搭建云桌面专有网络内 Windows AD 服务器

本文主要指导用户搭建基于专有网络（VPC）的 AD，并配置到云桌面环境设置中。

1. 云资源准备

1.1 创建 VPC 和交换机

此处创建的 VPC 将被设置到云桌面环境设置中，如已创建请忽略。

1. 在 VPC 控制台 选中需要配置云桌面环境的区域（图 1.1.1），如选中 **华东 1**，并点击 **创建专有网络**

图 1.1.1

2. 创建 VPC(图 1.1.2)时请设置好其名称和网段，点击 **创建 VPC**

图 1.1.2

专有网络创建完成以后，请创建交换机，为了保证高可用，请至少在两个不同的可用区创建两个交换机。在创建占有网络完成以后(图 1.1.3)，点击 **管理交换机**

图 1.1.3

3. 创建交换机时，请配置好其网段（图 1.1.4），点击 **确定**

图 1.1.4

交换机创建完成以后，可以在交换机列表里面查询到其配置，检查是否正确。

图 1.1.5

1.2 创建安全组

此处创建的安全组将设置到云桌面环境配置中，如已创建请忽略。

1. 在 ECS 控制台选择 **网络和安全 – 安全组，**并选中刚才创建 VPC 的区域，如华东 1，点击 **创建安全组** （图 1.2.1）

图 1.2.1

2. 在安全组创建页面，**网络类型** 选择 **专有网络，** **专有网络** 选择 1.1 中创建完成的专有网络（图 1.2.2）,点击 **确定，**在没有特殊网络控制的情况下，可以**不设置安全组规则**。

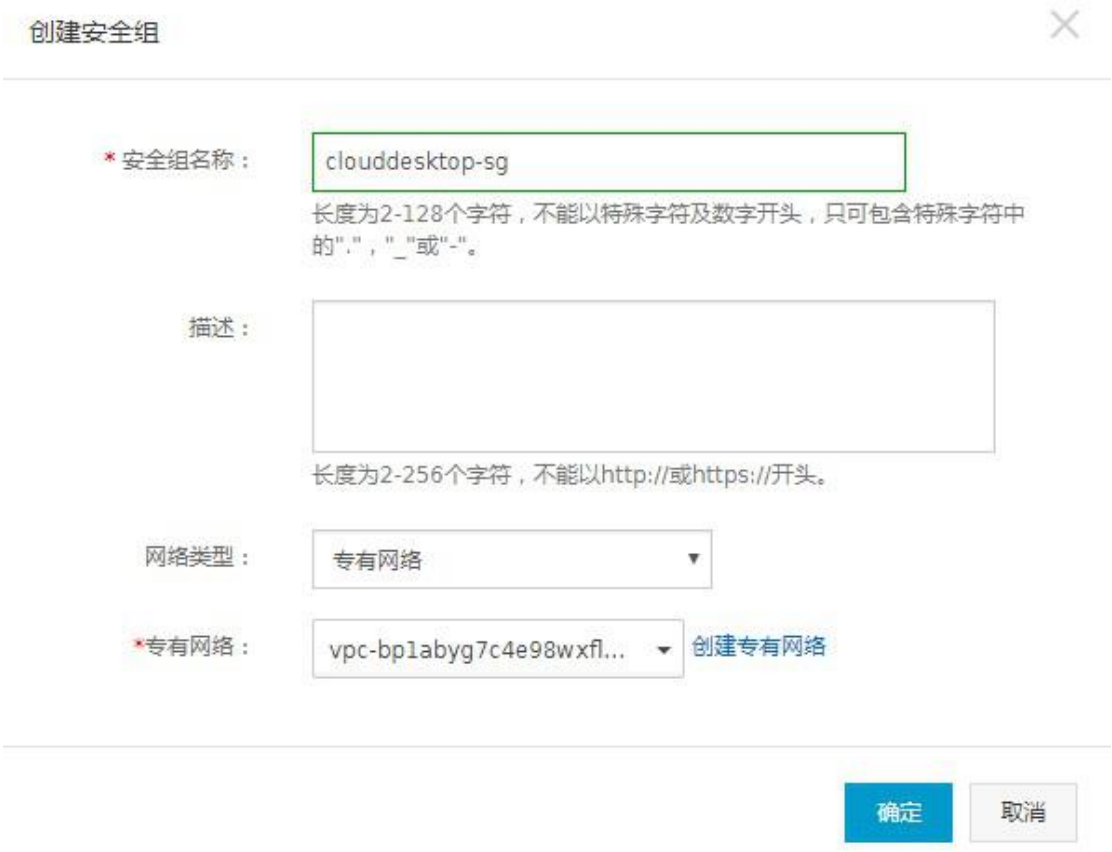

图 1.2.2

1.3 创建云服务器实例

为了保证 AD 的高可用性，最好购买两台基于 VPC 的云主机实例。

1. 在 ECS 控制台，选择 **实例**，选中需要配置云桌面环境的区域（图 1.3.1），必须和创建的 VPC 在同一个区域，如 **华东 1**，点击 **创建实例**

图 1.3.1

2. 在云服务器购买页面，请正确选择 **地域**，并选择前面创建的 **网络 VPC、交换机、安全组**（图 1.3.2），如遇到交换机对应的可用区无法购买实例，请返回 VPC 控制台重新选择新的可用区配置交换机。滚动页面，选择 **实例类型、实例配置、镜像、存储**等配置，假如需要管理的云桌面实例少于 1000，建议选择 **系列 II、共享计算型 n1、2 核 4G 配置**，镜像类型必须选择 **Windows server 2008 R2 企业版 64 位中文版。**继续滚动页面，在 **安全设置** 中输入 **登陆密码** 用于 Windows 登陆，请记住设置的密码。 最后点击 **立即购买。**

图 1.3.2

图 1.3.3

3. 重复步骤 2，并选择不同的交换机，购买另一台 ECS 实例作为备 AD 服务器，保证 AD 的高可用性。
4. 在 ECS 控制台确认云服务器实例是否已经创建成功。如没有创建，请点击右上角的刷新图标。

图 1.3.4

至此云资源都已准备完成，可以进行 AD 服务器搭建。

2.AD 服务器搭建

2.1 主 AD 服务器搭建

1. 在 ECS 控制台，选择需要作为主 AD 服务器的实例，点击 **远程连接**（图 2.1.1），跳转到

管理终端 页面，复制 **远程连接密码**。通过输入远程连接密码，和云服务器进行连接，并通过左上角 **发送远程命令 CTRUL+ALT+DELETE**，输入服务器购买时设置的密码登陆到 Windows 内部。

