IBM Tivoli Directory Server Messages and Codes for z/OS
# Contents

### Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>v</td>
<td></td>
</tr>
</tbody>
</table>

### About this document

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>v</td>
<td></td>
</tr>
<tr>
<td>vii</td>
<td></td>
</tr>
</tbody>
</table>

#### Intended audience

| v  |
| vii |

#### How to use this document

| vii |

#### Conventions used in this document

| vii |

#### Where to find more information

| vii |

### Softcopy publications

| viii |

### To request copies of IBM publications

| viii |

### IBM systems center publications

| viii |

#### Using LookAt to look up message explanations

| viii |

#### The z/OS Basic Skills Information Center

| ix |

### How to send your comments to IBM

| xi |

#### If you have a technical problem

| xi |

### Summary of changes

| xiii |

#### Changes made in z/OS Version 1 Release 13

| xiii |

#### Changes made in z/OS Version 1 Release 12

| xiv |

#### Changes made in z/OS Version 1 Release 11

| xv |

### Chapter 1. LDAP server and ldif2ds messages (1000)

| 1 |

#### LDAP server messages

| 1 |

#### ldif2ds utility messages

| 94 |

### Chapter 2. Utility messages (2000)

| 117 |

### Chapter 3. TDBM messages (3000)

| 139 |

### Chapter 4. LDBM messages (6000)

| 157 |

### Chapter 5. GDBM, advanced replication, and ldapdiff messages (8000)

| 175 |

#### GDBM backend messages

| 175 |

#### Advanced replication messages

| 176 |

#### ldapdiff utility messages

| 211 |

### Chapter 6. Return and reason codes

| 233 |

#### Changed return codes

| 233 |

#### Return codes

| 233 |

#### Reason codes

| 237 |

### Appendix. Accessibility

| 337 |

#### Using assistive technologies

| 337 |

#### Keyboard navigation of the user interface

| 337 |

#### z/OS information

| 337 |

### Notices

| 339 |

#### Policy for unsupported hardware

| 340 |

#### Trademarks

| 340 |

### Bibliography

| 343 |

#### IBM z/OS Security Server publications

| 343 |

#### IBM Tivoli Directory Server for z/OS

| 343 |

#### IBM C/C++ language publications

| 343 |

#### IBM DB2 publications

| 343 |

#### IBM z/OS Cryptographic Service publications

| 343 |

#### Other IBM publications

| 343 |

### Index

| 345 |

© Copyright IBM Corp. 2010, 2011
Tables

1. LDAP server return codes .................................. 233
About this document

This document supports z/OS® (5694-A01) and the LDAP server. The LDAP server supports Lightweight Directory Access Protocol (LDAP), part of IBM Tivoli Directory Server for z/OS (IBM TDS), and runs as a stand-alone daemon. It is based on a client/server model that provides client access to an LDAP server. The LDAP server provides an easy way to maintain directory information in a central location for storage, updating, retrieval, and exchange.

This document includes the messages and reason codes produced by the Lightweight Directory Access Protocol (LDAP) server.

Intended audience

This document is intended for anyone who uses the LDAP server and wants to know what caused a message to be displayed and what corrective action, if any, needs to be taken.

How to use this document

Messages are generally arranged in alphanumeric order by message identifier.

By using the message identifier, you might find the index helpful in finding the message itself.

Conventions used in this document

This document may use the following typographic conventions:

**Bold**

*Bold* words or characters represent API names, attributes, status codes, environment variables, parameter values, and system elements that you must enter into the system literally, such commands, options, or path names.

*Italic*

*Italic* words or characters represent values for variables that you must supply.

**Example Font**

Examples and information displayed by the system appear in constant width type style.

[]

Brackets enclose optional items in format and syntax descriptions.

{}

Braces enclose a list from which you must choose an item in format and syntax descriptions.

| |

A vertical bar separates items in a list of choices.

< >

Angle brackets enclose the name of a key on the keyboard.

...

Horizontal ellipsis points indicate that you may repeat the preceding item one or more times.

\

A backslash is used as a continuation character when entering commands from the shell that exceed one line (255 characters). If the command exceeds one line, use the backslash character \ as the last nonblank character on the line to be continued, and continue the command on the next line.

Where to find more information

Where necessary, this document references information in other documents. For complete titles and order numbers for all elements of z/OS, see [z/OS Information Roadmap, SA22-7500](https://www.ibm.com/). For a list of titles and order numbers of the documents that are useful for IBM® Tivoli® Directory Server for z/OS, see [Bibliography](https://www.ibm.com/).
Softcopy publications

The IBM Tivoli Directory Server library is available on the following DVD softcopy collection in both BookManager® and Portable Document Format (PDF) files. The collection includes Softcopy Reader, which is a program that enables you to view the BookManager files. You can view or print the PDF files with an Adobe Reader.

SK3T-4271   

**z/OS Version 1 Release 13 and Software Products DVD Collection**

This collection contains the documents for z/OS Version 1 Release 13 and the libraries for multiple releases of more than 400 z/OS-related software products, on DVD.

The softcopy z/OS publications are also available for web browsing and for viewing or printing PDFs by using:

http://www.ibm.com/servers/eserver/zseries/zos/bkserv

To request copies of IBM publications

Direct your request for copies of any IBM publication to your IBM representative or to the IBM branch office serving your locality.

There is also a toll-free customer support number (1-800-879-2755) available Monday through Friday from 8:30 a.m. through 5:00 p.m. Eastern Time. You can use this number to:

• Order or inquire about IBM publications
• Resolve any software manufacturing or delivery concerns
• Activate the program reorder form to provide faster and more convenient ordering of software updates

IBM systems center publications

IBM systems centers produce documents known as IBM Redbooks® that can help you set up and use IBM Tivoli Directory Server for z/OS. See the IBM Redbooks site at http://www.redbooks.ibm.com/.

These documents have not been subjected to any formal review nor have they been checked for technical accuracy, but they represent current product understanding (at the time of their publication) and provide valuable information about a wide range of IBM Tivoli Directory Server for z/OS topics. They are not shipped with IBM Tivoli Directory Server for z/OS; you must order them separately.

Using LookAt to look up message explanations

LookAt is an online facility that lets you look up explanations for most of the IBM messages you encounter, as well as for some system abends and codes. Using LookAt to find information is faster than a conventional search because in most cases LookAt goes directly to the message explanation.

You can use LookAt from these locations to find IBM message explanations for z/OS elements and features, z/VM®, z/VSE, and Clusters for AIX® and Linux:

• The Internet. You can access IBM message explanations directly from the LookAt Web site at www.ibm.com/servers/eserver/zseries/zos/bkserv/lookat/

• Your z/OS TSO/E host system. You can install code on your z/OS systems to access IBM message explanations using LookAt from a TSO/E command line (for example: TSO/E prompt, ISPF, or z/OS UNIX System Services).

• Your Microsoft Windows workstation. You can install LookAt directly from the z/OS and Software Products DVD Collection (SK3T-4271) and use it from the resulting Windows graphical user interface (GUI). The command prompt (also known as the DOS > command line) version can still be used from the directory in which you install the Windows version of LookAt.
Your wireless handheld device. You can use the LookAt Mobile Edition from www.ibm.com/servers/eserver/zseries/zos/bkserv/lookat/lookatm.html with a handheld device that has wireless access and an Internet browser.

You can obtain code to install LookAt on your host system or Microsoft Windows workstation from:
- The z/OS and Software Products DVD Collection (SK3T-4271).
- The LookAt Web site (click Download and then select the platform, release, collection, and location that suit your needs). More information is available in the LOOKAT.ME files available during the download process.

The z/OS Basic Skills Information Center

The z/OS Basic Skills Information Center is a Web-based information resource intended to help users learn the basic concepts of z/OS, the operating system that runs most of the IBM mainframe computers in use today. The Information Center is designed to introduce a new generation of Information Technology professionals to basic concepts and help them prepare for a career as a z/OS professional, such as a z/OS system programmer.

Specifically, the z/OS Basic Skills Information Center is intended to achieve the following objectives:
- Provide basic education and information about z/OS without charge
- Shorten the time it takes for people to become productive on the mainframe
- Make it easier for new people to learn z/OS.

To access the z/OS Basic Skills Information Center, open your Web browser to the following Web site, which is available to all users (no login required): [http://publib.boulder.ibm.com/infocenter/zos/basics/index.jsp](http://publib.boulder.ibm.com/infocenter/zos/basics/index.jsp)
How to send your comments to IBM

We appreciate your input on this publication. Feel free to comment on the clarity, accuracy, and completeness of the information or give us any other feedback that you might have.

Use one of the following methods to send us your comments:

1. Send an email to mhvrdfs@us.ibm.com
3. Mail the comments to the following address:
   IBM Corporation
   Attention: MHVRCFS Reader Comments
   Department H6MA, Building 707
   2455 South Road
   Poughkeepsie, NY 12601-5400
   U.S.A.
4. Fax the comments to us as follows:
   From the United States and Canada: 1+845+432-9405
   From all other countries: Your international access code +1+845+432-9405

Include the following information:
- Your name and address
- Your email address
- Your telephone or fax number
- The publication title and order number:
  IBM Tivoli Directory Server Messages and Codes for z/OS V1R13.0
  SA23-2262-01
- The topic and page number related to your comment
- The text of your comment.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you submit.

If you have a technical problem

Do not use the feedback methods listed above. Instead, do one of the following:
- Contact your IBM service representative
- Call IBM technical support
- Visit the IBM support portal at [http://www.ibm.com/systems/z/support/](http://www.ibm.com/systems/z/support/)
Summary of changes

This document contains terminology, maintenance, and editorial changes to improve consistency and retrievability. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

Changes made in z/OS Version 1 Release 13

This document contains information that was previously presented in IBM Tivoli Directory Server Messages and Codes for z/OS, SA23-2262-00, which supports z/OS Version 1 Release 12.

New information:

The following messages have been added:
- GLD1298E
- GLD1299I
- GLD1300E
- GLD1301E
- GLD1302E
- GLD1869W

The following reason codes have been added:
- R001108
- R001109
- R004203
- R004204
- R004205
- R004206
- R004207
- R004208
- R004209
- R004210
- R004211
- R010068
- R010069
- R010070
- R010071
- R010072
- R010073
- R010074

Changed information:

- The descriptions of LDAP reason codes within this publication have been updated to include response information or system action.
- The diagnostic traceback information within LDAP reason code messages has been updated to include the source code line number where the condition was detected.
- The following messages have been changed:
  - GLD1070E
  - GLD2401E
  - GLD3303E
The following reason codes have been changed:
  R006060
  R010029

Deleted information:
  The following message has been deleted:
    GLD1173E
  The following reason code has been deleted:
    R010063

Changes made in z/OS Version 1 Release 12

This document contains information that was previously presented in *IBM Tivoli Directory Server Administration and Use, SC23-5191-04*, which supports z/OS Version 1 Release 11.

New information:

The following messages have been added:

| GLD1280E | GLD1291E | GLD2436E | GLD8834W |
| GLD1281E | GLD1292E | GLD2437E | GLD8835E |
| GLD1282E | GLD1293E | GLD2438E | GLD8836E |
| GLD1283E | GLD1294E | GLD2439E | GLD8844E |
| GLD1284E | GLD1295E | GLD2440E | GLD8850E |
| GLD1285E | GLD1296E | GLD2441W | GLD8851E |
| GLD1286E | GLD1297E | GLD2442W | GLD8852E |
| GLD1287E | GLD2030E | GLD2443E | GLD8865E |
| GLD1288E | GLD2031E | GLD6053E | GLD8866E |
| GLD1289E | GLD2435E | GLD8829W | GLD8867E |
| GLD1290I |

The following reason codes have been added:

| R000150 | R002031 | R003140 | R004187 | R004201 |
| R001103 | R002032 | R003141 | R004188 | R004202 |
| R001104 | R002033 | R003142 | R004189 | R004211 |
| R001105 | R002034 | R003143 | R004191 | R006071 |
| R001106 | R002035 | R003144 | R004192 | R006072 |
| R001107 | R003130 | R003145 | R004193 | R008017 |
| R002022 | R003131 | R003146 | R004194 | R008018 |
| R002023 | R003132 | R003147 | R004195 | R008019 |
| R002024 | R003133 | R003148 | R004196 | R008020 |
| R002025 | R003134 | R003149 | R004197 | R008021 |
| R002026 | R003135 | R003150 | R004198 | R008022 |
| R002027 | R003136 | R003151 | R004199 | R008023 |
| R002028 | R003137 | R004184 | R004200 | R008024 |
| R002029 | R003138 | R004185 | R004201 | R008025 |
| R002030 | R003139 | R004186 |

Changed information:

  The following messages have been changed:
The following reason codes have been changed:
- R001102
- R002020

Changes made in z/OS Version 1 Release 11

This document contains information that was previously presented in IBM Tivoli Directory Server Administration and Use for z/OS, SC23-5191-03, which supports z/OS Version 1 Release 11.

This document is a refresh of Version 1 Release 11.

New information:
- The following messages have been added:
  - GLD1296I
  - GLD8502I
  - GLD8506I

Changes made in z/OS Version 1 Release 11

This document contains information that was previously presented in IBM Tivoli Directory Server Administration and Use for z/OS, SC23-5191-02, which supports z/OS Version 1 Release 10.

New information:

The following messages have been added:

```
GLD1254E GLD8516E GLD8566E GLD8633W GLD8820W
GLD1255E GLD8517I GLD8567E GLD8634I GLD8821E
GLD1256E GLD8518I GLD8568E GLD8635I GLD8822E
GLD1257E GLD8519E GLD8569I GLD8637I GLD8823E
GLD1258E GLD8520E GLD8570E GLD8639E GLD8824E
GLD1259I GLD8521E GLD8571I GLD8640F GLD8825E
GLD1260I GLD8522W GLD8572I GLD8642W GLD8826E
GLD1261E GLD8523E GLD8578W GLD8643E GLD8827E
GLD1262E GLD8524E GLD8579E GLD8644E GLD8828E
GLD1263I GLD8525E GLD8580L GLD8645E GLD8830E
GLD1264E GLD8526E GLD8581I GLD8647E GLD8831E
GLD1265E GLD8527W GLD8582I GLD8648E GLD8832E
GLD1266E GLD8528I GLD8583W GLD8649E GLD8833E
GLD1267E GLD8529I GLD8584E GLD8650I GLD8837I
GLD1268E GLD8530I GLD8586E GLD8651I GLD8838I
GLD1269A GLD8531I GLD8587E GLD8652I GLD8839W
GLD1270E GLD8532E GLD8588I GLD8653W GLD8840E
GLD1271E GLD8533E GLD8589E GLD8654I GLD8841E
GLD1272E GLD8534E GLD8590I GLD8797E GLD8842E
GLD1273I GLD8535E GLD8591E GLD8801E GLD8843E
GLD1274W GLD8536E GLD8592I GLD8802I GLD8845E
GLD1275W GLD8538E GLD8593E GLD8803I GLD8846E
GLD1276W GLD8539W GLD8594I GLD8804I GLD8847E
GLD1277W GLD8540W GLD8595E GLD8805I GLD8848E
```
The following reason codes have been added:

```
R000146 R010501 R010750 R010769 R010788
R000147 R010502 R010751 R010770 R010789
R000148 R010503 R010752 R010771 R010790
R000149 R010504 R010753 R010772 R010791
R004177 R010505 R010754 R010773 R010792
R004178 R010506 R010755 R010774 R010793
R004179 R010507 R010756 R010775 R010794
R004180 R010508 R010757 R010776 R010795
R004181 R010509 R010758 R010777 R010796
R004182 R010510 R010759 R010778 R010797
R004183 R010511 R010760 R010779 R010798
R006067 R010513 R010762 R010781 R010800
R006068 R010514 R010763 R010782 R010801
R006069 R010515 R010764 R010783 R010802
R006070 R010516 R010765 R010784 R010803
R001102 R010517 R010766 R010785 R010804
R010500 R010519 R010768 R010787
```

**Changed information:**

- The following reason codes have been changed:
  
  R000205  
  R004164  
  R006061  
  R006066

- The following messages have been changed:
  
  GLD1040E  
  GLD1158E  
  GLD1159E  
  GLD1257E  
  GLD2004I is now GLD2004D  
  GLD2262A  
  GLD2273R is now GLD2273D  
  GLD3342I  
  GLD3343E  
  GLD3344E
Deleted information:

The following messages have been deleted:

GLD2412A   GLD2422A
GLD2413A   GLD2423A
GLD2415A   GLD2430A
GLD2416A   GLD2431A
GLD2418A   GLD2432A
GLD2419A   GLD2433A
GLD2420I   GLD2434A
GLD2421I
Chapter 1. LDAP server and ldif2ds messages (1000)

This section lists the messages returned by the LDAP server and the ldif2ds utility.

### LDAP server messages

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GLD1001I</td>
<td>LDAP server version <strong>version.release</strong>, Service level <strong>level</strong>, Build date <strong>date</strong>, Time <strong>time</strong>.</td>
<td>The LDAP server with version, release, service level, build date, and build time indicated in the message is running.</td>
<td></td>
<td>The program continues.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
<td>LDAP</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td></td>
<td><strong>level</strong></td>
<td>Server service level</td>
<td></td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td></td>
<td><strong>date</strong></td>
<td>Server build date</td>
<td></td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td></td>
<td><strong>time</strong></td>
<td>Server build time</td>
<td></td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>GLD1002I</td>
<td>LDAP runtime version <strong>version.release</strong>, Service level <strong>level</strong>, Build date <strong>date</strong>, Time <strong>time</strong>.</td>
<td>The LDAP run time with version, release, service level, build date, and build time indicated in the message is running.</td>
<td></td>
<td>The program continues.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
<td>LDAP</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td></td>
<td><strong>date</strong></td>
<td>Runtime build date</td>
<td></td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>GLD1003I</td>
<td>LDAP server is starting.</td>
<td>The LDAP server is starting.</td>
<td></td>
<td>The program continues.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td></td>
<td><strong>date</strong></td>
<td>Runtime build date</td>
<td></td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>None.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>
GLD1004I  LDAP server is ready for requests.
Explanation: The LDAP server has started and is ready for requests.
Example: None.
System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1005I  LDAP server start command processed.
Explanation: The LDAP server has processed the START command.
Example: None.
System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1006I  LDAP server stop command received.
Explanation: The LDAP server has received the STOP command.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1007I  LDAP server is stopping.
Explanation: The LDAP server is stopping.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1008E  Unable to allocate storage.
Explanation: The LDAP server or utility is unable to allocate the necessary storage to continue processing the request.
Example: None.
System action: The program ends.
Operator response: Increase the storage available for use by the LDAP server or utility. Then restart the program. If the problem persists, contact the service representative.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1009A LDAP server is not APF-authorized.

Explanation: The LDAP server is not running with APF authorization. The PDS which contains the LDAP server, SYS1.SIEALNKE, and the PDSs containing all the DLLs that the LDAP server loads must be APF-authorized to allow the LDAP server to make the necessary program control threading calls.

Example: None.

System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Add SYS1.SIEALNKE to the list of APF-authorized data sets. If using a JOBLIB or STEPLIB for the LDAP server started task, verify that all data sets in the concatenation are also APF-authorized. Then restart the program.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1010E Unable to register for restart: Error error_code, Reason 0xreason_code.

Explanation: The LDAP server is unable to register with ARM (Automatic Restart Management). See the description of IXCARM in z/OS MVS Programming: Sysplex Services Reference for more information about the error.

In the message text:
error_code
   Error code from IXCARM
reason_code
   Reason code from IXCARM

Example: None.

System action: The LDAP server continues, but will not be automatically restarted if it fails unexpectedly.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Restart the program if ARM support is needed. If the problem persists, contact the service representative.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1011I LDAP server restart registration complete on system system_name.

Explanation: The LDAP server has successfully registered with ARM (Automatic Restart Management) on the system indicated in the message. The LDAP server will be automatically restarted if it fails

Example: None.

System action: The program ends.
Operator response: Contact the LDAP Administrator or see the Administrator response.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Then restart the program. If the problem persists, contact the service representative.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1012I LDAP server restart registration complete on system system_name.
unexpectedly. It will not be restarted if it detects an error and stops.

In the message text:

`GLD1013I LDAP server restarting on system system_name.`

*Explanation:* The LDAP server on the system indicated in the message is being restarted following an unexpected failure. The `RESTART_ATTEMPTS` value in the ARM policy determines the number of restarts which will be attempted.

In the message text:

`GLD1014E Unable to deregister for restart: Error error_code, Reason 0xreason_code.`

*Explanation:* The LDAP server is unable to unregister with ARM (Automatic Restart Management) during server shutdown. See the description of `IXCARM` in [z/OS MVS Programming: Sysplex Services Reference](#) for more information about the error.

In the message text:

`GLD1015I LDAP server restart deregistration complete on system system_name.`

*Explanation:* The LDAP server has successfully deregistered with ARM (Automatic Restart Management) on the system indicated in the message. The LDAP server will no longer be automatically restarted if it fails unexpectedly.
GLD1016E  Unable to create mutex:
   error_code/reason_code - error_text

Explanation: The LDAP server or utility is unable to create a mutex. See the description of
pthread_mutex_init() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:
   error_code
      Error code from pthread_mutex_init()
   reason_code
      Reason code from pthread_mutex_init()
   error_text
      Error text corresponding to the error code

Example: None.

System action: The program ends.
Operator response: None.
User response: None.

System programmer response: None.
Administrator response: Use the information in the message to correct the error. Then restart the program.
If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1018A  Unable to initialize the directory schema.

Explanation: The LDAP server or utility is unable to initialize the directory schema. A previous message indicates the reason for the failure.

Example: None.

System action: The program ends.
Operator response: None.
User response: None.

System programmer response: None.
Administrator response: Use the information in the earlier message to correct the error. Then restart the program. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD1019A  Unable to open from_code_page to to_code_page converter: error_code/reason_code - error_text

Explanation: The LDAP server or utility is unable to open a code page converter to convert character strings. See the description of iconv_open() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

from_code_page
  Code page to be converted from
to_code_page
  Code page to be converted to
error_code
  Error code from iconv_open()
reason_code
  Reason code from iconv_open()
error_text
  Error text corresponding to the error code

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Then restart the program. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1021E  Incorrect LDAP server command option specified.

Explanation: An incorrect command option was found within an LDAP server operator modify command.

Example: None.

System action: The LDAP server ignores the entered command and continues. A new LDAP server operator modify command may be entered.

Operator response: Issue a valid LDAP server operator modify command.

User response: None.

System programmer response: None.

Administrator response: See Operator response or contact Operator.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1020E  Unrecognized LDAP server command.

Explanation: An unrecognized LDAP server operator modify command is detected. The valid LDAP server commands are AUDIT, BACKEND, COMMIT, DEBUG, DISPLAY, LOG, MAINTMODE, REFRESH, RESET, SNAP, UNLOCK, and WLMEXCEPT. The SNAP command is available only with the 31-bit LDAP server.

Example: None.

System action: The LDAP server ignores the entered command and continues. A new LDAP server operator modify command may be entered.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: See Operator response or contact Operator.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1022I  Debug option processed: debug_level.

Explanation: The debug level for the LDAP server has been reset using the value indicated in the message.

In the message text:

default
  Debug level

Example: None.

System action: The LDAP server continues. Debug messages corresponding to the updated debug level are now created.

Operator response: None.
GLD1023I  Processing configuration file filename.

Explanation: The LDAP server or utility is processing the configuration file indicated in the message.

In the message text:

filename

LDAP server configuration file name

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1024I  Configuration file filename processed.

Explanation: The LDAP server or utility has successfully processed the configuration file indicated in the message.

In the message text:

filename

LDAP server configuration file name

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1025A  Unable to process command options.

Explanation: The LDAP server is unable to process the command-line options. A previous message indicates the reason for the failure.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the earlier message to correct the error. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1026E  Incorrect LDAP debug option specified: debug_options.

Explanation: The value specified for the -d parameter on the LDAP server or utility command line is not valid.

In the message text:

d debug_options

Debug options

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: See the description of the -d parameter on the LDAP server or utility command line for more information about the available debug options and how they are specified. Specify valid debug options for the -d command parameter. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1027E  parameter is an unrecognized command parameter.

Explanation: The command-line parameter indicated in the message is not supported by the LDAP server or utility.

In the message text:

parameter
   Unrecognized command parameter

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Specify a valid value for the command-line parameter. Then restart the program.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1028E  No value specified for the option parameter.

Explanation: The command-line parameter indicated in the message cannot be specified without a value when starting the LDAP server or utility. The parameter must have a value.

In the message text:

option
   Command parameter with missing value

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1030E  Unable to parse LDAP URL url:
        error_text.

Explanation: The LDAP URL specified for an LDAP server command-line parameter or in the LDAP server configuration file is not valid.

In the message text:

url
   LDAP URL

error_text
   Error message text

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1031A Unable to process the server configuration file.

Explanation: The LDAP server or utility is unable to process the LDAP server configuration file. A previous message indicates the reason for the failure.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1033E Unable to read configuration file filename: error_code/reason_code - error_text

Explanation: The LDAP server or utility is unable to read the LDAP server configuration file. The file can be a file system file or a data set. See the description of fgets() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1032E Unable to open configuration file filename: error_code/reason_code - error_text

Explanation: The LDAP server or utility is unable to open the LDAP server configuration file. See the description of fopen() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
GLD1034E  •  GLD1037E

Automation: Not applicable.

GLD1034E  Configuration line is too long.

Explanation: The LDAP server or utility cannot process the LDAP server configuration file because a line is too long. The maximum length of a line in the LDAP server configuration file is 1024 characters. This includes any continuation lines.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Correct the LDAP server configuration file. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1035E  option is an unrecognized configuration option.

Explanation: The LDAP server or utility cannot process the LDAP server configuration file because it contains an option that is not supported.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Correct the LDAP server configuration file. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1036W  option is an obsolete configuration option.

Explanation: The LDAP server or utility found an option that is no longer used in the LDAP server configuration file.

In the message text:

option

   LDAP server configuration option

Example: None.

System action: The program ignores the configuration option and continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Remove the obsolete option from the LDAP server configuration file.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1037E  Either no value or not enough values have been specified for the option configuration option.

Explanation: The LDAP server or utility found an option with either no value or not enough values in the LDAP server configuration file. Every configuration option must have an appropriate number of values specified for it.

In the message text:

option

   LDAP server configuration option

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Correct the LDAP server configuration file. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.
GLD1038E  Value value for configuration option option is not valid.

Explanation: The LDAP server or utility found an option in the LDAP server configuration file that has a value that is not supported for that option.

In the message text:

value
    LDAP server configuration option value
option
    LDAP server configuration option

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Correct the LDAP server configuration file. If the option value looks correct, check that the option on the next line after this option line starts in column 1. A blank in column 1 of the next line indicates that it is a continuation line. The next line is then appended to the preceding option line and thus can result in a value that is not supported for the option. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1039W  Extraneous value specified for the option configuration option.

Explanation: The LDAP server or utility found an option in the LDAP server configuration file that has more values than expected for a single instance of the option. The extra values are ignored. There are several common causes of this problem.

- The value contains a space. If the value of the option is more than one word (contains a space) but the option only accepts a single value, the extra words are ignored.
- The option in the next line after this option line does not start in column 1. A blank in column 1 of the next line indicates that it is a continuation line. The next line is then appended to the preceding option line and thus can result in more values than are allowed for the option.

- The extra values are intended to be a comment but they do not start with a '#' character.

In the message text:

option
    LDAP server configuration option

Example: None.

System action: The program continues, but the extra option values are ignored.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Correct the LDAP server configuration file. If a value contains a blank, enclose the value in double quotation marks. If the next line is not intended to be a continuation of this option value, ensure that the option on the next line begins in column 1. Ensure that a '#' is the first character of a comment placed at the end of an option line. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1040E  Unable to normalize name: error_text.

Explanation: The LDAP server or utility is unable to normalize a distinguished name (DN). This error can occur if any part of the DN does not contain an attribute type and value or if the attribute type is not defined in the directory schema or does not have an equality matching rule. The message displays either the DN or information about where the DN is specified. If a DN is displayed, the DN can be part of the value of an LDAP server configuration option, an LDAP utility command-line option, or an attribute value. Otherwise, the message displays a name indicating where the DN was specified, for example, the name of an LDAP server configuration option or of an attribute in an entry.

In the message text:

name
    DN or source of DN

error_text
    Error message text

Example: None.

System action:

- If the error occurs while running an LDAP utility, the program ends.
If the error occurs during LDAP server processing of the configuration file, the program ends.

If the error occurs during initialization of an LDAP server backend, then the backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to `terminate` (this is the default if the configuration option is not specified), the program ends.

If the error occurs while processing an LDAP server operation, the operation may fail.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the problem. This may involve changing the value of an option in the LDAP server configuration file, an LDAP utility command-line option, or an attribute value in an entry. Restart the program if it did not start or if a backend that did not initialize is needed. If the error occurs during an LDAP operation, retry the operation.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1041E** Configuration option `option` is not allowed in the section `section`.

**Explanation:** The LDAP server or utility found an option in a section of the LDAP server configuration file that is not appropriate for that section. Global options must be specified before the first `database` option, while backend-specific options must be specified following the `database` option for that backend.

In the message text:

- `option` LDAP server configuration option
- `section` LDAP server configuration section name

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Automation:** Not applicable.

---

**GLD1043E** Configuration file `filename` causes a recursion loop.

**Explanation:** The LDAP server or utility found an LDAP server configuration file that is included again while it is still being processed. This is a result of nested `include` options for the same configuration file.

In the message text:

- `filename` LDAP server configuration file name

**Example:** None.
GLD1045E • GLD1047E

**GLD1045E**

The MAC address must be 12 hexadecimal digits.

**Explanation:** The LDAP server or utility found that the value for the **serverEtherAddr** option in the LDAP server configuration file is not valid. The MAC address must consist of 12 hexadecimal digits.

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1047E**

Directory path is in use by another database instance.

**Explanation:** The LDAP server or utility found multiple LDBM, CDBM, or file-based GDBM backends using the same directory for database files. Each instance of the LDBM, CDBM, or file-based GDBM backend requires a unique directory for its database files. The file directory is specified by the **databaseDirectory** option in the backend section of the LDAP server configuration file.

In the message text:

**path**

Database directory path

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1046E**

Configuration option option cannot be converted to IBM-1047.

**Explanation:** The LDAP server or utility cannot convert the value of an option in the LDAP server configuration file. The value must be converted to the IBM-1047 code page but contains characters that cannot be represented in that code page.

In the message text:

**option**

LDAP server configuration option
GLD1048E  Unable to add schema definition:  

_error_text_.

Explanation:  The LDAP server is unable to add a new definition to the directory schema.

In the message text:

_error_text_
   Error message text

Example:  None.

System action:  The program ends.

Operator response:  None.

User response:  None.

System programmer response:  None.

Administrator response:  Use the information in the message to correct the error. Then restart the LDAP server. If the problem persists, contact the service representative.

Problem determination:  Not applicable.

Source:  LDAP

Module:  None.

Routing code:  None.

Descriptor code:  None.

Automation:  Not applicable.

---

GLD1050E  Unable to create thread:  

_error_code/ reason_code - error_text_

Explanation:  The LDAP server is unable to create a thread. See the description of pthread_create() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

_error_code_
   Error code from pthread_create()

_reason_code_
   Reason code from pthread_create()

_error_text_
   Error text corresponding to the error code

Example:  None.

System action:  The program continues. The request fails.

Operator response:  None.

User response:  None.

System programmer response:  None.

Administrator response:  Use the information in the message to correct the error. Then retry the request. If the problem persists, contact the service representative.

Problem determination:  Not applicable.

Source:  LDAP

Module:  None.

Routing code:  None.

Descriptor code:  None.

Automation:  Not applicable.

---

GLD1052A  Unable to start the network task.

Explanation:  The LDAP server is unable to start the interfaces used by the LDAP server. A previous message indicates the reason for the failure.

Example:  None.

System action:  The program ends.

Operator response:  None.

User response:  None.

System programmer response:  None.

Administrator response:  Use the information in the earlier message to correct the problem. Then restart the program. If the problem persists, contact the service representative.

Problem determination:  Not applicable.

Source:  LDAP

Module:  None.

Routing code:  None.

Descriptor code:  None.
GLD1053E  Unable to wait on condition variable:

- `error_code`  
- `reason_code`  
- `error_text`

**Explanation:** The LDAP server is unable to wait on a condition variable. See the description of `pthread_cond_wait()` in [z/OS XL C/C++ Run-Time Library Reference] for more information about the error.

In the message text:

- `error_code`  
  - Return code from `pthread_cond_wait()`

- `reason_code`  
  - Reason code from `pthread_cond_wait()`

- `error_text`  
  - Error text corresponding to the error code

**Example:** None.

**System action:** The program continues. The request fails.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. Then retry the request. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

GLD1055E  Unable to create a network socket:

- `error_code`  
- `reason_code`  
- `error_text`

**Explanation:** The LDAP server is unable to create a network socket. See the description of the `socket()` routine in [z/OS XL C/C++ Run-Time Library Reference] for more information about the error.

In the message text:

- `error_code`  
  - Error code from `socket()`

- `reason_code`  
  - Reason code from `socket()`

- `error_text`  
  - Error text corresponding to the error code

**Example:** None.

**System action:** The program continues. The request fails.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. Then retry the request. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
GLD1056E  Unable to obtain the network configuration: *error_code*/*reason_code* - *error_text*

**Explanation:** The LDAP server is unable to obtain the network configuration. See the description of the SIOCGIFCONF option for the `ioctl()` routine in *z/OS XL C/C++ Run-Time Library Reference* for more information about the error.

In the message text:
- *error_code*
  - Error code from `ioctl()`
- *reason_code*
  - Reason code from `ioctl()`
- *error_text*
  - Error text corresponding to the error code

**Example:** None.

**System action:** The program continues. The request fails.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. Then retry the request. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

GLD1058E  Unable to obtain the IPv6 home interfaces: *error_code*/*reason_code* - *error_text*

**Explanation:** The LDAP server is unable to obtain the list of IPv6 home interfaces. See the description of the SIOCGHOMEIF6 option for `ioctl()` in *z/OS XL C/C++ Run-Time Library Reference* for more information about the error.

In the message text:
- *error_code*
  - Error code from `ioctl()`
- *reason_code*
  - Reason code from `ioctl()`
- *error_text*
  - Error text corresponding to the error code

**Example:** None.

**System action:** The program continues. The request fails.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. Then retry the request. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

GLD1057E  Unable to obtain the status of the *name* interface: *error_code*/*reason_code* - *error_text*

**Explanation:** The LDAP server is unable to obtain the status of the indicated network interface. See the description of the SIOCGIFFLAGS option for `ioctl()` in *z/OS XL C/C++ Run-Time Library Reference* for more information about the error.

In the message text:
- *name*
  - Network interface name
- *error_code*
  - Error code from `ioctl()`
- *reason_code*
  - Reason code from `ioctl()`
- *error_text*
  - Error text corresponding to the error code

**Example:** None.

**System action:** The program continues. The request fails.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. Then retry the request. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.
GLD1059I  Listening for requests on ip port port.

Explanation: The LDAP server is listening for non-secure requests on the indicated network interface. If the listen option specifies ldap://INADDR_ANY, the IP address is displayed as 0.0.0.0. If the listen option specifies ldap://in6addr_any, the IP address is displayed as ::.

In the message text:

ip  IP address

port  TCP/IP port number

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1060I  No longer listening for requests on ip port port.

Explanation: The LDAP server is no longer listening for requests on the indicated network interface. This indicates that the network interface is no longer available. If the listen option specifies ldap://INADDR_ANY, the IP address is displayed as 0.0.0.0. If the listen option specifies ldap://in6addr_any, the IP address is displayed as ::.

In the message text:

ip  IP address

port  TCP/IP port number

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1063E  Unable to initialize the SSL environment: return_code - error_text.

Explanation: The LDAP server cannot initialize the SSL environment. See the description of the gsk_environment_open() and gsk_environment_init() routines in z/OS Cryptographic Services System SSL Programming for more information about the error.

In the message text:

return_code  Return code from SSL routine

error_text  Error text corresponding to the return code

Example: None.

System action: If the error occurs during LDAP server initialization, the tcpTerminate option in the LDAP server configuration file determines what the server does. If the tcpTerminate option is set to recover (this is the default if the configuration option is not specified), LDAP server initialization continues. In this case, SSL support is not available until the error is
corrected and the server is restarted. If the `tcpTerminate` option is set to `terminate`, the program ends. If the error occurs while processing the LDAP server `REFRESH SSL` operator modify command, the program continues, using the existing SSL environment.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. If SSL connections are not needed, remove the `sslKeyRingFile` option from the LDAP server configuration file. Restart the program if it ended or if SSL connections are needed.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

### GLD1064E Unable to load the System SSL runtime:

**error_code**

**reason_code**

**error_text**

**Explanation:** The LDAP server or utility cannot load the System SSL runtime DLL. The LDAP server uses the System SSL runtime DLL for initializing secure SSL sockets. Both the LDAP server and utility load the System SSL runtime DLL for obtaining access to the System SSL CMS runtime DLL which is used for random byte generation of `ibm-entryUUID` attribute values, CRAM-MD5 and DIGEST-MD5 binds, and the salt value for Salted SHA password hashing. See the description of `dllload()` in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

- `error_code`
- `reason_code` from `dllload()`
- `error_text`

**Example:** None.

**System action:**
- If the error occurs while loading the System SSL runtime for access to the random byte generation routine in the System SSL CMS runtime DLL, the program ends.

### GLD1065E Unable to query the gsk_get_ssl_vector routine:

**error_code**

**reason_code**

**error_text**

**Explanation:** The LDAP server or utility is unable to query the `gsk_get_ssl_vector()` routine in the System SSL runtime DLL. The LDAP server uses the System SSL runtime DLL for initializing secure SSL sockets. Both the LDAP server and utility load the System SSL runtime DLL for obtaining access to the System SSL CMS runtime DLL which is used for random byte generation of `ibm-entryUUID` attribute values, CRAM-MD5 and DIGEST-MD5 binds, and the salt value for Salted SHA password hashing. See the description of `dllqueryfn()` in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

- `error_code`
- `reason_code` from `dllqueryfn()`
- `error_text`

**Example:** None.

**System action:**
- If the error occurs while loading the System SSL runtime for access to the random byte generation routine in the System SSL CMS runtime DLL, the program ends.

- If the error occurs while during secure SSL sockets LDAP server initialization, the LDAP server continues if the `tcpTerminate` option in the LDAP server configuration file is set to `recover` (this is the default if the configuration option is not specified).
default if the configuration option is not specified). In this case, SSL support is not available until the error is corrected and the server is restarted. If the tcpTerminate option is set to terminate, the program ends.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Ensure that the correct level of System SSL is installed on the system. Restart the program if it ended. If the problem persists, contact the service representative.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1066E Unable to bind to ip port port:
   error_code/reason_code - error_text

Explanation: The LDAP server is unable to bind to the indicated network interface. See the description of bind() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

ip  IP address
port TCP/IP port number
error_code Error code from bind()
reason_code Reason code from bind()
error_text Error text corresponding to the error code

Example: None.
System action: The program continues. The request fails.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Then retry the request. If the problem persists, contact the service representative.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1068E Unable to accept connection:
   error_code/reason_code - error_text

Explanation: The LDAP server cannot accept a connection on a network interface. See the description of accept() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

error_code Error code from accept()
GLD1069E • GLD1071E

reason_code
Reason code from accept()

error_text
Error text corresponding to the error code

Example: None.

System action: The program continues. The request fails. This message will be issued at most once a minute for a limit of 60 times when this condition exists. Although this message may not be issued after being displayed 60 times on the console, the condition may still exist.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Then retry the request. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1070E  suffix is a reserved database suffix.

Explanation: The LDAP server or utility found a suffix option in the LDAP server configuration file which specifies a value that is reserved for use by the LDAP server. The LDAP server reserves ",", "cn=\-schema", and "cn=\-monitor" as suffixes for internal backends. It restricts usage of "cn=\-changelog" when the GDBM backend is configured. It also restricts usage of "cn=\-configuration" and "cn=\-ibmpolicies" when the CDBM backend is configured. The LDAP server also reserves "cn=\-Anybody", "cn=\-Authenticated" and "cn=\-\-This", because it uses these distinguished names to represent special-purpose access groups.

In the message text:

suffix
Suffix option value

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Correct the suffix option in the LDAP server configuration file. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1069E  Unable to receive data:

error_code/reason_code - error_text

Explanation: The LDAP server cannot receive data on a network interface. See the description of recv() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

error_code
Error code from recv()

reason_code
Reason code from recv()

error_text
Error text corresponding to the error code

Example: None.

System action: The program continues. The request fails.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Then retry the request. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1071E  suffix is a duplicate database suffix.

Explanation: The LDAP server or utility found a suffix option value in the LDAP server configuration file which specifies a value that is a duplicate of another suffix option value. Each suffix option value must be unique and must not be subordinate to another suffix value. For example, "o=IBM,c=US" and "c=US" cannot both be assigned as suffixes since the first value is a subordinate of the second value.

In the message text:

suffix
Suffix option value

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Correct the suffix option in the LDAP server configuration file. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
suffix
  Suffix option value
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Correct the suffix option in the LDAP server configuration file. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1072E Unable to send data: error_code/ reason_code - error_text

Explanation: The LDAP server cannot send data to a client application on a network interface. See the description of send() in [z/OS XL C/C++ Run-Time Library Reference] for more information about the error.

In the message text:
error_code
  Error code from send()
reason_code
  Reason code from send()
error_text
  Error text corresponding to the error code

Example: None.
System action: The program continues. The request may fail. This message could be accompanied by a failure of the client application due to lost response data. Client symptoms might include timeouts, long waits, or connection failures.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: If the maxConnections configuration option must be old_value, increase the values of the MAXFILEPROC statement and of MAXSOCKETS on the NETWORK statement in the BPXPRMxx member. It may also be necessary to increase the FILEPROCMAX value in the RACF OMVS segment of the user ID running the LDAP server so that the old_value can be supported. Then restart the LDAP server. See the description of the maxConnections configuration option in [Customizing the LDAP server configuration] for more information.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1074W Maximum client connections changed from old_value to new_value.

Explanation: The value for the maxConnections configuration option in the LDAP server configuration file is too large compared to the maximum number of file descriptors allowed for the LDAP server process. The maxConnections configuration option determines the maximum number of concurrent client connections. Each client connection requires a socket descriptor and each socket descriptor counts against the maximum number of files for a process. The LDAP server requires 4 file descriptors plus 2 file descriptors for each backend, plus a minimum of 30 file descriptors for network connections. To avoid running out of file descriptors, a limit is placed on the maximum number of concurrent client connections based on the current file limit.

In the message text:
old_value
  Old maximum client connections value
new_value
  New maximum client connections value

Example: None.
System action: The program continues, using the updated value for the maximum number of concurrent client connections in order to honor the current file limit for the LDAP server process.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Correct the suffix option in the LDAP server configuration file. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD1075W  Client connection threshold reached, currently using current_value of maximum_value.

Explanation: The number of concurrent client connections has reached 90% of the maximum number of connections allowed on the LDAP server.

In the message text:

- **current_value**: Current number of client connections
- **maximum_value**: Maximum number of client connections

Example: None.

System action: The program continues, but is in danger of reaching the maximum number of concurrent client connections allowed.

Operator response: Contact the LDAP Administrator or see Administrator response.

User response: None.

System programmer response: None.

Administrator response: A common reason that client connections are consumed in the LDAP server is because client applications are not unbinding from the LDAP server when they are finished making requests. Ensure that client applications disconnect when they are finished making requests to the LDAP server. If this is not the problem, increase the number of connections allowed on the LDAP server.

- If the **maxConnections** configuration option is set in the LDAP server configuration file, increase its value. Verify the increased value of **maxConnections** can be supported by obtaining the values of the **MAXFILEPROC** statement and of **MAXSOCKETS** on the **NETWORK** statement in the **BPXPRMxx** member. Also verify that the **FILEPROC** value in the RACF OMVS segment of the user ID running the LDAP server is set to a sufficient value to support the increased value of **maxConnections**.

- If **maxConnections** is not set in the LDAP server configuration file, the number of connections is limited by the values of the **MAXFILEPROC** statement and of **MAXSOCKETS** on the **NETWORK** statement in **BPXPRMxx**, and also by the value of **FILEPROC** in the RACF OMVS segment of the user ID running the LDAP server. Ensure these are set to a sufficient value.

If any of these values are updated, it is necessary to restart the LDAP server to put these changes into effect. See the description of the **maxConnections** configuration option in Customizing the LDAP server configuration for more information.

Problem determination: Not applicable.

Source: LDAP

---

GLD1076I  Number of client connections now below threshold, currently using current_value of maximum_value.

Explanation: The number of concurrent client connections has dropped below 90% of the maximum number of connections allowed on the LDAP server. Warning messages may be issued once again if the number of concurrent client connections exceeds the warning threshold.

In the message text:

- **current_value**: Current number of client connections
- **maximum_value**: Maximum number of client connections

Example: None.

System action: The program continues.

Operator response: Contact the LDAP Administrator or see Administrator response.

User response: None.

System programmer response: None.

Administrator response: If this message is repeatedly displayed, it means that the maximum number of file descriptors available to the LDAP server may be too low. In this case, it may be desirable to increase the number of concurrent connections that the LDAP server can support by changing the setting of the **maxConnections** option in the LDAP server configuration file. Verify the increased value of **maxConnections** can be supported by obtaining the values of the **MAXFILEPROC** statement and of **MAXSOCKETS** on the **NETWORK** statement in the **BPXPRMxx** member. Also verify that the **FILEPROC** setting in the RACF OMVS segment of the user ID running the LDAP server is set to a sufficient value to support the increased value of **maxConnections**. If any of these values are updated, it is necessary to restart the LDAP server to put these changes into effect. See the description of the **maxConnections** configuration option in Customizing the LDAP server configuration for more information.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.
GLD1077E Maximum client connections reached, connection from ip rejected.

Explanation: The maximum number of concurrent client connections has been reached and new connections are rejected until the number of client connections drops below the maximum value. This situation can be caused by client applications not unbinding when they are finished communicating with the LDAP server.

In the message text:

*ip* IP address

Example: None.

System action: The program continues. Additional client applications cannot connect to the LDAP server. This message will be issued at most once a minute for a limit of 60 times when this condition exists. Although this message may not be issued after being displayed 60 times on the console, the condition may still exist.

Operator response: Contact the LDAP Administrator or see Administrator response.

User response: None.

System programmer response: None.

Administrator response: A common reason that client connections are consumed in the LDAP server is because client applications are not unbinding from the LDAP server when they are finished making requests. Ensure that client applications disconnect when they are finished making requests to the LDAP server. If this is not the problem, increase the number of connections allowed on the LDAP server.

- If the maxConnections configuration option is set in the LDAP server configuration file, increase its value. Verify the increased value of maxConnections can be supported by obtaining the values of the MAXFILEPROC statement and of MAXSOCKETS on the NETWORK statement in the BPXPRMxx member. Also verify that the FILEPROCMAX value in the RACF OMVS segment of the user ID running the LDAP server is set to a sufficient value to support the increased value of maxConnections.
- If maxConnections is not set in the LDAP server configuration file, the number of connections is limited by the values of the MAXFILEPROC statement and of MAXSOCKETS on the NETWORK statement in BPXPRMxx, and also by the value of FILEPROCMAX in the RACF OMVS segment of the user ID running the LDAP server. Ensure these are set to a sufficient value.

If any of these values are updated, it is necessary to restart the LDAP server to put these changes into effect. See the description of the maxConnections configuration option in Customizing the LDAP server configuration for more information.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1078E Unable to get the value for the maximum number of files:

*error_code* / *reason_code* - *error_text*

Explanation: The LDAP server is unable to determine the maximum number of files allowed for a process. See the description of getrlimit() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

*error_code* Error code from getrlimit()

*reason_code* Reason code from getrlimit()

*error_text* Error text corresponding to the error code

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Then restart the program. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1079E Maximum file limit of current_limit is too small, change it to at least new_limit.

Explanation: The maximum number of files that can be opened by the LDAP server process is too small. The LDAP server requires 4 file descriptors plus 2 file descriptors for each backend, plus a minimum of 30 file descriptors for network connections. The current maximum file limit displayed in the message is not large enough to support the minimum of 30 file
GLD1080E  GLD1081A

descriptors required for network connections. The maximum file limit must be set to at least the indicated new limit for the LDAP server to start.

In the message text:

`current_limit`
Current maximum file limit

`new_limit`
Recommended maximum file limit

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Increase the values of the `MAXFILEPROC` statement and of `MAXSOCKETS` on the `NETWORK` statement in the `BPXPRMxx` member. It may also be necessary to increase the `FILEPROCMAX` value in the RACF OMVS segment of the user ID running the LDAP server. Then restart the LDAP server. See the description of the `maxConnections` configuration option in Customizing the LDAP server configuration for more information.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1080E  Unable to load the Kerberos runtime:

`return_code` `reason_code - error_text`

Explanation: The LDAP server encountered an error in attempting to load the Kerberos runtime DLL. See the description of `krb5_dll_load()` in [z/OS Integrated Security Services Network Authentication Service Programming](https://www.ibm.com) for more information about the return codes. See [z/OS UNIX System Services Messages and Codes](https://www.ibm.com) for more information about the reason codes.

In the message text:

`return_code`
Return code from `krb5_dll_load()`

`reason_code`
Reason code from `krb5_dll_load()`

`error_text`
Error text corresponding to the return code

Example: None.

System action: The LDAP server continues initialization if the `tcpTerminate` option in the LDAP server configuration file is set to `recover` (this is the default if the configuration option is not specified). In this case, Kerberos support is not available until the error is corrected and the server is restarted. If the `tcpTerminate` option is set to `terminate`, the program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Verify that the `SYS1.SIEALNKE` data set is available to the LDAP server job step. If Kerberos authentication is not needed, set the `supportKrb5` option in the LDAP server configuration file to `off`. Restart the program if it ended or if Kerberos support is needed.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1081A  No network interface is available for a 'listen' statement.

Explanation: There are no network interfaces available for a `listen` statement. This error can also occur if a `listen` option in the LDAP server configuration file or on the LDAP server command line specifies SSL connections but SSL support is not available.

Example: None.

System action: The LDAP server continues if the `tcpTerminate` option in the LDAP server configuration file is set to `recover` (this is the default if the configuration option is not specified). If the `tcpTerminate` option is set to `terminate`, the program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Either start the required network interfaces or remove the corresponding `listen` option from the LDAP server configuration file or command line. Restart the program if it ended.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.
GLD1082A  Network interface ip on port port is not available.

Explanation: A required network interface is not available for use.
In the message text:
  ip  IP address
  port  TCP/IP port number

Example: None.

System action: The LDAP server continues if the tcpTerminate option in the LDAP server configuration file is set to recover (this is the default if the configuration option is not specified) or if at least one network interface starts successfully. Otherwise, the program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1083A  Host host cannot be resolved.

Explanation: The host name specified on a listen option in the LDAP server configuration file or on the LDAP server command line cannot be resolved.
In the message text:
  host  Host name

Example: None.

System action: The LDAP server continues if the tcpTerminate option in the LDAP server configuration file is set to recover (this is the default if the configuration option is not specified) or if at least one network interface starts successfully. Otherwise, the program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1084I  Network interface status

Explanation: This message is displayed in response to the LDAP server DISPLAY NETWORK operator modify command. The remaining lines in this multi-line message display the status of each network interface. A network interface is ACTIVE if the LDAP server is listening for requests on that interface. A network interface is INACTIVE if the interface has been stopped and has not been restarted yet. No entry is displayed for network interfaces which were not started when the LDAP server was started. The LDAP server checks for network interface changes based on the value of the LDAP_NETWORK_POLL environment variable, which has a default value of 5 minutes.

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1085I  No active network interfaces.

Explanation: This message is displayed in response to the LDAP server DISPLAY NETWORK operator modify command when there are no active network interfaces to display, and no network interfaces ever started successfully.
GLD1086I  Maximum number of lines displayed.

Explanation: There is a limit of 254 lines of output from an LDAP server operator modify command. The maximum number of output lines has been reached for this command and the rest of the output is not displayed.

Example: None.
System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1087E  The type backend is already defined.

Explanation: The LDAP server or utility found multiple database options in the LDAP server configuration file for a CDBM, GDBM, SDBM, or EXOP backend. Each of these backends can be defined at most once in the configuration file.

In the message text:

**type**
Backend type

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1088E  The EXOP backend requires Program Call services.

Explanation: The Policy Directory extended operations backend requires Program Call services. The LDAP server must have a listen option specifying ldap://:pc or ldaps://:pc in order to provide Program Call services. The listen option can be specified in the LDAP server configuration file or on the LDAP server command line when starting the server.

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1089E  The option option must be specified for the type backend.

Explanation: The LDAP server or utility found that an option is missing from a backend section of the LDAP server configuration file. The option indicated in the message is required when configuring this type of backend.
In the message text:

**option**
Option name

**type**
Backend type

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Add the required option to the backend section of the LDAP server configuration file. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1090E** The SDBM backend supports a single suffix.

**Explanation:** The LDAP server or utility found multiple suffix options in the SDBM section of the LDAP server configuration file. There can only be one SDBM backend section in the configuration file and it must contain exactly one suffix option.

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Add the required option to the backend section of the LDAP server configuration file. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1091E** Unable to open schema database file

**filename: error_code/reason_code - error_text**

**Explanation:** The LDAP server or utility is unable to open the schema database file. See the description of fopen() in [z/OS XL C/C++ Run-Time Library Reference](https://www.ibm.com/support/knowledgecenter/SSSLTB82_2.3.0/com.ibm.zos.r23/response/c_rte_fopen.html) for more information about the error.

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Remove the extra suffix options from the SDBM section of the LDAP server configuration file. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1092E** Unable to read from schema database file

**filename: error_code/reason_code - error_text**

**Explanation:** The LDAP server or utility is unable to read the schema database file. See the description of fread() in [z/OS XL C/C++ Run-Time Library Reference](https://www.ibm.com/support/knowledgecenter/SSSLTB82_2.3.0/com.ibm.zos.r23/response/c_rte_fread.html) for more information about the error.

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
GLD1093E • GLD1094E

System action:
• If the error occurs during LDAP server initialization, the program ends.
• If the error occurs during a schema modify operation, the schema modification is successful. If the LDAP server is part of a cross-system group in a sysplex, the other LDAP servers in the sysplex may not apply the schema change to their version of the schema. In this case, add and modify operations on those LDAP servers may fail if they involve the modified schema elements.
• If the error occurs when processing a request for the schema from another LDAP server in the sysplex, the other LDAP server ends because it cannot obtain the schema.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Also verify that the schema database file has not been corrupted and that there are no file system errors. Restart the program if it did not start or retry the schema modify operation.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1093E Unable to write to schema database file
filename: error_code/reason_code - error_text

Explanation: The LDAP server is unable to write the schema database file. See the description of fwrite() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:
filename
  Schema database file name
error_code
  Error code from fwrite()
reason_code
  Reason code from fwrite()
error_text
  Error text corresponding to the error code

Example: None.

System action:
• If the error occurs during schema initialization, the program ends.
• If the error occurs during LDBM, CDBM, or GDBM initialization, then the LDBM, CDBM, or GDBM backend does not start. If the svrStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the svrStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.
If the error occurs during a modify operation of the schema, the modify operation fails and the server continues to run with its current schema.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. If an LDBM, CDBM, or a file-based GDBM backend is configured, the directory containing the checkpoint file is specified by the `databaseDirectory` option in the backend section of the LDAP server configuration file. The directory defaults to `/var/ldap/ldbm` and `/var/ldap/gdbm` if the configuration option is not specified for an LDBM or GDBM backend. If the configuration option is not specified for a CDBM backend, the directory defaults to the schema directory which is specified by the `schemaPath` option in the global section of the LDAP server configuration file. The directory containing the schema database file is specified by the `schemaPath` option. The directory defaults to `/var/ldap/schema` if the configuration option is not specified. Make sure that the directory can be created if it does not exist. Restart the LDAP server if it did not start or retry the schema modify operation. If the server started but an LDBM, CDBM, or GDBM backend is not available, then restart the server to make it available. For a utility, restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1095E** Schema database file *filename* is not valid.

**Explanation:** The LDAP server or utility is not able to load the schema from the schema database file. Either the record format is not as expected or the schema is not complete. If the file name indicated in the message is **XCF**, then the schema was sent to the LDAP server from another LDAP server in the sysplex.

In the message text:

`filename`  
Schema database file name

**Example:** None.

**System action:** The program ends unless the internal schema is still usable.

**Operator response:** None.

**User response:** None.

---

**GLD1096E** Unable to decode schema database record.

**Explanation:** The LDAP server or utility detected an error while trying to load the schema. The schema can be loaded from either the schema database file or from the sysplex group owner through XCF. This error indicates that the LDAP server could not decode one of the schema database records.

**Example:** None.

**System action:** The program ends unless the internal schema is still usable.

**Operator response:** None.

**User response:** None.

---

**GLD1097E** Unable to encode schema database record.

**Explanation:** The LDAP server detected an error while trying to save the schema to the schema database file. It could not encode one of the database records.

**Example:** None.

**System action:** If the error occurs during LDAP server initialization, the server ends. If it occurs during a modify operation of the schema, the modify operation
fails and the server continues to run with its current schema.

Operator response:  None.
User response:  None.
System programmer response:  None.
Administrator response:  Restart the program. If the problem persists, contact the service representative.

Problem determination:  Not applicable.

Source:  LDAP
Module:  None.
Routing code:  None.
Descriptor code:  None.
Automation:  Not applicable.

---

GLD1098E  Unable to rename oldfile to newfile:

error_code/reason_code - error_text

Explanation:  The LDAP server is unable to rename a file. See the description of rename() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

oldfile  Old file name
newfile  New file name
error_code  Error code from rename()
reason_code  Reason code from rename()
error_text  Error text corresponding to the error code

Example:  None.

System action:

- If the error occurs during schema initialization, the server ends.
- If the error occurs during LDBM, CDBM, or GDBM initialization, then the LDBM, CDBM, or GDBM backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends.
- If the error occurs during a modify operation of the schema, the modify operation fails and the LDAP server continues to run with its current schema.
- If the error occurs during an LDBM, CDBM, or GDBM operation, then, if the fileTerminate option in the LDAP server configuration file is set to recover (this is the default if the configuration option is not specified), the server continues to run but the LDBM, CDBM, or GDBM backend is placed in read-only state. If the fileTerminate option is set to terminate, the program ends.

- If the error occurs during activity log file rollover and the logfileRolloverDirectory option in the LDAP server configuration file specifies a z/OS UNIX System Services directory, the LDAP server continues with the rolled over activity log file remaining in the directory specified by the logfile option.

- If the error occurs during activity log file rollover and the logfile or the logfileRolloverDirectory configuration options specify a generated data group (GDG) base, the LDAP server continues with the current data set for the activity log file.

Operator response:  Use the information in the message to assist the LDAP administrator to correct the error. If requested, issue the LDAP server BACKEND operator modify command to set the LDBM, CDBM, or GDBM backend to read/write state.

User response:  None.
System programmer response:  None.
Administrator response:  Use the information in the message to correct the error. Also verify that the LDAP server has write access to the directory. Then restart the LDAP server if it did not start. If an LDBM, CDBM, or GDBM backend was placed in read-only state, it can be reset to read-write state by restarting the LDAP server or by using the LDAP server BACKEND operator modify command. If the error occurred during activity log file rollover and the logfileRolloverDirectory option specifies a z/OS UNIX System Services directory, create a directory with the appropriate permissions that the LDAP server can write to. Verify that the old and new activity log files reside in the same type of z/OS UNIX System Services file system.

Problem determination:  Not applicable.

Source:  LDAP
Module:  None.
Routing code:  None.
Descriptor code:  None.
Automation:  Not applicable.

---

GLD1099E  Schema unique identifier number is already assigned.

Explanation:  Each attribute and object class in the LDAP server schema is identified by a unique internal identifier. While adding an attribute or object class to the schema, the LDAP server has detected that the attribute or object class identifier is already in use. This should not occur.
In the message text:

number
    Identifier number
Example: None.

System action: If the error occurs during LDAP server initialization, the server ends. If it occurs during a modify operation of the schema, the modify operation fails and the server continues to run with its current schema.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Restart the LDAP server. If the problem persists, contact the service representative.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1100A LDAP server shutdown initiated because directory schema cannot be restored.
Explanation: The LDAP server is stopping because an attempt to load the directory schema has failed and the schema cannot be used. A previous message identifies the reason for the failure.
Example: None.
System action: The server ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the earlier message to correct the problem. Then restart the program. If the problem persists, contact the service representative.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1101E No type load module specified for 64-bit addressing mode.
Explanation: The LDAP server or utility is running in 64-bit addressing mode but one of the database options in the LDAP server configuration file does not specify a load module for 64-bit addressing mode. As a result, the backend is not loaded.

In the message text:

type
    Backend type
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Either specify a load module for 64-bit addressing mode on the database option or remove the backend section from the LDAP server configuration file. The backend section includes the database option and all the options following it until the next database option. Restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
GLD1103E  No backend load module specified for 31-bit addressing mode.

Explanation: The LDAP server or the utility is running in 31-bit addressing mode but one of the database options in the LDAP server configuration file does not specify a load module for 31-bit addressing mode. As a result, the backend is not loaded.

In the message text:

backend
   Backend type

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Ensure that the DLL is installed and can be accessed by the LDAP server or utility. If the DLL module name is specified on a database option in the LDAP server configuration file, ensure that it is entered correctly there. Restart the program if it did not start or if the backend is needed.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1105E  Unable to query entry point name in DLL module: error_code/reason_code - error_text

Explanation: The LDAP server or the utility is unable to locate a required entry point in the indicated DLL. See the description of dllqueryfn() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

name
   Entry point name

module
   DLL module

error_code
   Error code from dllload()

reason_code
   Reason code from dllload()

code
   Error code corresponding to the error code

Example: None.

System action: The backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Ensure that the DLL is installed and can be accessed by the LDAP server or utility. If the DLL module name is specified on a database option in the LDAP server configuration file, ensure that it is entered correctly there. Restart the program if it did not start or if the backend is needed.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
GLD1106E  GLD1108I

(GLD1106E) GLD1107I

**GLD1108I Server statistics reset.**

**Explanation:** The statistics monitored by the LDAP server have been reset. This message is displayed in response to the LDAP server `RESET THREADS` command.

**Example:** None.

**System action:** The LDAP server continues.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

(GLD1106E) GLD1108I

**GLD1106E  type backend initialization failed for backend named name.**

**Explanation:** The indicated backend failed to initialize. A previous message indicates the reason for the failure. In the message text:

- `type` Backend type
- `name` Backend name

**Example:** None.

**System action:** The backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends and plug-ins that successfully start. If the `srvStartUpError` option is set to `terminate` (this is the default if the configuration option is not specified), the program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the earlier message to correct the error. For a TDBM or DB2-based GDBM backend, ensure that DB2® is available. Restart the program if it did not start or if the backend is needed.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
GLD1109I Server activity statistics

Explanation: This message is displayed in response to the LDAP server DISPLAY THREADS operator modify command. The remaining lines in this multi-line message display the activity statistics. The RESET THREADS operator modify command can be used to reset the activity statistics.

Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1110E An administrator DN must be specified using the adminDN configuration option.

Explanation: The LDAP server or utility found that the adminDN option is missing in the LDAP server configuration file. This option defines the LDAP root administrator and is required.

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Add the adminDN option to the global section of the LDAP server configuration file. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1111E Unable to normalize schema owner: text.

Explanation: The LDAP server or utility is unable to normalize the distinguished name of the schema entry owner. This might occur due to a series of conflicting modifications to the schema entryowner attribute and one or more attributetypes definitions within the schema.

In the message text:

```
error_text
```

Error message text

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Then restart the program. It might be necessary to restore the schema from a backup. If the problem persists, contact the service representative.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1112E Unable to process schema ACL: error_text.

Explanation: The LDAP server or utility is unable to process the access control list for the schema entry. This might occur due to a series of conflicting modifications to the schema aclentry attribute and one or more attributetypes definitions within the schema.

In the message text:

```
error_text
```

Error message text

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Then restart the program. It might be necessary to restore the schema from a backup. If the problem persists, contact the service representative.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1113E  The keylabel record in the encryption keys dataset is incorrect.

Explanation: The LDAP server or utility found a record in the encryption keys dataset that is not valid. Each record in the encryption keys dataset consists of a key label followed by one or more key components. Each key component consists of 16 hexadecimal characters. Blank lines and lines beginning with '#' or an '*' are commentary records and are ignored. The following is an example of a properly formatted key in the encryption keys dataset.

```
label1 1010101010101010 1010101010101010
```

In the message text:

keylabel
   Encryption key label name

Example: None.

System action: The utility ends. The LDAP server continues, but encryption and decryption of values using a key in the key data set might fail. In particular, this might result in bind failures if the userPassword attribute value cannot be decrypted.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

GLD1114E  A record in the encryption keys dataset is longer than 255 bytes.

Explanation: The LDAP server or utility found a record in the encryption keys dataset that is too long. The maximum length of a record in the encryption keys data set is 255 bytes.

Example: None.

System action: The utility ends. The LDAP server continues, but encryption and decryption of values using a key in the key data set might fail. In particular, this might result in bind failures if the userPassword attribute value cannot be decrypted.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

GLD1115E  Label 'keylabel' is not available: error_text.

Explanation: The LDAP server or utility encountered an error attempting to encrypt a value using the key label indicated in the message and the AES or DES algorithm. The label and algorithm to use are specified on the pwEncryption or secretEncryption options in the LDAP server configuration file. If the key label is stored in ICSF, see z/OS Cryptographic Services ICSF Application Programmer’s Guide for more information about the error.

In the message text:

keylabel
   Encryption key label name

error_text
   Error message text

Example: None.

System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: If using an encryption keys data set to store AES or DES keys, ensure that keylabel matches the label on one of the records in the data set and that the keys are valid. A DES key that is specified in the encryption keys data set consists of 8, 16 or 24 bytes with odd parity while an AES key consists of 32 bytes. If AES or DES keys are stored in an ICSF CKDS data set, ensure that ICSF is running before starting the LDAP server or utility. Correct the LDAP server configuration file or the encryption keys data set. Then restart the program.
GLD1116E  GLD1118E

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1116E  Unable to initialize an SSL connection with IP_address: return_code - Error_text.

Explanation: The LDAP server encountered an error while initializing an SSL connection with the client connecting from the IP address indicated in the message. The failing routine can be gsk_secure_socket_open(), gsk_attribute_set_numeric_value(), gsk_attribute_get_buffer(), gsk_attribute_set_buffer(), or gsk_secure_socket_init(). See the descriptions of these routines in z/OS Cryptographic Services System SSL Programming for more information about the error.

In the message text:
IP_address
   Client IP address
return_code
   Return code from gsk_secure_socket_read()
Error_text
   Error text corresponding to the return code

Example: None.

System action: The LDAP server continues. The client request fails.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Then retry the client operation. If the problem persists, contact the service representative.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1118E  Unable to send SSL data to IP_address: return_code - Error_text.

Explanation: The LDAP server encountered an error while attempting to send data over an SSL connection with the client connecting from the IP address indicated in the message. See the description of gsk_secure_socket_write() in z/OS Cryptographic Services System SSL Programming for more information about the error.

In the message text:
IP_address
   Client IP address
return_code
   Return code from gsk_secure_socket_write()
Error_text
   Error text corresponding to the return code

Example: None.

System action: The LDAP server continues. The client request fails.
GLD1119E  Unable to get SSL certificate information: return_code - Error_text.

Explanation: The LDAP server encountered an error while attempting to obtain certificate information for a client performing an SASL EXTERNAL bind over SSL. See the description of gsk_attribute_get_cert_info() in z/OS Cryptographic Services System SSL Programming for more information about the error.

In the message text:

return_code
   Return code from gsk_attribute_get_cert_info()

Error_text
   Error text corresponding to the return code

Example: None.

System action: The LDAP server continues initialization if the tcpTerminate option in the LDAP server configuration file is set to recover (this is the default if the configuration option is not specified). In this case, Kerberos support is not available until the error is corrected and the server is restarted. If the tcpTerminate option is set to terminate, the program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Then retry the client operation. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1120E  Kerberos initialization failed: 0xreturn_code - error_text.

Explanation: The LDAP server encountered an error while attempting to initialize the Kerberos runtime environment. The failing routine can be krb5_init_context(), krb5_sname_to_principal(), or krb5_unparse_name(). See the descriptions of these routines in z/OS Integrated Security Services Network Authentication Service Programming for more information about the error.

In the message text:

return_code
   Return code from Kerberos routine

error_text
   Error text corresponding to the return code

Example: None.

System action: The LDAP server continues initialization if the tcpTerminate option in the LDAP server configuration file is set to recover (this is the default if the configuration option is not specified). In this case, Kerberos support is not available until the error is corrected and the server is restarted. If the tcpTerminate option is set to terminate, the program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. If Kerberos authentication is not needed, set the supportKrb5 option in the LDAP server configuration file to off. Restart the program if it ended or if Kerberos support is needed. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1121E  Unable to parse Kerberos principal 'principal_name': 0xreturn_code - error_text.

Explanation: The LDAP server is unable to parse the Kerberos principal specified by the serverKrbPrinc option in the LDAP server configuration file. See the description of krb5_parse_name() in z/OS Integrated Security Services Network Authentication Service Programming for more information about the error.

In the message text:
GLD1122E  •  GLD1123E

principal_name
Kerberos principal name

return_code
Return code from krb5_parse_name()

error_text
Error text corresponding to the return code

Example: None.

System action: The LDAP server continues initialization if the tcpTerminate option in the LDAP server configuration file is set to recover (this is the default if the configuration option is not specified). In this case, Kerberos support is not available until the error is corrected and the server is restarted. If the tcpTerminate option is set to terminate, the program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Verify that a valid Kerberos principal name is specified for the serverKrbPrinc option in the LDAP server configuration file. Correct the option, or, if Kerberos authentication is not needed, set the supportKrb5 option in the LDAP server configuration file to off. Restart the program if it ended or if Kerberos support is needed.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1122E  GSSAPI initialization failed: Major 0xmajor_error, Minor 0xminor_error - principal_name.

Explanation: The LDAP server encountered an error while attempting to initialize the GSSAPI environment. The failing routine can be gss_import_name() or gss_acquire_cred(). See the descriptions of these routines in z/OS Integrated Security Services Network Authentication Service Programming for more information about the error.

In the message text:

major_error
Major error code from Kerberos routine

minor_error
Minor error code from Kerberos routine

principal_name
Kerberos server principal name

Example: None.

System action: The LDAP server continues initialization if the tcpTerminate option in the LDAP server configuration file is set to recover (this is the default if the configuration option is not specified). In this case, Kerberos support is not available until the error is corrected and the server is restarted. If the tcpTerminate option is set to terminate, the program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Verify that the LDAP server has access to the encryption key for the Kerberos principal associated with the LDAP server. The encryption key is located in a key table or the local KDC depending on the krbKeytab option value in the LDAP server configuration file. Correct the LDAP server configuration file or the GSSAPI environment on the system. If Kerberos authentication is not needed, set the supportKrb5 option in the LDAP server configuration file to off. Restart the program if it ended or if Kerberos support is needed. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1123E  Unable to wrap a GSSAPI message: Major 0xmajor_error, Minor 0xminor_error - principal_name.

Explanation: The LDAP server encountered a problem while attempting to cryptographically sign and possibly encrypt (wrap) a GSSAPI message. See the description of gss_wrap() in z/OS Integrated Security Services Network Authentication Service Programming for more information about the error.

In the message text:

major_error
Major error code from gss_wrap()

minor_error
Minor error code gss_wrap()

principal_name
Kerberos server principal name

Example: None.
System action: The LDAP server continues. The client request fails.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Correct the GSSAPI environment on the system. Then retry the client operation. If the problem persists, contact the service representative.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1124E Unable to unwrap a GSSAPI message: Major 0xmajor_error, Minor 0xminor_error - principal_name.
Explanation: The LDAP server encountered a problem while attempting to unwrap a GSSAPI message sealed by the gss_wrap() routine and verify the embedded signature. See the description of gss_unwrap() in z/OS Integrated Security Services Network Authentication Service Programming for more information about the error.
In the message text:
major_error
    Major error code from gss_unwrap()
minor_error
    Minor error code from gss_unwrap()
principal_name
    Kerberos server principal name
Example: None.
System action: The LDAP server continues. The client request fails.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1125W The option configuration option is specified more than once.
Explanation: The LDAP server or utility found an option in the LDAP server configuration file that is specified more than once in the global section or in a backend section. The option can only be specified once in a section of the configuration file.
In the message text:
option
    LDAP server configuration option
Example: None.
System action: The program continues, using the value in the last occurrence of the option in the LDAP server configuration file.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Remove the extra occurrences of the option in the global or backend section of the LDAP server configuration file so that the option is only specified once in that section. Restart the program if the wanted option value is not being used.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1126I Server lock statistics
Explanation: This message is displayed in response to the LDAP server DISPLAY LOCKS operator modify command. The remaining lines in this multi-line message display the lock contention statistics. There are two types of contention: waiting for shared control of the lock and waiting for exclusive control of the lock. For each type of request, the number of times that contention was encountered and the average wait time until the lock was obtained is displayed. The LDAP server RESET LOCKS operator modify command can be used to reset the lock contention statistics.
Example: None.
System action: The LDAP server continues.
Operator response: None.
GLD1127I  Server lock statistics reset.
Explanation: The LDAP server has reset the lock contention statistics after the RESET LOCKS operator modify command has been issued.
Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1128E  ARM element name arm\_name is already in use.
Explanation: The LDAP server is unable to register with the Automatic Restart Management (ARM) service because the element name indicated in the message is already in use. This error can occur if the LDAP server is started multiple times on the same system and unique ARM names are not specified by the armName option in the LDAP server configuration file.
In the message text:

arm\_name  ARM element name

Example: None.
System action: The LDAP server continues, but Automatic Restart Management (ARM) is not available to the LDAP server. The LDAP server is not automatically restarted if it fails unexpectedly.
Operator response: None.

GLD1129I  Program Call communication is active.
Explanation: The Program Call support interface is now active on the LDAP server.
Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1130E  Program Call initialization failed:
      Return code return\_code, Reason code reason\_code.
Explanation: The LDAP server is unable to initialize the Program Call support. The return code has the following values:
1  Job step is not APF-authorized.
2  Program Call support is being used by another LDAP server on the same system.
3  ESTAEX create failed. The reason code is the ESTAEX return code. See the description of ESTAEX in z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG for more information about the error.
5  LXRES failed. The reason code is the LXRES return code. See the description of LXRES in GLD1127I  GLD1130E
GLD1131E • GLD1132E

GLD1131E  Program Call support not activated because another server already provides Program Call support.

Explanation: Another LDAP server is already running with Program Call support activated. Only one LDAP server on each system can provide Program Call support.

Example: None.

System action: If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: If Program Call support is needed on this LDAP server, stop the other LDAP server that is running with Program Call support and remove the listen option for Program Call support from the LDAP server configuration file for the other server. Then restart both LDAP servers. If Program Call support is not needed on this LDAP server, remove the listen option for Program Call support from the LDAP server configuration file for the LDAP server.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1132E  Program Call termination failed: Return code return_code, Reason code reason_code.

Explanation: The LDAP server is unable to stop the Program Call support. The return code has the following values:

101 ESTAEX cancel failed. The reason code is the ESTAEX return code. See the description of ESTAEX in z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG for more information about the error.

102 IEANTDL failed. The reason code is the IEANTDL return code. See the description of IEANTDL in z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG for more information about the error.
Unable to obtain control area lock. This indicates another task abnormally ended while holding the lock.

In the message text:

return_code
Return code

reason_code
Reason code

Example: None.

System action: The LDAP server continues. The server may be in the process of ending.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. If the problem persists, contact the service representative.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

Unable to start the Program Call support.

Explanation: The LDAP server is unable to initialize the Program Call support. A previous message identifies the reason for the failure.
Example: None.

System action: The Program Call interface is not available. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the earlier message to correct the error. Restart the program if it ended or if Program Call support is needed. Program Call support is used by RACF change logging and Policy Directory extended operations. If the problem persists, contact the service representative.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

Sysplex status

Explanation: This message is displayed in response to the LDAP server DISPLAY XCF operator modify command. The remaining lines in this multi-line message display the status of each LDAP server in the cross-system group.
Example: None.

System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

Cross-system services are not available.

Explanation: This message is displayed in response to the LDAP server DISPLAY XCF operator modify command when the LDAP server is not a member of a cross-system group.
Example: None.

System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD1137A Unable to initialize sysplex services.

Explanation: The LDAP server is unable to initialize the sysplex support. A previous message indicates the reason for the failure.

Example: None.

System action: The LDAP server ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the earlier message to correct the error. Then restart the program. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1138E Cross-system group name value is not valid.

