**对接AD域控配置手册**

—银河麒麟桌面操作系统v10sp1

2025年03月01日

**文档变更记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本号 | 变更说明 | 变更人 | 日期 | 备注 |
| V1.0 | 撰写 |  | 2025年03月01日 |  |
|  |  |  |  |  |
|  |  |  |  |  |

目录

[一、 引言 1](#_Toc32171)

[1. 文档概述 1](#_Toc24672)

[2. 适用范围 1](#_Toc26358)

[二、 配置前准备工作 1](#_Toc7297)

[三、 配置步骤 2](#_Toc24491)

[1. 步骤1： 2](#_Toc27579)

[修改麒麟桌面系统网络以及计算机名 2](#_Toc1044)

[2. 步骤2： 3](#_Toc3554)

[修改samba配置文件 3](#_Toc7833)

[3. 步骤3： 3](#_Toc11773)

[重启samba服务 3](#_Toc5991)

[4. 步骤4： 4](#_Toc16348)

[5. 步骤5： 4](#_Toc22035)

[6. 步骤6： 5](#_Toc27550)

[7. 步骤7： 5](#_Toc19866)

[8. 步骤8： 6](#_Toc32319)

[9. 步骤9： 6](#_Toc27956)

[10. 步骤10： 6](#_Toc20379)

[11. 步骤11 7](#_Toc17607)

[12. 步骤12： 7](#_Toc20877)

[13. 步骤13 10](#_Toc25097)

[14. 步骤14： 10](#_Toc22809)

[15. 步骤15： 10](#_Toc21389)

[四、 附录 11](#_Toc31162)

