**构力云·AD域**

**搭建使用教程**

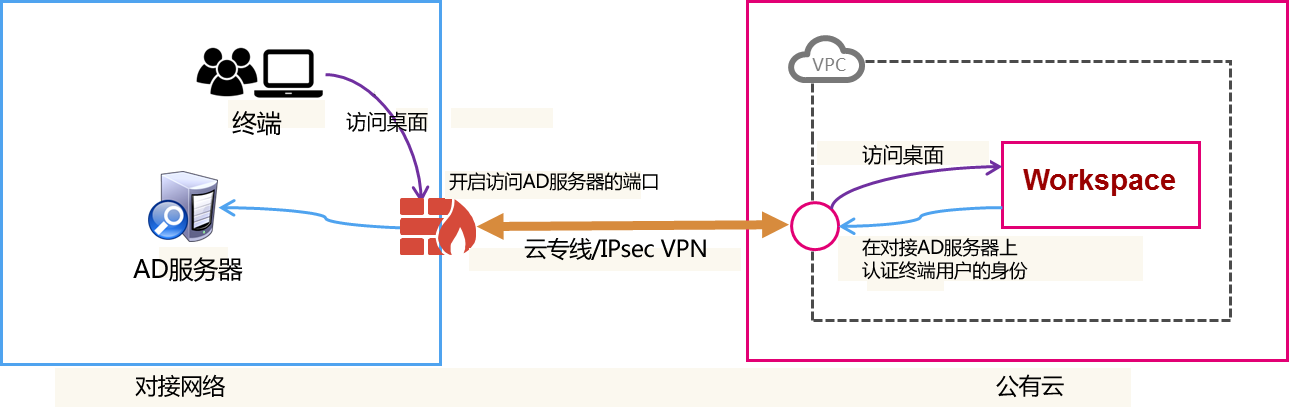
https

2019/04/04

@北京构力科技有限公司·前沿技术中心

优先参考华为官方教程《Workspace如何对接微软AD》

[**https://support.huaweicloud.com/usermanual-workspace/zh-cn\_topic\_0034938623.html**](https://support.huaweicloud.com/usermanual-workspace/zh-cn_topic_0034938623.html)



目录

[1 创建ECS 4](#_Toc5261763)

[2 修改服务器名及计算机名 4](#_Toc5261764)

[3 安装AD域服务 5](#_Toc5261765)

[4 打开相关服务 5](#_Toc5261766)

[5 SSL证书服务及自签署证书 6](#_Toc5261767)

[6 服务器安全组 7](#_Toc5261768)

[7 测试 7](#_Toc5261769)

[8 搭建AD辅域，构建AD主从（可选） 10](#_Toc5261770)

[8.1 **配置主域(计算机名ad)** 10](#_Toc5261771)

[8.2 配置从域(计算机名为ad-backup)加入主域(ad) 13](#_Toc5261772)

[9 使用云桌面连接自建AD域 8](#_Toc5261773)

[10 附录-AD域组织架构及华为组织架构 9](#_Toc5261774)

[11 **管理AD用户及基本操作(重置密码，禁用解禁，新建组织用户等)** 9](#_Toc5261775)

[11.1 AD管理中心 9](#_Toc5261776)

[12 更新密码组策略 10](#_Toc5261777)

