Red Hat Directory Server 12

搜索条目和调优搜索

查找目录条目并改进搜索性能

Last Updated: 2024-11-23

Red Hat Directory Server 12 搜索条目和调优搜索

查找目录条目并改进搜索性能

法律通告

摘要

您可以使用 Web 控制台、命令行并使用 LDAP 搜索实用程序搜索目录条目。可以使用资源限值提高搜索性能，并可在用户级别和匿名绑定全局设置资源限值。

目录

提供有关红帽目录服务器的反馈

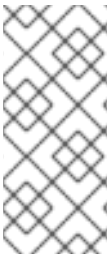
我们感谢您对我们文档和产品的输入信息。请让我们了解如何改进文档。要做到这一点：

- 要通过 JIRA 提交有关红帽目录服务器文档的反馈（需要帐户）：
  1. 转至 红帽问题跟踪程序。
  2. 在 **Summary** 字段中输入描述性标题。
  3. 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。
  4. 点对话框底部的 **Create**。
- 通过 JIRA 提交有关红帽目录服务器产品的反馈（需要帐户）：
  1. 转至 红帽问题跟踪程序。
  2. 在 **Create Issue** 页面上，单击 **Next**。
  3. 填写 **Summary** 字段。
  4. 在 **Component** 字段中选择组件。
  5. 填写 **Description** 字段，包括：
     a. 所选组件的版本号。
     b. 重现问题的步骤或您的建议以改进。
  6. 点 **Create**。

第 1 章 使用命令行查找条目(LDAPSEARCH)

您可以使用 **ldapsearch** 命令行工具搜索目录条目。此工具使用指定的身份和凭证打开到指定服务器的连接，并根据指定的搜索过滤器查找条目。搜索范围可以包括：

- 单个条目(**-s base**)
- 条目即时子条目(**-s one**)
- 整个树或子树(**-s 子**)



注意

ldapsearch 工具不会根据可分辨名称中的属性搜索目录条目。可分辨名称只是目录条目的唯一标识符，不能用作搜索键。相反，Keygester 根据条目中存储的属性值对搜索条目。**如果条目的可分辨名称为 uid=bjensen,ou=People,dc=example,dc=com，则搜索 dc=example 不匹配该条目，除非将 dc:example 明确添加为此条目的属性值对。**

ldapsearch 工具以 LDIF 格式返回 RFC 2849 规范中定义的 LDIF 格式。

1.1. LDAPSEARCH 命令格式

ldapsearch 命令必须使用以下格式：

```
# ldapsearch [-x | -Y mechanism] [options] [search_filter] [list_of_attributes]
```

- **-x 或 -Y**

  使用 -x （简单绑定）或 -Y (SASL 机制)来配置连接的类型。

- *选项*

  ldapsearch 命令行选项。如果使用了搜索过滤器前，指定搜索过滤器前的选项。

- ***search_filter***

  LDAP 搜索过滤器。如果您使用 -f 选项在文件中配置搜索过滤器，则不要指定搜索过滤器。

- *list_of_attributes*

  以空格分开的属性列表。指定属性列表可减少搜索结果中返回的属性数量。此属性列表必须在搜索过滤器后显示。如果没有指定属性列表，搜索会返回目录中设置的所有属性的值，但操作属性除外。

  如果您希望搜索返回操作属性，则必须在 ldapsearch search 命令中明确指定它。要返回对象的所有操作属性，请使用 +。要检索除明确指定的操作属性外的常规属性，请在属性列表中使用星号(DSL)。

  请注意，您可能需要使用反斜杠转义星号(\)。

  要仅检索匹配的 DN 列表，请使用属性 1.1。例如：

```
# ldapsearch -D "cn=Directory Manager" -W -H ldap://server.example.com \
   -b "dc=example,dc=com" -x "(objectclass=inetorgperson)" 1.1
```

其他资源

- LDAP 搜索过滤器
- 常用的 ldapsearch 选项

1.2. 常用的 LDAPSEARCH 选项

下表列出了最常用的 ldapsearch 工具选项。如果指定的值包含空格字符，则该值必须以单引号或双引号括起来，例如：

```
-b "cn=My Special Group,ou=groups,dc=example,dc=com"
```

重要

OpenLDAP 的 ldapsearch 工具默认使用 SASL 连接。要执行一个简单的绑定或使用 TLS，请使用 -x 参数来禁用 SASL 并允许其他连接方法。

选项	描述
-b	指定搜索的起点 - 基础可辨识名称(DN)。请注意，可以在数据库中存在区分名称。如果将 **LDAP_BASEDN** 环境变量设置为基本 DN，则不需要使用这个选项。 如果值包含空格字符，则必须在单引号或双引号中指定 option 值。例如： **-b "cn=user,ou=Product Development,dc=example,dc=com"**。 要搜索根 DSE 条目，请在此处指定一个空字符串，如 **-b ""**。
-D	指定用于向服务器进行身份验证的 DN。目录服务器必须识别 DN 值，并且 DN 必须具有搜索条目的授权。例如： **-D "uid=user_name,dc=example,dc=com"**。 如果服务器支持匿名访问，则不要指定这个选项。
-H	指定连接到服务器的 LDAP URL。LDAP URL 具有以下格式： > ldap[s]://*hostname*:[*port*] 指定 port 值是可选的。然后 **ldapsearch** 工具将使用默认的 LDAP 端口 389 或 LDAPS 端口 636。 该工具也可以使用 LDAPI URL，以及 HTML 十六进制代码 %2F 分隔的每个元素，而不是正斜杠(/)。例如： > ldapi://%2Ffull%2Fpath%2Fto%2Fslapd-example.socket 对于 LDAPI，指定代表服务器正在侦听的 LDAPI 套接字的文件的完整路径。如果您没有指定 URL，则 **ldapsearch** 将使用 localhost 或 **/etc/openldap/ldap.conf** 文件中指定的设置。
-h	指定安装了 Directory Server 的机器的主机名或 IP 地址。例如，**-h server.example.com**。如果您没有指定主机，则 **ldapsearch** 将使用 localhost。目录服务器支持 IPv4 和 IPv6 地址。  **注意** **-h** 选项已弃用，并将在以后的发行版本中删除。改为使用 **-H** 选项。

