tool, do the following:

- a. On the first window, click **Create**.
- b. On the Create a new directory server instance window, click **Migrate from a pre-6.0 version of directory server**. Then type the path where you backed up the configuration and schema files. Click **Next**.

The Instance Administration Tool prompts you for input to create a directory server instance, using your migrated information. (You do not need to configure the database if you preserved your data by following all the steps in the procedure.) See Chapter 13, “Creating and administering instances,” on page 109 for instructions.

- Use the **idsimigr** command for command-line migration. See “The command-line migration utility (idsimigr)” on page 40 for information about using the migration utility to migrate your configuration and schema files.

**Note:** If you are migrating from IBM Directory Server 4.1, the audit log settings are not migrated. If you are migrating from IBM Directory Server 5.1, these settings might not be migrated accurately. After you install IBM Tivoli Directory Server, you can check and respecify the settings for the audit log. If you want to use the audit log, you can enable the audit log or modify the audit log settings through the Web Administration Tool or the **idsldapmodify** command. See the *IBM Tivoli Directory Server 6.0 Administration Guide* for information.

---

## Database tasks before, during, and after migration

The information in the following sections describes how to prepare your database before migration, install a new version of DB2, and migrate the data.

### Preparing the database before migration

Use the information in this section to prepare the database for migration.

**On Windows systems:**

To prepare the database for migration:

1. Back up the databases and DB2 settings. See the *Administration Guide* for your release of IBM Directory Server or IBM Tivoli Directory Server for information about backing up databases using DB2 commands or the **dbback** command. Take an offline database backup for each local database on the server. These are required to back out of the migration.
2. (This step is optional.) Update the Database Manager configuration to set the diagnostic error level to 4. This captures all errors, warnings, and informational messages during the migration. These messages can be used for problem determination if you encounter errors during migration. Use the following command to set the diagnostic error level:

```
db2 update dbm cfg using diaglevel 4
```

3. Take the database offline. This ensures that all DB2 processes are terminated before migration. Use the following steps to take the database offline:
  - a. Start a DB2 command prompt by typing `db2` at the command line. stop all command line processor sessions by entering the `db2 terminate` command in each session.
  - b. Disconnect all applications and users by using the `db2 force application all` command.
  - c. Stop the DB2 license service by entering the `db2licd -end` command.
  - d. Stop each database manager instance by issuing the `db2stop` command.
  - e. From the Windows Services panel, stop all DB2 services that are running.
  - f. Check the Windows Task Manager to be sure that there are no DB2 processes running.
  - g. Stop the database instance by typing the following:

```
db2stop
exit
```
  - h. Rebind all packages stored in the database using the following command:

```
db2rbind db_alias -l logfile all
```
  - i. Run the following command to check the database status:

```
db2dart database-name /db
```

Check the log file to be sure there are no errors and the command completed successfully.

#### On AIX systems:

To prepare the database for migration:

1. Stop the database instance, as follows:
  - a. Log in as the DB2 instance owner.
  - b. Ensure that there are no applications using any databases owned by this DB2 instance. To get a list of all applications owned by the instance, enter the **db2 list applications** command. You can end a session by entering the **db2 terminate** command. Do not force termination of applications using the **db2 force applications all** command, because some applications might have unexpected behavior when they are terminated using this command. See the *DB2 Command Reference* for detailed information about these commands.
  - c. When all applications are terminated, stop all database server processes owned by the DB2 instance by entering the **db2stop** command.
  - d. Stop the DB2 license daemon by entering the **db2licd end** command.



- e. Stop all command-line processor sessions by entering the **db2 terminate** command in each session that was running the command line processor.
- f. On DB2 7.2 only, enter the **db2\_kill** command to clean up any remaining DB2 resources.
- g. Stop the instance using the **db2istop** command:
  - If your version of DB2 is 8.1:
 

```
/usr/opt/db2_08_01/instance/db2istop InstName
```
  - If your version of DB2 is 7.2:
 

```
/usr/lpp/db2_07_01/instance/db2istop InstName
```
- h. Log off.

#### On Linux, Solaris, and HP-UX systems:

To prepare the database for migration:

1. Stop the database instance, as follows:
2. Log in as the DB2 instance owner.
3. Ensure that there are no applications using any databases owned by this DB2 instance. To get a list of all applications owned by the instance, enter the **db2 list applications** command. You can end a session by entering the **db2 terminate** command. Do not force termination of applications using the **db2 force applications all** command, because some applications might have unexpected behavior when they are terminated using this command. See the *DB2 Command Reference* for detailed information about these commands.
4. When all applications are terminated, stop all database server processes owned by the DB2 instance by entering the **db2stop** command.
5. Stop the DB2 license daemon by entering the **db2licd end** command.
6. Stop all command-line processor sessions by entering the **db2 terminate** command in each session that was running the command line processor.
7. On DB2 7.2 only, enter the **db2\_kill** command to clean up any remaining DB2 resources.
8. Stop the instance using the **db2istop** command:
  - If your version of DB2 is 8.1:
 

```
/opt/IBM/db2/V8.1/instance/db2istop InstName
```

(The **db2istop** command might be in a different location on Solaris and HP-UX systems.)
  - If your version of DB2 is 7.2:
 

```
/usr/IBMDB2/V7.1/instance/db2istop InstName
```

(The **db2istop** command might be in a different location on Solaris and HP-UX systems.)
9. Log off.

## Replacing or installing a new version of DB2

Use the information in this section to install a newer, supported version of DB2.

#### On Windows systems:

To install a supported version of DB2:

- **If your existing version of DB2 is 7.2:**

Install DB2 8.2 Fix Pack 2 on top of DB2 7.2.

- **If your existing version of DB2 is 8.1 WSE Fix Pack 2:**
  1. Install DB2 8.1 WSE Fix Pack 8 on top of DB2 8.1 WSE Fix Pack 2. (You can obtain DB2 8.1 WSE Fix Pack 8 from the IBM Support Web site at <http://www.ibm.com/software/data/db2/udb/support/>.)
  2. Install DB2 8.2 ESE Fix Pack 2 (which is provided with IBM Tivoli Directory Server 6.0) on top of DB2 8.1 WSE Fix Pack 8.

#### On AIX and Linux systems:

To install a supported version of DB2:

- **If your version of DB2 is 8.1:**
  1. Uninstall DB2 Workgroup Server Edition 8.1.
  2. Delete all the IPC objects owned by the *instance\_name* instance, as follows:
    - a. At the command prompt, type:

```
ipcs -a | grep instance_name
```

This displays a list of all object IDs (message queues, shared memory, and semaphores) owned by instance *instance\_name*.
    - b. For each message queue object owned by *instance\_name*, type 

```
ipcrm -q object_id
```

.
    - c. For each semaphore owned by *instance\_name*, type 

```
ipcrm -s object_id
```

.
  3. Install DB2 Enterprise Server Edition 8 Fix Pack 8 refresh.
- **If your version of DB2 is 7.2:**

Install DB2 Enterprise Server Edition 8 Fix Pack 8 refresh on top of DB2 7.2.

## Migrating your database instances and databases

Use the information in this section to migrate database instances and databases during the migration process after you install IBM Tivoli Directory Server 6.0.

#### On Windows systems:

1. Instances are automatically migrated during DB2 installation on Windows. No manual steps are required.
2. To migrate the database:
  - a. Set the DB2INSTANCE environment variable to *instance\_name*. Then type `db2cmd` at a command prompt. From the DB2 command prompt, type:

```
db2  
migrate database
```

#### On AIX systems:

To migrate your database:

- **If your database is DB2 8.1:**
  1. Update the IBM Tivoli Directory Server database instance to a 64-bit width, as follows:
    - a. Log in as **root**.
    - b. Run the **db2iupdt** command as follows:

```
/usr/opt/db2_08_01/instance/db2iupdt -w 64 InstName
```
  2. To migrate the database, type the following at a command prompt:

```
migrate database database_name
```

where *database\_name* is the name of the database.

3. Bind the schema packages, using the following commands:

```
su - database_instance_owner
db2 connect to database_name
db2 update db config using STMTHEAP 50000
db2 update db config using APPLHEAPSZ 4096
cd sqllib/bnd (if you are not already in that directory)
db2 bind db2schema.bnd blocking all grant public
db2 bind db2clipk.bnd blocking all grant public
db2 bind db2clist.bnd blocking all grant public
db2 bind db2ckmig64.bnd blocking all grant public
```

- **If your database is DB2 7.2:**

1. After an instance is ready for migration, use the **db2imigr** command to migrate the instance as follows:
  - a. Log in as a user with root authority.
  - b. If the LIBPATH environment variable is set to /usr/lib and there is a link in /usr/lib to the Version 7 libdb2 shared library, this can cause an error when using the **db2imigr** command. To fix the error, reset the LIBPATH environment variable so that it does not reference the libraries in those paths by entering the following command:

```
unset LIBPATH
```

- c. Run the **db2imigr** command as follows:

```
/usr/opt/db2_08_01/instance/db2imigr [-d] [-a AuthType]
[-u fencedID] InstName
```

where

- **-d** sets the debug mode that you can use for problem determination. This parameter is optional.
- **-a *AuthType*** specifies the authentication type for the instance. Valid authentication types are (SERVER), (CLIENT), and (DCS). If the **-a** parameter is not specified, the authentication type defaults to (SERVER), if a DB2 server is installed. Otherwise, the *AuthType* is set to (CLIENT). This parameter is optional.

**Notes:**

- 1) The authentication type of the instance applies to all databases owned by the instance.
  - 2) While authentication type (DCE) is an optional parameter, it is not valid to choose (DCE) for this command
  - **-u *fencedID*** is the user under which the fenced user-defined functions (UDFs) and stored procedures will execute. This parameter is optional only when a DB2 Run-Time Client is installed. It is required for all other DB2 products.
  - *InstName* is the login name of the instance owner.
2. Convert the DB2 instance to a 64-bit width, using the following procedure:
    - a. Log in as a user with root authority.
    - b. Run the **db2iupdt** command as follows:

```
/usr/opt/db2_08_01/instance/db2iupdt -w 64 InstName
```
    - c. After migrating the DB2 instance, reset LIBPATH to its original setting
  3. Migrate the database owned by the instance, using the following steps:
    - a. Log on with a user ID that has SYSADM authority, such as the instance owner.
    - b. Ensure that the database you want to migrate is cataloged.

- c. Run **db2**.
  - d. At the DB2 command prompt, type the following:
 

```
migrate database DATABASE-NAME
```
4. Bind the schema packages, using the following commands:
- ```
su - database_instance_owner
db2 connect to database_name
db2 update db config using STMHEAP 50000
db2 update db config using APPLHEAPSZ 4096
cd sqllib/bnd (if you are not already in that directory)
db2 bind db2schema.bnd blocking all grant public
db2 bind db2clipk.bnd blocking all grant public
db2 bind db2clist.bnd blocking all grant public
db2 bind db2ckmig64.bnd blocking all grant public
```
5. Initialize the database manager configuration parameter UTIL\_IMPACT\_LIM to its default value. The UTIL\_IMPACT\_LIM configuration parameter did not exist for UDB 7.1 and on migration to Enterprise Server Edition 8.1 it is assigned a value of 0. The valid range for this parameter is 1 to 100. Use the following procedure:
- a. Log on with a user ID that has SYSADM authority.
  - b. Run **db2**.
  - c. At the DB2 command prompt, type the following:
 

```
update database manager configuration using UTIL_IMPACT_LIM value
```

*value* should be kept low: between 1 and 10.

#### On Linux systems:

To migrate your database:

- **If your database is DB2 8.1:**
  1. Update the IBM Tivoli Directory Server database instance, as follows:
    - a. Log in as root.
    - b. Run the db2iupdt command as follows:
 

```
/opt/IBM/db2/V8.1/instance/db2iupdt InstName
```
  2. To migrate the database, type the following at a command prompt:
 

```
migrate database database_name
```

where *database\_name* is the name of the database.
- Bind the schema packages, using the following commands:
 

```
su - database_instance_owner
db2 connect to database_name
db2 update db config using STMHEAP 50000
db2 update db config using APPLHEAPSZ 4096
cd sqllib/bnd (if you are not already in that directory)
db2 bind db2schema.bnd blocking all grant public
db2 bind db2clipk.bnd blocking all grant public
db2 bind db2clist.bnd blocking all grant public
```
- **If your database is DB2 7.2:**
  1. After an instance is ready for migration, use the **db2imigr** command to migrate the instance as follows:
    - a. Log in as a user with root authority.
    - b. If the LD\_LIBRARY\_PATH environment variable is set to /usr/lib and there is a link in /usr/lib to the Version 7 libdb2 shared library, this can cause an error when using the **db2imigr** command. To fix the error, reset

the LD\_LIBRARY\_PATH environment variable so that it does not reference the libraries in those paths by entering the following command:

```
unset LD_LIBRARY_PATH
```

- c. Run the **db2imigr** command as follows:

```
/opt/IBMDB2/V7.1/instance/db2imigr [-d] [-a AuthType]
[-u fencedID] InstName
```

where

- **-d** sets the debug mode that you can use for problem determination. This parameter is optional.
- **-a AuthType** specifies the authentication type for the instance. Valid authentication types are (SERVER), (CLIENT), and (DCS). If the **-a** parameter is not specified, the authentication type defaults to (SERVER), if a DB2 server is installed. Otherwise, the AuthType is set to (CLIENT). This parameter is optional.

**Notes:**

- 1) The authentication type of the instance applies to all databases owned by the instance.
  - 2) While authentication type (DCE) is an optional parameter, it is not valid to choose (DCE) for this command
  - **-u fencedID** is the user under which the fenced user-defined functions (UDFs) and stored procedures will execute. This parameter is optional only when a DB2 Run-Time Client is installed. It is required for all other DB2 products.
  - *InstName* is the login name of the instance owner.
2. Update the DB2 instance using the following procedure:
    - a. Log in as a user with root authority.
    - b. Run the **db2iupdt** command as follows:

```
/opt/IBMDB2/V7.1/instance/db2iupdt InstName
```
    - c. After migrating the DB2 instance, reset LD\_LIBRARY\_PATH to its original setting
  3. Migrate the database owned by the instance, using the following steps:
    - a. Log on with a user ID that has SYSADM authority, such as the instance owner.
    - b. Ensure that the database you want to migrate is cataloged.
    - c. Run db2.
    - d. At the DB2 command prompt, type the following:

```
migrate database database_name
```
  4. Bind the schema packages, using the following commands:

```
su - database_instance_owner
db2 connect to database_name
db2 update db config using STMTHEAP 50000
db2 update db config using APPLHEAPSZ 4096
cd sqllib/bnd (if you are not already in that directory)
db2 bind db2schema.bnd blocking all grant public
db2 bind db2clipk.bnd blocking all grant public
db2 bind db2clist.bnd blocking all grant public
```
  5. Initialize the database manager configuration parameter UTIL\_IMPACT\_LIM to its default value. The UTIL\_IMPACT\_LIM configuration parameter did not exist for DB2 7.1 and on migration to Enterprise Server Edition 8.1 it is assigned a value of 0. The valid range for this parameter is 1 to 100. Use the following procedure:

- a. Log on with a user ID that has SYSADM authority.
- b. Run db2.
- c. At the DB2 command prompt, type the following:  

```
update database manager configuration using UTIL_IMPACT_LIM value
```

Keep *value* a low number, between 1 and 10.

---

## The command-line migration utility (idsimigr)

The **idsimigr** migration utility migrates the schema and configuration files from an earlier release to IBM Tivoli Directory Server 6.0 versions of these files and creates a directory server instance with the migrated information. This directory server instance is the upgraded version of your previous server. As an alternative to the command-line utility, you can use the Instance Administration Tool, specifying that you want to migrate from a previous release. See Chapter 13, “Creating and administering instances,” on page 109 if you want to use the Instance Administration Tool.

**Attention:** When you create a new directory server instance, be aware of the information that follows.

1. If you want to use replication, use a distributed directory, or import and export LDIF data between server instances, you must cryptographically synchronize the server instances to obtain the best performance.

If you are creating a directory server instance that must be cryptographically synchronized with an existing directory server instance, you must synchronize the server instances *before* you do any of the following:

- Start the second server instance
- Run the **idsbulkload** command from the second server instance
- Run the **idsldif2db** command from the second server instance

See Appendix E, “Synchronizing two-way cryptography between server instances,” on page 177 for information about synchronizing directory server instances.

2. After you create a directory server instance and configure the database, use the **idsdbback** utility to create a backup of the directory server instance. The configuration and directory key stash files are archived along with the associated configuration and directory data. You can then use the **idsdbrestore** utility to restore the key stash files if necessary. (You can also use the **idsdbback** utility after you load data into the database. See “Backing up the database” on page 135 and “Backing up, restoring, and optimizing the database” on page 148 for information about backing up the database.)

The syntax for the **idsimigr** command is as follows:

```
idsimigr [-I instancename] [-t dbinstance] [-u backupdir]
[-e encryptseed] [-p port] [-s secureport] [-a admport]
[-c admsecureport] [-i ipaddress] [-r description] [-b outputfile]
[-d debuglevel] [-l instlocation] [-q] [-n] | [-v] | [-?]
```

where

**-?** Displays usage help for the command.

**-a *admport***

Specifies the port on which the administration daemon for the directory server instance will listen.

**Note:** If you have two or more directory server instances listening on the same IP address (or set of IP addresses), be sure that those directory server instances do not use any of the same port numbers.

Click **Next**.

**-b** *outputfile*

Specifies the full path of a file to redirect output into. If used in conjunction with the **-q** option, only errors are written to the file. If debugging is turned on, debugging information is also sent to the file.

**-c** *admsecureport*

Specifies the secure port on which the administration daemon for the directory server instance listens. Specify a positive number that is greater than 0 and less than or equal to 65535. The port specified must not cause a conflict with ports being used by any other directory server instance that is bound to a particular hostname or IP address.

**-d** *debuglevel*

Sets the LDAP debugging level to *<debuglevel>*. This option causes the utility to generate debug output to stdout. The *<debuglevel>* is a bit mask that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel. See the *IBM Tivoli Directory Server Problem Determination Guide* for more information about debug levels.

**-e** *encryptseed*

Specifies the seed to be used to create the key stash files for the directory server instance. This option is required if you use the **-n** option. If it is not specified, you will be prompted for an encryption seed.

The encryption seed must contain only printable ISO-8859-1 ASCII characters with values in the range of 33 to 126, and must be a minimum of 12 and a maximum of 1016 characters in length. For information about the characters that can be used, see Appendix J, "ASCII characters from 33 to 126," on page 189.

This encryption seed is used to generate a set of Advanced Encryption Standard (AES) secret key values. These values are stored in a directory stash file and used to encrypt and decrypt directory stored password and secretkey attributes. There is one encryption seed string for each directory server instance.

Record the encryption seed in a secure location; you might need it if you export data to an LDIF file (the **idsdb2ldif** command) or regenerate the key stash file (the **idsgendirksf** command.)

**-i** *ipaddress*

Specifies the IP address that the directory server instance binds to. If more than one IP address is specified, a comma separator is required with no spaces. Spaces are allowed only if the entire argument is enclosed in quotation marks (""). Use the key word "all" to specify that you want to use all available IP addresses. If you do not specify the **-i** option, all available IP addresses is the default setting.

**-I** *instancename*

Specifies the name of the directory server instance to be created or migrated. The instance name must be an existing user ID on the computer and must be no greater than 8 characters in length. If there is no corresponding user ID for the directory server instance name, the command fails. See Appendix D, "Setting up users and groups: directory



server instance owner, database instance owner, and database owner,” on page 173 for information about additional requirements for the instance name.

- l** *instlocation*  
Specifies the location in which to store the configuration files and logs for the directory server instance. On Windows systems, this option is required and a drive letter must be specified. The location must have at least 30 MB of free disk space. Additional disk space must be available to accommodate growth as directory server log files increase in size.
- n**  
Specifies that you want the command to run without prompting. All output is generated except for messages that require user interaction.
- p** *port*  
Specifies the port on which the directory server instance listens. Specify a positive number that is greater than 0 and less than or equal to 65535. The port specified must not cause a conflict with ports being used by any other directory server instance that is bound to a particular hostname or IP address.
- q**  
Specifies to run in quiet mode. All output is suppressed except error messages. If the **-d** option is also specified, trace output is not suppressed.
- r** *description*  
Specifies a description of the directory server instance.
- s** *secureport*  
Specifies the secure port that the directory server instance listens on. Specify a positive number that is greater than 0 and less than or equal to 65535. The port specified must not cause a conflict with ports being used by any other directory server instance that is bound to a particular hostname or IP address.
- t** *dbinstance*  
Specifies the DB2 database instance name. The database instance name is also the DB2 instance owner ID. By default, the database instance name is assumed to be the same as the directory server instance owner ID.
- u** *backupdir*  
Specifies the name of the directory in which the schema and configuration files to be migrated have been saved.  
  
If all the necessary files are not found in the specified directory, the command will fail. These files include the server configuration file and the following schema files: V3.ibm.at, V3.ibm.oc, V3.system.at, V3.system.oc, V3.user.at, V3.user.oc, and V3.modifiedschema.
- v**  
Prints version information about the command.

For example, you want to migrate from IBM Tivoli Directory Server 5.2 to IBM Tivoli Directory Server 6.0 and:

- You saved the configuration and schema files in a directory named /tmp/ITDS52
- You want to create an instance called **myinst** with an encryption seed of **my\_secret\_key!**

Use the following command:

```
idsimigr -I myinst -u /tmp/ITDS52 -e my_secret_key!
```



On Windows, you must specify a location for the directory server instance using the `-I` option. The following example creates a `c:\idsslapd-myinst` directory for the directory server instance being migrated.

```
idsimigr -I myinst -u c:\temp -l c: -e my_secret_key!
```

---

## Migrating the Web Administration Tool and upgrading the embedded version of WebSphere Application Server - Express

If you have the Web Administration Tool from IBM Directory Server 5.1 or IBM Tivoli Directory Server 5.2 installed into the embedded version of WebSphere Application Server - Express, the InstallShield GUI can upgrade the embedded version of WebSphere Application Server - Express to the 5.1.1 version and install the Web Administration Tool into it, migrating your previous Web Administration Tool configuration. If you do not choose to migrate through the InstallShield GUI when you use it to install, the 5.1.1 embedded version of WebSphere Application Server - Express will be installed, and the 6.0 version of the Web Administration Tool will be installed into it, but your previous configuration will be lost.

If you want to migrate manually because you are not using the InstallShield GUI to install, use the information in the following section.

### Migrating the embedded version of WebSphere Application Server - Express and the Web Administration Tool

You can use the `idswmigr` command-line utility to migrate an earlier version of the embedded version of WebSphere Application Server - Express to the 5.1.1 version and install the 6.0 version of the Web Administration Tool into it. (See “Location of migration utilities” on page 24 for the location of the `idswmigr` utility.)

The `idswmigr` tool does the following:

- Saves the configuration files for the previous version of the Web Administration Tool
- Uninstalls the previous version of the Web Administration Tool from the earlier version of the embedded version of WebSphere Application Server - Express
- Backs up the configuration for the earlier version of the embedded version of WebSphere Application Server - Express to a temporary location that you specify
- Restores the configuration for the earlier version of the embedded version of WebSphere Application Server - Express to the new location
- Installs the 6.0 version of the Web Administration Tool into the embedded version of WebSphere Application Server - Express 5.1.1
- Migrates the previous Web Administration Tool configuration files and restores these files into the new embedded version of WebSphere Application Server - Express

Before you use the `idswmigr` command, do the following:

1. Uninstall the version of the Web Administration Tool that you have installed. (This is the `IDSWebApp.war` file in the `idstools` directory.) However, leave the embedded version of WebSphere Application Server - Express installed, and leave the Web Administration Tool installed into it.
2. Install the new version of the Web Administration Tool.

3. Install the new version of the embedded version of WebSphere Application Server - Express. (Do not install the Web Administration Tool into the embedded version of WebSphere Application Server - Express. The **idswmigr** command will do this.

To use the **idswmigr** command-line utility to migrate the embedded version of WebSphere Application Server - Express and the Web Administration Tool, type the following at a command prompt:

```
idswmigr [-s source_path] [-t target_path] [-l temp_path] [-v] [-i prev_dir]
```

where:

**-s** *source\_path*

Specifies the source location for the previous version of the embedded version of WebSphere Application Server - Express.

**-t** *target\_path*

Specifies the target location where the new embedded version of WebSphere Application Server - Express has been installed.

**-l** *temp\_path*

Specifies a location for the temporary files.

**-v** Displays the command syntax.

**-i** *prev\_dir*

On Windows systems only, specifies the directory where the previous version of SecureWay Directory, IBM Directory Server, or IBM Tivoli Directory Server is installed.

---

## Chapter 5. Installing language packs using the InstallShield GUI

If you want to use the server in languages other than English, you must install language packs for the languages you want to use.

**Note:** You do not need to install language packs for the following:

- The Web Administration Tool.
- The client, unless you want to use the **idslink** and **idsrmlink** commands and you want messages from the commands displayed in a language other than English. For information about the **idslink** and **idsrmlink** commands, see “Using idslink to set links” on page 57 and “Using idsrmlink to remove links” on page 62.

You can install language packs using the InstallShield GUI (not available for HP-UX) or using operating system utilities on AIX, Linux, Solaris, and HP-UX platforms. To install language packs using the InstallShield GUI, use the information in this chapter. To install using operating system utilities, see the appropriate chapter; choose from one of the following:

- For AIX systems, see Chapter 8, “Installing IBM Tivoli Directory Server using AIX utilities,” on page 65.
- For Linux systems, see Chapter 9, “Installing IBM Tivoli Directory Server using Linux utilities,” on page 77.
- For Solaris systems, see Chapter 10, “Installing IBM Tivoli Directory Server using Solaris utilities,” on page 83.
- For HP-UX systems, see Chapter 11, “Installing IBM Tivoli Directory Server using HP-UX utilities,” on page 91.

To install language packs using the InstallShield GUI:

1. Do one of the following:

**On Windows systems:**

- a. Be sure that you are logged on as any member of the Administrators group.
- b. If you are installing from a CD, insert the CD in the CD-ROM drive. Go to the drive for your CD-ROM, and then change to the `\itdsLangpack` directory of the CD.  
If you downloaded a zipped file, go to the directory where you unzipped the file, and then to the `itdsV60\itdsLangpack` subdirectory.
- c. Double-click the **idslp\_setup\_win32** icon, or type `idslp_setup_win32.exe` at the command prompt.

**On AIX, Linux, and Solaris systems:**

- a. Log in as root.
- b. If you are installing from a CD, insert the CD in the CD-ROM drive and mount the CD, and then change to the `/itdsLangpack` directory of the CD.

If you downloaded a tar file, go to the directory where you untarred the file, and then change to the `itdsV60ismp/itdsLangpack` subdirectory.

- c. Type the following:
  - On AIX systems: `idslp_setup_aix.bin`
  - On xSeries Linux systems: `idslp_setup_linux.bin`
  - On zSeries Linux systems: `idslp_setup_linux390.bin`
  - On iSeries and pSeries Linux systems: `idslp_setup_linuxppc.bin`
  - On Solaris systems: `idslp_setup_solaris.bin`
2. The Welcome window is displayed. Click **Next**.
3. On the License Agreement window, after you read the license agreement, click **I accept the terms in the license agreement**. Click **Next**.
4. On Windows systems only, if you have not yet installed IBM Tivoli Directory Server, a window is displayed asking where you want to install the language packs. This path will also be the path where IBM Tivoli Directory Server is installed. Click **Next** to install in the default directory. You can specify a different directory by clicking **Browse** or typing the path you want. The directory will be created if it does not exist.

**Note:** Be sure that the installation location is not the same as the path where another version of the client is installed.

5. A window showing the languages is displayed. The languages you can choose are:
  - German
  - French
  - Italian
  - Spanish
  - Japanese
  - Korean
  - Portuguese
  - Simplified Chinese
  - Traditional Chinese

On AIX, the following additional languages are available:

- Czechoslovakian
- Hungarian
- Polish
- Russian
- Slovakian

Select the languages you want to install, and then click **Next**.

6. A summary window displays the languages you want installed, the path where these language packs will be installed, and the amount of disk space required. Click **Back** to change any of your selections. Click **Next** to begin installation.
7. After installation is complete, click **Finish** on the confirmation window.

Language packs are installed in the `LangPack` subdirectory of the directory where IBM Tivoli Directory Server is installed. A `LangPack_license` subdirectory is also created. This subdirectory contains translated language pack license files.

---

## Chapter 6. Installing IBM Tivoli Directory Server using the InstallShield GUI

You can use the InstallShield GUI to install IBM Tivoli Directory Server on Windows, AIX, Linux, and Solaris platforms. If you do not want to use the InstallShield GUI to install, this guide contains a manual installation procedure for each platform in separate chapters. For an example, see Chapter 8, “Installing IBM Tivoli Directory Server using AIX utilities,” on page 65. (For HP-UX, you must use operating system utilities to install.)

If you install IBM Tivoli Directory Server using the InstallShield GUI, you must also uninstall using the InstallShield GUI. This is also true for installation of corequisite products such as DB2, the embedded version of WebSphere Application Server - Express, and GSKit. See “Uninstalling IBM Tivoli Directory Server using the InstallShield GUI” on page 151 for instructions for removing IBM Tivoli Directory Server using the InstallShield GUI.

---

### Before you install

Be sure that the requirements for your operating system are met before you begin installation. See Chapter 3, “System requirements and supported software versions,” on page 9 for information.

#### Attention

Read and understand the migration process in Chapter 4, “Migration from previous releases,” on page 23 for instructions for migrating and restoring backed-up files after reinstallation.

Before installing, be sure that the following conditions are met. If these conditions are not met, the installation program will exit.

- **If you have a version of SecureWay Directory earlier than 3.2.2 installed on your system:**  
Upgrade to 3.2.2 or later before installing IBM Tivoli Directory Server 6.0. Then use the instructions in Chapter 4, “Migration from previous releases,” on page 23 to migrate your data and install IBM Tivoli Directory Server 6.0.
- **If you have SecureWay Directory version 3.2.2, IBM Directory Server 4.1 or 5.1, or IBM Tivoli Directory Server 5.2 installed on your computer:**  
Use the instructions in Chapter 4, “Migration from previous releases,” on page 23 to migrate your data and install IBM Tivoli Directory Server 6.0.
- **If you have a version of DB2 that is not supported installed on your computer:**  
Upgrade to a supported version of DB2, or remove DB2. DB2 8 Fix Pack 8 refresh is included with IBM Tivoli Directory Server. If you do not have a version of DB2 on your system, the InstallShield GUI installs it if you choose to install the full server.  
**Attention:** Export your data using **db2ldif** before unconfiguring and removing your current database. Do not use the **DB2BACKUP** command. If you do not export before unconfiguring and removing the database, you will lose your data.

- If you have a client from IBM Directory Server 4.1 or 5.1 or IBM Tivoli Directory Server 5.2, you can leave it installed. The server and the client from IBM Tivoli Directory Server 6.0 can coexist with the client from one of these versions.
- If you have the Web Administration Tool from IBM Directory Server 5.1 or IBM Tivoli Directory Server 5.2 installed and you want to migrate it, uninstall the Web Administration Tool, but leave the embedded version of WebSphere Application Server - Express with the Web Administration Tool installed into it. (To uninstall through the InstallShield GUI, select **Web Administration Tool**, but do not select **embedded version of WebSphere Application Server - Express** during uninstallation.)
- On Windows systems, if you are installing the proxy server or the full server, the Administrators group provided with the Windows operating system must exist.

## Creating user IDs

Before you create a directory server instance, you must create a user ID on the operating system for the owner of the directory server instance. You will be asked to provide this user ID and its password when you create a directory server instance after installation. For a full server, you must also create user IDs on the operating system for the owners of the database instance and the database that will be used to store the directory data. See Appendix D, "Setting up users and groups: directory server instance owner, database instance owner, and database owner," on page 173 for detailed information about these user IDs. You can create these user IDs before or after installation, but you must create them before you can successfully create a directory server instance.

---

## Installing IBM Tivoli Directory Server on a Windows platform

To install IBM Tivoli Directory Server 6.0:

1. Be sure that you are logged on as any member of the Administrators group. (You are not required to log on with the user ID you created for the DB2 database owner.)
2. On the computer where you are installing IBM Tivoli Directory Server, stop any programs that are running and close all windows. If you have open windows, the initial IBM Tivoli Directory Server installation window might be hidden behind other windows.
3. If you are installing from a CD:
  - a. Insert the CD in your CD-ROM drive.
  - b. Go to the drive for your CD-ROM, and then go to the \itds folder.
 If you are installing from the downloaded zip file:
  - a. Go to the folder where you unzipped the downloaded zip file, and then go to the itdsV60\itds folder .
4. Double-click the **setup.exe** icon.

If you prefer, you can use the command line to begin installation and specify a temporary directory other than the one specified by the TEMP environment variable. To use this option, go to the appropriate directory (from step 3) and type the following at a command prompt:

```
setup.exe -is:tempdir directory
```

where *directory* is the directory you want to use for temporary space. Be sure that you have at least 100 MB of free space in this directory. For example:

```
setup.exe -is:tempdir "c:\My Documents\temp"
```

The language window is displayed.

**Note:** If the installation program exits without displaying the language window, it might be because there is not enough space in the directory specified by the TEMP environment variable or the directory you specified for temporary space. Be sure that you have at least 100 MB of free space in this directory.

5. Select the language you want to use during IBM Tivoli Directory Server installation. Click **OK**.

**Note:** This is the language used in the installation program, not in IBM Tivoli Directory Server. The language used in IBM Tivoli Directory Server is determined by the language pack you install.

6. On the Welcome window, click **Next**.
7. After reading the Software license agreement, select **I accept the terms in the license agreement**. Click **Next**.
8. If you have any components already installed, they are displayed with their corresponding version levels. Click **Next**.
9. To install in the default directory, click **Next**. You can specify a different directory by clicking **Browse** or typing the directory path you want. The directory will be created if it does not exist. (The default installation directory is C:\Program Files\IBM\LDAP\V6.0.)

**Notes:**

- a. If you have already installed one or more language packs, the installation location is set to the path where you installed the language packs, and you are not asked where you want to install.
- b. Be sure that the installation location is not the same as the path where another version of the client is installed.
- c. Do not use special characters, such as hyphen (-) and period (.) in the name of the installation directory. For example, use **ldapdir** rather than **ldap-dir** or **ldap.dir**.

If the window in the following step is very slow to be displayed, you might have a slow network drive attached. You can detach the network drive and see if the window is displayed more quickly.

10. A window showing the following components for installation is displayed:

- Client SDK 6.0
- Java Client 6.0
- Web Administration Tool 6.0
- Proxy Server 6.0
- Server 6.0 (Full Server Package)
- embedded version of WebSphere Application Server - Express
- DB2 V8.2
- GSKit

The components that are not yet installed are preselected. You can choose to reinstall the server, the client, or the Web Administration Tool if they were previously installed.

**Notes:**

- a. If you install the client (which is also installed when you install a server), the Path environment variable is updated by adding the following directories to the beginning of the existing path:
  - *installpath*\bin



- *installpath*\lib

*installpath* is the directory where you installed IBM Tivoli Directory Server.

- If you install the proxy server (which is also installed when you install the full server), the Path environment variable is updated by adding the *installpath*\sbin directory to the beginning of the existing path. *installpath* is the directory where you installed IBM Tivoli Directory Server.
- If you install the Web Administration Tool, Directory Services Markup Language (DSML) files are also copied to your computer. See Appendix L, "Installing and configuring DSML," on page 193 for information about installing and configuring DSML.
- If you install the Web Administration Tool, an application server is required to run the tool. If you select **embedded version of WebSphere Application Server - Express**, v5.1.1 is installed and configured for you. If version 5.0 or 5.0.2 of the embedded version of WebSphere Application Server - Express is already installed, the InstallShield GUI installation program asks if you want to migrate it to version 5.1.1. Any configuration files from the previous Web Administration Tool are backed up and restored. If you use another application server, such as WebSphere, you must install the Web Administration Tool file, IDWebApp.war, into the application server after you install. For information about installing the Web Administration Tool into WebSphere, see Appendix I, "Installing the Web Administration Tool into WebSphere," on page 187.

This window also indicates the amount of disk space required and available on the selected drive.

Be sure the components you want to install are selected, and click **Next**.

- If you selected **DB2 V8.2** in step 10 on page 49, a window is displayed prompting you to enter a Windows user ID and password for the DB2 system ID. The default user ID is **db2admin**. On the window:
  - Type the user ID or accept the default. This user ID must **not** be the one you created in "Creating user IDs" on page 48.  
If you are not using an existing user ID, DB2 creates the user ID you specify with the password you type. This is the preferred method.  
If you are using an existing Windows user ID, it must be a member of the Administrators group.
  - Type the password, and then type the password again for verification. (If you are using an existing Windows user ID, be sure that your password is correct. Otherwise, DB2 does not install correctly.)
  - Click **Next**.
- The installation program now has enough information to begin installing. A summary window displays the components you selected and the locations where the selected components will be installed. Click **Back** to change any of your selections. Click **Next** to begin installation.

**Note:** After installation has begun, do not try to cancel the installation. If you inadvertently cancel the installation, see the information about recovering from a failed installation in the *IBM Tivoli Directory Server version 6.0 Problem Determination Guide* before you attempt to reinstall.

- If you are asked if you want to restart your computer now or later, select the option you want and click **Finish**. (You might need to restart your system to complete IBM Tivoli Directory Server installation. You are unable to use IBM Tivoli Directory Server until this is completed.)



**Note:** If you are installing on a Windows 2000 system and you installed DB2, restart your computer after installing. If you do not restart the computer and you receive a message that the dynamic link library DB2APP.dll could not be located, then you must restart before continuing.

If your computer is restarted, log in using the same user ID that you used to install IBM Tivoli Directory Server.

If you installed DB2, the DB2 First Steps GUI might be started. You can go through the DB2 First Steps or close this GUI.

**Note:** A license subdirectory is created in the directory where IBM Tivoli Directory Server is installed. This subdirectory contains IBM Tivoli Directory Server license files in all provided languages.

**Note:** If you installed the proxy server or the full server, you must install IBM Tivoli Directory Integrator 6.0 with Fix Pack 1 if you want to do the following. (If you acquire IBM Tivoli Directory Server through Passport Advantage, it includes a copy of IBM Tivoli Directory Integrator 6.0 with Fix Pack 1.)

- Use the **idsupport** tool, which gathers information from your system that you can supply to IBM Support if you encounter problems.
- Use the log management tool.

You can find information about the support tool and the log management tool in the *IBM Tivoli Directory Server version 6.0 Problem Determination Guide*.

- Use Simple Network Management Protocol (SNMP). For information about SNMP, see the *IBM Tivoli Directory Server version 6.0 Administration Guide*.

If you installed a server, the Instance Administration Tool automatically runs so that you can create a directory server instance and complete configuration. Before you can use the server, you must:

- Create a directory server instance
- Set the administrator DN and password for the instance
- If you installed and plan to use the full server, configure the database that will store the directory data

To create a directory server instance, use the instructions in “Creating an instance” on page 110. You can set the administrator DN and password and configure the database during the instance creation process.

To make changes to your configuration at a later time, see Chapter 14, “Configuration,” on page 125 for more information about using the Configuration Tool.

If any errors occurred during installation, instance creation, or configuration, see the information *IBM Tivoli Directory Server version 6.0 Problem Determination Guide* for information about recovering from these errors.

**Note:** IBM Network Authentication System (NAS) client for Windows is provided with IBM Tivoli Directory Server. If you want to install the NAS client for Windows, go to the \itdsV60\nas subdirectory of the directory where you unzipped the IBM Tivoli Directory Server file or the \nas directory on the CD-ROM. Installation instructions are provided in the *IBM Network*

## Installing IBM Tivoli Directory Server on an AIX, Linux, or Solaris system

IBM Tivoli Directory Server is installed in the following directory:

- On AIX and Solaris systems, the /opt/IBM/ldap/V6.0 directory
- On Linux systems, the /opt/ibm/ldap/V6.0 directory

To install IBM Tivoli Directory Server 6.0:

1. Log in as **root**.
2. If you are installing from a CD, insert the CD in your CD-ROM drive, and then change directories to the root directory on the CD.

If you are installing from the downloaded tar file, go to the itdsV60ismp subdirectory of the directory where you untarred the downloaded tar file.

3. Type `./setup`.

If you prefer, you can specify a temporary directory other than the system temporary directory. To use this option, change directories to the appropriate directory (from step 2) and type the following at a command prompt:

```
./setup -is:tempdir directory
```

where *directory* is the directory you want to use for temporary space. Be sure that you have at least 400 MB of free space in this directory. For example:

```
./setup -is:tempdir /opt/tmp
```

A language window is displayed.

4. Select the language you want to use during IBM Tivoli Directory Server installation. Click **OK**.

**Note:** This is the language used in the installation program, not in the IBM Tivoli Directory Server. The language used in the IBM Tivoli Directory Server is determined by the language pack you install.

5. On the Welcome window, click **Next**.
6. After reading the Software license, select **I accept the terms in the license agreement**. Click **Next**.
7. Any preinstalled components and corresponding version levels are displayed. Click **Next**.

If the window in the following step is very slow to be displayed, you might have a slow network drive mounted. You can unmount the network drive and see if the window is displayed more quickly.

8. A window is displayed with the following components:
  - Client SDK 6.0
  - Java Client 6.0
  - Web Administration Tool 6.0
  - Proxy Server 6.0
  - Server 6.0 (Full Server Package)
  - embedded version of WebSphere Application Server - Express
  - DB2 V8.2
  - GSKit

The components that are not yet installed are preselected.

This window also indicates the amount of disk space required and available.

Be sure the components you want to install are selected, and click **Next**.

**Notes:**

- a. If you install the Web Administration Tool, DSML files are also copied to your computer. See Appendix L, "Installing and configuring DSML," on page 193 for information about installing and configuring DSML.
  - b. If you install the Web Administration Tool, an application server is required to run the tool. If you select **embedded version of WebSphere Application Server - Express**, the embedded version of WebSphere Application Server - Express, v5.1.1 is installed and configured for you. If version 5.0 or 5.0.2 of the embedded version of WebSphere Application Server - Express is already installed and was installed by the earlier release in the appsrv subdirectory of the default installation path for the release, the InstallShield GUI installation program asks if you want to migrate it to version 5.1.1. Any configuration files from the previous Web Administration Tool are backed up and restored. If you use another application server, such as WebSphere, you must, after installation, install the IDWebApp.war file into the application directory for your application server. For information about installing and configuring the Web Administration Tool into WebSphere, see Appendix I, "Installing the Web Administration Tool into WebSphere," on page 187.
9. The installation program now has enough information to begin installing. A summary panel displays the components you selected and the locations where the selected components will be installed. Click **Back** to change any of your selections. Click **Next** to begin installation.
  10. By default, links are set automatically for client and server utilities. However, if a conflict is found, a window is displayed asking if you want to override the previous links. If this window is displayed and you want the installation program to override the links, click **Yes**. If you prefer to set links manually after installation, click **No**, and you can use the **idslink** command-line utility to set the links. See "Using idslink to set links" on page 57 for information about using the utility. You can find a list of the conflicts found in the `/var/idsldap/V6.0/idslink.preview` file. The `/var/idsldap/V6.0/idslink.log` file shows the links that were set.
  11. When the completion window is displayed, click **Finish**. Installation is complete.

**Note:** A license subdirectory is created in the directory where IBM Tivoli Directory Server is installed. This subdirectory contains IBM Tivoli Directory Server license files in all provided languages.

**Note:** If you installed the proxy server or the full server, you must install IBM Tivoli Directory Integrator 6.0 with Fix Pack 1 if you want to do the following. (If you acquire IBM Tivoli Directory Server through Passport Advantage, it includes a copy of IBM Tivoli Directory Integrator 6.0 with Fix Pack 1.)

- Use the **idsupport** tool, which gathers information from your system that you can supply to IBM Support if you encounter problems.
- Use the log management tool.

You can find information about the support tool and the log management tool in the *IBM Tivoli Directory Server version 6.0 Problem Determination Guide*

- Use Simple Network Management Protocol (SNMP). See the *IBM Tivoli Directory Server version 6.0 Administration Guide* for information about SNMP.

If you installed a server, the Instance Administration Tool automatically runs so that you can create a directory server instance and complete configuration. Before you can use the server, you must:

- Create a directory server instance
- Set the administrator DN and password for the instance
- If you installed and plan to use the full server, configure the database that will store the directory data

To create a directory server instance, use the instructions in “Creating an instance” on page 110. You can set the administrator DN and password and configure the database during the instance creation process.

To make changes to your configuration at a later time, see Chapter 14, “Configuration,” on page 125 for more information about using the Configuration Tool or the command-line utilities.

If any errors occurred during installation, instance creation, or configuration, see the *IBM Tivoli Directory Server version 6.0 Problem Determination Guide* for information about recovering from these errors.

---

## Chapter 7. Considerations on AIX, Linux, Solaris, and HP-UX systems

For AIX, Linux, Solaris, and HP-UX systems, there are several environments that might require special setup.

---

### The idslldap user and group

During installation of a server, the idslldap user and group are created if they do not already exist. If your environment requires that you have more control over this user and group, you can create them before you install. Requirements are:

- The idslldap user must be a member of the idslldap group.
- The root user must be a member of the idslldap group.
- The idslldap user must have a home directory.
- The default shell for the idslldap user must be the Korn shell.
- The idslldap user can have a password, but is not required to.
- The idslldap user can be the owner of the director server instance.

You can use the following commands to create the user idslldap and the group idslldap and set them up correctly:

#### On AIX systems:

Use the following commands.

To create the idslldap group:

```
mkgroup idslldap
```

To create user ID idslldap, which is a member of group idslldap, and set the korn shell as the default shell:

```
mkuser pgrp=idslldap home=/home/idslldap shell=/bin/ksh idslldap
```

To set the password for user idslldap:

```
passwd idslldap
```

To modify the root user ID so that root is a member of the group idslldap:

```
/usr/bin/chgrpmem -m + root idslldap
```

#### On Linux systems:

Use the following commands.

To create the idslldap group:

```
groupadd idslldap
```

To create user ID idslldap, which is a member of group idslldap, and set the korn shell as the default shell:

```
useradd -g idslldap -d /home/idslldap -m -s /bin/ksh idslldap
```

To set the password for user idslldap:

```
passwd idslldap
```

To modify the root user ID so that root is a member of the group idslldap:

```
usermod -G idslldap,rootgroups root
```

where *rootgroups* can be obtained by using the command: `groups root`

**On Solaris systems:**

Use the following commands.

To create the `idsldap` group:

```
groupadd idsldap
```

To create user ID `idsldap`, which is a member of group `idsldap`, and set the korn shell as the default shell:

```
useradd -g idsldap -d /export/home/idsldap -m -s /bin/ksh idsldap
```

To set the password for user `idsldap`:

```
passwd idsldap
```

To modify the root user ID so that root is a member of the group `idsldap`, use the AdminTool or another appropriate tool.

**On HP-UX systems:**

Use the following commands.

To create the `idsldap` group:

```
groupadd idsldap
```

To create user ID `idsldap`, which is a member of group `idsldap`, and set the korn shell as the default shell:

```
useradd -g idsldap -d /home/idsldap -m -s /bin/ksh idsldap
```

To set the password for user `idsldap`:

```
passwd idsldap
```

To modify the root user ID so that root is a member of the group `idsldap`, use the **sam** tool or another appropriate tool.

Be sure that all these requirements are met before you install. The proxy server does not install correctly if the `idsldap` user exists but does not meet the requirements.

**Note:** For information about requirements for other user IDs you must create, see Appendix D, "Setting up users and groups: directory server instance owner, database instance owner, and database owner," on page 173.

---

## Installation path on AIX, Linux, Solaris, and HP-UX platforms

IBM Tivoli Directory Server is installed in the following path:

**On AIX systems:**

```
/opt/IBM/ldap/V6.0
```

**On Linux systems:**

```
/opt/ibm/ldap/V6.0
```

**On Solaris systems:**

```
/opt/IBM/ldap/V6.0
```

**On HP-UX systems:**

```
/opt/IBM/ldap/V6.0
```

---

## Using commands to set and remove links

By default, links are set automatically for client and server utilities at the end of installation through the InstallShield GUI and through the native operating system utilities. However, if a conflict is found, during InstallShield GUI installation you are asked if you want to override the previous links. After installation, check the `/var/idsldap/V6.0/idslink.log` file to see what links were created. After InstallShield GUI installations, you can also check the `/var/idsldap/V6.0/idslink.preview` file to see if there were conflicts.

You can use the **idslink** utility to manually set the links to command-line utilities such as **ldapmodify** and **ldapadd** and libraries such as `libibmldap.so`. These links point to the location where the IBM Tivoli Directory Server utilities and libraries reside: `installpath/bin`, `installpath/sbin`, and `installpath/lib`. (*installpath* is the directory where IBM Tivoli Directory Server is installed. See “Installation path on AIX, Linux, Solaris, and HP-UX platforms” on page 56 for this directory.) To remove the links set by the **idslink** utility, you can use the **idsrmlink** utility. By default, links are removed automatically when you uninstall.

### Using idslink to set links

The **idslink** command creates links to LDAP client and server command-line utilities. This utility is installed with the client package.

The syntax for the **idslink** command is as follows (*installpath* is the directory where IBM Tivoli Directory Server is installed):

```
installpath/bin/idslink [-i -g -l bits -s mode [-n] [-q] [-f]] | -v | -h
```

where

- h** Displays usage help for the command.
- v** Displays version information about the command.
- n** Pretend option. Displays the links that will be set if you run the command with the options you specify. If specified, you must also specify one or more of the following options: **-i**, **-g**, or **-l**. After running the command with this option, check the `/var/idsldap/V6.0/idslink.preview` file, which will contain any conflicts that were found.
- i** Creates links only for client command utilities that begin with 'ids'. For example, creates the link from `/usr/bin/idsldapsearch` to `/opt/ibm/ldap/V6.0/bin/idsldapsearch`
- g** Creates links only for client command utilities that do not begin with 'ids'. For example, creates the link from `/usr/bin/ldapsearch` to `/opt/ibm/ldap/V6.0/bin/ldapsearch`.
- l bits** Creates links for 32-bit or 64-bit client library files. *bits* can be 32 or 64.
- s mode** Creates links for server command-line utilities only. *mode* can be **proxy** if the directory server instance is a proxy server or **fullsrv** if the directory server instance is a full server.
- q** Specifies to run in quiet mode. All output is suppressed except error messages.
- f** Force option. Specifies to override existing files or links, and back up any conflicts. For example, `/usr/bin/ldapsearch`.



