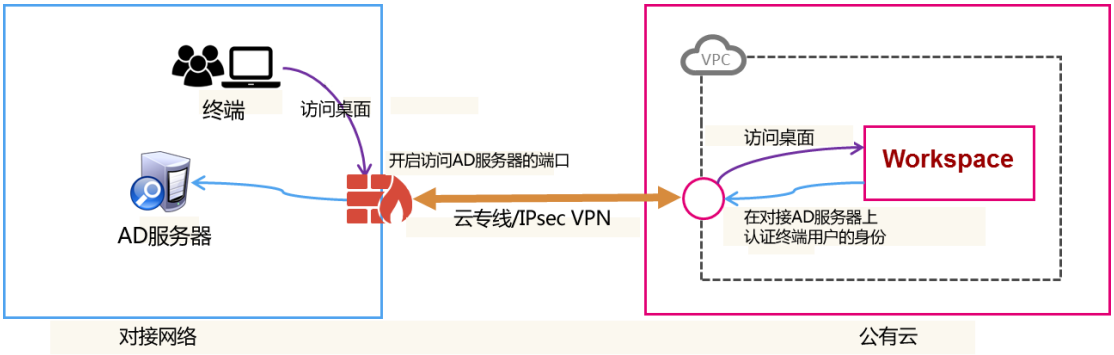
构力云·AD 域
搭建使用教程

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



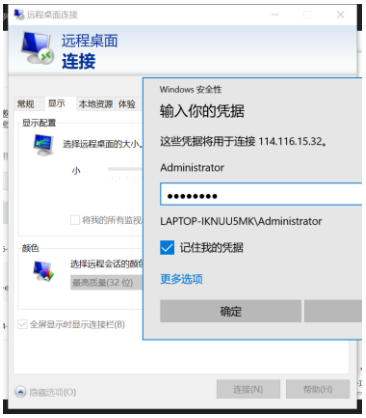
目录

1 创建 ECS

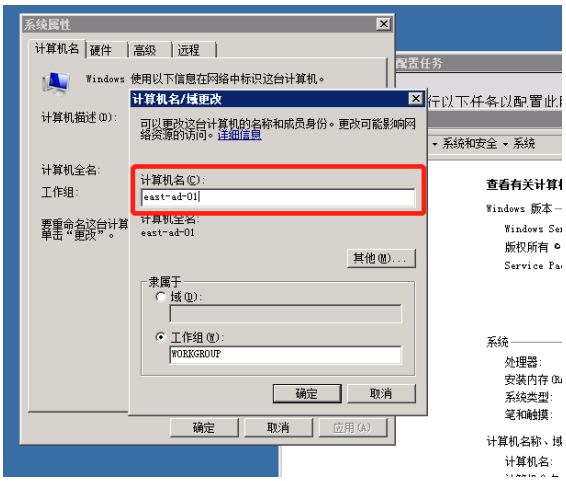
2 修改服务器名及计算机名

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

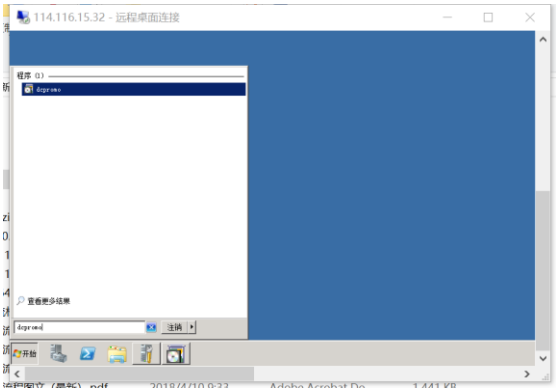


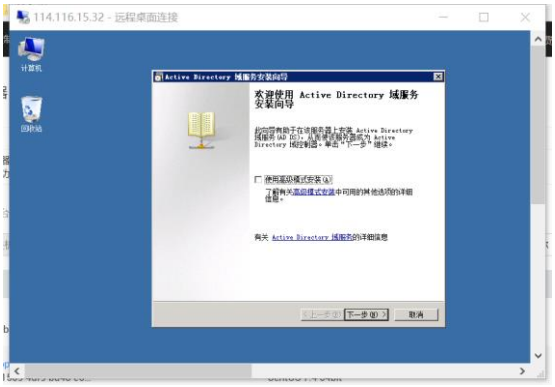
- 修改计算机名，如华东区 Ad 服务器及计算机名可命名为 east-ad-01