选项	描述
-p	指定 Directory 服务器使用的 TCP 端口号。例如，**-p 1049**。默认端口号为 **389**。  **注意** **p** 选项已弃用，并将在以后的发行版本中删除。
-l	指定搜索请求完成的最大时间限值（以秒为单位）。例如，**-l 300**。时间限制不应超过 **nsslapd-timelimit** 属性中指定的值，因为 **ldapsearch** 实用程序比较这两个值并使用最小的值。默认的 **nsslapd-timelimit** 属性值为 **3600** 秒。
-s scope	指定搜索的范围。您可以选择以下范围之一： • **子** 通过 **-b** 选项指定的条目及其所有子代条目进行搜索。这是默认设置。 • **一个** 通过 **-b** 选项指定的条目的直接子项进行搜索。**ldapsearch** 工具只考虑子项，而不是基本 DN 本身。 • **基本** 仅通过 **-b** 选项指定的条目搜索，或者由 **LDAP_BASEDN** 环境变量定义。
-W	提示密码。如果您没有指定选项，则 **ldapsearch** 工具将使用匿名访问。或者，使用 **-w** 选项将密码传递给实用程序。  **注意** 密码可以在用户的进程列表中可见，并保存在 shell 的历史记录中。
-x	禁用默认 SASL 连接以允许简单的绑定。
-Y SASL_mechanism	设置用于身份验证的 SASL 机制。如果您没有设置任何机制，则 **ldapsearch** 会选择服务器支持的最佳机制。如果不使用 **-x** 选项，您必须指定 **-Y** 选项。
-z number	设置在响应搜索请求时返回的最大条目数。在使用 root DN 绑定时，这个值会覆盖 **nsslapd-sizelimit** 属性。

选项	描述
-f	指定带有搜索过滤器的文件。

其他资源

- nsslapd-timelimit 描述
- nsslapd-sizelimit description

1.3. 使用特殊字符

使用 ldapsearch 工具时，您可能需要使用对命令行解释器有特殊含义的字符指定值，如空格字符、星号(VirtualMachine)或反斜杠(\)。根据命令行解释器，将具有特殊字符的值包含在单引号(' ')或双引号(" ")引号中。例如：

```
-D "cn=John Smith,ou=Product Development,dc=example,dc=com"
```

通常，使用单引号(')括起值。使用双引号(" ")在有 shell 变量时允许变量插入。

第 2 章 使用 WEB 控制台查找条目

您可以使用 Web 控制台搜索目录条目。

2.1. 使用 LDAP 浏览器查找条目

您可以使用 Web 控制台中的 LDAP 浏览器搜索目录服务器数据库中的条目。

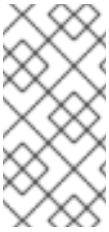
目录服务器根据条目中存储的属性值对搜索条目，而不是根据这些条目的可分辨名称(DN)中使用的属性。例如，如果条目的 DN 为 uid=user_name,ou=People, dc=example,dc=com，则仅在此条目中存在 dc:example 属性时搜索 dc=example。

先决条件

- 已登陆到 Directory Server web 控制台。
- 您有 root 权限。

流程

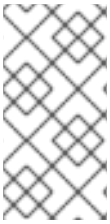
1. 在 Web 控制台中，导航到 LDAP 浏览器 → 搜索。
2. 展开并选择过滤条目的搜索条件：

搜索参数	描述
搜索基础	指定搜索的起点。它是当前存在于数据库中的可分辨名称(DN)。  **注意** 当您在 Tree View 或 Table View 中打开条目详细信息时，会打开带有预定义的搜索基础的 Search 标签页，点 Options 菜单(IANA)并选择 Search。

搜索参数	描述
搜索范围	选择 **Subtree** 来搜索整个子树中的条目，从搜索基础开始，并包含所有子条目。 从搜索基础开始选择一个 **级别** 来搜索条目，仅包含第一个子条目级别。 选择 **Base** 来仅在指定为搜索基础的条目中搜索属性值。
大小限制	设置从搜索操作返回的最大条目数。
时间限制	设置搜索引擎可以查找条目的时间（以秒为单位）。
显示锁定	切换到 **on** 以查看找到条目的锁定状态。
搜索属性	选择搜索中部分的属性。您可以从预定义的属性中选择并添加自定义属性。

3. **在搜索文本字段中输入属性值，然后按 Enter 键。**

4. **可选： 要进一步重新定义搜索，请使用 Filter 选项卡中的搜索过滤器来搜索条目。**



注意

目录服务器将所有搜索请求记录到访问日志文件，您可以在 Monitoring → Logging → Access Log 中查看。

其他资源

- **nsslapd-timelimit 描述**
- **nsslapd-sizelimit description**

第 3 章 LDAP 搜索过滤器

搜索过滤器选择搜索操作返回的特定条目。您可以在 ldapsearch 命令行工具或 Directory Server web 控制台中使用搜索过滤器。

目录服务器根据属性值对存储来搜索条目，而不是根据这些条目的可分辨名称(DN)中使用的属性。例如，如果条目具有 DN uid=user_name,ou=People, dc=example,dc=com，则仅在此条目中存在 attribute-value 对 dc:example 时搜索 dc=example。

使用 ldapsearch 时，您可以在一个文件中定义多个搜索过滤器，每个过滤器在单独的行中。或者，您可以直接在命令行中指定搜索过滤器。

搜索过滤器具有以下基本语法：

```
(<attribute><operator><value>)
```

例如，搜索过滤器 (employeeNumber >= 500) 将 employeeNumber 作为属性，& gt;= 作为 Operator，500 作为值。

带有匹配规则的搜索过滤器具有以下语法：

```
(<attribute>:<matching_rule>:=<value>)
```

例如，搜索过滤器 (givenName:caseExactMatch:=Daniel) 具有 givenName 作为属性，caseExact Match 作为匹配规则，Daniel 作为值。

您可以定义将不同属性与布尔值运算符结合使用的过滤器。

3.1. 使用 LDAP 搜索过滤器中的属性

基本搜索查找条目中存在属性或特定值。搜索可以以多种方式查找条目的属性：

- 检查属性是否存在（下级搜索）。存在搜索使用星号(*)返回设置特定属性的每个条目，而不考虑值。

例如，" (manager.4-1.) " 过滤器返回具有 manager 属性的每个条目。

- 匹配确切的属性值（例如，搜索质量）。平等搜索查找具有特定值的属性。例如，" (cn= example) " 过滤器返回包含通用名称(cn)设置为示例 的所有条目。

  当属性具有与语言标签关联的值时，搜索会返回所有值。因此，以下两个属性值都与 " (cn=example) " 过滤器匹配：

  ```
  cn: example
  cn;lang-fr: example
  ```

- 列表与部分值匹配（子字符串搜索）。例如，" (sn.4-1.erson) " 搜索过滤器返回以下值：

  ```
  sn: Derson
  sn: Anderson
  ```

  有关配置子字符串搜索长度的详情，请参阅 在子字符串索引中更改搜索密钥长度。

3.2. 在 LDAP 搜索过滤器中使用 OPERATOR

LDAP 搜索过滤器中的 Operator 会设置属性和给定搜索值之间的关系。在搜索人员时，您可以使用运算符设置范围，来返回位于特定数字后的字母数或员工数字子集中的姓氏。

```
(employeeNumber>=500)
(sn~=suret)
(salary<=150000)
```

当在国际目录中有 imperfect 信息或搜索，您可以使用运算符进行电话号码和大约搜索，以使搜索操作更高效。

您可以在搜索过滤器中使用以下 Operator：

搜索类型	操作符	描述
相等	=	返回带有与指定的值完全匹配的属性的条目。例如：**cn=example**。

搜索类型	操作符	描述
子字符串	=string* string	返回包含值中指定子字符串的属性的条目。例如：**cn=exa598l**。星号 (*) 表示零 (0) 或多个字符。
大于或等于	>=	返回包含值大于或等于指定的值的属性的条目。例如，**uidNumber>=5000**
小于或等于	<=	返回包含值小于或等于指定的值的属性的条目。例如：**uidNumber<=5000**
存在	=*	返回包含指定属性的一个或多个值的条目。例如：**cn= the**。
大约	~=	返回包含指定属性的条目，其值大约等于搜索过滤器中指定的值。例如，**l~=san fransico** 返回 **l=san francisco**。