If you use the force option, each conflicting link is backed up into a subdirectory with the same name as the file, directory, or link that had the conflict. For example, a conflict for the /usr/bin/ldapsearch command is backed up in a subdirectory called /usr/bin/V6.0\_idslink\_bkup\_timestamp, where *timestamp* is the date and time the backup was created.

If you do not use this option and conflicts with existing links are found, none of the links in the group are set.

## Links created by idslink

The following sections show links that are created by the **idslink** command.

**Note:** /opt/ibmdir/ldap/V6.0/ is /opt/IBM/ldap/V6.0/ on AIX, Solaris, and HP-UX systems. On Linux systems, /opt/ibmdir/ldap/V6.0/ is /opt/ibm/ldap/V6.0/

### Client commands:

#### Links created when -g option is specified: Set of links for client commands (that do not begin with 'ids') for the base client

```
/usr/bin/ldapsearch → /opt/ibmdir/ldap/V6.0/bin/ldapsearch
/usr/bin/ldapadd → /opt/ibmdir/ldap/V6.0/bin/ldapadd
/usr/bin/ldapmodify → /opt/ibmdir/ldap/V6.0/bin/ldapmodify
/usr/bin/ldapdelete → /opt/ibmdir/ldap/V6.0/bin/ldapdelete
/usr/bin/ldapmodrdn → /opt/ibmdir/ldap/V6.0/bin/ldapmodrdn
/usr/bin/ldapchangepwd →
/opt/ibmdir/ldap/V6.0/bin/ldapchangepwd
/usr/bin/ldaptrace → /opt/ibmdir/ldap/V6.0/bin/ldaptrace
/usr/bin/ldapexop → /opt/ibmdir/ldap/V6.0/bin/ldapexop
/usr/bin/ibmdirctl → /opt/ibmdir/ldap/V6.0/bin/ibmdirctl
```

#### Links created when -i option is specified: Set of links for client commands (that begin with 'ids') for the base client

```
/usr/bin/idsldapsearch → /opt/ibmdir/ldap/V6.0/bin/idsldapsearch
/usr/bin/idsldapadd → /opt/ibmdir/ldap/V6.0/bin/idsldapadd
/usr/bin/idsldapmodify → /opt/ibmdir/ldap/V6.0/bin/idsldapmodify
/usr/bin/idsldapdelete → /opt/ibmdir/ldap/V6.0/bin/idsldapdelete
/usr/bin/idsldapmodrdn →
/opt/ibmdir/ldap/V6.0/bin/idsldapmodrdn
/usr/bin/idsldapchangepwd →
/opt/ibm/ldap/V6.0/bin/idsldapchangepwd
/usr/bin/idsldaptrace → /opt/ibmdir/ldap/V6.0/bin/idsldaptrace
/usr/bin/idsldapexop → /opt/ibmdir/ldap/V6.0/bin/idsldapexop
/usr/bin/idsdirctl → /opt/ibmdir/ldap/V6.0/bin/idsdirctl
```

### Client libraries:

**Note:** XX is a library extension such as .so, .a, or .sl

#### Links created when -l 32 option is specified

The following groups or sets of links are created when the **-l bits** option is specified and *bits* is 32.

**Note:** Links common to all operating systems and links that are specific to a particular operating system are in one group or set.

#### Client libraries: Set of links for 32-bit client package Common links:



```

/usr/lib/libidsldap.XX →
/opt/ibmdir/ldap/V6.0/lib/libidsldap.XX
/usr/lib/libidsldapstatic.XX →
/opt/ibmdir/ldap/V6.0/lib/libidsldapstatic.XX
/usr/lib/idsldap_plugin_sasl_cram-md5.XX →
/opt/ibmdir/idsldap/V6.0/lib/idsldap_plugin_sasl_cram-md5.XX
/usr/lib/idsldap_plugin_sasl_digest-md5.XX →
/opt/ibmdir/ldap/V6.0/lib/idsldap_plugin_sasl_digest-md5.XX

```

**Operating system-specific links:**

```

/usr/lib/idsldap_plugin_ibm_gsskrb.XX →
/opt/ibmdir/ldap/V6.0/lib/idsldap_plugin_ibm_gsskrb.XX
(AIX only, Kerberos library file)
/usr/lib/libidsldif.XX →
/opt/ibmdir/ldap/V6.0/lib/libidsldif.XX
(Linux and HP_UX only)

```

**Client libraries: Set of links for 32-bit client package (backward compatibility support)**

**Common links:**

```

/usr/lib/libldap.XX →
/opt/ibmdir/ldap/V6.0/lib/libidsldap.XX
/usr/lib/libibmldap.XX →
/opt/ibmdir/ldap/V6.0/lib/libidsldap.XX
/usr/lib/libibmldapstatic.XX →
/opt/ibmdir/ldap/V6.0/lib/libidsldapstatic.XX
/usr/lib/libldapiconv.XX →
/opt/ibmdir/ldap/V6.0/lib/libidsldapiconv.XX
/usr/lib/ldap_plugin_sasl_cram-md5.XX →
/opt/ibmdir/ldap/V6.0/lib/idsldap_plugin_sasl_cram-md5.XX
/usr/lib/ldap_plugin_sasl_digest-md5.XX →
/opt/ibmdir/ldap/V6.0/lib/idsldap_plugin_sasl_digest-md5.XX

```

**Operating system-specific links:**

```

/usr/lib/ldap_plugin_ibm_gsskrb.XX →
/opt/ibmdir/ldap/V6.0/lib/idsldap_plugin_ibm_gsskrb.XX
(AIX only, Kerberos library file)
/usr/lib/libldif.XX →
/opt/ibmdir/ldap/V6.0/lib/libidsldif.XX
(Linux and HP_UX only)

```

**Links created when -l 64 option is specified**

The following groups or sets of links are created when the *-l bits* option is specified and *bits* is 64.

**Client libraries: Set of links with '64' in name for 64-bit client package**

**Common links:**

```

/usr/lib/libidsldap64.XX →
/opt/ibmdir/ldap/V6.0/lib64/libidsldap.XX
/usr/lib/libidsldapstatic64.XX →
/opt/ibmdir/ldap/V6.0/lib64/libidsldapstatic.XX
/usr/lib/idsldap_plugin_sasl_cram-md5_64.XX→
/opt/ibmdir/ldap/V6.0/lib64/idsldap_plugin_sasl_cram-md5.XX

```

*/usr/lib/idsldap\_plugin\_sasl\_digest-md5\_64.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/idsldap\_plugin\_sasl\_digest-md5.XX*

**Operating system-specific links:**

*/usr/lib/idsldap\_plugin\_ibm\_gsskrb\_64.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/idsldap\_plugin\_ibm\_gsskrb.XX*  
(AIX only, Kerberos library file)  
*/usr/lib/libidsldif64.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/libidsldif.XX*  
(Linux and HP\_UX only)

**Client libraries: Set of links with '64' in name for 64-bit client package (backward compatibility support)**

**Common links:**

*/usr/lib/libldap64.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/libidsldap.XX*  
*/usr/lib/libibmldap64.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/libidsldap.XX*  
*/usr/lib/libibmldapstatic64.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/libidsldapstatic.XXX*  
*/usr/lib/libldapiconv64.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/libidsldapiconv.XX*  
*/usr/lib/ldap\_plugin\_sasl\_cram-md5\_64.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/idsldap\_plugin\_sasl\_cram-md5.XX*  
*/usr/lib/ldap\_plugin\_sasl\_digest-md5\_64.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/idsldap\_plugin\_sasl\_digest-md5.XX*

**Operating system-specific links:**

*/usr/lib/ldap\_plugin\_ibm\_gsskrb\_64.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/idsldap\_plugin\_ibm\_gsskrb.XX*  
(AIX only, Kerberos library file)  
*/usr/lib/libldif64.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/libidsldif.XX*  
(Linux and HP\_UX only)

**Client libraries: Set of links without '64' in name for 64-bit client package**

**Common links:**

*/usr/lib/lib64/libidsldap.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/libidsldap.XX*  
*/usr/lib/lib64/libidsldapstatic.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/libidsldapstatic.XX*  
*/usr/lib/lib64/idsldap\_plugin\_sasl\_cram-md5.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/idsldap\_plugin\_sasl\_cram-md5.XX*  
*/usr/lib/lib64/idsldap\_plugin\_sasl\_digest-md5.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/idsldap\_plugin\_sasl\_digest-md5.XX*

**Operating system-specific links:**

*/usr/lib/lib64/idsldap\_plugin\_ibm\_gsskrb.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/idsldap\_plugin\_ibm\_gsskrb.XX*  
(AIX only, Kerberos library file)  
*/usr/lib/lib64/libidsldif.XX* →

*/opt/ibmdir/ldap/V6.0/lib64/libidsldif.XX*  
(Linux and HP\_UX only)

**Client libraries: Set of links without '64' in name for 64-bit client package (backward compatibility support)**

**Common links:**

*/usr/lib/lib64/libldap.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/libidsldap.XX*  
*/usr/lib/lib64/libibmldap.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/libidsldap.XX*  
*/usr/lib/lib64/libibmldapstatic.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/libidsldapstatic.XX*  
*/usr/lib/lib64/libldapiconv.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/libidsldapiconv.XX*  
*/usr/lib/lib64/ldap\_plugin\_sasl\_cram-md5.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/idsldap\_plugin\_sasl\_cram-md5.XX*  
*/usr/lib/lib64/ldap\_plugin\_sasl\_digest-md5.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/idsldap\_plugin\_sasl\_digest-md5.XX*

**Operating system-specific links:**

*/usr/lib/lib64/ldap\_plugin\_ibm\_gsskrb.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/idsldap\_plugin\_ibm\_gsskrb.XX*  
(AIX only, Kerberos library file)  
*/usr/lib/lib64/libldif.XX* →  
*/opt/ibmdir/ldap/V6.0/lib64/libidsldif.XX*  
(Linux and HP\_UX only)

**Server commands:**

**Links created when -s proxy option is specified: Set of links for server commands for proxy server package**

*/usr/bin/slapd* → */opt/ibmdir/ldap/V6.0/sbin/slapd* (5.2 legacy)  
*/usr/bin/ibmslapd* →  
*/opt/ibmdir/ldap/V6.0/sbin/ibmslapd* (5.2 legacy)  
*/usr/bin/idsslapd* →  
*/opt/ibmdir/ldap/V6.0/sbin/idsslapd*  
*/usr/bin/ibmdiradm* →  
*/opt/ibmdir/ldap/V6.0/sbin/ibmdiradm* (5.2 legacy)  
*/usr/bin/idsdiradm* → */opt/ibmdir/ldap/V6.0/sbin/idsdiradm*  
*/usr/bin/ldtrc* → */opt/ibmdir/ldap/V6.0/sbin/ldtrc* (5.2 legacy)  
*/usr/bin/ddsetup* → */opt/ibmdir/ldap/V6.0/sbin/ddsetup*  
*/usr/bin/idsxcfg* → */opt/ibmdir/ldap/V6.0/sbin/idsxcfg*  
*/usr/bin/idsxinst* → */opt/ibmdir/ldap/V6.0/sbin/idsxinst*  
*/usr/bin/idsilist* → */opt/ibmdir/ldap/V6.0/sbin/idsilist*  
*/usr/bin/idsicrt* → */opt/ibmdir/ldap/V6.0/sbin/idsicrt*  
*/usr/bin/idsidrop* → */opt/ibmdir/ldap/V6.0/sbin/idsidrop*  
*/usr/bin/idsdnpw* → */opt/ibmdir/ldap/V6.0/sbin/idsdnpw*  
*/usr/bin/idssetport* → */opt/ibmdir/ldap/V6.0/sbin/idssetport*  
*/usr/bin/idssethost* → */opt/ibmdir/ldap/V6.0/sbin/idssethost*  
*/usr/bin/idsimigr* → */opt/ibmdir/ldap/V6.0/sbin/idsimigr*  
*/usr/bin/idscfgsch* → */opt/ibmdir/ldap/V6.0/sbin/idscfgsch*  
*/usr/bin/idsucfgsch* → */opt/ibmdir/ldap/V6.0/sbin/idsucfgsch*  
*/usr/bin/idslogmgmt* → */opt/ibmdir/ldap/V6.0/sbin/idslogmgmt*  
*/usr/bin/idsgendirksf* → */opt/ibmdir/ldap/V6.0/sbin/idsgendirksf*  
*/usr/bin/idssupport* → */opt/ibmdir/ldap/V6.0/sbin/idssupport*

### Links created when -s fullsrv option is specified: Set of links for server commands for full server package

```
/usr/bin/bulkload -> /opt/ibmdir/ldap/V6.0/sbin/bulkload
                        (5.2 legacy)
/usr/bin/idsbulkload -> /opt/ibmdir/ldap/V6.0/sbin/idsbulkload
/usr/bin/ldif2db -> /opt/ibmdir/ldap/V6.0/sbin/ldif2db (5.2 legacy)
/usr/bin/idsldif2db -> /opt/ibmdir/ldap/V6.0/sbin/idsldif2db
/usr/bin/db2ldif -> /opt/ibmdir/ldap/V6.0/sbin/db2ldif (5.2 legacy)
/usr/bin/idsdb2ldif -> /opt/ibmdir/ldap/V6.0/sbin/idsdb2ldif
/usr/bin/dbback -> /opt/ibmdir/ldap/V6.0/sbin/dbback (5.2 legacy)
/usr/bin/idsdbback -> /opt/ibmdir/ldap/V6.0/sbin/idsdbback
/usr/bin/dbrestore ->
                        /opt/ibmdir/ldap/V6.0/sbin/dbrestore (5.2 legacy)
/usr/bin/idsdbrestore -> /opt/ibmdir/ldap/V6.0/sbin/idsdbrestore
/usr/bin/runstats -> /opt/ibmdir/ldap/V6.0/sbin/runstats
                        (5.2 legacy)
/usr/bin/idsrunstats ->
                        /opt/ibmdir/ldap/V6.0/sbin/idsrunstats (5.2 legacy)
/usr/bin/idscfgdb -> /opt/ibmdir/ldap/V6.0/sbin/idscfgdb
/usr/bin/idsucfgdb -> /opt/ibmdir/ldap/V6.0/sbin/idsucfgdb
/usr/bin/idscfgchglg -> /opt/ibmdir/ldap/V6.0/sbin/idscfgchglg
/usr/bin/idsucfgchglg -> /opt/ibmdir/ldap/V6.0/sbin/idsucfgchglg
/usr/bin/idscfgsuf -> /opt/ibmdir/ldap/V6.0/sbin/idscfgsuf
/usr/bin/idsucfgsuf -> /opt/ibmdir/ldap/V6.0/sbin/idsucfgsuf
```

## Using idsrmlink to remove links

You can use the **idsrmlink** command-line utility to remove links to the client and server utilities that were set by the **idslink** command. By default, links are removed automatically when you uninstall.

**Note:** **idsrmlink** does not restore any links previously backed up when **idslink** was run with the force option.

The syntax for the **idsrmlink** command is as follows (*installpath* is the path where IBM Tivoli Directory Server is installed):

```
installpath/bin/idsrmlink [-i -g -l bits -s mode[-n] [-q]] | -v | -h
```

where

- h** Displays usage help for the command.
- v** Displays version information about the command.
- n** Pretend option. Displays the links that will be removed if you run the command with the options you specify.
- i** Removes links only for client command utilities that begin with 'ids'.
- g** Removes links only for client command utilities that do not begin with 'ids'.
- l *bits*** Removes links for 32-bit or 64-bit client library files. *bits* can be 32 or 64.
- s *mode*** Removes links for server command-line utilities only. *mode* can be **proxy** if the directory server instance is a proxy server or **fullsrv** if the directory server instance is a full server.

- q Specifies to run in quiet mode. All output is suppressed except error messages.



---

## Chapter 8. Installing IBM Tivoli Directory Server using AIX utilities

You can use either of the following utilities to install IBM Tivoli Directory Server on AIX:

- **SMIT** (This is the preferred installation method.) See “SMIT installation” on page 69 for information.
- **installp**. See “Command line installation using installp” on page 72 for information.

**Attention:** If you are migrating from SecureWay Directory 3.2.2, IBM Directory Server 4.1 or 5.1, or IBM Tivoli Directory Server 5.2, use the appropriate migration process in Chapter 4, “Migration from previous releases,” on page 23. This chapter contains instructions for migrating and restoring backed-up files after reinstallation. It is very important that you back up and export previous versions of schema files and the server configuration file before installing IBM Tivoli Directory Server 6.0.

Before you install IBM Tivoli Directory Server, be sure you have a supported version of DB2 installed. (See “Requirements on AIX operating systems” on page 11 for supported versions of DB2.)

If you want to use the version of DB2 provided with IBM Tivoli Directory Server, you must use the **db2\_install** utility to install it. (If you do not use this utility, the DB2 license file is not added correctly.) The **db2\_install** utility is in the /db2 directory of the IBM Tivoli Directory Server CD-ROM if you created one, or in the db2v8fp8refresh-ese-aix-ppc directory of the directory where you untarred the DB2 tar file for AIX.

### Notes:

1. The **db2\_install** utility can install only in a C or en\_US locale. If you are installing on a computer with a different locale, set the locale in a shell to C or en\_US before you use the **db2\_install** utility.
2. After you start the **db2\_install** utility, you are prompted for a keyword. In response to this prompt, type DB2.ESE.
3. After you install DB2, you can check the following two files to verify that the installation was successful:  
    /tmp/db2\_install.rc.99999  
    /tmp/db2\_instal\_log.99999

99999 is a random number associated with the installation.

If you are installing the Web Administration Tool, you must also install an application server such as the embedded version of WebSphere Application Server - Express. See Appendix H, “Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express,” on page 183 for information.

If you have a client from IBM Directory Server 4.1 or 5.1 or IBM Tivoli Directory Server 5.2, you can leave it installed. The server and the client from IBM Tivoli Directory Server 6.0 can coexist with a client from one of these versions.

**Notes:**

1. For a server with no X11 support, do not install the Java client, which is in package `idsldap.cltjava60`, when you install the server. However, you will not be able to use the Instance Administration Tool or the Configuration Tool, which require Java, and you must use the command line to create directory server instances and configure the database.
2. You do not need to install security functions if you are not going to use them. You can provide SSL by installing the SSL package on the client, server, or both, as well as installing a Global Security Kit (GSKit), which is included with IBM Tivoli Directory Server 6.0. See “Installing GSKit” on page 74 for information about installing GSKit.
3. If you are installing IBM Tivoli Directory Server on a node within an RS/6000® SP™ environment, see “Before installing on a node within an RS/6000 SP environment” before beginning installation.

For more detailed information about installation procedures and commands for the AIX operating system, see the *AIX Installation Guide* provided with the operating system.

---

## Before installing on a node within an RS/6000 SP environment

**Attention:** Use this section **only** if you are installing on a node within an RS/6000 SP environment.

If you are installing IBM Tivoli Directory Server on a node within an RS/6000 SP environment you must first add the necessary users and groups to the Control Workstation (CWS) and propagate them to the nodes using the `/var/sysamn/supper update` command, as follows:

1. Add the **idsldap** user and group on the CWS, and add the `idsldap` and `root` users to the `idsldap` group. For example:

```
mkgroup idsldap
mkuser idsldap
chgrpmem -m + root,idsldap idsldap
```

2. Update the RS/6000 SP nodes with the new users and groups.  
`/var/sysamn/supper update`

You are now ready to install and configure IBM Tivoli Directory Server on the RS/6000 SP node.

**Note:** You might want to turn off the timer function on the CWS to each affected RS/6000 SP node to allow installation, instance creation, and configuration to complete before the CWS updates the timer to the RS/6000 SP node. After installation, instance creation, and configuration are complete and verified, turn the timer function on again.

---

## Packages, filesets, and prerequisites

The following information shows the packages you must install for each feature. You can install all the features at the same time, but if you install them separately, you must install them in the order shown.

**32-bit client (no SSL)**

Install (in this order):

1. **Package:** `idsldap.cltbase60`



Contains the following filesets:

- idslsap.cltbase60.rte – Base client runtime
- idslsap.cltbase60.adt – Base client SDK

2. **Package:** idslsap.clt32bit60

Contains fileset idslsap.clt32bit60.rte – 32-bit client (no SSL)

**32-bit client (SSL)**

Install (in this order):

1. **Package:** idslsap.cltbase60

Contains the following filesets:

- idslsap.cltbase60.rte – Base client runtime
- idslsap.cltbase60.adt – Base client SDK

2. **Package:** idslsap.clt32bit60

Contains fileset idslsap.clt32bit60.rte – 32-bit client (no SSL)

3. **Package:** idslsap.clt\_max\_crypto32bit60

Contains fileset idslsap.clt\_max\_crypto32bit60.rte – 32-bit client (SSL)

**64-bit client (no SSL)**

Install (in this order):

1. **Package:** idslsap.cltbase60

Contains the following filesets:

- idslsap.cltbase60.rte – Base client runtime
- idslsap.cltbase60.adt – Base client SDK

2. **Package:** idslsap.clt64bit60

Contains fileset idslsap.clt64bit60.rte – 64-bit client (no SSL)

**64-bit client (SSL)**

Install (in this order):

1. **Package:** idslsap.cltbase60

Contains the following filesets:

- idslsap.cltbase60.rte – Base client runtime
- idslsap.cltbase60.adt – Base client SDK

2. **Package:** idslsap.clt64bit60

Contains fileset idslsap.clt64bit60.rte – 64-bit client (no SSL)

3. **Package:** idslsap.clt\_max\_crypto64bit60

Contains fileset idslsap.clt\_max\_crypto64bit60.rte – 64-bit client (SSL)

**Proxy server (no SSL) (64-bit). (This includes the client packages.)**

Install (in this order):

1. **Package:** idslsap.cltbase60

Contains the following filesets:

- idslsap.cltbase60.rte – Base client runtime
- idslsap.cltbase60.adt – Base client SDK

2. **Package:** idslsap.clt64bit60

Contains fileset idslsap.clt64bit60.rte – 64-bit client (no SSL)

3. **Package:** idslsap.cltjava60

Contains fileset idslsap.cltjava60.rte – Java client

**Note:** If you do not want to require X11 support, do not install the Java client.

4. **Package:** idslldap.srvproxy64bit60  
Contains fileset idslldap.srvproxy64bit60.rte – Proxy server (64-bit)
5. **Package:** idslldap.msg60.en\_US  
Contains the English messages

**Proxy server (SSL) (64-bit). (This includes the client packages.)**

Install (in this order):

1. **Package:** idslldap.cltbase60  
Contains the following filesets:
  - idslldap.cltbase60.rte – Base client runtime
  - idslldap.cltbase60.adt – Base client SDK
2. **Package:** idslldap.clt64bit60  
Contains fileset idslldap.clt64bit60.rte – 64-bit client (no SSL)
3. **Package:** idslldap.clt\_max\_crypto64bit60  
Contains fileset idslldap.clt\_max\_crypto64bit60.rte – 64-bit client (SSL)
4. **Package:** idslldap.cltjava60  
Contains fileset idslldap.cltjava60.rte – Java client (no SSL)
5. **Package:** idslldap.cltjava\_max\_crypto60  
Contains fileset idslldap.cltjava\_max\_crypto60.rte – Java client (SSL)

**Note:** If you do not want to require X11 support, do not install the Java client.

6. **Package:** idslldap.srvproxy64bit60  
Contains fileset idslldap.srvproxy64bit60.rte – Proxy server (64-bit) (no SSL)
7. **Package:** idslldap.srv\_max\_cryptoproxy64bit60  
Contains fileset idslldap.srv\_max\_cryptoproxy64bit60.rte – Proxy server (64-bit) (SSL)
8. **Package:** idslldap.msg60.en\_US  
Contains the English messages

**Full server (no SSL) (64-bit). (This includes the client packages.)**

Install (in this order):

1. **Package:** idslldap.cltbase60  
Contains the following filesets:
  - idslldap.cltbase60.rte – Base client runtime
  - idslldap.cltbase60.adt – Base client SDK
2. **Package:** idslldap.clt64bit60  
Contains fileset idslldap.clt64bit60.rte – 64-bit client (no SSL)
3. **Package:** idslldap.cltjava60  
Contains fileset idslldap.cltjava60.rte – Java client (no SSL)

**Note:** If you do not want to require X11 support, do not install the Java client.

4. **Package:** idslldap.srvproxy64bit60. Contains fileset idslldap.srvproxy64bit60.rte – Proxy server (64-bit)

5. **Package:** idslldap.srv64bit60. Contains fileset idslldap.srv64bit60.rte – Full server (no SSL) (64-bit)
6. **Package:** idslldap.msg60.en\_US  
Contains the English messages

**Full server (SSL) (64-bit). (This includes the client packages.)**

Install (in this order):

1. **Package:** idslldap.cltbase60. Contains the following filesets:
  - idslldap.cltbase60.rte – Base client runtime
  - idslldap.cltbase60.adt – Base client SDK
2. **Package:** idslldap.clt64bit60  
Contains fileset idslldap.clt64bit60.rte – 64-bit client (no SSL)
3. **Package:** idslldap.clt\_max\_crypto64bit60  
Contains fileset idslldap.clt\_max\_crypto64bit60.rte – 64-bit client (SSL)
4. **Package:** idslldap.cltjava60  
Contains fileset idslldap.cltjava60.rte – Java client (no SSL)
5. **Package:** idslldap.cltjava\_max\_crypto60  
Contains fileset idslldap.cltjava\_max\_crypto60.rte – Java client (SSL)

**Note:** If you do not want to require X11 support, do not install the Java client.

6. **Package:** idslldap.srvproxy64bit60  
Contains fileset idslldap.srvproxy64bit60.rte – Proxy server (64-bit) (no SSL)
7. **Package:** idslldap.srv\_max\_cryptoproxy64bit60  
Contains fileset idslldap.srv\_max\_crypto64bit60.rte – Proxy server (64-bit) (SSL)
8. **Package:** idslldap.srv64bit60. Contains fileset idslldap.srv64bit60.rte – Full server (no SSL) (64-bit)
9. **Package:** idslldap.msg60.en\_US  
Contains the English messages

**Web Administration Tool (no SSL)**

Install the following:

**Package:** idslldap.webadmin60

Contains fileset idslldap.webadmin60.rte – Web Administration Tool (no SSL)

**Web Administration Tool (SSL)**

Install the following:

**Package:** idslldap.webadmin\_max\_crypto60

Contains fileset idslldap.webadmin\_max\_crypto60.rte – Web Administration Tool (SSL)

---

## SMIT installation

To install IBM Tivoli Directory Server using **SMIT**:

1. Log in as **root**.
2. **If you are installing from a CD**, insert the CD containing IBM Tivoli Directory Server 6.0 into the CD-ROM drive.

**If you are installing from the .tar file:**

- a. Go to the directory where you untarred the file.
- b. If you are installing the client, server, or Web Administration Tool, go to the /itdsV60/itds subdirectory.

If you are installing a language pack for a language other than English, go to the /itdsV60/itdsLangpack directory. (You must install a language pack for the language in which you want server messages displayed. You can install the language pack before or after you install the server.)

3. At the command prompt, type the following:

```
smit install
```

and press Enter. The Software Installation and Maintenance window is displayed.

4. Click **Install and Update Software**. The Install and Update Software window is displayed.
5. Click **Install and Update from ALL Available Software**.
6. Do one of the following:
  - If you are installing from the CD, click **List** next to the **INPUT device/directory for software** field, and select the appropriate CD-ROM drive or the directory containing the IBM Tivoli Directory Server images.
  - If you are installing from the untarred file, type **.** in the **INPUT device/directory for software** field.

Click **OK**.

7. Move your cursor to **Software to install**. Do one of the following:
  - Type `idsldap` to install all the `idsldap` filesets.
  - Click **List** to list all the filesets on the CD, and then select the filesets that you want to install.

If you are installing the product and you select the list option, you see, for example:

```
idsldap.clt32bit60
 6.0.0.0      Directory Server - 32 bit Client
idsldap.clt64bit60
 6.0.0.0      Directory Server - 64 bit Client
idsldap.clt_max_crypto32bit60
 6.0.0.0      Directory Server - 32 bit Client (SSL)
idsldap.clt_max_crypto64bit60
 6.0.0.0      Directory Server - 64 bit Client (SSL)
idsldap.cltbase60
 6.0.0.0      Directory Server - Base Client
idsldap.cltjava60
 6.0.0.0      Directory Server - Java Client
idsldap.cltjava_max_crypto60
 6.0.0.0      Directory Server - Java Client (SSL)
idsldap.msg60.en_US
 6.0.0.0      Directory Server - Messages - U.S. English (en)
idsldap.srv64bit60
 6.0.0.0      Directory Server - 64 bit Server
idsldap.srv_max_cryptoproxy64bit60
 6.0.0.0      Directory Server - Proxy Server (SSL)
idsldap.srvproxy64bit60
 6.0.0.0      Directory Server - Proxy Server
idsldap.webadmin60
 6.0.0.0      Directory Server - Web Administration
idsldap.webadmin_max_crypto60
 6.0.0.0      Directory Server - Web Administration (SSL)
```

If you are installing a language pack, you see, for example:

```

> idslldap.msg60.cs_CZ      Messages - Czech (cs)
> idslldap.msg60.de_DE     Messages - German (de)
> idslldap.msg60.es_ES     Messages - Spanish (es)
> idslldap.msg60.fr_FR     Messages - French (fr)
> idslldap.msg60.hu_HU     Messages - Hungarian (hu)
> idslldap.msg60.it_IT     Messages - Italian (it)
> idslldap.msg60.ja_JP     Messages - Japanese (ja)
> idslldap.msg60.ko_KO     Messages - Korean (ko)
> idslldap.msg60.pl_PL     Messages - Polish (pl)
> idslldap.msg60.pt_BR     Messages - Brazilian Portuguese (pt_BR)
> idslldap.msg60.ru_RU     Messages - Russian (ru)
> idslldap.msg60.sk_SK     Messages - Slovak (sk)
> idslldap.msg60.zh_CN     Messages - Simplified Chinese (zh_CN)
> idslldap.msg60.zh_TW     Messages - Traditional Chinese (zh_TW)

```

Select the filesets you want to install and click **OK**.

8. Click **OK**. The message Are You Sure? is displayed.
9. Click **OK** to start the installation.
10. Check the installation summary at the end of the output to verify successful installation of the filesets.
11. Click **Done**.
12. To exit **SMIT**, press F12, or click **Cancel** until you are back to a command prompt. To verify that IBM Tivoli Directory Server was installed successfully, type the following at a command prompt:

```
lslpp -aL idslldap.*
```

The output displayed lists all the filesets starting with idslldap. For example:

```

idslldap.clt32bit60.rte      6.0.0.0   C   F   Directory Server - 32 bit
                             Client
idslldap.clt64bit60.rte     6.0.0.0   C   F   Directory Server - 64 bit
                             Client
idslldap.clt_max_crypto32bit60.rte
                             6.0.0.0   C   F   Directory Server - 32 bit
                             Client (SSL)
idslldap.clt_max_crypto64bit60.rte
                             6.0.0.0   C   F   Directory Server - 64 bit
                             Client (SSL)
idslldap.cltbase60.adt      6.0.0.0   C   F   Directory Server - Base Client
idslldap.cltbase60.rte     6.0.0.0   C   F   Directory Server - Base Client
idslldap.cltjava60.rte     6.0.0.0   C   F   Directory Server - Java Client
idslldap.cltjava_max_crypto60.rte
                             6.0.0.0   C   F   Directory Server - Java Client
                             (SSL)
idslldap.msg60.en_US       6.0.0.0   C   F   Directory Server - Messages -
                             U.S. English (en)
idslldap.srv64bit60.rte    6.0.0.0   C   F   Directory Server - 64 bit
                             Server
idslldap.srv_max_cryptoproxy64bit60.rte
                             6.0.0.0   C   F   Directory Server - 64 bit
                             Server (SSL)

```

|                                   |         |   |   |   |
|-----------------------------------|---------|---|---|---|
| idsldap.srvproxy64bit60.rte       | 6.0.0.0 | C | F | Directory Server - Proxy Server             |
| idsldap.webadmin60.rte            | 6.0.0.0 | C | F | Directory Server - Web Administration       |
| idsldap.webadmin_max_crypto60.rte | 6.0.0.0 | C | F | Directory Server - Web Administration (SSL) |

13. If you want to include security functions, install GSKit 7.0.3.3. See “Installing GSKit” on page 74.
14. If you installed the proxy server or the full server, you must install IBM Tivoli Directory Integrator 6.0 with Fix Pack 1 if you want to do the following. (If you acquire IBM Tivoli Directory Server through Passport Advantage, it includes a copy of IBM Tivoli Directory Integrator 6.0 with Fix Pack 1.)
  - Use the **idssupport** tool, which gathers information from your system that you can supply to IBM Support if you encounter problems.
  - Use the log management tool.  
You can find information about the support tool and the log management tool in the *IBM Tivoli Directory Server version 6.0 Problem Determination Guide*.
  - Use Simple Network Management Protocol (SNMP). See the *IBM Tivoli Directory Server version 6.0 Administration Guide* for information about SNMP.

**Notes:**

1. If you install the Web Administration Tool, DSML files are also copied to your computer. See Appendix L, “Installing and configuring DSML,” on page 193 for information about installing and configuring DSML.
2. If you install the Web Administration Tool, an application server such as the embedded version of WebSphere Application Server - Express is required to run the tool. See Appendix H, “Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express,” on page 183 for information about installing and configuring an application server.

---

## Command line installation using installp

**Note:** If you want to migrate from a 3.2.x version of SecureWay Directory or a version of IBM Directory Server or IBM Tivoli Directory Server, use the instructions in Chapter 4, “Migration from previous releases,” on page 23.

To install IBM Tivoli Directory Server from a command prompt:

1. Log in as **root**.
2. **If you are installing from a CD:**
  - a. Insert the CD containing IBM Tivoli Directory Server 6.0 into the CD-ROM drive and mount the CD.
  - b. If you are installing the client, server, or Web Administration Tool, go to the /itds directory on the CD.

If you are installing a language pack for a language other than English, go to the /itdsLangpack directory on the CD. (You must install a language pack for the language in which you want server messages displayed. You can install the language pack before or after you install the server.)

**If you are installing from the .tar file:**

- a. Go to the directory where you untarred the file.
- b. If you are installing the client, server, or Web Administration Tool, go to the /itdsV60/itds subdirectory.

If you are installing a language pack for a language other than English, go to the /itdsV60/itdsLangpack directory. (You must install a language pack for the language in which you want server messages displayed. You can install the language pack before or after you install the server.)

3. Determine which IBM Tivoli Directory Server packages and which language packs you need. See “Packages, filesets, and prerequisites” on page 66 for information. To see the packages that are available, type the following command:

```
installp -ld . | grep idsldap
```

A list of all the installable IBM Tivoli Directory Server packages or language packs is displayed. (This depends on which subdirectory you started the **installp** command from.)

4. At the command prompt, install the required packages by typing the following command:

```
installp -acgXd . packages
```

where :

- **-a** stands for **apply**.
- **-c** stands for **commit**.
- **-g** installs prerequisites if necessary.
- **-X** increases the file system space if needed.
- **-d** stands for **device**.
- *packages* is the package name or list of package names you want to install.

#### Examples:

To install all of the IBM Tivoli Directory Server filesets, type:

```
installp -acgXd . idsldap
```

5. Upon completion of installation, the system generates an installation summary. Verify that the Result column shows **success** for all loaded files. You can also verify that the IBM Tivoli Directory Server was installed successfully by typing the following at a command prompt:

```
lslpp -aL idsldap.*
```

The output displayed lists all the filesets starting with idsldap. This list includes the server, client, Web Administration Tool, HTML, and message filesets. For example:

|                                   |         |   |   |   |
|-----------------------------------|---------|---|---|---|
| idsldap.clt32bit60.rte            | 6.0.0.0 | C | F | Directory Server - 32 bit Client                |
| idsldap.clt64bit60.rte            | 6.0.0.0 | C | F | Directory Server - 64 bit Client                |
| idsldap.clt_max_crypto32bit60.rte | 6.0.0.0 | C | F | Directory Server - 32 bit Client (SSL)          |
| idsldap.clt_max_crypto64bit60.rte | 6.0.0.0 | C | F | Directory Server - 64 bit Client (SSL)          |
| idsldap.cltbase60.adt             | 6.0.0.0 | C | F | Directory Server - Base Client                  |
| idsldap.cltbase60.rte             | 6.0.0.0 | C | F | Directory Server - Base Client                  |
| idsldap.cltjava60.rte             | 6.0.0.0 | C | F | Directory Server - Java Client                  |
| idsldap.cltjava_max_crypto60.rte  | 6.0.0.0 | C | F | Directory Server - Java Client (SSL)            |
| idsldap.msg60.en_US               | 6.0.0.0 | C | F | Directory Server - Messages - U.S. English (en) |
| idsldap.srv64bit60.rte            | 6.0.0.0 | C | F | Directory Server - 64 bit Server                |



|  |         |   |   |   |
|--|---------|---|---|---|
| idsldap.srv_max_cryptoproxy64bit60.rte | 6.0.0.0 | C | F | Directory Server - 64 bit Server (SSL)      |
| idsldap.srvproxy64bit60.rte            | 6.0.0.0 | C | F | Directory Server - Proxy Server             |
| idsldap.webadmin60.rte                 | 6.0.0.0 | C | F | Directory Server - Web Administration       |
| idsldap.webadmin_max_crypto60.rte      | 6.0.0.0 | C | F | Directory Server - Web Administration (SSL) |

6. If you want to include security functions, install GSKit 7.0.3.3. See "Installing GSKit."
7. If you installed the proxy server or the full server, you must install IBM Tivoli Directory Integrator 6.0 with Fix Pack 1 if you want to do the following. (If you acquire IBM Tivoli Directory Server through Passport Advantage, it includes a copy of IBM Tivoli Directory Integrator 6.0 with Fix Pack 1.)
  - Use the **idssupport** tool, which gathers information from your system that you can supply to IBM Support if you encounter problems.
  - Use the log management tool.  
You can find information about the support tool and the log management tool in the *IBM Tivoli Directory Server version 6.0 Problem Determination Guide*.
  - Use Simple Network Management Protocol (SNMP). See the *IBM Tivoli Directory Server version 6.0 Administration Guide* for information about SNMP.

**Notes:**

1. If you install the Web Administration Tool, DSML files are also copied to your computer. See Appendix L, "Installing and configuring DSML," on page 193 for information about installing and configuring DSML.
2. If you install the Web Administration Tool, an application server such as the embedded version of WebSphere Application Server - Express is required to run the tool. See Appendix H, "Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express," on page 183 for information about installing and configuring an application server.

---

## Installing GSKit

If you installed an SSL-enabled version of IBM Tivoli Directory Server, you must install GSKit to take advantage of the security features. You can use either SMIT or **installp**.

To install using SMIT:

1. Invoke SMIT by typing `smi t` at the command line.
2. Select **Software Installation & Maintenance**.
3. Select **Install and Update Software**.
4. Select **Install and Update from ALL Available Software**.
5. On the device/directory window specify the directory that contains the installable software.
6. Select the **gskta** and **gksa** packages from the multi-select list.
7. Select the filesets of the software packages to install
8. Select the options appropriate to your installation requirements from the Options window.

**Note:** Set the **Install all prereqs** option to **yes**.



9. Confirm that you want to complete the installation.

The **installp** command installs available software products in a compatible installation package. To install GSKit using **installp**, enter the following at a command prompt:

```
installp -acgXd . gskta.rte  
installp -acgXd . gsksa.rte
```

where

- **-a** stands for **apply**
- **-c** stands for **commit**
- **-g** automatically installs or commits any requisite software product.
- **-X** expands the filesystem if necessary.
- **-d** stands for **device**. This specifies where the installation media can be found.

See Appendix O, “Setting up GSKit to support CMS key databases,” on page 201 for more information about setting up GSKit after installation.

## Setting system variables for GSKit

You must set the following variable so that ikeyman can run:

**JAVA\_HOME**=*location*, where *location* is the location where JDK 1.4.2 is installed.

**Note:** If you are prompted to set **JAVA\_HOME**, you can set it to the system-installed Java. You also need to set the **LIBPATH** environment variable as follows:

```
export LIBPATH=$JAVA_HOME/bin:$JAVA_HOME/bin/classic:$LIBPATH
```

## Removing GSKit

To remove GSKit using SMIT:

1. Invoke SMIT by typing **smit** at the command line.
2. Select **Software Installation and Maintenance** on the menu.
3. Select **Software Maintenance and Utilities**.
4. On the Maintenance window, select **Remove Installed Software** to open the Remove Software Product window.
5. Enter the name of the software package
6. Set the flag for **REMOVE dependent software?** to **YES** to instruct the system to automatically remove software products and updates that are dependent upon the product you are removing.
7. Confirm the procedure to complete the removal of the software package.

To remove GSKit using **installp**, type the following at a command prompt:

```
installp -u -g -V2 gskta.rte  
installp -u -g -V2 gsksa.rte
```

where

- **-u** removes the specified software and any of its installed updates from the system.
- **-g** removes or rejects dependents of the specified software.
- **-V2** prints an alphabetically ordered list of **FAILURES** and **WARNINGS**.



---

## Chapter 9. Installing IBM Tivoli Directory Server using Linux utilities

**Attention:** If you are migrating from SecureWay Directory 3.2.2, IBM Directory Server 4.1 or 5.1, or IBM Tivoli Directory Server 5.2, use the appropriate migration process in Chapter 4, “Migration from previous releases,” on page 23. This chapter contains instructions for migrating and restoring backed-up files after reinstallation. It is very important that you back up and export previous versions of schema files and the server configuration file before installing IBM Tivoli Directory Server 6.0.

---

### Installing IBM Tivoli Directory Server

Before you install IBM Tivoli Directory Server, be sure you have a supported version of DB2 installed. (See “Requirements on xSeries Linux operating systems” on page 13, “Requirements on zSeries Linux operating systems” on page 15, or “Requirements on iSeries and pSeries Linux operating systems” on page 17 for supported versions of DB2.) If you want to use the version of DB2 provided with IBM Tivoli Directory Server, you must use the **db2\_install** utility to install it. (If you do not use this utility, the DB2 license file is not added correctly.) The **db2\_install** utility is in the /db2 directory of the IBM Tivoli Directory Server CD-ROM if you created one, or in the following subdirectory of the directory where you untarred the DB2 tar file for Linux:

- db2v8fp8refresh-ese-lin-ia32 for xSeries Linux
- db2v8fp8refresh-ese-lin-s390 for zSeries Linux
- db2v8fp8refresh-ese-lin-ppc for iSeries and pSeries Linux

**Notes:**

1. The **db2\_install** utility can install only in a C or en\_US locale. If you are installing on a computer with a different locale, set the locale in a shell to C or en\_US before you use the **db2\_install** utility.
2. After you start the **db2\_install** utility, you are prompted for a keyword. In response to this prompt, type DB2.ESE.
3. After you install DB2, you can check the following two files to verify that the installation was successful:  
    /tmp/db2\_install.rc.99999  
    /tmp/db2\_instal\_log.99999

99999 is a random number associated with the installation.

If you are installing the Web Administration Tool, you must install an application server such as the embedded version of WebSphere Application Server - Express. See Appendix H, “Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express,” on page 183 for information.

### Packages

The IBM Tivoli Directory Server for the Linux operating system is provided in the following packages.

**xSeries Linux packages:**

- idldap-cltbase60-6.0.0-0.i386.rpm – IBM Directory Server - Base Client
- idldap-clt32bit60-6.0.0-0.i386.rpm – IBM Directory Server - 32 bit Client

Requires idldap-cltbase60-6.0.0-0.i386.rpm

- idldap-cltjava60-6.0.0-0.i386.rpm – IBM Directory Server - Java Client
- idldap-srvproxy32bit60-6.0.0-0.i386.rpm – IBM Directory Server - Proxy Server

Requires idldap-clt32bit60-6.0.0-0.i386.rpm and idldap-cltjava60-6.0.0-0.i386.rpm

- idldap-srv32bit60-6.0.0-0.i386.rpm – IBM Directory Server - 32 bit Server  
Requires idldap-srvproxy32bit60-6.0.0-0.i386.rpm and its prerequisites
- idldap-webadmin60-6.0.0-0.i386.rpm – IBM Directory Server - Web Administration
- idldap-msg60-en-6.0.0-0.i386.rpm – IBM Directory Server - Messages U.S. English (en)

#### **zSeries Linux packages:**

- idldap-cltbase60-6.0.0-0.s390.rpm – IBM Directory Server - Base Client
- idldap-clt32bit60-6.0.0-0.s390.rpm – IBM Directory Server - 32 bit Client  
Requires idldap-cltbase60-6.0.0-0.s390.rpm
- idldap-clt64bit60-6.0.0-0.s390x.rpm – IBM Directory Server - 64 bit Client  
Requires idldap-cltbase60-6.0.0-0.s390.rpm
- idldap-cltjava60-6.0.0-0.s390.rpm – IBM Directory Server - Java Client
- idldap-srvproxy32bit60-6.0.0-0.s390.rpm – IBM Directory Server - Proxy Server  
Requires idldap-clt32bit60-6.0.0-0.s390.rpm and idldap-cltjava60-6.0.0-0.s390.rpm
- idldap-srv32bit60-6.0.0-0.s390.rpm – IBM Directory Server - 32 bit Server  
Requires idldap-srvproxy32bit60-6.0.0-0.s390.rpm and its prerequisites
- idldap-webadmin60-6.0.0-0.s390.rpm – IBM Directory Server - Web Administration
- idldap-msg60-en-6.0.0-0.s390.rpm – IBM Directory Server - Messages U.S. English (en)

#### **iSeries and pSeries Linux packages:**

- idldap-cltbase60-6.0.0-0.ppc.rpm – IBM Directory Server - Base Client
- idldap-clt32bit60-6.0.0-0.ppc.rpm – IBM Directory Server - 32 bit Client  
Requires idldap-cltbase60-6.0.0-0.ppc.rpm
- idldap-clt64bit60-6.0.0-0.ppc64.rpm – IBM Directory Server - 64 bit Client  
Requires idldap-cltbase60-6.0.0-0.ppc.rpm
- idldap-cltjava60-6.0.0-0.ppc.rpm – IBM Directory Server - Java Client
- idldap-srvproxy32bit60-6.0.0-0.ppc.rpm – IBM Directory Server - Proxy Server  
Requires idldap-clt32bit60-6.0.0-0.ppc.rpm and idldap-cltjava60-6.0.0-0.ppc.rpm
- idldap-srv32bit60-6.0.0-0.ppc.rpm – IBM Directory Server - 32 bit Server  
Requires idldap-srvproxy32bit60-6.0.0-0.ppc.rpm and its prerequisites
- idldap-webadmin60-6.0.0-0.ppc.rpm – IBM Directory Server - Web Administration

- `idsldap-msg60-en-6.0.0-0.ppc.rpm` – IBM Directory Server - Messages U.S. English (en)

**Note:** The instructions in this chapter use Linux Intel-based packages. For zSeries, iSeries, or pSeries Linux, substitute the appropriate package names.

## Installing features

To install the proxy server or the full server:

1. Log in as **root**.
2. Install the 32-bit client by typing the following at a command prompt:
 

```
rpm -ihv idsldap-cltbase60-6.0.0-0.i386.rpm
rpm -ihv idsldap-clt32bit60-6.0.0-0.i386.rpm
```
3. Depending on which type of server you want, do one of the following:
  - Install the proxy server by typing the following at a command prompt:
 

```
rpm -ihv idsldap-cltjava60-6.0.0-0.i386.rpm
rpm -ihv idsldap-srvproxy32bit60-6.0.0-0.i386.rpm
```
  - Install the full server by typing the following at a command prompt:
 

```
rpm -ihv idsldap-cltjava60-6.0.0-0.i386.rpm
rpm -ihv idsldap-srvproxy32bit60-6.0.0-0.i386.rpm
rpm -ihv idsldap-srv32bit60-6.0.0-0.i386.rpm
```
4. Verify that the packages have been installed correctly by typing the following at a command prompt:
 

```
rpm -qa | grep idsldap
```

If the product has been successfully installed, the following is displayed:

- For the proxy server:
 

```
idsldap-cltbase60-6.0.0-0
idsldap-clt32bit60-6.0.0-0
idsldap-cltjava60-6.0.0-0
idsldap-srvproxy32bit60-6.0.0-0
```
  - For the full server:
 

```
idsldap-cltbase60-6.0.0-0
idsldap-clt32bit60-6.0.0-0
idsldap-cltjava60-6.0.0-0
idsldap-srvproxy32bit60-6.0.0-0
idsldap-srv32bit60-6.0.0-0
```
5. Install the English messages:
 

```
rpm -ihv idsldap-msg60-en-6.0.0-0.i386.rpm
```

You can install messages in other languages by using the package names for those languages. These names are:

    - German: `idsldap-msg60-de-6.0.0-0.noarch.rpm`
    - Spanish: `idsldap-msg60-es-6.0.0-0.noarch.rpm`
    - French: `idsldap-msg60-fr-6.0.0-0.noarch.rpm`
    - Italian: `idsldap-msg60-it-6.0.0-0.noarch.rpm`
    - Japanese: `idsldap-msg60-ja-6.0.0-0.noarch.rpm`
    - Korean: `idsldap-msg60-ko-6.0.0-0.noarch.rpm`
    - Brazilian Portuguese: `idsldap-msg60-pt_BR-6.0.0-0.noarch.rpm`
    - Simplified Chinese: `idsldap-msg60-zh_CN-6.0.0-0.noarch.rpm`
    - Traditional Chinese: `idsldap-msg60-zh_TW-6.0.0-0.noarch.rpm`
  6. If you want to include security functions, install GSKit 7.0.3.3. See “Installing GSKit” on page 80.

7. If you installed the proxy server or the full server, you must install IBM Tivoli Directory Integrator 6.0 with Fix Pack 1 if you want to do the following. (If you acquire IBM Tivoli Directory Server through Passport Advantage, it includes a copy of IBM Tivoli Directory Integrator 6.0 with Fix Pack 1.)

- Use the **idssupport** tool, which gathers information from your system that you can supply to IBM Support if you encounter problems
- Use the log management tool
- Use Simple Network Management Protocol (SNMP)

You can find information about the support tool and the log management tool in the *IBM Tivoli Directory Server version 6.0 Problem Determination Guide*.