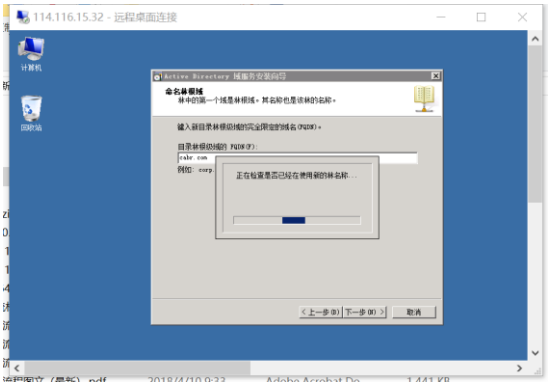


3 安装 AD 域服务

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



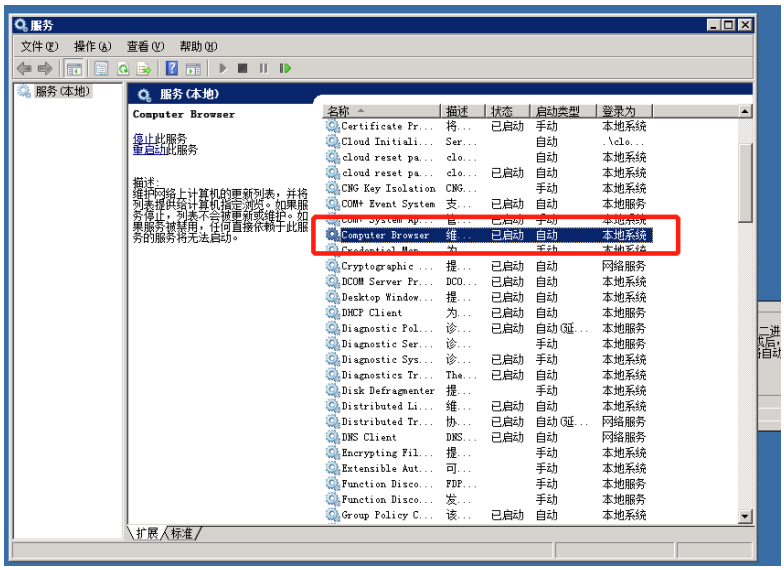




4 打开相关服务

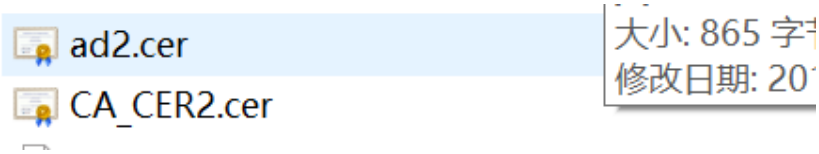
- Computer Browser
- Workstation

- Remote Procedure Call (RPC)
- TCP/IP NetBIOS Helper
- DNS client

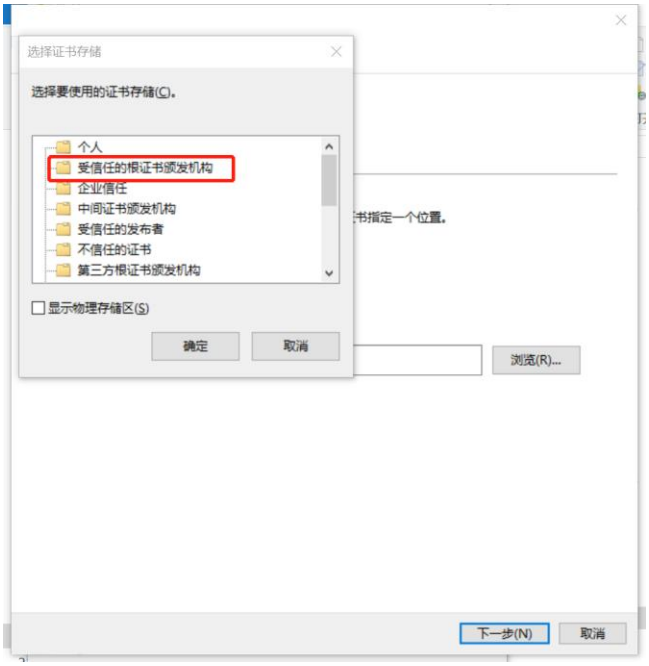


5 SSL 证书服务及自签署证书

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；

