



北京四通管理软件技术有限公司
Beijing Stone Software Technology Co., Ltd



POC标准化实施指南

基础环境

02 微软基础构架环境安装

版本：v1.0

修正历史	2
第 1 章 主要步骤.....	3
第 2 章 安装参数及注意事项一览表.....	3
第 3 章 域控服务器配置	4
第 4 章 组策略设置	12
第 5 章 配置 DNS 服务，安装及配置 DHCP 服务	14
第 6 章 活动目录用户和 OU 准备	24
第 7 章 组织单位（Citrix）委派.....	32
第 8 章 环境完成确认检查.....	35
第 9 章 Windows CA 服务器安装配置	36
产品版本	41

修正历史

修正	改变说明	更新者	日期
V1.0	新建	陈余南、李申君、 孙凌、杨华	2014年7月11日

第1章 主要步骤

本章节介绍了Citrix虚拟化环境下基础架构服务器安装的基本过程。其包括了：

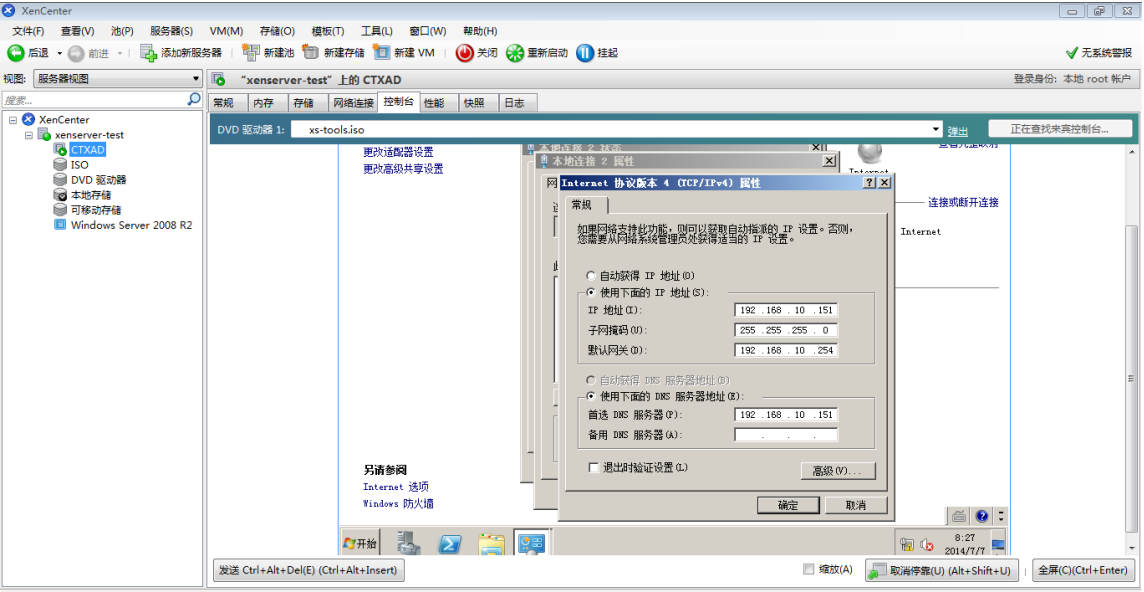
- 域控服务器的基本安装
- 安装配置活动目录（同时完成DNS安装）
- 配置DNS和安装并配置DHCP服务
- 环境完成确认

本章节开始前，请确认《PoC手册 - 1 基础环境 - Lab 01虚拟主机基础环境安装1.0》均已完成。

第2章 安装参数及注意事项一览表

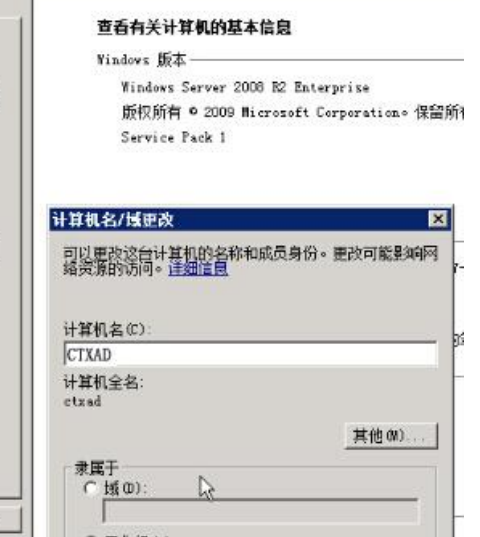

项目	配置	备注及注意事项
主机名及 IP 地址相关配置	请参考主机信息一览表	注意 License 服务所在的 CTXDDC 服务器，其主机名必须和 License 文件中的指定名字一致，并且大小写敏感。
活动目录域名	FQDN: citrixlab.local NetBIOS: citrixlab	
DNS 转发地址		按实际环境，配置可以工作的内网或者公网 DNS 服务器，以使测试环境可以正常解析外部资源的域名。
反向 DNS 查找区域	192.168.10.x	建立实际环境使用的 IP 地址段对应的反向查找区域
DHCP 地址段	192.168.10.x-192.168.10.x	请根据环境具体修改
DHCP Option	子网掩码: 255.255.255.0 DNS: 192.168.10.151 默认网关: 192.168.10.1	请根据环境具体修改

第3章 域控服务器配置

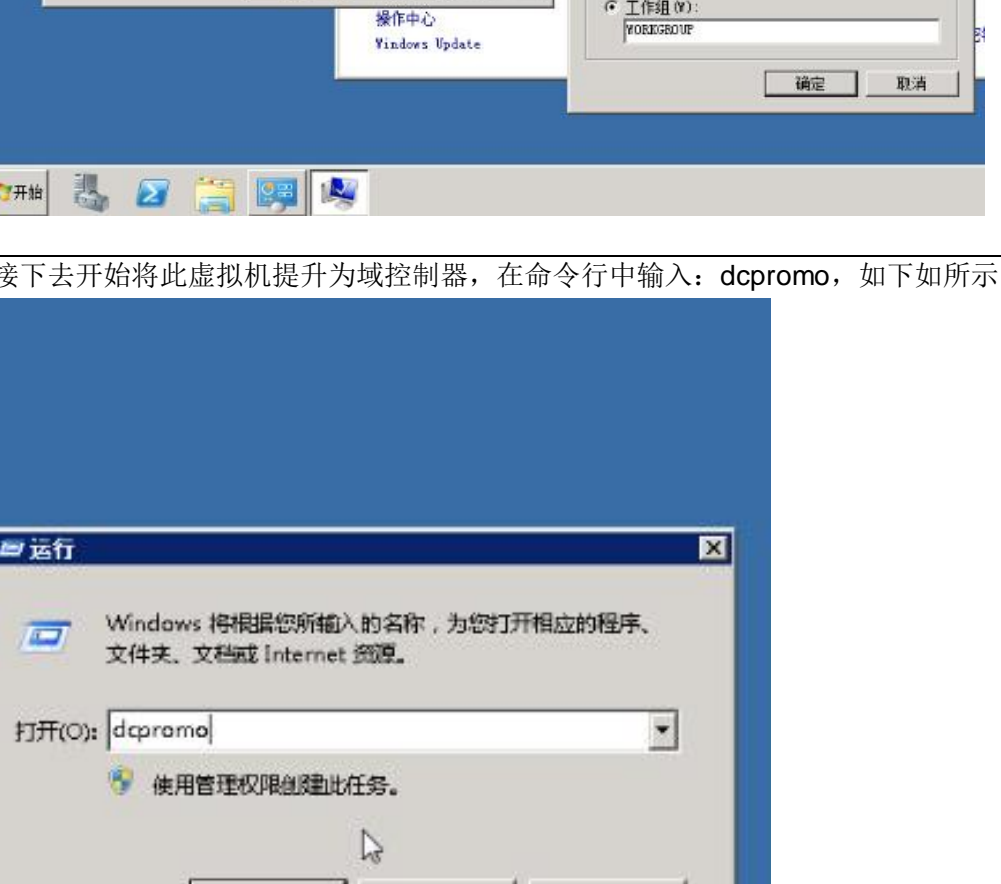
步骤	操作
1.	生成虚拟机请参考《PoC手册 - 1 基础环境 - Lab 01 虚拟主机基础环境安装1.0》第4.3节。由于我们创建的这台虚拟机适用于活动目录服务器，所以首先将该服务器的IP地址改为静态IP。
2.	<p>AD服务器 IP设置。</p> <p>在测试环境中，活动目录服务器同时要承担DNS和DHCP的功能，所以DNS地址我们设置为本机。</p> 