#### To install the client only:

Install the 32-bit client by typing the following at a command prompt:

```
rpm -ihv idslldap-cltbase60-6.0.0-0.i386.rpm
rpm -ihv idslldap-clt32bit60-6.0.0-0.i386.rpm
```

To install the **Web Administration Tool**, type the following at a command prompt:

```
rpm -ihv idslldap-webadmin60-6.0.0-0.i386.rpm
```

#### Notes:

1. If you install the Web Administration Tool, DSML files are also copied to your computer. See Appendix L, "Installing and configuring DSML," on page 193 for information about installing and configuring DSML.
2. If you install the Web Administration Tool, an application server such as the embedded version of WebSphere Application Server - Express is required to run the tool. See Appendix H, "Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express," on page 183 for information about installing and configuring an application server.

---

## Installing GSKit

Use the following information to install GSKit 7.0.3.3 through the command line.

The package names for GSKit 7.0.3.3 on the Linux platforms are as follows:

#### xSeries Linux:

```
gsk7bas-7.0-3.3.i386.rpm
```

#### zSeries Linux (32-bit):

```
gsk7bas-7.0-3.3.s390.rpm
```

#### zSeries Linux (64-bit):

```
gsk7bas-7.0-3.3.s390x.rpm
```

#### iSeries and pSeries Linux (32-bit):

```
gsk7bas-7.0-3.3.ppc32.rpm
```

#### iSeries and pSeries Linux (64-bit):

```
gsk7bas-7.0-3.3.ppc64.rpm
```

To install GSKit using **rpm**, log in as **root**, go to the directory where the GSKit file is, and type the following at a command prompt: (This example uses the xSeries Linux package name.)

```
rpm -ihv gsk7bas-7.0-3.3.i386.rpm
```

See Appendix O, “Setting up GSKit to support CMS key databases,” on page 201 for more information about setting up GSKit after installation.

## Removing GSKit

To remove GSKit, type the following at a command prompt:

```
rpm -evv gsk7bas-7.0-3.3
```

where

- **-evv** specifies to erase the package and display debugging information. If no trace or debug information is desired, use only **-e**.





---

## Chapter 10. Installing IBM Tivoli Directory Server using Solaris utilities

**Attention:** If you are migrating from SecureWay Directory 3.2.2, IBM Directory Server 4.1 or 5.1, or IBM Tivoli Directory Server 5.2, use the appropriate migration process in Chapter 4, “Migration from previous releases,” on page 23. This chapter contains instructions for migrating and restoring backed-up files after reinstallation. It is very important that you back up and export previous versions of schema files and the server configuration file before installing IBM Tivoli Directory Server 6.0.

---

### Before you install

Before you install IBM Tivoli Directory Server, be sure you have a supported version of DB2 installed. (See “Requirements on Solaris operating systems” on page 19 for supported versions of DB2.) If you want to use the version of DB2 provided with IBM Tivoli Directory Server, you must use the **db2\_install** utility to install it. (If you do not use this utility, the DB2 license file is not added correctly.) The **db2\_install** utility is in the /db2 directory of the IBM Tivoli Directory Server CD-ROM for DB2 if you created one, or in the db2v8fp8refresh-ese-sol-sparc directory of the directory where you untarred the DB2 tar file for Solaris.

#### Notes:

1. The **db2\_install** utility can install only in a C or en\_US locale. If you are installing on a computer with a different locale, set the locale in a shell to C or en\_US before you use the **db2\_install** utility.
2. After you start the **db2\_install** utility, you are prompted for a keyword. In response to this prompt, type DB2.ESE. When you are asked if you want to install to a directory other than the /opt directory, be sure to accept the default of /opt. IBM Tivoli Directory Server assumes that DB2 is installed in this directory.
3. You might see the message `test: argument expected` at the end of installation. You can ignore this message. After you install DB2, you can check the following two files to verify that the installation was successful:  
    /tmp/db2\_install.rc.99999  
    /tmp/db2\_instal\_log.99999

99999 is a random number associated with the installation.

If you have a client from IBM Directory Server 4.1 or 5.1 or IBM Tivoli Directory Server 5.2, you can leave it installed. The server and the client from IBM Tivoli Directory Server 6.0 can coexist with a client from one of these versions.

If you are installing the Web Administration Tool, you must install an application server such as the embedded version of WebSphere Application Server - Express. See Appendix H, “Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express,” on page 183 for information.

### Setting kernel parameters

You might need to update kernel parameters in the /etc/system file before you configure the database.

With the Solaris versions of DB2, version 8.1, a utility called **db2osconf** is provided. The **db2osconf** utility determines the correct kernel settings for your computer.

On the Solaris Operating Environment, there are two versions of the **db2osconf** utility: one for 64-bit kernels and one for 32-bit kernels. The utility must be run as root or with the group sys because it accesses the following special devices (accesses are read-only):

```
crw-r----- 1 root  sys      13,  1 Jul 19 18:06 /dev/kmem
crw-rw-rw-  1 root  sys      72,  0 Feb 19 1999 /dev/ksyms
crw-r----- 1 root  sys      13,  0 Feb 19 1999 /dev/mem
```

1. To run the utility, type **db2osconf** at a command prompt.

**Note:** To view the usage information for the utility, type **db2osconf -h**. The following information is displayed (but the parameters vary depending on the version of the utility that you have):

```
Usage:
-c                # Client only
-f                # Compare to current
-h                # Help screen
-l                # List current
-m <mem in GB>   # Specify memory in GB
-n <num CPUs>    # Specify number of CPUs
-p <perf level>  # Msg Q performance level (0-3)
-s <scale factor> # Scale factor (1-3)
-t <scale factor> # Number of threads
```

2. Use the output from the **db2osconf** utility to update the `/etc/system` file.

The following is an example of output:

```
set msgsys:msginfo_msgmax = 65535
set msgsys:msginfo_msgmnb = 65535
set msgsys:msginfo_msgmni = 1280
set msgsys:msginfo_msgtql = 1280
set semsys:seminfo_semmni = 1536
set semsys:seminfo_semmns = 3226
set semsys:seminfo_semmnu = 1536
set semsys:seminfo_semume = 240
set shmsys:shminfo_shmmax = 466086297
set shmsys:shminfo_shmmni = 1536
set shmsys:shminfo_shmseg = 240
```

```
Total kernel space for IPC:
0.21MB (shm) + 1.47MB (sem) + 1.22MB (msg) == 2.91MB (total)
```

End suggestions.

**Note:** If you do not use the **-l** or **-f** flags, the **db2osconf** utility displays the kernel parameters using the syntax of the `/etc/system` file. To prevent errors, you can copy and paste this output directly into the `/etc/system` file.

For more information, see the DB2 documentation.

If you make updates to your system configuration, run the utility again.

---

## Installing IBM Tivoli Directory Server

You can use either the **admintool** utility or **pkgadd** from a command prompt to install IBM Tivoli Directory Server.

**Note:** You do not need to install security functions if you are not going to use them. You can provide SSL by installing Global Security Kit (GSKit). See “Installing GSKit” on page 90 for information about installing GSKit.

The following instructions assume that you are installing from a CD-ROM drive.

## Package dependencies

The following IBM Tivoli Directory Server packages are available for installation:

- IDSlbc60: Base client
- IDSl32c60: 32-bit client
- IDSl64c60: 64-bit client
- IDSljc60: Java client
- IDSl32p60: Proxy server
- IDSl32s60: Full server (32-bit)
- IDSlweb60: Web Administration Tool
- IDSlen60: English messages

Because of package dependencies, the order of installation is significant. Install the packages in the following order:

### For the 32-bit client only:

Install in the following order:

1. Base client
2. 32-bit client

### For the 64-bit client only:

Install in the following order:

1. Base client
2. 64-bit client

### For the proxy server:

Install in the following order:

1. Base client
2. 32-bit client
3. Java client
4. Proxy server
5. English messages (can be in any order)

### For the full server:

Install in the following order:

1. Base client
2. 32-bit client
3. Java client
4. Proxy server
5. Full server
6. English messages (can be in any order)

If you do not install in the order shown, the installation fails.

**Note:** Because the Web Administration Tool package has no dependencies on any of the other packages, and none of the other packages are dependent on it, you can install it in any order.

## AdminTool installation

**Note:** The AdminTool might not be available on some versions of Solaris.

To install IBM Tivoli Directory Server using the **admintool** utility:

1. Log in as **root**.
2. Type the following at a root command prompt: **admintool** &  
The Users window is displayed.
3. Click **Browse** —> **Software**. The Software window is displayed.
4. Click **Edit** —> **Add**. The Set Source Media window is displayed.

**Attention:** Do not click **Customize** in the lower left corner of the Set Source Media window. If you click **Customize**, the AdminTool installation stops. Because LDAP does not have any customizable options, there is no need for you to click **Customize**.

The following two steps are only needed for the first package you install. For subsequent packages, the path is already set.

5. Select **CD with Volume Management**. The CD-ROM path defaults to `/cdrom/cdrom0/`
6. Change the path to `/cdrom/cdrom0/itds` and click **OK**.
7. Click **OK**.
8. Select a package from the following list of installable packages:

```
IBM Directory Server - Base Client
IBM Directory Server - 32 bit Client
IBM Directory Server - 64 bit Client
IBM Directory Server - Java Client
IBM Directory Server - Proxy Server
IBM Directory Server - 32 bit Server
IBM Directory Server - Web Administration
IBM Directory Server - Messages - U.S. English (en)
```

Remember that you must install the packages in the correct order. See “Package dependencies” on page 85 for the correct installation sequence.

9. Click **Add**.

### Notes:

- a. With the installation of client and server packages, the system prompts you with the following notice: This package contains scripts which will be executed with super-user permission during the process of installing the package. These scripts create the IBM Tivoli Directory Server user ID. Type **y** to continue.
- b. If you are installing the server package, you will also see the prompt, Do you want to install these as `setuid/setgid` files? Type **y** to continue.

After the package is installed, the Software window is displayed.

10. Repeat steps 4 through 9 for each additional package you want to install. When you have finished installing the packages, select **File** —> **Exit** to exit the **admintool** utility.
11. If you want to include security functions, install GSKit 7.0.3.3. See “Installing GSKit” on page 90.
12. If you installed the proxy server or the full server, you must install IBM Tivoli Directory Integrator 6.0 with Fix Pack 1 if you want to do the following. (If

you acquire IBM Tivoli Directory Server through Passport Advantage, it includes a copy of IBM Tivoli Directory Integrator 6.0 with Fix Pack 1.)

- Use the **idssupport** tool, which gathers information from your system that you can supply to IBM Support if you encounter problems
- Use the log management tool
- Use Simple Network Management Protocol (SNMP)

You can find information about the support tool and the log management tool in the *IBM Tivoli Directory Server version 6.0 Problem Determination Guide*.

**Notes:**

1. If you install the Web Administration Tool, DSML files are also copied to your computer. See Appendix L, “Installing and configuring DSML,” on page 193 for information about installing and configuring DSML.
2. If you install the Web Administration Tool, an application server such as the embedded version of WebSphere Application Server - Express is required to run the tool. See Appendix H, “Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express,” on page 183. for information about installing and configuring an application server.

## Command line installation using pkgadd

To install IBM Tivoli Directory Server from a command prompt:

1. Log in as **root**.
2. If you are installing from a CD, go to:
  - The /itds directory of the CD to install IBM Tivoli Directory Server packages
  - The /itdsLangpack directory of the CD to install language packs for languages other than English

If you are installing from a downloaded tar file, go to:

- The itdsV60/itds subdirectory of the directory where you untarred the tar file to install IBM Tivoli Directory Server packages
  - The itdsV60/itdsLangpack directory of the directory where you untarred the tar file to install language packs for languages other than English
3. 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. Be sure to install in the order shown in “Package dependencies” on page 85.

*Table 1. IBM Tivoli Directory Server packages for Solaris*

| Package                              | Package name | File name              |
|--------------------------------------|--------------|------------------------|
| IBM Directory Server - Base Client   | IDS1bc60     | idsldap.cltbase60.pkg  |
| IBM Directory Server - 32 bit Client | IDS132c60    | idsldap.clt32bit60.pkg |
| IBM Directory Server - 64 bit Client | IDS164c60    | idsldap.clt64bit60.pkg |
| IBM Directory Server - Java Client   | IDS1jc60     | idsldap.cltjava60.pkg  |

Table 1. IBM Tivoli Directory Server packages for Solaris (continued)

| Package   | Package name | File name                   |
|---|--------------|-----------------------------|
| IBM Directory Server - Proxy Server               | IDS132p60    | idsldap.srvproxy32bit60.pkg |
| IBM Directory Server - 32 bit Server              | IDS132s60    | idsldap.srv32bit60.pkg      |
| IBM Directory Server - Web Administration         | IDS1web60    | idsldap.webadmin60.pkg      |
| IBM Directory Server - Messages U.S. English (en) | IDS1en60     | idsldap.msg60.en.pkg        |

Table 2. IBM Tivoli Directory Server language packages for Solaris

| Package  | Package name | File name               |
|--|--------------|-------------------------|
| IBM Directory Server - Messages German (de)              | IDS1de60     | idsldap.msg60.de.pkg    |
| IBM Directory Server - Messages Spanish (es)             | IDS1es60     | idsldap.msg60.es.pkg    |
| IBM Directory Server - Messages French (fr)              | IDS1fr60     | idsldap.msg60.fr.pkg    |
| IBM Directory Server - Messages Italian (it)             | IDS1it60     | idsldap.msg60.it.pkg    |
| IBM Directory Server - Messages Japanese (ja)            | IDS1ja60     | idsldap.msg60.ja.pkg    |
| IBM Directory Server - Messages Korean (ko)              | IDS1ko60     | idsldap.msg60.ko.pkg    |
| IBM Directory Server - Messages Brazilian (br)           | IDS1br60     | idsldap.msg60.pt_BR.pkg |
| IBM Directory Server - Messages Simplified Chinese (cn)  | IDS1cn60     | idsldap.msg60.zh_CN.pkg |
| IBM Directory Server - Messages Traditional Chinese (tw) | IDS1tw60     | idsldap.msg60.zh_TW.pkg |

The following instructions show you how to install different features:

- To install the 32-bit client, type:
 

```
pkgadd -d idsldap.cltbodyase60.pkg
pkgadd -d idsldap.cltbody32bit60.pkg
```
- To install the 64-bit client, type:
 

```
pkgadd -d idsldap.cltbodyase60.pkg
pkgadd -d idsldap.cltbody64bit60.pkg
```
- To install the proxy server (with English messages), type:
 

```
pkgadd -d idsldap.cltbodyase60.pkg
pkgadd -d idsldap.cltbody32bit60.pkg
pkgadd -d idsldap.cltbodyjava60.pkg
pkgadd -d idsldap.srvtbodyproxy32bit60.pkg
pkgadd -d idsldap.msg60.en.pkg
```
- To install the full server (with English messages), type:
 

```
pkgadd -d idsldap.cltbodyase60.pkg
pkgadd -d idsldap.cltbody32bit60.pkg
pkgadd -d idsldap.cltbodyjava60.pkg
pkgadd -d idsldap.srvtbodyproxy32bit60.pkg
pkgadd -d idsldap.srvtbody32bit60.pkg
pkgadd -d idsldap.msg60.en.pkg
```

**Notes:**

- a. When you install client or server packages, the system might prompt you with the following query: This package contains scripts which will be executed with super-user permission during the process of installing the package. Continue with installation?  
Type *y* to continue. These scripts create the IBM Tivoli Directory Server user ID.
  - b. If you are installing a server package, you might also see the following prompt: Do you want to install these as *setuid* and/or *setgid* files?  
Type *y* to continue. The programs must be able to start daemons, run DB2 commands, and create the IBM Tivoli Directory Server DB2 instance user ID and group, so they must occasionally run as root.
- To install messages in another language, type the following:  

```
pkgadd -d idsldap.msg60.language_ID.pkg
```

where *language\_ID* is one of the following:

- **de** for German
  - **es** for Spanish
  - **fr** for French
  - **it** for Italian
  - **ja** for Japanese
  - **ko** for Korean
  - **pt\_BR** for Brazilian Portuguese
  - **zh\_CN** for simplified Chinese
  - **zh\_TW** for traditional Chinese
- To install the Web Administration Tool package, type:  

```
pkgadd -d idsldap.webadmin60.pkg
```

**Notes:**

- a. If you install the Web Administration Tool, DSML files are also copied to your computer. See Appendix L, "Installing and configuring DSML," on page 193 for information about installing and configuring DSML.
  - b. If you install the Web Administration Tool, an application server such as the embedded version of WebSphere Application Server - Express is required to run the tool. See Appendix H, "Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express," on page 183 for information about installing and configuring an application server.
4. If you want to include security functions, install GSKit 7.0.3.3. See "Installing GSKit" on page 90.
  5. If you installed the proxy server or the full server, you must install IBM Tivoli Directory Integrator 6.0 with Fix Pack 1 if you want to do the following. (If you acquire IBM Tivoli Directory Server through Passport Advantage, it includes a copy of IBM Tivoli Directory Integrator 6.0 with Fix Pack 1.)
    - Use the **idssupport** tool, which gathers information from your system that you can supply to IBM Support if you encounter problems
    - Use the log management tool
    - Use Simple Network Management Protocol (SNMP)

You can find information about the support tool and the log management tool in the *IBM Tivoli Directory Server version 6.0 Problem Determination Guide*.

---

## Installing GSKit

You can install GSKit 7.0.3.3 using either the AdminTool or the command line.

To install GSKit using the **admintool** utility:

1. Log in as **root**.
2. Type the following at a root command prompt: `admintool&`  
The Users window is displayed.
3. Click **Browse** —> **Software**. The Software window is displayed.
4. Click **Edit** —> **Add**. The Set Source Media window is displayed.
5. In the **Path** field, type the full path name to the directory that contains the GSKit installation code. For example, if you are installing from a CD-ROM:  
`/cdrom/cdrom0/gskit`
6. Click **OK**.
7. Select **Certificate and SSL Base Runtime (gsk7bas)**
8. Click **Add**. You are asked if you want to continue the installation.
9. Type `y` and press Enter. After the package is installed, a message is displayed and you are instructed to press Return.
10. Press Enter.
11. When you are finished installing packages, click **File** —> **Exit** to exit the **admintool** utility.

To install GSKit using the command line:

1. Insert the CD.
2. Log in as **root**.
3. At the command prompt, install the required tar file sets with the following command:  
`pkgadd -d /cdrom/cdrom0/gskit`

See Appendix O, “Setting up GSKit to support CMS key databases,” on page 201 for more information about setting up GSKit after installation.

## Removing GSKit

To remove GSKit, type the following at a command prompt:

```
pkgrm gsk7bas
```



---

## Chapter 11. Installing IBM Tivoli Directory Server using HP-UX utilities

**Attention:** If you are migrating from SecureWay Directory 3.2.2, IBM Directory Server 4.1 or 5.1, or IBM Tivoli Directory Server 5.2, use the appropriate migration process in Chapter 4, “Migration from previous releases,” on page 23. This chapter contains instructions for migrating and restoring backed-up files after reinstallation. It is very important that you back up and export previous versions of schema files and the server configuration file before installing IBM Tivoli Directory Server 6.0.

---

### Before you install

Before you install IBM Tivoli Directory Server, you must have the following:

**DB2** Before you install IBM Tivoli Directory Server, be sure you have a supported version of DB2 installed. (See “Requirements on HP-UX operating systems” on page 21 for supported versions of DB2.) If you want to use the version of DB2 provided with IBM Tivoli Directory Server, you must use the **db2\_install** utility to install it. The **db2\_install** utility is in the /db2 directory of the IBM Tivoli Directory Server CD-ROM if you created one, or in the db2v8fp2refresh-ese-hpux-parisc directory of the directory where you untarred the DB2 tar file for HP-UX.

Before installing DB2, you must remove any existing versions of DB2 that might have been installed previously. If you try to install DB2 over an existing version of DB2, DB2 does not install correctly. If this occurs you must remove DB2 and then reinstall it.

#### Notes:

1. The **db2\_install** utility can install only in a C or en\_US locale. If you are installing on a computer with a different locale, set the locale in a shell to C or en\_US before you use the **db2\_install** utility.
2. After you start the **db2\_install** utility, you are prompted for a keyword. In response to this prompt, type DB2.ESE.
3. You might see the message `test: argument expected` at the end of installation. You can ignore this message. After you install DB2, you can check the following file to verify that the installation was successful:  
/tmp/db2\_instal\_log.99999. (99999 is a random number associated with the installation.)

After you install DB2, use the following command to add the DB2 license:

- If you installed from the untarred DB2 tar file:

```
/opt/IBM/db2/V8.1/adm/db2licm  
-a <path>/db2v8fp2refresh-ese-hpux-parisc/db2/license/DB2_81fp2ese.lic
```

where *<path>* is the path to the untarred DB2 tar file.

- If you installed from a CD:

```
/opt/IBM/db2/V8.1/adm/db2licm -a <path>/db2/db2/license/DB2_81fp2ese.lic
```

where *<path>* is the mount point for the CD-ROM.

**Java** You must have the Java Runtime Environment 1.4.2 installed. The Java

Runtime Environment 1.4.2 is provided in the /java subdirectory of the IBM Tivoli Directory Server CD-ROM if you created one, or in the itdsV60/java subdirectory of the directory where you untarred the IBM Tivoli Directory Server .tar file. The file name is hpux142hybrid-20040916-1.4.2\_06-jre.tar.

To install the Java Runtime Environment 1.4.2:

1. Create the following directory: /opt/IBM/ldap/V6.0/java
2. Change directories to the /opt/IBM/ldap/V6.0/java directory.
3. Type the following at a command prompt:  

```
tar -xvf javapath /java/hpux142hybrid-20040916-1.4.2_06-jre.tar
```

where *javapath* is the path where the IBM Tivoli Directory Server CD is mounted or the path where you untarred the IBM Tivoli Directory Server file, with /itdsV60 appended.

### Application server

If you are installing the Web Administration Tool, you must install an application server such as the embedded version of WebSphere Application Server - Express. See Appendix H, "Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express," on page 183 for information.

If you have a client from IBM Directory Server 4.1 or 5.1 or IBM Tivoli Directory Server 5.2, you can leave it installed. The server and the client from IBM Tivoli Directory Server 6.0 can coexist with a client from one of these versions.

## Setting the kernel configuration parameters

You might need to update kernel parameters in the /etc/system file before you create a directory server instance and configure a database for it.

With the HP-UX version of DB2, version 8.1, a utility called **db2osconf** is provided. (Look for this utility in the /opt/IBM/db2/V8.1/bin64/db2osconf directory.) The **db2osconf** utility determines the correct kernel settings for your computer.

The utility must be run as root or with the group sys because it accesses the following special devices (accesses are read-only):

```
crw-r----- 1 root    sys      13,  1 Jul 19 18:06 /dev/kmem
crw-rw-rw-  1 root    sys      72,  0 Feb 19 1999 /dev/ksyms
crw-r----- 1 root    sys      13,  0 Feb 19 1999 /dev/mem
```

1. To run the utility, type db2osconf at a command prompt.

**Note:** To view the usage information for the utility, type db2osconf -h. The following information is displayed (but the parameters vary depending on the version of the utility that you have):

```
Usage:
-c          # Client only
-f          # Compare to current
-h          # Help screen
-l          # List current
-m <mem in GB> # Specify memory in GB
-n <num CPUs> # Specify number of CPUs
-p <perf level> # Msg Q performance level (0-3)
-s <scale factor> # Scale factor (1-3)
-t <scale factor> # Number of threads
```

2. Use the output from the **db2osconf** utility to update the /etc/system file.

The following is an example of output:

```
set msgsys:msginfo_msgmax = 65535
set msgsys:msginfo_msgmnb = 65535
set msgsys:msginfo_msgmni = 1280
set msgsys:msginfo_msgtql = 1280
set semsys:seminfo_semmni = 1536
set semsys:seminfo_semmns = 3226
set semsys:seminfo_semmnu = 1536
set semsys:seminfo_semume = 240
set shmsys:shminfo_shmmax = 466086297
set shmsys:shminfo_shmmni = 1536
set shmsys:shminfo_shmseg = 240
```

```
Total kernel space for IPC:
0.21MB (shm) + 1.47MB (sem) + 1.22MB (msg) == 2.91MB (total)
```

End suggestions.

**Note:** If you do not use the **-l** or **-f** flags, the **db2osconf** utility displays the kernel parameters using the syntax of the `/etc/system` file. To prevent errors, you can copy and paste this output directly into the `/etc/system` file.

For more information, see the DB2 documentation.

If you make updates to your system configuration, run the utility again.

To set a kernel configuration parameter:

1. At a command prompt, type: `sam`  
The System Administration Manager opens.
2. Double-click **Kernel Configuration**.
3. Double-click **Configurable Parameters**.
4. Double-click the parameter you want to edit and type the new value in the **Enter New Formula/Value** field. Click **OK**.
5. Repeat step 4 for each parameter that needs to be set.
6. Click **Actions** —> **Process New Kernel**.
7. To process the modifications, click **Yes**.
8. Select **Move Kernel Into Place and Shutdown/Reboot Now** and click **OK**.

## Mounting and unmounting the CD

To be sure that you install IBM Tivoli Directory Server correctly, use the following procedures to mount and unmount the CD.

### Mounting the CD

1. To verify that the Portable File Systems (PFS) daemons are enabled and active, type the following at a command prompt:

```
ps -aef | grep pfs
```

If the output of the command shows `pfs_mountd`, `pfsd` and the corresponding `rpc` processes as in the following example, go to step 3 on page 94.

```
ps -aef | grep pfs
root 20381 17407 0 14:04:51 pts/tb 0:00 /usr/sbin/pfs_mountd
root 20388 20387 0 14:05:20 pts/tb 1:06 pfsd.rpc
root 20382 20381 0 14:04:51 pts/tb 0:00 pfs_mountd.rpc
root 20387 17407 0 14:05:20 pts/tb 0:00 /usr/sbin/pfsd
```

Otherwise, continue to step 2 to start the PFS daemons.

2. To start the PFS processes on an HP-UX machine, issue the commands:

```
nohup /usr/sbin/pfs_mountd &  
nohup /usr/sbin/pfsd &
```

3. Mount the CD to /SD\_CDRROM or any other directory that can act as mount point. This directory must exist before you run the **pfs\_mount** command. To create this directory, type the following command:

```
mkdir /SD_CDRROM
```

To mount the CD, type the following command:

```
/usr/sbin/pfs_mount <CD_device_name> <mount_point_dir>
```

where <CD\_device\_name> is the device name of the CD drive on the computer, and <mount\_point\_dir> is the directory that is acting as the mount point. For example:

```
/usr/sbin/pfs_mount /dev/dsk/c0t0d0 /SD_CDRROM
```

The CD is now mounted and you can install IBM Tivoli Directory Server.

### Unmounting the CD

To unmount and eject the CD:

1. Be sure that no processes are using the CD.
2. Unmount the CD. Type the following command:

```
/usr/sbin/pfs_umount /SD_CDRROM
```

Where /SD\_CDRROM is the mount point.

3. Eject the CD.

**Note:** If the CD fails to eject, type the following command:

```
/usr/sbin/pfs_umount -c <CD_device_name>
```

For example:

```
/usr/sbin/pfs_umount -c /dev/dsk/c0t0d0
```

Then eject the CD.

---

## Installing IBM Tivoli Directory Server

Before installing IBM Tivoli Directory Server, be sure that you have the correct kernel configuration parameters set, and Java Runtime Environment 1.4.2 and a supported version of DB2 installed.

### Package dependencies

The following IBM Tivoli Directory Server packages are available for installation:

- idslldap.cltbase60.depot: Base client
- idslldap.clt32bit60.depot: 32-bit client
- idslldap.clt64bit60.depot: 64-bit client
- idslldap.cltjava60.depot: Java client
- idslldap.srvproxy32bit60.depot: Proxy server
- idslldap.srv32bit60.depot: Full server (32-bit)
- idslldap.webadmin60.depot: Web Administration Tool

- idldap.msg60.en.depot: English messages

In addition, the following language packs are available. Install a language pack if you are installing a server and you want server messages to be displayed in a language other than English.

- idldap.msg60.de.depot: German messages
- idldap.msg60.es.depot: Spanish messages
- idldap.msg60.fr.depot: French messages
- idldap.msg60.it.depot: Italian messages
- idldap.msg60.ja.depot: Japanese messages
- idldap.msg60.ko.depot: Korean messages
- idldap.msg60.zh\_CN.depot: Simplified Chinese messages
- idldap.msg60.zh\_TW.depot: Traditional Chinese messages

Because of package dependencies, the order of installation is significant. Install the packages in the following order:

**For the 32-bit client only:**

Install in the following order:

1. Base client
2. 32-bit client

**For the 64-bit client only:**

Install in the following order:

1. Base client
2. 64-bit client

**For the proxy server:**

Install in the following order:

1. Base client
2. 32-bit client
3. Java client
4. Proxy server
5. English messages (can be in any order)

**For the full server:**

Install in the following order:

1. Base client
2. 32-bit client
3. Java client
4. Proxy server
5. Full server
6. English messages (can be in any order)

If you do not install in the order shown, the installation fails.

**Note:** Because the Web Administration Tool package has no dependencies on any of the other packages, and none of the other packages are dependent on it, you can install it in any order.

## Installing using swinstall

The instructions in this section assume that you are logged in as **root** and have the IBM Tivoli Directory Server Version 6.0 CD mounted at `/SD_CDROM`.

To install IBM Tivoli Directory Server packages:

1. Log in as **root**.
2. Type `swinstall` at a command prompt.
3. Supply the full path under **Source Depot Path** for the package you want to install. For example, typing `/SD_CDROM/itds/idsldap.clbase60.depot` installs the base client package. You must select one package at a time, and follow the order shown in "Package dependencies" on page 94. You can select from the following list:
  - IBM Directory Server - Base Client
  - IBM Directory Server - 32 bit Client
  - IBM Directory Server - 64 bit Client
  - IBM Directory Server - Java Client
  - IBM Directory Server - Proxy Server
  - IBM Directory Server - Web Administration
  - IBM Directory Server - Messages U.S. English (en)

(For language packs, the path is `/SD_CDROM/itdsLangpack`.)

4. Click **Actions** → **Install** on the Install Analysis window. Analysis is complete when the Status field reads **Ready**.
5. Click **OK**.
6. Installation is complete when the Status field reads **Completed**. Click **Done**.
7. Select **Actions** → **Change Source**.
8. Repeat step 3 through step 7 until you have installed all the packages you want.
9. Click **File** → **Exit**.

### Notes:

1. To enable SSL, you must also install GSKit. See "Installing GSKit" on page 97.
2. If you installed the proxy server or the full server, you must install IBM Tivoli Directory Integrator 6.0 with Fix Pack 1 if you want to do the following. (If you acquire IBM Tivoli Directory Server through Passport Advantage, it includes a copy of IBM Tivoli Directory Integrator 6.0 with Fix Pack 1.)
  - Use the **idssupport** tool, which gathers information from your system that you can supply to IBM Support if you encounter problems
  - Use the log management tool
  - Use Simple Network Management Protocol (SNMP)

You can find information about the support tool and the log management tool in the *IBM Tivoli Directory Server version 6.0 Problem Determination Guide*.

3. If you install the Web Administration Tool, DSML files are also copied to your computer. See Appendix L, "Installing and configuring DSML," on page 193 for information about installing and configuring DSML.
4. If you install the Web Administration Tool, an application server such as the embedded version of WebSphere Application Server - Express is required to run the tool. See Appendix H, "Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express," on page 183 for information about installing and configuring an application server.

---

## Installing GSKit

You can install the GSKit package through the **swinstall** command.

To install GSKit:

1. Run the following command to install:

```
swinstall -s /SD_CDROM/gskit/gsk7bas gsk7bas
```

where

- **-s** specifies the full\_path of the software source.
- **SD\_CDROM** is your mount point for the CD-ROM.
- **gsk7bas** contains the Restricted GSKit Base Toolkit install image.

See Appendix O, “Setting up GSKit to support CMS key databases,” on page 201 for more information about setting up GSKit after installation.

## Removing GSKit

To remove GSKit, run the following command at a command prompt:

```
swremove gsk7bas
```





---

## Chapter 12. Installing and uninstalling silently on Windows platforms

This chapter provides instructions for installing and uninstalling IBM Tivoli Directory Server 6.0 and the language packs on a Windows computer using silent installation, and for installing and uninstalling GSKit from the command line on Windows.

To silently install and uninstall on AIX, Linux, Solaris, and HP-UX systems, use the operating system utilities for those operating systems.

---

### Silent installation

You can use silent installation to install IBM Tivoli Directory Server or the language packs with no user input required.

The following options and conditions apply to silent installation:

- You must have at least 100 MB of memory free before invoking silent installation.
- You do not need to install all features. You can choose to install:
  - The client only
  - The Java client
  - The Web Administration tool only
  - The proxy server (this includes the client and the Java client)
  - The full server (this includes the client, the Java client, and the proxy server)
- You cannot use IBM Tivoli Directory Server silent installation to install DB2, GSKit, or the embedded version of WebSphere Application Server - Express. If you want to install those products silently, refer to the product documentation for those products.
- You must have at least 100 MB of free space in the directory specified by the TEMP environment variable or the directory you want to use as a temporary directory.
- If you choose to install the full server, you must already have DB2 installed.
- If you are installing the proxy server or the full server, the Administrators group provided with the Windows operating system must exist.
- The installation must be run by a user ID with Administrator privileges.
- If the client is already installed, you can add the proxy server or full server in a later installation.
- If a server is selected for installation in the options file, the client and the Java client will automatically be installed if they are not there, regardless of whether they were selected for installation in the options file.
- The Web Administration Tool can be installed whether or not a server or the client is installed.
- The installation location cannot be the same as the path where another version of the client is installed.
- If you have a client from IBM Directory Server 4.1 or 5.1 or IBM Tivoli Directory Server 5.2, you can leave it installed. The server and the client from IBM Tivoli Directory Server 6.0 can coexist with a client from one of these versions.

Before you begin silent installation, be sure that the options file for the server, client, or language packs is updated with the correct information about the features you want to install and the installation path. To edit an options file, copy the file from the optionsFile directory to a writable location. The files are:

- Server options file: InstallServer.txt
- Client only options file: InstallClient.txt. (This file is provided in the client-only package.)
- Language pack options file: InstallLP.txt

For information about changing the installation options files, see “Options files for silent installation of servers and language packs” on page 103.

## Installing the server or client silently

To begin installing the IBM Tivoli Directory Server 6.0 using silent installation:

1. If you are installing from a CD:
  - a. Insert the CD in your CD-ROM drive.
  - b. Go to the drive for your CD-ROM,
  - c. At a command prompt, type the following:

```
cd \itds
```

If you are installing from the downloaded zip file:

- a. Go to the directory where you unzipped the downloaded zip file.
- b. At a command prompt, type the following:

```
cd itdsV60\itds
```

2. Type the following command:

```
consoleSetup -is:silent -options full_path\optionsFiles\InstallServer.txt
```

where *full\_path* is the full path to the optionsFiles directory.

(If you want to install only the client from the client-only package, substitute InstallClient.txt for InstallServer.txt.)

### Notes:

- a. If you want to specify a temporary directory other than the one specified by the TEMP environment variable, use the **-is:tempdir** option, as follows:

```
consoleSetup -is:silent -options optionsFiles\InstallServer.txt  
-is:tempdir temp_directory
```

where *temp\_directory* is the directory you want to use for temporary space. Be sure that you have at least 100 MB of free space in this directory.

- b. If you want to specify an additional log file, use the **-log** option, as follows:

```
consoleSetup -is:silent -options full_path\optionsFiles\InstallServer.txt  
-log !c:\mydirectory\ldapinst.log @ALL
```

where *full\_path* is the full path to the optionsFiles directory.

*c:\mydirectory\ldapinst.log* can be changed to point to where you want to place the log file. The log file will still be created in the target installation directory. The default location is

```
C:\Program Files\IBM\LDAP\V6.0\var\ldapinst.log.
```

- c. You must use consoleSetup.exe rather than setup.exe because only consoleSetup.exe returns a return code.

3. IBM Tivoli Directory Server is installed with no further input. If the installation exits for any reason, you can find information about the exit by viewing the

return code or checking the *installpath*\var\ldapinst.log file. (*installpath* is the path where you installed IBM Tivoli Directory Server.)

Check the return code by checking the value of %ERRORLEVEL% from a .bat file. A return code of 0 indicates that the installation was successful. A non-zero return code indicates that the installation failed. See “Checking the return code” on page 102 for a list of return codes.

Installation is complete when control returns to the command line or to the invoking program.

If installation is unsuccessful, check to be sure that your options file settings and command-line parameters are valid.

4. After installation, restart the system. If you are also installing other products, you can restart at an appropriate time. If the server was installed, you must do the following before the server is usable:
  - a. Create a directory server instance using the **idsicrt** command. See “Using idsicrt to create an instance” on page 116.
  - b. Set the administrator DN and password using the **idsdnpw** command. See “Using idsdnpw to set the administrator DN and password” on page 136.
  - c. If the directory server instance is a full server, configure the database using the **idscfgdb** command line utility to configure silently. See “Using idscfgdb to configure the database” on page 138.

## Installing language packs silently

To begin installing IBM Tivoli Directory Server 6.0 language packs using silent installation:

1. If you are installing from a CD:
  - a. Insert the CD in your CD-ROM drive.
  - b. Go to the drive for your CD-ROM,
  - c. At a command prompt, type the following:

```
cd \itdsLangpack
```

If you are installing from the downloaded zip file:

- a. Go to the directory where you unzipped the downloaded zip file.
  - b. At a command prompt, type the following:

```
cd itdsV60\itdsLangpack
```
2. At a command prompt, type the following:

```
idslp_setup_win32.exe -is:silent  
-options full_path_to_options_file\InstallLP.txt
```

where *full\_path\_to\_options\_file* is the full path to the InstallLP.txt file you are using. The InstallLP.txt file is in the itdsLangpack\optionsFiles subdirectory of the CD or the unzipped zip file, but if you moved it, you must specify the current location of the file.

**Note:** If you want to specify an additional log file, type the following:

```
idslp_setup_win32.exe -is:silent  
-options d:\itds\optionsFiles\InstallLP.txt  
-log !c:\mydirectory\ldaplp_inst.log @ALL
```

*c:\mydirectory\ldaplp\_inst.log* can be changed to point to where you want to place the log file. The log file will still be created in the target installation directory.

The default location is for the log is *install\_dir*\var\ldaplp\_inst.log. (If you installed in the default location, the log is C:\Program Files\IBM\LDAP\V6.0\var\ldaplp\_inst.log.)

## Verifying the silent installation

To verify that the silent installation was successful, you can check the return code, log file, and the Windows registry.

Common reasons for the silent installation failing are:

- A previous or current version of IBM Tivoli Directory Server is already installed. (Only a previous client is allowed, and it must be an IBM Directory Server 4.1 or 5.1 or IBM Tivoli Directory Server 5.2 client.)
- The prerequisites are not present. The server requires a valid version of DB2.
- There is not enough disk space to install.
- The options file is incorrect. Be very careful when editing the options file. There cannot be blank lines or control characters in the file. If the installation exits with no log file, this is usually because the options file is invalid (with blank lines, for example), or because the path to the options file was specified incorrectly.

### Checking the return code

The %ERRORLEVEL% variable contains the return code. The following return codes can be received:

- 2002 Java exception (A possible cause is that you are attempting to install to a location where another version is installed. If you receive this return code, entries might have been created for IBM Tivoli Directory Server 6.0 in the registry. Check the registry and, if there are any such entries, remove them before you try to install again.)
- 3001 Prerequisites missing
- 3002 Java exception
- 3003 No feature selected for silent install
- 3004 Attempting to install when version prior to 4.1 present
- 3009 Cannot install a feature. (A condition was detected that prevented a feature from being installed. A common cause is that the server or Web Administration Tool from a previous release is installed. If the server or Web Administration Tool from a previous release is installed, the only feature that can be installed is the client.)

Other return codes might be returned from the InstallShield program.

### Checking the log file

To verify that silent installation was successful using the log file:

1. Check the log file to see if it exists in the target directory. If the log is not there, the installation failed, and you can refer to the log file that was specified on the silent installation command with the **-log** option to see why the installation failed.
2. Check the log file for the string **Exiting LdapExit**.

### Checking the Windows registry

Verify that the installation was completed using the Windows registry. The following text should be in the registry, depending on which components were installed:

```
In HKEY_LOCAL_MACHINE\SOFTWARE\IBM\IDSLDAP\6.0
```

```
ClientMajorVersion 6.0  
JavaClientMajorVersion 6.0  
ServerMajorVersion 6.0  
ProxyServerMajorVersion 6.0  
WebadminMajorVersion 6.0  
WebSphereAppSrvMajorVersion 5.1  
LDAPHome install_location
```

```
In HKEY_LOCAL_MACHINE\SOFTWARE\IBM\IDSLDAP\6.0\Client\
```

```
ClientMinorVersion 0.0
```

```
In HKEY_LOCAL_MACHINE\SOFTWARE\IBM\IDSLDAP\6.0\JavaClient\
```

```
JavaClientMinorVersion 0.0
```

```
In HKEY_LOCAL_MACHINE\SOFTWARE\IBM\IDSLDAP\6.0\Webadmin\
```

```
WebadminMinorVersion 0.0
```

```
In HKEY_LOCAL_MACHINE\SOFTWARE\IBM\IDSLDAP\6.0\Server\
```

```
ServerMinorVersion 0.0
```

```
In HKEY_LOCAL_MACHINE\SOFTWARE\IBM\IDSLDAP\6.0\ProxyServer\
```

```
ProxyServerMinorVersion 0.0
```

```
In HKEY_LOCAL_MACHINE\SOFTWARE\IBM\IDSLDAP\6.0\
```

```
WebSphereAppSrv\
```

```
WebSphereAppSrvMinorVersion 1.0
```

## Options files for silent installation of servers and language packs

See the following sections for information about the silent installation options file for the servers, client only (from the client-only package), and language packs.

### Server installation options file

The following text is in the server installation options file, `InstallServer.txt`, provided with IBM Tivoli Directory Server:

```
#Sample response file for the Server/Client package  
#(Lines beginning with # are comments)  
# Be sure there are no blank lines in this file!  
# All lines that are not comments must be present; they cannot be commented out.  
# Where indicated, values can be changed.  
#  
# The following 3 lines MUST be present, and NOT modified  
-silent  
-G createDirectoryResponse="yes"  
-G replaceExistingResponse="yesToAll"  
#  
# install destination - this can be modified to install location  
-P product.installLocation="C:\Program Files\IBM\ldap\V6.0"  
#  
# Select the features to install. Note: if the server is selected, the  
# Client, JavaClient, and ProxyServer will automatically be installed. If the  
# ProxyServer is selected, the JavaClient and Client will automatically  
# be installed.  
# To deselect a feature, set the field to false.  
-P ServerFeature.active=true  
-P ProxyServerFeature.active=true  
-P JavaClientFeature.active=true
```

```
-P ClientFeature.active=true
-P WebadminFeature.active=true
# This must be last line. Be sure no blank lines or carriage controls follow!
```

You can edit the following line to point to the desired target installation directory:

```
-P product.installLocation="C:\Program Files\IBM\ldap\V6.0"
```

Be sure that the installation location is not the same as the path where another version of the client is installed.

You can edit the features lines to disable a feature from being installed. For example, to indicate that you do not want to install the IBM Tivoli Directory Server Web Administration Tool, change

```
-P WebadminFeature.active=true
```

to

```
-P WebadminFeature.active=false
```

**Note:** If you have any feature except the client, GSKit, or DB2 from a previous version installed, you can install only the client. If this is the case, be sure to disable all other features by setting them to false.

### Client installation options file

The following text is in the client installation options file, InstallClient.txt, provided with the client-only package:

```
# options file for silent install
# Use this file with the Client-only package
#(Lines beginning with # are comments)
# Be sure there are no blank lines in this file!
# All lines that are not comments must be present; they cannot be commented out.
# Where indicated, values can be changed.
#
# The following 3 lines MUST be present, and NOT modified
-silent
-G createDirectoryResponse="yes"
-G replaceExistingResponse="yesToAll"
#
# install destination - this can be modified to install location
-P product.installLocation="C:\Program Files\IBM\ldap\V6.0"
# This must be last line. Be sure no blank lines or carriage controls follow!
```

You can change only the installation location in this file.

To change the installation location, change the following line to point to the desired target installation directory:

```
-P product.installLocation="C:\Program Files\IBM\ldap\V6.0"
```

Be sure that the installation location is not the same as the path where another version of the client is installed.

### Language packs installation options file

The following text is in the language packs installation options file, InstallLP.txt, provided with IBM Tivoli Directory Server:

```
# Sample of a response file for the Language pack Uninstall
# (Lines beginning with # are comments)
# Be sure there are no blank lines in this file!
#
# The following 3 lines MUST be present
-silent
```

```

-G createDirectoryResponse="yes"
-G replaceExistingResponse="yesToAll"
#
# Language Pack support file install destination - can be modified to
# install location
-P product.installLocation="C:\Program Files\IBM\LDAP\V6.0"
#
# Set the following entries to true to install a language feature
# or keep it false to NOT install
#
-P GermanXlations.active=false
-P FrenchXlations.active=false
-P ItalianXlations.active=false
-P SpanishXlations.active=false
-P JapaneseXlations.active=false
-P KoreanXlations.active=false
-P BrazilianXlations.active=false
-P SChineseXlations.active=false
-P TChineseXlations.active=false
# This must be last line. Be sure no blank lines or carriage controls follow!

```

By default, no language packs are installed. To install the language pack for a language, edit the line for that language and change false to true. For example, to install the Japanese language pack, change

```
-P JapaneseXlations.active=false
```

to

```
-P JapaneseXlations.active=true
```

---

## Silent uninstallation

You can use silent uninstallation to uninstall IBM Tivoli Directory Server or the language packs with no user input required.

The following options and conditions apply to silent uninstallation:

- You must have at least 100 MB of memory free before invoking silent uninstallation.
- You cannot use IBM Tivoli Directory Server silent uninstallation to uninstall DB2, GSKit, or the embedded version of WebSphere Application Server - Express. To silently uninstall these product, refer to the product documentation for those products.
- You must have at least 100 MB of free space in the directory specified by the TEMP environment variable.

Before you begin silent uninstallation, be sure that the options file for the server or language packs is updated with the correct information about the features you want to install. To edit an options file, copy the file from the optionsFile directory to a writable location. The files are:

- Server options file: UnInstallServer.txt
- Client only options file: UnInstallClient.txt (You cannot change this file.)
- Language pack options file: UnInstallLP.txt

For information about changing the uninstallation options files, see “Options files for silent uninstallation of servers and language packs” on page 106.

To begin uninstalling IBM Tivoli Directory Server 6.0 using silent uninstallation, type the following at a command prompt:



```
"C:\Program Files\IBM\ldap\V6.0\_uninst\uninstall.exe" -is:silent
  -options C:\UnInstallServer.txt -log !C:\ldapuninst.log @ALL
```

(If you are uninstalling a client-only installation, substitute UnInstallClient.txt for UnInstallServer.txt.) This example assumes that IBM Tivoli Directory Server is installed in the C:\Program Files\IBM\ldap\V6.0 directory and that the UnInstallServer.txt file has been copied to the C:\ directory..

To begin uninstalling IBM Tivoli Directory Server 6.0 language packs using silent uninstallation, type the following at a command prompt:

```
"C:\Program Files\IBM\ldap\V6.0\LangPack\uninstall\idslp_uninstall_win32.exe"
  -is:silent -options C:\UnInstallLP.txt -log !C:\lpuninst.log @ALL
```

This example assumes that IBM Tivoli Directory Server is installed in the C:\Program Files\IBM\ldap\V6.0 directory and that the UninstallLP.txt file has been copied to the C:\ directory.

## Options files for silent uninstallation of servers and language packs

See the following sections for information about the silent uninstallation options file for the servers and the language packs. (You cannot change the client uninstallation options file.

### Server uninstallation options file

The following text is in the server uninstallation options file, UnInstallServer.txt, provided with IBM Tivoli Directory Server:

```
#Sample response file for uninstall
#(Lines beginning with # are comments)
# Be sure there are no blank lines in this file!
#
# The following 4 lines MUST be present
-silent
-G createDirectoryResponse="yes"
-G replaceExistingResponse="yesToAll"
-G removeModifiedResponse="yesToAll"
#
# Select the features to be uninstalled. If a feature was never installed then
# its line must be commented out.
# The "activeForUninstall" property specifies whether you want a feature to
# be uninstalled.
# The "activeForUninstall" property for a feature defaults to true if the feature
# is currently
# installed; it must be set to false if you want to leave it installed.
# The default action, if no features are specified, is to uninstall all features
# that are currently installed.
# Corequisite products such as DB2 are never uninstalled silently and cannot be
# specified here.
-P ClientFeature.activeForUninstall=true
-P JavaClientFeature.activeForUninstall=true
-P ProxyServerFeature.activeForUninstall=true
-P ServerFeature.activeForUninstall=true
-P WebadminFeature.activeForUninstall=true
# This must be last line. Be sure no blank lines or carriage controls follow!
```

You can edit the features lines to disable a feature from being uninstalled. For example, to indicate that you do not want to uninstall the IBM Tivoli Directory Server Web Administration Tool, change

```
-P WebadminFeature.activeForUninstall=true
```



to  
-P WebadminFeature.activeForUninstall=false

### Language packs options file

The following text is in the language packs uninstallation options file, UnInstallLP.txt, provided with IBM Tivoli Directory Server:

```
# Select the features to be uninstalled. If a feature was never installed the
# Sample of a response file for the Language pack Uninstall
# (Lines beginning with # are comments)
# Be sure there are no blank lines in this file!
#
# The following 4 lines MUST be present
-silent
-G createDirectoryResponse="yes"
-G replaceExistingResponse="yesToAll"
-G removeModifiedResponse="yesToAll"
#
#
# The "activeForUninstall" property specifies whether you want a feature to be
# uninstalled.
# Unless otherwise specified, the "activeForUninstall" property for all installed
# features by default is set to true;
# a property value must be set to false if you want to leave its feature installed.
# The default action, if no property values are specified, is to uninstall all
# features that are currently installed.
# The following list of features should only include languages installed on
# your system.
# If a language feature was already installed and you do not wish to uninstall it
# then uncomment its property entry. This will set the activeForUninstall property
# value to false and keep the corresponding
# language feature installed.
#-P GermanXlations.activeForUninstall=false
#-P FrenchXlations.activeForUninstall=false
#-P ItalianXlations.activeForUninstall=true
#-P SpanishXlations.activeForUninstall=false
#-P JapaneseXlations.activeForUninstall=false
#-P KoreanXlations.activeForUninstall=false
#-P BrazilianXlations.activeForUninstall=false
#-P SChineseXlations.activeForUninstall=false
#-P TChineseXlations.activeForUninstall=false
# This must be last line. Be sure no blank lines or carriage controls follow!
```

By default, no language packs are uninstalled. To uninstall the language pack for a language, edit the line for that language. Remove the # character from the line, and change false to true. For example, to uninstall the French language pack, change

```
#-P FrenchXlations.activeForUninstall=false
```

to  
-P FrenchXlations.activeForUninstall=true

---

## Installing GSKit on Windows operating systems

If you install IBM Tivoli Directory Server using silent installation, GSKit is not installed. You can use the following procedure to install it.