3.3. 使用复合 LDAP 搜索过滤器

您可以使用在前缀标记中表示的布尔值运算符组合多个 LDAP 搜索过滤器组件，如下所示：

```
(<boolean-operator>(filter)(filter)(filter)...)
```

您可以使用以下布尔值运算符：

Operator	符号	描述
和	Ampersand (&)	所有指定的过滤器都必须为 true，才能为 true。例如，**(& (filter) (filter) (filter)...)**
或者	垂直栏(|)	至少一个指定的过滤器必须为 true，声明必须为 true。例如，**(| (filter) (filter) (filter)...)**
非	感叹号(!)	对于该语句，指定语句不能为 true。只有一个过滤器会受到 not 运算符的影响。例如，**(! (filter))**

搜索操作会按照以下顺序评估布尔值表达式：

- Innerest toest parenthetical 表达式最先。
- 然后，服务器会更改顺序，以首先评估最严格的表达式。

当复合搜索过滤器组合到已完成的表达式中时，复合搜索过滤器最有用，例如：

```
(<boolean-operator>(filter)((<boolean-operator>(filter)(filter))))
```

您可以将复合过滤器与其他类型的搜索（大约、子字符串及其他运算符）相结合，来获取详细的结果。以下示例过滤器返回所有具有机构单元(ou)的条目，其 description 属性不包含子字符串 X.500 ：

```
(&(ou=Marketing)(!(description=*X.500*)))
```

另外，您可以扩展过滤器来返回将 管理器 设置为 example 或 demo 的条目：

```
(&(ou=Marketing)(!(description=*X.500*))(|
(manager=cn=example,ou=Marketing,dc=example,dc=com)
(manager=cn=demo,ou=Marketing,dc=example,dc=com)))
```

以下示例过滤器返回没有代表人的所有条目：

```
(!(objectClass=person))
```

以下过滤器返回没有代表人员以及通用名称(cn)与 printer3b 类似的所有条目：

```
(&(!(objectClass=person))(cn~=printer3b))
```

3.4. 在 LDAP 搜索过滤器中使用匹配规则

匹配规则指定目录服务器如何将属性中存储的值与搜索过滤器中的值进行比较。匹配规则与属性语法相关。当属性语法定义属性值的格式时，匹配的规则定义如何比较和索引格式。匹配规则也定义如何生成索引密钥。

匹配的规则是一个 schema 元素，它有一个对象标识符(OID)。目录服务器中的所有属性都定义了匹配的规则。有关匹配规则类型的更多信息，请参阅 匹配规则类型。通过在搜索过滤器中指定匹配规则，您可以使用与 schema 中属性定义的匹配规则匹配的规则搜索属性值。

具有可扩展匹配规则的过滤器具有以下语法：

```
(<attribute>:<matching_rule>:=<value>)
```

其中：

- <attribute > 是一个属于您搜索的条目的属性，如 cn,mail,name。
- <matching_rule > 是一个字符串，其中包含您要根据所需语法用于匹配属性值的规则的名称或 OID。例如，case ExactMatch 匹配规则。
- <value > 是属性值或关系运算符，加上要搜索的属性值。

匹配的规则必须与您搜索的属性的语法兼容。您可以为一个定义不区分大小写的匹配规则的属性运行区分大小写的搜索。例如，name 属性在 schema 定义中具有预定义的 caseIgnoreMatch equality 匹配规则。带有过滤器 (name=Daniel) 的基本等同性搜索会检索包含 名称 属性值（如 DAniel、daniel、Daniel ）的条目。带有匹配规则过滤器 (name:caseExactMatch:=Daniel) 的平等搜索会检索只包含 name 属性值 Daniel 的条目。

为 Directory 服务器定义的许多匹配规则与语言代码相关，并设置国际化的合计订单。例如，OID 2.16.840.1.113730.3.3.2.17.1 标识 Finnish collation 顺序。有关支持的国际化订单的完整列表，请参阅 语言排序匹配规则 和语言 子字符串匹配规则。

其他资源

- 匹配规则类型
- 使用 inchainMatch 匹配规则来查找 LDAP 条目的 ancestry
- LDAP 搜索(ldapsearch)示例

- 常用的匹配规则

3.4.1. 匹配规则类型

没有指定匹配规则的搜索过滤器，如(employeeNumber>=500)或(sncategorieserson)，使用其 schema 定义中属性语法定义的匹配规则。您可以为 schema 定义中的属性定义以下匹配规则类型：

相等

EQUALITY 匹配规则指定如何为相等匹配比较两个值。例如，如何处理 Fred 和 FRED 等字符串。更新操作使用 EQUALITY 规则来生成索引密钥。使用过滤器（如 (name=Fred) ）搜索操作，使用 EQUALITY 规则将过滤器中的值与条目中的值进行比较。

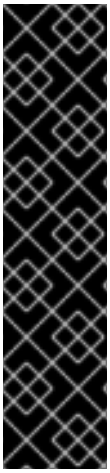
排序

ORDERING 匹配规则指定如何比较两个值，以确定一个值是否大于或等于另一个值。搜索过滤器，设置一个范围，如 (employeeNumber>=500) 或 (attribute value)，使用 ORDERING 规则。具有 ORDERING 规则顺序排列相等值的属性的索引。

SUBSTR

SUBSTR 匹配规则指定如何比较子字符串值。子字符串搜索过滤器，如 (name requireed)，使用 SUBSTR 规则。子字符串(sub)索引使用 SUBSTR 规则来生成索引密钥。

除了相等、排序和子字符串匹配规则外，您还可以在搜索过滤器中指定大约和其他可扩展匹配规则。



重要

目录需要匹配的规则来支持搜索或索引对应的搜索过滤器或索引类型。例如，属性必须具有与 EQUALITY 匹配规则，才能支持该属性的相等搜索过滤器和 eq 索引。属性必须具有 ORDERING 匹配规则和 EQUALITY 匹配规则，才能支持范围搜索过滤器和索引范围搜索。

如果搜索操作对没有对应的匹配规则的属性使用了搜索过滤器，则目录服务器会拒绝带有 PROTOCOL_ERROR 或 UNWILLING_TO_PERFORM 的搜索操作。

匹配规则和自定义属性

例如，您要创建一个带有 IA5 String (7-bit ASCII)语法的自定义属性 MyFirstName，在 schema 定义中创建一个 EQUALITY 匹配规则 caseExactIA5Match。带有过滤器 (MyFirstName=Fred) 的搜索返回条目仅具有 MyFirstName 值等于 Fred ；但是，Fred、FRED 和 fred 是所有有效的 IA5 String 值。