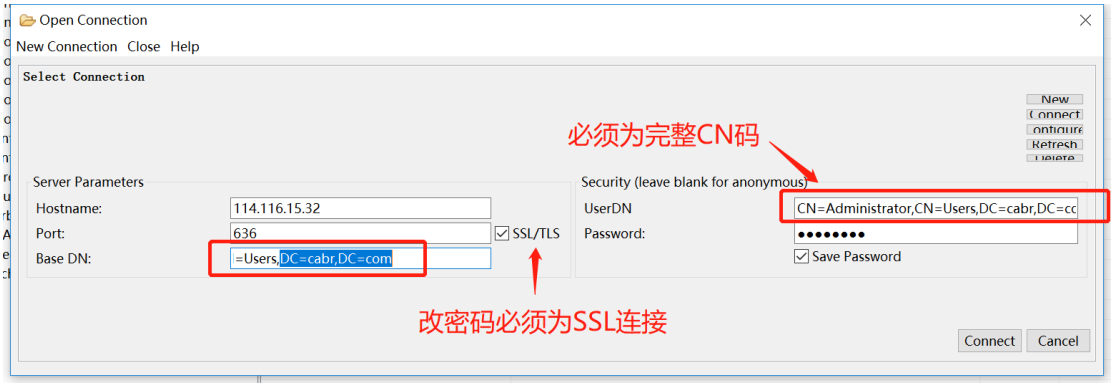


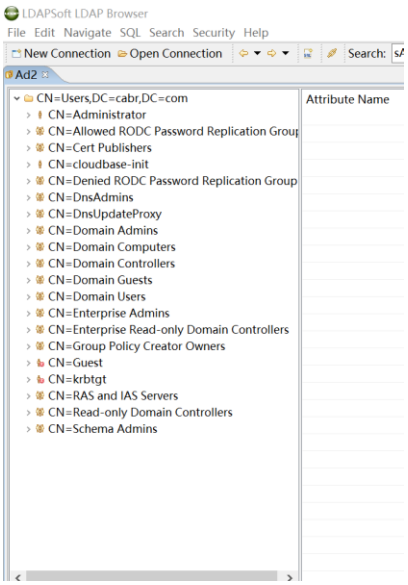
6 服务器安全组

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

7 测试

使用 LDAP Connection



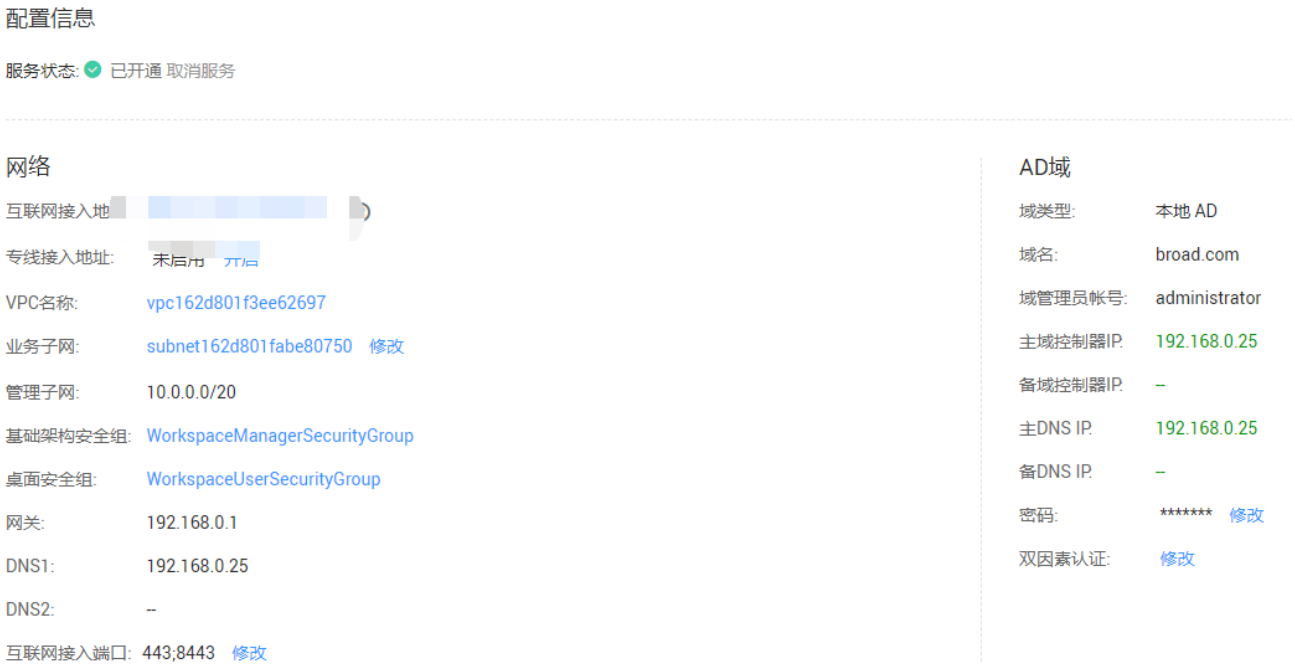


能够成功读取结果，则证明 AD 域创建成功

8 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

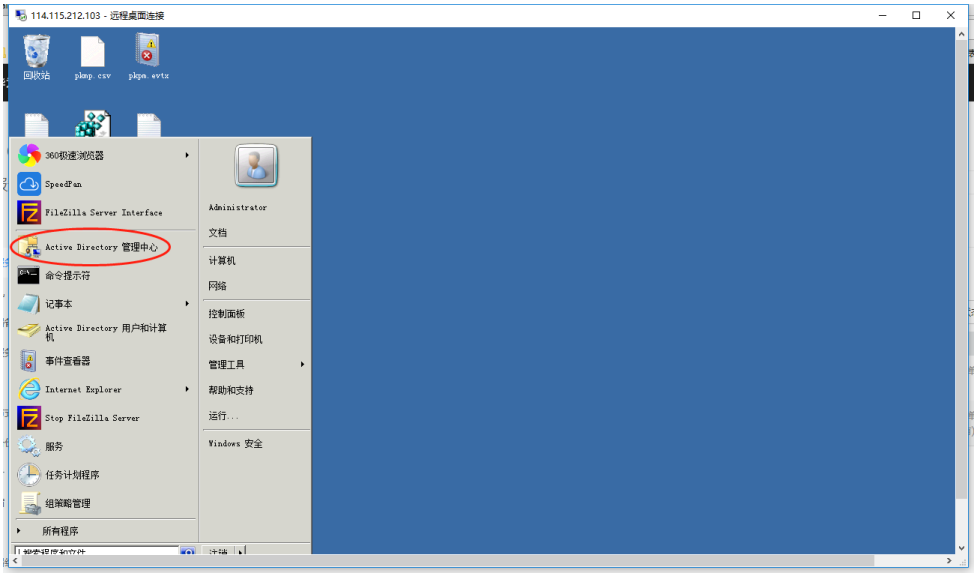
输入主域的 IP 地址和 DNS(内网地址)
输入从域的 IP 地址和 DNS(内网地址)(如果搭建了 AD 主从)
等待一段时间后，云桌面服务开通则成功