To install GSKit 7.0.3.3:

1. Change directories to the \gskit directory on the IBM Tivoli Directory Server CD or the itdsV60\gskit subdirectory of the directory where you unzipped the IBM Tivoli Directory Server .zip file.
2. Run the following command. (Do **not** start setup.exe by clicking on the icon.)

```
setup LDAP -s -f1"setup_file_location\setup.iss"
```

where LDAP is the name of your application and will be registered as a registered user of GSK in the Windows Registry (under the key HKEY\_LOCAL\_MACHINE\SOFTWARE\IBM\GSK\CurrentVersion\REGAPPS).

The following options can be used:

- **-s** to run the setup in the silent mode.
- **-f1**setup\_file\_location\setup.iss specifies the response file needed to run the setup in the silent mode. Note that there is no space between **-f1** and the beginning of the setup file location.

For example, if you unzipped the IBM Tivoli Directory Server .zip file into the d:\DirectoryServerV6.0 directory, type:

```
cd d:\DirectoryServerV60\itdsV60\gskit
setup LDAP -s -f1"d:\DirectoryServerV60\itdsV60\gskit\setup.iss"
```

See Appendix O, "Setting up GSKit to support CMS key databases," on page 201 for more information about setting up GSKit after installation.

## Removing GSKit

To remove GSKit, run the following command:

```
C:\WINNT\gsk7BUI LDAP
```

---

## Chapter 13. Creating and administering instances

You can use the Instance Administration Tool to create, view, change information about, and delete instances. You can also use command-line utilities for these tasks.

After installation of a server, you must create an instance. For a proxy server or a full server, you must then set the administrator DN and password for the instance. For a full server, you must also configure the database that is associated with the server instance.

---

### Using the Instance Administration Tool to work with instances

The Instance Administration Tool is a graphical user interface (GUI) that you can use to create and manage directory server instances. When you use the Instance Administration Tool, the tool guides you through the steps you need.

**Attention:** When you create a new directory server instance, be aware of the information that follows.

1. If you want to use replication, use a distributed directory, or import and export LDIF data between server instances, you must cryptographically synchronize the server instances to obtain the best performance.

If you are creating a directory server instance that must be cryptographically synchronized with an existing directory server instance, you must synchronize the server instances *before* you do any of the following:

- Start the second server instance
- Run the **idsbulkload** command from the second server instance
- Run the **idsldif2db** command from the second server instance

See Appendix E, “Synchronizing two-way cryptography between server instances,” on page 177 for information about synchronizing directory server instances.

2. After you create a directory server instance and configure the database, use the **idsdbback** utility to create a backup of the directory server instance. The configuration and directory key stash files are archived along with the associated configuration and directory data. You can then use the **idsdbrestore** utility to restore the key stash files if necessary. (You can also use the **idsdbback** utility after you load data into the database. See “Backing up the database” on page 135 and “Backing up, restoring, and optimizing the database” on page 148 for information about backing up the database.)

### Starting the Instance Administration Tool

The Instance Administration Tool can be started in different ways:

- When you install either the proxy server or the full server using the InstallShield GUI, the Instance Administration Tool starts after installation.
- If you want to create a new instance, you can start the Instance Administration Tool by typing `idsxinst` at the command line.
- Also, on Windows systems, you can click **Start** —> **Programs** —> **IBM Tivoli Directory Server 6.0** —> **Instance Administration Tool**.

To use the Instance Administration Tool on AIX, Linux, Solaris, and HP-UX systems, you must be logged in as **root**. On Windows systems, you must be logged on as a member of the Administrators group.

## Creating an instance

To create an instance with the Instance Administration Tool:

1. If the Instance Administration Tool is not started:
  - a. On AIX, Linux, Solaris, and HP-UX systems, log in as **root**. On Windows systems, log on as a member of the Administrators group.
  - b. Start the Instance Administration Tool by typing `idsxinst` at the command line. The IBM Tivoli Directory Server Instance Administration Tool window is displayed.
2. Click **Create**.
3. On the Create a new directory server instance window, click one of the following:
  - **Create a new directory server instance** if you are not migrating.
  - **Migrate from a pre-6.0 version of directory server** if you are migrating from a previous release. Then type the path where you backed up the configuration and schema files from the previous version.

Click **Next**.

4. On the Instance details window, complete the following fields:

### User name

Type the system user ID of the user who will own the directory server instance. The name you type will also be the name of the directory server instance. See Appendix D, "Setting up users and groups: directory server instance owner, database instance owner, and database owner," on page 173 for detailed information about the user ID.

### Notes:

- a. If you are migrating from a previous version and there was a DB2 instance already configured in the configuration files, that name is displayed in the **User name** field. You can edit this name.
- b. The name of the new directory server instance must be unique; if there is already a directory server instance on the computer with the same name, you will receive an error message.

### Install location

Type the location where the directory server instance files will be stored. Be sure that you have at least 30 MB of free disk space in this location.

On Windows systems, this location is a drive, such as **C:**. The directory instance files will be stored in the `\idsldapd-instance_name` directory on the drive you specify, where *instance\_name* is the name of the directory server instance.

On AIX, Linux, Solaris, and HP-UX systems, the default location for the instance files is in the directory instance owner's home directory, but you can specify a different path. Click **Browse** if you want to select a location.

### Encryption seed string

Type a string of characters that will be used as an encryption seed.

The encryption seed must contain only printable ISO-8859-1 ASCII characters with values in the range of 33 to 126, and must be a minimum of 12 and a maximum of 1016 characters in length. For information about what characters can be used, see Appendix J, “ASCII characters from 33 to 126,” on page 189.

This encryption seed is used to generate a set of Advanced Encryption Standard (AES) secret key values. These values are stored in the directory server instance’s directory key stash file and used to encrypt and decrypt directory stored password and secretkey attributes.

Record the encryption seed in a secure location; you might need it if you export data to an LDIF file (the **idsdb2ldif** command) or regenerate the key stash file (the **idsgendirksf** command.)

#### **Instance description**

Optionally, type a description of the directory server instance. This description is displayed in other windows to help identify the instance.

Click **Next**.

5. If the DB2 instance details window is displayed, either accept the name that is displayed in the **DB2 instance name** field, or type or select a different name for the DB2 instance, and then click **Next**.

By default, the DB2 instance name is the same as the name of the directory server instance, but you can specify a different name for the DB2 instance. If you specify a different name, there must be a system user ID by the same name. This name cannot be already associated with another directory server instance.

6. On the TCP/IP settings for multihomed hosts window, do one of the following:
  - If you want the directory server instance to listen on all IP addresses, select the **Listen on all configured IP addresses** check box.
  - If you want the directory server instance to listen on a particular set of IP addresses that are configured on the computer, clear the **Listen on all configured IP addresses** check box. Then select the IP address or addresses in the list that you want the directory server instance to listen on.

Click **Next**.

7. On the TCP/IP port settings window, complete the following fields:

#### **Server port number**

Type the number of the port you want the server to use as its contact port. The number must be between 1 and 65535.

#### **Server secure port number**

Type the number of the port you want the server to use as its secure port. The number must be between 1 and 65535.

#### **Admin daemon port number**

Type the number of the port you want the administration daemon to use as its port. The number must be between 1 and 65535.

#### **Admin daemon secure port number**

Type the number of the port you want the administration daemon to use as its secure port. The number must be between 1 and 65535.

**Note:** If you have two or more directory server instances listening on the same IP address (or set of IP addresses), be sure that those directory server instances do not use any of the same port numbers.

Click **Next**.

8. If the Optional steps window is displayed:
  - a. Select **Configure admin DN and password** if you want to configure the administrator DN and password for the directory server instance now. (The administrator DN and password are required for both proxy servers and full servers.)
  - b. Select **Configure database** if you want to configure the database for the directory server instance now. (A proxy server instance does not require a database.)

When you configure the database, the Instance Administration Tool adds information about the database that will be used to store directory data to the configuration file (ibmslapd.conf) for the directory server instance. In addition, if the database does not already exist, the Instance Administration Tool creates the database.

**Note:** In some cases (for example, if you are migrating from a previous release), these options might not be available.

Click **Next**.

**Note:** You can use the Configuration Tool or the command line later if you do not want to set the administrator DN or configure the database now, but you cannot use the directory server instance until you have done these steps.

9. If the Configure administrator DN and password window is displayed:
  - a. In the **Administrator DN** field, type a valid DN (or accept the default DN, **cn=root**).

The administrator DN is the DN used by the administrator of the directory server instance. This administrator is the one user who has full access to all data in the directory.

The default DN is **cn=root**. DNs are not case sensitive. If you are unfamiliar with X.500 format, or if for any other reason you do not want to define a new DN, accept the default DN.
  - b. Type the password for the administrator DN in the **Administrator Password** field. You must define a password. Passwords are case-sensitive. Double byte character set (DBCS) characters in the password are not valid. Record the password in a secure location for future reference.
  - c. Retype the password in the **Confirm password** field.
  - d. Click **Next**.

10. If the Configure database window is displayed:
  - a. Type a valid DB2 administrator ID in the **Database user name** field. This ID must already exist and must have the proper authority before you can configure the database.

**Note:** Before server startup, this user must have the locale set to the correct locale for the language in which you want server messages to be displayed. If necessary, log in as the user and change the locale to the correct one.

- b. Type the password for the user in the **Password** field. Passwords are case-sensitive.

**Note:** If you change the system password for the DB2 administrator, you cannot update it through the Instance Administration Tool. You must use the Configuration Tool or the `idscfgdb` command with the `-w` option. See “Changing the password for the database owner” on page 128 or “Using `idscfgdb` to configure the database” on page 138 for information.

- c. Type the name you want to give the DB2 database in the **Database name** field. The name can be from 1 to 8 characters long.
  - d. Click **Next**.
11. If the Database options window is displayed:
- a. Type the location for the database in the **Database install location** field. For Windows platforms, this must be a drive letter. For non-Windows platforms, the location must be a directory name, such as `/home/ldapdb`. (You can click **Browse** to locate a directory.)  
Be sure that you have at least 80 MB of free hard disk space in the location you specify and that additional disk space is available to accommodate growth as new entries are added to the directory.
  - b. In the **Character-set option** box:
    - 1) Click the type of database you want to create. Click one of the following:
      - **Create a universal DB2 database (UTF-8/UCS-2)** to create a UCS Transformation Format (UTF-8) database, in which LDAP clients can store UTF-8 character data.
      - **Create a local codepage DB2 database** to create a database in the local code page.If you want to use language tags, the database must be a UTF-8 database. For more information about UTF-8, see Appendix N, “UTF-8 support,” on page 197.
    - 2) Click **Next**.
12. In the Verify settings window, information is displayed about the options you specified. To return to an earlier window and change information, click **Back**. To begin creating the directory server instance, click **Finish**.
13. The Results window is displayed, and messages are displayed while the instance is being created. A completion message is displayed when instance creation is complete. Click **OK** to remove the message.
14. Click **Close** to close the window and return to the main window of the Instance Administration Tool.
15. If you have finished using the Instance Administration Tool, click **Close** to exit the tool.

**Note:** After you set the administrator DN and password and, for a full server, configure the database, see Chapter 15, “After you install and configure,” on page 149 for information about:

- Starting the server
- Starting the embedded version of WebSphere Application Server - Express service if you have installed and configured the Web Administration Tool.

You can find information about using the Web Administration Tool in the *IBM Tivoli Directory Server Version 6.0 Administration Guide*.

See “Using `idsicrt` to create an instance” on page 116 for information about using the `idsicrt` command-line utility to create a directory server instance.



## Changing the TCP/IP settings for an instance

To change the TCP/IP settings for an existing directory server instance:

1. If the Instance Administration Tool is not started:
  - a. On AIX, Linux, Solaris, and HP-UX systems, log in as **root**. On Windows systems, log on as a member of the Administrators group.
  - b. To start the Instance Administration Tool, type `idsxinst` at the command line. The IBM Tivoli Directory Server Instance Administration Tool window is displayed.
2. Select the directory server instance you want to change, and then click **Edit TCP/IP settings**.
3. On the first Edit TCP/IP settings window that is displayed, do one of the following:
  - If you want the directory server instance to listen on all IP addresses, select the **Listen on all configured IP addresses** check box.
  - If you want the directory server instance to listen on a particular set of IP addresses that are configured on the computer, clear the **Listen on all configured IP addresses** check box. Then select the IP address or addresses in the list that you want the directory server instance to listen on. (To select multiple addresses, press Shift or Ctrl and click the IP addresses you want.)

Click **Next**.

4. On the second Edit TCP/IP settings window that is displayed, complete the following fields:

**Server port number**

Type the number of the port you want the server to use as its contact port. The number must be between 1 and 65535.

**Server secure port number**

Type the number of the port you want the server to use as its secure port. The number must be between 1 and 65535.

**Admin daemon port number**

Type the number of the port you want the administration daemon to use as its port. The number must be between 1 and 65535.

**Admin daemon secure port number**

Type the number of the port you want the administration daemon to use as its secure port. The number must be between 1 and 65535.

**Note:** The port numbers you specify must not cause conflicts with ports being used by any other directory server instance that is bound to a particular hostname or IP address.

Click **Finish**.

5. A Results window is displayed. A completion message is displayed when instance creation is complete. Click **OK** to remove the message.
6. Click **Close** to close the window and return to the main window of the Instance Administration Tool.

See “Using `idssethost` to set IP addresses” on page 119 for information about using the `idssethost` command to set the IP addresses a directory server instance will bind to.

See “Using `idssetport` to set ports” on page 120 for information about using the `idssetport` command-line utility to set the ports a directory server instance will use.



## Viewing information about an instance

To view information about an existing directory server instance:

1. If the Instance Administration Tool is not started:
  - a. On AIX, Linux, Solaris, and HP-UX systems, log in as **root**. On Windows systems, log on as a member of the Administrators group.
  - b. To start the Instance Administration Tool, type `idsxinst` at the command line. The IBM Tivoli Directory Server Instance Administration Tool window is displayed.
2. Select the directory server instance for which you want to see information, and then click **View**.

The View instance details window is displayed.
3. Click **OK** when you have finished viewing the information.

See “Using `idsilist` to view instance details” on page 122 for information about using the `idsilist` command-line utility to view the directory server instances, including detailed information about the instances on the computer.

## Deleting an instance

To delete a directory server instance:

1. If the Instance Administration Tool is not started:
  - a. On AIX, Linux, Solaris, and HP-UX systems, log in as **root**. On Windows systems, log on as a member of the Administrators group.
  - b. To start the Instance Administration Tool, type `idsxinst` at the command line. The IBM Tivoli Directory Server Instance Administration Tool window is displayed.
2. Select the directory server instance you want to delete, and then click **Delete**.

The Delete directory server instance window is displayed.
3. In the **Options** box, click one of the following options:
  - Click **Delete directory server instance only** if you want to remove the directory server instance but leave the database instance intact.
  - Click **Delete directory server instance and destroy associated database instance** if you want to remove the database instance as well as removing the directory server instance.
4. Click **Delete**.
5. Messages are displayed in the window as the directory server instance is removed. A completion message is displayed when instance removal is complete. Click **OK** to remove the message.
6. When removal is complete, click **Close** to close the window and return to the main window of the Instance Administration Tool.

See “Using `idsidrop` to remove a directory server instance” on page 123 for information about using the `idsidrop` command-line utility to remove a directory server instance.

---

## Using commands to work with instances

You can use the commands in this section, instead of the Instance Administration Tool, to create and manage instances.

## Using idsicrt to create an instance

`idsicrt` is the command to create a directory server instance.

**Attention:** When you create a new directory server instance, be aware of the information that follows.

1. If you want to use replication, use a distributed directory, or import and export LDIF data between server instances, you must cryptographically synchronize the server instances to obtain the best performance. In the case of importing LDIF data, if the server instance that is importing the LDIF data is not cryptographically synchronized with the LDIF import file, any AES-encrypted entries in the LDIF import file will not be imported.

If you are creating a directory server instance that must be cryptographically synchronized with an existing directory server instance, you must synchronize the server instances *before* you do any of the following:

- Start the second server instance
- Run the `idsbulkload` command from the second server instance
- Run the `idsldif2db` command from the second server instance

See Appendix E, “Synchronizing two-way cryptography between server instances,” on page 177 for information about synchronizing directory server instances.

2. After you create a directory server instance and configure the database, use the `idsdbback` utility to create a backup of the directory server instance. The configuration and directory key stash files are archived along with the associated configuration and directory data. You can then use the `idsdbrestore` utility to restore the key stash files if necessary. (You can also use the `idsdbback` utility after you load data into the database. See “Backing up the database” on page 135 and “Backing up, restoring, and optimizing the database” on page 148 for information about backing up the database.)

### Synopsis

```
idsicrt [-I instancename [-e encryptseed] [-p port] [-s secureport] [-a admport]
        [-t dbinstance] [-c admsecureport] [-i ipaddress] [-l instlocation]
        [-r description] [-C] [-d debuglevel] [-b outputfile] [-q] [-n]] | -v | -?
```

### Description

The `idsicrt` command can be run only by root on AIX, Linux, Solaris, and HP-UX systems, or by a member of the Administrators group on Windows systems. The administrator specifies a directory server instance name and optionally can specify the port, secure port, administration daemon port, administration daemon secure port, and encryption seed. On Windows, the administrator must specify the location to store the directory server instance. On AIX, Linux, Solaris, and HP-UX platforms, specifying the location is optional.

By default, the DB2 database instance name (DB database instance owner) is assumed to have the same name as the directory server instance name. You can specify a different name by using the `-t` option; the DB2 instance owner ID must already exist on the operating system.

If a DB2 database instance already exists on the system, that DB2 instance is used. However, if the DB2 database instance is used by another directory server instance, the command will fail.

**Note:** No database instance is created if only the proxy server is installed on the computer.

## Options

### **-a** <admport>

Specifies the port on which the administration daemon for the directory server instance listens. Specify a positive number that is greater than 0 and less than 65535. The ports specified must not cause a conflict with ports being used by any other directory server instance that is bound to a particular hostname or IP address.

**Note:** If you have two or more directory server instances listening on the same IP address (or set of IP addresses), be sure that those directory server instances do not use any of the same port numbers.

Click **Next**.

### **-b** <outputfile>

Specifies the full path of a file to redirect output into. If used in conjunction with the **-q** option, only errors are sent to the file. If debugging is turned on, debugging information is sent to the file also.

### **-c** <admsecureport>

Specifies the secure port on which the administration daemon for the directory server instance listens. Specify a positive number that is greater than 0 and less than 65535. The ports specified must not cause a conflict with ports being used by any other directory server instance that is bound to a particular hostname or IP address.

### **-C** Specifies to configure a database instance for an existing directory server instance.

### **-d** <debuglevel>

Sets the LDAP debugging level to <debuglevel>. This option causes the utility to generate debug output to stdout. The <debuglevel> is a bit mask that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel. See the *IBM Tivoli Directory Server Problem Determination Guide* for more information about debug levels.

### **-e** <encryptseed>

Specifies the seed to be used to create the key stash files for a particular directory server instance. This option is required if you use the **-n** option. If it is not specified, you will be prompted for an encryption seed.

The encryption seed must contain only printable ISO-8859-1 ASCII characters with values in the range of 33 to 126, and must be a minimum of 12 and a maximum of 1016 characters in length. For information about the characters that can be used, see Appendix J, "ASCII characters from 33 to 126," on page 189.

This encryption seed is used to generate a set of Advanced Encryption Standard (AES) secret key values. These values are stored in a directory stash file and used to encrypt and decrypt directory stored password and secretkey attributes. There is one encryption seed string for each directory server instance.

Record the encryption seed in a secure location; you might need it if you export data to an LDIF file (the **idsdb2ldif** command) or regenerate the key stash file (the **idsgendirksf** command.)

### **-i** <ipaddress>

Specifies the IP address that the directory server instance binds to. If more than one IP address is specified, a comma separator is required with no

spaces. Spaces are allowed only if the entire argument is enclosed in quotation marks. Use the key word "all" to specify that you want to use all available IP addresses. If you do not specify the **-i** option, all available IP addresses is the default setting.

- I** *<instancename>*  
Specifies the name of the directory server instance. The instance name must be an existing user ID on the machine and must be no greater than 8 characters in length. See Appendix D, "Setting up users and groups: directory server instance owner, database instance owner, and database owner," on page 173 for information about additional requirements for the instance name.
- l** *<instancelocation>*  
Specifies the location to store the configuration files and logs for the directory server instance. On Windows systems, this option is required and a drive letter must be specified. This location must have at least 30 MB of free space. Additional disk space must be available to accommodate growth as the directory server log files increase.
- n**  
Specifies to run in no prompt mode. All output is generated, except for messages that require user interaction.
- p** *<port>*  
Specifies the port on which the directory server instance listens. Specify a positive number that is greater than 0 and less than 65535. The port specified must not cause a conflict with ports being used by any other directory server instance that is bound to a particular hostname or IP address.
- q**  
Specifies to run in quiet mode. All output is suppressed except error messages. If the **-d** option is also specified, trace output is not suppressed.
- r** *<description>*  
Specifies a description of the directory server instance.
- s** *<secureport>*  
Specifies the secure port that the directory server instance listens on. Specify a positive number that is greater than 0 and less than 65535. The ports specified must not cause a conflict with ports being used by any other directory server instance that is bound to a particular hostname or IP address.
- t** *<db2instance>*  
Specifies the DB2 database instance name. The database instance name is also the DB2 instance owner ID. By default, the database instance name is assumed to be the same as the directory server instance owner ID.
- v**  
Specifies to display version information about the command.
- ?**  
Displays the syntax format.

## Examples

To create a new directory server instance called **myinst** that has a port of 389, a secure port of 636, an encryption seed of **mysecretkey!**, and a DB2 instance with the name **myinst**, issue the command:

```
idsicrt -I myinst -p 389 -s 636 -e mysecretkey!
```

If the directory server instance already existed, this command would fail. If you did not specify the encryption seed, you would be prompted for the seed. In the following example, you are prompted to enter an encryption seed. The encryption

seed is not displayed on the command line when you enter it. After you type the encryption seed and press Enter, the command attempts to create the directory server instance.

```
idsicrt -I myinst -p 389 -s 636
```

The response is:

Enter encryption seed:

To create the same instance so that it binds to a particular IP address, issue the command:

```
idsicrt -I myinst -p 389 -s 636 -e mysecretkey! -i 1.9.86.566
```

To create a new directory server instance called **myinst** that has a port of 389, a secure port of 636, an encryption seed of **mysecretkey!**, and a DB2 instance with the name **mydbin**, the issue the command:

```
idsicrt -I myinst -p 389 -s 636 -e mysecretkey! -t mydbin
```

**Note:** If only the proxy server is installed on the computer, the **idsicrt** command does not create a DB2 database instance.

When created, a database instance normally requires 10 to 20 MB of space. This space is not used, however, if the directory server instance is configured as a proxy server.

## Using **idssethst** to set IP addresses

**idssethst** is the command to set the IP addresses a directory server instance binds to.

### Synopsis

```
idssethst [-I instancename -i ipaddress [-d debuglevel] [-b outputfile] [-q] [-n]] | -v | -?
```

### Description

The **idssethst** command can be run only by root on AIX, Linux, Solaris, or HP-UX, or a member of the Administrators group on Windows by default.

This command sets the IP addresses that a particular directory server instance binds to. The administrator specifies a directory server instance name and a list of IP addresses. The directory server instance and the administration daemon of the directory server instance being updated must be stopped. The **idssethst** command does not allow the IP addresses to be changed if another directory server instance is using any of the same ports on the specified IP addresses. The command replaces all of the current IP addresses configured for the directory server instance. If you specify to listen on all available IP addresses, the IP address attribute is removed from the configuration file.

### Options

**-b** <outputfile>

Specifies the full path of a file to redirect output into. If used in conjunction with the **-q** option, only errors are sent to the file. If debugging is turned on, that output is sent to the file also.

**-d** <debuglevel>

Sets the LDAP debugging level to <debuglevel>. This option causes the utility to generate debug output to stdout. The <debuglevel> is a bit mask

that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel. See the *IBM Tivoli Directory Server Problem Determination Guide* for more information about debug levels.

**-i** <ipaddress>

Specifies the IP address that the directory server instance binds to. If more than one IP address is specified, a comma separator is required with no spaces. Spaces are allowed only if the entire argument is enclosed in quotation marks. Use the key word "all" to specify to use all available IP addresses. If you do not specify the **-i** option, all available IP addresses is the default setting.

**-I** <instancename>

Specifies the name of the directory server instance that is to be updated.

**-n** Specifies to run in no prompt mode. All output is generated, except for messages that require user interaction.

**-q** Specifies to run in quiet mode. All output is suppressed except error messages. If the **-d** option is also specified, trace output is not suppressed.

**-v** Specifies to display version information about the command.

**-?** Displays the syntax format.

## Examples

To update the IP addresses of the directory server instance **myinst** to bind only to 1.3.45.668, issue the command:

```
idssethost -I myinst -i 1.3.45.668
```

To update the IP addresses of the directory server instance **myinst** to bind to all available IP addresses, issue the command:

```
idssethost -I myinst -i all
```

**Note:** You can also change the host name using the **idsldapmodify** command or the Web Administration tool. To be sure that there are no conflicts with other ports on particular IP addresses, be sure that IP address updates are done by the root administrator on the computer. If the IP address specified is not valid on the computer, the command fails.

## Using **idssetport** to set ports

**idssetport** is the command to set the ports that a directory server instance binds to.

### Synopsis

```
idssetport [-I instancename [-p port] [-s secureport] [-a admpport]
           [-c admsecureport] [-d debuglevel] [-b outputfile] [-q] [-n]] | -v | -?
```

### Description

By default, the **idssetport** command can be run only by root on AIX, Linux, Solaris, and HP-UX operating systems, or by a member of the Administrators group on Windows.

The command sets the specified ports that a particular directory server instance binds to. The administrator specifies a directory server instance name and the ports to update. The directory server instance that is being updated must be stopped before you run the command. If the administration daemon instance is running and an administration daemon instance port is changed, you must restart the administration daemon.

## Options

**-a** <admnport>

Specifies the port on which the administration daemon for the directory server instance listens. Specify a number that is greater than 1 and less than 65535. The ports specified must not cause a conflict with ports being used by any other directory server instance that is bound to a particular hostname or IP address.

**Note:** If you have two or more directory server instances listening on the same IP address (or set of IP addresses), be sure that those directory server instances do not use any of the same port numbers.

Click **Next**.

**-b** <outputfile>

Specifies the full path of a file to redirect output into. If used in conjunction with the **-q** option, only errors are sent to the file. If debugging is turned on, that output is sent to the file also.

**-c** <admsecureport>

Specifies the secure port on which the administration daemon for the directory server instance listens. Specify a number that is greater than 1 and less than 65535. The ports specified must not cause a conflict with ports being used by any other directory server instance that is bound to a particular hostname or IP address.

**-d** <debuglevel>

Sets the LDAP debugging level to <debuglevel>. This option causes the utility to generate debug output to stdout. The <debuglevel> is a bit mask that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel. See the *IBM Tivoli Directory Server Problem Determination Guide* for additional information on debug levels.

**-I** <instancename>

Specifies the name of the directory server instance that is to be updated.

**-n**

Specifies to run no prompt mode. All output is generated, except for messages that require user interaction.

**-p** <port>

Specifies the port that the directory server instance listens on. Specify a number that is greater than 1 and less than 65535. The port specified must not cause a conflict with ports being used by any other directory server instance that is bound to a particular hostname or IP address.

**-q**

Specifies to run in quiet mode. All output is suppressed except error messages. If the **-d** option is also specified, trace output is not suppressed.

**-s** <secureport>

Specifies the secure port on which the directory server instance will listen.

**-v**

Displays version information about the command.

**-?**

Displays the syntax format.

## Examples

To update the port of the directory server instance **myinst** to 555, issue the command:

```
idssetport -I myinst -p 555
```



### Notes:

1. By default, all ports between 1 and 1024, including ports 389 and 636, can be used only by the root administrator on AIX, Linux, Solaris, and HP-UX platforms.
2. You can also change the ports using the `idsldapmodify` command or the Web Administration tool. To be sure that there are no conflicts with other ports on particular IP addresses, be sure that IP address updates are done by the root administrator on the computer. If the port specified is not valid on the computer, the command fails.

## Using `idsilist` to view instance details

`idsilist` is the command to list directory server instances on the machine.

### Synopsis

```
idsilist [[-a | -r] [-d debuglevel] [-b outputfile]] | -v | -?
```

### Description

By default, the `idsilist` command can be run only by root on AIX, Linux, Solaris, or HP-UX, or by a member of the Administrators group on Windows. The command lists all of the directory server instances that exist on the machine. The command can also retrieve detailed information about each instance.

### Options

- a Specifies to list full information about each instance. This option cannot be used with the `-r` option.
- b *<outputfile>* Specifies the full path of a file to redirect output into. If debugging is turned on, that output is sent to this file also.
- d *<debuglevel>* Sets the LDAP debugging level to *<debuglevel>*. This option causes the utility to generate debug output to stdout. The *<debuglevel>* is a bit mask that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel. See the *IBM Tivoli Directory Server Problem Determination Guide* for more information on debug levels.
- r Specifies to list the full information about each instance. This provides the same information as the `-a` option, but the information is printed in a raw format. The information about each instance is printed on an individual line and each data item is separated by a number sign (#). This option cannot be used with the `-a` option.
- v Specifies to display version information about the command.
- ? Displays the syntax format.

### Examples

To get a list of directory server instances residing on the computer, issue the command:

```
idsilist
```

There are two instances in this example. The output is:

```
Directory server instances:  
myinst1  
myinst2
```



To obtain information about each instance, issue the same command with the **-a** or **-r** option. The command with the **-a** option is as follows:

```
idsilist -a
```

The output is:

Instance 1:

```
Name: myinst1
Version: 6.0
Location: c:
Description: IBM Tivoli Directory Server Instance V6.0
IP Addresses: All available
Port: 389
Secure Port: 636
Admin Daemon Port: 3538
Admin Daemon Secure Port: 3539
Type: Directory Server
```

Instance 2:

```
Name: myinst2
Version: 6.0
Location: c:
Description: IBM Tivoli Directory Server Instance V6.0
IP Addresses: All available
Port: 390
Secure Port: 637
Admin Daemon Port: 3540
Admin Daemon Secure Port: 3541
Type: Proxy Server
```

The command with the **-r** option is as follows:

```
idsilist -r
```

The output is:

```
Directory server instances:
myinst1#6.0#c:#IBM Tivoli Directory Server Instance V6.0#All available
#389#636#3538#3539#Directory Server
myinst2#6.0#c:#IBM Tivoli Directory Server Instance V6.0#All available
#390#637#3540#3541#Proxy Server
```

#### Notes:

1. The directory server types are Proxy Server, Directory Server, or Unknown. If no description is set for a directory server instance, no description is shown.
2. The IP address "All available" means that the directory server instance binds to all IP addresses. If the directory server instance binds only to certain IP addresses, a list separated by commas is presented. For example,  
IP Addresses: 1.3.45.333,1.2.45.222

## Using **idsidrop** to remove a directory server instance

**idsidrop** is the command to delete a directory server instance.

### Synopsis

```
idsidrop [-I instancename [-r] [-R] [-d debuglevel] [-b outputfile]
[-q] [-n]] | -v | -?
```

### Description

The **idsidrop** command can be run only by root on AIX, Linux, Solaris, and HP-UX, or by a member of the Administrators group on Windows. The administrator specifies a directory server instance name and optionally can specify

whether to delete the database instance. The command does not delete the directory server instance owner. The directory server instance must be stopped for this command to work.

## Options

**-b** *<outputfile>*

Specifies the full path of a file to redirect output into. Only errors are sent to the file if used in conjunction with the **-q** option. If debugging is turned on, that output is sent to this file also.

**-d** *<debuglevel>*

Sets the LDAP debugging level to *<debuglevel>*. This option causes the command to generate debug output to stdout. The *<debuglevel>* is a bit mask that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel. See the *IBM Tivoli Directory Server Problem Determination Guide* for more information about debug levels.

**-I** *<instancename>*

Specifies the name of the directory server instance.

**-n** Specifies to run in no prompt mode. All output is generated, except for messages that require user interaction.

**-q** Specifies to run in quiet mode. All output is suppressed except error messages. If the **-d** option is also specified, trace output is not suppressed.

**-r** Specifies to delete the database instance associated with the directory server instance. This option also deletes all databases contained in the database instance.

**-R** Specifies to only unconfigure the database instance and to retain the directory server instance.

**-v** Specifies to display version information about the command.

**-?** Displays the syntax format.

## Examples

To remove a directory server instance and retain the associated database instance, issue the command:

```
idsidrop -I <instancename>
```

To remove a directory server instance and destroy the associated database instance, issue the command:

```
idsidrop -I <instancename> -r
```

To unconfigure the associated database instance without removing a directory server instance, issue the command:

```
idsidrop -I <instancename> -R
```

---

## Chapter 14. Configuration

If you did not use the Instance Administration Tool to set the administrator DN and password or configure the database for the directory server instance, you can use either the Configuration Tool (**idsxcfg**) or command-line utilities for these tasks. You must set the administrator DN and password and, for a full server, configure the database before you can use the directory instance. Also, if you want to change the administrator DN or password after you have set it for the first time, you must use either the Configuration Tool or the command line.

**Note:** After you configure, see Chapter 15, “After you install and configure,” on page 149 for information about:

- Starting the server
- Starting the embedded version of WebSphere Application Server - Express service if you want to use the Web Administration Tool

You can find more information in the *IBM Tivoli Directory Server Version 6.0 Administration Guide*.

You can use the Configuration Tool for the following tasks:

- Managing the administrator DN and password.
- Configuring and unconfiguring the database
- Enabling and disabling the change log
- Adding and removing suffixes
- Adding and removing schema files
- Importing and exporting LDIF data
- Backing up, restoring, and optimizing the database

---

### Using the IBM Tivoli Directory Server Configuration Tool (**idsxcfg**)

To use the Configuration Tool:

1. On AIX, Linux, Solaris, or HP-UX systems, log in as **root**, as the directory server instance owner, or with a user ID that is in the primary group of the directory server instance owner. On Windows systems, log on as any user in the default Administrators group.
2. Type **idsxcfg** at a command prompt.

If you have more than one directory server instance on the computer, you must type **idsxcfg -I *instancename*** where *instancename* is the name of the directory server instance you want to configure.

3. The Configuration Tool window is displayed.

In the task list on the left, click the task you want to perform. For information about performing a task, see the section shown in the following list:

#### **Manage the administrator DN**

See “Managing the administrator DN for a directory server instance” on page 126.

#### **Manage the administrator password**

See “Managing the administrator password for a directory server instance” on page 127.

### **Configure the database**

See “Configuring the database for a directory server instance” on page 127. This option is not available if you are configuring a proxy server or if you have not installed the full server on the computer.

### **Unconfigure the database**

See “Unconfiguring the database for a directory server instance” on page 128. This option is not available if you are configuring a proxy server or if you have not installed the full server on the computer.

### **Manage the change log**

See “Enabling or disabling the change log for a directory server instance” on page 129. This option is not available if you are configuring a proxy server or if you have not installed the full server on the computer.

### **Manage suffixes**

See “Managing suffixes” on page 130. This option is not available if you are configuring a proxy server or if you have not installed the full server on the computer.

### **Manage schema files**

See “Managing schema files” on page 131.

**Note:** None of the following options are available if you are configuring a proxy server or if you have not installed the full server on the computer.

### **Import LDIF data**

See “Importing LDIF data” on page 132.

### **Export LDIF data**

See “Exporting LDIF data” on page 133.

### **Back up database**

See “Backing up the database” on page 135.

### **Restore database**

See “Restoring the database” on page 135.

### **Optimize database**

See “Optimizing the database” on page 135.

4. Close the Configuration Tool when you have completed all configuration tasks.

## **Managing the administrator DN for a directory server instance**

To set or change the administrator DN:

1. In the IBM Tivoli Directory Server Configuration Tool window, click **Manage administrator DN** in the task list on the left.
2. In the Manage administrator DN window on the right, type a valid DN (or accept the default DN, **cn=root**) in the **Administrator DN** field.

The IBM Directory Server administrator DN is the DN used by the administrator of the directory. This administrator is the one user who has full access to all data in the directory.

The default DN is **cn=root**. DNs are not case sensitive. If you are unfamiliar with X.500 format, or if for any other reason you do not want to define a new DN, accept the default DN.

3. Click **OK**.
4. A completion message is displayed. Click **OK**.

## Managing the administrator password for a directory server instance

To set or change the administrator password:

1. In the IBM Tivoli Directory Server Configuration Tool window, click **Manage administrator password** in the task list on the left.
2. In the Manage administrator password window on the right, type a password in the **Administrator password** field. Passwords are case-sensitive. Double byte character set (DBCS) characters in the password are not supported.

Record the password in a secure place for future reference.

**Note:** If the administration password policy has been enabled, the administrator's password must conform to the administration password policy requirements. See the *IBM Tivoli Directory Server Administration Guide* for information about the password policy.

3. Retype the password in the **Confirm password** field.
4. Click **OK**.
5. A completion message is displayed. Click **OK**.

## Configuring the database for a directory server instance

When you configure a database, the Configuration Tool adds information about the database that will be used to store directory data to the configuration file for the directory server instance. In addition, if the database does not already exist, the Configuration Tool creates the database.

### Notes:

1. Before configuring the database, be sure that the environment variable **DB2COMM** is **not** set.
2. The server must be stopped before you configure or unconfigure the database.
3. This option is not available if you are configuring a proxy server or if you have not installed the full server on the computer.

Before you configure the database, you must create a user ID for the owner of the database. This user ID must meet certain requirements. See Appendix D, "Setting up users and groups: directory server instance owner, database instance owner, and database owner," on page 173 for information about these requirements.

To configure a database for the directory server instance:

1. In the Configuration Tool, click **Configure database** in the task list on the left.
2. If a database user name is requested:
  - a. Type a user ID in the **Database user name** field. This user ID owns the database that is used by the directory instance, and the directory server instance uses this user ID to connect to the database. The user ID must already exist before you can configure the database. (See Appendix D, "Setting up users and groups: directory server instance owner, database instance owner, and database owner," on page 173 for more information about requirements for the user ID.)
  - b. Type a password for the user in the **Password** field. Passwords are case-sensitive.
  - c. In the **Database name** field, type the name you want to give the DB2 database that is used by the directory server instance to store directory data. The name can be from 1 to 8 characters long.

d. Click **Next**.

**Note:** If the database is already configured, only the password field is enabled. All other fields are pre-filled and disabled.

3. If the database installation location is requested:
  - a. Type the location for the database in the **Database install location** field. For Windows platforms, this location must be a drive letter. For AIX, Linux, Solaris, and HP-UX platforms, the location must be a directory name, such as /home/ldapdb, and you can click **Browse** to locate the directory.  
Be sure that you have at least 80 MB of free hard disk space in the location you specify and that additional disk space is available to accommodate growth as new entries are added to the directory.
  - b. Click the type of database you want to create. You can create a UCS Transformation Format (UTF-8) database, in which LDAP clients can store UTF-8 character data, or a local code page database, which is a database in the local code page.  
If you want to use language tags, the database must be a UTF-8 database. For more information about UTF-8, see Appendix N, "UTF-8 support," on page 197.
  - c. Click **Finish**.
4. Messages are displayed while the database is being configured. Click **Close** when database configuration is complete.

### Changing the password for the database owner

If you change the system password for the database owner after the database is configured for a directory server instance, the password is not automatically changed in the configuration file for the directory server instance. When the password for the database owner in the configuration file does not match the system password for the database owner user ID, the directory server instance starts only in configuration mode until you update the password in the configuration file.

To change the password for the database owner in the configuration file for the directory server instance:

1. In the Configuration Tool, click **Configure database** in the task list on the left.
2. Type the database owner's new password in the **Password** field. Passwords are case sensitive.
3. Click **Next**.
4. Click **Finish**.
5. Messages are displayed while the password is being changed. Click **Close** when processing is complete.

**Note:** If the change log is enabled, this procedure also updates the password for the change log database owner in the configuration file.

### Unconfiguring the database for a directory server instance

When you unconfigure the database, the Configuration Tool removes the database information for the directory server instance from the configuration file. Based on your selections, it might also delete the database (and all data in it).

**Note:** This option is not available if you are configuring a proxy server or if you have not installed the full server on the computer.

To unconfigure the database:

1. In the Configuration Tool, click **Unconfigure database** in the task list on the left.
2. In the Unconfigure database window, click one of the following:

**Unconfigure only**

Does not destroy any existing LDAP DB2 data. However, the configuration information for the database will be removed from the configuration file for the directory server instance, and the database will be inaccessible to the directory server instance.

**Unconfigure and destroy database**

Removes the existing database and its contents, and removes the configuration information for the database from the configuration file for the directory server instance.

3. Click **Unconfigure**.
4. In response to the confirmation message that is displayed, click **Yes**.

## Enabling or disabling the change log for a directory server instance

The change log database is used to record changes to the schema or directory entries in the typical LDAP entry structure that can be retrieved through the LDAP API. The change log records all update operations: add, delete, modify, and modrdn. The change log enables an IBM Tivoli Directory Server client application to retrieve a set of changes that have been made to an IBM Tivoli Directory Server database. The client might then update its own replicated or cached copy of the data.

You can use the Configuration Tool to enable or disable the change log.

**Notes:**

1. The server must be stopped before you enable or disable the change log.
2. This option is not available if you are configuring a proxy server or if you have not installed the full server on the computer.

### Enabling the change log

To enable the change log:

1. In the Configuration Tool, click **Manage changelog** in the task list on the left.
2. In the Configure/unconfigure changelog window, select the **Enable change log database** check box.
3. In the **Maximum number of log entries** box, click **Unlimited** if you want an unlimited number of entries in the change log. If you want to limit the number of entries, click **Entries** and type the maximum number of entries you want recorded. The default is 1,000,000 entries.
4. In the **Maximum age** box, accept the default of **Unlimited** if you want entries to remain in the change log indefinitely, or click **Age** and type the number of days and hours for which you want each entry to be kept.
5. Click **Update**.
6. Messages are displayed while the change log is being enabled. Click **Close** when the task is complete.

### Disabling the change log

To disable the change log:

1. In the Configuration Tool, click **Manage changelog** in the task list on the left.



2. In the Configure/unconfigure changelog window, clear the **Enable change log database** check box.
3. Click **Update**.
4. In response to the confirmation message, click **Yes**.
5. Messages are displayed while the change log is being disabled. Click **Close** when the task is complete.

## Managing suffixes

A suffix (also known as a naming context) is a DN that identifies the top entry in a locally held directory hierarchy. Because of the relative naming scheme used in LDAP, this DN is also the suffix of every other entry within that directory hierarchy. A directory server can have multiple suffixes, each identifying a locally held directory hierarchy; for example, `o=ibm,c=us`.

### Notes:

1. The specific entry that matches the suffix must be added to the directory.
2. This option is not available if you are configuring a proxy server or if you have not installed the full server on the computer.

Entries to be added to the directory must have a suffix that matches the DN value, such as `ou=Marketing,o=ibm,c=us`. If a query contains a suffix that does not match any suffix configured for the local database, the query is referred to the LDAP server that is identified by the default referral. If no LDAP default referral is specified, an **Object does not exist** result is returned.

**Note:** The server must be stopped before you add or remove suffixes.

### Adding a suffix

To add a suffix:

1. In the Configuration Tool, click **Manage suffixes** in the task list on the left. (This option is not available if you are configuring a proxy server or if you have not installed the full server on the computer.)
2. In the Manage suffixes window, type the suffix you want to add in the **SuffixDN** field, and click **Add**.
3. When you have added all the suffixes you want, click **OK**.

**Note:** When you click **Add**, the suffix is added to the list in the **Current suffix DNs** box; however, the suffix is not actually added to the directory until you click **OK**.

### Removing a suffix

Removing a suffix does not remove the entry from the directory, but only removes it from the configuration file.

To remove a suffix:

1. In the Configuration Tool, click **Manage suffixes** in the task list on the left. (This option is not available if you are configuring a proxy server or if you have not installed the full server on the computer.)
2. In the Manage suffixes window, click the suffix you want to remove in the **Current suffix DNs** box, and click **Remove**.
3. When you have selected all the suffixes you want to remove, click **OK**. The following suffixes cannot be removed:
  - `cn=pwdpolicy`



- cn=localhost
- cn=configuration
- cn=ibmpolicies

**Note:** When you click **Remove**, the suffix is removed from the list in the **Current suffix DNs** box; however, the suffix is not actually removed until you click **OK**.

4. In response to the confirmation message, click **Yes**.

## Managing schema files

You can use the Configuration Tool for the following schema file tasks:

- Adding a schema file to the list of schema files that will be loaded at startup
- Removing a schema file from the list of schema files that will be loaded at startup
- Changing the type of validation checking that is done for schema files

**Note:** The server must be stopped before you add or remove schema files.

### Adding a schema file

To add a schema file to the list of schema files that will be loaded at startup:

1. In the Configuration Tool, click **Manage schema files** in the task list on the left.
2. In the Manage schema files window, type the path and file name of the schema file you want to load at startup. (Alternatively, click **Browse** to search for the file.)
3. Click **Add**.

**Note:** When you click **Add**, the schema file is added to the list in the **Current schema files** box; however, the schema file is not actually added until you click **OK**.

4. When you have added all the schema files you want, click **OK**.

### Removing a schema file

To remove a schema file from the list of schema files that will be loaded at startup:

1. In the Configuration Tool, click **Manage schema files** in the task list on the left.
2. In the Manage schema files window, click the schema file you want to remove in the **Current schema files** box.
3. Click **Remove**.

#### Notes:

- a. The following schema files cannot be removed:

- V3.system.at
- V3.system.oc
- V3.config.at
- V3.config.oc
- V3.ibm.at
- V3.ibm.oc
- V3.user.at
- V3.user.oc
- V3.ldapsyntaxes
- V3.matchingrules

- V3.modifiedschema
- b. When you click **Remove**, the schema file is removed from the list in the **Current schema files** box; however, the schema file is not actually removed until you click **OK**.
  4. In response to the confirmation message, click **Yes**.
  5. When you have selected all the schema files you want to remove, click **OK** to process the files.

### Changing the type of validation checking that is done

To change the type of validation checking that is done on schema files:

1. In the Configuration Tool, click **Manage schema files** in the task list on the left.
2. In the Manage schema files window, accept the default schema validation rule in the **Schema validation rules** box, or click the rule you want. You can select one of the following rules:
  - Version 3 (Strict)  
LDAP version 3 strict validation checking is done. With this type of validation checking, all parent object classes must be present when adding entries.
  - Version 3 (Lenient)  
LDAP version 3 lenient validation checking is done. With this type of validation checking, all parent object classes do not need to be present when adding entries.  
This is the default.
  - Version 2  
LDAP version 2 checking is done.
  - None  
No validation checking is done.
3. Click **OK**.

## Importing and exporting LDIF data

You can use the Configuration Tool to import data from an LDAP Data Interchange Format (LDIF) file or to export data from the database to an LDIF file. LDIF is used to represent LDAP entries in text form. When importing, you can add entries to an empty directory database or to a database that already contains entries. You can also use the Configuration Tool to validate the data in the LDIF file without adding the data to the directory.

This option is not available if you are configuring a proxy server or if you have not installed the full server on the computer.

### Importing LDIF data

**Attention:** If you want to import LDIF data from another server instance, you must cryptographically synchronize the LDIF import file with the server instance that is importing the LDIF file; otherwise any AES-encrypted entries in the LDIF file will not be imported. See Appendix E, “Synchronizing two-way cryptography between server instances,” on page 177 for information about synchronizing directory server instances.

Before you begin to import data, also consider the following information:

**Notes:**

1. This option is not available if you are configuring a proxy server or if you have not installed the full server on the computer.
2. Before you import the data from an LDIF file, be sure to add any necessary suffixes. See “Adding a suffix” on page 130 for information about adding a suffix.
3. The server must be stopped before you import LDIF data.

To import data from an LDIF file:

1. In the Configuration Tool, click **Import LDIF data** in the task list on the left.
2. In the Import LDIF data window on the right, type the path and file name of the LDIF file in the **Path and LDIF file name** field. Alternatively, you can click **Browse** to locate the file.
3. If you want trailing spaces removed from the data, select the **Remove trailing spaces in Standard import or Bulkload** check box.
4. Click **Standard import** if you want to import the data using the **idsldif2db** utility, or click **Bulkload** if you want to import the data using the **idsbulkload** utility.

**Note:** For large LDIF files, the **idsbulkload** utility is a faster alternative to **idsldif2db** if you are importing a large number of entries.

5. If you clicked **Bulkload**, select the type or types of checking you want to perform on the LDIF data in the **Bulkload options** box. You can select one or more of the following:
  - Enable schema checking
  - Enable ACL checking
  - Enable password policy

Click **Import**.

**Note:** After loading large amounts of data, especially after populating the database using **idsbulkload**, be sure to optimize the database. This can make a significant improvement to the performance of the database

**Validating LDIF data without adding it to the database**

To validate the data in the LDIF file without adding it to the database:

1. In the Configuration Tool, click **Import LDIF data** in the task list on the left.
2. In the Import LDIF data window on the right, type the path and file name of the LDIF file in the **Path and LDIF file name** field. Alternatively, you can click **Browse** to locate the file.
3. Click **Data validation only**.
4. Click **Import**.

**Exporting LDIF data**

Before you export LDIF data, be sure that you have enough space to export all the data.