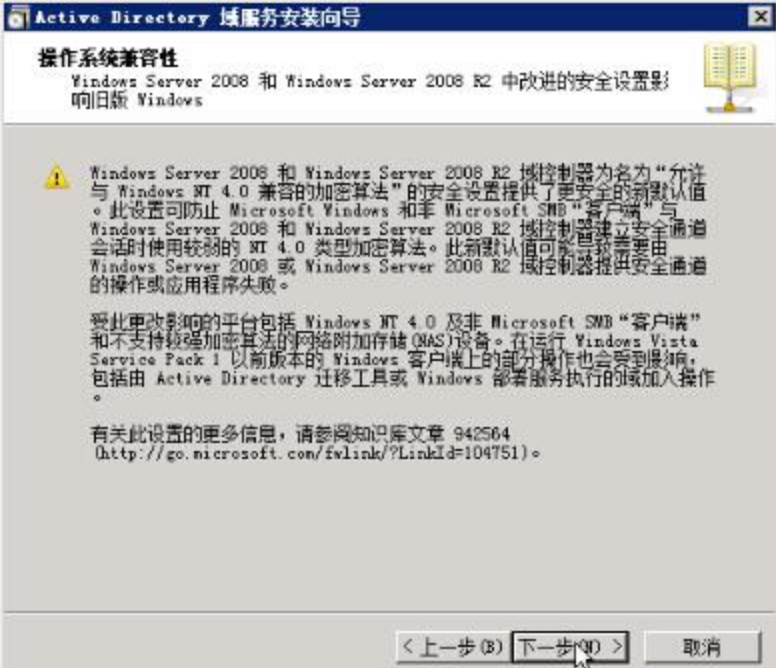
步骤 **操作**



3. 将本机的机器名修改为CTXAD，然后重启电脑





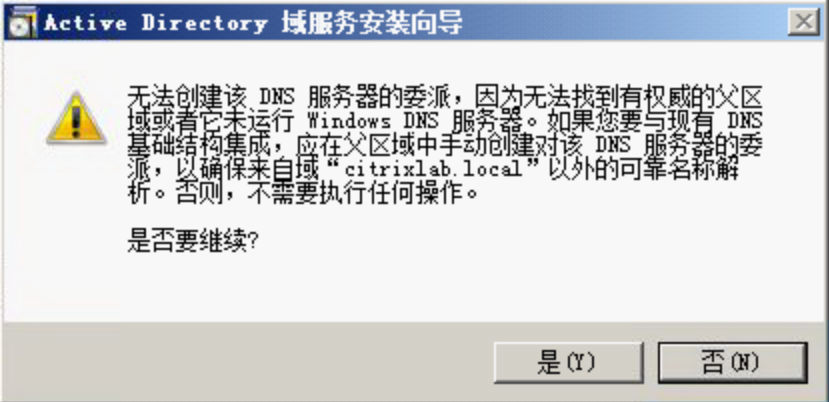

4. 接下去开始将此虚拟机提升为域控制器，在命令行中输入：dcpromo，如下如所示：

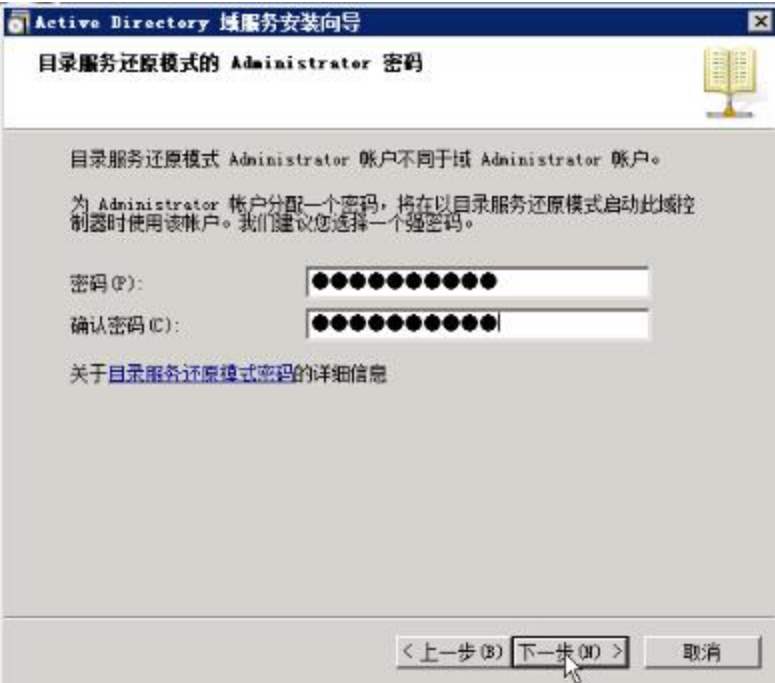
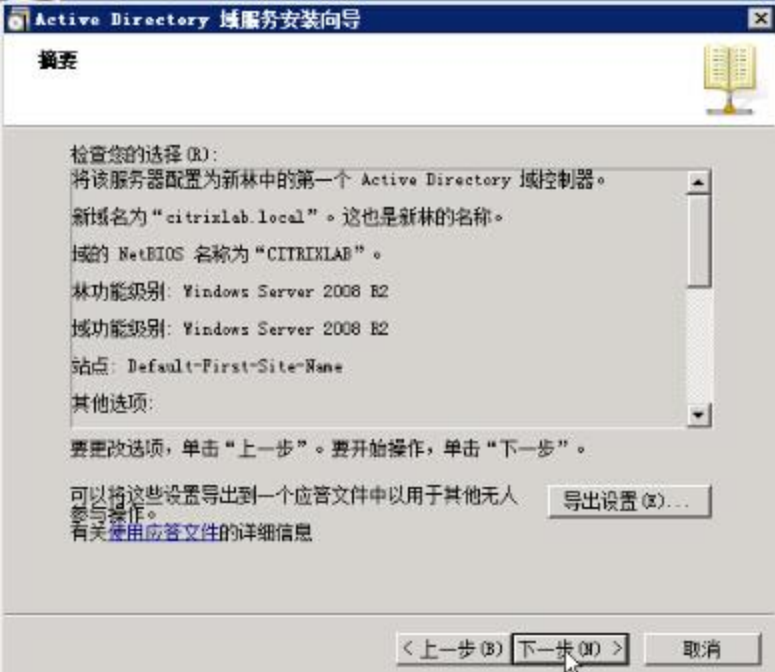


步骤	操作
5.	<p>“下一步”</p> 
6.	<p>“下一步”</p> 

步骤	操作
7.	<p>选择“在新林中新建域”</p> 
8.	<p>我们测试环境中的域名（FQDN）设置为：citrixlab.local，如下如所示： 注：请选择Windows 2008 R2域功能级别 “下一步”</p> 

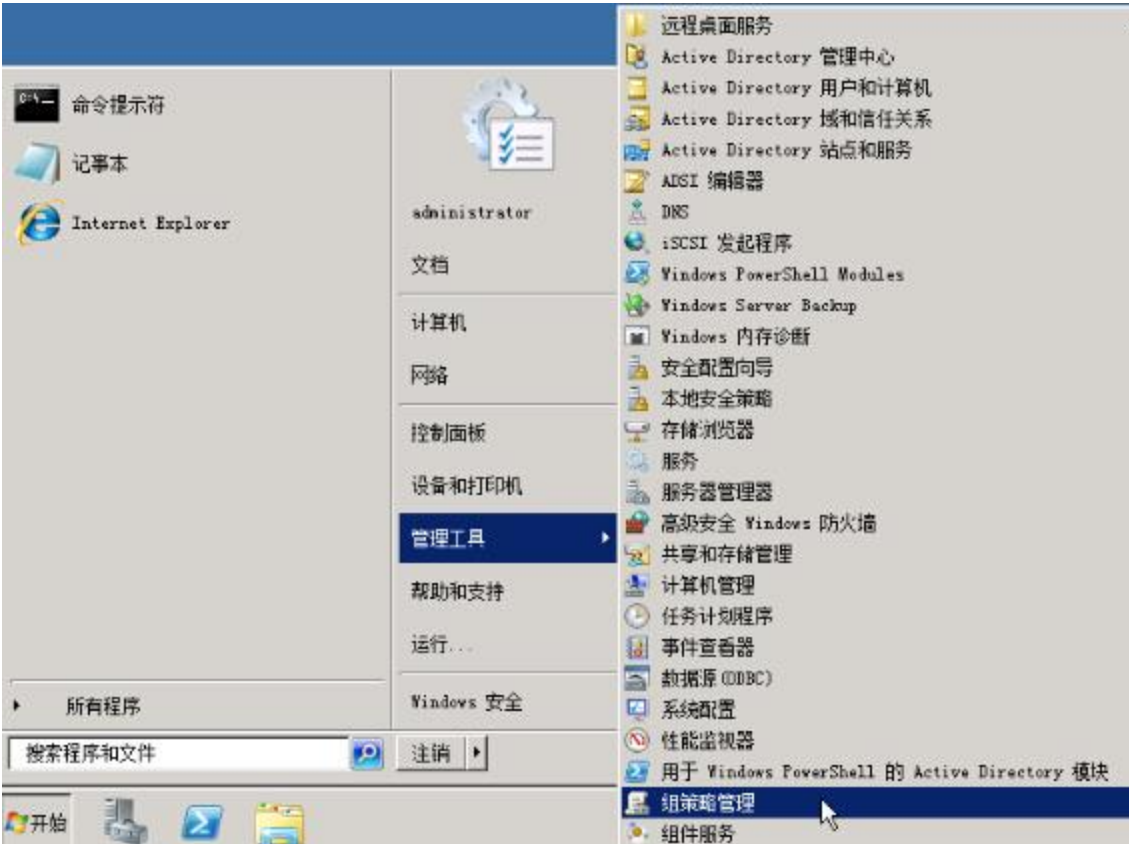
步骤	操作
9.	<p>选择“Windows Server 2008R2” “下一步”</p> 
10.	<p>“下一步”</p> 

步骤	操作
11.	<p>“是”</p> 
12.	<p>“下一步”</p> 

步骤	操作
13.	<p>密码设为: citrix@123 (用户可根据需要自行定义) 注: 目录服务还原模式密码, 在以后域做备份还原的时候需要“下一步”</p> 
14.	<p>“下一步”</p> 