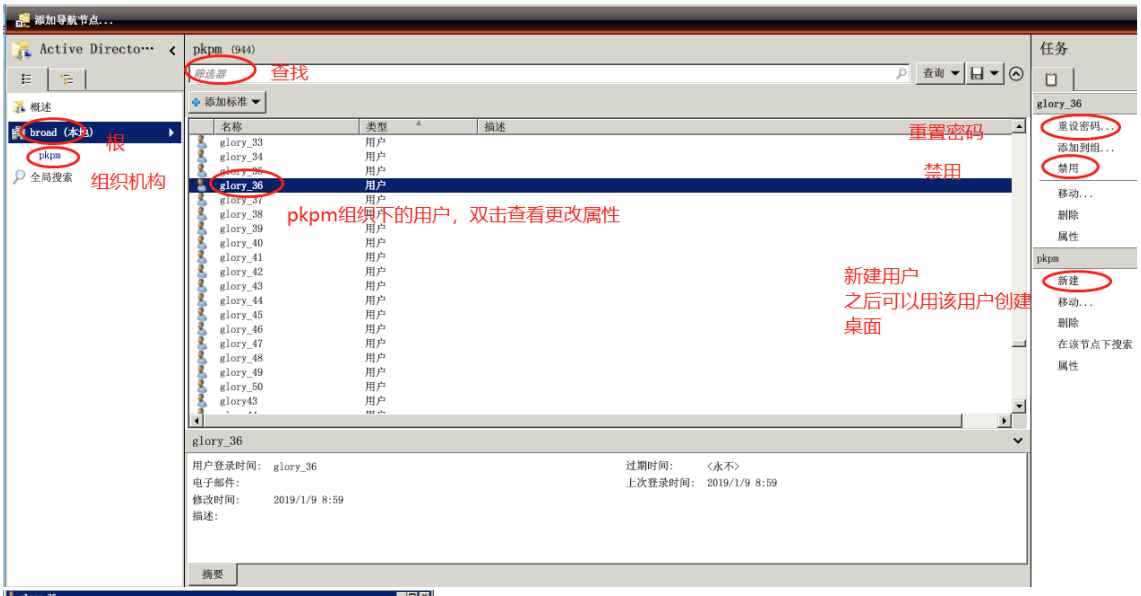


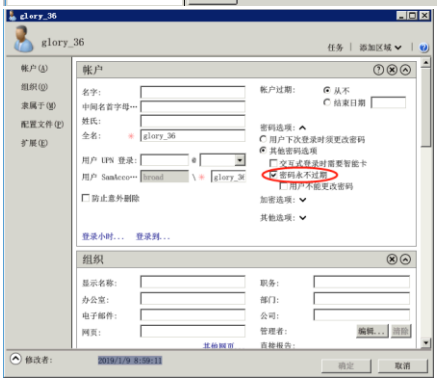
云桌面服务开通成功，证明云桌面服务与 AD 域互通成功

9 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)

9.1 AD 管理中心







10 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

11 搭建 AD 辅域，构建 AD 主从（可选 可选 可选）

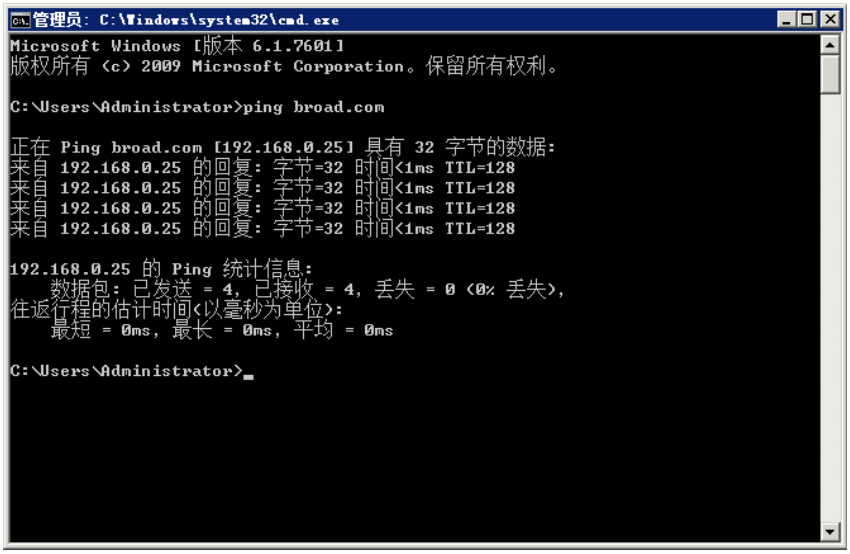
参考教程 http://www.cnblogs.com/zoulongbin/p/6013609.html

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

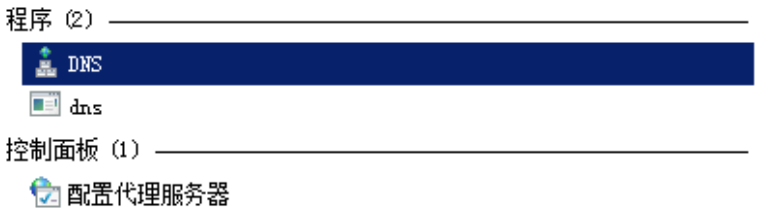
角色	计算机名	内网 ip
主域	ad	192.168.0.25
从域	ad-backup	192.168.0.157