图 2.1.1

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 2.1.2

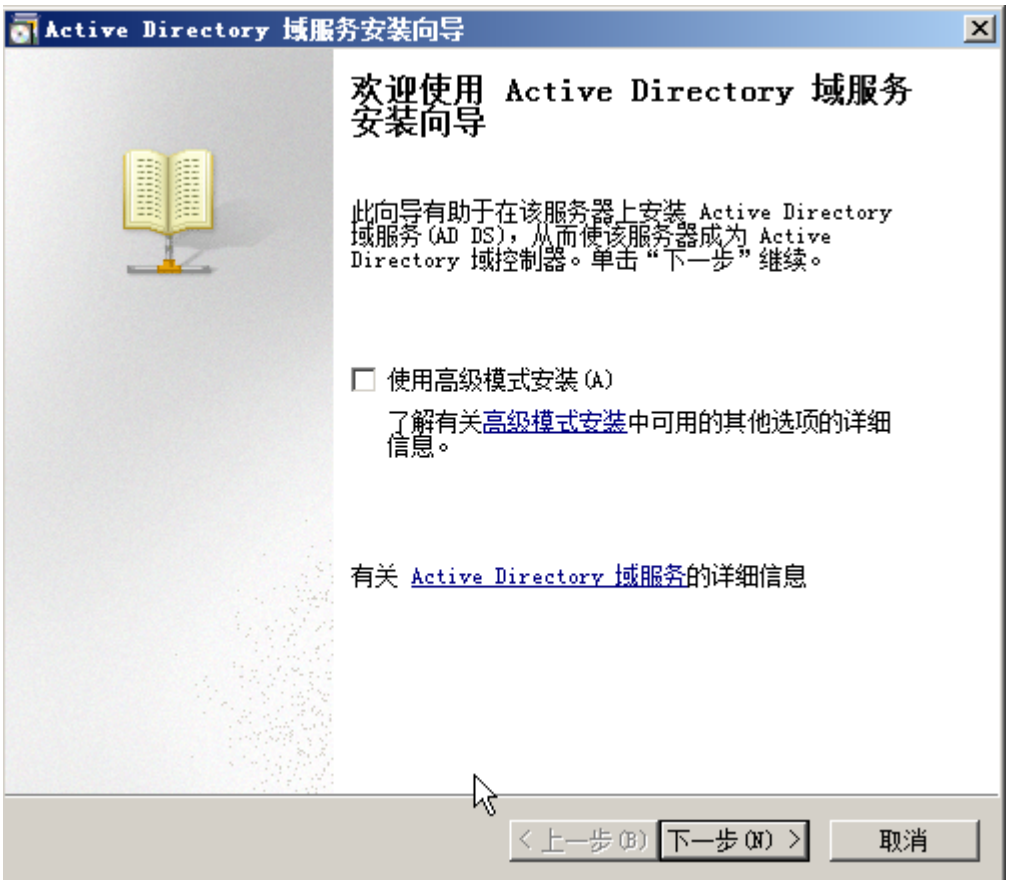

图 2.1.2

3. 点击下一步至 **选择某一部署配置** 图 2.1.3，选择中 **在新林中新建域**，并点击下一步

图 2.1.3

4. 在 **命名林根域** 图 2.1.4，输入 AD 域名（如 vpc.clouddesktop.com），点击下一步，系统自动验证创建 AD 相关的信息

图 2.1.4

5. 在 **设置林功能级别** 图 2.1.5 选择 Windows Server 2008 R2，点击下一步

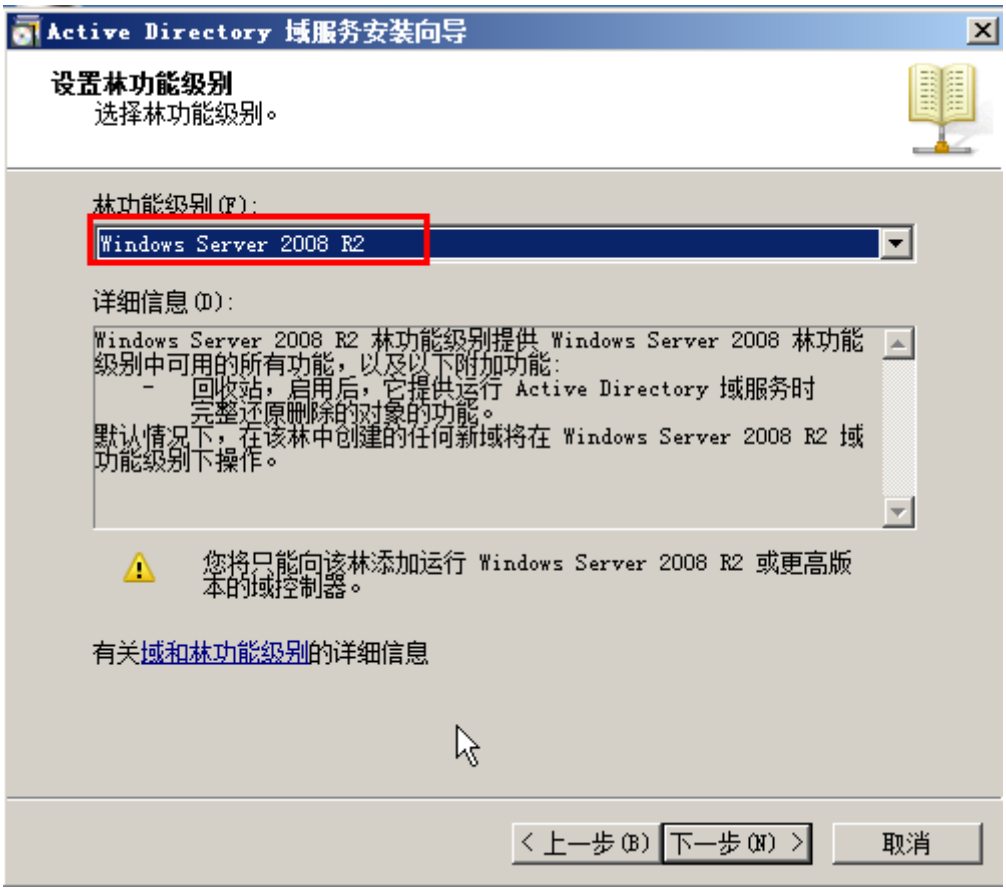

图 2.1.5

6. 在 **其他域控制器选项** 图 2.1.6，选中 **DNS 服务器(D)**,点击下一步

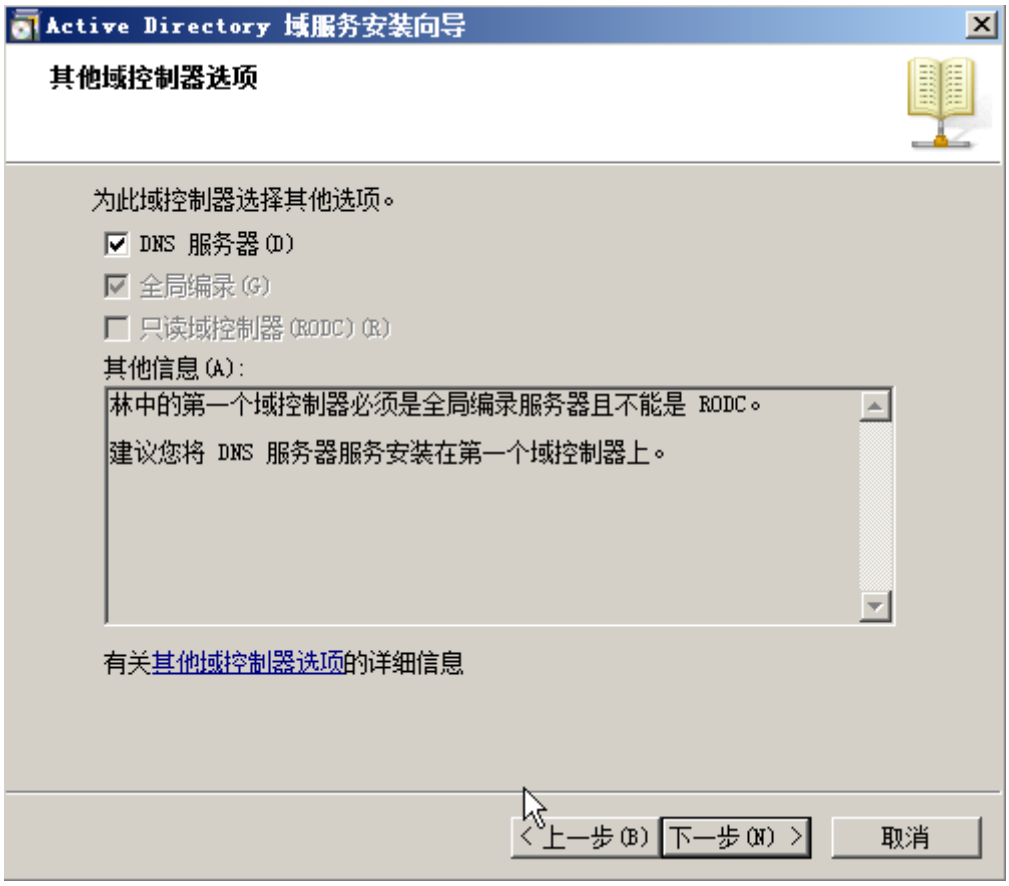

图 2.1.6

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 2.1.7，选择 **是**

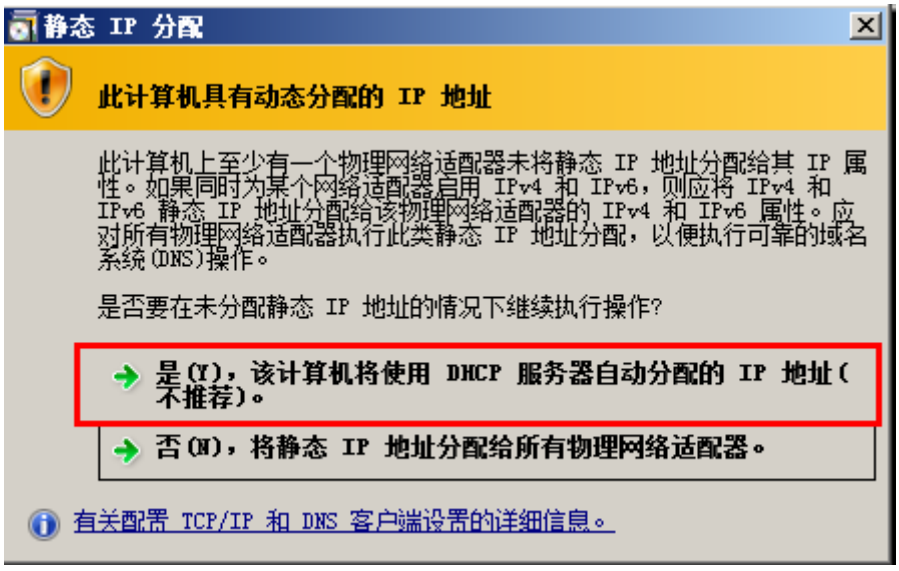

图 2.1.7

8. 在 **域服务安装向导** 图 2.1.8，选择 **是**

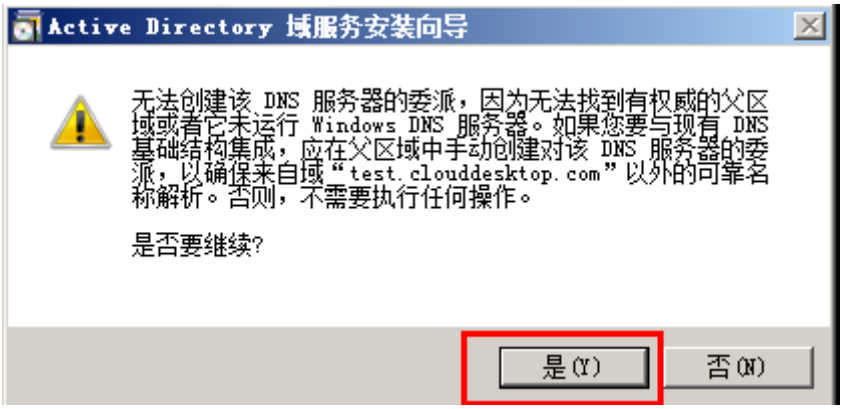

图 2.1.8

9. 在 **数据库、日志文件和 SYSVOL 的位置** 图 2.1.9，设置文件存放路径，点击下一步

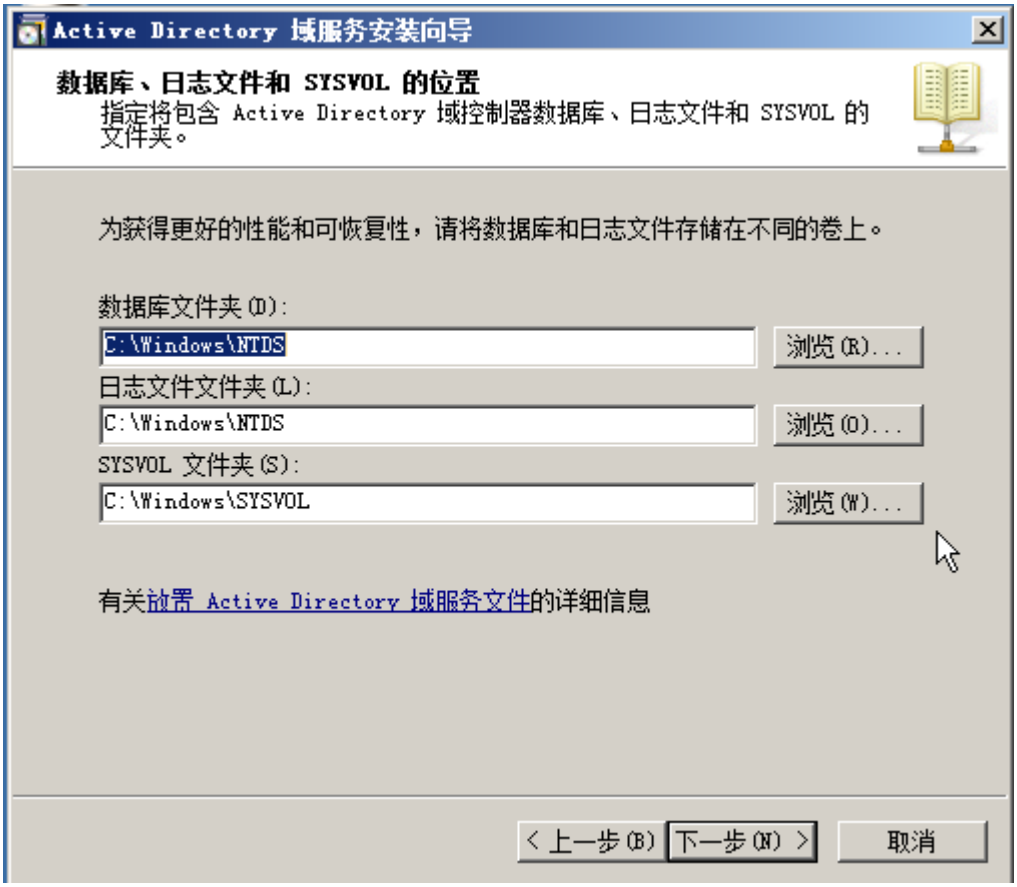

图 2.1.9

10. 在 **目录服务还原模式的 Administrator 密码** 图 2.1.10，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

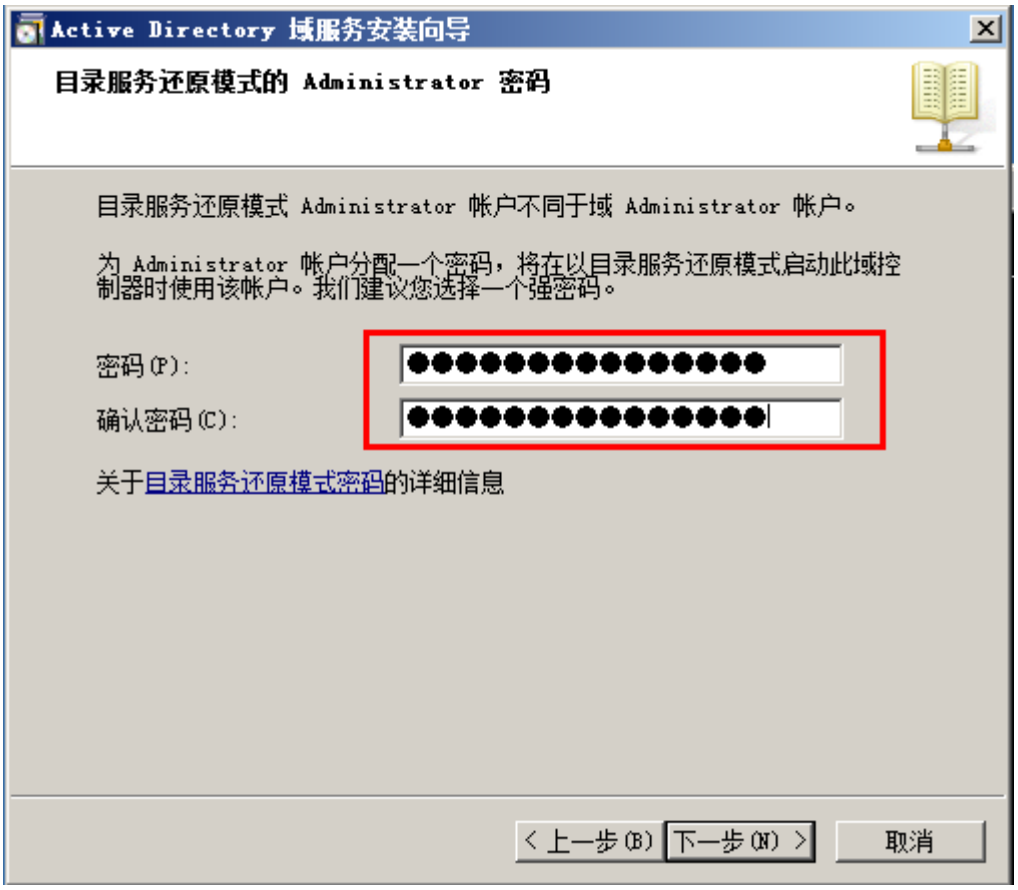

图 2.1.10

11. 在“摘要” 图 2.1.11

可以选择 **导出设置(E)…**，用来保存 AD 创建的设置(保存到文件 vpc.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/vpc.cldouddesktop.com.txt