Explanation: The cross-system group name specified by the serverSysplexGroup option in the LDAP server configuration file is not valid. A cross-system group name is 1-8 characters and consists of letters (A-Z), numbers (0-9) and special characters (#, @, $). The special characters must be in the IBM-1047 code page.

In the message text:

value
  Cross-system group name

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1139E Not authorized to join cross-system group group_name.

Explanation: The LDAP server is not authorized to join the cross-system group. The user ID associated with the LDAP server must have at least READ access to the GLD.XCF.GROUP.group_name resource in the FACILITY class. The group name is specified by the serverSysplexGroup option in the LDAP server configuration file.

In the message text:

group_name
  Cross-system group name

Example: None.

System action: The LDAP server ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Give the LDAP server user ID at least READ access to the cross-system resource. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1140E Cross-system group group_name is not defined.

Explanation: The cross-system group is not defined to the external security manager. The cross-system group for the LDAP server must have a profile in the FACILITY class. The resource name is GLD.XCF.GROUP.group_name, where the group name is specified by the serverSysplexGroup option in the LDAP server configuration file. For example, if the cross-system group name is LDAP6, then the resource name is GLD.XCF.GROUP.LDAP6.

In the message text:

group_name
  Cross-system group name

Example: None.

System action: The LDAP server ends.

Operator response: None.

User response: None.
GLD1141E  XCF initialization failed: Return code return_code, Reason code x’reason_code’.

Explanation: The LDAP server is unable to initialize the cross-system coupling facility (XCF) support. The return code has the following values:

1  IXCJOIN failed. The reason code contains the IXCJOIN return code in the upper 16 bits and the IXCJOIN reason code in the lower 16 bits. See the description of IXCJOIN in z/OS MVS Programming: Sysplex Services Reference for more information about the error.

2  IXCQUERY failed. The reason code contains the IXCQUERY return code in the upper 16 bits and the IXCQUERY reason code in the lower 16 bits. See the description of IXCQUERY in z/OS MVS Programming: Sysplex Services Reference for more information about the error.

3  IXCSETUS failed. The reason code contains the IXCSETUS return code in the upper 16 bits and the IXCSETUS reason code in the lower 16 bits. See the description of IXCSETUS in z/OS MVS Programming: Sysplex Services Reference for more information about the error.

In the message text:

return_code
  Return code

reason_code
  Reason code

Example: None.

System action: The LDAP server ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Then restart the program.

If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1143E  System system_name is already active in cross-system group group_name.

Explanation: Another LDAP server on the same system is already a member of the cross-system group. Only one LDAP server on each system in the sysplex can be a member of a particular cross-system group. The cross-system group name is specified by the serverSysplexGroup option in the LDAP server configuration file.

In the message text:

system_name
  System name

group_name
  Cross-system group name

Example: None.

System action: The LDAP server ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Either stop the other LDAP server or specify a different cross-system group in the serverSysplexGroup option in the LDAP server configuration file for this LDAP server. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1143E  XCF termination failed: Return code return_code, Reason code x’reason_code’.

Explanation: The LDAP server is unable to end the cross-system coupling facility (XCF) support. The return code has the following values:

1  IXCDELETE failed. The reason code contains the IXCDELETE return code in the upper 16
bits and the **IXCLEAVE** reason code in the lower 16 bits. See the description of **IXCLEAVE** in [z/OS MVS Programming: Sysplex Services Reference](#) for more information about the error.

In the message text:

```
return_code
  Return code
reason_code
  Reason code
```

Example: None.

System action: The LDAP server ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1144I  **SSL support is not active.**

Explanation: The LDAP server REFRESH SSL operator modify command cannot be processed because SSL support is not enabled in the LDAP server. Either SSL support is not configured or the LDAP server is unable to initialize the SSL environment.

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1146I  **System system_name has joined LDAP cross-system group group_name.**

Explanation: The LDAP server running on the indicated system has joined the LDAP cross-system group. Sysplex services are now active for that server. This message is displayed by each active LDAP server when a new LDAP server joins the cross-system group.

In the message text:

```
system_name
  System name
```

```
group_name
  Cross-system group name
```

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
GLD1147I  System system_name has left LDAP cross-system group group_name.

Explanation: The LDAP server running on the indicated system has left the LDAP cross-system group. Sysplex services are no longer active for that server. This message is displayed by each active LDAP server when an LDAP server leaves the cross-system group.

In the message text:

```
  system_name
    System name

group_name
  Cross-system group name
```

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD1148E Unable to set cross-system group owner:
Return code return_code, Reason code x’reason_code’.

Explanation: The LDAP server is unable to set the owner for the cross-system group. The return code has the following values:

1  IXCSETUS failed. The reason code contains the IXCSETUS return code in the upper 16 bits and the IXCSETUS reason code in the lower 16 bits. See the description of IXCSETUS in z/OS MVS Programming: Sysplex Services Reference for more information about the error.

In the message text:

```
  return_code
    Return code

  reason_code
    Reason code
```

Example: None.

System action: The LDAP server continues. Update operations to the LDAP server probably fail. Search operations might succeed.

---

GLD1149I  System system_name is leaving the sysplex.

Explanation: The LDAP server on the indicated system is leaving the sysplex and LDAP cross-system services are no longer available to this server.

In the message text:

```
  system_name
    System name
```

Example: None.

System action: The LDAP server issuing this message continues. If the server leaving the sysplex is the sysplex owner, another server becomes the sysplex owner. During that transition period, update operations to shared directories might fail.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD1150E Unable to send cross-system message:
Return code return_code, Reason code x’reason_code’.

Explanation: The LDAP server is unable to send a message to another member of the LDAP cross-system group. The return code has the following values:

2  XCF services are not available.
No response received.

Insufficient storage available on source system.

Insufficient storage available on target system.

Target member not defined.

Target member not active.

**IXCMSGO** failed. The reason code contains the **IXCMSGO** return code in the upper 16 bits and the **IXCMSGO** reason code in the lower 16 bits. See the description of **IXCMSGO** in [z/OS MVS Programming: Sysplex Services Reference](https://www.ibm.com) for more information about the error.

**IXCMSGI** failed on the target system. The reason code contains the **IXCMSGI** return code in the upper 16 bits and the **IXCMSGI** reason code in the lower 16 bits. See the description of **IXCMSGI** in [z/OS MVS Programming: Sysplex Services Reference](https://www.ibm.com) for more information about the error.

**IXCMSGI** failed on the source system. The reason code contains the **IXCMSGI** return code in the upper 16 bits and the **IXCMSGI** reason code in the lower 16 bits. See the description of **IXCMSGI** in [z/OS MVS Programming: Sysplex Services Reference](https://www.ibm.com) for more information about the error.

Message canceled or timed out.

Unknown notification response.

In the message text:

```
return_code
  Return code

reason_code
  Reason code
```

**Example:** None.

**System action:** The LDAP server might continue or might end, depending on which function attempted to send a message.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. Stop the server and then restart the program. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

---

**GLD1152E** • **GLD1152E**

Time limit exceeded while loading schema from group owner.

**Explanation:** The LDAP server waits a maximum of 30 seconds after requesting a copy of the schema from the LDAP cross-system owner. The owning LDAP
server is not responding to cross-system requests.

Example: None.

System action: If the error occurs during LDAP server initialization, the server ends. If the error occurs when requesting the new schema after it is modified by the schema owner, the server continues to run with its current (unmodified) schema. Add and modify operations that involve the modified schema elements might fail on this server.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Determine the owning system by issuing the LDAP server DISPLAY XCF operator modify command for the LDAP server reporting the error. The command output indicates which LDAP server is the group owner. Then issue the DISPLAY XCF operator modify command for the owning LDAP server and verify that this server is really the group owner. Restart the owning LDAP server if there is no response to the DISPLAY XCF operator modify command. Restart this LDAP server if it ended or if the updated schema is needed. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1154E A database name is required in multi-server mode.

Explanation: A backend name must be specified on the database option for an LDBM, TDBM, CDBM, or GDBM backend in the LDAP server configuration file when multi-server mode is enabled for the backend. Multi-server mode is enabled by specifying the serverSysplexGroup option in the global section and the multiserver on option in the backend section of the LDAP server configuration file.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Specify a backend name on the database option in the LDAP server configuration file. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1153E The schema owner cannot be contacted.

Explanation: The LDAP server is unable to contact the schema owner to obtain a copy of the current schema.

Example: None.

System action:

- If the error occurs during LDAP server initialization, the server ends.
- If the error occurs when requesting the new schema after it is modified by the schema owner, the server continues with its current (unmodified) schema. Add and modify operations that involve the modified schema elements might fail on this server.
- If the error occurs while sending a schema modify request to the schema owner, the server continues but the schema modify request fails.

Operator response: None.

User response: None.

System programmer response: None.
GLD1155E The database name may not exceed 8 characters in multi-server mode.

Explanation: The backend name for an LDBM, TDBM, CDBM, or GDBM backend has a maximum length of 8 characters when multi-server mode is enabled for the backend. Multi-server mode is enabled by specifying the serverSysplexGroup option in the global section and the multiserver on option in the backend section of the LDAP server configuration file.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Specify a valid backend name on the database option in the LDAP server configuration file. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1156E A fully-qualified path must be specified for the database directory.

Explanation: The directory specified by the databaseDirectory option in the LDBM, CDBM, or GDBM backend section of the LDAP server configuration file must be a fully-qualified path. That is, the path must start with a ‘/’.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Specify a fully-qualified path on the databaseDirectory option in the LDAP server configuration file. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1157E Multi-server mode requires cross-system services.

Explanation: The multiserver option in a backend section of the LDAP server configuration file cannot be set on unless cross-system services are configured. Cross-system services are configured by specifying the name of the LDAP cross-system group on the serverSysplexGroup option in the global section of the configuration file.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Either add the serverSysplexGroup option to the global section of the configuration file or set the multiserver option off in the backend section (or remove it from the backend section). Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1158E Multi-server change log support is required.

Explanation: The multiserver option in the GDBM section of the LDAP server configuration file must be set on because there is another backend section that has multiserver set on. When GDBM is configured, all LDBM, TDBM, CDBM, and GDBM backends must have the same setting for the multiserver option.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Either set the multiserver option in the GDBM section of the LDAP server configuration file on or set all the multiserver options off. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.
GLD1159E Multi-server support required for all LDBM, TDBM, CDBM, and GDBM backends.

Explanation: If the GDBM backend is configured, the multiserver option in the LDBM, TDBM, or CDBM section of the LDAP server configuration file must be set on because the GDBM section has multiserver set on. If the CDBM backend is configured, the multiserver option in the LDBM, TDBM, or GDBM section of the LDAP server configuration file must be set on because the CDBM section has multiserver set on. When a GDBM or CDBM backend is configured, all LDBM, TDBM, CDBM, and GDBM backends must have the same setting for the multiserver option.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Either set the multiserver option on in the LDBM, TDBM, CDBM, and GDBM backend sections of the LDAP server configuration file or set all the multiserver options off. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1161E The option1 configuration option requires the option2 configuration option.

Explanation: Certain LDAP server configuration options and values are dependent on other configurations options being specified to provide complete configuration information. Note that the value of some configuration options may be specified as a command-line parameter when starting the LDAP server (in this case, the command-line parameter overrides the value in the configuration file).

In the message text:

option1
   LDAP server configuration option

option2
   LDAP server configuration option

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: If option1 is needed, then either add option2 to the configuration file or change the value of option2 to support option1. If option1 is not needed, then either remove option1 or change its value to one that does not require option2. Then restart the program.

Problem determination: Not applicable.
GLD1162E  Configuration options option1 and option2 are mutually exclusive.

Explanation: The two options indicated in the message cannot both be specified in the same LDAP server configuration file.

In the message text:

option1  Configuration option one
option2  Configuration option two

Example: None.

System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.

GLD1163I  Replication status

Explanation: This message is displayed in response to the LDAP server DISPLAY REPLICAS operator modify command when there are no peer or replicas servers. It can also be displayed if the LDAP server that received the operator modify command is in a sysplex but is not the sysplex owner. Only the LDAP server that is the cross-system group owner has information about peer and replica servers.

Example: None.

System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: If this LDAP server is in a sysplex and is not the cross-system group owner, issue the LDAP server DISPLAY XCF operator modify command against this LDAP server to determine the cross-system group owner. Then direct the DISPLAY REPLICAS operator modify command to the group owner.

Problem determination: Not applicable.

GLD1165I  The LDAP server is in maintenance mode.

Explanation: The LDAP server has entered maintenance mode either because the LDAP server MAINMODE ON operator modify command is issued or because the -m command-line parameter is specified when the LDAP server is started.

Example: None.

System action: The LDAP server changes to maintenance mode. Update requests are accepted only from users who are bound with the distinguished name specified on the adminDN, masterServerDN, or peerServerDN options in the LDAP server configuration file.

Operator response: None.
GLD1166I LDAP server maintenance mode has ended.

Explanation: The LDAP server is no longer in maintenance mode, due to usage of the LDAP server MAINTMODE OFF operator modify command.

Example: None.
System action: The LDAP server changes to regular mode. Update requests are now accepted from all users.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1167I The LDAP server is already in maintenance mode.

Explanation: The LDAP server MAINTMODE ON operator modify command is issued when the LDAP server is already in maintenance mode.

Example: None.
System action: The LDAP server continues in regular mode.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1169E The option configuration option must be the same for all TDBM and DB2-based GDBM backends.

Explanation: The indicated option must be specified, with the same value, in all TDBM and DB2-based GDBM backends in the LDAP server configuration file.

In the message text:

option

LDAP server configuration option

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Either specify the same option and value in all TDBM and DB2-based GDBM backend sections or remove the option from all TDBM and DB2-based GDBM backend sections in the LDAP server configuration file. Then restart the program.

Problem determination: Not applicable.
Source: LDAP
GLD1171E  GLD1174E

Module:  None.
Routing code:  None.
Descriptor code:  None.
Automation:  Not applicable.

GLD1171E  Native return code return_code, SQL state state, SQL message: error_text

Explanation:  The LDAP server encountered an error while performing a DB2 database operation. See IBM Information Management Software for z/OS Solutions Information Center at http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/index.jsp for more information about DB2 errors.

In the message text:

- return_code
  Native return code
- state
  SQL state
- error_text
  SQL message text

Example:  None.

System action:  The backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends.

Operator response:  None.
User response:  None.
System programmer response:  None.
Administrator response:  Use the information in this message and the additional messages to correct the error. Restart the program if it ended or if the backend is needed. If the problem is unable to be resolved, contact the DB2 database administrator.

Problem determination:  Not applicable.
Source:  LDAP

GLD1174E  LDAP server stopping because DB2 is terminating.

Explanation:  The LDAP server DB2 monitor has detected that the DB2 database manager is ending. The LDAP server ends also because the db2Terminate option in the LDAP server configuration file is set to terminate.

Example:  None.

System action:  The program ends.
Operator response:  None.
User response:  None.
System programmer response:  None.
Administrator response:  Restart the LDAP server when the DB2 database manager is available. If the LDAP server should not terminate when the DB2 database manager ends, change the db2Terminate option.

GLD1172E  Error code error_code received for ODBC function name.

Explanation:  The LDAP server encountered an error for an ODBC (Open Database Connectivity) function. This message may be followed by additional messages providing further information about the error. See IBM Information Management Software for z/OS Solutions Information Center at http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/index.jsp for more information about ODBC errors.

In the message text:

- error_code
  Error code
- name
  ODBC function name

Example:  None.

System action:  The backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends.

Operator response:  None.
User response:  None.
System programmer response:  None.
Administrator response:  Use the information in this message and the additional messages to correct the error. Restart the program if it ended or if the backend is needed. If the problem is unable to be resolved, contact the DB2 database administrator.

Problem determination:  Not applicable.
Source:  LDAP

Module:  None.
Routing code:  None.
Descriptor code:  None.
Automation:  Not applicable.
option to recover or remove the option from the LDAP server configuration file.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1175E** Unable to establish DB2 monitor connection: type return code return_code, reason code reason_code.

**Explanation:** The LDAP server is unable to establish a connection with the DB2 server. The return code and reason code are from the CONNECT function if the type is DSNALI or from the IDENTIFY function if the type is DSNRLI. See [IBM Information Management Software for z/OS Solutions Information Center](http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/index.jsp) for more information about the error.

In the message text:

- **type** DB2 attachment facility type
- **return_code** Return code
- **reason_code** Reason code

**Example:** None.

**System action:** If the error occurs in the LDAP server during initialization, then the DB2-based backends do not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. If the error occurs after server initialization, the DB2-based backends are disabled and all requests to those backends are rejected.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. Verify that the encryption keys data set exists and can be accessed by the LDAP server or utility. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1177E** Unable to open the encryption keys dataset: error_code/reason_code - error_text.

**Explanation:** The LDAP server or utility is unable to open the encryption keys data set. See the description of fopen() in [z/OS XL C/C++ Run-Time Library Reference](http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/index.jsp) for more information about the error. The keys data set is specified by the -k parameter on the utility command line. For the LDAP server, and for the utility when the -k parameter is not specified, the keys data set can be specified in the LDAPKEYS DD statement in the JCL used to start the server or utility.

In the message text:

- **error_code** Error code from fopen()
- **reason_code** Reason code from fopen()
- **error_text** Error text corresponding to the error code

**Example:** None.

**System action:** The utility ends. The LDAP server continues, but encryption and decryption of values using a key in the key data set might fail. In particular, this might result in bind failures if the userPassword attribute value cannot be decrypted.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. Verify that the encryption keys data set exists and can be accessed by the LDAP server or utility. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1177E** Unable to read the encryption keys dataset: error_code/reason_code - error_text.

**Explanation:** The LDAP server or utility is unable to read the encryption keys data set. See the description of fgets() in [z/OS XL C/C++ Run-Time Library Reference](http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/index.jsp) for more information about the error. The keys data set is
specified by the -k parameter on the utility command line. For the LDAP server, and for the utility when the -k parameter is not specified, the keys data set can be specified in the LDAPKEYS DD statement in the JCL used to start the server or utility.

In the message text:

```
error_code
   Error code from fgets()
reason_code
   Reason code from fgets()
error_text
   Error text corresponding to the error code
```

Example: None.

System action: The utility ends. The LDAP server continues, but encryption and decryption of values using a key in the key data set might fail. In particular, this might result in bind failures if the userPassword attribute value cannot be decrypted.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Verify that the encryption keys data set has not been corrupted and that there are no I/O (input/output) errors. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1178E  The schema owner busy, retrying.

Explanation: The LDAP server which is the owner of the schema in the LDAP cross-system group in the sysplex is currently busy and cannot send the schema.

Example: None.

System action: The LDAP server continues and tries the request again.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: If the problem persists, restart the LDAP server that owns the schema. If the problem still persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1178E  The option configuration option value must be different for each type backend.

Explanation: The indicated option in the LDAP server configuration file must have a unique value for each backend section in which it is included.

In the message text:

```
option
   Configuration option name
type
   Backend type
```

Example: The dbuserid value must be unique for each DB2-based backend (TDBM and DB2-based GDBM). Different backends cannot share a DB2 database.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Correct the LDAP server configuration file so that the option value is unique throughout the LDAP server configuration file. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1180I  Activity log option processed: option.

Explanation: The indicated activity log option specified on an LDAP server LOG operator modify command has successfully been processed.

In the message text:

```
option
   Activity log option
```

Example: None.

System action: The LDAP server continues, with activity logging using the indicated log option.

Operator response: None.

User response: None.
**GLD1181E**  Incorrect LDAP server activity log option specified: option.

**Explanation:** An activity log option that is not valid is specified on an LDAP server LOG operator modify command.

In the message text:

```
option
Incorrect activity log option
```

**Example:** None.

**System action:** The LDAP server continues, with no change to activity logging.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1182A**  Unable to initialize activity logging.

**Explanation:** The LDAP server cannot initialize the activity logging facility. A previous message indicates the reason for the failure.

**Example:** None.

**System action:** The LDAP server ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1185I**  LDAP server audit option processed: option.

**Explanation:** The indicated audit option specified on an LDAP server AUDIT operator modify command has successfully been processed.

In the message text:

```
option
Audit option
```

**Example:** None.

**System action:** The LDAP server continues, with auditing using the indicated option.

**Operator response:** None.

**User response:** None.
GLD1186E  Incorrect LDAP server audit option specified: option.

Explanation: An audit option that is not valid is specified on an LDAP server AUDIT operator modify command.

In the message text:

option
  Incorrect audit option

Example: None.

System action: The LDAP server continues, with no change to auditing.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Retry the AUDIT operator modify command using a valid audit option.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD1187I  LDAP server SMF auditing ON.

Explanation: LDAP server auditing is activated, either by way of the audit option in the LDAP server configuration file or the LDAP server AUDIT operator modify command.

Example: None.

System action: The LDAP server continues, without auditing activated.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: If auditing is needed, use the LDAP server AUDIT operator modify command to turn on LDAP server auditing.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD1188I  LDAP server audit settings updated with values values.

Explanation: The LDAP server is updated with the indicated audit settings. The audit settings are specified either in the audit option in the LDAP server configuration file or on the LDAP server AUDIT operator modify command.

In the message text:

values
  String representation of audit values

Example: None.

System action: The LDAP server continues, with auditing using the indicated values.

Operator response: None.
GLD1190I  Audit status
Explanation: This message displays the current LDAP server audit settings as a result of issuing the LDAP server DISPLAY AUDIT operator modify command.
Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: The LDAP server DISPLAY AUDIT operator modify command can be used to review the current LDAP server auditing settings. Use the LDAP server AUDIT operator modify command to make any necessary updates.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1193E  XCF send for name timed out, retrying.
Explanation: XCF was unable to complete the send of a request from the indicated backend to the owner of the resource in the LDAP server cross-system group.
In the message text:
name
  Backend name
Example: None.
System action: The LDAP server continues and tries the request again.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: If the problem persists, restart this LDAP server and the LDAP server that owns the resource. If the problem still persists, contact the service representative.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1191I  LDAP server auditing is only available on V1R7 and above.
Explanation: LDAP server auditing is unavailable on this level of z/OS.
Example: None.
System action: The LDAP server continues. No audit records are created.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: The LDAP server DISPLAY AUDIT operator modify command can be used to review the current LDAP server auditing settings. Use the LDAP server AUDIT operator modify command to make any necessary updates.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1194I  Component Trace has been successfully started for GLDSRVR.
Explanation: Component TRACE (CTRACE) has successfully started on the LDAP server in CTRACE component name GLDSRVR. The LDAP server writes CTRACE records to a subnode under the GLDSRVR component name.
Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
**GLD1195A** Unable to start ctrace: Error return_code, Reason reason_code.

Explanation: The LDAP server cannot identify its component tracing facility to the z/OS CTRACE subsystem. See the description of CTRACE DEFINE in z/OS MVS Programming: Authorized Assembler Services Reference ALE-DYN for more information about the error.

In the message text:
- **return_code**: Return code from CTRACE DEFINE
- **reason_code**: Reason code from CTRACE DEFINE

Example: None.

System action: The program continues, but component trace is not used.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Restart the program if component tracing is needed. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

**GLD1197I** Active trace points now written to memory and trace file for GLDSRVR.

Explanation: The LDAP debug output generated by the LDAP server is written to both memory and the output trace file. The LDAP_DEBUG_FILENAME environment variable specifies the output trace filename. If the LDAP_DEBUG_FILENAME environment variable is not specified, then LDAP debug output goes to stdout.

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

**GLD1196I** Active trace points only written to memory now for GLDSRVR.

Explanation: The LDAP debug output generated by the LDAP server is only written to memory.

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

**GLD1198E** Unable to open logfile filename: error_code/reason_code - error_text

Explanation: The LDAP server is unable to open a log file. See the description of fopen() in z/OS XL C/C++ Run-Time Library Reference for more information about the error. For activity logging, the name of the file is specified by the logfile option in the LDAP server configuration file. The default log file name is /etc/ldap/gldlog.output if the configuration option is not specified. For replication error logging, the name of the file is specified by the ibm-slapdLog attribute in the replica entry.

In the message text:
- **filename**: Log file file name
- **error_code**: Error code from fopen()
**GLD1199I • GLD1201I**

*reason_code*

Reason code from `fopen()`

*error_text*

Error text corresponding to the error code

**Example:** None.

**System action:** The LDAP server continues, but logging using this file is not done. For replication, replication to the replica server using this log might stall.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Verifying that the LDAP server has write access to the log file and to its directory if the file does not exist. Restart the program if logging is needed.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1199I** The backend named `name` has been set to read-only mode.

**Explanation:** The indicated backend is successfully set to read-only mode after the LDAP server `BACKEND` operator modify command is issued.

In the message text:

`name`

Backend name

**Example:** None.

**System action:** The program continues.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1200I** The backend named `name` has been set to read/write mode.

**Explanation:** The indicated backend is successfully set to read/write mode after the LDAP server `BACKEND` operator modify command is issued.

In the message text:

`name`

Backend name

**Example:** None.

**System action:** The program continues.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1201I** The backend named `name` is already set to read-only mode.

**Explanation:** The indicated backend is already running in read-only mode. The LDAP server `BACKEND` operator modify command is ignored.

In the message text:

`name`

Backend name

**Example:** None.

**System action:** The program continues.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
GLD1202I  The backend named *name* is already set to read/write mode.

Explanation: The indicated backend is already running in read/write mode. The LDAP server **BACKEND** operator modify command is ignored.

In the message text:

*name*  Backend name

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1203E  Incorrect LDAP server backend option specified: *options*.

Explanation: An option that is not valid is specified on the LDAP server **BACKEND** operator modify command.

In the message text:

*options*  Options specified on LDAP server **BACKEND** operator modify command

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1204I  Schedule commit for all backends completed.

Explanation: A database commit resulting from an LDAP server **COMMIT** operator modify command has successfully completed on all backends.

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1205I  Schedule commit for all backends failed.

Explanation: A database commit resulting from an LDAP server **COMMIT** or **BACKEND** operator modify command has failed. A previous message may indicate the reason for the failure.

Example: None.

System action: The program continues, but the operator modify command fails. One or more databases are not been committed.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the earlier message (if any) to correct the error. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
GLD1206I  Only sysplex owner can perform command.

Explanation: A database commit resulting from an LDAP server COMMIT or BACKEND operator modify command has failed because the LDAP server is not the owner of the backend database in the sysplex. Only the LDAP server that is the database owner in the LDAP cross-system group can process this command.

Example: None.

System action: The program continues, but the operator modify command fails. One or more databases are not been committed.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Retry the operator modify command, directing it to the LDAP server that is the database owner in the sysplex.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1207E  type backend specified for a non-type database.

Explanation: The LDAP server or utility found that the backend type specified on a database option in the LDAP server configuration file does support the backend DLL specified on the configuration option.

Example: None.

System action: The backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the earlier message to correct the error in the LDAP server configuration file. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1208E  Configuration for type backend named name failed.

Explanation: The LDAP server backend indicated in the message cannot be started due to a configuration error. A previous message indicates the reason for the failure.

In the message text:

- type Backend type
- name Backend name

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1209E  Unable to obtain file lock with fcntl() on filename: error_code/reason_code - error_text

Explanation: The LDAP server or utility is not able to obtain a read or write lock on the file indicated in the message. See the description of fcntl() in [z/OS XL C/C++ Run-Time Library Reference](https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.2.0/com.ibm.zos.v2r2.doc/xlc/lm_rstlibref.html) for more information about the error.

In the message text:

- filename File name
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1210E • GLD1212E

GLD1210E Terminating LDAP server because tcpTerminate option is set to 'terminate'.
Explanation: The LDAP server has detected that there are no active network interfaces or has found an error while initializing SSL or Kerberos. The LDAP server is ending because the tcpTerminate option in the LDAP server configuration file is set to terminate.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1212E Unable to chmod file filename: error_code/reason_code - error_text
Explanation: The LDAP server or utility is unable to change the permission bits on the indicated file. The failing routine can be fchmod() or chmod(). See the
**GLD1213E**

Description of these routines in [z/OS XL C/C++ Run-Time Library Reference](https://www.ibm.com) for more information about the error.

In the message text:

- **filename**
  - LDBM database, CDBM database, schema file name, or replication error log

- **error_code**
  - Error code from routine

- **reason_code**
  - Reason code from routine

- **error_text**
  - Error text corresponding to the error code

**Example:** None.

**System action:**
- If the error occurs during backend initialization, the backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to *ignore*, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to *terminate* (this is the default if the configuration option is not specified), the program ends.
- If the error occurs while executing the `ds2ldif` utility to unload an LDBM or CDBM backend, an `unloadRequest` extended operation is attempted to unload the wanted backend data.
- If the error occurs during an LDBM, CDBM, or GDBM operation, then, if the `fileTerminate` option in the LDAP server configuration file is set to *recover* (this is the default if the configuration option is not specified), the server continues to run but the LDBM, CDBM, or GDBM backend is placed in read-only state. If the `fileTerminate` option is set to *terminate*, the program ends.
- For a replication error log file, the permission bits are changed when the file is first created. If an error occurs at this point, the replication error information is written to the error log file the next time a replication error occurs.
- If the error occurs while attempting to modify the global schema, the schema modification fails but the updates to the schema are saved in the `schema.db.new` file.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. Ensure that the LDAP server has the appropriate authority to change permission bits on all of the LDBM, CDBM, GDBM (file-based), schema, and replication error log files. Also ensure that the user ID that is running the `ds2ldif` utility is a superuser or is the owner of the LDBM or CDBM database files or in the same group as the LDAP server user ID. See [Setting up the user ID and security for the LDAP server](https://www.ibm.com) for more information about giving the authority to perform permission bit updates on the files. Restart the program if it ended or if the backend did not start and is needed. If an LDBM, CDBM, or GDBM backend was placed in read-only state, it can be reset to read/write state by restarting the LDAP server or by using the LDAP server `BACKEND` operator modify command. For a schema update, reissue the schema modify request.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**Explanation:** The LDAP server or utility is unable to change the owner or group of the indicated database file. The failing routine can be `fchown()` or `chown()`. See the description of these routines in [z/OS XL C/C++ Run-Time Library Reference](https://www.ibm.com) for more information about the error.

In the message text:

- **filename**
  - LDBM database or schema file name

- **error_code**
  - Error code from routine

- **reason_code**
  - Reason code routine

- **error_text**
  - Error text corresponding to the error code

**Example:** None.

**System action:**
- If the error occurs during backend initialization, the backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to *ignore*, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to *terminate* (this is the default if the configuration option is not specified), the program ends.
- If the error occurs while executing the `ds2ldif` utility to unload an LDBM or CDBM backend, an `unloadRequest` extended operation is attempted to unload the wanted backend data.
- If the error occurs during an LDBM, CDBM, or GDBM operation, then, if the `fileTerminate` option in the LDAP server configuration file is set to *recover* (this is the default if the configuration option is not specified), the server continues to run but the LDBM, CDBM, or GDBM backend is placed in read-only state. If the `fileTerminate` option is set to *terminate*, the program ends.

---

**GLD1213E** Unable to chown file `filename`:

(error_code)reason_code - (error_text)

**Explanation:** The LDAP server or utility is unable to change the owner or group of the indicated database file. The failing routine can be `fchown()` or `chown()`. See the description of these routines in [z/OS XL C/C++ Run-Time Library Reference](https://www.ibm.com) for more information about the error.

In the message text:

- **filename**
  - LDBM database or schema file name

- **error_code**
  - Error code from routine

- **reason_code**
  - Reason code routine

- **error_text**
  - Error text corresponding to the error code

**Example:** None.

**System action:**
- If the error occurs during backend initialization, the backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to *ignore*, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to *terminate* (this is the default if the configuration option is not specified), the program ends.
- If the error occurs while executing the `ds2ldif` utility to unload an LDBM or CDBM backend, an `unloadRequest` extended operation is attempted to unload the wanted backend data.
- If the error occurs during an LDBM, CDBM, or GDBM operation, then, if the `fileTerminate` option in the LDAP server configuration file is set to *recover* (this is the default if the configuration option is not specified), the server continues to run but the LDBM, CDBM, or GDBM backend is placed in read-only state. If the `fileTerminate` option is set to *terminate*, the program ends.

---

**IBM Tivoli Directory Server Messages and Codes for z/OS V1R13.0**
If the error occurs while attempting to modify the global schema, the schema modification fails but the updates to the schema are saved in the schema.db.new file.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. Ensure that the LDAP server has the appropriate authority to change the owner on all of the LDBM, CDBM, GDBM (file-based), and schema files. Also ensure that the user ID that is running the ds2ldif utility is a superuser or is the owner of the LDBM or CDBM database files or in the same group as the LDAP server user ID. See Setting up the user ID and security for the LDAP server for more information about giving the authority to perform ownership updates on the files. Restart the program if it ended or if the backend did not start and is needed. If an LDBM, CDBM, or GDBM backend was placed in read-only state, it can be reset to read/write state by restarting the LDAP server or by using the LDAP server BACKEND operator modify command. For a schema update, reissue the schema modify request.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1215A**  Unable to complete schema change due to failure in backend name: return code return_code - error_text

**Explanation:** During schema initialization or after schema modification, each active backend is notified that the schema has changed so that the backend can do any needed processing to use the new schema. In particular, if a TDBM backend is running in multi-server mode and has a DB_VERSION less than 4, then it must update the schema entry within the TDBM database. An error occurred during backend processing for the new schema.

In the message text:

- **name** Backend name
- **return_code** LDAP return code
- **error_text** Error text

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
GLD1216E  Unable to send request for backend name to sysplex group owner: return code return_code.

Explanation: An error occurred while sending an XCF request to the LDAP cross-system group owner in the sysplex. The return code has the following values:

1  An unavailable XCF service.
80  An XCF error.

In the message text:

name  Backend name
return_code  Return code

Example: None.

System action: If the error occurs during LDAP server initialization, the program ends. If the error occurs after initialization, the LDAP server continues if the LDAP server schema is still usable; otherwise the program ends.

Operator response: None.
User response: None.

System programmer response: None.
Administrator response: Use the information in the message to correct the error. Verify that the XCF service is available. Restart the program if it ended. If the problem persists, contact the service representative.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1218E  operation operation failed for dn to host:port, rc=return_code setting change aside into filename

Explanation: The LDAP server is unable to replicate a change to the indicated server. The change is removed from the replication queue and placed in the replication error log file.

In the message text:

operation  Operation name
dn  Distinguished name of entry to replicate
host  Replica server host name
port  Replica server port number
return_code  LDAP return code
filename  Replication error log file name

Example: None.

System action: The LDAP server continues. Replication to the indicated replica server continues.

Operator response: None.
User response: None.

System programmer response: None.
Administrator response: Examine the replication error log to determine the cause of the failure. Fix the problem on the replica server. Then apply the change in the replication error log to the replica server.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD1219I  The amount of replication changes set aside has reached the maximum for error log filename.

Explanation: The number of changes set aside into the replication error log since the LDAP server was last started has reached the maximum allowed. The maximum number is set in the ibm-slapdReplMaxErrors attribute in the replica entry.

In the message text:

filename
  Replication error log file name

Example: None.

System action: The LDAP server continues. Replication to the indicated server continues, although it might stall. Future replication failures will not be set aside.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the replication error log to correct the replication errors and apply the changes to the replica. To enable future operations to be set aside, restart the LDAP server, delete and add the replication entry, or increase the value of the ibm-slapdReplMaxErrors attribute in the replica entry. Note that these actions do not delete anything from the replication error log; they allow additional changes to be set aside into the error log.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1220I  Replication to replica hostport has stalled.

Explanation: A failed replication operation is preventing other replication operations from occurring.

In the message text:

host
  Replica server host name

port
  Replica server port number

Example: None.

System action: The LDAP server continues. The replication operation is tried again.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the replication error log to correct the error on the replica server, then wait for the replication operation to be tried again. If necessary, resynchronize the replica server. See Recovering from basic replication out-of-sync conditions for more information.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1221E  Unable to write to file filename: error_code/reason_code - error_text.

Explanation: The LDAP server is unable to write to the indicated file. See the description of fprintf() or fwrite() in z/OS XL C/C++ Run-Time Library Reference for more information about the error. If the indicated file is a replication error log, the file name is specified by the ibm-slapdLog attribute in the replica entry. If the indicated file is the activity log, an error occurred while writing an activity log record.

In the message text:

filename
  File name

error_code
  Error code from fprintf() or fwrite()

reason_code
  Reason code from fprintf() or fwrite()

error_text
  Error text corresponding to the error code

Example: None.

System action: The LDAP server continues. If the error occurs while writing to the replication error log, some information about the replication error cannot be written to the log and the replication operation cannot be set aside. In this case, the replication operation is tried again and replication stalls if it is not successful. If the error occurs while writing an activity log record, the LDAP server automatically turns off activity logging.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the replication error log to correct the replication errors and apply the changes to the replica. To enable future operations to be set aside, restart the LDAP server, delete and add the replication entry, or increase the value of the ibm-slapdReplMaxErrors attribute in the replica entry. Note that these actions do not delete anything from the replication error log; they allow additional changes to be set aside into the error log.
message to correct the error. Verify that the file can be written to by the LDAP server and is not full. If the error occurred while writing an activity log record, use the LDAP server LOG operator modify command to activate activity logging after the error is corrected.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1222I** End display output

**Explanation:** This message is displayed at the end of the output of the LDAP server DISPLAY AUDIT operator modify command.

**Example:** None.

**System action:** The LDAP server continues.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1224I** Backend status

**Explanation:** This message is displayed at the beginning of the output of the LDAP server DISPLAY BACKEND operator modify command. The status of each backend follows.

**Example:** None.

**System action:** The LDAP server continues.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1225I** Maintenance Mode status

**Explanation:** This message is displayed at the beginning of the output of the LDAP server DISPLAY MAINTMODE operator modify command. The maintenance mode status follows.

**Example:** None.

**System action:** The LDAP server continues.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1226I  Debug settings
Explanation: This message is displayed at the beginning of the output of the LDAP server DISPLAY DEBUG operator modify command. The debug settings follow.
Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1227I  This LDAP server has become LDAP sysplex group owner.
Explanation: The LDAP server is the database owner in the LDAP cross-system group in the sysplex. This can occur during LDAP server initialization if the server is the first server to join the sysplex group. It can also occur if the LDAP server assumes ownership of the sysplex group because the LDAP server that was the group owner has stopped.
Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1229E  Environment variable file cannot be opened. Processing is continuing without setting additional environment variables.
Explanation: The LDAP server or utility is unable to open the environment variables file. The name of the file is specified in the current value of the
LDAP_DS_ENNVARS_FILE environment variable. If this environment variable is not defined, the file name is specified by the //DD:ENVVAR statement in the procedure used to start the program. If the file in the DD statement cannot be opened, the program attempts to open /etc/ldap/ds.envvars.

Example: None.

System action: The program continues without setting additional environment variables.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that an environment variables file exists and can be read. Restart the program if environment variables must be set.

Problem determination: Not applicable.

Source: LDAP

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1230E Environment variable ignored because line is too long: line line_number, file filename.

Explanation: The LDAP server or utility encountered a line that is too long in its environment variables file. The total length of a line (including any continuation lines) must be less than 1024 characters.

In the message text:

```
line_number
  Line number

filename
  Environment variables file name
```

Example: None.

System action: The program continues without setting the environment variable on the indicated line.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1232E Environment variable ignored because name is NULL: line line_number, file filename.

Explanation: The LDAP server or utility encountered an incorrect line in its environment variables file. An environment variable line consists of name=value but the indicated line does not contain an = sign.

In the message text:

```
line_number
  Line number

filename
  Environment variables file name
```

Example: None.

System action: The program continues without setting the environment variable on the indicated line.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify the contents of the environment variables file. Restart the program if the environment variable must be set.

Problem determination: Not applicable.

Source: LDAP

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
GLD1233E  Environment variable is ignored because value could not be set: line line_number, file filename.

Explanation: An attempt by the LDAP server or utility to set an environment variable failed.

In the message text:

line_number
  Line number

filename
  Environment variables file name

Example: None.

System action: The program continues without setting the environment variable on the indicated line.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify the contents of the environment variables file. Restart the program if the environment variable must be set.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1234E  Last line in environment variables file ignored because it has a continuation character: line line_number, file filename.

Explanation: The LDAP server or utility found a continuation character at the end of the last line in its environment variables file. The line is ignored because there is no continuation line.

Example: None.

System action: The program continues without setting the environment variable on the indicated line.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify the contents of the environment variables file. Restart the program if the environment variable must be set.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1237E  Incomplete shutdown processing; some data may not be committed and resources not freed.

Explanation: During LDAP server shutdown processing, the server waits 60 seconds for all requests in process to complete. If the requests complete, then each backend is notified to free any resources and commit any data. The requests did not complete, thus the backends are not notified.

Example: None.

System action: The backends do not commit data and do not free resources.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Restart the LDAP server and reissue any incomplete requests.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.
GLD1238E  Unable to decode a request for type backend named name because attribute type attribute is not defined.

Explanation: The LDAP server found an attribute type used in a request for the indicated backend but the attribute type is not defined in the LDAP server schema.

In the message text:

type
  Backend type
name
  Backend name
attribute
  Undefined attribute type

Example: None.

System action: The request fails. The program might end depending on when the error occurs. A follow-on message indicates the effect on the program.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Check the system log for an earlier message indicating a cross-system communication error. After correcting the problem, restart this LDAP server to synchronize the indicated database with the group owner.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1241W  The option1 configuration option value value cannot be used because it is not in a configured suffix and option2 is not specified.

Explanation: The distinguished name specified for the LDAP root administrator (adminDN), peer server (peerServerDN), or master replica server (masterServerDN) in the LDAP server configuration file cannot be used to bind to the LDAP server because the password is not specified, either in the corresponding password configuration option (adminPW, peerServerPW, or masterServerPW) or in an entry for the distinguished name in the directory. The DN does not fall under any of the suffixes in the LDAP server configuration file or any of the suffixes added by plug-in extensions to the LDAP server, thus there cannot be an entry for the DN in the directory.

In the message text:

option1
  LDAP server configuration option
value
  LDAP server configuration option value
option2
  LDAP server configuration option

Example: None.

System action: The program continues but the LDAP root administrator, peer server DN, or master server DN cannot access the LDAP server.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: If intending to bind to the LDAP server using the root administrator, peer server, or master server distinguished name, it is recommended that the configuration option value be changed so that the DN falls under one of the suffixes.
in the LDAP server configuration file or one of the
suffixes added by plug-in extensions to the LDAP
server. Then restart the server and add an entry for the
distinguished name containing a `userPassword` value
to the directory. As a less-secure alternative, the
Corresponding password configuration option can be
added to LDAP server configuration file and then
restart the LDAP server.

**Problem determination:** Not applicable.
**Source:** LDAP
**Module:** None.
**Routing code:** None.
**Descriptor code:** None.
**Automation:** Not applicable.

---

**GLD1242W**  SDBM update operations and some
search operations cannot be performed
because there is no RACF address space.

**Explanation:** The SDBM backend has detected that the
RACF address space is not running. SDBM operations
that use the RACF address space fail and return a
return code of decimal 52 (LDAP_UNAVAILABLE -
'Directory server function is unavailable'). These
operations include all update operations and any
search operation that scans the RACF database using
the RACF SEARCH command. Binding to SDBM and
searches for a specific RACF user, group, connection, or
resource profile can be performed because they do not
use the RACF address space.

**Example:** None.
**System action:** The program continues but SDBM
update operations and some search operations cannot
be performed.
**Operator response:** None.
**User response:** None.
**System programmer response:** None.
**Administrator response:** None.
**Problem determination:** Not applicable.
**Source:** LDAP
**Module:** None.
**Routing code:** None.
**Descriptor code:** None.
**Automation:** Not applicable.

---

**GLD1244E**  Unable to analyze DB2 RUNSTATS
utility output.

**Explanation:** The LDAP server cannot analyze DB2
RUNSTATS utility output in the DB2 catalog. This
message is displayed when errors are encountered
during the LDAP server `REFRESH DB2RUNSTATS`
operator modify command.

**Example:** None.
**System action:** The LDAP server uses the updated
DB2 catalog statistics for those which were successfully
analyzed, but continues using the previous DB2 catalog
statistics for those which it could not process
successfully. Additional error messages might precede
this message which provides more details.
**Operator response:** None.
**User response:** None.
**System programmer response:** None.
**Administrator response:** None.
**Problem determination:** Not applicable.
**Source:** LDAP
**Module:** None.
**Routing code:** None.
**Descriptor code:** None.
**Automation:** Not applicable.
GLD1245E • GLD1247E

GLD1245E  Unable to get thread-specific value:
error_code/reason_code - error_text

Explanation: The LDAP server is unable to retrieve
thread specific information for a thread. See the
description of pthread_getspecific() in z/OS XL C/C++
Run-Time Library Reference for more information about
the error.

In the message text:

error_code
   Error code from pthread_getspecific()
reason_code
   Reason code from pthread_getspecific()
error_text
   Error text corresponding to the error code

Example: None.

System action: The program continues. The request
fails.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the
message to correct the error. Then try the request again.
If the problem persists, contact the service
representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1247E  Unable to create key identifier:
error_code/reason_code - error_text

Explanation: The LDAP server is unable to store
thread specific information for a thread. See the
description of pthread_key_create() in z/OS XL C/C++
Run-Time Library Reference for more information about
the error.

In the message text:

error_code
   Error code from pthread_key_create()
reason_code
   Reason code from pthread_key_create()
error_text
   Error text corresponding to the error code

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the
message to correct the error. Then restart the LDAP
server and try the request again. If the problem
persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1246E  Unable to set thread-specific value:
error_code/reason_code - error_text

Explanation: The LDAP server is unable to store
thread specific information for a thread. See the
description of pthread_setspecific() in z/OS XL C/C++
Run-Time Library Reference for more information about
the error.

In the message text:

error_code
   Error code from pthread_setspecific()
reason_code
   Reason code from pthread_setspecific()
error_text
   Error text corresponding to the error code

Example: None.
**GLD1248W** Unable to connect to DB2; will attempt retry current_retry of maximum_retries in number seconds.

**Explanation:** The LDAP server is unable to establish a connection with DB2 during LDAP server startup. It tries to connect to DB2 again. The LDAP server global configuration option `db2StartUpRetryLimit` sets the maximum number of times the LDAP server can try a DB2 connection again during server startup. The number of seconds to wait before each retry attempt is determined by the value of the `db2StartUpRetryInterval` LDAP server global configuration option. The LDAP server, by default, waits 45 seconds before each retry attempt.

In the message text:

`current_retry`  
Current retry attempt

`maximum_retries`  
Maximum retry attempts

`number`  
Interval before the next retry attempt

**Example:** None.

**System action:** The LDAP server waits for the specified number of seconds before trying to connect to DB2 again. If the final retry attempt is unsuccessful, then the DB2-based backends do not start.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the earlier message to correct the problem. Restart the program if it did not start or if DB2-based backends are needed.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

**GLD1250E** The option configuration option requires the type backend.

**Explanation:** The LDAP server or utility found an option in the LDAP server configuration file whose processing requires that a specific type of backend also be configured, but a backend of that type is not contained in the configuration file.

In the message text:

`option`  
LDAP server configuration option

`type`  
Backend type

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Either remove the option from the LDAP server configuration file or add a backend of the specified type to the configuration file. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

**GLD1248W • GLD1250E**

configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to terminate (this is the default if the configuration option is not specified), the LDAP server ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the earlier message to correct the problem. Restart the program if it did not start or if DB2-based backends are needed.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
GLD1251E  Schema database version \texttt{version1} not supported, highest supported \texttt{version2}.

**Explanation:** The LDAP server or utility found that the schema database is at a higher version level than is currently supported by the LDAP server. This indicates that the schema database may contain values that the LDAP server cannot process. The schema cannot be loaded from the database.

In the message text:

\texttt{version1}  
\texttt{database schema version}  
\texttt{version2}  
\texttt{server schema version}  

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Restore the LDAP server to the level used to create the schema database. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

GLD1252E  Unencrypted data from \texttt{IP_address1} has been sent to a secure connection on \texttt{IP_address2} port \texttt{port}.

**Explanation:** The LDAP server encountered unencrypted data sent from the IP address indicated in the message to a secure connection on the LDAP server. The server can only process encrypted data when using a secure connection.

In the message text:

\texttt{IP_address1}  
\texttt{Client IP address}  
\texttt{IP_address2}  
\texttt{Server IP address}  
\texttt{port}  
\texttt{Server port number}  

**Example:** None.

**System action:** The program continues, using the replacement configuration option or value. Support for the old configuration option or value may be removed in a future release of the LDAP server, resulting in the program ending.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Replace the old option or value with the new option or value in the LDAP server configuration file. If using a new option, ensure that the option is in the appropriate section of the configuration file. For example, if replacing the 'database ictx' option with the 'plug-in' option, move
GLD1254E  Plug-in initialization failed for plug-in named 'name'.

Explanation: The indicated plug-in failed to initialize. A previous message indicates the reason for the failure.

In the message text:

name
    Plug-in name

Example: None.

System action: The plug-in does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends and plug-ins that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the earlier message to correct the error. Restart the program if it did not start or if the plug-in is needed.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1256E  Replication entry 'name' is not supported in this replication configuration.

Explanation: The LDAP server or utility found a replication entry that is not supported in this replication configuration. If useAdvancedReplication on is specified in the LDAP server configuration file, then entries with an object class of replicaObject are not supported. If useAdvancedReplication off is specified in the LDAP server configuration file, then entries with object classes of ibm-replicationAgreement, ibm-replicationContext, ibm-replicationGroup, and ibm-replicationSubEntry are not supported. If running the ldif2ds utility, a previous message indicates the name of the LDIF file containing the entry.

In the message text:

name
    Entry distinguished name

Example: None.

System action:
- If the error occurs while running an LDAP utility, the program ends.
- If the error occurs during initialization of an LDAP server backend, then the backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the earlier message to correct the error. Restart the program if it did not start or if the plug-in is needed.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
System programmer response: None.

Administrator response:
- If `useAdvancedReplication on` is specified in the LDAP server configuration file, the LDAP server or utility does not support basic replication entries with an object class of `replicaObject`. If configuring a basic replication environment, change the `useAdvancedReplication` option setting from `on` to `off` to allow basic replication entries to be used. If configuring an advanced replication environment, then all entries with an object class of `replicaObject` must be removed from the LDAP server backend or the input LDIF file.
- If `useAdvancedReplication off` is specified in the LDAP server configuration file, the LDAP server or utility does not support advanced replication entries with object classes of `ibm-replicationAgreement`, `ibm-replicationContext`, `ibm-replicationGroup`, and `ibm-replicationSubEntry`. If configuring an advanced replication environment, change the `useAdvancedReplication` option setting from `off` to `on` to allow advanced replication entries to be used. If configuring a basic replication environment, then all entries with object classes of `ibm-replicationAgreement`, `ibm-replicationContext`, `ibm-replicationGroup`, and `ibm-replicationSubEntry` must be removed from the LDAP server backend or the input LDIF file.

Then restart the program.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

---

GLD1257E Multi-server configuration backend (CDBM) support is required.

Explanation: The `multiserver` option in the CDBM section of the LDAP server configuration file must be set on because there is another backend section that has `multiserver` set on. When CDBM is configured, all LDBM, TDBM, CDBM, and GDBM backends must have the same setting for the `multiserver` option.

Example: None.

System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.

Administrator response: Either set the `multiserver` option in the CDBM section of the LDAP server configuration file on or set all the `multiserver` options

off. Then restart the program.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

---

GLD1258E The operations monitor ID 'opid' is already associated with WLM transaction name 'name'.

Explanation: The operations monitor ID (OPID) specified on the LDAP server `WLMEXCEPT` operator modify command is already associated with a WLM transaction name. An OPID is only allowed to be associated with one WLM transaction name at a time.

In the message text:

```
    opid  operations monitor identifier
    name  WLM transaction name
```

Example: None.

System action: The LDAP server continues. The request fails.
Operator response: Contact the LDAP Administrator or see the Administrator response.
User response: None.
System programmer response: None.

Administrator response: Verify the OPID specified on the LDAP server `WLMEXCEPT` operator modify command is correct and is not already associated with a WLM transaction name. If the correct OPID was specified, issue the LDAP server `RESET WLMEXCEPT` operator modify command to remove the current OPID mapping. Then reissue the same LDAP server `WLMEXCEPT` operator modify command to set the OPID mapping to the WLM transaction name specified in the message.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
The operations monitor ID 'opid' is now associated with WLM transaction name 'name'.

Explanation: The operations monitor ID (OPID) is successfully associated with the WLM transaction name specified. Future client requests in the LDAP server that match the search pattern identified by the OPID are routed to the specified WLM transaction name.

In the message text:

\texttt{opid} \\
operations monitor identifier

\texttt{name} \\
WLM transaction name

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

Now setting the LDAP server health value to 'value' percent.

Explanation: The LDAP server has adjusted its internal health value to accurately reflect the number of errors that have occurred in the LDAP server. The health value is the number of failures that have occurred in the last 5000 client operations. The health value is only updated if one minute has passed since the internal health value was last set. The internal health value is used by the sysplex distributor to help distribute incoming client requests to the LDAP servers within the sysplex.

In the message text:

\texttt{value} \\
LDAP health percentage

Example: None.

System action: The LDAP server continues. The request fails.

Operator response: Issue an LDAP server \texttt{WLMEXCEPT} operator modify command with a valid OPID value. Contact the LDAP Administrator to determine a valid OPID value.

User response: None.

System programmer response: None.

Administrator response: Verify the OPID specified on the LDAP server \texttt{WLMEXCEPT} operator modify command is a valid number and exists as an id value in a search pattern returned on the \texttt{cn=operations,cn=monitor} entry.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
GLD1262E  The WLM transaction name 'name' is not valid.

Explanation: The WLM transaction name entered on the WLMEXCEPT operator modify command is not valid.

In the message text:

name  WLM transaction name

Example: None.

System action: The LDAP server continues. The request fails.

Operator response: Issue an LDAP server WLMEXCEPT operator modify command with a valid WLM transaction name. Contact the LDAP Administrator to determine a valid WLM transaction name.

User response: None.

System programmer response: None.

Administrator response: Verify the WLM transaction name specified on the LDAP server WLMEXCEPT operator modify command is 1 to 8 characters long. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1263I  wlmExcept reset completed.

Explanation: If an operations monitor ID (OPID) has been specified on the LDAP server RESET WLMEXCEPT operator modify command, then that OPID is no longer associated with a WLM transaction name. If an OPID has not been specified on the LDAP server RESET WLMEXCEPT operator modify command, then the LDAP server defaults to using only the configured wlmExcept options for routing incoming client requests to WLM transaction names.

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1264E  The Extended Operation owner cannot be contacted.

Explanation: The LDAP server is unable to contact the Extended Operation owner to request that a function be performed.

Example: None.

System action: An error is returned to the client requesting the operation, the LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Determine the owning system by issuing the LDAP server DISPLAY XCF operator modify command for the LDAP server reporting the error. The command output indicates which LDAP server is the group owner. Then issue the DISPLAY XCF operator modify command for the owning LDAP server and verify that this server is really the group owner. Restart the owning LDAP server if there is no response to the DISPLAY XCF operator modify command. Restart this LDAP server if it ended. Try the Extended Operation request again, if it failed. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1265E  The Extended Operation owner is busy, retrying.

Explanation: The LDAP server which is the owner of Extended Operations in the LDAP cross-system group in the sysplex is currently busy and cannot respond to the Extended Operation request.

Example: None.

System action: The LDAP server continues and tries the request again.

Operator response: None.

User response: None.

System programmer response: None.
Administrator response: If the problem persists, restart the LDAP server that owns the Extended Operations in the LDAP cross-system group. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1266E The LDAP server must have READ access to the BPX.WLMSERVER profile.

Explanation: The user ID that runs the LDAP server must have READ access to the BPX.WLMSERVER profile in the RACF FACILITY class so that the LDAP server can connect to Workload Manager (WLM).

Example: None.

System action: If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with no WLM support. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the LDAP server ends.

Operator response: None.
User response: None.
System programmer response: None.

Administrator response: If WLM support is needed and the BPX.WLMSERVER profile is not defined in the FACILITY class, add the profile by issuing a RACF RDEFINE command. Once the profile is defined, grant READ access to the user ID that runs the LDAP server by issuing a RACF PERMIT command. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1268E The serverCompatLevel is set to value. The sysplex owner has a different serverCompatLevel setting.

Explanation: The serverCompatLevel value specified in the configuration file for this server is incompatible with the serverCompatLevel value established by the sysplex owner.

In the message text:

value
serverCompatLevel option value

option
LDAP server configuration option

min_value
serverCompatLevel option minimum value

Example: None.

System action: The LDAP server ends.

Operator response: None.
User response: None.
System programmer response: None.

Administrator response: Obtain the serverCompatLevel value established by the sysplex owner. Either migrate the server to an appropriate level for the sysplex or upgrade this LDAP server to a level that is compatible with the sysplex.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
GLD1269A • GLD1272E

Descriptor code: None.
Automation: Not applicable.

---

**GLD1269A**  
Unable to initialize WLM support.

**Explanation:** The LDAP server is unable to initialize WLM support.

**Example:** None.

**System action:** If the `srvStartUpError` option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with no WLM support. If the `srvStartUpError` option is set to `terminate` (this is the default if the configuration option is not specified), the LDAP server ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** If WLM support is needed, restart the LDAP server with `ERROR` tracing turned on to determine the failure. The WLM routine that has failed is present in the LDAP ERROR traces. See the z/OS XL C/C++ Run-Time Library Reference for more information about the error. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

---

**GLD1272E**  
The operations monitor ID parameter is missing.

**Explanation:** The operations monitor id (OPID) parameter is missing on the LDAP server `WLMEXCEPT` operator modify command.

**Example:** None.

**System action:** The LDAP server continues. The request fails.

**Operator response:** Issue an LDAP server `WLMEXCEPT` operator modify command with an OPID value. Contact the LDAP Administrator to determine the correct OPID value.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Verify that an OPID is specified on the LDAP server `WLMEXCEPT` operator modify command.

**Problem determination:** Not applicable.

**Source:** LDAP

---

**GLD1270E**  
IP address 'value' for configuration option 'option' is not valid.

**Explanation:** The LDAP server or utility found an option in the LDAP server configuration file that has a value that is not supported for that option.

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Correct the LDAP server configuration file. If the option value looks correct, check that the option on the next line after this option line starts in column 1. A blank in column 1 of the next line indicates that it is a continuation line. The next line is then appended to the preceding option line and thus can result in a value that is not supported for the option. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

---

**GLD1272E**  
The WLM transaction name parameter is missing.

**Explanation:** The WLM transaction name parameter is missing on the LDAP server `WLMEXCEPT` operator modify command.

**Example:** None.

**System action:** The LDAP server continues. The request fails.

**Operator response:** Issue an LDAP server `WLMEXCEPT` operator modify command with a WLM...
transaction name. Contact the LDAP Administrator to
determine the correct WLM transaction name.

User response: None.
System programmer response: None.
Administrator response: Verify that a WLM
transaction name is specified on the WLMEXCEPT
operator modify command.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1273I  Replication conflict: a conflict is
detected on an add operation of 'dn' in
type backend named name. The add will
be converted into a modify because it
has a timestamp equal to or later than
the target entry timestamp.

Explanation: The LDAP server detected a replication
conflict on an add operation of an entry in the
specified backend. Since the replicated modify timestamp is
equal to or later than the modify timestamp of the
existing entry, this add conflict is resolved by
converting the operation into a modify operation. The
existing attributes that are being replaced are in the
lost and found log. The location of the lost and found
log is specified in the ibm-slapdLog attribute on the
cn=Replication,cn=Log Management,cn=Configuration
entry.

In the message text:

   dn  Entry distinguished name
type  Backend type
   name  Backend name

Example: None.

System action: The LDAP server converts the add
operation into a modify operation, and continues to
process the request.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1274W  Replication conflict: a conflict is
detected on a modify operation of 'dn' in
type backend named name. A refresh of
the entry will be requested because the
entry has been modified on this server
before it was modified on the supplier.

Explanation: The LDAP server detected a replication
conflict on a modify operation of an entry in the
specified backend. The conflict occurred because an
incoming modification has a newer timestamp than the
timestamp on the target entry. This server requests the
supplier to send a refreshed entry in order to resolve
this conflict.

In the message text:

   dn  Entry distinguished name
type  Backend type
   name  Backend name

Example: None.

System action: The LDAP server sends an entry
refresh request to the supplier.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1275W  Replication conflict: a conflict is
detected on a modify operation of 'dn' in
type backend named name. A refresh of
the entry will be requested because an
earlier update on the supplier has not
yet been applied to this server.

Explanation: The LDAP server detected a replication
conflict on a modify operation of an entry in the
specified backend. The conflict occurred because an
earlier update on the supplier has not yet been applied
to this server. This server requests the supplier to send
a refreshed entry in order to resolve this conflict.

In the message text:

**dn**  Entry distinguished name

**type**  Backend type

**name**  Backend name

**Example**: None.

**System action**: The LDAP server sends an entry refresh request to the supplier.

**Operator response**: None.

**User response**: None.

**System programmer response**: None.

**Administrator response**: None.

**Problem determination**: Not applicable.

**Source**: LDAP

**Module**: None.

**Routing code**: None.

**Descriptor code**: None.

**Automation**: Not applicable.

---

**GLD1277W**  Entries 'name1' and 'name2' contain conflicting password values for the masterServer DN 'value'. The entry is not processed.

**Explanation**: The LDAP server detected a difference in the password values for the same `ibm-masterServerDN` attribute value in two different consumer server credential entries. The same `ibm-masterServerPW` value should be used for the conflicting entries specified in this message. The replication information in the first entry is ignored.

In the message text:

**name1**  Entry distinguished name of conflicting entry

**name2**  Entry distinguished name of conflicting entry

**value**  Master server distinguished name

**Example**: None.

**System action**: The LDAP server continues, but the consumer server credential entry settings in the first entry are ignored.

**Operator response**: None.

**User response**: None.

**System programmer response**: None.

**Administrator response**: Update the `ibm-masterServerPW` attribute values on the conflicting consumer server credential entries to use the same value or use a different `ibm-masterServerDN` attribute value for one of the conflicting consumer server credential entries. A consumer server credential entry has an object class value of `ibm-slapdSupplier` or `ibm-slapdReplication` and must reside under the `cn=configuration` suffix in the CDBM backend.

**Problem determination**: Not applicable.

**Source**: LDAP

**Module**: None.

**Routing code**: None.

**Descriptor code**: None.
GLD1278E Routine ‘routine’ failed: Return code
return_code - error_text.

Explanation: An internal programming error has been
detected by the routine identified in the message.

In the message text:
routine
Routine name
return_code
Return code from routine
error_text
Error text corresponding to the return code

Example: None.

System action: The current LDAP operation being handled by the server ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the earlier message to correct the error, then restart the program.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1279A LDAP server stopping because it is unable to become owner of type backend named name.

Explanation: An error occurred when the LDAP server attempted to become the sysplex group owner for the named backend. A previous message indicates the reason for the failure.

In the message text:
type
Backend type
name
Backend name
Example: None.

System action: The LDAP server ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Try running the LDAP operation again with DEBUG ERROR activated in the server using the operator modify command. The debug output may assist in locating and correcting the error. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1280E Unable to load the System SSL CMS runtime: error_code/reason_code - error_text

Explanation: The LDAP server or utility cannot load the System SSL CMS runtime DLL. The LDAP server or utility uses the System SSL CMS runtime DLL to call the gsk_generate_random_bytes() routine for random byte generation of ibm-entryUUID attribute values, CRAM-MD5 and DIGEST-MD5 binds, and the salt value for Salted SHA password hashing. See the description of dllload() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:
error_code
Error code from dllload()
reason_code
Reason code from dllload()
error_text
Error text corresponding to the return code

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Verify that the SYS1.SIEALNKE data set is available to the LDAP server or utility job step, then restart the program. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD1281E Unable to query the gsk_get_cms_vector routine: error_code/reason_code - error_text

Explanation: The LDAP server or utility is unable to query the gsk_get_cms_vector() routine in the System SSL CMS runtime DLL. The LDAP server or utility uses the System SSL CMS runtime DLL to call the gsk_generate_random_bytes() routine for random byte generation of ibm-entryUUID attribute values, CRAM-MD5 and DIGEST-MD5 binds, and the salt value for Salted SHA password hashing. See the description of dllqueryfn() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

error_code
   Error code from dllqueryfn()
reason_code
   Reason code from dllqueryfn()
error_text
   Error text corresponding to the error code

Example: None.

System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error, then try the operation again. If the problem persists, contact the service representative.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1283W Filtered access control has reduced the access rights for DN 'name'.

Explanation: The LDAP server has matched filtered access control values for an LDAP administrator DN. This has reduced the access rights for the root administrator DN (adminDN), the Kerberos administrator DN (krbLDAPAdmin), or an administrative group member.

In the message text:

name
   DN of the administrator

Example: None.

System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1282E Unable to generate random data bytes: return_code - error_text

Explanation: The LDAP server or utility encountered an error while attempting to generate random data bytes using the gsk_generate_random_bytes() routine. See the description of gsk_generate_random_bytes() in z/OS Cryptographic Services System SSL Programming for more information about the error.

In the message text:

return_code
   Return code from gsk_generate_random_bytes()
error_text
   Error text corresponding to the return code

Example: None.

System action: The LDAP server or utility continues but the operation fails.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error, then try the operation again. If the problem persists, contact the service representative.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
Required attribute type attribute is not defined in the schema.

Explanation: The LDAP server or utility found that the required attribute type indicated in the message is not defined in the LDAP server schema.

In the message text:

attribute
  Undefined attribute type

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the schemaPath configuration option has the correct value and restart the program. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1285E Required object class objectclass is not defined in the schema.

Explanation: The LDAP server or utility found that the required object class indicated in the message is not defined in the LDAP server schema.

In the message text:

objectclass
  Undefined object class

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1286E The serverCompatLevel is set to value. A filtered 'attribute' value was found in backend 'name'. Filtered 'attribute' values require minimum serverCompatLevel min_value.

Explanation: The serverCompatLevel value specified in the configuration file is set to an unsupported level for filtered values in the backend indicated in the message.

In the message text:

value
  serverCompatLevel option value

attribute
  Attribute type

name
  Backend name

min_value
  serverCompatLevel option minimum value

Example: None.

System action: The backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value. If the error occurs in the schema backend, the LDAP server ends regardless of the option value.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Set the serverCompatLevel configuration option to the minimum level specified in the message. If the serverCompatLevel configuration option must remain at the current level, the filtered attribute values must be removed from the backend. To find the filtered attribute values in the specified backend, the following steps must be performed:

• Temporarily set the serverCompatLevel configuration option to the minimum level specified and use the ds2ldif utility to unload the specified backend.
• Analyze the unloaded LDIF file and look for entries that have filtered attribute values.
• Start the LDAP server and modify the entries that have filtered attribute values by removing the filtered attribute values.

Chapter 1. LDAP server and ldif2ds messages (1000)
• Set the serverCompatLevel configuration option back to the wanted setting and restart the LDAP server.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1287E  The LDAP administrator entry cannot be unlocked because the password is defined in the configuration file.

Explanation: The LDAP server UNLOCK operator modify command failed because the password for the LDAP root administrator entry is specified in the adminPW option in the LDAP server configuration file. The LDAP server UNLOCK operator modify command only works when the LDAP root administrator entry and password reside in an LDBM, TDBM, or CDBM backend.

Example: None.
System action: The LDAP server continues. The request fails.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: The LDAP root administrator entry is now unlocked and can now authenticate to the LDAP server.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1288I  The LDAP administrator entry is now unlocked.

Explanation: The LDAP server UNLOCK operator modify command has completed successfully and unlocked the LDAP root administrator entry.

Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1289E  The LDAP administrator entry cannot be unlocked because the credentials could not be set.

Explanation: The LDAP server UNLOCK operator modify command encountered an internal error while attempting to set the credentials for the LDAP root administrator. A previous message or LDAP error trace identifies the reason for the failure.

Example: None.
System action: The LDAP server continues. The request fails.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the earlier message or LDAP error trace to correct the problem. If LDAP error tracing is not active at the time of the failure, the error trace is automatically written to CTRACE. LDAP error tracing can be activated using the LDAP server DEBUG operator modify command to set ERROR tracing. Then try the request again. If the problem persists, contact the service representative.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD1290I  Activity log status

Explanation: This message displays the current LDAP server activity log settings as a result of issuing the LDAP server DISPLAY LOG operator modify command.

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: The LDAP server DISPLAY LOG operator modify command can be used to review the current LDAP server activity log settings. Use the LDAP server LOG operator modify command to make any necessary updates.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1292E The Activity log file cannot be rolled over.

Explanation: The activity log file could not be rolled over because an error was encountered. A previous message indicates the reason for the failure.

Example: None.

System action:
- If a z/OS UNIX System Services file is specified in the logfile configuration option, the LDAP server continues with activity logging writing to the same activity log file.
- If the logfile and the logfileRolloverDirectory configuration options specify a generated data group (GDG) base, the LDAP server continues with activity logging writing to the same data set generation.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response:
- If a z/OS UNIX System Services directory is specified in the logfileRolloverDirectory configuration option, verify that the directory exists and that the LDAP server has the appropriate permissions to write to the directory. If the directory does not exist, create the directory or update the logfileRolloverDirectory option in the LDAP server configuration file to specify a valid directory. Then try the request again.
- If the logfileRolloverDirectory configuration option is not specified, the activity log file specified in the logfile configuration option could not be found. Verify that the LDAP server can write to the directory and file specified in the logfile option still exists.
If the `logfile` and the `logfileRolloverDirectory` configuration options specify a z/OS UNIX System Services directory, ensure that the directories reside in the same type of file system. Activity log file rollover is not supported between different file system types.

If the `logfile` and the `logfileRolloverDirectory` configuration options specify a data set, verify that each data set specified is a generated data group (GDG) base. Activity log file rollover is only supported in data sets when using GDGs.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1293E** The LDAP administrator entry cannot be unlocked because the entry is not defined in a LDBM, TDBM, or CDBM backend.

**Explanation:** The LDAP server `UNLOCK` operator modify command was unable to unlock the LDAP root administrator entry because it is not defined within a configured LDBM, TDBM, or CDBM backend.

**Example:** None.

**System action:** The LDAP server continues. The request fails.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** If password policy should apply to the LDAP root administrator, add an LDAP root administrator user entry that has a `userPassword` attribute value in the LDBM, TDBM, or CDBM backend. The distinguished name (DN) specified in the `adminDN` option in the LDAP server configuration file must specify an LDBM, TDBM, or CDBM entry with a `userPassword` attribute value and the `adminPW` option must be removed from the LDAP server configuration file. Then stop and restart the server.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1294E** The LDAP administrator cannot be unlocked because a modify error occurred: `error_code`.

**Explanation:** The LDAP server `UNLOCK` operator modify command encountered an error while attempting to modify the LDAP root administrator entry in the backend. The error code has the following common values:

- `1` Operations error modifying the LDAP root administrator entry
- `32` LDAP root administrator entry does not exist
- `121` A parameter is not valid
- `122` Unable to process the MODIFY request
- `132` Insufficient storage is available

Any LDAP error codes documented in the `/usr/include/ldap.h` file may also be returned.

In the message text:

`error_code`

Error code from modify operation

**Example:** None.

**System action:** The LDAP server continues. The request fails.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Additional information about this error is provided in the LDAP error trace. Use the information in this message and error trace to correct the problem. If LDAP error tracing is not active at the time of the failure, the error trace is automatically written to CTRACE. LDAP error tracing can be activated using the LDAP server `DEBUG` operator modify command to set ERROR tracing. Then try the request again. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1295E** The LDAP administrator entry cannot be unlocked because the entry participates in native authentication.

**Explanation:** The LDAP server `UNLOCK` operator modify command was unable to unlock the LDAP root administrator entry because it participates in native authentication.

**Example:** None.

**System action:** The LDAP server continues. The request fails.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Additional information about this error is provided in the LDAP error trace. Use the information in this message and error trace to correct the problem. If LDAP error tracing is not active at the time of the failure, the error trace is automatically written to CTRACE. LDAP error tracing can be activated using the LDAP server `DEBUG` operator modify command to set ERROR tracing. Then try the request again. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
administrator entry because it is defined in a backend or subtree which participates in native authentication. The LDAP server UNLOCK operator modify command only works when the LDAP root administrator entry and password reside in an LDBM, TDBM, or CDBM backend.

Example: None.

System action: The LDAP server continues. The request fails.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: The LDAP server UNLOCK operator modify command only works when the adminDN server configuration option specifies a distinguished name (DN) that resides in an LDBM, TDBM, or CDBM backend and that entry must have a userPassword attribute value. If password policy should apply to the LDAP root administrator, update the adminDN option to specify a distinguished name (DN) that resides outside the scope of a backend or subtree that is participating in native authentication. Then stop and restart the server.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1296I  Display Replica completed.

Explanation: This message is displayed in response to the LDAP server DISPLAY REPLICAS operator modify command, when advanced replication is configured. The advanced replication DISPLAY REPLICAS output is only displayed in the LDAP server's job log.

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1297A  System failure in service_name, taking SYSMDUMP system dump with abend code abend_error_code and abend reason code abend_reason_code. Failure point: file filename, line line_number, function function_name.

Explanation: The LDAP server or utility encountered a problem using the LE system service or routine specified and is taking a SYSMDUMP system dump. The SYSMDUMP is written to the data set specified by the SYSMDUMP DD statement in the JCL used to start the LDAP server or utility. The abend error code is always 90 and indicates that the LDAP server or utility has requested the abend. The abend reason code ranges from 1 to 11 and there is a one to one relationship with the LE routine specified in the message. The file name, line number, and function name indicate the location in the LDAP code where the abend occurred.

In the message text:

service_name

LE routine name

abend_error_code

LDAP abend code

abend_reason_code

LDAP abend reason code

filename

LDAP file name where this abend occurred

line_number

Line number where this abend occurred

function_name

LDAP routine name where this abend occurred

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: Analyze the SYSMDUMP system dump and fix the problem, then restart the program. If the problem persists, contact the service representative.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
The following encryption or hashing method is not available: value, reason: error_text.

Explanation: The LDAP server or utility encountered an error attempting to encrypt or hash a value using the algorithm indicated in the message. The algorithm that is used is specified on the pwEncryption option in the LDAP server configuration file. See z/OS Cryptographic Services ICSF Application Programmer’s Guide for more information about the error.

In the message text:

value
  Encryption or hashing algorithm

error_text
  Error message text

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

The value value_specified specified for attribute attribute in entry entry is not valid. The default value value_default has been set.

Explanation: The LDAP server encountered an attribute value which is not valid. The default attribute value is used.

In the message text:

value_specified
  Attribute value specified

attribute
  Attribute

entry
  Entry name

value_default
  Default attribute value

Example: None.

System action: The LDAP server continues. When detected, the values in the administrative group member entry are ignored. These may include the ibm-slapdAdminPW and ibm-slapdAdminRole attribute values.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Modify the
GLD1301E  GLD1302E

ibm-slapdAdminDN attribute to specify a value that is not already in use by the entries or configuration options described in the explanation.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

Explanation: The LDAP server encountered a duplicate administrator member in the entry specified. A duplicate is detected if multiple administrative group member entries (ibm-slapdAdminMember objectclass) have the same ibm-slapdAdminDN value. Duplicates are also detected if an ibm-slapdAdminDN value matches the masterServerDN, peerServerDN, or the adminDN options in the LDAP server configuration file. If an ibm-slapdAdminDN value matches the ibm-slapdMasterDN value in an advanced replication supplier credentials entry (ibm-slapdSupplier or ibm-replicationConfiguration objectclasses), a duplicate is also detected. Finally, a duplicate is detected if the value matches a member value in the cn=safadmingroup,cn=configuration (ibm-SAFAAdminGroup objectclass).

In the message text:

value

Distinguished name

Example: None.

System action: The LDAP server continues. When detected, the security manager may not be queried for role assignments.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Modify the member attribute to specify a value that is not already in use by the entries or configuration options described in the explanation.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1302E Unable to query the SAF Administration roles for SAF_user; error_code/reason_code - error_text

Explanation: The LDAP server is unable to query SAF to determine the administration roles for the indicated SAF user ID. SAF is being queried for the administration roles because the SAF user ID is a member of the cn=safadmingroup,cn=configuration administration group entry. See the description of _check_resource_auth_np() in [z/OS XL C/C++] for more information about the error.

In the message text:

SAF_user

SAF user ID

error_code

Error code returned from _check_resource_auth_np()

reason_code

Reason code from _check_resource_auth_np()

error_text

Error text corresponding to the error code

Example: None.

System action: The LDAP server continues but the bound administrator is assigned the NOADMIN role. When detected, the security manager may not be queried for SAF role assignments.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message and the information in the _check_resource_auth_np() description to correct the error.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
Idif2ds utility messages

GLD1800E  Command options option1 and option2 are mutually exclusive.