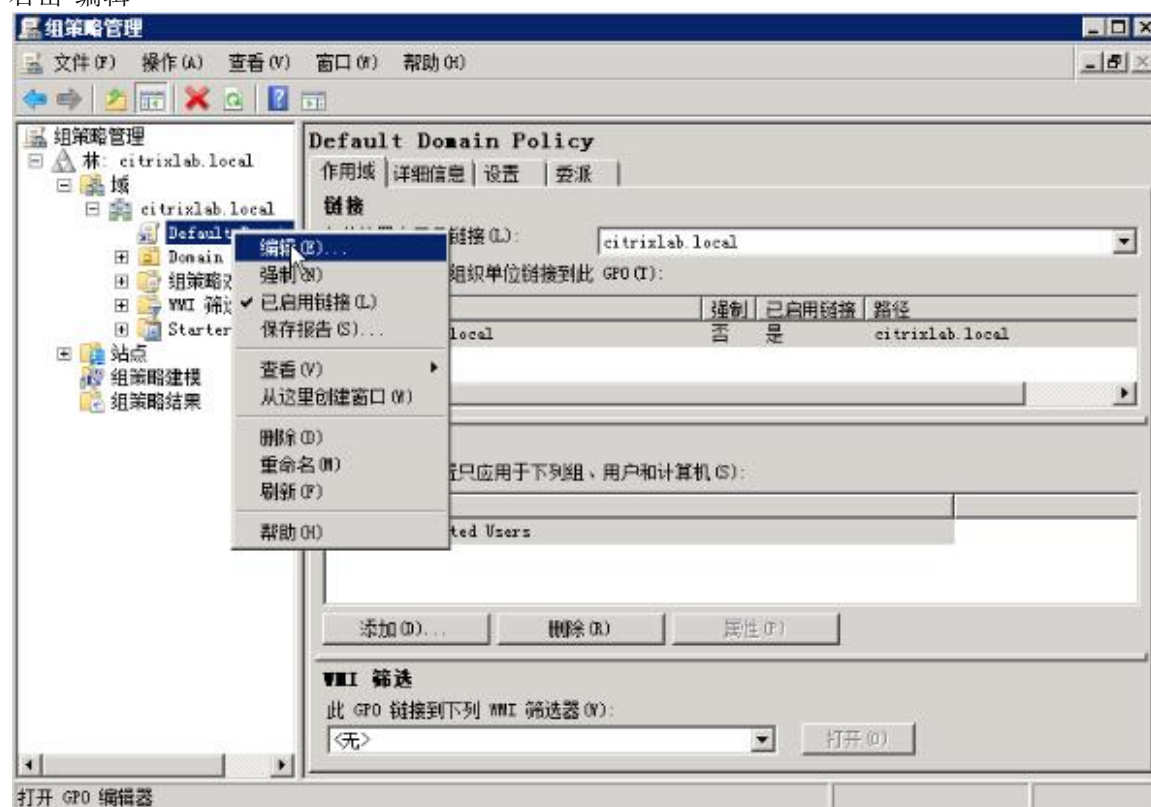
步骤	操作
15.	<p>“完成”，系统需要重启</p> 

第4章 组策略设置

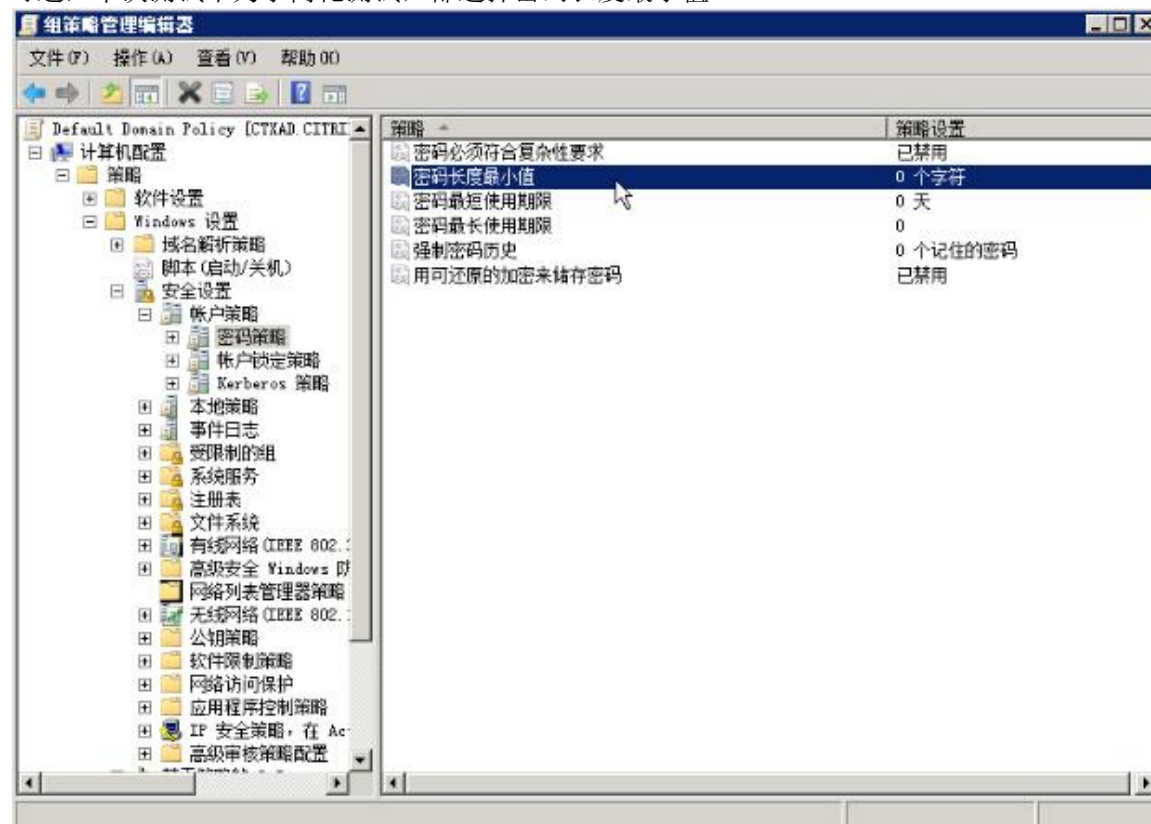
步骤	操作
1.	<p>开始-管理工具-组策略管理</p>  <p>The screenshot shows the Windows Server 2008 Start menu. The 'Administrative Tools' folder is expanded, displaying a list of system management tools. 'Group Policy Management' is highlighted at the bottom of the list. Other visible items include 'RemoteApp and Desktop Services', 'Active Directory Administrative Center', 'Active Directory Users and Computers', 'Active Directory Domain Services', 'Active Directory Sites and Services', 'ADSI Edit', 'DNS', 'iSCSI Initiator', 'Windows PowerShell Modules', 'Windows Server Backup', 'Windows Memory Diagnostics', 'Security Configuration Wizard', 'Local Security Policy', 'Storage Spaces', 'Services', 'Server Manager', 'Advanced Security Windows Firewall', 'Shared Storage Management', 'Computer Management', 'Task Scheduler', 'Event Viewer', 'Data Source (ODBC)', 'System Configuration', 'Performance Monitor', 'Active Directory PowerShell Module for Windows PowerShell', 'Group Policy Management', and 'Component Services'.</p>

步骤 操作

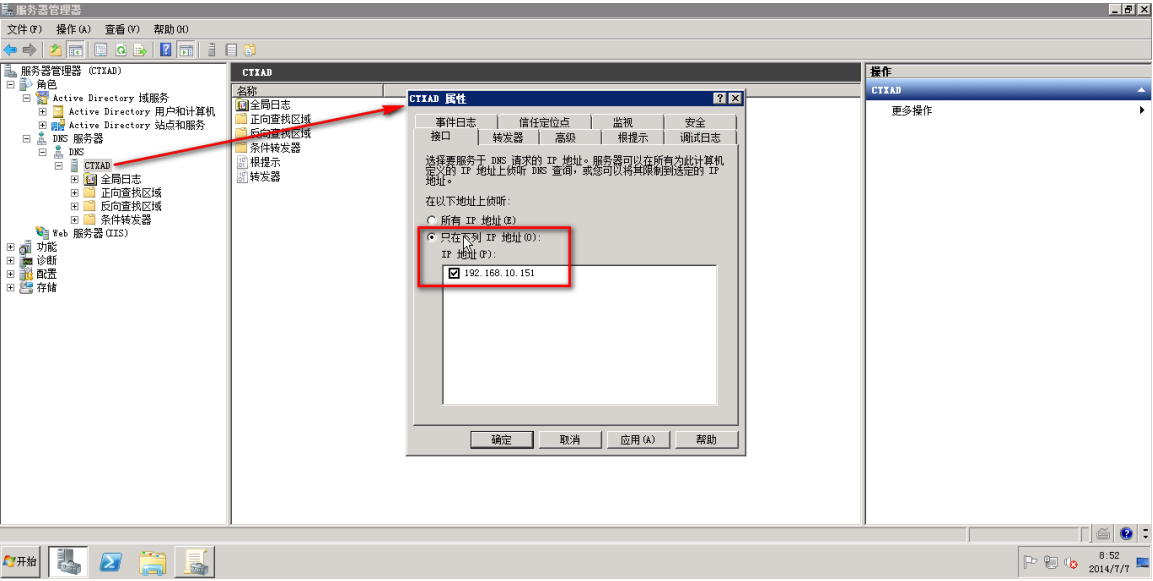
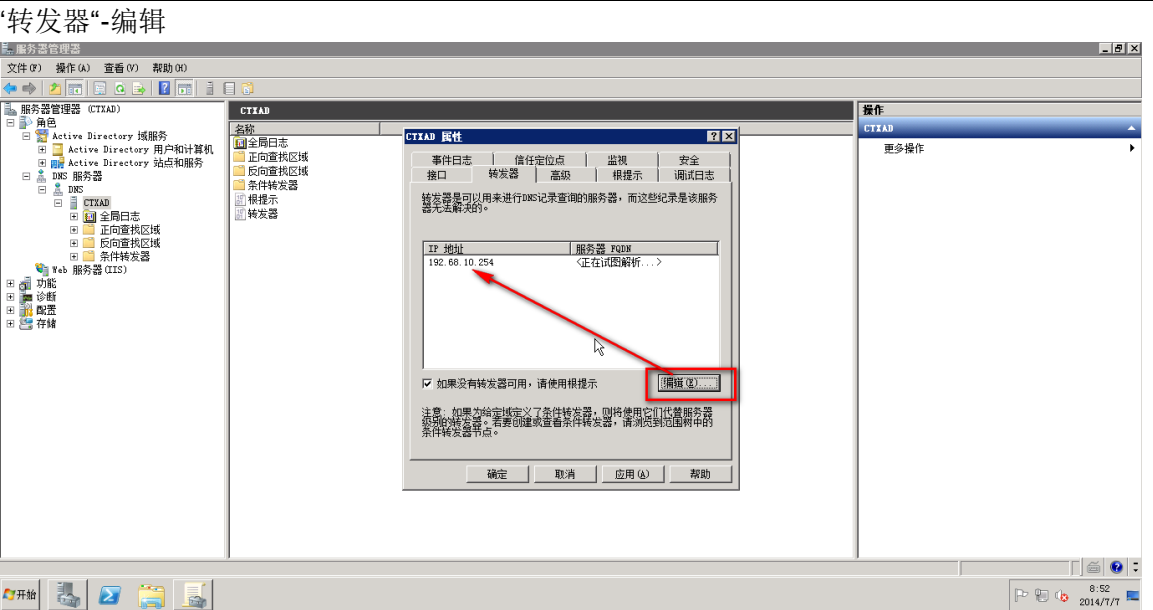
2. 右击“编辑”