# 引言

## 文档概述

文本主要介绍如何在银河麒麟桌面操作系统V10SP1系统上使用samba+winbind的方式对接ad域控，实现使用域账号登录麒麟操作系统。

## 适用范围

本手册面向具有Linux操作系统使用经验的用户、麒麟软件一线工程师及相关技术人员等，实现在银河麒麟桌面操作系统上使用ad域控登录。

# 配置前准备工作

Ad域控：windows server 2019

IP地址：10.0.0.189

域名：kylinos.com

域控账号密码：[zhangsan@kylinos.com](mailto:zhangsan@kylinos.com)/Kylin123123

银河麒麟桌面操作系统V10 SP1 2303/2403

# 配置步骤

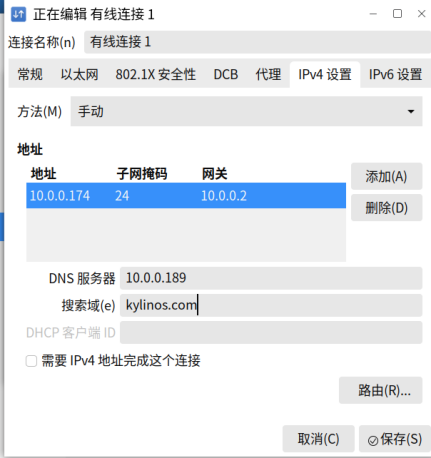
## 步骤1：

## 修改麒麟桌面系统网络以及计算机名

此处计算机名修改为client1



网络配置如下：



DNS服务器：配置域控地址

搜索域：配置ad域名

## 步骤2：

## 修改samba配置文件

配置如下：sudo vim /etc/samba/smb.conf

workgroup = KYLINOS

realm = KYLINOS.COM

netbios name = kylin

security = ads

dns forwarder = 10.0.0.189

idmap uid = 10000-20000

idmap gid = 10000-20000

client use spnego = yes

client ntlmv2 auth = yes

template homedir = /home/%D/%U

template shell = /bin/bash

winbind use default domain = true

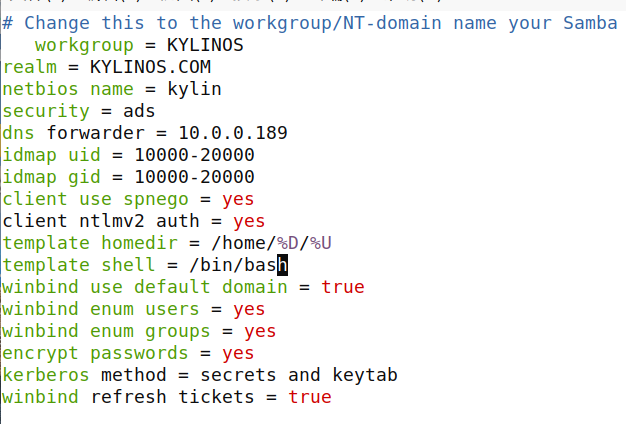
winbind enum users = yes

winbind enum groups = yes

encrypt passwords = yes

kerberos method = secrets and keytab

winbind refresh tickets = true



## 步骤3：

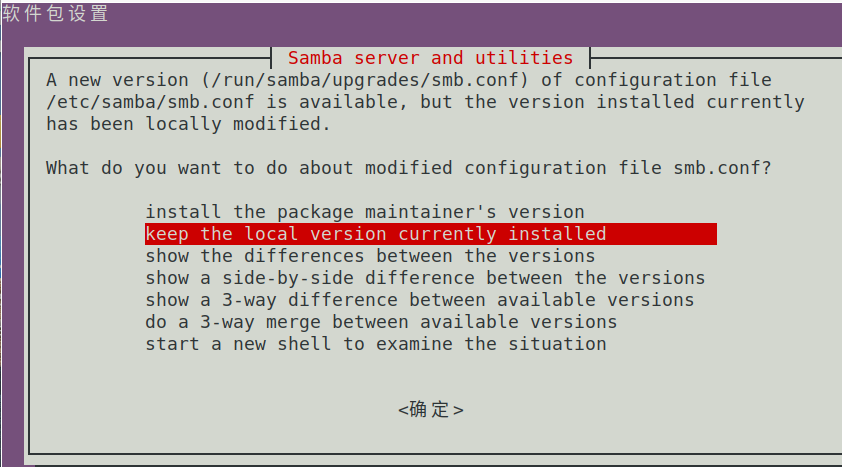
## 重启samba服务

sudo systemctl restart smbd

## 步骤4：

安装winbind相关软件sudo apt install samba krb5-config krb5-user winbind libpam-winbind libnss-winbind

2403以下版本安装过程中会升级samba版本，选择保留当前的samba版本（回车即可）



## 步骤5：

修改/etc/krb5.conf 配置文件

其中：KYLINOS.COM为你的ad域名，kdc与admin\_server写ad域控的FQDN（域计算机名.域名或者域控ip地址）

[libdefaults]

default\_realm = KYLINOS.COM

[realms]

KYLINOS.COM = {

kdc = winad.kylinos.com

admin\_server = winad.kylinos.com

}

[domain\_realm]

.kylinos.com = KYLINOS.COM

kylinos.com = KYLINOS.COM

## 步骤6：

创建ad域控的主目录：sudo pam-auth-update

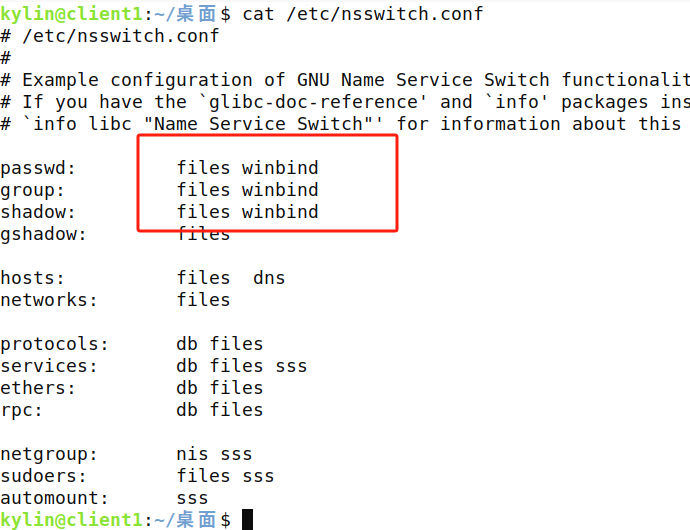
选择 Create home directory on login (在登录时创建主目录)，然后选择 Ok (确定)。