点击下一步

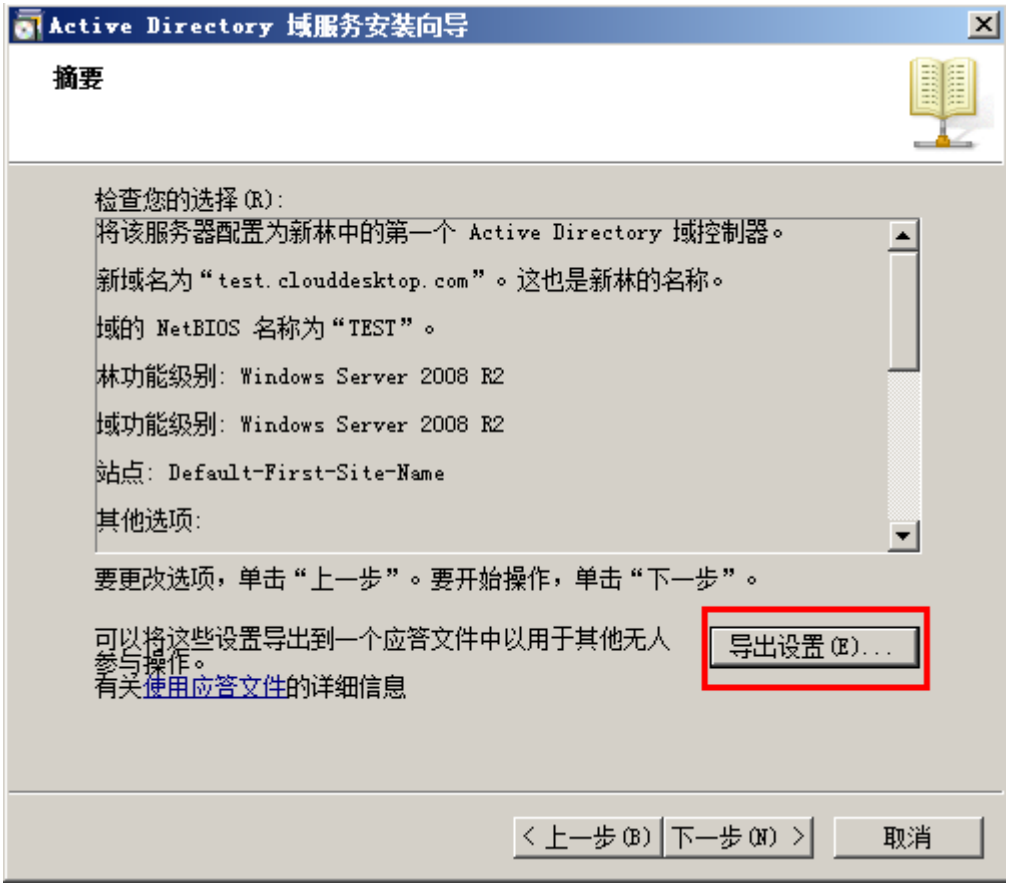

图 2.1.11

12. 系统开始创建 AD 图 2.1.12，创建完以后必须重启，因此可以选中 **完成后重新启动**

图 2.1.12

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 2.1.12，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

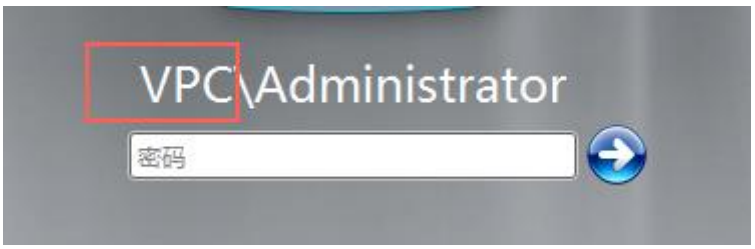

图 2.1.13

14. 在 Windows 任务栏启动 **服务器管理器** 图 2.1.14

图 2.1.14

在 **服务器管理器** 窗口 图 2.1.15，选中 **服务器管理器**，点击右键，点击 **添加角色**

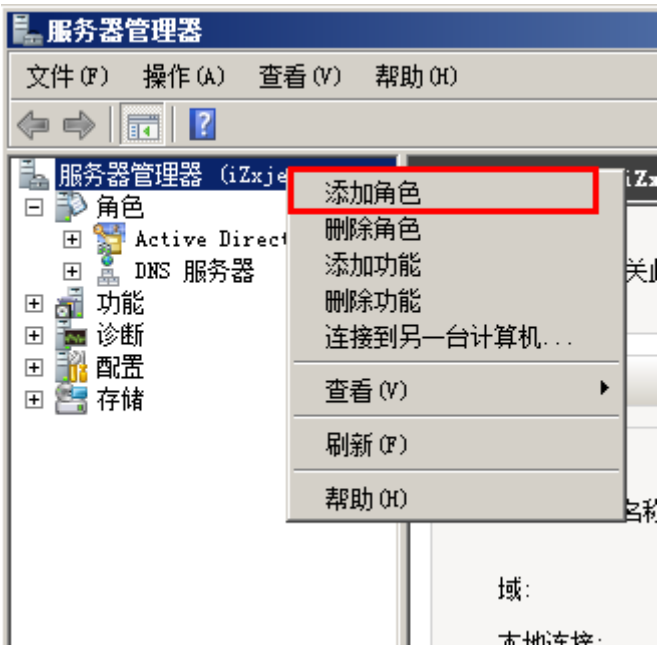

图 2.1.15

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 2.1.16，选中 **Activity Directory 证书服务**，点击下一步

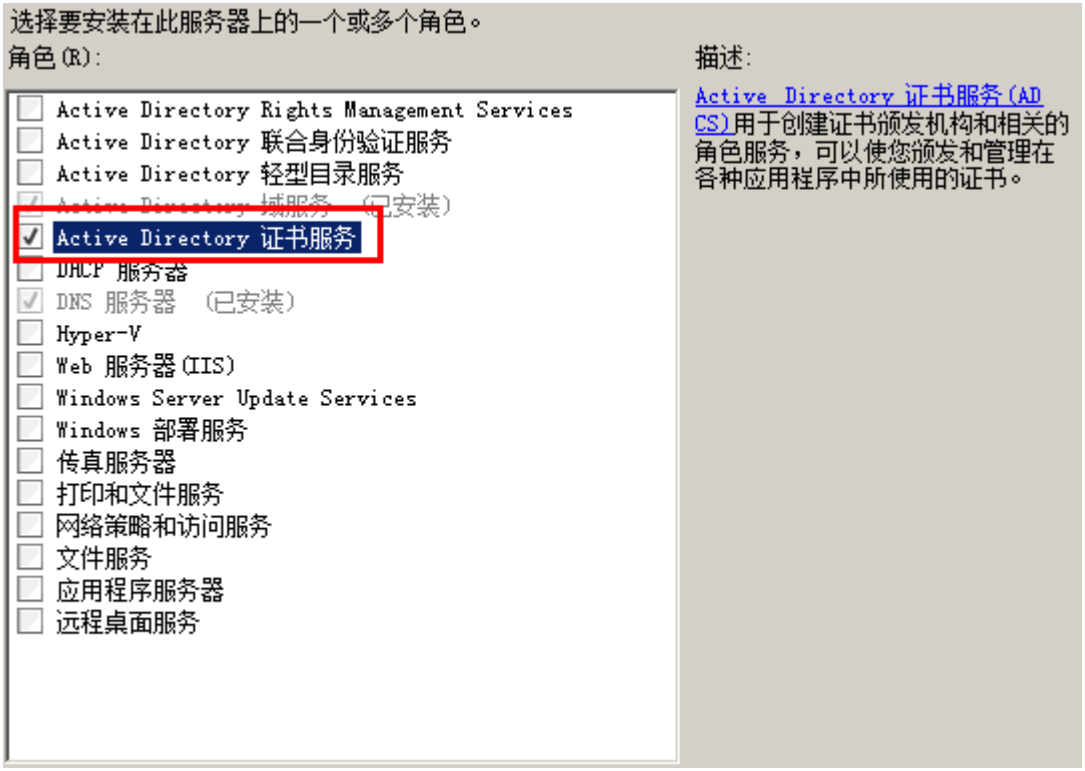

图 2.1.16

16. 在 **选择为 Activity Directory 证书服务安装的角色服务：** 图 2.1.17， 选中 **证书颁发机构 Web 注册** ，并点击 **添加所需的角色服务** 图 2.1.18，点击下一步

