Connecting to an LDAP Directory

中文标题【连接一个 LDAP 目录】

你可以连接你的 Confluence 到一个 LDAP 目录服务器上，你可以通过连接的 LDAP 目录服务器为你的 Confluence 进行授权，用户和用户组管理。

本页中的内容

相关页面：

- Connecting to an LDAP Directory

概述

一个 LDAP 目录是一个用户和用户组信息的数据库。LDAP（Lightweight Directory Access Protocol - 轻量目录访问协议）是一个 Web 应用程序的网络协议，可以从 LDAP 服务上访问和查找用户和用户组信息。

我们能够支持主流的 LDAP 目录服务器（为了便于理解，我们不将产品名翻译成中文了）：

- Microsoft Active Directory
- Apache Directory Server (ApacheDS)
- Apple Open Directory
- Fedora Directory Server
- Novell eDirectory
- OpenDS
- OpenLDAP
- OpenLDAP Using Posix Schema
- Posix Schema for LDAP
- Sun Directory Server Enterprise Edition (DSEE)
- A generic LDAP directory server

什么时候使用这些选项：当你的用户和用户组信息存储在公司的目录服务器上的时候，使用 LDAP 连接上这些目录服务器会非常有用。当配置目录的时候，你可以选择这些用户用户组是在本地否具有只读权限，或者允许对 LDAP 服务器进行读取和写入。如果你选择读取和写入权限的话，任何用户在本地进行修改的的信息，将会自动同步回目录服务器上。

在 Confluence 中连接一个 LDAP 目录

希望将 Confluence 连接到一个 LDAP 目录：

1. 在屏幕的右上角单击**控制台按钮**，然后选择 **基本配置（General Configuration）** 链接。
2. 在左侧的面板中单击 用户目录（**User Directories**）。
3. **添加（Add）**一个目录，并且选择下面的一些类型：
   - **Microsoft Active Directory** – 这个选项提供了一个快速选择 AD 的方法，因为这个是最流行的 LDAP 目录类型。
   - **LDAP** – 你可以在下面屏幕中选择一个特定的 LDAP 目录。
4. 按照下面描述的参数配置，输入需要配置目录的参数。
5. 保存目录设置。
6. 在用户目录界面中通过单击每一个目录边上蓝色的上下移动箭头定义 **目录顺序（ directory order）** 。 这里是有关目录顺序如何影响系统的摘要信息：
   - 当应用程序允许对 LDAP 进行信息修改的时候，用户在系统中修改的信息只会影响到第一个目录。
   - 目录的顺序是对用户和用户组查找的时候的搜索顺序（通过在所有目录中对 Confluence 默认的用户组聚集，所以目录的顺序将不会影响成员）。

   有关更多的详细信息，请参考页面Managing Multiple Directories。

服务器配置

设置	描述
名字（Name）	输入一个有意义的 LDAP 服务器名字，会让你更好的识别你的目录服务器。例如： • `Example Company Staff Directory` • `Example Company Corporate LDAP`

目录类型（Directory Type）	选择你将要连接的 LDAP 目录服务器类型。 如果你正在添加一个新的 LDAP 连接，你在这里进行的选择将会影响你下一步将要进行配置的参数。例如： • `Microsoft Active Directory` • `OpenDS` • `And More`
主机名（Hostname）	你目录服务器的主机名。例如： • `ad.example.com` • `ldap.example.com` • `opends.example.com`
端口（Port）	你目录服务器正在监听的端口。例如： • `389` • `10389` • `636` （例如针对 SSL）
使用 SSL（Use SSL）	如果你的目录服务器使用了 SSL（Secure Sockets Layer），你需要选择这个选项。 备注：如果你希望使用这个选项，你需要配置 SSL 证书。
用户名（Username）	这个用户名和使用系统的用户名是不一样的，这个用户名被用来连接你的目录服务器。例如： • `cn=administrator,cn=users,dc=ad,dc=example,dc=com` • `cn=user,dc=domain,dc=name` • `user@domain.name` 在默认情况下，所有用户名都可以读取 uSNChanged 属性。但是只有管理员或者有相关权限的用户才能访问删除对象容器（Deleted Objects container）。 用户可以连接 LDAP 服务器的特殊权限为 "Bind" 和 "Read"（用户信息，用户组信息，用户组成员，更新序列号，删除对象），这个权限只能成为活动目录的内部构建管理员权限才会具有。 注意：当你设置的这个用户没有这些权限的时候，用户目录的增量同步将会默认失败。这些可以报告给下面的链接 CWD-3093。
密码（Password）	上面指定用户的密码。 **注意：**连接一个 LDAP 目录服务器需要使用的用户名和密码都在这里进行配置。在默认的情况下，这个密码不能单一进行加密，这个密码必须能够在 Web 应用服务器上正常解密，所以你输入的这个密码将不会在数据库存储中进行加密处理，而是存储为文本字符。 为了保证系统的安全性，你需要其他的进程针对数据库或配置文件不具有操作系统级别的读取权限。