Explanation: The two command-line parameters indicated in the message cannot both be specified at the same time.

In the message text:
option1  Command-line parameter name
option2  Command-line parameter name

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1802E  The summary message frequency must be a non-negative decimal integer.

Explanation: The frequency value specified for the -q command-line parameter is not a positive integer.

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.

Administrator response: Specify a valid positive integer for the -q parameter on the command line. Then restart the program.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1803E  At least one phase option (-c, -p, -l) must be specified.

Explanation: At least one phase command-line parameter must be specified for the ldif2ds utility.

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.

Administrator response: Specify one or more phase parameters on the command line. Then restart the program.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
**GLD1804E**  Unable to open name:
*error_code/reason_code - error_text*

**Explanation:** The file indicated in the message cannot
be opened in the required way: read for an input file,
write for an output file. The file can be a file system file
or a data set. If the file name is //DD:INTRDR, the failure
occurred while opening the internal reader to submit
the load jobs. See the description of fopen() in [z/OS XL
C/C++ Run-Time Library Reference](https://www.ibm.com) for more information
about the error.

In the message text:

- name: Data set name or file name
- error_code: Error code from fopen()
- reason_code: Reason code from fopen()
- error_text: Error text corresponding to the error code

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the
message to correct the error. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

**GLD1806E**  Unable to write name using routine:
*error_code/reason_code - error_text*

**Explanation:** An attempt to write to the file indicated
in the message failed. The file can be a file system file
or a data set. If the file name is //DD:INTRDR, the failure
occurred while submitting a load job to the internal
reader. The routine used to perform the write is also
indicated in the message. See the description of the
routine in [z/OS XL C/C++ Run-Time Library Reference](https://www.ibm.com) for
more information about the error.

In the message text:

- name: Data set name or file name
- routine: Routine that failed
- error_code: Error code from the routine
- reason_code: Reason code from the routine
- error_text: Error text corresponding to the error code

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the
message to correct the error. Then restart the program.
GLD1807E • GLD1811E

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1807E  At least one LDIF file must be specified.
Explanation: The -c (check) or -p (prepare) parameter is specified on the ldif2ds command line but no LDIF files are specified with either the -i or -e command-line parameter.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1808I  Preparing LDIF file filename.
Explanation: The ldif2ds utility is starting the prepare phase for the directory entries in the indicated LDIF file.
In the message text:
filename  LDIF file name
Example: None.
System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1810I  ldif2ds utility version version.release,
Service level level.
Explanation: The ldif2ds utility with version, release, and service level indicated in the message is running.
In the message text:
version  Utility version
release  Utility release
level  Utility service level
Example: None.
System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1811E  ldif2ds utility terminating due to error condition.
Explanation: The ldif2ds utility is ending due to an error. Previous messages indicate the reason for the failure.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1812I name; number entries have been processed. error of them encountered errors.

Explanation: The utility has processed the indicated number of entries. This message is issued when all of the directory entries have been processed for the check or prepare phase. It is also issued as an intermediate status message as determined by the -q command-line parameter. Note that the program might have encountered errors during this processing. If so, processing of some entries may not have completed successfully. Additional messages are issued to indicate these errors.

In the message text:

name
  Program name
number
  Number of entries
error
  Number of error entries

Example: None.
System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1814E Syntax error at line line_number of filename.

Explanation: The ldif2ds utility has encountered a syntax error in the LDIF statement beginning at the indicated line of the LDIF file.

In the message text:

line_number
  Line number
filename
  LDIF file name

Example: None.
System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: If the statement is within an entry, verify that it has the correct format for specifying an entry record (either name: value or name:: value). If the statement is not within an entry and is not a comment, then it must be a version or dn statement. See [IBM Tivoli Directory Server Client Programming for z/OS] for more information about the format of LDIF statements. Correct the LDIF file. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
**GLD1815E • GLD1818E**

Routing code: None.
Descriptor code: None.
Automation: Not applicable.

---

**GLD1815E**  Unable to decode binary value at line

\[\text{line number}\]

of filename.

**Explanation:** The ldif2ds utility is unable to decode a base64-encoded value in the LDIF statement beginning at the indicated line of the LDIF file. The LDIF statement format is \text{name::value}, indicating that the value must be base64-encoded.

In the message text:

\[\text{line number}\]

\[\text{filename}\]

\[\text{Line number}\]

\[\text{LDIF file name}\]

**Example:** None.

**System action:** The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

**Operator response:** None.
**User response:** None.
**System programmer response:** None.
**Administrator response:** Correct the LDIF file by base64-encoding the value or by changing the statement format to \text{name::value}. Then restart the program.

**Problem determination:** Not applicable.
**Source:** LDAP
**Module:** None.
**Routing code:** None.
**Descriptor code:** None.
**Automation:** Not applicable.

---

**GLD1817E**  Unsupported 'changetype' directive at

\[\text{line number}\]

of filename.

**Explanation:** An entry in the LDIF file at the indicated line contains a \text{changetype} directive that does not specify an add operation. Only \text{changetype: add} is supported by the ldif2ds utility. Note that the \text{changetype} directive is not required.

In the message text:

\[\text{line number}\]

\[\text{filename}\]

\[\text{Line number}\]

\[\text{LDIF file name}\]

**Example:** None.

**System action:** The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

**Operator response:** None.
**User response:** None.
**System programmer response:** None.
**Administrator response:** Either correct the \text{changetype} directive by specifying \text{add} or remove the directive from the LDIF file. Then restart the program.

**Problem determination:** Not applicable.
**Source:** LDAP
**Module:** None.
**Routing code:** None.
**Descriptor code:** None.
**Automation:** Not applicable.

---

**GLD1816E**  LDIF version is not supported.

**Explanation:** The version directive in an LDIF file specifies a version number that is not supported by the ldif2ds utility. The utility only supports LDIF version 1. A previous message indicates the name of the LDIF file.

**Example:** None.

**System action:** The program ends.

**Operator response:** None.
**User response:** None.
**System programmer response:** None.
**Administrator response:** Correct the version number in the LDIF file. Then restart the program.

**Problem determination:** Not applicable.
**Source:** LDAP
**Module:** None.
**Routing code:** None.
**Descriptor code:** None.
**Automation:** Not applicable.

---

**GLD1818E**  Zero-length distinguished name found at line

\[\text{line number}\]

of filename.

**Explanation:** The ldif2ds utility found a zero-length distinguished name for a directory entry at the indicated line of the LDIF file. Every entry must have a distinguished name.

In the message text:

\[\text{line number}\]

**Example:** None.

**System action:** The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

**Operator response:** None.
**User response:** None.
**System programmer response:** None.
**Administrator response:** Correct the \text{distinguished name} directive by specifying \text{add} or remove the directive from the LDIF file. Then restart the program.

**Problem determination:** Not applicable.
Filename
LDIF file name

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.
User response: None.

System programmer response: None.
Administrator response: Specify a distinguished name for the entry in the LDIF file. Then restart the program.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1819E Unable to normalize value at line
line_number of filename: error_text.

Explanation: The ldif2ds utility cannot convert the value on the indicated line to normalized format. The value is either a distinguished name or an attribute value.

In the message text:
line_number
Line number
filename
LDIF file name
error_text
Error message text

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.
User response: None.

System programmer response: None.
Administrator response: Use the information in the message to correct the value in the LDIF file. Then restart the program.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1820E Unable to resolve attribute type attribute:
error_text.

Explanation: The ldif2ds utility is unable to find the attribute indicated in the message in the LDAP server schema. Every attribute contained in the entry, including the attributes in the relative distinguished name (RDN) of the entry, must be already defined in the schema. A previous message indicates the name of the LDIF file containing the entry.

In the message text:
attribute
Attribute type
error_text
Error message text

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.
User response: None.

System programmer response: None.
Administrator response: Either add the missing attribute to the LDAP server schema or remove the attribute from the LDIF file. Then restart the program. To add the attribute to the schema, start the LDAP server and issue an appropriate modify operation to the schema entry. Make sure to stop the LDAP server before using the ldif2ds utility to load entries into the server. See LDAP directory schema for more information about modifying the LDAP server schema.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1821E Unable to resolve object class objectclass:
error_text.

Explanation: The ldif2ds utility is unable to find the object class indicated in the message in the LDAP server schema. Every object class contained in the entry, including any object classes in the relative distinguished name (RDN) of the entry, must be already defined in the schema. A previous message indicates the name of the LDIF file containing the entry.

In the message text:
**GLD1822E • GLD1824E**

**objectclass**
Object class

**error_text**
Error message text

**Example:** None.

**System action:** The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Either add the missing object class to the LDAP server schema or remove the object class from the LDIF file. Then restart the program. To add the object class to the schema, start the LDAP server and issue an appropriate modify operation to the schema entry. Make sure to stop the LDAP server before using the ldif2ds utility to load entries into the server. See LDAP directory schema for more information about modifying the LDAP server schema.

**Problem determination:** Not applicable.

---

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

<table>
<thead>
<tr>
<th>GLD1823E</th>
<th>Entry 'name' is not in the same backend as previous entries.</th>
</tr>
</thead>
</table>

**Explanation:** The ldif2ds utility encountered an entry whose distinguished name (DN) belongs to a different backend in the LDAP server configuration file than the entries processed before this one. Each invocation of the ldif2ds utility can only load entries into one backend. All the entries in the LDIF files must belong to the same backend, using any of the suffixes listed for that backend in the LDAP server configuration file. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

```
name
```

Entry distinguished name

**Example:** None.

**System action:** The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Either change the distinguished name of the entry so that it has one of the suffixes of the backend being loaded or remove the entry from the LDIF file. Then restart the program.

**Problem determination:** Not applicable.

---

<table>
<thead>
<tr>
<th>GLD1822E</th>
<th>No backend configured for DN 'name'.</th>
</tr>
</thead>
</table>

**Explanation:** The ldif2ds utility encountered an entry whose distinguished name (DN) does not belong to any suffix in the backends contained in the LDAP server configuration file. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

```
name
```

Entry distinguished name

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Either add the missing object class to the LDAP server schema or remove the object class from the LDIF file. Then restart the program.

**Problem determination:** Not applicable.

---

<table>
<thead>
<tr>
<th>GLD1824E</th>
<th>Entry 'name' is not in a TDBM backend.</th>
</tr>
</thead>
</table>

**Explanation:** The ldif2ds utility encountered an entry whose distinguished name (DN) belongs to a backend in the LDAP server configuration file that is not a TDBM backend. The ldif2ds utility can only load entries into a single TDBM backend, thus all entries in the LDIF files must belong to the same TDBM backend. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

```
name
```

Entry distinguished name

**Example:** None.

**System action:** The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Either add the appropriate suffix option in the backend section of the LDAP server configuration file or change the distinguished name of the entry in the LDIF file. Then restart the program.

**Problem determination:** Not applicable.
GLD1825I • GLD1826E

name
Entry distinguished name
Example: None.
System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Either change the distinguished name of the entry so that it has one of the suffixes of the TDBM backend being loaded or remove the entry from the LDIF file. Then restart the program. Other types of backends can only be loaded using an add operation while the LDAP server is running.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

---

GLD1826E Unable to encrypt attribute value for entry 'name': error_text.
Explanation: The ldif2ds utility encountered an error while trying to encrypt or hash a value of an attribute that requires encryption or hashing: userPassword, secretKey, replicaCredentials, ibm-replicaKeyPwd, or ibm-slapdMasterPw. The type of encryption or hashing in use is determined by the values of the pwEncryption and secretEncryption options within the TDBM backend section in the LDAP server configuration file. A previous message indicates the name of the LDIF file containing the entry.
In the message text:
attribute
Attribute type
name
Entry distinguished name
error_text
Error message text
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

---

GLD1828E An internal error has occurred.
Explanation: An internal programming error has been detected by the utility.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Try running the utility again with -d ERROR specified on the command line. The debug output may assist in locating and correcting the
GLD1829E  GLD1832I

error. If the problem persists, contact the service representative.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1829E  Entry 'name' already exists.
Explanation: The ldif2ds utility encountered an entry that already exists, either as a prior entry in this LDIF file or in an LDIF file processed before this file, or as an existing entry in the TDBM backend being loaded. The duplicate entry cannot be added to the directory. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

name
    Entry distinguished name

Example: None.
System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: If appropriate, review the output of each load job to determine if it is successful. If a load job fails, use the information in the description of the ldif2ds utility to determine how to proceed.
Note: If a load job fails, do not run the ldif2ds utility again because this can add duplicate data to the database.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1832I  Checking LDIF file filename.
Explanation: The ldif2ds utility is starting the check phase for the directory entries in the indicated LDIF file. The check phase is performed when the -c or -p option is specified on the command line.

In the message text:

filename
    LDIF file name

Example: None.
System action: The utility continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1831I  ldif2ds utility is done.
Explanation: The ldif2ds utility has finished.

Note: If -l (load) was specified on the command line, then the load jobs have been successfully submitted, but this message does not indicate that the load jobs have ended successfully. The processing of the load jobs by DB2 is outside the scope of the ldif2ds utility.

Review the output generated by each load job to determine if it is successful.

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: If appropriate, review the output of each load job to determine if it is successful. If a load job fails, use the information in the description of the ldif2ds utility to determine how to proceed.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD1833E Unable to get directory entry 'name':
error_text.

Explanation: The ldif2ds utility has detected an entry whose parent entry cannot be retrieved from the TDBM database. The distinguished name of the parent entry is indicated in the message. A previous message indicates the name of the LDIF file containing the child entry.

In the message text:
name
  Parent entry distinguished name
error_text
  Error message text

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1834E The parent for entry 'name' does not exist.

Explanation: The ldif2ds utility encountered a non-suffix entry for which there is no parent. Every non-suffix entry must have a parent entry, either as a prior entry in this LDIF file or in an LDIF file processed before this file, or as an existing entry in the TDBM database being used. The entry cannot be added to the directory. A previous message indicates the name of the LDIF file containing the entry.

In the message text:
name
  Child entry distinguished name

Example: None.

System action: If the error occurs during the check phase, the utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded. If the error occurs during the prepare phase, the program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Remove the child entry from the LDIF file or change the distinguished name of the child entry to one for which the parent is not an alias or referral entry. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1835E Parent entry 'name' is a referral or an alias.

Explanation: The ldif2ds utility encountered an entry for which the parent entry is an alias entry or a referral entry. Alias and referral entries cannot have children. The parent entry can be a prior entry in this LDIF file or in an LDIF file processed before this file or it can be an existing entry in the TDBM backend being loaded. A previous message indicates the name of the LDIF file containing the child entry.

In the message text:
name
  Parent entry distinguished name

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Remove the child entry from the LDIF file or change the distinguished name of the child entry to one for which the parent is not an alias or referral entry. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
GLD1836E  DN 'name' exceeds the maximum length of length.

Explanation: The ldif2ds utility encountered an entry for which the normalized distinguished name (DN) is longer than the maximum length allowed. The maximum length of a DN is determined by the size of the DN column in the DIR_ENTRY table, set when creating the TDBM database tables. The normalized DN is stored in this column. The normalized DN may not be same as the DN specified for the entry in the LDIF file. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

name       Entry normalized distinguished name
length     Maximum DN length

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1838E  Multiple base structural object classes specified for 'name'.

Explanation: The ldif2ds utility encountered an entry which contains more than one base structural object class. Every entry must have a single base structural object class, specified on the objectclass attribute within the entry. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

name       Entry distinguished name

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1837E  No base structural object class specified for 'name'.

Explanation: The ldif2ds utility encountered an entry which does not contain a base structural object class. Every entry must have a single base structural object class, specified on the objectclass attribute within the entry. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

name       Entry distinguished name

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD1839E Entry 'name' contains obsolete attribute type 'attribute'.

Explanation: The ldif2ds utility encountered an entry which contains an attribute that is marked as obsolete in the LDAP server schema. Obsolete attribute types cannot be used in an entry. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

name  Entry distinguished name
attribute  Obsolete attribute name

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Remove the obsolete attribute type from the entry in the LDIF file or modify the LDAP server schema to remove the obsolete specification from the attribute definition. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1840E Entry 'name' contains abstract class 'objectclass' as a base object class.

Explanation: The ldif2ds utility encountered an entry which contains an abstract object class as one of its base object classes. An abstract class cannot be a base object class; it must be derived from another object class specified in the entry. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

name  Entry distinguished name
objectclass  Abstract object class name

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Remove the abstract object class from the entry. Verify that all the attributes used in the entry and in the relative distinguished name (RDN) of the entry are included in the remaining object classes. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1841E Entry 'name' contains restricted attribute type 'attribute'.

Explanation: The ldif2ds utility encountered an entry which contains an attribute that cannot be set when adding an entry. The value for this attribute is instead generated by the LDAP server itself. Except for the ibm-EntryUUID, creatorsName, createTimestamp, modifiersName, and modifyTimestamp attribute types, an attribute type that is marked as NO-USER-MODIFICATION in its definition in the LDAP schema may not be used to create a new directory entry. A previous message indicates the name of LDIF file containing the entry.

In the message text:

name  Entry distinguished name
attribute  Attribute type

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Remove the restricted attribute from the entry. Then restart the program.

Problem determination: Not applicable.

Source: LDAP
GLD1842E  Entry 'name' contains obsolete object class 'objectclass'.

Explanation: The ldif2ds utility encountered an entry which contains an object class that is marked as obsolete in the LDAP server schema. Obsolete object classes cannot be used in an entry. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

name     Entry distinguished name
objectclass  Obsolete object class name

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Either remove the obsolete object class from the entry in the LDIF file or modify the LDAP server schema to remove the obsolete specification from the object class definition. Then restart the program. If the object class is removed, verify that all the attributes used in the entry and in the relative distinguished name (RDN) of the entry are included in the remaining object classes. If modifying the schema, start the LDAP server and issue an appropriate modify operation to the schema entry. Make sure to stop the LDAP server before using the ldif2ds utility to load entries into the server. See LDAP directory schema for more information about modifying the LDAP server schema.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1844E  Entry 'name' cannot be both an alias and a referral.

Explanation: The ldif2ds utility encountered an entry which is both an alias entry and a referral entry. This combination is not supported by the LDAP server. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

name     Entry distinguished name

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.
GLD1845E  The aclPropagate attribute for entry 'name' requires the aclEntry attribute.

Explanation: The ldif2ds utility encountered an entry which contains the aclPropagate attribute but does not contain the aclEntry attribute. aclEntry must be specified along with aclPropagate. A previous message indicates the name of the LDIF file containing the entry. In the message text:

name

Entry distinguished name

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Either add the aclEntry attribute to the entry or remove the aclPropagate attribute. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1847E  Schema check failed for entry 'name': error_text.

Explanation: The ldif2ds utility encountered an entry whose attributes or object classes violate the LDAP server schema. The entry cannot be added to the directory. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

name

Entry distinguished name

error_text

Error message text

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the entry in the LDIF file. The error is usually that the entry contains an attribute that is not listed in any of the object classes specified in the entry or that the entry does not contain an attribute that is required by one of the object classes specified in the entry. Then restart the program.

Problem determination: Not applicable.
GLD1848E  The -o option must be specified if -p or -l is specified.

Explanation: The ldif2ds utility cannot be invoked without the -o command-line parameter when either the -p (prepare) or -l (load) command-line parameter is specified. -o is required during the prepare and load phases to identify the prefix part of the name of the output data sets.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Add the -o parameter to the command line. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1849E  The output dataset name prefix is too long.

Explanation: The maximum length of the output data set name prefix is 22. The prefix is specified by the -o parameter on the ldif2ds utility command line.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Specify a value that is at most 22 characters long for the -o parameter on the command line. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1850E  Unable to assign database attribute identifier: error_text.

Explanation: The ldif2ds utility could not assign an internal identifier for an attribute type that is not currently known to the TDBM backend being loaded.

In the message text:

error_text

   Error message text

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the problem. Then restart the program. If more information is needed, try running the utility again with -d ERROR specified on the command line. The debug output may assist in locating and correcting the error. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1851E  Unable to assign database entry identifier: error_text.

Explanation: The ldif2ds utility could not assign an internal entry identifier for a new entry.

In the message text:

error_text

   Error message text

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the problem. Then restart the program. If more information is needed, try running the utility again with -d ERROR specified on the command line. The debug output may assist in locating and correcting the error. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

108  IBM Tivoli Directory Server Messages and Codes for z/OS V1R13.0
command line. The debug output may assist in locating and correcting the error. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

GLD1852E  Alias entry 'name' points to itself.

**Explanation:** The ldif2ds utility encountered an alias entry in which a value of the `aliasedObjectName` attribute is the same as the distinguished name of the alias entry. This would cause an infinite loop when dereferencing the entry, thus is not allowed. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

```
name
```

Entry distinguished name

**Example:** None.

**System action:** The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Change the `aliasedObjectName` attribute value so that it is not the distinguished name of the entry or remove the alias entry from the LDIF file. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

GLD1853E  The JCL dataset must contain fixed-length 80-byte records.

**Explanation:** The ldif2ds utility has determined that the format of the JCL data set is not correct. The JCL data set must be a PDS or PDSE with a record format of RECFM=F or RECFM=FB and with a logical record length of LRECL=80. The name of this data set is `dspprefix.BULKLOAD.JCL`, where `dspprefix` is the value of the `-o` command-line parameter.

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Reallocate the JCL data set. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

GLD1854E  Unable to retrieve file information: `error_code/`reason_code - `error_text`

**Explanation:** The utility could not obtain file information for an open file. For the ldif2ds utility, the file is `dspprefix.BULKLOAD.JCL`, where `dspprefix` is the value of the `-o` command-line parameter. See the description of `fldata()` in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

```
error_code
reason_code
error_text
```

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
GLD1855E • GLD1858E

---

**GLD1855E** The SYSTEM member contains an unrecognized directive: `value`.

**Explanation:** The ldif2ds utility has found a record that it does not support in the SYSTEM member of the JCL data set. The supported records begin with `#` (a comment), `HLQ`, or `JOBCARD`. The name of the JCL data set is `dsprefix.BULKLOAD.JCL`, where `dsprefix` is the value of the `-o` command-line parameter.

In the message text:

*value*

Unrecognized directive

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1858E** The HLQ directive in the SYSTEM member is not valid.

**Explanation:** The ldif2ds utility has found a value that is not supported for the HLQ record in the SYSTEM member of the JCL data set. This value is the high-level-qualifier of the DB2 data sets, and must be at most 35 characters long. The name of the JCL data set is `dsprefix.BULKLOAD.JCL`, where `dsprefix` is the value of the `-o` command-line parameter.

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1858E** The load datasets are not in the correct state.

**Explanation:** The ldif2ds utility has been invoked with the `-l` (load) command-line parameter to submit the database load jobs, but it has determined that the load data sets may not be valid. ldif2ds expects the load phase to be run after the new entries in the LDIF files have been prepared, by specifying the `-p` (prepare) command-line parameter. When the utility successfully completes the prepare phase, it sets the first record in the STATUS member of the JCL data set to `STATUS P`. When the utility begins the load phase, it checks that the first record of the STATUS member is `STATUS P`. If the status is correct and the load phase completes successfully, then the status is reset to `STATUS L`. This prevents the ldif2ds utility from being run again to load the same data, which can result in a corrupted DB2 database that is not usable by the LDAP server. The name of the JCL data set is...
Note: If the load phase is successful, then the load jobs have been successfully submitted, but this does not indicate that the load jobs have ended successfully. The processing of the load jobs by DB2 is outside the scope of the ldif2ds utility. Review the output generated by each load job to determine if it is successful.

Example: None.

System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.

Administrator response: Use the information in the message to correct the error. Then restart the program. If the problem persists, contact the service representative.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1859E Unable to allocate an internal reader:
Error error_code, Reason reason_code.

Explanation: The ldif2ds utility has been unable to allocate an internal reader, needed to submit the load jobs. See the description of dynalloc() in [z/OS XL C/C++ Run-Time Library Reference] for more information about the error.

In the message text:

error_code
   Error code from dynalloc()
reason_code
   Reason code from dynalloc()

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.

GLD1862E The following specified options are ignored when performing phase options.

Explanation: The ldif2ds utility has been invoked with one or more command-line parameters that do not apply to the requested phases of processing (check, prepare, and/or load). The extraneous parameters are ignored.

In the message text:

phase
   Processing phases
options
   Ignored command-line parameters

Example: None.
System action: The utility continues.
Operator response: None.
GLD1863E  The 'attribute' attribute cannot be used in the entry distinguished name for entry 'name'.

Explanation: The ldif2ds utility encountered an entry which contains an attribute in its relative distinguished name (RDN) that is not allowed to be part of the RDN. The following attributes cannot be used in an entry RDN: aclEntry, aclPropagate, entryOwner, ownerPropagate, ibm-EntryUUID, creatorsName, createTimestamp, modifiersName, modifyTimestamp. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

attribute  Attribute type

name  Entry distinguished name

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Ensure that only the parameters that pertain to the requested phases of processing are specified on the utility command line.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1864E  The dynamic group URL 'url' on entry 'name' is not valid.

Explanation: The ldif2ds utility encountered a dynamic group entry with a memberURL attribute value that is not supported. The value is indicated in the message. A previous message indicates the name of the LDIF file containing the entry. The format of a dynamic group URL is ldap://dn?scope?filter, where dn is the distinguished name of the base entry for the search, scope is the search scope, and filter is the search filter. The valid values for the search scope are base, one, and sub. All of the attribute types specified in the search filter must be defined in the LDAP server schema and each assertion value must conform to the matching rule for the associated attribute type. BINARY attribute types cannot be specified in a search filter.

In the message text:

url  Dynamic group URL

name  Entry distinguished name

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Ensure that the memberURL attribute contains valid values for the distinguished name, search scope, and search filter. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1865E  An unsupported value 'value' is specified for attribute 'ref' in entry 'name'.

Explanation: The ldif2ds utility encountered a referral entry with a ref attribute value that is not supported by the LDAP server. The value is indicated in the message. A previous message indicates the name of the LDIF file containing the entry. If the value is '', then a 0-length string was specified for the value. This could occur if the attribute is specified without a value.

In the message text:
value
   Unsupported attribute value

name
   Entry distinguished name

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Ensure that the ref attribute contains non-blank values. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1866E  Entry 'parent_name' which is a parent of 'child_name' failed objectclass checking:
error_text.

Explanation: The ldif2ds utility encountered a child entry with an objectclass that is not allowed based on the objectclass attribute values in the parent entry. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

parent_name
   Parent entry distinguished name

child_name
   Child entry distinguished name

error_text
   Error message text

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1867E  Entry 'cn=localhost' is not allowed an objectclass value of 'ibm-replicationContext'.

Explanation: The ldif2ds utility encountered a cn=localhost entry with the ibm-replicationContext objectclass attribute value. The cn=localhost entry is not allowed to be the root of a replication context. A previous message indicates the name of the LDIF file containing the entry.

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Remove the objectclass value ibm-replicationContext from the cn=localhost entry. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD1868E  Entry 'name' must be a master server if it has both 'ibm-replicaSubEntry' and 'ibm-replicaGateway' objectclass values.

Explanation: The ldif2ds utility encountered an entry with objectclass attribute values of ibm-replicaSubEntry and ibm-replicaGateway and the ibm-replicaServerIsMaster attribute value is not set to TRUE. A previous message indicates the name of the LDIF file containing the entry.

In the message text:

name
   Entry distinguished name

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.
GLD1869W • GLD1871E

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Remove either the
ibm-replicaSubEntry or ibm-replicaGateway
objectclass attribute value or set the
ibm-replicaServerIsMaster attribute value to TRUE to
designate this server as a master server. Then restart
the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1869W  A mismatch is detected between the
serverCompatLevel (value) and the
database version value (major) in the
name backend. The utility checks entries
based on the serverCompatLevel setting.

Explanation: The ldif2ds utility detected a mismatch
between the serverCompatLevel value in the server
configuration file and the database version for the
backend identified in the message. The ldif2ds utility
does entry checking based on the serverCompatLevel
setting which indicates the entries that are supported in
the backend.

In the message text:
value
serverCompatLevel option value
major
database version number
name
Backend name
Example: None.
System action: The utility continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Verify that the correct LDAP
server configuration file is being used by the ldif2ds
utility. Also, verify that the serverCompatLevel option
is set to the correct value in the configuration file. See
the description of the serverCompatLevel configuration
option in Customizing the LDAP server configuration
for more information about the entries that are
supported at each compatibility level.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD1871E  Entry 'name' has a duplicate replication
consumer URL 'url'.

Explanation: The ldif2ds utility encountered an entry
with an objectclass attribute value of
ibm-replicationAgreement that contains a value for
ibm-replicaURL that already exists for the replication
context. The values for the ibm-replicaURL attribute
Example: None.
System action: The utility skips the rest of this entry
and continues the check phase with the next complete
entry. No entries are prepared or loaded.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Add the specified password
policy entry to the CDBM backend under the
cn=ibmpolicies subtree or update the
ibm-pwdIndividualPolicyDN or ibm-
pwdGroupPolicyDN attribute values in the entry to
specify a valid password policy. Then restart the
program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
type under an advanced replication context must all be unique.

In the message text:

- **name**
  - Entry distinguished name
- **url**
  - Replication consumer URL

**Example:** None.

**System action:** The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Ensure that the ibm-replicaURL attribute contains a unique value within the scope of the replication context. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1873E** Unable to decode the 'replicateOperationalAttributes' control found at line **line_number** of **filename**.

**Explanation:** The ldif2ds utility encountered an error decoding the replicateOperationalAttributes control. The replicateOperationalAttributes control contains base64 encoded values for the creatorsName, createTimestamp, modifiersName, and modifyTimestamp operational attribute values.

In the message text:

- **line_number**
  - Line Number
- **filename**
  - LDIF file name

**Example:** None.

**System action:** The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Ensure that the replicateOperationalAttributes control is properly encoded. Then restart the program. If the problem persists, remove the replicateOperationalAttributes control from the LDIF file.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD1872E** The replication filter 'value' on entry 'name' is not valid.

**Explanation:** The ldif2ds utility encountered a replication filter entry with an ibm-replicationFilterAttr attribute value that is not supported. The value is indicated in the message. A previous message indicates the name of the LDIF file containing the entry. The format of a replication filter is: (objectclass=objclass):[[attr1, attr2...]] where objclass is an objectclass attribute value and attr1, attr2, and so on, is a list of attribute values to filter separated by a comma. The objclass and any attribute values specified in the replication filter entry must be defined in the LDAP server schema.

In the message text:

- **value**
  - Filter value
- **name**
  - Entry distinguished name

**Example:** None.

**System action:** The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

**Operator response:** None.
Replication context entry 'name' missing explicit propagating type specification.

Explanation: The ldif2ds utility encountered an error processing the entry specified in the message. If a replication context entry is not a suffix level entry, an aclEntry and entryOwner attribute value must be defined explicitly in that entry.

In the message text:

- **name**: Entry distinguished name
- **type**: Attribute type

Example: None.

System action: The utility skips the rest of this entry and continues the check phase with the next complete entry. No entries are prepared or loaded.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Add the specified attribute type to the entry. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

This section lists the messages returned by the utility programs.

GLD2001I  No Directory Server service has been configured.

Explanation:  No LDAP server backends have been configured.
Example:  None.
System action:  The program ends.
Operator response:  None.
User response:  None.
System programmer response:  None.
Administrator response:  None.
Problem determination:  Not applicable.
Source:  LDAP
Module:  None.
Routing code:  None.
Descriptor code:  None.
Automation:  Not applicable.

GLD2002I  Directory Server configuration utility has started.

Explanation:  The dsconfig utility has started.
Example:  None.
System action:  The program continues.
Operator response:  None.
User response:  None.
System programmer response:  None.
Administrator response:  None.
Problem determination:  Not applicable.
Source:  LDAP
Module:  None.
Routing code:  None.
Descriptor code:  None.
Automation:  Not applicable.

GLD2003I  Directory Server configuration utility has ended.

Explanation:  The dsconfig utility has ended.
Example:  None.
System action:  The program ends.
Operator response:  None.
User response:  None.
System programmer response:  None.
Administrator response:  None.
Problem determination:  Not applicable.
Source:  LDAP
Module:  None.
Routing code:  None.
Descriptor code:  None.
Automation:  Not applicable.

GLD2004D  The output data set name has been previously used. Existing members may be overwritten and data lost. Do you wish to continue? (yes/no)

Explanation:  The output data set specified on the dsconfig command already contains output from a previous run. This prompt is asking the user if they want to overwrite existing members in the output data set. If the output data set is currently being used for an LDAP server, a different output data set should be used for this invocation of the dsconfig utility.

In the message text:

name  Output data set name

Example:  None.
System action:  The utility continues after a yes response has been entered. The utility ends if the response is no.
Operator response:  None.
User response:  None.
System programmer response:  None.
Administrator response:  Respond by entering either yes or no.
Problem determination:  Not applicable.
Source:  LDAP
Module:  None.
GLD2005I • GLD2009E

Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2005I Terminating upon user request.
Explanation: The dsconfig utility is terminating upon user request.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2006I dsconfig usage message.
Explanation: The dsconfig utility help and usage menu.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2007E A blank option was found in file filename and is not allowed.
Explanation: The dsconfig utility has detected a blank option in the input profile.
In the message text:
filename
File that contains the blank option

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Correct the blank option. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2008E The value for option name contains non-printable characters.
Explanation: The dsconfig utility has detected that the value of the indicated option contains characters that cannot be printed.
In the message text:
name
Option name

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Correct the value. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2009E An option was specified for a database backend (type) that is not configured.
Explanation: A database backend option is specified but the corresponding database backend is not configured.
In the message text:
type
Backend type
GLD2016E  ADDRMODE 'value' must be either 31 or 64.

Explanation: The ADDRMODE option must have a value of 31 or 64.

In the message text:

value
   ADDRMODE option value

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Either remove the database backend option or configure the corresponding database backend. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2017E  option with value 'current_value' in file
filename was previously set to 'original_value'.

Explanation: An option is specified more than once in the file. This option can only be specified once.

In the message text:

option
   Option name

current_value
   Current option value
filename
   File that contains the duplicate options
original_value
   Original option value

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Change the ADDRMODE value to either 31 or 64. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2018E  File filename: error_text

Explanation: An error occurred while processing a file or data set.

In the message text:

filename
   File or data set associated with the error
error_text
   Error message text

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Remove all but one of the duplicate options. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD2019E  *option* is not allowed in file *filename*.

Explanation: The indicated option is not allowed in the indicated profile.

In the message text:

*option*

  Option name not allowed

*filename*

  File containing the incorrect option

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Remove the option. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD2020E  Unable to allocate storage.

Explanation: An attempt to allocate storage was unsuccessful.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Increase the storage available for use by the utility. Then restart the program. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD2021E  The configuration profile has not been specified.

Explanation: The configuration profile name was not specified in the dsconfig command.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Re-issue the dsconfig command and specify the configuration profile using the -i command-line parameter.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD2022E  No network interface has been configured.

Explanation: No LISTEN option was found in the configuration profile.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Add one or more appropriate LISTEN options to the configuration profile. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD2023E  *option* in file *filename* has no input value.

Explanation: A required option is missing.

In the message text:

*option*

  Option name having no input value
**filename**
File in which option value must be included
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Add the required option to the indicated profile. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

---

**GLD2024E** The value for **option1** must be different from the value for **option2**.

Explanation: Values for the indicated options must be unique.
In the message text:

- **option1**
  - Option name
- **option2**
  - Option name

Example: Database directory names cannot be the same for LDBM, CDBM, and file-based GDBM backends. DB2 database user IDs cannot be the same for TDBM and DB2-based GDBM backends. Similarly, DB2 database names must be unique.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Change one of the option values so that the two option values are different. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

---

**GLD2025E** Operand missing for command parameter 'parameter'.

Explanation: No value was specified for the indicated `dsconfig` command-line parameter. This parameter must have a value.
In the message text:

- **parameter**
  - Command-line parameter

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Re-issue the `dsconfig` command and either specify a value for the parameter or remove the parameter from the command (if it is optional).
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

---

**GLD2026E** Value 'value' for option **option** is too long. It must be number characters or less.

Explanation: The `dsconfig` utility has detected that an option value is longer than the maximum characters allowed for that option.
In the message text:

- **value**
  - Option value
- **option**
  - Option name
- **number**
  - Maximum option length

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Edit the option value such that its length does not exceed the maximum allowed. Then restart the program.
Problem determination: Not applicable.
GLD2027E • GLD2030E

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2027E Command input 'value', is not valid.

Explanation: The dsconfig utility detected an incorrect command-line parameter. Either the parameter is not known or the value specified for the parameter is not supported. See [dsconfig utility] for more information about the dsconfig utility.

In the message text:

value
Incorrect command input

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2029E A required option has no input value.

Explanation: The dsconfig utility detected an option with no value. A previous message indicates the name of the option.

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2030E Value 'value' for option option is not valid.

Explanation: The dsconfig utility has detected that an option value is not valid.

In the message text:

value
Option value

option
Option name

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Specify a valid value for the option. Then restart the program.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
GLD2031E  The SERVERCOMPATLEVEL option must be value or greater when the option option is specified.

Explanation:  The usage of the configuration option indicated in the message text requires a minimum setting for the SERVERCOMPATLEVEL configuration option.

In the message text:
value
    Option value
option
    Option name

Example:  None.

System action:  The program ends.
Operator response:  None.
User response:  None.

System programmer response:  None.
Administrator response:  None.
Problem determination:  Not applicable.
Source:  LDAP
Module:  None.
Routing code:  None.
Descriptor code:  None.
Automation:  Not applicable.

GLD2256I utility_name: number entries have been processed.

Explanation:  The utility has processed the number of entries indicated in the message. If errors are encountered during processing, additional messages are issued to indicate these errors. The number of entries processed may not match the number of entries present in the output LDIF file if errors are encountered during processing.

In the message text:
utility_name
    Utility name
number
    Number of entries processed

Example:  None.

System action:  The program continues.
Operator response:  None.
User response:  None.

System programmer response:  None.
Administrator response:  None.
Problem determination:  Not applicable.
Source:  LDAP
Module:  None.
Routing code:  None.
Descriptor code:  None.
Automation:  Not applicable.

GLD2031E  GLD2258A
-d ALL on the command line of the utility. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

GLD2259I utility_name has terminated because there are no entries to process.

**Explanation:** The utility found no entries in the LDBM, TDBM, or CDBM backend to unload.

In the message text:

utility_name

Utility name

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Ensure that the backend that is to be unloaded contains entries. If necessary, correct the value specified for either the -s or the -n command line options. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

GLD2259I utility_name has terminated because there are no entries to process.

**Explanation:** The utility found no entries in the LDBM, TDBM, or CDBM backend to unload.

In the message text:

utility_name

Utility name

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Ensure that the backend that is to be unloaded contains entries. If necessary, correct the value specified for either the -s or the -n command line options. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

GLD2260I ds2dif_usage_message

**Explanation:** The utility help and usage menu.

In the message text:

utility_name

Utility name

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

GLD2263E utility_name found more than one backend section. Either use the -s or -n option to specify which TDBM, LDBM, or CDBM section to process or remove all but one of the database sections from the configuration file.

**Explanation:** If there are more than one TDBM, LDBM, or CDBM backends present in the LDAP server
configuration file, it is necessary to specify which backend needs to be unloaded by using the -n or -s command-line parameter on the ds2ldif utility. The utility is unable to determine which TDBM, LDBM, or CDBM backend needs to be unloaded if there are multiple TDBM, LDBM, or CDBM backends in the LDAP server configuration file.

In the message text:

utility_name
  Utility name

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: The ds2ldif utility provides two command-line parameters that are used to specify which TDBM, LDBM, or CDBM backend to process. These two parameters cannot be specified at the same time.

• The -s parameter specifies a subtree DN (distinguished name) whose entries are to be unloaded. The ds2ldif utility selects the TDBM, LDBM, or CDBM backend database section which contains this subtree from the LDAP server configuration file.

• The -n parameter indicates the name of a TDBM, LDBM, or CDBM backend whose entries are to be unloaded. This name is the optional fourth parameter that can be specified on the database option in the LDAP server configuration file. The ds2ldif utility selects the TDBM, LDBM, or CDBM database section with this name from the LDAP server configuration file.

Alternatively, modify the LDAP server configuration file and remove all TDBM, LDBM, or CDBM database sections except the one that needs to be unloaded.

Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD2265A There are no TDBM, LDBM, or CDBM backends with name 'name'.

Explanation: The ds2ldif utility is unable to find a TDBM, LDBM, or CDBM backend in the LDAP server configuration file with the backend name indicated in the message. This backend name is the value specified on the -n command-line parameter of the ds2ldif utility.

In the message text:

name
  Backend name

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.
Administrator response: Ensure that the LDAP server configuration file used by the `ds2ldif` utility has a `database` option for a TDBM, LDBM, or CDBM backend that includes the backend name indicated in the message. The backend name is the optional fourth parameter on the `database` configuration option. Verify that the TDBM, LDBM, or CDBM backend that is to be unloaded is correctly configured. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD2266I Unloading directory data from backend named `backend_name` under subtree DN: `entry_name`.

Explanation: The `ds2ldif` utility is unloading the entries under the indicated subtree DN (distinguished name) in the TDBM, LDBM, or CDBM backend with the indicated name.

In the message text:

`backend_name`
   Backend name

`entry_name`
   Distinguished name

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD2266E Unable to open file `filename`: `error_code`/`reason_code` - `error_text`

Explanation: The `ds2ldif` utility encountered an error while attempting to open the indicated file for writing. See the description of `fopen()` in [z/OS XL C/C++ Run-Time Library Reference](https://www.ibm.com/support/knowledgecenter/S特色V1R13/com.ibm.zos/v1r13.langz1e retailers) for more information about the error.

In the message text:

`filename`
   File name

`error_code`
   Error code from `fopen()`

`reason_code`
   Reason code from `fopen()`

`error_text`
   Text corresponding to the error code

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD2267I Unloading the `cn=schema` entry.

Explanation: The `ds2ldif` utility is unloading the LDAP server schema entry.

Example: None.

System action: The program continues.
GLD2269I  ds2ldif utility is starting.
Explanation: The ds2ldif utility has started.
Example: None.
System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2271E  Do not specify both of the following options: 'option1' and 'option2'.
Explanation: The ds2ldif utility encountered an error because it detected that the two indicated parameters are both specified on the utility command line, but they are mutually exclusive. These two command-line parameters cannot be specified at the same time. See ds2ldif utility for more information about the ds2ldif utility.
In the message text:

option1
Command-line parameter

option2
Command-line parameter

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Remove one of the mutually exclusive parameters from the command line of the ds2ldif utility. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2272I  ds2ldif version version, release, Service level level.
Explanation: The ds2ldif utility with version, release, and service level indicated in the message is running.
In the message text:

version
Utility version

release
Utility release

level
Utility service level

Example: None.
System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2273D Enter the LDAP administrator password to unload the directory:

Explanation: The ds2ldif utility has determined that it is necessary to perform an unloadRequest extended operation (OID 1.3.18.0.2.12.62), either because the LDAP server is already running or because the -r parameter is specified on the ds2ldif command line. When the utility uses the unloadRequest extended operation, it must first bind to the targeted LDAP server using the LDAP root administrator distinguished name, specified in the adminDN option in the LDAP server configuration file. The password used for the bind can be specified by the -w parameter on the ds2ldif command line, else by the adminPW option in the LDAP server configuration file. If neither of these is set, this prompt is displayed to obtain the password.

Example: None.
System action: The utility waits for a response from the user.
Operator response: None.
User response: None.
System programmer response: None.

GLD2275I Unloading directory data by using the unloadRequest extended operation.

Explanation: The ds2ldif utility is sending the unloadRequest extended operation (OID 1.3.18.0.2.12.62) to the LDAP server that is running to directly unload the wanted directory data. The utility sends the necessary information, including the values of the subtree DN (-s utility command-line parameter), the backend name (-n parameter), and the LDIF output file name (-o parameter) on the unloadRequest extended operation to the LDAP server.

Example: None.
System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.

GLD2276A The unloadRequest extended operation encountered an error: error_code - error_message.

Explanation: The unloadRequest extended operation (OID 1.3.18.0.2.12.62) encountered an error on the
targeted LDAP server while attempting to unload the wanted directory data.

In the message text:

**error_code**

unloadRequest server error code

**error_message**

unloadRequest server error message

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information returned from the targeted LDAP server in the message to correct the error. The error code is a standard LDAP protocol return code defined in RFC 2251 or in the /usr/lpp/ldapclient/include/ldap.h file. The information provided in the error message should be sufficient for determining the exact problem that was encountered on the LDAP server while attempting to perform the **unloadRequest** extended operation. It may be necessary to correct the LDAP server configuration file, restart the LDAP server, and then restart the ds2ldif utility with different command line options. If the problem persists, contact the service representative and provide the ds2ldif debug trace, the LDAP server configuration file, and the ds2ldif command that was attempted.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD2278A Unexpected error **error_code** occurred while decoding the **unloadResponse** extended operation.

**Explanation:** An unexpected error was encountered while attempting to BER decode the **unloadResponse** extended operation (OID 1.3.18.0.2.12.63) that was received from the targeted LDAP server. The **unloadResponse** extended operation is not valid.

In the message text:

**error_code**

unloadResponse decode error

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: The error code is an internal return code. To determine why the LDAP server constructed an **unloadResponse** extended operation that is not valid, turn on LDAP debug tracing by specifying -d ALL on both the ds2ldif utility and the LDAP server command lines (or use the LDAP server DEBUG operator modify command). Then restart the utility and the LDAP server if it is not running. If the problem persists, contact the service representative and provide the LDAP server and ds2ldif debug traces, the LDAP server configuration file, and the ds2ldif command that was attempted.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.
GLD2279A  Error encountered in getpass():

**Explanation:** An error was encountered while attempting to obtain the password for the LDAP root administrator so that an unloadRequest extended operation can be attempted. See the description of getpass() in [z/OS XL C/C++ Run-Time Library Reference](https://www.ibm.com/docs/en/zos-systems-library) for more information about the error.

**In the message text:**

- **error_code**
  - Error code from getpass()
- **reason_code**
  - Reason code from getpass()
- **error_text**
  - Text corresponding to the error code

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** getpass() is not supported in a TSO or batch environment. If the ds2ldif utility is run in those environments, you must specify the LDAP root administrator password using either the adminPW option in the LDAP server configuration file or the -w parameter on the ds2ldif utility command line. If you do not want to specify the LDAP root administrator's password in the clear, then run the ds2ldif utility from OMVS so that getpass() works correctly. If a problem with getpass() is encountered in an OMVS environment, verify that a password is entered. If the problem persists in an OMVS environment, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

GLD2278A  A fully qualified LDIF output filename must be specified on the -o option.

**Explanation:** The ds2ldif utility encountered an error in the LDIF output file name specified on the -o parameter on the utility command line. The ds2ldif utility requires a fully-qualified file name on the -o parameter.

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Verify that the LDIF output file name that is specified on the -o command-line parameter is in one of the following formats:

- **Fully-qualified z/OS UNIX System Services file name**
  - Example: /var/ldap/output.ldif

- **Fully-qualified file in a sequential dataset**
  - Example: //USER.OUTPUT.LDIF

- **Fully-qualified file in a partitioned dataset**
  - Example: //USER.OUTPUT(LDIF)

- **Fully-qualified file specified as a DD card in JCL**
  - Example: DD:OUTNAME

The fully-qualified z/OS UNIX System Services file names must start with an / and represent the pathname from the root directory. The fully-qualified sequential and partitioned data set names must start with the following two characters: // When ds2ldif is invoked from the shell, quotes must be used around the data set name. For example, the sequential data set name above would be specified as "//" 'USER.OUTPUT.LDIF". The DD card specified in JCL must start with the following three characters: DD: . However, a DD card cannot be used to specify the LDIF output file name if an unloadRequest extended operation is to be performed. Correct the -o parameter on the command line of the ds2ldif utility. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: An error occurred in the ldap_extended_operation() routine. The following are the common client errors:

81 The network connection to the targeted LDAP server has failed
89 A parameter specified on ldap_extended_operation is not valid
90 Insufficient storage is available
92 The LDAP protocol version must be V3 in order to initiate the unloadRequest extended operation
252 An unbind request has been issued for the LDAP handle

The following are the common server errors that are returned on the ldap_extended_operation() routine:

2 The server does not support the unloadRequest extended operation
12 A critical server control is either not recognized or is not supported for the unloadRequest extended operation.
53 The server is unable to perform the requested unloadRequest extended operation.

Depending upon the return code from ldap_extended_operation(), it may be necessary to correct the LDAP server configuration file, restart the LDAP server, and restart the ds2ldif utility. To obtain additional debug information, turn on LDAP debug tracing by specifying -d ALL on both the ds2ldif utility and the LDAP server command lines (or use the LDAP server DEBUG operator modify command). Then restart the utility and the LDAP server if it is not running. If the problem persists, contact the service representative and provide the ds2ldif debug trace, the LDAP server configuration file, and the ds2ldif command that was attempted.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2282A  GLD2283A

GLD2282A  An unexpected error occurred during the running of ds2ldif.
Explanation: The ds2ldif utility encountered an unexpected error during its processing.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: To obtain additional debug information, specify -d ALL on the command line of the utility. Then restart the program. Analyze the debug trace output and correct the error. If the problem persists, contact the service representative and provide the ds2ldif debug trace, the LDAP server configuration file, and the ds2ldif command that was attempted.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2283A  A DD card is not allowed to be specified when performing an unloadRequest extended operation.
Explanation: The ds2ldif utility does not allow a DD: card to be specified on the -o option when performing an unloadRequest extended operation. The ds2ldif utility will perform an unloadRequest extended operation when the LDAP server is already running or the -r option is specified on the ds2ldif command line.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Correct the -o parameter on the command line of the ds2ldif utility to no longer specify the DD: card. In order to use the same LDIF output file name that is specified on the DD card, update the -o option to specify that file name. If the unloadRequest extended operation is not wanted, stop the LDAP server and do not specify the -r option on the ds2ldif command line. Then restart the program.

Problem determination: Not applicable.
Source: LDAP
Module: None.
GLD2284A  There is no TDBM, LDBM, or CDBM backend present in the LDAP server configuration file to unload.

Explanation: When the ds2ldif utility is invoked without the -n or -s option, the utility searches for a TDBM, LDBM, or CDBM backend in the LDAP server configuration file. The utility was unable to find a TDBM, LDBM, or CDBM backend to unload.

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.

GLD2285E  The 'option1' option requires the 'option2' option.

Explanation: The ds2ldif utility encountered an error because it detected that option1 was missing required option2. If option1 is specified then option2 must be specified. See ds2ldif utility for more information about the ds2ldif utility.

Example: None.
System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2286I  Filtering directory data being unloaded using filters in filter DN: entry_name.

Explanation: The ds2ldif utility is using filters that are specified in the ibm-replicationfilterattr attribute values contained in the indicated filter DN (distinguished name). These filters may prevent some entries from being unloaded or may remove some attribute types and values from some unloaded directory entries.

Example: None.
System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD2401E  Encrypt all passwords that are presently unencrypted, AES encrypted, or DES encrypted (yes/no)?

Explanation: The db2pwden utility replaces any clear text (unencrypted), AES encrypted, or DES encrypted userPassword attribute values that exist in the directory with encrypted or hashed userPassword values based upon the setting of the pwEncryption option in the LDAP server configuration file. This message prompts the user of the db2pwden utility to ensure that encryption or hashing of the userPassword attribute values is really wanted.

Example: None.

System action: If the response is yes, y, or Y, the utility continues. Otherwise, the utility ends without encrypting or hashing userPassword attribute values.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: If clear text (unencrypted), AES encrypted, or DES encrypted userPassword attribute values in the directory are to be encrypted or hashed in the directory, enter yes, y, or Y. Otherwise, enter any other response to end the program.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2402A  No base is defined

Explanation: The utility encountered an error because a base DN (distinguished name) is not specified for the utility. The base DN can be specified on the -b command-line parameter of the utility or set on the LDAP_BASEDN environment variable. If set both ways, the command line value is used.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Specify the base DN (distinguished name) either by using the -b command-line parameter of the utility or by setting it on the LDAP_BASEDN environment variable. Then restart the program.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2410A  Memory allocation failed.

Explanation: An attempt to allocate storage was unsuccessful.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Increase the storage available for use by the utility. Then restart the program. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
GLD2411A  GLD2425A

Descriptor code: None.
Automation: Not applicable.

GLD2411A  The only supported mechanisms are EXTERNAL, GSSAPI, CRAM-MD5, and DIGEST-MD5.
Explanation: The utility encountered an error because an incorrect authentication mechanism is specified on the -m or -S command-line parameter.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Correct the -m or -S command-line parameter by specifying a valid authentication mechanism. The only supported authentication mechanisms are EXTERNAL, GSSAPI, CRAM-MD5, or DIGEST-MD5. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2417A  Error return_code reported parsing LDAP results.
Explanation: The ds2ldif utility encountered an error while attempting to parse LDAP results from the targeted LDAP server when performing the unloadRequest extended operation. The return code is from the ldap_result() routine. See the description of this routine in IBM Tivoli Directory Server Client Programming for z/OS for more information about the error.
In the message text:
return_code
  Return code from parsing results
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Verify that the targeted LDAP server is still running. To obtain additional debug information, specify -d ALL on the command line of the program. Then restart the utility. If the problem persists, contact the service representative.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2425A  A user name is required when doing a DIGEST-MD5 bind.
Explanation: When the -m DIGEST-MD5 or -S DIGEST-MD5 command-line parameter of the db2pwden utility is specified, the -U (user name) command-line option must also be specified.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Specify the user name on the -U command-line parameter of the db2pwd utility or change the -m or -S command-line parameter. Then restart the utility.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2426A Debug value is not valid.
Explanation: The utility encountered an error with the debug value that is specified on the -d command-line parameter of the utility. See the documentation for the utility for more information about valid debug values.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Specify a valid debug value on the -d command-line parameter of the utility or remove the parameter. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2435E Unable to retrieve LDAP results: error_code - 'error_text'
Explanation: The utility encountered an error while retrieving results from the targeted LDAP server. If running the ds2ldif utility, this occurred while attempting to perform an unloadRequest extended operation (OID 1.3.18.0.2.12.62) to unload the requested backend or subtree. See the description of ldap_result() in IBM Tivoli Directory Server Client Programming for z/OS for more information about the error.
In the message text:
error_code
   Error code from ldap_result()
error_text
   Error text corresponding to the error code
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Verify that the targeted LDAP server is still running when the request is sent and that TCP/IP is working properly between the utility and the LDAP server. To obtain additional debug information, specify -d ALL on the command line of the program. Then restart the utility. If the problem persists, contact the service representative.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD2426A Credentials are not valid for the specified LDAP server.
Explanation: The ds2ldif utility encountered an error while attempting to perform the LDAP root administrator authentication for the unloadRequest extended operation. The credentials specified on the -w command-line parameter are not valid for the adminDN configuration option.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Specify the correct credentials for the adminDN in the LDAP server configuration file on the -w command-line parameter of the ds2ldif utility. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD2436E  Unable to parse LDAP server results:
  error_code - 'error_text'.

Explanation: The utility encountered an error while attempting to parse results from the targeted LDAP server. If running the `ds2ldif` utility, this occurred while attempting to perform an `unloadRequest` extended operation (OID 1.3.18.0.2.12.62) to unload the requested backend or subtree. See the description of `ldap_parse_result()` in [IBM Tivoli Directory Server Client Programming for z/OS] for more information about the error.

In the message text:

- `error_code`
  - Error code from `ldap_parse_result()`

- `error_text`
  - Error text corresponding to the error code

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: If running the `ds2ldif` utility, verify that the correct LDAP administrator password is specified in the LDAP server configuration file or on the `-w` command line parameter of the `ds2ldif` utility. Verify that the correct adminDN is specified in the LDAP server configuration file used by the `ds2ldif` utility. Ensure that the LDAP administrator's account is not locked and the LDAP administrator's password is not expired. If the LDAP administrator's account is locked or the password has expired, the account must be unlocked or the password must be changed. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD2438E  Additional error information: error_text

Explanation: The targeted LDAP server returned an additional reason code message to the utility indicating a more specific reason for the request error. If running the `ds2ldif` utility, this occurred while attempting to perform an `unloadRequest` extended operation (OID 1.3.18.0.2.12.62) to unload the requested backend or subtree.

In the message text:

- `error_text`
  - Error text from `ldap_parse_result()`

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: If running the `ds2ldif` utility, verify that the correct LDAP root administrator password is specified in the LDAP server configuration file or on the `-w` command line parameter of the `ds2ldif` utility. Verify that the correct adminDN is specified in the LDAP server configuration file used by the `ds2ldif` utility. Ensure that the LDAP root administrator's account is not locked and the LDAP root administrator's password is not expired. If the LDAP root administrator's account is locked or the
password has expired, the account must be unlocked or
the password must be changed. Then restart the
program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD2439E Unable to parse password policy control
response: error_code - 'error_text'.

Explanation: The utility encountered an error while
 parsing the password policy control response from the
targeted LDAP server. If running the ds2ldif utility, this
occurred while attempting to perform an
unloadRequest extended operation (OID 1.3.18.0.2.12.62) to unload the requested backend or subtree. See the description of
ldap_parse_pwdpolicy_response() in IBM Tivoli
Directory Server Client Programming for z/OS for more
information about the error.

In the message text:

error_code
   Error code from ldap_parse_pwdpolicy_response()

error_text
   Error text corresponding to the error code

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: The password policy control
error message indicates the reason why authentication
may have failed on the targeted LDAP server. If
running the ds2ldif utility, verify that the password for
the LDAP root administrator is valid and the account is
not locked. After the LDAP root administrator’s
password is reset and the account is unlocked, restart
the utility.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD2441W Password policy control warning
response: warning_text

Explanation: The targeted LDAP server returned a
password policy control warning message to the utility. If
running the ds2ldif utility, this occurred while
attempting to perform an unloadRequest extended
operation (OID 1.3.18.0.2.12.62) to unload the requested backend or subtree.

In the message text:

warning_text
   Password policy control warning text

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.
Administrator response: The password policy control warning message indicates an informational message returned by the targeted LDAP server. If running the ds2ldif utility, this occurred while authenticating as the LDAP root administrator to the targeted LDAP server. The LDAP root administrator's password should be changed to allow continued access to the LDAP server.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD2442W  Time before password expiration is
         num_days days and
         num_hours hours num_minutes minutes
         num_seconds seconds.

Explanation: The targeted LDAP server returned a password policy control warning message to the utility indicating that the password is set to expire in the amount of time indicated in the message. If running the ds2ldif utility, this occurred while attempting to perform an unloadRequest extended operation (OID 1.3.18.0.2.12.62) to unload the requested backend or subtree.

In the message text:

num_days
  Number of days
num_hours
  Number of hours
num_minutes
  Number of minutes
num_seconds
  Number of seconds

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Verify that the targeted LDAP server is still running and that TCP/IP communication is working properly between the utility and the LDAP server. To obtain additional debug information, specify -d ALL on the command line of the utility. Then restart the program. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD2443E  Unable to connect to targeted LDAP
         server: error_code = 'error_text'.

Explanation: The utility encountered an error while attempting to connect to the targeted LDAP server during authentication. If running the ds2ldif utility, this occurred while attempting to perform an
unloadRequest extended operation (OID 1.3.18.0.2.12.62) to unload the requested backend or subtree. See the description of ldap_sasl_bind() in IBM Tivoli Directory Server Client Programming for z/OS for more information about the error.

In the message text:

error_code
  Error code from ldap_sasl_bind()

error_text
  Error text corresponding to the error code

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Verify that the targeted LDAP server is still running and that TCP/IP communication is working properly between the utility and the LDAP server. To obtain additional debug information, specify -d ALL on the command line of the utility. Then restart the program. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
Chapter 3. TDBM messages (3000)

This section lists the messages returned by the TDBM backend.

GLD3301E Unable to load type backend named name because attribute type attribute is not defined.

Explanation: The LDAP server or utility found an attribute type used by an entry in the indicated backend is not defined in the LDAP schema.

In the message text:

- **type**
  - Backend type
- **name**
  - Backend name
- **attribute**
  - Undefined attribute type

Example: None.

System action: The backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: If the backend is needed, restart the LDAP server or utility without the backend section in the LDAP server configuration file and add the missing attribute type to the LDAP server schema. Then restore the backend section and restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD3303E TDBM backend specified for a non-TDBM database.

Explanation: The LDAP server or utility found that the TDBM backend DLL, `GLDBTD31/GLDBTD64`, is specified on a database option in the LDAP server configuration file but the type parameter on the option is not TDBM.

Example: None.
GLD3304E – GLD3305E

System action: The TDBM backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Correct the database option in the LDAP server configuration file so that the DLL and backend type match. Restart the program if it ended or if the TDBM backend is needed.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD3304E  type initialization terminated because DB2 is not available.

Explanation: The LDAP server or utility cannot initialize the indicated backend because DB2 is not available.

In the message text:

code  Native return code
state  SQL state
text  SQL message text

Example: None.

System action: If the error occurs during backend initialization, the backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. If the error occurs while processing a client request, the LDAP server continues but the client request fails. The utility ends in all cases.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. Then retry the client operation or restart the program if it stopped or if the backend is needed. Contact your DB2 database administrator if you are unable to resolve the problem.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD3306E  Error code code received for ODBC function name.

Explanation: The LDAP server or utility encountered an error for an ODBC (Open Database Connectivity) function. This message may be followed by additional messages providing further information about the error. See IBM Information Management Software for z/OS Solutions Information Center at [http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/index.jsp](http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/index.jsp) for more information about ODBC errors.

In the message text:

- **code**: ODBC error code
- **name**: ODBC function that returned the error code

Example: None.

System action: If the error occurs during backend initialization, the backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Then retry the client operation or restart the program if it stopped or if the backend is needed. Contact your DB2 database administrator if you are unable to resolve the problem.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD3308E  An internal type backend error has occurred.

Explanation: The LDAP server or utility has detected an internal programming error.

In the message text:

- **type**: Backend type

Example: None.

System action: If the error occurs during backend initialization, the backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Then retry the client operation or restart the program if it stopped or if the backend is needed. Contact your DB2 database administrator if you are unable to resolve the problem.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD3307E  Unable to create key identifier:

- error_code
- reason_code
- error_text

Explanation: The LDAP server or utility encountered an error when creating a key identifier. See the description of pthread_key_create() in [z/OS XL C/C++ Run-Time Library Reference](https://www.ibm.com/support/knowledgecenter/SSY47D_2.2.20/crun/libref/threads pthread_key_create.html) for more information about the error.

In the message text:
GLD3309E • GLD3311E

GLD3309E Unable to get thread-specific value:

---

Description:

Administrator response: Retry the client operation or restart the program if it stopped or if the backend is needed. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD3309E Unable to get thread-specific value:

---

Explanation:

The LDAP server or utility is unable to retrieve a thread-specific value. See the description of `pthread_getspecific()` in `z/OS XL C/C++ Run-Time Library Reference` for more information about the error.

In the message text:

`error_code`
- Error code from `pthread_getspecific()`

`reason_code`
- Reason code from `pthread_getspecific()`

`error_text`
- Error text corresponding to the error code

Example: None.

System action: If the error occurs during backend initialization, the backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to `terminate` (this is the default if the configuration option is not specified), the program ends. If the error occurs while processing a client request, the LDAP server continues but the client request fails. The utility ends in all cases.

Operator response: None.

User response: None.

System programmer response: None.

---

GLD33111E Database access unavailable for type backend named name because DB2 is terminating.

---

Explanation:

The DB2 database manager is terminating and the `db2Terminate` option in the LDAP server configuration file is set to `recover` or `restore` (this is the default value).

Example: None.

System action: If the error occurs during backend initialization, the backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to `terminate` (this is the default if the configuration option is not specified), the program ends. If the error occurs while processing a client request, the LDAP server continues but the client request fails. The utility ends in all cases.

Operator response: None.

User response: None.

System programmer response: None.

---

GLD3310E Unable to set thread-specific value:

---

Explanation:

The LDAP server or utility is unable to set a thread-specific value. See the description of `pthread_setspecific()` in `z/OS XL C/C++ Run-Time Library Reference` for more information about the error.

In the message text:

`error_code`
- Error code from `pthread_setspecific()`

`reason_code`
- Reason code from `pthread_setspecific()`

`error_text`
- Error text corresponding to the error code

Example: None.

System action: If the error occurs during backend initialization, the backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to `terminate` (this is the default if the configuration option is not specified), the program ends. If the error occurs while processing a client request, the LDAP server continues but the client request fails. The utility ends in all cases.

Operator response: None.

User response: None.

System programmer response: None.
In the message text:

**type**
  Backend type

**name**
  Backend name

**Example:** None.

**System action:** The LDAP server continues to run but access to the indicated backend is not available until the DB2 database is available. Client requests to that backend are rejected.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Restart the DB2 database manager.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD3312I**

Database access available for **type** backend named **name** because DB2 has restarted.

**Explanation:** The DB2 database manager is restarting and the LDAP server can once more access the indicated backend.

In the message text:

**type**
  Backend type

**name**
  Backend name

**Example:** None.

**System action:** The LDAP server continues. Client requests to that backend are now processed.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD3314E**

Column **name** in the **owner.table** table is not defined correctly.

**Explanation:** The LDAP server or utility has found that a required column in the indicated DB2 table is not defined correctly. Either a non-modifiable column has the wrong length or a modifiable column has a length less than 8.

In the message text:

**name**
  Column name

**owner**
  Database owner

**table**
  Database table

**Example:** None.

**System action:** The backend does not start. If the **srvStartUpError** option in the LDAP server configuration file is set to **ignore**, the LDAP server continues to run with those backends that successfully start. If the **srvStartUpError** option is set to **terminate** (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Review the SPUFI script used to create the DB2 database and ensure that all tables and columns used by the IBM Tivoli Directory Server for z/OS are defined. A DB2 database created by using the SPUFI script shipped in the Integrated Security Services LDAP server must be migrated before it can be used by the IBM Tivoli Directory Server for z/OS. Correct or migrate the DB2 database. Then restart the program if it ended or if the backend is needed.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
GLD3315E • GLD3316E

In the message text:

**name**
Column name

**owner**
Database owner

**table**
Database table

Example: None.

**System action:** The backend does not start. If the **srvStartUpError** option in the LDAP server configuration file is set to **ignore**, the LDAP server continues to run with those backends that successfully start. If the **srvStartUpError** option is set to **terminate** (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Review the SPUFI script used to create the DB2 database and ensure that the column sizes are acceptable for the IBM Tivoli Directory Server for z/OS. A DB2 database created by using the SPUFI script shipped in the Integrated Security Services LDAP server may not have acceptable column sizes for the IBM Tivoli Directory Server for z/OS. Correct the DB2 database. Then restart the program if it ended or if the backend is needed.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

In the message text:

**type database version major.minor is not supported.**

**Explanation:** The DB_VERSION value in the DB2 DIR_MISC table for this backend is set to an unsupported database version for this level of the LDAP server. The **serverCompatLevel** configuration option sets the DB_VERSION value in the DB2 DIR_MISC table.

**Example:** None.

**System action:** The backend does not start. If the **srvStartUpError** option in the LDAP server configuration file is set to **ignore**, the LDAP server continues to run with those backends that successfully start. If the **srvStartUpError** option is set to **terminate** (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** The DB_VERSION value in the DB2 DIR_MISC table is not correct for this release of the z/OS LDAP server. The DB_VERSION value may have been updated when running this DB2-based backend on a later release of the z/OS LDAP server because the **serverCompatLevel** value was set or allowed to default to the incorrect value. See the **serverCompatLevel** option in **Customizing the LDAP server configuration** for information about the server compatibility levels supported at each z/OS LDAP server release. Also see **Fallback from a TDBM or DB2-based GDBM backend in z/OS IBM TDS to an earlier z/OS IBM TDS version** for fallback procedures to run one the later release. Then restart the program if it ended or if the backend is needed.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

GLD3316E  Attribute type identifier 'name' is too long.

**Explanation:** The LDAP server or utility found an attribute type in the schema whose identifier is too long. The TDBM database limits the maximum length of attribute type identifiers to 200 characters.

In the message text:

**name**
Attribute type identifier

**Example:** None.

**System action:** The backend does not start. If the **srvStartUpError** option in the LDAP server configuration file is set to **ignore**, the LDAP server continues to run with those backends that successfully start. If the **srvStartUpError** option is set to **terminate** (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: If the program ended or if the backend is needed, restart the LDAP server without the TDBM backend section in the LDAP server configuration file and modify the LDAP server schema to specify a shorter name for the attribute type. Then restore the backend section in the configuration file and restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

---

GLD3317E Object class identifier 'name' is too long.

Explanation: The LDAP server or utility found an object class in the schema whose identifier is too long. The TDBM database limits the maximum length of object class identifiers to 200 characters.
In the message text:

name Object class name

Example: None.

System action: The backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.
Operator response: None.
User response: None.
System programmer response: None.

---

GLD3318W Database suffix 'suffix' is not configured.

Explanation: A backend directory contains a suffix entry that is not in the list of suffixes specified by the suffix options for this backend in the LDAP server configuration file.
In the message text:

suffix Database suffix distinguished name

Example: None.

System action: Backend initialization continues, but directory entries under this suffix are not accessible.
Operator response: None.
User response: None.
System programmer response: None.

---

GLD3319E Database suffix 'directory_suffix' overlaps configured suffix 'configured_suffix'.

Explanation: The LDAP server or utility found that a backend directory contains a suffix entry that is an ancestor or descendant of a suffix in the list of suffixes for this backend. The list of suffixes is specified by the suffix options for this backend in the LDAP server configuration file.
In the message text:

directory_suffix Distinguished name of existing suffix in directory
configured_suffix Configured suffix distinguished name

Example: None.

System action: The backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not
specified), the program ends. The utility ends regardless of the option value.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Correct the LDAP server configuration file either by removing the suffix option for the suffix that is overlapped or by changing it to match the suffix that exists in the directory. Then restart the program if it ended or if the backend is needed.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD3321E The DIR_REPENTRY.CHNGDN column is smaller than the DIR_ENTRY.DN column.

Explanation: The LDAP server or utility found that a column in a DB2 table is too small. The size of the CHNGDN column in the DIR_REPENTRY table must be at least as large as the size of the DN column in the DIR_ENTRY table in the DB2 database for this backend.
Example: None.

System action: The backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Increase the size of the CHNGDN column in the DIR_REPENTRY table or decrease the size of the DN column in the DIR_ENTRY table so that the DN column size is not greater than the CHNGDN column size. Then restart the program if it ended or if the backend is needed.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD3322E The attribute attribute for replication entry 'name' is not valid.

Explanation: A replica entry contains an attribute whose value is not supported. Basic replication is not performed for the replica identified by this entry until the value is corrected.

In the message text:
attribute
attribute type
name
Replica entry distinguished name
Example: None.

System action: The LDAP server continues. Directory updates are not replicated to the replica identified by this entry.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Modify the attribute value in the replica entry to correct the error.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD3323E Unable to add 'name' to the replication list.

Explanation: The LDAP server is unable to add the indicated replica entry to the replica list. Basic replication is not performed for the replica identified by this entry until the error is corrected. A previous message may indicate the cause of the failure.

In the message text:

name
    Replica entry distinguished name

Example: None.

System action: The LDAP server continues. Directory updates are not replicated to the replica identified by this entry.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the earlier message to correct the error. If there is no earlier message, use the LDAP server DEBUG operator modify command to turn on the ERROR debug level and then re-issue the operation. The output may assist in locating and correcting the problem.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD3324E Unable to wait for network event: error_code/ reason_code - error_text

Explanation: The LDAP server is unable to wait for a network event. See the description of selectex() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

error_code
    Error code from selectex()
reason_code
    Reason code from selectex()
error_text
    Error text corresponding to the error code

Example: None.

System action: The LDAP server continues, however TDBM basic replication is not available.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Restart the program if basic replication is needed. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD3325E Replication entry 'name' requires SSL but SSL support is not configured.

Explanation: The replicaUseSSL attribute is set to TRUE in the replica entry but SSL support is not configured in the LDAP server configuration file. Basic replication is not performed for the replica identified by this entry until the error is corrected.

In the message text:

name
    Replica entry distinguished name

Example: None.

System action: The LDAP server continues. Directory updates are not replicated to the replica identified by this entry.

Operator response: None.

User response: None.
GLD3326E • GLD3328E

System programmer response: None.
Administrator response: Either configure SSL support for the LDAP server in the LDAP server configuration file and then restart the LDAP server or modify the replica entry to specify FALSE for the replicaUseSSL attribute.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD3326E Replication failed with host:port: Error

error_code - error_text.

Explanation: The LDAP server is unable to replicate a directory modification to the indicated replica.
In the message text:
host
  Replica server host name
port
  Replica server port number
error_code
  Error code
error_text
  Error text corresponding to the error code

Example: None.
System action: The LDAP server continues. The failing replication request is periodically tried again until basic replication is successful.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to correct the error. The associated replica entry should be deleted from the directory if replication is no longer wanted for the failing replica. Deleting and then adding the replica entry will reset the replication status so that only future directory modifications will be replicated to the replica.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD3327E Unable to create LDAP handle for replication with host.

Explanation: The LDAP server is unable to create an LDAP handle for use with the indicated replica. This indicates the ldap_init() or ldap_ssl_init() routine failed.
In the message text:
host
  Replica server host name
port
  Replica server port number

Example: None.
System action: The LDAP server continues. Basic replication does not occur for that replica.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Verify that the replica host name and port are correct. If not, modify them in the associated replica entry. If SSL is being used, verify that SSL is configured in the LDAP server configuration file and is available.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD3328E Additional information: text

Explanation: This message provides additional information for a replication error. The text is the error message returned by the replica server.
In the message text:
text
  Additional text

Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the message to assist in correcting the error.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD3329E  Group owner for type backend named name cannot be contacted.

Explanation: The LDAP server is unable to contact the LDAP server that owns the indicated database in the LDAP cross-system group in the sysplex.

In the message text:

  type  Backend type
  name  Backend name

Example: None.

System action: The LDAP server continues. Changes to the backend database may not be replicated to the replica servers for the backend.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Determine the owning system by issuing the LDAP server DISPLAY XCF operator modify command for the LDAP server reporting the error. The command output indicates which LDAP server is the group owner. Then issue the DISPLAY XCF operator modify command for the owning LDAP server and verify that this server is really the group owner. Restart the owning LDAP server if there is no response to the DISPLAY XCF command. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD3330E  Unable to decrypt change request: Error_text.

Explanation: The LDAP server encrypts pending replication requests when the request contains attributes subject to encryption or hashing based on the pwEncryption or the secretEncryption option settings (for example, userPassword, ibm-slapdAdminPw, secretKey, replicaCredentials, ibm-replicaKeyPwd, or ibm-slapdMasterPw attribute values) and the secretEncryption option is specified in the LDAP server configuration file. The request must then be decrypted before it is sent to a replica server. This error indicates the LDAP server is unable to decrypt the request.

In the message text:

  Error_text

Example: None.

System action: The LDAP server continues. Basic replication does not occur for that replica.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the encryption key label specified in the secretEncryption option in the LDAP server configuration file has not been changed. If it has been changed, ensure that the previous encryption key label is still defined. Then restart the program.

GLD3331E  Unable to decrypt replica credentials: error_text.

Explanation: The LDAP server encrypts the password specified by the replicaCredentials attribute in a replica entry if the secretEncryption option is specified in the LDAP server configuration file. The password must then be decrypted before the LDAP server can bind to the replica server. This error indicates the LDAP server is unable to decrypt the replica password.

In the message text:

  error_text

Example: None.

System action: The LDAP server continues, however, TDBM basic replication may stall because this replication request cannot be processed.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the encryption key label specified in the secretEncryption option in the LDAP server configuration file has not been
GLD3332I • GLD3334E

changed. If it has been changed, ensure that the
previous encryption key label is still defined.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD3332I  type backend named name schema
migration has started.

Explanation: A TDBM backend was initially created
by an Integrated Security Services LDAP server and the
schema used for the TDBM backend is contained in an
entry in the TDBM backend. In the IBM Tivoli
Directory Server for z/OS, there is a single LDAP
server schema for all backends. The LDAP server has
begun to merge the TDBM backend schema into the
LDAP server schema.

In the message text:

    type
        Backend type
    name
        Backend name
Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD3334E  Schema migration has failed. error_text.

Explanation: A TDBM backend was initially created
by an Integrated Security Services LDAP server and the
schema used for the TDBM backend is contained in an
entry in the TDBM backend. In the IBM Tivoli
Directory Server for z/OS, there is a single LDAP
server schema for all backends. An error occurred
while the LDAP server was merging the TDBM
backend schema into the LDAP server schema.

