

构力云·AD 域 搭建使用教程

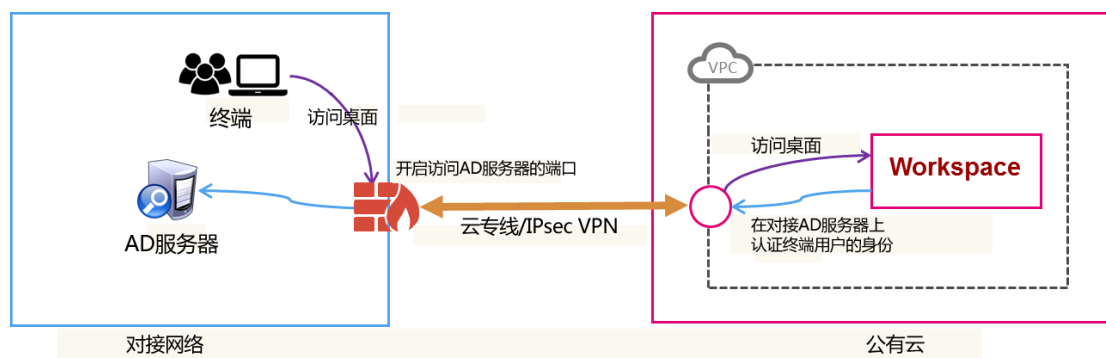


2019/04/04

@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	4
2	修改服务器名及计算机名	4
3	安装 AD 域服务	5
4	打开相关服务	5
5	SSL 证书服务及自签署证书	6
6	服务器安全组	7
7	测试	7
8	搭建 AD 辅域，构建 AD 主从（可选）	10
8.1	配置主域(计算机名 ad)	10
8.2	配置从域(计算机名为 ad-backup)加入主域(ad)	13
9	使用云桌面连接自建 AD 域	8
10	附录-AD 域组织架构及华为组织架构	9
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
11.1	AD 管理中心	9
12	更新密码组策略	10

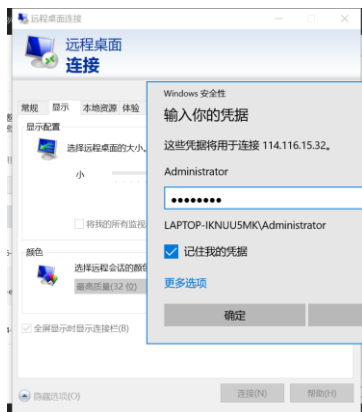
1 创建 ECS



2 修改服务器名及计算机名

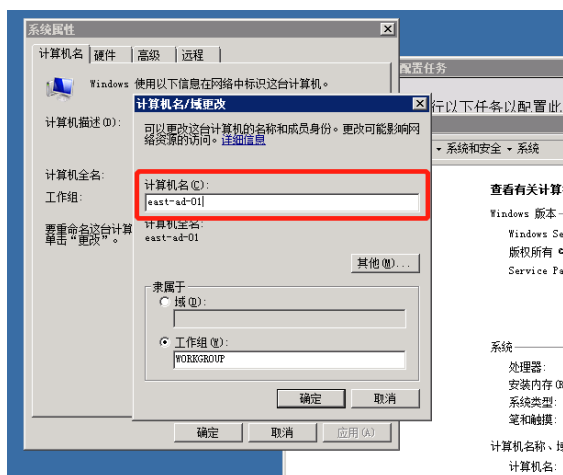
修改计算机名方便识别

- 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

名称/ID	可用分区	状态	规格/镜像
<div>EastAd01</div> <div>b04a560d-9116-4f32-9fb4-6d...</div>	可用区1	运行中	2核 8GB Windows Serv



