Red Hat Directory Server 12

管理目录属性和值

使用 ldapadd, ldapmodify, ldapdelete, 和 dsconf 实用程序或 web 控制台管理目录条目

Last Updated: 2024-07-03

Red Hat Directory Server 12 管理目录属性和值

使用 ldapadd, ldapmodify, ldapdelete, 和 dsconf 实用程序或 web 控制台管理目录条目

法律通告

摘要

了解如何使用 openldap-clients 软件包中的工具管理目录服务器条目。强制属性唯一性、分配服务类(CoS)以简化条目管理、减少存储要求并避免复制冲突。

目录

对红帽文档提供反馈

我们感谢您对文档提供反馈信息。请让我们了解如何改进文档。要做到这一点：

- 要通过 JIRA 提交反馈（需要帐户）：
  1. 登录到 Jira 网站。
  2. 在顶部导航栏中点 **Create**
  3. 在 **Summary** 字段中输入描述性标题。
  4. 在 **Description** 字段中输入您对改进的建议。包括到文档相关部分的链接。
  5. 点对话框底部的 **Create**。
- 要通过 Bugzilla 提交反馈（需要帐户）：
  1. 进入 Bugzilla 网站。
  2. 在 Component 中选择 **Documentation**。
  3. 在 **Description** 中输入您要提供的信息。包括文档相关部分的链接。
  4. 点 **Submit Bug**。

第 1 章 使用命令行管理目录条目

您可以使用命令行添加、编辑、重命名和删除 LDAP 条目。

1.1. 为 LDAPADD、LDAPMODIFY 和 LDAPDELETE 工具提供输入

当您添加、更新或删除目录中的条目或属性时，您可以使用工具的交互模式进入 LDAP 数据交换格式 (LDIF)语句或将 LDIF 文件传递给它们。

1.1.1. OpenLDAP 客户端工具的交互模式

在交互模式中，**ldapadd**、**ldapmodify** 和 **ldapdelete** 工具从命令行读取输入。要退出交互模式，请按 **Ctrl**+**D** (^D)组合键发送文件结束(EOF)转义序列。

在交互模式中，当您按 **Enter** 两次或发送 EOF 序列时，实用程序会将语句发送到 LDAP 服务器。

使用互动模式：

- 在不创建文件的情况下输入 LDAP 数据交换格式(LDIF)语句。

  例 1.1. 使用 ldapmodify 互动模式进入 LDIF 语句

  以下示例以互动模式运行 **ldapmodify**，删除 **telephoneNumber** 属性，并使用 **cn= manager _name,ou=people,dc=example,dc=com** 值将 manager 属性添加到 **uid=user,ou=people,dc=example,dc=com** 条目。在最后的声明后按 **Ctrl+D** 退出交互模式。

  ```
  # ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

  dn: uid=user,ou=people,dc=example,dc=com
  changetype: modify
  delete: telephoneNumber
  -
  add: manager
  manager: cn=manager_name,ou=people,dc=example,dc=com

  modifying entry "uid=user,ou=people,dc=example,dc=com"

  ^D
  ```

- 要将 LDIF 声明（由另一个命令输出）重定向到服务器：

  例 1.2. 使用带有重定向内容的 ldapmodify 互动模式

  以下示例将 **command_that_outputs_LDIF** 命令的输出重定向到 **ldapmodify**。在重定向的命令退出后，交互模式会自动退出。

  ```
  # command_that_outputs_LDIF | ldapmodify -D "cn=Directory Manager" -W -H
  ldap://server.example.com -x
  ```

其他资源

- **ldif (5)** 手册页

1.1.2. OpenLDAP 客户端工具的文件模式

在交互模式中，**ldapadd**、**ldapmodify** 和 **ldapdelete** 工具从文件中读取 LDAP 数据交换格式(LDIF)语句。使用此模式向服务器发送大量 LDIF 语句。

例 1.3. 将带有 LDIF 声明的文件传递给 ldapmodify

1. 使用 LDIF 语句创建文件。例如，使用以下语句创建 **~/example.ldif** 文件：

```
dn: uid=user,ou=people,dc=example,dc=com
changetype: modify
delete: telephoneNumber
-
add: manager
manager: cn=manager_name,ou=people,dc=example,dc=com
```

本例删除 **telephoneNumber** 属性，并使用 **cn= manager _name,ou=people,dc=example,dc=com** 值将 manager 属性添加到 **uid=user,ou=people,dc=example,dc=com** 条目。

2. 使用 **-f** 参数将文件传递给 **ldapmodify** 命令：

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x -f ~/example.ldif
```

其他资源

- **ldif (5)** 手册页

1.1.3. OpenLDAP 客户端工具的持续操作模式

默认情况下，如果您向服务器发送多个 LDAP 数据交换格式(LDIF)语句，另一个操作会失败，则进程将停止。但是，在错误发生前处理的条目已被成功添加、修改或删除。

要忽略错误并继续处理批处理中进一步的 LDIF 语句，请将 **-c** 参数传递给 **ldapadd** 和 **ldapmodify** ：

```
# ldpamodify -c -D "cn=Directory Manager" -W -H ldap://server.example.com -x
```

1.2. 使用命令行添加 LDAP 条目

要在目录中添加新条目，请使用 **ldapadd** 或 **ldapmodify** 工具。请注意，**/bin/ldapadd** 是到 **/bin/ldapmodify** 的符号链接。因此，**ldapadd** 执行与 **ldapmodify -a** 相同的操作。

注意

只有父条目已存在时，才能添加新目录条目。例如，如果 **ou=people,dc=example,dc=com** 不存在，则无法添加 **cn=user,ou=people,dc=example,dc=com** 父条目。

1.2.1. 使用 ldapadd 添加条目

要使用 **ldapadd** 工具来添加，例如 **cn=user,ou=people,dc=example,dc=com** 用户条目，请输入：