In the message text:

    error_text
        Error text
Example: None.
System action: The TDBM backend does not start. If
the srvStartUpError option in the LDAP server
configuration file is set to ignore, the LDAP server
continues to run with those backends that successfully
start. If the srvStartUpError option is set to terminate
(this is the default if the configuration option is not
specified), the program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the
message to correct the error. Then restart the program if
it stopped or if the backend is needed.
Problem determination: Not applicable.
Source: LDAP

GLD3333I  type backend named name schema
migration has ended.

Explanation: A TDBM backend was initially created
by an Integrated Security Services LDAP server and the
schema used for the TDBM backend is contained in an
entry in the TDBM backend. In the IBM Tivoli
Directory Server for z/OS, there is a single LDAP
server schema for all backends. The LDAP server has
completed merging the TDBM backend schema into the
LDAP server schema.
GLD3335I  The option option is not supported in multi-server mode with DB_VERSION less than 4. The option is ignored.

Explaination: The option indicated in the message is specified in the LDAP server configuration file. However, the database for this backend is running in multi-server mode and has a DB_VERSION less than 4. This indicates that the TDBM database is being shared with an earlier version of the LDAP server. The configuration option is not supported in this environment.

In the message text:

option
    LDAP server configuration option

Example: None.

System action: The LDAP server continues. The option is ignored.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

GLD3337E  Backend backend_name on LDAP server server_name in the sysplex group has different persistent search settings than this server.

Explaination: This LDAP server does not have persistent search enabled but another server in the sysplex group does have persistent search enabled. All LDAP servers in a sysplex group must have the same persistent search settings.

In the message text:

backend_name
    Backend name

server_name
    LDAP server name

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: To disable persistent search on the server named in the message, set the persistentSearch option to off in the LDAP server configuration file on that server. To enable persistent search on this server, set the persistentSearch option to on in the LDAP server configuration file on this server. The LDAP server containing the configuration file that is changed must be restarted to put the change into effect.

Problem determination: Not applicable.

Source: LDAP
GLD3338E The option option is not supported in multi-server mode with DB_VERSION less than 4.

Explanation: The option indicated in the message is specified in the LDAP server configuration file. However, the TDBM database for this backend is running in multi-server mode and has a DB_VERSION less than 4. This indicates that the TDBM database is being shared with an earlier version of the LDAP server. The configuration option or its value is not supported in this environment. If the option is:

- `pwEncryption` - AES encryption cannot be used. DES encryption can be used if the DES keys are stored in ICSF. All other encryption methods are supported.
- `secretEncryption` - cannot be used. Even when this option is not specified, there can be problems using the `secretKey` and `replicaCredentials` attributes in this environment.
- `pwCryptCompat` - cannot be set to `no`. The earlier LDAP server only supports the EBCDIC version of the `crypt()` algorithm.

In the message text:

```
option
    LDAP server configuration option
```

Example: None.

System action: The backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to `terminate` (this is the default if the configuration option is not specified), the program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Remove the option or change its value in the LDAP server configuration file. Restart the program if it ended or if the backend is needed.

Problem determination: Not applicable.

Source: LDAP

Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD3341W  Insufficient row statistics gathered on column column of table owner.table.

Explanation: The LDAP server did not find any row statistics for the specified columns in the DB2 Catalog. This may indicate that the DB2 RUNSTATS utility was run without the options suggested to gather statistics for the indicated table and columns. In the message text:

Example: None.

System action: The LDAP server continues, however database queries may not have optimal performance.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD3342I  type backend named name is enabled for partition based key assignment.

Explanation: The specified backend of the LDAP server or utility assigns keys to new directory entries by using the partition-based key assignment algorithm.

In the message text:

type
name

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD3343E  The partitioning information stored in type backend named name is no longer consistent with the information stored in the DB2 database for this backend.

Explanation: The partitioning information of the DIR_SEARCH table space stored in memory by the specified backend is no longer consistent with the information stored in the DIR_EID table by that
**GLD3344E** • **GLD3345E**

backend. The user must have repartitioned the DIR_SEARCH table space and then started another LDAP server that is sharing the same DB2 database.

In the message text:
- **type**
  - Backend type
- **name**
  - Backend name

**Example:** None.

**System action:** The program continues. The request fails. Future entries added to this backend are not guaranteed to succeed until the program is restarted.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Restarting the LDAP server or utility updates the partition control blocks for the specified backend, making them consistent with the information stored in the DIR_EID table. If the DIR_SEARCH table space has indeed been repartitioned by the user, it is recommended to unload the data from the specified backend using the `ds2ldif` utility, recreate the database belonging to this backend, and reload the data back using the `ldif2ds` utility. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD3345E** Unable to add new entries to the DB2 database in **type** backend named **name** because all unique keys have been exhausted.

**Explanation:** The LDAP server or utility is unable to accept new entries because there are no unique keys available.

In the message text:
- **type**
  - Backend type
- **name**
  - Backend name

**Example:** None.

**System action:** The program continues, but the request fails. Future entries added to this backend will not succeed.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Restart the program. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

GLD3345E Unable to process the DB2 database belonging to **type** backend named **name**; error code **error_code**.

**Explanation:** The LDAP server or utility is unable to process the DB2 database belonging to the specified backend. The error code has the following values:

1. The DIR_EID table is required by the partitioned entry identifier assignment algorithm, but it is not defined in the DB2 database belonging to the specified backend. This scenario should never happen. If it does happen, this is most likely the result of someone dropping the DIR_EID table from the DB2 database manually. Important entry identifier information is lost if the DIR_EID table is dropped.

2. The value detected for the PARTITIONED_EID column of the DIR_MISC table in the DB2 database belonging to the specified backend is not valid. The PARTITIONED_EID column, besides being a NULL column, only allows values 'T' or 'F'.

3. The number of entry identifiers that have been assigned and recorded in the DB2 database belonging to the specified backend has exceeded the maximum number of entry identifiers allowed by the LDAP server.

In the message text:
- **type**
  - Backend type
- **name**
  - Backend name
- **error_code**
  - Error code

**Example:** None.

**System action:** The specified backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends that successfully
start. If the srvStartUpErr option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.

Operator response: None.
User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the problem. For error codes 1 and 3, consider unloading the data from the specified backend using the ds2ldif utility, rebuilding the DB2 database belonging to this backend, and reloading the data back using the ldif2ds utility. Restart the program if it did not start or if the backend is needed. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD3346E Unable to initialize the entry identifier assignment algorithm for type backend named name.

Explanation: The LDAP server or utility is unable to initialize the entry identifier assignment algorithm. A previous message indicates the reason for the failure.

In the message text:

\begin{verbatim}
  type
    Backend type
  name
    Backend name
\end{verbatim}

Example: None.

System action: The specified backend does not start. If the srvStartUpErr option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpErr option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.

Operator response: None.
User response: None.

System programmer response: None.

Administrator response: Use the information in the earlier message to correct the problem. Restart the program if it did not start or if the backend is needed.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD3350E The name backend requires that the serverCompatLevel (value) match the database version value (major).

Explanation: The TDBM backend has detected that it is a sysplex replica server and that the
GLD3351E

serverCompatLevel value in the server configuration file for this server does not match the database version for the backend identified in the message.

In the message text:

name  Backend name
value  serverCompatLevel option value
major  database version number

Example: None.

System action: The specified backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify the serverCompatLevel configuration option value is the same for all servers sharing the backend. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD3351E The 'type' backend named 'name' requires an EBCDIC encoding scheme. Encoding Scheme 'codeset' was found for table 'owner.table'.

Explanation: The LDAP server has detected that a DB2 database table for a TDBM or GDBM backend was created with a non-EBCDIC encoding scheme. The LDAP server only supports DB2 database tables that are created with an EBCDIC encoding scheme.

In the message text:

type  Backend type
name  Backend name
codeset  Encoding scheme code set

owner  Database owner
table  Database table

Example: None.

System action: The backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: The DB2 database must be re-created with an EBCDIC encoding scheme.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
Chapter 4. LDBM messages (6000)

This section lists the messages returned by the LDBM backend.

GLD6001E  Insufficient storage available for database control block.

Explanation: The LDAP server or utility is unable to allocate storage.

Example: None.

System action:
- If the error occurs during backend initialization, the backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.
- If the error occurs when the database is being reloaded because a moddn operation failed, then the database is marked as disabled. The LDAP server continues, but requests to the affected backend fail.
- Otherwise, the fileTerminate option in the backend section of the LDAP server configuration determines what the server does. If the fileTerminate option is set to terminate, the program ends. If the fileTerminate option is set to recover (this is the default if the configuration option is not specified), the LDAP server continues processing, but the backend is set to read-only mode.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the file exists and can be accessed by the LDAP server. Restart the LDAP server if it ended or if the backend is needed. To change the backend to read/write mode, use the LDAP server BACKEND operator modify command. Then try the request again.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD6004E  Unable to get status for database file filename: error_code/reason_code - error_text

Explanation: The LDAP server is unable to get status information about the indicated database file. See the description of fstat() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

- filename: Database file name
- error_code: Error code from fstat()
- reason_code: Reason code from fstat()
- error_text: Error text corresponding to the error code

Example: None.

System action:
- If the error occurs during backend initialization, the backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.
- If the error occurs when the database is being reloaded because a moddn operation failed, then the database is marked as disabled. The LDAP server continues, but requests to the affected backend fail.
- Otherwise, the fileTerminate option in the backend section of the LDAP server configuration determines what the server does. If the fileTerminate option is set to terminate, the program ends. If the fileTerminate option is set to recover (this is the default if the configuration option is not specified), the LDAP server continues processing, but the backend is set to read-only mode.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the file exists and can be accessed by the LDAP server. Restart the LDAP server if it ended or if the backend is needed. To change the backend to read/write mode, use the LDAP server BACKEND operator modify command. Then try the request again.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD6005E  type backend named name disabled.

Explanation: The LDAP server is unable to load the database for a backend and has put the backend in disabled state. A previous message indicates the reason for the failure.

In the message text:
**GLD6006E • GLD6007E**

**type**
- Backend type

**name**
- Backend name

**Example:** None.

**System action:** The LDAP server continues, however the backend can no longer process requests.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the earlier message to correct the error. Restart the LDAP server if the backend is needed. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD6007E** Unable to load type backend named name because object class objectclass is not defined.

**Explanation:** The LDAP server or utility found an object class used by an entry in the indicated backend is not defined in the LDAP server schema.

In the message text:

**type**
- Backend type

**name**
- Backend name

**objectclass**
- Undefined object class

**Example:** None.

**System action:** The backend does not start. If the **srvStartUpError** option in the LDAP server configuration file is set to **ignore**, the LDAP server continues to run with those backends that successfully start. If the **srvStartUpError** option is set to **terminate** (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** If the backend is needed, restart the LDAP server without the backend section in the LDAP server configuration file and add the missing object class to the LDAP server schema. Then restore the backend section in the configuration file and restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
GLD6008E Unable to load type backend named name because database file filename is not valid.

Explanation: The LDAP server or utility is unable to decode an entry in the indicated database file. This indicates that the database file has been modified and is no longer usable.

In the message text:
- type Backend type
- name Backend name
- filename Database file name

Example: None.

System action:
- If the error occurs during backend initialization, the backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.
- If the error occurs when the database is being reloaded because a moddn operation failed, then the fileTerminate option in the backend section of the LDAP server configuration determines what the server does. If the fileTerminate option is set to terminate, the program ends. If the fileTerminate option is set to recover (this is the default if the configuration option is not specified), the LDAP server continues processing, but the backend is marked as disabled and requests to the affected backend fail.
- Otherwise, the fileTerminate option in the backend section of the LDAP server configuration determines what the server does. If the fileTerminate option is set to terminate, the program ends. If the fileTerminate option is set to recover (this is the default if the configuration option is not specified), the LDAP server continues processing, but the backend is set to read-only mode.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: If the backend is needed, restore the indicated database file from a backup. Then restart the program. If you must determine which entry in the database file is not valid, restart the LDAP server with -d ERROR specified on the command line.

GLD6009E Unable to open directory path:
  error_code/reason_code - error_text

Explanation: The LDAP server or utility is unable to open the indicated file directory. See the description of opendir() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:
- path LDBM database directory path
- error_code Error code from opendir()
- reason_code Reason code from opendir()
- error_text Error text corresponding to the error code

Example: None.

System action:
- If the error occurs during backend initialization, the backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.
- If the error occurs during an attempt to become the sysplex group owner, the LDAP server ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Verify that the directory exists and can be accessed by the LDAP server. Restart the program if it stopped or if the backend is needed.
GLD6010E • GLD6012E

**Automation:** Not applicable.

---

**GLD6010E** Unable to read directory paths

**Explanation:** The LDAP server or utility is unable to read the indicated file directory. See the description of readdir_r() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

- **path**
  - LDBM database directory path
- **error_code**
  - Error code from readdir_r()
- **reason_code**
  - Reason code from readdir_r()
- **error_text**
  - Error text corresponding to the error code

**Example:** None.

**System action:**

- If the error occurs during backend initialization, the backend does not start. If the **srvStartUpError** option in the LDAP server configuration file is set to **ignore**, the LDAP server continues to run with those backends that successfully start. If the **srvStartUpError** option is set to **terminate** (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.
- If the error occurs during an attempt to become the sysplex group owner, the LDAP server ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. Verify that the directory exists and can be accessed by the LDAP server. Restart the program if it stopped or if the backend is needed.

**Problem determination:** Not applicable.

**Source:** LDAP

---

**GLD6012E** Unable to open database file filename:

**Explanation:** The LDAP server is unable to open the indicated database file. See the description of open() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

- **filename**
  - LDBM database file name
- **error_code**
  - Error code from open()
- **reason_code**
  - Reason code from open()
- **error_text**
  - Error text corresponding to the error code

**Example:** None.

**System action:**

- If the error occurs during backend initialization, the backend does not start. If the **srvStartUpError** option in the LDAP server configuration file is set to **ignore**, the LDAP server continues to run with those backends that successfully start. If the **srvStartUpError** option is set to **terminate** (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.
- If the error occurs during an attempt to become the sysplex group owner, the LDAP server ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. Verify that the file can be accessed by the LDAP server. Restart the program if it stopped or if the backend is needed.

**Problem determination:** Not applicable.

**Source:** LDAP

---

**GLD6011E** Unable to delete database file filename:

**Explanation:** The LDAP server or utility is unable to delete the indicated database file. See the description of remove() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

- **filename**
  - Database file name
- **error_code**
  - Error code from remove()
GLD6013E

Unable to read database file filename:
error_code/reason_code - error_text

Explanation: The LDAP server is unable to read the indicated database file. The error occurred in the read() or readv() routine. See the description of these routines in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

reason_code
Reason code from open()

error_text
Error text corresponding to the error code

Example: None.

System action:

- If the error occurs during backend initialization, the backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.
- If the error occurs when the database is being reloaded because a moddn operation failed, then the database is marked as disabled. The LDAP server continues, but requests to the affected backend fail.
- Otherwise, the fileTerminate option in the backend section of the LDAP server configuration determines what the server does. If the fileTerminate option is set to terminate, the program ends. If the fileTerminate option is set to recover (this is the default if the configuration option is not specified), the LDAP server continues processing, but the backend is set to read-only mode.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the message to correct the error. Verify that the file exists and can be accessed by the LDAP server. Restart the LDAP server if it ended or if the backend is needed. To change the backend to read/write mode, use the LDAP server BACKEND operator modify command. Then try the request again.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
GLD6014E  Unable to write database file filename:
  error_code/reason_code - error_text

Explanation:  The LDAP server is unable to write the indicated database file. The error occurred in the write(), writev(), or close() routine. See the description of these routines in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:
  filename  Database file name
  error_code  Error code from routine
  reason_code  Reason code from routine
  error_text  Error text corresponding to the error code

Example:  None.

System action:
  • If the error occurs during backend initialization, the backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends.
  • If the error occurs when the database is being reloaded because a moddn operation failed, then the database is marked as disabled. The LDAP server continues, but requests to the affected backend fail.
  • Otherwise, the fileTerminate option in the backend section of the LDAP server configuration determines what the server does. If the fileTerminate option is set to terminate, the program ends. If the fileTerminate option is set to recover (this is the default if the configuration option is not specified), the LDAP server continues processing, but the backend is set to read-only mode.

Operator response:  None.
User response:  None.
System programmer response:  None.
Administrator response:  Use the information in the message to correct the error. Verify that the file can be accessed by the LDAP server. Restart the LDAP server if it ended or if the backend is needed. To change the backend to read/write mode, use the LDAP server BACKEND operator modify command. Then try the request again.

Problem determination:  Not applicable.
Source:  LDAP
Module:  None.
Routing code:  None.
Descriptor code:  None.
Automation:  Not applicable.

GLD6015E  type version number file_type files are not supported.

Explanation:  The indicated file format is not supported by the current level of the LDAP server.

In the message text:
  type  Backend type
  number  File version number
  file_type  File type

Example:  None.

System action:
  • If the error occurs during initialization, the backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.
  • If the error occurs after initialization, the program continues but replication is not performed.

Operator response:  None.
User response:  None.
System programmer response:  None.
Administrator response:  Either restore the LDAP server to the level used to create the database file or remove the indicated backend from the LDAP server configuration file. Restart the LDAP server if it ended or if the backend is needed.

Problem determination:  Not applicable.
Source:  LDAP
Module:  None.
Routing code:  None.
Descriptor code:  None.
Automation:  Not applicable.

GLD6016I  Suffix suffix in database file filename is not configured and will be ignored.

Explanation:  A backend directory contains a suffix entry that is not in the list of suffixes specified by the suffix options for this backend in the LDAP server configuration file.
In the message text:

**suffix**
- Database suffix distinguished name

**filename**
- Database file name

**Example:** None.

**System action:** Backend initialization continues, but directory entries under this suffix are not accessible.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** If access to the entries using this suffix is needed, add a `suffix` option specifying this suffix to the backend section of the LDAP server configuration file. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD6020E**

**Suffix `suffix` is not configured but the checkpoint file is not empty.**

**Explanation:** A suffix has been removed from the LDBM backend section of the LDAP server configuration file, but there are one or more checkpoint records to be processed for that suffix.

In the message text:

**suffix**
- Database suffix distinguished name

**Example:** None.

**System action:** The backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to `terminate` (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Add a `suffix` option with the indicated value to the LDBM backend section of the LDAP server configuration file. Then restart the LDAP server. After LDAP server initialization is complete and the checkpoint records have been processed, you can stop the LDAP server and remove the added `suffix` option if you do not need that suffix. The LDAP server can now be started without the indicated suffix in the LDAP server configuration file.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD6021W**

**Group `name` contains an incorrect memberURL attribute value.**

**Explanation:** The dynamic group membership URL cannot be evaluated. The format of a dynamic group URL is `ldap:///?dn=scope?filter`, where `dn` is the distinguished name of the base entry for the search, `scope` is the search scope, and `filter` is the search filter. The valid values for the search scope are `base`, `one`, and `sub`. All of the attribute types specified in the search filter must be defined in the LDAP server schema and each assertion value must conform to the matching rule for the associated attribute type. BINARY attribute types cannot be specified in a search filter.

In the message text:

**name**
- Dynamic group distinguished name

**Example:** None.

**System action:** The LDAP server continues. The dynamic group is not used in determining group memberships.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Modify the dynamic group URL to contain valid values for the base distinguished name, search scope, and search filter.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
### GLD6022E  
**Time limit exceeded while loading** *type*  
**backend named** *name*  
**from group owner.**

**Explanation:** The LDAP server waits a maximum of 60 seconds after requesting a copy of the indicated backend database from the LDAP server that owns the database in the cross-system group. This message indicates that the owning LDAP server is not responding to the request.

In the message text:

- **type**  
  Backend type
- **name**  
  Backend name

**Example:** None.

**System action:**
- If the error occurs during initialization, the backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to `terminate` (this is the default if the configuration option is not specified), the program ends.
- If the error occurs after initialization, the program continues. Update operations to the LDAP server probably fail. Search operations may succeed.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Determine the owning system for this backend by issuing the LDAP server `DISPLAY XCF` operator `modify` command for the LDAP server reporting the error. The command output indicates which LDAP server is the group owner. Then issue `DISPLAY XCF` for the owning LDAP server and verify that this server is really the group owner. Restart the owning LDAP server if there is no response to the `DISPLAY XCF` command. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

### GLD6023E  
**Database owner for** *type*  
**backend named** *name*  
**database XCF data record is not valid.**

**Explanation:** The LDAP server is unable to obtain a current copy of the database indicated in the message from the LDAP server that owns the database in the cross-system group. The return code displayed in the message is either from the attempt to send an XCF message to the database owner or from the reply from the owner if it could not send back the database.

In the message text:

- **type**  
  Backend type
- **name**  
  Backend name
- **return_code**  
  LDAP return code

**Example:** None.

**System action:**
- If the error occurs during initialization, the backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to `terminate` (this is the default if the configuration option is not specified), the program ends.
- If the error occurs after initialization, the program continues. Update operations to the LDAP server probably fail. Search operations may succeed.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Determine the owning system for this backend by issuing the LDAP server `DISPLAY XCF` operator `modify` command for the LDAP server reporting the error. The command output indicates which LDAP server is the group owner. Then issue `DISPLAY XCF` for the owning LDAP server and verify that this server is really the group owner. Restart the owning LDAP server if there is no response to the `DISPLAY XCF` command. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
Example:  None.

**System action:**
- If the error occurs during initialization, the backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to `terminate` (this is the default if the configuration option is not specified), the program ends.
- If the error occurs after initialization, the program continues but some operations may fail. A follow-on message indicates the effect on the program.

**Operator response:**  None.

**User response:**  None.

**System programmer response:**  None.

**Administrator response:**  Use the information in the follow-on message to resolve the problem. Restart the program if it ended or if the backend is needed.

**Problem determination:**  Not applicable.

**Source:**  LDAP

**Module:**  None.

**Routing code:**  None.

**Descriptor code:**  None.

**Automation:**  Not applicable.

---

**GLD6025E  GLD6026E**

---

**GLD6025E**  

**Suffix list for type backend named name does not match owner suffix list.**

**Explanation:**  The suffix list defined for the indicated backend in the LDAP server configuration file is not the same as the suffix list defined in the LDAP server configuration file of the LDAP server that owns the cross-system group resources.

In the message text:

- `type`  Backend type
- `name`  Backend name

**Example:**  None.

**System action:**  The backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to `terminate` (this is the default if the configuration option is not specified), the program ends.

**Operator response:**  None.

**User response:**  None.

**System programmer response:**  None.

**Administrator response:**  Use the information in the earlier message to correct the error. Then restart the LDAP server on each of the other systems to refresh its copy of the directory.

**Problem determination:**  Not applicable.

**Source:**  LDAP

**Module:**  None.

**Routing code:**  None.

**Descriptor code:**  None.

**Automation:**  Not applicable.

---

**GLD6026E**  

**Unable to send type backend named name database update to group members.**

**Explanation:**  The LDAP server is unable to send a database update to the other members of the cross-system group. The indicated backend directory has been successfully updated on this LDAP server, but the other members in the group do not have the updated database entry. A previous message indicates the reason for the failure.

In the message text:

- `type`  Backend type
- `name`  Backend name

**Example:**  None.

**System action:**  The LDAP server continues, but an LDAP operation for the indicated backend may return different results depending on if it is processed by this LDAP server or by another LDAP server in the cross-system group.

**Operator response:**  None.

**User response:**  None.

**System programmer response:**  None.

**Administrator response:**  Use the information in the earlier message to correct the error. Then restart the LDAP server on each of the other systems to refresh its copy of the directory.

**Problem determination:**  Not applicable.

**Source:**  LDAP

**Module:**  None.

**Routing code:**  None.

**Descriptor code:**  None.

**Automation:**  Not applicable.
GLD6028E  GLD6030E

GLD6028E  type directory path does not match group owner directory owner_path.

Explanation: The directory path specified by the databaseDirectory option in the backend section of the LDAP server configuration file is not correct. When multi-server mode is active, the directory path must be the same for this backend in each LDAP server in the cross-system group.

In the message text:

- **type**: Backend type
- **path**: Directory path in the LDAP server
- **owner_path**: Directory path in the owning LDAP server

Example: None.

System action: The backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends. The utility ends regardless of the option value.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Correct the database option in the LDAP server configuration file so that the DLL and backend type match. Restart the program if it ended or if the LDBM backend is needed.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD6030E  Unable to truncate database file filename: error_code/reason_code - error_text

Explanation: The LDAP server is unable to truncate the indicated database file. See the description of ftruncate() in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

- **filename**: Database file name
- **error_code**: Error code from ftruncate()
- **reason_code**: Reason code from ftruncate()
- **error_text**: Error text corresponding to the error code

Example: None.

System action: If the fileTerminate option in the backend section of the LDAP server configuration file is set to terminate, the program ends. If the fileTerminate option is set to recover (this is the default if the configuration option is not specified), the LDAP server continues processing, but the backend is set to read-only mode.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Correct the file system problem. Verify that the file can be accessed by the LDAP server. Then restart the program if it has ended.
or change the backend to read/write mode using the LDAP server BACKEND operator modify command.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

GLD6031E Setting backend named \textit{name} to read-only because file\textit{Terminate} option is set to 'recover'.

**Explanation:** A write error is encountered while an LDAP server file-based backend is writing to the file system. Since the file\textit{Terminate} option in the backend section of the LDAP server configuration file is set to recover or the option is not specified at all, the LDAP server forces the backend directory into read-only mode.

In the message text:

\textit{name} Backend name

**Example:** None.

**System action:** The LDAP server continues to run. The backend contents cannot be modified.

**Operator response:** Verify that there is enough free space on the file system. Also verify that the LDAP server has read and write permissions on the database directory and files. A previous message indicates the reason for the failure.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the earlier message to correct the file system error. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

GLD6033I Committing changes to database for type backend named \textit{name}.

**Explanation:** The indicated LDAP server backend is going to commit changes in its checkpoint file to its database files. This can occur periodically during normal processing or when the server is shutting down. See Database commit processing for more information about file-based backend committing.

In the message text:

\textit{name} Backend name

**Example:** None.

**System action:** The LDAP server continues.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

GLD6032A Terminating LDAP server because file\textit{Terminate} option is set to 'terminate' in backend named \textit{name}.

**Explanation:** A write error is encountered while an LDAP server file-based backend is writing to the file system. Since the file\textit{Terminate} option in the backend section of the LDAP server configuration file is set to terminate, the program is ending. A previous message indicates the reason for the failure.

In the message text:

\textit{name} Backend name

**Example:** None.

**System action:** The program ends.

**Operator response:** Verify that there is enough free space on the file system. Also verify that the LDAP server has read and write permissions on the database directory and files.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the earlier message to correct the file system error. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
GLD6034I • GLD6036W

Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

---

GLD6034I Completed committing changes to database for type backend named name.

Explanation: The indicated LDAP server backend committed changes in its checkpoint file to its database files. This can occur periodically during normal processing or when the server is shutting down. See Database commit processing for more information about file-based backend committing.

In the message text:

- **type**: Backend type
- **name**: Backend name

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

---

GLD6035E Unable to commit changes to database for type backend named name, rc=rcode.

Explanation: The indicated LDAP server file-based backend failed to commit changes in its checkpoint file to its database files. A previous message indicates the reason for the failure. The contents of the backend are still there but the changes present in the checkpoint file were not successfully added to the appropriate database files. See Database commit processing for more information about file-based backend committing.

In the message text:

- **type**: Backend type
- **name**: Backend name

Example: None.

System action: The LDAP server continues and tries the request again.

Operator response: None.

User response: None.

System programmer response: None.

---

GLD6036W type backend named name database owner is busy, retrying.

Explanation: A request was sent from this LDAP server to the LDAP server that owns the database in the cross-system group. The database owner is either too busy to respond to the request or it is waiting for a DB2 connection.

In the message text:

- **type**: Backend type
- **name**: Backend name

Example: None.

System action: The LDAP server continues and tries the request again.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in the earlier message to correct the file system error. Then restart the program if it has ended or change the backend to read/write mode using the LDAP server BACKEND operator modify command.

Problem determination: Not applicable.

Source: LDAP

---
connection problem or shut down the LDAP server that owns the database.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD6037E** Value value for attribute type in replication entry 'name' is not valid.

**Explanation:** The replica entry contains an attribute value that is not supported. See [Basic replication] for more information about the attribute and its values.

In the message text:

- **value** Attribute value
- **type** Attribute type that contains value
- **name** Replica entry distinguished name

**Example:** None.

**System action:** The LDAP server continues to run. Basic replication is not performed to the replica server identified by this entry.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Modify the replica entry to correct the error.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD6038E** Unable to add 'name' to the replication list.

**Explanation:** The LDAP server is unable to synchronize the directory tree with the replication progress file.

In the message text:

- **name** Entry distinguished name

**Example:** None.

**System action:** The LDAP server continues. Basic replication is not performed to the replica server identified by this entry.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Resynchronize the replica server. See [Recovering from basic replication out-of-sync conditions] for more information.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD6039E** Unable to wait for network event:

```
error_code/reason_code - error_text
```

**Explanation:** The LDAP server is unable to wait for a network event. See the description of `selectex()` in [z/OS XL C/C++ Run-Time Library Reference] for more information about the error.

In the message text:

- **error_code** Error code from `selectex()`
- **reason_code** Reason code from `selectex()`
- **error_text** Error text corresponding to the error code

**Example:** None.

**System action:** The LDAP server continues, but basic replication is not performed.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the message to correct the error. Restart the program if replication is needed. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---
GLD6040E  Replication entry 'name' requires SSL but SSL support is not configured.

Explanation: The indicated replica entry specifies TRUE for the replicaUseSSL attribute but SSL support is not configured in the LDAP server configuration file.

In the message text:

name  Replica entry distinguished name

Example: None.

System action: The LDAP server continues. Basic replication is not performed to the replica server identified by this entry.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Either configure SSL support in the LDAP server configuration file and then restart the LDAP server, or modify the value of the replicaUseSSL attribute to FALSE.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD6041E  Replication failed with host:port: Error error_code - error_text.

Explanation: The LDAP server is unable to replicate a directory modification to the indicated replica server.

In the message text:

host  Replica server host name

port  Replica server port number

error_code  Error code

error_text  Error text corresponding to the error code

Example: None.

System action: The LDAP server periodically tries the failing replication request again until replication is successful.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD6042E  Unable to create LDAP handle for replication with host:port.

Explanation: The LDAP server is unable to create an LDAP handle for use with the indicated replica server. Either the ldap_init() or the ldap_ssl_init() routine failed. See the descriptions of ldap_init() or ldap_ssl_init() in [IBM Tivoli Directory Server Client Programming for z/OS] for more information about the error.

In the message text:

host  Replica server host name

port  Replica server port number

Example: None.

System action: The LDAP server continues. Basic replication does not occur for the indicated replica server.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the replica host
name and port are correct. If not, modify the replica entry to correct the values. If SSL is being used, verify that SSL is configured in the LDAP server configuration file and is available.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD6043E Additional information: error_text
Explanation: This message provides additional information for a replication error. The text is the error message returned by the replica server.
In the message text:

error_text
  Additional error text

Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD6045E Replica object name does not have corresponding progress table entry.
Explanation: The LDAP server has found a replica entry for which there is no replication progress information in the replica progress file.
In the message text:

name
  Replica entry distinguished name

Example: None.
System action: The LDAP server continues. Basic replication does not occur to this replica server. If the error occurs while adding or modifying a replica entry, the operation fails.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD6044E Unable to decrypt replica credentials: text.
Explanation: The LDAP server encrypts the password specified by the replicaCredentials attribute in a replica entry if the secretEncryption option is specified in the LDAP server configuration file. The password must then be decrypted before the LDAP server can bind to the replica server. The LDAP server is unable to decrypt the replica password.
In the message text:

text
  Error text

Example: None.
System action: The LDAP server continues. Basic replication does not occur to this replica server. If the error occurs while adding or modifying a replica entry, the operation fails.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD6046E  Progress table entry uuid does not have corresponding Replica object.

Explanation: The LDAP server detected data for a replica in the progress file that does not have a corresponding replica entry in the directory for this backend. The ibm-entryUUID of each replica entry is kept in the progress file to associate the progress data with the replica to which it pertains.

In the message text:

```
uuid
```

Replica entry ibm-entryUUID

Example: None.

System action: The LDAP server continues. The data for the replica is deleted from the progress file and replication to that replica server does not occur.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Search the backend for the specified ibm-entryUUID value to locate the replica entry for the replica. Delete and add the replica entry to restart basic replication to the replica.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD6047E  Unexpected state of replica type file, attempting recovery.

Explanation: The LDBM backend maintains several types of files containing replication information. When one of these files is changed, the current version of the file is renamed and eventually deleted when the new version of the file is created. The backend has found an old version of the file when it is not expected.

In the message text:

```
type
```

Type of replica file

Example: None.

System action: The LDAP server tries to correct the error and continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD6048E  Partial record read from file filename length=amount.

Explanation: The LDAP server is not able to read an entire record from the replication operations progress file.

In the message text:

```
filename
```

Replication operations progress file

```
amount
```

The amount of the record that was read

Example: None.

System action:

- If the error occurs during backend initialization, the backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the program ends.
- If the error occurs during an attempt to become the sysplex group owner, the LDAP server ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: If the backend is needed with basic replication, the replica servers for this backend must be resynchronized. See Recovering from basic replication out-of-sync conditions for more information. You might need to delete the file displayed in the message first. If basic replication is not needed, then stop the LDAP server if it is running, delete the indicated file, and restart the server.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
GLD6050E File filename missing.

Explanation: The replication progress file is not present when the replication queue file is present. Both files are needed for basic replication processing.

In the message text:

filename

Missing file name

Example: None.

System action:

• If the error occurs during backend initialization, the backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to `terminate` (this is the default if the configuration option is not specified), the program ends.
• If the error occurs during an attempt to become the sysplex group owner, the LDAP server ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD6050E File filename missing.

Explanation: The replication progress file is not present when the replication queue file is present. Both files are needed for basic replication processing.

In the message text:

filename

Missing file name

Example: None.

System action:

• If the error occurs during backend initialization, the backend does not start. If the `srvStartUpError` option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` option is set to `terminate` (this is the default if the configuration option is not specified), the program ends.
• If the error occurs during an attempt to become the sysplex group owner, the LDAP server ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD6051I No database changes to commit for type backend named name.

Explanation: The indicated backend has no changes to commit in its checkpoint file. See Database commit processing for more information about file-based backend committing.

In the message text:

type

Backend type

name

Backend name

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD6052E Unable to unload data from LDBM backend named name because file cannot be found.

Explanation: The `ds2ldif` utility found a `.new` or `.old` version of the LDBM database file indicated in the message, but not the `.db` version of the file. This indicates that part of the directory in the backend to be unloaded may be missing. The unload cannot proceed. The `.new` and `.old` files are temporary versions of the database file created during checkpoint replay processing, when the database is updated using the contents of the checkpoint file. The temporary files are removed when the final updated `.db` database file is created. For some reason, this process must not have completed the last time it occurred.

In the message text:

name

Backend name

file

Database file name

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the LDAP server has write access to the file directory specified by the `databaseDirectory` option located in the named LDBM backend section of the LDAP server configuration file. Start the LDAP server, which attempts to fix the problems in the database files. Then restart `ds2ldif` using the `-r` option to force `ds2ldif` to use an `unloadRequest` extended operation to unload the requested entries.

Problem determination: Not applicable.

Source: LDAP
GLD6053E

Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD6053E Unable to load directory data for type backend named name because of an inconsistent commit state.

Explanation: The utility found that the checkpoint file was committed while processing the LDBM or CDBM database files. This may result in a partial load of the updates committed in the checkpoint file resulting in an inconsistent state. See Database commit processing for more information about file-based backend committing.

In the message text:

type
  Backend type

name
  Backend name

Example: None.

System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: If the LDAP server is running, issue the COMMIT operator modify command to force a commit of all file-based backends. This merges all updates in the file-based checkpoint files into

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
Chapter 5. GDBM, advanced replication, and ldapdiff messages (8000)

This section lists the messages returned by the GDBM backend, advanced replication, and the ldapdiff utility.

GDBM backend messages

GLD8001E Unable to load the GDBM database because attribute type 'attribute' is not defined.

Explanation: An attribute type used by an entry in the GDBM directory is not defined in the LDAP server schema.

In the message text:

attribute

Undefined attribute type

Example: None.

System action: The GDBM backend does not start. If the srvStartUpError configuration option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError configuration option is set to terminate (this is the default if the configuration option is not specified), the program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: If the GDBM backend is needed, restart the LDAP server without the GDBM backend section in the LDAP server configuration file and add the missing attribute type to the LDAP server schema. Then restore the GDBM backend section in the configuration file and restart the LDAP server.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8002E Unable to load the GDBM database because object class 'objectclass' is not defined.

Explanation: An object class used by an entry in the GDBM directory is not defined in the LDAP server schema.

In the message text:

objectclass

Undefined object class

Example: None.

System action: The GDBM backend does not start. If the srvStartUpError configuration option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError configuration option is set to terminate (this is the default if the configuration option is not specified), the program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: If the GDBM backend is needed, restart the LDAP server without the GDBM backend section in the LDAP server configuration file and add the missing object class to the LDAP server schema. Then restore the GDBM backend section in the configuration file and restart the LDAP server.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8003E GDBM backend specified for a non-GDBM database.

Explanation: The GDBM backend DLL, GLDBGD31 or GLDBGD64, is specified on a database option in the LDAP server configuration file but the type parameter on the option is not GDBM.

Example: None.

System action: The GDBM backend does not start. If
the `srvStartUpError` configuration option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends that successfully start. If the `srvStartUpError` configuration option is set to `terminate` (this is the default if the configuration option is not specified), the program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Correct the `database` option in the LDAP server configuration file so that the DLL and backend type match. Restart the LDAP server if it ended or if the GDBM backend is needed.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

### Advanced replication messages

**GLD8501E** Unable to connect to replica `host_name` on port `port_number`. Verify that the replica is started.

**Explanation:** The LDAP server is unable to establish a connection to the consumer server and port number specified in the message.

In the message text:

- `host_name`: LDAP host name
- `port_number`: LDAP port number

**Example:** None.

**System action:** The LDAP server continues however replication to the consumer server identified by the replication agreement is not started.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Verify that the consumer server is started or contact the operator to start the consumer server. Ensure that the consumer server information in the `ibm-replicaURL` attribute value of the replication agreement entry is correct.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

**GLD8502I** Replication context `context_name` replication type: `repl_type` context state: `repl_state` ibm-serverID: `repl_serverId` ibm-subentryDN: `repl_subentry_name` agreements: `num_agreements` agreements defined referrals: `referral_list`

**Explanation:** The status of the specified replication context entry is displayed in this message.

In the message text:

- `context_name`: Replication context entry distinguished name
- `repl_type`: Replication type
- `repl_state`: Replication state
- `repl_serverId`: Replication server ID
- `repl_subentry_name`: Replica subentry distinguished name
- `num_agreements`: Number of replication agreements under replication context
- `referral_list`: Replication referral list

**Example:** None.

**System action:** The LDAP server continues.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Verify that the replication context entry is configured properly and is working as expected.

**Problem determination:** Not applicable.

**Source:** LDAP
GLD8503W The DN of the credential entry 'credential_name' defined for the replication agreement 'agreement_name' cannot be found.

Explanation: The supplier server credentials entry which contains authentication information used to bind with the consumer server cannot be found. The supplier server credentials entry is specified in the ibm-replicaCredentialsDN attribute value in the replication agreement entry.

In the message text:

credential_name Credentials entry distinguished name
agreement_name Replication agreement entry distinguished name

Example: None.

System action: The LDAP server continues however replication to the consumer server identified by the replication agreement is not started.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the supplier server credentials entry distinguished name specified in the replication agreement entry by the ibm-replicaCredentialsDN attribute value is correct and the entry exists. See Credentials entries for more information about the supplier server credentials entry.

Problem determination: Not applicable.

Source: LDAP

Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8504E The credential entry 'credential_name' is in use and cannot be deleted.

Explanation: The supplier server credentials entry specified in the message cannot be deleted because it is referenced by a replication agreement entry in the ibm-replicaCredentialsDN attribute value.

In the message text:

credential_name Credentials entry distinguished name

Example: None.

System action: The LDAP server continues however the requested delete client operation is not successful.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Ensure that the correct entry is specified in the ibm-replicationCredentialsDN attribute value of the replication agreement entry. Verify that the object class for the supplier server credentials entry is ibm-replicationCredentialsSimple or ibm-replicationCredentialsExternal. See Credentials entries for more information about the supplier server credentials entry.

Problem determination: Not applicable.

Source: LDAP

Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8505E The credential entry 'credential_name' defined for the replication agreement 'agreement_name' is not valid.

Explanation: The object class of the supplier server credentials entry defined in the ibm-replicaCredentialsDN attribute value for the replication agreement entry is not valid. The only supported object class values for supplier server credential entries are ibm-replicationCredentialsSimple and ibm-replicationCredentialsExternal.

In the message text:

credential_name Credentials entry distinguished name
agreement_name Replication agreement entry distinguished name

Example: None.

System action: The LDAP server continues however replication to the consumer server identified by the replication agreement is not started.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the entry being deleted is not already referenced in the ibm-replicaCredentialsDN attribute value of any replication agreement entries. Either delete the
replication agreement entry or modify the ibm-replicaCredentialsDN attribute value so that there are no longer any references to the entry that is being deleted. Then retry the delete client operation.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

### GLD8506I

**Replication agreement**

<table>
<thead>
<tr>
<th>attr</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>agreement_name</td>
<td>Replication agreement entry distinguished name</td>
</tr>
<tr>
<td>context_name</td>
<td>Replication context entry distinguished name</td>
</tr>
<tr>
<td>repl_state</td>
<td>Replication state</td>
</tr>
<tr>
<td>repl_url</td>
<td>Consumer server URL</td>
</tr>
<tr>
<td>credentials_name</td>
<td>Replica credentials distinguished name</td>
</tr>
<tr>
<td>filter_name</td>
<td>Replication filter distinguished name</td>
</tr>
<tr>
<td>schedule_name</td>
<td>Replication schedule distinguished name</td>
</tr>
<tr>
<td>bind_name</td>
<td>Replica bind distinguished name</td>
</tr>
<tr>
<td>bind_type</td>
<td>Bind authentication method</td>
</tr>
<tr>
<td>conn_state</td>
<td>Replica connection state</td>
</tr>
</tbody>
</table>

**Explanation:** The status of the specified replication agreement entry is displayed in this message.

In the message text:

- **agreement_name**: Replication agreement entry distinguished name
- **context_name**: Replication context entry distinguished name
- **repl_state**: Replication state
- **repl_url**: Consumer server URL
- **credentials_name**: Replica credentials distinguished name
- **filter_name**: Replication filter distinguished name
- **schedule_name**: Replication schedule distinguished name
- **bind_name**: Replica bind distinguished name
- **bind_type**: Bind authentication method
- **conn_state**: Replica connection state

---

### GLD8510E

**The consumer URL defined in replication agreement entry 'agreement_name' is a duplicate.**

**Explanation:** In this replication context, the supplier server already has a replication agreement entry that has the same consumer server URL defined in the ibm-replicaURL attribute value. Within a replication context, each replication agreement entry must have a unique ibm-replicaURL attribute value. A supplier server is only allowed one connection to the same consumer server URL.

In the message text:

- **agreement_name**: Replication agreement entry distinguished name

**Example:** None.

**System action:** The LDAP server continues however the requested client add or modify operation is not successful.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** In the replication agreement...
entry that is being added or modified, verify that the consumer server URL in the `ibm-replicaURL` attribute value is correct and does not the same value as any existing replication agreement entry within this replication context. Then retry the requested client add or modify operation.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD8516E** Internal processing error in server; replication thread cannot start.

**Explanation:** An internal error occurred while attempting to initialize the thread for advanced replication. A previously issued message specifies the replication agreement entry that had problems initializing.

**Example:** None.

**System action:** The LDAP server continues however advanced replication does not initialize.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** This is an internal processing error that occurred while initializing the advanced replication thread. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD8517I** Replication starting for replica `agreement_name`.

**Explanation:** Replication to the consumer server identified by the replication agreement entry is initializing.

In the message text:

- `agreement_name`: Replication agreement entry distinguished name

**Example:** None.

**System action:** The LDAP server continues.

---

**GLD8518I** Replication terminating for replica `agreement_name`.

**Explanation:** Replication to the consumer server identified by the replication agreement entry is ending.

In the message text:

- `agreement_name`: Replication agreement entry distinguished name

**Example:** None.

**System action:** If there are additional replication agreements active, the LDAP server continues however replication to the consumer server identified by the replication agreement is ending. If there are no active replication agreements active, the LDAP server ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** None.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD8519E** Unable to create schedule for replica `agreement_name`; all changes will be replicated immediately.

**Explanation:** An internal error occurred while attempting to initialize the replication schedule for the replication agreement entry specified in the message.

In the message text:

- `agreement_name`: Replication agreement entry distinguished name

**Example:** None.
System action: The LDAP server continues however replication updates to the consumer server identified by the replication agreement are immediately replicated.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: This is an internal processing error that occurred while initializing the replication scheduling support for the replication agreement entry. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD8520E Unable to locate schedule entry with DN 'schedule_name'.

Explanation: The replication schedule entry which contains scheduling information for the replication agreement cannot be found. The replication schedule entry is specified in the ibm-replicaScheduleDN attribute value in the replication agreement entry which is specified in a previously issued message.

In the message text:

schedule_name
Replication schedule entry distinguished name

Example: None.

System action: The LDAP server continues however replication updates to the consumer server identified by the replication agreement are immediately replicated.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the ibm-replicaScheduleDN attribute value is correct for the replication agreement entry and that the replication schedule entry exists. Either add the replication schedule entry to the directory or remove the ibm-replicaScheduleDN attribute value from the replication agreement entry. See Schedule entries for information about replication schedule entries.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD8521E Error on schedule entry with DN 'schedule_name' attribute attribute_name value 'attribute_value'. Value ignored.

Explanation: The daily replication schedule entry does not have the correct time format for the attribute type and value specified in the message. The attribute type and value are ignored in the daily replication entry.

In the message text:

schedule_name
Replication schedule entry distinguished name

attribute_name
Attribute type

attribute_value
Attribute value

Example: None.

System action: The LDAP server continues however the specified time in the daily replication schedule entry is ignored.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the time format for the daily replication schedule entry attribute type and value is the following: Thhmmss where time is based on a 24 hour clock. Modify the attribute value in the daily schedule replication entry specified in the message to have the correct time format. See Schedule entries for information about replication schedule entries.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD8522W Replica 'agreement_name' missing schedule DN; all changes will be replicated immediately.

Explanation: The replication agreement entry does not have a replication schedule entry specified in the ibm-replicaScheduleDN attribute so the replication agreement defaults to replicating all updates immediately.

In the message text:
agreement_name

Replication agreement entry distinguished name

Example: None.

System action: The LDAP server continues with replication updates to the consumer server identified by the replication agreement immediately occurring.

Operator response: None.

System programmer response: None.

Administrator response: If the consumer server defined by the replication agreement entry should not immediately receive replication updates, modify the replication agreement entry to add an ibm-replicaScheduleDN attribute value. The ibm-replicaScheduleDN attribute value must be a weekly replication schedule entry with an object class value of ibm-replicationWeeklySchedule. See Schedule entries for information about replication schedule entries.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8523E Error retrieving pending changes for replica 'agreement_name'. Will try again.

Explanation: An internal search error occurred while retrieving the pending replication changes from the backend where the replication agreement entry resides.

In the message text:

agreement_name

Replication agreement entry distinguished name

Example: None.

System action: The LDAP server continues however the pending replication changes cannot be retrieved from the backend where the replication agreement entry resides.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8525E Error while removing status entry for replica 'agreement_name'.

Explanation: An internal error occurred while deleting the replication agreement entry from the backend replication status table where the replication agreement entry resides.

In the message text:

agreement_name

Replication agreement entry distinguished name
GLD8526E  Error while updating status for replica 'agreement_name' to last change ID changeID.

Explanation: An internal error occurred while updating the last change ID in the backend replication status table where the replication agreement entry resides.

In the message text:

- agreement_name
  Replication agreement entry distinguished name
- changeID
  Replication change identifier

Example: None.

System action: The LDAP server continues however the replication agreement status cannot be updated in the backend replication status table.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the backend where the replication agreement entry resides is functioning and handling requests correctly. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8528I  Dropping connection to replica 'agreement_name' on host 'host_name' port port_number.

Explanation: The LDAP server is no longer connected to the consumer server and port number identified by the replication agreement entry in the ibm-replicaURL attribute value.

In the message text:

- agreement_name
  Replication agreement entry distinguished name
- host_name
  LDAP host name
- port_number
  LDAP port number

Example: None.
System action: The LDAP server continues however replication to the consumer server identified by the replication agreement is no longer occurring.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the consumer server for the replication agreement entry is still running and that this server can still successfully connect to it.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8529I Established connection for replica 'agreement_name' on host 'host_name' port port_number.

Explanation: The LDAP server has successfully established a non-secure connection to the replica server and port number identified by the replication agreement entry. The replica server and port number are specified in LDAP URL format in the ibm-replicaURL attribute value of the replication agreement entry.

In the message text:

agreement_name
  Replication agreement entry distinguished name

host_name
  LDAP host name

port_number
  LDAP port number

Example: None.

System action: The LDAP server continues with replication to the consumer server identified by the replication agreement.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8530I Established secure connection for replica 'agreement_name' on host 'host_name' port port_number.

Explanation: The LDAP server has successfully established a secure connection to the replica server and port number identified by the replication agreement entry. The replica server and port number are specified in LDAP URL format in the ibm-replicaURL attribute value of the replication agreement entry.

In the message text:

agreement_name
  Replication agreement entry distinguished name

host_name
  LDAP host name

port_number
  LDAP port number

Example: None.

System action: The LDAP server continues with replication to the consumer server identified by the replication agreement.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8531I Replicating all pending changes for replica 'agreement_name'.

Explanation: The replication schedule entry identified by the ibm-replicaScheduleDN in the replication agreement entry indicates that all pending replication changes are now allowed to be replicated to the consumer server identified by the replication agreement.

In the message text:

agreement_name
  Replication agreement entry distinguished name

Example: None.
System action: The LDAP server continues with scheduled replication to the consumer server identified by the replication agreement.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD8532E Error 'error_text' occurred for replica 'agreement_name': add failed for entry 'name' change ID changeID.

Explanation: During replication from this supplier server to the consumer server defined in the replication agreement, an add operation failed. The error string shows the reason why the operation failed. The change ID is used to record the replication change in the backend where the replication agreement entry resides.

In the message text:

error_text Error message text
agreement_name Replication agreement entry distinguished name
name Entry distinguished name
changeID Replication change identifier

Example: None.

System action: The LDAP server continues however replication to the consumer server identified by the replication agreement may be stalled.

Operator response: None.

User response: None.

System programmer response: None.

System administrator response: See Monitoring and diagnosing advanced replication problems for information about recovering from advanced replication problems.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD8532E  GLD8534E

GLD8534E Error 'error_text' occurred for replica 'agreement_name': modify failed for entry 'name' change ID changeID.

Explanation: During replication from this supplier server to the consumer server defined in the replication agreement, a modify operation failed. The error string shows the reason why the operation failed. The change ID is used to record the replication change in the backend where the replication agreement entry resides.

In the message text:

error_text Error message text
agreement_name Replication agreement entry distinguished name
name Entry distinguished name
changeID Replication change identifier

Example: None.

System action: The LDAP server continues however replication to the consumer server identified by the replication agreement may be stalled.

Operator response: None.

User response: None.

System programmer response: None.

System administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
In the message text:

**error_text**

Error message text

**agreement_name**

Replication agreement entry distinguished name

**name**

Entry distinguished name

**changeID**

Replication change identifier

**Example:** None.

**System action:** The LDAP server continues however replication to the consumer server identified by the replication agreement may be stalled.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** See [Monitoring and diagnosing advanced replication problems](#) for information about recovering from advanced replication problems.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD8535E**

`Error 'error_text' occurred for replica 'agreement_name': delete failed for entry 'name' change ID changeID.`

**Explanation:** During replication from this supplier server to the consumer server defined in the replication agreement, a delete operation failed. The error string shows the reason why the operation failed. The change ID is used to record the replication change in the backend where the replication agreement entry resides.

In the message text:

**error_text**

Error message text

**agreement_name**

Replication agreement entry distinguished name

**name**

Entry distinguished name

**changeID**

Replication change identifier

**Example:** None.

**System action:** The LDAP server continues however replication to the consumer server identified by the replication agreement is not started.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Verify that the supplier server credentials entry specified by the `ibm-replicaCredentialsDN` attribute value in the replication agreement entry has correct values for the `replicaBindDN` and `replicaCredentials`. See [Credentials entries](#) for more information about the supplier server credentials entry.

If the consumer server is an IBM Tivoli Directory Server with advanced replication, the `replicaBindDN`
attribute value must have the same value as the
ibm-slapdMasterDN attribute value in the consumer
server credentials entry used by the replication context.
The replicaCredentials must have the same value as the
ibm-slapdMasterPW attribute value in the consumer server credentials entry used by the
replication context. See Consumer server entries for more information about the consumer server
credentials entry.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8539W Replication agreement 'agreement_name'
has consumer server ID 'consumerID', but
connected to server with ID 'serverID'.

Explanation: The consumer server ID defined in the
replication agreement entry by the
ibm-replicaConsumerID attribute value has a different
value than the ID of the connected consumer server.
In the message text:

agreement_name
    Replication agreement entry distinguished name
cn=consumerID
    Replication consumer server identifier
cn=serverID
    Replication server identifier

Example: None.

System action: The LDAP server continues with
replication to the consumer server identified by the
replication agreement.
Operator response: None.
User response: None.

System programmer response: None.

Administrator response: Verify that the replication
agreement on the supplier server is connected to the
correct consumer server. If the consumer server is an
IBM Tivoli Directory Server with advanced replication,
ensure that the ibm-replicaConsumerID attribute value
in the replication agreement entry has the same value as the
ibm-slapdServerID attribute defined in the
cn=configuration entry on the consumer server.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD8540W  Replication for replica 'agreement_name' will continue to retry the same update after receiving an error.

Explanation: The current replication change has failed to replicate to the consumer server so the supplier server retries the failed replication change every minute until it is successful. This error may cause replication from this replication agreement to be stalled until it is corrected by the LDAP root administrator or an administrative group member with the root or replication administrator roles. The `ibm-replicationState` operational attribute in the replication agreement entry is set to `retrying` to indicate the current replication status.

In the message text:

agreement_name
Replication agreement entry distinguished name

Example: None.

System action: The LDAP server continues, however, replication to the consumer server identified by the replication agreement may be stalled.

Operator response: None.

User response: None.

Administrator response: See Monitoring and diagnosing advanced replication problems for information about recovering from advanced replication problems.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8542W  Replication continuing for replica 'agreement_name' after logging `update_type` for entry 'name' ignoring error:

return_code 'error_text'

'additional_error_text'.

Explanation: This change has failed to replicate to the consumer server for the reason specified so the supplier server continues to the next replication change after receiving this error. This failure may cause replication from this agreement to be stalled unless it is corrected by the LDAP root administrator or an administrative group member with the root or replication administrator roles.

In the message text:

agreement_name
Replication agreement entry distinguished name

update_type
Operation type

name
Entry distinguished name

return_code
LDAP return code
**GLD8543W • GLD8545E**

```plaintext
error_text
   Error text for LDAP return code
additional_error_text
   Additional error text

Example: None.
System action: The LDAP server continues however replication from this replication agreement may be stalled.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Verify that replication between the supplier and consumer servers is successfully occurring by querying the replication agreement entry operational attribute values which provide replication status from the replication agreement. If the ibm-replicationState operational attribute is set to retrying or the number of ibm-replicationFailedChanges attribute values is near the maximum number of replication failures allowed per backend (as specified by the ibm-slapdReplMaxErrors attribute value in the cn=Replication,cn=configuration entry), it may be necessary to compare and re-synchronize the replication context on both servers. See [Monitoring and diagnosing advanced replication problems](#) for information about the replication agreement entry operational attributes.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
```

---

```plaintext
GLD8545E  Unable to connect to replica 'host_name' on port port_number. Verify that the replica is started.

Explanation: The supplier server was unable to connect with the consumer server host and port number identified in the replication agreement entry.
In the message text:

- `host_name`  
  LDAP host name
- `port_number`  
  LDAP port number

Example: None.
System action: The LDAP server continues however replication to the consumer server identified by the replication agreement is not started.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Verify that the entry on the supplier and consumer servers is the same by using the ldapdiff utility.
```

---

```plaintext
GLD8543W  Replication continuing for replica 'agreement_entry' after skipping update_type for entry 'name' because of error: return_code 'error_text' 'additional_error_text'.

Explanation: After successfully skipping (deleting) the failed replication change, replication to the consumer server identified by the replication agreement is now continuing.
In the message text:

- `agreement_name`  
  Replication agreement entry distinguished name
- `update_type`  
  Operation type
- `name`  
  Entry distinguished name
```

---

```plaintext
return_code
   LDAP return code
error_text
   Error text for LDAP return code
additional_error_text
   Additional error text

Example: None.
System action: The LDAP server continues with replication to the consumer server identified by the replication agreement.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Verify that the consumer server for the replication agreement is running and the replication agreement has the correct ibm-replicaURL attribute value specified.
```

---

```plaintext
Verify that the supplier server credentials entry specified by the ibm-replicaCredentialsDN attribute
```
value in the replication agreement entry is using correct bind information. See Credentials entries for more information about the supplier server credentials entry.

If the consumer server is an IBM Tivoli Directory Server with advanced replication configured, ensure that it is properly configured to accept the supplier server bind credentials. Verify that the consumer server credentials entry is using the correct distinguished name for the \texttt{ibm-slapdMasterDN} attribute value. See Consumer server entries for more information about the consumer server credentials entry.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD8547E** The DN of the credential entry '\texttt{credential\_name}' defined for the replication agreement '\texttt{agreement\_name}' cannot be found.

**Explanation:** An internal search error occurred while attempting to retrieve the supplier server credentials entry specified by the \texttt{ibm-replicaCredentialsDN} attribute value in the replication agreement entry. This entry contains the bind information necessary for the supplier server to authenticate with the consumer server.

In the message text:

- **credential\_name** Credentials entry distinguished name
- **agreement\_name** Replication agreement entry distinguished name

**Example:** None.

**System action:** The LDAP server continues however replication to the consumer server identified by the replication agreement is not started.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Verify that the supplier server credentials entry specified by the \texttt{ibm-replicaCredentialsDN} attribute value in the replication agreement is correct and exists in the directory. Either add the supplier server credentials entry specified by the \texttt{ibm-replicaCredentialsDN} attribute value or modify the \texttt{ibm-replicaCredentialsDN} attribute value to specify a valid supplier server credentials entry. See Credentials entries for more information about the supplier server credentials entry. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
GLD8551E  GLD8556E

GLD8551E  Error 'error_text' occurred for replica 'agreement_name'; delete failed for entry 'name' change ID changeID.

Explanation: During replication from this supplier server to the consumer server defined in the replication agreement, a delete operation failed. The error string shows the reason why the operation failed. The change ID is used to record the replication change in the backend where the replication agreement entry resides.
In the message text:
error_text
  Error text
agreement_name
  Replication agreement entry distinguished name
name
  Entry distinguished name
changeID
  Replication change identifier
Example: None.

System action: The LDAP server continues however the search of the replication agreement entry is not successful.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Verify that the backend where the replication agreement entry resides is functioning and handling requests correctly. If the problem persists, contact the service representative.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8556E  The weekly schedule DN object 'schedule_name' specified in the replication agreement cannot be found or is not a weekly schedule entry.

Explanation: The weekly schedule entry which contains replication scheduling information for the replication agreement entry cannot be found or is not a valid weekly schedule entry. A valid weekly schedule entry has an object class value of ibm-replicationWeeklySchedule. The weekly schedule entry is specified in the ibm-replicaScheduleDN attribute value of the replication agreement entry.
In the message text:
schedule_name
  Replication schedule entry distinguished name
Example: None.

System action: The LDAP server continues however replication updates to the consumer server identified by the replication agreement are immediately replicated.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Verify that the object class value of the weekly schedule entry specified in the replication agreement entry is ibm-replicationWeeklySchedule and that the entry exists.
Problem determination: Not applicable.

GLD8553E  Error retrieving pending change count for replica 'agreement_name'.

Explanation: An internal error occurred while attempting to retrieve the number of pending replication changes from the backend where the replication agreement entry resides. The current number of pending replication changes are returned in the ibm-replicationPendingChanges operational attribute in the replication agreement entry.
In the message text:
agreement_name
  Replication agreement entry distinguished name
Example: None.

System action: The LDAP server continues however the search of the replication agreement entry is not successful.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
**GLD8559E** The daily schedule DN object 'schedule_name' specified in the weekly schedule entry cannot be found or is not a daily schedule entry.

**Explanation:** The weekly schedule entry contains a daily replication schedule entry that cannot be found or is not a valid daily schedule entry. The weekly schedule entry uses the `ibm-scheduleSunday`, `ibm-scheduleMonday`, `ibm-scheduleTuesday`, `ibm-scheduleWednesday`, `ibm-scheduleThursday`, `ibm-scheduleFriday`, and `ibm-scheduleSaturday` attribute values to point to daily replication schedule entries.

In the message text:

- **schedule_name**: Replication schedule entry distinguished name

**Example:** None.

**System action:** The LDAP server continues however replication updates to the consumer server identified by the replication agreement are immediately replicated.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Verify that the object class value of the daily schedule entry specified in the weekly schedule entry is `ibm-replicationDailySchedule` and that the entry exists. See Schedule entries for information about replication schedule entries.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD8563E** Cannot move 'name' from one replication context to another.

**Explanation:** An entry is not allowed to be moved into or out of a replication context using the modify DN operation. When a replication context is configured, a modify dn operation is only allowed to occur within the same replication context.

In the message text:

- **name**: Entry distinguished name

**Example:** None.

**System action:** The LDAP server continues however the requested client modify dn operation is not successful.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** If an entry must be moved from one replication context to another, retrieve the entry by performing a search operation and then delete the entry from the replication context. Then re-add the entry to the correct replication context.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
entry with the new distinguished name to the wanted replication context.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8564E The replication configuration could not be read.

Explanation: An internal error occurred while performing a search for the advanced replication configuration entries in the CDBM backend.
Example: None.
System action: The LDAP server continues however advanced replication configuration is not successful.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Verify that the CDBM backend is configured correctly, the server has access to the CDBM backend, and that the specified advanced replication configuration entry exists in the CDBM backend. If the problem persists, contact the service representative.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8565E The replication configuration DN object 'name' cannot be found.

Explanation: An internal error occurred while performing a search for an advanced replication configuration entry in the CDBM backend.
In the message text:
name Entry distinguished name
Example: None.
System action: The LDAP server continues however advanced replication configuration is not successful.
Operator response: None.
User response: None.
System programmer response: None.

GLD8566E Error on configuration entry with DN 'name'; required attribute attribute_name is missing.

Explanation: An advanced replication configuration entry in the CDBM backend is missing a required attribute.
In the message text:
name
attribute_name Attribute type
Example: None.
System action: The LDAP server continues however advanced replication configuration is not successful.
Operator response: None.
User response: None.
System programmer response: None.

GLD8567E Error on configuration entry with DN 'name' attribute attribute_name value 'attribute_value'. Value ignored.

Explanation: An advanced replication configuration entry in the CDBM backend has an attribute value that
is not correct. The attribute value in the configuration entry is ignored.

In the message text:

name
   Entry distinguished name
attribute_name
   Attribute type
attribute_value
   Attribute value

Example: None.

System action: The LDAP server continues however advanced replication configuration is not successful.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the specified replication advanced configuration entry has the correct attribute value data. If the problem persists, contact the service representative.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8569I  Propagation of replication topology entries to host host_name port port_number finished successfully.

Explanation: The Replication topology extended operation has successfully synchronized replication topology entries on the specified consumer server.

In the message text:

host_name
   LDAP host name
port_number
   LDAP port number

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: None.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8570E  Propagation of replication topology entries to host host_name port port_number failed with error code return_code.

Explanation: An error occurred while using the Replication topology extended operation to synchronize the replication topology entries on the specified consumer server.

In the message text:

host_name
   LDAP host name
port_number
   LDAP port number
return_code
   LDAP return code

Example: None.

System action: The LDAP server continues however
the replication topology entries are not successfully synchronized on the specified consumer server.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8571I  Propagation of replication topology entries will continue with the next target server.

Explanation: The Replication topology extended operation is continuing to synchronize replication topology entries on the next targeted consumer server.
Example: None.
System action: The LDAP server continues with the Replication topology extended operation on the next targeted consumer server.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8578W  The extended operation cannot replicate to target server 'host_name' port port_number because the target server does not support replication topology entries.

Explanation: An error occurred while using the Replication topology extended operation against a consumer server that is not configured for synchronizing replication topology entries. The Replication topology extended operation cannot synchronize replication topology entries on the specified consumer server.
In the message text:
host_name  LDAP host name
port_number  LDAP port number
Example: None.
System action: The LDAP server continues however the replication topology entries are not successfully synchronized on the specified consumer server.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Verify that the targeted consumer server supports the Replication topology extended operation. If the targeted consumer server does not support the Replication topology extended operation, exclude that server as a target of the extended operation.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8578W  Propagation of replication topology entries is complete.

Explanation: The Replication topology extended operation has successfully synchronized replication topology entries on all consumer servers defined within the replication context.
Example: None.
System action: The LDAP server continues.
GLD8579E  The extended operation cannot replicate entries to the target server 'host_name' port port_number because the target server does not have the suffix 'name'.

Explanation: An error occurred while using the Replication topology extended operation against a consumer server that does not have the appropriate suffix configured in its server configuration file. Since the consumer server does not have the appropriate suffix configured, the replication topology entries are not allowed to be added.

In the message text:

- host_name: LDAP host name
- port_number: LDAP port number
- name: Entry distinguished name

Example: None.

System action: The LDAP server continues however the replication topology entries are not successfully synchronized on the specified consumer server.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8581I  Replication conflict: re-add DN 'name' to solve a replication conflict on host 'host_name' port port_number.

Explanation: A replication conflict occurred between the supplier and the targeted consumer server with the specified entry. Since the consumer server supports replication conflict resolution within this replication context, the conflicted entry has been resent to the consumer server. The intention is to re-synchronize the entry on the supplier and consumer servers.

In the message text:

- name: Entry distinguished name
- host_name: LDAP host name
- port_number: LDAP port number

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8580I  Replication conflict: a conflict has been detected on host 'host_name' port port_number. A request to re-add the entry of DN 'name' has been received.

Explanation: A replication conflict occurred between the supplier and the targeted consumer server with the specified entry. Since the consumer server supports replication conflict resolution within this replication context, a request has been received by the supplier server from the consumer server to resend the conflicted entry back to the consumer server.

In the message text:

- name: Entry distinguished name
- host_name: LDAP host name
- port_number: LDAP port number

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP
GLD8582I  •  GLD8584E

Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8582I  Replication conflict: re-add of DN 'name' to host 'host_name' port port_number succeeded.

Explanation: The replication conflict that occurred with the specified entry between the supplier and consumer servers has been resolved successfully. The entry is now synchronized between the supplier and consumer servers.

In the message text:

name  Entry distinguished name
host_name  LDAP host name
port_number  LDAP port number

Example: None.

System action: The LDAP server continues however the specified entry is not synchronized between the supplier and consumer servers.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

---

GLD8584E  Replication conflict: re-add of DN 'name' to resolve a conflict will not continue because the entry is too large.

Explanation: A replication conflict occurred between the supplier and the consumer server with the specified entry. Since the consumer server supports replication conflict resolution within this replication context, this supplier server has been requested to resend the conflicted entry to the consumer server however the size of the conflicted entry exceeds the maximum size allowed. The maximum conflicted entry size that a supplier server can resend to the consumer server is specified by the ibm-slapdReplConflictMaxEntrySize attribute value in the cn=Replication,cn=configuration configuration entry.

In the message text:

name  Entry distinguished name

Example: None.

System action: The LDAP server continues however the specified entry is not synchronized between the supplier and consumer servers.

Operator response: None.

User response: None.

System programmer response: None.
Administrator response: Since the entry is not synchronized between the supplier and consumer servers, future replication conflicts may occur with this entry. See Recovering from advanced replication errors for information about synchronizing the supplier and consumer servers.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8586E Attribute 'attribute_name' is missing from entry 'name'.

Explanation: If a replication context is created with an entry that is not a suffix level entry, ACLs must be defined explicitly in that entry. The following ACL attribute values must be added to the replication context entry for non-suffix level entries: aclEntry, aclPropagate, entryOwner, and ownerPropagate.

In the message text:

attribute_name
       Attribute type
name
       Entry distinguished name

Example: None.

System action: The LDAP server continues, however, the requested client add operation is not successful.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the specified attribute is added to the entry and then retry the client add operation.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8588I The Replication Topology extended operation successfully quiesced the context 'context_name' on host 'host_name' port port_number.

Explanation: The Replication Topology extended operation has successfully quiesced the replication context on the specified consumer server.

In the message text:

context_name
       Replication context entry distinguished name
host_name
       LDAP host name
port_number
       LDAP port number

Example: None.

System action: The LDAP server continues however the replication context on the consumer server identified by the replication agreement is not quiesced.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the replication context entry on the specified consumer server is not already quiesced and is a valid entry. Then retry the Replication Topology extended operation. See Monitoring and diagnosing advanced replication problems for information about searching the replication context operational attribute values to obtain the current replication status.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD85887E The Replication Topology extended operation failed to quiesce the context 'context_name' on host 'host_name' port port_number. The operation will not continue with this server.

Explanation: An error occurred while using the Replication Topology extended operation to quiesce a replication context on the specified consumer server. The Replication Topology extended operation continues to the next targeted consumer server.

In the message text:

context_name
       Replication context entry distinguished name
host_name
       LDAP host name
port_number
       LDAP port number

Example: None.
GLD8589E  GLD8591E

System action:  The LDAP server continues.
Operator response:  None.
User response:  None.
System programmer response:  None.
Administrator response:  None.
Problem determination:  Not applicable.
Source:  LDAP
Module:  None.
Routing code:  None.
Descriptor code:  None.
Automation:  Not applicable.

GLD8589E  The Replication Topology extended operation failed to unquiesce the context 'context_name' on host 'host_name' port port_number. The operation will not continue with this server.

Explanation:  An error occurred while using the Replication topology extended operation to unquiesce the replication context on the targeted consumer server.
In the message text:
context_name  Replication context entry distinguished name
host_name  LDAP host name
port_number  LDAP port number
Example:  None.

System action:  The LDAP server continues however the Replication topology extended operation on the consumer server identified by the replication agreement is still quiesced.
Operator response:  None.
User response:  None.
System programmer response:  None.
Administrator response:  None.
Problem determination:  Not applicable.
Source:  LDAP
Module:  None.
Routing code:  None.
Descriptor code:  None.
Automation:  Not applicable.

GLD8590I  The Replication Topology extended operation successfully unquiesced the context 'context_name' on host 'host_name' port port_number.

Explanation:  The Replication topology extended operation has successfully unquiesced the replication context on the specified consumer server.
In the message text:
context_name  Replication context entry distinguished name
host_name  LDAP host name
port_number  LDAP port number
Example:  None.

System action:  The LDAP server continues.
Operator response:  None.
User response:  None.
System programmer response:  None.
Administrator response:  None.
Problem determination:  Not applicable.
Source:  LDAP
Module:  None.
Routing code:  None.
Descriptor code:  None.
Automation:  Not applicable.

GLD8591E  The Replication Topology extended operation failed to add a suffix 'name' to the configuration file of target host 'host_name' port port_number. The operation will not continue with this server.

Explanation:  An error occurred while using the Replication topology extended operation to add replication topology entries on the targeted consumer server.
If the Replication topology extended operation was targeted against a server other than a z/OS IBM Tivoli Directory server or a z/VM LDAP server, the add of an ibm-slappedSuffix attribute value to the cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration entry was not successful.
If the Replication topology extended operation was targeted against a z/OS IBM Tivoli Directory Server, verify that the targeted consumer server has the suffix
in its server configuration file.
In the message text:

name
    Entry distinguished name

host_name
    LDAP host name

port_number
    LDAP port number

Example: None.

System action: The LDAP server continues however the Replication topology extended operation on the consumer server identified by the replication agreement is not successful.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8592I The Replication Topology extended operation successfully added a suffix 'name' to the configuration file of target host 'host_name' port port_number.

Explanation: If the Replication topology extended operation was targeted against a server other than a z/OS IBM Tivoli Directory server or a z/VM LDAP server, manually add the suffix on the consumer server.

If the Replication topology extended operation was targeted against a server other than a z/OS IBM Tivoli Directory server or a z/VM LDAP server, update the server configuration file on the targeted consumer server to add an appropriate suffix option. Then restart the consumer server and retry the Replication topology extended operation.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8593E The Replication Topology extended operation failed to purge the queue that is associated with the replication agreement 'agreement_name' on host 'host_name' port port_number.

Explanation: An error occurred while purging the replication queue for the specified replication agreement entry when using the Replication topology extended operation. The replication queue on the supplier server is purged when the replication agreement entry already exists on the consumer server.

In the message text:

agreement_name
    Replication agreement entry distinguished name

host_name
    LDAP host name

port_number
    LDAP port number

Example: None.

System action: The LDAP server continues however the Replication topology extended operation on the consumer server identified by the replication agreement is not successful.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Correct the problem by purging the replication queue or by deleting the replication agreement entry on the consumer server.

The replication queue for the agreement can be purged
by using the Control replication queue extended operation in the \textit{ldapexop} utility. Then retry the Replication topology extended operation. See Recovering from advanced replication errors for information about recovering from advanced replication problems.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD8594I** There is no replication queue that is associated with the replication agreement 'agreement_name' on host 'host_name' port port_number. Or the Replication Topology extended operation successfully purged the queue.

**Explanation:** The Replication topology extended operation has successfully purged the replication queue associated with the specified replication agreement entry.

In the message text:

- \textit{agreement_name}  
  Replication agreement entry distinguished name
- \textit{host_name}  
  LDAP host name
- \textit{port_number}  
  LDAP port number

**Example:** None.

**System action:** The LDAP server continues.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Verify that the consumer server for the replication agreement is running and the replication agreement has the correct \texttt{ibm-replicaURL} attribute value specified. Then retry the Replication topology extended operation.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD8596I** Topology successfully replicated to \texttt{number} of \texttt{maximum_number} servers.

**Explanation:** The Replication topology extended operation has successfully synchronized the replication topology entries on the number of consumer servers specified.

In the message text:

- \texttt{number}  
  Number of consumer servers successfully replicated
- \texttt{maximum_number}  
  Total number of consumer servers

---

IBM Tivoli Directory Server Messages and Codes for z/OS V1R13.0
Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8598E The Replication Topology extended operation timed out.
Explanation: A timeout error occurred while using the Replication topology extended operation. The time limit specified on the Replication topology extended operation has been exceeded.
Example: None.
System action: The LDAP server continues however the Replication topology extended operation is not successful.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8602I All updates logged as failures for replication agreement DN 'agreement_name' have been removed from the backend replication failure table.
Explanation: The Control replication error log extended operation has successfully removed all replication failures from the backend replication table.
In the message text:
agreement_name
   Replication agreement entry distinguished name
Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8601I The update logged as a failure with failure ID failureID for replication agreement DN 'agreement_name' has been removed from the backend replication failure table.
Explanation: The Control replication error log extended operation has successfully removed the specified replication failure ID from the backend replication table.
In the message text:
failureID
   Replication failure change identifier
agreement_name
   Replication agreement entry distinguished name
Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD8603E  Unable to log failure in the backend replication failure table for replication agreement DN 'agreement_name' for entry with change ID changeID.

Explanation: An internal error occurred while adding the replication failure ID in the backend replication table.

In the message text:

- agreement_name: Replication agreement entry distinguished name
- changeID: Replication change identifier

Example: None.

System action: The LDAP server continues however the replication failure cannot be added to the backend replication table.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8608I  Replication for DN 'agreement_name' will use the single threaded, synchronous method.

Explanation: Replication to the consumer server identified by the replication agreement is using the synchronous, single threaded method. The synchronous method is the only supported replication method on the IBM Tivoli Directory Server for z/OS.

In the message text:

- agreement_name: Replication agreement entry distinguished name

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
GLD8610E  Replication for DN 'agreement_name' terminated because of an unsupported replication method.

Explanation: Replication to the consumer server identified by the replication agreement is using a replication method that is not supported. The synchronous, single threaded method is the only supported replication method on the IBM Tivoli Directory Server for z/OS.

In the message text:

agreement_name
   Replication agreement entry distinguished name
method
   Replication method
Example: None.

System action: The LDAP server continues however replication to the consumer server identified by the replication agreement is not started.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8618E  Replication for replica 'agreement_name' will continue to retry the same failed update with change ID changeID until it is successful.