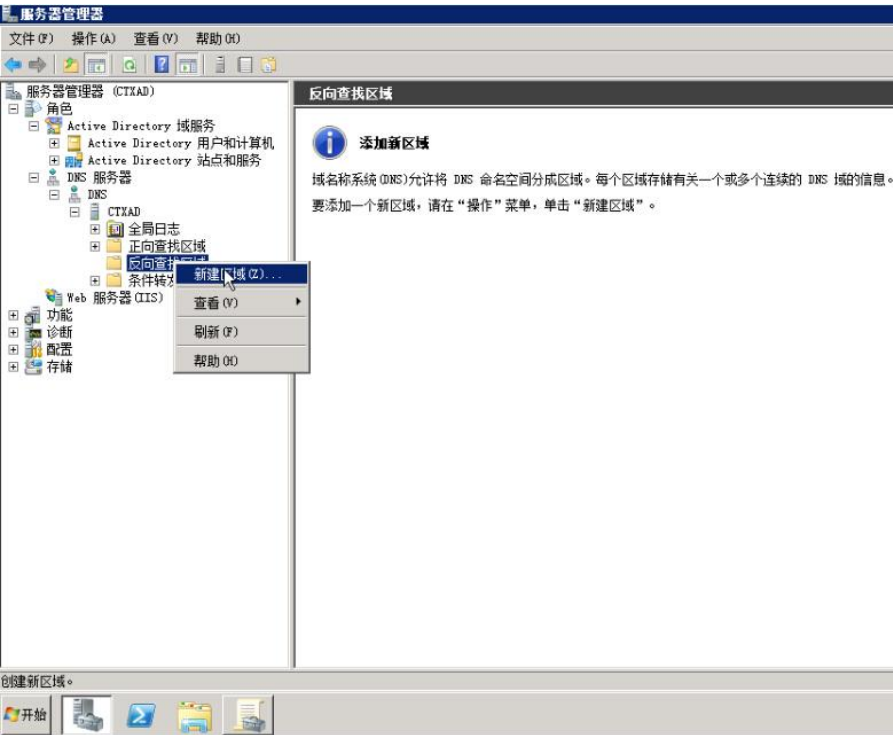
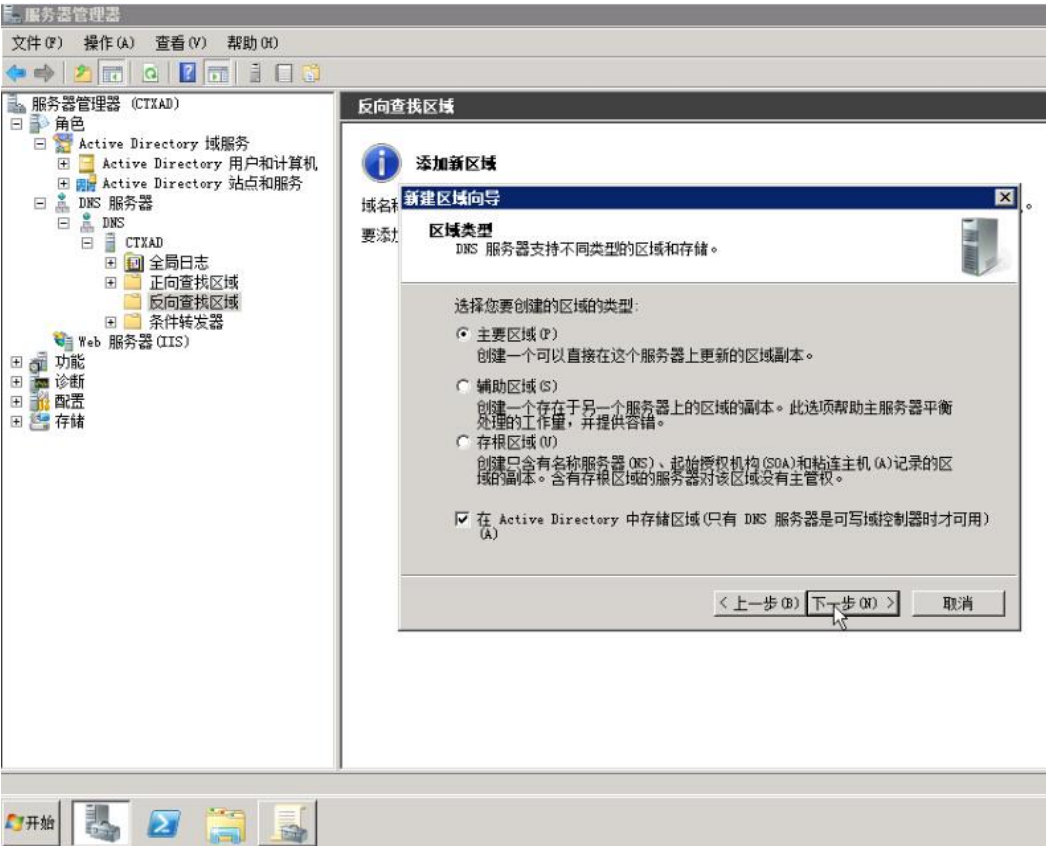


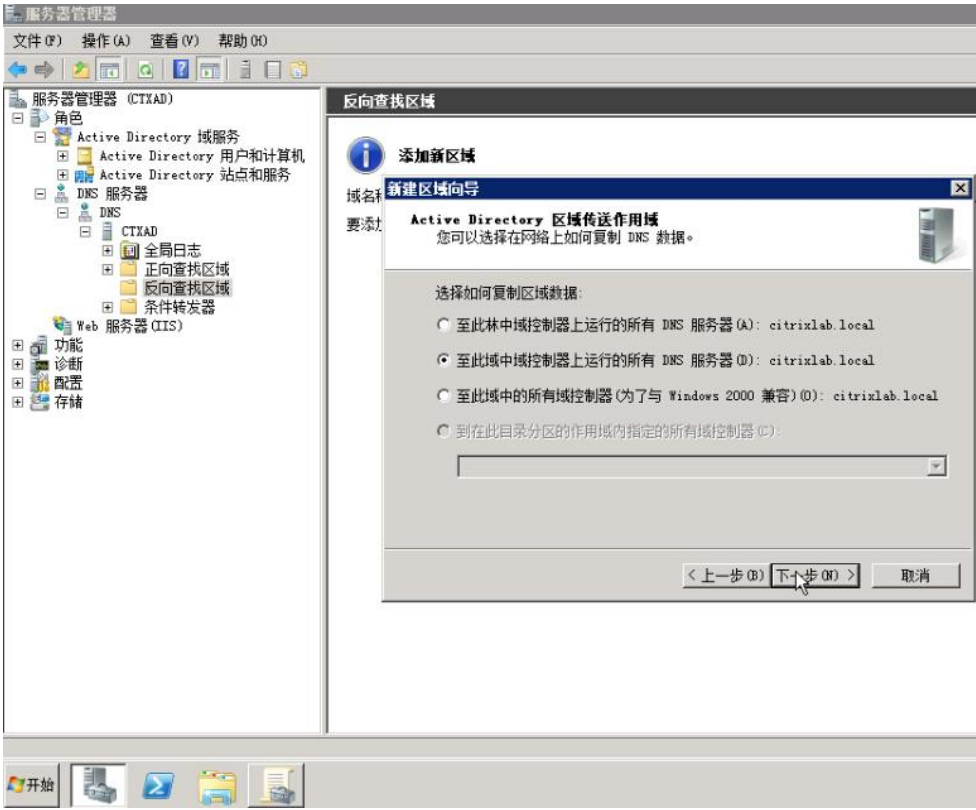
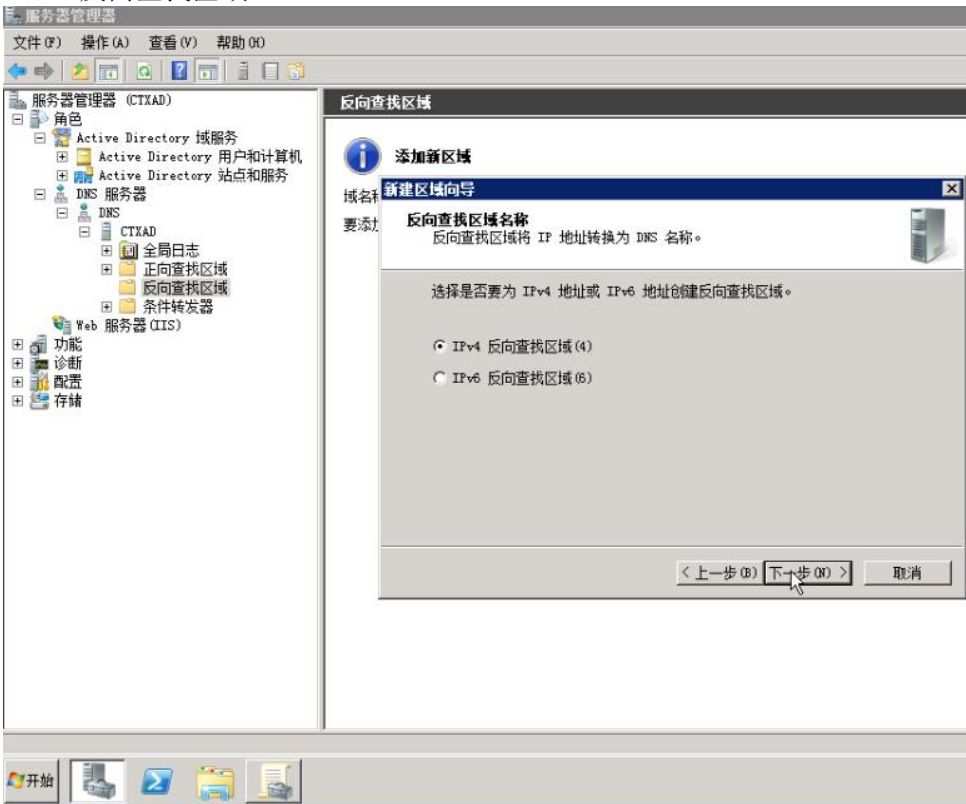
3. 可选，本次测试中为了简化测试，都选择密码长度最小值