```
# ldapadd -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
uid: user
givenName: given_name
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
sn: surname
cn: user
```

注意

运行 **ldapadd** 会自动执行 **changetype: add** operation。因此，您不需要在 LDIF 语句中指定 **changetype: add**。

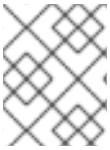
其他资源

- **ldapadd (1)** 手册页

1.2.2. 使用 ldapmodify 添加条目

要使用 **ldapmodify** 工具来添加 **cn=user,ou=people,dc=example,dc=com** 用户条目，请输入：

```
# ldapmodify -a -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
uid: user
givenName: given_name
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
sn: surname
cn: user
```



注意

将 **-a** 参数传递给 **ldapmodify** 命令时，实用程序会自动执行 **changetype: add** 操作。因此，您不需要在 LDIF 语句中指定 **changetype: add**。

其他资源

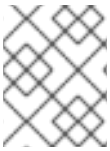
- **ldapmodify (1)** 手册页

1.2.3. 创建数据库后缀的根条目

要创建数据库后缀的根条目，如 **dc=example,dc=com**，以 **cn=Directory Manager** 用户身份绑定，并添加该条目。可区分名称(DN)对应于数据库的根或子后缀的 DN。

例如，要添加 **dc=example,dc=com** 后缀，请输入：

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: dc=example,dc=com
changetype: add
objectClass: top
objectClass: domain
dc: example
```



注意

只有在每个后缀有一个数据库时，才能添加 root 对象。如果创建存储在多个数据库中的后缀，则必须使用 **dsctl ldif2db** 命令来设置包含新条目的数据库。

其他资源

- 在服务器离线时使用命令行导入数据

1.3. 使用命令行更新 LDAP 条目

修改目录条目时，请使用 **changetype: modify** 语句。根据更改操作，您可以添加、更改或删除条目中的属性。

1.3.1. 在 LDAP 条目中添加属性

要为 LDAP 条目添加属性，请使用 **add** 操作。

例如，要将带有 **555-1234567** 值的 **telephoneNumber** 属性添加到 **uid=user,ou=People,dc=example,dc=com** 条目，请输入：

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
changetype: modify
add: telephoneNumber
telephoneNumber: 555-1234567
```

如果属性是多值值，您可以多次指定属性名称，以便在单个操作中添加所有值。例如，要将两个 **telephoneNumber** 属性一次添加到 **uid=user,ou=People,dc=example,dc=com** 中，请输入：

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
changetype: modify
add: telephoneNumber
telephoneNumber: 555-1234567
telephoneNumber: 555-7654321
```

1.3.2. 更新属性值

更新属性值的流程取决于属性是单值还是多值：

- 更新单值属性：

更新单值属性时，请使用 **replace** 操作来覆盖现有的值。以下命令更新 **uid=user,ou=People,dc=example,dc=com** 条目的 **manager** 属性：

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
changetype: modify
replace: manager
manager: uid=manager_name,ou=People,dc=example,dc=com
```

- 更新多值属性的特定值：
  要更新多值属性的特定值，首先删除您要替换的条目，然后添加新值。以下命令只更新 **uid=user,ou=People,dc=example,dc=com** 条目中当前设置为 **555-1234567** 的 **telephoneNumber** 属性：

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
changetype: modify
delete: telephoneNumber
telephoneNumber: 555-1234567
-
add: telephoneNumber
telephoneNumber: 555-9876543
```

1.3.3. 从条目中删除属性

要从条目中删除属性，请使用 **delete** 操作：

- 删除属性：
  例如，要从 **uid=user,ou=People,dc=example,dc=com** 条目中删除 **manager** 属性，请输入：