Explanation: An error occurred while replicating the update with the specified change ID to the consumer server identified by the replication agreement entry. The failed change gets retried every minute until it succeeds or the failed change is removed from the replication queue by the LDAP root administrator or an administrative group member with the root or replication administrator roles. When this failed change occupies the lead position in the pending replication queue, all other replication updates are blocked and replication is stalled.

In the message text:

agreement_name
   Replication agreement entry distinguished name
changeID
   Replication change identifier
Example: None.

System action: The LDAP server continues however replication to the consumer server identified by the replication agreement is stalled.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8620E  Error occurred processing the replica URL for replication agreement 'agreement_name'.

Explanation: An error occurred while parsing the ibm-replicaURL attribute value in the replication agreement entry. The value specified is not a valid LDAP URL or is empty.

In the message text:

agreement_name
   Replication agreement entry distinguished name
Example: None.

System action: The LDAP server continues however replication to the consumer server identified by the replication agreement is not started.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8628I Creating surrogate entry 'name' on partial replica 'host_name' port port_number.

Explanation: The specified entry is being created on the consumer server because this parent entry is missing. If the ibm-replicationCreateMissingEntries optional attribute in the replication agreement is set to true, then missing parent entries on the consumer server are automatically created.

In the message text:

name  Entry distinguished name
host_name  LDAP host name
port_number  LDAP port number

Example: None.
System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP

GLD8630I Creation of a surrogate entry 'name' on partial replica 'host_name' port port_number succeeded.

Explanation: The specified entry has successfully been created because this parent entry was originally missing on the consumer server. If the ibm-replicationCreateMissingEntries optional attribute in the replication agreement is set to true, then missing parent entries on the consumer server are automatically created.

In the message text:

name  Entry distinguished name
host_name  LDAP host name
port_number  LDAP port number

Example: None.
System action: The LDAP server continues.
Operator response: None.

GLD8629E Creation of surrogate entry 'name' on partial replica 'host_name' port port_number failed.

Explanation: An error occurred while attempting to automatically create the specified entry on the consumer server. This parent entry was probably missing because the replication filter excluded it from being replicated to the consumer server. If the ibm-replicationCreateMissingEntries optional attribute in the replication agreement is set to true, then missing parent entries on the consumer server are automatically created.

In the message text:

name  Entry distinguished name
host_name  LDAP host name
port_number  LDAP port number

Example: None.
System action: The LDAP server continues.
Operator response: None.
GLD8632E  GLD8634I

GLD8632E  The replication filter entry 'filter_name' defined for the replication agreement 'agreement_name' cannot be found.

Explanation: An internal search error occurred while querying the replication filter entry specified in the ibm-replicationFilterDN attribute value of the replication agreement entry. The replication filter entry specified in the replication agreement cannot be found or the entry specified does not have an object class value of ibm-replicationFilter.

In the message text:

filter_name
  Replication filter entry distinguished name
agreement_name
  Replication agreement entry distinguished name

Example: None.

System action: The LDAP server continues however replication to the consumer server identified by the replication agreement is not started.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8633W  The operational attribute attribute_name specified as part of the replication filter inclusion/exclusion list is not allowed.

Explanation: An error occurred while attempting to add or modify a replication filter that had an operational attribute specified. Operational attributes cannot be specified as part of the filter inclusion or exclusion list. Replication filters are specified in the ibm-replicationFilterAttr attribute value in the replication filter entry.

In the message text:

attribute_name
  Attribute type

Example: None.

System action: The LDAP server continues however the add or modify operation of the replication filter entry is not successful.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Update the add or modify of the ibm-replicationFilterAttr attribute value in the replication filter entry to only specify non-operational attributes as part of the inclusion or exclusion list in a replication filter. See Partial replication for information about replication filter entries.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8634I  Modifications to only the ACL attributes of an entry will not be filtered.

Explanation: Partial replication is configured for the replication agreement however replication filtering has been bypassed since only the ACL attribute values of an entry have been modified. Updates to ACL attribute values are always replicated to a consumer server.

Example: None.

System action: The LDAP server continues.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.

Problem determination: Not applicable.

Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
The replication agreement entry does not support filtered replication. However, the replication agreement has a replication filter entry specified in the `ibm-replicationFilterDN` attribute value. Although the consumer server does not support partial replication, filtered entries are still replicated to the consumer server.

In the message text:

- `host_name`: LDAP host name
- `port_number`: LDAP port number

Example: None.

System action: The LDAP server continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.

---

The filter entry `filter_name` is in use and cannot be deleted.

Explanation: The replication filter entry cannot be deleted because a replication agreement entry has a reference to this entry in an `ibm-replicationFilterDN` attribute value.

In the message text:

- `filter_name`: Replication filter entry distinguished name

Example: None.

System action: The LDAP server continues however the requested delete client operation is not successful.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Perform a search on all replication agreement entries in the directory to find the entry that has an `ibm-replicationFilterDN` attribute value with the distinguished name (DN) of the entry being deleted. Modify the `ibm-replicationFilterDN` attribute value in the replication agreement entry to remove the reference to the entry that is being deleted. Then retry the delete client operation.

Problem determination: Not applicable.

---

Restricted Access to the replication topology is set to `value`.

Explanation: The `ibm-slapdReplRestrictedAccess` attribute value in the `cn=Replication,cn=configuration` entry has been set to the value specified in this message. If set to true, only the LDAP root administrator or an administrative group member with the root or replication administrator roles and the master server DN have access to replication topology entries. If set to false, other users with the proper ACL authority can access the replication topology entries.

In the message text:

- `value`: True or false

Example: None.
Replication error logging for replication agreement DN 'agreement_name' is unlimited.

Explanation: The number of replication failures stored for the specified replication agreement is unlimited. When the ibm-slapdReplMaxErrors attribute value in the cn=Replication,cn=configuration entry is set to -1, there is no limit on the number of replication failures stored in the backend where the replication agreement entry resides.

In the message text:

agreement_name
- Replication agreement entry distinguished name

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the missing parent entry exists on this supplier server by performing a search operation. If the entry does not exist, add the entry to the supplier server. The supplier and consumer servers may need to be synchronized. See [Recovering from advanced replication errors] for information about synchronizing the supplier and consumer servers.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

The attribute attribute_name specified in the replication filter is not found in the schema.

Explanation: The specified attribute type in the replication filter was not found in the schema. A replication filter was specified in the ibm-replSymbolicAttr attribute value in the replication filter entry. Another message identifies the replication filter entry and value that is in error.

In the message text:

attribute_name
- Attribute type

Example: None.

System action: The LDAP server continues however the requested replication filter update client operation is not successful. If the replication filter is an existing replication filter entry, the filter is ignored.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the attribute type specified in the replication filter exists in the schema. Modify the replication filter to use an attribute type that exists in the schema or update the schema to add the missing attribute type.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

Internal search for the parent entry 'name' failed.

Explanation: An internal server error occurred while searching for the specified parent entry in this server. This entry is a missing parent entry on the consumer server and is needed for replication to the consumer server to continue.

In the message text:

name
- Entry distinguished name

Example: None.

System action: The LDAP server continues however the missing parent entry is not added to the consumer server.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
GLD8644E The objectclass value specified in the replication filter is not found in the schema.

Explanation: The specified object class value in the replication filter was not found in the schema. A replication filter was specified in the ibm-replicationFilterAttr attribute value in the replication filter entry. Another message identifies the replication filter entry and value that is in error.

In the message text:

value

Objectclass value

Example: None.

System action: The LDAP server continues however the requested replication filter update client operation is not successful. If the replication filter is an existing replication filter entry, the filter is ignored.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the object class value specified in the replication filter exists in the schema. Modify the replication filter to use an object class value that exists in the schema or update the schema to add the missing object class value.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8647E Kerberos authentication is specified for the replication agreement 'agreement_name'. Kerberos authentication is not supported on this platform.

Explanation: The object class of the supplier server credentials entry defined in the ibm-replicaCredentialsDN attribute value for the replication agreement entry is not valid. The only supported object class values for supplier server credential entries are ibm-replicationCredentialsSimple and ibm-replicationCredentialsExternal. The IBM Tivoli Directory Server for z/OS does not support a supplier server credentials entry that has an object class value of ibm-replicationCredentialsKerberos.

In the message text:

agreement_name

Replication agreement entry distinguished name

Example: None.

System action: The LDAP server continues however replication to the consumer server identified by the replication agreement is not started.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the ibm-replicaCredentialsDN attribute value for the replication agreement entry does not reference a supplier server credentials entry with an ibm-replicationCredentialsKerberos object class value. Modify the ibm-replicaCredentialsDN attribute value in the replication agreement entry to reference a supplier server credentials entry with an object class value of ibm-replicationCredentialsSimple or ibm-replicationCredentialsExternal.

Problem determination: Not applicable.

Source: LDAP

Module: None.
GLD8648E Unable to open lost and found log file 'filename'.

Explanation: The lost and found log file specified by the ibm-slapdLog attribute value in the cn=Replication,cn=Log Management,cn=Configuration entry cannot be opened. The lost and found log file is created by the consumer server any time a replication conflict occurs. Any entries that are deleted on the consumer server because of a replication conflict are stored in LDIF format in this file.

In the message text:

filename
    Replication lost and found log file

Example: None.

System action: The LDAP server continues however replication conflicts are not written to the lost and found log file.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the LDAP server has the appropriate access to the directories and to the file itself. Modify the ibm-slapdLog attribute value in the cn=Replication,cn=Log Management,cn=Configuration entry to specify a fully-qualified z/OS UNIX System Services file name and directory location where the LDAP server can create the lost and found log file.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8649E Replication agreement 'agreement_name' is now suspended because 'filter_name' is not a valid filter entry.

Explanation: The replication agreement is now suspended because the replication filter entry specified in the ibm-replicationFilterDN attribute value does not exist or there are no valid ibm-replicationFilterAttr attribute values specified in the entry. The ibm-replicationOnHold attribute value has been automatically set to true in the replication agreement until the problems can be corrected.

In the message text:

agreement_name
    Replication agreement entry distinguished name

filter_name
    Replication filter entry distinguished name

Example: None.

System action: The LDAP server continues however replication to the consumer server identified by the replication agreement is suspended. Replication updates are queued until replication is resumed for this replication agreement.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the ibm-replicationFilterDN attribute value in the replication agreement specifies an entry that exists in the directory. If a valid replication filter entry is specified, verify each of the ibm-replicationFilterAttr attribute values in the replication filter entry are in an acceptable format. See [Partial replication] in for information about replication filter entries.

When the problems have been corrected, use the Control replication extended operation on the ldapexop utility to resume replication. If the extended operation is successful, the ibm-replicationOnHold attribute in the replication agreement entry is changed from true to false.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8650I Replication agreement 'agreement_name' is active.

Explanation: Replication to the consumer server identified by the replication agreement is active because the ibm-replicationOnHold attribute is set to false or is not present.

In the message text:

agreement_name
    Replication agreement entry distinguished name

Example: None.

System action: The LDAP server continues.

Operator response: None.

User response: None.
GLD8651I  Replication agreement 'agreement_name' is suspended.

Explanation: Replication to the consumer server identified by the replication agreement is suspended because the ibm-replicationOnHold attribute is set to true.

In the message text:

agreement_name

   Replication agreement entry distinguished name

Example: None.

System action: The LDAP server continues however replication to the consumer server identified by the replication agreement is suspended. Replication updates are queued until replication is resumed for this replication agreement.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8653W Duplicate ibm-replicaServerId value 'replicaServerId' defined in subentry 'name' for replication context 'context_name'.

Explanation: The ibm-replicaServerID value defined in a replica subentry is already in use by another replica subentry defined under the replication context indicated in the message. All replica subentries in the same replication context should have unique ibm-replicaServerID values defined. Specifications for the ibm-replicationServerIsMaster and ibm-replicaGateway attribute values are derived from the last replica subentry processed that matches this server's ibm-slapdServerID. The replication configuration may change when the server is restarted based on the internal processing order of the replica subentries.

In the message text:

replicaServerId

   Value of duplicate serverID

name

   Entry distinguished name containing duplicate serverID

context_name

   Replication context distinguished name related to the subentry

Example: None.
**GLD8654I**  Advanced replication initialization failed.

**Explanation:** An internal error occurred while attempting to initialize advanced replication support.

**Example:** None.

**System action:** If the srvStartUpError option in the LDAP server configuration file is set to `ignore`, the LDAP server continues to run with those backends that successfully start however advanced replication does not start. If the srvStartUpError option is set to `terminate` (this is the default if the configuration option is not specified), the LDAP server ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Verify that a unique `ibm-replicaServerID` attribute value has been assigned to each replica subentry under the replication context indicated in the message.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD8797E**  Internal processing error in the server; return code `return_code` from pthread library.

**Explanation:** An error occurred in one of the following Language Environment pthread library functions:
- `pthread_mutex_lock()`
- `pthread_mutex_unlock()`
- `pthread_cond_timedwait()`
- `pthread_setspecific()`
- `pthread_cond_broadcast()`

The name of the pthread routine is in an LDAP ERROR trace. See the description of the Language Environment pthread routines in [z/OS XL C/C++ Run-Time Library Reference](#) for more information about the error.

In the message text:

```
return_code
```

Return code from pthread library

**Example:** None.

**System action:** The LDAP server continues.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Restart the LDAP server with ERROR debug level set. The LDAP trace debug output may assist in locating and correcting the problem. Then retry the request. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**Idapdiff utility messages**

**GLD8801I**  This tool synchronizes a replica server with its master.

**Explanation:** The `ldapdiff` utility help and usage menu.

**Example:** None.

**System action:** The program ends.

---

Chapter 5. GDBM, advanced replication, and ldapdiff messages (8000)  211
GLD8802I  Only operational attributes differ for this entry.

Explanation: The ldapdiff utility has detected a difference in the operational attributes for the entry. The ldapdiff utility is using the ibm-entryCheckSumOp attribute, which contains a checksum value of the operational attribute values, to quickly detect entry differences.

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8803I  Schema compare is complete.

Explanation: The ldapdiff utility has completed schema comparison on both LDAP servers.

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8804I  Schema compare is in progress...
This might take a few minutes...

Explanation: The ldapdiff utility is performing schema comparison on both LDAP servers.

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8805I  Successfully connected to both servers.

Explanation: The ldapdiff utility has successfully connected to both LDAP servers that are to be compared.

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8806E  Error occurred while connecting to server: exception_text.

Explanation: The ldapdiff utility encountered an error while attempting to connect to the LDAP server. The exception occurred while attempting to connect to the LDAP server that is indicated in the exception.

In the message text:

exception_text

Exception text
GLD8807E  Incorrect SSL options specified for server "server_host:server_port".

Explanation: The ldapdiff utility detected missing or incorrect SSL command line parameters while attempting to initialize the SSL connection to the LDAP server and port number indicated in the message. Either the parameter is not known, the value specified for the parameter is not supported, or a parameter is missing.

In the message text:

server_host
  Server hostname

server_port
  Server port number

Example: None.

System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Correct the command line of the ldapdiff utility to ensure that the correct SSL parameters are specified. See the ldapdiff utility for the correct ldapdiff utility syntax for the SSL options. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8809I  Successfully finished traversing the tree on both the servers.

Explanation: The ldapdiff utility has successfully retrieved and compared entries on both LDAP servers that reside under the baseDn specified on the -b command line parameter.

Example: None.

System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD8810I Either normal or operational attributes or both differ for this entry.

Explanation: The ldapdiff utility has detected a difference in the non-operational or operational attributes for the entry. The ldapdiff utility is using the ibm-entryCheckSum and ibm-entryCheckSumOp attribute values, to quickly detect entry differences. The ibm-entryCheckSum attribute value is a checksum value of non-operational attribute values while the ibm-entryCheckSumOp attribute value is a checksum value of the operational attribute values.

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8811E Unable to start subtree comparison.

Explanation: The ldapdiff utility is unable to start subtree comparison on both LDAP servers for one of the following reasons:

- The baseDn specified on the -b command line parameter does not have valid DN syntax.
- The baseDn specified on the -b command line parameter cannot be found on both the supplier and consumer servers.
- The encryption settings of the supplier and consumer servers cannot be retrieved.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: None.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8812I Exceeded the specified number of non-matching entries.

Explanation: The ldapdiff utility has encountered the maximum number of non-matching entries between the LDAP servers being compared. The number of non-matching entries exceeds the number specified on the -C command line parameter.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the maximum number of entry mismatches allowed by ldapdiff utility is correct. Consider increasing the number of entry mismatches allowed or removing the -C command line parameter. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8813E Exception: exception_text

Explanation: The ldapdiff utility encountered an exception while performing the requested task. This message is typically accompanied by another message indicating the operation that resulted in this exception.

In the message text:

exception_text

Exception text

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the information in this message and other messages issued to correct the problem. If additional information is required to solve the problem, specify -d ALL on the command line.
Then restart the program. If the problem persists,
contact the service representative.

**Problem determination:** Not applicable.
**Source:** LDAP
**Module:** None.
**Routing code:** None.
**Descriptor code:** None.
**Automation:** Not applicable.

---

**GLD8814I**  
No attributes returned for *name* entry.

**Explanation:** The `ldapdiff` utility is unable to retrieve attribute values indicating encryption settings or password policy for the entry indicated in the message.

In the message text:

*name*  
Entry distinguished name

**Example:** None.

**System action:** The program continues without taking into account the encryption settings or password policy established on the LDAP server.

**Operator response:** None.
**User response:** None.
**System programmer response:** None.
**Administrator response:** None.

**Problem determination:** Not applicable.
**Source:** LDAP
**Module:** None.
**Routing code:** None.
**Descriptor code:** None.
**Automation:** Not applicable.

---

**GLD8816W**  
Password policy is not enabled on one of the servers. Password policy attributes on entries will be ignored during comparisons.

**Explanation:** The `ldapdiff` utility has determined one of the servers does not have password policy enabled. Any password policy attributes that exist on entries are ignored during comparisons.

**Example:** None.

**System action:** The program continues but any password policy attributes that exist on entries are ignored during comparisons.

**Operator response:** None.
**User response:** None.
**System programmer response:** None.
**Administrator response:** If password policy attributes must be compared on both servers, verify that the `cn=pwdpolicy,cn=ibmpolicies` entries on the supplier and consumer servers have the `ibm-pwdPolicy` attribute set to `true`. Then restart the program.

**Problem determination:** Not applicable.
**Source:** LDAP
**Module:** None.
**Routing code:** None.
**Descriptor code:** None.
**Automation:** Not applicable.

---

**GLD8817E**  
Failed to determine the server version for one of the servers.

**Explanation:** The `ldapdiff` utility is unable to determine the LDAP server version because the `ibmdirctoryversion` attribute value does not exist in the rootDSE entry. The `ldapdiff` utility only properly works with the IBM Tivoli Directory Servers on z/OS and other platforms.

**Example:** None.

**System action:** The program continues but the results are unexpected.

**Operator response:** None.
**User response:** None.
**System programmer response:** None.

**Problem determination:** Not applicable.
**Source:** LDAP
**Module:** None.
**Routing code:** None.
**Descriptor code:** None.
**Automation:** Not applicable.

---

**GLD8817E**  
Cannot open the specified file for LDIF output generation.
LDIF file will not be created.

**Explanation:** The `ldapdiff` utility encountered an error while attempting to open the output LDIF file specified on the `-L` command line parameter for writing.

**Example:** None.

**System action:** The program continues with the differences between the LDAP servers being written to standard output.
GLD8818E  GLD8820W

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Verify the directory containing the output LDIF file exists and the user has the appropriate permissions to write the file to that directory. Correct the output LDIF file name specified on the -L command line parameter. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8818E  Exception occurred while closing the LDIF file: exception_text

Explanation: The ldapdiff utility encountered an exception when closing the output LDIF file specified on the -L command line parameter. The exception might have occurred for one of the following reasons:
- The output LDIF file is already closed.
- The output LDIF file does not exist at the specified location.
- The internal file reference is not valid.
- The user running the ldapdiff utility does not have the appropriate permissions to access the output LDIF file.

In the message text:

exception_text  Exception text

Example: None.
System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Correct the command line of the ldapdiff utility to specify a valid value for the command line parameter indicated in the message. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8820W  The supplier and consumer servers have different encryption seed or salt values. The operation will take longer.

Explanation: The ldapdiff utility has detected that the supplier and consumer servers have different encryption seed or salt values. This message is generally only issued when the ldapdiff utility is targeting a supplier or consumer server that is running against an non-z/OS IBM Tivoli Directory Server. The comparison operation is faster if the supplier and consumer servers have the same encryption seed and salt values.

Example: None.
System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
GLD8821E  Missing required argument; refer to the usage description for valid syntax.

Explanation: The *ldapdiff* utility has detected one of the following required parameters are missing from the command line:

- `-ch host`
- `-sh host`
- `-b baseDn` or `-S`

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify the *ldapdiff* command line has the required parameters specified. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD8822E  Exception occurred while adding DN to LDIF file: *exception_text*

Explanation: The *ldapdiff* utility encountered an exception while writing the entry to the output LDIF file. The exception that occurred while writing to the output LDIF file is indicated in the message.

In the message text:

`exception_text`

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the exception text indicated in the message to correct the problem. Verify the output LDIF file exists and the user has the appropriate permissions to write to the file. If additional information is required to solve the problem, specify `-d ALL` on the command line. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

---

GLD8824E  Exception occurred while modifying DN in LDIF file: *exception_text*

Explanation: The *ldapdiff* utility encountered an exception while writing the entry to the output LDIF file. The exception that occurred while writing to the output LDIF file is indicated in the message.

In the message text:

`exception_text`

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Use the exception text indicated in the message to correct the problem. Verify the output LDIF file exists and the user has the appropriate permissions to write to the file. If additional information is required to solve the problem, specify `-d ALL` on the command line. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.
GLD8825E  •  GLD8827E

Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the exception text indicated in the message to correct the problem. Verify the output LDIF file exists and the user has the appropriate permissions to write to the file. If additional information is required to solve the problem, specify -d ALL on the command line. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

---

GLD8825E  Unable to search RootDSE: DirContext is Null.
Explanation: The ldapdiff utility encountered an internal problem while performing a rootDSE search.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the exception text indicated in the message to correct the problem. Verify the output LDIF file exists and the user has the appropriate permissions to write to the file. If additional information is required to solve the problem, specify -d ALL on the command line. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

---

GLD8826E  No RootDSE attributes were returned.
Explanation: The ldapdiff utility encountered an error while performing a rootDSE search. The rootDSE entry returned from the targeted LDAP server did not have any attribute types or values.
Example: None.
System action: The program continues by using a default distinguished name (DN) of cn=schema for schema comparison on the targeted LDAP servers.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Ensure that the targeted LDAP servers are running when using the ldapdiff utility. Verify that TCP/IP communication is working properly between the utility and each targeted LDAP server. If additional information is required to solve the problem, specify -d ALL on the command line. Then restart the program. If the problem persists, contact the service representative.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

---

GLD8827E  Error occurred during enumeration of attributes from the rootDSE entry.
Explanation: The ldapdiff utility encountered an internal error while retrieving the rootDSE entry attribute values returned on a search.
Example: None.
System action: The program continues by using a default distinguished name (DN) of cn=schema for schema comparison on the targeted LDAP servers.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Ensure that the targeted LDAP servers are running when using the ldapdiff utility. Verify that TCP/IP communication is working properly between the utility and each targeted LDAP server. If additional information is required to solve the problem, specify -d ALL on the command line. Then restart the program. If the problem persists, contact the service representative.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.
### GLD8828E Error occurred while reading rootDSE attributes: exception_text

**Explanation:** The `ldapdiff` utility encountered an internal error while reading and parsing the rootDSE entry attribute values.

In the message text:

**exception_text**

Exception text

**Example:** None.

**System action:** The program continues by using a default distinguished name (DN) of `cn=schema` for schema comparison on the targeted LDAP servers.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the exception text indicated in the message to correct the problem. Ensure that the targeted LDAP servers are running when using the `ldapdiff` utility. Verify that TCP/IP communication is working properly between the utility and each targeted LDAP server. If additional information is required to solve the problem, specify `-d ALL` on the command line. Then restart the program. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

### GLD8830E No subschemasubentry found in rootDSE.

**Explanation:** The `ldapdiff` utility is unable to find the `subschemasubentry` attribute on the search of the rootDSE entry. The `subschemasubentry` attribute specifies the distinguished name of the schema entry. Generally, this error can only occur when targeting the `ldapdiff` utility against a non-z/OS IBM Tivoli Directory Server.

**Example:** None.

**System action:** The program continues schema comparison by using the default distinguished name (DN) of `cn=schema` on the targeted LDAP server.

**Operator response:** None.

**User response:** None.

**System programmer response:** Define a `subschemasubentry` attribute value on the non-z/OS IBM Tivoli Directory Server. If additional information is required to solve the problem, specify `-d ALL` on the command line. Then restart the program. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

### GLD8829W Number of grace logins remaining is number for entry "name" on server "server_url".

**Explanation:** The authenticating user is only allowed the specified number of grace logins before the password expires. When the user’s password expires, the authenticating user is no longer able to access the server.

In the message text:

**number**

Number of grace logins

**Example:** None.

**System action:** The program continues.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** The password for the authenticating user should be changed before the number of allowed grace logins is exceeded. When the number of grace logins is exceeded, the authenticating user is no longer able to authenticate to the targeted LDAP server. The password can be modified using the `ldapmodify` or `ldapchangepwd` utilities. See [IBM Tivoli Directory Server Client Programming for z/OS](https://www.ibm.com/support/docview.wss?uid=swg27018540) for more information about these utilities.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
GLD8831E  GLD8833E

Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8831E  An exception occurred during search: exception_text.

Explanation: The ldapdiff utility encountered an internal error while performing a search operation on the LDAP server. The exception is indicated in the message.

In the message text:

exception_text
Exception text

Example: None.

System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the exception text indicated in the message to correct the problem. Verify that the targeted LDAP servers are running when using the ldapdiff utility. Verify that TCP/IP communication is working properly between the utility and each targeted LDAP server. If additional information is required to solve the problem, specify -d ALL on the command line. Then restart the program. If the problem persists, contact the service representative.

Problem determination: Not applicable.
Source: LDAP

GLD8833E  Error occurred while processing search results for server: exception_text.

Explanation: The ldapdiff utility encountered an error while parsing through LDAP search results. The exception is indicated in the message.

In the message text:

exception_text
Exception text

Example: None.

System action: The program continues but the environment settings are not set.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the exception text indicated in the message to correct the problem. Verify that the user has enough permissions to set the environment settings or the system property settings. If additional information is required to solve the problem, specify -d ALL on the command line. Then restart the program. If the problem persists, contact the service representative.

Problem determination: Not applicable.
Source: LDAP
GLD8834W  Password expires in number_seconds seconds (number_days days and number_hours: number_minutes: number_seconds) for entry "name" on server "server_url".

Explanation: The authenticating user is only allowed the specified amount of time before the password expires. When the user's password expires, the authenticating user is no longer able to access the server.

In the message text:

- **number_seconds**: Password expiration in seconds
- **number_days**: Password expiration in days
- **number_hours**: Password expiration in hours
- **number_minutes**: Password expiration in minutes
- **number_seconds**: Password expiration in seconds
- **name**: Entry distinguished name
- **server_url**: LDAP server url

Example: None.

System action: The program continues.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: The password for the authenticating user should be changed before the password expiration time is exceeded. When the password has expired, the authenticating user is no longer able to access the server. The password can be modified using the `ldapmodify` or `ldapchangepwd` utilities. See [IBM Tivoli Directory Server Client Programming for z/OS](https://www.ibm.com/support/docview.wss?uid=swg27026735) for more information about these utilities. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8836E  Account is locked for entry "name" on server "server_url".

Explanation: The authenticating user's account has been locked and is prevented from accessing the specified server.

In the message text:

- **name**: Entry distinguished name
- **server_url**: LDAP server url

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: The authenticating user's account must be unlocked by an LDAP root or
password administrator. If the authenticating user is the LDAP root administrator (adminDN) and the server being accessed is the z/OS LDAP server, use the UNLOCK ADMIN operator modify command to unlock the account. When the account is unlocked, the authenticating user must access to the server. Then restart the program.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8837I  The specified base DN is not found on the consumer server.

Explanation: The ldapdiff utility was unable to find the baseDn on the consumer server. The baseDn was specified on the -b command line parameter of the ldapdiff utility.
Example: None.

System action: The program continues without traversing the subtree on the consumer server. If the -F command line parameter is specified, any entries that exist on the supplier server in that subtree are deleted.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8839W  The supplier and consumer servers have different encryption settings. The operation may take longer.

Explanation: The ldapdiff utility performed a search of the cn=configuration subtree to obtain the ibm-slapdPwEncryption attribute value. This search is only performed when the ldapdiff utility is used with a non-z/OS IBM Tivoli Directory Server. The ldapdiff utility determined the supplier and consumer servers have different encryption settings so the comparison operation may take a longer period of time. The operation is faster if the supplier and consumer servers have the same encryption settings.
Example: None.

System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8838I  The specified base DN is not found on the supplier server.

Explanation: The ldapdiff utility was unable to find the baseDn on the supplier server. The baseDn was specified on the -b command line parameter of the ldapdiff utility.
Example: None.

System action: The program continues without traversing the subtree on the supplier server. If the -F command line parameter is specified, any entries that exist on the consumer server in that subtree are deleted.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8840E  Error while retrieving attributes of DN: exception_text.

Explanation: The ldapdiff utility encountered an internal error while adding the attributes to an internal hash table. The exception that occurred is indicated in the message.
In the message text:
GLD8841E • GLD8843E

GLD8841E Exception occurred while parsing "name" DN: exception_text.

Explanation: The ldapdiff utility encountered an exception while parsing the string representation of a distinguished name (DN). The exception that occurred is indicated in the message.

In the message text:

name  String representation of a DN
exception_text  Exception text

Example: None.
System action: If the distinguished name that is being parsed is the baseDn specified on the -b command line parameter, the program ends. If other distinguished names are being parsed, the program continues.
Operator response: None.
User response: None.
System programmer response: None.
Automation: Not applicable.

GLD8843E Traverse exception occurred: exception_text

Explanation: The ldapdiff utility encountered an error while traversing the LDAP servers. The exception is indicated in the message. The error might have occurred for one of the following reasons:

• There is a problem performing a search operation on the LDAP server. Verify that the search request controls are valid.
• There is a problem traversing the search entry results from the LDAP server.
• There is a generic error traversing the LDAP server entries.

In the message text:
GLD8844E • GLD8846E  

---

**GLD8844E**  
Password must be changed for "name" on server "server_url".

**Explanation:**  
The password for the authenticating user or the entry being modified must be changed. The effective password policy on the server indicates that the entry’s password value must be changed.

In the message text:

- **name**  
  Entry distinguished name

- **server_url**  
  LDAP server url

**Example:**  
None.

**System action:**  
If authentication is being done, the program continues, however, the comparison and fix operations might fail. If an entry is being modified on the consumer server, the program ends.

**Operator response:**  
None.

**User response:**  
None.

**System programmer response:**  
None.

---

**GLD8846E**  
Entry format for "option" is not valid.

**Explanation:**  
The ldapdiff utility encountered an error while parsing the -C countNumber, -sp port, or -cp port command line parameters. The number specified is less than zero or not a proper numeric number.

In the message text:

- **option**  
  Option name

**Example:**  
None.

**System action:**  
The program ends.

**Operator response:**  
None.

**User response:**  
None.

**System programmer response:**  
None.

---

**GLD8846E**  
Missing JSSE package for SSL connection.

**Explanation:**  
The installed version of Java is missing the Java secure socket extension (JSSE) package or the JSEE settings are not correct.

**Example:**  
None.

**System action:**  
The program continues but connecting with the proper JSSE settings is not successful.

**Operator response:**  
None.

**User response:**  
None.

**System programmer response:**  
None.

---

**Exception text**

---

**Example:**  
None.

**System action:**  
The program continues.

**Operator response:**  
None.

**User response:**  
None.

**System programmer response:**  
None.

**Administrator response:**  
Verify that the targeted LDAP servers are still running. Use the information in this message and other messages to correct the problem. If additional information is required to solve the problem, specify -d ALL on the command line. Then restart the program.

**Problem determination:**  
Not applicable.

**Source:**  
LDAP

**Module:**  
None.

**Routing code:**  
None.

**Descriptor code:**  
None.

**Automation:**  
Not applicable.

---

**GLD8844E**  
Password must be changed for "name" on server "server_url".

**Explanation:**  
The password for the authenticating user or the entry being modified must be changed. The effective password policy on the server indicates that the entry’s password value must be changed.

In the message text:

- **name**  
  Entry distinguished name

- **server_url**  
  LDAP server url

**Example:**  
None.

**System action:**  
The program continues.

**Operator response:**  
None.

**User response:**  
None.

**System programmer response:**  
None.

---

**GLD8845E**  
Entry format for "option" is not valid.

**Explanation:**  
The ldapdiff utility encountered an error while parsing the -C countNumber, -sp port, or -cp port command line parameters. The number specified is less than zero or not a proper numeric number.

In the message text:

- **option**  
  Option name

**Example:**  
None.

**System action:**  
The program ends.

**Operator response:**  
None.

**User response:**  
None.

**System programmer response:**  
None.

---

**GLD8846E**  
Missing JSSE package for SSL connection.

**Explanation:**  
The installed version of Java is missing the Java secure socket extension (JSSE) package or the JSEE settings are not correct.

**Example:**  
None.

**System action:**  
The program continues but connecting with the proper JSSE settings is not successful.

**Operator response:**  
None.

**User response:**  
None.

**System programmer response:**  
None.

---

**Administrator response:**  
Verify that the targeted LDAP servers are still running. Use the information in this message and other messages to correct the problem. If additional information is required to solve the problem, specify -d ALL on the command line. Then restart the program.

**Problem determination:**  
Not applicable.

**Source:**  
LDAP

**Module:**  
None.

**Routing code:**  
None.

**Descriptor code:**  
None.

**Automation:**  
Not applicable.

---

**GLD8844E**  
Password must be changed for "name" on server "server_url".

**Explanation:**  
The password for the authenticating user or the entry being modified must be changed. The effective password policy on the server indicates that the entry’s password value must be changed.

In the message text:

- **name**  
  Entry distinguished name

- **server_url**  
  LDAP server url

**Example:**  
None.

**System action:**  
The program continues.

**Operator response:**  
None.

**User response:**  
None.

**System programmer response:**  
None.

---

**GLD8845E**  
Entry format for "option" is not valid.

**Explanation:**  
The ldapdiff utility encountered an error while parsing the -C countNumber, -sp port, or -cp port command line parameters. The number specified is less than zero or not a proper numeric number.

In the message text:

- **option**  
  Option name

**Example:**  
None.

**System action:**  
The program ends.

**Operator response:**  
None.

**User response:**  
None.

**System programmer response:**  
None.

---

**GLD8846E**  
Missing JSSE package for SSL connection.

**Explanation:**  
The installed version of Java is missing the Java secure socket extension (JSSE) package or the JSEE settings are not correct.

**Example:**  
None.

**System action:**  
The program continues but connecting with the proper JSSE settings is not successful.

**Operator response:**  
None.

**User response:**  
None.

**System programmer response:**  
None.

---

**Administrator response:**  
Verify that the targeted LDAP servers are still running. Use the information in this message and other messages to correct the problem. If additional information is required to solve the problem, specify -d ALL on the command line. Then restart the program.

**Problem determination:**  
Not applicable.

**Source:**  
LDAP

**Module:**  
None.

**Routing code:**  
None.

**Descriptor code:**  
None.

**Automation:**  
Not applicable.
program. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD8847E** Specified SASL mechanism is not available for server name.

**Explanation:** The ldifdiff utility encountered an error because the LDAP server does not support the SASL authentication mechanism specified. This message is typically accompanied by another message indicating the exact cause of the error.

In the message text:

name

Server name

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the accompanying message to correct the problem. If additional information is required to solve the problem, specify -d ALL on the command line. Then restart the program. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD8848E** Unable to fix entry

**Explanation:** The ldifdiff utility encountered an error while attempting to fix an entry on the consumer server because the bindDn specified on the -cD command line parameter does not have the appropriate permissions. This message is typically accompanied by another message indicating the exact cause of the error.

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the accompanying message to correct the problem. If additional information is required to solve the problem, specify -d ALL on the command line. Then restart the program. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.

---

**GLD8849E** Error occurred while retrieving filter ACL support of the server.

**Explanation:** The ldifdiff utility encountered an error while retrieving the rootDSE entry attributes from the LDAP server to determine if it supports filter ACL support. This message is usually accompanied by another message indicating the exact cause of the error.

**Example:** None.

**System action:** The program continues however filter ACL support is assumed not to be supported on the LDAP server.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Use the information in the accompanying message to correct the problem. If additional information is required to solve the problem, specify -d ALL on the command line. Then restart the program. If the problem persists, contact the service representative.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
GLD8850E  Password may not be modified for "name" on server "server_url".

Explanation: The password for the entry being modified is not allowed to be changed by the authenticated user.

In the message text:

name  Entry distinguished name
server_url  LDAP server url

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the authenticated user has the appropriate permissions to change password values on the consumer server. Ensure that the effective password policy for the entry being modified on the consumer server allows the password to be modified. Use the Effective password policy extended operation in the ldapexop utility to query the effective password policy on both servers. If there are differences in the effective password policies on both servers, synchronize the password policies using the ldapdiff utility to allow this password value on the consumer server. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8852E  Password syntax is not valid for "name" on server "server_url".

Explanation: The syntax of the password value for the entry being modified on the consumer server is not valid. The effective password policy on the consumer server does not allow this password value because it does not conform to the allowed password syntax.

In the message text:

name  Entry distinguished name
server_url  LDAP server url

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the effective password policy for the entry being modified on the consumer server is the same as it is on the supplier server. Use the Effective password policy extended operation in the ldapexop utility to query the effective password policy on both servers. If there are differences in the effective password policies on both servers, synchronize the password policies using the ldapdiff utility to allow this password value on the consumer server. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8851E  Must supply old password for "name" on server "server_url".

Explanation: The old password value must be supplied with the new password value while modifying the entry on the consumer server.

In the message text:

name  Entry distinguished name
server_url  LDAP server url

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that the effective password policy for the entry being modified on the consumer server is the same as it is on the supplier server. Use the Effective password policy extended operation in the ldapexop utility to query the effective password policy on both servers. If there are differences in the effective password policies on both servers, synchronize the password policies using the ldapdiff utility to allow this password value on the consumer server. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8853I Finished comparing number entries...
Explanation: The ldapdiff utility has processed the number of entries indicated in the message.
In the message text:
  number
  Number of entries processed
Example: None.
System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8854E Error occurred while setting the replication controls.
Explanation: The ldapdiff utility encountered an internal error while setting the advanced replication request controls. This message is accompanied by another message indicating the exact cause of the error.
Example: None.
System action: The program continues without sending the advanced replication controls to the consumer server.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Correct the host and port values specified for the supplier and consumer servers. Then restart the program.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8855E Supplier and consumer servers cannot be the same.
Explanation: The ldapdiff utility requires the host and port specified for the supplier and consumer servers be different. The ldapdiff utility does not support comparing and fixing entries on the same server.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8856E Internal error occurred.
Explanation: The ldapdiff utility encountered an internal error while removing controls from the previous request. This message is accompanied by another message indicating the exact cause of the error.
Example: None.
System action: The program continues without removing the control from the previous request.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: Use the information in the accompanying message to correct the problem. If additional information is required to solve the problem, specify -d ALL on the command line. Then restart the program. If the problem persists, contact the service representative.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
GLD8857E Unable to display DNs only for non-matching entries. Servers must be able to calculate entry checksums in order to use this feature.

Explanation: If the -O command line parameter is specified on the ldapdiff utility, both servers must support entry checksum calculation with the ibm-entryChecksum and the ibm-entryChecksumOp attributes. The utility uses these attribute values to compare each entry on the supplier and consumer servers to quickly detect differences.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Verify that both servers support the calculation of entry checksums by searching the rootDSE entry. Each LDAP server must have an ibm-supportedCapabilities attribute value of 1.3.18.0.2.32.56 on the rootDSE entry to use the -O command line parameter. If both LDAP servers do not have this support, remove the -O command line parameter. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8858W Schema differences will not be automatically fixed.

Explanation: The ldapdiff utility does not support automatically fixing schema differences. The -F command line parameter is only supported for automatically fixing non-schema related entries.

Example: None.

System action: The program continues but the schema is not automatically fixed.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: If the -L command line parameter is specified, the schema differences between the LDAP servers are written to an output schema LDIF file. This generated LDIF file can be used to manually modify the consumer server. If the -L command line parameter is not specified, the schema differences are written to standard output.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8859E A KeyStorePwd or TrustStorePwd is required.

Explanation: A KeyStorePwd or TrustStorePwd is required when the keyStoreType or trustStoreType options on the ldapdiff command line are set to JCEKS. The password must be specified on the -sP, -sY, -cP, or -cY command line parameters to gain access to the keyStore or trustStore.

Example: None.

System action: The program ends.

Operator response: None.

User response: None.

System programmer response: None.

Administrator response: Specify a password value for the keyStore or trustStore. Then restart the program.

Problem determination: Not applicable.

Source: LDAP

Module: None.

Routing code: None.

Descriptor code: None.

Automation: Not applicable.

GLD8860E The "name" DN is not valid.

Explanation: The ldapdiff utility is unable to search the supplier and consumer servers for the distinguished name indicated in the message because the name is not valid.

In the message text:

name
Entry distinguished name

Example: None.

System action: If the -S command line parameter is specified to compare the schema on both LDAP servers, the program continues; otherwise the program ends.

Operator response: None.
User response: None.
System programmer response: None.
Administrator response: If the distinguished name indicated in the message is the baseDn specified on the -b command line parameter, verify that it is valid and exists on both LDAP servers being compared. If the distinguished name is not the baseDn, check the entry on the LDAP server to verify that it is valid. Then restart the program.

Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8861E A specified option is not supported.
Explanation: The ldapdiff utility has detected an option that it does not support.
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.

GLD8862I The -O option overrides the -F and -L options.
Explanation: The -O command line parameter was specified with either the -F or -L parameters on the ldapdiff utility command line. When this occurs, the distinguished names (DNs) of entries that differ between the LDAP servers are only displayed to standard output. The differences are not fixed and are not written to the output LDIF file specified on the -L command line parameter.
Example: None.

System action: The program continues but entry differences are not fixed and are not written to the output LDIF file specified on the -L command line parameter.
Operator response: None.
User response: None.
System programmer response: None.

GLD8863I LDIF output will be written to filename.
Explanation: Since the -L command line parameter was specified, the entry differences between the LDAP servers are written to the output LDIF file that is indicated in the message.
In the message text:

filename Output LDIF file

Example: None.
System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.

GLD8864I Schema LDIF output will be written to filename.
Explanation: Since the -S and -L command line parameters were specified together on the ldapdiff utility, the schema differences between the LDAP servers are written to the schema output LDIF file that is indicated in the message.
GLD8865E  GLD8867E

In the message text:

filename
   Schema output LDIF file
Example: None.
System action: The program continues.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8865E  Password is too short for "name" on server "server_url".

Explanation: The password value for the entry being modified on the consumer server is too short in length. The effective password policy on the consumer server does not allow the entry to have a password value this short.

In the message text:

name
   Entry distinguished name
server_url
   LDAP server url
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8866E  Password is too young for "name" on server "server_url".

Explanation: The password value for the entry being modified on the consumer server is not allowed to be changed because it has been modified too recently. The effective password policy on the consumer server does not allow the entry's password value to be modified at this time.

In the message text:

name
   Entry distinguished name
server_url
   LDAP server url
Example: None.
System action: The program ends.
Operator response: None.
User response: None.
System programmer response: None.
Administrator response: None.
Problem determination: Not applicable.
Source: LDAP
Module: None.
Routing code: None.
Descriptor code: None.
Automation: Not applicable.

GLD8867E  Password is in history for "name" on server "server_url".

Explanation: The password value for the entry being modified on the consumer server is not allowed to be changed to this value because it already exists in the entry's password history. The effective password policy on the consumer server does not allow the entry's password value to be set to this value.

In the message text:
**name**  
Entry distinguished name

**server_url**  
LDAP server url

**Example:** None.

**System action:** The program ends.

**Operator response:** None.

**User response:** None.

**System programmer response:** None.

**Administrator response:** Verify that the effective password policy for the entry being modified on the consumer server is the same as it is on the supplier server. Use the **Effective password policy** extended operation in the `ldapexop` utility to query the effective password policy on both servers. If there are differences in the effective password policies on both servers, synchronize the password policies using the `ldapdiff` utility to allow this password value on the consumer server. All **pwdHistory** attribute values for the entry may need to be removed from the consumer server using the `ldapmodify` utility to allow the entry to be synchronized. Then restart the program.

**Problem determination:** Not applicable.

**Source:** LDAP

**Module:** None.

**Routing code:** None.

**Descriptor code:** None.

**Automation:** Not applicable.
Chapter 6. Return and reason codes

Changed return codes

For information about changed LDAP return codes, see z/OS Migration or see Migration considerations for applications.

Return codes

If errors occur in the LDAP server during a client request, a return code is returned as part of the operations response. The return codes that are returned by the z/OS LDAP server on client requests are documented in /usr/include/ldap.h. However, only a subset of the documented return codes in ldap.h are allowed to be returned by the z/OS LDAP server. When an error occurs in the LDAP server, more specific information about the error is returned to the client application in the reason code message. See Reason codes for information about the reason codes.

Table 1 summarizes these return codes in the ldap.h file. All other return codes documented in the ldap.h file are returned by the LDAP C client routines.

<table>
<thead>
<tr>
<th>#define in ldap.h file</th>
<th>LDAP return code decimal (hexadecimal)</th>
<th>LDAP return code description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP_SUCCESS</td>
<td>0 (0x00)</td>
<td>The operation is successful.</td>
</tr>
<tr>
<td>LDAP_OPERATIONS_ERROR</td>
<td>1 (0x01)</td>
<td>An internal operations error occurred in the LDAP server.</td>
</tr>
<tr>
<td>LDAP_PROTOCOL_ERROR</td>
<td>2 (0x02)</td>
<td>The LDAP server encountered an LDAP client request that is not a valid LDAP message. Verify that the LDAP client request messages are encoded properly.</td>
</tr>
<tr>
<td>LDAP_TIMELIMIT_EXCEEDED</td>
<td>3 (0x03)</td>
<td>The time limit for the search request has been exceeded. See Customizing the LDAP server configuration about the timelimit option for more information about how time limits are processed in the LDAP server.</td>
</tr>
<tr>
<td>LDAP_SIZELIMIT_EXCEEDED</td>
<td>4 (0x04)</td>
<td>The size limit on the search request has been exceeded. See the Customizing the LDAP server configuration about the sizelimit option for more information about how size limits are processed in the LDAP server.</td>
</tr>
<tr>
<td>LDAP_COMPARE_FALSE</td>
<td>5 (0x05)</td>
<td>The attribute value specified for the attribute type on the compare request does not exist in the entry.</td>
</tr>
<tr>
<td>LDAP_COMPARE_TRUE</td>
<td>6 (0x06)</td>
<td>The attribute value specified for the attribute type on the compare request does exist in the entry.</td>
</tr>
<tr>
<td><code>#define</code> in <code>ldap.h</code> file</td>
<td>LDAP return code decimal (hexadecimal)</td>
<td>LDAP return code description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LDAP_STRONG_AUTH_NOT_SUPPORTED</td>
<td>7 (0x07)</td>
<td>The requested authentication mechanism is not supported by the z/OS LDAP server. The bind mechanisms supported by the z/OS LDAP server are: anonymous, simple, CRAM-MD5, DIGEST-MD5, GSSAPI (Kerberos), and SASL EXTERNAL.</td>
</tr>
<tr>
<td>LDAP_STRONG_AUTH_REQUIRED</td>
<td>8 (0x08)</td>
<td>Not currently returned by the z/OS LDAP server.</td>
</tr>
<tr>
<td>LDAP_PARTIAL_RESULTS</td>
<td>9 (0x09)</td>
<td>The LDAP server encountered an error while processing an LDAP Version 2 search request and a referral entry was encountered. This return code is used to indicate that not all search results have been obtained because LDAP version 2 client applications do not follow referrals automatically.</td>
</tr>
<tr>
<td>LDAP_REFERRAL</td>
<td>10 (0x0A)</td>
<td>The LDAP server encountered a referral while processing a search request. The client application may follow the referral to another LDAP server to process the remainder of the request.</td>
</tr>
<tr>
<td>LDAP_ADMIN_LIMIT_EXCEEDED</td>
<td>11 (0x0B)</td>
<td>Not currently returned by the z/OS LDAP server.</td>
</tr>
<tr>
<td>LDAP_UNAVAILABLE_CRITICAL_EXTENSION</td>
<td>12 (0x0C)</td>
<td>Not currently returned by the z/OS LDAP server.</td>
</tr>
<tr>
<td>LDAP_CONFIDENTIALITY_REQUIRED</td>
<td>13 (0x0D)</td>
<td>A control specified on an LDAP client request had the control criticality set to true however the server does not recognize the control or the control is not appropriate for the operation. If the control is not critical, set the criticality to false to allow the LDAP server to ignore the control if it is always sent on all client requests. See <a href="#">Supported server controls</a> for more information about the supported controls in the z/OS LDAP server.</td>
</tr>
<tr>
<td>LDAP_SASLBIND_IN_PROGRESS</td>
<td>14 (0x0E)</td>
<td>A CRAM-MD5, DIGEST-MD5, or GSSAPI (Kerberos) bind is currently in progress. This is a temporary error that occurs on these multi handshake binds between the client and server.</td>
</tr>
<tr>
<td>LDAP_NO_SUCH_ATTRIBUTE</td>
<td>16 (0x10)</td>
<td>An attribute type specified on the LDAP client request does not exist in the entry. Verify that the entry being modified or compared has the attribute that was specified.</td>
</tr>
<tr>
<td>LDAP_UNDEFINED_TYPE</td>
<td>17 (0x11)</td>
<td>An attribute specified on the LDAP client request does not exist in the LDAP server's schema. The attribute must be added to the LDAP server's schema so that it can be used.</td>
</tr>
<tr>
<td>#define in ldap.h file</td>
<td>LDAP return code decimal (hexadecimal)</td>
<td>LDAP return code description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>LDAP_INAPPROPRIATE_MATCHING</td>
<td>18 (0x12)</td>
<td>The LDAP server encountered an error during a search request because the search filter is attempting to use a matching rule that is not supported by the attribute type. This can occur while attempting to use an attribute type/value pair in the search filter that has binary syntax. These types of search filters are not supported in the z/OS LDAP server.</td>
</tr>
<tr>
<td>LDAP_CONSTRAINT_VIOLATION</td>
<td>19 (0x13)</td>
<td>The LDAP server encountered a constraint error during a client request. This error can occur if an integer value specified on an integer syntax attribute is too large or small, an entry is attempted to be added or modified with an obsoleted objectclass or attribute type, or a non-user modifiable attribute type in the schema.</td>
</tr>
<tr>
<td>LDAP_TYPE_OR_VALUE_EXISTS</td>
<td>20 (0x14)</td>
<td>The LDAP server encountered an error during a client request because the attribute type or the attribute type and value pair exist in the targeted entry.</td>
</tr>
<tr>
<td>LDAP_INVALID_SYNTAX</td>
<td>21 (0x15)</td>
<td>An attribute value specified on an LDAP client request does not have a valid syntax specified. For example, if an attribute type in the schema has an integer syntax, an integer value must be specified on an add or modify request.</td>
</tr>
<tr>
<td>LDAP_NO_SUCH_OBJECT</td>
<td>32 (0x20)</td>
<td>The LDAP server encountered an error during a client request because the target entry does not exist in the directory.</td>
</tr>
<tr>
<td>LDAP_ALIAS_PROBLEM</td>
<td>33 (0x21)</td>
<td>The LDAP server encountered an error while attempting to process alias entries on a client request. Verify that there are no alias loops in the directory (for example, alias entries pointing at each other) and that the alias entries are properly configured. See the Alias section for more information about configuring aliases in the LDAP server.</td>
</tr>
<tr>
<td>LDAP_INVALID_DN_SYNTAX</td>
<td>34 (0x22)</td>
<td>The LDAP client request is not allowed because the DN does not have valid syntax. This error can occur on add and modify requests if the distinguished name (DN) is missing an equal sign (‘=’) between an attribute type and value or the DN does not contain a correct escaping sequence before a multi-byte UTF8 value.</td>
</tr>
<tr>
<td>LDAP_ALIAS_DEREF_PROBLEM</td>
<td>36 (0x24)</td>
<td>The LDAP server encountered an error on a search request while attempting to dereference an alias entry however the dereferenced entry does not exist in the directory. Verify that alias entries in the directory point to valid entries in the DIT.</td>
</tr>
<tr>
<td>#define in ldap.h file</td>
<td>LDAP return code</td>
<td>LDAP return code description</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>LDAP_INAPPROPRIATE_AUTH</td>
<td>48 (0x30)</td>
<td>The LDAP client request is not allowed because the password (credentials) specified is not correct or the authenticating user’s distinguished name is not correct. Verify that the authenticating user’s distinguished name and password are correct.</td>
</tr>
<tr>
<td>LDAP_INVALID_CREDENTIALS</td>
<td>49 (0x31)</td>
<td>The LDAP client request is not allowed because the password (credentials) specified is not correct or the authenticating user’s distinguished name is not correct. Verify that the authenticating user’s distinguished name and password are correct.</td>
</tr>
<tr>
<td>LDAP_INSUFFICIENT_ACCESS</td>
<td>50 (0x32)</td>
<td>The LDAP client request is not allowed because the authenticated user does not have the appropriate authority to perform the requested operation. Verify that ACLs are configured correctly for the authenticated user or the groups that the authenticated user belongs to.</td>
</tr>
<tr>
<td>LDAP_BUSY</td>
<td>51 (0x33)</td>
<td>The LDAP server is currently busy processing another request.</td>
</tr>
<tr>
<td>LDAP_UNAVAILABLE</td>
<td>52 (0x34)</td>
<td>The LDAP server is currently not available to process the client request. This error occurs for variety of reasons including DB2 is not available for configured TDBM or GDBM backends, ICSF is not available for password encryption or decryption, and RACF is not available for the SDBM backend. Verify that products the LDAP server must use to process the request are available.</td>
</tr>
<tr>
<td>LDAP_UNWILLING_TO_PERFORM</td>
<td>53 (0x35)</td>
<td>The LDAP server is unwilling to perform the requested LDAP client request.</td>
</tr>
<tr>
<td>LDAP_LOOP_DETECT</td>
<td>54 (0x36)</td>
<td>Not currently returned by the z/OS LDAP server.</td>
</tr>
<tr>
<td>LDAP_NAMING_VIOLATION</td>
<td>64 (0x40)</td>
<td>The LDAP client request is not allowed because of a distinguished name violation. This error occurs on add requests when the superior entry is a referral or an alias entry. This error also occurs on add and modify requests when the distinguished name (DN) contains an attribute type that has binary syntax, which is not allowed in distinguished names.</td>
</tr>
<tr>
<td>LDAP_OBJECT_CLASS_VIOLATION</td>
<td>65 (0x41)</td>
<td>The LDAP client request is not allowed because it does not adhere to the LDAP server's schema. This error occurs on add, modify, and modify dn requests when adding or modifying an entry in such a way that it does not have all required attribute values for the entry's object class.</td>
</tr>
</tbody>
</table>
### Table 1. LDAP server return codes (continued)

<table>
<thead>
<tr>
<th>#define in ldap.h file</th>
<th>LDAP return code decimal (hexadecimal)</th>
<th>LDAP return code description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP_NOT_ALLOWED_ON_NONLEAF</td>
<td>66 (0x42)</td>
<td>The LDAP client request is not allowed on a non-leaf node in the directory. This error generally occurs while attempting to delete an entry that has child entries underneath it in the DIT. The leaf or child entries must be deleted before removing this entry from the DIT.</td>
</tr>
<tr>
<td>LDAP_NOT_ALLOWED_ON_RDN</td>
<td>67 (0x43)</td>
<td>The LDAP client request is attempting to change a relative distinguished name (RDN) component of a distinguished name (DN) which is not allowed. For example, this can occur when attempting to delete the cn attribute from the DN, cn=yvonne,o=ibm, but the cn attribute value is a required attribute for the entry’s object class.</td>
</tr>
<tr>
<td>LDAP_ALREADY_EXISTS</td>
<td>68 (0x44)</td>
<td>The LDAP client request is attempting to add an entry to the LDAP server that already exists or attempting to modify the schema to include an attribute type or object class that is already present in the schema.</td>
</tr>
<tr>
<td>LDAP_NO_OBJECT_CLASS_MODS</td>
<td>69 (0x45)</td>
<td>Not currently returned by the z/OS LDAP server.</td>
</tr>
<tr>
<td>LDAP_AFFECTS_MULTIPLE_DSAS</td>
<td>71 (0x47)</td>
<td>Not currently returned by the z/OS LDAP server.</td>
</tr>
<tr>
<td>LDAP_OTHER</td>
<td>80 (0x50)</td>
<td>An internal error occurred in the LDAP server that does not fall under one of the previously documented return codes. It is commonly used for indicating an out of storage error in the LDAP server.</td>
</tr>
</tbody>
</table>

### Reason codes

The **LDAPResult** construct is used by the LDAP protocol to return success or failure indications from servers to clients. This construct contains an error message field. Servers can optionally provide “human-readable” diagnostic information in this field. Depending on the location in the LDAP server where errors are detected, error messages generated may have the following format:

\[ <\text{numeric digits}> <\text{diagnostic information}> <\text{traceback information}> \]

where:

- **numeric digits**
  - Represents a specific reason code.

- **diagnostic information**
  - Provides details about the reason for the failure.

- **traceback information**
  - Is of the form \((\text{function name}:\text{line number})\) and assists you in diagnosing application or configuration problems.
Note the following regarding this error information:
- It is intended to be “human-readable” to assist in identifying problems detected by the server.
- It is not translated (English text only).
- It is not intended to be used as an application programming interface (API).
- Data returned may be changed by service or new releases of the product.
  (Again, it is not intended to be an API.)
- The reason code returned for a particular error can change and the reason code text can change.

Following is the current list of reason codes and associated diagnostic information returned by the LDAP server.

R000001  Unable to allocate storage

Explanation: An LDAP operation failed because the LDAP server is unable to allocate the necessary storage to continue processing the request.

System action: Depending on the severity of the storage problem, the LDAP server may continue or may end. The LDAP operation fails.

Operator response: Increase the storage available for use by the LDAP server. Then restart the LDAP server. If the problem persists, contact the service representative.

User response: Contact the operator and an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: If running the 31-bit LDAP server (GLDSRV31), consider using the 64-bit LDAP server (GLDSRV64) to use the additional storage available in a 64-bit address space. Then restart the LDAP server.

R000004  Internal server error encountered

Explanation: An LDAP operation failed because the LDAP server detects an internal programming error.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Use server ERROR debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

R000005  Unable to translate value for attribute 'name' from source_codepage to target_codepage

Explanation: An LDAP operation failed because the LDAP server cannot translate an attribute name or value between local code page and UTF8. The name of the attribute and the source and target code pages are indicated in the reason code.

In the message text:

- name
  - Attribute name
- source_codepage
  - Source code page name
- target_codepage
  - Target code page name

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Use server ERROR debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

R000100  The password has expired

Explanation: An LDAP bind operation to the SDBM backend failed because the password of the z/OS Security Server user associated with the bind distinguished name is expired.

System action: The LDAP server continues to run, but the operation fails.

User response: The expired password must be reset. A new password can be specified during bind by using the old_password/new_password format. For RACF, the password can be a password or a password phrase. Also, for RACF, the password or phrase can be changed by another LDAP user using an SDBM modify command of the racfPassword or racfPassPhrase attribute, assuming that the user has the RACF authorization to change a password or phrase.

R000101  The new password is not valid

Explanation: An LDAP bind operation to the SDBM backend failed. The bind tries to change the current
password of the z/OS Security Server user associated with the bind distinguished name but the new password is not valid to the z/OS Security Server. For RACF, the password can be a password or a password phrase.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Review the password requirements of the z/OS Security Server, including rules on password history and syntax. For RACF, when using the `old_password/new_password` format to change a password, the old and new values must both be passwords or both be password phrases. Correct the passwords and then reissue the operation.

---

R000102  The user id has been revoked

**Explanation:** An LDAP bind operation to the SDBM backend failed because the z/OS Security Server user associated with the bind distinguished name is revoked. This user cannot be used until the user is no longer revoked.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact a z/OS Security Server administrator to unrevvoke the user. For RACF, this can also be accomplished by another LDAP user using an SDBM modify operation specifying a value of `resume` for the `racfAttributes` attribute, assuming that the user has the RACF authorization to do this. Then reissue the operation.

---

R000105  A bind argument is not valid

**Explanation:** An LDAP bind operation to the SDBM backend failed because of a problem using the password or parsing the old and new passwords when using the `old_password/new_password` format to change a password. The length of the old password and new password (if specified) must be greater than 0 and less than 101. For RACF, the passwords can be passwords or password phrases.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Check that the supplied passwords are not too short or long. When using the `old_password/new_password` format, leaving out the old or new password (by specifying `/new_password` or `old_password/`) produces a zero-length password. Then reissue the operation.

---

R000114  The realm portion of the value of attribute 'name' is not the RACF default realm

**Explanation:** An LDAP add, modify, or search operation to the SDBM backend failed. The operation specifies an attribute value using `principal@realm` format, but the `realm` part of the value does not match the name of the local z/OS Kerberos Security Server (KERBDFLT) realm. The name of the attribute is indicated in the reason code.

In the message text:

```
name
```

Attribute name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Either contact a z/OS Security Server administrator to determine the correct realm name to use in the attribute value or remove the `@realm` part of the value. Then reissue the operation.

---

R000115  There is no RACF default realm

**Explanation:** An LDAP operation to the SDBM backend failed because SDBM is not able to determine the local z/OS Kerberos Security Server (KERBDFLT) realm. SDBM uses the RACF R_kerbinfo callable service to retrieve the realm name. Either there is no realm name or the callable service failed to retrieve it.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact a z/OS Security Server administrator to correct the problem. Then reissue the operation.

**System programmer response:** Determine why the R_kerbinfo callable service failed. LDAP server ERROR
debug trace output contains the various return codes from R_kerbinfo.

**R000116** Cannot specify a value when deleting attribute 'name'

**Explanation:** An LDAP modify operation to the SDBM backend failed because it tries to delete a specific value from the attribute indicated in the reason code. SDBM does not support deleting individual values for this attribute.

In the message text:

```
name
Attribute name
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the modify operation input to delete the entire attribute or to replace the attribute values with the wanted values. Then reissue the operation.

---

**R000117** Cannot delete attribute 'name'

**Explanation:** An SDBM modify operation failed because it is trying to delete an attribute that corresponds to a RACF profile field that cannot be deleted. This reason code can also occur when the LDAP server is processing a replicated add or modify operation that attempts to delete a value for certain operational attributes that cannot be deleted. The attribute that cannot be deleted is indicated in the reason code.

In the message text:

```
name
Attribute name
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the modify input to delete the entire attribute or to replace the attribute values with the wanted values. Then reissue the operation.

---

**R000119** Cannot add or replace attribute 'name'

**Explanation:** An LDAP add or modify operation to the SDBM backend failed because it specifies an attribute value that is not the same as in the relative distinguished name (RDN) of the entry. The RDN is the leftmost part of the entry’s distinguished name. An attribute that is in the RDN cannot be assigned a value other than its value in the RDN. This applies to cn, racfid, racfuserid, racfgroupid, and profilename if they appear in the RDN. The name of the attribute is indicated in the reason code.

In the message text:

```
name
Attribute name
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the add or modify input so that it does not specify multiple values for single-valued attributes. Then reissue the operation.
R000122  The value for attribute ’name’ must be the DN of a user

Explanation: An LDAP add or modify operation to the SDBM backend failed because a distinguished name (DN) value is specified for the attribute indicated in the reason code but the DN does not have the correct format for an SDBM user DN. The format of an SDBM user DN is racfid=userid,profiletype=user,SDBMsuffix. In the message text:

name
  Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Correct each value for this attribute in the modify input to specify a valid, complete SDBM user DN. Alternatively, specify just the userid as the attribute value instead of a complete SDBM user DN. Then reissue the operation.

R000123  The value for attribute ’name’ must be the DN of a group

Explanation: An LDAP add or modify operation to the SDBM backend failed because a distinguished name (DN) value is specified for the attribute indicated in the reason code but the DN does not have the correct format for an SDBM group DN. The format of an SDBM group DN is racfid=groupid,profiletype=group,SDBMsuffix. In the message text:

name
  Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Correct each value for this attribute in the modify input to specify a valid, complete SDBM user or group DN. Alternatively, specify just the userid or groupid as the attribute value instead of a complete SDBM user or group DN. Then reissue the operation.

R000124  The value for attribute ’name’ must be the DN of a user or a group

Explanation: An LDAP add or modify operation to the SDBM backend failed because a distinguished name (DN) value is specified for the attribute indicated in the reason code but the DN does not have the correct format for an SDBM user DN or group DN. The format of an SDBM user DN is racfid=userid,profiletype=user,SDBMsuffix and the format of an SDBM group DN is racfid=groupid,profiletype=group,SDBMsuffix. In the message text:

name
  Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Correct each value for this attribute in the modify operation input to specify a valid, complete SDBM user or group DN. Alternatively, specify just the userid or groupid as the attribute value instead of a complete SDBM user or group DN. Then reissue the operation.

R000125  Attribute ’name’ is not supported

Explanation: An LDAP add or modify operation to the SDBM backend failed because the operation input includes an attribute that is not supported by SDBM. SDBM only allows using the attributes that map to fields in the corresponding RACF profile. The name of the attribute indicated in the reason code. In the message text:

name
  Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Remove the attribute from the add or modify input. Then reissue the operation.

R000126  Filter ’filter’ is not supported for this base

Explanation: An LDAP search operation to the SDBM backend failed because the search filter contains an attribute that is not allowed for the base (target entry) of the search. The name of the attribute is indicated in the reason code. SDBM has limited search support. Only certain filters can be used, depending on the base of the search. The acceptable combinations are documented in SDBM search capabilities. In the message text:

filter
  Search filter attribute name
**R000127 • R000132**

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the search input to use a combination of filter and base that is supported by SDBM. Then reissue the operation.

---

**R000127** Filter 'filter' contains a type without a value

**Explanation:** An LDAP search operation to the SDBM backend failed because the search filter contains an attribute without a value. The name of the attribute is indicated in the reason code. All attributes in the filter must have a non-blank value after leading blanks are removed.

In the message text:

`filter`

Search filter attribute name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the search input to use a combination of filter and base that is supported by SDBM. Then reissue the operation.

---

**R000128** Filter is not supported

**Explanation:** An LDAP search operation to the SDBM backend failed because the search filter is not one of the few that SDBM accepts. Either the filter syntax or the attributes used in the filter are not supported by SDBM. SDBM has limited search support. Only certain filters can be used. The supported filters are documented in [SDBM search capabilities](#).

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the search input to specify a non-blank value for the attribute in filter. Then reissue the operation.

---

**R000129** Value 'value' is not supported for filter 'name'

**Explanation:** An LDAP search operation to the SDBM backend failed because the value of an attribute in the search filter is not acceptable to SDBM. The name of the attribute and its value are indicated in the reason code. SDBM has limited search support. Only certain filters and values can be used. The supported filters are documented in [SDBM search capabilities](#).

In the message text:

`value`

Search filter attribute value

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the search input to specify a non-blank value for the attribute in filter. Then reissue the operation.

---

**R000131** 'name' is not a valid RACF DN

**Explanation:** An LDAP operation to the SDBM backend failed because it involved a distinguished name (DN) that is not a valid SDBM DN. The DN might have been used, for example, as the target of the operation. The DN that is not valid is indicated in the reason code.

In the message text:

`name`

Distinguished name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the operation input to specify a DN value that is a valid SDBM DN. In particular:

- For the DN of a RACF user, group, connection, class, or resource, the `racfid`, `racfuserid`, `racfgroupid`, and `profiletype` value must be from 1 to 8 characters long. The value must not contain a space or a comma, and the value cannot be an asterisk (*).
- For the DN of a RACF resource, the `profilename` value must be from 1 to 256 characters long. The value cannot contain a space or a comma. The value can be an asterisk (*).

Then reissue the operation.

---

**R000132** Value for attribute 'name' cannot be more than size characters

**Explanation:** An LDAP search operation to the SDBM backend failed because the value of an attribute in the search filter is too long for that attribute. The name of the attribute and the maximum length allowed for its value are indicated in the reason code. SDBM has limited search support. Only certain filters and values can be used. The supported filters are documented in [SDBM search capabilities](#).

In the message text:

`name`

Search filter attribute name

`size`

Maximum length for value

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the search input to specify a value that does not exceed the maximum length for the
attribute in the search filter. Then reissue the operation.

**R000133** Value for attribute 'name' must be an integer less than size

**Explanation:** An LDAP search operation to the SDBM backend failed because the value of an attribute in the search filter is too large. The name of the attribute and its maximum value are indicated in the reason code. SDBM has limited search support. Only certain filters and values can be used. The supported filters are documented in [SDBM search capabilities](#).

In the message text:

name
   Search filter attribute name
size
   Maximum value for attribute

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the search input to specify a value that does not exceed the maximum value for the attribute in the search filter. Then reissue the operation.

**R000134** The RACF type command created to satisfy this request is too long, probably due to specifying a long filter or attribute value or too many attribute values

**Explanation:** An LDAP operation to the SDBM backend failed because the RACF command created by SDBM to process the SDBM operation is too long. The type of RACF command is indicated in the reason code. For example, SDBM parses the attributes and values in an add operation for a user and translates them into the keywords and values of a RACF ADDUSER command. The maximum length of a RACF command is 4093.

In the message text:

name
   Distinguished name of target entry

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the operation input to reduce the number and length of attributes and values specified. This might involve dividing an add operation into a smaller add operation followed by a modify operation, or dividing a modify operation into two smaller modify operations. Then reissue the operation.

**R000135** Cannot perform this request on a reserved SDBM DN, 'name'

**Explanation:** An LDAP operation to the SDBM backend failed because it cannot be performed on the entry to which it was targeted. The distinguished name (DN) of the entry is indicated in the reason code. When the LDAP server is started, SDBM automatically creates the following entries to provide a directory hierarchy: suffix entry, user subtree top entry, group subtree top entry, connect subtree top entry, and class entries. These reserved entries cannot be added, modified, or deleted by SDBM operations. SDBM also creates a setropts entry. This entry cannot be added or deleted by SDBM operations, but it can be modified. All reserved entries can be searched and compared.

In the message text:

name
   Distinguished name of target entry

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the target of the operation so that it is not one of the SDBM reserved entries. Then reissue the operation.

**R000137** 'name' is not a valid RACF DN for bind, check that the syntax is correct for a RACF user DN

**Explanation:** An LDAP operation to the SDBM backend failed because the distinguished name (DN) of the requester is not valid for an SDBM user. The requester DN is indicated in the reason code. The format of an SDBM user DN is racfid=userid,profiletype=user,SDBMsuffix.

In the message text:

name
   Distinguished name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** When binding to SDBM, check that the distinguished name is valid for an SDBM user. When issuing other SDBM commands, ensure that the requester has bound using an SDBM distinguished name or using some other bind method that is associated to an SDBM user (for example, an LDBM or TDBM native authentication bind). Then reissue the operation.

**R000139** RACF type command failed

**Explanation:** An LDAP operation to the SDBM backend failed because the RACF command or service invoked by SDBM to do the operation does not succeed for some unknown reason. The type of RACF command is indicated in the reason code.

In the message text:

type
   Type of RACF command

**System action:** The LDAP server continues to run, but the operation fails.
**R000140** Cannot parse RACF 'type' output

**Explanation:** An LDAP operation to the SDBM backend failed because SDBM cannot process the output from the RACF command or service invoked by SDBM to perform the operation. Either the format of the output is not what SDBM expects or there is not enough storage available to parse the output.

In the message text:

- **type**
  Type of RACF command

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Use the information in server messages and ERROR debug trace output to assist in locating and correcting the problem.

---

**R000141** Routine 'name' failed, rc=return_code

**Explanation:** An LDAP operation to the SDBM backend failed because a routine called to process the operation did not succeed for an unknown reason. The reason code can also occur when trying to parse an addChangeLogEntry extended operation. The name of the routine and the LDAP return code from the routine are indicated in the reason code.

In the message text:

- **name**
  Routine name

- **return_code**
  Return code from routine

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Use the information in server messages and ERROR debug trace output to assist in locating and correcting the problem.

---

**R000142** Cannot obtain the password of a RACF user

**Explanation:** There are several types of bind methods, for example CRAM-MD5 and DIGEST-MD5, that require retrieval of a password for the bound user. These methods are not supported when binding with an SDBM user, because the password cannot be retrieved from the z/OS Security Server. SDBM only supports simple bind when binding with an SDBM user.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the bind input to use a bind method supported by SDBM. Then reissue the operation.

**Administrator response:** Use the information in the reason code and from server messages and ERROR debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

---

**R000143** Bound user does not have the authority to perform this operation

**Explanation:** An LDAP operation to the SDBM backend failed because it tries to extract or modify RACF information but the RACF user associated with the bound user does not have the necessary RACF authority. When SDBM issues RACF commands and uses RACF interfaces to process an SDBM request, it does so under the context of the RACF user associated with the bound user.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Ensure that the RACF user associated with the bound user has the RACF authority to perform the RACF operations required to process the SDBM operation. You might have to contact a z/OS Security Server administrator to obtain the necessary authorization. Then reissue the operation.

---

**R000144** Cannot specify a binary attribute in a compare operation

**Explanation:** An LDAP compare operation to the SDBM backend failed because the attribute to compare has binary syntax. SDBM does not support comparing binary values. For example, SDBM compare operations using the racfPasswordEnvelope and racfPassPhraseEnvelope attributes are not allowed.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the compare input to specify an attribute that does not have binary syntax. Then reissue the operation.

---

**R000145** Must specify a value when deleting attribute 'name'

**Explanation:** An LDAP modify operation to the SDBM backend failed because it tries to delete the attribute indicated in the reason code rather than specifying
values to delete from the attribute. SDBM only supports deleting specific values from this attribute.

In the message text:

name

Attribute name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the modify input to specify which values to delete for the attribute. Or, use a replace operation to replace all the values of the attribute with the wanted values. Then reissue the operation.

---

**R000146** Cannot access entry with DN 'name' because SDBM is not configured to support RACF resources

**Explanation:** An LDAP operation to the SDBM backend or the changeLogAddEntry extended operation failed because operation involves a class entry, resource entry, or the setropts entry, but the SDBM support for these entries is not enabled in the LDAP server. The enableResources on option must be specified in the SDBM section of the LDAP server configuration file when using one of these types of entries. The distinguished name (DN) of the unsupported entry is indicated in the reason code.

In the message text:

name

Distinguished name of target

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the target of the operation so that it is supported by SDBM. Then reissue the operation.

---

**R000147** The value for attribute 'attribute' must be the DN of a class

**Explanation:** An LDAP modify operation to the SDBM backend failed because a distinguished name (DN) value is specified for the attribute indicated in the reason code but the DN does not have the correct format for a class DN. The format of a class DN is profilename=classname,profiletype=DATASET,SDBMsuffix. For example:

```
profilename=SUSET1.PRIVATE.SQL,profiletype=DATASET,cn=myRACF
```

The DN that is the operation target is indicated in the reason code.

In the message text:

attribute

Attribute name

name

Distinguished name of the entry

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct each value for this attribute in the modify input to specify a valid, complete class DN. Alternatively, specify just a classname as the attribute value instead of a complete class DN. Then reissue the operation.

---

**R000148** DN 'name' is not supported as a target of an SDBM operation

**Explanation:** An LDAP operation to the SDBM backend failed because SDBM does not allow that operation to be performed on the target of the request. In particular, SDBM does not support any operation on a data set profile, which is represented by a distinguished name (DN) whose format is profilename=classname,profiletype=DATASET,SDBMsuffix. For example:

