搭建基于公网访问的 Windows AD 和 DNS 服务器

1. 搭建 AD 服务器

1.2 购买 ECS 虚机

在阿里云 ECS 至少购买两台带有公网 IP 的虚机，镜像请选择 Windows server 2008 R2 企业版

1 台用来搭建 AD 服务器，安全组中开发 53(TCP/UDP)、88(TCP/UDP)、123(UDP)、135(TCP)、137(UDP)、138(UDP)、139(TCP)、389(TCP/UDP)、445(TCP)、464(TCP)、500(UDP)、593(TCP)、636(TCP)、3268(TCP)、3269(TCP)、49152~65535(TCP/UDP)端口

1 台用来搭建 DNS 服务器，安全组中开放 53 (TCP/UDP)端口

图 1

1.3 AD 服务安装和配置

1. 通过远程连接，登陆到 Windows 虚机
2. 在开始菜单—搜索程序和文件中输入 CMD，打开命令窗口，并输入 dcpromo,启动 AD 安装向导，图 2

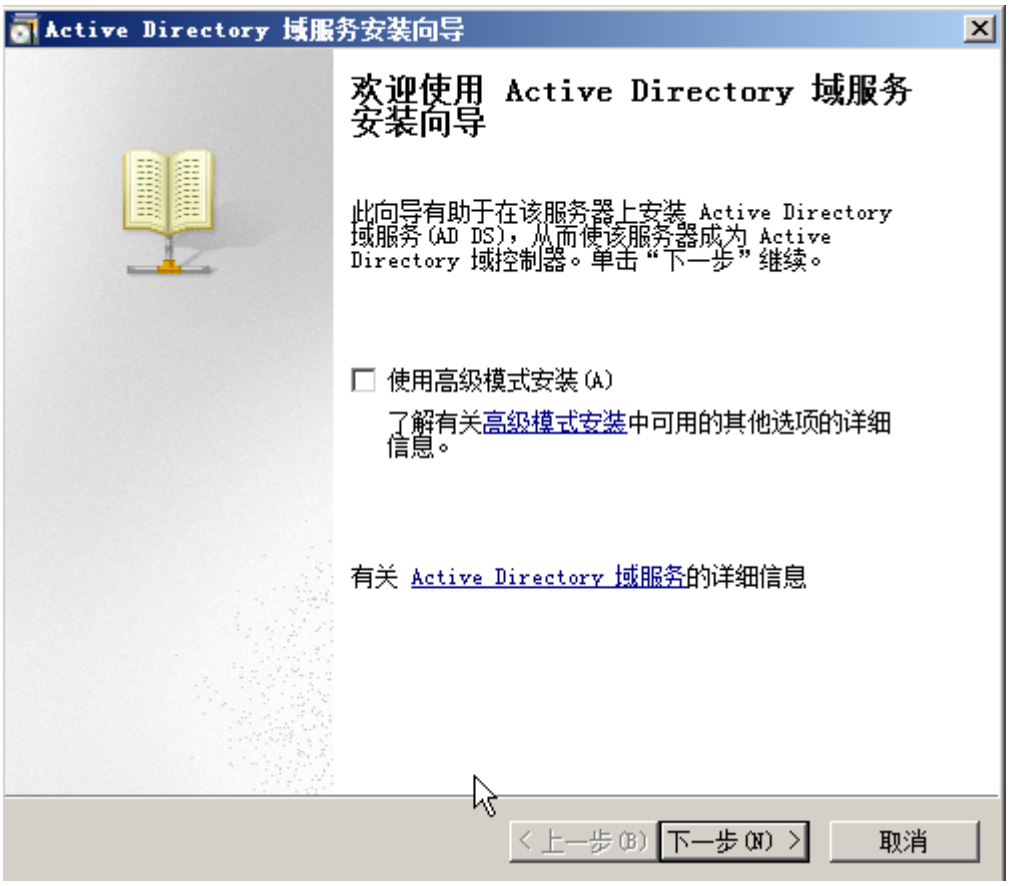

图 2

3. 点击下一步至“选择某一部署配置” 图 3，选择中“在新林中新建域”，并点击下一步

图 3

4. 在“命名林根域” 图 4，输入 AD 域名（如 test.clouddesktop.com），点击下一步，系统自动验证创建 AD 相关的信息