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
changetype: modify
delete: manager
```

重要

如果属性包含多个值，则此操作会删除所有值。

- 删除多值属性的特定值：
  如果要从多值属性中删除特定值，请在 LDAP Data Interchange Format (LDIF)语句中列出属性及其值。例如，要从 **uid=user,ou=People,dc=example,dc=com** 条目中删除设置为 **555-1234567** 的 **telephoneNumber** 属性，请输入：

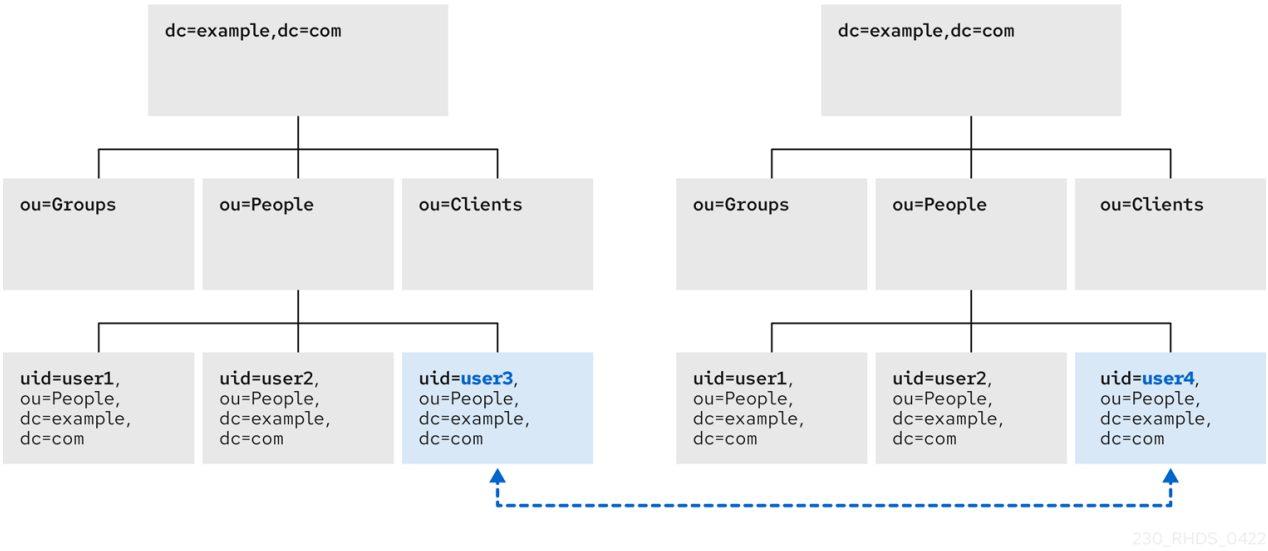
```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
changetype: modify
delete: telephoneNumber
telephoneNumber: 555-1234567
```

1.4. 重命名和移动 LDAP 条目

The following rename operations exist:

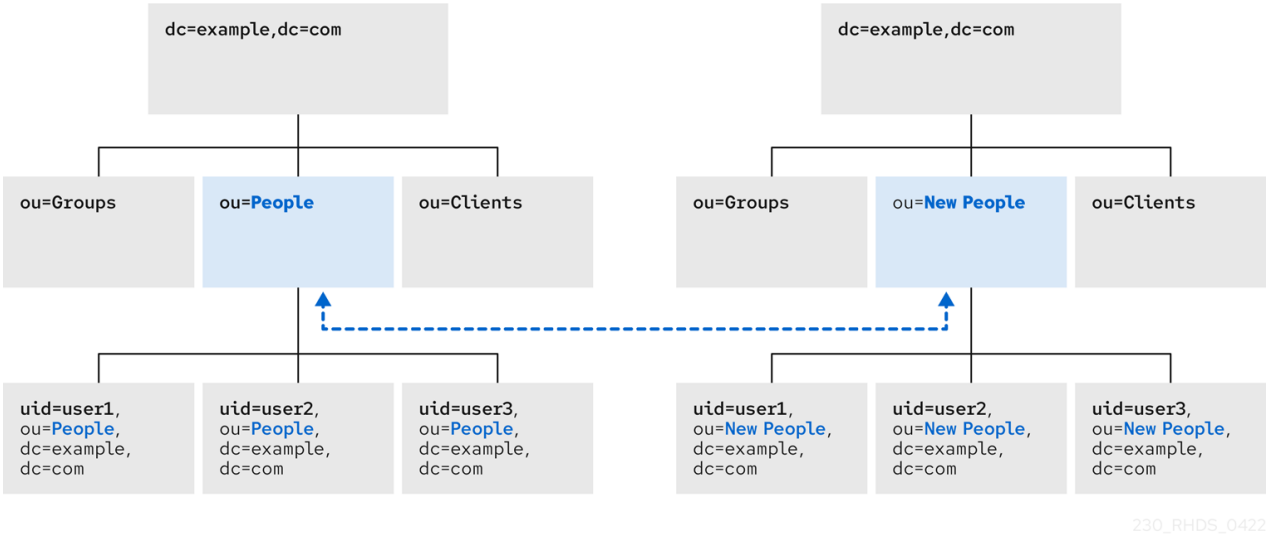
重命名条目

如果您重命名条目，**modrdn** 操作会更改条目的相对可分辨名称(RDN)：



重命名子条目

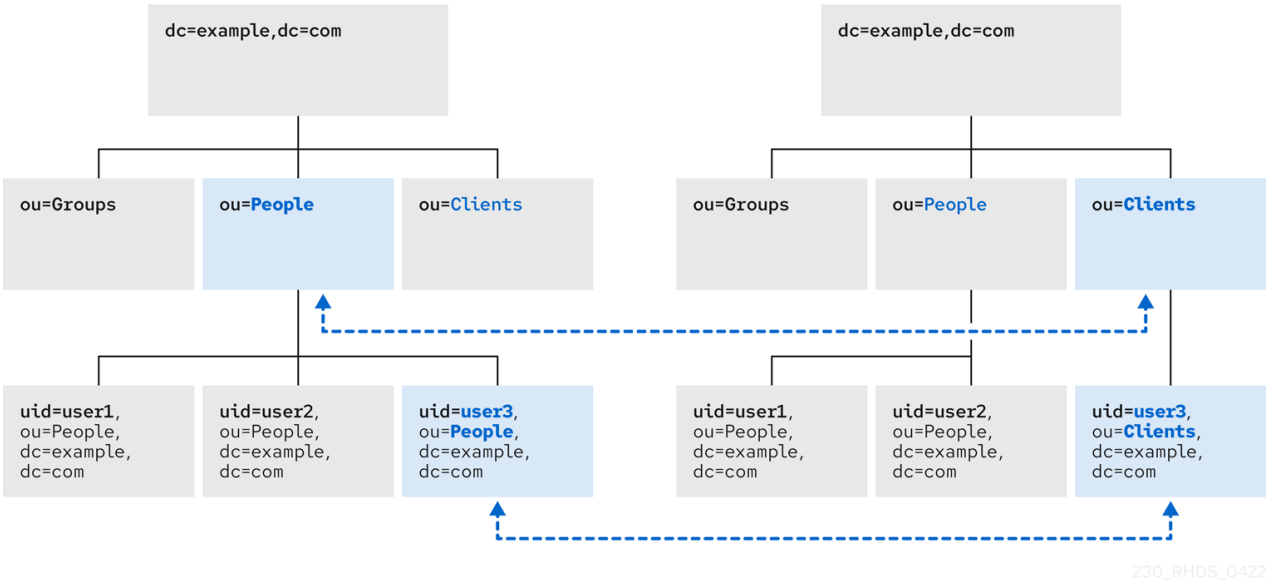
对于子树条目，**modrdn** 操作重命名子树以及子条目的 DN 组件：



请注意，对于大型子树，这个过程可能需要大量时间和资源。

将条目移到新父项

重命名子树的类似操作是将条目从一个子树移到另一个子树。这是展开的 **modrdn** 操作类型，它同时重命名条目并设置 **newSuperior** 属性，该属性将条目从一个父项移到另一个父属性：



1.4.1. 重命名 LDAP 条目的注意事项

在执行重命名操作时请注意以下几点：

- 您不能重命名 root 后缀。
- 子树重命名操作对复制具有最小效果。复制协议应用于整个数据库，不适用于数据库内的子树。因此，子树重命名操作不需要重新配置复制协议。子树重命名操作之后的所有名称都会正常进行复制。
- 重命名子树可能需要重新配置任何同步协议。同步协议在后缀或子树级别上设置。因此，重命名子树可能会破坏同步。
- 重命名子树要求手动为子树设置的任何子树级访问控制指令(ACI)，以及为子树的子条目设置的任何条目级 ACI。
- 尝试更改子树的组件，如从 **ou** 移到 **dc**，可能会因为 schema 违反而失败。例如，**organizationalUnit** 对象类需要 **ou** 属性。如果该属性作为重命名子树的一部分被删除，则操作会失败。
- 如果您移动组，**MemberOf** 插件会自动更新 **memberOf** 属性。但是，如果您移动包含组的子树，您必须在 **cn=memberof** 任务条目中手动创建任务，或使用 **dsconf memberof fixup** 命令来更新相关的 **memberOf** 属性。

1.4.2. 控制重命名条目时的相对可分辨名称行为

当您重命名条目时，**deleteOldRDN** 属性控制是否删除或保留旧的相对可分辨名称(RDN)：

deleteOldRDN: 0

现有 RDN 保留为新条目中的值。生成的条目包含两个 **cn** 属性：一个带有旧属性，另一个带有新的通用名称(CN)。
例如，以下属性属于从 **cn=old_group,dc=example,dc=com** 重命名为 **cn=new_group,dc=example,dc=com** 的组，并将 **deleteOldRDN** 属性设置为 **0** ：

> dn: *cn=new_group,ou=Groups,dc=example,dc=com*