```
profilename=SUSET1.PRIVATE.SQL,profiletype=DATASET,cn=myRACF
```

In the message text:

name

Distinguished name of target

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the target of the operation so that it is supported by SDBM. Then reissue the operation.

---

**R000149** Attribute 'attribute' is not supported for entry with DN 'name'

**Explanation:** An LDAP add or modify operation to the SDBM backend failed because it tries to add an attribute that is not supported for the type of entry being added or modified. In particular, the setropts entry (cn=setropts,SDBMsuffix) supports a very limited set of attributes. Also, the racfAccessControl attribute can only be used in a resource entry, which is represented by a DN whose format is profilename=classname,profiletype=class, profiletype=DATASET,SDBMsuffix.

The attribute name and the distinguished name of the entry being added or modified are indicated in the reason code.

In the message text:

attribute

Attribute name

name

Distinguished name of the entry

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the attribute from the add or modify input. Then reissue the operation.
R000150  Unable to generate random data bytes

Explanation: An LDAP operation or utility failed because it uses random data and the routine to generate the random data does not succeed. Random data are used during CRAM-MD5 or DIGEST-MD5 bind operations and any operation that involves passwords that must be hashed using Salted SHA-1 or Salted SHA-2 methods, including when using the ldif2ds utility to load entries with passwords.

System action: The LDAP server continues to run, but the operation fails. The ldif2ds utility ends.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the request or restart the utility.

Administrator response: Use server messages and ERROR debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

R000200  Change log not active

Explanation: A changeLogAddEntry extended operation to create a change log entry failed because the LDAP server is not set up to do change logging. The GDBM backend must be configured in the LDAP server configuration file and the changeLogging off option must not be specified.

System action: The LDAP server continues to run, but the extended operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Add a GDBM section to the LDAP server configuration file. Do not specify the changeLogging off option in the section. Then restart the LDAP server.

R000201  Cannot decode field from request, rc=return_code

Explanation: An LDAP changeLogAddEntry extended operation to create a change log entry failed because it includes a field value that cannot be decoded. The field name is indicated in the reason code along with the return code from the routine that is invoked to decode the field. The most likely return codes are:

- 83 (LDAP_ENCODING_ERROR): Some part of the extended operation data is not encoded correctly.
- 90 (LDAP_NO_MEMORY): The LDAP server ran out of storage.

In the message text:

field
  Request field

return_code
  Return code from decode routine

System action: The LDAP server continues to run, but the extended operation fails.

User response: For a storage problem, increase the storage available for use by the LDAP server. Then restart the LDAP server. If the problem persists, contact the service representative.

Administrator response: For a storage problem, if running the 31-bit LDAP server (GLDSRV31), consider using the 64-bit LDAP server (GLDSRV64) to use the additional storage available in a 64-bit address space. Then restart the LDAP server.

R000202  Request did not come over PC interface

Explanation: There are some LDAP extended operations (for example, changeLogAddEntry) that are only supported by the LDAP server when they are received over the Program Call (PC) interface. The request failed because the requester did not use the PC interface.

System action: The LDAP server continues to run, but the extended operation fails.

User response: Ensure that your program is using the Program Call interface to communicate with the LDAP server. Then reissue the extended operation.

R000203  Value for name out of range

Explanation: An LDAP extended operation failed because it specifies a value that is not supported for a field. For example, the changeLogAddEntry extended operation requires the version field value be 2. The name of the field is indicated in the reason code. See Supported extended operations for information about the extended operations supported by the LDAP server.

In the message text:

name
  Field name

System action: The LDAP server continues to run, but the extended operation fails.

User response: Correct the value of the field in the extended operation input so that it is within the supported range. Then reissue the extended operation.

R000204  Required value for name is missing

Explanation: An LDAP extended operation failed because it does not include a required field. For example, the changeLogAddEntry extended operation requires at least one of the userid, group, or class and
resource fields. The missing field of the extended operation is indicated in the reason code. See [Supported extended operations](#) for more information about the extended operations supported by the LDAP server.

In the message text:

**name**

Field name

**System action:** The LDAP server continues to run, but the extended operation fails.

**User response:** Correct the extended operation input so that it contains all the required fields. Then reissue the extended operation.

**R000205** Unable to convert userid (user), group (group), class (class), or resource (resource) to DN, rc=return_code

**Explanation:** An LDAP extended operation failed because it is not able to convert the values indicated in the reason code into an SDBM distinguished name (DN). The LDAP return code is also displayed in the reason code. The most likely return codes are:

- 80 (LDAP_OTHER): Either a value contains a character that cannot be a user or the LDAP server ran out of storage. An error message is typically printed to the server output when there is a storage problem.

In the message text:

**user**

Userid name (if any)

**group**

Group name (if any)

**class**

Class name (if any)

**resource**

Resource name (if any)

**return_code**

Return code from routine

**System action:** The LDAP server continues to run, but the extended operation fails.

**Operator response:** For a storage problem, increase the storage available for use by the LDAP server. Then restart the LDAP server. If the problem persists, contact the service representative.

**User response:** Ensure that all values used in the extended operation input contain valid characters. Then reissue the extended operation. If the problem is storage, contact the operator and an LDAP administrator. After the problem is resolved, reissue the extended operation.

**Administrator response:** For a storage problem, if running the 31-bit LDAP server (GLDSRV31), consider using the 64-bit LDAP server (GLDSRV64) to use the additional storage available in a 64-bit address space. Then restart the LDAP server.

**R000206** PC caller must be in supervisor state

**Explanation:** An LDAP extended operation received over the Program Call (PC) interface failed because the requester is not in supervisor state. The LDAP server only processes requests from PC callers who are in supervisor state.

**System action:** The LDAP server continues to run, but the extended operation fails.

**User response:** Ensure that your program is running in supervisor state when it sends an extended operation request by a Program Call to the LDAP server. Then reissue the extended operation.

**R000207** name1 cannot be specified with name2

**Explanation:** An LDAP extended operation request to create a change log entry (changeLogAddEntry) failed because it specifies two fields that cannot be used together. For example, if the userid or group field is specified in the extended operation, then do not specify the class or resource field. The names of the conflicting fields are indicated in the reason code. See [Supported extended operations](#) for more information about the changeLogAddEntry extended operation.

In the message text:

**name1**

First field name

**name2**

Second field name

**System action:** The LDAP server continues to run, but the extended operation fails.

**User response:** Remove one of the conflicting fields in the changeLogAddEntry extended operation input. Then reissue the extended operation.

**R001001** Generalized Time value 'value' is not valid

**Explanation:** An LDAP operation failed because an attribute value involved in the operation contains a character that is not allowed by the Generalized Time syntax of the attribute. The format of a Generalized Time value is

- `yyyyymmddhhmmss.fffffff` for local time
- `yyyyymmddhhmms.fffffffZ` for Greenwich Mean Time
- `yyyyymmddhhmms.fffffff-hhmm` for time zone west of GMT
- `yyyyymmddhhmms.fffffff+hhmm` for time zone east of GMT

where `yyyy` is year, `mm` is month, `dd` is day, `hh` is hour, `mm` is minutes, `ss` is seconds, and `ffffff` is microseconds.
The seconds (ss) and microseconds (ffffff) can be omitted and default to 0. The value that is not valid is indicated in the reason code.

In the message text:

value
   Attribute value

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the value used in the operation input so that it is valid for the Generalized Time syntax. Then reissue the operation.

Duplicate value encountered: value

Explanation: An LDAP schema modify operation of an attribute or object class definition failed because the definition involves a duplicate value. The object identifier of the attribute or object class cannot be the same as an existing attribute, object class, matching rule, or syntax. It also cannot be the same as another attribute or object class added in this schema modify. Also, for an object class, the same attribute name cannot be specified twice within the SUP values, within the MUST values, or within the MAY values. The duplicate name or object identifier is indicated in the reason code.

In the message text:

value
   Name or object identifier

System action: The LDAP server continues to run, but the operation fails.

User response: Review the modify input to ensure that there are no duplicate names or object identifiers involved. Then reissue the operation.

COLLECTIVE keyword is not supported for attribute type 'name'

Explanation: An LDAP schema modify operation of an attribute failed because the attribute definition includes the COLLECTIVE keyword. The LDAP server does not support usage of this keyword. The name of the attribute is indicated in the reason code.

In the message text:

name
   Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Remove the COLLECTIVE keyword from the modify input. Then reissue the operation.

Syntax/matching rule inconsistency for attribute type 'identifier'

Explanation: An LDAP schema modify operation failed because it results in an attribute with a matching rule that is not valid for the syntax of the attribute. The numeric identifier of the attribute is indicated in the reason code. See [LDAP directory schema] for more information about the acceptable combinations of syntax and matching rules. Note that the failing attribute might not be directly modified in the schema modify operation. Instead, the modify may change a
syntax or matching rule in an attribute from which the failing attribute inherits its syntax or a matching rule, resulting in the inconsistency.

In the message text:

**identifier**

Attribute numeric identifier

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Analyze the modify input to ensure that it does not create any inconsistencies between syntax and matching rules for the modified attributes and the attributes that inherit from them. Then reissue the operation.

---

**R001018  Attribute type 'name' is obsolete**

**Explanation:** An LDAP add, modify, or modify DN operation failed because it involves an attribute that is marked as OBSOLETE in the schema. An obsolete attribute cannot be added or replaced in an entry. The attribute can be deleted from the entry. Note that an add or modify DN operation may try to add an obsolete attribute to the entry if the attribute is part of the new relative distinguished name (RDN) of the entry, because the LDAP server automatically adds the RDN attributes and values to the entry. The RDN is the leftmost part of the distinguished name. The name of the obsolete attribute is indicated in the reason code.

In the message text:

**name**

Attribute class name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Analyze the operation input to ensure that it does not involve adding or replacing an obsolete attribute in the entry. Then reissue the operation.

---

**R001024  Abstract class 'name' may not be a base object class**

**Explanation:** An LDAP add, modify, or modify DN operation failed because it results in specifying an ABSTRACT object class in the entry that is not in the superior hierarchy of some other STRUCTURAL or AUXILIARY object class in the entry. An ABSTRACT object class that is not in the superior hierarchy cannot be included in the entry. Note that an add or modify DN operation may try to add an object class if the objectclass attribute is part of the new relative distinguished name (RDN) of the entry, because the LDAP server automatically adds the RDN attributes and values to the entry. The RDN is the leftmost part of the distinguished name. The name of the abstract object class is indicated in the reason code.

In the message text:

**name**

Distinguished name of entry

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Check the operation input to ensure that it does not result in multiple base structural object classes. Then reissue the operation.

---

**R001026  No structural object class specified for 'name'**

**Explanation:** An LDAP add operation failed because it does not include a base structural object class in the entry. An entry's base structural object class is the STRUCTURAL object class that identifies the type of information kept in the entry. Examples are the person and organization object classes. There must be a single base structural object class in an entry and the object class cannot be changed. The distinguished name of the entry is indicated in the reason code.

In the message text:

**name**

Distinguished name of entry

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Check the add input to ensure that it
includes a base structural object class in the entry. Then reissue the operation.

**R001027 Base structural object class 'name' may not be changed**

**Explanation:** An LDAP modify or modify DN operation failed because it results in changing the base structural object class of the entry. An entry’s base structural object class is the STRUCTURAL object class that identifies the type of information kept in the entry. Examples are the person and organization object classes. There must be a single base structural object class in an entry and the object class cannot be changed. Note that a modify DN operation may try to change the object class if the objectclass attribute is part of the relative distinguished name (RDN) of the entry, the RDN is being changed, and the modify DN operation specifies removing the current RDN. The RDN is the leftmost part of the distinguished name. The name of the base structural object class is indicated in the reason code.

In the message text:

```
name
```

Object class name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Check the operation input to ensure that it does not change the base structural object class for the entry. Then reissue the operation. To change the base structural object class, delete the entry and then add it back using the new base structural object class.

**R001029 Entry does not contain MUST attribute 'name'**

**Explanation:** An LDAP add, modify, or modify DN operation failed because it results in an entry which does not contain all the MUST attributes required by the object classes in the entry (including those in the object class superior hierarchies). Every MUST attribute must appear in the entry. Note that a modify DN operation may try to remove attributes from an entry if they are in the current relative distinguished name (RDN) of the entry but not the new RDN and the modify DN operation specifies removing the current RDN. The RDN is the leftmost part of the distinguished name. The name of the missing attribute is indicated in the reason code.

In the message text:

```
name
```

Attribute name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Analyze the operation input to ensure that it does not result in an entry that contains attributes not allowed by the object classes in the entry. Then reissue the operation.

**R001030 Entry contains attribute 'name' which is not allowed for object class**

**Explanation:** An LDAP add, modify, or modify DN operation failed because it results in an entry which contains an attribute that is not in the MUST or MAY lists of the object classes in the entry (including those in the object class superior hierarchies). Every non-operational attribute must appear in the MUST or MAY lists of an object class associated with the entry. Note that an add or modify DN operation may try to add an attribute to an entry if it is in the new relative distinguished name (RDN) of the entry, because the LDAP server automatically adds the RDN attributes and values to the entry. The RDN is the leftmost part of the distinguished name. The name of the attribute is indicated in the reason code.

In the message text:

```
name
```

Attribute name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Analyze the operation input to ensure that it does not result in an entry that contains attributes not allowed by the object classes in the entry. Then reissue the operation.

**R001031 Missing left parenthesis in definition:**

**R001031 Missing left parenthesis in definition:**

**Explanation:** An LDAP schema modify operation failed because a left parenthesis is missing in a schema definition. The part of the definition that is in error is indicated in the reason code. See [LDAP directory schema](#) for more information about the format for the definitions of the various elements of the schema. The reason code may also occur on an entry add or modify operation when adding a value that does not begin with a left parenthesis for an attribute that is defined with the `integerFirstComponentMatch` matching rule. In this case, the value is indicated in the reason code.

In the message text:

```
definition
```

```
definition
```

Attribute or object class definition or value

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** For a schema modify operation, check the input to ensure that all the schema definitions are complete and correctly formatted. For an entry add or modify operation, put a left parenthesis at the beginning of the value for the attribute defined with the `integerFirstComponentMatch` matching rule. Then reissue the operation.

---

IBM Tivoli Directory Server Messages and Codes for z/OS V1R13.0

250
R001032  Missing right parenthesis in definition:

Explaination: An LDAP schema modify operation failed because a right parenthesis is missing in a schema definition. The part of the definition that is in error is indicated in the reason code. See LDAP directory schema for more information about the format for the definitions of the various elements of the schema.

In the message text:

**definition**

Attribute or object class definition

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Check the modify input to ensure that all the schema definitions are complete and correctly formatted. Then reissue the operation.

---

R001038  Numeric object identifier 'value' is not valid

Explaination: An LDAP operation or extended operation failed because it includes a value that is supposed to be a numeric object identifier but is not. A numeric object identifier consists of digits separated by periods. It must start with a digit and cannot have two periods in a row. Numeric object identifiers can be used in schema definitions and within entries. They are also contained in controls that are specified with the operation and in identifying extended operations.

In the message text:

**value**

Numeric object identifier

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Check the operation input to ensure that all numeric object identifiers are correctly formatted. Then reissue the operation.

---

R001046  Missing closing quote for value 'value'

Explaination: An LDAP schema modify operation failed because a quoted value does not end with a quotation mark in a schema definition. The part of the definition that is in error is indicated in the reason code. See LDAP directory schema for more information about the format for the definitions of the various elements of the schema.

In the message text:

**value**

Attribute or object class definition

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Check the modify input to ensure that all the schema definitions are complete and correctly formatted. Then reissue the operation.

---

R001047  Missing opening quote for value 'value'

Explaination: An LDAP schema modify operation failed because a quoted value does not begin with a quotation mark in a schema definition. The part of the definition that is in error is indicated in the reason code. See LDAP directory schema for more information about the format for the definitions of the various elements of the schema.

In the message text:

**value**

Attribute or object class definition

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Check the modify input to ensure that all the schema definitions are complete and correctly formatted. Then reissue the operation.

---

R001048  Missing closing brace for value 'value'

Explaination: An LDAP schema modify operation failed because a value that starts with an open brace does not end with a closing brace in a schema definition. The part of the definition that is in error is indicated in the reason code. See LDAP directory schema for more information about the format for the definitions of the various elements of the schema.

In the message text:

**value**

Attribute or object class definition

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Check the modify input to ensure that all the schema definitions are complete and correctly formatted. Then reissue the operation.

---

R001052  Non-numeric character found in integer value 'value'

Explaination: An LDAP operation failed because an attribute value involved in the operation contains a character that is not allowed by the Integer syntax of the attribute. An Integer value consists of one or more digits, optionally starting with a plus sign or minus sign. The value that is not valid is indicated in the reason code.

In the message text:

**value**

Attribute value

**System action:** The LDAP server continues to run, but the operation fails.
In the message text:

**name**

Object class name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Analyze the operation input to ensure that it does not involve adding or replacing an obsolete object class in the entry. Then reissue the operation.

---

**R001053**  
**Integer value of length** size **exceeds maximum length of** max_size

**Explanation:** An LDAP operation failed because an attribute value involved in the operation is too long for the Integer syntax of the attribute. The length of the value and the maximum length of an Integer value are indicated in the reason code.

In the message text:

size  
Integer value length

max_size  
Maximum integer length

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the value used in the operation input so that it is valid for the Integer syntax. Then reissue the operation.

---

**R001055**  
**Attribute type** 'name' **is not valid for the directory schema**

**Explanation:** An LDAP schema modify operation failed because it involves an attribute that is not supported for the schema entry. The schema entry itself contains a fixed set of attributes that can be changed, the most useful of which are: attributeTypes, ibmAttributeTypes, objectClasses, aclEntry, and entryOwner. The name of the attribute is indicated in the reason code.

In the message text:

name  
Attribute name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the value used in the operation input so that the length is valid for the Integer syntax. Then reissue the operation.

---

**R001060**  
**Object class** 'name' **is obsolete**

**Explanation:** An LDAP add, modify, or modify DN operation failed because it involves an object class that is marked as OBSOLETE in the schema. An obsolete object class cannot be added or replaced in an entry. The object class can be deleted from the entry. Note that an add or modify DN operation may try to add an obsolete object class if the object class is part of the new relative distinguished name (RDN) of the entry, because the LDAP server automatically adds the RDN attributes and values to the entry. The RDN is the leftmost part of the distinguished entry. The name of the obsolete object class is indicated in the reason code.

In the message text:

definition  
Object class definition

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the value used in the operation input so that it does not involve adding or replacing an obsolete object class in the entry. Then reissue the operation.
R001075  Object identifier missing in schema definition: definition

Explanation: An LDAP schema modify operation failed because there is a schema definition that does not include an object identifier. The definition that is in error is indicated in the reason code. The object identifier is required in all schema definitions. See [LDAP directory schema] for more information about the format for the definitions of the various elements of the schema.

In the message text:

- definition
  - Attribute or object class definition

System action: The LDAP server continues to run, but the operation fails.

User response: Check the modify input to ensure that all the schema definitions are complete and correctly formatted. Then reissue the operation.

R001076  Keyword specified multiple times in schema definition: definition

Explanation: An LDAP schema modify operation failed because the same keyword is specified more than once in a schema definition. The keyword and the definition that is in error are indicated in the reason code. See [LDAP directory schema] for more information about the format for the definitions of the various elements of the schema.

In the message text:

- keyword
  - Duplicated keyword

System action: The LDAP server continues to run, but the operation fails.

User response: Check the modify input to ensure that all the schema definitions are complete and correctly formatted. Then reissue the operation.

R001077  Keyword not supported in schema definition: definition

Explanation: An LDAP schema modify operation failed because it contains a keyword that is not supported in a schema definition. Note that unknown keywords are ignored if they occur in an ibmattributetypes definition, but not in other definitions. The keyword and the definition that is in error are indicated in the reason code. See [LDAP directory schema] for more information about the format for the definitions of the various elements of the schema.

In the message text:

- keyword
  - Keyword in definition

System action: The LDAP server continues to run, but the operation fails.

User response: Check the modify input to ensure that all the schema definitions are complete and correctly formatted. Then reissue the operation.

R001078  Value missing for keyword keyword in schema definition: definition

Explanation: An LDAP schema modify operation failed because it does not specify a value for a keyword in a schema definition. The keyword and the definition that is in error are indicated in the reason code. See [LDAP directory schema] for more information about the format for the definitions of the various elements of the schema.

In the message text:

- key
  - Keyword missing a value

System action: The LDAP server continues to run, but the operation fails.

User response: Check the modify input to ensure that all the schema definitions are complete and correctly formatted. Then reissue the operation.

R001079  Unsupported value for keyword keyword in schema definition: definition

Explanation: An LDAP schema modify operation failed because a schema definition contains a keyword value that is not supported for that keyword. The keyword and the definition that is in error are indicated in the reason code. Note that the acceptable values for the SYNTAX, EQUALITY, ORDERING, and SUBSTR keywords in an attribute definition depend on the compatibility level at which the server is running. See [LDAP directory schema] for more information about the format for the definitions of the various elements of the schema.

In the message text:

- keyword
  - Keyword in definition

System action: The LDAP server continues to run, but the operation fails.

User response: Check the modify input to ensure that all the schema definitions are complete and correctly formatted. Then reissue the operation.
formatted. Then reissue the operation. Contact an LDAP administrator if you must use values that are not supported by the compatibility level at which the LDAP server is running. After the problem is resolved, reissue the operation.

**Administrator response:** If the server is running at a compatibility level that does not support needed values, change the value of the `serverCompatLevel` option in the LDAP server configuration file. Then restart the LDAP server.

---

**R001080**  
**Attribute type 'identifier' is already defined**

**Explanation:** An LDAP schema modify operation failed because it tries to add an attribute definition with the same identifier as an attribute that is already in the schema or that is added in a previous modification in the schema modify operation. Two attributes cannot have the same identifier. The attribute identifier is indicated in the reason code.

In the message text:

`identifier`  
Attribute identifier

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Check the modify input to ensure that the identifier for each attribute being added is unique. Then reissue the operation.

---

**R001081**  
**Object class 'identifier' is already defined**

**Explanation:** An LDAP schema modify operation failed because it tries to add an object class definition with the same identifier as an object class that is already in the schema or that is added in a previous modification in the schema modify operation. Two object classes cannot have the same identifier. The object class identifier is indicated in the reason code.

In the message text:

`identifier`  
Object class identifier

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Check the modify input to ensure that the identifier for each object class being added is unique. Then reissue the operation.

---

**R001082**  
**Inappropriate type matching rule in schema definition: definition**

**Explanation:** An LDAP schema modify operation failed because an attribute definition specifies a value for a matching rule that is not appropriate for the matching rule. The matching rule type (EQUALITY, ORDERING, or SUBSTR) and the definition that is in error are indicated in the reason code. See the LDAP directory schema more information about the values that can be specified for each type of matching rule.

In the message text:

`type`  
Matching rule type

`definition`  
Attribute definition

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Check the modify input to ensure that all the schema definitions are complete and correctly formatted. Then reissue the operation.

---

**R001083**  
**Object class 'identifier' is not defined**

**Explanation:** An LDAP operation or utility failed because it involves an object class that is not defined in the schema. For a schema modify, an object class definition cannot reference an object class that does not exist in the schema or that is deleted in a previous modification in the modify operation. Similarly, an object class being deleted from the schema must exist in the schema, and must not be deleted in a previous modification. For an add operation to another backend and the `ldif2ds` utility, the object class specified in the entry must exist in the schema. The identifier of the object class is indicated in the reason code.

In the message text:

`identifier`  
Object class identifier

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Either add the object class to the schema or remove the object class from the operation input. Then reissue the operation.

---

**R001084**  
**IBM attribute type 'identifier' is not defined**

**Explanation:** An LDAP schema modify operation failed because it tries to delete an `ibmattributetypes` definition that does not exist or is already being deleted or whose corresponding `attributetypes` definition is being deleted in a previous modification in the modify operation. The numeric identifier of the `ibmattributetypes` definition is indicated in the reason code.

In the message text:

`identifier`  
IBM attributetypes numeric identifier

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the delete of the
ibmattributetypes definition from the modify input. Then reissue the operation.

**R001085** IBM attribute type 'identifier' is already defined

**Explanation:** An LDAP schema modify operation failed because it tries to add an ibmattributetypes definition that already exists or is already being added in a previous modification in the modify operation. The numeric identifier of the ibmattributetypes definition is indicated in the reason code.

In the message text:

**identifier**

ibmattributetypes numeric identifier

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the add of the ibmattributetypes definition from the modify input. Then reissue the operation.

**R001086** No syntax value specified for attribute type 'identifier'

**Explanation:** An LDAP schema modify operation failed because an attribute definition does not contain the SYNTAX keyword or the SUP keyword. The numeric identifier of the attribute definition in error is indicated in the reason code. Every attribute must have a syntax, either specified directly using the SYNTAX keyword or derived by inheritance by specifying the SUP keyword. See [LDAP directory schema](#) for more information about the values that can be specified for an attribute definition.

In the message text:

**identifier**

Attribute numeric identifier

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Check the modify input to ensure that all the schema definitions are complete and correctly formatted. Then reissue the operation.

**R001087** Attribute type 'identifier' is in use and cannot be replaced or deleted

**Explanation:** An LDAP schema modify operation failed because it tries to delete or change the definition of an attribute that is in use by some entry in a backend directory. The modification cannot be made because it could make the values in the entry no longer valid. The identifier of the object class is indicated in the reason code.

In the message text:

**identifier**

Object class identifier

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the modification from the modify input. Then reissue the operation. Alternatively, remove usage of the object class from all the entries that are currently using it. This involves searching the entire LDAP server for entries that contain that attribute and then modifying each of the entries to remove the attribute. This might not be possible if the attribute is required by an object class in an entry. Then reissue the original operation. For the special attributes in CDBM entries, see Advanced replication for more information.

**R001088** Object class 'identifier' is in use and cannot be replaced or deleted

**Explanation:** An LDAP schema modify operation failed because it tries to delete or change the definition of an object class that is in use by some entry in a backend directory. The modification cannot be made because it could make the values in the entry no longer valid. The identifier of the object class is indicated in the reason code.

In the message text:

**identifier**

Object class identifier

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the modification from the modify input. Then reissue the operation. Alternatively, remove usage of the object class from all the entries that are currently using it. This involves searching the entire LDAP server for entries that contain that object class and then modifying each of the entries to remove the object class and any attributes that are included only in that object class in the entry. Then reissue the original operation.

**R001089** Attribute type name 'name' is already assigned

**Explanation:** An LDAP schema modify operation failed because the name used in an attribute definition conflicts with the name used by an existing attribute or by an attribute added by a previous modification in the modify operation. The attribute name is indicated in the reason code.

In the message text:

**name**

Attribute type name

**Management, cn=configuration** entry cannot be changed if these values are in use. The identifier of the attribute is indicated in the reason code.

In the message text:

**identifier**

Attribute identifier

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the modification from the modify input. Then reissue the operation. Alternatively, remove usage of the attribute from all the entries that are currently using it. This involves searching the entire LDAP server for entries that contain that attribute and then modifying each of the entries to remove the attribute. This might not be possible if the attribute is required by an object class in an entry. Then reissue the original operation. For the special attributes in CDBM entries, see Advanced replication for more information.
**R001090 • R001095**

**name**

---

**Attribute name**

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Check the modify input to ensure that the names for each attribute being added are unique. Then reissue the operation.

---

**R001090**

Object class name 'name' is already assigned

**Explanation:** An LDAP schema modify operation failed because the name used in an object class definition conflicts with the name used by an existing object class or by an object class added by a previous modification in the modify operation. The object class name is indicated in the reason code.

In the message text:

```
name
Object class name
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Check the modify input to ensure that the names for each object class being added are unique. Then reissue the operation.

---

**R001091**

TOP object class not found in superior hierarchy for 'identifier'

**Explanation:** An LDAP schema modify operation failed because the object class named TOP in its superior hierarchy. Every structural object class definition (one in which the ABSTRACT or AUXILIARY keywords are not specified) must include a SUP keyword and the superior chain must eventually include object class TOP. The numeric identifier of the object class definition in error is indicated in the reason code.

In the message text:

```
identifier
Deleted attribute numeric identifier
```

**User response:** Remove the modification that deletes the attribute definition from the modify input. Then reissue the operation. If that is the case, you must remove usage of the referencing attributes or object classes from all the entries that are currently using them. Then reissue the operation.

---

**R001092**

Unable to save directory schema

**Explanation:** An LDAP schema modify operation failed because the modified schema cannot be saved to the schema database.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Use any server messages and ERROR debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

---

**R001094**

Attribute type 'identifier1' is referenced by 'identifier2' and cannot be deleted

**Explanation:** An LDAP schema modify operation failed because it is deleting an attribute definition of an attribute that is used as a SUP value in another attribute or as a MUST or MAY value in an object class. The numeric identifiers of the attribute being deleted and the attribute or object class that references it are indicated in the reason code.

In the message text:

```
identifier1
Deleted attribute numeric identifier
```

```
identifier2
Referencing attribute or object class numeric identifier
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the modification that deletes the attribute definition from the modify input. Then reissue the operation. If that is the case, you must remove usage of the referencing attributes or object classes from all the entries that are currently using them. Then reissue the operation.

---

**R001095**

Object class 'identifier1' is referenced by 'identifier2' and cannot be deleted

**Explanation:** An LDAP schema modify operation failed because it is deleting an object class that is used as a SUP value in another object class. The numeric identifiers of the object class being deleted and the object class that references it are indicated in the reason code.

In the message text:
Deleted object class numeric identifier

Referencing object class numeric identifier

System action: The LDAP server continues to run, but the operation fails.

User response: Remove the modification that deletes the object class from the schema modify input. Then reissue the schema modify operation.

R001096  OID change not allowed because the new definition is not the same as the current definition

Explanation: An LDAP schema modify operation to change the numeric identifier of an attribute or object class failed because it also changes some other part of the attribute or object class definition that cannot be changed. For an attribute numeric identifier change, the values of the NAME, SUP, EQUALITY, ORDERING, SUBSTR, and SYNTAX keywords cannot be changed. Also, the SINGLE-VALUE keyword cannot be specified in the new definition if it is not also in the current definition. For an object class numeric identifier change, the values of the NAME, SUP, MUST, and MAY keywords cannot be changed.

System action: The LDAP server continues to run, but the operation fails.

User response: Change the modify input so that the definition of the new attribute or object class does not change any of the keywords listed above. Then reissue the operation.

R001097  Attribute type 'identifier' conflicts with existing type, cannot be replaced for migration

Explanation: A migration of the TDBM schema failed because the current schema contains a different definition for an attribute than is in the TDBM schema to be migrated. As a result, TDBM entries using the attribute might not be valid under the current schema definition of the attribute. The numeric identifier of the attribute is indicated in the reason code.

In the message text:

identifier  Attribute numeric identifier

System action: The TDBM backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the LDAP server ends.

Administrator response: Analyze the difference between the object class definition in the LDAP schema and in the TDBM schema. Resolve the problem by modifying the definition in one of the two places. Then restart the LDAP server if it stopped or if the TDBM backend is needed.

R001098  Object class 'identifier' conflicts with existing class, cannot be replaced for migration

Explanation: A migration of the TDBM schema failed because the current schema contains a different definition for an object class than is in the TDBM schema to be migrated. As a result, TDBM entries using the object class might not be valid under the current schema definition of the object class. The numeric identifier of the object class is indicated in the reason code.

In the message text:

identifier  Object class numeric identifier

System action: The TDBM backend does not start. If the srvStartUpError option in the LDAP server configuration file is set to ignore, the LDAP server continues to run with those backends that successfully start. If the srvStartUpError option is set to terminate (this is the default if the configuration option is not specified), the LDAP server ends.

Administrator response: Analyze the difference between the object class definition in the LDAP schema and in the TDBM schema. Resolve the problem by modifying the definition in one of the two places. Then restart the LDAP server if it stopped or if the TDBM backend is needed.

R001099  Duplicate values specified for attribute 'name'

Explanation: An LDAP schema modify operation failed because it specifies a duplicate value for a schema attribute, such as aclEntry or entryOwner. The name of the attribute is indicated in the reason code.

Note that two aclEntry values or two entryOwner values are the same if they contain the same distinguished name, even if other parts of the values are different.

In the message text:

name  Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Remove the duplicate value from the modify input. Then reissue the operation.
Syntax specified in attribute 'identifier' is not valid when RACFFIELD is included in IBM attribute type

Explanation: An LDAP schema modify operation failed because of one of the following:

- An ibmattributetypes definition contains the RACFFIELD keyword but the syntax of the corresponding attribute is not IA5 String.
- An attribute definition sets the attribute syntax to something other than IA5 String, but the corresponding ibmattributetypes definition contains the RACFFIELD keyword.

When the RACFFIELD keyword is specified in an ibmattributetypes definition, the syntax of the associated attribute definition (the one with the same numeric identifier) must be IA5 String, as specified directly in the SYNTAX keyword or as derived from the superior hierarchy created by the SUP keyword. The numeric identifier of the ibmattributetypes or the attribute definition in error is indicated in the reason code.

In the message text:

identifier
Attribute numeric identifier

System action: The LDAP server continues to run, but the operation fails.

User response: Depending on which definition is in error, either remove the RACFFIELD keyword from the ibmattributetypes definition or change the attribute definition to use the IA5 String syntax. Then reissue the operation.

Duplicate value for name in RACFFIELD in IBM attribute types 'identifier1' and 'identifier2'

Explanation: An LDAP schema modify operation failed because it tries to add an ibmattributetypes definition with the same RACFFIELD name value as is already in an existing ibmattributetypes definition or in a previous ibmattributetypes definition in the modify operation. The name part of the RACFFIELD value must be unique within the schema. The numeric identifiers of the two ibmattributetypes definitions are indicated in the reason code.

In the message text:

identifier1
First ibmattributetypes numeric identifier

identifier2
Second ibmattributetypes numeric identifier

System action: The LDAP server continues to run, but the operation fails.

User response: Remove the duplicate ibmattributetypes definition from the modify input or change its RACFFIELD value to be unique. Then reissue the operation.

Value 'value' specified for attribute 'name' is not valid. Schema Description:
description

Explanation: An LDAP operation failed because it uses an attribute value that is not acceptable for that attribute. The syntax and equality matching rule of the attribute determine what values are valid for the attribute. The value, attribute name, and description of the attribute (from the attribute definition in the schema) are indicated in the reason code.

In the message text:

value
Attribute value

name
Attribute name

description
Attribute description

System action: The LDAP server continues to run, but the operation fails.

User response: Use the attribute description to correct the value used in the operation input so that it is valid for the attribute. Then reissue the operation.

Syntax or matching rule specified in attribute 'name' is not supported at compatibility level level

Explanation: The LDAP server or utility cannot load the schema because the schema contains an attribute that uses a syntax or matching rule that is not valid when the LDAP server or utility is running at the current compatibility level. The name of the attribute and the current server compatibility level are indicated in the reason code. Some syntaxes and matching rules are not supported when the LDAP server is running at lower compatibility levels. See LDAP directory schema for more information about syntaxes and matching rules. Also see the serverCompatLevel option in Customizing the LDAP server configuration for more information about setting the server compatibility level.

In the message text:

name
Attribute name or numeric identifier

level
Server compatibility level

System action: The LDAP server or utility ends.

Administrator response: Set the serverCompatLevel option in the LDAP server configuration file to a value that supports all the syntaxes and matching rules used in the schema. Then restart the LDAP server.
R001104 Numeric String value 'value' is not valid

Explanation: An LDAP operation failed because an attribute value involved in the operation contains a character that is not allowed by the Numeric String syntax of the attribute. A complete Numeric String value must be a list of space-separated numbers, and must contain at least one number. An example is 1 524 44. A substring value used in a substring filter can be any part of the complete value, and can be just spaces. An example is 24 4 The value that is not valid is indicated in the reason code.

In the message text:

value

Attribute value

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the value used in the operation input so that it is valid for the Numeric String syntax. Then reissue the operation.

R001105 Facsimile Telephone Number value 'value' is not valid

Explanation: An LDAP operation failed because an attribute value involved in the operation contains a character that is not allowed by the Facsimile Telephone Number syntax of the attribute. The characters that can be used in a Facsimile Telephone Number value are: letters, numbers, quote, open parens, close parens, plus sign, comma, dash, period, forward slash, colon, question mark, and space. The value that is not valid is indicated in the reason code.

In the message text:

value

Attribute value

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the value used in the operation input so that it is valid for the Facsimile Telephone Number syntax. Then reissue the operation.

R001106 Telex Number value 'value' is not valid

Explanation: An LDAP operation failed because an attribute value involved in the operation contains a character that is not allowed by the Telex Number syntax of the attribute. The characters that can be used in a Telex Number value are: letters, numbers, quote, open parens, close parens, plus sign, comma, dash, period, forward slash, colon, question mark, and space. The value that is not valid is indicated in the reason code.

In the message text:

value

Attribute value

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the value used in the operation input so that it is valid for the Telex Number syntax. Then reissue the operation.

R001107 Printable String value 'value' is not valid

Explanation: An LDAP operation failed because an attribute value involved in the operation contains a character that is not allowed by the Printable String syntax of the attribute. The characters that can be used in a Printable String value are: letters, numbers, quote, open parens, close parens, plus sign, comma, dash, period, forward slash, colon, question mark, and space. The value that is not valid is indicated in the reason code.

In the message text:

value

Attribute value

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the value used in the operation input so that it is valid for the Printable String syntax. Then reissue the operation.

R001108 ibm-slapdSAFSecurityDomain value 'value' is too long

Explanation: An LDAP operation failed because the value specified for the ibm-slapdSAFSecurityDomain attribute is more than 228 characters long. This is determined by the maximum length of a RACF general resource class (246 characters) and the length of the fixed fields (.ADMINROLE.) (11 characters) and the length of the longest administrative role (DIRDATA) (7 characters).

In the message text:

value

Attribute value

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the value used in the operation input so that it is valid for the ibm-slapdSAFSecurityDomain attribute. Then reissue the operation.

R001109 'name' value 'value' contains a character 'character' that is not valid.

Explanation: An LDAP operation failed because the value for the specified attribute type contains a character that is not valid. If the attribute type is
R002001  Missing equal sign in DN component 'component'

Explanation: An LDAP operation failed because it involves a distinguished name (DN) in which one of the components has an attribute without a value. The equal sign (=) which indicates the end of the attribute name and the beginning of the value is missing. For example, in the DN cn=fred,ou=test,o=ibm, the ou=test,o=ibm component contains an attribute (oudeptG1) without a value, because the equal sign after ou is missing. The component with the missing equal sign is indicated in the reason code.

In the message text:

component  Component of the DN
System action: The LDAP server continues to run, but the operation fails.
User response: Correct the operation input so that all the distinguished names that it uses are complete. Then reissue the operation.

R002004  Incomplete escape sequence in DN component 'component'

Explanation: An LDAP operation failed because it involves a distinguished name (DN) in which one of the components has started an escape sequence with a double quotation mark (") but there is no corresponding double quotation mark to end the sequence. For example, in the DN cn=fred,ou="test,o=ibm, the ou="test,o=ibm component contains an incomplete escape sequence ("test,o=ibm). The component with the incomplete escape sequence is indicated in the reason code.

In the message text:

name  Attribute name
value  Attribute value

System action: The LDAP server continues to run, but the operation or utility fails.
User response: Correct the operation or utility input so that all values for the attribute are valid. Then reissue the operation or restart the utility.

R002008  Permissions missing in aclEntry attribute value 'value'

Explanation: An LDAP operation or utility failed because it involves an aclEntry attribute value that specified an access class without permissions. For example, cn=fred,o=ldbm:normal::rws contains an access class (normal) without permissions. See [Using access control] for more information about the syntax of values for aclEntry and entryOwner attributes. The attribute value is indicated in the reason code.

In the message text:

value  Attribute value
System action: The LDAP server continues to run, but the operation or utility fails.

User response: Correct the operation or utility input so that all values for the aclEntry attribute are valid. Then reissue the operation or restart the utility.

R002018 An extraneous colon was found in aclEntry attribute value 'value'

Explanation: An LDAP operation or utility failed because it involves an aclEntry attribute value that contains an extra colon. For example, cn=fred, o=ldbm: normal:: contains an extra colon, where the normal access permissions should be. See [Using access control] for more information about the syntax of values for this attribute. The attribute value is indicated in the reason code.

In the message text:
value
Attribute value

System action: The LDAP server continues to run, but the operation or utility fails.

User response: Correct the operation or utility input so that all values for the aclEntry attribute are valid. Then reissue the operation or restart the utility.

R002019 An unsupported extensible filter was specified

Explanation: An LDAP operation or utility failed because an extensible search filter was specified in an attribute value or on a search request. Extensible search filters are not supported in the z/OS LDAP server. Search filters can be specified in aclEntry, entryOwner, and memberURL attribute types.

System action: The LDAP server continues to run, but the operation or utility fails.

User response: Correct the operation or utility input so that LDAP search operation or attribute value does not specify an extensible search filter. Then reissue the operation or restart the utility.

R002020 An error occurred while base64-decoding attribute 'name'

Explanation: An LDAP operation or utility failed because a value for the attribute type could not be base64 decoded. The attribute value may already exist in the directory (for example Salted SHA, SHA-2, or Salted SHA-2 userPassword values) or was specified in an LDAP operation or utility input. The attribute type is indicated in the reason code.

In the message text:
name
Attribute name

System action: The LDAP server continues to run, but the operation or utility fails.

User response: Correct the operation or utility input so that attribute value specifies a value that is base64 encoded properly. If the attribute value exists in the directory, the value may have to be replaced with a valid value. Then reissue the operation or restart the utility.

R002021 An incorrectly formatted 'name' attribute value has been encountered

Explanation: An LDAP operation or utility failed because a value for the attribute type is not correctly formatted. If the attribute type is userPassword or ibm-slapdAdminPw and the value is hashed or encrypted value, verify the following:

- If the value has an {MD5} encryption tag, the length of data after the tag must be 16 bytes or 24 bytes long.
- If the value has an {SHA} encryption tag, the length of data after the tag must be 20 bytes or 28 bytes long.
- If the value has an {SSHA} encryption tag, the length of data after the tag must be at least 20 bytes long.
- If the value has an {SHA224}, {SHA256}, {SHA384}, or {SHA512} encryption tag, the length of data after the tag must be 40, 44, 64, 88 bytes long respectively.
- If the value has an {SSHA224}, {SSHA256}, {SSHA384}, or {SSHA512} encryption tag, the length of data after the tag must be at least 40, 44, 64, 88 bytes long respectively.

The attribute value is indicated in the reason code.

In the message text:
name
Attribute name

System action: The LDAP server continues to run, but the operation or utility fails.

User response: Correct the operation or utility input so that all values for the attribute are valid. Then reissue the operation or restart the utility.

R002033 IP address 'value' is not valid

Explanation: An LDAP operation or utility failed because an IP address specified in a search filter in an aclEntry or entryOwner attribute is not valid. The IP address is specified in an ACL filter when using the ibm-filterIP attribute. See [Using access control] for more information about the syntax of values for this attribute. The IP address that is not valid is indicated in the reason code.

In the message text:
value
IP address
**System action:** The LDAP server continues to run, but the operation or utility fails.

**User response:** Correct the operation or utility input so that all values for the aclEntry or entryOwner attribute are valid. Then reissue the operation or restart the utility.

---

**R002034** Attribute type 'name' only supports a trailing wildcard

**Explanation:** An LDAP operation or utility failed because an IP address in the specified attribute type only supports a trailing wildcard character (*). If using the ibm-filterIP attribute type in an ACL filter, see [Using access control](#) for more information about the syntax of values for this attribute. The attribute type that is not valid is indicated in the reason code.

In the message text:

- name
  - Attribute name

**System action:** The LDAP server continues to run, but the operation or utility fails.

**User response:** Correct the operation or utility input so that all values for the attribute type are valid. Then reissue the operation or restart the utility.

---

**R002035** Unable to convert timestamp 'value' to time_t

**Explanation:** An LDAP operation or utility failed because an error occurred when attempting to convert the timestamp to a time_t structure. The timestamp value may be a password policy timestamp attribute type, createTimestamp, or modifyTimestamp attribute values. The timestamp is indicated in the reason code.

In the message text:

- value
  - Timestamp value

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the attribute from the entry DN in the add input or from the new relative distinguished name in the modify DN input. Then reissue the operation.

---

**R003030** The 'name' attribute cannot be used in the entry distinguished name

**Explanation:** An LDAP add operation failed because the distinguished name (DN) of the entry contains an attribute that is not allowed in a DN. In particular, the aclEntry, aclPropagate, entryOwner, and ownerPropagate attributes are not supported in a DN. Note that a modify DN operation may cause this error if it specifies an attribute that is not supported in the new relative distinguished name for the renamed entry. The name of the attribute is indicated in the reason code.

In the message text:

- name
  - Attribute name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the attribute from the entry DN in the add input or from the new relative distinguished name in the modify DN input. Then reissue the operation.

---

**R003032** The ownerPropagate attribute requires the entryOwner attribute

**Explanation:** An LDAP add or modify operation failed because it sets the ownerPropagate attribute but the entry does not contain any entryOwner attribute values. The attribute to control propagation of the entry owner values cannot be specified if there are no entry owner values in the entry. See [Using access control](#) for more information about LDAP access control.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the ownerPropagate attribute from the operation input. Then reissue the operation.

---

**R003057** Access denied because user does not have 'add' permission for the parent entry

**Explanation:** An LDAP add operation failed because the requester does not have add permission in the parent entry for the entry being added. Add permission is required to create an entry under the parent entry. The requester's authority is determined using the aclEntry and entryOwner attribute values associated with the parent of the new entry. See [Using access control](#) for more information about LDAP access control.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the aclPropagate attribute from the operation input. Then reissue the operation.
for more information about LDAP access control.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator to grant add permission to the parent entry. Then reissue the operation.

**Administrator response:** Modify the aclEntry values for the parent entry to give the requester add permission. To determine the authority a bound user has in the directory, use the `ldapexop` utility.

---

**R003062** Access denied because user does not have 'write' permission for all attributes in the new entry

**Explanation:** An LDAP add operation failed because the requester does not have write permission for all the attributes being added. Note that this includes the attributes in the relative distinguished name (RDN) of the entry, because the LDAP server automatically adds the RDN attributes and values to the entry. The RDN is the leftmost part of the distinguished name. The requester's authority is determined using the aclEntry and entryOwner attribute values associated with the parent of the new entry. See [Using access control](#) for more information about LDAP access control.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator to grant write permission to the parent entry. Then reissue the operation.

**Administrator response:** Modify the aclEntry values for the parent entry to give the requester write permission. To determine the authority a bound user has in the directory, use the `GetEffectiveACL` extended operation in the `ldapexop` utility.

---

**R003076** Access denied because user does not have 'delete' permission for the entry

**Explanation:** An LDAP delete operation or a modify DN operation which is moving an entry to another subtree failed because the requester does not have delete permission for the parent of the entry being deleted or moved. Moving an entry involves deleting the entry from its current parent and adding the entry under its new parent. When deleting or moving an entry, the requester must have delete permission in the parent entry. The requester's authority is determined using the aclEntry and entryOwner attribute values associated with the parent entry. See [Using access control](#) for more information about LDAP access control.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator to grant delete permission to the entry. Then reissue the operation.

**Administrator response:** Modify the aclEntry values for the entry to give the requester delete permission. To determine the authority a bound user has in the directory, use the `GetEffectiveACL` extended operation in the `ldapexop` utility.

---

**R003070** Access denied because user does not have 'write' permission for all modified attributes

**Explanation:** An LDAP modify operation failed because the requester does not have write permission for all the attributes being modified. The requester's authority is determined using the aclEntry and entryOwner attribute values associated with the entry being modified. See [Using access control](#) for more information about LDAP access control.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator to grant write permission to the entry. Then reissue the operation.

**Administrator response:** Modify the aclEntry values for the entry to give the requester write permission to these values To determine the authority a bound user has in the directory, use the `GetEffectiveACL` extended operation in the `ldapexop` utility.
R003095  Access denied because user does not have 'compare' permission for the attribute

Explanation: An LDAP compare operation failed because the requester does not have compare permission for the attribute being compared. The requester's authority is determined using the aclEntry and entryOwner attribute values associated with the entry that is the target of the compare operation. See [Using access control] for more information about LDAP access control.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator to grant compare permission to the entry. Then reissue the operation.

Administrator response: Modify the aclEntry values for the entry to give the requester compare permission. To determine the authority a bound user has in the directory, use the GetEffectiveACL extended operation in the ldapexop utility.

R003119  Access denied because user does not have 'write' permission for all attributes in the new name

Explanation: An LDAP modify DN operation failed because it does not have write permission to add the attributes in the new relative distinguished name (the RDN is the leftmost part of the distinguished name) of the entry being renamed. The attribute values in the RDN must always be part of the entry and are automatically added by the LDAP server to the entry. The requester must have write permission for each of these attributes in the entry being renamed. The requester's authority is determined using the aclEntry and entryOwner attribute values associated with the entry. See [Using access control] for more information about LDAP access control.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator to grant write permission to the entry. Then reissue the operation.

Administrator response: Modify the aclEntry values for the entry to give the requester write permission. To determine the authority a bound user has in the directory, use the GetEffectiveACL extended operation in the ldapexop utility.

R003128  Unable to realign DN attributes because user does not have 'write' permission for attributes in 'name'

Explanation: An LDAP modify DN operation which includes the control to realign other distinguished name (DN) attributes failed because the requester does not have write permission for an attribute that is being realigned. Realignment results in changing the original DN of the entry being renamed to the new DN of the entry in all the entries where the original DN occurs in a value of an aclEntry attribute, entryOwner attribute, or attribute with Distinguished Name syntax. The requester must have write permission for each attribute being changed in those entries. The requester's authority is determined using the aclEntry and entryOwner attribute values associated with each of those entries. See [Using access control] for more information about LDAP access control. The DN of the entry where the requester lacks write permission is indicated in the reason code.

In the message text:

name

Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator to grant write permission to the entries affected by realignment. Then reissue the operation.

Administrator response: Modify the aclEntry values for each of the entries affected by realignment to give the requester write permission. To determine the authority a bound user has in the directory, use the GetEffectiveACL extended operation in the ldapexop utility.
R003129  Realigning DN attributes would result in duplicate values for attribute 'name' in 'entry'

Explanation: An LDAP modify DN operation which includes the control to realign other distinguished name (DN) attributes failed because realigning an attribute value creates a duplicate value in some entry. Realignment results in changing the original DN of the entry being renamed to the new DN of the entry in all the entries where the original DN occurs in a value of an aclEntry attribute, entryOwner attribute, or attribute with Distinguished Name syntax. The new value must not already exist in the attribute. The name of the attribute with the duplicate value and the DN of the entry containing the attribute are indicated in the reason code.

In the message text:

name  Attribute name

entry  Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: Remove the duplicate attribute value from the entry. Then reissue the operation.

R003130  Filter included with an aclEntry or entryOwner attribute is not valid: 'filter'

Explanation: An LDAP operation or utility failed because an ACL filter specified in an aclEntry or entryOwner attribute value is not valid. See Using access control for more information about the supported ACL search filters. The value that is not valid is indicated in the reason code.

In the message text:

filter  Filter value

System action: The LDAP server continues to run, but the operation or utility fails.

User response: Correct the operation or utility input so that the value is valid. Then reissue the operation or restart the utility.

R003131  Access control filter attribute type 'name' is not defined

Explanation: An LDAP operation or utility failed because an ACL filter specified in an aclEntry or entryOwner attribute value contains attribute types that are not in the schema. See Using access control for more information about the supported ACL search filters. The attribute type that is not valid is indicated in the reason code.

R003132  Normalization failed for access control filter attribute type 'name'

Explanation: An LDAP operation or utility failed because an ACL filter specified in an aclEntry or entryOwner attribute value cannot be normalized. See Using access control for more information about the supported ACL search filters. The attribute type that is not valid is indicated in the reason code.

In the message text:

name  Attribute name

System action: The LDAP server continues to run, but the operation or utility fails.

User response: Correct the operation or utility input so that a valid ACL filter is specified. Then reissue the operation or restart the utility.

R003133  Normalization failed for access control filter substring type 'type'

Explanation: An LDAP operation or utility failed because an ACL filter specified in an aclEntry or entryOwner attribute value cannot be substring normalized. See Using access control for more information about the supported ACL search filters. The attribute type that is not valid is indicated in the reason code.

In the message text:

type  Substring type

System action: The LDAP server continues to run, but the operation or utility fails.

User response: Correct the operation or utility input so that a valid ACL filter is specified. Then reissue the operation or restart the utility.

R003134  Access control filter attribute type 'name' does not have an equality matching rule

Explanation: An LDAP operation or utility failed because an ACL filter specified in an aclEntry or entryOwner attribute value does not have an equality matching rule specified in the schema. See Using access control for more information about the supported ACL search filters. The attribute type that is not valid is
indicated in the reason code.

In the message text:

**name**
Attribute name

**System action:** The LDAP server continues to run, but the operation or utility fails.

**User response:** Correct the operation or utility input so that a valid ACL filter is specified. Then reissue the operation or restart the utility.

---

**R003136** Value specified for access control filter attribute type 'name' is not valid

**Explanation:** An LDAP operation or utility failed because an ACL filter specified in an aclEntry or entryOwner attribute value is not valid. See [Using access control](#) for more information about the supported ACL search filters. The attribute type that is not valid in the ACL filter is indicated in the reason code.

In the message text:

**name**
Attribute name

**System action:** The LDAP server continues to run, but the operation or utility fails.

**User response:** Correct the operation or utility input so that a valid ACL filter is specified. Then reissue the operation or restart the utility.

---

**R003137** Attribute type 'name' cannot be specified within an access control filter

**Explanation:** An LDAP operation or utility failed because an ACL filter specified in an aclEntry or entryOwner attribute value is not valid. See [Using access control](#) for more information about the supported ACL search filters. The attribute type that is not valid in the ACL filter is indicated in the reason code.

In the message text:

**name**
Attribute name

**System action:** The LDAP server continues to run, but the operation or utility fails.

**User response:** Correct the operation or utility input so that a valid ACL filter is specified. Then reissue the operation or restart the utility.

---

**R003138** Operation not specified or not valid in aclFilter 'filter'

**Explanation:** An LDAP operation or utility failed because the aclFilter component of an aclEntry value does not specify an operation or the operation specified is not valid. See [Using access control](#) for more information about the supported ACL search filters. The aclFilter component that is not valid is indicated in the reason code.

In the message text:

**filter**
Filter value

**System action:** The LDAP server continues to run, but the operation or utility fails.

**User response:** Correct the operation or utility input so that a valid operation is specified for the aclFilter component. Then reissue the operation or restart the utility.

---

**R003139** Mode not specified or not valid in ownerFilter 'filter'

**Explanation:** An LDAP operation or utility failed because the ownerFilter component of an entryOwner value does not specify a mode or the mode specified is not valid. See [Using access control](#) for more information about the supported ACL search filters. The ownerFilter component that is not valid is indicated in the reason code.

In the message text:

**filter**
Filter value

**System action:** The LDAP server continues to run, but the operation or utility fails.

**User response:** Correct the operation or utility input so that a valid operation is specified for the ownerFilter component. Then reissue the operation or restart the utility.

---

**R003141** Entry 'name' is a referral entry. Effective ACL information cannot be retrieved for a referral

**Explanation:** The GetEffectiveAcl extended operation failed because a referral entry is encountered and effective ACL information cannot be obtained for a referral entry. The entry is indicated in the reason code.

In the message text:

**name**
Distinguished name of entry

**System action:** The LDAP server continues to run, but the operation or utility fails.

**User response:** Correct the GetEffectiveAcl extended operation so that the effective ACL information is not retrieved for the referral entry. The GetEffectiveAcl extended operation must be run against the referral server to obtain the effective ACL information. Then reissue the operation.
R003142 Unable to build a filter string from a filtered value

Explanation: An LDAP operation or utility failed because an ACL filter specified in an aclEntry or entryOwner attribute value cannot be normalized. See Using access control for more information about the supported ACL search filters.

System action: The LDAP server continues to run, but the operation or utility fails.

User response: Correct the operation or utility input so that a valid ACL filter is specified. Then reissue the operation or restart the utility. If the problem persists, contact an LDAP administrator.

Administrator response: Use the information in server messages and ERROR debug trace output to assist in locating and correcting the problem.

R003143 Only an LDAP administrator can execute Get Effective ACL extended operation

Explanation: A GetEffectiveAcl extended operation failed because it is only allowed to be ran by an LDAP root, schema, or server configuration administrator.

System action: The LDAP server continues to run, but the operation or utility fails.

User response: Authenticate as an LDAP root, schema, or server configuration administrator. Then reissue the operation or restart the utility.

Administrator response: Use the information in server messages and ERROR debug trace output to assist in locating and correcting the problem.

R003144 Bind DN not specified for SimpleCramDigestBind sequence

Explanation: A GetEffectiveAcl extended operation failed because a bind distinguished name (DN) must be specified in the SimpleCramDigestBind sequence when simulating a CRAM-MD5 or DIGEST-MD5 bind.

System action: The LDAP server continues to run, but the operation or utility fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Use the information in server messages and ERROR debug trace output to assist in locating and correcting the problem.

R003145 Kerberos principal@realm not specified for gssApiBind sequence

Explanation: A GetEffectiveAcl extended operation failed because a Kerberos principal must be specified in the gssApiBind sequence when simulating a GSSAPI (Kerberos) bind.

System action: The LDAP server continues to run, but the operation or utility fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Use the information in server messages and ERROR debug trace output to assist in locating and correcting the problem.

R003146 Certificate subject DN not specified for externalBind sequence

Explanation: A GetEffectiveAcl extended operation failed because a certificate subject distinguished name (DN) must be specified in the externalBind sequence when simulating a SASL EXTERNAL bind.

System action: The LDAP server continues to run, but the operation or utility fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Use the information in server messages and ERROR debug trace output to assist in locating and correcting the problem.

R003147 The value 'value' passed to the Get Effective ACL extended operation is not valid

Explanation: A GetEffectiveAcl extended operation failed because a value specified in the request is not valid. See the GetEffectiveAcl description for the ldapexop utility in Running and using the LDAP server utilities for more information about the options and their values. The value that is not valid is indicated in the reason code.

In the message text:
value

Extended operation value

System action: The LDAP server continues to run, but the utility ends.

User response: Correct the utility input. Then restart the utility.

R003148 Decode of Get Effective ACL extended operation request failed.

Explanation: A GetEffectiveAcl extended operation failed because the extended operation cannot be decoded. The format or contents of the extended operation are not valid. A text string explaining the problem is included in the reason code.
R003149  Encode of Get Effective ACL extended operation response failed. reason

Explanation: A GetEffectiveAcl extended operation failed because the extended operation response cannot be encoded. A text string explaining the problem is included in the reason code.

In the message text:

reason
Reason for encode failure

System action: The LDAP server continues to run, but the operation or utility fails.
User response: Correct the operation or utility input so that a valid aclEntry attribute value is specified. Then reissue the operation.
Administrator response: If filtered attribute values are to be supported, update the serverCompatLevel option in the LDAP server configuration file to the minimum level specified in the message. Then restart the server or utility.

R003150 A filtered 'name1' value cannot be added or modified. Filtered 'name2' values require minimum serverCompatLevel level

Explanation: An LDAP operation or utility failed because a filtered attribute value was specified in an attribute type that requires a minimum server compatibility level. The filtered attribute type and the minimum server compatibility level are indicated in the reason code.

In the message text:

name1
Attribute name
name2
Attribute name
level
Minimum compatibility level

System action: The LDAP server continues to run, but the operation or utility fails.
User response: Either correct the operation or utility input so that a filter is not specified in the attribute type or contact an LDAP administrator to update the server compatibility to the minimum level specified. Then reissue the operation or restart the utility.
Administrator response: Update the serverCompatLevel option in the LDAP server configuration file to the minimum level specified in the message. Then restart the server or utility.

R004017 No attributes specified for entry 'name'

Explanation: An LDAP add operation failed because it does not contain any attributes to include in the entry. All entries must have at least the objectClass attribute. The distinguished name of the entry is indicated in the reason code.

In the message text:

name
Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.
User response: Add the appropriate attributes to the add input. Then reissue the operation.

R004019 Entry data is missing required RDN components

Explanation: An LDAP modify operation failed because it changes or deletes attribute values that are in the relative distinguished name (RDN) of the entry. The RDN is the leftmost part of the distinguished name. Every attribute and value in the RDN must also be in
the entry and cannot be removed unless the entry is renamed.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the modify input so that it does not remove the attribute values that are in the RDN. Then reissue the operation.

---

### R004020 RDN contains duplicate values for attribute 'name'

**Explanation:** An LDAP operation failed because it involves a distinguished name (DN) that contains the same attribute value twice in the relative distinguished name (RDN). The RDN is the leftmost part of the DN. The name of the attribute is indicated in the reason code.

In the message text:

- **name**: Attribute name

- **System action:** The LDAP server continues to run, but the operation ends.

**User response:** Remove the duplicate attribute value from the distinguished name in the operation input. Then reissue the operation.

---

### R004022 Parent not found for entry 'name'

**Explanation:** An LDAP operation failed because the parent entry could not be found in the backend. The parent entry must exist for the LDAP operation to succeed. The distinguished name (DN) of the entry whose parent does not exist name is indicated in the reason code.

In the message text:

- **name**: Distinguished name of entry

**System action:** The LDAP server continues to run, but the search operation ends.

**User response:** If the distinguished name of the entry specified in the LDAP operation or the utility is correct. Then reissue the operation or restart the utility.

---

### R004031 Search time limit exceeded

**Explanation:** An LDAP search operation ended because it has exceeded the maximum amount of time allowed for the search. The search time limit restricts the amount of time that a search can take. For each search, it is determined using a combination of the time limit specified for the targeted backend in the LDAP server configuration file, and the time limits specified in LDAP groups to which the requester belongs. See the description of the **timesLimit** server configuration option in **Customizing the LDAP server configuration** for more information.

**System action:** The LDAP server continues to run, but the operation ends.

**User response:** If additional search output is needed, increase the time limit specified on the search operation. Then reissue the operation. If the search output is still limited, contact an LDAP administrator. After the problem is resolved, rebind to the server and reissue the operation.

**Administrator response:** Use the **timesLimit** option in the LDAP server configuration file or search limit groups to increase the search time limit for this requester. If the configuration option is changed, restart the server. If search limit groups are changed, then the requester must rebind to use the changed limits.
output is still limited, contact an LDAP administrator. After the problem is resolved, rebind to the server and reissue the operation.

Administrator response: Use either the timeLimit option in the LDAP server configuration file or search limit groups to increase the search time limit for this requester. If the configuration option is changed, restart the server. If search limit groups are changed, then the requester must rebind to use the changed limits.

R004035  Attribute type 'name' may not be added or modified by users

Explanation: An LDAP add, modify, or modify DN operation failed because it attempts to specify a value for an attribute that cannot be set by a user. This attribute is only set by the LDAP server. In general, an attribute which includes NO-USER-MODIFICATION in its schema definition falls into this category. Note that an add or modify DN operation may cause this error if the attribute is part of the new relative distinguished name (RDN) of the entry, because the LDAP server automatically adds the RDN attributes and values to the entry. The RDN is the leftmost part of the distinguished name. The name of the attribute is indicated in the reason code.

In the message text:

name

Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Remove the attribute from the operation input. Then reissue the operation.

R004038  Operation not allowed because backend is in read-only mode

Explanation: An LDAP add, modify, delete, or modify DN operation failed because the backend which is the target of the operation is running in read-only mode. In general, the backend cannot be updated when running in this mode. A backend can be configured to run in read-only mode using the readOnly on option in the LDAP server configuration file. While the server is running, the BACKEND LDAP operator modify command can be used to switch the backend between read-only mode and read/write mode. Also, some backends can be switched to read-only mode automatically by the LDAP server if it detects problems with updating entries in the backend.

System action: The LDAP server continues to run, but the operation fails.

User response: If update operations on the backend are required, contact an LDAP administrator. After the problem is resolved, reissue the operation. Otherwise, do not issue update operations to the backend.

Administrator response: If requested, use the BACKEND LDAP operator modify command to change the backend to read/write mode.

R004041  Entry 'name' is not a leaf and may not be deleted

Explanation: An LDAP delete operation failed because it tries to delete an entry that has child entries. Only leaf entries (those with no entries below them) can be deleted. The distinguished name of the entry is indicated in the reason code.

In the message text:

name

Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: First delete all the entries below the target entry, starting with those on the lowest level of the subtree hierarchy. Then reissue the operation.

R004051  Entry 'name1' does not contain attribute 'name2'

Explanation: An LDAP operation failed because the entry does not contain the attribute type. The distinguished name of the entry and the attribute type are indicated in the reason code.

In the message text:

name1

Distinguished name of entry

name2

Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Remove the attribute from the operation input or correct the distinguished name of entry in the operation input. Then reissue the operation.

R004054  Invalid UTF-8 character found in string value 'value'

Explanation: An LDAP operation failed because a non-UTF8 character was detected in an attribute that is a string value. The value is indicated in the reason code.

In the message text:

value

Attribute value

System action: The LDAP server continues to run, but the operation fails.

User response: Remove or update the value so that it is a valid string value in the operation input. Then reissue the operation.
R004060 Entry does not contain a password

Explanation: A CRAM-MD5 or DIGEST-MD5 bind operation failed because there are no values for the userPassword attribute in the entry that contains the user ID specified in the bind information. The entry must have userPassword values and the values must be either in the clear or encrypted using a two-way encryption algorithm.

System action: The LDAP server continues to run, but the operation fails.

User response: Change the operation input so that the distinguished name in the request is correct. Then reissue the operation.

R004073 Entry is not a leaf and cannot be modified to be a referral entry

Explanation: An LDAP modify or modify DN operation failed because it results in a referral entry that has child entries. A referral entry is one which contains the referral object class and the ref attribute. A referral entry must be a leaf entry. Thus, a modify operation that adds this object class to an entry must not be targeted to a non-leaf entry. Similarly, a modify DN operation cannot result in changing an entry to a referral entry if that entry has entries under it. This can occur if the object class and attribute are part of the new relative distinguished name (RDN) of the renamed entry, because the LDAP server automatically adds the RDN attributes and values to the entry.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that it does not change a non-leaf entry to a referral entry. Then reissue the operation.

R004077 DN 'name' already exists

Explanation: An LDAP add or modify DN operation failed because there is already an entry with the distinguished name (DN) of the new entry. Every entry must have a unique DN. The DN of the duplicate entry is indicated in the reason code.

In the message text:

name Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: Either change the operation input so that the distinguished name of the new entry is unique or delete the existing duplicate entry. Then reissue the operation.

R004083 New superior is not allowed for an LDAP V2 request

Explanation: An LDAP modify DN operation failed because it specifies a value for new superior, but that parameter is not supported when the requester is not using LDAP protocol version 3. The requester established the protocol version to use during bind. Protocol levels below 3 do not support using the
modify DN operation to move an entry to another subtree by specifying a new superior for the entry.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Either remove the new superior value in the modify DN input or rebind using protocol version 3. Then reissue the operation.

---

**R004086**

**Entry 'name1' already contains attribute 'name2' with value 'value'**

**Explanation:** An LDAP modify operation failed because it attempts to add an attribute value that already exists in the entry. Each attribute value must be different. Note that the server 'normalizes' values before comparing them. This normalization depends on the syntax and equality matching rule specified in the attribute definition in the schema. For example, normalization using the **caseIgnoreMatch** matching rule removes extraneous spaces and changes all alphabetic characters to uppercase. See [LDAP directory schema](https://www.ietf.org/rfc/rfc4512.txt) for more information. In particular, only the distinguished name or filter part of an aclEntry or entryOwner attribute value is used when comparing values for these attributes. The distinguished name of the entry being modified and the duplicate attribute name and value from the modify input are indicated in the reason code.

In the message text:

```
name1  Distinguished name of entry
name2  Attribute name
value  Attribute value
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the duplicate attribute value from the modify input. Then reissue the operation.

---

**R004091**

**Non-IA5 data received for an LDAP V2 request**

**Explanation:** An LDAP operation failed because the client request is using LDAP Version 2 protocol and contains characters that are not valid IA5. The LDAP server checks that the client request contains only IA5 characters when the client is using LDAP Version 2 protocol, the **sendV3StringsOverV2As ISO8859-1** and **validateIncomingV2Strings on** configuration options are specified in the LDAP server configuration file. Note that **validateIncomingV2Strings on** is the default if the option is not specified in the configuration file. The requester established the protocol version to use during bind. IA5 characters are the 7-bit ASCII characters, from x'00' to x'7F'. Note that the null character (x'00') is a valid IA5 character.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the attribute value from the modify input. Then reissue the operation.

---

**R004096**

**Entry 'name1' does not contain attribute 'name2' with value 'value'**

**Explanation:** An LDAP modify operation failed because it attempts to delete an attribute value that does not exist in the entry. Note that the server 'normalizes' values before comparing them. This normalization depends on the syntax and equality matching rule specified in the attribute definition in the schema. For example, normalization of a value using the **caseIgnoreMatch** matching rule removes extraneous spaces and changes all alphabetic characters to uppercase. See [LDAP directory schema](https://www.ietf.org/rfc/rfc4512.txt) for more information. In particular, only the distinguished name or filter part of an aclEntry or entryOwner attribute value is used when comparing values for these attributes. The distinguished name of the entry being modified and the attribute name and value from the modify input are indicated in the reason code.