# 创建ECS



# 修改服务器名及计算机名

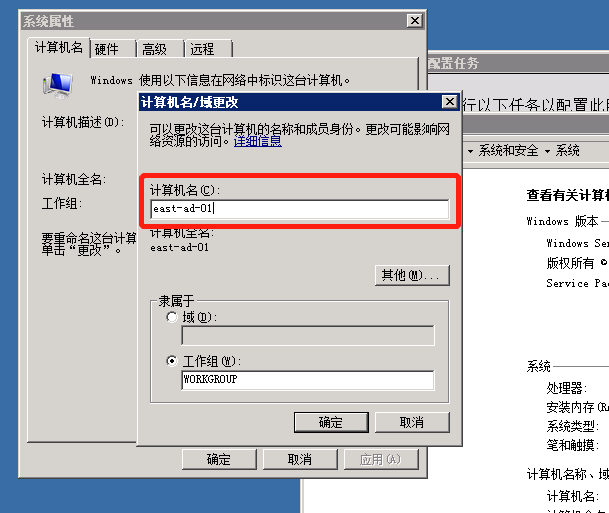
修改计算机名方便识别

* 使用华为远程登录 或者 mstsc远程桌面登录ECS



* 修改计算机名，如华东区Ad服务器及计算机名可命名为east-ad-01





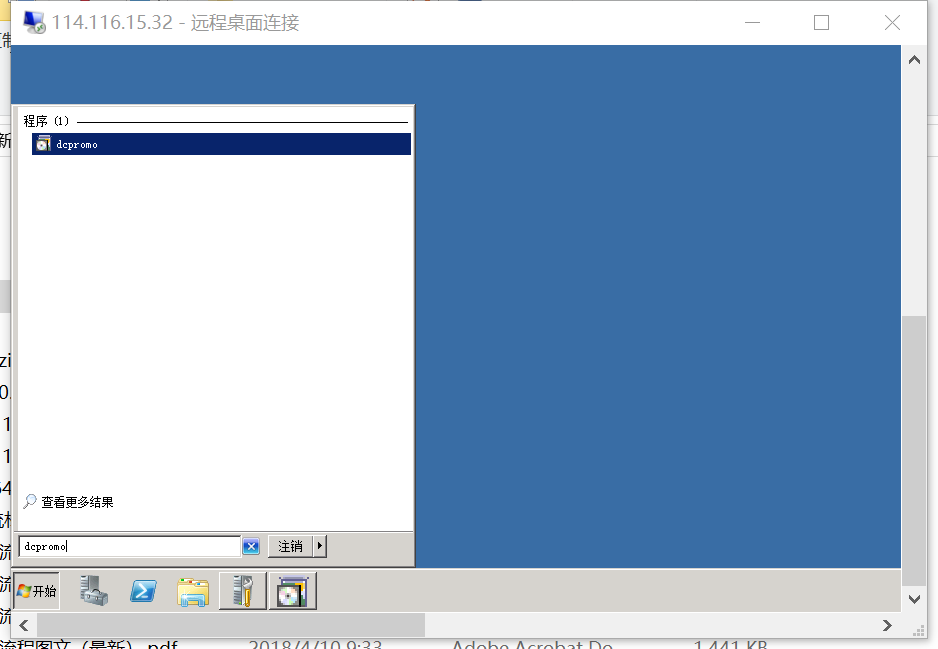
# 安装AD域服务

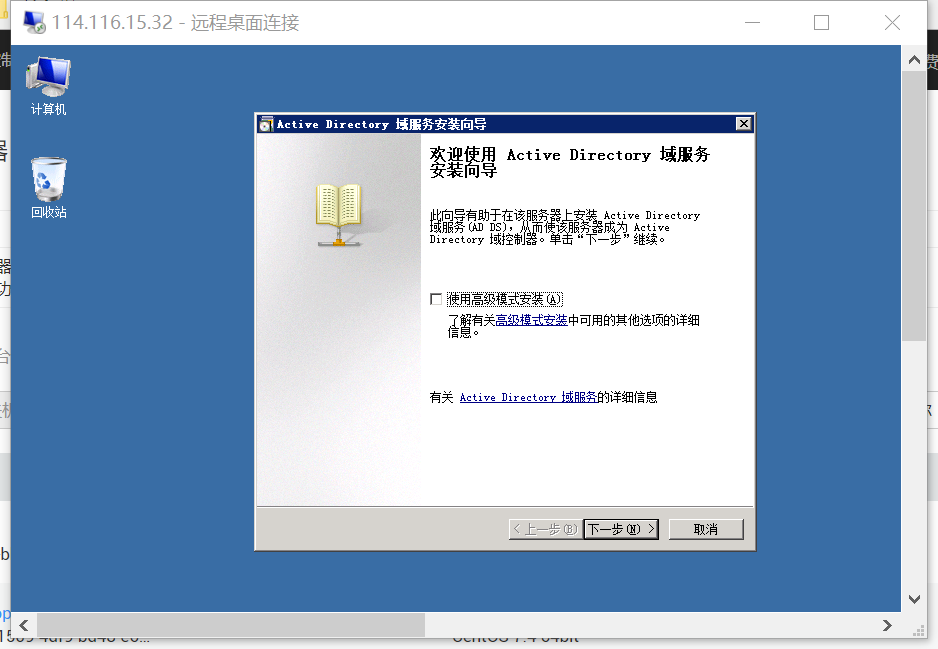
教程

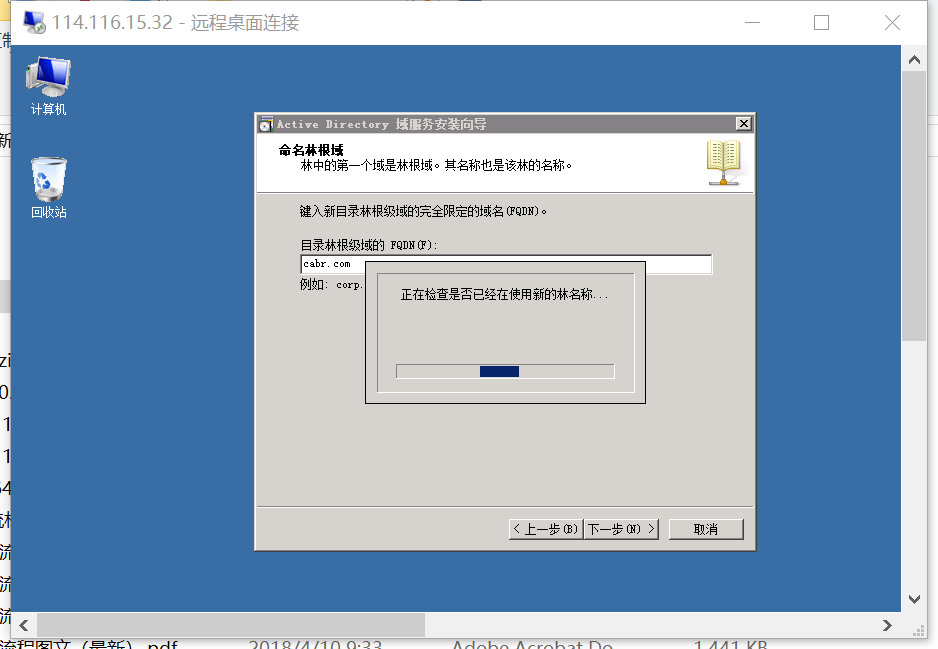
<https://jingyan.baidu.com/article/3c48dd3491921fe10be35839.html>

略过第一步ip地址设置，采用默认值即可

注意！同一区域属于同一VPC（VPC可理解为同一局域网），因而在同一区域同一VPC下，即使项目不同，目录林根目录也不能相同 如根目录pkpm.com只能存在一个

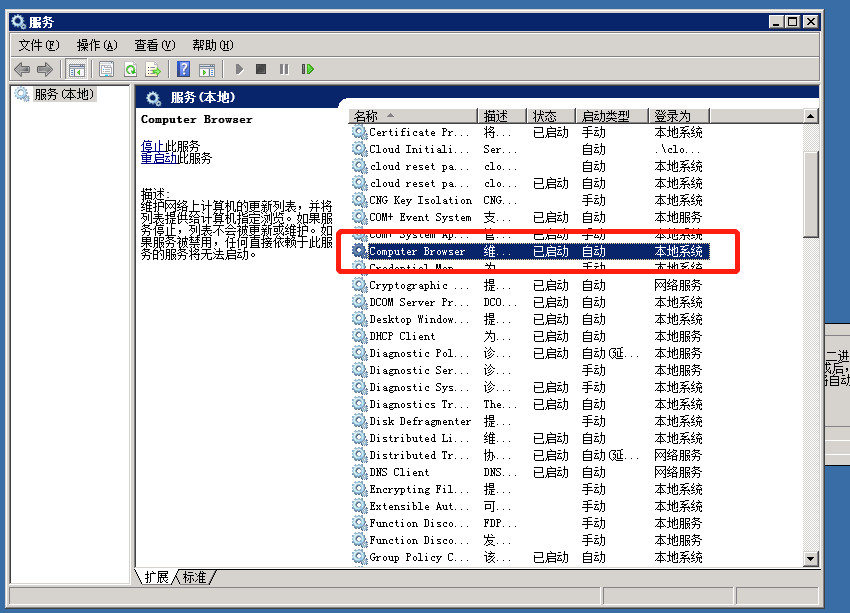






# 打开相关服务

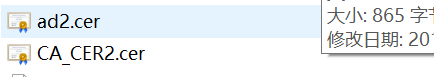
* Computer Browser
* Workstation
* Remote Procedure Call (RPC)
* TCP/IP NetBIOS Helper
* DNS client