如果您希望搜索返回属性值的所有变体，您必须在搜索过滤器中定义 MyFirstName 属性，以使用相等匹配规则 caseIgnoreIA5Match 或明确指定匹配的规则 (MyFirstName:caseIgnoreIA5Match:=Fred)。

其他资源

- 维护特定数据库的索引
- 管理目录模式.
- 常用的匹配规则

3.4.2. 常用的匹配规则

以下是常用匹配规则的列表：

匹配规则	描述	对象标识符(OID)	兼容语法
位 **AND** 匹配	执行位 **和** 匹配项.	1.2.840.113556.1.4.803	通常与 **整数和数字** 字符串一起使用。目录服务器自动将数字字符串转换为整数。
位 **OR** 匹配	执行位 **OR** 匹配。	1.2.840.113556.1.4.804	通常与 **整数和数字** 字符串一起使用。目录服务器自动将数字字符串转换为整数。
booleanMatch	评估要匹配的值是否为 **TRUE** 或 **FALSE**。	2.5.13.13	布尔值
caseExactIA5Match	对值进行区分大小写的比较。	1.3.6.1.4.1.1466.109.114.1	IA5 语法、URI
caseExactMatch	对值进行区分大小写的比较。	2.5.13.5	目录字符串, 可打印字符串, OID
caseExactOrderingMatch	允许区分大小写的搜索（小于和大于）。	2.5.13.6	目录字符串, 可打印字符串, OID
caseExactSubstringsMatch	执行区分大小写的子字符串和索引搜索。	2.5.13.7	目录字符串, 可打印字符串, OID

匹配规则	描述	对象标识符(OID)	兼容语法
caseIgnoreIA5Match	执行值不区分大小写的比较。	1.3.6.1.4.1.1466.109.114.2	IA5 语法、URI
caseIgnoreIA5SubstringsMatch	对子字符串和索引执行不区分大小写的搜索。	1.3.6.1.4.1.1466.109.114.3	IA5 语法、URI
caseIgnoreListMatch	执行值不区分大小写的比较。	2.5.13.11	邮政地址
caseIgnoreListSubstringsMatch	对子字符串和索引执行不区分大小写的搜索。	2.5.13.12	邮政地址
caseIgnoreMatch	执行值不区分大小写的比较。	2.5.13.2	目录字符串, 可打印字符串, OID
caseIgnoreOrderingMatch	允许不区分大小写的搜索（小于和大于）。	2.5.13.3	目录字符串, 可打印字符串, OID
caseIgnoreSubstringsMatch	对子字符串和索引执行不区分大小写的搜索。	2.5.13.4	目录字符串, 可打印字符串, OID
distinguishedNameMatch	比较可分辨名称值。	2.5.13.1	可区分名称(DN)
generalizedTimeMatch	比较采用常规时间格式的值。	2.5.13.27	常规时间
generalizedTimeOrderingMatch	允许对采用 Generalized Time 格式的值进行范围搜索（不超过和大于）。	2.5.13.28	常规时间
integerMatch	评估整数值。	2.5.13.14	整数
integerOrderingMatch	允许对整数值进行范围搜索（小于和大于）。	2.5.13.15	整数
keywordMatch	将给定的搜索值与属性值中的字符串进行比较。	2.5.13.33	目录字符串
numericStringMatch	比较更常规的数字值。	2.5.13.8	数字字符串
numericStringOrderingMatch	对更常规的数字值支持范围搜索（小于和大于）。	2.5.13.9	数字字符串
numericStringSubstringMatch	比较更常规的数字值。	2.5.13.10	数字字符串

匹配规则	描述	对象标识符(OID)	兼容语法
objectIdentifierMatch	比较对象标识符(OID)值。	2.5.13.0	对象标识符(OID)
octetStringMatch	评估 octet 字符串值。	2.5.13.17	octet String
octetStringOrderingMatch	在一系列 octet 字符串值上支持范围搜索（小于和大于）。	2.5.13.18	octet String
telephoneNumberMatch	评估电话号码值。	2.5.13.20	电话号码
telephoneNumberSubstringsMatch	对电话号码值执行子字符串和索引搜索。	2.5.13.21	电话号码
uniqueMemberMatch	将 Name & Optional UID 语法的断言值与语法的属性值进行比较	2.5.13.23	名称和可选 UID
wordMatch	将给定的搜索值与属性值中的字符串进行比较。此匹配规则区分大小写。	2.5.13.32	目录字符串

其他资源

- 语言排序匹配规则
- 语言子字符串匹配规则
- LDAP 搜索(ldapsearch)示例

3.4.3. 语言排序匹配规则

对于国际搜索，您可以使用以下语言排序匹配规则：

匹配规则	对象标识符(OID)
English (Case Exact Ordering Match)	2.16.840.1.113730.3.3.2.11.3
Albanian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.44.1

匹配规则	对象标识符(OID)
Arabic (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.1.1
Belorussian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.2.1
Bulgarian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.3.1
Catalan (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.4.1
中文 - 简体（区分大小写的排序匹配）	2.16.840.1.113730.3.3.2.49.1
中文 - 繁体（区分大小写的排序匹配）	2.16.840.1.113730.3.3.2.50.1
Croatian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.22.1
Czech (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.5.1
Danish （区分大小写的排序匹配大小）	2.16.840.1.113730.3.3.2.6.1
Dutch (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.33.1
Dutch - Belgian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.34.1
英语 - 美国（区分大小写的排序匹配）	2.16.840.1.113730.3.3.2.11.1
英语 - Canadian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.12.1
英语 - 爱尔兰（问题单不区分大小写的排序匹配）	2.16.840.1.113730.3.3.2.14.1
Estonian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.16.1
Finnish (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.17.1
法语（区分大小写的排序匹配大小写）	2.16.840.1.113730.3.3.2.18.1
法语 - 比利利（区分大小写的排序匹配）	2.16.840.1.113730.3.3.2.19.1
法语 - Canadian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.20.1
法语 - Swiss (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.21.1
德语（区分大小写的排序匹配大小）	2.16.840.1.113730.3.3.2.7.1
德语 - Austrian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.8.1

匹配规则	对象标识符(OID)
德语 - Swiss （区分大小写的排序匹配）	2.16.840.1.113730.3.3.2.9.1
Greek (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.10.1
Hebrew (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.27.1
Hungarian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.23.1
Icelandic (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.24.1
Italian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.25.1
Italian - Swiss (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.26.1
日语（区分大小写的排序匹配大小）	2.16.840.1.113730.3.3.2.28.1
韩语(Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.29.1
Latvian, Lettish (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.31.1
Lithuanian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.30.1
Macedonian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.32.1
Norwegian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.35.1
Norwegian - Bokmul (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.36.1
Norwegian - Nynorsk (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.37.1
polish (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.38.1
Romanian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.39.1
Russian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.40.1
Serbian - Cyrillic (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.45.1
Serbian - 拉丁语(Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.41.1
Slovak (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.42.1