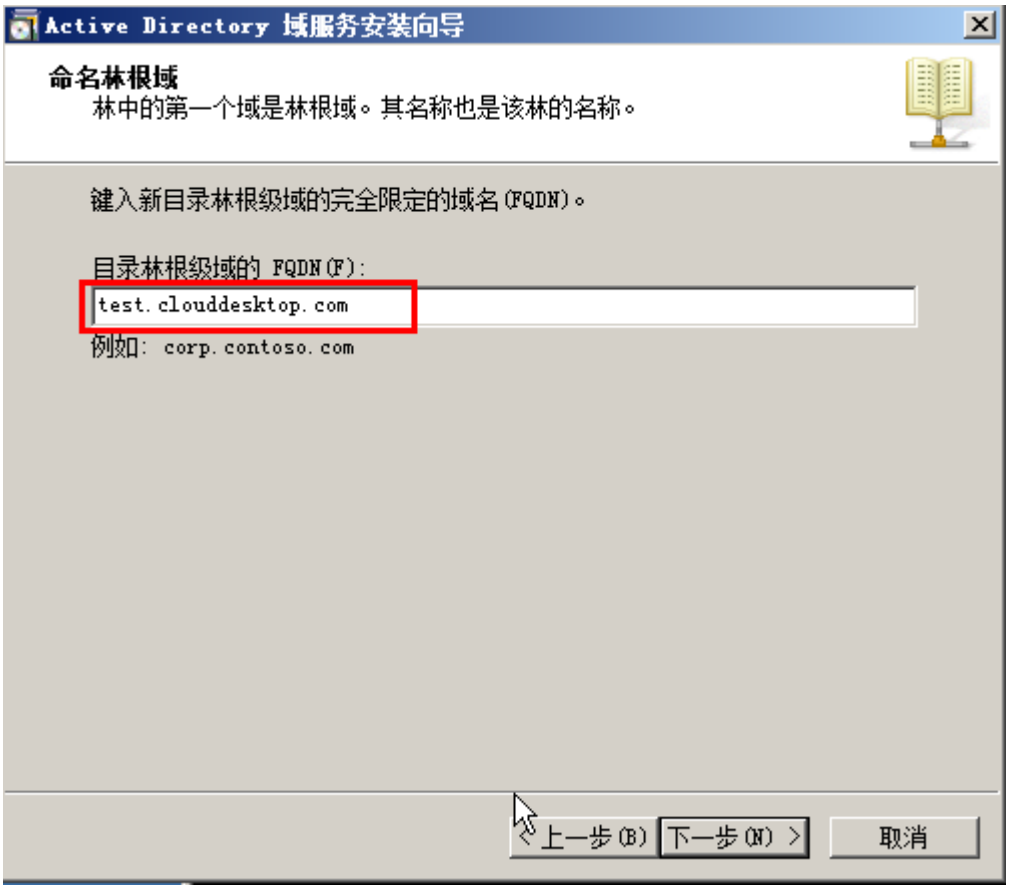

图 4

5. 在“设置林功能级别” 图 5 选择 Windows Server 2008 R2，点击下一步

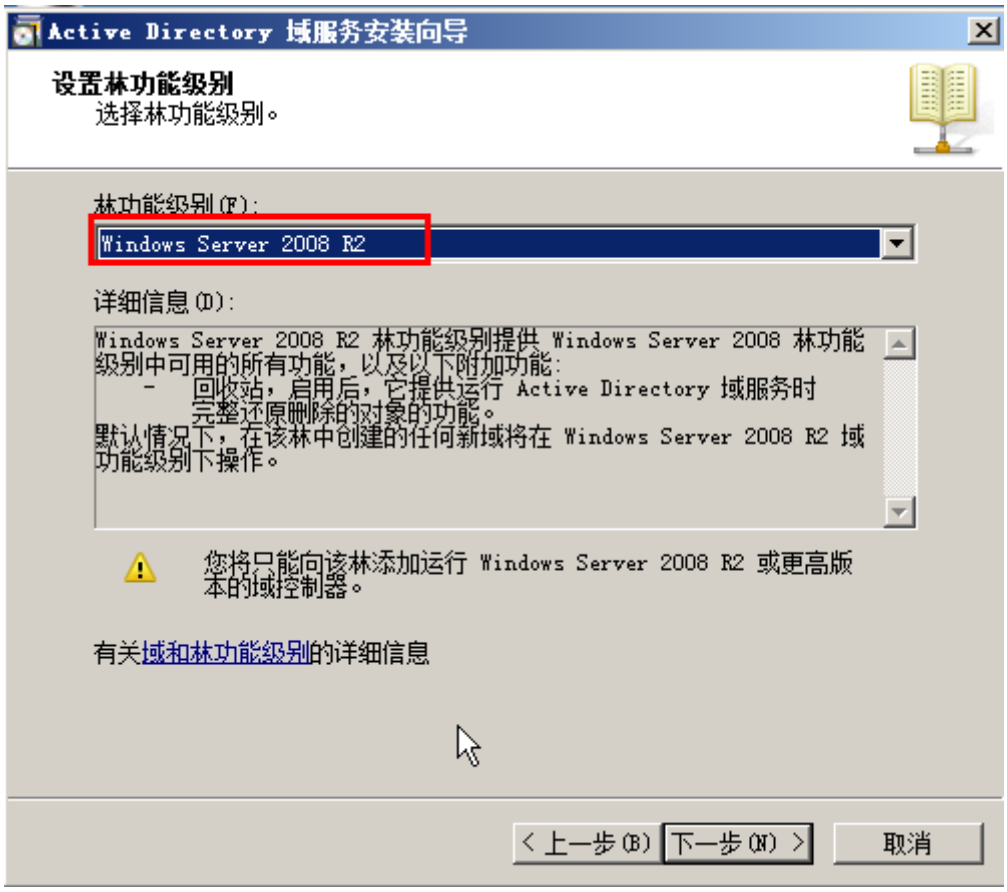

图 5

6. 在“其他域控制器选项”图 6，选中“DNS 服务器(D)”,点击下一步

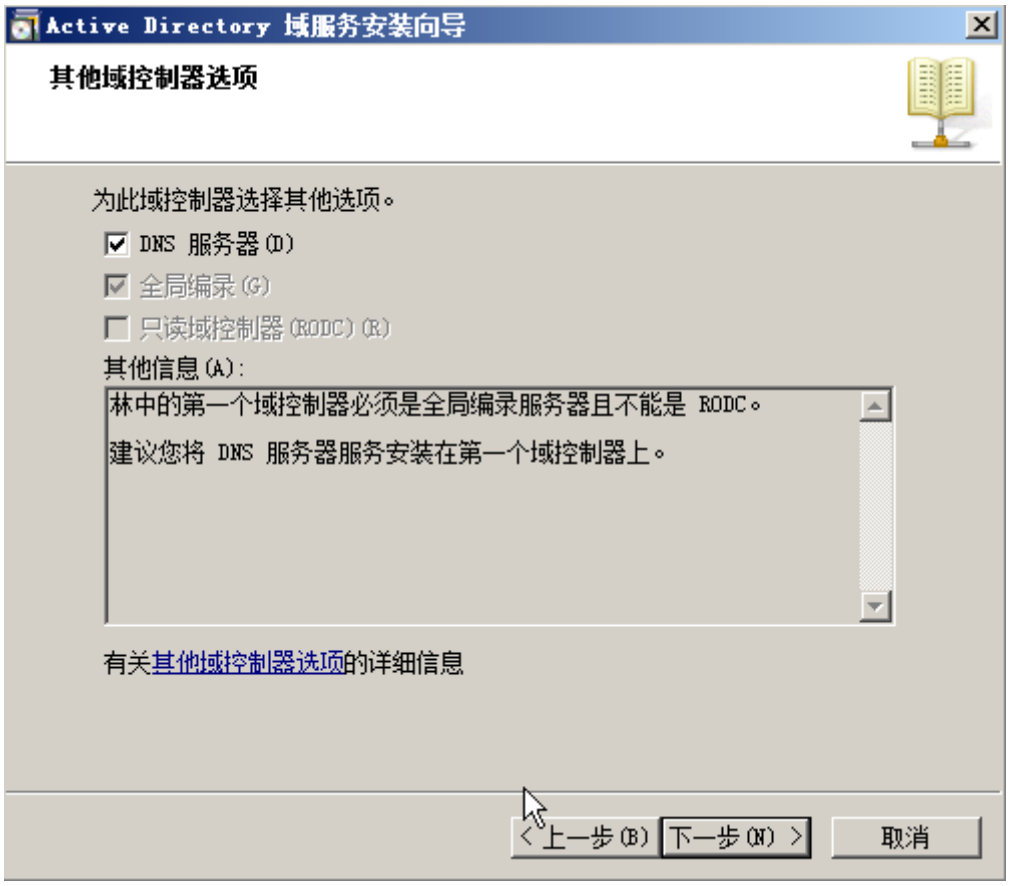

图 6

说明这里安装的 DNS 服务器只能被查找内网 IP 地址

7. 在“静态 IP 分配” 图 7，选择 是

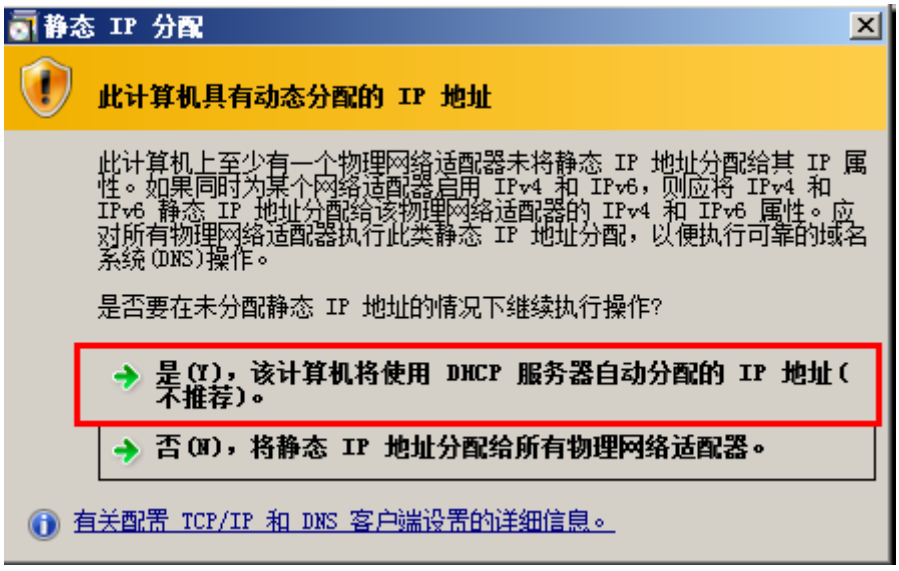

图 7

8. 在“域服务安装向导” 图 8，选择 是

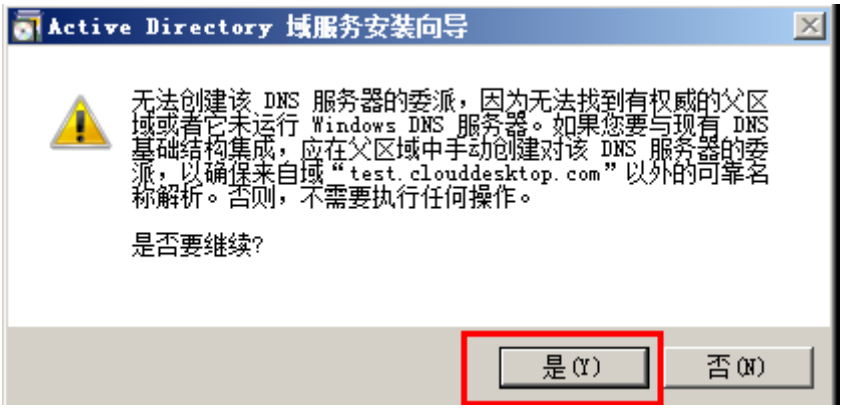

图 8

9. 在“数据库、日志文件和 SYSVOL 的位置” 图 9，设置文件存放路径，点击下一步

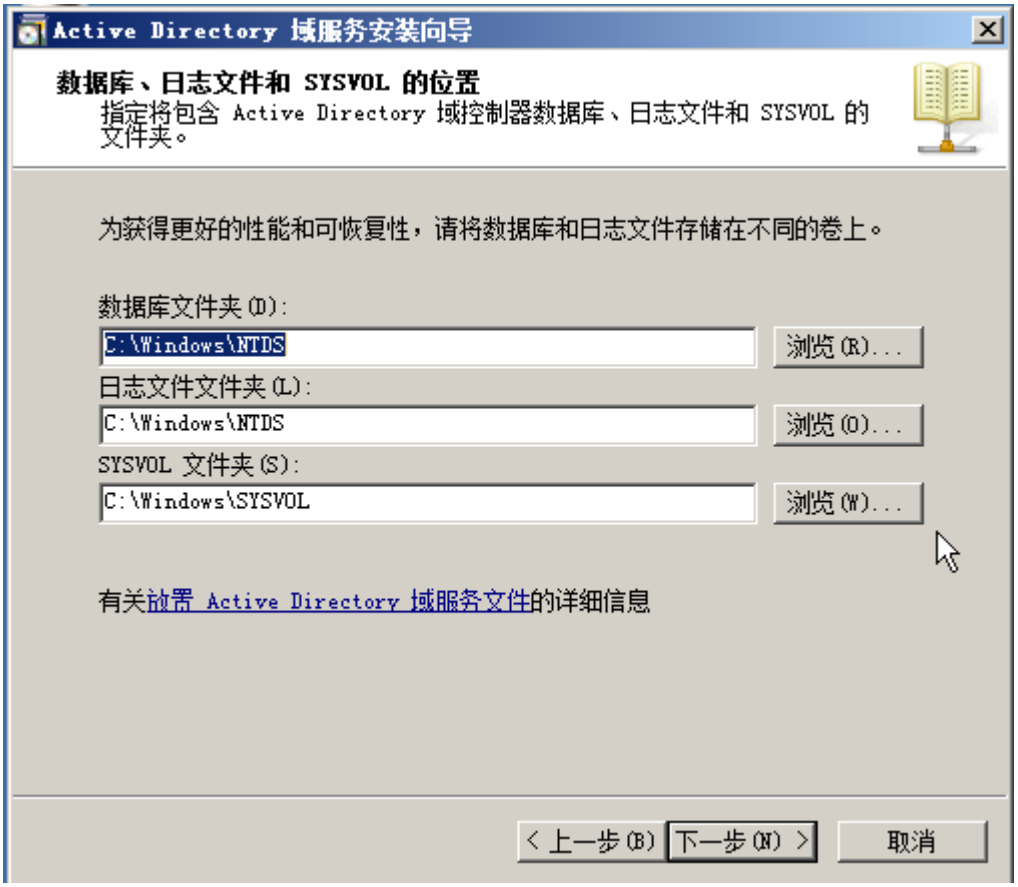

图 9

10. 在“目录服务还原模式的 Administrator 密码” 图 10，设置 Administrator 密码，必须包含大写字母、小写字母、数字和特殊字符中的 3 种，点击下一步

