
张京 RP 8.2k 发布于 日新亭
2018-05-02 发布

我花了一个五一终于搞懂了OpenLDAP

> **轻型目录访问协议**（英文： Lightweight Directory Access Protocol ，缩写： LDAP ）是一个开放的，中立的，工业标准的应用协议，通过IP协议提供访问控制和维护分布式信息的目录信息。
>
> OpenLDAP 是轻型目录访问协议（ Lightweight Directory Access Protocol ， LDAP ）的自由和开源的实现，在其 OpenLDAP 许可证下发行，并已经被包含在众多流行的 Linux 发行版中。
>
> 可以这样讲：市面上只要你能够想像得到的所有工具软件，全部都支持 LDAP 协议。比如说你公司要安装一个项目管理工具，那么这个工具几乎必然支持 LDAP 协议，你公司要安装一个 bug 管理工具，这工具必然也支持 LDAP 协议，你公司要安装一套软件版本管理工具，这工具也必然支持 LDAP 协议。 LDAP 协议的好处就是你公司的所有员工在所有这些工具里共享同一套用户名和密码，来人的时候新增一个用户就能自动访问所有系统，走人的时候一键删除就取消了他对所有系统的访问权限，这就是 LDAP 。

有些领域并不像前端世界那么潮那么性感，但是缺了这个环节又总觉得很别扭。如果深入到运维的世界，你会发现大部分工具还活在上个世纪，产品设计完全反人类，比如 cn，dc，dn，ou 这样的命名方式，如果不钻研个一天两天，鬼知道它在说什么，比如说 dns ， dns 是什么鬼？域名吗？不是，它只是某个懒惰的工程师起了 dn 这么一个缩写，再加一个复数，就成了 dns ，和域名服务器没有任何关系； cn 是什么？中国的缩写？你想多了，这和中国没有任何关系。经过一系列这样疯狂的洗脑之后，你才能逐渐明白 LDAP 到底想干什么。抛弃你所有的认知，把自己当成一个什么都不懂的幼儿园孩子，然后我们从头学起 LDAP 。

如果你搜索 OpenLDAP 的安装指南，很不幸地告诉你，网上不管中文的英文的， 90% 都是错的，它们都还活在上个世纪，它们会告诉你要去修改一个叫做 slapd.conf 的文件，基本上看到这里，你就不用往下看了，这个文件早就被抛弃，新版的 OpenLDAP 里根本就没有这个文件！取而代之的是 slapd.d 的文件夹，然后另一部分教程会告诉你，让你修改这个文件夹下的某一个 ldif 文件，看到这里，你也不用往下看了，你又看到了伪教程，因为这个文件夹下的所有文件的第一行都明确地写着：『 这是一个自动生成的文件，不要修改它！ 』你修改了它之后，它的 md5 校验值会匹配不上，造成更多的问题。你应该用 ldapmodify 来修改这个文件，而关于 ldapmodify 的教程，可以说几乎就没有！我一开始不知道面临这样荒谬的处境，很多运维人员是怎么活下来的，不过等我自己配通了以后，真的是累到连写教程的精力

架构

实际上，我的操作步骤很多都是反的，架构这部分是最后才意识到的，但实际上从最一开始就应该先想到。实际上整个 `OpenLDAP` 的架构大致包含 `3` 个部分，而网上没有教材提到这块。

OpenLDAP

首先，是 `OpenLDAP` 的服务器本身，这个东西其实只相当于是一个 `mysql` 数据库，它是没有酷炫的图形界面的，如果你愿意每次都手敲一大堆代码，也可以用它，但这种反人类的设计真的不是给人用的。