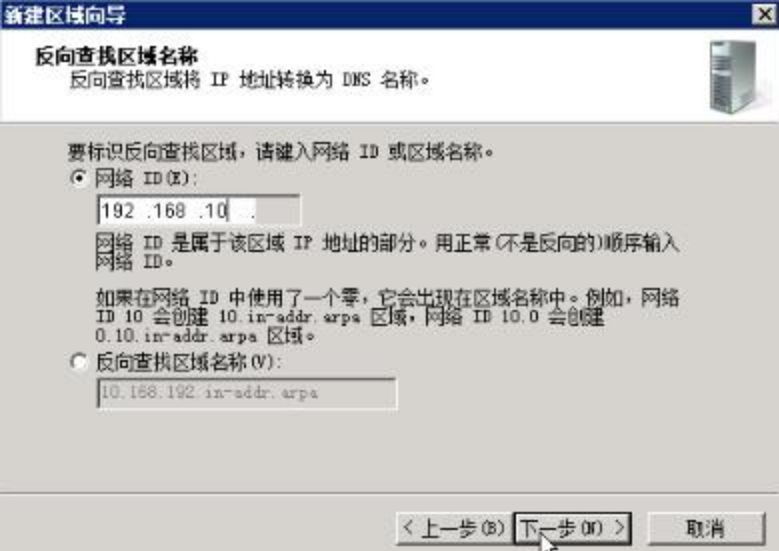
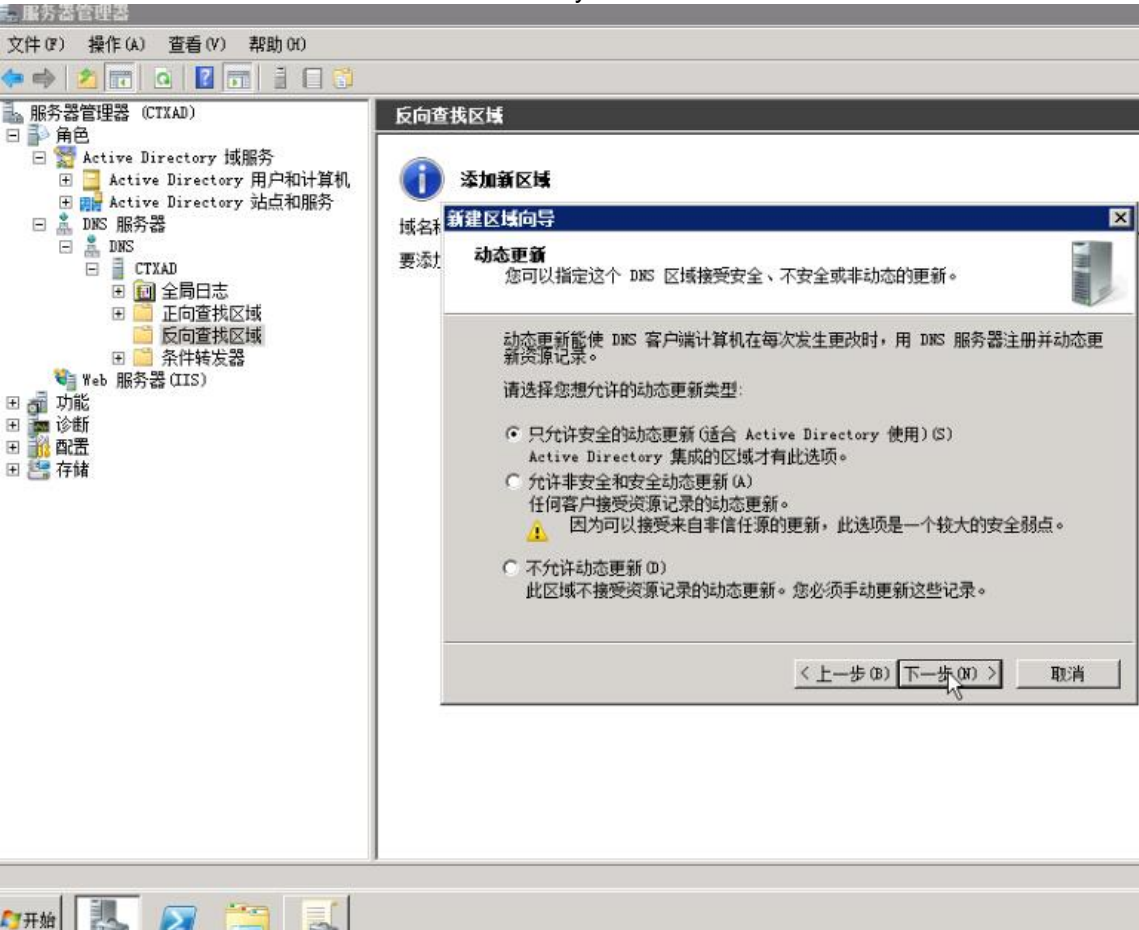


第5章 配置 DNS 服务，安装及配置 DHCP 服务

步骤	操作
1.	<p>设置DNS服务器的转发地址</p> <p>CTXAD右击属性-接口，选择“只在下列IP地址”</p> <p>注 1：当用户的 DNS 请求服务器送给活动目录服务器无法解析时，DNS 服务器会自动将解析请求转发给上一级的 DNS 服务器。</p> <p>注 2：如果只是在一个内网中，没有公网访问需求，此步骤可以省略。</p> 
	<p>“转发器”-编辑</p> 

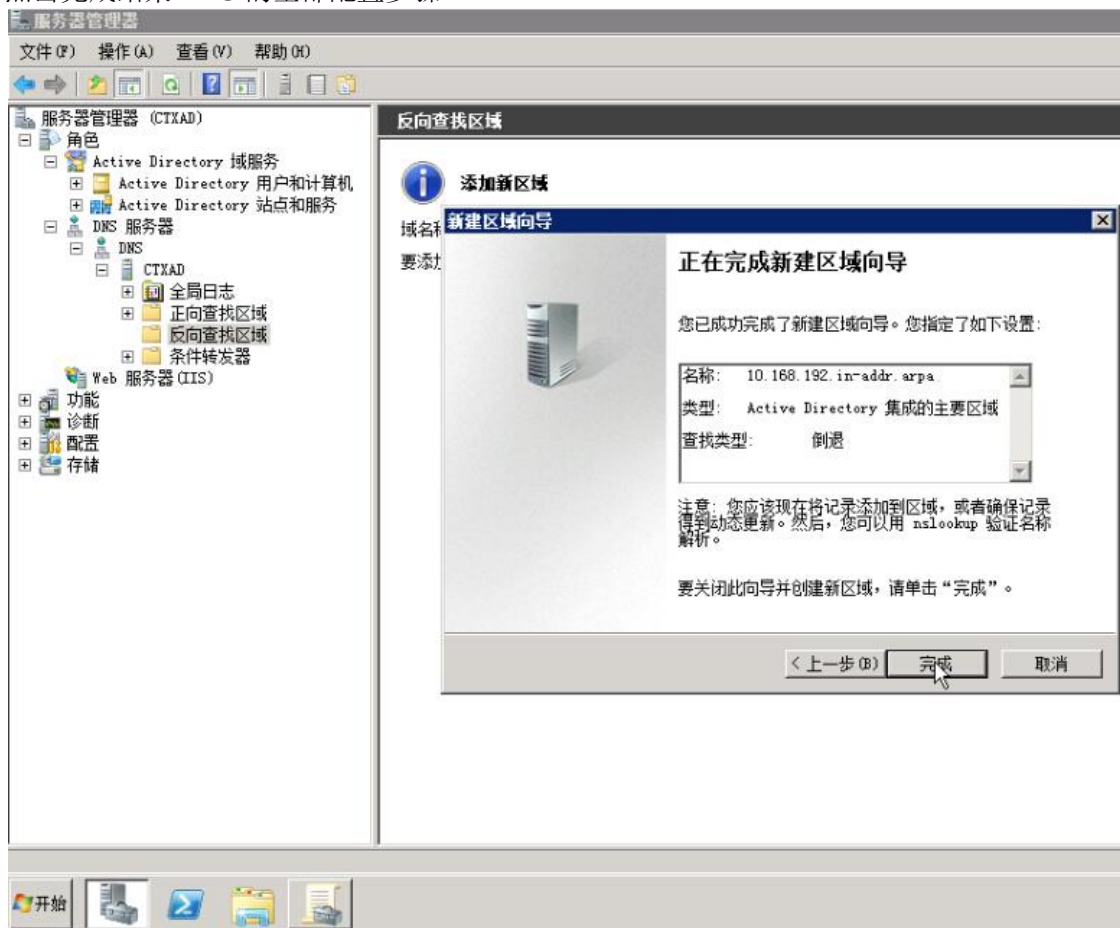
步骤	操作
2.	<p>DNS 配置完毕之后我们还需要配置 DNS 反向解析。点击“反向查找区域”鼠标右键，选择“新建区域”，如下图所示：</p> 
3.	<p>选择主要区域等设置，如下图所示：</p> 

步骤	操作
4.	<p>选择“至此域中域控制器上运行的所有 DNS 服务器 (D)”</p> 
5.	<p>“IPv4 反向查找区域”</p> 

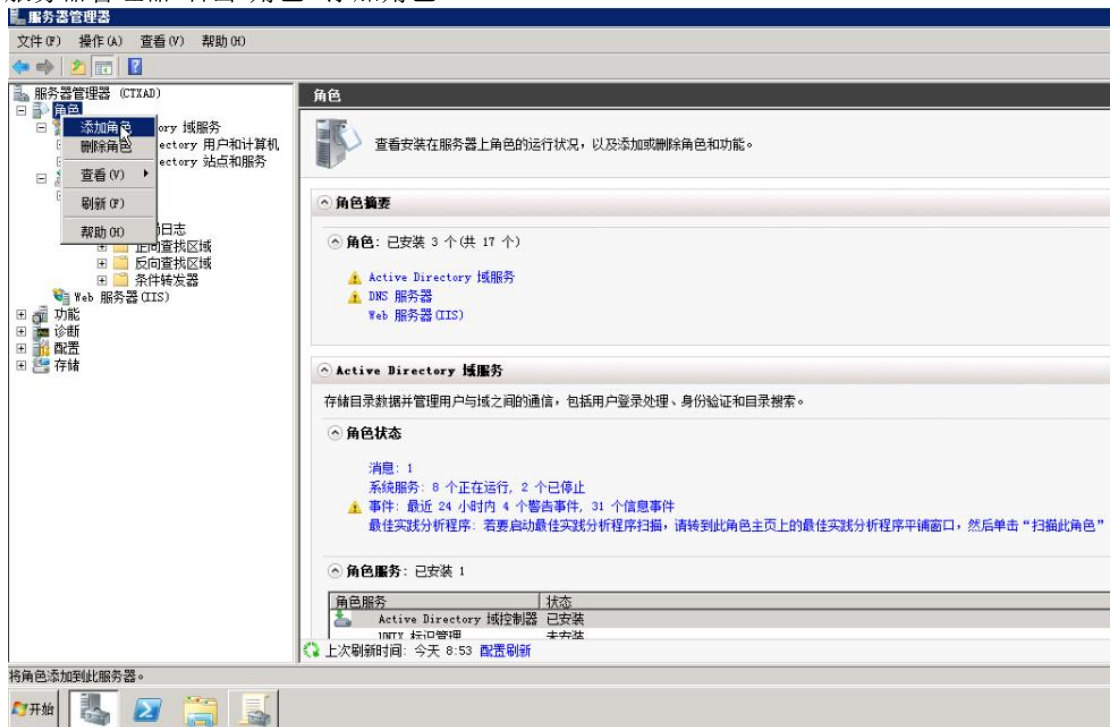
步骤	操作
6.	<p>按照实际情况填写网络 ID “下一步”</p> 
7.	<p>“只允许安全的动态更新（适合 Active Directory 使用）（S）”</p> 