结构（Schema）设置

设置	描述
基本 DN（Base DN）	根专有名称（DN）将会在你在目录服务器上运行查询的时候使用到。例如： • `o=example,c=com` • `cn=users,dc=ad,dc=example,dc=com` • 针对 Microsoft Active Directory，使用下面的格式来指定基本 DN： `dc=domain1,dc=local`。你需要针对你特定的配置来修改 `domain1` 和 `local`。Microsoft Server 提供了一个名为 `ldp.exe` 工具，你可以用这个工具在你的 LDAP 服务器上进行查找和配置。
其他用户 DN（Additional User DN）	这个值被用在进行用户查找和载入的时候来针对 base DN 配置一些扩展信息。如果你没有为这个字段提供任何值，那么子树的查找将会从 base DN 上开始查找。例如： • `ou=Users`

其他用户组 DN（Additional Group DN）	这个值被用在进行用户组查找和载入的时候来针对 base DN 配置一些扩展信息。如果你没有为这个字段提供任何值，那么子树的查找将会从 base DN 上开始查找。例如： • `ou=Groups`

⚠ 如果你没有提供 ***Additional User DN*** 或者 ***Additional Group DN***，这个将会让子树的查找从 base DN 开始，在这种情况下可能会对目录树进行大范围遍历。这种情况将会对用户登录和登录后进行的操作产生性能上的问题。

权限设置

备注：当 '外部用户管理' 权限没有被选择的时候，你仅可以指派 LDAP 用户到本地用户组中。

设置	描述
只读（Read Only）	从你目录服务器上获得 LDAP 用户，用户组只能通过你的目录服务器进行修改。你不能通过应用程序的界面对你的用户，用户组，用户组成员进行修改后修改同步更新 LDAP 服务器。
本地用户组只读（Read Only, with Local Groups）	从你目录服务器上获得 LDAP 用户，用户组只能通过你的目录服务器进行修改。你不能通过应用程序的界面对你的用户，用户组，用户组成员进行修改后修改同步更新 LDAP 服务器。 但是，你可以在内部目录中添加用户组，并且将这些用户添加到你在内部目录中添加的用户组中。 针对 Confluence 用户请注意：从 LDAP 服务器上获得用户只能在用户第一次登陆的时候可以添加到Confluence 维护的内部目录中。 这个操作只能进行一次。因为已知针对 LDAP 只读，但是本地用户组可以操作的方式存在有下面的问题https://jira.atlassian.com/browse/CONFSERVER-28621。
读写（Read /Write）	从你目录服务器上获得 LDAP 用户。当你通过应用程序的界面对你的用户，用户组，或者用户组程序信息的时候。你的修改将会同步回 LDAP 服务器，并对 LDAP 服务器上的配置信息也同时进行修改。 请确定你配置的 LDAP 服务器连接用户在 LDAP 服务器上具有可写的权限。