In the message text:

```
name1  Distinguished name of entry
name2  Attribute name
value  Attribute value
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the attribute value from the modify input. Then reissue the operation.

---

**R004098**

**Filtering on non-textual attribute 'name' is not allowed**

**Explanation:** An LDAP search operation failed because the search filter contains an attribute type that is non-textual. The z/OS LDAP server does not support search filters that contain attributes that are non-textual. For example, a search filter of (userPassword=secret) is not supported in z/OS LDAP because the userPassword attribute has an octet string syntax. The attribute name from the search filter is indicated in the reason code.
In the message text:

(name)

Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that it does not contain a search filter that contains a non-textual attribute. Then reissue the operation.

R004099  Parent of new entry 'name' is a referral entry

Explanation: An LDAP add or modify DN operation failed because it results in creating an entry under a referral entry. A referral entry is one which contains the referral object class and the ref attribute. A referral entry must be a leaf entry. Thus, an LDAP add operation cannot add an entry whose parent is a referral entry. Similarly, a modify DN operation cannot move an entry under a referral entry.

In the message text:

(name)

Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that it does not add or move an entry under a referral entry. Then reissue the operation.

R004107  The __passwd function failed; not loaded from a program controlled library

Explanation: An LDAP operation failed because a system function that it calls, __passwd(), is not supported when a load is done from an uncontrolled library. The function cannot be used by the LDAP server. The operation can be an SDBM bind, native authentication bind, or a native password modify.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Ensure that the appropriate program controlled environment is set up for the LDAP server. Then restart the server.

R004108  Native user ID 'name' is either not defined or no UID is present in the OMVS segment

Explanation: An LDAP operation involving a native authentication entry failed because the password or password phrase of the native user associated with the entry is expired in the z/OS Security Server. The operation can be a native authentication bind or a native password modify.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Reset the native user password or password phrase in the z/OS Security Server.

R004110  The password has expired

Explanation: An LDAP operation involving a native authentication entry failed because the password or password phrase of the native user associated with the entry is expired in the z/OS Security Server. The operation can be a native authentication bind or a native password modify.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Reset the native user password or password phrase in the z/OS Security Server.

R004110  The user id has been revoked

Explanation: An LDAP operation involving a native authentication entry failed because the native user associated with the entry is revoked in the z/OS Security Server. The operation can be a native authentication bind or a native password modify.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Reset the native user in the z/OS Security Server.
R004111  The password is not correct

Explanation: An LDAP operation involving a native authentication entry failed because the existing password or password phrase specified in the operation is not correct for the native user associated with the entry. The operation can be a native authentication bind or a native password modify.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the password in the operation input. Then reissue the operation.

R004112  A bind argument is not valid

Explanation: An LDAP bind operation failed because one of the values used during the bind is missing or is not valid. This error can also be caused by a modify of a native authentication password. When performing a native authentication bind or modify, the password lengths must be between 1 to 100. If a new password is specified during native authentication bind using the oldpassword/oldpassword format, there can be only one unescaped forward slash. See Native authentication for more information about changing native authentication passwords.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input. Then reissue the operation.

R004113  Native authentication cannot be performed when multiple uid values exist

Explanation: An LDAP bind or modify operation involving a native authentication entry failed because the entry contains more than one value for the uid attribute. The LDAP server cannot determine which of the values to use to associate the native authentication entry with a native user in the z/OS Security Server.

System action: The LDAP server continues to run, but the operation fails.

User response: Modify the native authentication entry so that the uid attribute has a single value, representing the z/OS Security Server user to be used. Then reissue the operation.

R004114  The modify-delete of the old password must occur before the modify-add of the new password

Explanation: An LDAP native password modify operation failed because the input does not contain a userPassword attribute modification to delete the existing password or password phrase value before the userPassword modification to add the new password or password phrase value. Both modifications are needed and the delete must precede the add in order to change a native password or password phrase.

System action: The LDAP server continues to run, but the operation fails.

User response: In the modify input, add a delete modification for the existing userPassword value before the add modification of the new value. Then reissue the operation.

R004115  More than one password cannot be specified for a native authentication password update

Explanation: An LDAP native password modify operation failed because the input either contains an add or delete userPassword attribute modification which specifies multiple values or contains multiple add modifications or multiple delete modifications. There must be a single delete modification with one value (the existing password or password phrase value) and a single add modification with one value (the new value), and the delete modification must precede the add modification.

System action: The LDAP server continues to run, but the operation fails.

User response: In the modify input, remove extraneous add and delete modifications for userPassword and ensure that there is one value in the add modification and one in the delete modification. Then reissue the operation.

R004116  Password change not allowed because native updates are not enabled

Explanation: An LDAP native password modify operation failed because the targeted backend is not configured to support this. Native password modify is enabled by setting the nativeUpdateAllowed option to on or reset in the section for this backend in the LDAP server configuration file. If the option is not specified in the backend section or if the value is set to off, then native password modify is not permitted within the backend. See Customizing the LDAP server configuration for more information about the nativeUpdateAllowed configuration option.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Add the nativeUpdateAllowed option with a value of on or reset to the backend section of the LDAP server configuration file. Then restart the server.
R004117 Native authentication replace is not allowed

Explanation: An LDAP native password modify operation failed because the input contained a replace modification for the userPassword value. This is not supported by native password modify. Instead, the input must contain a modification to delete the existing userPassword value followed by a modification to add the new userPassword value.

System action: The LDAP server continues to run, but the operation fails.

User response: In the modify input, remove the replace modification for the userPassword attribute and put in a delete of the existing value followed by an add of the new value. Then reissue the operation.

R004118 Native user ID 'name' is either not defined or no UID is present in the OMVS segment

Explanation: An LDAP native password modify operation failed because the native user associated with the native entry either does not exist in the z/OS Security Server or is not completely defined there. When using RACF as the security server, the RACF user must have an OMVS segment containing a UID value. The name of the native user is indicated in the reason code.

In the message text:

name

User ID

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the modify input to use a native authentication entry for which the associated native user is completely defined or modify the native user value within the native authentication entry to a native user that is completely defined. Then reissue the operation. If the native user is supposed to exist in the z/OS Security Server, contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Ensure that the required native users are completely defined in the z/OS Security Server.

R004119 A modify-add of the new password must follow the modify-delete of the old password

Explanation: An LDAP native password modify operation failed because the input does not contain a userPassword attribute modification to add the new password or password phrase value. This modification must follow the userPassword modification to delete the existing value. Both modifications are needed and the delete must precede the add in order to change a native password or password phrase.

System action: The LDAP server continues to run, but the operation fails.

User response: In the modify input, add an add modification for the new userPassword password or password phrase value after the delete modification of the existing value. Then reissue the operation.

R004120 The userPassword attribute cannot be added because the entry uses native authentication

Explanation: An LDAP add operation failed because the new entry is set up to use native authentication but a value for the userPassword attribute is specified. A native authentication entry cannot contain that attribute. See Native authentication for more information.

System action: The LDAP server continues to run, but the operation fails.

User response: Remove the userPassword attribute from the add input. Then reissue the operation.

R004121 Entry is using native authentication but without a native userid

Explanation: An LDAP modify operation failed because the modified entry is subject to native authentication but does not contain a uid or ibm-nativeId attribute value. Depending on how native authentication is configured, one of these values is required. See Native authentication for more information.

System action: The LDAP server continues to run, but the operation fails.

User response: Change the modify input to add the appropriate uid or ibm-nativeId attribute value to the entry. Then reissue the operation.

Administrator response: Ensure that the required native users are completely defined in the z/OS Security Server.

R004128 Native authentication password change failed: The new password is not valid, or does not meet requirements

Explanation: An LDAP native password modify operation failed because the new password is not specified (has zero length) or is not acceptable. The new native password is checked by the z/OS Security Server, not the LDAP server. The password must meet any password requirements of the z/OS Security Server, such as length, format, and change history.

System action: The LDAP server continues to run, but the operation fails.

User response: Ensure that the new password in the modify input is acceptable to the z/OS Security Server. Then reissue the operation.
R004129  •  R004153

R004129  New superior 'name' does not exist
Explanation:  An LDAP modify DN operation failed because it attempts to move an entry under an entry that does not exist. When specifying a new superior entry to move the target entry under, the new superior entry must already exist unless the target entry is becoming a new suffix entry. The distinguished name of the new superior is indicated in the reason code.
In the message text:

name  Distinguished name of new superior

System action:  The LDAP server continues to run, but the operation fails.
User response:  Correct the modify DN input so that the new superior is an existing entry. Then reissue the operation.

R004133  The new superior DN is located in the subtree to be moved
Explanation:  An LDAP modify DN operation failed because it tries to move an entry under itself. When specifying a new superior entry to move the target entry under, the new superior entry must not be a lower entry in the target entry’s subtree.

System action:  The LDAP server continues to run, but the operation fails.
User response:  Correct the modify DN input so that the new superior is not within the target entry’s subtree. Then reissue the operation.

R004130  Time limit exceeded for Modify DN operation
Explanation:  An LDAP modify DN operation that includes the IBMModifyDNTimelimitControl control failed because the processing time exceeds the limit specified in the control. This can occur when the modify DN operation also specifies the IBMModifyDNRealignDNAttributesControl control, which results in the LDAP server searching the backend for attribute values that specify the renamed entry and updating each such value to the new name for the entry.

System action:  The LDAP server continues to run, but the operation fails.
User response:  Specify a larger time limit in the IBMModifyDNTimelimitControl control. Then reissue the operation.

R004132  The new superior DN must exist in the same backend
Explanation:  An LDAP modify DN operation failed because it tries to move an entry under an entry that is in a different backend. When specifying a new superior entry to move the target entry under, the new superior entry must be within the same backend (but not necessarily the same suffix) as the target entry. A modify DN operation cannot move an entry between backends.

System action:  The LDAP server continues to run, but the operation fails.
User response:  Correct the modify DN input so that the new superior is an entry in the same backend as the target entry. Then reissue the operation.

R004133  The new superior DN is located in the subtree to be moved
Explanation:  An LDAP modify DN operation failed because it tries to move an entry under itself. When specifying a new superior entry to move the target entry under, the new superior entry must not be a lower entry in the target entry’s subtree.

System action:  The LDAP server continues to run, but the operation fails.
User response:  Correct the modify DN input so that the new superior is not within the target entry’s subtree. Then reissue the operation.

R004141  New RDN 'name' is not valid
Explanation:  An LDAP modify DN operation failed because the new relative distinguished name (RDN) is not acceptable. The RDN must have a single component. For example, cn=abc,ou=dept83 has two components, cn=abc and ou=dept83, thus is not a valid RDN. The new relative distinguished name is indicated in the reason code.

In the message text:

name  New relative distinguished name

System action:  The LDAP server continues to run, but the operation fails.
User response:  Correct the modify DN input so that the new relative distinguished name is valid. Then reissue the operation.

R004153  Parent of new entry 'name' is an alias entry
Explanation:  An LDAP add or modify DN operation failed because it results in creating an entry under an alias entry. An alias entry is one which contains the alias or aliasObject object class and the aliasedObjectName attribute. An alias entry must be a leaf entry. Thus, an LDAP add operation cannot add an entry whose parent is an alias entry. Similarly, a modify DN operation cannot move an entry under an alias entry.

In the message text:

name  Distinguished name of entry

System action:  The LDAP server continues to run, but the operation fails.
User response:  Correct the operation input so that an add does not try to add an entry under an alias entry and a modify DN does not try to move an entry under an alias entry. Then reissue the operation.
R004154  Entry is not a leaf and cannot be modified to be an alias entry

Explanation: An LDAP modify or modify DN operation failed because it results in an alias entry that has child entries. An alias entry is one which contains the alias or aliasObject object class and the aliasedObjectName attribute. An alias entry must be a leaf entry. Thus, an LDAP modify operation that adds one of these object classes must not be targeted to a non-leaf entry. Similarly, a modify DN operation cannot result in changing an entry to an alias entry if that entry has entries under it. This can occur if the object class and attribute are part of the new relative distinguished name (RDN) of the renamed entry, because the LDAP server automatically adds the RDN attributes and values to the entry.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that a modify does not try to add an alias to a non-leaf entry and a modify DN does not try to change a non-leaf entry to an alias entry. Then reissue the operation.

R004155  Alias entry 'name' points to itself

Explanation: An LDAP add, modify, or modify DN operation failed because it results in an alias entry that specifies itself as its alias. An alias entry is one which contains the alias or aliasObject object class and the aliasedObjectName attribute. The aliasedObjectName value must be the distinguished name (DN) of some other entry. Note that a modify DN operation cannot rename an alias entry such that the entry DN becomes the same as the alias DN within the entry. The DN of the entry is indicated in the reason code.

In the message text:

name  Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: Modify the entry so that the aliasedObjectName attribute value points to an entry within the same backend. Then reissue the operation.

R004159  Dereferencing 'name' failed because the resulting DN does not exist in this backend

Explanation: An LDAP search operation that is dereferencing aliases failed because an alias points to an entry that is not in the same backend as the initial alias entry. Aliasing between backends is not supported. An alias entry is one which contains the alias or aliasObject object class and the aliasedObjectName attribute. The distinguished name of the initial alias entry is indicated in the reason code.

In the message text:

name  Distinguished name of alias entry

System action: The LDAP server continues to run, but the operation fails.

User response: Starting from the initial alias value, analyze the alias chain and end the chain by removing or modifying the appropriate aliasedObjectName value. Then reissue the operation.

R004160  Entry 'name' cannot be both an alias and a referral

Explanation: An LDAP add, modify, or modify DN operation failed because it results in an entry that is both an alias entry and a referral entry. An alias entry is one which contains the alias or aliasObject object class and the aliasedObjectName attribute. A referral entry is one which contains the referral object class and the ref attribute. An entry cannot be both an alias and a referral because during a search there is no way to decide whether search should dereference the entry or use it as a referral. Note that a modify DN operation may cause this error if the alias and referral object classes and attributes are part of the new relative distinguished name (RDN) of the renamed entry, because the LDAP server automatically adds the RDN attributes and values to the entry. The distinguished name of the entry is indicated in the reason code.

In the message text:

name  Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that it
R004161  Persistent search terminated because search base entry has been deleted

Explanation: An LDAP persistent search operation ends because an LDAP delete or modify DN operation is deleting or renaming the search base entry.

System action: The LDAP server continues to run. The delete or modify DN operation continues but the persistent search operation ends.

User response: You might want to start a new persistent search using the renamed base when the modify DN operation completes.

R004163  Dynamic group URL 'url' is not valid

Explanation: An LDAP operation failed because the dynamic group URL in the memberURL attribute is not valid. The format of a dynamic group URL is: ldap:///baseDN[?][searchScope][?][searchFilter]. See Dynamic groups for more information. The dynamic group URL is indicated in the reason code.

In the message text:

url  Dynamic group URL

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that the value is valid for the memberURL attribute. Then reissue the operation.

R004164  An unsupported value 'value' is specified for attribute 'name'

Explanation: An LDAP operation failed because it specifies a value that is not supported for an attribute. The value and attribute name are indicated in the reason code.

In the message text:

value  Unsupported value

name  Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that the value is valid for the attribute. Then reissue the operation.

R004165  request is not supported by plugin

Explanation: An LDAP operation failed because it is not supported by the plugin. The LDAP operation is indicated in the reason code.

In the message text:

request  Unsupported operation

System action: The LDAP server continues to run, but the operation fails.

User response: Do not issue this request to the plugin.

R004166  The LDAP server is shutting down

Explanation: An LDAP operation failed because the LDAP server sysplex owner is in the process of ending and this LDAP server is unable to communicate with the sysplex owner. Another server in the sysplex group becomes the sysplex group owner.

System action: The LDAP server shutdown processing continues. The operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Check the other servers in the sysplex group and verify that another server becomes the sysplex owner.

R004176  The __passwd() function failed with error error_code

Explanation: An LDAP operation involving a native password failed because an unexpected return code from the __passwd() function used to process the password. The operation can be an SDBM bind, a native authentication bind, or a native authentication password modify. The error code returned by __passwd() is indicated in the reason code. See the description of this routine in [z/OS XL C/C++ Run-Time Library Reference] for more information about the error.

In the message text:

error_code  Error code from __passwd()

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Use any server messages and ERROR debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.
R004177  Parent entry must have an objectclass attribute value of "value"

Explanation: An LDAP operation or utility failed because the parent entry does not have the appropriate objectclass value for advanced replication configuration. See [Advanced replication] for more information. The objectclass value is indicated in the reason code.

In the message text:

value

Attribute value

System action: The LDAP server continues to run, but the operation or utility fails.

User response: Update the objectclass value of the parent entry or the objectclass value of entry being added or modified while configuring advanced replication. Then reissue the operation.

R004178  Entry of objectclass 'name' not permitted with this level of replication

Explanation: An LDAP operation or utility failed because an objectclass value in an entry is not supported with basic or advanced replication. If useAdvancedReplication on is specified in the CDBM backend section of the configuration file, basic replication entries with an objectclass value of replicaObject are not supported in the z/OS LDAP server. If useAdvancedReplication off is specified in the CDBM backend section of the configuration file, advanced replication entries with an objectclass value of ibm-replicationContext, ibm-replicaGroup, ibm-replicaSubEntry, and ibm-replicationAgreement are not supported in the z/OS LDAP server. See [Advanced replication] and [Basic replication] for more information. The objectclass value is indicated in the reason code.

In the message text:

name

Distinguished name of subtree

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator to verify whether basic or advanced replication entries are supported with the current level of replication. Then reissue the operation.

Administrator response: Verify that the subtree should be quiesced. Issue a Quiesce or unquiesce context extended operation to unquiesce the replication context.

R004179  Refusing request, subtree 'name' is quiesced

Explanation: An LDAP add, modify, or modify DN operation failed because the subtree is currently quiesced. When a replication context is quiesced, only the master server distinguished name (DN) or LDAP root administrator with the Server administration control can update entries under a quiesced subtree; other users are only allowed to perform search or compare operations. See [Advanced replication] for more information. The quiesced subtree DN is indicated in the reason code.

In the message text:

name

Distinguished name of subtree

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator to unquiesce the subtree. Then reissue the operation.

Administrator response: Verify that the subtree should be quiesced. Issue a Quiesce or unquiesce context extended operation to unquiesce the replication context.

R004180  Refusing request, access to replication topology is restricted

Explanation: An LDAP compare or search operation failed because access to advanced replication topology entries is restricted to an LDAP administrator. The ibm-slapdReplRestrictedAccess attribute value in the cn=Replication,cn=configuration entry indicates whether other users are allowed to update advanced replication topology entries. See CDBM backend configuration and policy entries for more information.

System action: The LDAP server continues to run, but the operation fails.

User response: If update access to advanced replication topology entries is needed, contact an LDAP administrator to allow this access. Then reissue the operation.

Administrator response: If necessary, update the ibm-slapdRestrictedAccess attribute value in the cn=Replication,cn=configuration entry.

R004181  An entry can not be moved into replication topology subtree 'name'

Explanation: An LDAP modify DN operation failed because an entry cannot be moved under an advanced replication topology subtree. The replication subtree distinguished name (DN) is indicated in the reason code.

In the message text:
Distinguished name of subtree

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the modify DN operation to specify a different parent entry. Then reissue the operation.

---

**R004182**

*Timestamps indicate a modify conflict, requesting refresh of entry 'name'*

**Explanation:** An LDAP modify operation resulted in a modify conflict on this server. A refresh of the entry from the advanced replication supplier server is requested to synchronize the entry on both servers. The distinguished name (DN) of the entry to be refreshed is indicated in the reason code.

In the message text:

*name*

Distinguished name of entry

**System action:** The LDAP server continues to run and a refresh of the entry from the supplier server is requested to synchronize the entry on both servers.

---

**R004183**

*Advanced replication is configured but not available*

**Explanation:** An LDAP operation failed because advanced replication is configuring but not currently available. The advanced replication engine is loaded when the `useAdvancedReplication on` option is specified in the CDBM section of the LDAP server configuration file.

**System action:** The LDAP server continues, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Use server ERROR debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

---

**R004185**

*Entry 'name' contains attribute values currently in use and cannot be deleted or renamed*

**Explanation:** An LDAP delete or modify DN operation failed because the entry contains attribute values that are currently in use by the LDAP server for features such as advanced replication and password policy. The distinguished name of the entry in use is indicated in the reason code.

In the message text:

*name*

Distinguished name of entry

**System action:** The LDAP server continues, but the operation fails.

**User response:** Update the request to no longer modify the attribute values in the distinguished entry. Then reissue the operation.

---

**R004186**

*Unable to find specified password policy entry 'name'*

**Explanation:** An LDAP add or modify operation failed because the individual or group password policy entry does not exist in the `cn=ibmpolicies` suffix of the CDBM backend. The distinguished name of the password policy that does not exist is indicated in the reason code.

In the message text:

*name*

Distinguished name of entry

**System action:** The LDAP server continues, but the operation fails.

**User response:** Update the request to specify a valid value for the `ibm-pwdGroupPolicyDN` or `ibm-pwdIndividualPolicyDN` attribute value. Then reissue the operation.

---

**R004187**

*The 'name' attribute value requires a minimum of number alphabetical characters*

**Explanation:** An LDAP add or modify operation of an attribute subject to password policy failed because the new value does not contain enough alphabetic characters. The name of the attribute and the minimum number of alphabetic characters required are indicated in the reason code.

In the message text:

*name*

Attribute name

*number*

Minimum number of alphabetic characters

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the operation input so that the attribute value meets all password policy requirements. Then reissue the operation.

---

**R004188**

*The 'name' attribute value requires a minimum of number non-alphabetical characters*

**Explanation:** An LDAP add or modify operation of an attribute subject to password policy failed because the new value does not contain enough non-alphabetic characters (numbers and special characters). The name of the attribute and the minimum number of non-alphabetic characters required are indicated in the reason code.

In the message text:
non-alphabetic characters required are indicated in the reason code.

In the message text:

\textit{name}  
Attribute name

\textit{number}  
Minimum number of non-alphabetic characters

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that the attribute value meets all password policy requirements. Then reissue the operation.

R004189 The 'name' attribute value requires a minimum of \textit{number} different characters

Explanation: An LDAP modify operation of an attribute subject to password policy failed because the new value does not contain enough characters that are different from the current attribute value. The name of the attribute and the minimum number of different characters required are indicated in the reason code.

In the message text:

\textit{name}  
Attribute name

\textit{number}  
Minimum number of different characters

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that the attribute value meets all password policy requirements. Then reissue the operation.

R004190 The 'name' attribute value allows a maximum of \textit{number} repeated characters

Explanation: An LDAP add or modify operation of an attribute subject to password policy failed because the new value specifies the same character too many times in a row (consecutively). The name of the attribute and the maximum number of times a character can be consecutively used are indicated in the reason code.

In the message text:

\textit{name}  
Attribute name

\textit{number}  
Maximum number of times a character can be used consecutively

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that the attribute value meets all password policy requirements. Then reissue the operation.

R004192 Password policy does not allow more than one password per entry

Explanation: An LDAP add or modify operation failed because it results in more than one value for the \texttt{userPassword} attribute when password policy is enabled. An entry subject to password policy can have at most one value for the \texttt{userPassword} attribute.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the add or modify input so that it does not specify multiple values for the \texttt{userPassword} attribute. Then reissue the operation.

R004193 Operation not allowed because backend (\textit{name}) is unable to perform I/O at this time

Explanation: An LDAP add, modify, modify DN, or delete operation failed because the targeted backend cannot write to the file system to save the update information. The file-based backend can perform search and compare operations, but operations that update the directory are rejected until the file system problem is resolved and the backend is restored to read/write mode. The name of the backend is indicated in the reason code. This is the name specified for the backend on the \texttt{database} option in the LDAP server configuration file, or, if no name is specified, the name generated for that backend by the LDAP server when the server is started.

In the message text:

\textit{name}  
Backend name
The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Use any server messages and ERROR debug trace output to assist in locating and correcting the file system problem. Then, use the BACKEND LDAP operator modify command to change the backend to read/write mode. The LDAP server does not have to be restarted.

R004194 The 'name' attribute value requires a minimum of number characters

Explanation: An LDAP add or modify operation of an attribute subject to password policy failed because the new value is too short. The name of the attribute and the minimum length of a value are indicated in the reason code.

In the message text:

name
  Attribute name

number
  Minimum length of value

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that the attribute value meets all password policy requirements. Then reissue the operation.

R004197 The encrypted 'name' attribute value cannot be validated

Explanation: An LDAP operation specifying an attribute value subject to password policy failed because the syntax of the value cannot be checked. See Password policy for more information. The name of the attribute is indicated in the reason code.

In the message text:

name
  Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Either change the password policy to allow one-way hashed password values to bypass syntax checking (pwdCheckSyntax) or update the encryption method used to allow password syntax checking to work.

R004195 The account is locked

Explanation: An LDAP operation failed because the user's account is locked because of excessive incorrect authentications or has been administratively locked by an LDAP administrator. The user is unable to successfully authenticate to the LDAP server.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: See Overriding password policy and unlocking accounts for information about unlocking accounts.

R004196 The 'name' attribute value has passed its maximum age of number seconds

Explanation: An LDAP bind operation specifying an attribute value subject to password policy failed because the value has expired. The name of the attribute and the length of time that it could be used before expiring are indicated in the reason code.

In the message text:

name
  Attribute name

number
  Maximum age of a value

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Reset the attribute value for the user.

R004198 User modification of the 'name' attribute is not allowed

Explanation: An LDAP modify operation of an attribute subject to password policy failed because password policy is configured to reject update of this attribute from this user. The name of the attribute is indicated in the reason code.

In the message text:

name
  Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator to update the attribute value. After the problem is resolved, reissue the operation.

Administrator response: Either update the attribute value or change the password policy to allow the user to do it.
**R004199**  
Current value for the 'name' attribute must be supplied

**Explanation:** An LDAP modify operation of an attribute subject to password policy failed because the modify operation does not contain a delete modification of the current attribute value. A delete modification of the current value is required when password policy is configured to perform safe modifications of this attribute's values. The name of the attribute is indicated in the reason code.

In the message text:

```
name
```

**Attribute name**

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the modify input so that the attribute value is not a repeat of a value used in the past. Then reissue the operation.

---

**R004200**  
The 'name' attribute value must be number seconds old before it can be changed

**Explanation:** An LDAP modify operation of an attribute subject to password policy failed because the current value is not yet old enough to be changed. Password policy tracks the last time the attribute subject to the policy was changed in the `pwdChangedTime` attribute. The name of the attribute and the minimum age that a value must be before it can be changed are indicated in the reason code.

In the message text:

```
name
```

**Attribute name**

```
number
```

**Minimum age of value**

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Wait until the value is older than the minimum required age. Then reissue the operation.

---

**R004201**  
The 'name' attribute value exists in the history and may not be reused

**Explanation:** An LDAP modify operation of an attribute subject to password policy failed because the value is a repeat of a value used in the past. Password policy tracks the past values in the `pwdHistory` attribute and requires that a value can only be reused after the attribute has been changed a certain number of times. The name of the attribute is indicated in the reason code.

In the message text:

```
name
```

**Distinguished name**

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the operation input so that the
<table>
<thead>
<tr>
<th><strong>R004204</strong> • <strong>R004208</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>value</strong> is a different distinguished name. Then reissue the operation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>R004204</strong></th>
<th><strong>The value 'value' for the 'name' attribute is not a valid admin role</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> An LDAP add or modify operation to assign an administrator role value to an attribute failed because the value is not one of the supported administrative roles. The attribute name and the value in error are indicated in the reason code. See <a href="#">Administration groups and roles</a> for more information about the supported administrative roles.</td>
<td></td>
</tr>
</tbody>
</table>

In the message text:

<table>
<thead>
<tr>
<th><strong>value</strong></th>
<th>Attribute value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>name</strong></td>
<td>Attribute name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>System action:</strong> The LDAP server continues to run, but the operation fails.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User response:</strong> Change the operation input so that the value is a valid administrative role. Then reissue the operation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>R004205</strong></th>
<th><strong>The DN 'name' cannot be added to the master server DN list</strong></th>
</tr>
</thead>
</table>
| **Explanation:** An LDAP add or modify operation has failed because a duplicate was detected while attempting to add the distinguished name (DN) to the `ibm-slapdMasterDN` in a consumer server credentials entry. A duplicate is detected when:
- An administrative group member entry
  - (`ibm-slapdAdminMember` objectclass) has an `ibm-slapdAdminDN` with the same value.
- An `ibm-slapdMasterDN` value matches the `masterServerDN`, `peerServerDN`, or the `adminDN` options in the LDAP server configuration file.
- An `ibm-slapdMasterDN` value matches the `member` value in the `cn=safadmingroup,cn=configuration` entry. |

The duplicate DN is indicated in the reason code. |

In the message text:

<table>
<thead>
<tr>
<th><strong>name</strong></th>
<th>Distinguished name</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>System action:</strong> The LDAP server continues to run, but the operation fails.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User response:</strong> Change the operation input so that the value is a different distinguished name. Then reissue the operation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>R004206</strong></th>
<th><strong>Access denied because user does not have permission to lock an account</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> An LDAP modify operation has failed because the user does not have the authority to lock a user's account. An LDAP password administrator does not have the authority to lock a user's account.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>System action:</strong> The LDAP server continues to run, but the operation fails.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User response:</strong> Contact an LDAP root administrator to lock the user's account.</td>
</tr>
</tbody>
</table>

| **Administrator response:** See [Password policy](#) for information about locking accounts. |

<table>
<thead>
<tr>
<th><strong>R004207</strong></th>
<th><strong>Access denied because user does not have permission to update attributes that may result in a locked account</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> An LDAP modify operation has failed because the user does not have the authority to update password policy operational attributes that may result in locking a user's account. An LDAP password administrator only has the authority to unlock a user's account and therefore does not have the authority to add <code>pwdExpirationWarned</code>, <code>pwdAccountLockedTime</code>, <code>pwdGraceUseTime</code>, <code>pwdExpirationWarned</code>, or <code>pwdGraceUseTime</code> attributes.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>System action:</strong> The LDAP server continues to run, but the operation fails.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User response:</strong> Contact an LDAP root administrator to lock the user's account.</td>
</tr>
</tbody>
</table>

| **Administrator response:** See [Password policy](#) for information about locking accounts. |

<table>
<thead>
<tr>
<th><strong>R004208</strong></th>
<th><strong>Objectclass 'value' is not valid for entry 'name'</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> When adding or modifying entries under the <code>cn=SAFAdminGroup,cn=configuration</code> and <code>cn=AdminGroup,cn=configuration</code> entries, the only supported objectclass values are <code>top</code>, <code>ibm-slapdSAFAdminGroup</code>, <code>ibm-slapdConfigEntry</code>, and <code>ibm-slapdConfigEntry</code>.</td>
<td></td>
</tr>
</tbody>
</table>

| **In the message text:** |
|---|---|
| **value** | Object class name |
| **name** | Distinguished name of entry |

<table>
<thead>
<tr>
<th><strong>System action:</strong> The LDAP server continues to run, but the operation fails.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User response:</strong> Correct the operation input to specify an objectclass value that is valid for the entry. Then reissue the operation.</td>
</tr>
</tbody>
</table>
R004209 New superior 'value' is not valid for entry 'name'

Explanation: An LDAP modify DN operation has failed because the new superior is not valid for the entry. An administrative group member entry is not allowed to be a parent or superior entry. The superior and distinguished name of the entry are indicated in the reason code.

In the message text:
value  New superior value
name  Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input to no longer specify a new superior entry. Then reissue the operation.

R004210 Objectclass 'value' is required for entry 'name'

Explanation: An LDAP add or modify operation has failed a required objectclass is missing for the entry. The objectclass value and distinguished name of the entry are indicated in the reason code.

In the message text:
value  Object class name
name  Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that it is not targeted to a GDBM entry. Then reissue the operation.

R004211 Credentials are not valid for DN 'name'

Explanation: An LDAP bind operation failed because the credentials specified on the request are not correct. The password specified on a simple, CRAM-MD5, or DIGEST-MD5 bind must match a userPassword value on the bind distinguished name entry. If SSL certificate mapping is activated and an EXTERNAL bind is performed, the certificate could not be mapped to a SAF user. See Support of certificate bind for more information. The bind distinguished name is indicated in the reason code.

In the message text:
name  Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: If performing a simple, CRAM-MD5, or DIGEST-MD5 bind, update the bind distinguished name (DN), user ID, or password value specified on the bind request. If performing an EXTERNAL bind and SSL certificate mapping is active, verify that the certificate is being used, otherwise contact an LDAP administrator. Then reissue the operation.

Administrator response: If the user is performing an EXTERNAL bind, determine whether the user’s certificate should be mapped to a RACF (SAF) user ID by doing an RACDCERT MAP command. Also verify that the sslMapCertificate option settings are correct when SSL certificates cannot be mapped to a RACF or SAF user ID.

R005001 Requested operation is not supported by the GDBM backend

Explanation: An LDAP operation to the GDBM backend failed because it is not allowed for this backend. GDBM only supports modify, delete, search, and compare operations. In particular, add operations are not allowed.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that it is not targeted to a GDBM entry. Then reissue the operation.

R005002 Only the base change log entry can be modified

Explanation: An LDAP modify operation to the GDBM backend failed because it tries to modify an entry other than the GDBM suffix entry (cn=changelog). The only GDBM entry that can be modified is the suffix entry and only the aclEntry and entryOwner attribute values can be changed.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the modify input so that it is targeted to the GDBM suffix entry, cn=changelog, and only includes the aclEntry and entryOwner attributes. Then reissue the operation.

R005003 The base change log entry cannot be deleted

Explanation: An LDAP delete operation to the GDBM backend failed because it tries to delete the GDBM suffix entry (cn=changelog). The GDBM suffix entry is created by the LDAP server and cannot be deleted.

GDBM changelog entries can be deleted.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the delete input so that it is
targeted to a GDBM changelog entry. Then reissue the operation.

R005004 Only the aclEntry and entryOwner attributes can be modified

Explanation: An LDAP modify operation to the GDBM backend failed because it includes changes for attributes that cannot be modified. GDBM only supports modifying the aclEntry and entryOwner attributes in the GDBM suffix (cn=changelog).

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the modify input so that it is targeted to the GDBM suffix entry, cn=changelog, and only includes the aclEntry and entryOwner attributes. Then reissue the operation.

R006001 LDAP Client API api_name has returned an error code=error_code with an error message='error_text'

Explanation: An LDAP extended operation or utility failed because during its processing it invokes an LDAP client application programming interface (API) that does not succeed. The name of the interface and the error code and error text that it returned are indicated in the reason code. See the description of the API in IBM Tivoli Directory Server Client Programming for z/OS for more information about the error.

In the message text:

api_name
  Name of the client interface

error_code
  Error code from the interface

error_text
  Error text corresponding to the error code

System action: The LDAP server continues to run, but the extended operation or utility fails.

User response: Use the information in the reason code to resolve the problem. Then reissue the extended operation or restart the utility.

R006003 A decoding error has been encountered while decoding attribute(s): field, return_code

Explanation: An LDAP extended operation failed because it includes a field value that cannot be decoded. The field name is indicated in the reason code along with the return code from the routine that is invoked to decode the field. The most likely return codes are:

- 90 (LDAP_NO_MEMORY): The LDAP server ran out of storage.

In the message text:

field
  Field name

return_code
  Return code from decode routine

System action: The LDAP server continues to run, but the extended operation fails.

Administrator response: For a storage problem, if running the 31-bit LDAP server (GLDSRV31), consider using the 64-bit LDAP server (GLDSRV64) to use the additional storage available in a 64-bit address space. Then restart the LDAP server.

R006004 An encoding error return_code has been encountered while encoding response

Explanation: An LDAP operation failed because the response message could not be encoded by the LDAP server. The return code from the encoding routine is indicated in the reason code.

In the message text:

return_code
  Return code from encoding routine

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. Then reissue the operation.

Administrator response: Use any server messages and ERROR debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

R006006 Unsupported or inappropriate critical control 'identifier'

Explanation: An LDAP operation failed because it includes a critical control that the LDAP does not support. Possible reasons for this are:

- The control is not supported at all.
- The control is specified for an operation that does not allow that control.
The control is only supported for certain users.
The control identifier is indicated in the reason code.
See **Supported server controls** for more information about the supported controls.

In the message text:

**identifier**  
Control identifier

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the control from the operation. Then reissue the operation.

---

R006009  The extended operation request with OID=oid1 requires the critical control with OID=oid2

**Explanation:** An LDAP extended operation failed because it does not include a control that must be sent with the operation. The extended operation cannot be processed without the control. The identifiers of the extended operation and the control are indicated in the reason code. See **Supported extended operations** for more information about the extended operation.

In the message text:

*oid1*  
Extended operation identifier

*oid2*  
Control identifier

**System action:** The LDAP server continues to run, but the extended operation fails.

**User response:** Remove the control from the extended operation. Then reissue the operation.

---

R006010  Unsupported extended operation *identifier*

**Explanation:** An LDAP extended operation failed because it is not supported by the LDAP server. The extended operation identifier is indicated in the reason code. See **Supported extended operations** for more information about the supported extended operations.

In the message text:

*identifier*  
Extended operation identifier

**System action:** The LDAP server continues to run, but the extended operation fails.

**User response:** Do not issue the extended operation.

---

R006011  The extended operation request with OID=oid1 does not support the critical control with OID=oid2

**Explanation:** An LDAP extended operation failed because it includes a critical control that is not supported by the extended operation. The identifiers of the extended operation and the control are indicated in the reason code. See **Supported extended operations** for more information about the extended operation.

In the message text:

*oid1*  
Extended operation identifier

*oid2*  
Control identifier

**System action:** The LDAP server continues to run, but the extended operation fails.

**User response:** Remove the control from the extended operation. Then reissue the operation.

---

R006023  Required field (name) missing

**Explanation:** An LDAP extended operation failed because it is missing a required field or the field value is a zero-length string. The name of the field is indicated in the reason code. See **Supported extended operations** for more information about the extended operation.

In the message text:

*name*  
Field name

**System action:** The LDAP server continues to run, but the extended operation fails.

**User response:** Specify an acceptable value for the field in the extended operation input. Then reissue the extended operation.

---

R006024  Connection to server (url) failed

**Explanation:** An LDAP extended operation failed because it involves connecting to a remote server but cannot establish the connection. The URL identifying the remote server is indicated in the reason code.

In the message text:

*url*  
URL of a remote server

**System action:** The LDAP server continues to run, but the extended operation fails.

**User response:** Ensure that the remote server is active and accessible. Then reissue the extended operation.
R006025 Incorrect ldapURL specified (url)

Explanations: An LDAP extended operation failed because it involves connecting to a remote server but the format of the URL identifying the remote server is not valid. The URL identifying the remote server is indicated in the reason code.

In the message text:

url
  URL of a remote server

System action: The LDAP server continues to run, but the extended operation fails.

User response: Correct the format of the URL. Then reissue the extended operation.

R006026 ldap_search failed rc=return_code

Explanations: An LDAP getDnForUserid extended operation failed because there are no entries on the remote server that match the user ID specified in the extended operation. The most likely return code indicated in the reason code is 32 (NO_SUCH_OBJECT).

In the message text:

return_code
  Return code from remote search

System action: The LDAP server continues to run, but the extended operation fails.

User response: Ensure that the remote server contains the appropriate entries for the user ID specified in the extended operation. Then reissue the extended operation.

R006027 Unsupported authorization type=type

Explanations: An LDAP extended operation failed because it involves connecting to a remote server but the authorization type specified for the bind is not supported by the extended operation. The most likely bind types indicated in the reason code are 128 (simple) and 163 (SASL). See [Supported extended operations](#) for more information about the extended operation.

In the message text:

type
  Type of authorization

System action: The LDAP server continues to run, but the extended operation fails.

User response: Ensure that a supported bind type is specified for the extended operation. Then reissue the extended operation.

R006028 Expected attribute name missing from entry

Explanations: A GetPrivileges extended operation failed because the information returned from the remote server does not include all the required attributes. The name of a missing attribute is indicated in the reason code.

In the message text:

name
  Attribute name

System action: The LDAP server continues to run, but the extended operation fails.

User response: Ensure that the appropriate entries in the remote server contain all the required attributes. Then reissue the extended operation.

R006029 Empty sequence in extended operation request name

Explanations: An extended operation failed because it includes an empty sequence, thus cannot be decoded. The name of the extended operation is indicated in the reason code.

In the message text:

name
  Extended operation name

System action: The LDAP server continues to run, but the extended operation fails.

User response: Check that all the sequences in the extended operation input are correctly encoded. Contact an LDAP administrator to determine if there are any server messages or ERROR debug trace output generated during the extended operation process that might assist in locating and correcting the problem. Then reissue the extended operation.

Administrator response: If requested, gather any server message and ERROR debug output created by the extended operation processing.

R006050 Extended operation request does not have an object identifier

Explanations: An LDAP extended operation failed because it does not contain an identifier indicating the type of extended operation.

System action: The LDAP server continues to run, but the extended operation fails.

User response: Ensure that the appropriate extended operation identifier is included in the extended operation. Then reissue the extended operation.
R006051 The type backend is not defined
Explanation: An LDAP extended operation or utility failed because it requires a backend that is not running. The backend can be the target of the operation or utility. Alternatively, it can be another backend needed to complete processing of the request. For example:
- The GetDnForUserid and GetPrivileges extended operations require that the EXOP backend is running.
- The changeLogAddEntry extended operation requires that the SDBM backend is running. This extended operation is used to log changes to RACF profiles.
- The unloadRequest extended operation requires the CDBM backend be running if a distinguished name of a filter entry (the filterDN field) is specified in the extended operation. This extended operation is used by the ds2ldif utility.

The type of backend that is needed is indicated in the reason code.

In the message text:

**type**

Type of backend

System action: The LDAP server continues to run, but the extended operation or utility fails.

User response: For the unloadRequest, remove the filterDN field from the extended operation or do not specify the -q option for the ds2ldif utility. Then reissue the extended operation or restart the utility. Alternatively, contact an LDAP administrator to configure the needed backend. After the problem is resolved, reissue the extended operation or restart the utility.

Administrator response: If requested, add the needed backend to the LDAP server configuration file. Then restart the LDAP server.

R006052 Persistent search is allowed only when bound as an LDAP administrator with sufficient authority

Explanation: An LDAP search operation including the PersistentSearch control failed because the search involves dereferencing aliases. Alias dereferencing of any entry other than the base of the search is not supported for a persistent search.

System action: The LDAP server continues to run, but the operation fails.

User response: Either change the search input to specify LDAP_DEREF_NEVER or LDAP_DEREF_FINDING rather than LDAP_DEREF_SEARCHING or LDAP_DEREF_ALWAYS, or remove the PersistentSearch control. Then reissue the operation.

R006053 Persistent search must specify LDAP_DEREF_NEVER or LDAP_DEREF_FINDING

Explanation: An LDAP search operation including the PersistentSearch control failed because the search involves dereferencing aliases. Alias dereferencing of any entry other than the base of the search is not supported for a persistent search.

System action: The LDAP server continues to run, but the operation fails.

User response: Either remove the PersistentSearch control or remove the PageResults and SortKeyRequest controls. Then reissue the operation.

R006054 Persistent search is not allowed using the Program Call interface

Explanation: An LDAP search operation including the PersistentSearch control failed because it is received over the local Program Call (PC) interface rather than over the network. Persistent searches are not supported using the PC interface.

System action: The LDAP server continues to run, but the operation fails.

User response: Do not issue a persistent search over the Program Call interface. The operation can be issued using network communications.

R006055 Persistent search is not allowed with paged or sorted results

Explanation: An LDAP search operation including the PersistentSearch control failed because it also includes either the PageResults or SortKeyRequest control. Paging and sorting are not supported for a persistent search.

System action: The LDAP server continues to run, but the operation fails.

User response: Either remove the PersistentSearch control or remove the PageResults and SortKeyRequest controls. Then reissue the operation.

R006056 Persistent search is not supported by the backend

Explanation: An LDAP search operation including the PersistentSearch control failed because the backend containing the target of the search does not support persistent search. Only LDBM, TDBM, GDBM, and CDBM backends can process a persistent search. To enable the support in these backends, the persistentSearch on option must be specified in the backend section of the LDAP server configuration file.
R006057  Persistent search is not allowed for an internal request
Explanation: An LDAP search operation including the PersistentSearch control failed because it is received over an internal plug-in request rather than over the network. Persistent searches are not supported using an internal plug-in request.
System action: The LDAP server continues to run, but the operation fails.
User response: Do not issue a persistent search over an internal plug-in request. The operation can be issued using network communications directly to the plug-in.

R006058  Paged search results not allowed for an internal request
Explanation: An LDAP search operation including the PagedResults control failed because it is received over an internal plug-in request rather than over the network. Paged searches are not supported using an internal plug-in request.
System action: The LDAP server continues to run, but the operation fails.
User response: Do not issue a paged search over an internal plug-in request. The operation can be issued using network communications directly to the plug-in.

R006059  Unload extended operation found multiple LDBM, TDBM, or CDBM backends to unload
Explanation: An LDAP unloadRequest extended operation failed because there is more than one backend to unload. When the extended operation does not include the backendName or subtreeDN fields, it looks in the LDAP server configuration file for an LDBM, TDBM, or CDBM backend to unload. If the configuration file does not contain any backend of these types or contains more than one, then processing ends.
System action: The LDAP server continues to run, but the extended operation fails.
User response: Add either the backendName or the subtreeDN field (but not both) to the extended operation to indicate what entries to unload. Then reissue the extended operation.

R006060  Unload extended operation is allowed only when bound as administrator group member with the appropriate roles assigned
Explanation: An LDAP unloadRequest extended operation failed because the requester is not an LDAP administrator. This extended operation can only be performed by an LDAP root, directory, or schema (only if unloading the schema entry) administrator.
System action: The LDAP server continues to run, but the extended operation fails.
User response: Rebind as an LDAP administrator.

R006061  Unload extended operation cannot find backend name 'name' to unload
Explanation: An LDAP unloadRequest extended operation failed because it specifies a distinguished name (DN) of a subtree to unload but either there is no backend that contains the DN or the backend containing the DN is not an LDBM, TDBM, or CDBM backend and the DN is not cn=schema. The subtree DN is specified in the subtreeDN field in the extended operation. The subtree DN value is indicated in the reason code.
In the message text:
name  Distinguished name of the subtree
System action: The LDAP server continues to run, but the extended operation fails.
User response: Correct the subtreeDN value in the extended operation input by specifying an existing DN in an LDBM, TDBM, or CDBM backend or by specifying cn=schema (to unload the schema). Then reissue the extended operation.

R006062  Unload extended operation cannot find subtree DN 'name' to unload
Explanation: An LDAP unloadRequest extended operation failed because it specifies a distinguished name (DN) of a subtree to unload but either there is no backend that contains the DN or the backend containing the DN is not an LDBM, TDBM, or CDBM backend and the DN is not cn=schema. The subtree DN is specified in the subtreeDN field in the extended operation. The subtree DN value is indicated in the reason code.
In the message text:
name  Distinguished name of the subtree
System action: The LDAP server continues to run, but the extended operation fails.
User response: Correct the subtreeDN value in the extended operation input by specifying an existing DN in an LDBM, TDBM, or CDBM backend or by specifying cn=schema (to unload the schema). Then reissue the extended operation.

R006063  Unload extended operation cannot find backend name 'name' to unload
Explanation: An LDAP unloadRequest extended operation failed because it specifies the name of a backend to unload but either there is no backend with that name or the backend with that name is not an LDBM, TDBM, GDBM, or CDBM backend. The backend name is specified in the backendName field in the extended operation. The name specified in the extended operation is indicated in the reason code. The name of each backend is established when the LDAP server is started and is either the name specified for the
backend on its database option in the LDAP server configuration file, or, if no name is specified, a name generated for that backend by the LDAP server.

In the message text:

name

Name of backend to unload

System action: The LDAP server continues to run, but the extended operation fails.

User response: Correct the extended operation input by specifying the name of an existing LDBM, TDBM, GDBM, or CDBM backend in the backendName field. Then reissue the extended operation.

R006064   Unload extended operation unable to open file 'filename', errno=error_code, errstring=error_text

Explanation: An LDAP unloadRequest extended operation failed because it cannot open the output file for write access. The file name is specified in the outputFileName field in the extended operation. See the description of fopen() in z/OS XL C/C++ Run-Time Library Reference for more information about the error. Note that the unloadRequest extended operation request can result from usage of the ds2ldif unload utility. The -o option of the utility corresponds to setting the outputFileName field. The file name and the fopen() error code and text are indicated in the reason code.

In the message text:

filename

Output file name

error_code

Error code from fopen()

error_text

Error text corresponding to the error code

System action: The LDAP server continues to run, but the extended operation or utility fails.

User response: Ensure that the output file specified using the outputFileName value exists and can be opened for write access. For the ds2ldif utility, the file name is specified in the -o option. Then reissue the extended operation or restart the utility.

R006065   Unload extended operation has both backend name and subtree DN specified

Explanation: An LDAP unloadRequest extended operation failed because it specifies both the name of a backend to unload and the DN of a subtree to unload. The extended operation does not support specifying both of these values. The backend name is specified in the backendName field in the extended operation. The subtree DN is specified in the subtreeDN field.

System action: The LDAP server continues to run, but the extended operation fails.

User response: Correct the extended operation input by removing either the backendName value or the subtreeDN value. Then reissue the extended operation.

R006066   Unload extended operation cannot find any LDBM, TDBM, or CDBM backend in the LDAP server configuration file to unload

Explanation: An LDAP unloadRequest extended operation failed because there is no backend to unload. When the extended operation does not include the backendName or subtreeDN fields, it looks in the LDAP server configuration file for an LDBM, TDBM, or CDBM backend to unload. If the configuration file does not contain any backend of these types or contains more than one, then processing ends.

System action: The LDAP server continues to run, but the extended operation fails.

User response: If there are multiple LDBM, TDBM, or CDBM backends in the LDAP server configuration file, add a backendName or subtreeDN value (but not both) to the extended operation input to indicate what to unload. Then reissue the extended operation. If there are no eligible backends in the configuration file, do not issue the extended operation.

R006067   Unload extended operation with a filter DN is only supported when advanced replication is activated in the CDBM backend

Explanation: An LDAP unloadRequest extended operation failed because it tries to use filtering but advanced replication is not configured. Filtering is requested by including the filterDN field in the extended operation. Filtering requires that the CDBM backend is configured and the useAdvancedReplication on option is included in the CDBM section of the LDAP server configuration file. Note that the unloadRequest extended operation request can result from usage of the ds2ldif unload utility. The -q option of the utility corresponds to setting the filterDN field.

System action: The LDAP server continues to run, but the extended operation or utility fails.

User response: Correct the extended operation input by removing the filterDN value. For the ds2ldif utility, remove the -q option. Then reissue the extended operation or restart the utility. If filtering is needed, contact an LDAP administrator. After the problem is resolved, reissue the extended operation or restart the utility.

Administrator response: If filtering is requested, ensure that CDBM is configured with the useAdvancedReplication on option in the LDAP server configuration file. Then restart the server.
Unload extended operation is not able to find valid filters in filter DN 'name'

**Explanation:** An LDAP *unloadRequest* extended operation failed because it tries to use filtering but there are no acceptable filter values in the specified filter entry. The distinguished name (DN) of the filter entry is specified in the *filterDN* field. Note that the *unloadRequest* extended operation request can result from usage of the *ds2ldif* unload utility. The `-q` option of the utility corresponds to setting the *filterDN* field. See [Partial replication](#) for more information about filters. The DN of the filter entry is indicated in the reason code.

In the message text:

- **name**: Distinguished name of filter entry

**System action:** The LDAP server continues to run, but the extended operation or utility fails.

**User response:** Correct the extended operation input by removing the *filterDN* value or by specifying the DN of an entry that contains acceptable filter values. For the *ds2ldif* utility, remove the `-q` option or change the value. Then reissue the extended operation or restart the utility.

---

unload extended operation does not support filtering of the schema entry

**Explanation:** An LDAP *unloadRequest* extended operation failed because it tries to use filtering when unloading the schema entry. This combination is not supported. If the *subtreeDN* field is set to `cn=schema`, then the *filterDN* field cannot be set. Note that the *unloadRequest* extended operation request can result from usage of the *ds2ldif* unload utility. The `-s` option of the utility corresponds to setting the *subtreeDN* field and the `-q` option corresponds to setting the *filterDN* field.

**System action:** The LDAP server continues to run, but the extended operation or utility fails.

**User response:** Remove the *filterDN* value from the extended operation input. For the *ds2ldif* utility, remove the `-q` option. Then reissue the extended operation or restart the utility.

---

unload extended operation does not support subtreeDN with unload localhost set to TRUE

**Explanation:** An LDAP *unloadRequest* extended operation failed because it tries to unload both a specific subtree and the localhost subtree. This combination is not supported. If the *unloadLocalhost* field is set to `TRUE`, then a value cannot be specified for the *subtreeDN* field.

**System action:** The LDAP server continues to run, but the extended operation fails.

**User response:** Change the extended operation input to specify the distinguished name of an entry that does not use native authentication. Then reissue the extended operation.

---

Password policy is not available with native authentication

**Explanation:** An LDAP *effectPasswordPolicy* or *acctStatus* extended operation failed because the target entry of the extended operation uses native authentication. Entries that use native authentication do not contain the *userPassword* attribute and are not subject to LDAP password policy.

**System action:** The LDAP server continues to run, but the extended operation fails.

**User response:** Change the extended operation input to specify the distinguished name of an entry that does not use native authentication. Then reissue the extended operation.

---

SASL authentication requires the LDAP Version 3 protocol

**Explanation:** An LDAP bind operation failed because it uses SASL authentication, but the requester is not using LDAP Version 3 protocol. Protocol levels below 3 do not support SASL authentication.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the bind input to not use SASL authentication or use LDAP Version 3 protocol. Then reissue the operation.
R007002  Unsupported SASL authentication method 'name'

Explanation: An LDAP bind operation failed because it specifies a SASL authentication method that is not allowed. The unsupported authentication method is indicated in the reason code.

In the message text:

name  Authentication method

System action: The LDAP server continues to run, but the operation fails.

User response: Change the bind input to use one of the supported authentication methods. Then reissue the operation.

R007005  Server is not configured for client authentication

Explanation: An LDAP bind operation using EXTERNAL (certificate) authentication failed because the LDAP server is not configured to do the client authentication used by this bind. EXTERNAL bind requires that the sslAuth serverClientAuth option appear in the global section of the LDAP server configuration file.

System action: The LDAP server continues to run, but the operation fails.

User response: Change the bind input to not use the EXTERNAL authentication method. Then reissue the operation.

Administrator response: If requested, add the sslAuth serverClientAuth option to the global section of the LDAP server configuration file. Then restart the LDAP server.

R007006  Client certificate is not available

Explanation: An LDAP bind operation using EXTERNAL (certificate) authentication failed because the LDAP server cannot obtain the client certificate or the certificate did not contain the CERT_DN_PRINTABLE field needed for authentication.

System action: The LDAP server continues to run, but the operation fails.

User response: Ensure that the client certificate is complete and available, or change the bind input to not use the EXTERNAL authentication method. Then reissue the operation.

R007020  User password is not available with native authentication

Explanation: An LDAP bind operation using CRAM-MD5 or DIGEST-MD5 authentication failed because the target entry is using native authentication, thus does not contain a password. The password for the target entry is in the z/OS Security Server. There is no userPassword attribute in the entry.

System action: The LDAP server continues to run, but the operation fails.

User response: Change the bind input to not use the CRAM-MD5 or DIGEST-MD5 authentication method. Then reissue the operation.

R007027  TLS is not supported on the connection

Explanation: An LDAP Start TLS extended operation failed because the LDAP server is not set up for SSL. Either the LDAP server is not configured to use SSL or SSL initialization failed. The sslKeyRingFile option must be specified in the global section of the LDAP server configuration file.

System action: The LDAP server continues to run, but the extended operation fails.

User response: Do not issue the extended operation. Alternatively, contact an LDAP administrator to restart the LDAP server using SSL. After the problem is resolved, reissue the extended operation.

Administrator response: If requested, add the sslKeyRingFile option to the global section of the LDAP server configuration file. Then restart the LDAP server.

R007028  SSL/TLS is already active on the connection

Explanation: An LDAP Start TLS extended operation failed because the LDAP server is already using SSL on this connection. The extended operation cannot switch the connection to use SSL.

System action: The LDAP server continues to run, but the extended operation fails.

User response: Do not issue the extended operation.

R007029  Other operations are outstanding for the connection

Explanation: An LDAP Start TLS extended operation failed because the connection is currently in use by other operations. A connection cannot be switched to use SSL while it is in use.

System action: The LDAP server continues to run, but the extended operation fails.

User response: Wait until all activity on the
connection is complete. Then reissue the extended operation.

**R007030** Multiple 'name' attributes found in DIGEST-MD5 response

**Explanation:** An LDAP bind operation using DIGEST-MD5 authentication failed because the LDAP server finds multiple values for an attribute in the bind response from the client. The server does not know which value to use. The name of the attribute is indicated in the reason code.

In the message text:

```plaintext
name
   Attribute name
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the client so that the encoded DIGEST-MD5 bind response does not contain multiple values for the attribute. See [RFC 2831: Using Digest Authentication as a SASL Mechanism](https://tools.ietf.org/html/rfc2831) for more information about DIGEST-MD5. Then reissue the operation.

**R007031** Required 'name' attribute not found in DIGEST-MD5 response

**Explanation:** An LDAP bind operation using DIGEST-MD5 authentication failed because the LDAP server does not find a needed value in the bind response from the client. The name of the missing attribute is indicated in the reason code.

In the message text:

```plaintext
name
   Attribute name
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the client so that the encoded DIGEST-MD5 bind response contains a required value for the attribute. See [RFC 2831: Using Digest Authentication as a SASL Mechanism](https://tools.ietf.org/html/rfc2831) for more information about DIGEST-MD5. Then reissue the operation.

**R007032** Syntax error in DIGEST-MD5 response

**Explanation:** An LDAP bind operation using DIGEST-MD5 authentication failed because the LDAP server cannot parse the bind response from the client. The syntax of the bind response is not correct.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the client so that the DIGEST-MD5 bind response is encoded properly. See [RFC 2831: Using Digest Authentication as a SASL Mechanism](https://tools.ietf.org/html/rfc2831) for more information about DIGEST-MD5. Then reissue the operation.

**R007033** Authorization DN in DIGEST-MD5 response does not match DN associated with user name

**Explanation:** An LDAP bind operation using DIGEST-MD5 authentication failed because there is a mismatch in the bind information. The LDAP server uses the authorization distinguished name (DN) in the bind request to locate the target entry in the directory. If the user name does not exist as a **uid** attribute value in the authorization DN entry, the bind response is not successful.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Update the bind input to specify the correct authorization DN or user name in the request. Then reissue the operation.

**R007034** BIND DN 'name1' is not the same as authentication DN 'name2'

**Explanation:** An LDAP bind operation using EXTERNAL (certificate), CRAM-MD5, DIGEST-MD5, or GSSAPI (Kerberos) failed because there is a mismatch between the distinguished name (DN) in the bind request and the resulting authentication DN. When a DN is specified in the bind request, it must match the resulting authentication DN. The DN in the bind request and the resulting authentication DN are indicated in the reason code.

In the message text:

```plaintext
name1
   Distinguished name from bind

name2
   Distinguished name from authentication
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Either correct the DN in the bind request to match the resulting authentication DN or remove it from the bind input. Then reissue the operation.

**R007035** The value of DIGEST-MD5 response attribute 'name' is not valid

**Explanation:** An LDAP bind operation using DIGEST-MD5 authentication failed because an attribute value in the bind response from the client is not acceptable. The name of the attribute is indicated in the reason code.

In the message text:

```plaintext
name
   Attribute name
```
**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the client so that the DIGEST-MD5 bind response attribute is valid. See [RFC 2831: Using Digest Authentication as a SASL Mechanism](https://tools.ietf.org/html/rfc2831) for more information about DIGEST-MD5. Then reissue the operation.

**Explanation:** An LDAP bind operation using DIGEST-MD5 authentication failed because the authzid value in the bind response from the client is not acceptable. The value must begin with `dn:` followed by a distinguished name of non-zero length.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the client so that the authzid attribute starts with `dn:`. See [RFC 2831: Using Digest Authentication as a SASL Mechanism](https://tools.ietf.org/html/rfc2831) for more information about DIGEST-MD5. Then reissue the operation.

**Explanation:** An LDAP bind operation using DIGEST-MD5 authentication failed because the value sent to the client in the server challenge. Certain values, such as for the nonce and the realm, must not be changed in the bind response. The name of the changed attribute is indicated in the reason code.

In the message text:

- `name` Attribute name.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the client so that the response attribute value is not changed. See [RFC 2831: Using Digest Authentication as a SASL Mechanism](https://tools.ietf.org/html/rfc2831) for more information about DIGEST-MD5. Then reissue the operation.

**Explanation:** An LDAP bind operation using DIGEST-MD5 authentication failed because the format of the digest-uri value in the bind response from the client is not valid or the value cannot be checked. The value format must be `ldap/hostname` where `hostname` is the local host name or the realm name specified in the digestRealm configuration option. The URL value is indicated in the reason code.

In the message text:

- `value` URL value.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. Then reissue the operation.

**Administrator response:** If the LDAP server is not able to determine the local host name from the Domain Name Server (DNS), update the digestRealm option to specify the hostname from the digest-uri value. Then restart the LDAP server.

**Explanation:** An LDAP bind operation using DIGEST-MD5 authentication failed because the format of the digest-uri value in the bind response from the client is not valid or the value cannot be verified. The value format must be `ldap/hostname` where `hostname` is the local host name or the realm name specified in the digestRealm configuration option. The URL value is indicated in the reason code.

In the message text:

- `value` URL value.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. Then reissue the operation.

**Administrator response:** Add an SDBM backend section to the LDAP configuration file. Then restart the LDAP server.

**Explanation:** An LDAP bind operation using EXTERNAL (certificate) authentication failed because it is received over the local Program Call interface but the SDBM backend is not running in the LDAP server. The SDBM backend is required when performing EXTERNAL binds over the Program Call interface. The bind can be issued using network communications when SDBM is not configured.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Add an SDBM backend section to the LDAP configuration file. Then restart the LDAP server.

**Explanation:** An LDAP bind operation using EXTERNAL (certificate) authentication failed because it is received over the local Program Call interface but the SDBM backend is not running in the LDAP server. The SDBM backend is required when performing EXTERNAL binds over the Program Call interface. The bind can be issued using network communications when SDBM is not configured.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the client so that the response maxbuf value is at least 256. See [RFC 2831: Using Digest Authentication as a SASL Mechanism](https://tools.ietf.org/html/rfc2831) for more information about DIGEST-MD5. Then reissue the operation.

**Explanation:** An LDAP bind operation using DIGEST-MD5 authentication failed because the maxbuf value in the bind response from the client is too small. The buffer size must be at least 256.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the client so that the response maxbuf value is at least 256. See [RFC 2831: Using Digest Authentication as a SASL Mechanism](https://tools.ietf.org/html/rfc2831) for more information about DIGEST-MD5. Then reissue the operation.

**Explanation:** An LDAP operation or extended operation failed because it is not allowed from this requester when the LDAP server is running in maintenance mode; operations restricted to an LDAP administrator, masterServerDN and peerServerDN.
maintenance mode. Only requests from an LDAP administrator or from a peer or master server for this backend are allowed.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Either rebind as a user authorized to perform operations while the server is in maintenance mode or contact an LDAP administrator to take the server out of maintenance mode. Then reissue the operation.

**Administrator response:** If requested, use the MAINTMODE OFF operator modify command to change the server to normal operating mode.

---

**R007060**  
**SASL bind is in progress**

**Explanation:** An LDAP operation or extended operation failed because a bind using a SASL authentication method is already in progress on the connection. The bind must complete before other operations can be performed.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Wait until the bind has completed. Then reissue the operation.

---

**R007061**  
**No SASL mechanism specified**

**Explanation:** An LDAP bind operation failed because it indicates it is using a SASL authentication method but does not specify the method.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the bind input to specify the SASL authentication method. Then reissue the operation.

---

**R007062**  
**The EXTERNAL SASL mechanism is not available for the connection**

**Explanation:** An LDAP bind operation using EXTERNAL (certificate) authentication failed because the connection is not set up to use SSL. SSL is required when performing an EXTERNAL bind.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the client to use SSL when performing an EXTERNAL bind. Then reissue the operation.

---

**R007063**  
**Client credentials may not be specified for the EXTERNAL SASL mechanism**

**Explanation:** An LDAP bind operation using EXTERNAL (certificate) authentication failed because it included the client credentials. This is not supported when using EXTERNAL authentication.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Remove the credentials from the bind input. Then reissue the operation.

---

**R007064**  
**Concurrent BIND requests are not supported**

**Explanation:** An LDAP bind operation failed because there is already a bind operation outstanding on the same connection. The previous bind operation must complete before a new one can be processed.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Wait for the previous bind operation to complete. Then reissue the operation.

---

**R007065**  
**No SASL BIND credentials**

**Explanation:** An LDAP bind operation using a SASL authentication method failed because the bind data are missing in the initial bind request or in follow-up client bind responses.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the client to send the credentials information during the initial bind request or follow-up client bind responses. Then reissue the operation.

---

**R007066**  
**Unable to accept GSSAPI security context:** Major 0xmajor_error, Minor 0xminor_error - error_text

**Explanation:** An LDAP bind operation using GSSAPI (Kerberos) authentication failed because the LDAP server cannot accept the Kerberos security context. The call to gss_accept_sec_context() does not succeed. See the description of this routine in z/OS Integrated Security Services Network Authentication Service Programming for more information about the error. The major and minor error codes and the error text from gss_accept_sec_context() are indicated in the reason code.

In the message text:

- major_error  
  - Major error code from gss_accept_sec_context()

- minor_error  
  - Minor error code from gss_accept_sec_context()

- error_text  
  - Error text corresponding to the error codes

**System action:** The LDAP server continues to run, but the operation fails.
User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Use the information in the reason code to assist in locating and correcting the problem.

R007067 Unexpected security token received for GSSAPI continuation

Explanation: An LDAP bind operation using GSSAPI (Kerberos) authentication failed because a follow-up bind response contained additional data that the LDAP server cannot process.

System action: The LDAP server continues to run, but the operation fails.

User response: Verify that the client is not creating an additional GSSAPI security token. Then reissue the operation. If the problem persists, contact the service representative.

R007068 Unable to wrap GSSAPI response:

Major 0xmajor_error, Minor 0xminor_error - error_text

Explanation: An LDAP bind operation using GSSAPI (Kerberos) authentication failed because the LDAP server cannot encrypt (wrap) a server negotiation. The call to gss_wrap() does not succeed. See the description of this routine in z/OS Integrated Security Services Network Authentication Service Programming for more information about the error. The major and minor error codes and the error text from gss_wrap() are indicated in the reason code.

In the message text:

major_error
Major error code from gss_wrap()

minor_error
Minor error code from gss_wrap()

error_text
Error text corresponding to the error codes

System action: The LDAP server continues to run, but the operation fails.

User response: Use the information in the reason code to resolve the problem. Then reissue the operation.

R007070 Requested GSSAPI security layer number is not supported

Explanation: An LDAP bind operation using GSSAPI (Kerberos) authentication failed because the client negotiation specifies a security layer service that is not supported by the LDAP server. The supported security layer values are: 1 (no security layer), 2 (integrity protection), and 4 (confidentiality protection). The requested security layer value is indicated in the reason code.

In the message text:

number
Security layer service

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the security layer service in the client negotiation. Then reissue the operation.

---

Chapter 6. Return and reason codes 297
R007072  Maximum GSSAPI receive length size is too small

Explanation: An LDAP bind operation using GSSAPI (Kerberos) authentication failed because the client negotiation specifies a maximum protocol message length that is too small. The message length must be at least 256.

In the message text:

size
Maximum message length

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the maximum message length in the client negotiation. Then reissue the operation.

R007073  Unable to get GSSAPI wrap size limit: Major 0xmajor_error, Minor 0xminor_error - error_text

Explanation: An LDAP bind operation using GSSAPI (Kerberos) authentication failed because the LDAP server cannot use the maximum protocol message length specified in the client negotiation. The call to gss_wrap_size_limit() does not succeed. See the description of this routine in z/OS Integrated Security Services Network Authentication Service Programming for more information about the error. The major and minor error codes and the error text from gss_wrap_size_limit() are indicated in the reason code.

In the message text:

major_error
Major error code from gss_wrap_size_limit()

minor_error
Minor error code from gss_wrap_size_limit()

error_text
Error text corresponding to the error codes

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Use the information in the reason code to assist in locating and correcting the problem.

R007076  No digest realm name is available

Explanation: An LDAP bind operation using CRAM-MD5 or DIGEST-MD5 authentication failed because the LDAP server cannot determine the name of the digest realm. The digest realm name can be specified in the digestRealm option in the LDAP server configuration file. If the option is not set in the configuration file, then the fully qualified host name of the LDAP server is used if a Domain Name Server (DNS) is active on the system. Otherwise, the name of the host processor is used. See the description of the digestRealm option in the Customizing the LDAP server configuration for more information about setting the digest realm.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Use any server messages and ERROR debug trace output to assist in locating and correcting the DNS problem. The digestRealm option
can be updated to specify a realm name if DNS is not active on the system. Then restart the LDAP server.

**R007077**  
**Explanation:** An LDAP bind operation using CRAM-MD5 or DIGEST-MD5 authentication because the client challenge response does not contain a user name and there is no bind distinguished name (DN) specified in the initial bind request. A name must be supplied in either the initial bind request or in the client challenge response.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the bind request processing so that it supplies either the bind DN, authorization DN, or the user name. Then reissue the operation.

**R007078**  
**HMAC digest in SASL BIND request is not valid**

**Explanation:** An LDAP bind operation using CRAM-MD5 authentication failed because the digest contained in the client challenge response cannot be converted. The value is not valid.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the digest in the client challenge response. Then reissue the operation.

**R007079**  
**The local Program Call interface supports just the EXTERNAL SASL mechanism**

**Explanation:** An LDAP bind operation received over the local Program Control (PC) interface failed because it does not use EXTERNAL authentication. Only EXTERNAL binds can be performed when using the local PC interface.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the bind input to use EXTERNAL authentication. Then reissue the operation.

**R007081**  
**Anonymous binds are not allowed and no bind distinguished name exists**

**Explanation:** An LDAP bind operation failed because the requester has not bound with a distinguished name and the LDAP server is configured to reject anonymous binds. The reason code can also occur when other operations and extended operations are requested from an unauthenticated client. The `allowAnonymousBinds` option in the LDAP server configuration file controls if anonymous binds are allowed and if operations can be performed from an unauthenticated client. See Customizing the LDAP server configuration for more information about this option.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** If binding, change the bind input to specify a distinguished name. Then reissue the operation. If anonymous binds are needed, contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** If requested, configure the LDAP server to allow anonymous binds by changing the value of the `allowAnonymousBinds` option to on in the LDAP server configuration file. Then restart the LDAP server.

**R007082**  
**An internal SSL error has been encountered**

**Explanation:** An LDAP operation failed because the LDAP server detects a problem when using SSL. This can occur when trying to map a certificate used in an EXTERNAL (certificate) bind operation to a RACF user.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Use any messages and ERROR debug trace output to assist in locating and correcting the problem. If certificate mapping is not needed, set the `sslMapCertificate` option to off in the LDAP server configuration file. Then restart the LDAP server. If the problem persists, contact the service representative.

**R007083**  
**Authentication with a reserved bind DN is not allowed**

**Explanation:** An LDAP bind operation failed because the requester tries to bind using a DN that is reserved for usage by the LDAP server. In particular, a bind using EXTERNAL (certificate) authentication cannot specify a bind DN such as `cn=thisthis`.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the bind input to not use a reserved DN. Then reissue the operation.

**R008001**  
**LDBM backend database is disabled**

**Explanation:** An LDAP operation failed because the LDBM backend is in disabled state. This state can occur when the LDBM backend cannot recover from a problem.

**System action:** The LDAP server continues to run, but the operation fails.
**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Use any server messages and ERROR debug trace output to assist in locating and correcting the problem. Then restart the LDAP server. If the problem persists, contact the service representative.

---

**R008003  Multiple entries contain uid 'userid'**

**Explanation:** An LDAP bind operation using CRAM-MD5 or DIGEST-MD5 authentication failed because there is more than one entry in an LDBM backend that contains the user ID specified in the bind information. The LDAP server does not know which entry to use for bind processing. The user ID is indicated in the reason code.

In the message text:

`userid`

User ID used in the bind operation

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Use an LDAP search operation with the filter `uid=userid` to determine which entries in the LDBM backend contain the indicated user ID. Modify the `uid` attribute in the entries so that only the entry you want to bind with has the indicated value. Then reissue the operation.

---

**R008004  Clear password is not available**

**Explanation:** An LDAP bind operation using CRAM-MD5 or DIGEST-MD5 authentication failed because it cannot decrypt a value for the `userPassword` attribute in the entry that contains the bind distinguished name (DN) or user ID specified in the bind information. The `userPassword` values in the entry must be either in the clear or encrypted using a two-way encryption algorithm.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** If a user ID is only specified in the bind information, use an LDAP search operation with the filter `uid=userid` to determine which entry contains the indicated user ID. Modify the entry to remove all the `userPassword` values that are not in the clear or encrypted using a two-way algorithm. Then reissue the operation.

---

**R008005  Nested group recursion detected for group 'name'**

**Explanation:** An LDAP operation or utility failed because a nested group loop has been detected in the backend. For example, a nested group loop is detected when group A includes group B as an `ibm-memberGroup` value while group B also includes group A as an `ibm-memberGroup` value. See Nested groups for more information. The group entry is indicated in the reason code.

In the message text:

`name`

Distinguished name of group

**System action:** The LDAP server continues to run, but the operation or utility fails.

**User response:** Either remove or update the `ibm-memberGroup` attribute value to avoid introducing a nested group loop in the operation or utility input. Then reissue the operation.

---

**R008006  Dynamic group search filter 'value' is not valid**

**Explanation:** An LDAP operation or utility failed because it involves a dynamic group whose filter value is not acceptable. See Dynamic groups for more information. The filter value is indicated in the reason code.

In the message text:

`value`

Filter value

**System action:** The LDAP server continues to run, but the operation or utility fails.

**User response:** Correct the filter value in the operation or utility input. Then reissue the operation.

---

**R008007  No base entry specified in dynamic group URL 'url'**

**Explanation:** An LDAP operation or utility failed because the `memberURL` attribute value specifying the dynamic group search expression does not contain a base entry. A base entry is required in a dynamic group URL. The format of a dynamic group URL is:

```
ldap:///baseDN[??[searchScope][?searchFilter]]
```

See Dynamic groups for more information. The dynamic group URL is indicated in the reason code.

In the message text:

`url`

Dynamic group URL

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Update the `memberURL` attribute value to specify a baseDN in the operation or utility input. Then reissue the operation.

---

**R008008  An internal LDBM backend error has occurred**

**Explanation:** An LDAP operation failed because the LDAP server has detected an internal programming error in the LDBM backend.
R008010  Subtree move is not supported by the replica servers

Explanation: An LDAP modify DN operation failed because it tries to move a subtree to another subtree but a replica of the LDAP server does not support this type of rename. This operation is only allowed if all the server replicas support it.

System action: The LDAP server continues to run, but the operation fails.

User response: Change the modify DN input so that it does not specify a new superior for a subtree entry. Then reissue the operation. Alternatively, contact an LDAP administrator to change the replica servers so that they support modify DN operations that move subtrees. After the problem is resolved, reissue the operation.

Administrator response: If the replica server can support modify DN operations with subtree move, restart the replica with that capability enabled. The replica server must return 1.3.18.0.2.32.33 as one of the values of the ibm-enabledCapabilities attribute when searching the root DSE entry.

R008013  DN attribute realignment is not supported by the replica servers

Explanation: An LDAP modify DN operation failed because it tries to realign other DN attributes included in the operation but a replica of the LDAP server does not support this type of modify DN. This operation is only allowed if all the server replicas support it.

System action: The LDAP server continues to run, but the operation fails.

User response: Change the modify DN input so that it does not include the control. Then reissue the operation. Alternatively, contact an LDAP administrator to change the replica servers so that they support realignment. After the problem is resolved, reissue the operation.

Administrator response: If the replica server can support realignment of other DN attributes, restart the replica with this capability enabled. The replica server must return 1.3.18.0.2.10.11 as a value of the supportedControl attribute when searching the root DSE entry.

R008014  Value value for attribute name is not valid

Explanation: An LDAP add or modify operation involving a basic replica entry failed because it specifies an attribute value that is not valid. A basic replica entry is one that contains the replicaObject object class. See [Basic replication](#) for more information. The name and value of the attribute are indicated in the reason code.
In the message text:

value
  Attribute value

name
  Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the add or modify input to specify a value that is valid for the attribute. Then reissue the operation.

R008015  Value value for attribute name is out of range

Explanation: An LDAP add or modify operation involving a basic replica entry failed because it specifies an attribute value that is not valid. A basic replica entry is one that contains the replicaObject object class. In particular, the replicaPort attribute value must be within 0 to 65535. See [Basic replication] for more information. The name and value of the attribute are indicated in the reason code.

In the message text:

value
  Attribute value

name
  Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the add or modify input to specify a value that is valid for the attribute. Then reissue the operation.

R008017  Password policy entry 'name' is in use and cannot be deleted

Explanation: An LDAP delete operation failed because the entry is a password policy entry that is in use by a user or a group. A password policy entry can only be deleted when it is no longer referenced from another entry. The distinguished name of the password policy entry is indicated in the reason code.

In the message text:

name
  Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: Determine which entries are referencing the password policy entry by searching the server using the filter (|(ibm-pwdIndividualPolicyDN=name)(ibm-pwdGroupPolicyDN=name)). Remove or change these values in these attributes in the entries. Then reissue the operation.

R008018  Value for attribute 'name' must be positive

Explanation: An LDAP add or modify operation failed because it tries to set an attribute value that is not valid for the attribute. The value must be a number greater than or equal to 0. The name of the attribute is indicated in the reason code.

In the message text:

name
  Attribute name

R008019  Value for attribute 'name' must be less than value

Explanation: An LDAP add or modify operation failed because it tries to set an attribute value that is not valid for the attribute. The value must be a number less than the maximum value indicated in the reason code. The name of the attribute is also indicated in the reason code.

In the message text:

name
  Attribute name

value
  Maximum value

System action: The LDAP server continues to run, but the operation fails.
User response: Correct the attribute value in the operation input. Then reissue the operation.

R008020  Value for attribute 'name1' must be less than value for attribute 'name2'

Explanation: An LDAP add or modify operation failed because it tries to set an attribute value that is not valid for the attribute when used with another attribute in the entry. The value of the first attribute indicated in the reason code must be less than the value of the second attribute indicated in the reason code.

In the message text:

name1  First attribute name
name2  Second attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that the values are appropriate. Then reissue the operation.

R008021  Value for attribute 'name1' cannot be greater than value for attribute 'name2'

Explanation: An LDAP add or modify operation failed because it tries to set an attribute value that is not valid for the attribute when used with another attribute in the entry. The value of the first attribute indicated in the reason code must be less than or equal to the value of the second attribute indicated in the reason code.

In the message text:

name1  First attribute name
name2  Second attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that the first attribute value is not larger than the second one. Then reissue the operation.

R008022  passwordMinAlphaChars plus passwordMinOtherChars must be less than pwdMinLength

Explanation: An LDAP add or modify operation failed because it tries to set an attribute value that is not valid for the attribute when used with other attributes in the entry. The values must be set so that the sum of the passwordMinAlphaChars and passwordMinOtherChars values is less than the pwdMinLength value.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that the values are appropriate. Then reissue the operation.

R008023  Must allow a user to change their password if they are required to change their password

Explanation: An LDAP add or modify operation failed because it tries to set an attribute value that is not valid for the attribute when used with another attribute in the entry. The pwdAllowUserChange attribute value cannot be FALSE when the pwdMustChange attribute value is TRUE.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that the values are appropriate. Then reissue the operation.

R008024  Password policy entry 'name' is in use and cannot be renamed

Explanation: An LDAP modify DN operation failed because the entry is a password policy entry that is in use by a user or a group. A password policy entry can only be renamed when it is no longer referenced from another entry. The distinguished name of the password policy entry is indicated in the reason code.

In the message text:

name  Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: Determine which entries are referencing the password policy entry by searching using the filter (|(ibm-pwddIndividualPolicyDN=\"name\")(ibm-pwddGroupPolicyDN=\"name\")). Remove or change these values in these attributes in the entries. Then, reissue the operation.

R008025  Password policy entry 'name' is in use and cannot have objectclass pwdpolicy removed

Explanation: An LDAP modify operation failed because it changes the entry from a password policy entry to a non-password policy entry, but the entry is in use by a user or a group. A password policy entry can only be changed to a non-password policy entry when it is no longer referenced from another entry. The distinguished name of the password policy entry is indicated in the reason code.

In the message text:
**R008101 • R008107**

**name**
Distinguished name of entry

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Determine which entries are referencing the password policy entry by searching using the filter `(|(ibm-pwdIndividualPolicyDN=name)(ibm-pwdGroupPolicyDN=name))`. Remove or change these values in these attributes in the entries. Then reissue the operation.

---

**R008101**  
**TDBM backend database is disabled**

**Explanation:** An LDAP operation involving a TDBM backend failed or partially failed because the TDBM backend is not enabled. TDBM cannot process the operation.

**System action:** The LDAP server continues to run. If the operation is targeted to the TDBM backend, the operation fails. For a bind to a different backend, the bind succeeds but the disabled TDBM backend is skipped when determining the groups to which the bound user belongs. Also, for a Kerberos bind, the disabled TDBM backend is not used to map the Kerberos identity to a TDBM distinguished name.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Use any server messages and ERROR debug trace output to assist in determining why the TDBM backend is not active. If necessary, restart the LDAP server.

---

**R008103**  
**Multiple entries contain uid 'userid'**

**Explanation:** An LDAP bind operation using CRAM-MD5 or DIGEST-MD5 authentication failed because there is more than one entry in a TDBM backend that contains the user ID specified in the bind information. The LDAP server does not know which entry to use for bind processing. The user ID is indicated in the reason code.

In the message text:

*userid*

- User ID used in the bind operation

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Use an LDAP search operation with the filter `uid=userid` to determine which entry contains the indicated user ID. Modify the `uid` attribute in the entries so that only the entry you want to bind with has the indicated value. Then reissue the operation.

---

**R008104**  
**Clear password is not available**

**Explanation:** An LDAP bind operation using CRAM-MD5 or DIGEST-MD5 authentication failed because it cannot decrypt a value for the `userPassword` attribute in the entry that contains the bind distinguished name (DN) or user ID specified in the bind information. The `userPassword` values in the entry must be either in the clear or encrypted using a two-way encryption algorithm.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** If a user ID is only specified in the bind information, use an LDAP search operation with the filter `uid=userid` to determine which entry contains the indicated user ID. Modify the entry to remove all the `userPassword` values that are not in the clear or encrypted using a two-way algorithm. Then reissue the operation.

---

**R008106**  
**Dynamic group search filter 'value' is not valid**

**Explanation:** An LDAP operation or utility failed because it involves a dynamic group whose filter value is not acceptable. See [Dynamic groups](#) for more information. The filter value is indicated in the reason code.

In the message text:

*value*

- Filter value

**System action:** The LDAP server continues to run, but the operation or utility fails.

**User response:** Correct the filter value in the operation or utility input. Then reissue the operation.

---

**R008107**  
**Non-numeric object identifier 'identifier' is not allowed when using a TDBM database with DB_VERSION less than 4.0**

**Explanation:** An LDAP schema modify operation failed because a non-numeric object identifier is used in an object class or attribute modification but a TDBM backend is running at a level that only supports usage of numeric identifiers. The value of the `DB_VERSION` column in the `DIR_MISC` table in the TDBM DB2 database must be 4.0 or higher to allow usage of non-numeric identifiers. The identifier is indicated in the reason code.

In the message text:

*identifier*

- Non-numeric identifier

**System action:** The LDAP server continues to run, but the operation fails.
User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Specify a value of at least 4 for the srvCompatLevel option in the LDAP server configuration file. Then restart the LDAP server. Alternatively, update DB_VERSION value directly in DB2 after the LDAP server has been stopped. Then restart the LDAP server.

R008108  No base entry specified in dynamic group URL 'url'

Explanation: An LDAP operation or utility failed because the memberURL attribute value specifying the dynamic group search expression does not contain a base entry. A base entry is required in a dynamic group URL. The format of a dynamic group URL is: ldap:///baseDN[?searchScope][?searchFilter] See Dynamic groups for more information. The dynamic group URL is indicated in the reason code.

In the message text:
url  Dynamic group URL

System action: The LDAP server continues to run, but the operation or utility fails.

User response: Update the memberURL attribute value to specify a baseDN in the operation or utility input. Then reissue the operation.