匹配规则	对象标识符(OID)
Slovenian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.43.1
西班牙语（区分大小写的排序匹配大小写）	2.16.840.1.113730.3.3.2.15.1
Swedish (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.46.1
Turkish (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.47.1
Ukrainian (Case Insensitive Ordering Match)	2.16.840.1.113730.3.3.2.48.1

其他资源

- 搜索国际化目录.
- 国际搜索示例

3.4.4. 语言子字符串匹配规则

对于国际搜索，您可以使用以下语言子字符串匹配规则：

匹配规则	对象标识符(OID)
English (Case Exact Substring Match)	2.16.840.1.113730.3.3.2.11.3.6
Albanian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.44.1.6
Arabic (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.1.1.6
Belorussian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.2.1.6
Bulgarian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.3.1.6
Catalan (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.4.1.6
中文 - 简体（区分大小写的子字符串匹配）	2.16.840.1.113730.3.3.2.49.1.6
中文 - 繁体（区分大小写的子字符串匹配）	2.16.840.1.113730.3.3.2.50.1.6
Croatian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.22.1.6

匹配规则	对象标识符(OID)
Czech (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.5.1.6
Danish (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.6.1.6
Dutch (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.33.1.6
Dutch - Belgian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.34.1.6
英语 - 美国（区分大小写的子字符串匹配）	2.16.840.1.113730.3.3.2.11.1.6
英语 - Canadian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.12.1.6
英语 - 爱尔兰（问题单不区分大小写的子字符串匹配）	2.16.840.1.113730.3.3.2.14.1.6
Estonian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.16.1.6
Finnish (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.17.1.6
法语（区分大小写的子字符串匹配大小写）	2.16.840.1.113730.3.3.2.18.1.6
法语 - 比利福尼亚（区分大小写的子字符串匹配）	2.16.840.1.113730.3.3.2.19.1.6
法语 - Canadian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.20.1.6
法语 - Swiss (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.21.1.6
德语（区分大小写的子字符串匹配大小写）	2.16.840.1.113730.3.3.2.7.1.6
德语 - Austrian （区分大小写的子字符串匹配）	2.16.840.1.113730.3.3.2.8.1.6
德语 - Swiss （区分大小写的子字符串匹配）	2.16.840.1.113730.3.3.2.9.1.6
Greek (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.10.1.6
Hebrew (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.27.1.6
Hungarian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.23.1.6
Icelandic (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.24.1.6
Italian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.25.1.6
Italian - Swiss (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.26.1.6

匹配规则	对象标识符(OID)
日语（区分大小写的子字符串匹配）	2.16.840.1.113730.3.3.2.28.1.6
韩语(Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.29.1.6
Latvian, Lettish (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.31.1.6
Lithuanian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.30.1.6
Macedonian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.32.1.6
Norwegian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.35.1.6
Norwegian - Bokmul (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.36.1.6
Norwegian - Nynorsk (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.37.1.6
polish (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.38.1.6
Romanian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.39.1.6
Russian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.40.1.6
Serbian - Cyrillic (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.45.1.6
Serbian - 拉丁语(Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.41.1.6
Slovak (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.42.1.6
Slovenian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.43.1.6
西班牙语（区分大小写的子字符串匹配大小写）	2.16.840.1.113730.3.3.2.15.1.6
Swedish (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.46.1.6
Turkish (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.47.1.6
Ukrainian (Case Insensitive Substring Match)	2.16.840.1.113730.3.3.2.48.1.6

其他资源

- 搜索国际化目录

- 国际搜索示例

3.4.5. 使用 inchainMatch 匹配规则在嵌套组中查找 LDAP 条目的成员资格

inchainMatch 匹配规则是搜索过滤器的可扩展匹配，用于在嵌套组中找到 LDAP 条目成员资格。目录服务器支持对象标识符(OID) 1.2.840.113556.1.4.1941 和 chainMatch 中 的人类可读名称。

使用匹配规则仅限于带有可辨识名称(DN)语法的属性。您可以使用 chainMatch 匹配规则来执行以下搜索：

- 搜索过滤器 (member:1.2.840.113556.1.4.1941:=uid=jdoe,ou=people,dc=example,dc=com) 找到用户 jdoe 是成员的所有直接或间接组。
- 搜索过滤器 (manager:1.2.840.113556.1.4.1941:=uid=jsmith,ou=people,dc=example,dc=com) 找到其管理器是 jsmith 的所有直接或间接用户。
- 搜索过滤器 (parentOrganization:1.2.840.113556.1.4.1941:=ou=ExampleCom,ou=europe,dc=example,dc=com) 找到 ExampleCom 所属的所有直接或间接机构。
- 搜索过滤器 (memberof:1.2.840.113556.1.4.1941:=cn= marketing ,ou=groups,dc=example,dc=com) 找到 marketing 组的所有直接或间接成员。

请注意，出于性能的原因，您必须索引 成员、manager、parentOrganization、chainMatch 中的 memberof 属性。

目录服务器通过 In Chain 插件默认启用 inchainMatch 匹配规则。但是，在chainMatch 中的 compute 昂贵，只有 Directory Manager 默认具有在 chainMatch 中使用 的权限。要为其他用户授予权限，请修改 oid=1.2.840.113556.1.4.1941,cn=features,cn=config 条目中的访问控制指令(ACI)。如需了解更多详细信息，请参阅为 用户条目启用chainMatch 匹配规则。

3.4.5.1. 为用户条目启用 inchainMatch 匹配规则

默认情况下，只有 Directory Manager 具有使用chainMatch 匹配规则的权限，因为 inchainMatch 昂贵。要为其他用户授予权限，请修改 oid=1.2.840.113556.1.4.1941,cn=features,cn=config 条目中的

访问控制指令(ACI)。以下流程为 admin 用户授予 读取和 搜索 权限。

先决条件

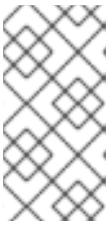
- uid=admin,ou=people,dc=example,dc=com 用户条目存在。
- uid=jdoe,ou=people,dc=example,dc=com 用户条目存在，并属于 cn=Marketing_Germany,ou=groups,dc=example,dc=com 组。
- cn=Marketing_Germany,ou=groups,dc=example,dc=com 组是 cn=Marketing_EU,ou=groups,dc=example,dc=com 组的嵌套组。

流程

- 通过替换 oid=1.2.840.113556.1.4.1941,cn=config 条目中的默认 ACI，对 uid=admin,ou=people,dc=example,dc= com 的 读取和 搜索 权限：

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

dn: oid=1.2.840.113556.1.4.1941,cn=features,cn=config
changetype: modify
replace: aci
aci: (targetattr != "aci")(version 3.0; acl "InChain Matching Rule"; allow( read, search )
userdn = "ldap:///uid=admin,ou=people,dc=example,dc=com";)
```



注意

要获取多个用户的权限，请将这些用户添加到组中，并在 ACI 的绑定规则中将 groupdn 设为关键字。如需了解更多详细信息，请参阅 定义基于组的访问。

验证

- 搜索用户 uid=jdoe,ou=people,dc=example,dc=com 属于 admin 用户的组：