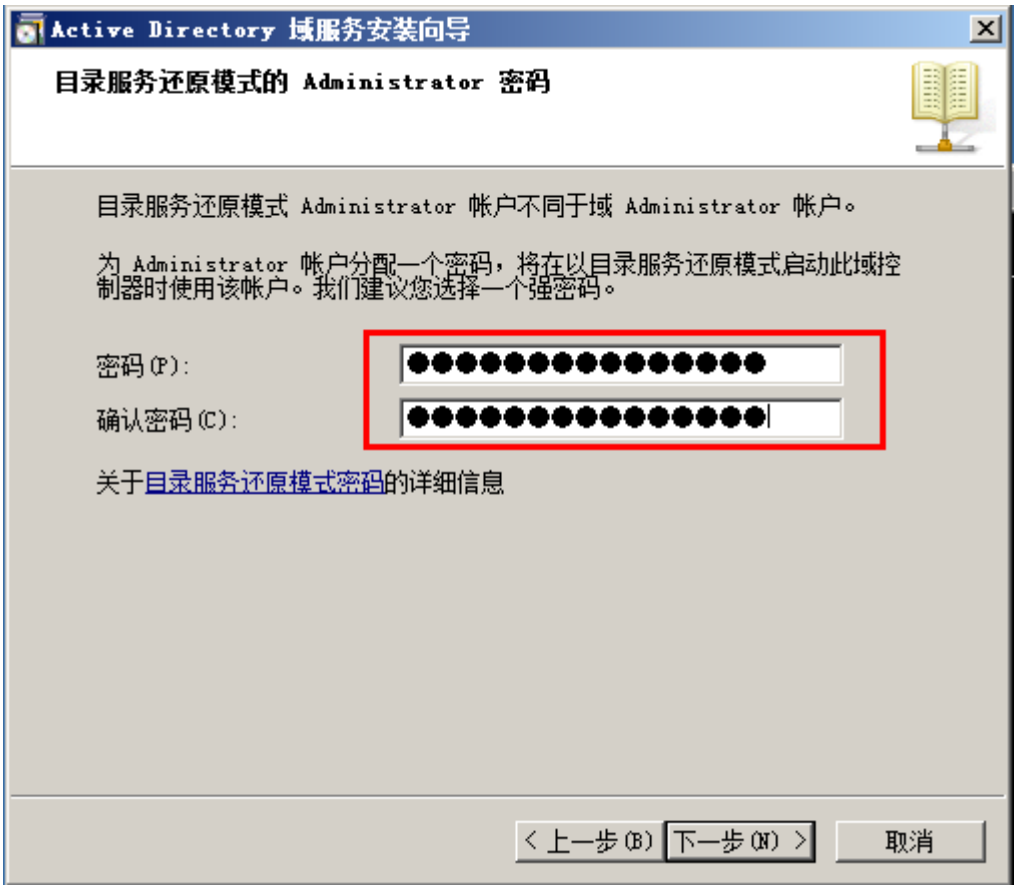

图 10

11. 在“摘要” 图 11
可以选择“导出设置(E)…”，用来保存 AD 创建的设置(保存到文件 test.cldouddesktop.com.txt)，下次假如需要创建配置类似的 AD，只需要用以下 CM 命令进行无人值守创建 AD：
dcpromo /unattend:filepath/test.cldouddesktop.com.txt
点击下一步

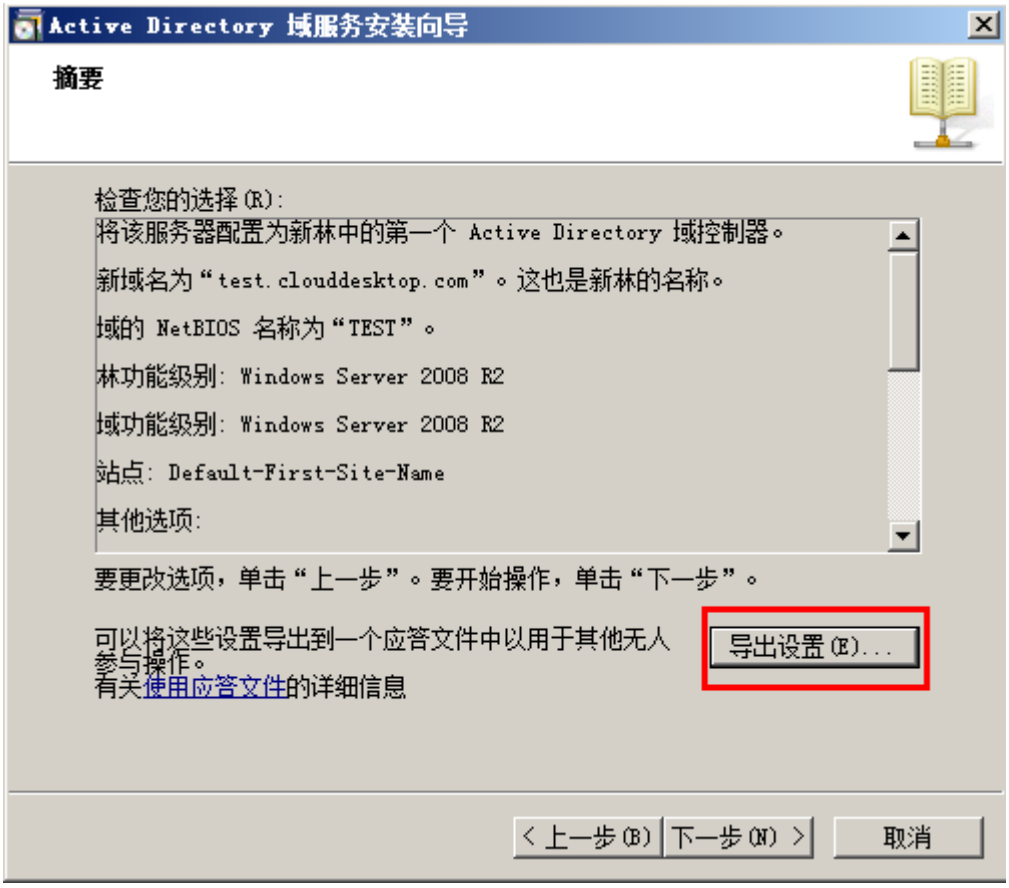

图 11

12. 系统开始创建 AD 图 12，创建完以后必须重启，因此可以选中“完成后重新启动”

图 12

13. 重启完成以后，可以看到在登陆界面 Administrator 前面多了一个域名第一个字段图 12，说明 AD 已经创建成功，同时登陆到 Windows 内部，进行“证书服务”创建

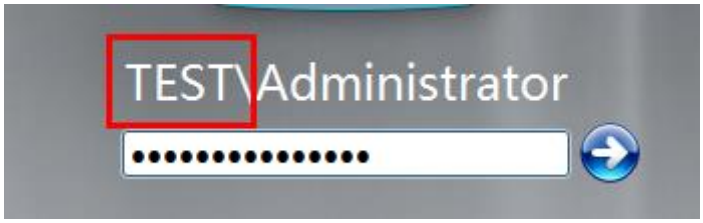

图 13

14. 在 Windows 任务栏启动“服务器管理器” 图 14

图 14

在“服务器管理器”窗口 图 15，选中“服务器管理器”，点击右键，点击“添加角色”

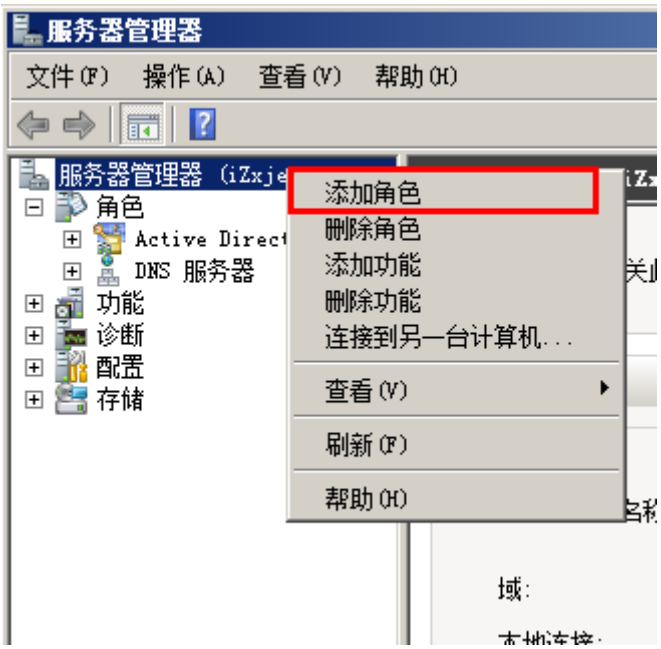

图 15

15. 启动“添加角色向导”，在“开始之前”页面点击下一步，进入“选择服务器角色”图 16，选中“Activity Directory 证书服务”，点击下一步

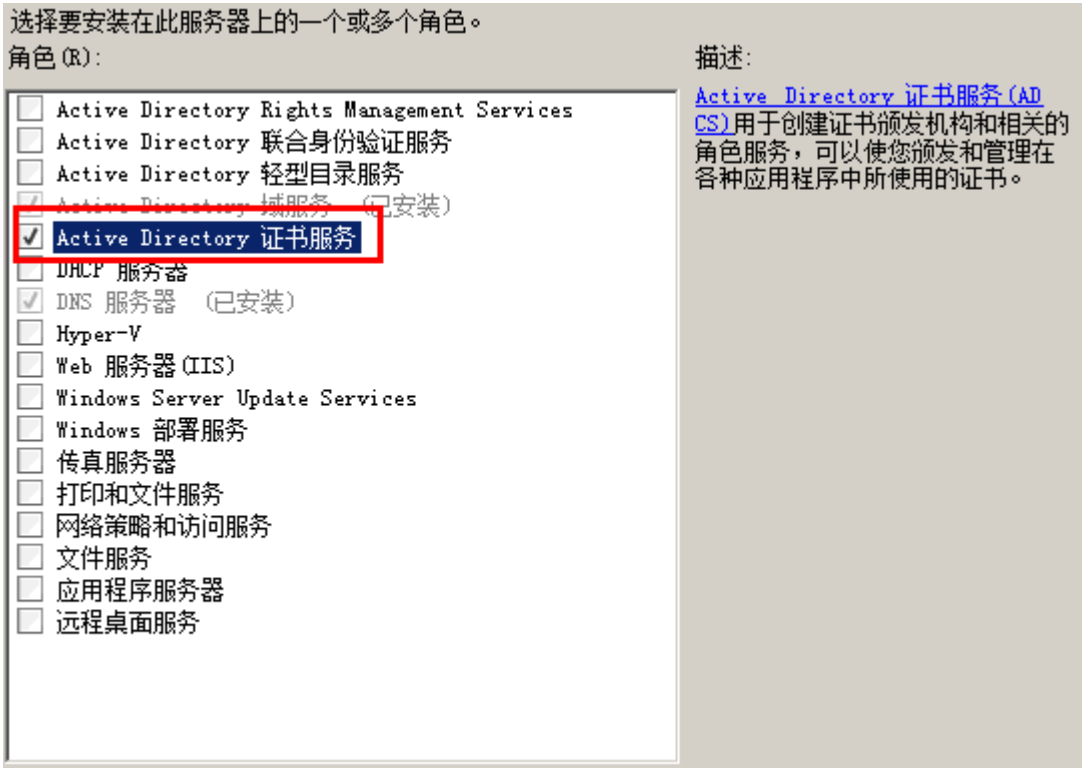

图 16

16. 在“选择为 Activity Directory 证书服务安装的角色服务：” 图 17， 选中“证书颁发机构 Web 注册”，并点击“添加所需的角色服务” 图 18，点击下一步