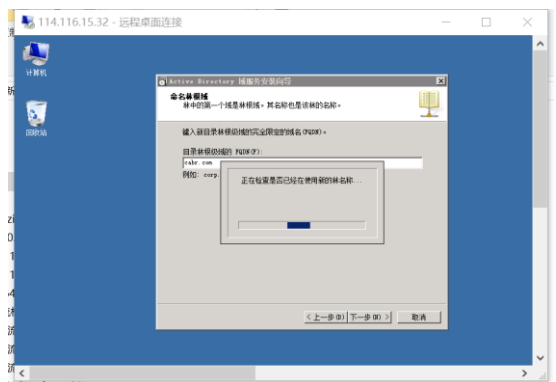
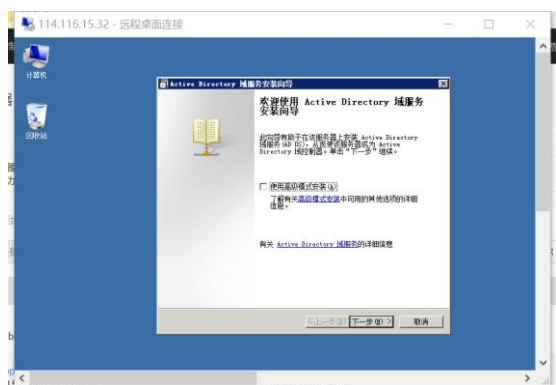
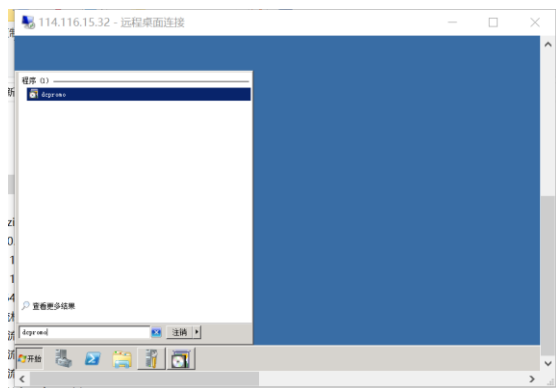
3 安装 AD 域服务

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

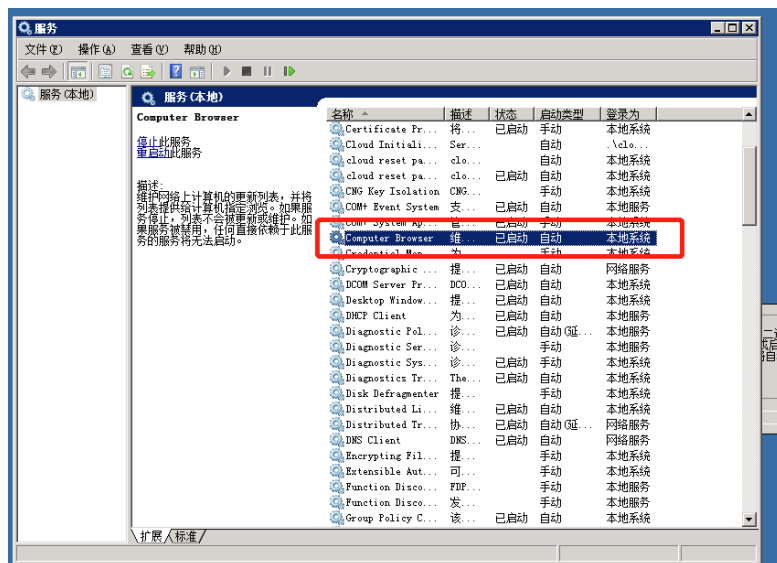
注意！同一区域属于同一 VPC（VPC 可理解为同一局域网），因而在同一区域同一 VPC 下，即使项目不同，目录林根目录也不能相同 如根目录 pkpm.com 只能存在一个



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

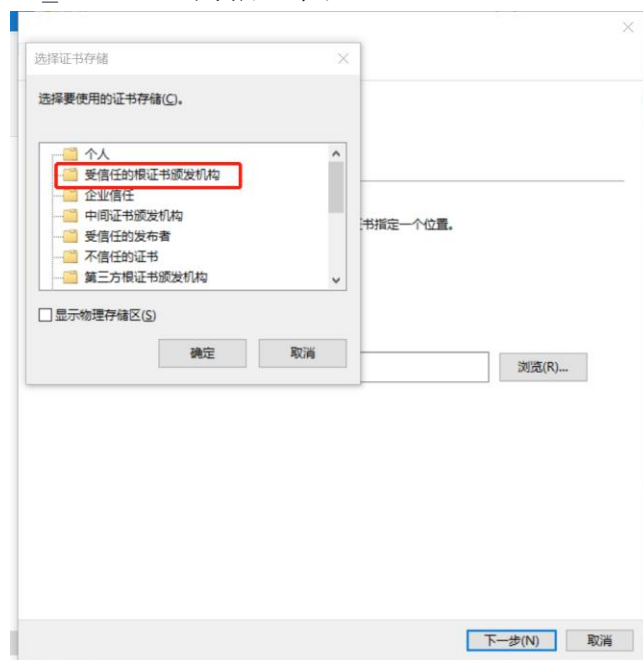
<https://yq.aliyun.com/articles/118657?t=1>

ad2.cer

CA_CER2.cer

大小: 865 字节
修改日期: 20...