phpLDAPadmin

所以，你需要安装一个叫作 `phpLDAPadmin` 的工具，好歹这是一个图形界面，虽然奇丑无比，并且配置起来也并不容易。

PWM

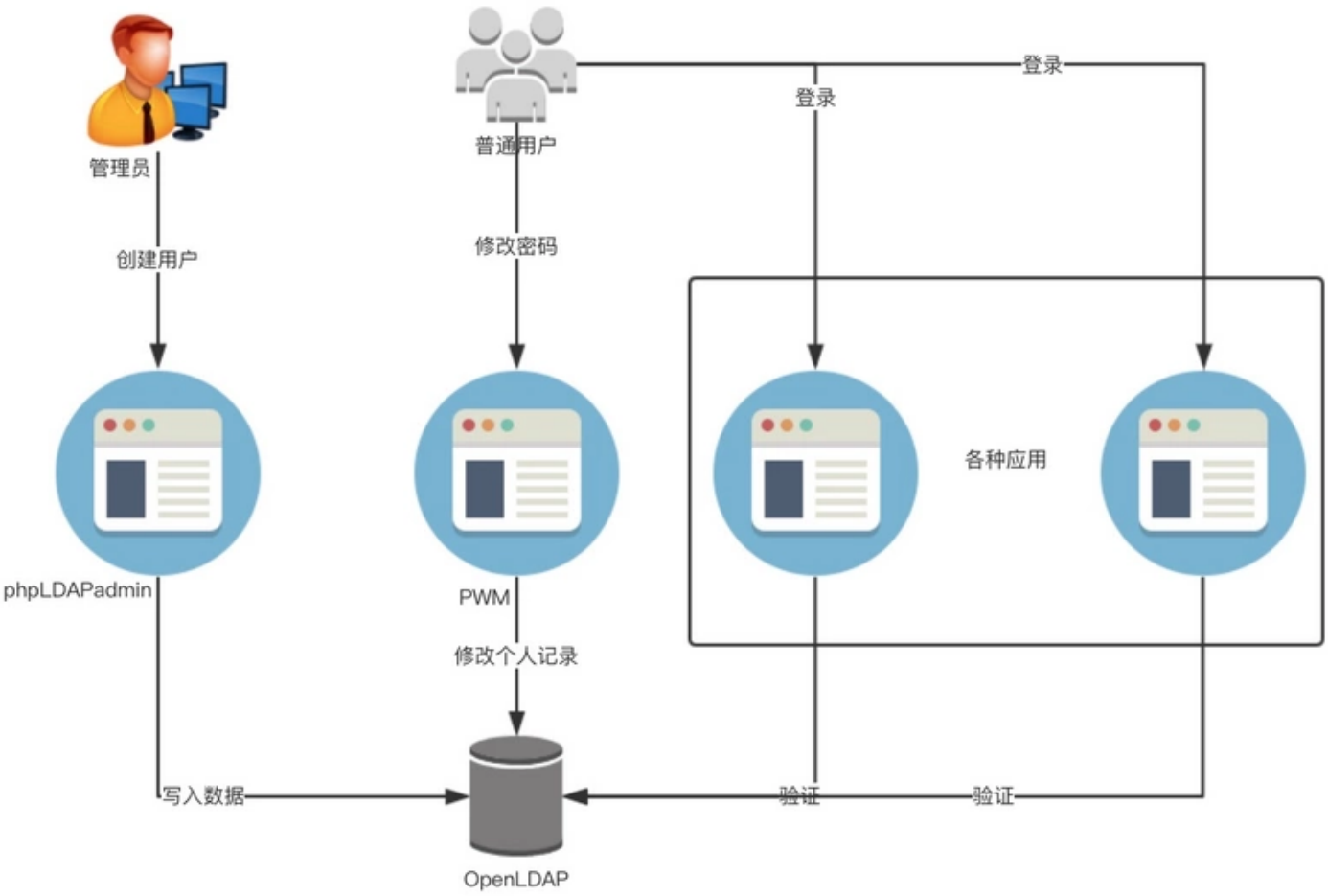
光装管理工具还不够，你总要给用户提供一个修改密码的地方。

客户端

最后，你还需要配置各种工具。

架构图

我画了一个简单的架构图如下：



安装

安装OpenLDAP

安装 OpenLDAP 非常简单，直接安装这 3 个东西就够了，甚至运气好的话，也许你的操作系统已经自带安装好了：

```
yum install openldap openldap-clients openldap-servers
```

安装完了之后可以直接启动 OpenLDAP 服务，不需要做任何配置，我一开始还有顾虑，后来发现完全不用多想直接启动即可：

```
service slapd start
```