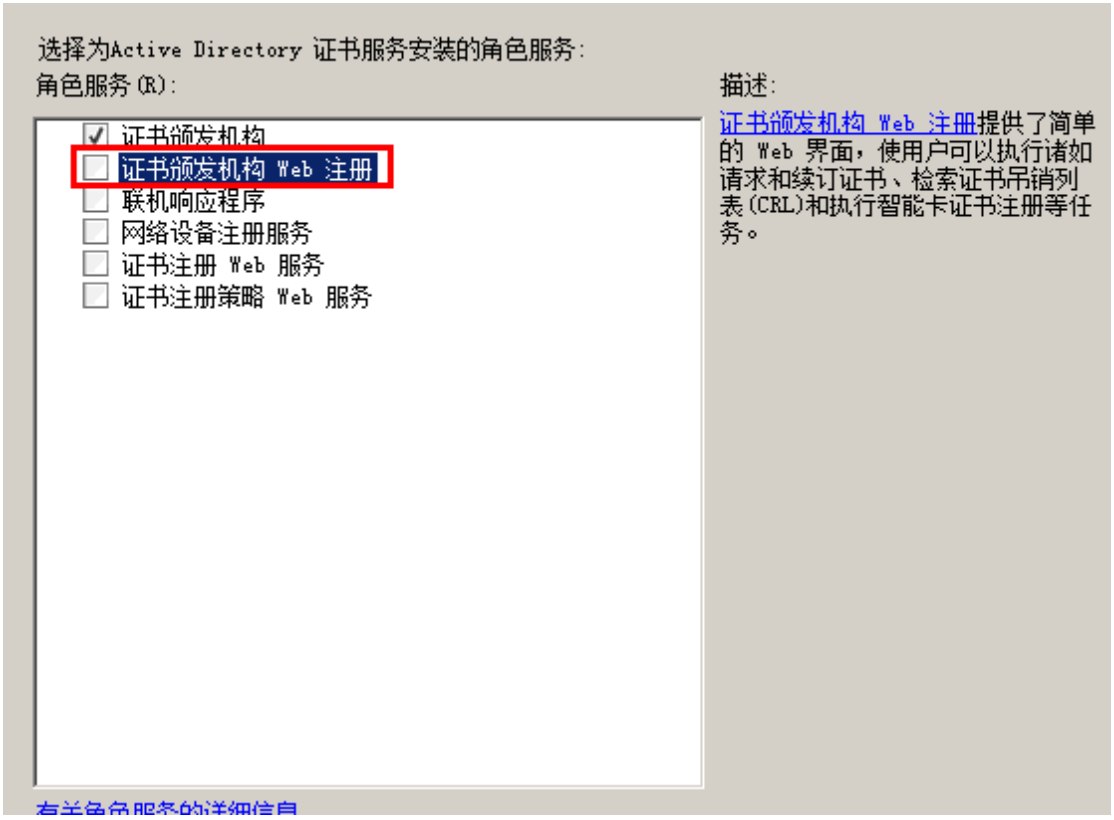

图 17

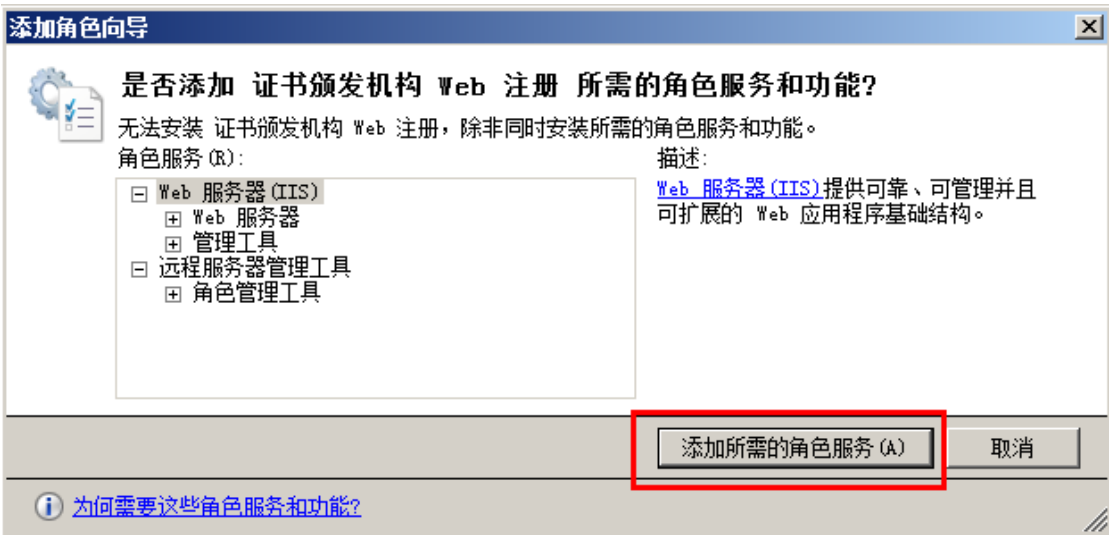

图 18

在“指定安装类型” 图 19，选择“企业”，点击下一步

图 19

在“指定 CA 类型” 图 20，选择“根 CA(R)”,点击下一步

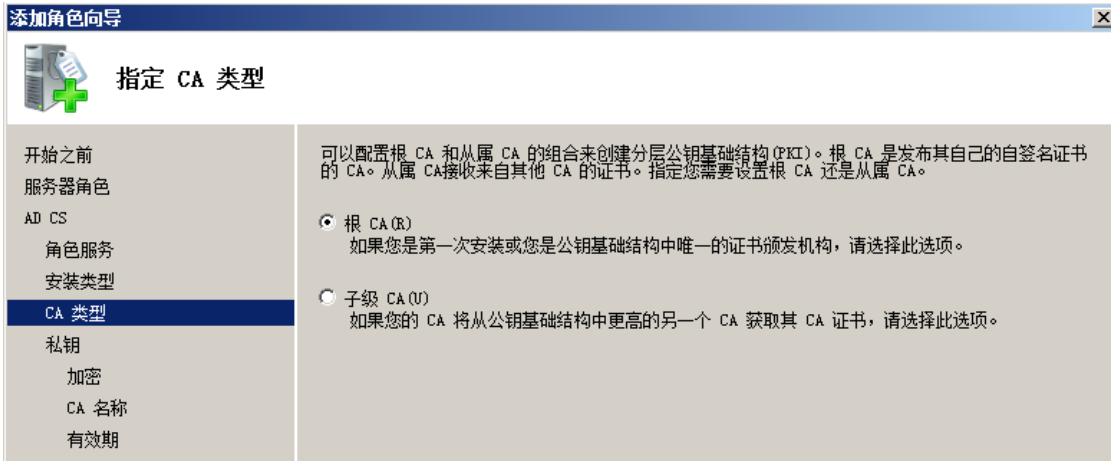

图 20

在“设置私钥” 图 21，选择“新建私钥”