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

添加规则

快速添加规则

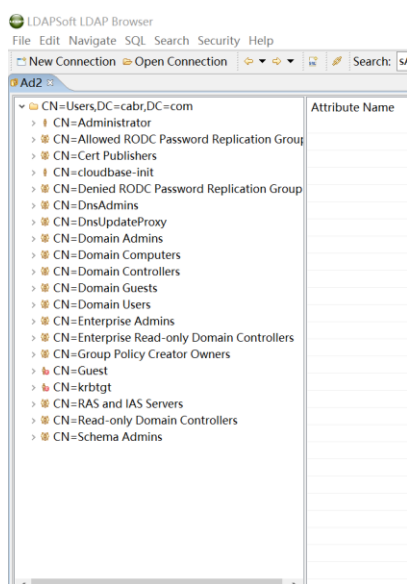
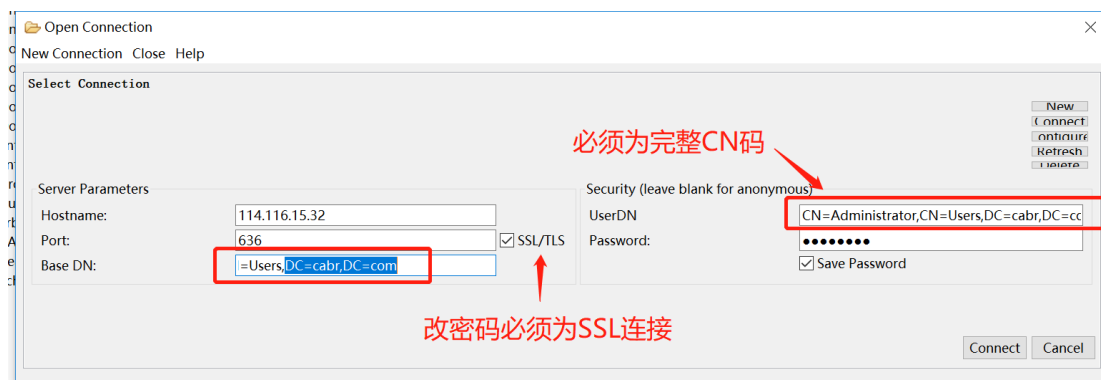
出方向规则 1

入方向规则 4

方向	类型	协议	端口范围/ICMP类型	远端	操作
入方向	IPv4	Any	Any	Sys-default(b0739cf8-b719-4fe5-a6fa-dea90bc7ab54)	删除
出方向	IPv4	Any	Any	Any ②	删除
入方向	IPv4	TCP	22	0.0.0.0/0 ②	删除
入方向	IPv4	TCP	3389	0.0.0.0/0 ②	删除
入方向	IPv4	TCP	636	0.0.0.0/0 ②	删除

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

申请开通云桌面服务

可用分区: ②

可用区1

虚拟私有云: ②

--请选择--

查看VPC

配置AD: ②

创建一个AD域

连接到已有AD域

AD服务管理器

• 域名: ②

• 域管理员帐号:

• 域管理员密码:

• 主域控制器IP:

. . .

备域控制器IP:

. . .

• 主DNS IP:

. . .

备DNS IP:

. . .

☒ Internet接入

☐ 专线接入 (为保证体验, GPU实例要求开通专线接入) [了解专线接入...](#)

立即申请

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

配置信息

服务状态: ✔ 已开通 [取消服务](#)

网络

互联网接入地:

专线接入地址: 未启用 [开启](#)

VPC名称: [vpc162d801f3ee62697](#)

业务子网: [subnet162d801fabe80750](#) [修改](#)

管理子网: 10.0.0.0/20

基础架构安全组: [WorkspaceManagerSecurityGroup](#)

桌面安全组: [WorkspaceUserSecurityGroup](#)

网关: 192.168.0.1

DNS1: 192.168.0.25

DNS2: --

互联网接入端口: 443;8443 [修改](#)