```
$ ldapsearch -D "uid=admin,ou=people,dc=example,dc=com"
ldap://server.example.com -W -xLL -b "dc=example,dc=com" "
(member:1.2.840.113556.1.4.1941:=uid=jdoe,ou=people,dc=example,dc=com)" dn

  dn: cn=Marketing_EU,ou=groups,dc=example,dc=com
  dn: cn=Marketing_Germany,ou=groups,dc=example,dc=com
```

3.4.5.2. 禁用 inchainMatch 匹配规则

要实现 inchainMatch 匹配规则，目录服务器使用默认启用的 In Chain 插件。如果要在 chainMatch 中禁用，请使用 dsconf 工具禁用 In Chain 插件。

流程

1. 检查 In Chain 插件是否已启用：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com plugin show 'In Chain'
dn: cn=In Chain,cn=plugins,cn=config
cn: In Chain
nsslapd-pluginDescription: inchain matching rule plugin
nsslapd-pluginEnabled: on
...
```

2. 禁用 In Chain 插件：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com plugin set --enabled
off 'In Chain'

Successfully changed the cn=In Chain,cn=plugins,cn=config
```

该命令为所有用户禁用 inchainMatch 匹配规则。

验证

- 检查 Directory 服务器是否禁用了 In Chain 插件：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com plugin show 'In Chain'
dn: cn=In Chain,cn=plugins,cn=config
cn: In Chain
nsslapd-pluginDescription: inchain matching rule plugin
nsslapd-pluginEnabled: off
...
```

第 4 章 LDAP 搜索(LDAPSEARCH)示例

以下示例提供了在目录中搜索的最常见"ldapsearch"es。

先决条件

- 您可以对目录中的所有条目执行搜索。
- 您已将该目录配置为支持匿名搜索和读取操作。因此，您不需要在命令中使用 -W 和 -D 选项来提供任何绑定信息。有关匿名访问的更多信息，请参阅 授予匿名访问。
- 服务器使用默认端口号 389。您不需要在搜索请求中指定它。
- 服务器具有 server.example.com 主机名。
- 您为端口 636 上的服务器（默认的 LDAPS 端口号）启用了 TLS。
- 目录服务器将所有数据存储在 dc=example,dc=com 后缀下。

返回所有条目

以下 LDAP 搜索返回目录中的所有条目：

```
# ldapsearch -H ldap://server.example.com -b "dc=example,dc=com" -s sub -x "
(objectclass=*)"
```

使用 (objectclass categories)搜索过滤器返回 目录中的每个条目。每个条目都必须有一个对象类，并且始终索引 objectclass 属性。

在命令行中指定搜索过滤器

您可以通过将过滤器放在引号("*filter*")中直接对命令指定搜索过滤器。如果您在命令中提供过滤器，请不要指定 -f 选项。例如，要指定 "cn=babs jensen"，请输入：

```
# ldapsearch -H ldap://server.example.com -b "dc=example,dc=com" -s sub -x "cn=babs
jensen"
```

-

搜索 Root DSE 条目

root DSE 是一个特殊的条目，其中包含有关目录服务器实例的信息，包括本地目录服务器支持的所有后缀。通过提供搜索基础 ""、搜索范围 基础，以及过滤器 "objectclassPROFILE" 来搜索此条目，例如：

```
# ldapsearch -H ldap://server.example.com -x -b "" -s base "objectclass=*"
```

搜索 schema 条目

cn=schema 条目是一个特殊的条目，其中包含与目录架构相关的信息，如对象类和属性类型。

要列出 cn=schema 条目的内容，请输入以下命令之一：

```
# ldapsearch -x -o ldif-wrap=no -b "cn=schema" \ '(objectClass=subSchema)' -s sub
objectClasses attributeTypes matchingRules \ matchingRuleUse dITStructureRules
nameForms ITContentRules ldapSyntaxes
```

或者

```
# ldapsearch -x -o ldif-wrap=no -b "cn=schema" \ '(objectClass=subSchema)' -s sub "+"
```

使用 LDAP_BASEDN 变量

要简化搜索，您可以使用 LDAP_BASEDN 环境变量设置搜索基础。您可以设置 LDAP_BASEDN，而不是使用带有 -b 选项的 ldapsearch 命令。有关设置环境变量的更多信息，请参阅操作系统文档。

将 LDAP_BASEDN 设置为目录后缀值。因为目录后缀等于目录中 root 条目，所以所有搜索都从目录根条目开始。

例如，要将 LDAP_BASEDN 变量设置为 dc=example,dc=com，并在目录中搜索 cn=babs jensen，请输入：

```
# export LDAP_BASEDN="dc=example,dc=com"

# ldapsearch -H ldap://server.example.com -x "cn=babs jensen"
```

命令使用默认范围 子，因为未提供 -s 选项指定范围。

显示属性的子集

ldapsearch 命令以 LDIF 格式返回所有搜索结果。默认情况下，ldapsearch 返回条目可区分名称(DN)以及允许用户读取的所有属性。您可以设置目录访问控制，允许用户只读取任何给定目录条目的属性子集。

默认情况下，目录服务器不会返回操作属性。要在搜索操作后返回操作属性，请在 search 命令中明确指定这些属性，或使用 + 参数返回所有操作属性。如需更多信息，请参阅搜索操作属性。

您可以通过在搜索过滤器后在命令行中指定所需属性，将返回的属性限制为几个特定属性。

例如，要显示目录中每个条目的 cn 和 sn 属性，请输入：

```
# ldapsearch -H ldap://server.example.com -b "dc=example,dc=com" -s sub -x "
(objectclass=*)" sn cn
```

搜索操作属性

操作属性是目录服务器设置自身的特殊属性。目录服务器使用操作属性来执行维护任务，如处理访问控制指令。这些属性显示有关条目的具体信息，如最初创建此条目的时间以及创建它的用户名称。

您可以在目录中的每一条目上使用操作属性，即使属性是为条目的对象类定义的。

常规 ldapsearch 命令不会返回操作属性。根据 RFC3673，使用 + 返回搜索请求中的所有操作属性：

```
# ldapsearch -H ldap://server.example.com -b "dc=example,dc=com" -s sub -x "
(objectclass=*)" '+'
```

要只返回某些定义的操作属性，请在 ldapsearch 请求中明确指定它们：

```
# ldapsearch -H ldap://server.example.com -b "dc=example,dc=com" -s sub -x "
(objectclass=*)" creatorsName createTimestamp modifiersName modifyTimestamp
```

有关操作属性的完整列表，请参阅操作属性和对象类。

注意

要返回所有常规条目属性以及指定的操作属性，除了您列出的操作属性外，还使用特殊的搜索属性 "*"。

```
# ldapsearch -H ldap://server.example.com -b "dc=example,dc=com" -s sub -x "(objectclass=*)" "*" aci
```