步骤 操作



8. 点击完成结束 DNS 的全部配置步骤。

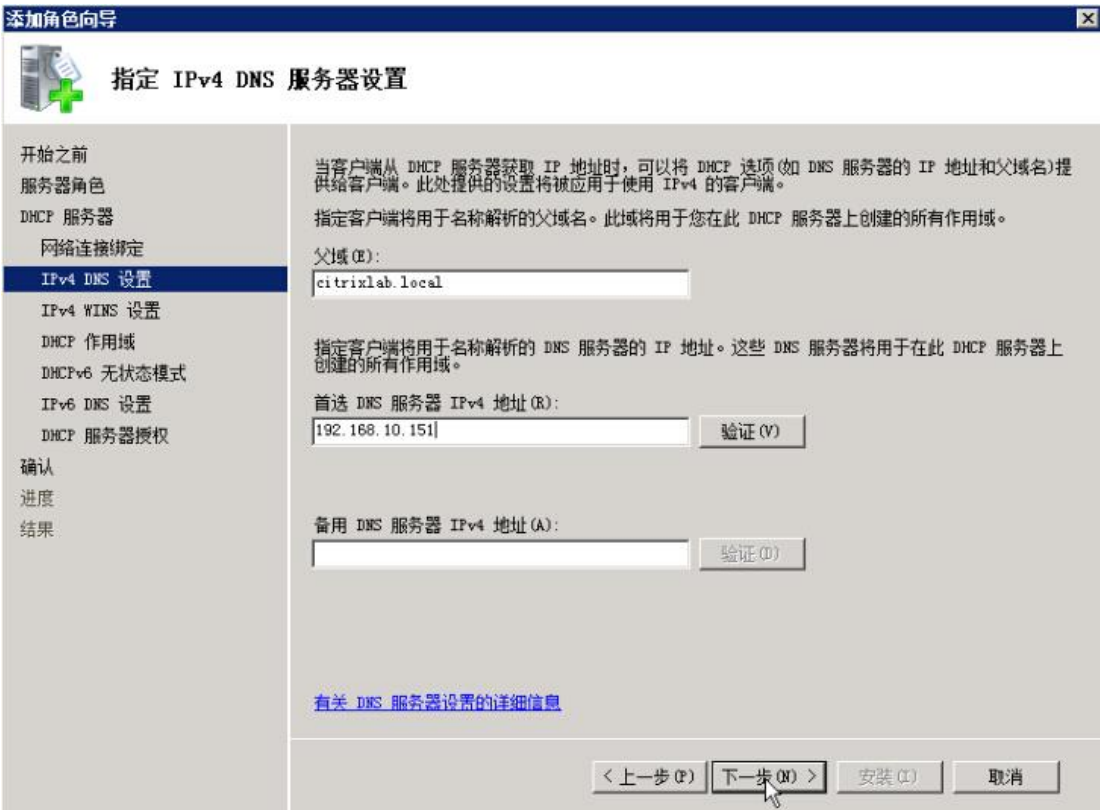
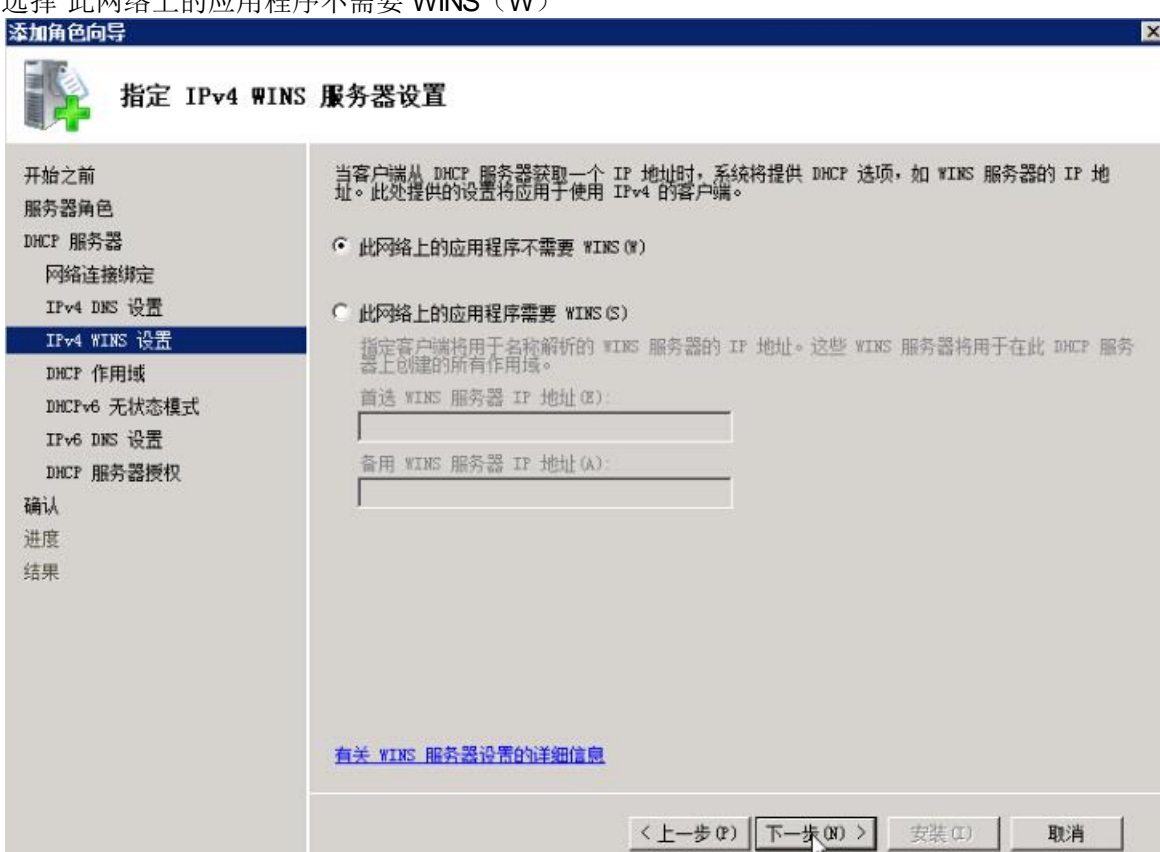


9. 由于操作系统默认还没有安装 DHCP 组件, 再单独安装和配置 DHCP 服务。
服务器管理器-右击“角色”-添加角色



步骤	操作
10.	<div> <div>添加角色向导</div> <div>  开始之前 </div> <div> <div>开始之前</div> <div>服务器角色</div> <div>确认</div> <div>进度</div> <div>结果</div> </div> <div> <p>此向导帮助您在此服务器上安装角色。根据要求此服务器执行的任务来确定要安装的角色，例如共享文档或主持网站。</p> <p>继续操作之前，请验证以下事项：</p> <ul style="list-style-type: none"> • Administrator 帐户具有强密码 • 已配置网络设置，例如静态 IP 地址 • 已安装 Windows Update 中的最新安全更新 <p>如果您必须结束上述的任何操作，请取消此向导，结束操作，然后再次运行向导。</p> <p>若要继续，请单击“下一步”。</p> <p><input type="checkbox"/> 默认情况下将跳过此页(S)</p> <div> < 上一步 (P) 下一步 (N) > 安装 (I) 取消 </div> </div> </div>
11.	<div> <div>勾选“DHCP”</div> <div>添加角色向导</div> <div>  选择服务器角色 </div> <div> <div>开始之前</div> <div>服务器角色</div> <div>DHCP 服务器</div> <div>网络连接绑定</div> <div>IPv4 DNS 设置</div> <div>IPv4 WINS 设置</div> <div>DHCP 作用域</div> <div>DHCPv6 无状态模式</div> <div>IPv6 DNS 设置</div> <div>DHCP 服务器授权</div> <div>确认</div> <div>进度</div> <div>结果</div> </div> <div> <p>选择要安装在此服务器上的一个或多个角色。</p> <p>角色(R):</p> <div> <input type="checkbox"/> Active Directory Rights Management Services <input type="checkbox"/> Active Directory 联合身份验证服务 <input type="checkbox"/> Active Directory 轻型目录服务 <input checked="" type="checkbox"/> Active Directory 域服务 (已安装) <input type="checkbox"/> Active Directory 证书服务 <input checked="" type="checkbox"/> DHCP 服务器 <input checked="" type="checkbox"/> DNS 服务器 (已安装) <input type="checkbox"/> Hyper-V <input checked="" type="checkbox"/> Web 服务器 (IIS) (已安装) <input type="checkbox"/> Windows Server Update Services <input type="checkbox"/> Windows 部署服务 <input type="checkbox"/> 传真服务器 <input type="checkbox"/> 打印和文件服务 <input type="checkbox"/> 网络策略和访问服务 <input type="checkbox"/> 文件服务 <input type="checkbox"/> 应用程序服务器 <input type="checkbox"/> 远程桌面服务 </div> <p>有关服务器角色的详细信息</p> <div> < 上一步 (P) 下一步 (N) > 安装 (I) 取消 </div> </div> <div> <p>描述:</p> <p>动态主机配置协议 (DHCP) 服务器 支持集中配置、管理和提供客户端计算机的临时 IP 地址和相关信息。</p> </div> </div>


步骤	操作				
12.	<p>“下一步”</p> <p>添加角色向导</p> <p> DHCP 服务器</p> <div> <p>开始之前</p> <p>服务器角色</p> <p>DHCP 服务器</p> <p>网络连接绑定</p> <p>IPv4 DNS 设置</p> <p>IPv4 WINS 设置</p> <p>DHCP 作用域</p> <p>DHCPv6 无状态模式</p> <p>IPv6 DNS 设置</p> <p>DHCP 服务器授权</p> <p>确认</p> <p>进度</p> <p>结果</p> </div> <p>DHCP 服务器简介</p> <p>动态主机配置协议允许服务器将 IP 地址分配或租用到已作为 DHCP 客户端启用的计算机和其他设备。在网络上部署 DHCP 服务器将为计算机和其他基于 TCP/IP 的网络设备提供有效的 IP 地址和这些设备需要的其他配置参数 (称为 DHCP 选项)。这就允许将这些设备连接到其他网络资源, 例如 DNS 服务器、WINS 服务器和路由器。</p> <p>注意事项</p> <ul style="list-style-type: none"> ① 应在此计算机上至少配置一个静态 IP 地址。 ① 安装 DHCP 服务器之前, 应规划子网、作用域和例外。将规划的记录保存在安全位置以供日后参考。 <p>其他信息</p> <p>DHCP 服务器概述</p> <p>定义 DHCP 作用域</p> <p>将 DHCP 与 DNS 集成</p> <p>< 上一步(B) 下一步(N) > 安装(I) 取消</p>				
13.	<p>“下一步”</p> <p>添加角色向导</p> <p> 选择网络连接绑定</p> <div> <p>开始之前</p> <p>服务器角色</p> <p>DHCP 服务器</p> <p>网络连接绑定</p> <p>IPv4 DNS 设置</p> <p>IPv4 WINS 设置</p> <p>DHCP 作用域</p> <p>DHCPv6 无状态模式</p> <p>IPv6 DNS 设置</p> <p>DHCP 服务器授权</p> <p>确认</p> <p>进度</p> <p>结果</p> </div> <p>已检测到具有静态 IP 地址的一个或多个网络连接。每个网络连接都可用于为单独子网上的 DHCP 客户端提供服务。</p> <p>请选择此 DHCP 服务器将用于向客户端提供服务的网络连接。</p> <p>网络连接(E):</p> <table border="1"> <thead> <tr> <th>IP 地址</th> <th>类型</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> 192.168.10.151</td> <td>IPv4</td> </tr> </tbody> </table> <p>详细信息</p> <p>名称: 本地连接 2</p> <p>网络适配器: 本地连接 2</p> <p>物理地址: 42-AD-2C-80-56-13</p> <p>< 上一步(B) 下一步(N) > 安装(I) 取消</p>	IP 地址	类型	<input checked="" type="checkbox"/> 192.168.10.151	IPv4
IP 地址	类型				
<input checked="" type="checkbox"/> 192.168.10.151	IPv4				