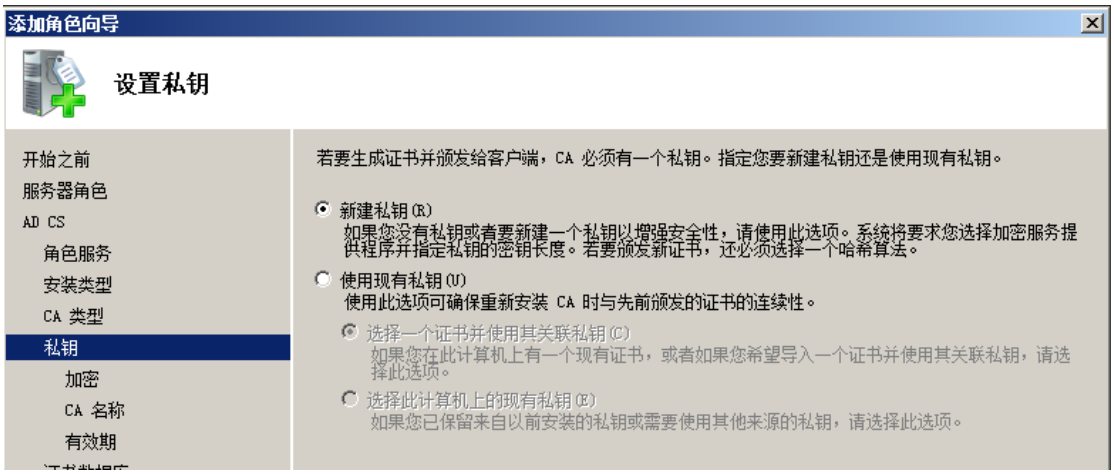

图 21

在“为 CA 配置加密” 图 22，设置秘钥相关内容，点击下一步

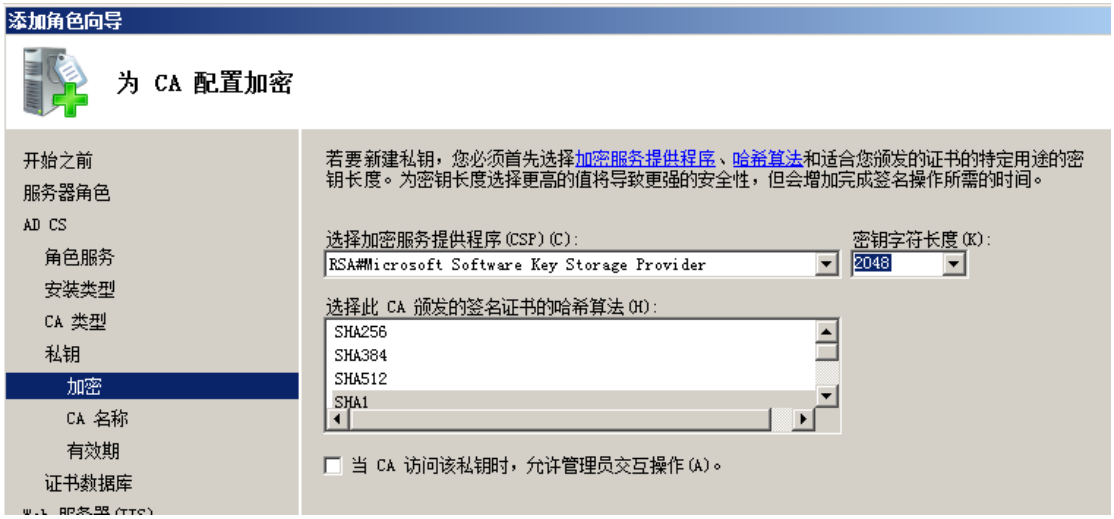

图 22

在“配置 CA 名称”，设置证书名称，点击下一步

图 23

在“设置有效期” 图 24，设置证书有效期，点击下一步

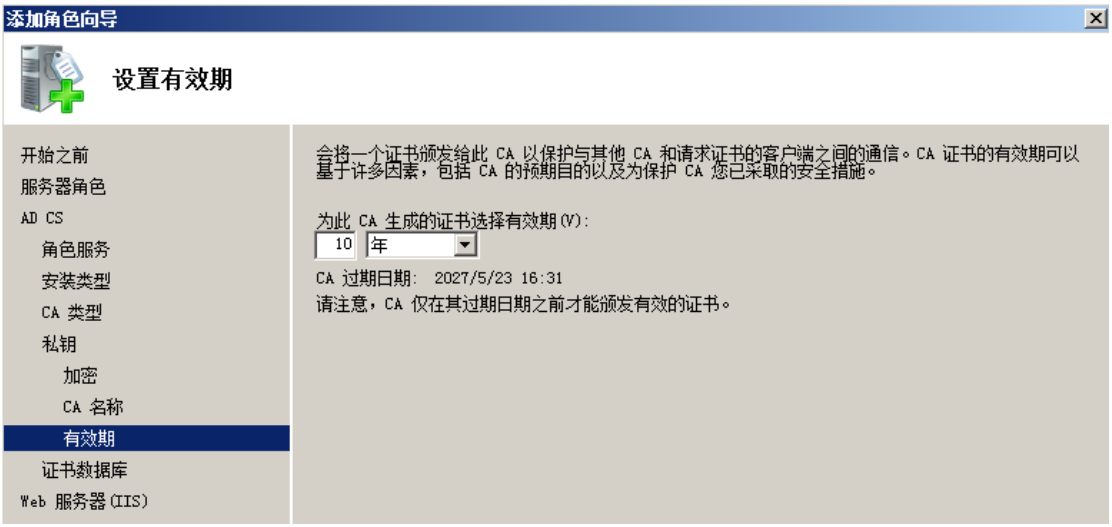

图 24

在“配置证书数据库” 图 25，设置数据库位置，点击下一步

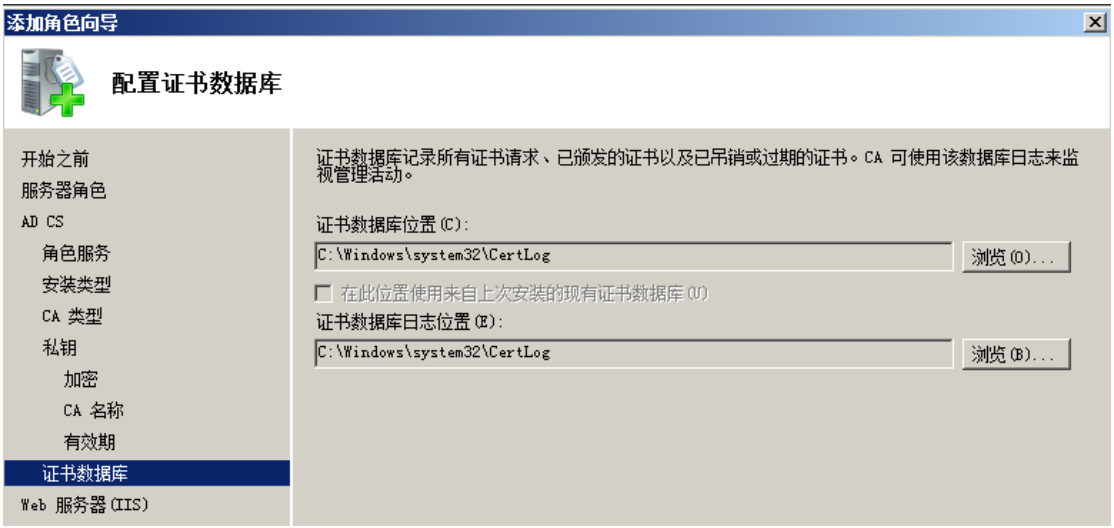

图 25

在“选择角色服务” 图 26，选择系统默认的服务即可，点击下一步

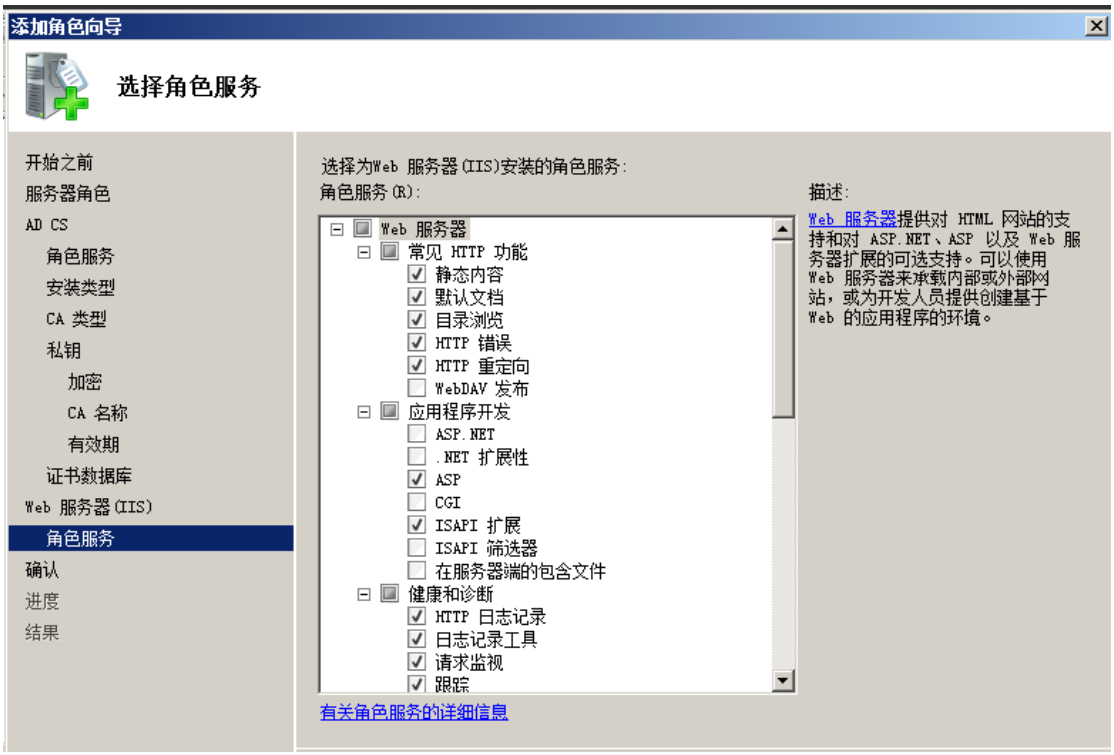

图 26

17. 在“确认安装选择” 图 27，可以检查配置是否正确，如果没有问题，点击安装，进行证书安装

图 27

18. 证书服务安装完成以后，可以在“服务器管理器”窗口 图 28，确认证书服务是否安装成功。

同时，我们可以通过 LDAP SSL 协议访问 AD。

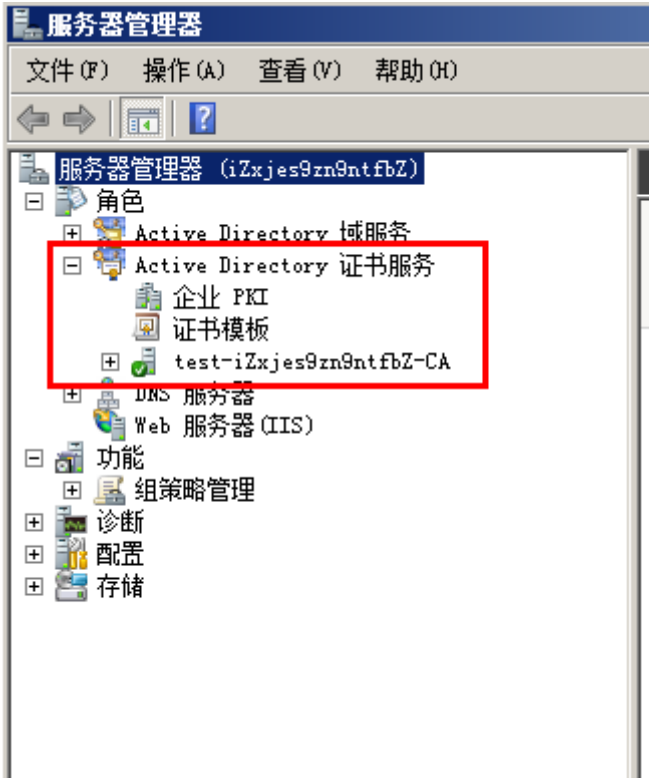

图 28

19. 至此，AD 服务器已经安装和配置完成。

3. DNS 服务器安装和配置

3.1 DNS 服务安装

由于 ESC 虚机的公网 IP 无法直接绑定到 AD 的 DNS 服务器中，因此我们需要用另外一台 DNS 服务器来将 AD 的域名和 AD 的公网地址做映射。

1. 通过远程连接，登陆到 Windows 虚机
2. 在 Windows 任务栏启动“服务器管理器” 图 29

图 29

在“服务器管理” 图 30，选中“角色”点击右键，点击添加角色

图 30

3. 在“选中服务器角色” 图 31，选中“DNS 服务器”

图 31

选中时，会提示“在没有静态 IP 地址情况下安装 DNS 服务器？” 图 32，选择“仍要安装 DNS 服务器 （不推荐）”，并点击下一步，最后点击安装。

说明：访问该 DNS 服务器是通过 ECS 的公网 IP，而该公网 IP 是不会被修改的，因此没有静态 IP 地址不受影响。

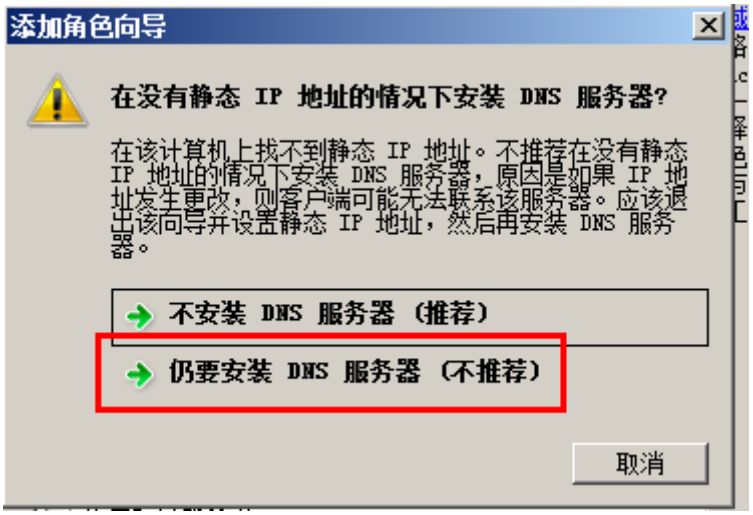

图 32

4. 登陆前面创建的 AD 服务器，打开 AD 服务器里面的 DNS 服务 图 33，为了确保 AD 功能正常使用，需要把 AD 服务器中 DNS 的配置复制到新建的 DNS 中，并将域名对应的 IP 改为 ECS 虚机的公网 IP 地址。