自动添加用户到用户组

设置	描述
默认组成员（Default Group Memberships）	*选项在 Confluence 3.5 及后续版本和 JIRA 4.3.3 及后续版本中可用*。这字段将会在你选择 'Read Only, with Local Groups' 权限后出现。如果你希望你的用户能自动添加到用户组或多个用户组，在这里输入你希望添加的用户组的名字，如果有多个用户组，使用逗号分隔不同的用户组。 *在 Confluence 3.5 到 Confluence 3.5.1 版本*：每次用户登录的时候，用户属于的用户组成员将会被检查。如果用户不属于你指定的这些用户组的话，用户将会被自动添加到这些用户组中。如果用户组不存在，这些用户组将会在本地被添加。 *在 Confluence 3.5.2 及后续版本，和 JIRA 4.3.3 及后续版本*：当用户第一次进行登录的时候，用户所属的用户组状态将会被检查。如果用户不属于你指定的这些用户组的话，用户将会被自动添加到这些用户组中。 如果用户组不存在，这些用户组将会在本地被添加。在后续的登录校验中，用户将**不会**自动被添加到任何用户组。这个修改主要是为了允许用户可以从自动添加的用户组中移除。在 Confluence 3.5 到 3.5.1 的版本中，这些用户将会在下次登录的时候有被自动添加到用户组中了。 请注意用户组名不存在的情况，如果你错误的输入了用户组的名字，将会导致授权失败 —— 基于错误的用户组的名字，用户将不会被允许访问系统和使用系统的功能。 例如： • `confluence-users` • `confluence-users,jira-administrators,jira-core-users`

高级设置

设置	描述

启用嵌套组（Enable Nested Groups）	为嵌套组启用或禁用支持。 一些目录服务器能够允许你在一个组中定义另外一个组。在这种结构下的用户组称为用户组嵌套。嵌套组的配置能够让子用户组继承上级用户组的权限，使系统的权限配置变得简单。
管理本地用户状态（Manage User Status Locally）	如果设置为 True，你可以在 Crowd 中激活或者取消激活用户。这个配置基于你目录服务器的状态。
过滤过期的用户（Filter out expired users）	如果设置为 True，用户账号可以在 ActiveDirectory 中被标记为过期的将会被系统自动移除。针对缓存的用户目录，用户的删除将会在用户过期日期后的第一次同步中完成。 **注意：**这个功能在嵌入的Crowd 2.0.0 及后续版本中可用，但是在 2.0.0 m04 release 版本中不可用。
结果分页（Use Paged Results）	启用或者禁用使用 LDAP 为查询结果进行简单的分页。如果分页功能被启用，查询功能将会返回一部分查询的结果而不是所有的查询结果 输入希望分页的页面大小——这样将会返回在一次查询中最大允许返回的记录数量，默认这个值为 1000。
转移引荐（Follow Referrals）	选择启用这个功能的话，将会运行目录服务器将请求转移到其他的服务器上。这个选项使用的是节点转移（JNDI lookup`java.naming.referral`）配置设置。 这个配置通常需要 Active Directory 配置正确的 DNS 来避免在操作的时候出现 'javax.naming. PartialResultException: Unprocessed Continuation Reference(s)' 异常。
Naive DN 匹配（Naive DN Matching）	如果你的目录服务器总是返回一个 DN，你可以选择启用 Naive DN 匹配。选择使用 Naive DN 匹配将会让你的系统性能得到显著的提升。我们建议在你目录服务器可用的情况下启用这个配置。 这个设置决定了你的应用程序在 DN 相同的情况如何进行 DN 比较。 • 如果选择框选择的话，应用程序将会进行目录，大小写敏感的字符串比较。这个是默认推荐使用的 Active Directory 设置，因为 Active Directory 能够保证 DN 的格式。 • 如果这个选择框**没有**选择的话，应用程序将会对 DN 进行处理，然后检查处理的版本。
启用增量同步（Enable Incremental Synchronization）	如果你希望在对目录进行同步的时候，仅仅些对上次同步以后进行的变化进行同步的话，请启用增量同步。 ⚠️ 在使用这个选项希望对系统 DN 进行增量同步的时候请注意，系统配置的 LDAP 账户应该具有下面的可读权限： • 针对在目录中所有用户和用户组的 uSNChanged 属性，因为这个属性需要被同步。 • Active Directory 删除的对象容器中的对象和属性。 如果在上面的 2 个条没有一条是满足的，那么你可能在进行增量同步的时候出现错误。用户在目录中被添加或删除将不能在应用程序中同样的被添加和删除。 这个功能仅仅在用户目录类型被设置为 "Microsoft Active Directory" 时可用。
同步时间间隔（分钟）（Synchronization Interval (minutes)）	同步指的是处理应用内部存储的用户信息针对目录服务器上存储的用户进行进行比较和更新。应用服务器将会每隔 X 分钟向目录服务器发送同步的请求。 这个 X 指定的时间就在这里进行设置。默认的值是 60 分钟。
读取超时（秒）（Read Timeout (seconds)）	等待目录服务器返回结果的时间。如果等待目录服务器返回结果的时间超过了这里设置的值的话，这次同步请求将会被取消。设置为 0 的话，表示永远不超时，默认值为 120 秒。
查找超时（秒）（Search Timeout (seconds)）	在对目录服务器进行查找操作时，等待目录服务器返回数据的时间。设置为 0 的话，表示永远不超时，默认值为 60秒。
连接超时（秒）（Connection Timeout (seconds)）	这个设置将会影响下面 2 个操作。默认值为 0。 • 等待从连接池中获得连接的时间。设置为 0 的话表示没有限制，意思是一直等待。 • 打开一个新服务器连接的等待时间（单位是秒）。设置为 0 的话，表示的是 TCP 网络超时将会被使用，这里可能有会有几分钟的等待。