请注意，您必须将星号 packagemanifests 包含在引号中，以防止 shell 对其进行解释。

使用文件指定搜索过滤器

您可以在文件中指定搜索过滤器，而不是在命令行中输入它们。

在文件中的单独行中指定每个搜索过滤器。ldapsearch 命令按文件中显示的顺序运行每个搜索。

例如，该文件包含以下过滤器：

```
sn=example
givenname=user
```

ldapsearch 命令首先查找将 surname 设置为 example 的所有条目，然后查找将 givenname 设置为用户 的所有条目。如果搜索请求找到与这两个搜索条件匹配的条目，则条目会返回两次。

在以下搜索中，过滤器在名为 searchdb 的文件中指定：

```
# ldapsearch -H ldap://server.example.com -x -f searchdb
```

您可以通过在搜索行末尾指定属性名称来限制返回的属性集合。例如，以下 ldapsearch 命令执行这两个搜索，但只返回每个条目的 DN 和 givenname 和 sn 属性：

```
# ldapsearch -H ldap://server.example.com -x -f searchdb sn givenname
```

指定在搜索过滤器中包含逗号的 DN

当搜索过滤器中的 DN 包含作为值一部分的逗号时，search 命令必须使用反斜杠(\)转义逗号。例如，要查找 example .com Bolivia (S.A. 子树)中的每个人，请输入：

```
# ldapsearch -H ldap://server.example.com -x -s base -b "l=Bolivia\, S.A.,dc=example,dc=com"
"objectclass=*"
```

在过滤器中使用 nsRole 虚拟属性

在以下示例中，ldap search 命令搜索包含 nsrole 属性设置为 managed_role 值的所有用户条目的 DN：

```
# ldapsearch -H ldap://server.example.com -x -b "dc=example,dc=com" "
(nsrole=cn=managed_role,dc=example,dc=com)" dn
```

使用客户端证书绑定到目录服务器

有关基于证书的身份验证的更多信息，请参阅配置基于证书的身份验证。

使用语言匹配规则搜索

要在搜索过滤器中显式提交匹配规则，请在属性后面插入匹配的规则：

```
attr:matchingRule:=value
```

匹配规则通常用于搜索国际化目录。以下命令在 Swedish (2.16.840.1.113730.3.3.2.46.1)匹配规则中的 N4709 后搜索部门号。

```
departmentNumber:2.16.840.1.113730.3.3.2.46.1:=>= N4709
```

有关执行国际化搜索的更多信息，请参阅 搜索国际化的目录。

查找用户所属的组

要查找用户 uid=jdoe,ou=people,dc=example,dc=com 的所有直接或间接组，请输入：

```
# ldapsearch -D "cn=Directory Manager" -W -H ldap://server.example.com -xLL -b
"dc=example,dc=com" "
(member:1.2.840.113556.1.4.1941:=uid=jdoe,ou=people,dc=example,dc=com)" dn
```

带有 chainMatch 匹配规则 的搜索不支持 匿名访问。有关使用 inchainMatch 匹配规则的详情，请参阅 在chainMatch 匹配规则中使用 来查找 LDAP 条目的 ancestry。

查找组成员

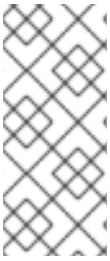
要查找 marketing 组的所有直接或间接成员，请输入：

```
# ldapsearch -D "cn=Directory Manager" -W -H ldap://server.example.com -xLL -b
"dc=example,dc=com" "
(memberof:1.2.840.113556.1.4.1941:=cn=marketing,ou=groups,dc=example,dc=com)" dn
```

带有 chainMatch 匹配规则 的搜索不支持 匿名访问。有关使用 inchainMatch 匹配规则的详情，请参阅 在chainMatch 匹配规则中使用 来查找 LDAP 条目的 ancestry。

使用位字段值搜索属性

位的搜索使用位 AND 或 bitwise OR 匹配规则对带有位字段的属性执行位搜索操作。



注意

LDAP 中不常见带有位字段的值的属性。默认目录服务器模式不使用位字段作为属性语法。但是，几个 LDAP 语法支持整数风格的值。您可以定义自定义属性以使用位字段值。应用程序可以使用自定义属性对位字段值执行位操作。

位的 AND 匹配规则(1.2.840.113556.1.4.803)检查在 bit 字段属性值中是否设置了断言值中的位。它与等同的搜索类似。以下示例将 userAccountControl 值设置为代表 2 的位：

```
"(UserAccountControl:1.2.840.113556.1.4.803:=2)"
```

以下示例显示 userAccountControl 值必须具有值 6 中设置的所有位（位 2 和 4）：

```
"(UserAccountControl:1.2.840.113556.1.4.803:=6)”
```

位 或 匹配规则(1.2.840.113556.1.4.804)检查断言字符串中的任何位是否在属性值中表示。它与子字符串搜索类似。在本例中，UserAccountControl 值必须具有 6 位字段设置的任何位，表示属性值可以是 2、4 或 6 ：

```
"(UserAccountControl:1.2.840.113556.1.4.804:=6)"
```

您可以将位搜索与 Windows-Linux 集成一起使用，例如使用 Samba 文件服务器。

其他资源

- ldapsearch 命令格式
- 常用的 ldapsearch 选项

第 5 章 通过资源限值提高搜索性能

搜索数据库中的每个条目可能会对更大目录的服务器性能造成负面影响。在大型数据库中，有效的索引可能不够地减少搜索范围以提高性能。

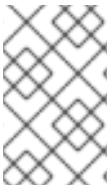
您可以设置用户和客户端帐户的限值，以减少条目总数或单个搜索中花费的时间总量。这使得搜索速度更快，并提高了整体服务器性能。

5.1. 大型目录的搜索操作限制

您可以使用客户端应用绑定到目录的特殊操作属性值来控制搜索操作的服务器限制。您可以设置以下搜索操作限制：

- Look through limit 指定您可以检查搜索操作的条目数量。
- Size 限制指定服务器返回到客户端应用程序的最大条目数，以响应搜索操作。
- Time limit 指定服务器可以花费在处理搜索操作的最长时间。
- Idle timeout 限制指定连接在连接被丢弃前可以闲置的时间。
- Range timeout 限制指定单独的 look-through 限制，专门用于使用范围进行搜索。

在全局服务器配置中，为客户端应用程序设置的资源限值优先于设置默认资源限制。



注意

目录管理器默认接收无限的资源，但范围搜索除外。

5.2. 使用索引扫描限制提高搜索性能

对于大型索引，可以将任何与索引匹配的搜索视为未索引的搜索是效率。搜索操作必须查看整个目录，以便处理结果，而不是搜索在目录本身中几乎还包含目录大小的索引。

其他资源

- 设置索引扫描限制

5.3. 细粒度 ID 列表大小

在大型数据库中，一些查询可能会消耗大量 CPU 和 RAM 资源。要提高性能，您可以使用 nsslapd-idlistscanlimit 属性设置应用到数据库中的所有索引的默认 ID 扫描限制。但是，对于为特定索引定义限制或者没有定义 ID 的列表，这非常有用。您可以使用 nsIndexIDListScanLimit 属性为不同类型的搜索过滤器设置 ID 列表扫描限制。

