版本信息

日期	版本	描述	作者
2004-03-02	v1.0	最初版本	LDAPChina.com

The LDAP Data Interchange Format (LDIF) - Technical Specification

LDAP 数据交换格式（LDIF）- 技术规范

本备忘录的状态（Status of this Memo）

本文档定义了一个用于 Internet 通讯的 Internet 标准跟踪协议，为了发展的需要讨论和建议。对于这个协议的状况和地位请参照 Internet 官方协议标准（"Internet Official Protocol Standards"（STD 1））的当前版。这个备忘录的传播是不受限制的。

版权提示（Copyright Notice）

目 录

摘要（Abstract）

本文档描述了一种文件格式，该文件格式描述目录信息或描述目录信息的修改。该文件格式称为 LDIF（LDAP Data Interchange Format），即 LDAP 数据交换格式，它一般用于在 LDAP 目录服务器之间导入、导出目录信息，或者描述应用到目录的一系列修改。

背景和用途（Background and Intended Usage）

交换格式描述了多种情况。例如，某人希望把目录服务器中的内容导出到一个文件中，然后拿到其他的机器上导入另一台目录服务器。

另外，通过使用一种定义完好的交换格式，在原有系统上开发导入工具将是非常便利的。用 awk 或 perl 编写的一套相当简单的工具可以将人员信息数据库转换成 LDIF 文件。这个文件随后可以被导入到其他的目录服务器中，无论这个目录服务器使用的是那种内部数据库。

LDIF 格式最初在密歇根大学实现的 LDAP 服务器中被开发并使用。最一开始 LDIF 用于描述目录的条目。后来，这种格式被扩展，并允许表达目录条目的改变。

应用程序/目录的 MIME（多用途的网际邮件扩充协议）内容类型（content-type）的关系：

应用程序/目录的 MIME 内容类型（参考文档[1]）是一种转换目录信息的通用构架和格式，它不依赖于任何一种特定的目录服务。LDIF 格式是一种更简单的格式，可以更易于创建，也可以被当作注释使用，来描述一系列应用于目录的更改。

本文档使用的关键字"MUST"，"MUST NOT"，"MAY"，"SHOULD"和"SHOULD NOT"与参考文档[7]中所描述的含意相同。

LDAP 数据交换格式定义（Definition of the LDAP Data Interchange Format）

LDIF 格式用于传送目录信息，或者描述一组目录条目的修改，LDIF 文件由一系列被行分隔符分开的记录组成。一条记录由一个描述目录条目的行的序列或者由一个描述一组目录条目变化的行的序列组成。一个 LDIF 文件指定一组目录条目，或者一组应用于目录条目的更改，但二者不能兼顾。

修改目录条目的操作（添加、删除、修改及修改 RDN）和下面描述的修改记录的类型

（”add”,”delete”,” modify”及”modrdn”或”moddn”）是一一对应的。这种对应关系是有意安排的，它允许将 LDIF 更改记录直接翻译成协议操作。