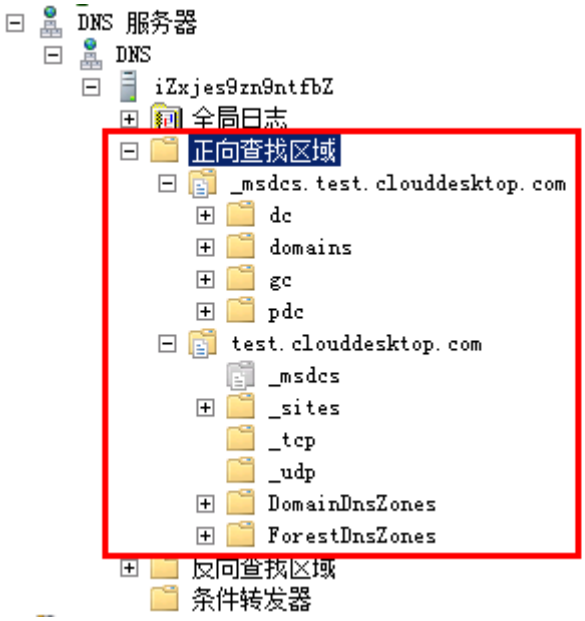

图 33

3.2 DNS 配置案例

下面是 DNS 服务器配置的例子（注意：**例子里面没有把所有记录到配置到 DNS 服务器中**）

1. 安装完成以后，可以在“服务器管理器”窗口 图 34，展开“角色”下面“DNS 服务器”进行确认

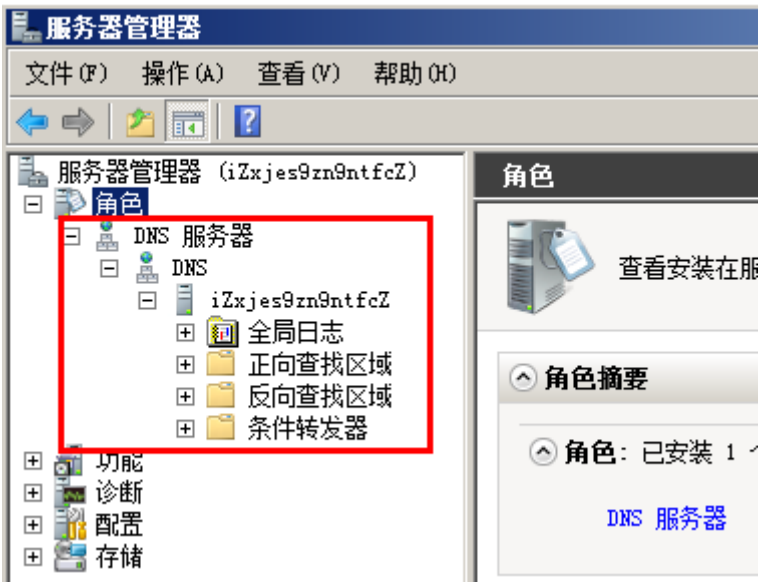

图 34

2. 在“服务器管理器” 图 35，展开 “DNS 服务器”，选中“正向查找区域”，点击右键，选中“新建区域(Z)...”