```
objectClass: top
objectClass: groupOfUniqueNames
cn: old_group
cn: new_group
```

deleteOldRDN: 1

目录服务器删除旧条目，并使用新的 RDN 创建新条目。新条目仅包含新条目的 **cn** 属性。
例如，以下组被重命名为 **cn=new_group,dc=example,dc=com**，并将 **deleteOldRDN 属性**设置为 1：

```
dn: cn=new_group,ou=Groups,dc=example,dc=com
objectClass: top
objectClass: groupofuniquenames
cn: new_group
```

其他资源

- 重命名 LDAP 条目或子树

1.4.3. 重命名 LDAP 条目或子树

要重命名条目或子树，请使用 **changetype: modrdn** 操作，并在 **newrdn** 属性中设置新的相对可分辨名称(RDN)。

例如，要将 **cn=demo1,dc=example,dc=com** 条目重命名为 **cn=demo2,dc=example,dc=com**，请输入：

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: cn=demo1,dc=example,dc=com
changetype: modrdn
newrdn: cn=demo2
deleteOldRDN: 1
```

其他资源

- 控制重命名条目时的相对可分辨名称行为

1.4.4. 将 LDAP 条目移到新父项

要将条目移到新父项，请使用 **changetype: modrdn** 操作，并将以下内容设置为属性：

- **newrdn** ：设置移动条目的相对可分辨名称(RDN)。您必须设置此条目，即使 RDN 保持不变。
- **newsuperior** ：设置新 父条目的可分辨名称(DN)。

例如，要将 **cn=demo** 条目从 **ou=Germany,dc=example,dc=com** 移到 **ou=France,dc=example,dc=com**，请输入：

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: cn=demo,ou=Germany,dc=example,dc=com
```

```
changetype: modrdn
newrdn: cn=demo
newSuperior: ou=France,dc=example,dc=com
deleteOldRDN: 1
```

其他资源

- 控制重命名条目时的相对可分辨名称行为

1.5. 使用命令行删除 LDAP 条目

您可以从 LDAP 目录中删除条目，但只能删除没有子条目的条目。例如，如果 **uid=user, ou=People,dc=example,dc=com 条目仍然存在，则无法删除 ou=People,dc=example,dc=com** 条目。

1.5.1. 使用 ldapdelete 删除条目

ldapdelete 工具允许您删除一个或多个条目。例如，要删除 **uid=user,ou=People,dc=example,dc=com** 条目，请输入：