To export data from the database to an LDIF file:

1. In the Configuration Tool, click **Export LDIF data** in the task list on the left.
2. In the Export LDIF data window on the right, type the path and file name of the LDIF file in the **Path and LDIF file name** field. Alternatively, you can click **Browse** to locate the file.

3. If you want to overwrite the data in an existing file, select the **Overwrite if file exists** check box.
4. If you want to export the `creatorsName`, `createTimestamp`, `modifiersName`, and `modifyTimestamp` operational attributes, select the **Export operational attributes** check box.

These operational attributes are created and modified by the server when a directory entry is created or modified; they are also modified any time the entry is modified. They contain information about the user who created or modified the entry and the time the entry was created or modified. These entries are stored as a base-64-encoded control in the LDIF file.

5. If you are exporting data that will be imported into an Advanced Encryption Standard (AES)-enabled server and *if the two servers are not cryptographically synchronized*, select the **Export data for AES-enabled destination server** check box. Then complete the **Encryption seed** and **Encryption salt** fields with the values for the destination server. (See Appendix E, "Synchronizing two-way cryptography between server instances," on page 177 for information about cryptographic synchronization of servers.)

When the source server (the server you are exporting data from) and the destination server (the server into which you will be importing the data) are using non-matching directory key stash files, and you specify the encryption seed and salt values of the destination server, any AES-encrypted data will be decrypted using the source server's AES keys, then re-encrypted using the destination server's encryption seed and salt values. This encrypted data is stored in the LDIF file.

The encryption seed is used to generate a set of AES secret key values. These values are stored in a directory stash file and used to encrypt and decrypt directory stored password and secret key attributes. The encryption seed must contain only printable ISO-8859-1 ASCII characters with values in the range of 33 to 126, and must be a minimum of 12 and a maximum of 1016 characters in length. See Appendix J, "ASCII characters from 33 to 126," on page 189 for information about these characters.

The encryption salt is a randomly generated value that is used to generate AES encryption keys. You can obtain the destination server's salt value by searching (using the `ldapsearch` utility) the destination server's "`cn=crypto,cn=localhost`" entry. The attribute type is `ibm-slapdCryptoSalt`.

6. If you want to export only some of the data in the directory, complete the **Subtree DN** field. The subtree DN identifies the top entry of the subtree that is to be written to the LDIF output file. This entry, plus all entries below it in the directory hierarchy, are written to the file. If you do not specify this option, all directory entries stored in the database are written to the output file based on the suffixes specified in the IBM Tivoli Directory Server configuration file.
7. Click **Export**.

## Backing up, restoring, and optimizing the database

You can use the Configuration Tool for the following database tasks:

- Backing up the data in the database
- Restoring data and, optionally, configuration settings that were previously backed up
- Updating statistics related to the data tables for the purpose of improving performance and query speed

This option is not available if you are configuring a proxy server or if you have not installed the full server on the computer.

## Backing up the database

The server must be stopped before you can back up the database.

To back up the database:

1. In the Configuration Tool, click **Backup database** in the task list on the left.
2. In the Backup database window on the right, in the **Backup directory** field, type the directory path in which to back up all directory data and configuration settings. Alternatively, click **Browse** to locate the directory path.
3. Click one of the following:
  - **Create backup directory as needed** if you want the directory to be created if it does not exist.
  - **Halt if backup directory is not found** if you do not want the directory you specified to be created. If this directory does not exist and you select this option, the database will not be backed up.
4. Click **Backup**.

## Restoring the database

The server must be stopped before you can restore the database.

### Notes:

1. A database can be restored only into a database and database instance with the same names that were used for the database backup.
2. The restore function works only if a database is currently configured for a given directory server instance. The restore function restores the backup database into the currently configured database. The command fails if the backed up database instance and database do not match the configured database instance and database. Additionally, the restore function requires that the database location of the backed up database and the database it is restoring are the same.

To restore the database:

1. In the Configuration Tool, click **Restore database** in the task list on the left.
2. In the Restore database window on the right, in the **Restore directory** field, type the path in which the directory was previously backed up. Alternatively, click **Browse** to locate the path.
3. If you want to restore only the directory data, but not the configuration settings, select the **Restore data only (not configuration settings)** check box. If you want to restore both data and configuration settings, be sure the check box is cleared.
4. Click **Restore**.

## Optimizing the database

The server must be stopped before you can optimize the database.

Optimize the database to update statistics related to the data tables; this can improve performance and query speed. Perform this action periodically or after heavy database updates; for example, after importing database entries.

1. In the Configuration Tool, click **Optimize database** in the task list on the left.
2. In the Optimize database window on the right, click **Optimize**.

## Using command-line utilities for configuration

You can use command-line utilities instead of the Configuration Tool for the following tasks:

- Setting or changing the administrator DN and password. See “Using `idsdnpw` to set the administrator DN and password” for instructions.
- Configuring a database. See “Using `idscfgdb` to configure the database” on page 138 for instructions.
- Unconfiguring a database. See “Using `idsucfgdb` to unconfigure the database” on page 140 for instructions.
- Enabling the change log. See “Using `idscfgchglg` to configure the change log” on page 141 for instructions.
- Disabling the change log. See “Using `idsucfgchglg` to unconfigure the change log” on page 142 for instructions.
- Adding a suffix. See “Using `idscfgsuf` to add a suffix” on page 143 for instructions.
- Removing a suffix. See “Using `idsucfgsuf` to remove a suffix” on page 144 for instructions.
- Adding a schema file. See “Using `idscfgsch` to add a schema file” on page 146 for instructions.
- Removing a schema file. See “Using `idsucfgsch` to unconfigure a schema file” on page 146 for instructions.

**Note:** In previous releases, the `ldapcfg` and `ldapucfg` commands were used for many of these tasks. See the following table for information about the commands that are used in IBM Tivoli Directory Server 6.0 for configuration, and the equivalent commands used in previous releases.

Table 3. Commands for configuration in current and previous releases

| Task  | IBM Tivoli Directory Server 6.0 command | Earlier release command          |
|---|---|----------------------------------|
| Setting or changing the administrator DN and password | <code>idsdnpw</code>                    | <code>ldapcfg -u -p</code>       |
| Configuring the database                              | <code>idscfgdb</code>                   | <code>ldapcfg -l -a -w -d</code> |
| Unconfiguring the database                            | <code>idsucfgdb</code>                  | <code>ldapucfg -d</code>         |
| Enabling the change log                               | <code>idscfgchglg</code>                | <code>ldapcfg -g</code>          |
| Disabling the change log                              | <code>idsucfgchglg</code>               | <code>ldapucfg -g</code>         |
| Adding a suffix                                       | <code>idscfgsuf</code>                  | <code>ldapcfg -s</code>          |
| Removing a suffix                                     | <code>idsucfgsuf</code>                 | No command-line equivalent       |
| Adding a schema file                                  | <code>idscfgsch</code>                  | No command-line equivalent       |
| Removing a schema file                                | <code>idsucfgsch</code>                 | No command-line equivalent       |

## Using `idsdnpw` to set the administrator DN and password

`idsdnpw` is the administrator DN and password utility.

### Synopsis

```
idsdnpw [-I instancename] [[-u userDN] -p password] [-f configfile] [-d debuglevel]
        [-b outputfile] [-q] [-n]] | -v | -?
```

## Description

The **idsdnpw** command provides a way to change the administrator DN and password for a directory server instance. The command can be run only when the directory server instance is not running. The administrator specifies an administrator password and, optionally, an administrator DN, which the utility writes to the `ibmslapd.conf` file for the directory server instance. The administrator DN is set to `cn=root` by default.

## Options

**-b** *<outputfile>*

Specifies the full path of a file to redirect output into. If used in conjunction with the **-q** option, only errors are sent to the file. If debugging is turned on, that output is sent to the file also.

**-d** *<debuglevel>*

Sets the LDAP debugging level to *<debuglevel>*. This option causes the utility to generate debug output to stdout. The *<debuglevel>* is a bit mask that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel. See the *IBM Tivoli Directory Server Problem Determination Guide* for additional information about debug levels.

**-f** *<configfile>*

Specifies the full path to the configuration file that is to be updated. If this option is not specified, the default configuration file for the directory server instance is used.

**-I** *<instancename>*

Specifies the name of the directory server instance. This option is required if there are additional directory server instances on the computer.

**-n**

Causes the command to run in no prompt mode. All output is generated, except for messages that require user interaction. This option requires the **-p** option.

**-p** *<password>*

Specifies the directory administrator password to change to. If an administrator DN value is not specified (the **-u** option), the current value of the administrator DN is used. If the administrator DN is not defined, the default value, `cn=root`, is used. This option is required if the **-n** option is specified.

**Note:** Double byte character set (DBCS) characters in the password are not supported.

**-q**

Causes the command to run in quiet mode. All output is suppressed except error messages. If the **-d** option is also specified, trace output is not suppressed.

**-u** *<userDN>*

Specifies the directory administrator DN to create or change to.

**Note:**

Do not use single quotation marks (') to define DNs with spaces in them. They are not interpreted correctly.

**-v**

Causes the command to display version information.

**-?**

Displays the syntax format.



## Examples

To set the administrator DN to cn=myname and the password to secret, issue the command:

```
idsdnpw -u cn=myname -p secret
```

If the password is not specified, you are prompted for the password. Your password is not displayed on the command line when you enter it.

**Note:** If the administration password policy has been enabled, the administrator's password must conform to the administration password policy requirements. See the *IBM Tivoli Directory Server Administration Guide* for information about the password policy.

## Using idscfgdb to configure the database

**idscfgdb** is the command to configure a database for a directory server instance.

This command cannot be used for a proxy server instance.

### Synopsis

```
idscfgdb [-I instancename [-w dbadminpw] [-a dbadminid -t dbname -l dblocation  
[-x]] [-f configfile] [-d debuglevel] [-b outputfile] [-q] [-n]] | -v | -?
```

### Description

The **idscfgdb** command configures the database for a directory server instance. The database instance must already exist and for AIX, Linux, Solaris, and HP-UX systems, the local loopback service must be registered in the `/etc/services` file. Otherwise, the command fails.

The directory server instance owner specifies a database administrator user ID, a database administrator password, the location to store the database, and the name of the database. The database administrator ID specified must already exist on the system. See Appendix D, "Setting up users and groups: directory server instance owner, database instance owner, and database owner," on page 173 for information about requirements for this ID.

By using the **-w** option, you can reset the password for the database administrator and the change log database owner in the configuration file for the directory server instance.

After successfully creating the database, the command adds information about the database to the `ibmslapd.conf` file of the directory server instance. The database and local loopback settings are created, if they do not exist. You can specify whether to create the database as a local codepage database or as a UTF-8 database, which is the default.

#### Attention:

1. Before configuring the database, be sure that the environment variable `DB2COMM` is **not** set.
2. The server must be stopped before you configure the database.

### Options

**-a** *<dbadminid>*

Specifies the DB2 administrator ID. This ID must already exist on the system and have the proper authority.



- b** <outputfile>  
Specifies the full path of a file to redirect output into. If used in conjunction with the **-q** option, only errors are sent to the file. If debugging is turned on, that output is sent to the file also.
- d** <debuglevel>  
Sets the LDAP debugging level to <debuglevel>. This option causes the utility to generate debug output to stdout. The <debuglevel> is a bit mask that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel. See the *IBM Tivoli Directory Server Problem Determination Guide* for more information about debug levels.
- f** <configfile>  
Specifies the full path to the configuration file that is to be updated. If this option is not specified, the default configuration file for the directory server instance is used.
- I** <instancename>  
Specifies the name of the directory server instance that is to be updated.
- l** <dblocation>  
Specifies the DB2 database location. For AIX, Linux, Solaris, and HP-UX systems, this is a directory name (for example, /home/ldapdb2). For Windows systems, this must be a drive letter. The database requires at least 80 MB of free space. Additional disk space is needed to accommodate growth as directory entries are added.
- n**  
Causes the command to run in no prompt mode. All output is generated, except for messages that require user interaction. This option requires the **-w** option.
- q**  
Causes the command to run in quiet mode. All output is suppressed except error messages. If the **-d** option is also specified, trace output is not suppressed.
- t** <dbname>  
Specifies the DB2 database name.
- v**  
Displays version information about the command.
- w** <dbadminpw>  
Sets the password for the DB2 administrator in the configuration file for the directory server instance. Also sets the password for the change log database owner in the configuration file if the change log is enabled.  
  
This option is required for the **-n** option.
- x**  
Creates the DB2 database in a local codepage.
- ?**  
Displays the syntax format.

## Examples

To configure a database called ldapdb for directory server instance ldapdb in the location /home/ldapdb with a DB2 database administrator ID of ldapdb whose password is secret, issue the command:

```
idscfgdb -I ldapdb -a ldapdb -w secret -t ldapdb -l /home/ldapdb
```

If the password is not specified, you are prompted for the password. The password is not displayed on the command line when you type it.

## Using idsucfgdb to unconfigure the database

**idsucfgdb** is the command to unconfigure a database for a directory server instance.

This command cannot be used for a proxy server instance.

### Synopsis

```
idsucfgdb [-I instancename [-r] [-f configfile] [-d debuglevel] [-b outputfile]
          [-q] [-n]] | -v | -?
```

### Description

The **idsucfgdb** command unconfigures the database for a directory server instance. By default, the command only unconfigures the database from the `ibmslapd.conf` file and does not delete the database. You can use the `-r` option to specify that you want to delete the database during the unconfiguration process. You are prompted to confirm that you want to continue with the actions you requested.

### Options

**-b** <outputfile>

Specifies the full path of a file to redirect output into. Only errors are sent to the file if used in conjunction with the `-q` option. If debugging is turned on, that output is sent to the file also.

**-d** <debuglevel>

Sets the LDAP debugging level to <debuglevel>. This option causes the utility to generate debug output to stdout. The <debuglevel> is a bit mask that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel. See the *IBM Tivoli Directory Server Problem Determination Guide* for more information about debug levels.

**-f** <configfile>

Specifies the full path to the configuration file that is to be updated. If this option is not specified, the default configuration file for the directory server instance is used.

**-I** <instancename>

Specifies the name of the directory server instance that is to be updated.

**-n**

Causes the command to run no prompt mode. All output is generated, except for messages that require user interaction. This option requires the `-w` option.

**-q**

Causes the command to run in quiet mode. All output is suppressed except error messages. If the `-d` option is also specified, trace output is not suppressed.

**-r**

Causes the command to destroy any database currently configured with the directory server instance.

**-v**

Displays version information about the command.

**-?**

Displays the syntax format.

### Examples

To unconfigure the database for directory server instance `myinstance` and not prompt before unconfiguring, issue the command:

```
idsucfgdb -n -I myinstance
```

To unconfigure and delete the database for directory server instance `myinstance` and not prompt for confirmation before removing the directory server instance, issue the command:

```
idsucfgdb -r -n -I myinstance
```

## Using `idscfgchglg` to configure the change log

`idscfgchglg` is the command to configure a change log for a directory server instance.

This command cannot be used for a proxy server instance.

### Synopsis

```
idscfgchglg [-I instancename [-m maxentries] [-y maxdays] [-h maxhours]
             [-f configfile] [-d debuglevel] [-b outputfile] [-q] [-n]] |
             -v | -?
```

### Description

The `idscfgchglg` command configures a change log for a directory server instance. The change log is a database that is created in the same database instance as the directory server instance database. An additional 30 MB of hard disk space are required. The change log information is added to the directory server instance's `ibmslapd.conf` file. A change log requires the following:

- A database instance with the same name as the directory server instance must already exist.
- A database for the directory server instance must already be configured.
- For AIX, Linux, Solaris, and HP-UX platforms, the local loopback service must be registered in the `/etc/services` file.

Otherwise, the command fails.

You can optionally specify the maximum number of entries to keep in the change log and the maximum age to which each entry in the change log is kept until it is automatically destroyed. If you do not specify any options, the entries in the change log never expire and the size of the change log is a maximum of 1,000,000 entries.

### Options

**-b** *<outputfile>*

Specifies the full path of a file to redirect output into. If used in conjunction with the **-q** option, only errors are sent to the file. If debugging is turned on, that output is sent to the file also.

**-d** *<debuglevel>*

Sets the LDAP debugging level to *<debuglevel>*. This option causes the utility to generate debug output to stdout. The *<debuglevel>* is a bit mask that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel. See the *IBM Tivoli Directory Server Problem Determination Guide* for more information about debug levels.

**-f** *<configfile>*

Specifies the full path to the configuration file that is to be updated. If this option is not specified, the default configuration file for the directory server instance is used.

**-h** *<maxhours>*

Specifies in hours the maximum amount of time to keep entries in the

change log. This option can be used with the **-y** *<maxdays>* option to specify the maximum age of a change log entry.

- I** *<instancename>*  
Specifies the name of the directory server instance that is to be updated.
- n**  
Causes the command to run no prompt mode. All output is generated, except for messages that require user interaction.
- m** *<maxentries>*  
Specifies the maximum number of entries to keep in the change log. A value of 0 means there is no limit on the number of entries.
- q**  
Causes the command to run in quiet mode. All output is suppressed except error messages. If the **-d** option is also specified, trace output is not suppressed.
- y** *<maxdays>*  
Specifies in days the maximum amount of time to keep entries in the change log. A value of 0 means that there is no age limit on entries in the change log. This option can be used with the **-h** *<maxhours>* option to specify the maximum age of a change log entry.
- v**  
Displays version information about the command.
- ?**  
Displays the syntax format.

## Examples

To configure a change log for directory server instance `ldapdb` with no age limit or size limit, issue the command:

```
idsucfgchglg -I ldapdb -m 0
```

To configure a default change log for directory server instance `ldapdb` with a size limit of 1,000,000 and an entry age of 25 hours, issue the command:

```
idsucfgchglg -I ldapdb -y 1 -h 1
```

**Note:** After the change log is configured, the **-y**, **-h**, and **-m** options can be used to update the maximum age and maximum size of the entries in the change log.

## Using `idsucfgchglg` to unconfigure the change log

`idsucfgchglg` is the command to unconfigure a change log for a directory server instance.

This command cannot be used for a proxy server instance.

### Synopsis

```
idsucfgchglg [-I instancename [-f configfile] [-d debuglevel]  
              [-b outputfile] [-q] [-n]] | -v | -?
```

### Description

The `idsucfgchglg` command unconfigures a change log for a directory server instance. A change log must be currently configured in the `ibmslapd.conf` file for the directory server instance. No parameters are needed to remove the change log and the change log information from the `ibmslapd.conf` file. The directory server instance owner is prompted to confirm the action before the change log is deleted.

## Options

**-b** <outputfile>

Specifies the full path of a file to redirect output into. Only errors are sent to the file if used in conjunction with the **-q** option. If debugging is turned on, that output is sent to the file also.

**-d** <debuglevel>

Sets the LDAP debugging level to <debuglevel>. This option causes the utility to generate debug output to stdout. The <debuglevel> is a bit mask that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel. See the *IBM Tivoli Directory Server Problem Determination Guide* for more information about debug levels.

**-f** <configfile>

Specifies the full path to the configuration file that is to be updated. If this option is not specified, the default configuration file for the directory server instance is used.

**-I** <instancename>

Specifies the name of the directory server instance that is to be updated.

**-n** Causes the command to run no prompt mode. All output is generated, except for messages that require user interaction.

**-q** Causes the command to run in quiet mode. All output is suppressed except error messages. If the **-d** option is also specified, trace output is not suppressed.

**-v** Displays version information about the command.

**-?** Displays the syntax format.

## Examples

To unconfigure the directory server instance's change log without prompting the user for confirmation, issue the command:

```
idsucfgchglg -I <instancename> -n
```

To unconfigure the change log for the directory server instance myinstance on a computer with multiple instances, issue the command:

```
idsucfgchglg -I myinstance
```

## Using idscfgsuf to add a suffix

**idscfgsuf** is the command to configure a suffix for a directory server instance.

This command cannot be used for a proxy server instance.

### Synopsis

```
idscfgsuf [-I instancename -s suffix [-f configfile] [-d debuglevel] [-b outputfile] [-q] [-n]] | -v | -?
```

### Description

The **idscfgsuf** command configures a new suffix for a directory server instance. The suffix is added to the directory server instance's `ibmslapd.conf` file. This command fails if the directory server instance is a proxy server or if the suffix already exists in the configuration file.

## Options

- b** <outputfile>  
Specifies the full path of a file to redirect output into. If used in conjunction with the **-q** option, only errors are sent to the file. If debugging is turned on, that output is sent to the file also.
- d** <debuglevel>  
Sets the LDAP debugging level to <debuglevel>. This option causes the utility to generate debug output to stdout. The <debuglevel> is a bit mask that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel. See the *IBM Tivoli Directory Server Problem Determination Guide* for more information about debug levels.
- f** <configfile>  
Specifies the full path to the configuration file that is to be updated. If this option is not specified, the default configuration file for the directory server instance is used.
- I** <instancename>  
Specifies the name of the directory server instance. This option is required if there are additional directory server instances on the local machine.
- n**  
Causes the command to run no prompt mode. All output is generated, except for messages that require user interaction.
- q**  
Causes the command to run in quiet mode. All output is suppressed except error messages. If the **-d** option is also specified, trace output is not suppressed.
- s** <suffix>  
Specifies the suffix to add to the directory server instance.
- v**  
Displays version information about the command.
- ?**  
Displays the syntax format.

## Examples

To configure the suffix `o=ibm,c=us` on a computer with a single directory server instance, issue the command:

```
idsucfgsuf -s o=ibm,c=us
```

To configure the suffix `o=ibm,c=us` on a computer with a multiple directory server instances, issue the command:

```
idsucfgsuf -I <instancename> -s o=ibm,c=us
```

## Using idsucfgsuf to remove a suffix

**idsucfgsuf** is the command to remove a suffix from a directory server instance.

This command cannot be used for a proxy server instance.

## Synopsis

```
idsucfgsuf [-I instancename -s suffix [-f configfile] [-d debuglevel]  
           [-b outputfile] [-q] [-n]] | -v | -?
```

## Description

The `idsucfgsuf` removes a suffix from a directory server instance. The suffix is removed from the directory server instance's `ibmslapd.conf` file. This command fails if the directory server instance is a proxy server or if the suffix does not exist in the configuration file.

## Options

**-b** *<outputfile>*

Specifies the full path of a file to redirect output into. Only errors are sent to the file if used in conjunction with the **-q** option. If debugging is turned on, that output is sent to the file also.

**-d** *<debuglevel>*

Sets the LDAP debugging level to *<debuglevel>*. This option causes the utility to generate debug output to stdout. The *<debuglevel>* is a bit mask that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel. See the *IBM Tivoli Directory Server Problem Determination Guide* for more information about debug levels.

**-f** *<configfile>*

Specifies the full path to the configuration file that is to be updated. If this option is not specified, the default configuration file for the directory server instance is used.

**-I** *<instancename>*

Specifies the name of the directory server instance. This option is required if there are additional directory server instances on the computer.

**-n** Causes the command to run no prompt mode. All output is generated, except for messages that require user interaction.

**-q** Causes the command to run in quiet mode. All output is suppressed except error messages. If the **-d** option is also specified, trace output is not suppressed.

**-s** *<suffix>*

Specifies the suffix to remove from the directory server instance.

**-v** Displays version information about the command.

**-?** Displays the syntax format.

## Examples

To remove the suffix `o=ibm,c=us` from the `ibmslapd.conf` file on a computer with a single directory server instance, issue the command:

```
idsucfgsuf -s o=ibm,c=us
```

To remove the suffix `o=ibm,c=us` from the `ibmslapd.conf` file of a directory server instance on a computer with multiple directory server instances, issue the command:

```
idsucfgsuf -I <instancename> -s o=ibm,c=us
```

**Note:** These system defined suffixes cannot be removed:

- `cn=pwdpolicy`
- `cn=localhost`
- `cn=configuration`
- `cn=ibmpolicies`

## Using idscfgsch to add a schema file

`idscfgsch` is the command to configure a schema file for a directory server instance.

### Synopsis

```
idscfgsch [-I instancename -s schemafile [-f configfile] [-d debuglevel]
          [-b outputfile] [-q] [-n]] | -v | -?
```

### Description

The `idscfgsch` command configures a schema file for a directory server instance. The schema file must exist on the computer. The directory server instance owner must specify the schema file to add to the directory server instance's `ibmslapd.conf` file.

### Options

- b** <outputfile>  
Specifies the full path of a file to redirect output into. If used in conjunction with the **-q** option, only errors are sent to the file. If debugging is turned on, that output is sent to the file also.
- d** <debuglevel>  
Sets the LDAP debugging level to <debuglevel>. This option causes the utility to generate debug output to stdout. The <debuglevel> is a bit mask that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel. See the *IBM Tivoli Directory Server Problem Determination Guide* for more information about debug levels.
- f** <configfile>  
Specifies the full path to the configuration file that is to be updated. If this option is not specified, the default configuration file for the directory server instance is used.
- I** <instancename>  
Specifies the name of the directory server instance that is to be updated.
- n**  
Causes the command to run no prompt mode. All output is generated, except for messages that require user interaction.
- q**  
Causes the command to run in quiet mode. All output is suppressed except error messages. If the **-d** option is also specified, trace output is not suppressed.
- s** <schemafile>  
Specifies the schema file to add to the directory server instance.
- v**  
Displays version information about the command.
- ?**  
Displays the syntax format.

### Examples

To configure the schema file `/home/mydir/myschema.oc` in the directory server instance's `ibmslapd.conf` file, issue the command:

```
idscfgsch -s /home/mydir/myschema.oc
```

## Using idsucfgsch to unconfigure a schema file

`idsucfgsch` is the command to unconfigure a schema file for a directory server instance.



## Synopsis

```
idsucfgsch [-I instancename -s schemafile [-f configfile] [-d debuglevel]
           [-b outputfile] [-q] [-n]] | -v | -?
```

## Description

The **idsucfgsch** command unconfigures a schema file for a directory server instance. The schema file must be currently configured in the directory server instance's `ibmslapd.conf` file. The directory server instance owner must specify the schema file to remove from the directory server instance's `ibmslapd.conf` file.

## Options

**-b** <outputfile>

Specifies the full path of a file to redirect output into. If used in conjunction with the **-q** option, only errors are sent to the file. If debugging is turned on, that output is sent to the file also.

**-d** <debuglevel>

Sets the LDAP debugging level to <debuglevel>. This option causes the utility to generate debug output to stdout. The <debuglevel> is a bit mask that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel. See the *IBM Tivoli Directory Server Problem Determination Guide* for more information about debug levels.

**-f** <configfile>

Specifies the full path to the configuration file that is to be updated. If this option is not specified, the default configuration file for the directory server instance is used.

**-I** <instancename>

Specifies the name of the directory server instance that is to be updated.

**-n** Causes the command to run no prompt mode. All output is generated, except for messages that require user interaction.

**-q** Causes the command to run in quiet mode. All output is suppressed except error messages. If the **-d** option is also specified, trace output is not suppressed.

**-s** <schemafile>

Specifies the schema file to remove from the directory server instance.

**-v** Displays version information about the command.

**-?** Displays the syntax format.

## Examples

To unconfigure the schema file `/home/mydir/myschema.oc` from the directory server instance's `ibmslapd.conf` file, issue the command:

```
idsucfgsch -s /home/mydir/myschema.oc
```

**Note:** The following system-defined schema files cannot be removed:

1. V3.system.at
2. V3.system.oc
3. V3.config.at
4. V3.config.oc
5. V3.ibm.at
6. V3.ibm.oc

7. V3.user.at
8. V3.user.oc
9. V3.ldapsyntaxes
10. V3.matchingrules
11. V3.modifiedschema

---

## Importing or exporting data

To import data from an LDIF file, you can use either the **idsldif2db** or the **idsbulkload** utility.

To export data to an LDIF file, you can use the **idsdb2ldif** utility.

See the *IBM Tivoli Directory Server Version 6.0 Administration Guide* for instructions.

---

## Backing up, restoring, and optimizing the database

For information about the following command-line utilities, see the *IBM Tivoli Directory Server version 6.0 Administration Guide*:

- Backing up the database using the **idsdbback** command
- Restoring the database using the **idsdbrestore** command
- Optimizing the database using the **idsrunstats** command

These commands cannot be used for proxy server instances.

---

## Chapter 15. After you install and configure

After you install the server, create the directory server instance, set the administrator DN and password, and configure the database (for a full server only), you can start the directory server instance. If you installed the Web Administration Tool and the embedded version of WebSphere Application Server - Express, you can also start the application server.

---

### Starting the directory server instance

To start the directory server instance using the command line, type `idsslapd -I instancename` at a command prompt. *instancename* is the name of the directory server instance you want to start.

On Windows systems, you can also start and stop the directory server instance through the **Services** folder.

- To start the directory server instance, in the **Services** folder, click **IBM Tivoli Directory Server Instance V6.0 - instancename**. Then click **Actions** → **Start**.
- To stop the directory server instance, in the **Services** folder, click **IBM Tivoli Directory Server Instance V6.0 - instancename**. Then click **Actions** → **Stop**.

*instancename* is the name of the directory server instance you want to start or stop.

For information about starting and stopping the server and performing other administrative tasks using the Web Administration Tool and the command line, see the *IBM Tivoli Directory Server Version 6.0 Administration Guide*.

---

### Starting the application server to use the Web Administration Tool

To start the application server if you are using the embedded version of WebSphere Application Server - Express as your application server:

Type one of the following at a command prompt.

- `WASPath\bin\startServer.bat server1` for Windows systems
- `WASPath/bin/startServer.sh server1` for AIX, Linux, Solaris, or HP-UX systems

where *WASPath* is the path where you installed the embedded version of WebSphere Application Server - Express. This path is:

- By default on Windows: `c:\Program Files\IBM\LDAP\V6.0\appsrv`
- On AIX, Solaris, and HP-UX: `/opt/IBM/ldap/V6.0/appsrv`
- On Linux: `/opt/ibm/ldap/V6.0/appsrv`

---

### Starting the Web Administration Tool

To start the Web Administration Tool:

1. After you have started the application server, from a Web browser, type the following address: `http://localhost:12100/IDSWebApp/IDSjsp/Login.jsp`  
The IBM Tivoli Directory Server Web Administration Tool Login page is displayed.

**Note:** This address works only if you are running the browser on the computer on which the Web Administration Tool is installed. If the Web Administration Tool is installed on a different computer, replace **localhost** with the hostname or IP address of the computer where the Web Administration Tool is installed.

2. Log in to the console as the console administrator, using the following instructions:
  - a. Be sure that **Console Admin** is displayed in the **LDAP Hostname** field.
  - b. In the **Username** field, type superadmin.
  - c. In the **Password** field, type secret.

The IBM Tivoli Directory Server Web Administration Tool console is displayed.

3. Add the server to the console, using the following instructions:
  - a. Expand **Console administration** in the navigation area.
  - b. Click **Manage console servers**. A table of server host names and port numbers is displayed.
  - c. Click **Add**.
  - d. Type the hostname or the IP address of the server in the **Hostname** field; for example, myserver.mycity.mycompany.com
  - e. Specify the server port number in the **Port** field and the Admin daemon port number in the **Administration port** field. You can accept the defaults.
  - f. Select the **Enable SSL encryption** check box if the server is SSL-enabled.
  - g. Click **OK**, and then click **OK** again on the confirmation panel.
4. Click **Logout** in the navigation area.
5. Log in as the directory server instance administrator:
  - a. On the IBM Tivoli Directory Server Web Administration Login Tool page, select the LDAP host name or IP address for your computer from the drop-down menu for the **LDAP Hostname** field.
  - b. Type the administrator DN and the password for the directory server instance. You specified these fields during instance creation.
  - c. Click **Login**.

For detailed information about using the Web Administration Tool, see the *IBM Tivoli Directory Server Version 6.0 Administration Guide*.

---

## Stopping the application server

Use one of the following commands to stop the application server:

- On Windows systems:

```
WASPath\bin\stopServer.bat server1
```
- On AIX, Linux, Solaris, or HP-UX systems:

```
WASPath/bin/stopServer.sh server1
```

where *WASPath* is the path where you installed the embedded version of WebSphere Application Server - Express. This path is:

- By default on Windows: c:\Program Files\IBM\LDAP\V6.0\appsrv
- On AIX, Solaris, and HP-UX: /opt/IBM/ldap/V6.0/appsrv
- On Linux: /opt/ibm/ldap/V6.0/appsrv

---

## Chapter 16. Uninstalling IBM Tivoli Directory Server

Use the following sections to uninstall IBM Tivoli Directory Server.

### Notes:

1. If you uninstall IBM Tivoli Directory Server without unconfiguring your databases or deleting your directory server instances, they are left intact. If you plan to install IBM Tivoli Directory Server again and you want to preserve your data, do not unconfigure the database or remove the directory server instance or instances before you uninstall.
2. The `idsldap` user and group are left on the system after you uninstall IBM Tivoli Directory Server. If you do not want this user and group defined, you can remove them using operating system utilities for your operating system. This user and group are needed by both the proxy and the full server and they must remain defined if you have either server installed.

---

### Uninstalling IBM Tivoli Directory Server using the InstallShield GUI

This section describes how to uninstall the IBM Tivoli Directory Server using the InstallShield GUI.

### Notes:

1. If you installed IBM Tivoli Directory Server using the InstallShield GUI, use the InstallShield GUI to uninstall.

If you inadvertently uninstall IBM Tivoli Directory Server using operating system utilities after installing using the InstallShield GUI, follow the process in “Uninstalling IBM Tivoli Directory Server using the InstallShield GUI” and the instructions in the *IBM Tivoli Directory Server Problem Determination Guide* for a failed installation to clean up your system files and registry.

2. If you are uninstalling the embedded version of WebSphere Application Server - Express, you must stop the application server. (See “Stopping the application server” on page 150 for information.) Before you start to uninstall, close all windows to make sure that the `installpath/appsrv` (`installpath\appsrv` on Windows) directory is not in use.

After uninstalling the embedded version of WebSphere Application Server - Express, verify that the `installpath/appsrv` directory (`installpath\appsrv` on Windows) is removed. If it is not, you must remove it before you attempt to install again.

To remove IBM Tivoli Directory Server using the InstallShield GUI:

1. To start the InstallShield GUI uninstallation program:
  - On Windows systems:
    - a. In the Control Panel, click **Add/Remove Programs**.
    - b. Select **IBM Tivoli Directory Server 6.0**. Click **Change/Remove**.
  - On AIX, Linux, and Solaris systems: (The InstallShield GUI is not available on HP-UX systems.)
    - a. At a command prompt, go to the IBM Tivoli Directory Server `_uninst` directory.
      - On AIX and Solaris systems, this directory is `/opt/IBM/ldap/V6.0/_uninst`.

- On Linux systems, this directory is /opt/ibm/ldap/V6.0/\_uninst.
- b. Run the uninstall command:
  - ./uninstall
- 2. Select the language you want to use during the uninstallation procedure. Click **OK**.
- 3. On the Welcome window, click **Next**.
- 4. Select the features you want to uninstall. Click **Next**. Be sure that you do not select:
  - The client or the proxy server unless you also select the full server
  - The java client unless you also select the proxy server
  - DB2 unless you also select the full server

If you remove features that are required for other features, your system is left in an inconsistent state and unpredictable results will occur.

**Notes:**

- a. If you selected the embedded version of WebSphere Application Server - Express for removal, the following message is displayed:
  - Do you wish to cancel the embedded version of WebSphere Application Server - Express uninstallation so you can back up your files?
  
  - To continue uninstalling the embedded version of WebSphere Application Server - Express, click **No**.
- b. If features are deselected, and then you re-select all features, be sure to select the top check box (the **Product Uninstallation** check box) so that the InstallShield GUI removes everything associated with the product. The **Product Uninstallation** check box must always be selected unless you want to leave one or more features installed.
- 5. On the confirmation window, to uninstall the selected features, click **Next**.

**Note:** At the end of uninstallation on AIX systems only, the following message is displayed:

An unhandled error occurred -- Specify system property "is:debug" for more information.

The message is harmless and you can ignore it.

- 6. If you are asked if you want to restart your computer now or later, select the option you want. Click **Finish**.

## Uninstalling language packs using the InstallShield GUI

This section describes how to uninstall the IBM Tivoli Directory Server language packs using the InstallShield GUI.

**Notes:**

- 1. If you installed the language packs using the InstallShield GUI, use the InstallShield GUI to uninstall.

To remove language packs using the InstallShield GUI:

- 1. To start the InstallShield GUI uninstallation program:
  - On Windows systems:
    - a. In the Control Panel, click **Add/Remove Programs**.

- b. Select **IBM Tivoli Directory Server 6.0 Language Pack**. Click **Change/Remove**.
- On AIX, Linux, and Solaris systems: (The InstallShield GUI is not available on HP-UX systems.)
  - a. At a command prompt, go to the IBM Tivoli Directory Server language pack uninstallation directory.
    - On AIX and Solaris systems, this directory is `/opt/IBM/ldap/V6.0/LangPack/uninstall`
    - On Linux systems, this directory is `/opt/ibm/ldap/V6.0/LangPack/uninstall`
  - b. Run the uninstall command:
    - On AIX systems: `idslp_uninstall_aix.bin`
    - On xSeries Linux systems: `idslp_uninstall_linux.bin`
    - On zSeries Linux systems: `idslp_uninstall_linux390.bin`
    - On iSeries and pSeries Linux systems: `idslp_uninstall_linuxppc.bin`
    - On Solaris systems: `idslp_uninstall_solaris.bin`
- 2. On the Welcome window, click **Next**.
- 3. Select the language packs you want to uninstall. Click **Next**.
- 4. On the confirmation window, to uninstall the selected features, click **Next**.
- 5. Click **Finish** when the uninstallation is complete.

---

## Uninstalling using operating system utilities

Use one of the following procedures to uninstall IBM Tivoli Directory Server using operating system utilities for your operating system.

### Notes:

1. If you installed IBM Tivoli Directory Server using the InstallShield GUI, uninstall using the process in “Uninstalling IBM Tivoli Directory Server using the InstallShield GUI” on page 151.
2. If you inadvertently uninstall IBM Tivoli Directory Server using operating system utilities after installing using the InstallShield GUI, follow the process in “Uninstalling IBM Tivoli Directory Server using the InstallShield GUI” on page 151 and the instructions in the *IBM Tivoli Directory Server Problem Determination Guide* for a failed installation to clean up your system files and registry.
3. Uninstalling IBM Tivoli Directory Server does not remove any databases you created using IBM Tivoli Directory Server.

## AIX operating system

You can uninstall IBM Tivoli Directory Server from an AIX system using **SMIT** or **installp**.

### SMIT removal

To uninstall IBM Tivoli Directory Server using **SMIT**:

1. Log in as **root**.
2. Type `smit` at a command prompt and press Enter.
3. Select **Software Installation and Maintenance**.
4. Select **Software Maintenance and Utilities**.
5. Select **Remove Installed software**.

6. In the **Software Name** field, you can press F4 to display a list of installed software. (You can search for **idsldap** in the list to display only the IBM Tivoli Directory Server packages.)
7. Select the packages you want to remove, and press Enter.

### installp removal

To uninstall all of the IBM Tivoli Directory Server filesets using the **installp** command-line utility:

1. Log in as **root**.
2. Type the following at a command prompt:

```
installp -u idsldap
```

This removes only IBM Tivoli Directory Server filesets. It does not remove other components such as DB2.

## Linux operating system

The following procedures show how to remove IBM Tivoli Directory Server from an xSeries Linux computer. If you do not have the full server installed, remove only the packages that you do have installed, but be sure that you follow the order shown. See “Installing IBM Tivoli Directory Server” on page 77 for package names. Before removing IBM Tivoli Directory Server, ensure that the server is stopped and then issue the following commands.

1. Log in as **root**.
2. Uninstall the English messages:  

```
rpm -ev idsldap-msg60-en-6.0.0-0
```
3. Do one of the following, based on what you want to uninstall:
  - Uninstall the full server (and the client) by typing the following at a command prompt:  

```
rpm -ev idsldap-srv32bit60-6.0.0-0  
rpm -ev idsldap-srvproxy32bit60-6.0.0-0  
rpm -ev idsldap-cltjava60-6.0.0-0  
rpm -ev idsldap-clt32bit60-6.0.0-0  
rpm -ev idsldap-cltbase60-6.0.0-0
```
  - Uninstall the proxy server (and the client) by typing the following at a command prompt:  

```
rpm -ev idsldap-srvproxy32bit60-6.0.0-0  
rpm -ev idsldap-cltjava60-6.0.0-0  
rpm -ev idsldap-clt32bit60-6.0.0-0  
rpm -ev idsldap-cltbase60-6.0.0-0
```
  - Uninstall only the 32-bit client by typing the following at a command prompt: (If you have a server installed, you must uninstall it before you can uninstall the client.)  

```
rpm -ev idsldap-clt32bit60-6.0.0-0  
rpm -ev idsldap-cltbase60-6.0.0-0
```

**Note:** You can uninstall the 64-bit client by typing the following at a command prompt:

```
rpm -ev idsldap-clt64bit60-6.0.0-0  
rpm -ev idsldap-cltbase60-6.0.0-0
```

To uninstall only the Web Administration Tool, type the following at a command prompt:

```
rpm -ev idsldap-webadmin60-6.0.0-0
```



## Solaris operating system

You can uninstall IBM Tivoli Directory Server using the **admintool** utility or from a command line using **pkgrm**.

### AdminTool removal

To remove IBM Tivoli Directory Server using the **admintool** utility:

1. Log in as **root**.
2. Type the following at a command prompt:  
`admintool`

The **Users** window is displayed.

3. Click **Browse** → **Software**. The Software window is displayed.
4. Select the packages to delete from the displayed list.

```
IBM Directory Server - Base Client
IBM Directory Server - 32 bit Client
IBM Directory Server - 64 bit Client
IBM Directory Server - Java Client
IBM Directory Server - Proxy Server
IBM Directory Server - 32 bit Server
IBM Directory Server - Web Administration
IBM Directory Server - Messages U.S. English (en)
```

(Only the installed packages are shown.)

5. Click **Edit** → **Delete**. The AdminTool: Warning window is displayed.
6. Click **Delete**.

**Note:** When you remove client and server packages, the system might prompt 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 the removal of this package? Type y to continue. If you are removing a server package, you also see the prompt, Do you want to remove these as setuid and/or setgid files? Type y to continue.

7. After the package is removed, the Software window is displayed. When the removal is complete, type q to return to the command prompt.

### Command line removal using pkgrm

To see what IBM Tivoli Directory Server components are installed, type:

```
pkginfo | grep -i IDS1
```

The output displayed is similar to the following: (Only the installed packages are displayed.)

```
application IDS132c60      IBM Directory Server - 32 bit Client
application IDS132p60      IBM Directory Server - Proxy Server
application IDS132s60      IBM Directory Server - 32 bit Server
application IDS164c60      IBM Directory Server - 64 bit Client
application IDS1bc60       IBM Directory Server - Base Client
application IDS1jc60       IBM Directory Server - Java Client
application IDS1en60       IBM Directory Server - Messages U.S. English (en)
application IDS1web60      IBM Directory Server - Web Administration
```

Use **pkgrm** to remove the desired packages. For example:

- To uninstall the full server (with the client and English messages), type:

```
pkgrm IDS1en60 IDS132s60 IDS132p60 IDS1jc60 IDS132c60 IDS1bc60
```

- To uninstall the proxy server (with the client and English messages), type:  

```
pkgrm IDS1en60 IDS132p60 IDS1jc60 IDS132c60 IDS1bc60
```
- To uninstall only the 32-bit client, type: (You cannot uninstall only the client if you have a server installed.)  

```
pkgrm IDS132c60 IDS1bc60
```
- To uninstall the 64-bit client, type:  

```
pkgrm IDS164c60 IDS1bc60
```
- To uninstall the Web Administration Tool package, type:  

```
pkgrm IDS1web60
```

Remove the packages in the reverse order of the installation sequence. (The order in which you remove the Web Administration Tool is not important.)

## HP-UX

To remove IBM Tivoli Directory Server, complete the following steps:

1. Type `swremove` at a command prompt.
2. On the list that is displayed, select the IBM Tivoli Directory Server packages you want to remove.
3. Click **Actions** → **Mark For Remove**.
4. Click **Actions** → **Remove**.
5. Click **OK** when analysis is complete.
6. When removal is complete, click **Done**.
7. Click **File** → **Exit**.

**Note:** The subdirectories of `/opt/IBM/ldap/V6.0/` and `/var/idsldap/V6.0/` might not be removed when you uninstall IBM Tivoli Directory Server. You can use the `rm -rf` command to remove these directories.

---

## Appendix A. Directory structure of unzipped and untarred files

The following information shows the directory structure and, at a high level, the contents of the zip and tar files for IBM Tivoli Directory Server 6.0 for each operating system.

---

### The top level directory

The top level directory in this appendix will be designated as *topdir*. This directory is one of the following:

**For .iso (CD image) files**

*top\_dir* is \ (for Windows) or / (for AIX, Linux, Solaris, and HP-UX)

**For .zip files for InstallShield GUI installation**

*top\_dir* is itdsV60\

**For .tar files for InstallShield GUI installation**

*top\_dir* is itdsV60ismp/

**For .tar files for operating system utility installation**

*top\_dir* is itdsV60/

---

### Server InstallShield GUI installation files

The file names and contents of the Installshield GUI files for the server packages are as follows:

**Windows platforms**

The file names for the IBM Tivoli Directory Server 6.0 for Windows server packages are:

- CD image file: itds60-win-ia32-ismp.iso
- .zip file: itds60-win-ia32-ismp.zip

After you create the CD or unzip the .zip file, the directory structure is as follows:

*top\_dir* (Top level directory)

- appsrv\ (the embedded version of WebSphere Application Server - Express, version 5.1.1)
- db2\ (DB2 v8 Fix Pack 8 refresh)
- doc\ (Contains pointer to online books)
- gskit\ (GSKit 7.0.3.3)
- itds\ (IBM Tivoli Directory Server v6.0 and setup.exe command)
- itdsLangpack\ (IBM Tivoli Directory Server language packs)
- license\ (Licenses for IBM Tivoli Directory Server and other provided products)
- nas\ (NAS v1.4 client for Windows)
- tools\ (Tools including **migbkup** and **idswmigr**)

**AIX platforms**

The file names for the IBM Tivoli Directory Server 6.0 for AIX InstallShield GUI server packages are:

- CD image file: itds60-aix-ppc-ismp.iso
- .tar file: itds60-aix-ppc-ismp.tar

After you create the CD or untar the .tar file, the directory structure is as follows:

```

top_dir  (Top level directory)
  --appsrv/  (the embedded version of WebSphere Application
              Server - Express, version 5.1.1)
  --doc/    (Contains pointer to online books)
  --itds/   (IBM Tivoli Directory Server v6.0,
              DB2 v8 Fix Pack 8 refresh, GSKit 7.0.3.3)
  --itdsLangpack/ (IBM Tivoli Directory Server language packs)
  --license/ (Licenses for IBM Tivoli Directory Server and
              other provided products)
  --setup  (Setup command)
  --tools/ (Tools including migbkup and idswmigr)

```

**Note:** The AIX file includes a 32-bit client in addition to the 64-bit client that is installed through the InstallShield GUI installation program.

### Linux platforms

The file names for the IBM Tivoli Directory Server 6.0 for xSeries, zSeries, and iSeries and pSeries Linux InstallShield GUI server packages are:

#### xSeries Linux

- CD image: itds60-lin-ia32-ismp.iso
- .tar file: itds60-lin-ia32-ismp.tar

#### zSeries Linux

- CD image: itds60-lin-s390-ismp.iso
- .tar file: itds60-lin-s390-ismp.tar

#### iSeries and pSeries Linux

- CD image: itds60-lin-ppc-ismp.iso
- .tar file: itds60-lin-ppc-ismp.tar

After you create the CD or untar the .tar file, the directory structure is as follows:

```

top_dir  (Top level directory)
  --appsrv/  (the embedded version of WebSphere Application
              Server - Express, version 5.1.1)
  --doc/    (Contains pointer to online books)
  --itds/   (IBM Tivoli Directory Server v6.0,
              DB2 v8 Fix Pack 8 refresh, GSKit 7.0.3.3)
  --itdsLangpack/ (IBM Tivoli Directory Server language packs)
  --license/ (Licenses for IBM Tivoli Directory Server and
              other provided products)
  --setup  (Setup command)
  --tools/ (Tools including migbkup and idswmigr)n

```

#### Notes:

1. The installation command for installing language packs is different for different versions of Linux.

2. The iSeries and pSeries file includes a 64-bit client in addition to the 32-bit client that is installed through the InstallShield GUI installation program.

### Solaris platforms

The file names for the IBM Tivoli Directory Server 6.0 for Solaris InstallShield GUI server packages are:

- CD image file: itds60-sol-sparc-ismp.iso
- .tar file: itds60-sol-sparc-ismp.tar

After you create the CD or untar the .tar file, the directory structure is as follows:

```
top_dir  (Top level directory)
  —appsrv/  (the embedded version of WebSphere Application
             Server - Express, version 5.1.1)
  —doc/    (Contains pointer to online books)
  —itds/   (IBM Tivoli Directory Server v6.0,
             DB2 v8 Fix Pack 8 refresh, GSKit 7.0.3.3)
  —itdsLangpack/ (IBM Tivoli Directory Server language packs)
  —license/ (Licenses for IBM Tivoli Directory Server and
             other provided products)
  —tools/  (Tools including migbkup and idswmigr)
```

**Note:** The Solaris file includes a 64-bit client in addition to the 32-bit client that is installed through the InstallShield GUI installation program.

**Note:** There is no InstallShield GUI installation for HP-UX systems.

---

## Server operating system utility installation files

Operating system utility installation files are provided for AIX, Linux, Solaris, and HP-UX.

For CD image files, DB2 and GSKit are provided on the CD image (for Solaris, however, DB2 is on a separate CD image).

For the .tar files, there are three separate files for each operating system: one for IBM Tivoli Directory Server, one for DB2, and one for GSKit.