配置OpenLDAP

这一块在最一开始是最麻烦的部分，网上所有教程讲的都不对。因为现在是 2018 年了，而很多教程还停留在 2008 年甚至 1998 年。配置 OpenLDAP 最正确的姿势是通过 ldapmodify 命令执行**一系列自己写好的** ldif文件，而**不要修改任何OpenLDAP装好的配置文件**。

举个例子来说，你要想修改 RootDN ，那么你就自己写这么一个 ldif 文件，假设给它起名叫 a.ldif ，然后执行它就可以了：

```
dn: olcDatabase={2}bdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=admin,dc=qiban,dc=com
-
replace: olcSuffix
olcSuffix: dc=qiban,dc=com
```

怎么执行呢？

```
ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f a.ldif
```

这么长的命令是什么意思？ -Q 表示安静执行， -Y 和后面的 EXTERNAL 表示，好吧，我也不知道什么意思，总之需要这样配合，然后 -H 表示地址， -f 表示文件名。几乎所有的 ldapmodify 命令都这么执行就好了。

再来讲解一下上面的 ldif 文件的内容，你不要问为什么叫 ldif 这么一个破后缀，总之你记住它就是这个后缀就好了。 dn 表示你要修改什么东西，在这里我们用的是 {2}bdb ，你的系统不一定是 {2}bdb ，不管是几，总之你去查一下目录里的内容就好了：

```
ls /etc/openldap/slapd.d/cn=config/
```

得到的结果大概如下，不一样也不要害怕：

```
cn=module{0}.ldif cn=schema/ cn=schema.ldif olcDatabase={0}config.ldif olcDatabase=
{-1}frontend.ldif olcDatabase={1}monitor.ldif olcDatabase={2}bdb/ olcDatabase=
{2}bdb.ldif
```

这里面有一大堆奇奇怪怪的数字，不要担心，其中有一个带什么 db.ldif 的就是你最终需要修改的数据库文件，我这里是 bdb.ldif ，你的可能是 mdb.ldif ，还有人是 hdb.ldif ，不管什么 db ，总之你要改的是一个叫 db 的文件就对了。你可以 cat 打开看一看，但是不要用 vi 去修改它。

changetype 就是 modify ，表示我们要修改这个文件。第 3 行是 replace ，表示我们要替换里面的某个值，你可以把这个操作理解为 mysql 数据库的 update 操作，如果你把第 3 行改成 add ，那就是 mysql 的 insert 操作了。不过这里我们操作的只是配置文件本身，还牵涉不到添加用户或者更改用户，如果你以为事情就这么简单，那就是你太天真了。

RootDN 在这里就表示你整个 OpenLDAP 系统的管理员用户名是什么，不要奇怪，后面这一砣都是用户名 cn=admin,dc=qiban,dc=com ，长的有点像 email 地址，实际意思也差不多，但总之就不是 email 就行了。不要问为什么，总之 cn 就是 email 前面的那个名字，后面带 dc 的都是域名。

真实情况是你还需要给这个用户设置一个密码，具体怎么设自行 Google ，但还是那句话：不要修改系统文件，要用ldapmodify来执行。

添加memberOf模块

这个工作应该一开始就做好，要不然后面要做的话，还得把建好的组全删掉再重建。这个模块的作用是当你建一个组的时候，把一些用户添加到这个组里去，它会自动给这些用户添加一个 memberOf 属性，有很多应用需要检查这个属性。

添加的时候比较麻烦，需要建 3 个 ldif 文件，然后 1 个执行 ldapmodify ， 2 个执行 ldapadd ，错一点都不行：

memberof_config.ldif

再一次重申：文件名叫做什么根本无所谓，只要后缀名为 ldif 即可。

```
dn: cn=module,cn=config
cn: module
objectClass: olcModuleList
olcModuleLoad: memberof
olcModulePath: /usr/lib64/openldap

dn: olcOverlay={0}memberof,olcDatabase={2}bdb,cn=config
objectClass: olcConfig
objectClass: olcMemberOf
objectClass: olcOverlayConfig
objectClass: top
olcOverlay: memberof
olcMemberOfDangling: ignore
olcMemberOfRefInt: TRUE
olcMemberOfGroupOC: groupOfNames
olcMemberOfMemberAD: member
```