AD域

域类型: 本地 AD

域名: broad.com

域管理员帐号: administrator

主域控制器IP: 192.168.0.25

备域控制器IP: --

主DNS IP: 192.168.0.25

备DNS IP: --

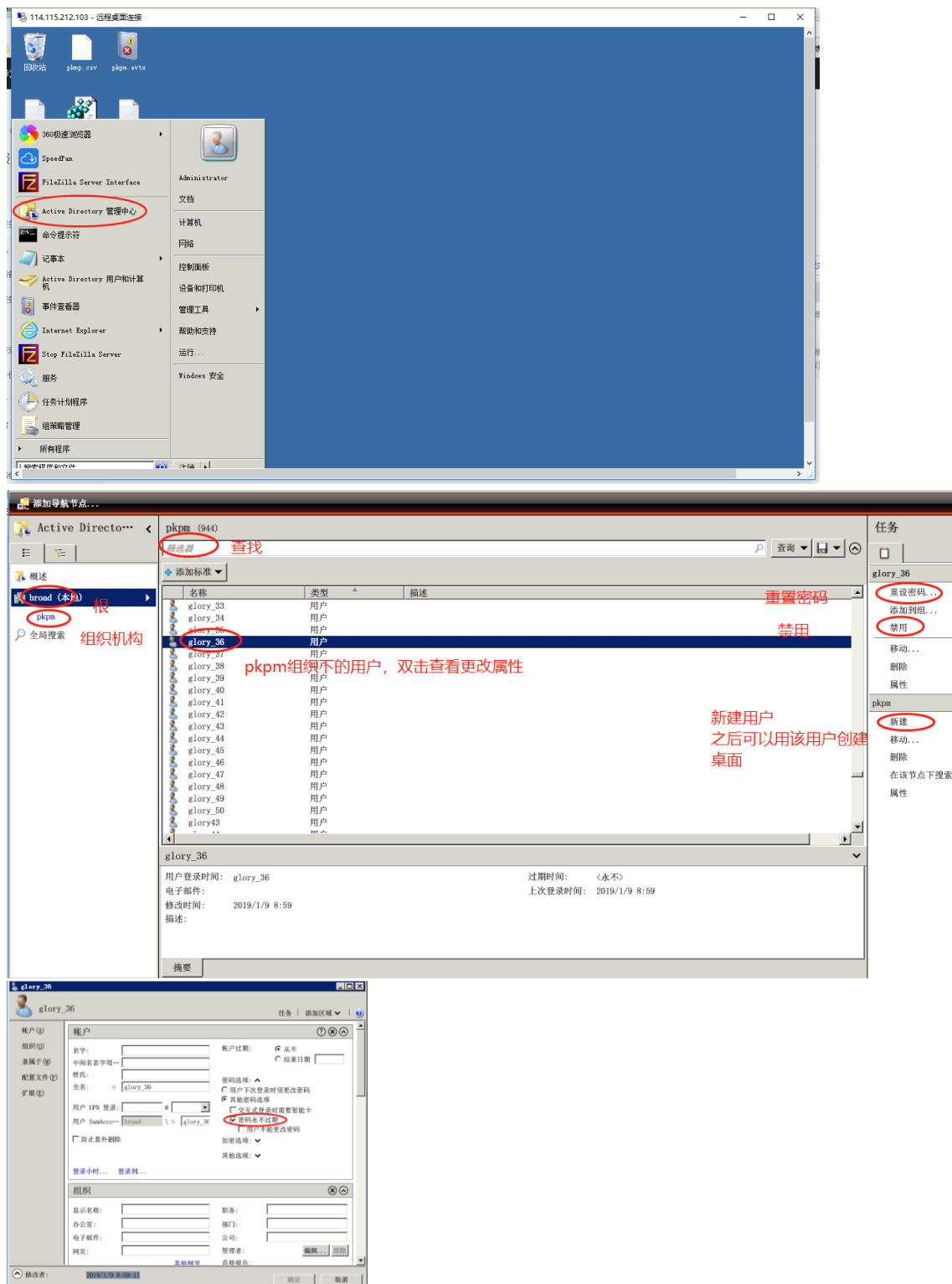
密码: ***** [修改](#)

双因素认证: [修改](#)

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>

名称/ID	可用区	状态	规格/镜像	私有IP地址	弹性IP	计费模式	操作
<input type="checkbox"/> ad-backup b8f31bb5-6b17-4f73-b6c6-c1...	可用区2	运行中	4核 8GB Windows Server 200...	192.168.0.157	139.159.250.69	按需付费	远程登录 更多 ▾
<input type="checkbox"/> ad cdc50c58-1792-4cc6-bc70-11...	可用区2	运行中	2核 4GB Windows Server 200...	192.168.0.25	139.159.254.20	包年/包月 335天后到期	远程登录 更多 ▾

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

```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ping broad.com

正在 Ping broad.com [192.168.0.25] 具有 32 字节的数据:
来自 192.168.0.25 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.0.25 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.0.25 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.0.25 的回复: 字节=32 时间<1ms TTL=128

192.168.0.25 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms

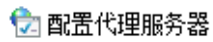
C:\Users\Administrator>
```