11.1配置主域(计算机名 ad) 云桌面一个 AD 域 是否需要从看需求

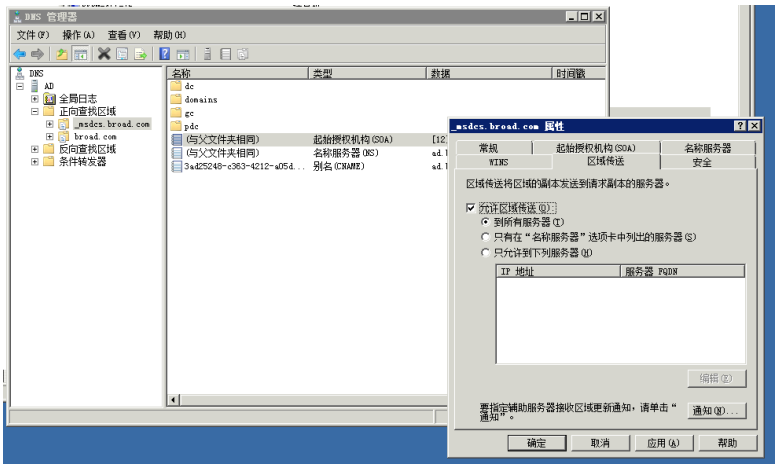
登陆主域 ECS，此时是**主域**！！！
确保**三个服务**已开启；
安全组所需端口均已打开
ping broad.com 可以显示自己的 ip，证明 DNS 配置成功

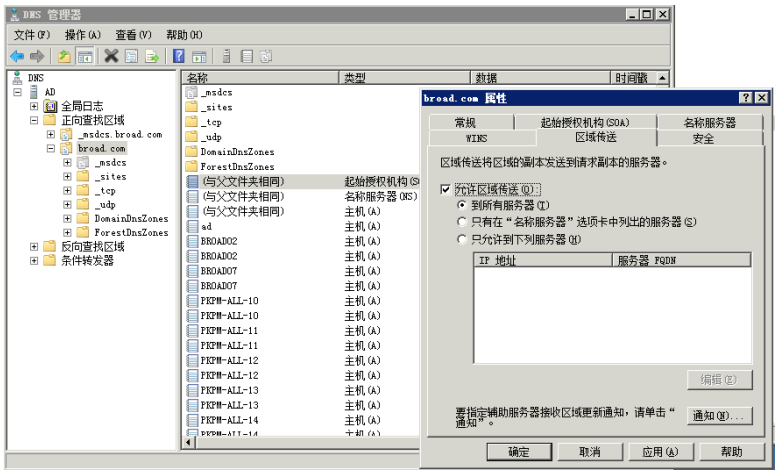


开始-》输入 DNS 打开 **DNS 服务器设置**

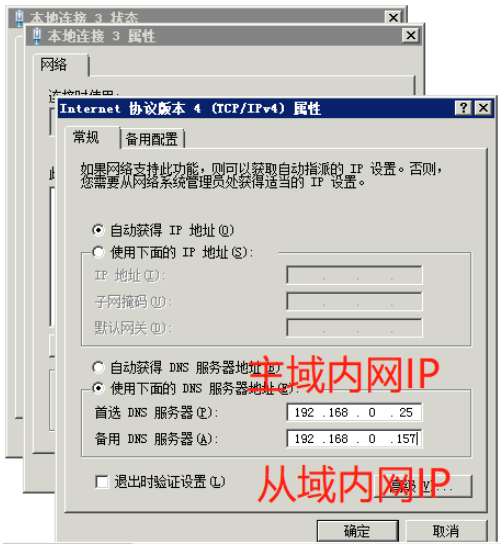


区域传送设置为允许区域传送到所有服务器(两个都要设置)