下列定义使用 RFC2234（参考文档[4]）中定义的扩展 Backus-Naur 形式。

```
ldif-file                = ldif-content / ldif-changes

ldif-content             = version-spec 1*(1*SEP ldif-attrval-record)

ldif-changes             = version-spec 1*(1*SEP ldif-change-record)

ldif-attrval-record      = dn-spec SEP 1*attrval-spec

ldif-change-record       = dn-spec SEP *control changerecord

version-spec             = "version:" FILL version-number

version-number           = 1*DIGIT
                             ; version-number MUST be "1" for the
                             ; LDIF format described in this document.

dn-spec                  = "dn:" (FILL distinguishedName /
                                  ":" FILL base64-distinguishedName)

distinguishedName        = SAFE-STRING
                             ; a distinguished name, as defined in [3]

base64-distinguishedName = BASE64-UTF8-STRING
                             ; a distinguishedName which has been base64
                             ; encoded (see note 10, below)

rdn                      = SAFE-STRING
                             ; a relative distinguished name, defined as
                             ; <name-component> in [3]

base64-rdn               = BASE64-UTF8-STRING
                             ; an rdn which has been base64 encoded (see
                             ; note 10, below)

control                  = "control:" FILL ldap-oid          ; controlType
                             0*1(1*SPACE ("true" / "false")) ; criticality
                             0*1(value-spec)                 ; controlValue
                             SEP
                             ; (See note 9, below)
```

```
ldap-oid                = 1*DIGIT 0*1("." 1*DIGIT)
                            ; An LDAPOID, as defined in [4]

attrval-spec            = AttributeDescription value-spec SEP

value-spec              = ":" (     FILL 0*1(SAFE-STRING) /
                                    ":" FILL (BASE64-STRING) /
                                    "<" FILL url)
                            ; See notes 7 and 8, below

url                     = <a Uniform Resource Locator,
                            as defined in [6]>
                                    ; (See Note 6, below)

AttributeDescription    = AttributeType [";" options]
                            ; Definition taken from [4]

AttributeType           = ldap-oid / (ALPHA *(attr-type-chars))

options                 = option / (option ";" options)

option                  = 1*opt-char

attr-type-chars         = ALPHA / DIGIT / "-"

opt-char                = attr-type-chars

changerecord            = "changetype:" FILL
                          (change-add / change-delete /
                            change-modify / change-moddn)

change-add              = "add"                 SEP 1*attrval-spec

change-delete           = "delete"              SEP

change-moddn            = ("modrdn" / "moddn") SEP
                            "newrdn:" (     FILL rdn /
                                        ":" FILL base64-rdn) SEP
                            "deleteoldrdn:" FILL ("0" / "1")    SEP
                            0*1("newsuperior:"
                            (       FILL distinguishedName /
                              ":" FILL base64-distinguishedName) SEP)
```

```
change-modify       = "modify"          SEP *mod-spec

mod-spec            = ("add:" / "delete:" / "replace:")
                      FILL AttributeDescription SEP
                      *attrval-spec
                      "-" SEP

SPACE               = %x20
                      ; ASCII SP, space

FILL                = *SPACE

SEP                 = (CR LF / LF)

CR                  = %x0D
                      ; ASCII CR, carriage return

LF                  = %x0A
                      ; ASCII LF, line feed

ALPHA               = %x41-5A / %x61-7A
                      ; A-Z / a-z

DIGIT               = %x30-39
                      ; 0-9

UTF8-1              = %x80-BF

UTF8-2              = %xC0-DF UTF8-1

UTF8-3              = %xE0-EF 2UTF8-1

UTF8-4              = %xF0-F7 3UTF8-1

UTF8-5              = %xF8-FB 4UTF8-1

UTF8-6              = %xFC-FD 5UTF8-1

SAFE-CHAR           = %x01-09 / %x0B-0C / %x0E-7F
                      ; any value <= 127 decimal except NUL, LF,
                      ; and CR
```

```
SAFE-INIT-CHAR          = %x01-09 / %x0B-0C / %x0E-1F /
                          %x21-39 / %x3B / %x3D-7F
                          ; any value <= 127 except NUL, LF, CR,
                          ; SPACE, colon (":", ASCII 58 decimal)
                          ; and less-than ("<" , ASCII 60 decimal)

SAFE-STRING             = [SAFE-INIT-CHAR *SAFE-CHAR]

UTF8-CHAR               = SAFE-CHAR / UTF8-2 / UTF8-3 /
                          UTF8-4 / UTF8-5 / UTF8-6

UTF8-STRING             = *UTF8-CHAR

BASE64-UTF8-STRING      = BASE64-STRING
                          ; MUST be the base64 encoding of a
                          ; UTF8-STRING

BASE64-CHAR             = %x2B / %x2F / %x30-39 / %x3D / %x41-5A /
                          %x61-7A
                          ; +, /, 0-9, =, A-Z, and a-z
                          ; as specified in [5]

BASE64-STRING           = [*(BASE64-CHAR)]
```

LDIF 语法的注意事项

1、 本文档中描述的 LDIF 格式版本号**必须**（MUST）为"1"。如果未标明版本号，实现**可以**（MAY）选择将其内容翻译成旧的 LDIF 文件格式，该格式由密歇根大学 ldap-3.3 实现（参考文档[8]）支持。

2、 在 LDIF 文件中，任何非空的行（即包含内容的行）**可以**（MAY）使用插入一个行分隔符（SEP）和一个空格符（SPACE）的方式进行拆分。用于拆分行的字符**绝不**（MUST NOT）能出现在行的第一个字符。换句话说，当将一行拆分成两行时，如果第一行为空，将是不允许的。任何以单个空格字符（space）开始的行**必须**（MUST）被看待为上一个非空行的延续。当连接多个被拆分的行时，必须精确地将每个延续行的开头的一个空格字符（译者注：若在每个延续行的开头存在多个空格，则也只能忽略其中一个空格）忽略。实现**不应该**（SHOULD NOT）在多字节 UTF-8 字符（multi-byte character）的中间拆分行。

