**二木运维**

**centos7系统部署openldap**

版权所有 侵权必究

文档版本修改历史

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本号 | 修订日期 | 修订人 | 变更内容 | 备注 |
| 0.0.1 | 2022.08.02 | 林令 | 初稿 | Centos7系统部署Openldap |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

审核

|  |  |  |
| --- | --- | --- |
|  | **签名(Signature)** | **日期(Date)** |
|  | **签名(Signature)** | **日期(Date)** |

目录

[centos7系统部署openldap 1](#_Toc29149)

[文档版本修改历史 1](#_Toc3109)

[审核 1](#_Toc22356)

[第一章 文档说明 3](#_Toc18982)

[1.1 文档目的 3](#_Toc19780)

[1.2 使用范围 3](#_Toc26394)

[1.3术语及缩写解释 3](#_Toc20019)

[第二章 组织与工作安排 4](#_Toc24712)

[2.1前期准备概述 4](#_Toc25178)

[2.2 工作思路 4](#_Toc17254)

[2.3 人员组织 4](#_Toc31212)

[2.4 职责分工 5](#_Toc25031)

[第三章 实施步骤 6](#_Toc32412)

[3.1 Linux系统初始化 6](#_Toc1754)

[3.1.1 主机名修改 6](#_Toc32280)

[3.1.2 配置静态IP 6](#_Toc9190)

[3.1.3 hosts文件 7](#_Toc7574)

[3.1.4关闭SElinux 7](#_Toc1579)

[3.1.5配置yum源 8](#_Toc18094)

[3.1.6普通用户sudo管理 8](#_Toc25810)

[3.1.7 ssh服务配置 9](#_Toc16399)

[3.1.8安装必要软件 10](#_Toc20303)

[3.1.9主机自动更新时间 10](#_Toc14548)

[3.1.10设置主机最大打开数 11](#_Toc2022)

[3.1.11防火墙管理 11](#_Toc17281)

[3.2 Openldap安装 11](#_Toc29482)

[3.3配置变更 12](#_Toc26100)

[3.3.1配置管理员密码 12](#_Toc19636)

[3.3.2 Openldap架构导入 13](#_Toc19916)

[3.4域名和管理员 13](#_Toc4714)

[3.5启用memberof功能 14](#_Toc29969)

[3.6创建组织角色和组织单元 15](#_Toc25347)

[3.7 Phpldapadmin可视化 16](#_Toc8490)

[3.7.1软件说明 16](#_Toc12720)

[3.7.2安装phpldapadmin 16](#_Toc13916)

[3.7.3配置更改 16](#_Toc20)

[3.7.4启用开机自启并开启服务 17](#_Toc27750)

[3.7.5网页登陆 17](#_Toc6384)

# 文档说明

## 1.1 文档目的

撰写此文档目的是记录部署Openldap环境的配置过程，其他工程师可供参考。

## 1.2 使用范围

文档主要适用于centos7和redhat7版本，其他系统或是低版本系统小部分适用。

## 1.3术语及缩写解释

|  |  |
| --- | --- |
| 术语、缩写 | 解释 |
| 主机 | Centos7.4系统 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# 第二章 组织与工作安排

## 2.1前期准备概述

优化前安装好centos7系统，下方是本人环境

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 操作系统 | IP地址 | CPU | 内存 | 硬盘 |
| Centos7.4 | 192.168.179.125 | 1核 | 2G | 20G |

镜像的下载地址：

|  |
| --- |
| https://mirrors.tuna.tsinghua.edu.cn/centos/7.6.1810/isos/x86\_64/CentOS-7-x86\_64-DVD-1810.iso |

## 2.2 工作思路

首先安装openldap软件，然后对配置变更，创建域名和管理员，启用memberof功能，创建组织角色和组织单元，Phpldapadmin可视化管理。

## 2.3 人员组织

人员信息如下

|  |  |  |  |
| --- | --- | --- | --- |
| **姓名** | **单位** | **联系方式** | **职责** |
| 林令 | 二木工作室 | 13672781335 | 现场实施 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 2.4 职责分工

由二木工作室工程师负责实施过程。

# 第三章 实施步骤

## 3.1 Linux系统初始化

### 3.1.1 主机名修改

查看主机名

|  |
| --- |
| hostname |

临时修改主机名

|  |
| --- |
| hostname Openldap.ermu.com |

永久修改主机名(主机重启后生效)

|  |
| --- |
| hostnamectl set-hostname Openldap.ermu.com |

修改建议：临时修改后再永久修改，避免重启主机

### 3.1.2 配置静态IP

备份当前的网卡配置(注意网卡与配置的对应)

|  |
| --- |
| cp /etc/sysconfig/network-scripts/ifcfg-ens33 /etc/sysconfig/ifcfg-ens33.`date +%Y-%m-%d` |