R008109  Unable to connect to DB2 subsystem 'name'

Explanation: An LDAP operation failed because a connection could not be established with the DB2 subsystem. This may occur because the DB2 subsystem is down or the DB2 connections have been exhausted. The DB2 subsystem is required when communicating with the TDBM or DB2-based GDBM backend while the LDAP server is running. The DB2 subsystem name is indicated in the reason code.

In the message text:
name  DB2 subsystem name

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: If the DB2 subsystem is down, the subsystem must be brought back up. If the DB2 subsystem is running, verify that there are enough DB2 connections. See [Installing and setting up DB2 for TDBM and GDBM (DB2-based)] for more information. If there are enough DB2 connections, use any server messages and server debug ERROR+PERF+TDBM trace output to assist in locating and correcting the problem.

If the problem persists, contact the service representative.

R008110  Unable to read an entry from the DB2 database

Explanation: An LDAP operation failed because the entry could not be read from the TDBM or DB2-based GDBM backend.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Use any server messages and ERROR+PERF+TDBM debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

R008111  Unable to update an entry in the DB2 database

Explanation: An LDAP operation failed because the entry could not be updated in the TDBM or DB2-based GDBM backend.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Use any server messages and ERROR+PERF+TDBM debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

R008112  Unable to add an entry to the DB2 database

Explanation: An LDAP operation failed because the entry could not be added to the TDBM or DB2-based GDBM backend.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Use any server messages and ERROR+PERF+TDBM debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

R008113  Unable to delete an entry from the DB2 database

Explanation: An LDAP operation failed because the entry could not be deleted from the TDBM or DB2-based GDBM backend.
**R008114**  
Unable to commit the changes to the DB2 database

**Explanation:** An LDAP operation failed because the changes could not be committed to the TDBM or DB2-based GDBM backend.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Use any server messages and ERROR+PERF+TDBM debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

---

**R008115**  
An internal TDBM backend error has occurred

**Explanation:** An LDAP operation failed because the LDAP server has detected an internal programming error in the TDBM backend.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Use any server messages and ERROR+PERF+TDBM debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

---

**R008116**  
DB2 subsystem 'name' is not available

**Explanation:** An LDAP operation failed because the DB2 subsystem is down or a connection cannot be established. The DB2 subsystem is required when communicating with the TDBM or DB2-based GDBM backend when the LDAP server is running. The DB2 subsystem name is indicated in the reason code.

In the message text:

```
name
```

DB2 subsystem name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

---

**R008117**  
Attribute object identifier 'identifier' is longer than 200 characters

**Explanation:** An LDAP schema modify operation failed because an attribute object identifier that is too long for usage in TDBM appears in a modification. The maximum length of an object identifier in TDBM is 200. The identifier is indicated in the reason code.

In the message text:

```
identifier
```

Attribute identifier

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the identifier in the modify input to have an acceptable length. Then reissue the operation.

---

**R008118**  
Object class name 'name' is longer than 200 characters

**Explanation:** An LDAP schema modify operation failed because an object class name that is too long for usage in TDBM appears in a modification. The maximum length of an object class name in TDBM is 200. The name is indicated in the reason code.

In the message text:

```
name
```

Object class name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the object class name in the modify input to have an acceptable length. Then reissue the operation.

---

**R008119**  
DN 'name' exceeds the maximum length of size

**Explanation:** An LDAP add or modify DN operation failed because a distinguished name (DN) involved in the operation is too long for usage in TDBM. This DN can be the target of the operation or, for a modify DN, another DN affected by renaming the target DN. The maximum DN length in TDBM is the size set for the DN column in the DIR_ENTRY table when TDBM DB2 database is created. The DN that is too long and the maximum allowed length of a TDBM DN are indicated in the reason code.

In the message text:

```
name
```

DB2 subsystem name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.
**R008120**  
**Subtree move is not supported by the replica servers**

**Explanation:** An LDAP modify DN operation failed because it tries to move a subtree to another subtree but a replica of the LDAP server does not support this type of modify DN. This operation is only allowed if all the server replicas support it.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the modify DN input so that it does not specify a new superior for a subtree entry. Then reissue the operation. Alternatively, contact an LDAP administrator to change the replica servers so that they support modify DN operations that move leaf entries. After the problem is resolved, reissue the operation.

**Administrator response:** If the replica server can support modify DN operations with leaf or subtree move, restart the replica with either or both of those capabilities enabled. The replica server must return 1.3.18.0.2.32.35 or 1.3.18.0.2.32.33 (or both) as values of the `ibm-enabledCapabilities` attribute when searching the root DSE entry.

**R008123**  
**DN attribute realignment is not supported by the replica servers**

**Explanation:** An LDAP modify DN operation failed because the `IBMMODIFYDNREALIGNDNATTRIBUTESCONTROL` control to realign other DN attributes is included in the operation but a replica of the LDAP server does not support this type of modify DN. This operation is only allowed if all the server replicas support it.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Change the modify DN input so that it does not include the control. Then reissue the operation. Alternatively, contact an LDAP administrator to change the replica servers so that they support realignment. After the problem is resolved, reissue the operation.

**Administrator response:** If the replica server can support realignment of other DN attributes, restart the
replica with this capability enabled. The replica server must return 1.3.18.0.2.10.11 as a value of the supportedControl attribute when searching the root DSE entry.

R008124 Changelog root must have an explicit and propagating ACL

Explanation: An LDAP modify operation to a DB2-based GDBM failed because it deletes the aclEntry or entryOwner attribute in the change log suffix entry (cn=changelog). The change log suffix entry must always have explicit values for these attributes when GDBM is DB2-based. These values are always propagated to the entries in the change log to provide access control for these entries.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the modify input so that it does not remove all the values for the aclEntry or entryOwner attribute. Then reissue the operation.

R008125 Matching rule 'rule' is not supported for syntax 'syntax (description)' when using a TDBM database with DB_VERSION less than 4.0

Explanation: An LDAP schema modify operation failed because a modified attribute includes a matching rule and syntax combination that is not supported in a TDBM backend. The TDBM backend is running at an older level that does not allow the combination. The matching rule and the syntax are indicated in the reason code. The combinations that are not supported by a TDBM backend running at an older level are:

- integerFirstComponentMatch equality rule with Integer syntax
- objectIdentifierFirstComponentMatch equality rule with Object Identifier syntax
- generalizedTimeMatch equality rule with UTC Time syntax

In the message text:

descriptor
   Descriptor that is not valid

description
   Syntax description

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that all the descriptors are valid. Then reissue the operation.

R010001 Invalid character in descriptor 'descriptor'

Explanation: An LDAP operation failed because it involves a descriptor value that contains a character that is not allowed in a descriptor. A text descriptor consists of letters, numbers, dash, underscore, and semicolon, while an object identifier descriptor consists of digits separated by periods. An object identifier can optionally be prefixed with oid:. When used within a schema definition, a text descriptor cannot contain a semicolon and must start with a letter. The descriptor is indicated in the reason code.

In the message text:

descriptor
   Descriptor that is not valid

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that all the descriptors are valid. Then reissue the operation.

R010002 Missing attribute type in DN component 'component'

Explanation: An LDAP operation failed because it involves a distinguished name (DN) in which one of the components has an attribute value without an attribute. For example, in the DN cn=fred,=test,o=ibm, the =test,o=ibm component contains a value (test)
without an attribute. The component with the missing attribute is indicated in the reason code.

In the message text:

```
component
    Component of the DN
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the operation input so that all the distinguished names that it uses are complete. Then reissue the operation.

---

**R010003  Missing attribute value in DN component 'component'**

**Explanation:** An LDAP operation failed because it involves a distinguished name (DN) in which one of the components has an attribute without a value. For example, in the DN `cn=fred,ou=,o=ibm`, the `ou=,o=ibm` component contains an attribute (ou) without a value. The component with the missing value is indicated in the reason code.

In the message text:

```
component
    Component of the DN
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the operation input so that all the distinguished names that it uses are complete. Then reissue the operation.

---

**R010004  No equality matching rule for DN attribute 'name'**

**Explanation:** An LDAP operation failed because it involves a distinguished name (DN) which contains an attribute whose schema definition does not include an equality matching rule. The name of the attribute is indicated in the reason code.

In the message text:

```
name
    Attribute name
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the operation input so that every DN uses attributes that have an equality matching rule. Then reissue the operation.

---

**R010005  No matching rule defined for string value 'value'**

**Explanation:** An LDAP operation such as a compare or search failed because it involves a comparison using a value for an attribute whose schema definition does not include a matching rule that allows comparing the value. In particular, some matching rules, such as `booleanMatch`, do not support using a value in a substring filter.

In the message text:

```
value
    Attribute value
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the value used in the operation input so that it uses attribute values that are supported for the type of usage. Then reissue the operation.

---

**R010006  UTC Time value 'value' is not valid**

**Explanation:** An LDAP operation failed because an attribute value involved in the operation contains a character that is not allowed by the UTC Time syntax of the attribute. The format of a UTC Time value is

- `yyymmddhhmmssffffff` for local time
- `yyymddhhmssffffffZ` for Greenwich Mean Time
- `yyymddhhmssffffff-hhmm` for time zone west of GMT
- `yyymddhhmssffffff+hhmm` for time zone east of GMT

where `yy` is year, `mm` is month, `dd` is day, `hh` is hour, `mm` is minutes, `ss` is seconds, and `ffffff` is microseconds. The seconds (`ss`) and microseconds (`ffffff`) can be omitted and default to 0. The value that is not valid is indicated in the reason code.

In the message text:

```
value
    Attribute value
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the value used in the operation input so that it is valid for the UTC Time syntax. Then reissue the operation.

---

**R010007  Invalid IA5 character found in string value 'value'**

**Explanation:** An LDAP operation failed because an attribute value involved in the operation contains a character that is not allowed by the IA5 String syntax of the attribute. The characters that can be used in an IA5 String are those that translate to the 7-bit ASCII characters. Note that the null character (x'00') is a valid IA5 String character. The value that is not valid is indicated in the reason code.

In the message text:

```
value
    Attribute value
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the operation input so that every DN uses attributes that have an equality matching rule. Then reissue the operation.
R010008 • R010014

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the value used in the operation input so that it is valid for the IA5 String syntax. Then reissue the operation.

---

R010008 Bit string value 'value' is not valid

Explanation: An LDAP operation failed because an attribute value involved in the operation contains a character that is not allowed by the bit string syntax of the attribute. A complete bit string value must be a series of 0 and 1 characters enclosed in single quote marks and suffixed with b or B. The value must contain at least one 0 or 1. An example is '01011'B. A substring value used in a substring filter can be any part of the complete value, and does not have to contain a 0 or 1. An example is '1'. The value that is not valid is indicated in the reason code.

In the message text:

value

Attribute value

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the value used in the operation input so that it is valid for the bit string syntax. Then reissue the operation.

---

R010009 Boolean value 'value' is not valid

Explanation: An LDAP operation failed because an attribute value involved in the operation contains a value that is not allowed by the Boolean syntax of the attribute. A Boolean value must be TRUE or FALSE, with case ignored. The value that is not valid is indicated in the reason code.

In the message text:

value

Attribute value

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the value used in the operation input so that it is valid for the Boolean syntax. Then reissue the operation.

---

R010011 Telephone number value 'value' is not valid

Explanation: An LDAP operation failed because an attribute value involved in the operation contains a character that is not allowed by the Telephone Number syntax of the attribute. The characters that can be used in a Telephone Number value are: letters, numbers, double quote, open parens, close parens, plus sign, comma, dash, period, forward slash, colon, question mark, and space. Note that the quote character is not allowed for a Telephone Number value. The value that is not valid is indicated in the reason code.

In the message text:

value

Attribute value

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the value used in the operation input so that it is valid for the Telephone Number syntax. Then reissue the operation.

---

R010012 UUID value 'value' is not valid

Explanation: An LDAP operation failed because an attribute value involved in the operation contains a character that is not allowed by the IBM Entry UUID syntax of the attribute. A complete IBM Entry UUID value is a 36-character string composed of groups of hexadecimal digits separated by hyphens in the following format: 8_digits-4_digits-4_digits-4_digits. An example is 55A4C000-B93F-1A5C-86B3-402084027431. A substring value used in a substring filter can be any part of the complete value. An example is 4C000-893F-1A. The value that is not valid is indicated in the reason code.

In the message text:

value

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the value used in the operation input so that it is valid for the IBM Entry UUID syntax. Then reissue the operation.

---

R010014 Country string value 'value' is not valid

Explanation: An LDAP operation failed because an attribute value involved in the operation contains a character that is not allowed by the Country String syntax of the attribute. A complete Country String value must consist of exactly two of the following characters: letters, numbers, quote, open parens, close parens, plus sign, comma, dash, period, forward slash, colon, question mark, and space. A substring value used in a substring filter can be one or two of those characters. The value that is not valid is indicated in the reason code.

In the message text:

value

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the value used in the operation input so that it is valid for the Country String syntax. Then reissue the operation.
R010015  No backend for DN ‘name’

Explanation: An LDAP operation (or extended operation) failed because the distinguished name (DN) of the target of the operation either does not fall under any backend in the LDAP server or falls under a backend which does not support that operation. The backend is determined using the suffix part of the DN of the target of the operation. In particular, the GetEffectiveAcl extended operation is only supported by LDBM, TDBM, GDBM, CDBM, and schema backends. Similarly, the Effective password policy and Account status extended operations are not supported by the SDBM backend. The DN of the target is indicated in the reason code.

In the message text:

name
   Distinguished name of target

System action: The LDAP server continues to run, but the operation fails.

User response: Change the target of the operation to be in an existing backend that supports the operation. Then reissue the operation.

R010016  Backend initialization failed for DN ‘name’

Explanation: An LDAP operation or utility failed because the backend to which it is targeted did not complete initialization, thus cannot process the operation. The backend is determined using the suffix part of the distinguished name (DN) of the target of the operation. For a change log request, the target is the GDBM backend (suffix is cn=changeLog). The DN of the target is indicated in the reason code.

In the message text:

name
   Distinguished name of target

System action: The LDAP server continues to run, but the operation fails.

User response: Change the target of the operation to be in a backend that is active. Then reissue the operation.

R010017  operation is not supported by the type backend

Explanation: An LDAP operation failed because the backend to which it is targeted does not support that type of operation. In particular, the schema (suffix is cn=schema), root DSE (suffix is zero-length string, ""), and monitor (suffix is cn=monitor) backends are very limited in the operations they allow. The schema backend is restricted to modify and search operations. The root DSE and cn=monitor backends are restricted to search operations. The name of the operation and the type of targeted backend are indicated in the reason code.

In the message text:

operation
   Operation name

   type
   Backend type

System action: The LDAP server continues to run, but the operation fails.

User response: Do not issue the unsupported operation for this type of backend.

R010018  Search with null base DN requires either scope=base (for root DSE search) or scope=subtree (for null based subtree search)

Explanation: An LDAP search operation using the null based distinguished name (search target is the zero-length string, or "") failed because the search scope is not base or subtree. The scope of a null based search must be either base or sub. A base scope search retrieves the attributes in the root DSE entry. This search requires that the filter is objectclass=* . A sub scope search retrieves all the entries in the LDBM, TDBM, and CDBM backends of the LDAP server. Any search filter can be used with this scope.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the null based search input. Then reissue the operation.

R010019  Search with null base DN requires filter (objectclass=*)

Explanation: An LDAP search operation using the null based distinguished name (search target is the zero-length string, or ") failed because the search filter is not objectclass=*. This is the only filter supported when using a null based search to retrieve the attributes of the root DSE entry.

System action: The LDAP server continues to run, but the operation fails.
R010020  Schema search requires scope=base
Explanation: An LDAP search operation for the schema entry failed because the search scope specified in the operation is not base. To search the schema entry, specify a target of cn=schema, a scope of base, and a filter of objectclass=* or objectclass=name, where name is ibmsubschema, subentry, subschema, or top.
System action: The LDAP server continues to run, but the operation fails.
User response: Correct the schema search input. Then reissue the operation.

R010021  Schema search requires an object class presence or equality filter
Explanation: An LDAP search operation for the schema entry failed because the search filter is not supported when searching the schema. To search the schema entry, specify a target of cn=schema, a scope of base, and a filter of objectclass=* or objectclass=name where name is ibmsubschema, subentry, subschema, or top.
System action: The LDAP server continues to run, but the operation fails.
User response: Correct the schema search input. Then reissue the operation.

R010022  Binary option is not supported by the type backend
Explanation: An LDAP search operation failed because the search specifies attributes to be returned with the binary option but the backend to which the search is targeted does not support the binary option. The binary option is specified by appending .binary to the attribute to be returned, for example cn;binary. In particular, the schema (suffix is cn=schema), root DSE (suffix is zero-length string, ""), and monitor (suffix is cn=monitor) backends do not support using the binary option. The type of targeted backend is indicated in the reason code.
In the message text:

type
    Backend type

System action: The LDAP server continues to run, but the operation fails.
User response: Remove the binary option from the attributes to be returned in the search input. Then reissue the operation.
operation input or ensure that there is a properly encoded control value. Then reissue the operation.

R010027  Control 'identifier' is specified multiple times

Explanation:  An LDAP operation failed because the operation contains the same server control more than once. Some controls cannot be specified multiple times. The identifier of the control is indicated in the reason code.

In the message text:

identifier
Server control identifier

System action:  The LDAP server continues to run, but the operation fails.

User response:  Remove the extra server controls from the operation input. Then reissue the operation.

R010028  Critical control 'identifier' cannot be processed

Explanation:  An LDAP operation failed because the operation contains a server control sent as critical but an error occurs when the server tries to process the control. An operation is rejected if the server cannot use a critical control. For example, a search containing the SortedResults control (identifier is 1.2.840.113556.1.4.473) fails if there is a problem decoding the sort keys and the control is critical. The identifier of the control is indicated in the reason code.

In the message text:

identifier
Server control identifier

System action:  The LDAP server continues to run, but the operation fails.

User response:  If sorting is needed, ensure that the control contents are valid. If sorting is not needed, remove the control or send it as non-critical. Then reissue the operation.

R010030  Unable to compute search message digest

Explanation:  An LDAP search operation failed because the server cannot create a digest representing the search parameters (base, scope, filter, controls, etc). This is used to ensure that each successive search operation for the next page of results matches the original search criteria.

In the message text:

identifier
Server control identifier

System action:  The LDAP server continues to run, but the operation fails.

User response:  Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response:  Use any server messages and ERROR debug trace output to assist in locating and solving the problem. If the problem persists, contact the service representative.
User response: Correct the paged search input so that the initial page size in the PagedResults control is not 0. Then reissue the operation.

R010032 Paged search results not found

Explanation: An LDAP search operation to obtain the next page of results for a search failed because the server cannot find the search results identified in the PagedResults control (identifier is 1.2.840.113556.1.4.319) in the continuation search request.

System action: The LDAP server continues to run, but the operation fails.

User response: Specify a valid cookie on the paged search request. To obtain the next page of search results, the cookie specified on the paged search request must be the cookie returned by the previous paged search response. Then reissue the operation.

R010033 Continuation search request not same as initial request

Explanation: An LDAP search operation to obtain the next page of results for a search failed because the search criteria (base, scope, filter, controls, etc.) are not the same as for the initial search. The continuation search request must match the initial search request.

System action: The LDAP server continues to run, but the operation fails.

User response: Specify a paged search request with all values identical to the initial request, except for the message ID, the cookie, and optionally a modified pageSize. Then reissue the operation.

R010034 Unknown LDAP message type type

Explanation: An LDAP operation failed because the type of operation is not supported by the LDAP server. The message (operation) type is indicated in the reason code.

In the message text:

<table>
<thead>
<tr>
<th>type</th>
<th>Message type</th>
</tr>
</thead>
</table>

System action: The LDAP server continues to run, but the operation fails.

User response: Do not issue this type of operation to the LDAP server.

R010035 Binary attribute type 'name' not allowed in DN

Explanation: An LDAP operation failed because a distinguished name (DN) involved in the operation contains a binary attribute. Binary attributes cannot be used within a DN. A binary attribute has one of the following syntaxes: Binary, Certificate, Certificate List, Certificate Pair, Fax, JPEG, or Octet String. The name of the binary attribute is indicated in the reason code.

In the message text:

| name | Attribute name |

System action: The LDAP server continues to run, but the operation fails.

User response: Remove the binary attribute from the distinguished name. Then reissue the operation.

R010036 No value provided for attribute 'name'

Explanation: An LDAP operation failed because an attribute without a value is included in the operation. This can occur, for example, if an add or modify operation does not specify any value for an attribute being added or replaced (note that a value does not need to be specified for an attribute being deleted - this deletes the entire attribute). The name of the attribute is indicated in the reason code.

In the message text:

| name | Attribute name |

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input to specify a value where appropriate for all attributes. Then reissue the operation.

R010037 Binary transfer is not supported for non-binary attribute type 'name'

Explanation: An LDAP operation failed because an attribute involved in the operation specifies binary transfer but the attribute is not a binary attribute. The server can only use binary transfer when processing a binary attribute. Binary transfer is specified by appending ;binary to the attribute, for example cn;binary. An attribute is binary if it has one of the following syntaxes: Binary, Certificate, Certificate List, Certificate Pair, Fax, JPEG, or Octet String. This error can occur when specifying the attribute in the operation input, including in the filter of a search operation.

In the message text:

| name | Attribute name |

System action: The LDAP server continues to run, but the operation fails.

User response: Remove the binary transfer option from the attribute in the operation input. Then reissue the operation.
R010039 Incorrect ASN.1 encoding in DN

Explanation: An LDAP operation failed because it involves a distinguished name (DN) in which one of the components has an attribute value which begins with a number sign (#) but is not a valid ASN.1 encoded value. A number sign is used at the beginning of an attribute value in a DN to indicate that the value is ASN.1-encoded value. The number sign must be followed by an even number of hexadecimal digits representing the encoding of each of the octets of the BER encoding of the value. The component with the incorrect attribute value is indicated in the reason code.

In the message text:

component

Component of the DN

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that all the distinguished names that it uses are acceptable. Then reissue the operation.

R010040 Unsupported ASN.1 type in DN

Explanation: An LDAP operation failed because it involves a distinguished name (DN) in which one of the components has an attribute value which is not supported. This can occur if the value is ASN.1 encoded (it begins with a number sign (#)) but the underlying value syntax is not supported by the server. It can also result from using an attribute which has generalizedTimeMatch or utcTimeMatch as its equality matching rule. The server does not allow using attributes with these matching rules in a DN. The component with the unsupported value is indicated in the reason code.

In the message text:

component

Component of the DN

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input so that all the distinguished names that it uses are acceptable. Then reissue the operation.

R010041 Server control does not have an object identifier

Explanation: An LDAP operation failed because the operation contained a server control that does not contain an identifier. The server does not know how to decode the control.

System action: The LDAP server continues to run, but the operation fails.

R010042 Definition has no components: definition

Explanation: An LDAP schema modify operation failed because there is no value after a left parenthesis in the definition of an attribute, object class, or ibmattributetypes. The part of the definition that is in error is indicated in the reason code. See LDAP directory schema for more information about the format for the definitions of the various elements of the schema. The reason code may also occur on an entry add or modify operation when adding a value that has no characters after the beginning left parenthesis for an attribute that is defined with the integerFirstComponentMatch matching rule. In this case, the value is indicated in the reason code.

In the message text:

definition

Attribute or object class definition or value

System action: The LDAP server continues to run, but the operation fails.

User response: For a schema modify operation, check the input to ensure that all the definitions are correctly formatted. For an entry add or modify operation, add characters after the left parenthesis at the beginning of the value for the attribute defined with the integerFirstComponentMatch matching rule. Then reissue the operation.

R010043 Substring filter for attribute 'name' has no value

Explanation: An LDAP search operation failed because it uses a substring filter in which one of the substring parts has no value. Every part of a substring filter must contain a non-zero length string. The name of the attribute in the substring filter is indicated in the reason code.

In the message text:

name

Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the search input so that every part of the substring filter has a value. Then reissue the operation.

R010044 Substring filter type type is used incorrectly

Explanation: An LDAP operation failed because part of a substring filter involved in the operation is out of order. Each part of a substring filter is tagged as initial
R010045  R010050

(type 0), any (type 1), or final (type 2) and the
substring parts must be sequenced in that order. In this
substring filter, either a substring part typed as initial is
not the first part or a substring part typed as final is
not the last part. The type of the incorrectly ordered
part is indicated in the reason code.

In the message text:

_incorrectly ordered part_

_System action:_ The LDAP server continues to run, but
the operation fails.

_User response:_ Correct the search filter so that the
parts of the substring filter are in the correct sequence.
Then reissue the operation.

R010045  _substring filter part type_

_Explanation:_ An LDAP search operation failed
because some part of the filter involved in the
operation is missing. This can occur, for example, if an
_AND_ filter is missing the attribute value to search on.
The type of filter is indicated in the reason code.

In the message text:

_type_

_System action:_ The LDAP server continues to run, but
the operation fails.

_User response:_ Correct the search input so that all
parts of the filter are completely specified. Then reissue
the operation.

R010047  _new entry DN must exist in the same backend_

_Explanation:_ An LDAP modify DN operation failed
because it attempts to create an entry under a referral
entry. A referral entry is one which contains the _referral_
object class and the _ref_ attribute. A referral entry refers
to a different entry and cannot be the parent of any
entry.

_System action:_ The LDAP server continues to run, but
the operation fails.

_User response:_ Correct the modify DN input so that it
does not attempt to move entries under a referral entry.
Then reissue the operation.

R010048  _specified permissions are not allowed for the access class in aclEntry_

_Explanation:_ An LDAP modify or add operation failed
because it includes a value for the _aclEntry_ attribute
that is not valid. The value specifies the wrong type of
permissions for an access class. The acceptable
permissions for the _object_ access class are _a_ and _d_. The
acceptable permissions for all other access classes are _r_,
_w_, _s_ and _c_. The _aclEntry_ value is indicated in the
reason code.

In the message text:

_value_

Attribute value

_System action:_ The LDAP server continues to run, but
the operation fails.

_User response:_ Correct the _aclEntry_ value in the add
or modify input. Then reissue the operation.

R010049  _name failed with return code return_code, reason code reason_code_

_Explanation:_ An LDAP operation or utility failed
because an attribute value cannot be hashed, encrypted,
or decrypted. The attribute is encrypted or hashed
based on the _pwEncryption_ or _secretEncryption_ option
in the LDAP server configuration file. The attribute is
usually one of the following: _userPassword_, _ibm-slapdAdminPwd_, _secretKey_, _replicaCredentials_, _ibm-replicaKeyPwd_, or _ibm-slapdMasterPw_. The name
of the routine that failed and its return code and reason
code are indicated in the reason code.

In the message text:

_name_

_Routine name_

_return_code_

_Return code from routine_

_reason_code_

_Reason code from routine_

_System action:_ The LDAP server continues to run, but
the operation fails. The _ds2ldif_ or _ldif2ds_ utility ends.

_User response:_ Contact an LDAP administrator. After
the problem is resolved, reissue the operation or restart
the utility.

_Administrator response:_ Use any server messages and
ERROR debug trace output to assist in locating and
correcting the problem. If the routine indicated is
CRYPT, see the description of _crypt0_ in [z/OS XL C/C++
Run-Time Library Reference](https://www.ibm.com/support/knowledgecenter/STXKQR_1.3.2/icc/crunlibr.html)for more information about
the error. If an ICSF routine is indicated, see the
description of the routine in [z/OS Cryptographic Services
ICSF Application Programmer's Guide](https://www.ibm.com/support/knowledgecenter/SSLTBW_AboutThisGuide_1.3.2/icsf/czosa61a.html) for more
information about the error. If the problem persists,
contact the service representative.

R010050  _Label 'name' is not defined_

_Explanation:_ An LDAP operation or utility failed
because an attribute value set up to use AES or DES
encryption cannot be encrypted or decrypted. During
encryption, the AES or DES key label specified in the
_pwEncryption_ or _secretEncryption_ option in the LDAP
server configuration file must match a key label in the
LDAPKEYS data set or the ICSF CKDS. The same is true during decryption for the key label contained in the encrypted attribute value. The attribute is usually one of the following: userPassword, ibm-slapdAdminPw, secretKey, replicaCredentials, ibm-replicaKeyPwd, or ibm-slapdMasterPw. The name of the key label missing from the LDAPKEYS data set or the ICSF CKDS is indicated in the reason code.

In the message text:

```
name
Label name
```

**System action:** The LDAP server continues to run, but the operation fails. The ds2dif or ldif2ds utility ends.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation or restart the utility.

**Administrator response:** Use any server messages and ERROR debug trace output to assist in locating and correcting the problem. If the AES or DES key label indicated in the message is not present in the LDAPKEYS data set or the ICSF CKDS, add the label and key. If the error occurs during decryption, the original AES or DES key label that was used for encryption of the value must be added to the LDAPKEYS data set or the ICSF CKDS to allow successful AES or DES decryption. If using the LDAPKEYS data set with the LDAP server, then restart the LDAP server. If the problem persists, contact the service representative.

---

**R010051**  
ICSF services are not available

**Explanation:** An LDAP operation or utility failed because ICSF is not running while hashing, encrypting, or decrypting an attribute value set up to use AES, DES, SHA-2, or salted SHA-2. The attribute is usually one of the following: userPassword, ibm-slapdAdminPw, secretKey, replicaCredentials, ibm-replicaKeyPwd, or ibm-slapdMasterPw.

**System action:** The LDAP server continues to run, but the operation fails. The ds2dif or ldif2ds utility ends.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation or restart the utility.

**Administrator response:** Use any server messages and ERROR debug trace output to assist in locating and correcting the problem. Start ICSF if it is not already running. If the problem persists, contact the service representative.

---

**R010052**  
Incorrect key length for label 'name'

**Explanation:** An LDAP operation or utility failed because an attribute value is set up to use AES or DES encryption with a key in the LDAPKEYS data set which is not the correct length. During encryption, the AES or DES key label specified in the pwEncryption or secretEncryption option in the LDAP server configuration file must match a key label in the LDAPKEYS data set or the ICSF CKDS. The same is true during decryption for the key label contained in the encrypted attribute value. A DES key in the LDAPKEYS data set must be 8, 16, or 32 bytes long and have odd parity. In a DES key, the lower-order bit of each byte is the parity bit. The parity bit must be set so that there is an odd number of ones in each byte, but the bit is not used for encryption. An AES key in the LDAPKEYS data set must be 32 bytes long. See Symmetric encryption keys for more information. The name of the key label is indicated in the reason code.

In the message text:

```
name
Label name
```

**System action:** The LDAP server continues to run, but the operation fails. The ds2dif or ldif2ds utility ends.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation or restart the utility.

**Administrator response:** Use any server messages and ERROR debug trace output to assist in locating and correcting the problem. If the AES or DES key label specified in the LDAPKEYS data set must be 32 bytes long, add the label and key. If the error occurs during decryption, the key label is indicated in the reason code.

---

**R010053**  
Incorrect key parity for label 'name'

**Explanation:** An LDAP operation or utility failed because an attribute value is set up to use DES encryption with a key in the LDAPKEYS data set which does not have odd parity. During encryption, the DES key label specified in the pwEncryption or secretEncryption option in the LDAP server configuration file must match a key label in the LDAPKEYS data set or the ICSF CKDS. The same is true during decryption for the key label contained in the encrypted attribute value. A DES key in the LDAPKEYS data set must be 8, 16, or 32 bytes long and have odd parity. In a DES key, the lower-order bit of each byte is the parity bit. The parity bit must be set so that there is an odd number of ones in each byte, but the bit is not used for encryption. See Symmetric encryption keys for more information. The name of the key label is indicated in the reason code.

In the message text:

```
name
Label name
```

**System action:** The LDAP server continues to run, but the operation fails. The ds2dif or ldif2ds utility ends.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation or restart the utility.

**Administrator response:** Use any server messages and ERROR debug trace output to assist in locating and correcting the problem. If the AES or DES key label specified in the LDAPKEYS data set must be 32 bytes long, add the label and key. If the error occurs during decryption, the key label is indicated in the reason code.
R010054 • R010057

Correcting the problem. Update the DES key in the LDAPKEYS data set to specify a valid key. If using the LDAP server, then restart the LDAP server.

R010054 Encryption type type is not supported

Explanation: An LDAP operation or utility failed because an attribute value cannot be hashed or encrypted by the method specified in the pwEncryption or secretEncryption option in the LDAP server configuration file. The hashing or encryption method specified in the pwEncryption or secretEncryption option is not recognized by the LDAP server or utility because an internal programming error occurred. The attribute is usually one of the following: userPassword, ibm-slapdAdminPw, secretKey, replicaCredentials, ibm-replicaKeyPwd, or ibm-slapdMasterPw. The numeric identifier of the hashing or encryption method is indicated in the reason code.

In the message text:

   type
      Encryption type

System action: The LDAP server continues to run, but the operation fails. The ldif2ds utility ends.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation or restart the utility.

Administrator response: Use any server messages and ERROR debug trace output to assist in locating and correcting the problem. Verify that the serverCompatLevel option is set to the correct value and the encryption tag is recognized by the LDAP server or utility. See the pwEncryption option in Customizing the LDAP server configuration for more information. If necessary, restart the LDAP server. If the problem persists, contact the service representative.

R010056 Encrypted data length is not a multiple of number

Explanation: An LDAP operation or utility failed because an attribute value set up to use AES or DES encryption cannot be decrypted because the encrypted data is not a valid length. The length of the encrypted data must be a multiple of the length indicated in the reason code. The attribute is usually one of the following: userPassword, ibm-slapdAdminPw, secretKey, replicaCredentials, ibm-replicaKeyPwd, or ibm-slapdMasterPw.

In the message text:

   number
      Data length multiplier

System action: The LDAP server continues to run, but the operation fails. The ds2ldif utility ends.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation or restart the utility.

Administrator response: Use any server messages and ERROR debug trace output to assist in locating and correcting the problem. The attribute value may need to be replaced with a new value because the encrypted data is corrupted. If the problem persists, contact the service representative.

R010055 Encryption tag 'value' is not supported

Explanation: An LDAP operation or utility failed because the encryption tag specified in an attribute value is not valid. The attribute is usually one of the following: userPassword or ibm-slapdAdminPw. The server compatibility level must be 6 or greater to use Salted SHA-1 ({SSHA}) tagged attribute values. The server compatibility level must be 7 or greater to use SHA-2 or Salted SHA-2 tagged attribute values. The encryption tag of the attribute value is indicated in the reason code.

In the message text:

   value
      Tag value

System action: The LDAP server continues to run, but the operation fails. The ldif2ds or ldif2ds utility ends.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation or restart the utility.

Administrator response: Use any server messages and ERROR debug trace output to assist in locating and correcting the problem. Verify that the serverCompatLevel option is set to the correct value and the encryption tag is recognized by the LDAP server or utility. See the pwEncryption option in Customizing the LDAP server configuration for more information. If necessary, restart the LDAP server. If the problem persists, contact the service representative.

R010057 Incorrect key value for label 'name'

Explanation: An LDAP operation or utility failed because an attribute value set up to use AES or DES encryption cannot be decrypted. During decryption, the AES or DES key label is specified in the encrypted attribute value. The AES or DES key is unable to decrypt the AES or DES encrypted data. The attribute is usually one of the following: userPassword, ibm-slapdAdminPw, secretKey, replicaCredentials, ibm-replicaKeyPwd, or ibm-slapdMasterPw. The name of the key label is indicated in the reason code.

In the message text:

   name
      Label name

System action: The LDAP server continues to run, but the operation fails. The ds2ldif utility ends.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation or restart the utility.
R010058 Old and new password values were not supplied

**Explanation:** An LDAP native password modify operation failed because the input contains a `userPassword` attribute add or delete modification which does not contain a value. The delete modification must specify the existing password or password phrase value and the add modification must specify the new value. The delete modification must precede the add modification.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** In the modify input, specify the existing password or password phrase value in the delete modification for `userPassword` and the new value in the add modification. Then reissue the operation.

R010060 LDAP protocol version 3 is required for extended operations

**Explanation:** An LDAP extended operation failed because the requester is not using LDAP protocol version 3. The requester established the protocol version to use during bind. Protocol levels below 3 do not support extended operations.

**System action:** The LDAP server continues to run, but the extended operation fails.

**User response:** Either do not use extended operations, or rebind using protocol version 3 and then reissue the extended operation.

R010061 Only `GetDnForUserid` and `GetPrivileges` extended operations are supported

**Explanation:** An LDAP operation failed because this connection to the LDAP server is restricted to usage for Policy Director. Only the Policy Director extended operations, `GetDnForUserid` and `GetPrivileges` can be processed on this connection.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Do not use this connection for any operations other than the Policy Director extended operations.

R010062 Unable to communicate with cross-system group owner

**Explanation:** An LDAP operation failed because the sysplex replica server is unable to communicate with the sysplex owner server over XCF (Cross System Facility).

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

R010064 `cn=monitor search requires filter (objectclass=*)`

**Explanation:** An LDAP search operation of the monitor backend failed because the search filter specified in the operation is not `objectclass=`. To search the monitor backend, specify a target of `cn=monitor` and a filter of `objectclass=`.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Correct the filter in the search input. Then reissue the operation.

R010065 Unable to write attribute type 'name'

**Explanation:** The LDAP `ds2ldif` utility failed because it is unable to write an attribute to a buffer. The name of the attribute (and sometimes its value) is indicated in the reason code.

In the message text:

```
name
```

Attribute name

**System action:** The LDAP server continues to run, but the utility fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, restart the utility.

R010066 Unable to write to file 'file_name': error_code/reason_code - error_string

**Explanation:** The `ds2ldif` utility or the LDAP server encountered an error while attempting to write a record to the output file indicated in the reason code. The output file is either a z/OS UNIX System Services file, a partitioned data set, or a sequential data set. The file
name is specified on -o option of the ds2ldif utility. The error code, reason code, and error text indicated in the are returned from one of the following: fputs(), fflush(), or fclose(). See the descriptions of these routines in z/OS XL C/C++ Run-Time Library Reference for more information about the error.

In the message text:

- **file_name**
  - Output file name

- **error_code**
  - Error code from function

- **reason_code**
  - Reason code from function

- **error_string**
  - Text corresponding to the error code

**System action:** The LDAP server continues to run, but the utility fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, restart the utility.

**Administrator response:** Use the information in the reason code to resolve the problem.

---

**R010067**  
No referrals defined for read only replica, unable to update entry 'name'

**Explanation:** An LDAP add, modify, delete, or modify DN operation failed because the targeted LDAP server is a read-only replica or consumer server that does not know to what master or supplier server it should resend the operation. A read-only replica or consumer server cannot perform operations that update the directory. For basic replication, it uses the masterServer configuration option to determine the master server, otherwise it uses the referral configuration option. For advanced replication, it uses the servers specified in the ibm-replicaReferralURL attribute value of the replication context entry. See Basic replication and Advanced replication for more information. The distinguished name of the target of the operation is indicated in the reason code.

In the message text:

- **name**
  - Distinguished name of entry

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** For basic replication, ensure that the appropriate values are specified for the masterServer and referral options in the LDAP server configuration file. Then restart the LDAP server. For advanced replication, ensure that the appropriate values are specified for the ibm-replicaReferralURL attribute value of the replication context entry.

---

**R010068**  
Paged search is allowed only when bound as an LDAP administrator

**Explanation:** An LDAP search operation failed because a user that is not an LDAP administrator specified the PagedResults control (identifier is 1.2.840.113556.1.4.319). Paged searches are only supported when bound as an LDAP administrator.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Do not specify the PagedResults control on the search request. If a paged search is needed, contact an LDAP administrator. Then reissue the operation.

**Administrator response:** If non-administrators must issue paged searches, set the ibm-slapdPagedResAllowNonAdmin attribute value to true in the cn=configuration entry.

---

**R010069**  
Sorted search is allowed only when bound as an LDAP administrator

**Explanation:** An LDAP search operation failed because a user that is not an LDAP administrator specified the SortKeyRequest control (identifier is 1.2.840.113556.1.4.473). Sorted searches are only supported when bound as an LDAP administrator.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Do not specify the SortKeyRequest control on the search request. If a sorted search is needed, contact an LDAP administrator. Then reissue the operation.

**Administrator response:** If non-administrators must issue sorted searches, set the ibm-slapdSortSrchAllowNonAdmin attribute value to true in the cn=configuration entry.

---

**R010070**  
Paged search support is disabled

**Explanation:** An LDAP search operation failed because the PagedResults control (identifier is 1.2.840.113556.1.4.319) was specified in the request but paged searches are not enabled in the LDAP server. Paged searches are enabled in the LDAP server when the ibm-slapdPagedResLmt attribute value in the cn=configuration entry is greater than 0.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Do not specify the PagedResults control (identifier is 1.2.840.113556.1.4.319). If a paged search is needed, contact an LDAP administrator. Then reissue the operation.

**Administrator response:** If paged search is needed, update the ibm-slapdPagedResLmt attribute value in
the \texttt{cn=configuration} entry to have a value greater than 0.

**R010071  Sorted search support is disabled**

**Explanation:** An LDAP search operation failed because the \texttt{SortKeyRequest} control (identifier is 1.2.840.113556.1.4.473) was specified in the request but sorted searches are not enabled in the LDAP server. Sorted searches are enabled in the LDAP server when the \texttt{ibm-slapdSortKeyLimit} attribute value in the \texttt{cn=configuration} entry is greater than 0.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Do not specify the \texttt{SortKeyRequest} control (identifier is 1.2.840.113556.1.4.473). If a sorted search is needed, contact an LDAP administrator. Then reissue the operation.

**Administrator response:** If sorted search is needed, update the \texttt{ibm-slapdSortKeyLimit} attribute value in the \texttt{cn=configuration} entry to have a value greater than 0.

**R010072  Maximum of size sorted search keys has been exceeded**

**Explanation:** An LDAP search operation failed because the number of sort keys in the \texttt{SortKeyRequest} control (identifier is 1.2.840.113556.1.4.473) exceeded the maximum number of sort keys allowed by the LDAP server. The number of sort keys that are allowed to be specified on a sorted search request is controlled by the \texttt{ibm-slapdSortKeyLimit} attribute value in the \texttt{cn=configuration} entry.

In the message text:

\begin{itemize}
  \item \texttt{size}  Maximum number of sorted search keys
\end{itemize}

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Reduce the number of sort keys in the \texttt{SortKeyRequest} control (identifier is 1.2.840.113556.1.4.473). If all sort keys are needed, contact an LDAP administrator. Then reissue the operation.

**Administrator response:** If the maximum allowed number of sort keys must be increased, update the \texttt{ibm-slapdSortKeyLimit} attribute value in the \texttt{cn=configuration} entry.

**R010073  Sort key matching rule is inappropriate**

**Explanation:** An LDAP search operation failed because the ordering rule specified in the \texttt{SortKeyRequest} control (identifier is 1.2.840.113556.1.4.473) is not appropriate for the schema syntax. See [LDAP directory schema](#) for information about the appropriate matching or ordering rules with the schema syntax.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Update the ordering rule in the \texttt{SortKeyRequest} control (identifier is 1.2.840.113556.1.4.473) to use an appropriate ordering rule for the schema syntax. Then reissue the operation.

**R010074  Sort key attribute specified more than once**

**Explanation:** An LDAP search operation failed because an attribute type was specified more than once in the \texttt{SortKeyRequest} control (identifier is 1.2.840.113556.1.4.473).

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Update the \texttt{SortKeyRequest} control (identifier is 1.2.840.113556.1.4.473) to specify each sort key attribute type once. Then reissue the operation.

**R010500  Unable to retrieve normalized values for attribute \texttt{name}**

**Explanation:** An LDAP operation failed because the normalized attribute values could not be retrieved for the attribute type. The attribute type is indicated in the reason code.

In the message text:

\begin{itemize}
  \item \texttt{name}  Attribute name
\end{itemize}

**System action:** The LDAP server continues to run, but the operation fails to be replicated.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Use any server messages and ERROR+REPL debug trace output to assist in locating and resolving the problem. If the problem persists, contact the service representative.

**R010501  Unable to retrieve the next change ID for replication context with DN \texttt{name}**

**Explanation:** An LDAP operation failed because the next change identifier could not be obtained for the replication context. The replication context distinguished name (DN) is indicated in the reason code.

In the message text:

\begin{itemize}
  \item \texttt{name}  Distinguished name of context
\end{itemize}

**System action:** The LDAP server continues to run, but the operation fails to be replicated.

---

Chapter 6. Return and reason codes 321
R010502  •  R010506

**User response:**  Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:**  Use any server messages and ERROR+REPL debug trace output to assist in locating and resolving the problem. If the problem persists, contact the service representative.

R010502  More than one replication agreement exists for DN 'name' and consumer URL 'url'

**Explanation:**  An LDAP add or modify operation failed because more than one replication agreement entry with the same consumer server URL (ibm-replicaURL) was found under the replication context entry. The duplicate replication agreement entry and consumer server URL are indicated in the reason code.

In the message text:

```
name
  Distinguished name
url
  Consumer URL
```

**System action:**  The LDAP server continues to run, but the operation fails.

**User response:**  Update the operation input to specify a different consumer server URL for the ibm-replicaURL attribute value in the replication agreement entry. Then reissue the operation input.

R010503  The 'name1' and 'name2' attributes are not allowed on DN 'name3'

**Explanation:**  An LDAP add operation failed because the attribute types are not allowed to be in the distinguished name (DN) entry. The attribute types and DN of the entry are indicated in the reason code.

In the message text:

```
name
  Distinguished name
name1
  First attribute name
name2
  Second attribute name
name3
  Distinguished name of entry
```

**System action:**  The LDAP server continues to run, but the operation fails.

**User response:**  Update the operation input to specify a different consumer server URL for the ibm-replicaURL attribute value in the replication agreement entry. Then reissue the operation input.

R010504  DN 'name' cannot be a replication context

**Explanation:**  An LDAP add or modify operation failed because the distinguished name (DN) is not allowed to be a replication context entry. The cn=localhost, cn=pwdpolicy, cn=ibmpolicies, and cn=configuration entries are not allowed to be replication contexts. The DN of the entry is indicated in the reason code.

In the message text:

```
name
  Distinguished name of entry
```

**System action:**  Use any server messages and ERROR+REPL debug trace output to assist in locating and resolving the problem. If the problem persists, contact the service representative.

R010505  Unable to find replication context for DN 'name'

**Explanation:**  An LDAP operation failed because the replication context entry could not be found. The distinguished name (DN) of the replication context entry is indicated in the reason code.

In the message text:

```
name
  Distinguished name of context
```

**System action:**  The LDAP server continues to run, but the operation fails.

**User response:**  Verify that a replication context entry is specified in the request. If it is a replication context entry, contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:**  Use any server messages and ERROR+REPL debug trace output to assist in locating and resolving the problem. If the problem persists, contact the service representative.

R010506  Gateway server must be a Master server

**Explanation:**  An LDAP operation failed because a gateway server must be configured as a master server. The ibm-replicationServerIsMaster attribute value in the replica subentry must be set to true to designate this server as a master server.

**System action:**  The LDAP server continues to run, but the operation fails.

**User response:**  Update the distinguished name entry to remove the attribute types from the entry or operation input. Then reissue the operation input.
**R010507  Credential objectclass not found**

**Explanation:** An LDAP operation failed because the credentials entry referenced by the ibm-replicaCredentialsDN in the replication agreement does not have a valid objectclass value. A credentials entry must have an objectclass value of ibm-replicationCredentialsSimple or ibm-replicationCredentialsExternal.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Either update the ibm-replicaCredentialsDN attribute value in the replication agreement entry or modify the existing entry to specify an objectclass value of ibm-replicationCredentialsSimple or ibm-replicationCredentialsExternal.

---

**R010508  No objectclass attribute found in entry**

**Explanation:** An LDAP operation failed because does not have an objectclass attribute value.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. Then reissue the operation.

**Administrator response:** Use any server messages and ERROR+REPL debug trace output to assist in locating and resolving the problem. If the problem persists, contact the service representative.

---

**R010509  Credential DN 'name' is in use and cannot be deleted**

**Explanation:** An LDAP delete operation failed because the supplier server credentials entry is in use by a replication agreement entry. The distinguished name (DN) of the credentials entry is indicated in the reason code.

In the message text:

- **name**
  - Distinguished name of credential entry

**User response:** If the credentials entry must be deleted, all references to the entry in the ibm-replicaCredentialsDN attribute value of replication agreement entries must be removed. To find all references to the credentials entry, use an LDAP search operation with the filter: ibm-replicaCredentialsDN=dn. Update those entries to reference another credentials entry or delete those entries. Then reissue the operation.

---

**R010510  Filter DN 'name' is in use and cannot be deleted**

**Explanation:** An LDAP delete operation failed because the replication filter entry is in use by a replication agreement entry. The distinguished name (DN) of the filter entry is indicated in the reason code.

In the message text:

- **name**
  - Distinguished name of filter entry

**User response:** If the replication filter entry must be deleted, all references to the entry in the ibm-replicationFilterDN attribute value of replication agreement entries must be removed. To find all references to the replication filter entry, use an LDAP search operation with the filter: ibm-replicationFilterDN=dn. Update those entries to reference another filter entry, remove the ibm-replicationFilter value, or delete those entries. Then reissue the operation.

---

**R010511  Adding an ibm-replicationContext to DN 'name' is not allowed**

**Explanation:** An LDAP modify operation failed because the distinguished name (DN) is not allowed to be a replication context entry. The cn=localhost, cn=pwdpolicy,cn=ibmpolicies, and cn=configuration entries are not allowed to be replication contexts. The DN of the entry is indicated in the reason code.

In the message text:

- **name**
  - Distinguished name of entry

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Update the operation input to no longer specify an objectclass value of ibm-replicationContext in the entry. Then reissue the operation.

---

**R010512  Modification of the replication subentry's 'name' attribute is not allowed**

**Explanation:** An LDAP modify operation failed because modification of the replica subentry is not allowed. The ibm-replicaServerID attribute value cannot be modified after this entry is created. If this attribute value must be changed, all entries under the replica subentry must be deleted and then readded. The attribute type is indicated in the reason code.

In the message text:

- **name**
  - Attribute name

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Update the operation input to no
R010513  Modification is not valid. Replication context entry is no longer a replication context entry

Explanation: An LDAP modify operation failed because modifying a replication context entry to no longer be a replication context is not allowed when replica group, replica subentry, or replication agreement entries still exist under the replication context entry. Other replication topology entries must be modified or deleted before modifying this entry to no longer be a replication context.

System action: The LDAP server continues to run, but the operation fails.

User response: If the advanced replication topology is no longer needed, delete all advanced replication topology entries that reside under the replication context. Then reissue the operation.

R010514  Cannot rename a replication topology entry

Explanation: An LDAP modify DN operation failed because renaming of a replication topology entry is not allowed. Replication topology entries that are not allowed to be changed include replication contexts, replica subentry, and replication agreements. See Advanced replication for more information.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the modify DN input so that it does not rename a replication topology entry. Then reissue the operation.

R010515  Agreement with DN ’name’ does not support realignment

Explanation: An LDAP modify DN operation with realignment failed because the consumer server does not support attribute value realignment. The distinguished name (DN) of the replication agreement entry is indicated in the reason code.

In the message text:

name

Distinguished name of agreement

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator or the master server DN to create or update replication topology entries.

R010516  Resulting entry is not in same replication context as target entry

Explanation: An LDAP modify DN operation failed because the resulting name of the entry results in it being in a different replication context. Modify DN operations are supported with advanced replication as long the renamed entry resides in the same replication context.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the modify DN input so that the rename resides in the same replication context. Then reissue the operation.

R010517  Unable to parse URL for attribute ’name’

Explanation: An LDAP modify operation failed because the attribute value did not specify a valid URL. The URL format is: ldap[s]://[IP_address|hostname][:portNumber] The attribute name is indicated in the reason code.

In the message text:

name

Attribute name

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the URL attribute value so that it has a valid format. Then reissue the operation.

R010518  User does not have authority to create/update a replication topology entry

Explanation: An LDAP add, modify, or delete operation failed because the user does not have the appropriate authority to add, modify, or delete a replication topology entry. An LDAP root, directory data, or replication administrator or the master server distinguished name (DN) are allowed to administer replication topology entries.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator or the master server DN to create or update replication topology entries.

R010519  Cannot modify a replication topology entry

Explanation: An LDAP modify operation failed because a replica group, replica subentry, or replication agreement entry was attempted to be modified into a replication context entry. These replication topology entries are not allowed to have dual roles in a replication topology.
System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input to no longer modify the entry into a replication context entry. Then reissue the operation.

R010750  No request data is found

Explanation: An LDAP extended operation failed because there was no data to process in the request. See Supported extended operations for more information.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Verify that the extended operation is properly encoded. Use any server messages and ERROR+REPL debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

R010751  Decoding error occurs when processing extended operation

Explanation: An LDAP extended operation failed because the request could not be decoded. See Supported extended operations for more information.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Verify that the extended operation is properly encoded. Use any server messages and ERROR+REPL debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

R010752  The syntax of the replication context DN is not valid

Explanation: An LDAP extended operation failed because the syntax of the replication context distinguished name (DN) is not valid.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input to specify a valid replication context DN that exists and is a valid DN. Then reissue the operation.

R010753  The backend for entry 'name' does not replicate

Explanation: An LDAP extended operation failed because the distinguished name (DN) specified in the request is not participating in a replication topology. The DN is indicated in the reason code.

User response: Correct the operation input to specify a valid replication topology DN. Then reissue the operation.

R010754  The entry 'name' does not exist or is not a replication context

Explanation: An LDAP extended operation failed because the distinguished name (DN) specified in the request does not exist or is not a valid replication context. The DN is indicated in the reason code.

In the message text:

name

Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input to specify a valid replication context or replication agreement DN that participates in a replication topology. Then reissue the operation.

R010755  User does not have the authority to perform this extended operation

Explanation: An LDAP extended operation failed because the bound user does not have the authority to perform the extended operation. See Supported extended operations for more information.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator to issue the extended operation or grant authorization for you to issue the extended operation. Then reissue the operation.

R010756  Error encountered when normalizing the DN

Explanation: An LDAP extended operation failed because the syntax of the distinguished name (DN) of the replication topology entry is not valid and could not be normalized.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input to specify a valid replication topology DN. Then reissue the operation.
R010757  Unexpected error occurs while processing the extended operation
Explanation: An LDAP extended operation failed because the LDAP server detects an internal programming error during processing.
System action: The LDAP server continues to run, but the operation fails.
User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

R010758  The action specified on the extended operation input is not valid
Explanation: An LDAP extended operation failed because the action field encoded in the request is not valid. The action field is used in the Cascading control replication, Control replication queue, and Control replication extended operations. See Supported extended operations for more information.
System action: The LDAP server continues to run, but the operation fails.
User response: Correct the operation input to specify a valid integer for the action field. Then reissue the operation.

R010759  The timeout value specified on the extended operation input cannot be negative
Explanation: An LDAP extended operation failed because the timeout field encoded in the request is a negative number which is not valid. The timeout field is used in the Cascading control replication and Replication topology extended operations and must be zero or greater. See Supported extended operations for more information.
System action: The LDAP server continues to run, but the operation fails.
User response: Correct the operation input to specify a valid integer for the timeout field. Then reissue the operation.

R010760  The requested option specified for the error log extended operation is not valid
Explanation: An LDAP extended operation failed because the errorOption field encoded in the request is not valid. The errorOption field is used in the Control replication error log extended operation. See Supported extended operations for more information.
System action: The LDAP server continues to run, but the operation fails.
User response: Correct the operation input to specify a valid integer for the errorOption. Then reissue the operation.

R010761  No replication agreement DN is specified
Explanation: An LDAP extended operation failed because the replication agreement distinguished name (DN) is not encoded in the request. The replication agreement DN must be encoded in the Control replication error log extended operation. See Supported extended operations for more information.
System action: The LDAP server continues to run, but the operation fails.
User response: Correct the operation input to specify a replication agreement DN. Then reissue the operation.

R010762  The syntax of the replication agreement DN is not valid
Explanation: An LDAP extended operation failed because the syntax of the replication context distinguished name (DN) is not valid. See Supported extended operations for more information.
System action: The LDAP server continues to run, but the operation fails.
User response: Correct the operation input to specify a valid replication agreement DN that exists and is a valid DN. Then reissue the operation.

R010763  The entry 'name' does not exist or is not under a replication context
Explanation: An LDAP extended operation failed because the distinguished name (DN) specified in the request does not exist or is not under a valid replication context entry. See Supported extended operations for more information about the extended operations. The DN is indicated in the reason code.
In the message text:

name  Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.
User response: Correct the operation input to specify a valid DN that exists and is under a replication context. Then reissue the operation.
R010764  R010769

R010764  The entry 'name' does not exist, is not an agreement, or is not serviced by this server.

Explanation: An LDAP extended operation failed because the distinguished name (DN) specified in the request does not exist, is not a valid replication agreement, or the entry is managed by another server. See Supported extended operations for more information. The DN is indicated in the reason code.

In the message text:

name

Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input to specify a valid DN that exists, is a replication agreement, and is managed by this server. Then reissue the operation.

R010765  The failure ID 'identifier' exists but is not logged for 'name'

Explanation: An LDAP extended operation failed because the failureId field encoded in the request exists in the directory but is not present in the replication agreement entry. The failureId field is used in the Control replication error log extended operation. See Supported extended operations for more information. The distinguished name (DN) of the replication agreement entry and the failure ID are indicated in the reason code.

In the message text:

identifier

Failure identifier

name

Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input to specify the correct replication agreement entry and failure ID. Then reissue the operation.

R010766  Data for the requested failure ID 'identifier' cannot be retrieved or formatted

Explanation: An LDAP extended operation failed because the failureId field encoded in the request cannot be retrieved or formatted. The failureId field is used in the Control replication error log extended operation. See Supported extended operations for more information. The failure ID is indicated in the reason code.

In the message text:

identifier

Failure identifier

name

Distinguished name of entry

System action: The LDAP server continues to run, but the operation fails.

User response: Update the operation input to specify a valid scope value. Then reissue the operation.

R010767  The scope specified on the extended operation input is not valid

Explanation: An LDAP extended operation failed because the scope field encoded in the request is not valid. The scope field is used in the Control replication extended operation. See Supported extended operations for more information.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input to specify a valid scope value. Then reissue the operation.

R010768  No replication agreement found for the context entry 'name'

Explanation: An LDAP extended operation failed because the replication context distinguished name (DN) encoded in the request does not have at least one valid replication agreement entry. The replication context is used in the Control replication error log and Replication topology extended operations. See Supported extended operations for more information.

In the message text:

name

Distinguished name of context

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input to specify a replication context DN that has at least one replication agreement entry. Then reissue the operation.

R010769  Change ID is not specified or is not valid with skip single option

Explanation: An LDAP extended operation failed because the changeld field encoded in the request is not valid when skipping a single replication change. The changeld field is used in the Control replication queue extended operation. See Supported extended operations for more information.
R010770  •  R010775

System action:  The LDAP server continues to run, but the operation fails.

User response:  Correct the operation input to specify a valid change ID or update the operation input to skip all replication changes. Then reissue the operation.

R010770  Error encountered while retrieving the list of changes

Explanation:  An LDAP extended operation failed because the list of replication changes or updates cannot be retrieved when performing the Control replication queue extended operation.

System action:  The LDAP server continues to run, but the operation fails.

User response:  Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response:  Use any server messages and ERROR+REPL debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

R010773  There are no pending changes to skip

Explanation:  An LDAP extended operation did not find any pending changes in the replication queue that needed to be skipped. Pending replication changes can be skipped by using the Control replication queue extended operation. The extended operation has completed successfully since there are no pending changes to skip in the replication queue. See Supported extended operations for more information.

System action:  The LDAP server continues to run.

R010774  Context DN is required but not specified

Explanation:  An LDAP extended operation failed because a replication context distinguished name (DN) is required but has not been specified. A replication context DN is required in the Replication topology extended operation. See Supported extended operations for more information.

System action:  The LDAP server continues to run, but the operation fails.

User response:  Correct the operation input to specify a valid replication context DN. Then reissue the operation.

R010775  Replication agreement entry 'name' was deleted

Explanation:  An LDAP extended operation failed because the replication agreement distinguished name (DN) entry has been deleted. The Replication topology extended operation requires a valid and existing replication agreement entry. See Supported extended operations for more information.

In the message text:

name

Distinguished name of agreement

System action:  The LDAP server continues to run, but the operation fails.

User response:  Correct the operation input to specify a valid replication agreement DN. Then reissue the operation.

R010777  Requested change ID 'identifier1' does not match next change ID 'identifier2'

Explanation:  An LDAP extended operation failed because the changedId field encoded in the request does not match the next change identifier in the replication agreement. The changedId field is used in the Control replication queue extended operation and must match the next pending change in the replication queue. See Supported extended operations for more information.

The requested change ID and next pending change ID are indicated in the reason code.

In the message text:

identifier1

Change identifier

dererator2

Next change identifier

System action:  The LDAP server continues to run, but the operation fails.

User response:  Correct the operation input to specify the next pending change ID. The next pending change ID can be found in the multi-valued ibm-replicationPendingChanges attribute type. Then reissue the operation.

R010772  Error encountered when server is updating the replication status

Explanation:  An LDAP extended operation failed because an error was encountered while updating the replication status. The replication status is updated while performing the Control replication queue extended operation. See Supported extended operations for more information.

System action:  The LDAP server continues to run, but the operation fails.

User response:  Correct the operation input to specify a valid change ID or update the operation input to skip all replication changes. Then reissue the operation.
Failed to contact target 'host:port' using replication agreement 'name'

Explanation: An LDAP extended operation failed because the LDAP server is not able to connect to the consumer server identified in the replication agreement entry. The host name, port number, and distinguished name (DN) of the replication agreement entry are indicated in the reason code.

In the message text:

host
Host name

port
Host port

name
Distinguished name of agreement

System action: The LDAP server continues to run, but the operation fails.

User response: Verify that the replication agreement entry has the correct host name, port number, and credentials entry specified for the consumer server. If the replication agreement entry is correct, contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: If the server is not already running on the specified host or port numbers, start the server. Verify that the credentials entries on the supplier and consumer servers are using the same bind distinguished name and password values.

Replication extended operation timed out

Explanation: An LDAP extended operation failed because the timeout field encoded in the request has been exceeded. The timeout field is used in the Cascading control replication and Replication topology extended operations. See Supported extended operations for more information.

System action: The LDAP server continues to run, but the operation fails.

User response: Increase the timeout value field to allow enough time for the extended operation to complete. Then reissue the operation.

Replication topology extended operation failed

Explanation: An LDAP extended operation failed because an error occurred while attempting to synchronize replication topology entries. Replication topology entries are synchronized by using the Replication topology extended operation. See Supported extended operations for more information.

System action: The LDAP server continues to run, but the operation fails.

User response: If the operation is not successful, verify that all replication topology entries that are being synchronized are correct. In particular, verify that the credentials entries used on the supplier and consumer servers are using the bind distinguished name (DN) or password values with a simple bind credentials entry or the same SSL certificate with an SASL EXTERNAL bind credentials entry. Then reissue the operation.

Server 'host:port' skipped because there is no connection to it

Explanation: An LDAP extended operation skipped the consumer server indicated in the message because there is no current connection to it. The Cascading control replication extended operation provides the ability for an operation to be passed to all replication agreements under the replication context. See Supported extended operations for more information.

The consumer server host and port numbers are indicated in the reason code.

In the message text:

host
Host name
port
Host port

System action: The LDAP server continues to run, but the operation to the specified server fails.

User response: Verify that the indicated server is running. If there is not a configured server running on the indicated host name and port numbers, delete or modify the replication agreement entry that has the specified host and port number in the ibm-replicaURL attribute value. Then reissue the operation.

R010781 Server 'host:port' skipped because it is on hold

Explanation: An LDAP extended operation skipped the consumer server indicated in the message because replication is on hold or suspended. The **Cascading control replication** extended operation provides the ability for an operation to be passed to all replication agreements under the replication context. However a replication agreement is skipped if replication is already on hold or suspended. See Supported extended operations for more information. The consumer server host and port numbers are indicated in the reason code.

In the message text:

```
host
Host name
```

```
port
Host port
```

System action: The LDAP server continues to run, but the operation fails.

User response: Verify that replication for the indicated server is to be on hold or suspended by requesting the ibm-replicationOnHold attribute in the replication agreement entry. Modify the replication agreement entry with the specified host and port number if replication should not be on hold or suspended. Then reissue the operation.

R010784 Replication context is already quiesced/unquiesced

Explanation: An LDAP extended operation failed because the replication context is already quiesce or unquiesced. The **Cascading control replication** and Quiesce or unquiesce context extended operations allow a replication context to be quiesced or unquiesced. See Supported extended operations for more information. The operation input is to specify the opposite value. Then reissue the operation.

R010785 The replication extended operation will not continue since the target server is a master server

Explanation: An LDAP extended operation failed because the target server is a master server and it does not support the replicated request. The replicated extended operation request is not supported by the master server.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input to no longer target a master server with the extended
R010786 Failed to quiesce supplier

**Explanation:** An LDAP extended operation failed because the supplier server was not able to be quiesced. The [Replication topology extended operation](https://www.ibm.com) is used to quiesce a supplier server. See [Supported extended operations](https://www.ibm.com) for more information.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Use any server messages and ERROR+REPL debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

---

R010787 Failed to build 'type' list

**Explanation:** An LDAP extended operation failed because an internal list could not be built. The type of list is indicated in the reason code.

In the message text:

- **type**
  - Type of list

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Use any server messages and ERROR+REPL debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

---

R010788 Consumer server down or not accepting updates from supplier. Retry for failure ID 'identifier' failed

**Explanation:** An LDAP extended operation failed because an error occurred while trying the request again in the replication agreement entry for the `failureId` encoded in the request. The `failureId` field is used in the [Control replication error log](https://www.ibm.com) extended operation to delete, display, or retry a replication failure. See [Supported extended operations](https://www.ibm.com) for more information. The failure ID is indicated in the reason code.

In the message text:

- **identifier**
  - Failure identifier

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Verify that the consumer server is running and the backend containing the replication topology successfully started. Then reissue the operation.

---

R010789 Target server 'host:port' skipped by gateway

**Explanation:** An LDAP extended operation skipped the server indicated in the message because requests are not forwarded from one gateway server to another gateway server. The [Cascading control replication](https://www.ibm.com) extended operation enables an operation to be passed to all replication agreements under the replication context. See [Supported extended operations](https://www.ibm.com) for more information. The consumer server host and port numbers are indicated in the reason code.

In the message text:

- **host**
  - Host name
- **port**
  - Host port

**System action:** The LDAP server continues to run, but the operation to the specified server is skipped.

---

R010790 Number changes were skipped

**Explanation:** An LDAP extended operation successfully skipped the number of changes in the replication queue. The [Control replication queue](https://www.ibm.com) extended operation enables you to skip pending replication changes. The number of pending changes skipped in the replication queue is indicated in the reason code.

In the message text:

- **number**
  - Number of changes

**System action:** The LDAP server continues to run.

---

R010791 Error occurs while parsing data for change ID 'identifier' for replica 'name'

**Explanation:** An LDAP extended operation failed because an error occurred while parsing and retrieving data from the replication agreement entry for the `failureId` encoded in the request. The `failureId` field is used in the [Control replication error log](https://www.ibm.com) extended operation to delete, display, or retry a replication failure. See [Supported extended operations](https://www.ibm.com) for more information. The failure ID is indicated in the reason code.

In the message text:

- **identifier**
  - Failure identifier
- **name**
  - Replica name
**R010792**  
**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Use any server messages and ERROR+REPL debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

---

**R010792  Error occurs while applying filter to replication operation**

**Explanation:** An LDAP extended operation failed because an error occurred while applying a replication filter to the entries being replicated. The replication filter entry used by a replication agreement entry is specified in the `ibm-replicationFilterDN` attribute value.

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Verify that the replication filters in use by the replication agreement are valid. Ensure that the replication filters in use do not exclude any required attribute types from being replicated to a consumer server. If necessary, remove the `ibm-replicationFilterDN` attribute value from the replication agreement or update the replication filters. Then reissue the operation.

---

**R010793**  
**Failed to retrieve data for failure ID 'identifier'**

**Explanation:** An LDAP extended operation failed because an error occurred while parsing and retrieving data from the replication agreement entry for the `failureId` encoded in the request. The `failureId` field is used in the Control replication error log extended operation to delete, display, or retry a replication failure. See [Supported extended operations](#) for more information. The failure ID is indicated in the reason code.

In the message text:

```
identifier
  Failure identifier
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Verify the correct failure ID is specified in the request by requesting the `ibm-replicationFailedChanges` attribute in the replication agreement entry. If the correct failure ID is specified, contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Use any server messages and ERROR+REPL debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

---

**R010795  The target server 'host:port' does not support replication topology entries**

**Explanation:** An LDAP extended operation failed because the target server does not support advanced replication topology entries. The host name and port number of the target server are indicated in the reason code.

In the message text:

```
host
  Host name
port
  Host port
```

**System action:** The LDAP server continues to run, but the operation fails.

**User response:** Contact an LDAP administrator. After the problem is resolved, reissue the operation.

**Administrator response:** Verify that the target server supports advanced replication topology entries by ensuring that `useAdvancedReplication on` is specified in the CDBM backend section of the target server's configuration file. If a non-z/OS IBM Tivoli Directory Server is used for the target server, ensure that it is 6.0 or later.
R010796  Failed to add the context DN as a suffix to the config file of the target server 'host:port'

Explanation: An LDAP extended operation failed because the target server does not have a required suffix in its configuration file and does not support the non-z/OS IBM Tivoli Directory Server Dynamic update requests extended operation to automatically update the server configuration file. The Replication topology extended operation attempted to synchronize replication topology entries on the target server but it does not have the appropriate suffix. It also does not support the non-z/OS IBM Tivoli Directory Server Dynamic update requests extended operation to automatically update the server configuration file. The target server host and port number are indicated in the reason code.

In the message text:

host  Host name
port  Host port

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Update the configuration file of the target server to specify the suffix used by the replication context or replication agreement entry in an LDBM or TDBM backend. Then restart the target server.

R010798  Unable to quiesce the target server

Explanation: An LDAP extended operation failed because the distinguished name specified in the request does not exist or is not a valid replication context entry. The Replication topology extended operation attempted to synchronize replication topology entries on the target server.

System action: The LDAP server continues to run, but the operation fails.

User response: Correct the operation input to specify a valid replication context entry. Then reissue the operation.

R010799  Unable to update the topology entries on the target server

Explanation: An LDAP extended operation failed because the replication topology entries could not be added, modified, or deleted from the target server. The Replication topology extended operation attempted to synchronize replication topology entries on the target server.

System action: The LDAP server continues to run, but the operation fails.

User response: Contact an LDAP administrator. After the problem is resolved, reissue the operation.

Administrator response: Use any server messages and ERROR+REPL debug trace output to assist in locating and correcting the problem. If the problem persists, contact the service representative.

R010800 number1 failures removed successfully, number2 remain

Explanation: An LDAP extended operation successfully removed replication failures from the replication error log. The Control replication error log extended operation enables you to delete, display, or retry replication failures. See Supported extended operations for more information. The number of replication failures successfully removed and failures remaining in the replication error log are indicated in the reason code.

In the message text:

host  Host name
port  Host port

Chapter 6. Return and reason codes  333
R010801  Number of failures removed

R010802  Failure ID 'identifier' was not successfully retried

R010803  Failure ID 'identifier' successfully retried

R010804  The target server 'host:port' does not support the extended operation

R010805  Extended operation failed since target server is not a master server for the context 'name'.

System action:  The LDAP server continues to run.
User response:  Correct the operation input to target

R010801  Number of failures removed

R010802  Failure ID 'identifier' was not successfully retried

R010803  Failure ID 'identifier' successfully retried

R010804  The target server 'host:port' does not support the extended operation

R010805  Extended operation failed since target server is not a master server for the context 'name'.

System action:  The LDAP server continues to run.
User response:  Correct the operation input to target
the extended operation against the master or supplier server in the replication topology. Then reissue the operation.
Appendix. Accessibility

Publications for this product are offered in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when using PDF files, you may view the information through the z/OS Internet Library website or the z/OS Information Center. If you continue to experience problems, send an email to mhvrcfs@us.ibm.com or write to:

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
U.S.A.

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS enable users to:
• Use assistive technologies such as screen readers and screen magnifier software
• Operate specific or equivalent features using only the keyboard
• Customize display attributes such as color, contrast, and font size

Using assistive technologies

Assistive technology products, such as screen readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using such products to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to z/OS TSO/E Primer, z/OS TSO/E User’s Guide and z/OS ISPF User’s Guide Vol I for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

z/OS information

z/OS information is accessible using screen readers with the BookServer or Library Server versions of z/OS books in the Internet library at:
http://www.ibm.com/systems/z/os/zos/bkserv/
Notices

This information was developed for products and services offered in the U.S.A. or elsewhere.

IBM may 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 described 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 character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 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 publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication 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:

Site Counsel
IBM Corporation
2455 South Road
Poughkeepsie, NY 12601-5400
USA

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 information 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.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Policy for unsupported hardware

Various z/OS elements, such as DFSMS, HCD, JES2, JES3, and MVS™, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

UNIX is a registered trademark of The Open Group in the United States and other countries.
Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Bibliography

This bibliography provides a list of publications that are useful when implementing the Tivoli directory server product.

### IBM z/OS Security Server publications
- [z/OS Migration](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), GA22-7499
- [z/OS Security Server RACF Command Language Reference](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SA22-7687
- [z/OS Security Server RACF Callable Services](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SA22-7691
- [z/OS Integrated Security Services Network Authentication Service Administration](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SC24-5926
- [z/OS Integrated Security Services Network Authentication Service Programming](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SC24-5927

### IBM Tivoli Directory Server for z/OS
- [IBM Tivoli Directory Server Administration and Use for z/OS](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SC23-5191
- [IBM Tivoli Directory Server Client Programming for z/OS](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SA23-2214
- [IBM Tivoli Directory Server Plug-in Reference for z/OS](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SA22-7621

### IBM C/C++ language publications
- [z/OS XL C/C++ Programming Guide](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SC09-4765
- [z/OS XL C/C++ Run-Time Library Reference](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SA22-7821

### IBM DB2 publications

### IBM z/OS Cryptographic Service publications
- [z/OS Open Cryptographic Services Facility Application Programming](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SC24-5899
- [z/OS Cryptographic Services ICSF Administrator’s Guide](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SA22-7521

### Other IBM publications
- [z/OS Communications Server: IP Configuration Guide](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SC31-8775
- [z/OS Communications Server: IP Configuration Reference](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SC31-8776
- [z/OS Program Directory](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), GH10-0670
- [z/OS Cryptographic Services System SSL Programming](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SC24-5901
- [z/OS UNIX System Services Planning](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), GA22-7800
- [z/OS Parallel Sysplex Overview](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SA22-7661
- [z/OS MVS Setting Up a Sysplex](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SA22-7625
- [z/OS SDSF Operation and Customization](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SA22-7670
- [z/OS Planning for Installation](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), GA22-7504
- [z/OS Introduction and Release Guide](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), GA22-7502
- [z/OS Licensed Program Specifications](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), GA22-7503
- [z/OS Collection](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SK3T-4271
- [Policy Director Authorization Services for z/OS and OS/390 Customization and Use](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SC24-6040
- [ServerPac: Using the Installation Dialog](http://publib.boulder.ibm.com/infocenter/zos/v2r1/index.jsp), SA22-7815
Index

A
About this document vii
accessibility 337
advanced replication messages 176

B
bibliography 343
books, related 343

C
C/C++ language publications 343
changed return codes 233
Conventions used in this document vii
Cryptographic Service publications 343

D
DB2 publications 343
disability 337
documentation
related 343

E
error codes 237
extended operations
messages 175

G
GDBM messages 175
advanced replication 175

H
How to use this document vii

I
IBM systems center publications viii
IBM Tivoli Directory Server for
z/OS 343
Intended audience vii

K
keyboard 337

L
LDAP server
messages 1
LDAP server messages 1
ldapdiff utility messages 211
LDAPResult construct 237
LDBM backend
messages 157
LDBM messages 157
ldif2ds utility messages 94
LookAt message retrieval tool viii

M
mainframe
education ix
message retrieval tool, LookAt viii

N
Notices 339

O
Other IBM publications 343

P
publications, related 343

R
reason codes 237
return and reason codes 233

S
server and bulkload messages 1
shortcut keys 337
Softcopy publications viii

T
TDBM backend
messages 139
TDBM messages
TDBM 139
Trademarks 340
troubleshooting
reason codes 237

U
Utility messages 117

V
V1R11 changed information xvi
V1R11 deleted information xvii
V1R11 new information xv
V1R11 refresh-new information xv
V1R12 changed information xiv
V1R12 new information xiv
V1R13 changed information xiii
V1R13 deleted information xiv
V1R13 new information xiii

W
Where to find more information vii

Z
z/OS Basic Skills information center ix
z/OS Security Server publications 343