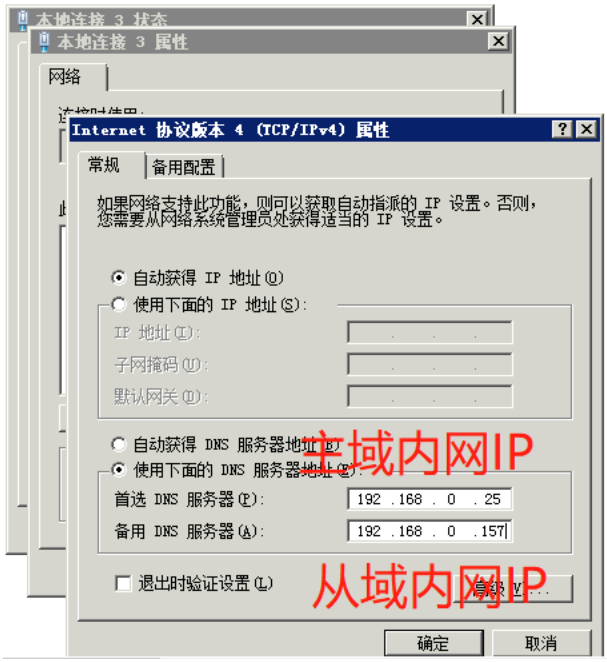


DNS 添加从域 ip 使得主域可以连接从域

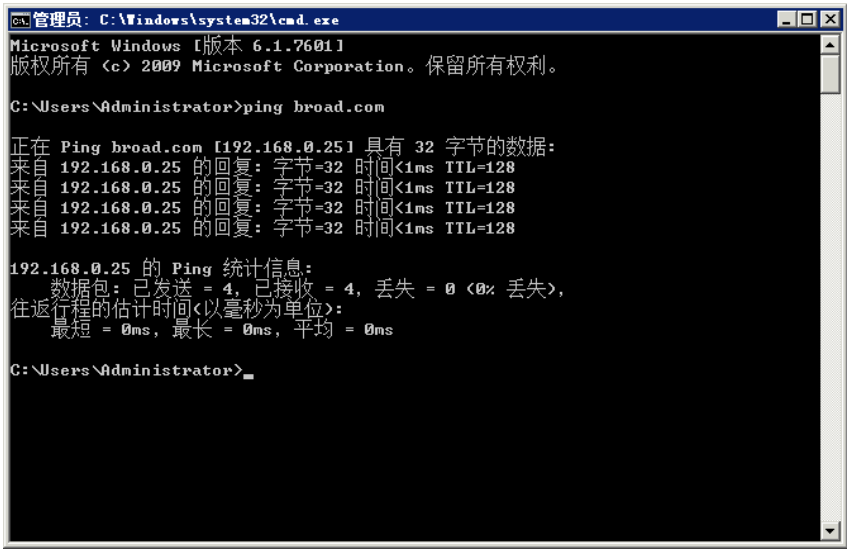

本地连接 3 状态
本地连接 3 属性
网络
Internet 协议版本 4 (TCP/IPv4) 属性
常规
备用配置
如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，
您需要从网络系统管理员处获得适当的 IP 设置。
自动获得 IP 地址(O)
使用下面的 IP 地址(S):
IP 地址(I):
子网掩码(U):
默认网关(D):
自动获得 DNS 服务器地址(B)
使用下面的 DNS 服务器地址(E):
首选 DNS 服务器(P): 192 .168 . 0 . 25
备用 DNS 服务器(A): 192 .168 . 0 .157
退出时验证设置(L)
高级(V)...
确定
取消
主域内网IP
从域内网IP

11.2配置从域(计算机名为 ad-backup)加入主域(ad)

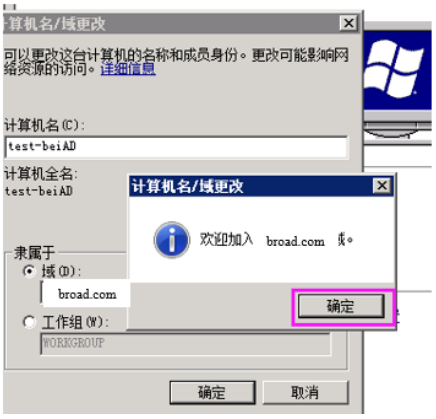
登陆从域 ECS，注意下列操作是针对**从域 ECS**
确保**三个服务**已开启；
安全组所需端口均已打开
并配置 DNS
DNS 设置为



ping broad.com 可以显示主域的 ip，证明从域和主域连接成功

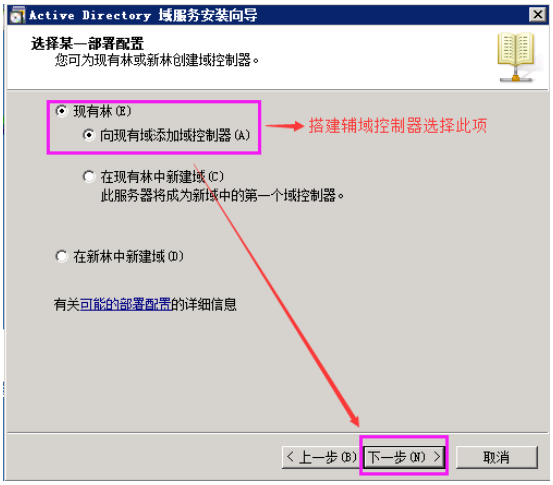


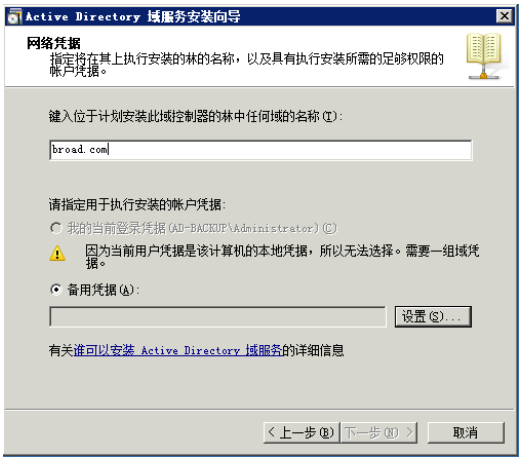
首先从域 ECS 加入主域 ECS
计算机-右键属性-高级系统设置-更改计算机名
域 broad.com 输入 Administrator/主域密码