```
# ldapdelete -D "cn=Directory Manager" -W -H ldap://server.example.com -x
"uid=user,ou=People,dc=example,dc=com"
```

要删除一个操作中的多个条目，请将其附加到命令中：

```
# ldapdelete -D "cn=Directory Manager" -W -H ldap://server.example.com -x
"uid=user1,ou=People,dc=example,dc=com" "uid=user2,ou=People,dc=example,dc=com"
```

其他资源

- **ldapdelete (1)** 手册页

1.5.2. 使用 ldapmodify 删除条目

要使用 **ldapmodify** 工具删除条目，请使用 **changetype: delete** 操作。例如，要删除 **uid=user,ou=People,dc=example,dc=com** 条目，请输入：

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
changetype: delete
```

1.6. 在 OPENLDAP 客户端工具中使用特殊字符

使用命令行时，用引号括起有特殊含义的字符，如命令行解释器，如空格（）、星号 glock 或反斜杠(\)。根据命令行解释器，使用单引号或双引号。例如，要以 **cn=Directory Manager** 用户进行身份验证，请将用户的可分辨名称(DN)包含在引号中：

```
# ldapmodify -a -D "cn=Directory Manager" -W -H ldap://server.example.com -x
```

另外，如果 DN 在组件中包含逗号，请使用反斜杠转义。例如，要以 **uid=user,ou=People,dc=example.com Chicago** 进行身份验证，请输入：

```
# ldapmodify -a -D "cn=uid=user,ou=People,dc=example.com Chicago\, IL" -W -H
ldap://server.example.com -x
```

1.7. 在 LDIF 语句中使用二进制属性

某些属性支持二进制值，如 **jpegPhoto** 属性。添加或更新这样的属性时，实用程序会从文件中读取 属性的值。要添加或更新这样的属性，您可以使用 **ldapmodify** 工具。

例如，要将 **jpegPhoto** 属性添加到 **uid=user,ou=People,dc=example,dc=com** 条目，并从 **/home/user_name/photo.jpg** 文件读取属性值，请输入：

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
changetype: modify
add: jpegPhoto
jpegPhoto:< file:///home/user_name/photo.jpg
```

重要

请注意，：和 &lt ; 之间 **没有空格**。

1.8. 更新国际化目录中的 LDAP 条目

要将属性值与英语以外的语言搭配使用，请将属性的值与语言标签关联。

当使用 **ldapmodify** 更新设置了语言标签的属性时，您必须完全匹配值和语言标签，否则操作将失败。

例如，要修改设置了 **lang-fr** 语言标签的属性值，请在 modify 操作中包含该标签：

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
changetype: modify
replace: homePostalAddress;lang-fr
homePostalAddress;lang-fr: 34 rue de Seine
```

第 2 章 使用 WEB 控制台管理目录条目

您可以使用 Web 控制台添加、编辑、重命名和删除 LDAP 条目。

2.1. 使用 WEB 控制台添加 LDAP 条目

您可以使用 Web 控制台创建以下条目：

- users
- groups
- roles
- 组织单元(OU)
- 自定义条目

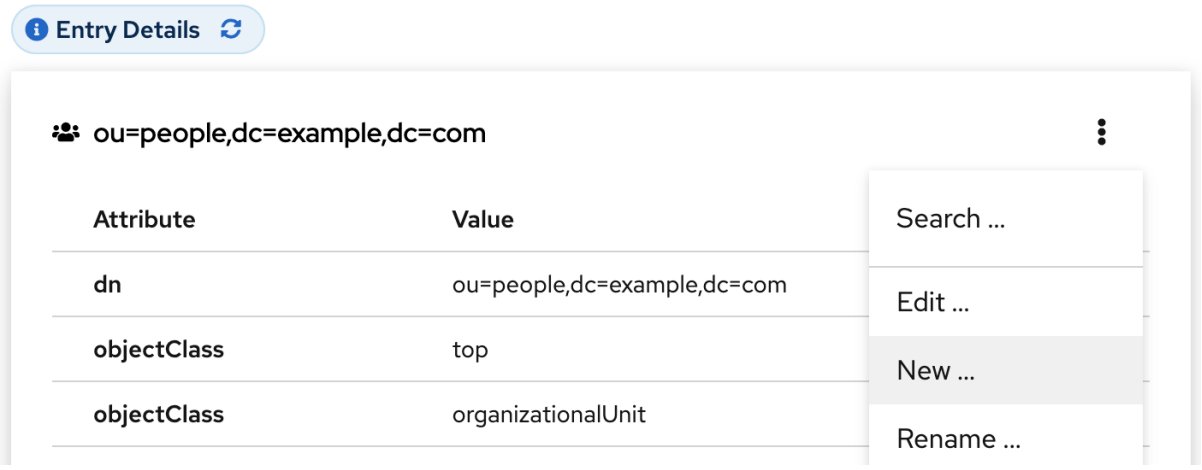
例如，您要创建带有密码的 POSIX 用户 **cn=John Smith,ou=people,dc=example,dc=com**。