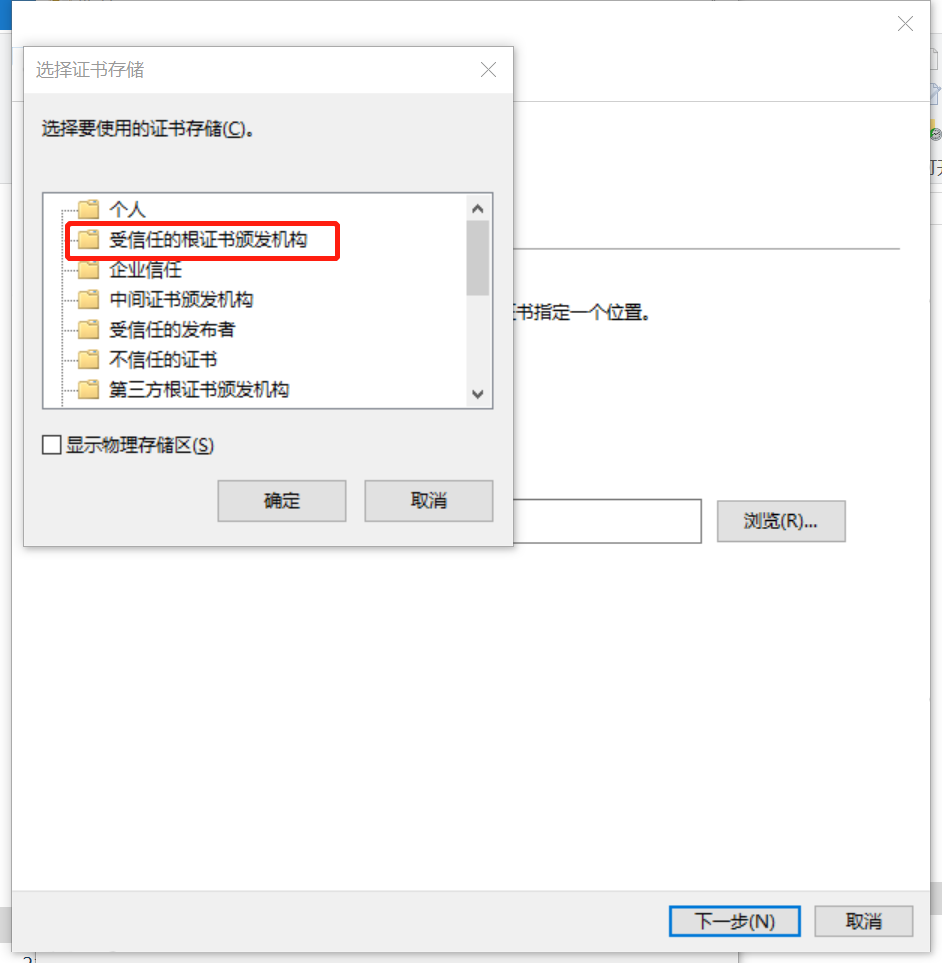
# SSL证书服务及自签署证书

参照文章到第五步，将两个证书复制到本地

<https://yq.aliyun.com/articles/118657?t=t1>



CA\_CER2.cer为根证书；



# 服务器安全组

修改ECS服务器安全组策略**389 636**端口的入方向出方向

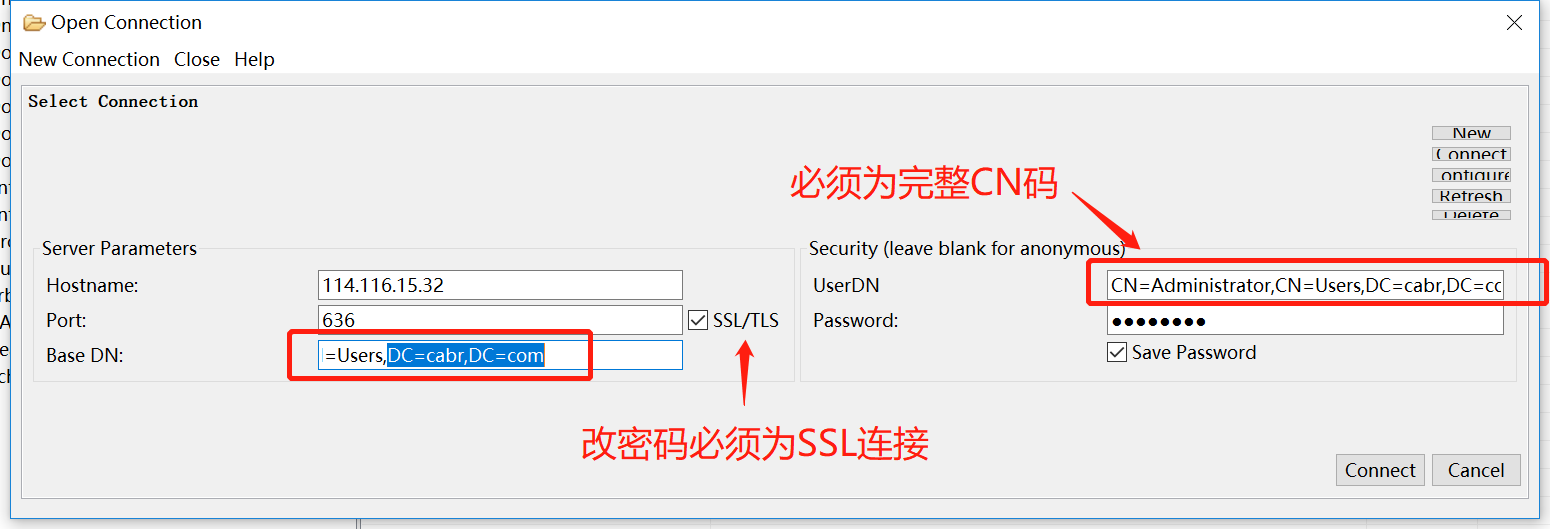
以及下面文章规定的**所有端口**

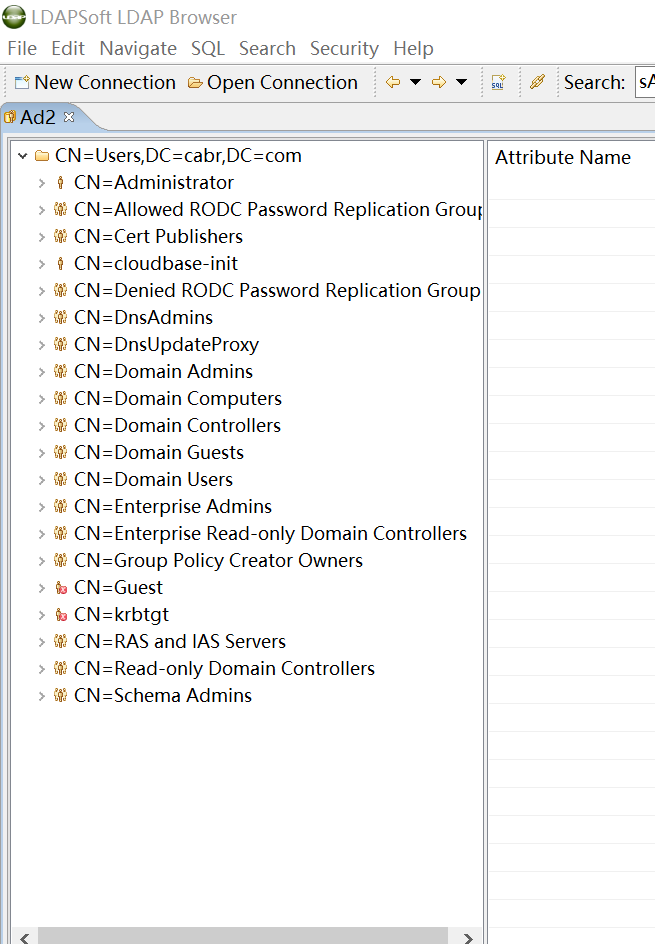
或者添加入方向ANY端口，开放所有端口

<https://support.huaweicloud.com/usermanual-workspace/zh-cn_topic_0034938623.html>