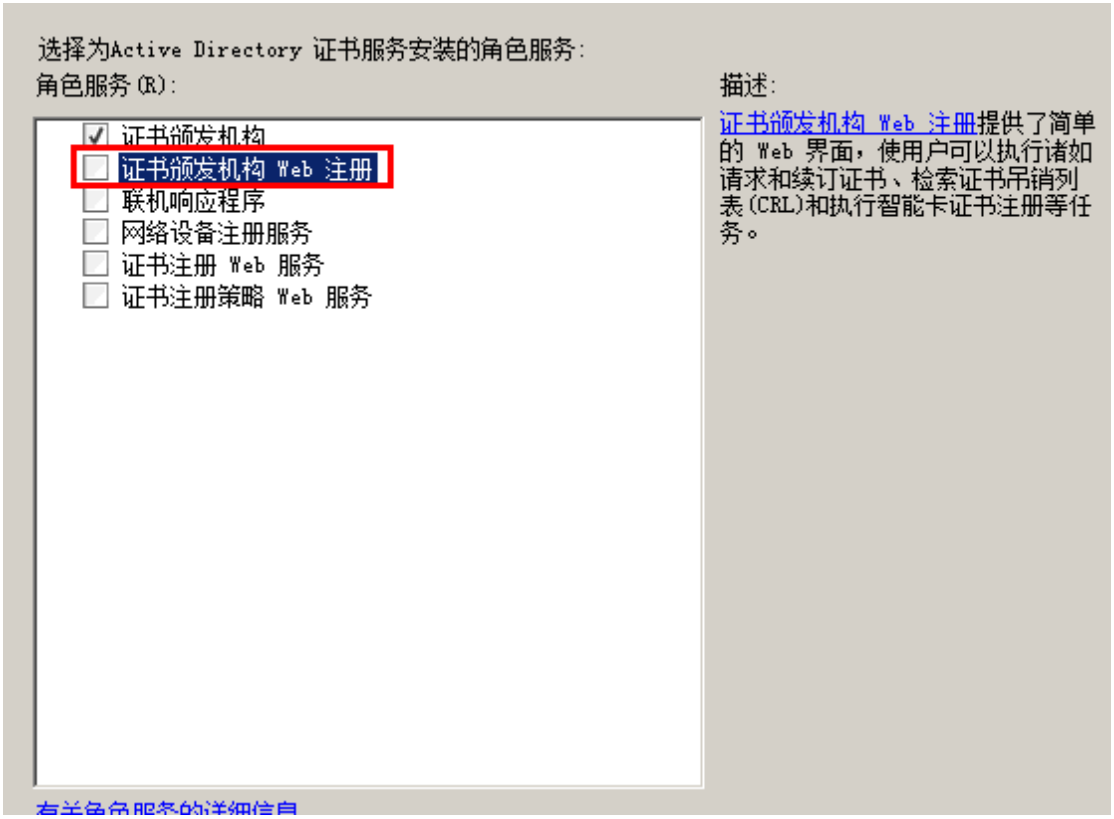

图 2.1.17

图 2.1.18

在 **指定安装类型** 图 2.1.19，选择 **企业**，点击下一步

图 2.1.19

在 **指定 CA 类型** 图 2.1.20，选择 **根 CA(R)**,点击下一步

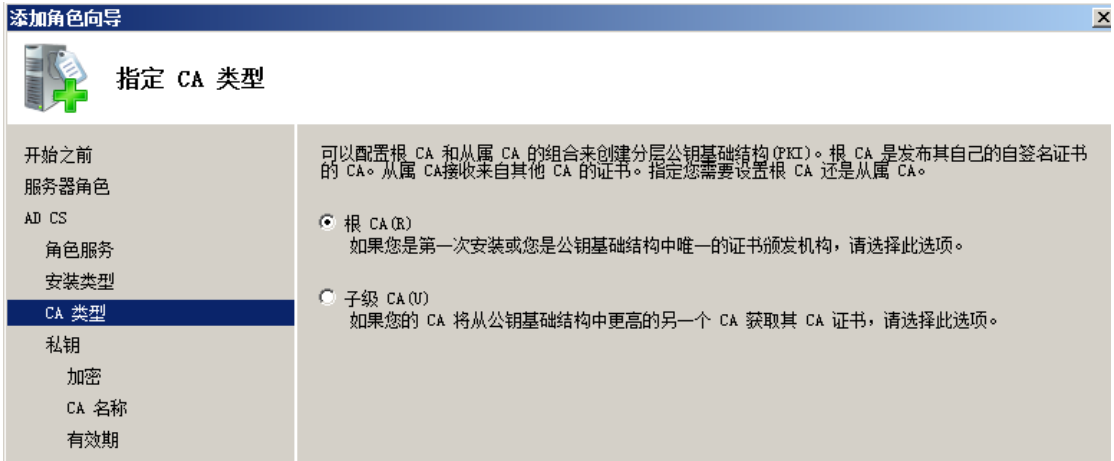

图 2.1.20

在 **设置私钥** 图 2.1.21，选择 **新建私钥**

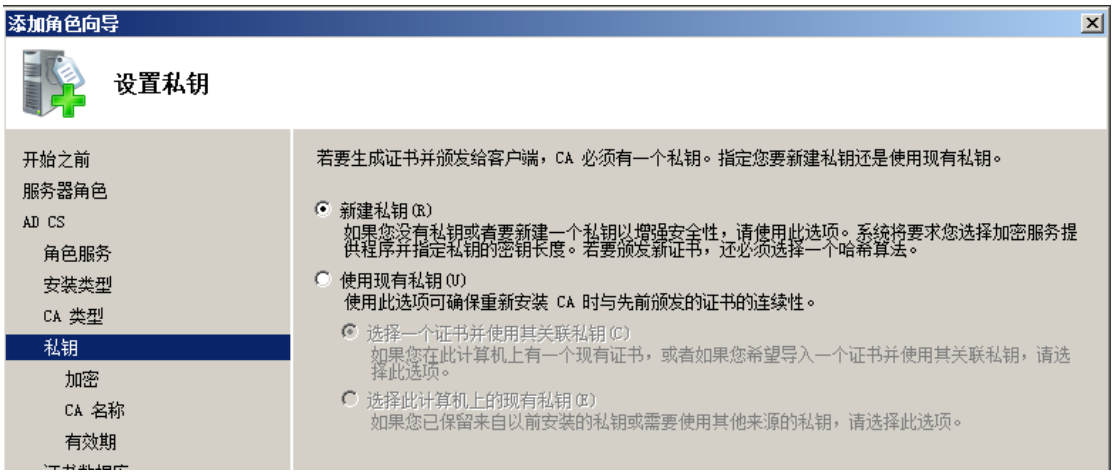

图 2.1.21

在 **为 CA 配置加密** 图 2.1.22，设置秘钥相关内容，点击下一步

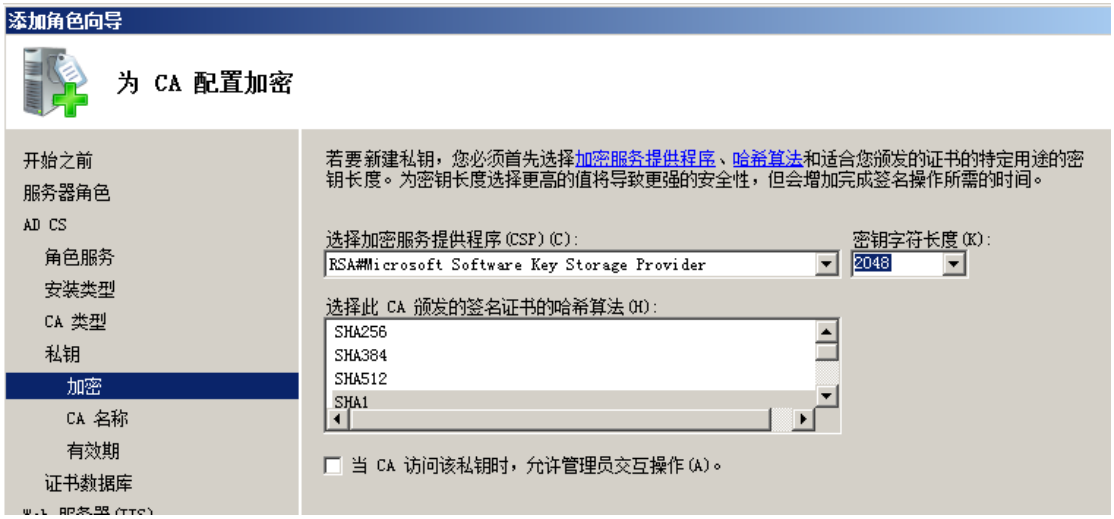

图 2.1.22

在 **配置 CA 名称** ，设置证书名称，点击下一步

图 2.1.23

在 **设置有效期** 图 2.1.24，设置证书有效期，点击下一步

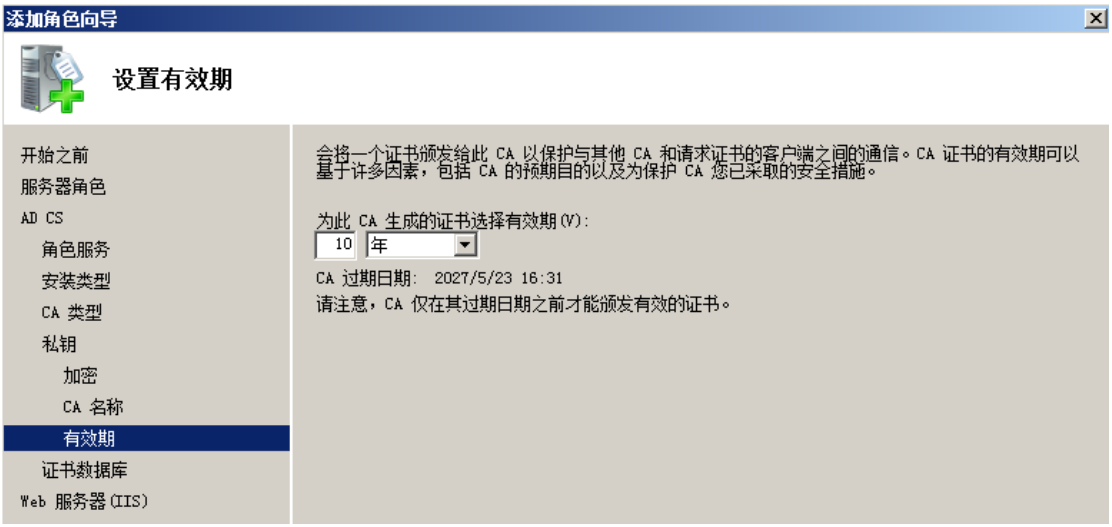

图 2.1.24

在 **配置证书数据库** 图 2.1.25，设置数据库位置，点击下一步

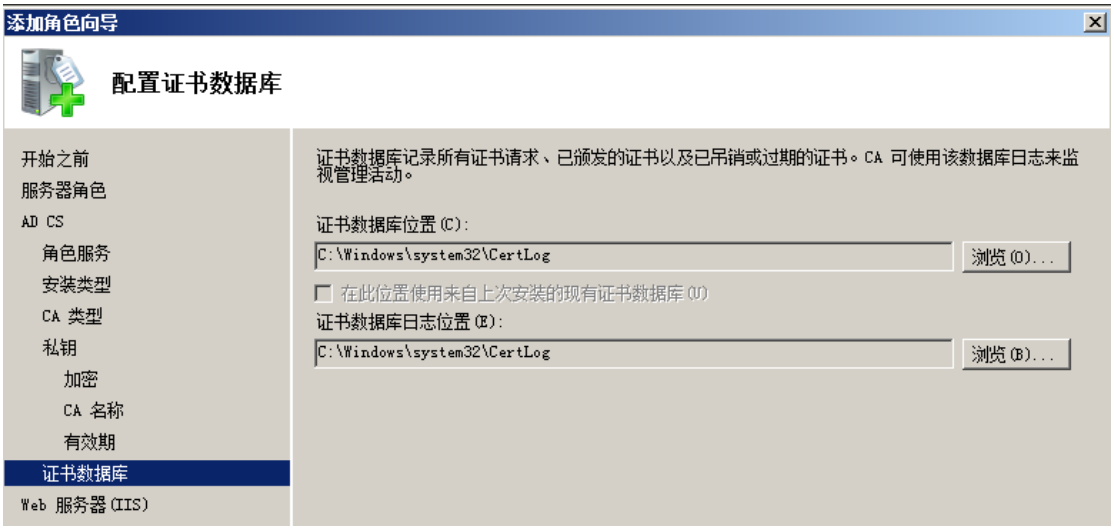

图 2.1.25

在 **选择角色服务** 图 2.1.26，选择系统默认的服务即可，点击下一步

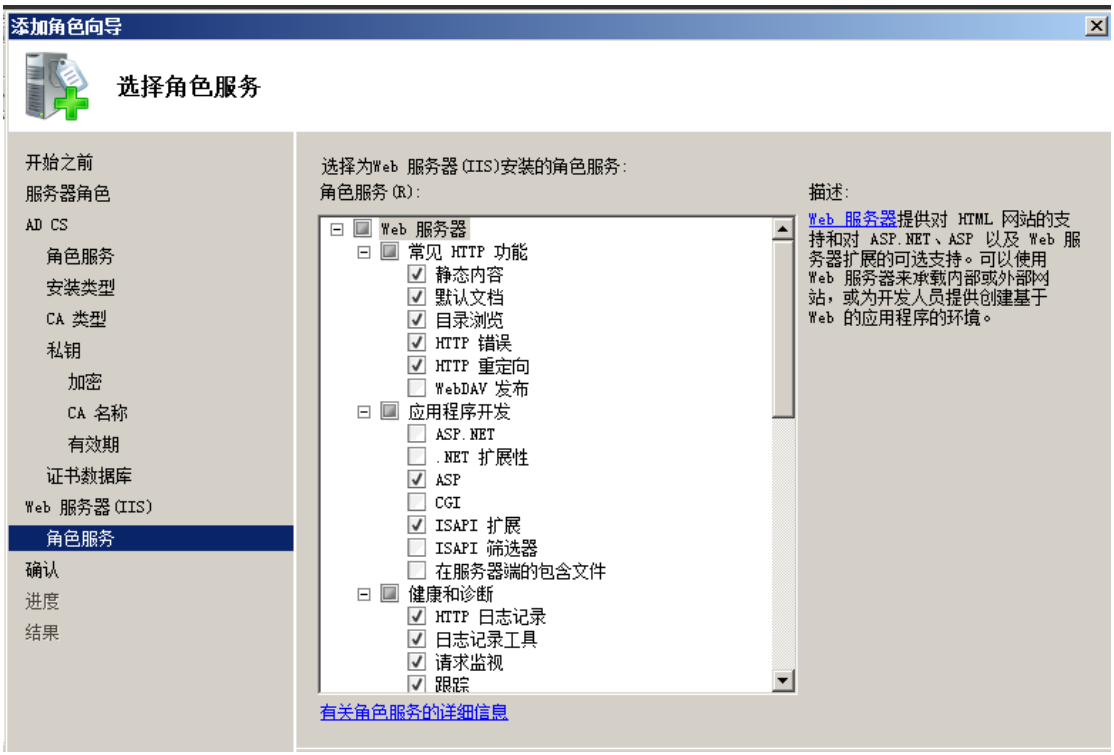

图 2.1.26

17. 在 **确认安装选择** 图 2.1.27，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 2.1.27