前提条件

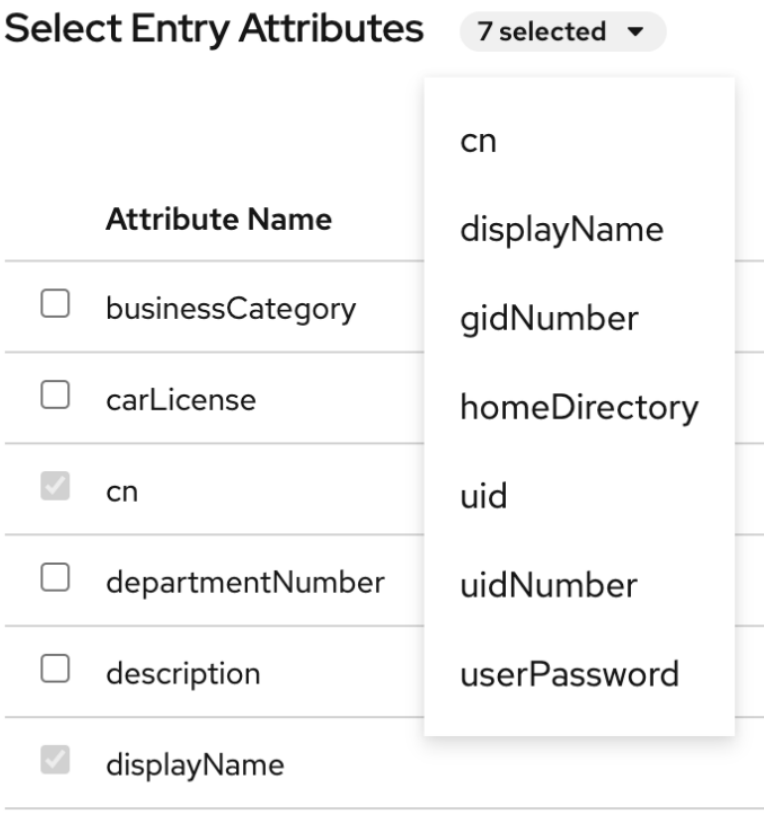
- 已登陆到 Directory Server web 控制台。
- 父条目存在。例如，**ou=people,dc=example,dc=com**。

流程

1. 打开 **LDAP 浏览器** 菜单，以显示现有后缀的列表。
2. 使用 **Tree** 或 **Table** 视图，展开您要创建用户的父条目 **ou=people,dc=example,dc=com**。
3. 点 Options 菜单(iwl)，然后选择 **New** 以打开向导窗口。

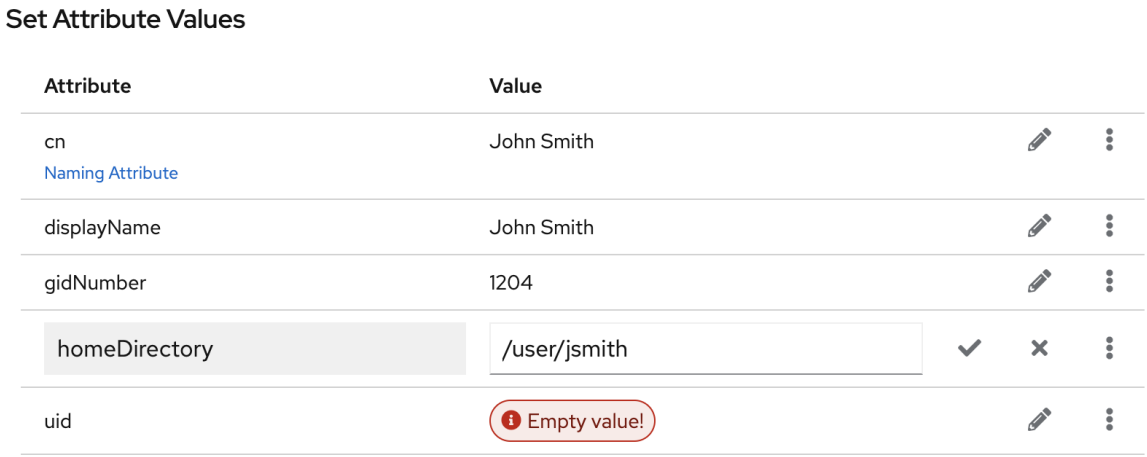


4. 选择 **Create a new User**选项，再单击 **Next**。
5. 对于用户条目，选择 **Posix 帐户类型** 并单击 **Next**。
6. 可选： 选择附加属性，如 **userPassword**，然后点 **Next**。您可以通过展开步骤名称旁边的下拉列表来查看所有选择的属性。



7. 为每个属性设置值：

   a. 单击属性的铅笔图标，再添加一个值。

   请注意，当您设置 **userPassword** 值时，会打开一个单独的菜单。该值被填充星号 packagemanifests 来隐藏纯文本。

   b. 点检查按钮保存更改。

   c. 可选：点 **Options** 菜单(busybox) → **Add Another Value** 来设置额外的属性值。

   d. 设置所有值后，单击 **Next**。

8. 验证所有条目详情都正确，然后单击 **创建用户**。目录服务器为 POSIX 用户创建带有强制属性的条目，并将密码设置为它。您可以点 **Back** 来修改条目设置，或者点击 **Cancel** 以取消条目创建。

9. 查看 **Entry Creation** 的 **Result**，再点 **Finish**。

验证

1. 导航到 **LDAP 浏览器 → 搜索**。
2. 选择包含条目的数据库后缀，如 **dc=example,cd=com**。
3. 在字段中输入您的搜索条件，如 **John**，然后按 **Enter** 键。
4. 在条目列表中找到您最近创建的条目。

2.2. 使用 WEB 控制台编辑 LDAP 条目

您可以使用 Web 控制台修改目录条目。本例通过以下方法修改用户条目 **cn=John Smith,ou=people,dc=example,dc=com** ：