步骤	操作
14.	<p>填入相对应的域，和首选 DNS 地址，“下一步”</p> 
15.	<p>选择“此网络上的应用程序不需要 WINS (W)”</p> 

步骤 操作

16. 添加，填入对应域名，IP 地址段，子网掩码及默认网关信息，“下一步”

添加角色向导

 添加或编辑 DHCP 作用域

开始之前
服务器角色
DHCP 服务器
 网络连接绑定
 IPv4 DNS 设置
 IPv4 WINS 设置
 DHCP 作用域
 DHCPv6 无状态模式
 IPv6 DNS 设置
 DHCP 服务器授权
确认
进度
结果

作用域是网络中可能的 IP 地址的范围。只有创建作用域之后，DHCP 服务器才可以将 IP 地址分

添加作用域

作用域是网络可能的 IP 地址范围。只有创建作用域后，DHCP 服务器才能将 IP 地址分配给各个客户端。

DHCP 服务器的配置设置

作用域名称 (S): citrixlab

起始 IP 地址 (T): 192.168.10.200

结束 IP 地址 (E): 192.168.10.250

子网类型 (B): 有线 (租用持续时间将为 8 天)

☒ 激活此作用域 (A)

传播到 DHCP 客户端的配置设置

子网掩码 (U): 255.255.255.0

默认网关 (可选) (D): 192.168.10.254

确定 取消

[有关添加作用域的详细信息](#)

< 上一步 (P) 下一步 (N) > 安装 (I) 取消

17. “下一步”

添加角色向导

 添加或编辑 DHCP 作用域

开始之前
服务器角色
DHCP 服务器
 网络连接绑定
 IPv4 DNS 设置
 IPv4 WINS 设置
 DHCP 作用域
 DHCPv6 无状态模式
 IPv6 DNS 设置
 DHCP 服务器授权
确认
进度
结果

作用域是网络中可能的 IP 地址的范围。只有创建作用域之后，DHCP 服务器才可以将 IP 地址分

发到客户端。

作用域 (S):

名称	IP 地址范围
citrixlab	192.168.10.200 - 192.168.10...




添加 (A)...
编辑 (E)...
删除 (D)

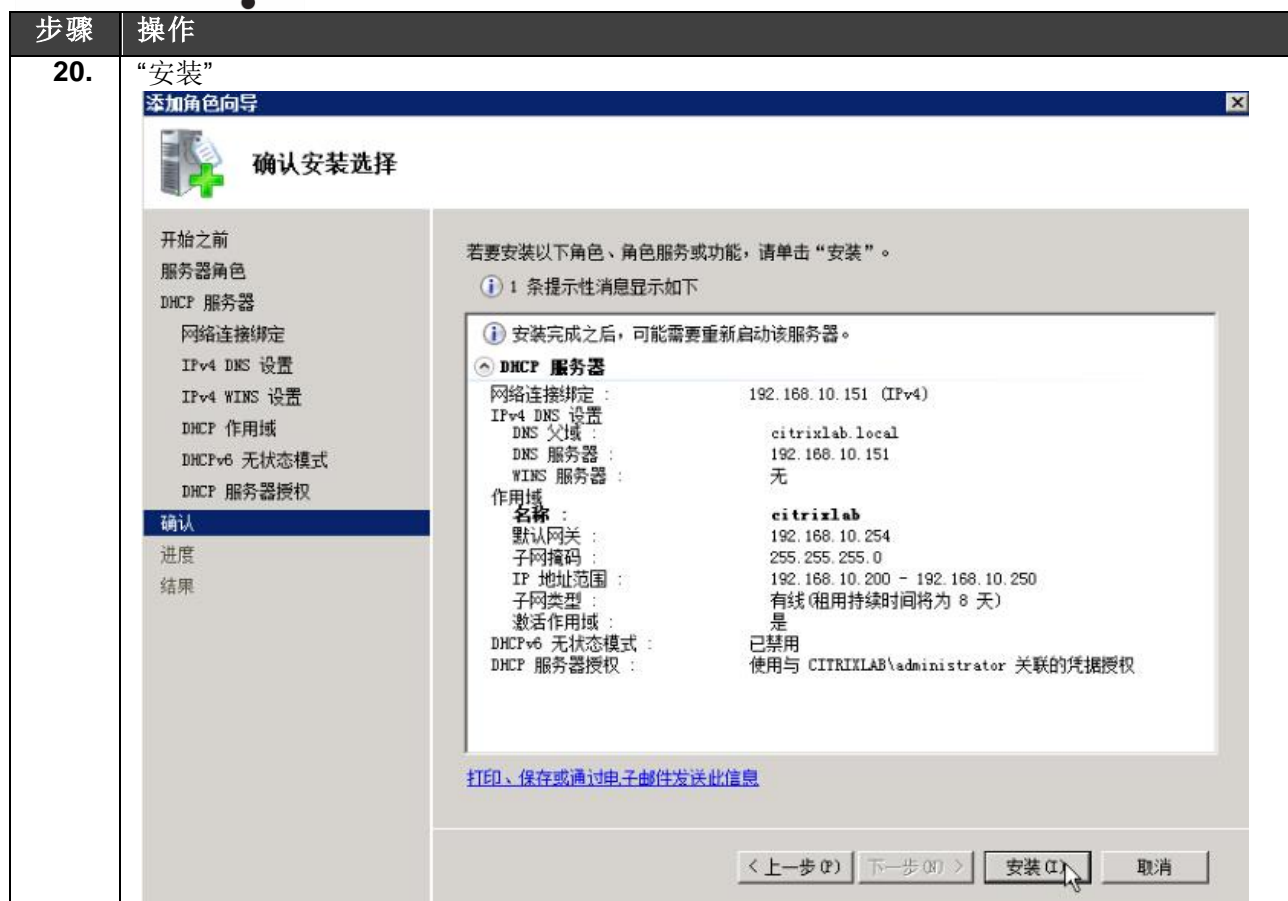
属性

添加或选择一个作用域以查看其属性。

[有关添加作用域的详细信息](#)

< 上一步 (P) 下一步 (N) > 安装 (I) 取消

步骤	操作
18.	<p>“对此服务器禁用 DHCPv6”无状态模式 (D)</p> <p>添加角色向导</p> <p> 配置 DHCPv6 无状态模式</p> <p>开始之前 服务器角色 DHCP 服务器 网络连接绑定 IPv4 DNS 设置 IPv4 WINS 设置 DHCP 作用域 DHCPv6 无状态模式 DHCP 服务器授权 确认 进度 结果</p> <p>DHCP 服务器支持用于服务 IPv6 客户端的 DHCPv6 协议。通过 DHCPv6，客户端可以使用无状态模式自动配置其 IPv6 地址，或以有状态模式从 DHCP 服务器获取 IPv6 地址。如果将网络中的路由器配置为支持 DHCPv6，请确认以下选项是否与路由器配置相匹配。</p> <p>选择此服务器的 DHCPv6 无状态模式配置。</p> <p><input type="radio"/> 对此服务器启用 DHCPv6 无状态模式 (E) 自动配置 IPv6 客户端，而不使用此 DHCP 服务器。</p> <p><input checked="" type="radio"/> 对此服务器禁用 DHCPv6 无状态模式 (D) 安装 DHCP 服务器之后，您可以使用 DHCP 管理控制台配置 DHCPv6 模式。</p> <p>有关 DHCPv6 无状态模式的详细信息</p> <p>< 上一步 (P) 下一步 (N) > 安装 (I) 取消</p>
19.	<p>“下一步”</p> <p>添加角色向导</p> <p> 授权 DHCP 服务器</p> <p>开始之前 服务器角色 DHCP 服务器 网络连接绑定 IPv4 DNS 设置 IPv4 WINS 设置 DHCP 作用域 DHCPv6 无状态模式 DHCP 服务器授权 确认 进度 结果</p> <p>Active Directory 域服务 (AD DS) 会存储网络中已被授权服务客户端的 DHCP 服务器列表。授权 DHCP 服务器有助于避免因使用不正确的配置运行 DHCP 服务器或在错误的网络上使用正确的配置运行 DHCP 服务器所导致的意外损坏。</p> <p>指定用于授权 AD DS 中此 DHCP 服务器的凭据。</p> <p><input checked="" type="radio"/> 使用当前凭据 (U) 使用当前用户的凭据在 AD DS 中授权此 DHCP 服务器。 用户名: CITRIXLAB\administrator</p> <p><input type="radio"/> 使用备用凭据 (S) 为授权 AD DS 中的 DHCP 服务器指定域管理员凭据。 用户名: 指定 (E)...</p> <p><input type="radio"/> 跳过 AD DS 中此 DHCP 服务器的授权 (K)  此 DHCP 服务器必须在 AD DS 中被授权才能向客户端提供服务。</p> <p>有关在 AD DS 中授权 DHCP 服务器的详细信息</p> <p>< 上一步 (P) 下一步 (N) > 安装 (I) 取消</p>