用户结构设置

设置	描述

用户对象类（User Object Class）	这个是在 LDAP 用户对象中对用户分类的名字。例如： • `user`
用户对象过滤器（User Object Filter）	当对用户对象进行搜索的时候使用的过滤器。例如： • `(&(objectCategory=Person)(sAMAccountName=*))` 有关更多的示例可以在知识库上找到。请查看 How to write LDAP search filters。
用户全名属性（User Name Attribute）	当载入用户名的时候使用的属性字段。例如： • `cn` • `sAMAccountName` NB: 在 Active Directory 中，'sAMAccountName' 是 'User Logon Name （Windows 2000 之前的版本）(pre-Windows 2000)' 字段。用户登录名字段参考为 'cn'。
用户全名 RDN 属性（User Name RDN Attribute）	RDN（相对区分的名字）在载入用户名的时候会被使用。针对每一个 LDAP 实例，DN 将会被区分为2 个部分：RDN 和 LDAP 目录服务器记录的位置。RDN 是你 DN 的一部分，这部分将不会关联到目录树结构。例如： • `cn`
用户名属性（User First Name Attribute）	这个特性将会在用户名载入的时候被使用。例如： • `givenName`
用户姓属性（User Last Name Attribute）	这个特性将会在用户姓载入的时候被使用。例如： • `sn`
用户显示名属性（User Display Name Attribute）	这个特性将会在用户全名载入的时候被使用。例如： • `displayName`
用户邮件属性（User Email Attribute）	这个特性将会在用户电子邮件地址载入的时候被使用。例如： • `mail`
用户密码属性（User Password Attribute）	这个特性将会在用户密码载入的时候被使用。例如： • `unicodePwd`
用户唯一 ID 属性（User UniqueID Attribute）	这个属性将会被用来唯一识别用户对象。这个设置通常被用来跟踪用户名的修改，这个选项是可选的。 如果这个属性没有被设置的话（或设置的值不正确），用户重命名将不会被系统访问到 — 当你进行用户重命名操作的话，系统将会解释为删除再添加一个新用户的操作。 这个字段通常被指定为 UUID 值。标准的 LDAP 服务器将会实践这个字段配置为 'entryUUID'，请参考 RFC 4530 的说明。这个字段存在的意思是针对不同的目录服务器，同一个用户名也能被识别。例如在 Microsoft Active Directory 中的 'objectGUID' 字段。

用户组结构设置

设置	描述
用户组对象类（Group Object Class）	这是在 LDAP 用户组对象中使用的类的名字。例如： • `groupOfUniqueNames` • `group`

用户组对象过滤器（Group Object Filter）	这个过滤器将会在查找用户组对象的时候被使用。例如： • (&(objectClass=group)(cn=*))
用户组名字属性（Group Name Attribute）	当载入用户组名字的时候，这个字段将会被使用。例如： • `cn`
用户组描述属性（Group Description Attribute）	当载入用户组描述的时候，这个字段将会被使用。例如： • `description`