小心第 5 行和第 7 行，先找到你的模块目录是不是在 /usr/lib64 下面，然后看清楚你的数据库类型和数字，不要瞎复制。

对于这个文件，我们需要执行 ldapadd ：

```
ldapadd -Q -Y EXTERNAL -H ldapi:/// -f memberof_config.ldif
```

执行完之后，检查你的 /etc/openldap/slapd.d/cn=config/ ，看是不是多了一个模块，这个模块的数字编号直接影响下一步操作。

refint1.ldif

```
dn: cn=module{0},cn=config
add: olcmoduleload
olcmoduleload: refint
```

这个文件里我的 memberOf 是第一个模块，所以编号是 0 ，你的不一定，要看清楚到底第几号模块是 memberof ，然后就改成几就可以了，对于这个文件，我们要执行 ldapmodify 操作：

```
ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f refint1.ldif
```

你如果能看懂它的意思的话，它的大意是说要修改我们刚刚添加的那个模块文件的内容。

refint2.ldif

```
dn: olcOverlay={1}refint,olcDatabase={2}bdb,cn=config
objectClass: olcConfig
objectClass: olcOverlayConfig
objectClass: olcRefintConfig
objectClass: top
olcOverlay: {1}refint
olcRefintAttribute: memberof member manager owner
```

对这个文件执行 ldapadd 操作：

```
ldapadd -Q -Y EXTERNAL -H ldapi:/// -f refint2.ldif
```

安装phpLDAPadmin

好吧，干完了上面这些啰里巴嗦的事情，你可以先给自己泡杯咖啡，接下来还有很多工作要做，不过难度已经没有刚才那么大了。

我们开始安装 phpLDAPadmin 。

```
yum install phpldapadmin
```

CentOS 的 yum 安装总是这么令人赏心悦目。

配置phpLDAPadmin

接下来让我们在 nginx 里配置好它，以便让我们的管理员能够看到它。

```
    location /htdocs {
        alias /usr/share/phpldapadmin/htdocs;
        index index.php;
        location ~ \.php$ {
            alias /usr/share/phpldapadmin;
            fastcgi_pass 127.0.0.1:9000;
            fastcgi_index index.php;
            fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
            include fastcgi_params;
        }
    }
```

缺省文件安装在 /usr/share/phpldapadmin/htdocs 下，我们必得要在这里配置一个 alias 才能访问到它，但在 php-fpm 时又要配置另外一个 alias ，这也是比较坑人的一个地方。

接下来你需要修改 /etc/phpldapadmin/config.php 这个文件，里面有大段大段的注释，看到人头晕，注意这么 2 点就够了，其它的都不要改：

- 把 $servers->setValue('login','anon_bind',false); 改成 false ，因为我们不想让人匿名访问；
- 把 $servers->setValue('login','allowed_dns',array('cn=admin,dc=qiban,dc=com')); ，我们只允许管理员访问，其他任何人不得访问。

你现在可以通过 URL 地址访问 phpLDAPadmin 了，登录的时候输入你那一坨用户名：`cn=admin,dc=qiban,dc=com` ，然后输入密码，如果你前面一切都设置对了，那么这里就可以登录进去了。

界面里透出一股浓浓的上世纪九十年代风格，不过好歹我们终于可以脱离纯手写代码管理的窘境了。

这时候你首先要建立两个 `organizationalUnit` ，一个叫作 `groups` ，一个叫作 `users` 。不要问为什么。

然后在 `users` 下面建几个 `inetOrgPerson` ，这些就是你的用户了。注意，在创建新条目时，一定要选择 `默认` ，不要选择什么 `Posix` 或者 `Generic User Account` ，那只会帮你建出一堆没用的 `Linux` 账号出来，我们只想要 `web` 用户，不想建什么 `Linux` 用户。**注意：密码这个地方一定要选 `md5` ，否则你后面和其它系统连接会出问题。**

然后在 `groups` 下面建几个组吧，比如 `admins` ， `users` 等等，注意选择 `objectClass` 为 `groupOfNames` 就行了。然后把你刚刚建好的几个用户分门别类的给他们加到组里去。