## 步骤7：

配置本地域认证

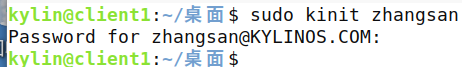
sudo vim /etc/nsswitch.conf



## 步骤8：

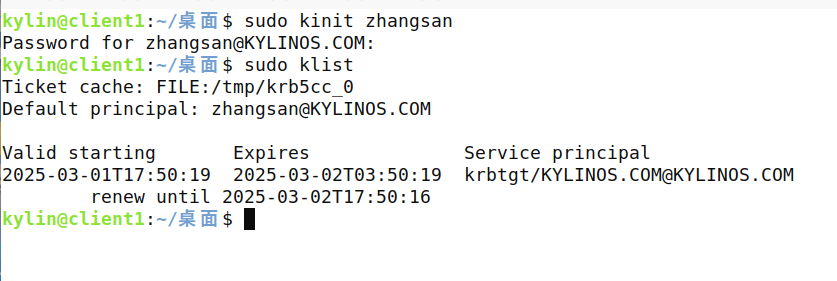
启动Kerberos 票证，zhangsan为域账号，回车后属于域账号密码

sudo kinit zhangsan



确认已成功创建票证：

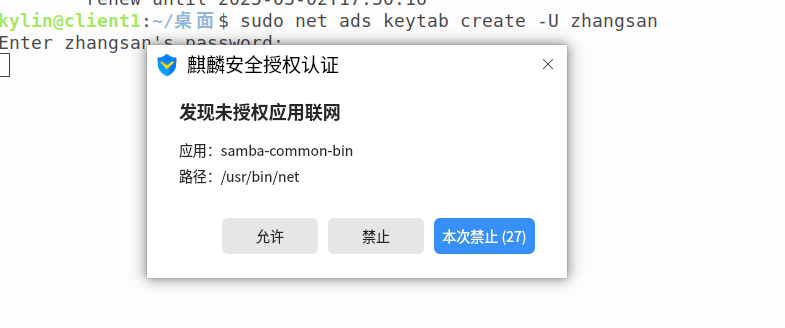
sudo klist



## 步骤9：

创建一个 Kerberos keytab 文件

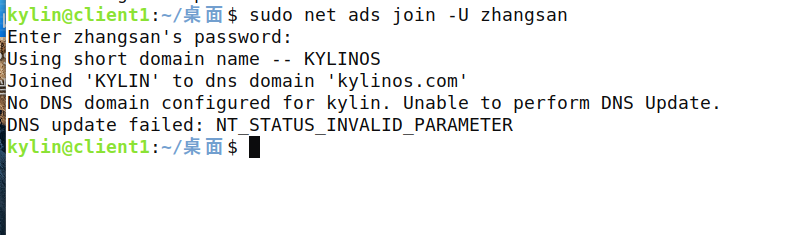
sudo net ads keytab create -U zhangsan（若是没有关闭麒麟安全设置会弹窗认证，点击允许即可）