重启后，可以发现从域 ECS 已加入主域

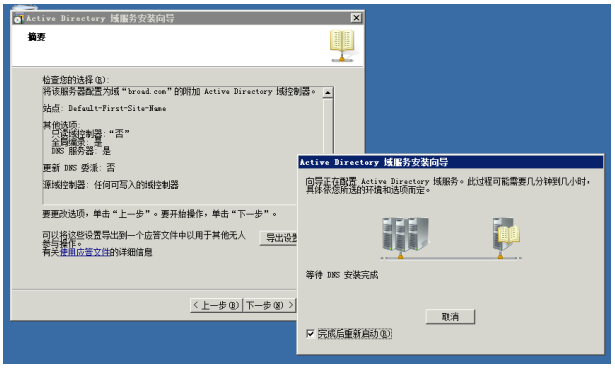
运行-输入 dcpromo



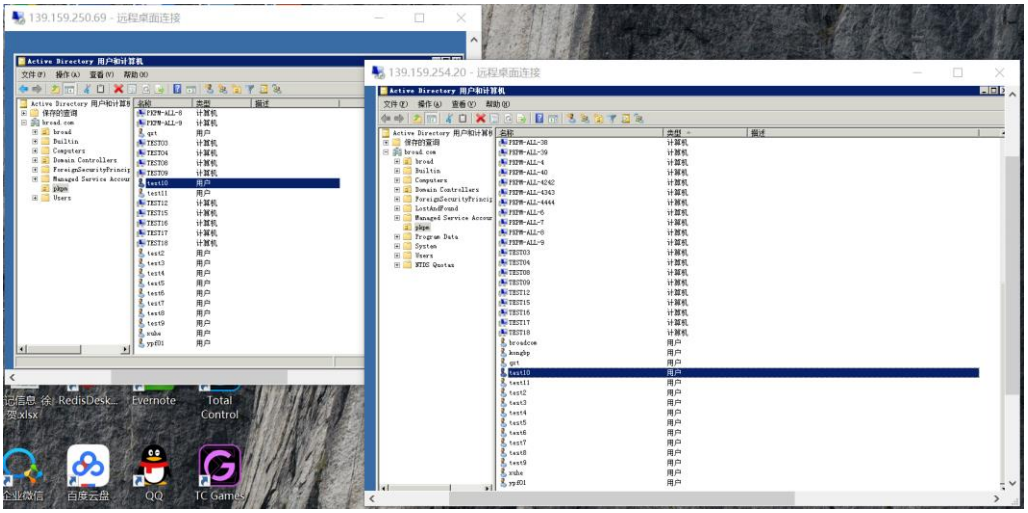


备用凭据输入之前登陆的用户名密码

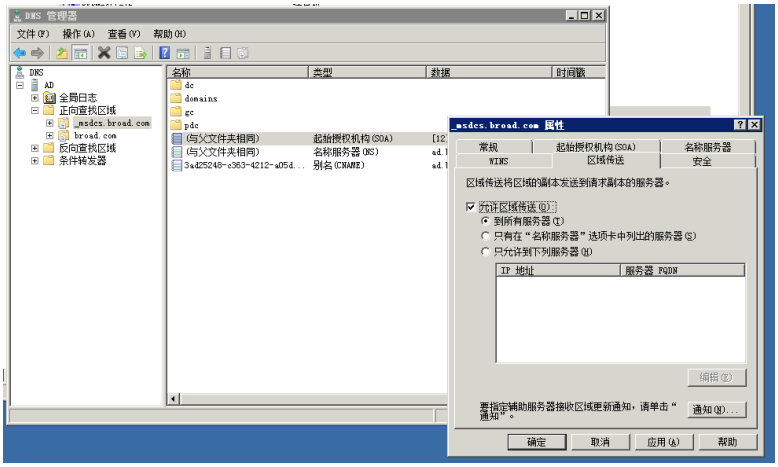
勾选 DNS 服务器和全局编录

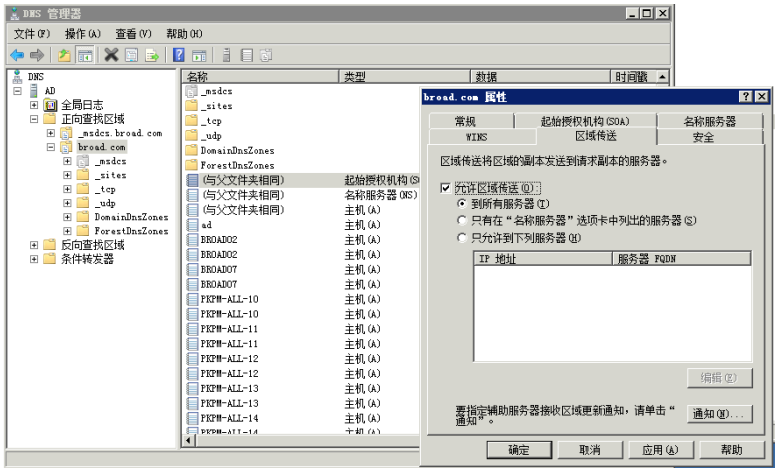


主备后，向 AD 主域添加用户 test10 用户，该用户则会自动同步到 AD 从域，反之亦可。

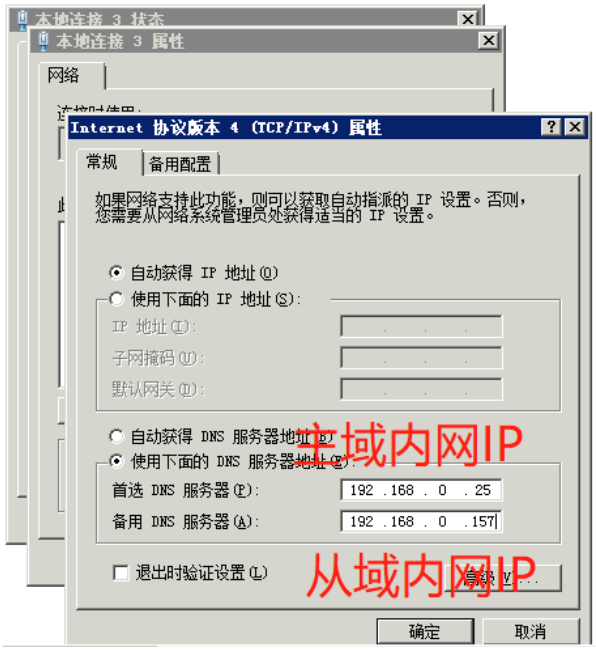