# 测试

使用LDAP Connection





能够成功读取结果，则证明AD域创建成功

# 使用云桌面连接自建AD域

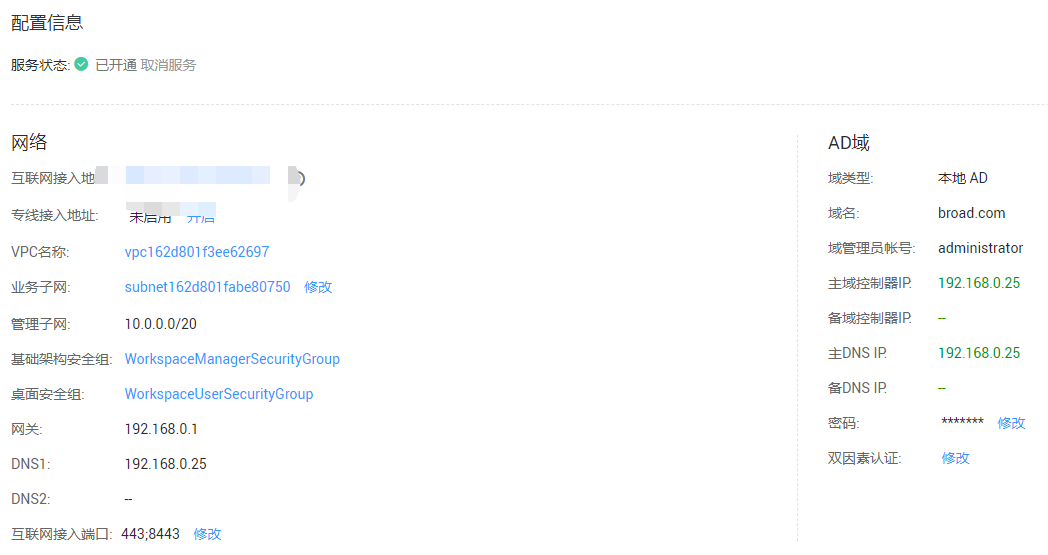
选择云桌面选项卡，点击创建云桌面服务



输入主域的IP地址和DNS(内网地址)

输入从域的IP地址和DNS(内网地址)(如果搭建了AD主从)