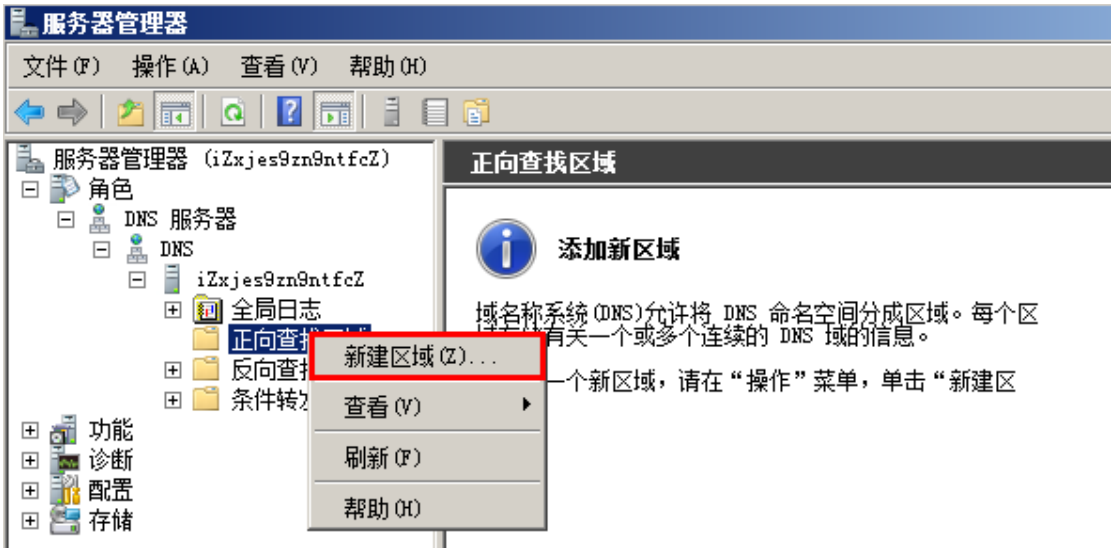

图 35

3. 在“新建区域向导”-“区域类型” 图 36，选中“主要区域”，点击下一步

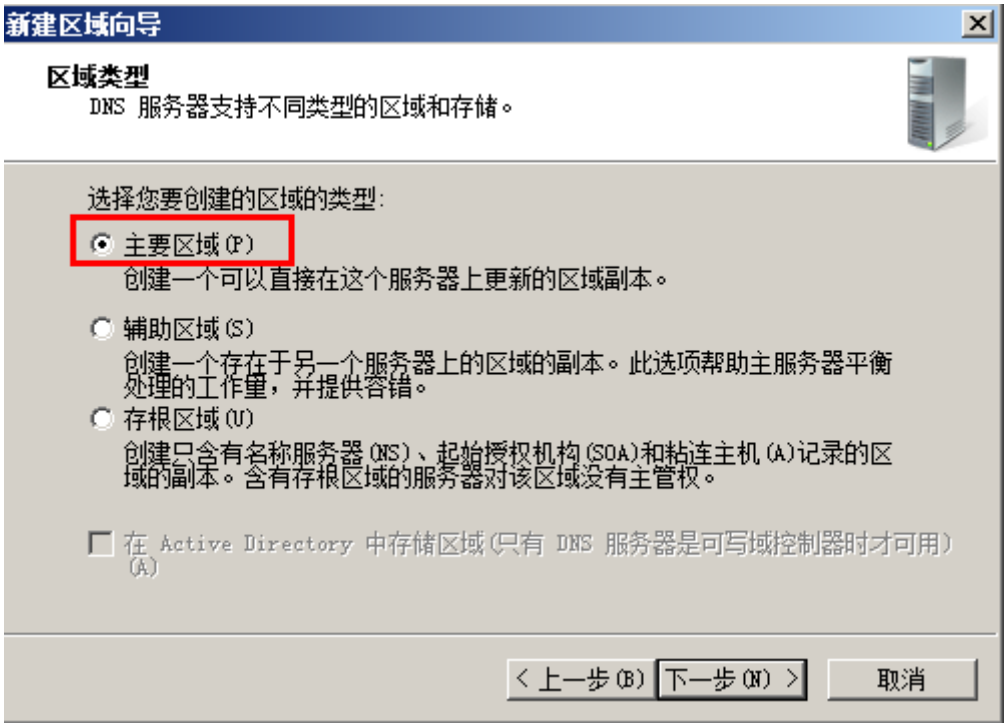

图 36

4. 在“区域名称”图 37 中输入，前面创建的 AD 域名（如 test.clouddesktop.com），点击下一步

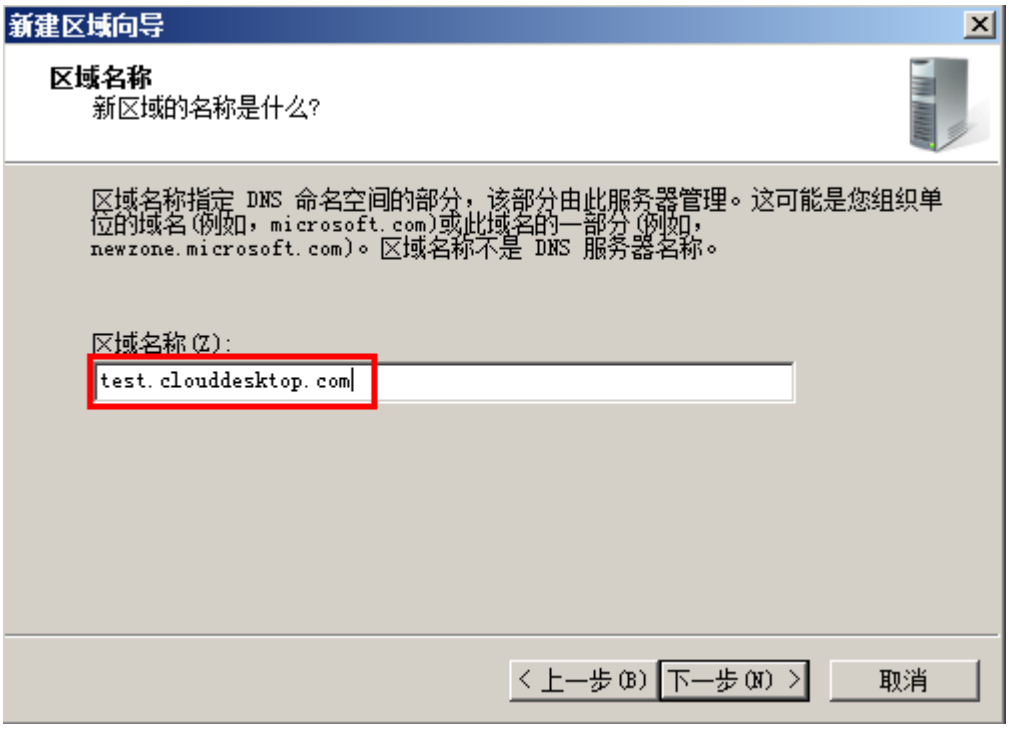

图 37

在“区域文件” 图 38，设置文件名，点击下一步

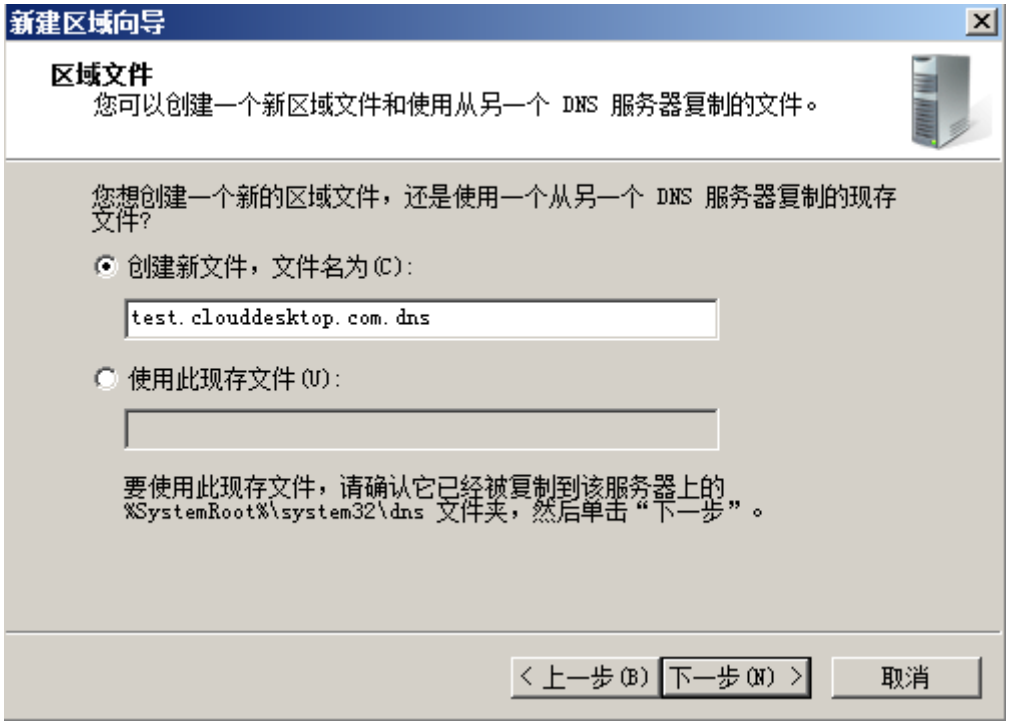

图 38

在“动态更新”中，选中“不允许动态更新”，点击下一步，最后点击完成。

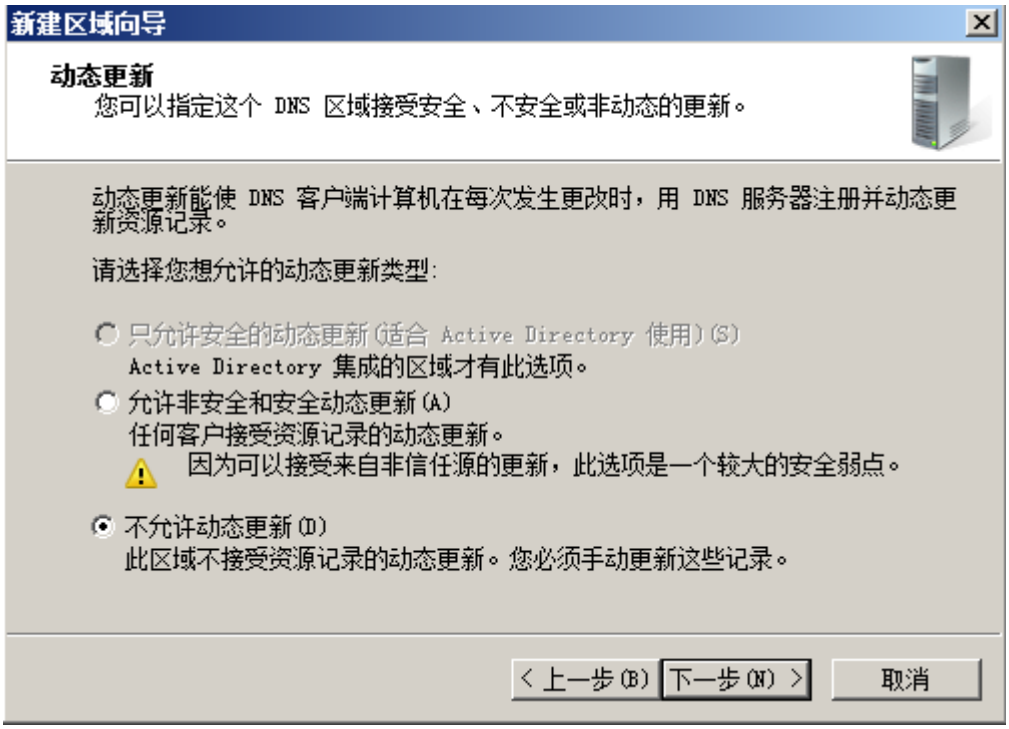

图 39

5. 在“服务器管理器”窗口，“DNS 服务器”中选中刚才创建的域名，点击右键，选择“新建主机”