在这一步上，如果你前面配置 `memberOf` 模块配置正确的话，你会在 `user` 的 `显示内部属性` 里看到它的 `memberOf` 属性，如果看不到，说明你没有配对。

配置第三方应用

到此为止，似乎真没有什么好说的了， `Phabricator` ， `Confluence` ， `Zabbix` ， `Grafana` ， `禅道` 等等，几乎你能想到的任何一个第三方应用都会有说明书教你怎么配置 `dc` ， `cn` ， `ou` 这些东西，经过了上面这一番折腾，你怎么着也应该对 `LDAP` 的一些术语有所了解了，如果还是不行，说明你玩它的时间还是不够长，再多玩两天，也就明白了。

配置好之后的好处就是你再也不用东一块西一块地建用户了，而可以在一个统一的地方集中管理你的用户和群组授权。

结语

总之，配置 `OpenLDAP` 不是一个轻松的活，但是考虑到有那么多第三方应用都支持这个鬼东西，花点代价把它配通还是值得的。希望你一切顺利。

赞 | 69　　收藏 | 61

赞赏支持

如果觉得我的文章对你有用，请随意赞赏 已赞赏

你可能感兴趣的

- **LDAP开发学习** Corwien openldap sso ldap
- **centos6搭建ldap服务** shenpeng ldap openldap
- **LDAP服务器的概念和原理简单介绍** seanlook openldap
- **LDIF修改ldap记录或配置示例** seanlook openldap
- **openldap账号管理及web管理** Lancger openldap
- **单点登录实现原理及小结** Corwien openldap ldap sso php
- **OpenLDAP(2.4.3x)服务器搭建及配置说明** seanlook openldap
- **phpLDAPadmin 安装** Steve_Wang_ openldap ldap ubuntu

34 条评论

默认排序 | 时间排序

Loading · 2018年10月10日

我觉得openldap能活这么久也是挺难得的

赞 +1　回复

daydaygo · 2018年05月06日

看完没明白 openLDAP 干嘛的 -_-

赞　回复

> 一般把企业员工资料保存在LDAP里，包括姓名、部门、联系方式、Email地址、登录账号、密码、密钥等等。然后各种系统利用LDAP里的资料作为系统用户。
>
> — **SyuTingSong** · 2018年05月07日

> @SyuTingSong 做过一个涉及windows域的项目才接触到这个, 当时懵逼了好几天. 现在还有哪个OA系统用LDAP处理员工信息?
>
> — **ssy** · 2018年05月08日

2　@ssy 老外的一堆一堆。其实Windows Server和Mac OS X Server都有GUI的LDAP设置，只有Linux上配置比较麻烦。文档也比较老。

添加回复

carefor · 2018年05月07日

建议用ApacheLdapStudio，开源免费，功能强大

赞　回复

Rambone · 2018年05月08日

虽然LDAP协议可能古老 实现又比较原始 但是兄弟 看完你写的 我还是没懂dc ou cn 另外它提供的uri schema结构解析 更重要的ldif文件的解析 都还是懵进懵出啊 Confluence gitlab Grafana的接入例子也应该多举一下啊

赞　回复

> @Rambone 写这篇文章的时候刚刚从坑里爬起来，情绪比较大，回头再补充一下。
> — **张京** 作者 · 2018年05月09日

添加回复

leo_liao · 2018年05月09日

app可以调用ldap认证吗？

赞　回复

> 你可以把ldap理解为一个mysql数据库，app或者js如何调用mysql？中间加一层就行了。有很多这方面的类库，包括java, php, node.js都有，例如：https://github.com/jeremycx/n...
> — **张京** 作者 · 2018年05月09日

添加回复

LittleLawson · 2018年07月05日

这篇文章字里行间都是火气。我也被openLDAP搞伤了，什么玩意儿。
附注：博主的这个系统版本不是centos 7，如果是centos 7的同志请绕道。【我在centos 6.5上能够运行出来，但是centos 7就是不行mlgb】