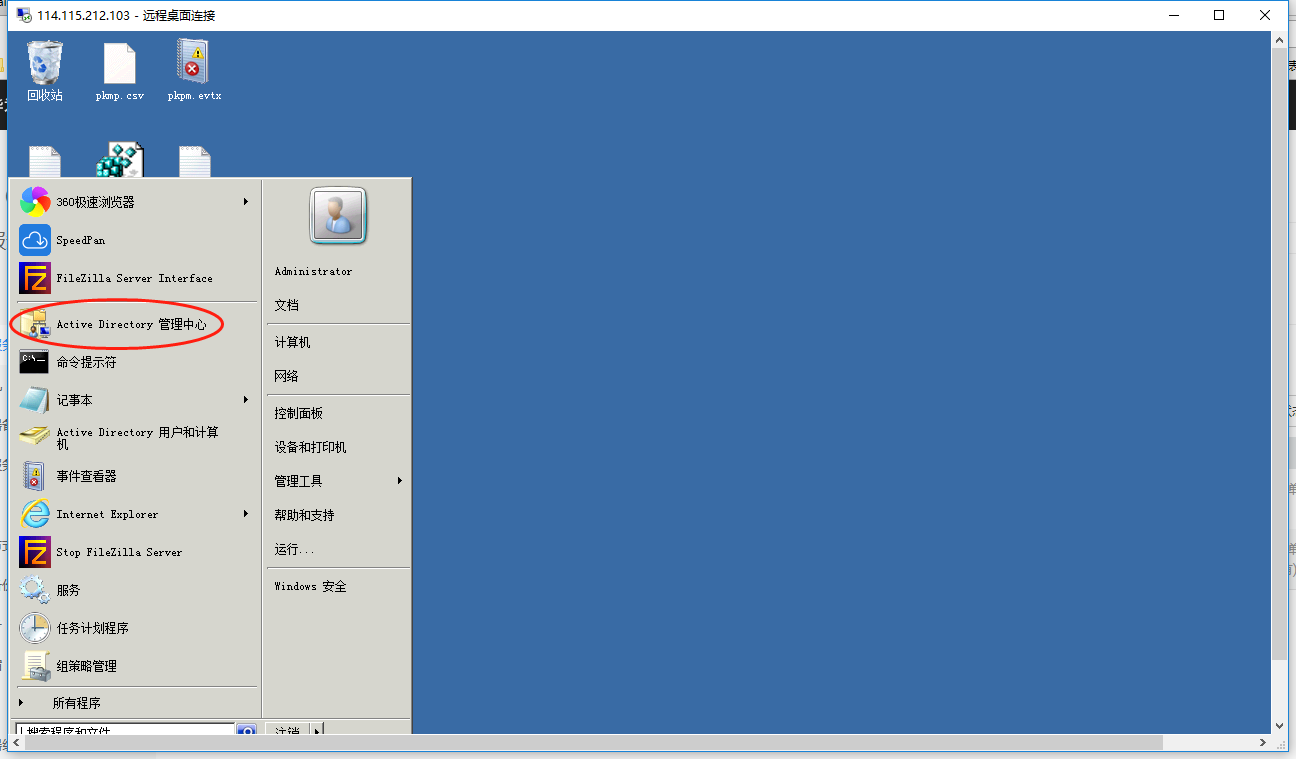
等待一段时间后，云桌面服务开通则成功

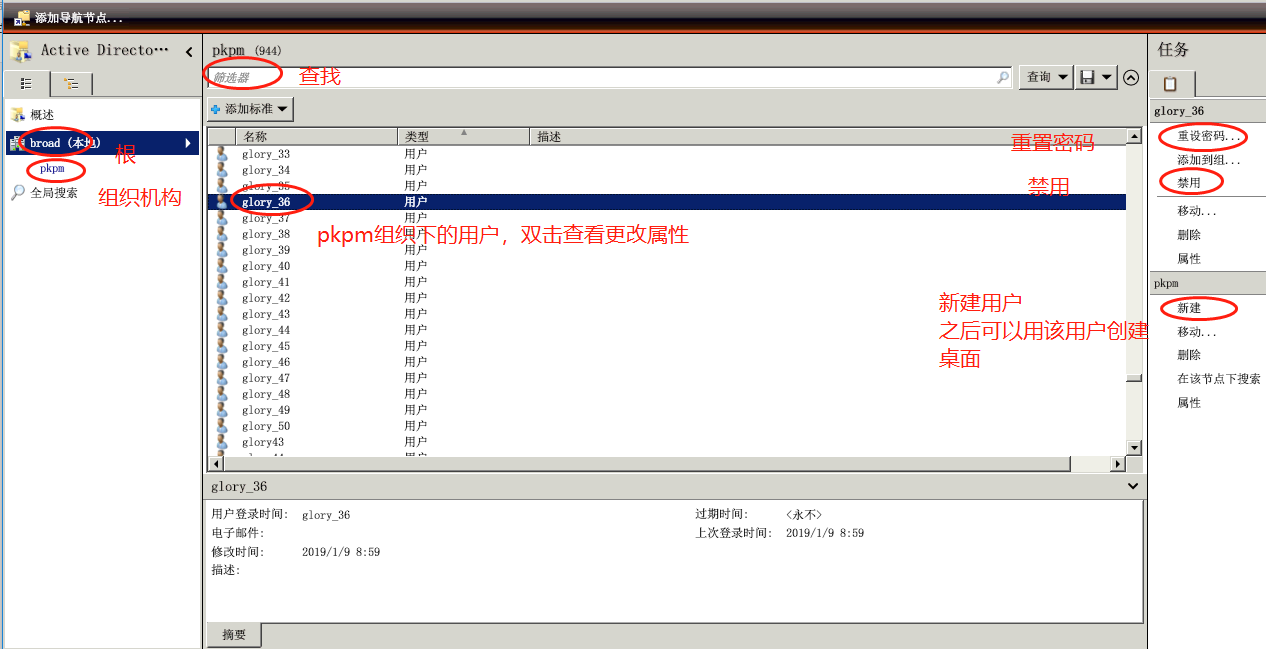


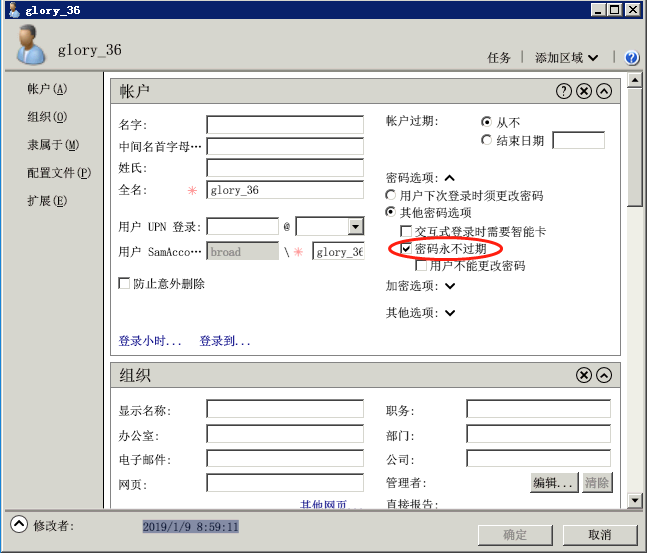
云桌面服务开通成功，证明云桌面服务与AD域互通成功

# 管理AD用户及基本操作(重置密码，禁用解禁，新建组织用户等)

## AD管理中心







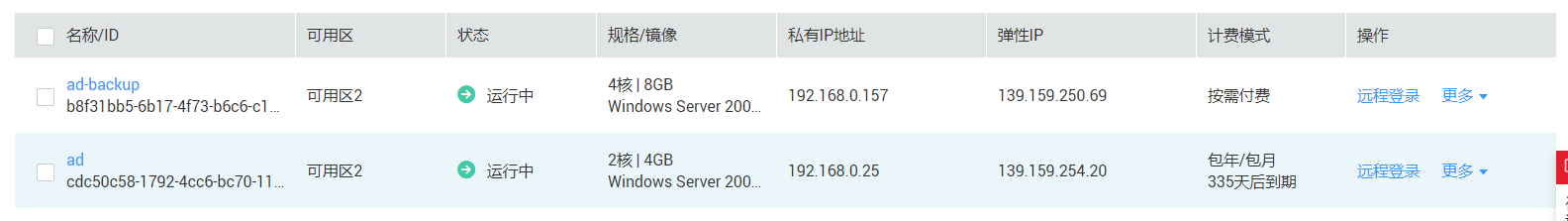
# 更新密码组策略

更新密码组策略 类似密码长度 密码过期时间等

<https://www.cnblogs.com/sjdn/p/5379034.html>

# 搭建AD辅域，构建AD主从（可选 可选 可选）

参考教程<http://www.cnblogs.com/zoulongbin/p/6013609.html>



新建另外一台WindowsServer2008操作系统，系统名ad-backup

|  |  |  |
| --- | --- | --- |
| 角色 | 计算机名 | 内网ip |
| 主域 | ad | 192.168.0.25 |
| 从域 | ad-backup | 192.168.0.157 |