18. 证书服务安装完成以后，可以在 **服务器管理器** 窗口 图 2.1.28，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。

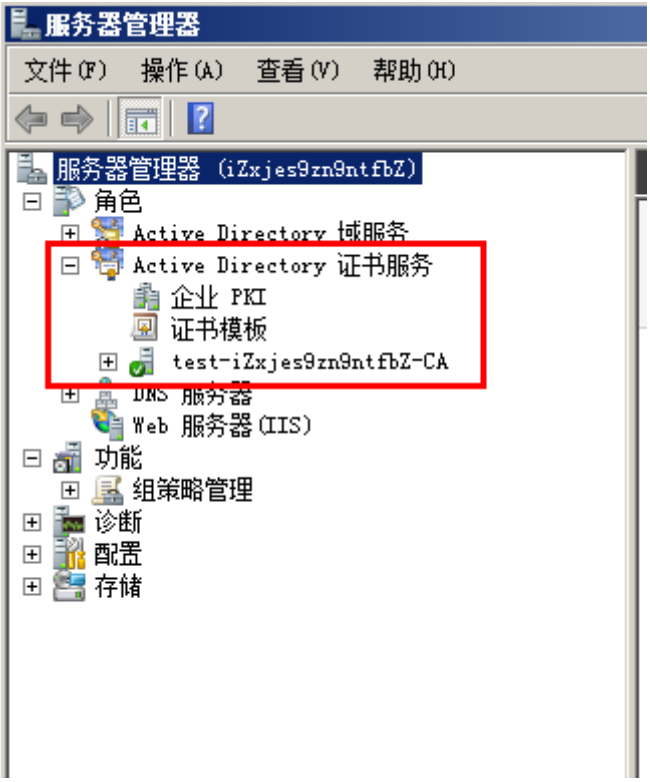

图 2.1.28

19. 为了确保 AD 服务器可以正确设置到云桌面系统中，请手动重置一下管理员密码（图 2.1.29），重置密码时，请不要勾选 **用户下次登录时需更改密码**（图 2.1.30）

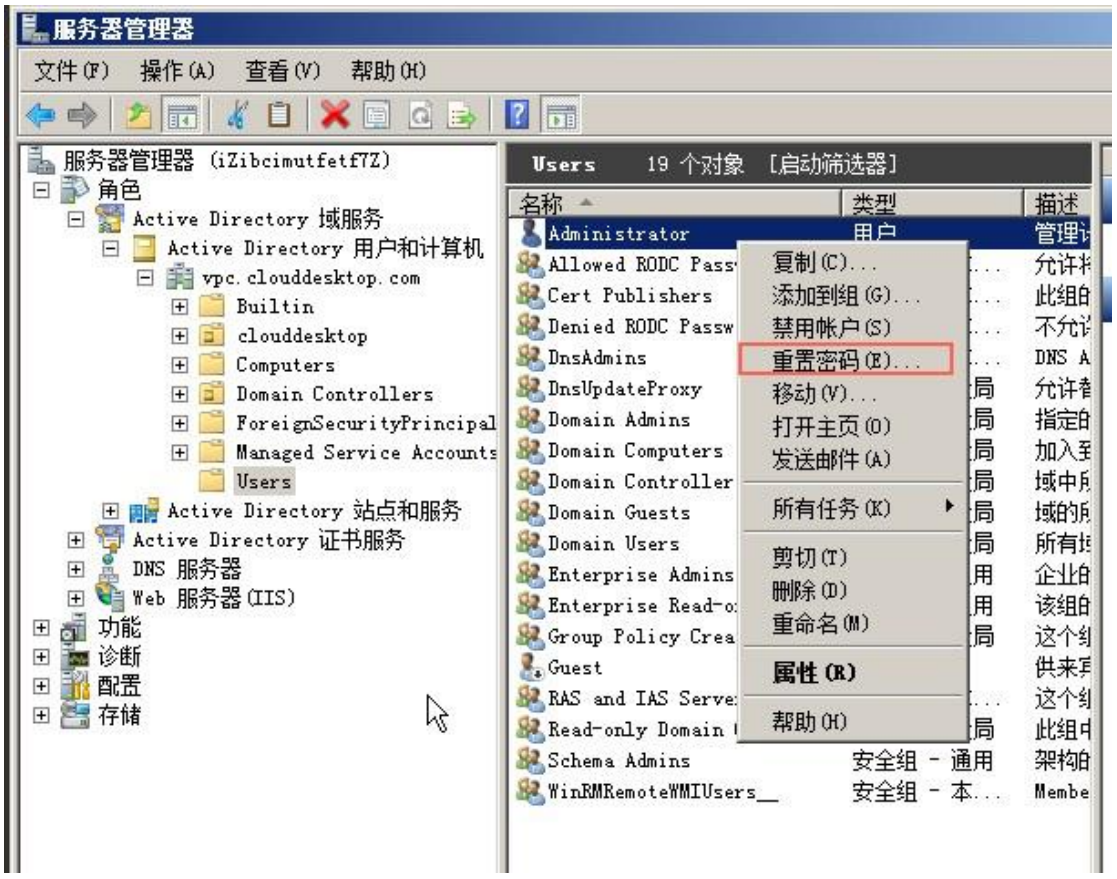

图 2.1.29

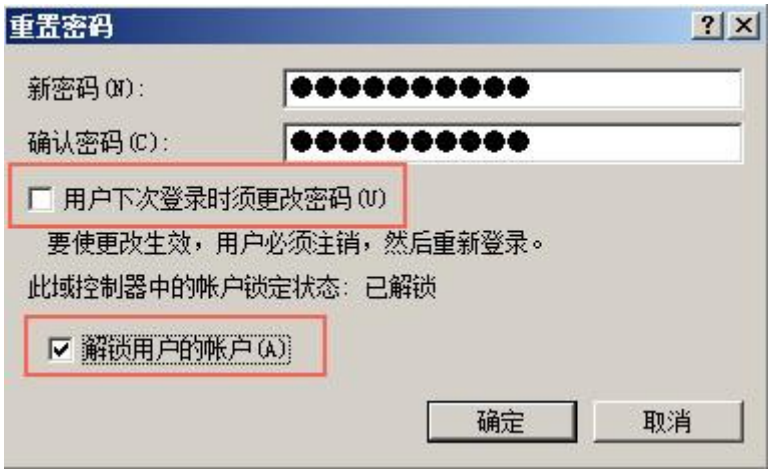

图 2.1.30

20. 主 AD 服务器已经安装和配置完成，重启 AD 服务器。

2.2 备 AD 服务器搭建

1. 在 ECS 控制台查看主 AD 服务器的 IP 地址（图 2.2.1），并记录。选择另一台需要搭建备 AD 服务器，通过远程连接登陆到 Windows 内部。

图 2.2.1

2. 在 Windows 中，打开命令窗口，输入 **c:\windows\system32\sysprep\sysprep.exe**，打开 **系统准备工具**（图 2.2.2），选中 **进入系统全新体验** 勾选 **通用**，点击 **确定**。等系统清理完成后重启系统（有可能会提示 **尝试使用 Sysprep 处理计算机时出错**，直接手动重启即可）。系统重启后，需要重新设置登录密码。

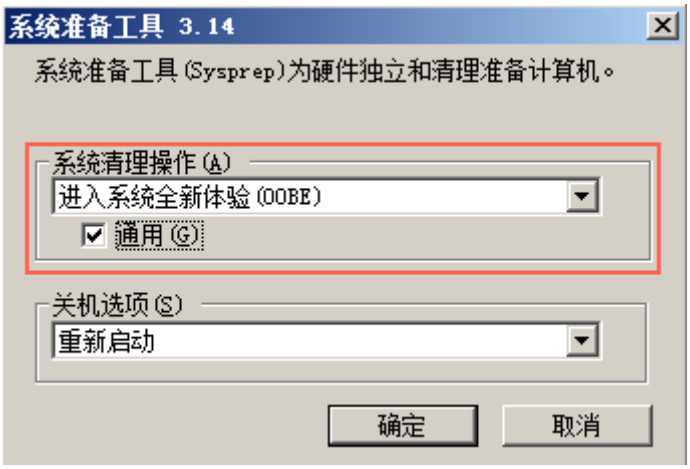

图 2.2.2

3. 在 Windows 中，打开 **网络连接 – 本地连接 – Internet 协议版本 4（TCP/IPV4）属性**（图 2.2.3），选中 **使用下面的 DNS 服务器地址**，在 **首先 DNS 服务器** 中填入主域控的 IP 地址，点击 **确定**。DNS 配置完成以后，可以打开命令窗口，ping 主域控设置的域名。

假如域名成功转换成解析成主域控的 IP 地址，并收到回复，说明 DNS 设置正确，否则请检查 AD 服务器和 DNS 配置是否正确。

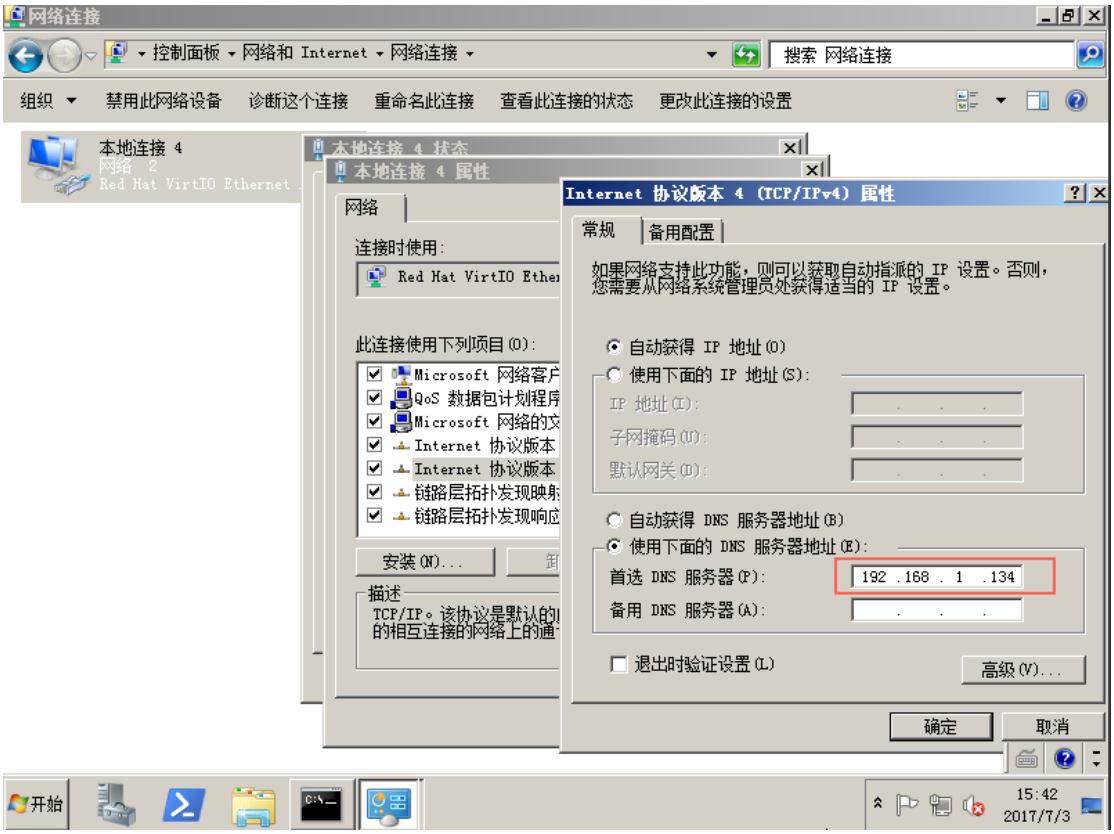

图 2.2.3

4. 打开一个命令窗口，并输入 dcpromo,打开 **Activity Directory 域服务安装向导** (图 2.2.4)，点击下一步至 **选择某一部署配置** 中 **现有林 – 向现有域添加域控制器** (图 2.2.5)，点击下一步