开始-》输入 DNS 打开 DNS 服务器设置

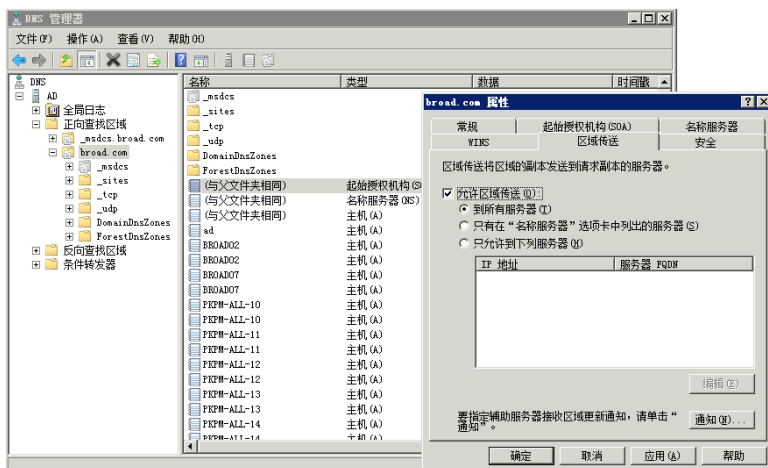
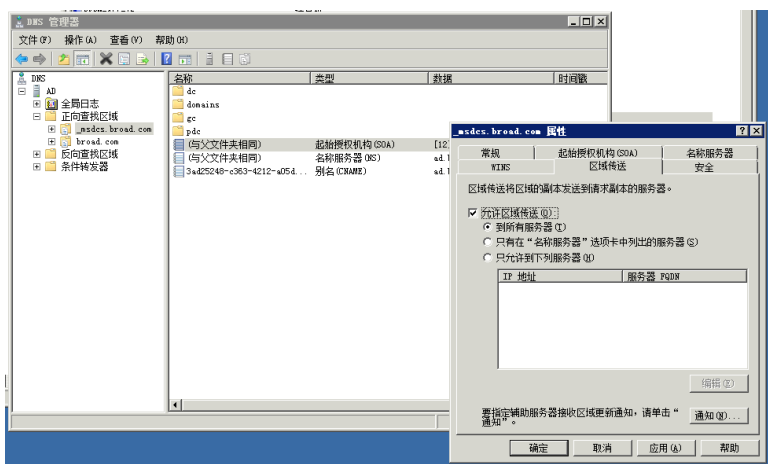
程序 (2)



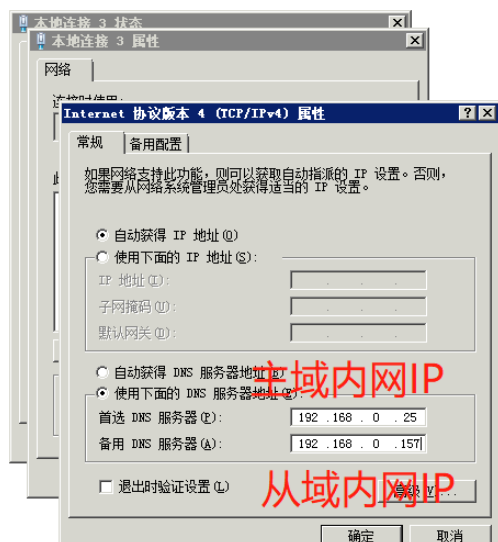
控制面板 (1)



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



11.2配置从域(计算机名为 ad-backup)加入主域(ad)