### AIX platforms

The file names and contents for the IBM Tivoli Directory Server 6.0 for AIX operating system utility server packages are:

- CD image file: itds60-aix-ppc-native.iso

After you create the CD, the directory structure is as follows:

```
/  (Top level directory)
  —appsrv/  (the embedded version of WebSphere Application
             Server - Express, version 5.1.1)
  —db2/    (DB2 v8 Fix Pack 8 refresh)
  —doc/    (Contains pointer to online books)
  —gskit/  (GSKit 7.0.3.3)
  —itds/   (IBM Tivoli Directory Server v6.0,
             DB2 v8 Fix Pack 8 refresh, GSKit 7.0.3.3)
  —itdsLangpack/ (IBM Tivoli Directory Server language packs)
  —license/ (Licenses for IBM Tivoli Directory Server and
```

- other provided products)
  - tools/ (Tools including **migbkup** and **idswmigr**)
- IBM Tivoli Directory Server .tar file: itds60-aix-ppc-native.tar  
After you untar this file, the directory structure is as follows:
  - itdsV60/ (Top level directory)
    - appsrv/ (the embedded version of WebSphere Application Server - Express, version 5.1.1)
    - doc/ (Contains pointer to online books)
    - itds/ (IBM Tivoli Directory Server v6.0)
    - itdsLangpack/ (IBM Tivoli Directory Server language packs)
    - license/ (Licenses for IBM Tivoli Directory Server and other provided products)
    - tools/ (Tools including **migbkup** and **idswmigr**)
- DB2 v8 Fix Pack 8 refresh .tar file: db2v8fp8refresh-ese-aix-ppc.tar  
After you untar this file, the directory structure is as follows:
  - db2v8fp8refresh-ese-aix-ppc/ (Top level directory)
    - db2/ (DB2 v8 Fix Pack 8 refresh, condensed for IBM Tivoli Directory Server)
    - db2\_deinstall
    - db2\_install
    - doc/
- GSKit 7.0.3.3 .tar file: gskit7c-aix-ppc.tar  
After you untar this file, the directory structure is as follows:
  - gskit7c-aix-ppc/ (GSKit 7.0.3.3)

### Linux platforms

The file names and contents for the IBM Tivoli Directory Server 6.0 for Linux operating system utility server packages are:

- CD image files:
    - For xSeries Linux: itds60-lin-ia32-native.iso
    - For zSeries Linux: itds60-lin-s390-native.iso
    - For iSeries and pSeries Linux: itds60-lin-ppc-native.iso
- After you untar any of these files, the directory structure is as follows:
- / (Top level directory)
    - appsrv/ (the embedded version of WebSphere Application Server - Express, version 5.1.1)
    - db2/ (DB2 v8 Fix Pack 8 refresh)
    - doc/ (Contains pointer to online books)
    - gskit/ (GSKit 7.0.3.3)
    - itds/ (IBM Tivoli Directory Server v6.0)
    - itdsLangpack/ (IBM Tivoli Directory Server language packs)
    - license/ (Licenses for IBM Tivoli Directory Server and other provided products)
    - tools/ (Tools including **migbkup** and **idswmigr**)
  - IBM Tivoli Directory Server .tar files:
    - For xSeries Linux: itds60-lin-ia32-native.tar
    - For zSeries Linux: itds60-lin-s390-native.tar
    - For iSeries and pSeries Linux: itds60-lin-ppc-native.tar

After you untar any of these files, the directory structure is as follows:

- itdsV60/ (Top level directory)
  - appsrv/ (the embedded version of WebSphere Application Server - Express, version 5.1.1)
  - doc/ (Contains pointer to online books)
  - itds/ (IBM Tivoli Directory Server v6.0)
  - itdsLangpack/ (IBM Tivoli Directory Server language packs)
  - license/ (Licenses for IBM Tivoli Directory Server and other provided products)
  - tools/ (Tools including **migbkup** and **idswmigr**)

- DB2 .tar files:

- For xSeries Linux: db2v8fp8refresh-ese-lin-ia32.tar

After you untar this file, the directory structure is as follows:

- db2v8fp8refresh-ese-lin-ia32/ (Top level directory)
  - db2/ (DB2 v8 Fix Pack 8 refresh, condensed for IBM Tivoli Directory Server)
  - db2\_deinstall
  - db2\_install
  - doc/

- For zSeries Linux: db2v8fp8refresh-ese-lin-s390.tar

After you untar this file, the directory structure is as follows:

- db2v8fp8refresh-ese-lin-s390/ (Top level directory)
  - db2/ (DB2 v8 Fix Pack 8 refresh, condensed for IBM Tivoli Directory Server)
  - db2\_deinstall
  - db2\_install
  - doc/

- For iSeries and pSeries Linux: db2v8fp8refresh-ese-lin-ppc.tar

After you untar this file, the directory structure is as follows:

- db2v8fp8refresh-ese-lin-ppc/ (Top level directory)
  - db2/ (DB2 v8 Fix Pack 8 refresh, condensed for IBM Tivoli Directory Server)
  - db2\_deinstall
  - db2\_install
  - doc/

- GSKit 7.0.3.3 .tar file:

- For xSeries Linux: gskit7c-lin-ia32.tar

After you untar this file, the directory structure is as follows:

- gskit7c-lin-ia32/ (GSKit 7.0.3.3)

- For zSeries Linux: gskit7c-lin-s390.tar

After you untar this file, the directory structure is as follows:

- gskit7c-lin-s390/ (GSKit 7.0.3.3)

- For Linux s390x (64-bit client): gskit7c-lin-s390x.tar

After you untar this file, the directory structure is as follows:

- gskit7c-lin-s390x/ (GSKit 7.0.3.3)

- For iSeries and pSeriesLinux: gskit7c-lin-ppc.tar  
After you untar this file, the directory structure is as follows:

gskit7c-lin-ppc/ (GSKit 7.0.3.3)

### Solaris platforms

The file names and contents for the IBM Tivoli Directory Server 6.0 for Solaris operating system utility server packages are:

- IBM Tivoli Directory Server CD image file: itds60-sol-sparc-native.iso  
After you create the CD, the directory structure is as follows:

```

/ (Top level directory)
--appsrv/ (the embedded version of WebSphere Application
           Server - Express, version 5.1.1)
--doc/ (Contains pointer to online books)
--gskit/ (GSKit 7.0.3.3)
--itds/ (IBM Tivoli Directory Server v6.0,
         DB2 v8 Fix Pack 8 refresh, GSKit 7.0.3.3)
--itdsLangpack/ (IBM Tivoli Directory Server language packs)
--license/ (Licenses for IBM Tivoli Directory Server and
            other provided products)
--tools/ (Tools including migbkup and idswmigr)

```

- DB2 CD image file: db2v8fp8refresh-ese-sol-sparc.iso

On Solaris only, DB2 is in a separate .iso file.

After you create the CD, the directory structure is as follows:

```

/ (Top level directory)
--db2/ (DB2 v8 Fix Pack 8 refresh,
        condensed for IBM Tivoli Directory Server)
--db2_deinstall
--db2_install
--doc/

```

- IBM Tivoli Directory Server .tar file: itds60-sol-sparc-native.tar

After you untar this file, the directory structure is as follows:

```

itdsV60/ (Top level directory)
--appsrv/ (the embedded version of WebSphere Application
           Server - Express, version 5.1.1)
--doc/ (Contains pointer to online books)
--itds/ (IBM Tivoli Directory Server v6.0)
--itdsLangpack/ (IBM Tivoli Directory Server language packs)
--license/ (Licenses for IBM Tivoli Directory Server and
            other provided products)
--tools/ (Tools including migbkup and idswmigr)

```

- DB2 v8 Fix Pack 8 refresh .tar file: db2v8fp8refresh-ese-sol-sparc.tar

After you untar this file, the directory structure is as follows:

```

db2v8fp8refresh-ese-sol-sparc/ (Top level directory)
--db2/ (DB2 v8 Fix Pack 8 refresh,
        condensed for IBM Tivoli Directory Server)
--db2_deinstall
--db2_install
--doc/

```

- GSKit 7.0.3.3 .tar file: gskit7c-sol-sparc.tar



After you untar this file, the directory structure is as follows:

gskit7c-sol-sparc/ (GSKit 7.0.3.3)

### HP-UX platforms

The file names and contents for the IBM Tivoli Directory Server 6.0 for HP-UX operating system utility server packages are:

- CD image file: itds60-hpux-parisc-native.iso

After you create the CD, the directory structure is as follows:

```
/ (Top level directory)
—appsrv/ (the embedded version of WebSphere Application
          Server - Express, version 5.1.1)
—db2 (DB2 8 Fix Pack 2 refresh)
—doc/ (Contains pointer to online books)
—gskit/ (GSKit 7.0.3.3)
—itds/ (IBM Tivoli Directory Server v6.0)
—itdsLangpack/ (IBM Tivoli Directory Server language packs)
—java (Java 1.4.2 for HP-UX)
—license/ (Licenses for IBM Tivoli Directory Server and
           other provided products)
—tools/ (Tools including migbkup and idswmigr)
```

- IBM Tivoli Directory Server .tar file: itds60-hpux-parisc-native.tar

After you untar this file, the directory structure is as follows:

```
itdsV60/ (Top level directory)
—appsrv/ (the embedded version of WebSphere Application
          Server - Express, version 5.1.1)
—doc/ (Contains pointer to online books)
—itds/ (IBM Tivoli Directory Server v6.0)
—itdsLangpack/ (IBM Tivoli Directory Server language packs)
—licenses/ (Licenses for IBM Tivoli Directory Server and
            other provided products)
—tools/ (Tools including migbkup and idswmigr)
```

- DB2 v8 Fix Pack 2 refresh .tar file: db2v8fp2refresh-ese-hpux-parisc.tar

After you untar this file, the directory structure is as follows:

```
db2v8fp2refresh-ese-hpux-parisc/ (Top level directory)
—db2/ (DB2 v8 Fix Pack 2 refresh,
       condensed for IBM Tivoli Directory Server)
—db2_deinstall
—db2_install
—doc/
```

- GSKit 7.0.3.3 .tar file: gskit7c-hpux-parisc.tar

After you untar this file, the directory structure is as follows:

gskit7c-hpux-parisc/ (GSKit 7.0.3.3)

---

## Client InstallShield GUI installation files

For the client-only package, there are only .zip and .tar files; no CD image files are provided. The file names and contents of the InstallShield GUI files for the client only are as follows:

### Windows platforms

The file name for the IBM Tivoli Directory Server 6.0 for Windows client-only package is itds60-client-win-ia32-ismp.zip

After you unzip the file, the directory structure is as follows:

```
itdsV60ismpClient\ (Top level directory)
  —doc\ (Contains pointer to online books)
  —gskit\ (GSKit 7.0.3.3)
  —itds\ (IBM Tivoli Directory Server v6.0 client)
  —license\ (Licenses for IBM Tivoli Directory Server and
             other provided products)
  —nas\ (NAS v1.4 client for Windows)
```

### AIX platforms

The file name for the IBM Tivoli Directory Server 6.0 for AIX client-only package for InstallShield GUI installation is itds60-client-aix-ppc-ismp.tar

After you untar the file, the directory structure is as follows:

```
itdsV60ismpClient/ (Top level directory)
  —doc/ (Contains pointer to online books)
  —itdsclient/ (IBM Tivoli Directory Server v6.0 client)
  —license/ (Licenses for IBM Tivoli Directory Server and
             other provided products)
  —setup (Setup command)
```

**Note:** The AIX file includes a 32-bit client in addition to the 64-bit client that is installed through the InstallShield GUI installation program.

### Linux platforms

The file names and contents for the IBM Tivoli Directory Server 6.0 for Linux client-only packages for InstallShield GUI installation are:

- For xSeries Linux: itds60-client-lin-ia32-ismp.tar
- For zSeries Linux: itds60-client-lin-s390-ismp.tar
- For iSeries and pSeries Linux: itds60-client-lin-ppc-ismp.tar

After you untar these files, the directory structure is as follows:

```
itdsV60ismpClient/ (Top level directory)
  —doc/ (Contains pointer to online books)
  —itds/ (IBM Tivoli Directory Server v6.0 client)
  —license/ (Licenses for IBM Tivoli Directory Server and
             other provided products)
  —setup (Setup command)
```

**Note:** The iSeries and pSeries file includes a 64-bit client in addition to the 32-bit client that is installed through the InstallShield GUI installation program.

### Solaris platforms

The file name for the IBM Tivoli Directory Server 6.0 for AIX client-only package for InstallShield GUI installation is itds60-client-sol-sparc-ismp.tar

After you untar the file, the directory structure is as follows:

```
itdsV60ismpClient/ (Top level directory)
  —doc/ (Contains pointer to online books)
  —itds/ (IBM Tivoli Directory Server v6.0 client)
```

- license/ (Licenses for IBM Tivoli Directory Server and other provided products)
- setup (Setup command)

**Note:** The Solaris file includes a 64-bit client in addition to the 32-bit client that is installed through the InstallShield GUI installation program.

There is no InstallShield GUI installation for HP-UX systems.

---

## Client operating system utility installation files

Operating system utility installation files for the client are provided for AIX, Linux, Solaris, and HP-UX.

### AIX platforms

The file name for the client-only package for operating system utility installation for AIX is `itds60-client-aix-ppc-native.tar`

After you untar the file, the directory structure is as follows:

- itdsV60Client/ (Top level directory)
  - doc/ (Contains pointer to online books)
  - gskit/ (GSKit 7.0.3.3)
  - itdsClient/ (IBM Tivoli Directory Server v6.0 client)
  - license/ (Licenses for IBM Tivoli Directory Server and other provided products)

### Linux platforms

The file names for the client-only package for operating system utility installation for Linux are:

- For xSeries Linux: `itds60-client-lin-ia32-native.tar`
- For zSeries Linux: `itds60-client-lin-s390-native.tar`
- For iSeries and pSeries Linux: `itds60-client-lin-ppc-native.tar`

After you untar any of these files, the directory structure is as follows:

- itdsV60Client/ (Top level directory)
  - doc/ (Contains pointer to online books)
  - gskit/ (GSKit 7.0.3.3)
  - itdsClient/ (IBM Tivoli Directory Server v6.0 client)
  - license/ (Licenses for IBM Tivoli Directory Server and other provided products)

### Solaris platforms

The file name for the client-only package for operating system utility installation for Solaris is `itds60-client-sol-sparc-native.tar`

After you untar the file, the directory structure is as follows:

- itdsV60Client/ (Top level directory)
  - doc/ (Contains pointer to online books)
  - gskit/ (GSKit 7.0.3.3)
  - itdsClient/ (IBM Tivoli Directory Server v6.0 client)
  - license/ (Licenses for IBM Tivoli Directory Server and other provided products)

### HP-UX platforms

The file name for the client-only package for operating system utility installation for HP-UX is `itds60-client-hpux-parisc-native.tar`

After you untar the file, the directory structure is as follows:

- itdsV60Client/ (Top level directory)
  - doc/ (Contains pointer to online books)
  - gskit/ (GSKit 7.0.3.3)
  - itdsClient/ (IBM Tivoli Directory Server v6.0 client)
  - license/ (Licenses for IBM Tivoli Directory Server and other provided products)

---

## Appendix B. Disk space requirements for installable features

IBM Tivoli Directory Server requires the following amounts of disk space for each installable feature. Information is given for each supported operating system.

---

### Windows disk space requirements

On Windows systems, the following amounts of disk space are required:

*Table 4. Sizes of installable features (in MB) on Windows systems*

| Installable feature   | Installed size |
|---|----------------|
| Client SDK  | 16 MB          |
| Java client   | 50 MB          |
| Web Administration Tool   | 18 MB          |
| Proxy server (Be sure to add the sizes for the client SDK and Java client.)               | 27 MB          |
| Full server (Be sure to add the sizes for the proxy server, client SDK, and Java client.) | 5 MB           |
| embedded version of WebSphere Application Server - Express                                | 148 MB         |
| DB2   | 377 MB         |
| GSKit   | 10 MB          |

---

### AIX disk space requirements

On AIX systems, the following amounts of disk space are required:

*Table 5. Sizes of installable features (in MB) on AIX systems*

| Installable feature   | Installed size |
|---|----------------|
| Client SDK  | 10 MB          |
| Java client   | 52 MB          |
| Web Administration Tool   | 34 MB          |
| Proxy server (Be sure to add the sizes for the client SDK and Java client.)               | 40 MB          |
| Full server (Be sure to add the sizes for the proxy server, client SDK, and Java client.) | 7 MB           |
| embedded version of WebSphere Application Server - Express                                | 152 MB         |
| DB2   | 450 MB         |
| GSKit   | 31 MB          |

---

## Linux disk space requirements

On Linux systems, the following amounts of disk space are required:

*Table 6. Sizes of installable features (in MB) on Linux systems*

| Installable feature   | Installed size |
|---|----------------|
| Client SDK  | 7 MB           |
| Java client   | 62 MB          |
| Web Administration Tool   | 18 MB          |
| Proxy server (Be sure to add the sizes for the client SDK and Java client.)               | 28 MB          |
| Full server (Be sure to add the sizes for the proxy server, client SDK, and Java client.) | 5 MB           |
| embedded version of WebSphere Application Server - Express                                | 168 MB         |
| DB2 (xSeries Linux)   | 365 MB         |
| DB2 (zSeries Linux)   | 425 MB         |
| DB2 (iSeries and pSeries Linux)   | 450 MB         |
| GSKit   | 16 MB          |

---

## Solaris disk space requirements

On Solaris systems, the following amounts of disk space are required:

*Table 7. Sizes of installable features (in MB) on Solaris systems*

| Installable feature   | Installed size |
|---|----------------|
| Client SDK  | 16 MB          |
| Java client   | 99 MB          |
| Web Administration Tool   | 18 MB          |
| Proxy server (Be sure to add the sizes for the client SDK and Java client.)               | 54 MB          |
| Full server (Be sure to add the sizes for the proxy server, client SDK, and Java client.) | 5 MB           |
| embedded version of WebSphere Application Server - Express                                | 205 MB         |
| DB2   | 595 MB         |
| GSKit   | 16 MB          |

---

## HP-UX disk space requirements

On HP-UX systems, the following amounts of disk space are required:

*Table 8. Sizes of installable features (in MB) on HP-UX systems*

| Installable feature                             | Installed size |
|---|----------------|
| Client SDK                                      | 8 MB           |
| Java client (includes untarring Java .tar file) | 98 MB          |
| Web Administration Tool                         | 18 MB          |

Table 8. Sizes of installable features (in MB) on HP-UX systems (continued)

| Installable feature   | Installed size |
|---|----------------|
| Proxy server (Be sure to add the sizes for the client SDK and Java client.)               | 39 MB          |
| Full server (Be sure to add the sizes for the proxy server, client SDK, and Java client.) | 8 MB           |
| embedded version of WebSphere Application Server - Express                                | 207 MB         |
| DB2   | 438 MB         |
| GSKit   | 22 MB          |





---

## Appendix C. Database configuration planning

Before configuring and populating your database, determine:

### What type of data you are going to store in the directory

Decide what sort of schema you need to support the type of data you want to keep in your directory. A standard set of attribute-type definitions and object-class definitions is included with the directory server. Before you begin adding entries to the directory, you might want to add new attribute-type and object-class definitions that are customized to your data.

**Note:** You can make schema additions after the directory is already populated with data, but schema changes might require you to unload and reload your data.

### Which code page you are going to use

Decide whether to create your database using the local code page or using the Universal Character Set (UTF-8). Selecting the local code page enables IBM Tivoli Directory Server applications and users to get search results as expected for the collation sequence of the native language. Using UTF-8 enables the storing of any UTF-8 character data in the directory. IBM Tivoli Directory Server clients running anywhere in the world (in any UTF-8 supported language) can access and search the directory. In many cases, however, the client might have limited ability to properly display the results retrieved from the directory in a particular language or character set. See Appendix N, "UTF-8 support," on page 197 for more information.

**Note:** If you want to use language tags, the database must be a UTF-8 database.

### How you want to structure your directory data

An IBM Directory is stored in a hierarchical tree structure. The names of entries in the directory are based on their relative position within the tree structure. It is important to define some logical organization to the directory. A logical organization makes it easier for clients to determine which branch of the tree contains the information they are trying to locate. If you are storing data about the people in an organization, it is easy to map the structure of the organization onto the structure of the directory. If you are storing descriptions of applications, machine configuration data, or customer data, it might take more planning to decide how to structure your directory.

### Your data security requirements

See the Secure Sockets Layer information in the *IBM Tivoli Directory Server Version 6.0 Administration Guide* for information about how your data is secured.

### How you want to allocate access permissions

See the access control lists information in the *IBM Tivoli Directory Server version 6.0 Administration Guide* for information about using access permissions.



---

## Appendix D. Setting up users and groups: directory server instance owner, database instance owner, and database owner

Before you create an instance, you must create a user ID on the operating system for the owner of the directory server instance. For a full server, you must also create user IDs on the operating system for the owners of the database instance and the database. This section discusses the requirements for the IDs.

Use the following information to understand these roles before you create the user ID or IDs. You can use the same user ID for all three roles; if you do this, the directory server instance, the database instance, and the database owner all have the same name.

The roles are defined as follows:

### Directory server instance owner

You must have a user ID for the owner of the directory server instance. The user ID for the directory server instance owner is also the name of the directory server instance. This user has the authority to manage the directory server instance.

On Windows systems, any member of the Administrators group also has the authority to manage the directory server instance.

On AIX, Linux, Solaris, and HP-UX systems, the primary group of the directory server instance owner also has the authority to manage the directory server instance.

**Note:** On AIX, Linux, Solaris, and HP-UX systems, these names are case-sensitive. You must always specify the directory server instance name and owner exactly as the user ID is specified. For example, JoeSmith and joesmith are different names.

### Database instance owner

This user ID owns the database instance that is configured to be used by the directory server instance. The database instance name and the database instance owner name are the same. This user manages the database instance. The directory server instance owner can also manage the database instance. By default, this user ID is the same as the directory server instance owner ID.

### Database owner

This user ID owns the database that is used by the directory server instance to store the directory data. The database resides in the database instance owned by the database instance owner. The directory server instance uses this user ID and its password to connect to the database.

---

## Naming rules

The requirements in this section apply to the following:

- The directory server instance name (the user ID that owns the directory server instance).

- The database instance name (the user ID that owns the database instance). This is usually the same as the directory server instance name .
- On AIX, Linux, Solaris, and HP-UX, the primary groups of the directory server instance owner user ID and the database instance owner user ID.

These user and group IDs:

- Can be no longer than 8 characters
- Cannot be any of the following:
  - USERS
  - ADMINS
  - GUESTS
  - PUBLIC
  - LOCAL
- Cannot begin with any of the following:
  - IBM
  - SQL
  - SYS
- Cannot include accented characters
- Can include the following characters:
  - A through Z
  - a through z
  - 0 through 9
- Must begin with one of the following characters:
  - A through Z
  - a through z

---

## Additional restrictions for users and groups

In addition to the naming rules, be sure that the following requirements are met:

- On Windows systems,
  - The directory server instance owner and the database instance owner must be members of the Administrators group.
  - The database instance owner must have the locale set to the correct locale for the language in which you want server messages to be displayed. If necessary, log in as the user and change the locale to the correct one.
- On AIX, Linux, Solaris, and HP-UX systems:
  - The root ID must be a member of the primary group of the directory server instance owner and the database instance owner.
  - The root ID must be a member of the idslldap group.
  - The directory server instance owner and the database instance owner must be members of the idslldap group.
  - The directory server instance owner and the database instance owner must have home directories.
  - The specific permissions for the home directory of the directory server instance owner must be as follows:
    - The user ownership is the directory server instance owner.
    - The group ownership is the directory server instance owner's primary group.

- The directory server instance owner and its primary group must have read, write, and execute permissions to the home directory.
- The directory server instance owner and its primary group must have read, write, and execute access to the location where the database will be created.
- If the directory server instance owner and the database instance owner for a given directory server instance are different users, the directory server instance owner must be a member of the database instance owner's primary group.
- The database instance owner and the database owner for a given directory server instance must have the same primary group.
- For best results, the login shell of the directory server instance owner, the database instance owner, and the database owner should be the Korn shell script (/usr/bin/ksh).
- The password of the directory server instance owner, the database instance owner, and the database owner 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 customary, to specify the home directory of the database instance owner as the database location. However, if you specify some other location, the database instance owner'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 database instance owner even though the database itself is elsewhere. If you do not have enough space in the home directory, you can either create enough space or change the database instance owner's home directory.

---

## Creating instance owners: examples

To create instance owners and place them in an appropriate group, you can use the following information to create users and groups that could be used to create a directory server instance.

**Note:** Numeric IDs used for groups and users are examples only. Look in the /etc/group and /etc/password files to select appropriate numeric IDs.

### Windows systems

On Windows operating systems, use the graphical user interface to create users and groups. See the documentation for your operating system for instructions.

If you prefer to use the command line, use the following information.

To create user **db2inst1** and add this user ID to the Administrators group, type the following at a command prompt:

```
net user db2inst1 password /add
net localgroup Administrators db2inst1 /add
net localgroup Administrators
```

where *password* is the password for user **db2inst1**.

### AIX systems

To create a group called **db2iadm1**:

```
mkgroup db2iadm1
```

To create user ID **db2inst1**, which is a member of groups **db2iadm1** and **idsldap**:

```
mkuser pgrp=db2iadm1 groups=db2iadm1,idsldap home=/home/db2inst1 db2inst1
```

To set the password for user **db2inst1**:

```
passwd db2inst1
```

To modify the root user ID so that root is a member of the group **db2iadm1**:

```
/usr/bin/chgrpmem -m + root db2iadm1
```

### Linux systems

To create a group called **db2iadm1**:

```
groupadd db2iadm1
```

To create user ID **db2inst1**, which is a member of groups **db2iadm1** and **idsldap**:

```
useradd -g db2iadm1 -G idsldap -d /home/db2inst1 -m db2inst1
```

To set the password for user **db2inst1**:

```
passwd db2inst1
```

To modify the root user ID so that root is a member of the group **db2iadm1**:

```
usermod -G db2iadm1,rootgroups root
```

where *rootgroups* can be obtained by using the command: `groups root`

### Solaris systems

To create a group called **db2iadm1**:

```
groupadd db2iadm1
```

To create user ID **db2inst1**, which is a member of groups **db2iadm1** and **idsldap**:

```
useradd -g db2iadm1 -G idsldap -d /export/home/db2inst1 -m db2inst1
```

To set the password for user **db2inst1**:

```
passwd db2inst1
```

To modify the root user ID so that root is a member of the group **db2iadm1**, use the AdminTool or another appropriate tool.

### HP-UX systems

To create a group called **db2iadm1**:

```
groupadd db2iadm1
```

To create user ID **db2inst1**, which is a member of groups **db2iadm1** and **idsldap**:

```
useradd -g db2iadm1 -G idsldap -d /home/db2inst1 -m db2inst1
```

To set the password for user **db2inst1**:

```
passwd db2inst1
```

To modify the root user ID so that root is a member of the group **db2iadm1**, use the **sam** tool or another appropriate tool.

---

## Appendix E. Synchronizing two-way cryptography between server instances

If you want to use replication, use a distributed directory, or import and export LDIF data between server instances, you must cryptographically synchronize the server instances to obtain the best performance.

If you already have a server instance, and you have another server instance that you want to cryptographically synchronize with the first server instance, use the following procedure *before* you do any of the following:

- Start the second server instance
- Run the **idsbulkload** command from the second server instance
- Run the **idsldif2db** command from the second server instance

To cryptographically synchronize two server instances, assuming that you have already created the first server instance:

1. Create the second server instance, but do not start the server instance, run the **idsbulkload** command, or run the **idsldif2db** command on the second server instance.
2. Use the **idsgendirksf** utility to recreate the `ibmslapddir.ksf` file (the key stash file) from the first server instance. This file is used to replace the second server instance's original `ibmslapddir.ksf` file. For information about the **idsgendirksf** utility, see the *IBM Tivoli Directory Server Version 6.0 Administration Guide*. The file is in the `idsslapd-instance_name\etc` directory on Windows systems, or in the `idsslapd-instance_name/etc` directory on AIX, Linux, Solaris, and HP-UX systems. (*instance\_name* is the name of the directory server instance).
3. Start the second server instance, run the **idsbulkload** command, or run the **idsldif2db** command on the second server instance.

The server instances are now cryptographically synchronized, and AES-encrypted data will load correctly.

Although the procedure discusses two server instances, you might need a group of server instances that are cryptographically synchronized.

**Note:** When importing LDIF data, if the LDIF import file is not cryptographically synchronized with the server instance that is importing the LDIF data, any AES-encrypted entries in the LDIF import file will not be imported.





---

## Appendix F. Directory server instances

A directory server instance consists of all non-executable files that are required for a directory server and its corresponding administration daemon to run on a computer. The administration daemon (idsdiradm) enables remote management of the directory server instance. When it is running, the administration daemon supports starting, stopping, restarting, and monitoring the status of the directory server instance.

Directory server instance files include:

- The `ibmslapd.conf` file (the configuration file)
- Schema files
- Log files
- Key stash files
- Temporary status files

The files for a directory server instance are stored in a directory named `idsslapd-instance_name`, where *instance\_name* is the name of the directory server instance.

**Note:** The SSL key database and the key tab files are not directly part of a directory server instance. A default SSL key database attribute value exists in the `ibmslapd.conf` file of each directory server instance. However, it is the responsibility of the directory server instance owner to create the SSL key database and the key tab as needed and to add the information into the `ibmslapd.conf` file of the directory server instance. These files can be shared by multiple directory server instances on the computer and should be stored in a secure location on the system that is independent of a given directory server instance.

---

### Directory server instance content on Windows systems

On Windows systems, the `idsslapd-instance_name` directory is in the root directory of a drive that you specify during instance creation.

The directory server instance owner user ID and by all members of the Administrators group have read and write access to files in the `idsslapd-instance_name` directory.

The `idsslapd-instance_name` directory on Windows systems contains the following subdirectories and files:

- `etc`
- `tmp`
- `logs`
- `idsprofile.bat`
- `userprofile.bat`

The `idsprofile.bat` file is used to set the environment for the directory server instance. The `userprofile.bat` file is used to customize the environment. The

idsprofile.bat file invokes the userprofile.bat file after setting the environment. If you want to customize the environment, be sure to change the userprofile.bat file and not the idsprofile.bat file.

---

## Directory server instance content on AIX, Linux, Solaris, and HP-UX systems

On AIX, Linux, Solaris, and HP-UX systems, the `idsslapd-instance_name` directory is, by default, in the directory server instance owner's home directory, but you can specify a different location during instance creation.

For AIX, Linux, Solaris, and HP-UX systems, the `idsslapd-instance_name` directory contains the following subdirectories and files:

- adworkdir
- db2instance → *DB2\_instance\_directory* (for example, /home/ldapdb2/sqllib)
- etc
- idsprofile
- logs
- tmp
- userprofile
- workdir

The `idsprofile` file is used to set the environment for the directory server instance. The `userprofile` file is used to customize the environment. The `idsprofile` file invokes the `userprofile` file after setting the environment. If you want to customize the environment, be sure to change the `userprofile` file and not the `idsprofile` file.

Files in the `idsslapd-instance_name` directory are owned by the directory server instance owner user ID and the primary group of the directory server instance owner user ID.

---

## Appendix G. Migrating a replicating environment from SecureWay Directory 3.2.2

When migrating from IBM SecureWay Directory 3.2.2 to IBM Tivoli Directory Server 6.0, you must unconfigure the database. Before unconfiguring the database, be sure 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 AIX, Solaris, and Linux platforms:**

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

**Note:** If you are not issuing this command as the root, you must 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, 3.2.2 replicas and 4.1 replicas with a 6.0 master.

If you are moving your whole enterprise to IBM Tivoli Directory Server 6.0 from IBM SecureWay Directory 3.2.2 you can:

1. Create an LDIF file using **idsdb2ldif** on the master.
2. Unconfigure the database on all the servers.
3. Install IBM Tivoli Directory Server Version 6.0 on each server.
4. Perform the migration procedure.
5. Use the **idsldif2db** or **idsbulkload** command to load the master's data onto 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>
```



---

## Appendix H. Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express

To use the Web Administration Tool, an application server is required. The embedded version of WebSphere Application Server - Express, v5.1.1 is provided with IBM Tivoli Directory Server 6.0 as an application server.

If you use the InstallShield GUI to install the Web Administration Tool, you can select the embedded version of WebSphere Application Server - Express for installation. In this case, configuration is also done automatically.

If you use native installation methods, you can install and configure the embedded version of WebSphere Application Server - Express manually. If you already have the embedded version of WebSphere Application Server - Express v5.1.1 installed, you must configure manually before you can use the Web Administration Tool.

---

### Manually installing and configuring the embedded version of WebSphere Application Server - Express

The following instructions show how to manually install the embedded version of WebSphere Application Server - Express, and then how to install the Web Administration Tool into it. If you install the Web Administration Tool and the embedded version of WebSphere Application Server - Express through the InstallShield GUI, this setup is done for you.

#### Installing the embedded version of WebSphere Application Server - Express

To manually install the embedded version of WebSphere Application Server - Express, use the following procedure:

1. After you download and unzip (or untar) the IBM Tivoli Directory Server zip or tar file, change directories to the directory where you expanded the file, and then change to the appsrv subdirectory.
2. Type the following command at a command prompt:

- On Windows systems:

```
install.bat -installRoot embWASE_installpath -hostName localhost
```

- On AIX, Linux, Solaris, and HP-UX systems:

```
install.sh -installRoot embWASE_installpath -hostName localhost
```

where *embWASE\_installpath* is the directory where you are installing the embedded version of WebSphere Application Server - Express. By convention, this directory is the appsrv subdirectory of the directory where IBM Tivoli Directory Server is installed, but you can use any directory. (This directory is /opt/IBM/ldap/V6.0/appsrv on AIX, Solaris, and HP-UX systems and /opt/ibm/ldap/V6.0/appsrv on Linux systems, by convention.)

Install the Web Administration Tool, using either the InstallShield GUI or an operating system utility for your operating system. After installing the Web Administration Tool, copy the Web Administration Tool to the embedded version of WebSphere Application Server - Express directory by using the following commands:

- On Windows systems:  

```
md embWASE_installpath\installableApps\
copy installpath\idstools\IDSWebApp.war embWASE_installpath\installableApps\
```
  - On AIX, Linux, Solaris, and HP-UX systems:  

```
mkdir embWASE_installpath/installableApps/
cp installpath/idstools/IDSWebApp.war embWASE_installpath/installableApps/
```
- where
- *embWASE\_installpath* is the directory where you are installing the embedded version of WebSphere Application Server - Express. By convention, this directory is the appsrv subdirectory of the directory where IBM Tivoli Directory Server is installed, but you can use any directory.
  - *installpath* is the directory where IBM Tivoli Directory Server is installed.

## Installing the Web Administration Tool into the embedded version of WebSphere Application Server - Express

Install the Web Administration Tool into the embedded version of WebSphere Application Server - Express by using the following command:

- On Windows systems:  

```
"embWASE_installpath\bin\wsadmin.bat" -conntype NONE -c "$AdminApp
install {embWASE_installpath\installableApps\IDSWebApp.war}
{-configroot \"embWASE_installpath/config\"
-node DefaultNode -usedefaultbindings -nodeployejb -appname IDSWebApp.war
-contextroot \"IDSWebApp\"}"
```

**Note:** Type the command on one line.

- On AIX, Linux, Solaris, and HP-UX systems:  

```
"embWASE_installpath/bin/wsadmin.sh" -conntype NONE -c "\$AdminApp
install {embWASE_installpath/installableApps/IDSWebApp.war}
{-configroot \"embWASE_installpath/config\"
-node DefaultNode -usedefaultbindings -nodeployejb -appname IDSWebApp.war
-contextroot \"IDSWebApp\"}"
```

*embWASE\_installpath* is the directory where you are installing the embedded version of WebSphere Application Server - Express. By convention, this directory is the appsrv subdirectory of the directory where IBM Tivoli Directory Server is installed, but you can use any directory.

**Note:** If you install the Web Administration Tool and the embedded version of WebSphere Application Server - Express through the InstallShield GUI, these commands are run automatically.

---

## Uninstalling the Web Administration Tool from the embedded version of WebSphere Application Server - Express

To uninstall the Web Administration Tool from the embedded version of WebSphere Application Server - Express manually:

1. Be sure that the application server is started. See "Starting the application server to use the Web Administration Tool" on page 149 for instructions.
2. Type the following at a command prompt to uninstall the Web Administration Tool:
  - On Windows systems:  

```
embWASE_installpath\bin\wsadmin.bat -conntype NONE -c "$AdminApp
uninstall IDSWebApp.war"
```

- On AIX, Linux, Solaris, and HP-UX systems:

```
embWASE_installpath/bin/wsadmin.sh -conntype NONE -c "\$AdminApp  
uninstall IDSWebApp.war"
```

where *embWASE\_installpath* is the directory where you installed the embedded version of WebSphere Application Server - Express. By convention, this directory is the appsrv subdirectory of the directory where IBM Tivoli Directory Server is installed, but you can use any directory.

---

## Default ports for the embedded version of WebSphere Application Server - Express

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

- Http Transport (port 1): 12100
- Http Transport (port 2): 12101
- Bootstrap/rmi port: 12102
- Soap connector port: 12103

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

### Http Transport port 1

Find the line containing the port number 12100 in the following files and replace the 12100 with the port number that you want:

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

where *embWASE\_installpath* is the directory where the embedded version of WebSphere Application Server - Express is installed.

### Http Transport port 2

Find the line containing the port number 12101 in the following files and replace the 12101 with the port number that you want:

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

where *embWASE\_installpath* is the directory where the embedded version of WebSphere Application Server - Express is installed.

### Bootstrap/rmi port

Find the line containing the port number 12102 in the following file and replace the 12102 with the port number that you want:

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

where *embWASE\_installpath* is the directory where the embedded version of WebSphere Application Server - Express is installed.

### Soap connector port

Find the line containing the port number 12103 in the following file and replace the 12103 with the port number that you want:

```
$embWASE_installpath\config\cells\DefaultNode\nodes\  
DefaultNode\serverindex.html  
$embWASE_installpath\properties\wsadmin.properties
```

where *embWASE\_installpath* is the directory where the embedded version of WebSphere Application Server - Express is installed.

---

## Using HTTPS for the embedded version of WebSphere Application Server - Express Version 5.1.1

The embedded version of WebSphere Application Server - Express, Version 5.1.1, by default, has HTTPS set up on port 12101. To use HTTPS, you must change your login Web address to the following:

```
https://<hostname>:12101/IDSWebApp/IDSjsp/Login.jsp
```

For non-HTTPS connections, continue to use the following Web address:

```
http://<hostname>:12100/IDSWebApp/IDSjsp/Login.jsp
```

Additionally, if you want to change the application server's SSL certificate, you can create new key and trust store database files for the embedded version of 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="DefaultNode/DefaultSSLSettings">  
  <setting xmi:id="DefaultSSLSettings"  
    <setting xmi:id="SecureSocketLayer_1"  
      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>
```



---

## Appendix I. Installing the Web Administration Tool into WebSphere

IBM Tivoli Directory Server 6.0 provides the embedded version of WebSphere Application Server - Express version 5.1.1 as an application server for the Web Administration Tool. However, you can also use WebSphere version 5.1.1 as an application server for the Web Administration Tool. If you use WebSphere, you must install the Web Administration Tool into WebSphere. Use the following instructions as a guide:

1. Install WebSphere, using the installation information provided with it.
2. Install the Web Administration Tool using either the InstallShield GUI or the installation utility for your operating system. The file containing the Web Administration Tool is named `IDSWebApp.war`, and it is in the `idstools` subdirectory of the installation directory you specified during installation.
3. Install the Web Administration Tool application into WebSphere, using the information provided with WebSphere. For example, if you use the Administrative Console, on the Install New Application window, set the **Local path** to `installdirectory/idstools/IDSWebApp.war`, and the **Context root** to `/IDSWebApp`.

*installdirectory* is the directory you specified when installing the Web Administration Tool.

4. Start the Web Administration Tool (for example, through the Administrative Console).
5. From a Web browser, type the following address:

- For http, type `http://localhost:12100/IDSWebApp/IDSjsp/Login.jsp`
- For https, type `http://localhost:12101/IDSWebApp/IDSjsp/Login.jsp`

The IBM Tivoli Directory Server Web Administration login page window is displayed.

**Note:** This address works only if you are running the browser on the computer on which the Web Administration Tool is installed. If the Web Administration Tool is installed on a different computer, replace `localhost` with the hostname or IP address of the computer where the Web Administration Tool is installed.



## Appendix J. ASCII characters from 33 to 126

The following table shows ASCII characters from 33 to 126. These are the characters that can be used in the encryption seed string.

| ASCII code | Character              | ASCII code | Character             | ASCII code | Character           |
|------------|------------------------|------------|-----------------------|------------|---------------------|
| 33         | ! exclamation point    | 34         | " double quotation    | 35         | # number sign       |
| 36         | \$ dollar sign         | 37         | % percent sign        | 38         | & ampersand         |
| 39         | ' apostrophe           | 40         | ( left parenthesis    | 41         | ) right parenthesis |
| 42         | * asterisk             | 43         | + plus sign           | 44         | , comma             |
| 45         | - hyphen               | 46         | . period              | 47         | / slash             |
| 48         | 0                      | 49         | 1                     | 50         | 2                   |
| 51         | 3                      | 52         | 4                     | 53         | 5                   |
| 54         | 6                      | 55         | 7                     | 56         | 8                   |
| 57         | 9                      | 58         | : colon               | 59         | ; semicolon         |
| 60         | < less-than sign       | 61         | = equals sign         | 62         | > greater-than sign |
| 63         | ? question mark        | 64         | @ at sign             | 65         | A uppercase a       |
| 66         | B uppercase b          | 67         | C uppercase c         | 68         | D uppercase d       |
| 69         | E uppercase e          | 70         | F uppercase f         | 71         | G uppercase g       |
| 72         | H uppercase h          | 73         | I uppercase i         | 74         | J uppercase j       |
| 75         | K uppercase k          | 76         | L uppercase l         | 77         | M uppercase m       |
| 78         | N uppercase n          | 79         | O uppercase o         | 80         | P uppercase p       |
| 81         | Q uppercase q          | 82         | R uppercase r         | 83         | S uppercase s       |
| 84         | T uppercase t          | 85         | U uppercase u         | 86         | V uppercase v       |
| 87         | W uppercase w          | 88         | X uppercase x         | 89         | Y uppercase y       |
| 90         | Z uppercase z          | 91         | [ left square bracket | 92         | \ backslash         |
| 93         | ] right square bracket | 94         | ^ caret               | 95         | _ underscore        |
| 96         | ` grave accent         | 97         | a lowercase a         | 98         | b lowercase b       |
| 99         | c lowercase c          | 100        | d lowercase d         | 101        | e lowercase e       |
| 102        | f lowercase f          | 103        | g lowercase g         | 104        | h lowercase h       |
| 105        | i lowercase i          | 106        | j lowercase j         | 107        | k lowercase k       |
| 108        | l lowercase l          | 109        | m lowercase m         | 110        | n lowercase n       |
| 111        | o lowercase o          | 112        | p lowercase p         | 113        | q lowercase q       |
| 114        | r lowercase r          | 115        | s lowercase s         | 116        | t lowercase t       |
| 117        | u lowercase u          | 118        | v lowercase v         | 119        | w lowercase w       |
| 120        | x lowercase x          | 121        | y lowercase y         | 122        | z lowercase z       |
| 123        | { left curly brace     | 124        | vertical bar          | 125        | } right curly brace |
| 126        | ~ tilde                |            |                       |            |                     |



---

## Appendix K. Information for bundlers

If you produce a product that bundles IBM Tivoli Directory Server, use the information in this appendix:

---

### How to install silently

To install IBM Tivoli Directory Server silently:

#### On Windows systems:

Use the silent installation provided with IBM Tivoli Directory Server. See Chapter 12, "Installing and uninstalling silently on Windows platforms," on page 99 for instructions.

**Note:** For Windows systems, you can eliminate the `\db2`, `\gskit`, and `\appsrv` directories from the image you are bundling for IBM Tivoli Directory Server for silent installation.

#### On AIX, Linux, Solaris, and HP-UX systems:

**Note:** Silent installation using the IBM Tivoli Directory Server InstallShield GUI installation is not supported on AIX, Linux, Solaris, and HP-UX systems.

- If you want to use InstallShield for Multi-platforms to build your installation program, you can use the native install beans provided by InstallShield for Multi-platforms to bundle and launch native installation of the IBM Tivoli Directory Server native packages for the appropriate operating system.
- To use native operating system commands to install the native installation packages, you can launch a script during your installation that runs the native commands.

For information about the native installation packages for each operating system, see one of the following:

- Chapter 8, "Installing IBM Tivoli Directory Server using AIX utilities," on page 65
- Chapter 9, "Installing IBM Tivoli Directory Server using Linux utilities," on page 77
- Chapter 10, "Installing IBM Tivoli Directory Server using Solaris utilities," on page 83
- Chapter 11, "Installing IBM Tivoli Directory Server using HP-UX utilities," on page 91

---

### Environment variable for silent installation with native packages

To install IBM Tivoli Directory Server using the native installation packages, you must set the environment variable `IBMLDAP_INSTALL_SILENT` to **yes**. If you do not set this environment variable, the installation might hang when an echo or prompt statement in the native package is reached.

**Note:** This does not apply to Solaris or HP-UX systems.

---

## Installing corequisite products silently

For information about installing corequisite products such as DB2 silently, see the documentation for the product.

**Note:** Be sure that you meet any licensing requirements for any product that you bundle with your product.

---

## Starting the instance administration tool in migration mode

If you are migrating a directory server from a previous release to a directory server instance, you can start the Instance Administration Tool in *migration mode*. The command for starting the Instance Administration Tool in this way is:

```
idsxinst -migrate path
```

where *path* is the path where the backed-up configuration and schema files are stored.

The first window displayed in the Instance Administration Tool when you start it in this way is the Instance details window. See step 4 on page 110 for information about how to use the Instance Administration Tool starting on this window.

---

## Additional information about GSKit

GSKit has shipped the following jar files for your convenience:

- lib/ext/ibmjceprovider.jar
- lib/ext/ibmpkcs.jar
- lib/ibmjcefw.jar
- lib/security/local\_policy.jar
- lib/security/US\_export\_policy.jar
- lib/ibmpkcs11.jar

It is up to each individual product to decide whether to provide these JSSE jar files in the product. The following are GSKit's recommendations:

- A product should ship whatever JSSE jar files it used for system testing with the product.
- If your existing Java 1.3 or 1.4 installation's JSSE jar files are later than those required by GSKit, no action is required.
- If your existing Java 1.3 or 1.4.1 installation's JSSE jar files are older than those required by GSKit, you should replace your old JSSE jar files with GSKit's. GSKit IKeyman will work with the old JSSE jar files. However, the support for IPv6 may not work and some IKeyman functions may fail due to known bug fixes that are not included in your JDK installation.

---

## Appendix L. Installing and configuring DSML

Directory Services Markup Language (DSML) is installed as a .zip file named DSML.zip in the *installpath/idstools* (or *installpath\idstools* for Windows systems) directory when you install the Web Administration Tool. After you unzip the DSML.zip file, documentation files are available that tell you how to install, configure, and use DSML. These files are:

**DSMLReadme.txt**

Describes the files in the package and tells you how to install and configure DSML.

**dsml.pdf**

Describes how to use DSML. This file is in PDF format.

**dsml.htm**

Describes how to use DSML, in HTML format.





---

## Appendix M. Loading a sample database

Use the following procedure to load a sample database.

1. In the Configuration Tool, click **Manage suffixes** in the task list on the left. (See “Using the IBM Tivoli Directory Server Configuration Tool (idsxcfg)” on page 125 for information about using the Configuration Tool.)
2. In the Manage suffixes window, in the **SuffixDN** field, type `o=ibm,c=us`. This is the suffix DN that will hold the sample data. Because the sample data is part of the suffix `o=ibm,c=us`, this is the suffix DN you must add.
3. Click **Add**.
4. Click **OK**.

**Note:** When you click **Add**, the suffix is added to the list in the **Current suffix DNs** box; however, the suffix is not actually added until you click **OK**.

5. In the Configuration Tool, click **Import LDIF data** in the task list on the left.
6. In the Import LDIF data window on the right, in the **Path and LDIF file name** field, type one of the following:
  - `install_dir\examples\sample.ldif` on Windows systems. *install\_dir* is the directory where you installed IBM Tivoli Directory Server. By default on Windows systems, this directory is `C:\Program Files\IBM\LDAP\V6.0`.
  - `/opt/IBM/ldap/V6.0/examples/sample.ldif` on AIX, Solaris, and HP-UX systems.
  - `/opt/ibm/ldap/V6.0/examples/sample.ldif` on Linux systems.

Alternatively, you can click **Browse** to locate the file.

7. Click **Standard import**.
8. Click **Import**.

**Note:** As an alternative, you can use:

- The `idscfgsuf` command to add the suffix: `idscfgsuf -s "o=ibm,c=us"`
- The `idsldif2db` utility to import the data. For example, `idsldif2db -i install_dir\examples\sample.ldif -I myinstance` where *myinstance* is the name of the directory server instance.

9. After processing is complete, click **Close**.
10. To start the directory server instance:
  - a. Go to the `sbin` subdirectory of the directory where you installed IBM Tivoli Directory Server.
  - b. If you have only one directory server instance, type `idsslapd` at a command prompt. If you have more than one directory server instance, type `idsslapd -I instancename`, where *instancename* is the name of the instance you want to start.

Messages are displayed while the server is starting. The following message is displayed if the server starts successfully:

```
IBM Tivoli Directory, Version 6.0 Server started.
```

You have verified that the sample database is loaded correctly and that the installation is successful.

Use the instructions in “Starting the Web Administration Tool” on page 149 to start the Web Administration Tool if you installed it. See the *IBM Tivoli Directory Server Version 6.0 Administration Guide* for information about using the Web Administration Tool and using the server.

---

## Appendix N. UTF-8 support

IBM Tivoli Directory Server supports a wide variety of national language characters through the UTF-8 (UCS Transformation Format) character set. As specified for the LDAP Version 3 protocol, all character data that is passed between an LDAP client and a server is in UTF-8. Consequently, the directory server can be configured to store any national language characters that can be represented in UTF-8. The limitations on what types of characters can be stored and searched for are determined by how the database is created. The database character set can be specified as UTF-8 or it can be set to use the server system's local character set (based on the locale, language, and code page environment).

If you specify UTF-8, you can store any UTF-8 character data in the directory. LDAP clients running anywhere in the world (in any UTF-8 supported language) can access and search the directory. In many cases, however, the client has limited ability to properly display the results retrieved from the directory in a particular language/character set. There is also a performance advantage to using a UTF-8 database because no data conversion is required when storing data to or retrieving data from the database.

**Note:** If you want to use language tags, the database must be a UTF-8 database.

---

### Why choose anything other than UTF-8?

A UTF-8 database has a fixed collation sequence. That sequence is the binary order of the UTF-8 characters. It is not possible to do language-sensitive collation with a UTF-8 database.