## 配置主域(计算机名ad) 云桌面一个AD域 是否需要从看需求

登陆主域ECS，此时是**主域**！！！

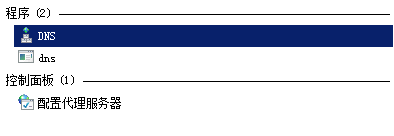
确保**三个服务**已开启；

**安全组**所需端口均已打开

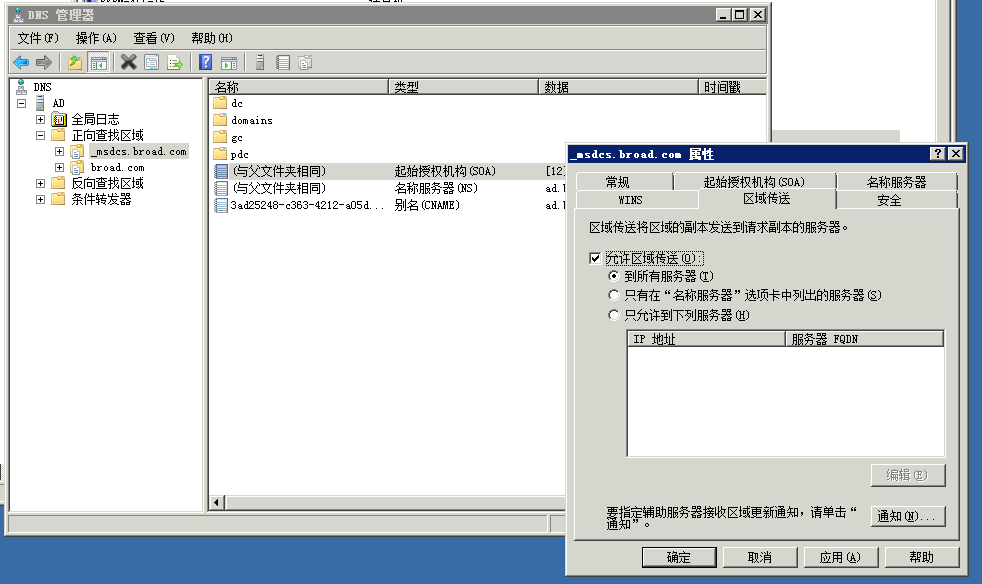
ping broad.com 可以显示自己的ip，证明DNS配置成功

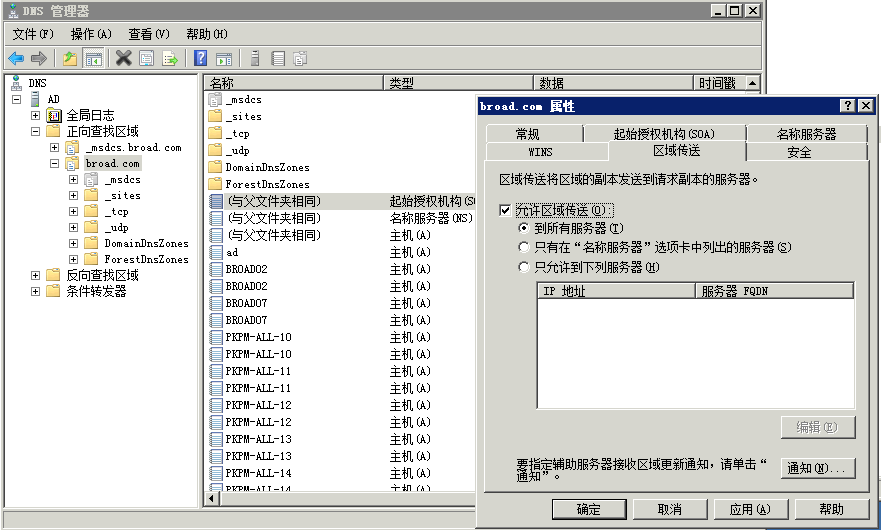


开始-》输入DNS 打开**DNS服务器设置**

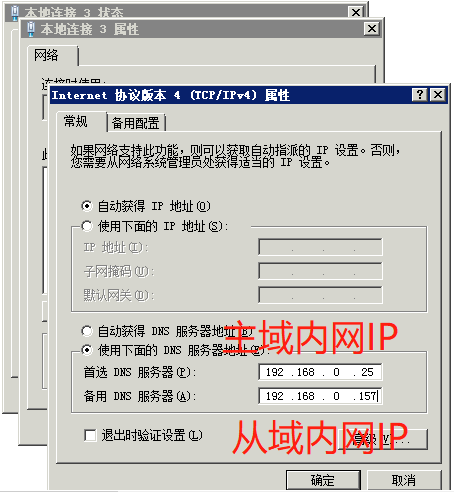


区域传送设置为允许区域传送到所有服务器(两个都要设置)