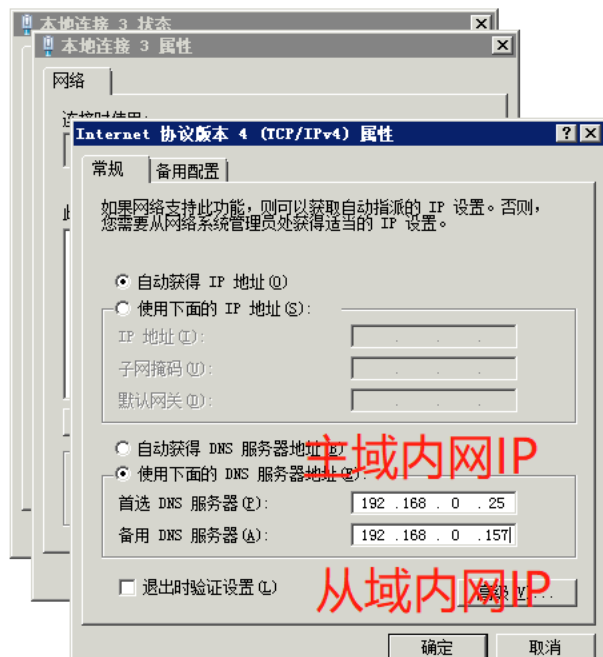
登陆从域 ECS，注意下列操作是针对从域 ECS

确保三个服务已开启：

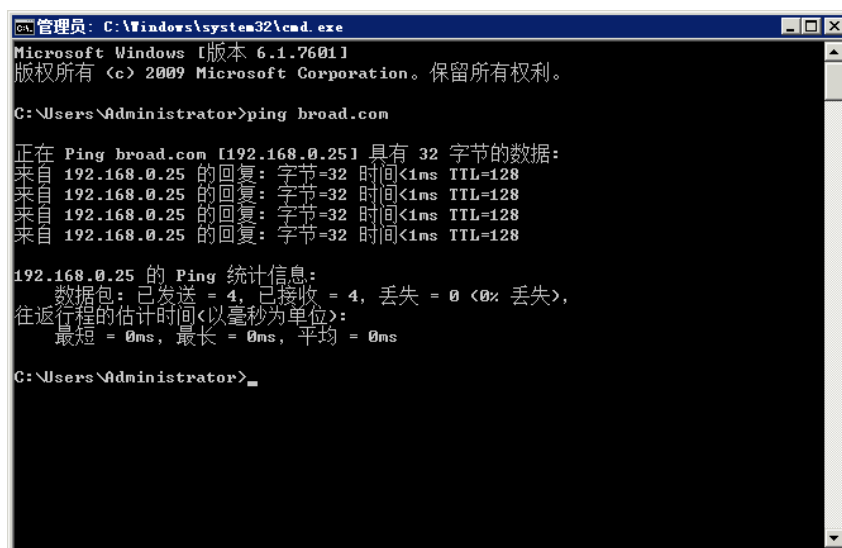
安全组所需端口均已打开

并配置 DNS

DNS 设置为



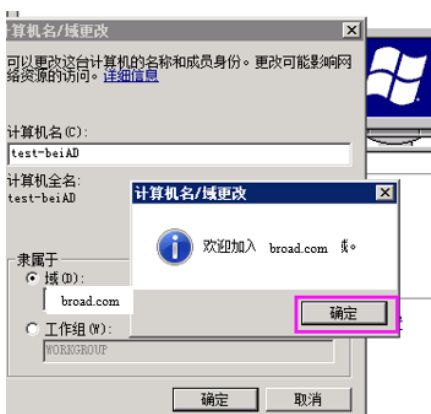
ping broad.com 可以显示主域的 ip，证明从域和主域连接成功



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

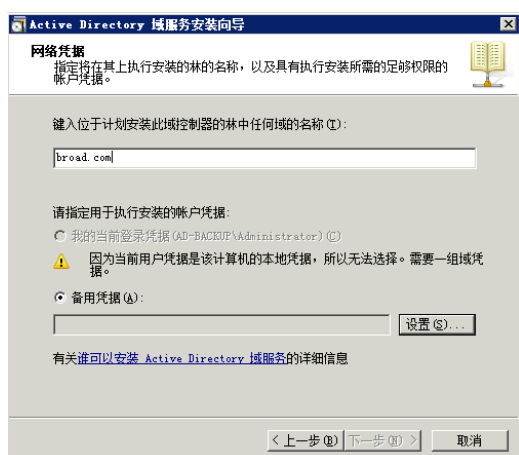
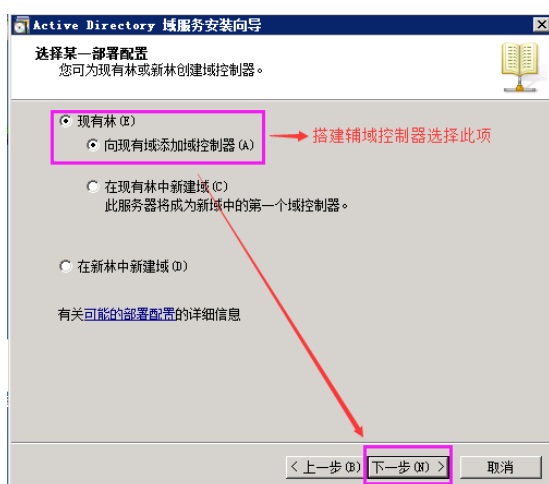
域 broad.com 输入 Administrator/主域密码