配置静态ip地址

|  |
| --- |
| cat<<\EOF > /etc/sysconfig/network-scripts/ifcfg-ens33  TYPE="Ethernet"  BOOTPROTO="static"  IPADDR=192.168.179.125  NETMASK=255.255.255.0  GATEWAY=192.168.179.2  DEFROUTE="yes"  NAME="ens33"  DEVICE="ens33"  ONBOOT="yes"  DNS1=114.114.114.114  EOF |

重启生效

|  |
| --- |
| systemctl restart network |

查看

|  |
| --- |
| ip addr show |

### 3.1.3 hosts文件

将修改的主机名和静态ip写入hosts文件

|  |
| --- |
| echo "192.168.179.125 Openldap.ermu.com" >> /etc/hosts |

通过脚本写入

|  |
| --- |
| cat<<\EOF > /root/host.sh  #!/bin/bash  #Filename: hosts.shell  #auto Get the host name and IP address  #by authors linling 2019  IP=`ip addr show|grep ens33|grep global|awk '{print $2}'|awk -F '/' '{print $1}'`  Hostname=`hostname`  echo "$IP" "$Hostname" >> /etc/hosts  EOF  chmod +x /root/host.sh  sh /root/host.sh |

### 3.1.4关闭SElinux

查看selinux

|  |
| --- |
| getenforce |

临时修改

|  |
| --- |
| setenforce 0 |

备份主机当前selinux配置文件

|  |
| --- |
| cp /etc/selinux/config /etc/selinux/config.`date +%Y-%m-%d` |

永久修改(主机重启后生效)

|  |
| --- |
| sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config |

修改建议：临时修改后永久修改，避免主机重启

### 3.1.5配置yum源

备份默认yum源

|  |
| --- |
| cp -r /etc/yum.repos.d/ /etc/yum.repos.d.`date +%Y-%m-%d` |

配置yum源

|  |
| --- |
| rm -rf /etc/yum.repos.d/\*  cat<<\EOF > /etc/yum.repos.d/dvd.repo  [dvd]  name=dvd  baseurl=https://mirrors.tuna.tsinghua.edu.cn/centos/7/os/x86\_64/  enabled=1  gpgcheck=0  [dvd1]  name=dvd1  baseurl=https://mirrors.tuna.tsinghua.edu.cn/epel/7/x86\_64/  enabled=1  gpgcheck=0  [dvd2]  name=dvd2  baseurl=https://mirrors.tuna.tsinghua.edu.cn/centos/7/extras/x86\_64/  enabled=1  gpgcheck=0  EOF |

清理缓存

|  |
| --- |
| yum clean all |

显示可用仓库

|  |
| --- |
| yum makecache all |

### 3.1.6普通用户sudo管理

创建普通用户

|  |
| --- |
| useradd -u 1050 ai  echo ai | passwd ai --stdin > /dev/null 2>&1 |

备份默认的sudo文件

|  |
| --- |
| cp /etc/sudoers /etc/sudoers.`date +%Y-%m-%d` |

添加普通用户至sudo

|  |
| --- |
| echo "ai ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers |

配置sudo日志

|  |
| --- |
| touch /var/log/sudolog  echo \*.debug /var/log/sudolog >> /etc/rsyslog.conf |

重启日志服务

|  |
| --- |
| systemctl restart rsyslog |

### 3.1.7 ssh服务配置

备份默认的ssh服务配置

|  |
| --- |
| cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.`date +%Y-%m-%d` |

配置

|  |
| --- |
| cat<<\EOF > /etc/ssh/sshd\_config  Port 918  PermitRootLogin yes  PermitEmptyPasswords no  PasswordAuthentication yes  X11Forwarding yes  UseDNS no  GSSAPIAuthentication no  Subsystem sftp /usr/libexec/openssh/sftp-server  EOF |

配置说明

|  |  |
| --- | --- |
| Port | 端口号修改为918，默认22 |
| PermitRootLogin | 不允许root远程登录 |
| PermitEmptyPasswords | 不允许用口令为空的账号登录系统 |
| PasswordAuthentication | 允许密码登录 |

重启服务

|  |
| --- |
| systemctl restart sshd |

查看

|  |
| --- |
| netstat -ntl |grep 918 |

### 3.1.8安装必要软件

软件安装

|  |
| --- |
| yum install lrzsz ntpdate sysstat net-tools wget unzip -y |

说明

|  |  |
| --- | --- |
| lrzsz | 上传下载的软件 |
| sysstat | 用来检测系统性能及效率的工具 |
| net-tools | 没有ifconfig命令时候需要安装工具 |