3、 任何以"#"号（ASCII 码 35）开始的行都是注释行，并且解析 LDIF 文件时**必须**（MUST）被忽略。

4、 任何包含非已定义的"SAFE-UTF8-CHAR"字符，或者起始字符不是已定义的"SAFE-INIT-UTF8-CHAR"字符的 dn 或 rdn **必须**（MUST）使用 base-64 编码。其它值**可以**（MAY）使用 base-64 编码。任何包含非已定义的"SAFE-CHAR"字符，或其起始字符不是已定义的"SAFE-INIT-CHAR"字符的值**必须**（MUST）使用 base-64 编码。其它值**可以**（MAY）使用 base-64 编码。

5、 当 LDIF 文件直接包含一个 0 长度（zero-length）的属性值时，该值**必须**（MUST）表示为如下格式： AttributeDescription ":" FILL SEP（译者注：这里讲的 AttributeDescription 就是属性类型名，":"就是在属性类型名后面跟一个冒号，然后在":"后面跟一个行拆分符）。例如，后跟一个新行的"seeAlso:"表示一个 0 长度的"seeAlso"属性值。同时也允许 URL 参照的值为 0 长度值。

6、 当 URL 在 attrval-spec 中被指定时，应使用下列惯例：

a、 实现**应该**（SHOULD）支持 file:// URL 格式。被参照的文件的内容将被逐字逐句地包括至已翻译 LDIF 文件输出中。

b、 现实**可以**（MAY）支持其它 URL 格式。与每种支持的 URL 相关的语义将归档在相关的应用声明中。

7、 dn，rdn 和目录字符串（DirectoryString）的值语法**必须**（MUST）是有效的 UTF-8 字符串。读取 LDIF 的实现（译者注：这里的实现是指有解析 LDIF 能力的 LDAP 服务器或相关应用）**可以**（MAY）具有解释如下文件的功能，这种文件在存储上述实体（译者注：“这些实体”指上述的 dn，rdn 等）时，使用了其它字符集对这些实体进行编码。但实现**绝不**（MUST NOT）能产生不包含有效 UTF-8 数据的 LDIF 文件。

8、 以空格（SPACE）字符结尾的值或 dn 是 base-64 编码。

9、 当 LDIF 文件中包括 control（控制）时，实现**可以**（MAY）选择忽略其中的一部分或全部。这样做可能是必要的，因为有可能在 LDIF 文件中描述修改正在一个 LDAPv2 连接（LDAPv2 不支持 control）传递，或者有可能远程服务器不支持特殊的 control。如果 control 的关键性标志为"true"，则实现**必须**（MUST）或者包括该 control，或者**绝不**（MUST NOT）向远程服务器发送该操作。

10、 当 attrval-spec，dn，rdn 是 base-64 编码时，则在参考文档[5]中定义的编码规则与下列例外一同使用：

a、 base64 输出流必须表达为每行不多于 76 个字符的行，这一需求被去掉。LDIF 文件中的行可以仅按照在注意事项 2 中描述的拆分规则进行拆分。

b、 参考文档[5]中的 base64 字符串可以包含 BASE64-CHAR 定义之外的字符，并

被忽略。除了行拆分字符之外，LDIF 不允许任何无关字符。

LDIF 范例（Examples of LDAP Data Interchange Format）

范例 1：仅有两个条目的简单 LDAP 文件（Example 1: An simple LDAP file with two entries）

```
dn: cn=Barbara Jensen, ou=Product Development, dc=airius, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Barbara Jensen
cn: Barbara J Jensen
cn: Babs Jensen
sn: Jensen
uid: bjensen
telephonenumber: +1 408 555 1212
description: A big sailing fan.

dn: cn=Bjorn Jensen, ou=Accounting, dc=airius, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Bjorn Jensen
sn: Jensen
telephonenumber: +1 408 555 1212
```

范例 2：包含被拆分属性值的条目的文件（Example 2: A file containing an entry with a folded attribute value）

```
version: 1
dn:cn=Barbara Jensen, ou=Product Development, dc=airius, dc=com
objectclass:top
objectclass:person
objectclass:organizationalPerson
cn:Barbara Jensen
cn:Barbara J Jensen
cn:Babs Jensen
sn:Jensen
```

uid:bjensen
telephonenumber:+1 408 555 1212
description:Babs is a big sailing fan, and travels extensively in sea
 rch of perfect sailing conditions.
title:Product Manager, Rod and Reel Division