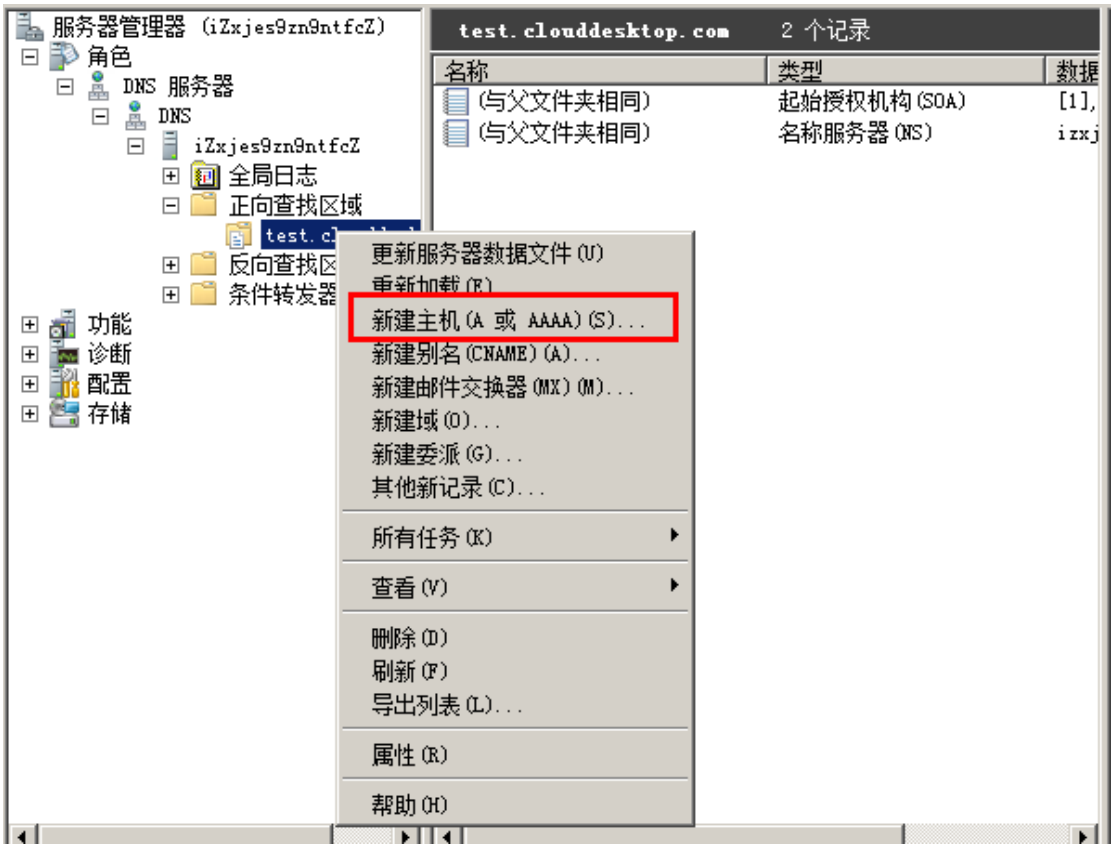

图 40

在“新建主机”窗口 图 41，“IP 地址(P)”栏输入 AD 的公网 IP 地址，点击添加

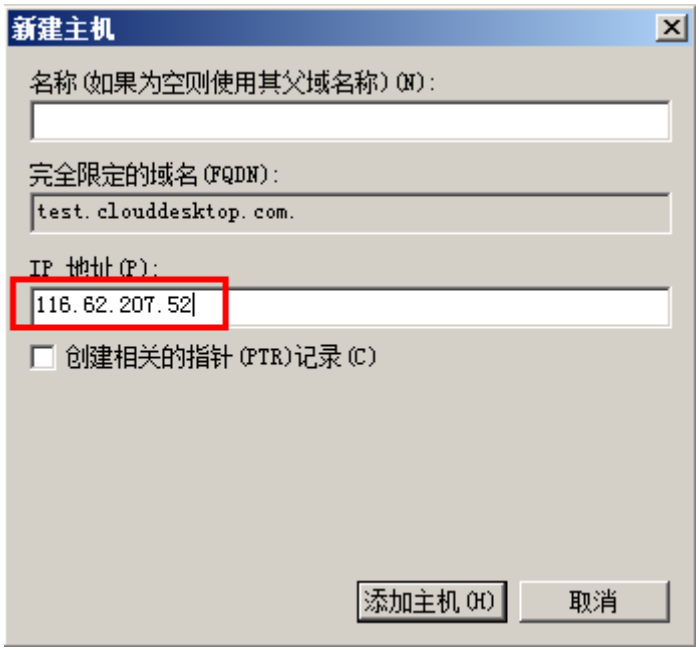

图 41

再次“新建主机”，在名称中填上新建 AD 服务器的名称。注意，非 DNS 服务器的名称。

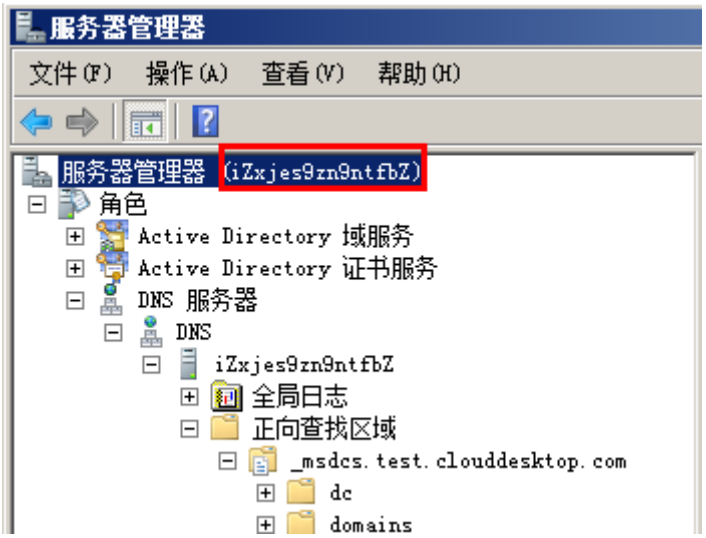

图 42

图 43

6. 重复步骤 G，新建名称为_msdcs+域名（如_msdcs.test.clouddesktop.com）的区域 图 44

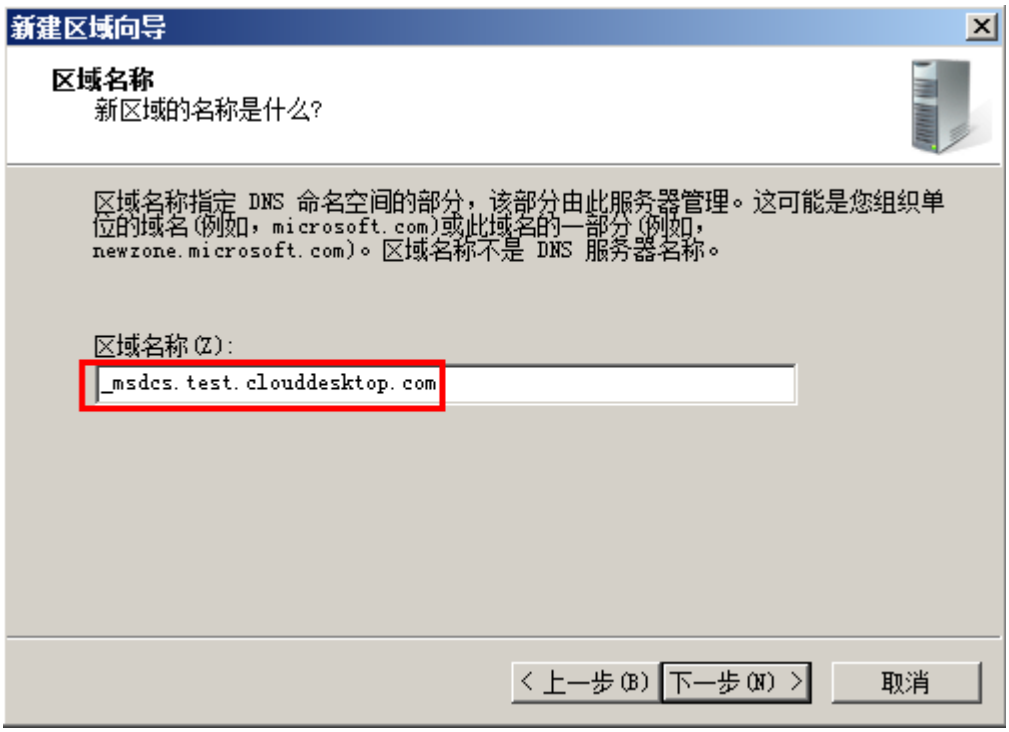

图 44

完成区域新建后，选中，点击右键，选择“新建域”

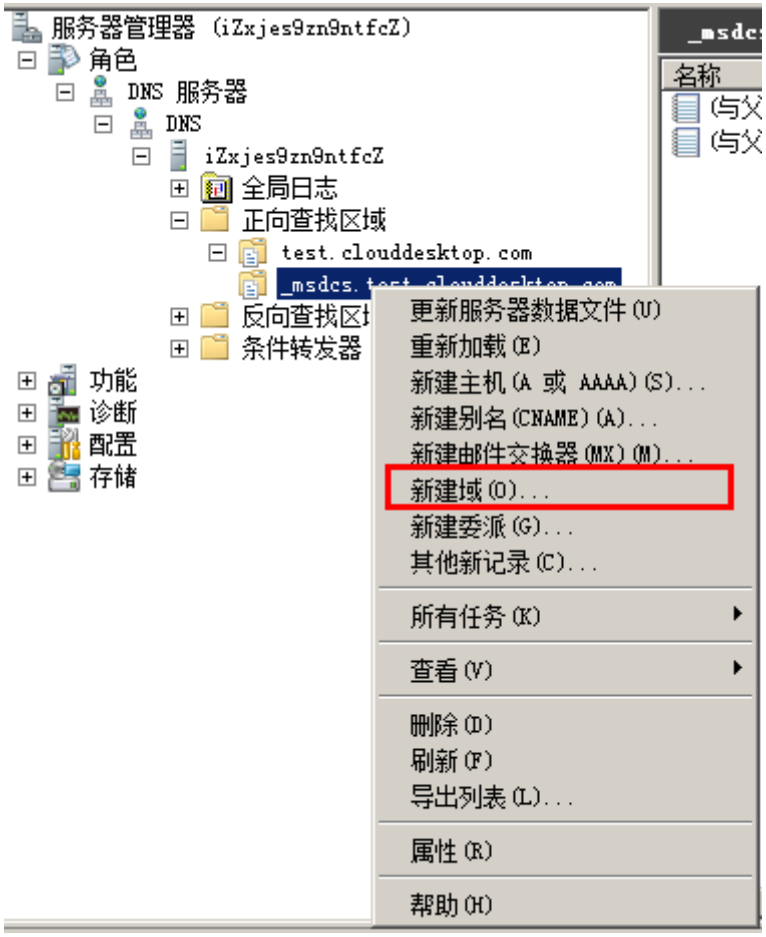

图 45

在“新建 DNS 域” 图 46 中输入 dc，点击确定

图 46

7. 选择新建的域 dc，并点击右键，选择“其他新记录” 图 47

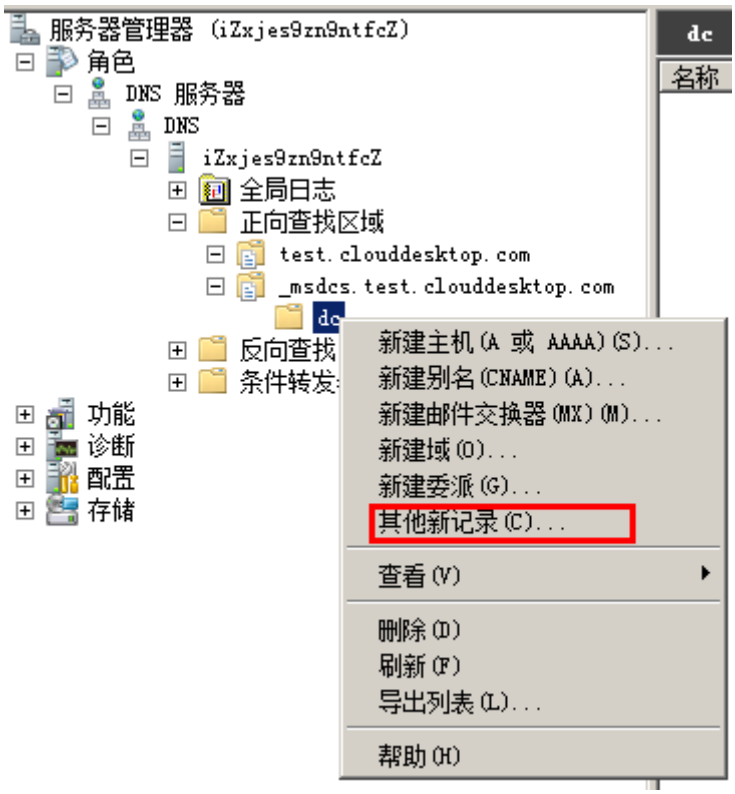

图 47

在“资源记录类型”中选中“服务位置(SRV)”,并点击“创建记录” 图 48

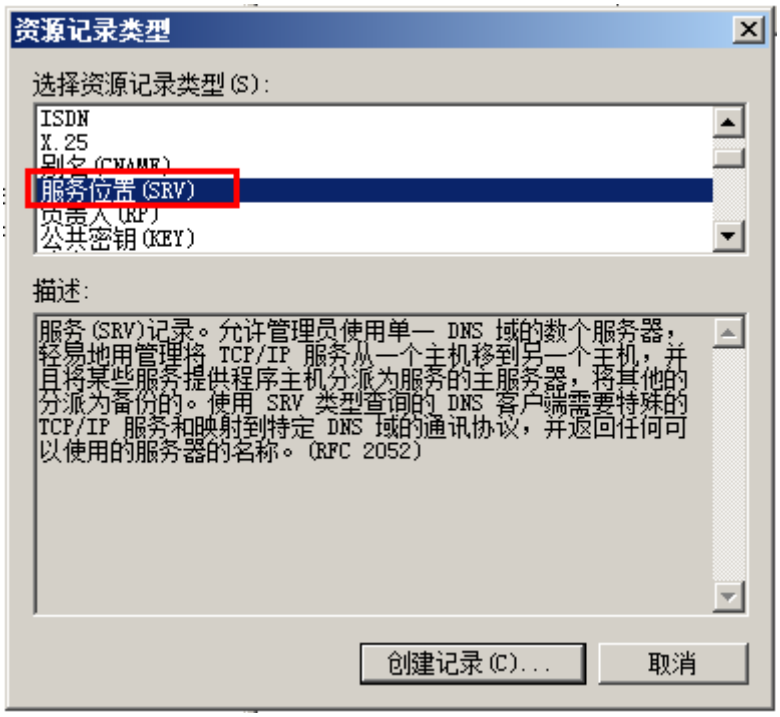

图 48

在“新建资源记录”窗口，“服务(S)”栏中选中_ldap，在“提供此服务的主机”中输入 AD 域控服务器的域地址，即步骤 F 中新建的第二个区域地址，点击确定和完成