### 3.1.9主机自动更新时间

安装ntp

|  |
| --- |
| yum install -y ntp |

关闭chronyd服务

|  |
| --- |
| systemctl stop chronyd  systemctl disable chronyd |

备份默认配置文件

|  |
| --- |
| cp /etc/ntp.conf /etc/ntp.conf.`date +%Y-%m-%d` |

配置

|  |
| --- |
| sed -i '/server 0/d' /etc/ntp.conf  sed -i '/server 1/d' /etc/ntp.conf  sed -i '/server 2/d' /etc/ntp.conf  sed -i '/server 3/d' /etc/ntp.conf  sed -i '/Please/a server ntp.aliyun.com iburst' /etc/ntp.conf |

服务重启并设置开机自启

|  |
| --- |
| systemctl restart ntpd  systemctl enable ntpd |

### 3.1.10设置主机最大打开数

查看

|  |
| --- |
| ulimit -a |

临时修改

|  |
| --- |
| ulimit -HSn 65535 |

永久修改(主机重启后生效)

|  |
| --- |
| echo "\* soft nofile 65535" >> /etc/security/limits.conf  echo "\* hard nofile 65535" >> /etc/security/limits.conf |

修改建议：临时修改后永久修改，避免主机重启

### 3.1.11防火墙管理

关闭并禁止开机自启firewalld防火墙服务

|  |
| --- |
| systemctl stop firewalld  systemctl disable firewalld |

## 3.2 Openldap安装

安装

|  |
| --- |
| yum install -y openldap openldap-clients openldap-servers |

DB配置

|  |
| --- |
| cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG |

授权

|  |
| --- |
| chown -R ldap. /var/lib/ldap/DB\_CONFIG |

启用开机自启并开启服务

|  |
| --- |
| systemctl start slapd && systemctl enable slapd |

查看状态

|  |
| --- |
| systemctl status slapd |

## 3.3配置变更

### 3.3.1配置管理员密码

配置说明

|  |
| --- |
| openldap2.4.23以后的版本，所有配置都保存在/etc/openldap/slapd.d/cn=config 目录下，后缀为ldif。且每个配置都是通过命令自动生成的。在每个配置顶部都会有注释，提示请勿编辑。使用ldapmodify命令编辑  # AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.  安装openldap后，会有三个命令用于修改配置文件，分别是ldapadd、ldapmodify、ldapdelete。顾名思义就是添加、修改、删除。  后缀是ldif,文件名随意。不可在/etc/openldap/slapd.d/目录下创建 |

生成olcRootPW密码

|  |
| --- |
| slappasswd -s 123456 |

changepwd.ldif文件

|  |
| --- |
| cat<<\EOF > changepwd.ldif  dn: olcDatabase={0}config,cn=config  changetype: modify  add: olcRootPW  olcRootPW: {SSHA}JrHpNp+rGc6FiiLUbHXw2uiswwNnSdg4  EOF |

配置说明

|  |
| --- |
| # 第一行执行配置文件，这里就表示指定为cn=config/olcDatabase={0}config文件。你到/etc/openldap/slapd.d/目录下就能找到此文件  # 第二行 changetype 指定类型为修改  # 第三行 add 表示添加 olcRootPW 配置项  # 第四行指定 olcRootPW 配置项的值 |

执行

|  |
| --- |
| ldapadd -Y EXTERNAL -H ldapi:/// -f changepwd.ldif |

检查

|  |
| --- |
| cat /etc/openldap/slapd.d/cn\=config/olcDatabase\=\{0\}config.ldif |grep olcRootPW |

### 3.3.2 Openldap架构导入

依次执行

|  |
| --- |
| 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  ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/collective.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/corba.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/duaconf.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/dyngroup.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/java.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/misc.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/openldap.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/pmi.ldif  ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/ppolicy.ldif |

## 3.4域名和管理员

changedomain.ldif文件

|  |
| --- |
| cat<<\EOF > changedomain.ldif  dn: olcDatabase={1}monitor,cn=config  changetype: modify  replace: olcAccess  olcAccess: {0}to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read by dn.base="cn=admin,dc=test,dc=com" read by \* none  dn: olcDatabase={2}hdb,cn=config  changetype: modify  replace: olcSuffix  olcSuffix: dc=test,dc=com  dn: olcDatabase={2}hdb,cn=config  changetype: modify  replace: olcRootDN  olcRootDN: cn=admin,dc=test,dc=com  dn: olcDatabase={2}hdb,cn=config  changetype: modify  replace: olcRootPW  olcRootPW: {SSHA}+H44q8jlJdTM9YwI7OElzxcjLN+5GGIV  dn: olcDatabase={2}hdb,cn=config  changetype: modify  add: olcAccess  olcAccess: {0}to attrs=userPassword,shadowLastChange by dn="cn=admin,dc=test,dc=com" write by anonymous auth by self write by \* none  olcAccess: {1}to dn.base="" by \* read  olcAccess: {2}to \* by dn="cn=admin,dc=test,dc=com" write by \* read  EOF |