- 添加电话号码 **556778987** 和 **556897445**.
- 添加电子邮件 **jsmith@example.com**.
- 更改密码。

前提条件

- 已登陆到 Directory Server web 控制台。

流程

1. 打开 **LDAP 浏览器** 菜单。
2. 使用 **Tree** 或 **Table** 视图，展开您要编辑的条目，如 **cn=John Smith,ou=people,dc=example,dc=com**。
3. 点 Options 菜单(busybox)，然后选择 **Edit** 以打开向导窗口。
4. 可选：在 **Select ObjectClasses** 步骤中，为条目添加或删除对象类。点击 **Next**。
5. 在 **Select Attributes** 步骤中，向条目添加 **telephoneNumber** 和 **mail** 属性，然后点 **Next**。如果没有看到您要添加到条目中的属性，这意味着您没有在上一步中添加对应的对象类。

注意

在这一步中，**您无法删除** 所选对象类的强制属性。

6. 在 **Edit Attribute Values** 步骤中，将 **telephoneNumber** 设置为 **556778987** 和 **556897445**，将**mail** 设置为 **jsmith@example.com** 并更改 **userPassword** 值：
   a. 单击属性的铅笔图标，并添加或更改新值。
   b. 点检查按钮保存更改。
   c. 可选：点 **Options 菜单(criu) → Add Another Value** 来为属性设置额外的值。本例中的 **telephoneNumber** 属性有两个值。设置所有值时，单击 **Next**。
7. 检查您的更改并点 **Next**。

8. 要编辑条目，请单击 **Modify Entry**。您可以点 **Back** 对条目进行其他更改，或者点击 **Cancel** 来取消条目编辑。

9. 查看 **Result for Entry Modification** 并点 **Finish**。

验证

- 展开条目详情，并查看条目属性中出现的新更改。

2.3. 使用 WEB 控制台重命名和重新定位 LDAP 条目或子树

其他资源

您可以使用 Web 控制台重命名或重新定位目录条目或子树。这个示例将条目 **cn=John Smith,ou=people,dc=example,dc=com** 重命名为 **cn=Tom Smith,ou=clients,dc=example,dc=com**。

前提条件

- 已登陆到 Directory Server web 控制台。

流程

1. 打开 **LDAP 浏览器** 菜单。

2. 使用 **Tree** 或 **Table** 视图，展开您要修改的条目，如 **cn=John Smith,ou=people,dc=example,dc=com**。

3. 点 Options 菜单(busybox)并选择 **Rename** 来打开向导窗口。

4. 在 **Select the Naming Attribute and Value** 步骤中：

   a. 为 naming 属性 **cn** 设置新值 **Tom Smith**，然后点 **Next**。

   b. 可选：从下拉菜单中选择另一个 naming 属性。

   c. 可选： 如果您要删除旧条目并使用新 RDN 创建新条目，请检查 **Delete the old RDN**。

5. 在 **Select The Entry Location** 步骤中，选择新位置的父条目，然后单击 **Next**。

6. 检查您对条目所做的更改，然后点 **Next**。

7. 如果条目详细信息正确，请单击 **Change Entry Name**。您可以点击 **Back** 对条目进行其他更改，或者点击 **Cancel** 来取消条目修改。

8. 查看 **Result for Entry Modification** 并点 **Finish**。

验证

- 展开条目详情并查看更新的条目。

2.4. 使用 WEB 控制台删除 LDAP 条目

您可以使用 web 控制台删除目录条目或子树。这个示例删除条目 **cn=Tom Smith,ou=clients,dc=example,dc=com**。

前提条件

前提条件

- 已登陆到 Directory Server web 控制台。

流程

1. 打开 **LDAP 浏览器** 菜单。
2. 使用 **Tree** 或 **Table** 视图，展开您要删除的条目，如 **cn=Tom Smith,ou=people,dc=example,dc=com**。
3. 点 Options 菜单(busybox)，然后选择 **Delete** 以打开向导窗口。
4. 查看您要删除的条目的数据后，点 **Next**。
5. 在 **Deletion** 步骤中，将开关切换到 **Yes，我确定** 位置并点 **Delete**。您可以单击 **Cancel** 来取消删除条目。
6. 查看 **Entry Deletion 的 Result**，然后点 **Finish**。

验证

1. 导航到 **LDAP 浏览器 → 搜索**。
2. 选择之前存在条目的后缀，如 **dc=example,cd=com**。
3. 在字段中输入您的搜索条件，如 **Tom**，然后按 **Enter** 键。
4. 验证删除的条目不再存在。

第 3 章 分配和管理唯一的数字属性值

有些条目属性需要唯一的数字标识符，如 **uidNumber** 和 **gidNumber**。目录服务器可以使用分布式数字分配(DNA)插件为指定属性自动生成这些唯一数字。

注意

DNA 插件不能保证 *属性唯一性*。pug-in 分配非重叠范围，允许在不执行或验证其唯一性的情况下手动将数字分配给受管属性。

使用 DNA 插件时，您可以有效地避免复制冲突。DNA 插件 *在单个* 后端间分配唯一数字。对于多层次复制，当每个供应商运行本地 DNA 插件实例时，您必须为每台服务器分配不同的数字范围。这样可确保每个实例都使用一组真正唯一的数字。