## 步骤10：

加入AD域控

sudo net ads join -U zhangsan



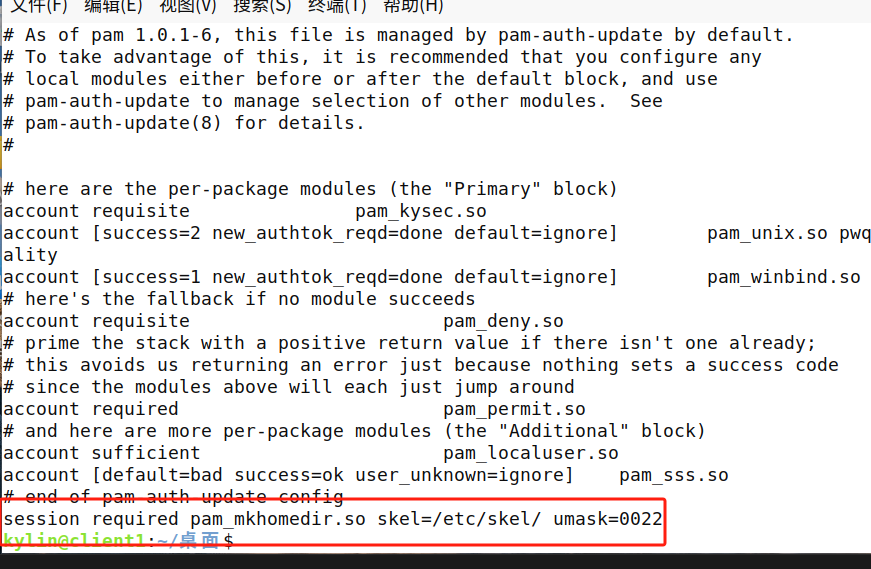
## 步骤11

重启winbind服务（若是没有关闭麒麟安全设置会弹窗认证，点击允许即可）