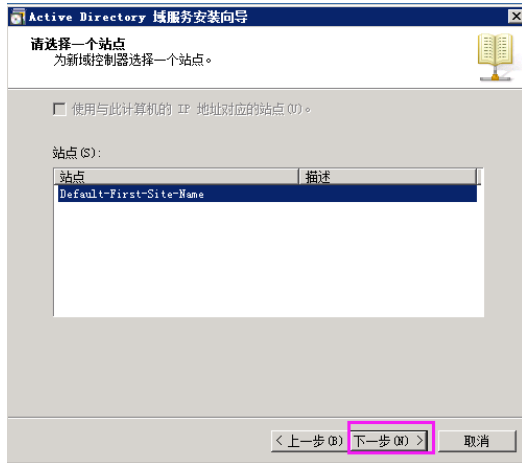
计算机名称、域和工作组设置

计算机名: ad-backup
 计算机全名: ad-backup.broad.com
 计算机描述:
 域: broad.com

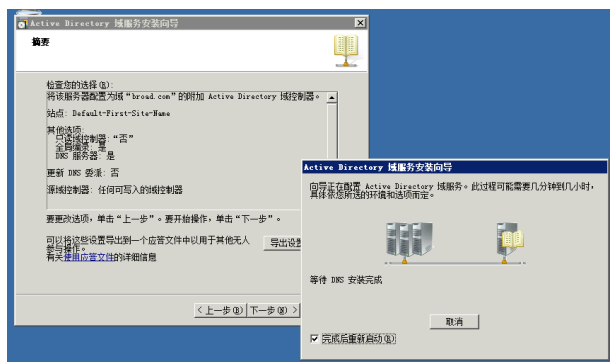
重启后，可以发现从域 ECS 已加入主域
 运行-输入 dcpromo



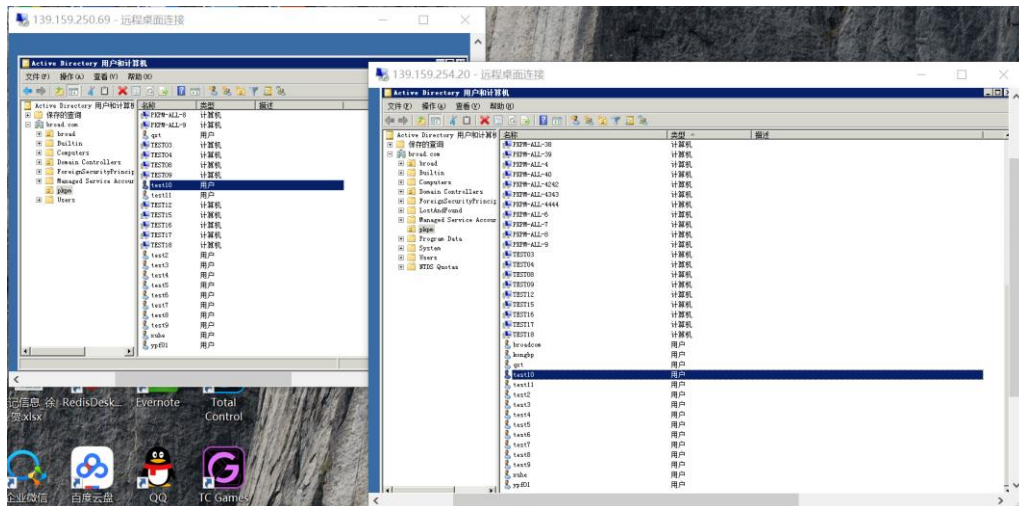
备用凭据输入之前登陆的用户名密码



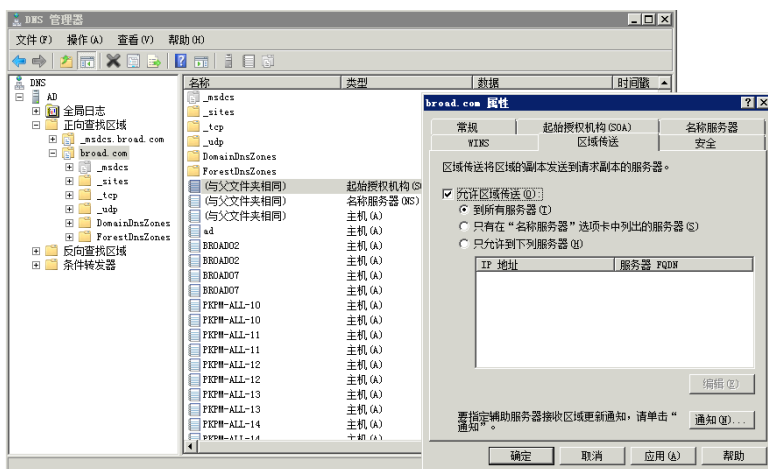
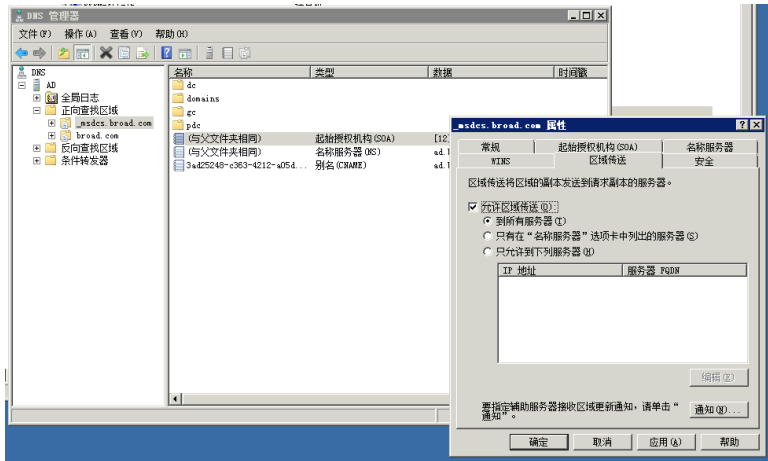
勾选 DNS 服务器和全局编录