If it is important to your LDAP applications or users to get results for a search using an ordering filter (for example, "name >= SMITH") or any search specifying the control to sort the results as they would expect for their native language, then UTF-8 might not be the appropriate character set for their directory database. In that instance, the LDAP server system and all client systems should run using the same character set and locale. For example, an LDAP server running in a Spanish locale with a database created using that locale returns results of searches based on character ordering, as Spanish-language clients would expect. This configuration does limit your directory user community to a single end-user character set and collation sequence.

---

### Server utilities

Manual creation of an LDIF file containing UTF-8 values is difficult. To simplify this process, a charset extension to the LDIF format is supported. This extension allows an Internet Assigned Numbers Authority (IANA) character set name to be specified in the header of the LDIF file (along with the version number). A limited set of the IANA character sets are supported.

### Examples

You can use the optional charset tag so that the server utilities automatically convert from the specified character set to UTF-8 as in the following example:

```

version: 1
charset: ISO-8859-1

dn: cn=Juan Griego, o=University of New Mexico, c=US
cn: Juan Griego
sn: Griego
description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIH1vd
title: Associate Dean
title: [title in Spanish]
jpegPhoto:< file:///usr/local/photos/jgriego.jpg

```

In this instance, all values following an attribute name and a single colon are translated from the ISO-8859-1 character set to UTF-8. Values following an attribute name and a double colon (such as `description:: V2hhdCBhIGNhcm...`) should be base 64-encoded, and are expected to be either binary or UTF-8 character strings. Values read from a file, such as the `jpegPhoto` attribute specified by the Web address in the example above, are also expected to be either binary or UTF-8. No translation from the specified "charset" to UTF-8 is done on those values.

In this example of an LDIF file without the charset tag, content is expected to be in UTF-8:

```

# IBM IBM Directorysample LDIF file
#
# The suffix "o=IBM, c=US" should be defined before attempting to load
# this data.

version: 1

dn: o=IBM, c=US
objectclass: top
objectclass: organization
o: IBM

dn: ou=Austin, o=IBM, c=US
ou: Austin
objectclass: organizationalUnit
seealso: cn=Mary Smith, ou=Austin, o=IBM, c=US

```

This same file could be used without the `version: 1` header information, as in previous releases of IBM Tivoli Directory Server:

```

# IBM IBM Directorysample LDIF file
#
#The suffix "o=IBM, c=US" should be defined before attempting to load
#this data.

dn: o=IBM, c=US
objectclass: top
objectclass: organization
o: IBM

dn: ou=Austin, o=IBM, c=US
ou: Austin
objectclass: organizationalUnit
seealso: cn=Linda Carlesberg, ou=Austin, o=IBM, c=US

```

---

## Supported IANA character sets

IBM Tivoli Directory Server supports the Internet Assigned Number Authority (IANA) character set names by platform, as shown in the following table. These are the character set names that can be specified in an LDIF file or using the C-client interface to identify the character set of input data to be used with the directory.

Table 9. Supported IANA character sets by platform

| Character<br>Set Name | Locale                                  |     |     |         | DB2 Code Page                       |      |
|-----------------------|---|-----|-----|---------|-------------------------------------|------|
|                       | Linux,<br>Linux for<br>S/390®,<br>HP-UX | NT  | AIX | Solaris | AIX, Linux,<br>Solaris, or<br>HP-UX | NT   |
| ISO-8859-1            | X                                       | X   | X   | X       | 819                                 | 1252 |
| ISO-8859-2            | X                                       | X   | X   | X       | 912                                 | 1250 |
| ISO-8859-5            | X                                       | X   | X   | X       | 915                                 | 1251 |
| ISO-8859-6            | X                                       | X   | X   | n/a     | 1089                                | 1256 |
| ISO-8859-7            | X                                       | X   | X   | n/a     | 813                                 | 1253 |
| ISO-8859-8            | X                                       | X   | X   | n/a     | 916                                 | 1255 |
| ISO-8859-9            | X                                       | X   | X   | n/a     | 920                                 | 1254 |
| IBM437                | n/a                                     | X   | n/a | n/a     | 437                                 | 437  |
| IBM850                | n/a                                     | X   | X   | n/a     | 850                                 | 850  |
| IBM852                | n/a                                     | X   | n/a | n/a     | 852                                 | 852  |
| IBM857                | n/a                                     | X   | n/a | n/a     | 857                                 | 857  |
| IBM862                | n/a                                     | X   | n/a | n/a     | 862                                 | 862  |
| IBM864                | n/a                                     | X   | n/a | n/a     | 864                                 | 864  |
| IBM866                | n/a                                     | X   | n/a | n/a     | 866                                 | 866  |
| IBM869                | n/a                                     | X   | n/a | n/a     | 869                                 | 869  |
| TIS-620               | n/a                                     | X   | X   | n/a     | 874                                 | 874  |
| EUC-JP                | X                                       | n/a | X   | X       | 954                                 | n/a  |
| EUC-KR                | n/a                                     | n/a | X   | X       | 970                                 | n/a  |
| EUC-CN                | n/a                                     | n/a | X   | X       | 1383                                | n/a  |
| EUC-TW                | n/a                                     | n/a | X   | X       | 964                                 | n/a  |
| Shift-JIS             | X                                       | X   | X   | X       | 932                                 | 943  |
| KSC                   | n/a                                     | X   | n/a | n/a     | n/a                                 | 949  |
| GBK                   | n/a                                     | X   | X   | n/a     | 1386                                | 1386 |
| Big5                  | n/a                                     | X   | X   | X       | 950                                 | 950  |



---

## Appendix O. Setting up GSKit to support CMS key databases

To set up GSKit to support Certificate Management Services (CMS) key databases, complete the following procedure before starting the iKeyman GUI:

1. Be sure that you have installed GSKit 7.0.3.3.
2. Install the IBM JDK 1.4.1 or 1.4.2, or an equivalent JDK.
3. Set JAVA\_HOME to point to the directory where the JDK was installed. For example:
  - On Windows, set JAVA\_HOME=c:\Program Files\IBM\Java14.
  - On AIX, export JAVA\_HOME=/usr/java14.  
If you are using a 64-bit JDK and 64-bit GSKit (gksa) on AIX, export  
JAVA\_HOME-/usr/java14\_64
4. Remove the ibmjssc.jar, gskikm.jar (if it exists) and ibmjcaprovider.jar files from your JAVA\_HOME\jre\lib\ext directory.
5. Be sure that the JAVA\_HOME\jre directory has the following JAR files:
  - lib/ext/ibmjceprovider.jar
  - lib/ext/ibmpkcs.jar
  - lib/ibmjcefw.jar
  - lib/ext/ibmjcefips.jar (optional to support FIPS)
  - lib/security/local\_policy.jar
  - lib/security/US\_export\_policy.jar
  - lib/ibmpkcs11.jar

JDK 1.4 requires the user to have jurisdiction policy files. Due to the import restrictions for some countries, the jurisdiction policy files distributed with the J2SDK version 1.4.1 software have built-in restrictions on the available cryptographic strength. The Solaris JDK and many other installations require jurisdiction policy files that contain no restrictions on cryptographic strength. For more information about jurisdiction policy files, access the following Web site: <http://java.sun.com/products/jce/index-14.html>

To download jurisdiction policy files, access the following Web site:

<http://java.sun.com/j2se/1.4/download.html#docs>

6. GSKit users must register both IBM CMS and IBM JCE service providers as follows:

Update the JAVA\_HOME/jre/lib/security/java.security file to add both IBM CMS and IBM JCE providers after the Sun provider. For example:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.ibm.spi.IBMCMSProvider
security.provider.3=com.ibm.crypto.provider.IBMJCE
```

A sample java.security file can be found in  
*GSKit\_Installation\_path*\classes\gsk\_java.security.

To enable FIPS operation, update the  
JAVA\_HOME/jre/lib/security/java.security file to add IBMCMS, IBMJCE, and  
IBMJCEFIPS providers after the Sun provider. Be sure that the IBMJCEFIPS  
provider was registered at a higher priority than IBMJCE. For example:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.ibm.spi.IBMCMSProvider
security.provider.3=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.4=com.ibm.crypto.provider.IBMJCE
```

On Windows, *GSKit\_Installation\_path* is c:\Program Files\IBM\GSK7

On AIX, *GSKit\_Installation\_path* is /usr/opt/ibm/gskta or /usr/opt/ibm/gksa

7. This step is optional. If you are a JSSE user and use JSSE to access cryptographic hardware, install the `ibmpkcs11.jar` file in the `JAVA_HOME\jre\lib\ext` directory and follow the instructions in `GSKit_Installation_path/classes/native/native-support.zip` to set up the cryptographic hardware DLLs.

**Note:** You could also find the `ibmpkcs11.jar` file in the JSSE package released after August 5, 2002. To register an IBMPKCS11 service provider, the following example updates the

`JAVA_HOME/jre/lib/security/java.security` file:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.crypto.pkcs11.provider.IBMPKCS11
```



---

## Appendix P. IBM Tivoli Directory Server configuration schema

This appendix describes the Directory Information Tree (DIT) and the attributes that are used to configure the `ibmslapd.conf` file. The directory settings are stored using the LDIF format in the configuration file.

The configuration file was renamed from `slapd32.conf` to `ibmslapd.conf` in the 5.1 release. The schema used by the configuration file is also now available. Attribute types can be found in the `v3.config.at` file, and object classes are in the `v3.config.oc` file. Attributes can be modified using the `idsldapmodify` command. See the *IBM Tivoli Directory Server Version 6.0 Administration Guide* for information about the `idsldapmodify` command.

---

### Directory Information Tree

- cn=Configuration
  - cn=Admin
  - cn=AdminGroup
  - cn=Front End
    - cn=Connection Management
  - cn=Event Notification
  - cn=Kerberos
  - cn=Master Server
  - cn=Referral
  - cn=Schemas
    - cn=IBM Directory
      - cn=Config Backends
        - cn=ConfigDB
      - cn=RDBM Backends
        - cn=Directory
        - cn=ChangeLog
      - cn=LDCF Backends
        - cn=SchemaDB
      - cn=ProxyBackends
        - cn=ProxyDB
  - cn=Replication
  - cn=Log Management
    - cn=Default
    - cn=ibmslapd
    - cn=Audit
    - cn=Bulkload
    - cn=DB2CLI
    - cn=Tools
    - cn=Replication
    - cn=Admin

- cn=admin audit
- cn=pwdPolicy Admin
- cn=SSL
  - cn=CRL
- cn=Transaction
- cn=Digest

## cn=Configuration

DN cn=Configuration

### Description

This is the top-level entry in the configuration DIT. It holds data of global interest to the server, although in practice it also contains miscellaneous items. Every attribute in this entry comes from the first section (global stanza) of the `ibmslapd.conf` file.

### Number

1 (required)

### Object Class

ibm-slapdTop

### Mandatory Attributes

- cn
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdSizeLimit
- ibm-slapdTimeLimit
- ibm-slapdDerefAliases
- ibm-slapdCryptoSync
- objectClass

### Optional Attributes

- ibm-slapdConcurrentRW (Deprecated)
- ibm-slapdServerId
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdVersion
- ibm-slapdAdminGroupEnabled
- ibm-slapdStartupTraceEnabled
- ibm-slapdTraceMessageLevel
- ibm-slapdTraceMessageLog
- ibm-slapdIPAddress
- ibm-slapdServerBackend

## cn=Admin

DN cn=Admin, cn=Configuration

### Description

Global configuration settings for IBM Admin Daemon

- Number**  
1 (required)
- Object Class**  
ibm-slapdAdmin
- Mandatory Attributes**
- cn
  - ibm-slapdPort
- Optional Attributes**
- ibm-slapdSecurePort

## cn=AdminGroup

**DN** cn=<id>, cn=AdminGroup, cn=Configuration

**Description**

A user belonging to the Administration Group. Must be an entry under the cn=AdminGroup, cn=Configuration subtree.

**Number**

0 or more (optional) Needed only if you want administrative group members.

**Object Class**

ibm-slapdAdminGroupMember

**Mandatory Attributes**

- ibm-slapdAdminDN
- ibm-slapdAdminPW
- objectClass

**Optional Attributes**

- ibm-slapdKrbAdminDN
- ibm-slapdDigestAdminUser

## cn=Front End

**DN** cn=Front End, cn=Configuration

**Description**

Global environment settings that the server applies at startup.

**Number**

0 or 1 (optional)

**Object Class**

ibm-slapdFrontEnd

**Mandatory Attributes**

- cn
- objectClass

**Optional Attributes**

- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdDB2CP
- ibm-slapdEntryCacheSize

- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdPlugin
- ibm-slapdSetenv
- ibm-slapdIdleTimeOut

## cn=Connection Management

DN cn=Connection Management, cn=Front End, cn=Configuration

### Description

Global connection settings

### Number

0 or 1 (optional)

### Object Class

ibm-slapdConnectionManagement

### Mandatory Attributes

- cn
- objectClass

### Optional Attributes

- ibm-slapdAllowAnon
- ibm-slapdAllReapingThreshold
- ibm-slapdAnonReapingThreshold
- ibm-slapdBoundReapingThreshold
- ibm-slapdESizeThreshold
- ibm-slapdEThreadActivate
- ibm-slapdEThreadEnable
- ibm-slapdETimeThreshold
- ibm-slapdIdleTimeOut
- ibm-slapdWriteTimeout

## cn=Event Notification

DN cn=Event Notification, cn=Configuration

### Description

Global event notification settings for IBM Tivoli Directory Server

### Number

0 or 1 (optional; needed only if you want to enable event notification)

### Object Class

ibm-slapdEventNotification

### Mandatory Attributes

- cn
- ibm-slapdEnableEventNotification
- objectClass

### Optional Attributes

- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal

## cn=Kerberos

**DN** cn=Kerberos, cn=Configuration

**Description**

Global Kerberos authentication settings for IBM Tivoli Directory Server 6.0.

**Number**

0 or 1 (optional)

**Object Class**

ibm-slapdKerberos

**Mandatory Attributes**

- cn
- ibm-slapdKrbEnable
- ibm-slapdKrbRealm
- ibm-slapdKrbKeyTab
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbAdminDN
- objectClass

**Optional Attributes**

- None

## cn=Master Server

**DN** cn=Master Server, cn=Configuration

**Description**

When configuring a replica, this entry holds the bind credentials and referral URL of the master server.

**Number**

0 or 1 (optional)

**Object Class**

ibm-slapdReplication

**Mandatory Attributes**

- cn
- ibm-slapdMasterPW (Mandatory if not using Kerberos authentication.)
- objectClass

**Optional Attributes**

- ibm-slapdMasterDN
- ibm-slapdMasterPW (Optional if using Kerberos authentication.)
- ibm-slapdMasterReferral

## cn=Referral

**DN** cn=Referral, cn=Configuration

**Description**

This entry contains all the referral entries from the first section (global stanza) of the ibmslapd.conf file. If there are no referrals (there are none by default), this entry is optional.

- Number**  
0 or 1 (optional)
- Object Class**  
ibm-slapdReferral
- Mandatory Attributes**
  - cn
  - ibm-slapdReferral
  - objectClass
- Optional Attributes**
  - None

## cn=Schemas

**DN** cn=Schemas, cn=Configuration

### Description

This entry serves as a container for the schemas. This entry is not really necessary because the schemas can be distinguished by the object class `ibm-slapdSchema`. It is included to improve the readability of the DIT.

Only one schema entry is currently allowed: `cn=IBM Directory`.

- Number**  
1 (required)
- Object Class**  
Container
- Mandatory Attributes**
  - cn
  - objectClass
- Optional Attributes**
  - None

## cn=IBM Directory

**DN** cn=IBM Directory, cn=Schemas, cn=Configuration

### Description

This entry contains all the schema configuration data from the first section (global stanza) of the `ibmslapd.conf` file. It also serves as a container for all the backends that use the schema. Multiple schemas are not supported, but if they were, there would be one `ibm-slapdSchema` entry per schema. Note that multiple schemas are assumed to be incompatible. Therefore, a backend can be associated with a single schema only.

- Number**  
1 (required)
- Object Class**  
ibm-slapdSchema
- Mandatory Attributes**
  - cn
  - ibm-slapdSchemaCheck
  - ibm-slapdIncludeSchema

- objectClass

**Optional Attributes**

- ibm-slapdSchemaAdditions

## cn=Config Backends

**DN** cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Description**

This entry serves as a container for the Config backends.

**Number**

1 (required)

**Object Class**

Container

**Mandatory Attributes**

- cn
- objectClass

**Optional Attributes**

None

## cn=ConfigDB

**DN** cn=ConfigDB, cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Description**

Configuration backend for IBM Tivoli Directory Server server configuration

**Number**

0 - n (optional)

**Object Class**

ibm-slapdConfigBackend

**Mandatory Attributes**

- cn
- ibm-slapdSuffix
- ibm-slapdPlugin
- objectClass

**Optional Attributes**

- ibm-slapdReadOnly

## cn=RDBM Backends

**DN** cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Description**

This entry serves as a container for the RDBM backends. It effectively replaces the database rdbm line from ibmslapd.conf by identifying all sub-entries as DB2 backends. This entry is not really necessary because the RDBM backends can be distinguished by object class ibm-slapdRdbmBackend. It is included to improve the readability of the DIT.

**Number**

0 or 1 (optional)

**Object Class**

Container

**Mandatory Attributes**

- cn
- objectClass

**Optional Attributes**

- None

## cn=Directory

**DN** cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Description**

This entry contains all the database configuration settings for the default RDBM database backend.

Although multiple backends with arbitrary names can be created, the Server Administration assumes that "cn=Directory" is the main directory backend, and that "cn=Change Log" is the optional changelog backend. Only the suffixes displayed in "cn=Directory" are configurable through the Server Administration (except for the changelog suffix, which is set transparently by enabling changelog).

**Number**

0 - n (optional)

**Object Class**

ibm-slapdRdbmBackend

**Mandatory Attributes**

- cn
- objectClass

**Optional Attributes**

- ibm-slapdBulkloadErrors
- ibm-slapdCachedAttribute
- ibm-slapdCachedAttributeSize
- ibm-slapdChangeLogMaxAge
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- ibm-slapdLanguageTagsEnabled
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt



- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

**Note:** If you are using **ibm-slapdUseProcessIdPw**, you must modify the schema to make **ibm-slapdDbUserPW** optional.

## cn=Change Log

**DN** cn=Change Log, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

### Description

This entry contains all the database configuration settings for the change log backend.

### Number

0 - n (optional)

### Object Class

ibm-slapdRdbmBackend

### Mandatory Attributes

- cn
- objectClass

### Optional Attributes

- ibm-slapdBulkloadErrors
- ibm-slapdCachedAttribute
- ibm-slapdCachedAttributeSize
- ibm-slapdChangeLogMaxAge
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDB2CP
- ibm-slapdDBAlias
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- ibm-slapdLanguageTagsEnabled
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns

- `ibm-slapdSortKeyLimit`
- `ibm-slapdSortSrchAllowNonAdmin`
- `ibm-slapdSuffix`
- `ibm-slapdUseProcessIdPw`

**Note:** If you are using `ibm-slapdUseProcessIdPw`, you must modify the schema to make `ibm-slapdDbUserPW` optional.

## cn=LDCF Backends

**DN** `cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration`

### Description

This entry serves as a container for the LDCF backends. It effectively replaces the database `ldcf` line from `ibmslapd.conf` by identifying all sub-entries as LDCF backends. This entry is not really necessary because the LDCF backends can be distinguished by the object class `ibm-slapdLdcfBackend`. It is included to improve the readability of the DIT.

### Number

1 (required)

### Object Class

Container

### Mandatory Attributes

- `cn`
- `objectClass`

### Optional Attributes

- `ibm-slapdPlugin`

## cn=SchemaDB

**DN** `cn=SchemaDB, cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration`

### Description

This entry contains all the database configuration data from the `ldcf` database section of `ibmslapd.conf`.

### Number

1 (required)

### Object Class

`ibm-slapdLdcfBackend`

### Mandatory Attributes

- `cn`
- `objectClass`

### Optional Attributes

- `ibm-slapdPlugin`
- `ibm-slapdReadOnly`
- `ibm-slapdSuffix`

## cn=Proxy Backends

**DN** `cn=Proxy Backends, cn=IBM Directory, cn=Schemas, cn=Configuration`

**Description**

This entry serves as a container for the proxy backends.

**Number**

1 (required)

**Object Class**

Container

**Mandatory Attributes**

- cn
- objectClass

**Optional Attributes**

- None

## cn=Proxy DB

**DN** cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Description**

This entry contains information related to loading the proxy plug-in.

**Number**

1 (required)

**Object Class**

ibm-slapdProxyBackend

**Mandatory Attributes**

- cn
- ibm-slapdPlugin
- objectClass

**Optional Attributes**

ibm-slapdSuffix

## cn=Replication

**DN** cn=Replication, cn=Configuration

**Description**

This entry configures a server that is a supplier for replication.

**Number**

1 (required)

**Object Class**

ibm-slapdReplicationConfiguration

**Mandatory Attributes**

- cn
- objectClass

**Optional Attributes**

- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdReplContextCacheSize
- ibm-slapdReplMaxErrors
- ibm-slapdReplConflictMaxEntrySize

- ibm-replicationOnHold

## cn=Log Management

DN cn=Log Management, cn=Configuration

### Description

This entry serves as a container for the log management entries.

### Number

1 (required)

### Object Class

Container

### Mandatory Attributes

- cn
- objectClass

### Optional Attributes

- None

## cn=Default

DN cn=Default, cn=Log Management, cn=Configuration

### Description

This entry contains the default log settings for all logs with the exception of the `ibm-slapdLog` attribute. These settings can be overridden in the specific log management entries. By default this entry has no attributes; therefore, no log limits are enforced.

If the `ibm-slapdLogArchivePath` is not specified, the archived logs will be placed in the directory specified by the `ibm-slapdLog` setting. If the `ibm-slapdLogArchivePath` is specified, the archive path should exist already with the desired permission and ownership. The archived log file names will have the file name specified by `ibm-slapdLog` with the a timestamp prepended.

### Number

0 or 1 (optional)

### Object Class

Container  
`ibm-slapdLogConfig`

### Mandatory Attributes

- cn
- objectClass

### Optional Attributes

- `ibm-slapdLogArchivePath`
- `ibm-slapdLogMaxArchives`
- `ibm-slapdLogSizeThreshold`

## cn=ibmslapd

DN cn=ibmslapd, cn=Log Management, cn=Configuration

**Description**

This entry contains log management configuration information for the ibmslapd log.

**Number**

1 (required)

**Object Class**

Container  
ibm-slapdLogConfig

**Mandatory Attributes**

- cn
- objectClass

**Optional Attributes**

- ibm-slapdLog
- ibm-slapdLogArchivePath
- ibm-slapdLogMaxArchives
- ibm-slapdLogOptions
- ibm-slapdLogSizeThreshold

**cn=Audit**

DN cn=Audit, cn=Log Management, cn=Configuration

**Description**

This entry contains log management configuration information for the audit log.

**Number**

1 (required)

**Object Class**

ibm-auditConfig  
ibm-slapdLogConfig

**Mandatory Attributes**

- cn
- objectClass

**Optional Attributes**

- ibm-audit
- ibm-auditAdd
- ibm-auditAttributesOnGroupEvalOp
- ibm-auditBind
- ibm-auditCompare
- ibm-auditDelete
- ibm-auditExtOpEvent
- ibm-auditFailedOpOnly
- ibm-auditGroupsOnGroupControl
- ibm-auditLog
- ibm-auditModify
- ibm-auditModifyDN
- ibm-auditSearch

- ibm-auditUnbind
- ibm-auditVersion
- ibm-auditExtOp
- ibm-slapdLogMaxArchives
- ibm-slapdLogOptions
- ibm-slapdLogSizeThreshold
- ibm-slapdLogArchivePath
- ibm-slapdLog

## cn=Bulkload

DN cn=Bulkload, cn=Log Management, cn=Configuration

### Description

This entry contains log management configuration information for the bulkload error log.

### Number

1 (required)

### Object Class

- Container
- ibm-slapdLogConfig

### Mandatory Attributes

- cn
- objectClass

### Optional Attributes

- ibm-slapdLogMaxArchives
- ibm-slapdLogOptions
- ibm-slapdLogSizeThreshold
- ibm-slapdLogArchivePath
- ibm-slapdLog

## cn=DB2CLI

DN cn=DB2CLI, cn=Log Management, cn=Configuration

### Description

This entry contains log management configuration information for the db2cli log. Database errors that occur as a result of LDAP operations are recorded in this log.

### Number

1 (required)

### Object Class

- Container
- ibm-slapdLogConfig

### Mandatory Attributes

- cn
- objectClass

### Optional Attributes

- ibm-slapdLogMaxArchives
- ibm-slapdLogOptions
- ibm-slapdLogSizeThreshold
- ibm-slapdLogArchivePath
- ibm-slapdLog

## cn=Tools

**DN** cn=Tools, cn=Log Management, cn=Configuration

### Description

This entry contains log management configuration information for the idstools log. This log contains status and error messages from the configuration tools.

### Number

1 (required)

### Object Class

- Container
- ibm-slapdLogConfig

### Mandatory Attributes

- cn
- objectClass

### Optional Attributes

- ibm-slapdLogMaxArchives
- ibm-slapdLogOptions
- ibm-slapdLogSizeThreshold
- ibm-slapdLogArchivePath
- ibm-slapdLog

## cn=Replication

**DN** cn=Replication, cn=Log Management, cn=Configuration

### Description

This entry contains log management configuration information for the replication lostandfound log.

### Number

1 (required)

### Object Class

- Container
- ibm-slapdLogConfig

### Mandatory Attributes

- cn
- objectClass

### Optional Attributes

- ibm-slapdLogMaxArchives
- ibm-slapdLogOptions
- ibm-slapdLogSizeThreshold

- ibm-slapdLogArchivePath
- ibm-slapdLog

## cn=Admin

**DN** cn=Replication, cn=Log Management, cn=Configuration

### Description

This entry contains log management configuration information for the administration daemon error log.

### Number

1 (required)

### Object Class

- Container
- ibm-slapdLogConfig

### Mandatory Attributes

- cn
- objectClass

### Optional Attributes

- ibm-slapdLogMaxArchives
- ibm-slapdLogOptions
- ibm-slapdLogSizeThreshold
- ibm-slapdLogArchivePath
- ibm-slapdLog

## cn=admin audit

**DN** cn=Admin Audit, cn=Log Management, cn=Configuration

### Description

This entry contains log management configuration information for the administration daemon audit log.

### Number

1 (required)

### Object Class

- Container
- ibm-auditConfig
- ibm-slapdLogConfig

### Mandatory Attributes

- cn
- objectClass

### Optional Attributes

- ibm-slapdLogMaxArchives
- ibm-slapdLogOptions
- ibm-slapdLogSizeThreshold
- ibm-slapdLogArchivePath
- ibm-slapdLog



## cn=pwdPolicy Admin

**DN** cn=pwdPolicy Admin, cn=configuration

### Description

This entry defines the configuration for the IBM Administrative Password Policy for IBM Tivoli Directory Server.

### Number

1 (required)

### Object Class

- ibm-slapdPwdPolicyAdmin

### Mandatory Attributes

- ibm-slapdConfigPwdPolicyOn
- cn
- objectClass

### Optional Attributes

- pwdLockout
- pwdLockoutDuration
- pwdAccountLockedTime
- pwdMaxFailure
- pwdFailureCountInterval
- passwordMinAlphaChars
- passwordMinOtherChars
- passwordMinDiffChars
- passwordMaxRepeatedChars
- pwdMinLength

## cn=SSL

**DN** cn=SSL, cn=Configuration

### Description

Global SSL connection settings for IBM Tivoli Directory Server 6.0.

### Number

0 or 1 (optional)

### Object Class

ibm-slapdSSL

### Mandatory Attributes

- cn
- ibm-slapdSecurePort
- ibm-slapdSecurity
- ibm-slapdSslAuth
- objectClass

### Optional Attributes

- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec

**Note:** `ibm-slapdSslCipherSpecs` is deprecated. Use `ibm-slapdSslCipherSpec` instead. If you use `ibm-slapdSslCipherSpecs`, the server will convert to the supported attribute.

- `ibm-slapdSslKeyDatabase`
- `ibm-slapdSslKeyDatabasePW`
- `ibm-slapdSslKeyRingFilePW`
- `ibm-slapdSslFIPsModeEnabled`
- `ibm-slapdSslFIPsProcessingMode`

## cn=CRL

DN `cn=CRL, cn=SSL, cn=Configuration`

### Description

This entry contains certificate revocation list data from the first section (global stanza) of `ibmslapd.conf`. It is needed only if `"ibm-slapdSslAuth = serverclientauth"` in the `cn=SSL` entry and the client certificates have been issued for CRL validation.

### Number

0 or 1 (optional)

### Object Class

`ibm-slapdCRL`

### Mandatory Attributes

- `cn`
- `ibm-slapdLdapCrlHost`
- `ibm-slapdLdapCrlPort`
- `objectClass`

### Optional Attributes

- `ibm-slapdLdapCrlPassword`
- `ibm-slapdLdapCrlUser`

## cn=Transaction

DN `cn = Transaction, cn = Configuration`

### Description

Specifies Global transaction support settings. Transaction support is provided using the plug-in:

*Windows systems:*

```
extendedop /lib/libtranext.dll tranExtOpInit 1.3.18.0.2.12.5  
1.3.18.0.2.12.6
```

*AIX systems:*

```
extendedop /lib/libtranext.a tranExtOpInit 1.3.18.0.2.12.5  
1.3.18.0.2.12.6
```

*Solaris systems:*