区域传送设置为允许区域传送到所有服务器(都要设置)，实现与**主 AD 双向同步**



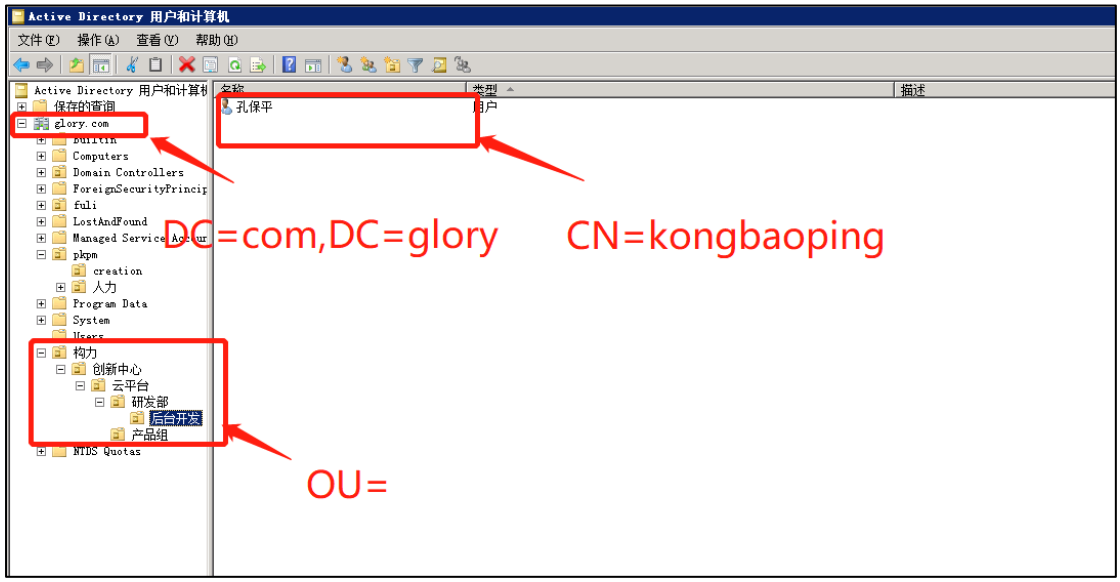


安装 ad 域会清空 ECS 的 DNS 配置，请登陆主域从域分别设置 DNS（可选）



12 附录-AD 域组织架构及华为组织架构

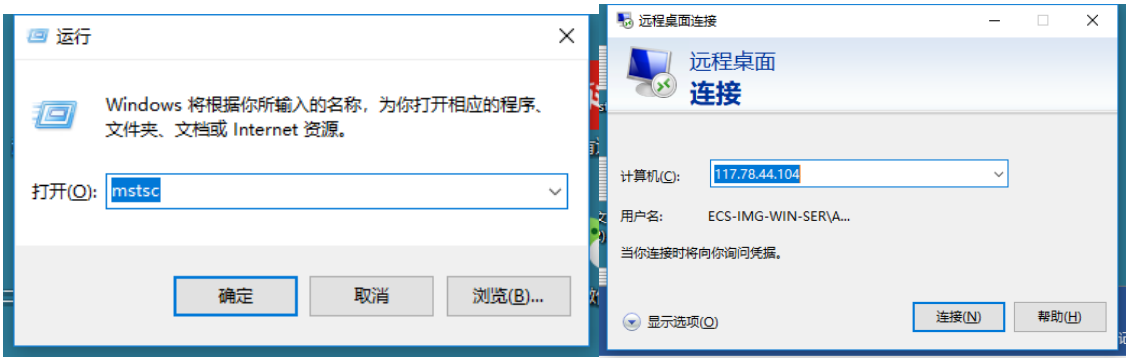
AD 域组织分配及华为云桌面对应关系



LDAP，每一个用户对应的唯一 DN(DistinguishedName)

CN=孔保平,OU=后台开发,OU=研发部,OU=云平台,OU=创新中心,OU=构力,DC=glory,DC=com

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