执行

|  |
| --- |
| ldapmodify -Y EXTERNAL -H ldapi:/// -f changedomain.ldif |

## 3.5启用memberof功能

说明

|  |
| --- |
| 开启memberof支持并新增用户支持memberof配置 |

add-memberof.ldif文件

|  |
| --- |
| cat<<\EOF > add-memberof.ldif  dn: cn=module{0},cn=config  cn: modulle{0}  objectClass: olcModuleList  objectclass: top  olcModuleload: memberof.la  olcModulePath: /usr/lib64/openldap  dn: olcOverlay={0}memberof,olcDatabase={2}hdb,cn=config  objectClass: olcConfig  objectClass: olcMemberOf  objectClass: olcOverlayConfig  objectClass: top  olcOverlay: memberof  olcMemberOfDangling: ignore  olcMemberOfRefInt: TRUE  olcMemberOfGroupOC: groupOfUniqueNames  olcMemberOfMemberAD: uniqueMember  olcMemberOfMemberOfAD: memberOf  EOF |

refint1.ldif文件

|  |
| --- |
| cat<<\EOF > refint1.ldif  dn: cn=module{0},cn=config  add: olcmoduleload  olcmoduleload: refint  EOF |

refint2.ldif文件

|  |
| --- |
| cat<<\EOF > refint2.ldif  dn: olcOverlay=refint,olcDatabase={2}hdb,cn=config  objectClass: olcConfig  objectClass: olcOverlayConfig  objectClass: olcRefintConfig  objectClass: top  olcOverlay: refint  olcRefintAttribute: memberof uniqueMember manager owner  EOF |

依次执行

|  |
| --- |
| ldapadd -Q -Y EXTERNAL -H ldapi:/// -f add-memberof.ldif  ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f refint1.ldif  ldapadd -Q -Y EXTERNAL -H ldapi:/// -f refint2.ldif |

## 3.6创建组织角色和组织单元

base.ldif文件

|  |
| --- |
| cat<<\EOF > base.ldif  dn: dc=test,dc=com  objectClass: top  objectClass: dcObject  objectClass: organization  o: test Company  dc: test  dn: cn=admin,dc=test,dc=com  objectClass: organizationalRole  cn: admin  dn: ou=People,dc=test,dc=com  objectClass: organizationalUnit  ou: People  dn: ou=Group,dc=test,dc=com  objectClass: organizationalRole  cn: Group  EOF |

执行

|  |
| --- |
| ldapadd -x -D cn=admin,dc=test,dc=com -W -f base.ldif |

## 3.7 Phpldapadmin可视化

### 3.7.1软件说明

说明

|  |
| --- |
| phpldapadmin很多没更新了，只支持php5，如果你服务器的环境是php7，则会有问题，页面会有各种报错，需要epel源。 |

### 3.7.2安装phpldapadmin

安装

|  |
| --- |
| yum install -y phpldapadmin |

### 3.7.3配置更改

配置说明

|  |
| --- |
| 根据版本更改配置，centos7默认安装的是apache2.4 |

备份phpldapadmin.conf

|  |
| --- |
| cp /etc/httpd/conf.d/phpldapadmin.conf /etc/httpd/conf.d/phpldapadmin.conf.`date +%Y-%m-%d` |

配置apache访问权限

|  |
| --- |
| sed -i 's/Require local/Require all granted/g' /etc/httpd/conf.d/phpldapadmin.conf |

备份

|  |
| --- |
| cp /etc/phpldapadmin/config.php /etc/phpldapadmin/config.php.`date +%Y-%m-%d` |

修改配置用DN登录ldap

|  |
| --- |
| vim /etc/phpldapadmin/config.php  # 398行，默认是使用uid进行登录，我这里改为cn，也就是用户名  $servers->setValue('login','attr','cn');  # 460行，关闭匿名登录，否则任何人都可以直接匿名登录查看所有人的信息  $servers->setValue('login','anon\_bind',false);    # 519行，设置用户属性的唯一性，这里我将cn,sn加上了，以确保用户名的唯一性  $servers->setValue('unique','attrs',array('mail','uid','uidNumber','cn','sn')); |

### 3.7.4启用开机自启并开启服务

启用开机自启

|  |
| --- |
| systemctl enable httpd |

开启服务

|  |
| --- |
| systemctl start httpd |

### 3.7.5网页登陆

登陆

|  |
| --- |
| http://192.168.179.125/ldapadmin |

账密

|  |
| --- |
| admin/123456 |