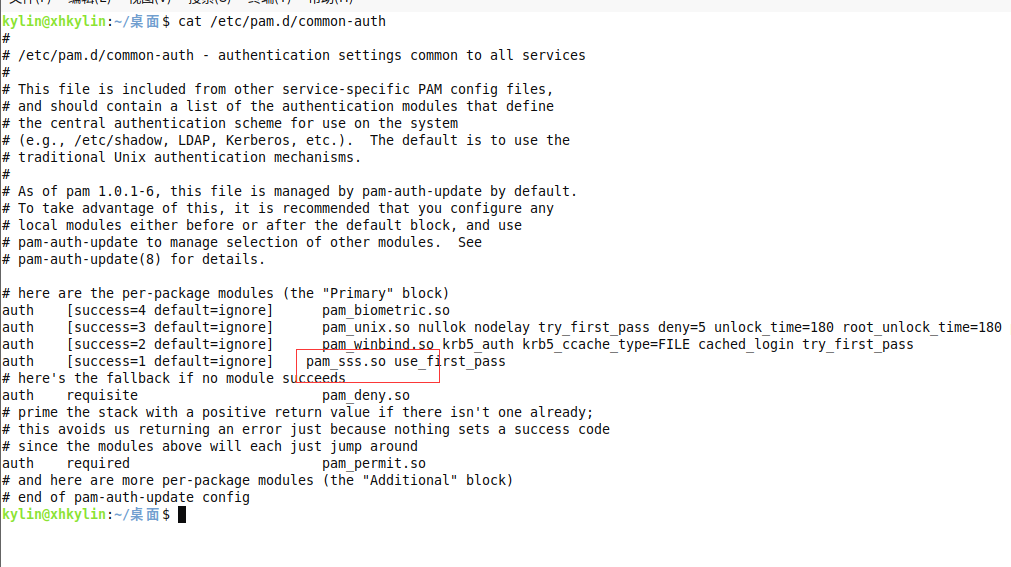


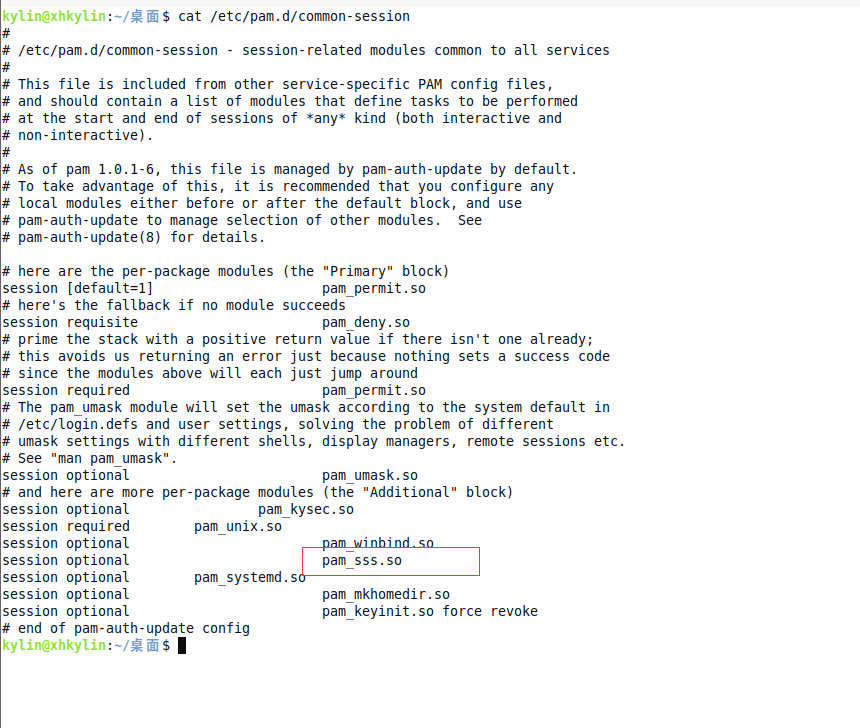
## 步骤12：

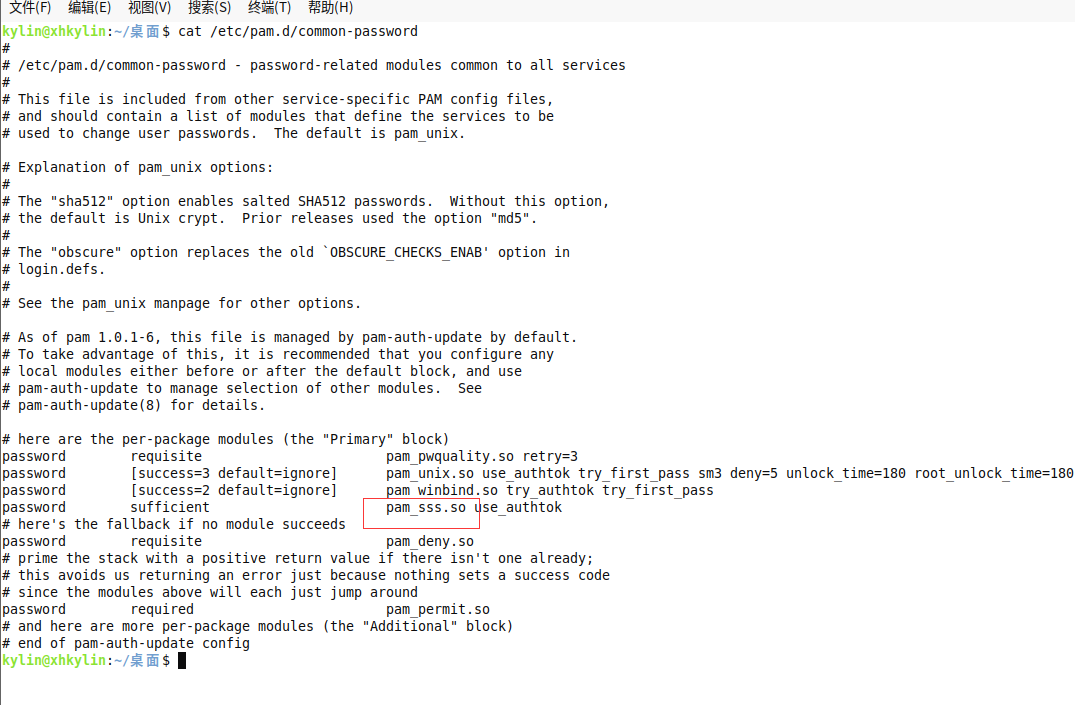
修改/etc/pam.d/common-account，以便域账号能够创建家目录