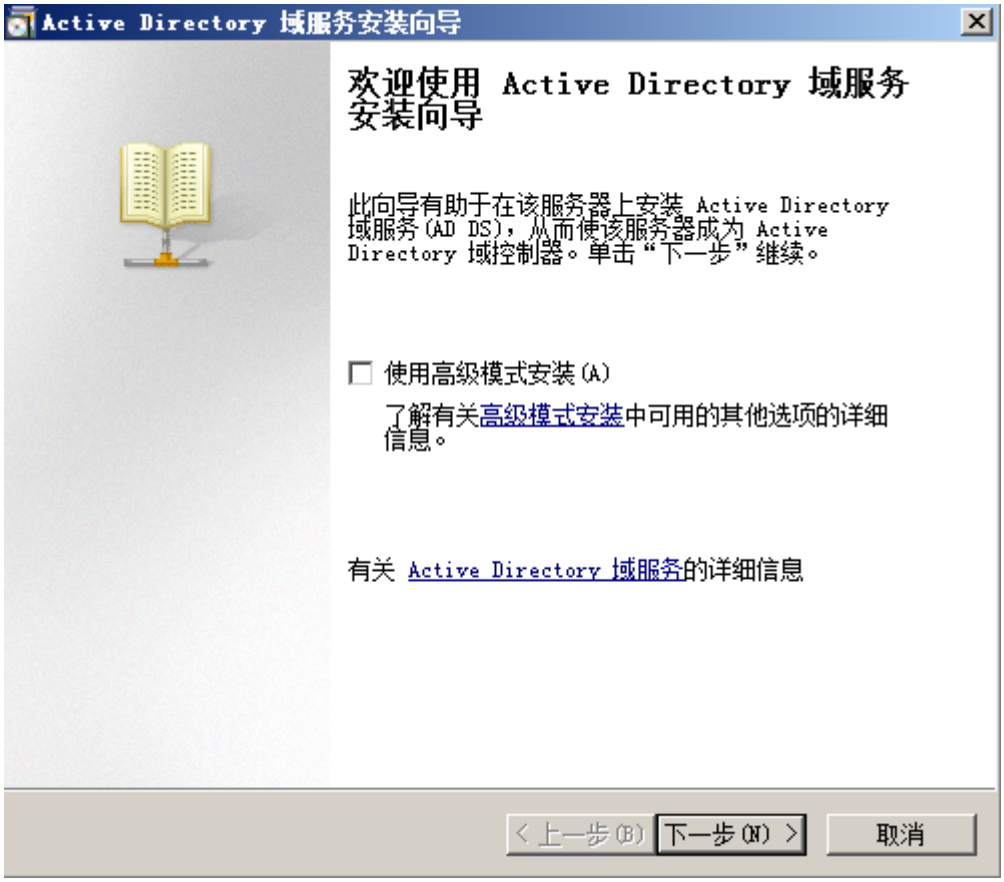
Active Directory 域服务安装向导
欢迎使用 Active Directory 域服务安装向导
此向导有助于在该服务器上安装 Active Directory 域服务(AD DS),从而使该服务器成为 Active Directory 域控制器。单击“下一步”继续。
使用高级模式安装(A)
了解有关高级模式安装中可用的其他选项的详细信息。
有关 Active Directory 域服务的详细信息
< 上一步(B)
下一步(N) >
取消

图 2.2.4

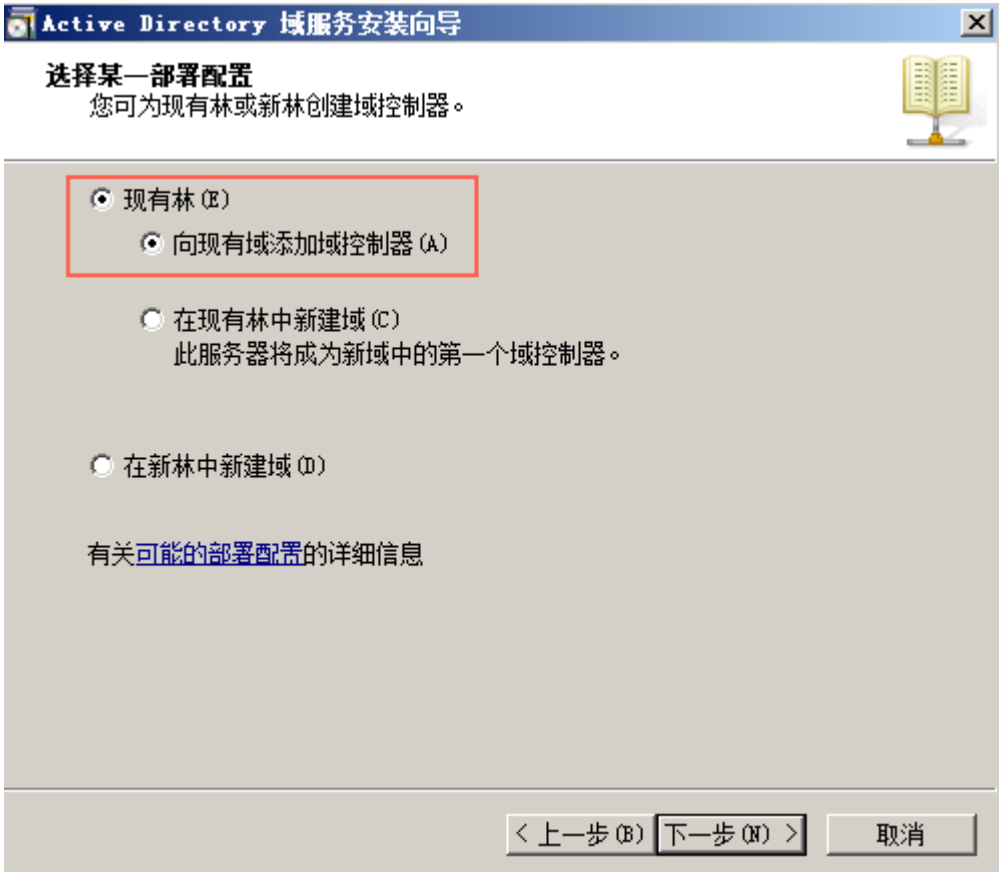
Active Directory 域服务安装向导
选择某一部署配置
您可为现有林或新林创建域控制器。
现有林(E)
向现有域添加域控制器(A)
在现有林中新建域(C)
此服务器将成为新域中的第一个域控制器。
在新林中新建域(D)
有关可能的部署配置的详细信息
< 上一步(B)
下一步(N) >
取消

图 2.2.5

5. 在 **网络凭据** （图 2.2.6）窗口，输入 AD 的域名，选择 **备用凭据** ，点击 **设置** ，在 **网络凭据** （图 2.2.7）窗口中输入 AD 的管理员用户名和密码，点击确定，并点击下一步。

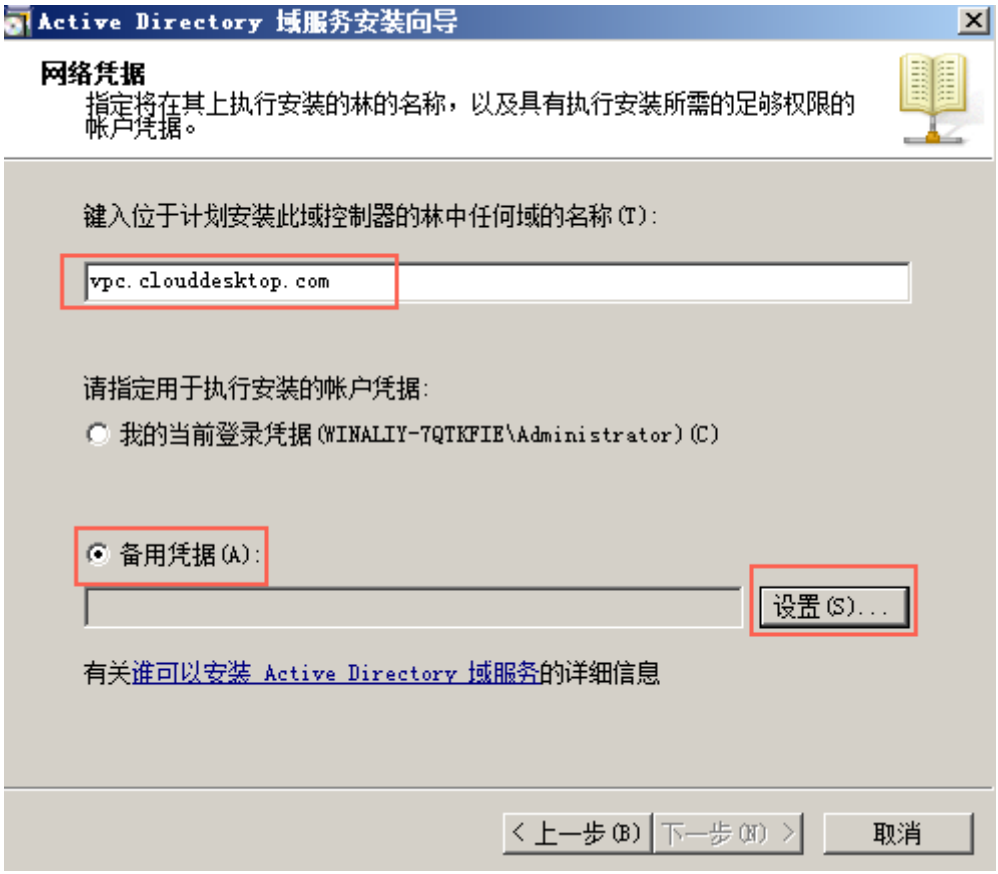

图 2.2.6

图 2.2.7

6. 在 其他域控制器选项 窗口(图 2.2.8)，默认**选中 DNS 服务器和全局编录**，点击下一步，在 **静态 IP 分配** （图 2.2.9）中点击 **否（是）**，点击下一步。在图 2.2.9 显示窗口中单击 是。