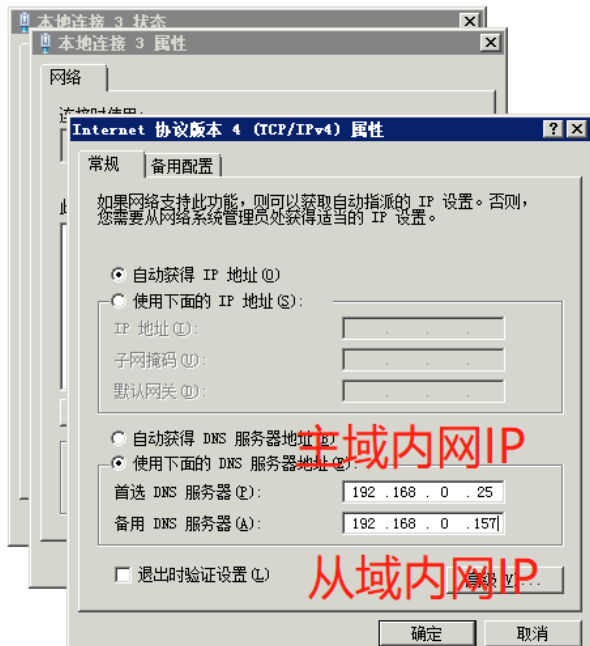
主备后，向 AD 主域添加用户 test10 用户，该用户则会自动同步到 AD 从域，反之亦可。



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

分配桌面

导入方式: 手工输入 批量导入

桌面信息:

- * 用户名: kongbaoping
- * 邮箱: evanxuhe@163.com
- * 用户组: Administrators

+ 添加桌面 您还可以添加9个桌面, 每个桌面只能属于单个用户。

发送通知邮件: 是 否

组织单元: 构力/创新中心/云平台/研发部

OU最多5级 A/B/C/D/E

Active Directory 用户和计算机

文件(F) 操作(O) 查看(V) 帮助(H)

Active Directory 用户和计算机

- 保存的查询
- glory.com
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - fulli
 - LostAndFound
 - Managed Service Accounts
 - plpkm
 - creation
 - 人力
 - Program Data
 - System
 - Users
 - 构力
 - 创新中心
 - 云平台
 - 研发部
 - 后台开发
 - 产品组
 - NTFS Quotas

孔保平

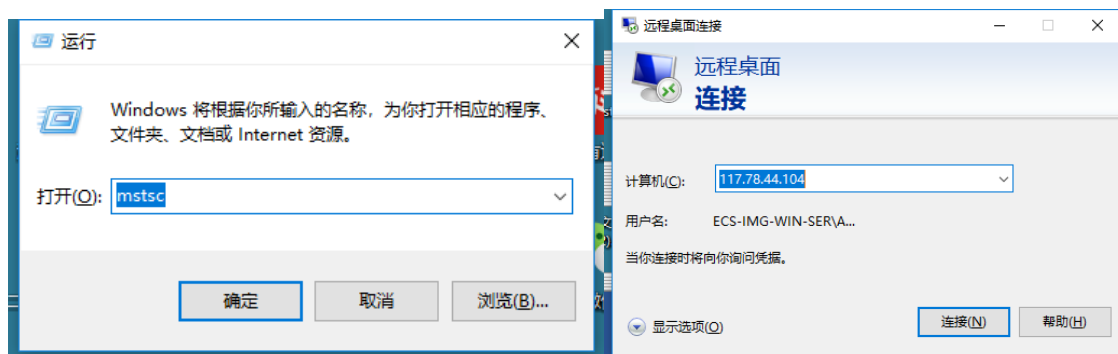
DC=com, DC=glory CN=kongbaoping

OU=

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