3.1. 关于动态数字分配

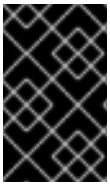
DNA 插件分配实例可以发布的可用数字范围。两个属性定义范围定义：服务器下一个可用数字（范围的 botton 值）及其最大值(范围的上限)。在配置插件时，您可以设置初始底部值。之后，插件会更新这个底部值。

通过将可用数字分解为每个副本上的独立范围，服务器可以持续分配数字，而不会相互重叠。

3.1.1. 过滤器、搜索和目标条目

服务器在内部执行排序的搜索，以验证其他服务器是否已采用下一个指定范围，要求 managed 属性具有具有正确顺序匹配规则的平等索引。

DNA 插件始终应用于目录树的特定区域(*范围*)和该子树中的特定条目类型(*过滤器*)。



重要

DNA 插件仅适用于 *单* 一后端，无法管理多个数据库的数量分配。DNA 插件使用排序控制来检查值是否在 DNA 插件外手动分配。但是，使用排序控制进行这个验证仅在 *单* 一后端上正常工作。

3.1.2. 范围和分配数字

目录服务器可以使用几种不同方法生成属性值：

- 在基本场景中，当向带有对象类的目录添加用户条目时，需要 unique-number 属性，但没有属性值，它会激活 DNA 插件来分配值。当 DNA 插件配置为为单个属性分配唯一值时，会出现这种情况。
- 更简单的选项使用 *magic 号* 作为 managed 属性的模板值。这个数字可以是数字，甚至是一个单词，位于服务器范围之外。该插件将其识别为信号，将其替换为新分配的值。当使用 magic 值添加条目并属于配置的 DNA 插件的范围和过滤器时，它会提示插件生成新值。例如，使用 **ldapmodify**，您可以添加 0 作为数字：

```
dn: uid=jsmith,ou=people,dc=example,dc=com
 changetype: add
 objectClass: top
 objectClass: person
 objectClass: posixAccount
```

```
uid: jsmith
cn: John Smith
uidNumber: 0
gidNumber: 0
```

DNA 插件仅生成一个新的、唯一的值。如果向条目添加或修改为 DNA 插件控制的属性使用特定值，则插件不会覆盖它。

3.1.3. 同一范围内的多个属性

DNA 插件可以从单个范围的唯一数字分配给单个或多个属性类型。

这为为属性分配唯一数字的多个选项：

- 来自唯一范围内的单个属性类型的单个数字。
- 个条目中两个属性的唯一数字相同。
- 为两个不同的属性分配与同一唯一范围不同的属性。

在很多情况下，为每个属性 type suffices 分配唯一数字。例如，当为新的员工条目分配 **employeeID** 时，确保每个员工条目都收到唯一的 **employeeID** 至关重要。

然而，在某些情况下，将同一数量范围内的唯一数字分配给多个属性非常有用。例如，当将 **uidNumber** 和 **gidNumber** 分配给 **posixAccount** 条目时，DNA 插件为这两个属性分配相同的数字。要达到此目的，请将两个受管属性传给修改操作，指定 magic 值。使用 **ldapmodify** ：

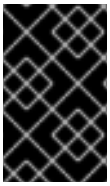
```
#  ldapmodify -D "cn=Directory Manager" -W -x

dn: uid=jsmith,ou=people,dc=example,dc=com
changetype: modify
add: uidNumber
uidNumber: 0
-
add:gidNumber
gidNumber: 0
```

当 DNA 插件处理多个属性时，如果对象类只允许一个属性，它只能为一个属性分配一个唯一值。例如，**posixGroup** 对象类允许 **gidNumber** 而不是 **uidNumber**。如果 DNA 插件同时管理 **uidNumber** 和 **gidNumber**，它会在创建 **posixGroup** 条目 时从 **uidNumber** 和 **gidNumber** 属性范围内分配 gidNumber 的唯一数字。为所有受管属性共享池可确保统一分配唯一数字，从而防止在不同条目上的 **uidNumber** 和 **gidNumber** 冲突，与单独的范围相同。

如果 DNA 插件管理多个属性，它将在单个修改操作中为所有属性分配相同的值。要分配同一范围内的 *不同* 数字，您需要执行单独的修改操作。例如，您可以使用 **ldapmodify** ：

```
# ldapmodify -D "cn=Directory Manager" -W -x
dn: uid=jsmith,ou=people,dc=example,dc=com
changetype: modify
add: uidNumber
uidNumber: 0
^D

# ldapmodify -D "cn=Directory Manager" -W -x
dn: uid=jsmith,ou=people,dc=example,dc=com
```

```
changetype: modify
add: employeeId
employeeId: magic
```



重要

要使用 DNA 插件为多个属性分配唯一数字，请为需要它的每个属性指定一个唯一值。与不需要此属性的单个属性不同，多个属性需要您可以指定唯一值。在某些情况下，条目不允许范围中的所有属性，或者可能允许所有类型，但只有需要唯一值的子集。

例 3.1. 示例。DNA 和唯一银行客户号码

示例 bank 管理员配置 DNA 插件，为客户的 **primaryAccount** 和 **customerID** 属性分配共享的唯一号码。

该银行还希望为次要帐户分配唯一数字，与主要帐户不同，但与客户 ID 和主要帐户相同。Example bank 管理员配置 DNA 插件，以管理 **secondaryAccount** 属性，并在将唯一数字分配给 **primaryAccount** 和 **customerID** 后添加后输入的属性。这为 **primaryAccount** 和 **customerID** 保证一个共享的唯一号码，它们具有相同的范围的不同和唯一的 **secondaryAccount** 号码。