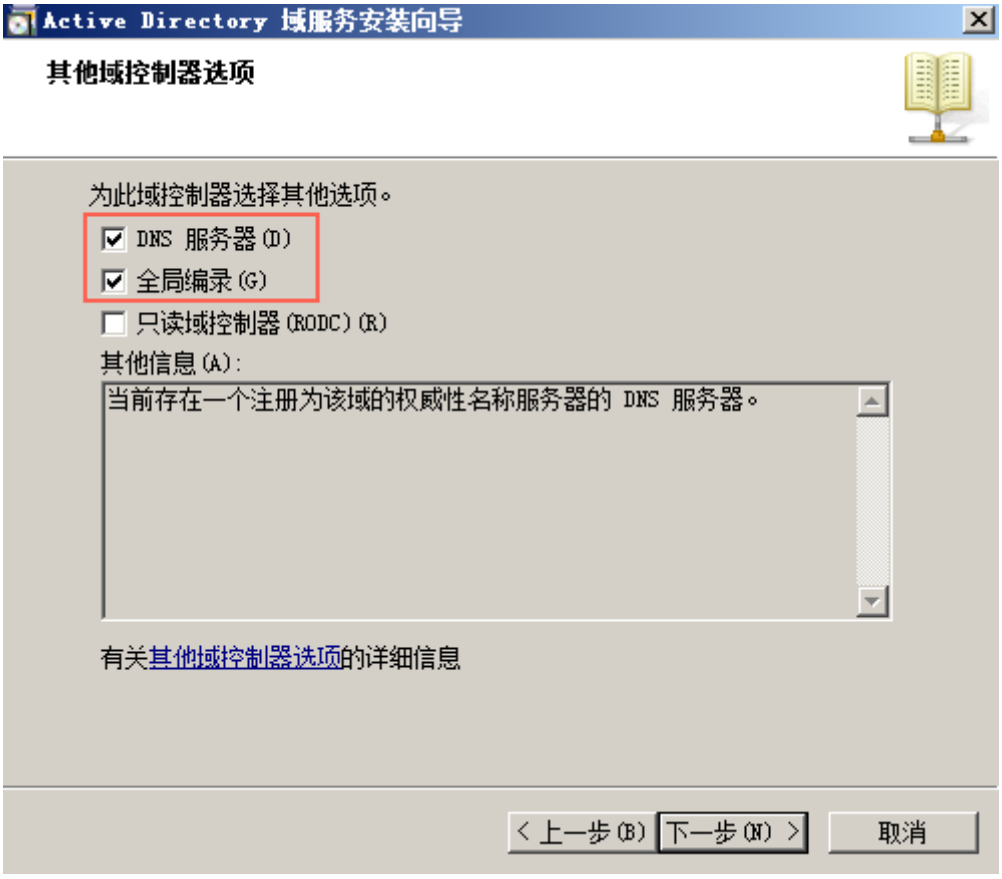
Active Directory 域服务安装向导
其他域控制器选项
为此域控制器选择其他选项。
DNS 服务器(D)
全局编录(G)
只读域控制器(RODC)(R)
其他信息(A):
当前存在一个注册为该域的权威性名称服务器的 DNS 服务器。
有关其他域控制器选项的详细信息
< 上一步(B)
下一步(N) >
取消

图 2.2.8

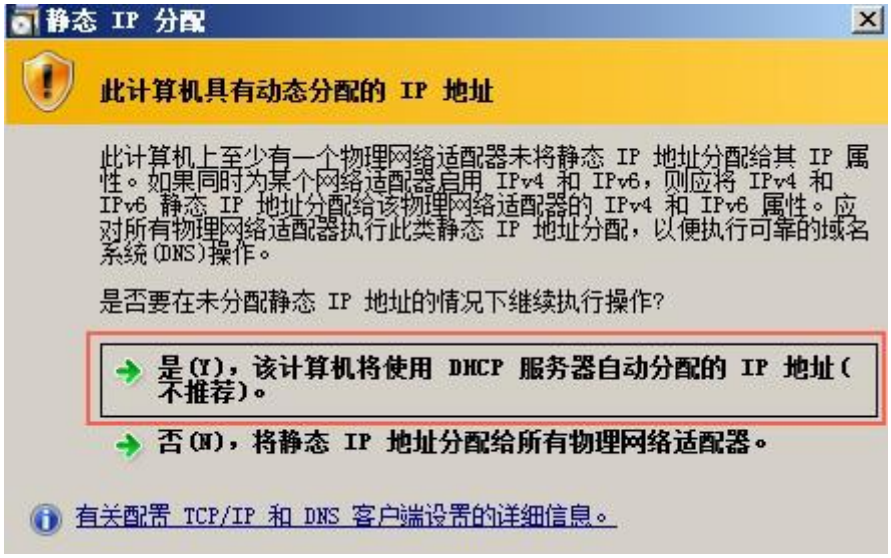
静态 IP 分配
此计算机具有动态分配的 IP 地址
此计算机上至少有一个物理网络适配器未将静态 IP 地址分配给其 IP 属性。如果同时为某个网络适配器启用 IPv4 和 IPv6，则应将 IPv4 和 IPv6 静态 IP 地址分配给该物理网络适配器的 IPv4 和 IPv6 属性。应对所有物理网络适配器执行此类静态 IP 地址分配，以便执行可靠的域名系统(DNS)操作。
是否要在未分配静态 IP 地址的情况下继续执行操作?
是(Y)，该计算机将使用 DHCP 服务器自动分配的 IP 地址(不推荐)。
否(N)，将静态 IP 地址分配给所有物理网络适配器。
有关配置 TCP/IP 和 DNS 客户端设置的详细信息。

图 2.2.9

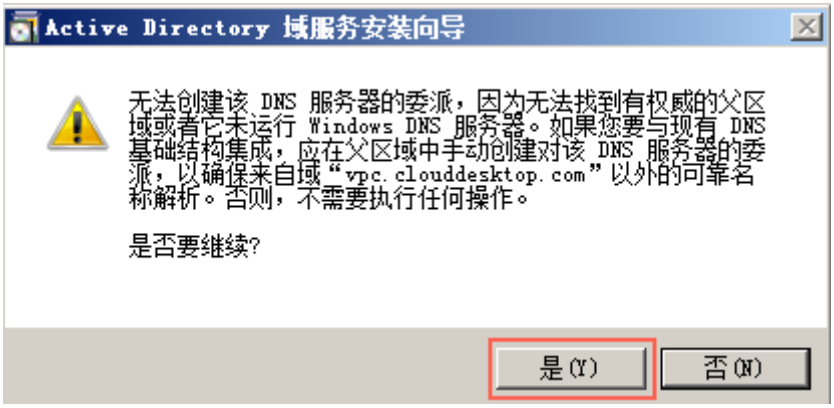

图 2.2.10

7. 在 **数据库、日志文件和 SYSVOL 的位置** （图 2.2.11）窗口中设置这几个文件的保存位置。

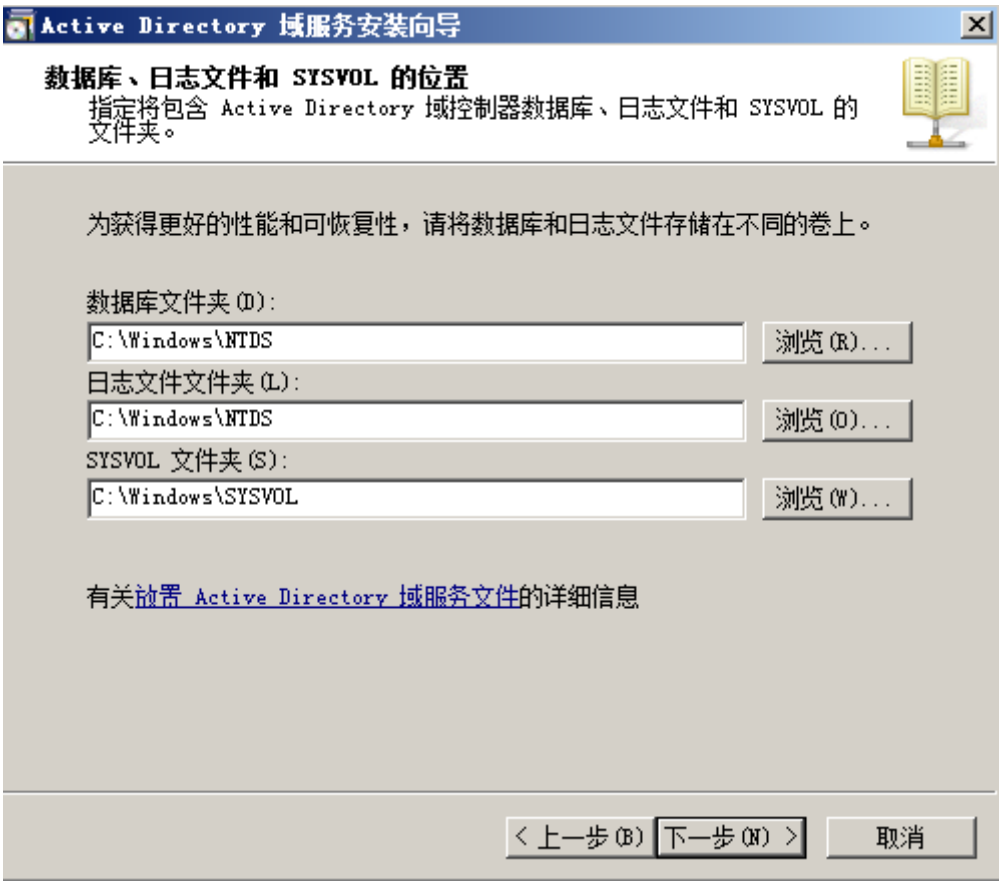

图 2.2.11

8. 在 **目录服务还原模式的 Administrator 密码** （图 2.2.12）中设置还原密码。点击下一步，等待备 AD 服务器配置完成后重启。

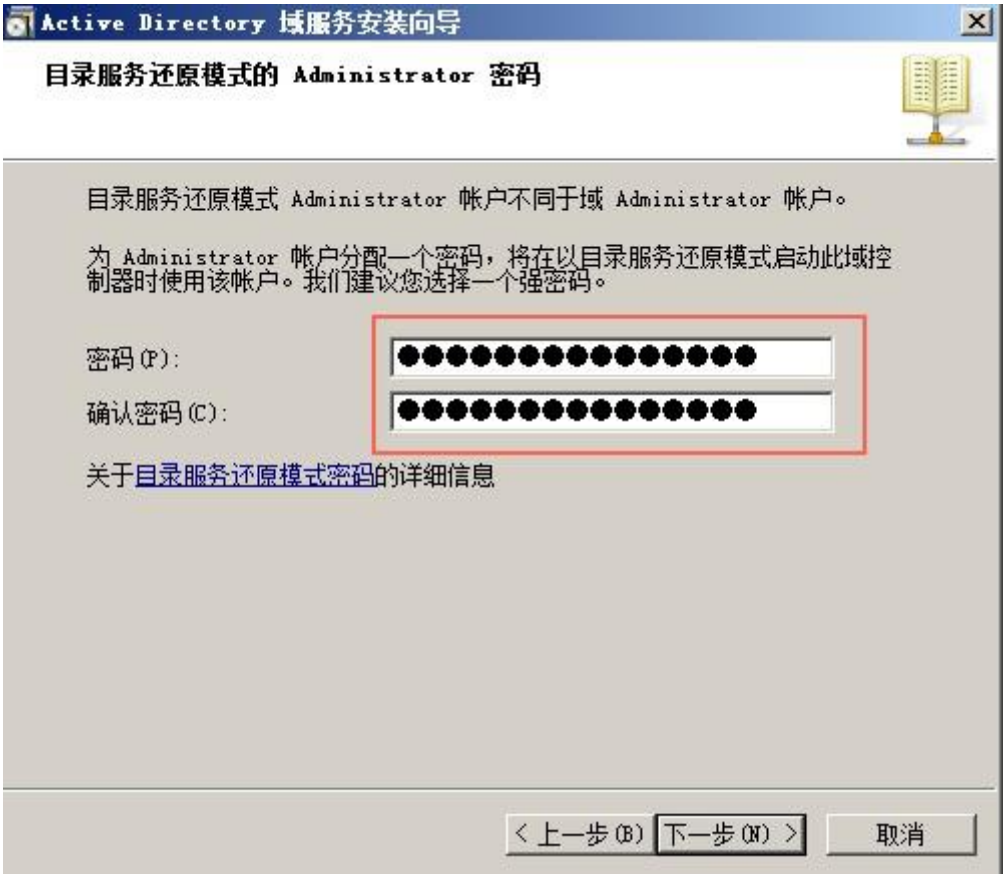
Active Directory 域服务安装向导
目录服务还原模式的 Administrator 密码
目录服务还原模式 Administrator 帐户不同于域 Administrator 帐户。
为 Administrator 帐户分配一个密码，将在以目录服务还原模式启动此域控制器时使用该帐户。我们建议您选择一个强密码。
密码(P):
确认密码(C):
关于目录服务还原模式密码的详细信息
< 上一步(B)
下一步(N) >
取消