DNS添加从域ip 使得主域可以连接从域



## 配置从域(计算机名为ad-backup)加入主域(ad)

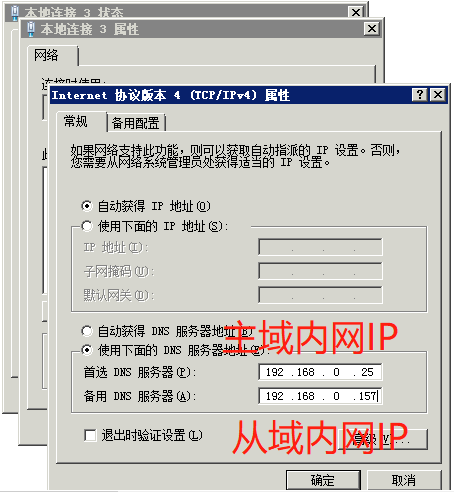
登陆从域ECS，注意下列操作是针对**从域ECS**

确保**三个服务**已开启；

**安全组**所需端口均已打开

并配置DNS

DNS设置为



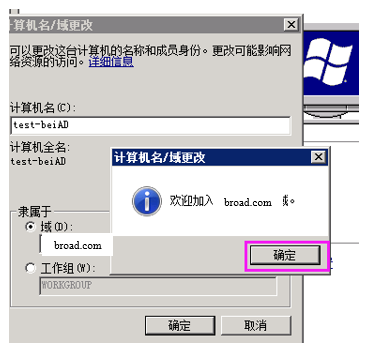
ping broad.com 可以显示主域的ip，证明从域和主域连接成功



首先从域ECS加入主域ECS

计算机-右键属性-高级系统设置-更改计算机名

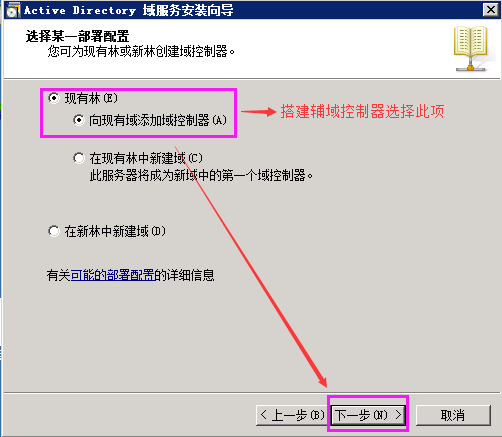
域 broad.com 输入Administrator/主域密码

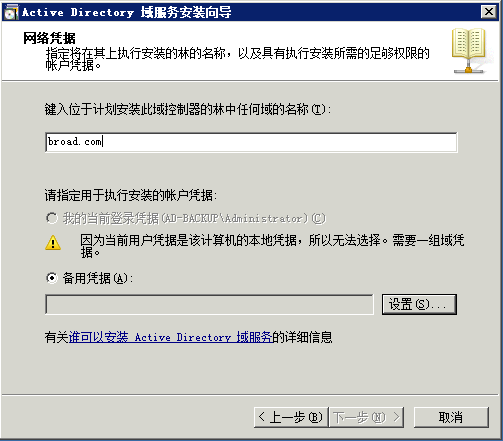




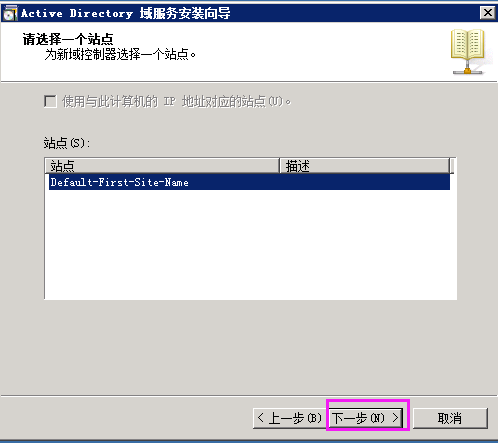
重启后，可以发现从域ECS已加入主域

运行-输入dcpromo

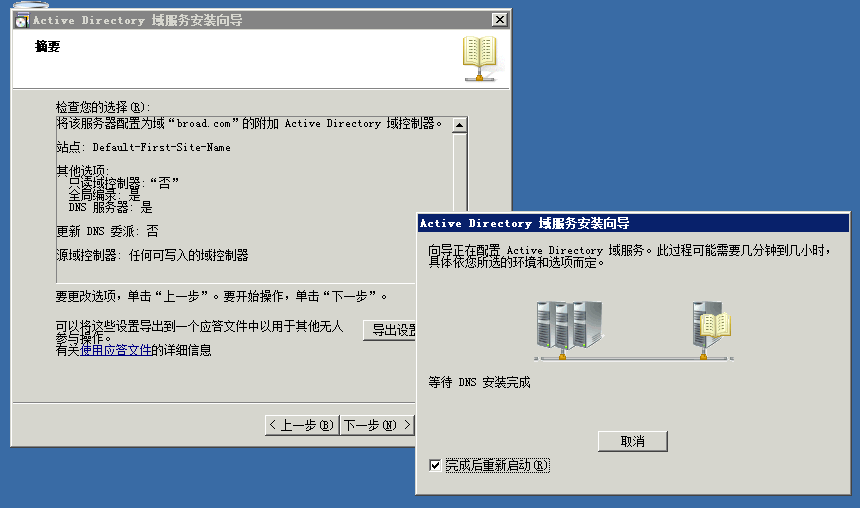




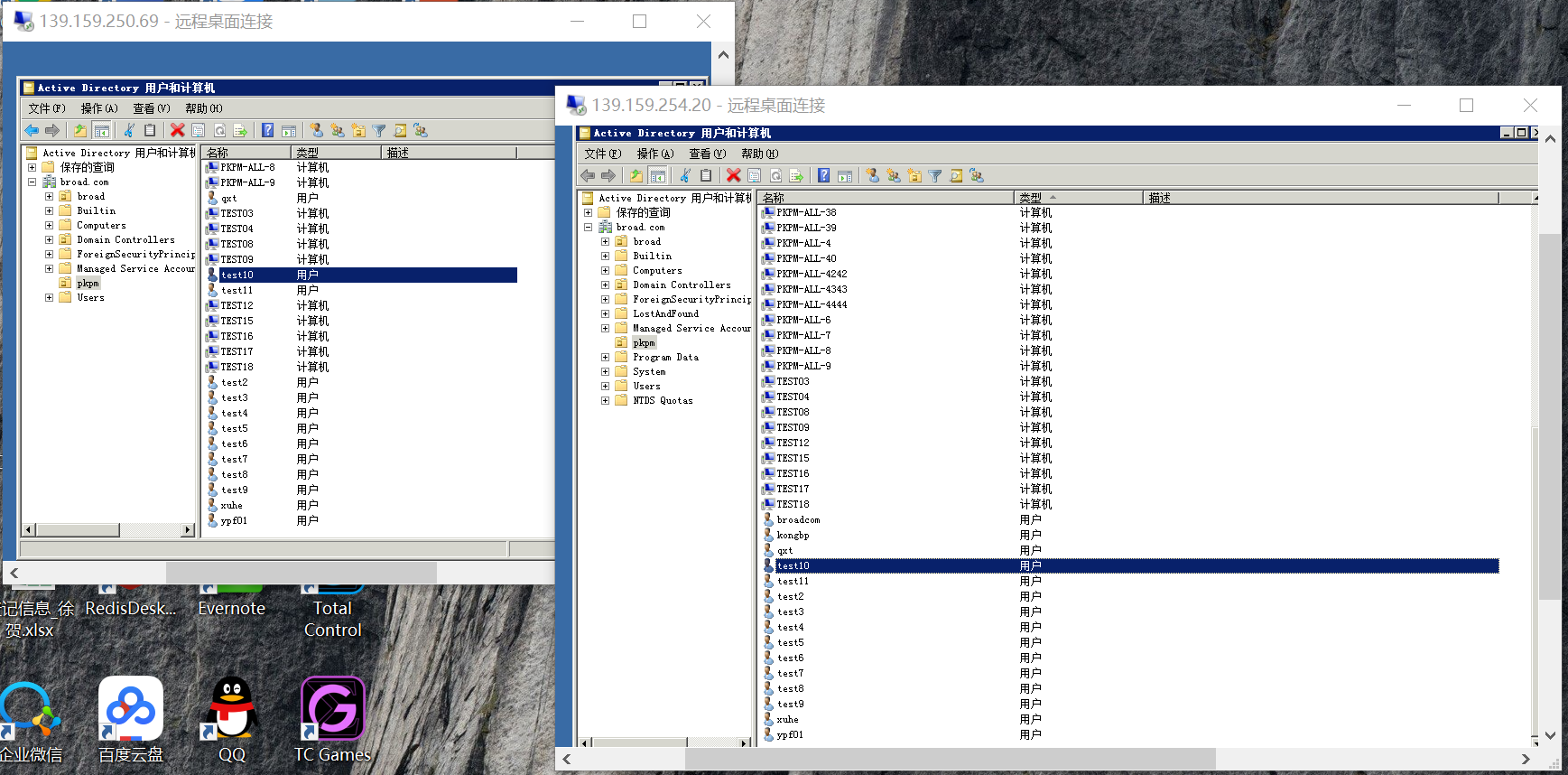
备用凭据输入之前登陆的用户名密码



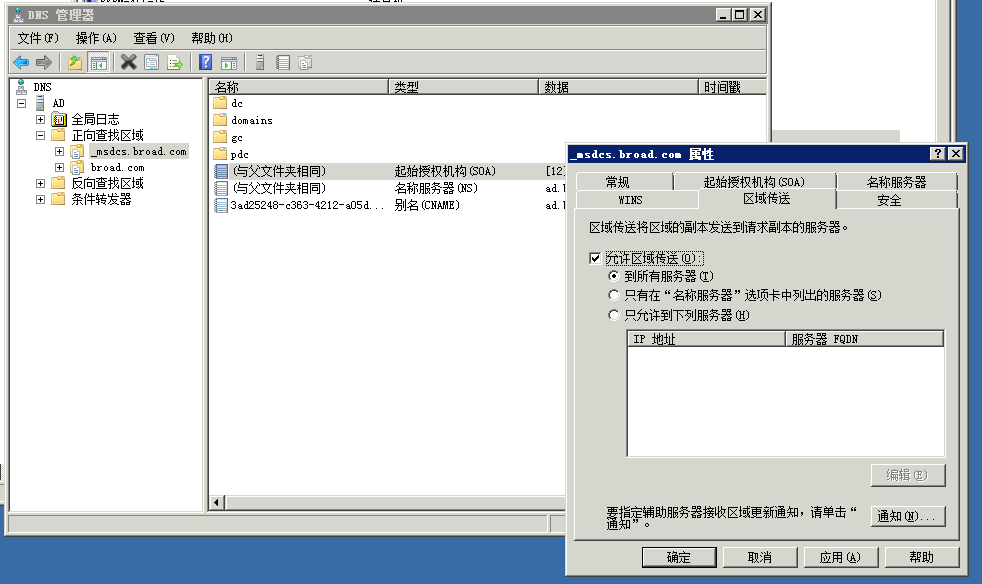