范例 3：包含 base-64 编码值的文件（Eample 3: A file containing a base-64-encoded value）

version: 1
dn: cn=Gern Jensen, ou=Product Testing, dc=airius, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Gern Jensen
cn: Gern O Jensen
sn: Jensen
uid: gernj
telephonenumber: +1 408 555 1212
description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvdSBhcmUhICBUaGlzIHZhbHVl
IGlzIGJhc2UtNjQtZW5jb2RlZCBiZWNhdXNlIGl0IGhhcyBhIGNvbnRyb2wgY2hhcmFjdG
VyIGluIGl0IChhIENSKS4NICBCeSB0aGUgd2F5LCB5b3Ugc2hvdWxkIHJlYWxseSBnZXQg
b3V0IG1vcmUu

范例 4：包含一个 UTF-8 编码属性值和语言标签的条目的文件。注释声明了 UTF-8 编码属性和 dn 的内容（Example 4: A file containing an entries with UTF-8-encoded attribute values, including language tags. Comments indicate the contents of UTF-8-encoded attributes and distinguished names）

version: 1
dn:: b3U95Za25qWt6YOoLG89QWlyaXVz
dn:: ou=<JapaneseOU>,o=Airius
objectclass: top
objectclass: organizationalUnit

ou:: 5Za25qWt6YOo
ou:: <JapaneseOU>
ou;lang-ja:: 5Za25qWt6YOo
ou;lang-ja:: <JapaneseOU>
ou;lang-ja;phonetic:: 44GI44GE44GO44KH44GG44G2
ou;lang-ja:: <JapaneseOU_in_phonetic_representation>
ou;lang-en: Sales
description: Japanese office
dn:: dWlkPXJvZ2FzYXdhcmEsb3U95Za25qWt6YOoLG89QWlyaXVz
dn:: uid=<uid>,ou=<JapaneseOU>,o=Airius
userpassword: {SHA}O3HSv1MusyL4kTjP+HKI5uxuNoM=
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
uid: rogasawara
mail: rogasawara@airius.co.jp
givenname;lang-ja:: 44Ot44OJ44OL44O8
givenname;lang-ja:: <JapaneseGivenname>
sn;lang-ja:: 5bCP56yg5Y6f
sn;lang-ja:: <JapaneseSn>
cn;lang-ja:: 5bCP56yg5Y6fIOODreODieODi+ODvA==
cn;lang-ja:: <JapaneseCn>
title;lang-ja:: 5Za25qWt6YOoIOmDqOmVtw==
title;lang-ja:: <JapaneseTitle>
preferredlanguage: ja
givenname:: 44Ot44OJ44OL44O8
givenname:: <JapaneseGivenname>
sn:: 5bCP56yg5Y6f
sn:: <JapaneseSn>
cn:: 5bCP56yg5Y6fIOODreODieODi+ODvA==
cn:: <JapaneseCn>
title:: 5Za25qWt6YOoIOmDqOmVtw==
title:: <JapaneseTitle>
givenname;lang-ja;phonetic:: 44KN44Gp44Gr44O8
givenname;lang-ja;phonetic::
<JapaneseGivenname_in_phonetic_representation_kana>
sn;lang-ja;phonetic:: 44GK44GM44GV44KP44KJ
sn;lang-ja;phonetic:: <JapaneseSn_in_phonetic_representation_kana>
cn;lang-ja;phonetic:: 44GK44GM44GV44KP44KJIOOCjeOBqeOBq+ODvA==
cn;lang-ja;phonetic:: <JapaneseCn_in_phonetic_representation_kana>
title;lang-ja;phonetic:: 44GI44GE44GO44KH44GG44G2IOOBtuOBoeOCh+OBhg==
title;lang-ja;phonetic::

```
# <JapaneseTitle_in_phonetic_representation_kana>
givenname;lang-en: Rodney
sn;lang-en: Ogasawara
cn;lang-en: Rodney Ogasawara
title;lang-en: Sales, Director
```

范例 5：包含一个外部文件参照的文件（Example 5: A file containing a reference to an external file）

```
version: 1
dn: cn=Horatio Jensen, ou=Product Testing, dc=airius, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Horatio Jensen

cn: Horatio N Jensen
sn: Jensen
uid: hjensen
telephonenumber: +1 408 555 1212
jpegphoto:< file:///usr/local/directory/photos/hjensen.jpg
```