```
extendedop /lib/libtranext.so tranExtOpInit 1.3.18.0.2.12.5  
1.3.18.0.2.12.6
```

The server (**idsslapd**) loads this plug-in automatically at startup if **ibm-slapdTransactionEnable = TRUE**. The plug-in does not need to be explicitly added to the **ibmslapd.conf** file.

**Number**

0 or 1 (optional; required only if you want to use transactions.)

**Object Class**

ibm-slapdTransaction

**Mandatory Attributes**

- cn
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdTransactionEnable
- objectClass

**Optional Attributes**

- None

## cn=Digest

DN cn = Digest, cn = Configuration

**Description**

Global configuration entries for the DIGEST-MD5 SASL bind mechanism.

**Number**

0 or 1 (optional)

**Object Class**

ibm-slapdDigest

**Mandatory Attributes**

- cn
- objectClass

**Optional Attributes**

- ibm-slapdDigestAdminUser
- ibm-slapdDigestAttr
- ibm-slapdDigestRealm

---

## Attributes

- cn
- ibm-replicationOnHold
- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdAdminDN
- ibm-slapdAdminGroupEnabled
- ibm-slapdAdminPW
- ibm-slapdAllowAnon
- ibm-slapdAllReapingThreshold
- ibm-slapdAnonReapingThreshold

- ibm-slapdBoundReapingThreshold
- ibm-slapdBulkloadErrors
- ibm-slapdCachedAttribute
- ibm-slapdCachedAttributeSize
- ibm-slapdChangeLogMaxAge
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdConcurrentRW
- ibm-slapdCryptoSync
- ibm-slapdDB2CP
- ibm-slapdDBAlias
- ibm-slapdConfigPwdPolicyOn
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- ibm-slapdDerefAliases
- ibm-slapdDigestAdminUser
- ibm-slapdDigestAttr
- ibm-slapdDigestRealm
- ibm-slapdDistributedDynamicGroups
- ibm-slapdEnableEventNotification
- ibm-slapdEntryCacheSize
- ibm-slapdESizeThreshold
- ibm-slapdEThreadActivate
- ibm-slapdEThreadEnable
- ibm-slapdETimeThreshold
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdIdleTimeOut
- ibm-slapdIncludeSchema
- ibm-slapdIpAddress
- ibm-slapdKrbAdminDN
- ibm-slapdKrbEnable
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbKeyTab
- ibm-slapdKrbRealm
- ibm-slapdLanguageTagsEnabled
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPassword
- ibm-slapdLdapCrlPort
- ibm-slapdLdapCrlUser
- ibm-slapdLog

- ibm-slapdLogArchivePath
- ibm-slapdLogMaxArchives
- ibm-slapdLogOptions
- ibm-slapdLogSizeThreshold
- ibm-slapdMasterDN
- ibm-slapdMasterPW
- ibm-slapdMasterReferral
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdPort
- ibm-slapdProxyBackendServerDn
- ibm-slapdProxyBindMethod
- ibm-slapdProxyConnectionPoolSize
- ibm-slapdProxyDigestRealm
- ibm-slapdProxyDigestUserName
- ibm-slapdProxyDn
- ibm-slapdProxyNumPartitions
- ibm-slapdProxyPartitionBase
- ibm-slapdProxyPartitionIndex
- ibm-slapdProxyPw
- ibm-slapdProxyTargetURL
- ibm-slapdPwEncryption
- ibm-slapdReadOnly
- ibm-slapdReferral
- ibm-slapdReplConflictMaxEntrySize
- ibm-slapdReplContextCacheSize
- ibm-slapdReplDbConns
- ibm-slapdReplMaxErrors
- ibm-slapdReplicaSubtree
- ibm-slapdSchemaAdditions
- ibm-slapdSchemaCheck
- ibm-slapdSecurePort
- ibm-slapdSecurity
- ibm-slapdServerBackend
- ibm-slapdServerId
- ibm-slapdSetenv
- ibm-slapdSizeLimit

- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSslAuth
- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec
- ibm-slapdSslFIPsModeEnabled
- ibm-slapdSslFIPsProcessingMode
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW
- ibm-slapdSslKeyRingFile
- ibm-slapdSslKeyRingFilePW
- ibm-slapdStartupTraceEnabled
- ibm-slapdSuffix
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdTimeLimit
- ibm-slapdTraceMessageLevel
- ibm-slapdTraceMessageLog
- ibm-slapdTransactionEnable
- ibm-slapdUseProcessIdPw
- ibm-slapdVersion
- ibm-slapdWriteTimeout
- ids-instanceDesc
- ids-instanceLocation
- ids-instanceVersion
- objectClass

## cn

### Description

This is the X.500 common Name attribute, which contains a name of an object.

### Syntax

Directory string

### Maximum Length

256

**Value** Multi-valued

## ibm-ReplicationOnHold

### Description

Controls whether or not the server puts all replication agreements on hold when it starts. Each replication agreement also specifies this, but if this attribute is set to True for the server, it overrides the individual replication agreements. If you are experiencing problems and do not want the server to start replicating at startup, you can set this attribute to True until you are ready for the server to start replicating again. If this attribute is True, you must unsuspend replication each individual replication agreement. See the *IBM Tivoli Directory Server Version 6.0 Administration Guide* for information about unsuspending replication agreements.

- If set to True, replication is on hold.
- If set to False, replication starts.

**Default**

True

**Syntax**

Boolean

**Maximum Length**

5

**Value** Single-valued

## **ibm-slapdACLCache**

**Description**

Controls whether or not the server caches ACL information.

- If set to TRUE, the server caches ACL information.
- If set to FALSE, the server does not cache ACL information.

**Default**

TRUE

**Syntax**

Boolean

**Maximum Length**

5

**Value** Single-valued

## **ibm-slapdACLCacheSize**

**Description**

Maximum number of entries to keep in the ACL Cache.

**Default**

25000

**Syntax**

Integer

**Maximum Length**

11

**Value** Single-valued

## **ibm-slapdAdminDN**

**Description**

The administrator bind DN for IBM Tivoli Directory Server server.

**Default**

cn=root

**Syntax**

DN

**Maximum Length**

Unlimited

**Value** Single-valued

## **ibm-slapdAdminGroupEnabled**

**Description**

Specifies whether the Administrative Group is currently enabled. If set to TRUE, the server will allow users in the administrative group to log in.

**Default**

FALSE

**Syntax**

Boolean

**Maximum Length**

128

**Value** Single-valued

## **ibm-slapdAdminPW**

**Description**

The administrator bind password for IBM Tivoli Directory Server server.

**Default**

secret

**Syntax**

Binary

**Maximum Length**

128

**Value** Single-valued

## **ibm-slapdAllowAnon**

**Description**

Specifies if anonymous binds are allowed.

**Default**

True

**Syntax**

Boolean

**Maximum Length**

128

**Value** Single-valued

## **ibm-slapdAllReapingThreshold**

**Description**

Specifies a number of connections to maintain in the server before connection management is activated.

**Default**

1200

**Syntax**

Directory string with case-exact matching.

**Maximum Length**

1024

**Value** Single-valued



## ibm-slapdAnonReapingThreshold

### Description

Specifies a number of connections to maintain in the server before connection management of anonymous connections is activated.

### Default

0

### Syntax

Directory string with case-exact matching.

### Maximum Length

1024

**Value** Single-valued

## ibm-slapdBoundReapingThreshold

### Description

Specifies a number of connections to maintain in the server before connection management of anonymous and bound connections is activated.

### Default

1100

### Syntax

Directory string with case-exact matching.

### Maximum Length

1024

**Value** Single-valued

## ibm-slapdBulkloadErrors

### Description

File path or device on ibmslapd host machine to which bulkload error messages will be written. On Windows, forward slashes are allowed, and a leading slash not preceded by a drive letter is assumed to be rooted at the installation directory (for example, /tmp/bulkload.errors = D:\Program Files\IBM\ldap\tmp\bulkload.errors).

### Default

/var/bulkload.log

### Syntax

Directory string with case-exact matching

### Maximum Length

1024

**Value** Single-valued

## ibm-slapdCachedAttribute

### Description

Contains the names of the attributes to be cached in the attribute cache, one attribute name per value.

### Default

None

**Syntax**  
Directory string

**Maximum Length**  
256

**Value** Multi-valued

## **ibm-slapdCachedAttributeSize**

**Description**  
Amount of memory, in bytes, that can be used by the attribute cache. A value of 0 indicates not use an attribute cache.

**Default**  
0

**Syntax**  
Integer

**Maximum Length**  
11

**Value** Single-valued.

## **ibm-slapdChangeLogMaxAge**

**Description**  
Specifies the maximum age of changelog entries, in hours, allowed in the associated backend. Each changelog backend has its own `ibm-slapdChangeLogMaxAge` attribute. If the attribute is undefined or out of range (negative), it defaults to 0. Can be between 0 (no limit) and 2,147,483,647.

**Default**  
0

**Syntax**  
Signed Integer

**Maximum Length**  
11

**Value** Single-valued

## **ibm-slapdChangeLogMaxEntries**

**Description**  
This attribute is used by a changelog plug-in to specify the maximum number of changelog entries allowed in the RDBM database. Each changelog has its own `changeLogMaxEntries` attribute.

Minimum = 0 (unlimited)  
Maximum = 2,147,483,647 (32-bit, signed integer)

**Default**  
0

**Syntax**  
Integer

**Maximum Length**  
11

**Value** Single-valued

## **ibm-slapdCLIErrors**

### **Description**

File path or device on ibmslapd host machine to which CLI error messages will be written. On Windows, forward slashes are allowed, and a leading slash not preceded by a drive letter is assumed to be rooted at the install directory (for example, /tmp/cli.errors = D:\Program Files\IBM\ldap\tmp\cli.errors).

### **Default**

/var/db2cli.log

### **Syntax**

Directory string with case-exact matching

### **Maximum Length**

1024

**Value** Single-valued

## **ibm-slapdConcurrentRW**

### **Description**

Setting this attribute to TRUE allows searches to proceed simultaneously with updates. It allows for 'dirty reads', that is, results that might not be consistent with the committed state of the database.

**Attention:** This attribute is deprecated.

### **Default**

FALSE

### **Syntax**

Boolean

### **Maximum Length**

5

**Value** Single-valued

## **ibm-slapdCryptoSync**

### **Description**

A key stash file consistency marker string. It is queried by the server at startup as part of a verification process to ensure that the key stash files match any data that has been two-way encrypted.

### **Default**

None

### **Syntax**

Binary

### **Maximum Length**

None

**Value** Single-valued

## ibm-slapdDB2CP

### Description

Specifies the code page of the directory database. 1208 is the code page for UTF-8 databases.

### Syntax

Directory string with case-exact matching

### Maximum Length

11

**Value** Single-valued

## ibm-slapdDBAlias

### Description

The DB2 database alias.

### Syntax

Directory string with case-exact matching

### Maximum Length

8

**Value** Single-valued

## ibm-slapdConfigPwdPolicyOn

### Description

Indicates whether the IBM Administrative Password Policy is ON.

### Default

FALSE

### Syntax

Boolean

### Maximum Length

5

**Value** Single-valued

## ibm-slapdDbConnections

### Description

Specify the number of DB2 connections the server will dedicate to the DB2 backend. The value must be between 5 and 50 (inclusive).

**Note:** ODBCCONS environment variable overrides the value of this directive.

If `ibm-slapdDbConnections` (or `ODBCCONS`) is less than 5 or greater than 50, the server will use 5 or 50 respectively. One additional connection will be created for replication (even if no replication is defined). 2 additional connections will be created for the change log (if change log is enabled).

### Default

15

### Syntax

Integer

**Maximum Length**

50

**Value** Single-valued**ibm-slapdDbInstance****Description**

Specifies the DB2 database instance for this backend.

**Default**

ldapdb2

**Syntax**

Directory string with case-exact matching

**Maximum Length**

8

**Value** Single-valued

**Note:** All `ibm-slapdRdbmBackend` objects must use the same `ibm-slapdDbInstance`, `ibm-slapdDbUserID`, `ibm-slapdDbUserPW` and DB2 character set.

**ibm-slapdDbLocation****Description**The file system path where the backend database is located. On AIX, Linux, Solaris, and HP-UX, this is usually the home directory of the DB2 instance owner (for example, `/home/ldapdb2`). On Windows, it is a drive (for example, `D:`).**Syntax**

Directory string with case-exact matching

**Maximum Length**

1024

**Value** Single-valued**ibm-slapdDbName****Description**

Specifies the DB2 database name for this backend.

**Default**

ldapdb2

**Syntax**

Directory string with case-exact matching

**Maximum Length**

8

**Value** Single-valued**ibm-slapdDbUserID****Description**

Specifies the user name with which to bind to the DB2 database for this backend.

**Default**

ldapdb2

**Syntax**

Directory string with case-exact matching

**Maximum Length**

8

**Value** Single-valued

**Note:** All ibm-slappedRdbmBackend objects must use the same ibm-slappedDbInstance ibm-slappedDbUserID, ibm-slappedDbUserPW and DB2 character set.

## ibm-slappedDbUserPW

**Description**

Specifies the user password with which to bind to the DB2 database for this backend. The password can be plain text or imask encrypted.

**Default**

ldapdb2

**Syntax**

Binary

**Maximum Length**

128

**Value** Single-valued

**Note:** All ibm-slappedRdbmBackend objects must use the same ibm-slappedDbInstance, ibm-slappedDbUserID, ibm-slappedDbUserPW and DB2 character set.

## ibm-slappedDerefAliases

**Description**

Maximum alias dereferencing level on search requests, regardless of any derefAliases that may have been specified on the client requests. Allowed values are **never**, **find**, **search** and **always**.

**Default**

always

**Syntax**

Directory string

**Maximum Length**

6

**Value** Single-valued

## ibm-slappedDigestAdminUser

**Description**

Specifies the Digest MD5 User Name of the LDAP administrator or administrative group member. Used when MD5 Digest authentication is used to authenticate an administrator.

**Default**  
None

**Syntax**  
Directory string

**Maximum Length**  
512

**Value** Single-valued

## **ibm-slapdDigestAttr**

**Description**  
Overrides the default DIGEST-MD5 username attribute. The name of the attribute to use for DIGEST-MD5 SASL bind username lookup. If the value is not specified, the server uses uid.

**Default**  
If not specified, the server uses uid.

**Syntax**  
Directory string.

**Maximum Length**  
64

**Value** Single-valued

## **ibm-slapdDigestRealm**

**Description**  
Overrides the default DIGEST-MD5 realm. A string that can enable users to know which username and password to use, in case they might have different ones for different servers. Conceptually, it is the name of a collection of accounts that might include the users account. This string should contain at least the name of the host performing the authentication and might additionally indicate the collection of users who might have access. An example might be `registered_users@gotham.news.example.com`. If the attribute is not specified, the server uses the fully qualified hostname of the server.

**Default**  
The fully qualified hostname of the server

**Syntax**  
Directory string.

**Maximum Length**  
1024

**Value** Single-valued

## **ibm-slapdDistributedDynamicGroups**

**Description**  
Switch that determines whether the proxy server allows for dynamic group evaluation (for example, `ibm-allmembers`).

**Default**  
None

**Syntax** Directory String with case-ignored matching  
**Maximum Length** 11  
**Value** Single-valued

## **ibm-slapdEnableEventNotification**

**Description**  
Specifies whether to enable Event Notification. It must be set to either TRUE or FALSE.  
  
If set to FALSE, the server rejects all client requests to register event notifications with the extended result LDAP\_UNWILLING\_TO\_PERFORM.  
**Default** TRUE  
**Syntax** Boolean  
**Maximum Length** 5  
**Value** Single-valued

## **ibm-slapdEntryCacheSize**

**Description**  
Maximum number of entries to keep in the entry cache.  
**Default** 25000  
**Syntax** Integer  
**Maximum Length** 11  
**Value** Single-valued

## **ibm-slapdESizeThreshold**

**Description**  
Specifies the number of work items on the work queue before the Emergency thread is activated.  
**Default** 50  
**Syntax** Integer  
**Maximum Length** 1024  
**Value** Single-valued



## ibm-slapdEThreadActivate

### Description

Specifies which conditions will activate the Emergency Thread. Must be set to one of the following values:

- S** Size only
- T** Time only
- SOT** Size or time
- SAT** Size and time

### Default

SAT

### Syntax

String

### Maximum Length

1024

**Value** Single-valued

## ibm-slapdEThreadEnable

### Description

Specifies if the Emergency Thread is active.

### Default

True

### Syntax

Boolean

### Maximum Length

1024

**Value** Single-valued

## ibm-slapdETimeThreshold

### Description

Specifies the amount of time in minutes between items removed from the work queue before the Emergency thread is activated.

### Default

5

### Syntax

Integer

### Maximum Length

1024

**Value** Single-valued

## ibm-slapdFilterCacheBypassLimit

### Description

Search filters that match more than this number of entries will not be added to the Search Filter cache. Because the list of entry IDs that matched the filter are included in this cache, this setting helps to limit memory use. A value of 0 indicates no limit.

**Default**  
100

**Syntax**  
Integer

**Maximum Length**  
11

**Value** Single-valued

## **ibm-slapdFilterCacheSize**

**Description**  
Specifies the maximum number of entries to keep in the Search Filter Cache.

**Default**  
25000

**Syntax**  
Integer

**Maximum Length**  
11

**Value** Single-valued

## **ibm-slapdIdleTimeOut**

**Description**  
Maximum time to keep an LDAP connection open when there is no activity on the connection. The idle time for an LDAP connection is the time (in seconds) between the last activity on the connection and the current time. If the connection has expired, based on the idle time being greater than the value of this attribute, the LDAP server will clean up and end the LDAP connection, making it available for other incoming requests.

**Default**  
300

**Syntax**  
Integer

**Length**  
11

**Count** Single

**Usage** Directory operation

**User Modify**  
Yes

**Access Class**  
Critical

**Required**  
No

## **ibm-slapdIncludeSchema**

**Description**  
Specifies a file path on the IBM Tivoli Directory Server server machine

containing schema definitions. On Windows 2000, Windows NT®, or Windows XP operating systems, forward slashes are allowed, and a leading slash not preceded by a drive letter (D:) is assumed to be rooted at the installation directory; that is, /etc/V3.system.at = D:\Program Files\IBM\ldap\etc\V3.system.at.

**Default**

/etc/V3.system.at  
/etc/V3.system.oc  
/etc/V3.config.at  
/etc/V3.config.oc  
/etc/V3.ibm.at  
/etc/V3.ibm.oc  
/etc/V3.user.at  
/etc/V3.user.oc  
/etc/V3.ldapsyntaxes  
/etc/V3.matchingrules

**Syntax**

Directory string with case-exact matching

**Maximum Length**

1024

**Value** Multi-valued

## **ibm-slapdIpAddress**

**Description**

Specifies IP addresses the server will listen on. These can be IPv4 or IPv6 addresses. If the attribute is not specified, the server uses all IP addresses assigned to the host computer. This is supported on i5/OS only.

**Default**

None

**Syntax**

IA5 string syntax

**Maximum Length**

32

**Value** Multi-valued

## **ibm-slapdKrbAdminDN**

**Description**

Specifies the Kerberos ID of the LDAP administrator (for example, ibm-kn=admin1@realm1). Used when Kerberos authentication is used to authenticate the administrator when logged onto the Server Administration interface. This attribute might be specified instead of or in addition to adminDN and adminPW.

**Default**

No preset default is defined.

**Syntax**

Directory string with case-exact matching

**Maximum Length**  
128

**Value** Single-valued

## **ibm-slapdKrbEnable**

**Description**  
Specifies whether the server supports Kerberos authentication. It must be either TRUE or FALSE.

**Default**  
TRUE

**Syntax**  
Boolean

**Maximum Length**  
5

**Value** Single-valued

## **ibm-slapdKrbIdentityMap**

**Description**  
Specifies whether to use Kerberos identity mapping. It must be set to either TRUE or FALSE. If set to TRUE, when a client is authenticated with a Kerberos ID, the server searches for all local users with matching Kerberos credentials, and adds those user DN's to the bind credentials of the connection. This allows ACLs based on LDAP user DN's to still be usable with Kerberos authentication.

**Default**  
FALSE

**Syntax**  
Boolean

**Maximum Length**  
5

**Value** Single-valued

## **ibm-slapdKrbKeyTab**

**Description**  
Specifies the LDAP server Kerberos keytab file. This file contains the LDAP server private key, that is associated with its Kerberos account. This file is to be protected (like the server SSL key database file).

On Windows 2000, Windows NT, or Windows XP operating systems, forward slashes are allowed, and any path not preceded by a drive letter. (D:) is assumed to be rooted at the installation directory (that is: /tmp/slapd.errors = D:\Program Files\IBM\ldap\tmp\slapd.errors).

**Default**  
No preset default is defined.

**Syntax**  
Directory string with case-exact matching

**Maximum Length**  
1024

**Value** Single-valued

## **ibm-slapdKrbRealm**

### **Description**

Specifies the Kerberos realm of the LDAP server. It is used to publish the `ldapservicename` attribute in the root DSE. Note that an LDAP server can serve as the repository of account information for multiple KDCs (and realms), but the LDAP server, as a server that is using Kerberos, can only be a member of a single realm.

### **Default**

No preset default is defined.

### **Syntax**

Directory string with case-insensitive matching

### **Maximum Length**

256

**Value** Single-valued

## **ibm-slapdLanguageTagsEnabled**

### **Description**

Whether or not the server should allow language tags. The value read from the `ibmslapd.conf` file for this attribute is `FALSE`, but, can be set to `TRUE`.

### **Default**

`FALSE`

### **Syntax**

Boolean

### **Maximum Length**

5

**Value** Single-valued

## **ibm-slapdLdapCrlHost**

### **Description**

Specifies the host name of the LDAP server that contains the Certificate Revocation Lists (CRLs) for validating client x.509v3 certificates. This parameter is needed when `ibm-slapdSslAuth=serverclientauth` and the client certificates have been issued for CRL validation.

### **Default**

No preset default is defined.

### **Syntax**

Directory string with case-insensitive matching

### **Maximum Length**

256

**Value** Single-valued

## **ibm-slapdLdapCrlPassword**

### **Description**

Specifies the password that server-side SSL uses to bind to the LDAP

server that contains the Certificate Revocation Lists (CRLs) for validating client x.509v3 certificates. This parameter might be needed when `ibm-slapdSslAuth=serverclientauth` and the client certificates have been issued for CRL validation.

**Note:** If the LDAP server holding the CRLs permits unauthenticated access to the CRLs (that is, anonymous access), then `ibm-slapdLdapCrIPassword` is not required.

**Default**

No preset default is defined.

**Syntax**

Binary

**Maximum Length**

128

**Value** Single-valued

## **ibm-slapdLdapCrIPort**

**Description**

Specifies the port used to connect to the LDAP server that contains the Certificate Revocation Lists (CRLs) for validating client x.509v3 certificates. This parameter is needed when `ibm-slapdSslAuth=serverclientauth` and the client certificates have been issued for CRL validation. (IP ports are unsigned, 16-bit integers in the range 1 - 65535)

**Default**

No preset default is defined.

**Syntax**

Integer

**Maximum Length**

11

**Value** Single-valued

## **ibm-slapdLdapCrIUser**

**Description**

Specifies the `bindDN` that the server-side SSL uses to bind to the LDAP server that contains the Certificate Revocation Lists (CRLs) for validating client x.509v3 certificates. This parameter might be needed when `ibm-slapdSslAuth=serverclientauth` and the client certificates have been issued for CRL validation.

**Note:** If the LDAP server holding the CRLs permits unauthenticated access to the CRLs (that is, anonymous access), then `ibm-slapdLdapCrIUser` is not required.

**Default**

No preset default is defined.

**Syntax**

DN

**Maximum Length**

1000

**Value** Single-valued

## **ibm-slapdLog**

### **Description**

Log path and file name. On Windows systems, forward slashes are allowed, and a leading slash not preceded by a drive letter is assumed to be rooted at the installation directory (for example, /tmp/bulkload.errors = D:\Program Files\IBM\ldap\tmp\bulkload.errors).

### **Default**

Path and file name of the appropriate log.

### **Syntax**

Directory string with case-exact matching

### **Maximum Length**

1024

**Value** Single-valued

## **ibm-slapdLogArchivePath**

### **Description**

Path for archived files. On Windows systems, forward slashes are allowed, and a leading slash not preceded by a drive letter is assumed to be rooted at the installation directory (for example, /tmp = D:\Program Files\IBM\ldap\tmp).

### **Default**

Same directory as log file

### **Syntax**

Directory string with case-exact matching

### **Maximum Length**

1024

**Value** Single-valued

## **ibm-slapdLogMaxArchives**

### **Description**

The maximum number of archived logs, where 0 means no archive files will be kept and -1 means an unlimited number of archive files will be kept.

### **Default**

-1

### **Syntax**

Integer

### **Maximum Length**

11

**Value** Single-valued

## **ibm-slapdLogOptions**

### **Description**

Any log options that the log uses; for example, log level or mask.

**Default**  
m for ibmslapd log; unused for others.

**Syntax**  
Directory string with case-ignore matching

**Maximum Length**  
30

**Value** Single-valued

## **ibm-slapdLogSizeThreshold**

**Description**  
When this size threshold, in MB, is exceeded the file will be archived, where 0 means no threshold and thus no archiving.

**Default**  
0

**Syntax**  
Integer

**Maximum Length**  
11

**Value** Single-valued

## **ibm-slapdMasterDN**

**Description**  
Specifies the bind DN of master server. The value must match the replicaBindDN in the replicaObject defined for the master server. When Kerberos is used to authenticate to the replica, ibm-slapdMasterDN must specify the DN representation of the Kerberos ID (for example, ibm-kn=freddy@realm1). When Kerberos is used, MasterServerPW is ignored.

**Default**  
No preset default is defined.

**Syntax**  
DN

**Maximum Length**  
1000

**Value** Single-valued

## **ibm-slapdMasterPW**

**Description**  
Specifies the bind password of master replica server. The value must match replicaBindDN in the replicaObject defined for the master server. When Kerberos is used to authenticate to the replica, ibm-slapdMasterDN must specify the DN representation of the Kerberos ID (for example, ibm-kn=freddy@realm1). When Kerberos is used, MasterServerPW is ignored.

**Default**  
No preset default is defined.



**Syntax**  
Binary

**Maximum Length**  
128

**Value** Single-valued

## **ibm-slapdMasterReferral**

**Description**  
Specifies the URL of the master replica server. For example:  
ldap://master.us.ibm.com

For security set to SSL only:  
ldaps://master.us.ibm.com:636

For security set to none and use a nonstandard port:  
ldap://master.us.ibm.com:1389

**Default**  
none

**Syntax**  
Directory string with case-insensitive matching

**Maximum Length**  
256

**Value** Single-valued

## **ibm-slapdMaxEventsPerConnection**

**Description**  
Specifies the maximum number of event notifications that can be registered per connection.  
Minimum = 0 (unlimited)  
Maximum = 2,147,483,647

**Default**  
100

**Syntax**  
Integer

**Maximum Length**  
11

**Value** Single-valued

## **ibm-slapdMaxEventsTotal**

**Description**  
Specifies the maximum total number of event notifications that can be registered for all connections.  
Minimum = 0 (unlimited)  
Maximum = 2,147,483,647

**Default**  
0

**Syntax**  
Integer

**Maximum Length**  
11

**Value** Single-valued

## **ibm-slapdMaxNumOfTransactions**

**Description**  
Specifies the maximum number of transactions per server.  
Minimum = 0 (unlimited)  
Maximum = 2,147,483,647

**Default**  
20

**Syntax**  
Integer

**Maximum Length**  
11

**Value** Single-valued

## **ibm-slapdMaxOpPerTransaction**

**Description**  
Specifies the maximum number of operations per transaction.  
Minimum = 0 (unlimited)  
Maximum = 2,147,483,647

**Default**  
5

**Syntax**  
Integer

**Maximum Length**  
11

**Value** Single-valued

## **ibm-slapdMaxPendingChangesDisplayed**

**Description**  
Maximum number of pending replication updates or failed updates to be displayed for any given replication agreement on a supplier server. The value is dynamic.

**Default**  
200

**Syntax**  
Integer

**Maximum Length**  
11

**Value** Single-valued

## ibm-slapdMaxTimeLimitOfTransactions

### Description

Specifies the maximum timeout value of a pending transaction in seconds.

Minimum = 0 (unlimited)

Maximum = 2,147,483,647

### Default

300

### Syntax

Integer

### Maximum Length

11

**Value** Single-valued

## ibm-slapdPagedResAllowNonAdmin

### Description

Whether or not the server should allow non-administrator bind for paged results requests on a search request. If the value read from the `ibmslapd.conf` file is `FALSE`, the server will process only those client requests submitted by a user with administrator authority. If a client requests paged results for a search operation, does not have administrator authority, and the value read from the `ibmslapd.conf` file for this attribute is `FALSE`, the server will return to the client with return code `insufficientAccessRights`; no searching or paging will be performed.

### Default

FALSE

### Syntax

Boolean

### Length

5

**Count** Single

**Usage** `directoryOperation`

### User Modify

Yes

### Access Class

critical

### Objectclass

`ibm-slapdRdbmBackend`

### Required

No

## ibm-slapdPagedResLmt

### Description

Maximum number of outstanding paged results search requests allowed active simultaneously. Range = 0.... If a client requests a paged results operation, and a maximum number of outstanding paged results are currently active, then the server will return to the client with return code of `busy`; no searching or paging will be performed.

**Default**  
3

**Syntax**  
Integer

**Length**  
11

**Count** Single

**Usage** directoryOperation

**User Modify**  
Yes

**Access Class**  
critical

**Required**  
No

**Objectclass**  
ibm-slapdRdbmBackend

## ibm-slapdPageSizeLmt

### Description

Maximum number of entries to return from a search for an individual page when paged results control is specified, regardless of any pagesize that might have been specified on the client search request. Range = 0.... If a client has passed a page size, then the smaller value of the client value and the value read from ibmslapd.conf will be used.

**Default**  
50

**Syntax**  
Integer

**Length**  
11

**Count** Single

**Usage** directoryOperation

**User Modify**  
Yes

**Access Class**  
critical

**Required**  
No

**Objectclass**  
ibm-slapdRdbmBackend

## ibm-slapdPlugin

### Description

A plug-in is a dynamically loaded library that extends the capabilities of the server. An ibm-slapdPlugin attribute specifies to the server how to load and initialize a plug-in library. The syntax is:

*keyword filename init\_function [args...]*

The syntax is slightly different for each platform because of library naming conventions. See the *Server Plug-ins Reference* for a list of plug-ins included with IBM Tivoli Directory Server.

Most plug-ins are optional, but the RDBM backend plug-in is required for all RDBM backends.

**Default**

*database /bin/libback-rdbm.dll rdbm\_backend\_init*

**Syntax**

Directory string with case-exact matching

**Maximum Length**

2000

**Value** Multi-valued

## **ibm-slapdPort**

**Description**

Specifies the TCP/IP port used for non-SSL connections. It cannot have the same value as `ibm-slapdSecurePort`. (IP ports are unsigned, 16-bit integers in the range 1 - 65535.)

**Default**

389

**Syntax**

Integer

**Maximum Length**

5

**Value** Single-valued

## **ibm-slapdProxyBackendServerDn**

**Description**

Reference to a configuration file entry describing a proxy backend server.

**Default**

No pre-set default is defined

**Syntax**

DN

**Maximum Length**

2048

**Value** Single-valued

## **ibm-slapdProxyBindMethod**

**Description**

The method used to bind to back-end servers. Must be simple, digest, or Kerberos.

This attribute is not used in the 6.0 release.

**Default**

Simple

**Syntax** Directory string with case-ignore matching

**Maximum Length**  
50

**Value** Single-valued

## **ibm-slapdProxyConnectionPoolSize**

**Description**  
The number of connections to be maintained by the proxy server to an individual back-end server.

**Default**  
1

**Syntax**  
Integer

**Maximum Length**  
11

**Value** Single-valued

## **ibm-slapdProxyDigestRealm**

**Description**  
Optional attribute to provide the realm of the digest MD-5 bind when binding to a back-end server.  
  
This attribute is not used in the 6.0 release.

**Default**  
None

**Syntax**  
Directory string

**Maximum Length**  
2048

**Value** Single-valued

## **ibm-slapdProxyDigestUserName**

**Description**  
The user name to be used when DIGEST is selected as the bind method to a back-end server.  
  
This attribute is not used in the 6.0 release.

**Default**  
None

**Syntax**  
Directory string

**Maximum Length**  
2048

**Value** Single-valued

## ibm-slapdProxyDn

**Description**

The DN that the proxy server will use to bind to back-end server nodes.

**Default**

None

**Syntax**

DN

**Maximum Length**

2048

**Value** Single-valued

## ibm-slapdProxyNumPartitions

**Description**

Specifies the number of servers that a given container is split among.

**Default**

None

**Syntax**

Integer

**Maximum Length**

11

**Value** Single-valued

## ibm-slapdProxyPartitionBase

**Description**

Defines the base at which a container is to be split. Entries below this DN will be split among any number of servers defined with the same base.

**Default**

None

**Syntax**

DN

**Maximum Length**

2048

**Value** Single-valued

## ibm-slapdProxyPartitionIndex

**Description**

The unique index that a given server is assigned in a split container. The value must be less than or equal to the corresponding `ibm-slapdProxyNumPartitionsValue`. The first value begins at 1.

**Default**

None

**Syntax**

Integer

**Maximum Length**

11

**Value** Single-valued

## **ibm-slapdProxyPw**

### **Description**

The password credentials the proxy server will use when binding to a back-end server node.

### **Default**

None

### **Syntax**

Binary

### **Maximum Length**

2048

**Value** Single-valued

## **ibm-slapdProxyTargetURL**

### **Description**

The URL of a backend server. This must be in the form ldap:// or ldaps:// (To indicate SSL, use ldaps).

### **Default**

None

### **Syntax**

Directory string

### **Maximum Length**

2048

**Value** Single-valued

## **ibm-slapdPWEncryption**

### **Description**

Specifies the encoding mechanism for the user passwords before they are stored in the directory. It must be specified as none, aes128, aes192, aes256, crypt, or sha (you must use the keyword **sha** in order to get SHA-1 encoding). The value must be set to none for the SASL cram-md5 bind to succeed.

### **Default**

none

### **Syntax**

Directory string with case-insensitive matching

### **Maximum Length**

6

**Value** Single-valued

## **ibm-slapdReadOnly**

### **Description**

This attribute is normally applied to only the Directory backend. It specifies whether the backend can be written to. It must be specified as either TRUE or FALSE. It defaults to FALSE if unspecified. If set to TRUE,



the server returns LDAP\_UNWILLING\_TO\_PERFORM (0x35) in response to any client request that changes data in the readOnly database.

**Default**  
FALSE

**Syntax**  
Boolean

**Maximum Length**  
5

**Value** Single-valued

## **ibm-slapdReferral**

**Description**  
Specifies the referral LDAP URL to pass back when the local suffixes do not match the request. It is used for superior referral (that is, the suffix is not within the naming context of the server).

**Default**  
No preset default is defined.

**Syntax**  
Directory string with case-exact matching

**Maximum Length**  
32700

**Value** Multi-valued

## **ibm-slapdReplConflictMaxEntrySize**

**Description**  
Maximum number of bytes that an entry can contain and still be re-sent to a target server as a result of replication conflict resolution. This value is dynamic.

**Default**  
0 (unlimited)

**Syntax**  
Integer

**Maximum Length**

**Value** Single-valued

## **ibm-slapdReplContextCacheSize**

**Description**  
Size in bytes of the replication context cache. The value is dynamic.

**Default**  
10000

**Syntax**  
Integer

**Maximum Length**

Value Single-valued

## **ibm-slapdReplDbConns**

### **Description**

Maximum number of database connections for use by replication.

### **Default**

4

### **Syntax**

Integer

### **Maximum Length**

11

Value Single-valued

## **ibm-slapdReplMaxErrors**

### **Description**

Limit to allowed errors per replication agreement. A value of 0 means there is an unlimited number of errors. The value is dynamic.

### **Default**

0

### **Syntax**

Integer

### **Maximum Length**

11

Value Single-valued

## **ibm-slapdReplicaSubtree**

### **Description**

Identifies the DN of a replicated subtree

### **Syntax**

DN

### **Maximum Length**

1000

Value Single-valued

## **ibm-slapdSchemaAdditions**

### **Description**

The `ibm-slapdSchemaAdditions` attribute is used to identify explicitly which file holds new schema entries. This attribute is set by default to be `/etc/V3.modifiedschema`. If this attribute is not defined, the server reverts to using the last `ibm-slapdIncludeSchema` file as in previous releases.

Before Version 3.2, the last `includeSchema` entry in `slapd.conf` was the file to which any new schema entries were added by the server if it received an add request from a client. Normally the last `includeSchema` is the `V3.modifiedschema` file, which is an empty file installed just for this purpose.

**Note:** The name modified is misleading, for it only stores new entries. Changes to existing schema entries are made in their original files.

**Default**

/etc/V3.modifiedschema

**Syntax**

Directory string with case-exact matching

**Maximum Length**

1024

**Value** Single-valued

## ibm-slapdSchemaCheck

**Description**

Specifies the schema checking mechanism for the add/modify/delete operation. It must be specified as V2, V3, or V3\_lenient.

- V2 - Retain v2 and v2.1 checking. Recommended for migration purpose.
- V3 - Perform v3 checking.
- V3\_lenient - Not all parent object classes are needed. Only the immediate object class is needed when adding entries.

**Default**

V3\_lenient

**Syntax**

Directory string with case-insensitive matching

**Maximum Length**

10

**Value** Single-valued

## ibm-slapdSecurePort

**Description**

Specifies the TCP/IP port used for SSL connections. It cannot have the same value as ibm-slapdPort. (IP ports are unsigned, 16-bit integers in the range 1 - 65535.)

**Default**

636

**Syntax**

Integer

**Maximum Length**

5

**Value** Single-valued

## ibm-slapdSecurity

**Description**

Enables SSL and TLS connections. Must be none, SSL, SSLOnly, TLS, or SSLTLS.

- none - server listens on the non-SSL port only.
- SSL - server listens on both the SSL and the non-SSL ports.
- SSLOnly - server listens on the SSL port only.

- TLS - server listens on the TLS port only.
- SSLTLS - server listens on both the TLS and SSL ports.

**Default**

none

**Syntax**

Directory string with case-insensitive matching

**Maximum Length**

7

**Value** Single-valued

## **ibm-slapdServerBackend**

**Description**

Specifies whether this server loads a database or proxy backend.

**Syntax**

Directory string

**Maximum Length**

1000

**Value** Single-valued

## **ibm-slapdServerId**

**Description**

Identifies the server for use in replication.

**Syntax**

IA5 String with case-sensitive matching

**Maximum Length**

240

**Value** Single-valued

## **ibm-slapdSetenv**

**Description**

The server runs **putenv()** for all values of **ibm-slapdSetenv** at startup to modify the server runtime environment. Shell variables (like **%PATH%** or **\$LANG**) are not expanded.

**Default**

No preset default is defined.

**Syntax**

Directory string with case-exact matching

**Maximum Length**

2000

**Value** Multi-valued

## **ibm-slapdSizeLimit**

**Description**

The maximum number of entries to return from search, regardless of any size limit that might have been specified on the client search request

(Range = 0...). If a client has passed a limit, then the smaller value of the client values and the value read from the `ibmslapd.conf` file are used. If a client has not passed a limit and has bound as admin DN, the limit is considered unlimited. If the client has not passed a limit and has not bound as admin DN, then the limit is that which was read from the `ibmslapd.conf` file. 0 = unlimited.

**Default**

500

**Syntax**

Integer

**Maximum Length**

12

**Value** Single-valued

## ibm-slapdSortKeyLimit

**Description**

The maximum number of sort conditions (keys) that can be specified on a single search request. Range = 0.... If a client has passed a search request with more sort keys than the limit allows, and the sorted search control criticality is FALSE, then the server will honor the value read from the `ibmslapd.conf` file and ignore any sort keys encountered after the limit has been reached - searching and sorting will be performed. If a client has passed a search a request with more keys than the limit allows, and the sorted search control criticality is TRUE, then the server will return to the client with a return code of **adminLimitExceeded** - no searching or sorting will be performed.

**Default**

3

**Syntax**

cis

**Length**

11

**Count** Single

**Usage** directoryOperation

**User Modify**

Yes

**Access Class**

critical

**Objectclass**

ibm-slapdRdbmBackend

**Required**

No

## ibm-slapdSortSrchAllowNonAdmin

**Description**

Whether or not the server should allow non-administrator bind for sort on a search request. If the value read from the `ibmslapd.conf` file is FALSE, the server will process only those client requests submitted by a user with

administrator authority. If a client requests sort for a search operation, does not have administrator authority, and the value read from the `ibmslapd.conf` file for this attribute is `FALSE`, the server will return to the client with return code `insufficientAccessRights` - no searching or sorting will be performed.

**Default**

FALSE

**Syntax**

Boolean

**Length**

5

**Count** Single

**Usage** `directoryOperation`

**User Modify**

Yes

**Access Class**

critical

**Objectclass**

`ibm-slapdRdbmBackend`

**Required**

No

## **ibm-slapdSslAuth**

**Description**

Specifies the authentication type for the SSL connection, either `serverauth` or `serverclientauth`.

- `serverauth` - supports server authentication at the client. This is the default.
- `serverclientauth` - supports both server and client authentication.

**Default**

`serverauth`

**Syntax**

Directory string with case-insensitive matching

**Maximum Length**

16

**Value** Single-valued

## **ibm-slapdSslCertificate**

**Description**

Specifies the label that identifies the server Personal Certificate in the key database file. This label is specified when the server private key and certificate are created with the `gsk4ikm` application. If `ibm-slapdSslCertificate` is not defined, the default private key, as defined in the key database file, is used by the LDAP server for SSL connections.

**Default**

No preset default is defined.

**Syntax**

Directory string with case-exact matching

**Maximum Length**

128

**Value** Single-valued**ibm-slapdSslCipherSpec**

Specifies the method of SSL encryption for clients accessing the server. Must be set to one of the following:

*Table 10. Methods of SSL encryption*

| Attribute     | Encryption level   |
|---------------|--|
| TripleDES-168 | Triple DES encryption with a 168-bit key and a SHA-1 MAC |
| DES-56        | DES encryption with a 56-bit key and a SHA-1 MAC         |
| RC4-128-SHA   | RC4 encryption with a 128-bit key and a SHA-1 MAC        |
| RC4-128-MD5   | RC4 encryption with a 128-bit key and a MD5 MAC          |
| RC2-40-MD5    | RC4 encryption with a 40-bit key and a MD5 MAC           |
| RC4-40-MD5    | RC4 encryption with a 40-bit key and a MD5 MAC           |
| AES           | AES encryption   |

**Syntax**

IA5 String

**Maximum Length**

30

**ibm-slapdSslFIPsModeEnabled****Description**

If TRUE, specifies that the server will use the ICC version of GSKit ; if FALSE, specifies that the server will use the BSAFE version.

**Default**

Varies by platform

**Syntax**

Boolean

**Maximum Length**

5

**Value** Single-valued**ibm-slapdSslFIPsProcessingMode****Description**

Specifies that the server will operate in FIPS mode. (Requires `ibm-slapdSslFIPsModeEnabled` to be true.)

**Default**  
False

**Syntax**  
Boolean

**Maximum Length**  
5

**Value** Single-valued

## ibm-slapdSslKeyDatabase

### Description

Specifies the file path to the LDAP server SSL key database file. This key database file is used for handling SSL connections from LDAP clients, as well as for creating secure SSL connections to replica LDAP servers.

On Windows 2000, Windows NT, or Windows XP operating systems, forward slashes are allowed, and a leading slash not preceded by a drive specifier (D:) is assumed to be rooted at the installation directory (that is, /etc/key.kdb = D:\Program Files\IBM\ldap\etc\key.kdb).

**Default**  
/etc/key.kdb

**Syntax**  
Directory string with case-exact matching

**Maximum Length**  
1024

**Value** Single-valued

## ibm-slapdSslKeyDatabasePW

### Description

Specifies the password associated with the LDAP server SSL key database file, as specified on the `ibm-slapdSslKeyDatabase` parameter. If the LDAP server key database file has an associated password stash file, then the `ibm-slapdSslKeyDatabasePW` parameter can be omitted, or set to none.

**Note:** The password stash file must be located in the same directory as the key database file and it must have the same file name as the key database file, but with an extension of `.sth` instead of `.kdb`.

**Default**  
none

**Syntax**  
Binary

**Maximum Length**  
128

**Value** Single-valued

## ibm-slapdSslKeyRingFile

### Description

Path to the LDAP server's SSL key database file. This key database file is used for handling SSL connections from LDAP clients, as well as for



creating secure SSL connections to replica LDAP servers. On Windows, forward slashes are allowed, and a leading slash not preceded by a drive specifier is assumed to be rooted at the installation directory (for example, /etc/key.kdb = c:\Program Files\IBM\ldap\etc\key.kdb).

**Default**

key.kdb

**Syntax**

Directory String with case-sensitive matching

**Maximum Length**

1024

**Value** Single-valued

## **ibm-slapdSslKeyRingFilePW**

**Description**

Specifies the password associated with the LDAP server's SSL key database file, as specified on the `ibm-slapdSslKeyRingFile` parameter. If the LDAP server's key database file has an associated password stash file, then the `ibm-slapdSslKeyRingFilePW` parameter can be omitted or set to `ibm-slapdSslKeyRingFilePW = none`.

**Note:** The password stash file must be located in the same directory as the key database file and it must have the same file name as the key database file, but with an extension of `.sth` instead of `.kdb`.

**Default**

None.

**Syntax**

Directory string

**Maximum Length**

128

**Value** Single-valued

## **ibm-slapdStartupTraceEnabled**

**Description**

Specifies whether trace information is to be collected at server startup. Must be TRUE or FALSE.

**Default**

FALSE

**Syntax**

Boolean

**Maximum Length**

5

**Value** Single-valued

## **ibm-slapdSuffix**

**Description**

Specifies a naming context to be stored in this backend.

**Note:** This has the same name as the object class.

**Default**

No preset default is defined.

**Syntax**

DN

**Maximum Length**

1000

**Value** Multi-valued

## **ibm-slapdSupportedWebAdmVersion**

**Description**

This attribute defines the earliest version of the Web Administration Tool that supports this server of cn=configuration.

**Default**

**Syntax**

Directory String

**Maximum Length**

**Value** Single-valued

## **ibm-slapdTimeLimit**

**Description**

Specifies the maximum number of seconds to spend on a search request, regardless of any time limit that might have been specified on the client request. If a client has passed a limit, then the smaller value of the client values and the value read from **ibmslapd.conf** are used. If a client has not passed a limit and has bound as admin DN, the limit is considered unlimited. If the client has not passed a limit and has not bound as admin DN, then the limit is that which was read from the **ibmslapd.conf** file. 0 = unlimited.

**Default**

900

**Syntax**

Integer

**Maximum Length**

**Value** Single-valued

## **ibm-slapdTraceMessageLevel**

**Description**

Sets the debug message level. Use the command `ibmslapd -h ?` to see the available levels.

**Default**

0xFFFF (or 65535)

**Syntax**

Directory string

**Maximum Length**

16

**Value** Single-valued

## **ibm-slapdTraceMessageLog**

### **Description**

File path or device on the ibmslapd host computer to which LDAP C API and Debug macro messages will be written. On Windows, forward slashes are allowed, and a leading slash not preceded by a drive letter is assumed to be rooted at the installation directory (for example, /tmp/tracemsg.log = C:\Program Files\IBM\ldap\tmp\tracemsg.log).

### **Default**

Varies by platform

### **Syntax**

Directory string

### **Maximum Length**

1024

**Value** Single-valued

## **ibm-slapdTransactionEnable**

### **Description**

If the transaction plug-in is loaded but `ibm-slapdTransactionEnable` is set to `FALSE`, the server rejects all `StartTransaction` requests with the response `LDAP_UNWILLING_TO_PERFORM`.

### **Default**

TRUE

### **Syntax**

Boolean

### **Maximum Length**

5

**Value** Single-valued

## **ibm-slapdUseProcessIdPw**

### **Description**

If set to `TRUE`, the server ignores the `ibm-slapdDbUserID` and the `ibm-slapdDbUserPW` attributes and uses its own process credentials to authenticate to DB2.

### **Default**

FALSE

### **Syntax**

Boolean

### **Maximum Length**

5

**Value** Single-valued

## **ibm-slapdVersion**

### **Description**

Directory Server version Number

**Default**  
6.0

**Syntax**  
Directory String with case-sensitive matching

**Maximum Length**  
1024

**Value** Single-valued

## **ibm-slapdWriteTimeout**

**Description**  
Specifies a timeout value in seconds for blocked writes. When the time limit is reached the connection will be dropped.

**Default**  
120

**Syntax**  
Integer

**Maximum Length**  
1024

**Value** Single-valued

## **ids-instanceDesc**

**Description**  
A description of what this particular directory server instance is to be used for. This attribute is used in the Server Instance Repository LDIF file and **not** in the `ibmslapd.conf` file.

**Syntax**  
Directory string

**Maximum Length**  
256

**Value** Single-valued

## **ids-instanceLocation**

**Description**  
File path or device on server host computer to which the directory server instance `idsslapd-instance_name` directory is located. On Windows forward slashes are allowed and a leading slash not preceded by a drive letter is assumed to be rooted at the installation directory for example, `/tmp/idsslapd-server1 = C:\Program Files\IBM\LDAP\tmp\idsslapd-server1`). This attribute is used in the Server Instance Repository LDIF file and **not** in the `ibmslapd.conf` file.

**Syntax**  
Directory string

**Maximum Length**  
1024

**Value** Single-valued

## **ids-instanceVersion**

**Description**

IBM Slapd version Number for the directory server instance.

**Syntax**

Directory string

**Maximum Length**

1024

**Value** Single-valued

## **objectClass**

**Description**

The values of the objectClass attribute describe the kind of object that an entry represents.

**Syntax**

Directory string

**Maximum Length**

128

**Value** Multi-valued



---

## Appendix Q. Support information

This section describes the following options for obtaining support for IBM products:

- “Searching knowledge bases”
- “Obtaining fixes”
- “Contacting IBM Software Support” on page 266

---

### Searching knowledge bases

If you have a problem with your IBM software, you want it resolved quickly. Begin by searching the available knowledge bases to determine whether the resolution to your problem is already documented.

#### Search the information center on your local system or network

IBM provides extensive documentation that can be installed on your local computer or on an intranet server. You can use the search function of this information center to query conceptual information, instructions for completing tasks, reference information, and support documents.

#### Search the Internet

If you cannot find an answer to your question in the information center, search the Internet for the latest, most complete information that might help you resolve your problem. To search multiple Internet resources for your product, expand the product folder in the navigation frame to the left and select **Web search**. From this topic, you can search a variety of resources including:

- IBM technotes
- IBM downloads
- IBM Redbooks
- IBM developerWorks
- Forums and newsgroups
- Google

---

### Obtaining fixes

A product fix might be available to resolve your problem. You can determine what fixes are available for your IBM software product by checking the product support Web site:

1. Go to the IBM Software Support Web site (<http://www.ibm.com/software/support>).
2. Under **Products A - Z**, select your product name. This opens a product-specific support site.
3. Under **Self help**, follow the link to **All Updates**, where you will find a list of fixes, fix packs, and other service updates for your product. For tips on refining your search, click **Search tips**.
4. Click the name of a fix to read the description and optionally download the fix.

To receive weekly e-mail notifications about fixes and other news about IBM products, follow these steps:

1. From the support page for any IBM product, click **My support** in the upper-right corner of the page.
2. If you have already registered, skip to the next step. If you have not registered, click register in the upper-right corner of the support page to establish your user ID and password.
3. Sign in to **My support**.
4. On the My support page, click **Edit profiles** in the left navigation pane, and scroll to **Select Mail Preferences**. Select a product family and check the appropriate boxes for the type of information you want.
5. Click **Submit**.
6. For e-mail notification for other products, repeat Steps 4 and 5.

For more information about types of fixes, see the *Software Support Handbook* (<http://techsupport.services.ibm.com/guides/handbook.html>).

---

## Contacting IBM Software Support

IBM Software Support provides assistance with product defects.

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus, and Rational products, as well as DB2 and WebSphere products that run on Windows or UNIX operating systems), enroll in Passport Advantage in one of the following ways:
  - **Online:** Go to the Passport Advantage Web page ([http://www.lotus.com/services/passport.nsf/WebDocs/Passport\\_Advantage\\_Home](http://www.lotus.com/services/passport.nsf/WebDocs/Passport_Advantage_Home)) and click **How to Enroll**
  - **By phone:** For the phone number to call in your country, go to the IBM Software Support Web site (<http://techsupport.services.ibm.com/guides/contacts.html>) and click the name of your geographic region.
- For IBM eServer software products (including, but not limited to, DB2 and WebSphere products that run in zSeries, pSeries, and iSeries environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web page (<http://www.ibm.com/servers/eserver/techsupport.html>).

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States or, from other countries, go to the contacts page of the IBM Software Support Handbook on the Web (<http://techsupport.services.ibm.com/guides/contacts.html>) and click the name of your geographic region for phone numbers of people who provide support for your location.

Follow the steps in this topic to contact IBM Software Support:

1. Determine the business impact of your problem.
2. Describe your problem and gather background information.



3. Submit your problem to IBM Software Support.

## Determine the business impact of your problem

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem you are reporting. Use the following criteria:

|                   |  |
|-------------------|--|
| <b>Severity 1</b> | <b>Critical</b> business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution. |
| <b>Severity 2</b> | <b>Significant</b> business impact: The program is usable but is severely limited.   |
| <b>Severity 3</b> | <b>Some</b> business impact: The program is usable with less significant features (not critical to operations) unavailable.                                      |
| <b>Severity 4</b> | <b>Minimal</b> business impact: The problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented.               |

## Describe your problem and gather background information

When explaining a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be re-created? If so, what steps led to the failure?
- Have any changes been made to the system? (For example, hardware, operating system, networking software, and so on.)
- Are you currently using a workaround for this problem? If so, please be prepared to explain it when you report the problem.

## Submit your problem to IBM Software Support

You can submit your problem in one of two ways:

- **Online:** Go to the "Submit and track problems" page on the IBM Software Support site (<http://www.ibm.com/software/support/probsub.html>). Enter your information into the appropriate problem submission tool.
- **By phone:** For the phone number to call in your country, go to the contacts page of the IBM Software Support Handbook on the Web ([techsupport.services.ibm.com/guides/contacts.html](http://techsupport.services.ibm.com/guides/contacts.html)) and click the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround for you to implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM product support Web pages daily, so that other users who experience the same problem can benefit from the same resolutions.

For more information about problem resolution, see Searching knowledge bases and Obtaining fixes.



---

## Appendix R. 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 MU5A46  
11301 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.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

---

## Trademarks

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

AIX  
DB2  
IBM  
iSeries  
pSeries  
RS/6000  
S/390  
SecureWay  
SP

Tivoli  
WebSphere  
xSeries  
z/OS  
zSeries

Intel, Intel Inside (logos), MMX™ and Pentium® are trademarks of Intel Corporation in the United States, other countries, or both.

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®, MS-DOS, 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.

Linux is a 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.



---

# Index

## A

- administrator DN
  - changing 136
  - setting
    - Configuration Tool 126
    - idsdnpw command 136
    - Instance Administration Tool 112
- administrator password
  - setting
    - Configuration Tool 127
    - Instance Administration Tool 112
- AdminTool 86
- AIX
  - command line 72
  - DB2 version provided 11
  - DB2 versions supported 11
  - disk space requirements 167
  - installp installation 72
  - SMIT installation 69
  - supported versions 11
  - system requirements 11
- application server
  - installing manually 183
  - starting 149
- ASCII characters
  - 33 to 126 189
  - allowable in encryption seed string 189

## B

- backing up database
  - Configuration Tool 135
  - idsdbback command 148
- books, IBM Tivoli Directory Server 6.0
  - accessing online x
  - list of ix
  - ordering x
- bundlers, information for 191

## C

- change log
  - disabling
    - idsucfgchglg 142
  - enabling
    - idscfgchglg 141
- change log, disabling
  - Configuration Tool 129
- change log, enabling
  - Configuration Tool 129
- changing database owner password
  - Configuration Tool 128
  - idscfgdb command 139
- character set
  - IANA 198
- client
  - overview 4
  - removing 151
- code page, DB2 198

- commands
  - idscfgchglg 141
  - idscfgdb 138
  - idscfgsch 146
  - idscfgsuf 143
  - idsdnpw 136
  - idsicrt 116
  - idsidrop 123
  - idsilist 122
  - idssethost 119
  - idssetport 120
  - idsucfgchglg 142
  - idsucfgdb 140
  - idsucfgsch 146
  - idsucfgsuf 144
- configuration
  - after installation 125
  - embedded version of WebSphere
    - Application Server - Express 183
  - idsxcfg 125
  - overview 7, 125
  - planning
    - database 171
    - using command-line utilities 136
- configuration schema 203
- Configuration Tool 125
- configuring database
  - Configuration Tool 127
- cryptography, two-way, synchronizing 177
- customer support
  - see Software Support 266

## D

- database
  - configuration planning 171
    - access permissions 171
    - code page 171
    - security requirements 171
    - structure 171
    - type of data 171
  - configuring
    - Configuration Tool 127
    - idscfgdb command 138
    - Instance Administration Tool 112
  - unconfiguring
    - Configuration Tool 128
    - idsucfgdb 140
- database instance owner
  - creating 48, 173
  - requirements 173
- database name 127
- database owner
  - creating 48, 173
  - requirements 173
- database owner password, changing
  - Configuration Tool 128
  - idscfgdb command 139
- database, backing up
  - Configuration Tool 135

- database, backing up (*continued*)
  - idsdbback command 148
- database, configuring
  - Configuration Tool 127
- database, optimizing
  - Configuration Tool 135
- database, optimizng
  - idsrunstats command 148
- database, restoring
  - Configuration Tool 135
  - idsdbrestore command 148
- DB2
  - code page 198
  - overview 6
  - DB2 versions provided
    - AIX 11
    - HP-UX 21
    - iSeries Linux 17
    - overview 6
    - pSeries Linux 17
    - Solaris 19
    - Windows 10
    - xSeries Linux 14
    - zSeries Linux 16
  - DB2 versions supported
    - AIX 11
    - HP-UX 21
    - iSeries Linux 17
    - pSeries Linux 17
    - Solaris 19
    - Windows 10
    - xSeries Linux 14
    - zSeries Linux 16
- directory server instance
  - adding a schema file 146
  - changing TCP/IP settings for 114
  - configuring a database 138
  - content on AIX, Linux, Solaris, HP-UX 180
  - content on Windows 179
  - contents of 179
  - creating 116
  - creating with Instance Administration Tool 110
  - deleting 115
  - disabling changelog 142
  - enabling changelog 141
  - files 179
  - listing 122
  - overview 6
  - removing 123
  - removing a schema file 146
  - starting 149
  - unconfiguring database 140
  - viewing information about 115
- directory server instance owner
  - creating 48, 173
  - requirements 173
- Directory Services Markup Language
  - configuring 193
  - documentation 193

- Directory Services Markup Language
  - (continued)
  - installing 193
- directory structure
  - client InstallShield GUI installation files
    - AIX 164
    - Linux 164
    - Solaris 164
    - Windows 163
  - client operating system utility installation files
    - AIX 165
    - HP-UX 165
    - Linux 165
    - Solaris 165
  - iso, zip, tar files 157
  - server InstallShield GUI installation files
    - AIX 157
    - Linux 158
    - Solaris 159
    - Windows 157
  - server operating system utility installation files
    - AIX 159
    - HP-UX 163
    - Linux 160
    - Solaris 162
- disk space requirements
  - AIX 167
  - HP-UX 168
  - Linux 168
  - Solaris 168
  - Windows 167
- DSML
  - configuring 193
  - documentation 193
  - installing 193

## E

- embedded version of WebSphere
  - Application Server - Express
    - configuration 183
    - default ports 185
    - installing manually 183
    - migrating using idswmigr 43
    - overview 5
    - ports, default 185
    - starting 149
    - uninstalling 183
    - upgrading 43
    - using HTTPS 186
- encryption seed
  - specifying 41, 110, 117, 134
- encryption seed string
  - ASCII characters allowed in 189
- exporting LDIF data
  - Configuration Tool 133
  - idsdb2ldif 148

## F

- fixes, obtaining 265

- full server
  - overview 5

## G

- GSKit
  - installing
    - AIX 74
    - HP-UX 97
    - Linux 80
    - Solaris 90
  - installing on Linux 80
  - installing silently
    - Windows 107
  - overview 6
  - removing
    - AIX 75
    - HP-UX 97
    - Linux 81
    - Solaris 90
  - removing silently
    - Windows 108
  - setting up for CMS key databases 201
  - version provided 6

## H

- HP-UX
  - before installing 91
  - DB2 version provided 21
  - DB2 versions supported 21
  - disk space requirements 168
  - mounting CD 93
  - setting kernel configuration parameters 92
  - supported versions 21
  - system requirements 21
  - unmounting CD 94

## I

- IANA 198
- IBM Directory Server 4.1
  - migration from
    - AIX systems 31
    - non-AIX systems 29
- IBM Directory Server 5.1
  - migration from
    - AIX systems 31
    - non-AIX systems 29
- IBM Tivoli Directory Integrator
  - for idssupport tool 51, 53, 72, 74, 80, 86, 89, 96
  - for log management tool 51, 53, 72, 74, 80, 86, 89, 96
  - for SNMP 51, 53, 72, 74, 80, 86, 89, 96
  - for use with IBM Tivoli Directory Server 11, 12, 15, 17, 19, 21, 22
  - installation instructions 11, 12, 15, 17, 19, 21, 22
  - where to acquire 11, 12, 15, 17, 19, 21, 22
- IBM Tivoli Directory Server 5.2
  - migration from 29

- idscfgchglg 141
- idscfgdb 138
- idscfgsch 146
- idscfgsuf 143
- idsdbback command 148
- idsdbrestore command 148
- idsdnpw 136
- idsicrt 116
- idsidrop 123
- idsilist 122
- idsimigr utility
  - syntax 40
  - using 40
- idsldap group 55
- idsldap user
  - requirements 55
- idslink utility
  - links created by 58
  - using 57
- idsrmlink utility 62
- idsrunstats command 148
- idssethost 119
- idssetport 120
- idsslapd command 149
- idssupport tool
  - requirement for IBM Tivoli Directory Integrator 51, 53, 72, 74, 80, 86, 89, 96
- idsucfgchglg 142
- idsucfgdb 140
- idsucfgsch 146
- idsucfgsuf 144
- idswmigr utility
  - location 24
  - syntax 43
  - using 43
- idsxcfg 125
- importing LDIF data
  - Configuration Tool 132
  - idsldif2db 148
- information centers, searching to find
  - software problem resolution 265
- installation
  - AdminTool 86
  - AIX utilities 65
  - checklist 1
  - embedded version of WebSphere
    - Application Server - Express 183
  - HP-UX 96
  - installp 72
  - InstallShield GUI 47
    - AIX, Linux, or Solaris 52
    - before installing 47
    - language packs 45
    - Windows 48
  - language packs
    - InstallShield GUI 45
  - Linux 77
  - manual
    - AIX 65
    - HP-UX 91
    - Linux 77
    - Solaris 83
    - Windows 99
  - overview 4
  - pkgadd 87
  - quick path 1



- installation (*continued*)
  - silent 99
  - SMIT 69
  - Solaris 83
  - Solaris command line 87
  - Web Administration Tool into WebSphere 187
- installation packages
  - AIX 66
  - HP-UX 94
  - Linux 77
  - Solaris 85
- installation path
  - AIX, Linux, Solaris, HP-UX 52, 56
  - default, Windows 49
- InstallShield GUI
  - before installing 47
  - installing language packs 45
  - overview 47
- instance
  - directory server
    - creating 110, 116
    - listing 122
    - removing 123
- Instance Administration Tool
  - description 109
  - starting 109
- instance, directory server
  - changing TCP/IP settings for 114
  - creating with Instance Administration Tool 110
  - deleting 115
  - overview 6
  - viewing information about 115
- Internet, searching to find software problem resolution 265
- iSeries Linux
  - DB2 version provided 17
  - DB2 versions supported 17
  - supported versions 17
  - system requirements 17
- iso file, IBM Tivoli Directory Server 3

## J

- Java client
  - overview 4

## K

- kernel configuration parameters
  - HP-UX 92
  - Solaris 83
- knowledge bases, searching to find software problem resolution 265

## L

- language packs
  - installing silently 101
  - installing with InstallShield GUI 45
  - uninstalling with InstallShield GUI 152
- languages supported 46
- LDIF data, exporting
  - Configuration Tool 133

- LDIF data, exporting (*continued*)
  - idsdb2ldif 148
- LDIF data, importing
  - Configuration Tool 132
  - idsldif2db 148
- LDIF data, validating 133
- Linux
  - disk space requirements 168
- loading sample database 195
- locale 198
- log management tool
  - requirement for IBM Tivoli Directory Integrator 51, 53, 72, 74, 80, 86, 89, 96

## M

- migbkup utility
  - location 24
- migration
  - client information 23
  - from IBM Directory Server 4.1 or 5.1
    - AIX systems 31
    - non-AIX systems 29
  - from IBM Tivoli Directory Server 5.2 29
  - from SecureWay Directory 24
  - high-level steps 28
  - overview 3, 23
  - replicating environment 180
  - Web Administration Tool 43
- migration utilities
  - idsimigr 40
  - idswmigr 43
  - location 24
- mounting CD
  - HP-UX 93

## N

- national language characters 197

## O

- operating systems, requirements on all 9
- optimizing database
  - Configuration Tool 135
- optimizing database
  - idsrunstats command 148

## P

- package dependencies, HP-UX 94
- package dependencies, Solaris 85
- packages, installation
  - AIX 66
  - HP-UX 94
  - Linux 77
  - Solaris 85
- password for database owner, changing
  - Configuration Tool 128
  - idscfgdb command 139
- pkgadd 87

- problem determination
  - describing problem for IBM Software Support 267
  - determining business impact for IBM Software Support 267
  - submitting problem to IBM Software Support 267
- proxy server
  - overview 5
- pSeries Linux
  - DB2 version provided 17
  - DB2 versions supported 17
  - supported versions 17
  - system requirements 17
- publications, IBM Tivoli Directory Server 6.0
  - accessing online x
  - list of ix
  - ordering x

## R

- removing
  - client 151
  - IBM Tivoli Directory Server
    - AIX 153
    - HP-UX 156
    - InstallShield GUI 151
    - Linux 154
    - operating system utilities 153
    - Solaris 155
  - language packs
    - InstallShield GUI 152
  - server 151
- requirements
  - AIX 11
  - HP-UX 21
  - iSeries Linux 17
  - pSeries Linux 17
  - Solaris 19
  - Windows 10
  - xSeries Linux 13
  - zSeries Linux 15
- requirements, client
  - memory 9
- requirements, server
  - memory 9
- restoring database
  - Configuration Tool 135
  - idsdbrestore command 148
- RS/6000 SP environment, installation on node 66

## S

- sample database, loading 195
- schema
  - configuration 203
- schema file
  - adding
    - Configuration Tool 131
    - idscfgsch 146
  - removing
    - Configuration Tool 131
    - idsucfgsch 146

- schema file, changing validation type 132
- SecureWay Directory
  - downloading 3.2.2 version 3, 24
  - migrating from 3.2.2 version 24
  - migrating replicating environment 180
- security
  - GSKit 6
  - SSL 6
- server
  - installation checklist 1
  - overview 4
  - removing 151
  - starting 149
- server utilities
  - idsbulkload 197
  - idscfgsuf 143
  - idsdb2ldif 197
  - idslidif2db 197
  - idssethost 119
  - idssetport 120
  - idsucfgsuf 144
- servers
  - types administered by Web Administration Tool 5
- setting system variables
  - AIX 75
- silent installation
  - checking log file 102
  - checking Windows registry 102
  - client options file 104
  - language packs options file 104
  - overview 99
  - return codes 102
  - server options file 103
  - using 100
  - verifying 102
- silent uninstallation
  - language packs options file 107
  - overview 105
  - server options file 106
  - using 105
- SMIT installation 69
- SNMP
  - requirement for IBM Tivoli Directory Integrator 51, 53, 72, 74, 80, 86, 89, 96
- Software Support
  - contacting 266
  - describing problem for IBM Software Support 267
  - determining business impact for IBM Software Support 267
  - submitting problem to IBM Software Support 267
- Solaris
  - AdminTool 86
  - command line 87
  - DB2 version provided 19
  - DB2 versions supported 19
  - disk space requirements 168
  - supported versions 19
  - system requirements 19
- SSL 6
- starting Web Administration Tool 149
- stopping Web Administration Tool 150

- suffix
  - adding
    - idscfgsuf 143
  - removing
    - idsucfgsuf 144
- suffix, adding
  - Configuration Tool 130
- suffix, removing 130
- swinstall 96
- synchronizing two-way cryptography 177
- system requirements
  - AIX 11
  - HP-UX 21
  - iSeries Linux 17
  - pSeries Linux 17
  - Solaris 19
  - Windows 10
  - xSeries Linux 13
  - zSeries Linux 15
- system requirements, client memory 9
- system requirements, server memory 9
- system variables, setting
  - AIX 75

## T

- tar file, IBM Tivoli Directory Server 3

## U

- unconfiguring
  - database 128
- uninstallation
  - silent 105
- uninstalling
  - client 151
  - embedded version of WebSphere Application Server - Express 184
  - IBM Tivoli Directory Server
    - operating system utilities 153
  - language packs 152
  - server 151
- unmounting CD
  - HP-UX 94
- UTF-8 197
- utilities
  - command line
    - idscfgchglg 141
    - idscfgddb 138
    - idscfgsch 146
    - idscfgsuf 143
    - idsdnpw 136
    - idsicrt 116
    - idsidrop 123
    - idsilist 122
    - idsimigr 40
    - idslink 57
    - idsrmlink 62
    - idssethost 119
    - idssetport 120
    - idsucfgchglg 142
    - idsucfgddb 140
    - idsucfgsch 146

- utilities (*continued*)
  - command line (*continued*)
    - idsucfgsuf 144
    - idswmigr 43
- utilities, server
  - idsbulkload 197
  - idsdb2ldif 197
  - idslidif2db 197

## V

- validating LDIF data 133

## W

- Web Administration Tool
  - installing into WebSphere 187
  - migrating using idswmigr 43
  - overview 5
  - starting 149
  - stopping 150
  - types of servers administered by 5
- WebSphere, installing Web Administration Tool into 187
- Windows
  - DB2 version provided 10
  - DB2 versions supported 10
  - disk space requirements 167
  - supported versions 10
  - system requirements 10

## X

- xSeries Linux
  - DB2 version provided 14
  - DB2 versions supported 14
- xSeries Linux supported versions 13
- xSeries Linux system requirements 13

## Z

- zip file, IBM Tivoli Directory Server 3
- zSeries Linux
  - DB2 version provided 16
  - DB2 versions supported 16
  - supported versions 15
  - system requirements 15





Printed in USA

SC32-1673-00