勾选DNS服务器和全局编录

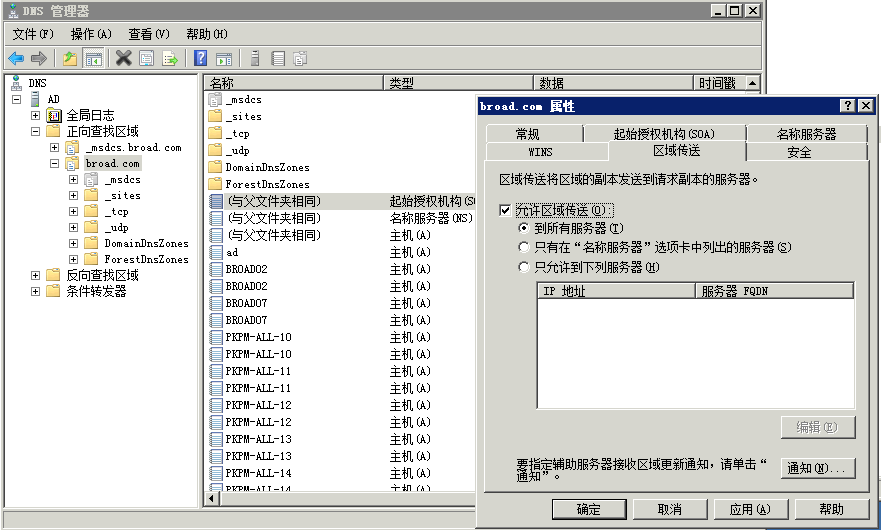


主备后，向AD主域添加用户test10用户，该用户则会自动同步到AD从域，反之亦可。

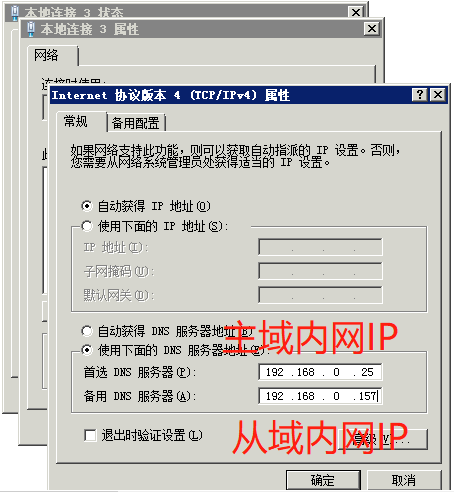


区域传送设置为允许区域传送到所有服务器(都要设置)，实现与**主AD双向同步**





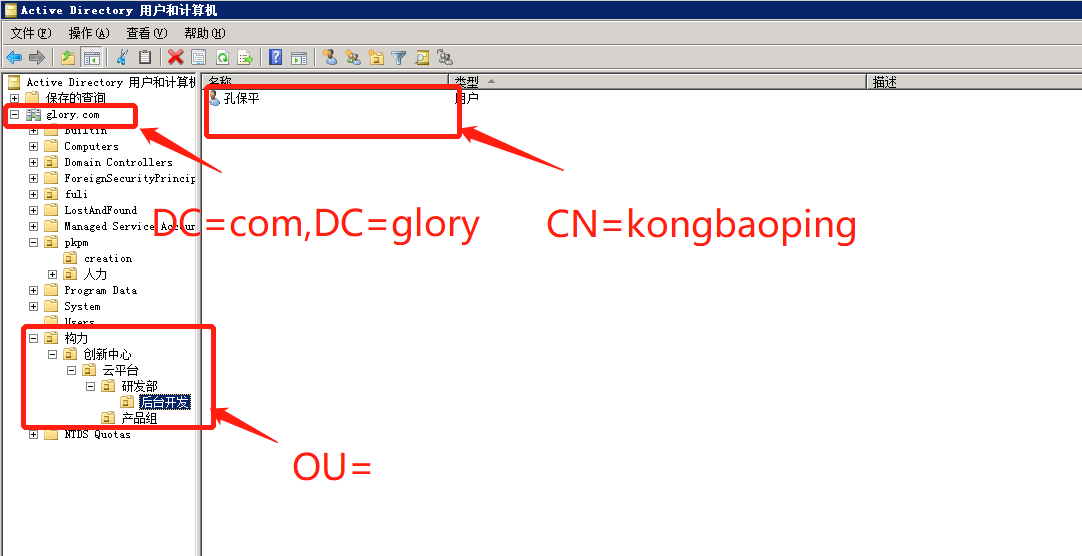
安装ad域会清空ECS的DNS配置，请登陆主域从域分别设置DNS（可选）



# 附录-AD域组织架构及华为组织架构

AD域组织分配及华为云桌面对应关系



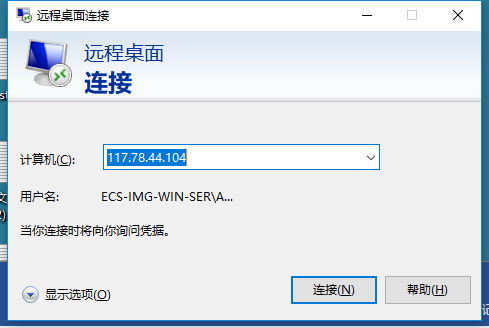
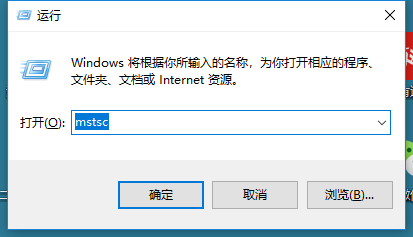


LDAP，每一个用户对应的唯一DN(DistinguishedName)



图形界面操作AD用户

远程桌面登录AD域所在ECS



目前glorycloud下AD地址为114.115.212.103

默认用户名

Broad\Administrator

Abc=1234

如果报用户不存在，可能是缺少域前缀的问题，例如域为BROAD 则登录名为BROAD\Administrator 实际用户可以使用华为控制台VNC登录ECS点击开始查看用户