赞　回复

> 最后搞定了吗
> — **blueli** · 1月24日

添加回复

vickey · 2018年07月31日

```
[root@effe24310246 cn=config]# ls
cn=module{0}.ldif  cn=schema.ldif        olcDatabase={0}config.ldif     olcDatabase={1}m
cn=schema          memberof_config.ldif  olcDatabase={-1}frontend.ldif  olcDatabase={2}b
[root@effe24310246 cn=config]# ldapmodify -H ldapi:// -Y EXTERNAL -f password.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={2}bdb,cn=config"
ldap_modify: No such object (32)
    matched DN: cn=config
```

password.ldif

```
dn: olcDatabase={2}bdb,cn=config
changetype: modify
replace: olcRootPW
olcRootPW: {SSHA}xxxxx
-
replace: olcRootDN
olcRootDN: cn=admin,dc=test,dc=com
-
replace: olcSuffix
olcSuffix: dc=test,dc=com
```

赞 回复

> 我也是，没搞定，☹
> — **张文剑** · 1月15日

添加回复

咸鱼delion · 2018年08月07日

博主一开始就帮我吐槽了一下刚开始接触这玩意的人的真实想法，多么痛的领悟！！！！！

赞 回复

咸鱼delion · 2018年08月07日

博主你好，我在配置menberof的时候，报错manager没有定义，请问是什么原因

赞 回复

> 我遇到同样问题。。。
> — **Jiang** · 2018年10月24日

> @张京 同样的问题。。麻烦博主知道什么原因吗？
> — **liguettkl** · 2018年11月07日

我之前遇到了，应该是没有执行
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif

— **小仓鼠看世界** · 2018年11月28日

添加回复 | 显示更多

大优 · 2018年08月15日

2018年,启动命令就不要用service slapd start了，默认得用systemctl start slapd吧。

赞 回复

用docker吧，不用纠结这些le

— **panpanlala** · 2018年10月08日

docker可以打包所有应用吗，我怎么感觉有了docker不需要运维了。

— **大优** · 2018年10月08日

添加回复

12345678 · 2018年09月21日

有很多东西是可以变通的，
在centos7上搭建有slapd.conf这个文件的版本，复制出这个文件，
卸载这个版本，安装最新版本，用这个文件修改配置（需要略做修改），
用 slaptest -f slapd.conf -F slapd.d/ 生成最新版本用的配置文件，然后就不用管配置了。
最后使用ApacheLdapStudio 做为管理端，进行管理。

赞 回复

ApacheLdapStudio作为管理端有什么文档推荐的吗，自己查询了一下感觉都不是很实用

— **team_jer** · 2018年10月18日

添加回复

panpanlala · 2018年10月09日

github openldap使用docker 启动openldap，默认会将groupOfUniqueNames添加memberOf支持，用户账号使用inetPerson，就不用如上那么麻烦的配置了，当然前提还是要对openldap有一定的理解，边实践边参考文档~

赞 回复

yj7778826 · 2018年10月26日

顶上去，让更多人看到，妈的我也被一堆旧教程坑了半天，推荐大家去看ubuntu的官方文档，挺全的，

星星之火 · 2018年10月31日

是作者的总结，仅此而已。

赞 回复

胡孝义 · 2018年11月05日

轻松幽默的语言风格，赞一个👍

赞 回复

LBQQ · 2018年11月12日

“openladp” 和 “Django+ladp” 这两个有什么区别，到现在也不是很清楚。博主大大可以简单回答下吗= = 拜托

赞 回复

予安 · 1月8日

老哥啊，我必须要来回复你一下，我按照老哥你的步骤报了很多错误，最后解决了，感谢！老哥的步骤是我在网上看到最正确的了！

赞 回复

> 在执行时报错ldapadd -Q -Y EXTERNAL -H ldapi:/// -f refint2.ldif，数据库改了。你遇到了么
> — **Mikey** · 1月9日

添加回复

evan · 1月17日

我也是18年五一的时候，3天假期就在折腾这玩意。
因被要下架所有的winserver机器，花了3天把从AD迁移到OpenLDAP, 对接了内部10多个系统。

赞 回复

T、 · 1月26日

大佬 ，我的centos7上按照你的文档搞得，但是配置了nginx访问不了phpldapadmin呀
The page you are looking for is not found.

赞 回复

文明社会，理性评论

发布评论