图 2.2.12

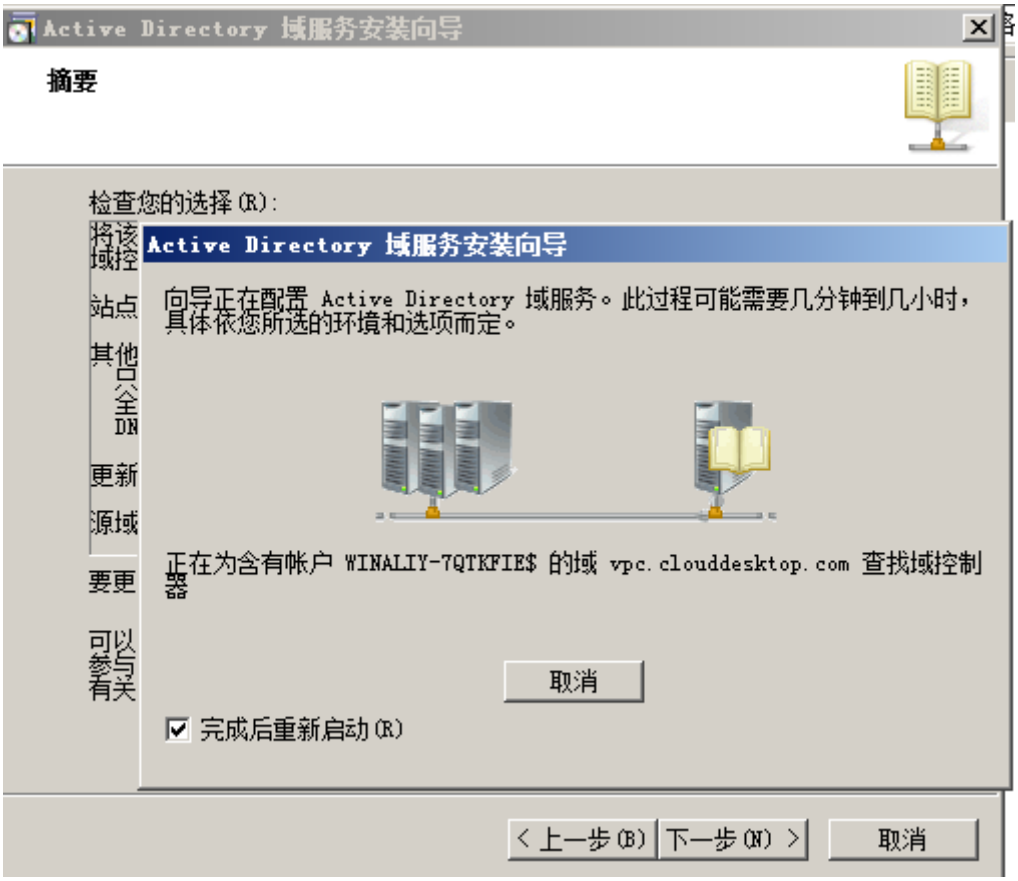
Active Directory 域服务安装向导
摘要
检查您的选择(R):
Active Directory 域服务安装向导
向导正在配置 Active Directory 域服务。此过程可能需要几分钟到几小时，具体依您所选的环境和选项而定。
正在为含有帐户 WINALIY-7QTKFIE$ 的域 vpc.clouddesktop.com 查找域控制器
取消
完成后重新启动(R)
< 上一步(B)
下一步(N) >
取消

图 2.2.13

9. 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 2.2.14，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 2.2.14

10. 打开 **服务器管理器 – 添加角色 – 添加角色向导**，点击下一步到 **选择服务器角色**（图 2.2.15），点击下一步到 **选择角色服务**（图 2.2.16），选中 **证书颁发机构 Web 注册**，在 **添加角色向导** 弹框中，点击 **添加手续的角色服务** （图 2.2.17），点击下一步

图 2.2.15

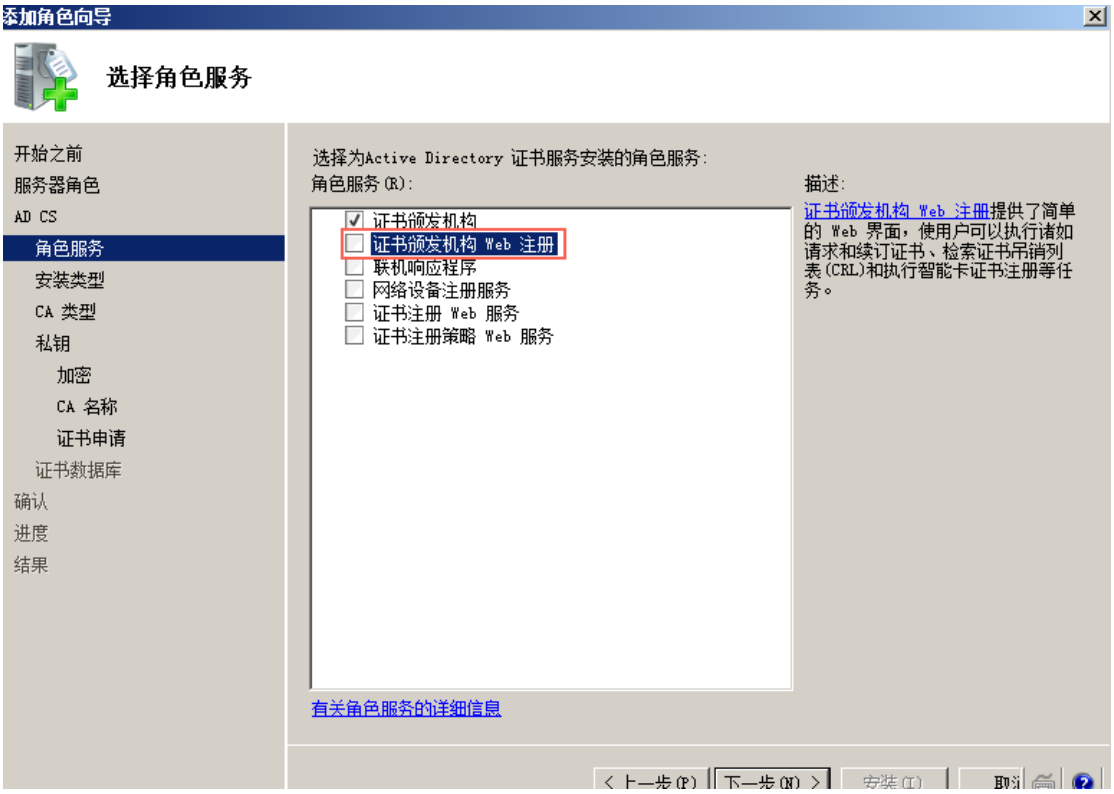

图 2.2.16

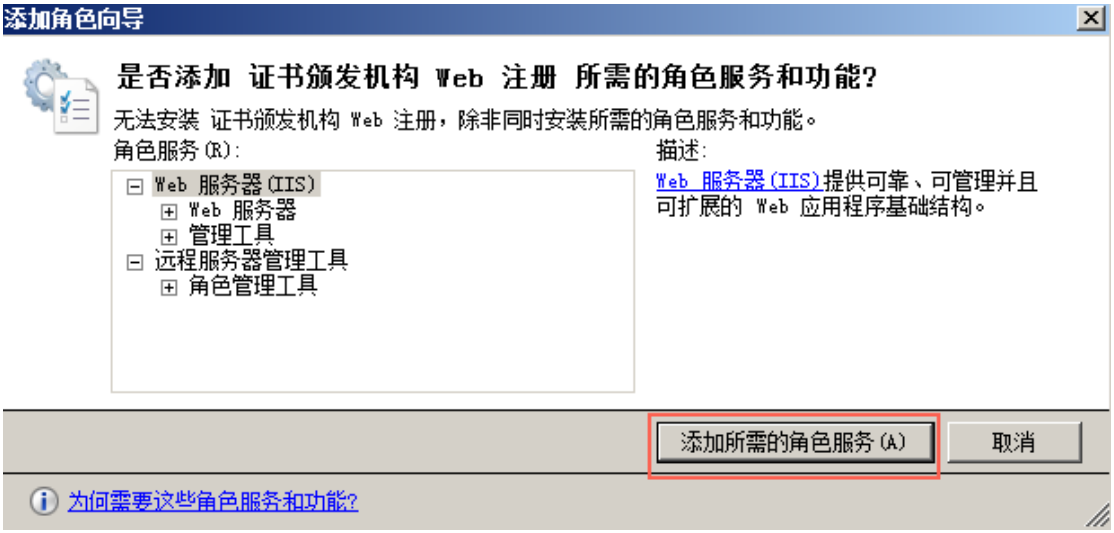

图 2.2.17

11. 在接下来的配置窗口中都选择系统默认配置，下一步直到 **向父 CA 申请证书** 窗口（图 2.2.18），选中 **将证书请求发送给父级 CA** ，点击 父 CA 后面的 **浏览**，弹出 **选择证书颁发机构**， 在弹框中过会列出主域控的 CA，选中，点击确定即可。最后点击下一步直到 **安装**，并点击安装。

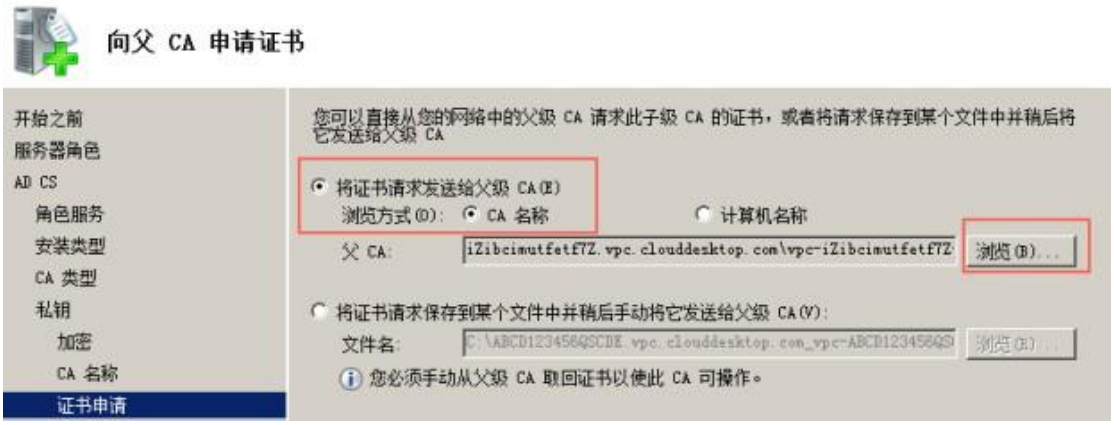

图 2.2.18

12. 等服务器安装 **证书服务和 Web 服务器** 完成以后，备 AD 服务器的证书服务也安装完成。
13. 重启 AD 服务器，重启完成以后，可以进行云桌面环境设置了。

3. 云桌面环境设置

1. 进入云桌面控制台，选中需要配置的区域（如华东 1），点击 桌面管理 – 创建，弹出 **云桌面环境设置** 窗口。
2. 在 **云桌面环境设置 – 选择专用网络** （图 3.1）中选择创建好的专有网络。点击下一步

图 3.1

3. 在 **云桌面环境设置 – 选择安全组**（图 3.2）中，选中域控服务器对应的安全组，点击下一步。

图 3.2

4. 在**云桌面环境设置 – AD 设置** 中，选择 AD 网络类型 为 专有网络，并根据 ECS 控制台上面的 IP 地址，填写到主 AD 服务器 IP 和备 AD 服务器 IP 中,最后填写好 AD 域名和管理员账号、密码，点击确定。