其他资源

- 设置索引扫描限制，以便在加载长时间 ID 列表时提高性能

5.4. 使用命令行设置用户和全局资源限值

您可以使用命令行为特定类型的搜索设置 用户级 资源限值、全局 资源限值和限值，如 简单页面 和 范围搜索。您可以在单独的条目和全局配置属性上设置用户级属性。

您可以使用 ldapmodify 命令为每个条目设置以下上述操作属性：

- **look-through**

  您可以使用 look-through limit 属性指定检查搜索操作的条目数量。将属性的值设为 -1 表示没有限制。

  1. **user-level 属性： nsLookThroughLimit**
  2. **全局配置：**
     a. **attribute: nsslapd-lookthroughlimit**

b. entry: cn=config,cn=ldbm database,cn=plugins,cn=config

```
# dsconf instance backend config set --lookthroughlimit value
```

- paged look-through

您可以使用 paged look-through limit 属性指定检查简单页面的搜索操作的条目数量。将属性的值设为 -1 表示没有限制。

1. user-level 属性： nsPagedLookThroughLimit
2. 全局配置：
   a. attribute: nsslapd-pagedlookthroughlimit
   b. entry: cn=config,cn=ldbm database,cn=plugins,cn=config

```
# dsconf instance backend config set --pagedlookthroughlimit value
```

- size

您可以使用 size limit 属性指定服务器返回到客户端应用程序的最大条目数。将属性的值设为 -1 表示没有限制。

1. user-level 属性： nsSizeLimit
2. 全局配置：
   a. attribute: nsslapd-sizelimit
   b. entry: cn=config

```
# dsconf instance config replace nsslapd-sizelimit value
```

您可以将 nsSizeLimit 属性添加到用户条目中，例如为它指定搜索返回大小限制 500 条目：

```
# ldapmodify -D "cn=Directory Manager" -W -p 389 -h server.example.com -x
...
dn: uid=user_name,ou=People,dc=example,dc=com
changetype: modify
add: nsSizeLimit
nsSizeLimit: 500
...
```

- 页面大小

  您可以使用 paged size limit 属性指定服务器返回到客户端应用程序的最大条目数，以进行简单的页面搜索操作。将属性的值设为 -1 表示没有限制。

  1. user-level 属性： nsPagedSizeLimit
  2. 全局配置：
     a. attribute: nsslapd-pagedsizelimit
     b. entry: cn=config

```
# dsconf instance config replace nsslapd-pagedsizelimit value
```

- time

  您可以使用 时间限制 属性指定服务器处理搜索操作的最大时间。将属性的值设为 -1 表示没有时间限制。

  1. user-level 属性： nsTimeLimit

2. 全局配置：

   a. attribute: nsslapd-timelimit

   b. entry: cn=config

```
# dsconf instance config replace nsslapd-timelimit value
```

- 闲置超时

  您可以使用 idle timeout 属性指定连接到服务器在连接被丢弃前可以闲置的时间（以秒为单位）。将属性的值设为 -1 表示没有限制。

1. user-level 属性： nsidletimeout

2. 全局配置：

   a. attribute: nsslapd-idletimeout

   b. entry: cn=config

```
# dsconf instance config replace nsslapd-idletimeout value
```

- ID 列表扫描

  您可以为搜索结果指定从索引文件加载的最大条目 ID 数。如果 ID 列表大小大于最大 ID 数，则搜索将不会使用索引列表，而是将搜索视为未索引的搜索，并查找整个数据库。

1. user-level 属性： nsIDListScanLimit

2. 全局配置：

a.
attribute: nsslapd-idlistscanlimit

b.
entry: cn=config,cn=ldbm database,cn=plugins,cn=config

```
# dsconf instance backend config set --idlistscanlimit value
```

- **页面的 ID 列表扫描**

您可以使用页面的 ID 列表扫描限制指定从索引文件中加载的最大条目 ID 数，以了解搜索结果，特别是页 化搜索操作。

1.
user-level 属性： nsPagedIDListScanLimit

2.
全局配置：

a.
attribute: nsslapd-pagedidlistscanlimit

b.
entry: cn=config,cn=ldbm database,cn=plugins,cn=config

```
# dsconf instance backend config set --pagedidlistscanlimit value
```

- **范围查找**

您可以使用范围 look-through 限制来指定检查范围搜索操作 的条目数。将属性的值设为 -1 表示没有限制。

注意

范围搜索是通过使用 greater-than、equal-to-or-greater-than、less-than 或 equal-to-less-than 运算符进行搜索。

1.
user-level 属性： not available

2. 全局配置：

a. attribute: nsslapd-rangelookthroughlimit

b. entry: cn=config,cn=ldbm database,cn=plugins,cn=config

```
# dsconf instance backend config set ----rangelookthroughlimit value
```

注意

您可以设置访问控制列表以防止用户更改设置。

其他资源

- 管理访问控制

5.5. 对匿名绑定设置资源限值

您可以通过创建一个具有资源限值的模板用户条目来为匿名绑定配置资源限值，然后将此模板应用到匿名绑定，因为资源限值是在用户条目上设置的，匿名绑定没有与之关联的用户条目。

先决条件

- 创建了一个模板条目。

流程

1. 设置您要应用到匿名绑定的资源限值：

```
# ldapadd -D "cn=Directory Manager" -W -p 389 -h server.example.com -x
...
dn: cn=anonymous_template,ou=people,dc=example,dc=com
objectclass: nsContainer
objectclass: top
cn: anonymous_template
nsSizeLimit: 250
```

```
nsLookThroughLimit: 1000
nsTimeLimit: 60
...
```

注意

出于性能的原因，模板必须位于正常后端，而不是在不使用条目缓存的 cn=config 后缀中。

2. 将 nsslapd-anonlimitsdn 参数添加到服务器配置，指向复制拓扑中所有供应商上模板条目的 DN ：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com config replace
nsslapd-anonlimitsdn="cn=anonymous_template,ou=people,dc=example,dc=com"
```

5.6. 改进了范围搜索的性能

范围搜索（所有 ID 搜索）使用运算符设置括号来搜索并返回目录中条目的整个子集。范围搜索可以评估目录中的每个条目，以检查条目是否在提供的范围内。

例如，要在 1 月 1 日午夜后搜索修改的每个条目，请运行以下命令：

```
# (modifyTimestamp>=20210101010101Z)
```

要防止范围搜索进入所有 ID 搜索，您可以使用 look-through 限制。通过使用这个限制，您可以提高整体性能并加快范围的搜索结果。但是，一些客户端或管理用户（如 Directory Manager）不能设置 look-through 限制。在这种情况下，范围搜索可能需要几分钟才能完成，甚至可以无限期地继续。

但是，您可以设置单独的范围 查找限制。通过设置此限制，客户端和管理用户可以具有较高的 查找 限制，仍然可以对可能对性能范围搜索设置合理的限制。

您可以使用 nsslapd-rangelookthroughlimit 属性配置这样的设置。默认值为 5000。

要将单独的范围 look-through 限制设置为 7500，请运行以下命令：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com backend config set --
rangelookthroughlimit 7500
```