成员结构设置

设置	描述
用户组成员属性（Group Members Attribute）	这个属性字段将在载入用户组成员的时候使用。例如： • `member`
用户成员属性（User Membership Attribute）	这个属性字段将在载入用户组的时候使用。例如： • `memberOf`
当找到用户组成员的时候，使用用户成员属性（Use the User Membership Attribute, when finding the user's group membership）	如果你的目录服务器为用户支持组成员属性的话，你可以选择这个（在默认的情况下，这个是 'memberOf' 属性）。 • 如果这个选择框选择的话，你的应用程序在 **retrieving the list of groups to which a given user belongs** 操作的时候会为用户使用用户组成员的属性。这个会带来更高效的检索效率。 • 如果这个选择框**没有**选择的话，你的应用程在查找的时候为用户组使用成员属性（默认是 'member'）。 • 如果 **启用嵌套用户组（Enable Nested Groups）** 选择框被选择的话，你的应用程序将会忽略 **使用用户成员属性（Use the User Membership Attribute）** 选项，而在组成员查找的时候使用成员属性。
当找到一个用户组成员的时候，使用用户成员属性（Use the User Membership Attribute, when finding the members of a group）	如果你的目录服务器在用户组中支持用户成员属性的话，你可以选择这个（在默认的情况下，这个是 'member' 属性）。 • 如果这个选择框被选择的话，你的应用程序在使用 **retrieving the members of a given group** 的时候，将会使用组成员属性。这个会带来更高效的检索效率。 • 如果这个选择框**没有**被选择的话，你的应用程序在查找的时候将会使用在用户组中使用成员属性（默认是 'member'）。

一些可能配置的图例

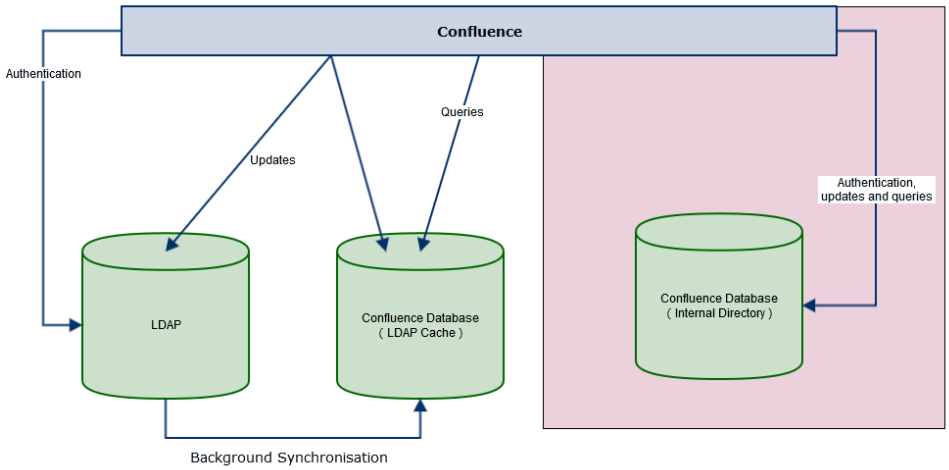

Diagram above: Confluence connecting to an LDAP directory.

上面的图：Confluence 连接到一个 LDAP 目录。

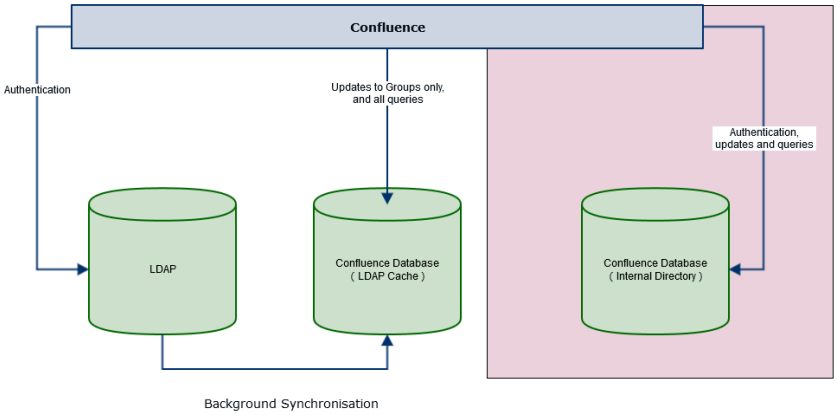

Diagram above: Confluence connecting to an LDAP directory with permissions set to read only and local groups.

上面的图：Confluence 连接到一 LDAP 目录，权限对本地用户组设置为只读。