银河麒麟桌面系统2403版本还需要更改以下配置



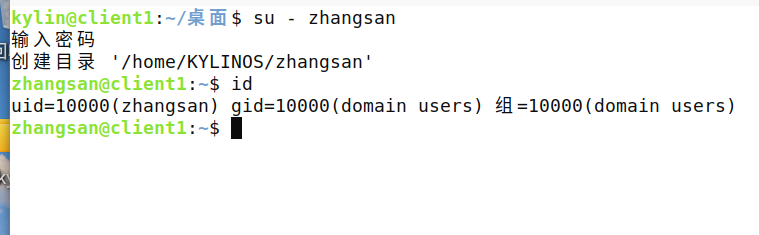






## 步骤13

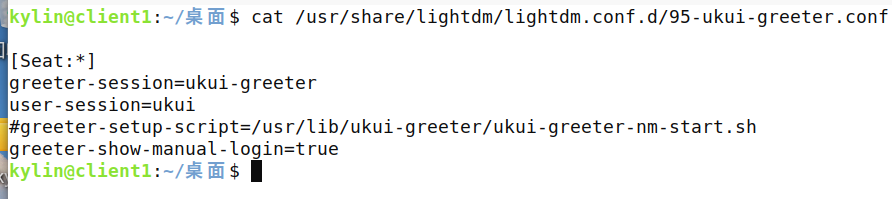
验证域账号是否能够正常登录系统



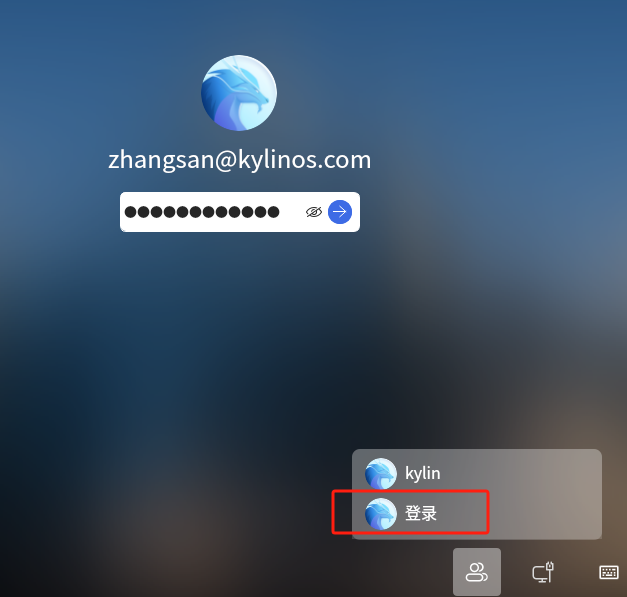
## 步骤14：

修改 lightdm 配置

/usr/share/lightdm/lightdm.conf.d/95-ukui-greeter.conf



## 步骤15：

重启验证：登录账号需带域名

# 附录

步骤2说明

workgroup：指定域名或工作组名，就是“.com”之前的名字，例如 qr.com。这里

就填“qr”，不区分大小写。

realm：指要加入的域的名称

netbios name：就是在“网上邻居”里看到的名字，通常是计算机名字中的第一

部分

security：

指定 samba 的安全模式，现有五种安全模式；security = ads 当 samba 服

务器加入到 windows AD 域时使用该模式，也是将验证工作交给 windows 域

控制器负责。使用这个模式需要在 samba 服务器上安装 Kerberos。注意，在

这个模式中 samba 是作为一个域成员，并不是 AD 域控制器。ads 验证方式必须配合 realm 参数

dns forwarder：指定 dns 服务器，这里可以直接写 AD 域控

idmap uid/idmap gid：指定将域用户映射成 linux 本地用户的 UID 和 GID 范围。实

际上 linux 系统内部运行是只识别 uid 和 gid。

client use spnego：这个变量控制 samba 客户端是否将尝试对 WindowsXP 和

Windows2000 服务器使用简单和受保护的协商(由 rfc2478 指定)以同意一种身份

验证机制。SPNEGO客户端对SMB签名的支持目前已经中断，因此在使用Windows

2003 域控制器时，您可能需要关闭此选项。缺省状态下为 yes

client ntlmv2 auth：该参数确定是否将尝试使用 NTLMv2 加密的密码响应向服务

器验证自己。

如果启用，只会发送 NTLMv2 和 LMv2 响应(两者都比以前的版本安全得多)。

许多服务器(包括 NT4 < SP4、Win9x 和 Samba 2.2)不兼容 NTLMv2。类似地，如果

启用，NTLMv1、客户端 lan 认证和客户端明文认证将被禁用。这还禁用共享级身

份验证。

如果禁用，客户端将发送一个 NTLM 响应(也可能是一个 LANMAN 响应)，这

取决于客户端 LANMAN 权限的值。

请注意，一些站点(特别是那些遵循“最佳实践”安全策略的站点)只允许 NTLMv2

响应，而不允许较弱的 LM 或 NTLM。缺省情况下为禁用

template homedir：当填写 Windows NT 用户的用户信息时，winbindd(8)守护进程

使用此参数填写该用户的主目录。如果字符串%D 存在，它将被替换为用户的

windowsnt 域名。如果字符串%U 存在，它将被替换为用户的 Windows NT 用户名。

template shell：当为 Windows NT 用户填写用户信息时，winbindd(8)守护进程使用此参数为该用户填写登录 shell。

winbind use default domain：该参数指定 winbindd(8)守护进程是否应该在用户名

中没有域组件的用户上运行。没有域组件的用户被视为 winbind 服务器自己域的

一部分。虽然这对 Windows 用户没有好处，但它使 SSH、FTP 和电子邮件功能在

某种程度上更接近于它们在本地 unix 系统中的功能。缺省状态下为 NO

winbind enum users：在使用 winbind(8)的大型安装中，可能需要通过系统调用的

setpwent()、getpwent()和 endpwent()组来抑制用户枚举。如果 winbind enum users

参数为 no，调用 getpwent 系统调用将不会返回任何数据。关闭用户枚举可能会

导致某些程序的行为异常。例如，手指程序在搜索匹配的用户名时依赖于能够访

问完整的用户列表。缺省状态下为 yes

winbind enum groups：在使用 winbind(8)的大型安装中，可能需要通过系统调用

的 setgreent()、getgreent()和 endgreent()组来抑制组的枚举。如果 winbind enum

groups 参数为 no，调用 getgrent()系统调用将不会返回任何数据。关闭组枚举可

能导致某些程序的行为异常。缺省状态下为 yes

encrypt passwords：这个布尔型值控制着是否与客户端用加密口令进行交谈，缺

省状态下为 yes