范例 6：包含一系列变更记录和注释的文件（Example 6: A file containing a series of change records and comments）

```
version: 1
# Add a new entry
dn: cn=Fiona Jensen, ou=Marketing, dc=airius, dc=com
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Fiona Jensen
sn: Jensen
uid: fiona
telephonenumber: +1 408 555 1212
jpegphoto:< file:///usr/local/directory/photos/fiona.jpg

# Delete an existing entry
dn: cn=Robert Jensen, ou=Marketing, dc=airius, dc=com
```

```
changetype: delete

# Modify an entry's relative distinguished name
dn: cn=Paul Jensen, ou=Product Development, dc=airius, dc=com
changetype: modrdn
newrdn: cn=Paula Jensen
deleteoldrdn: 1

# Rename an entry and move all of its children to a new location in
# the directory tree (only implemented by LDAPv3 servers).
dn: ou=PD Accountants, ou=Product Development, dc=airius, dc=com
changetype: modrdn
newrdn: ou=Product Development Accountants
deleteoldrdn: 0
newsuperior: ou=Accounting, dc=airius, dc=com

# Modify an entry: add an additional value to the postaladdress
# attribute, completely delete the description attribute, replace
# the telephonenumber attribute with two values, and delete a specific
# value from the facsimiletelephonenumber attribute
dn: cn=Paula Jensen, ou=Product Development, dc=airius, dc=com
changetype: modify
add: postaladdress
postaladdress: 123 Anystreet $ Sunnyvale, CA $ 94086
-

delete: description
-
replace: telephonenumber
telephonenumber: +1 408 555 1234
telephonenumber: +1 408 555 5678
-
delete: facsimiletelephonenumber
facsimiletelephonenumber: +1 408 555 9876
-

# Modify an entry: replace the postaladdress attribute with an empty
# set of values (which will cause the attribute to be removed), and
# delete the entire description attribute. Note that the first will
# always succeed, while the second will only succeed if at least
# one value for the description attribute is present.
dn: cn=Ingrid Jensen, ou=Product Support, dc=airius, dc=com
changetype: modify
```

```
replace: postaladdress
-
delete: description
-
```

范例 7：包含一个带有 control 的变更记录的 LDIF 文件（Example 7: An LDIF file containing a change record with a control）

```
version: 1
# Delete an entry. The operation will attach the LDAPv3
# Tree Delete Control defined in [9]. The criticality
# field is "true" and the controlValue field is
# absent, as required by [9].
dn: ou=Product Development, dc=airius, dc=com
control: 1.2.840.113556.1.4.805 true
changetype: delete
```

安全考虑（Security Considerations）

对于典型的目录应用程序，LDIF 文件通常会涉及到一些敏感的私人数据。通过适当的方法处理可以保护 LDIF 文件中的隐私数据。

":<"标识符可以指向一个外部内容，以供处理 LDIF 文件时使用，因此在接受外部文件时要相当谨慎。一个“特洛伊”（"trojan"）LDIF 文件可以以敏感内容命名，然后诱使接收者将其条目导入目录，再利用非法条目通过 LDAP 读取目录。

对于 LDIF 文件 LDIF 不提供任何方法加载认证信息。LDIF 文件的使用者必须仔细验证从外部接受到的 LDIF 文件的完整性。

感谢（Acknowledgements）

LDAP 交换格式被开发作为 Michigan 大学 LDAP 参考实现的一部分，由 Tim Howes，Mark Smith 和 Gordon Good 负责开发。这个材料是基于国家科学基金（National Science Foundation under Grant No. NCR-9416667）支持的工作之上。

IETF LDAP 扩展工作组的几位人士对本文档提出了有价值的意见。特别是 Oslo 大学的 Hallvard B. Furuseth 对本文档提出了许多重要的建议，其中包括对 BNF 的全部检查和重写。

参考书目（References）

[1] Howes, T. and M. Smith, "A MIME Content-Type for Directory Information", RFC 2425, September 1998.

[2] Crocker, D., and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[3] Wahl, M., Kille, S. and T. Howes, "A String Representation of Distinguished Names", RFC 2253, December 1997.

[4] Wahl, M., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, July 1997.

[5] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

[6] Berners-Lee, T., Masinter, L. and M. McCahill, "Uniform Resource Locators (URL)", RFC 1738, December 1994.

[7] Bradner, S., "Key Words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[8] The SLAPD and SLURPD Administrators Guide. University of Michigan, April 1996. <URL: http://www.umich.edu/~dirsvcs/ldap/doc/guides/slapd/toc.html>

[9] M. P. Armijo, "Tree Delete Control", Work in Progress.

作者地址（Authors' Addresses）

Gordon Good
iPlanet e-commerce Solutions
150 Network Circle
Mailstop USCA17-201
Santa Clara, CA 95054, USA
Phone: +1 408 276 4351
EMail: ggood@netscape.com

完整的版权声明（Full Copyright Statement）

略