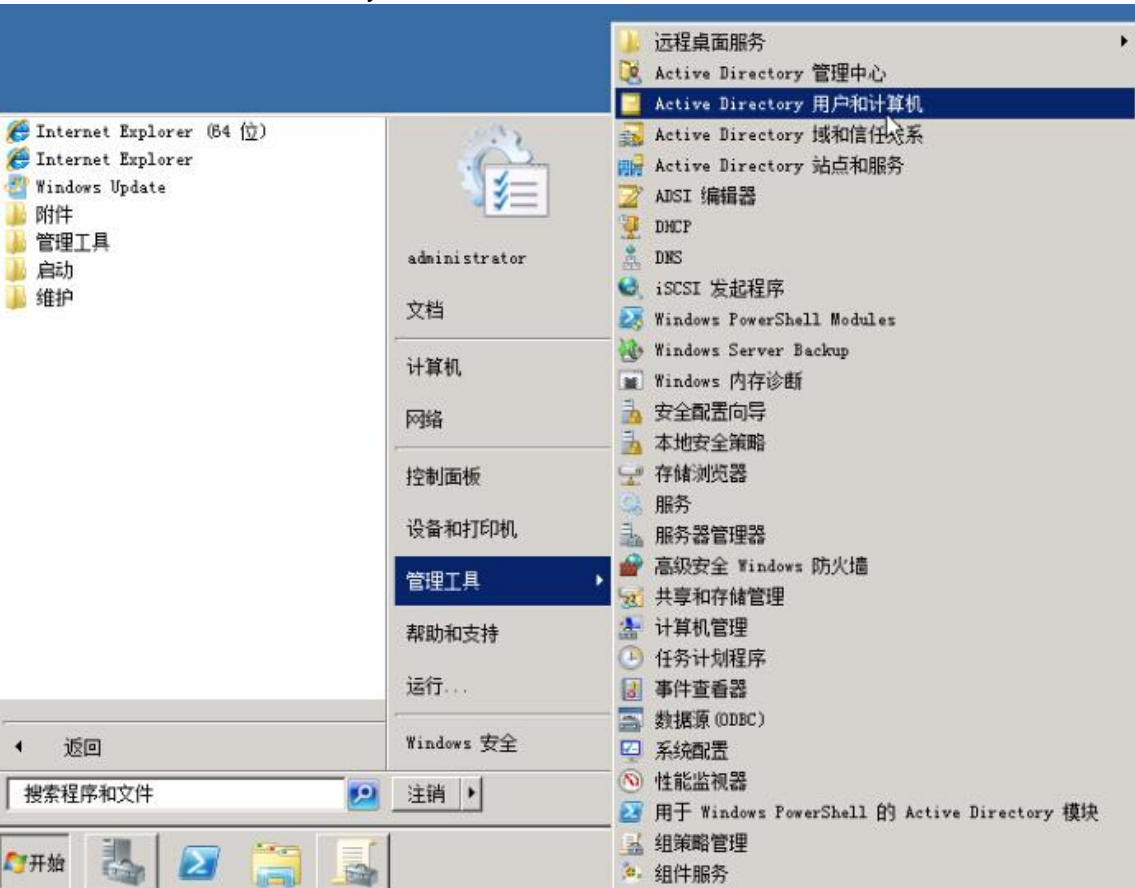


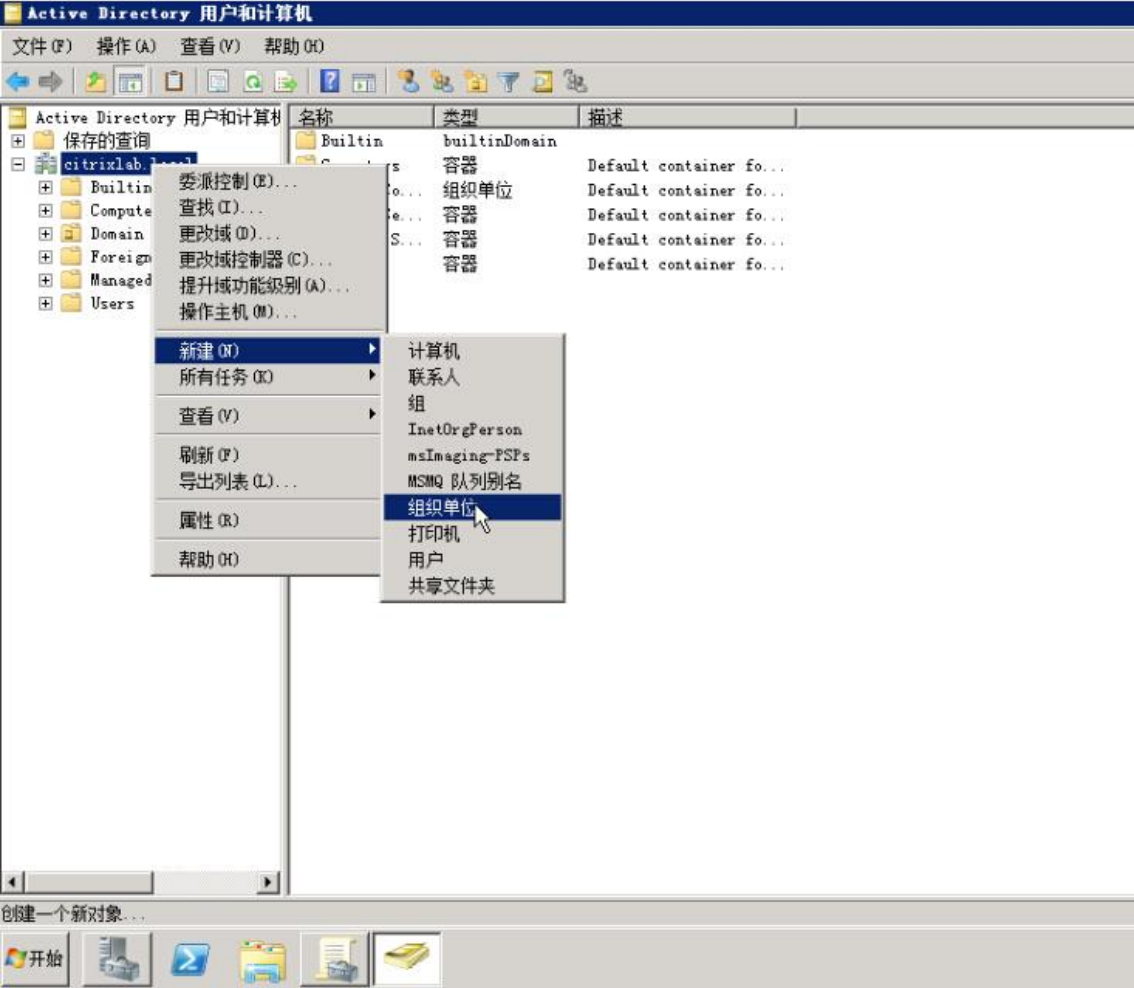
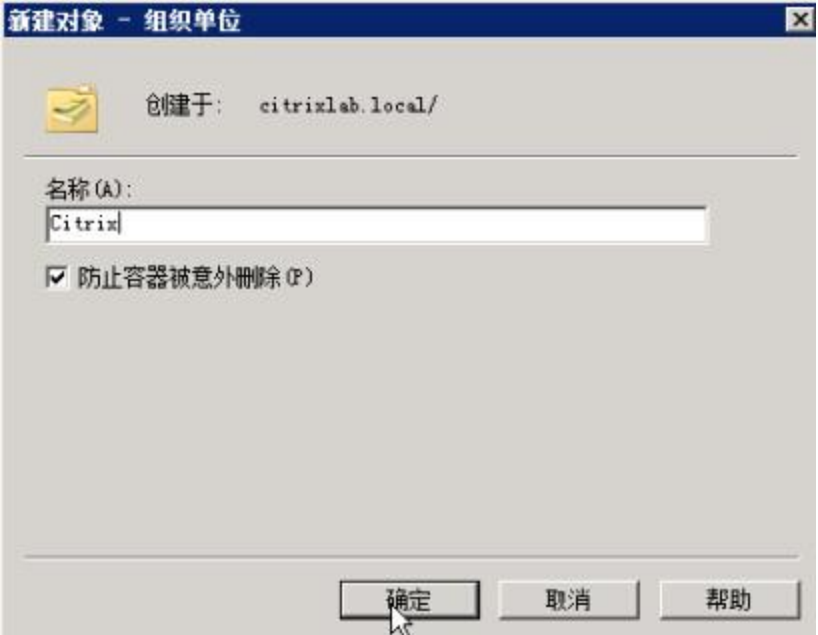
第6章 活动目录用户和 OU 准备



请在活动目录 AD 内建立以下用户和 OU，以备测试环境使用

AD 类 别	名 称	位 置	备 注
OU 组织单元	请按右面结构创建相应的 OU: Citrix, CTXUsers, Infra, XenApp, XenDesktop vWin7	Domain Root --Citrix --Infra ---CTXUsers ---XenApp ---XenDesktop --vWin7	Citrix , 存放所有本 POC 有关的对象 Infra, 存放基础构架服务器的计算机账号, 如 DDC。 CTXUsers, 存放测试用户账号 XenApp, 存放 XenApp 服务器计算机账号 XenDesktop, 存放虚拟桌面计算机账号 vWin7, 存放 Win7 虚拟桌面计算机账号

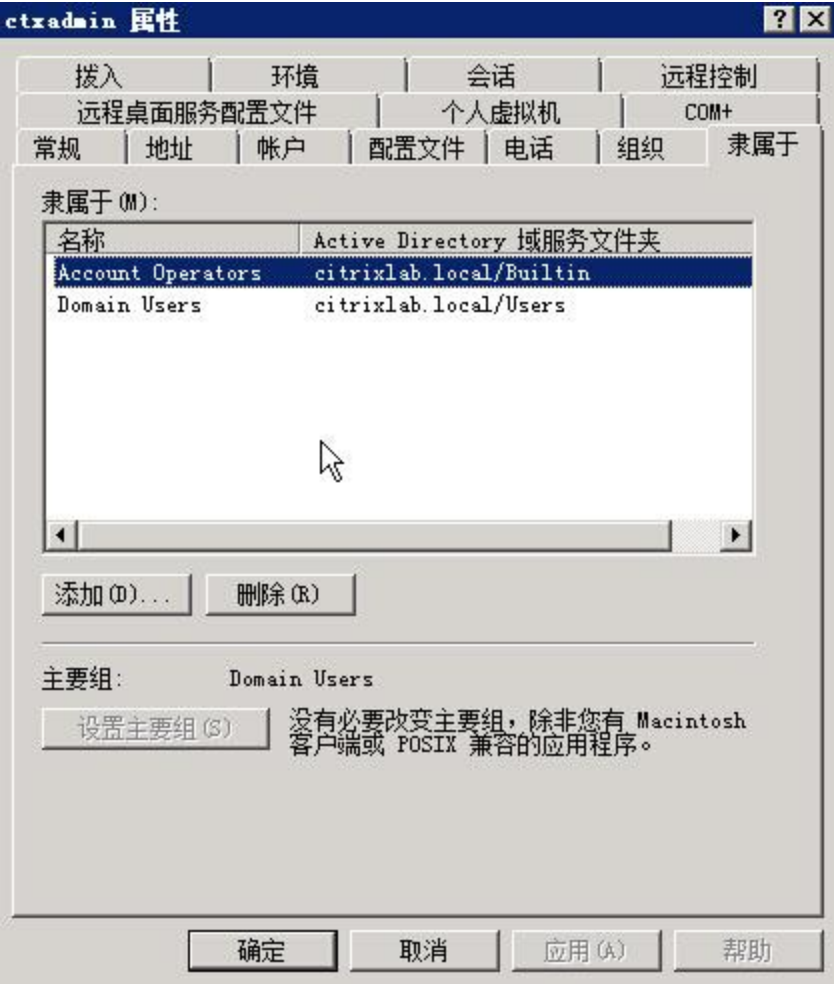

用户	ctxadmin	CTXUsers OU 内	citrix 环境管理员。记得将其加入 XD 和 XA 服务器的本地管理员组内。 使用该账号创建新的虚拟桌面时候，还需要赋予其将计算机加入域的权限。（但请不要加入 Domain Admins，指派特定的权限，如加入 Account operation 组）
用户	User01 User02 ... User05	CTXUsers OU 内	测试用用胡账号
组	USB Allow USB Deny XenApp Shared Desktop VDI	CTXUsers OU	测试用各种 Group


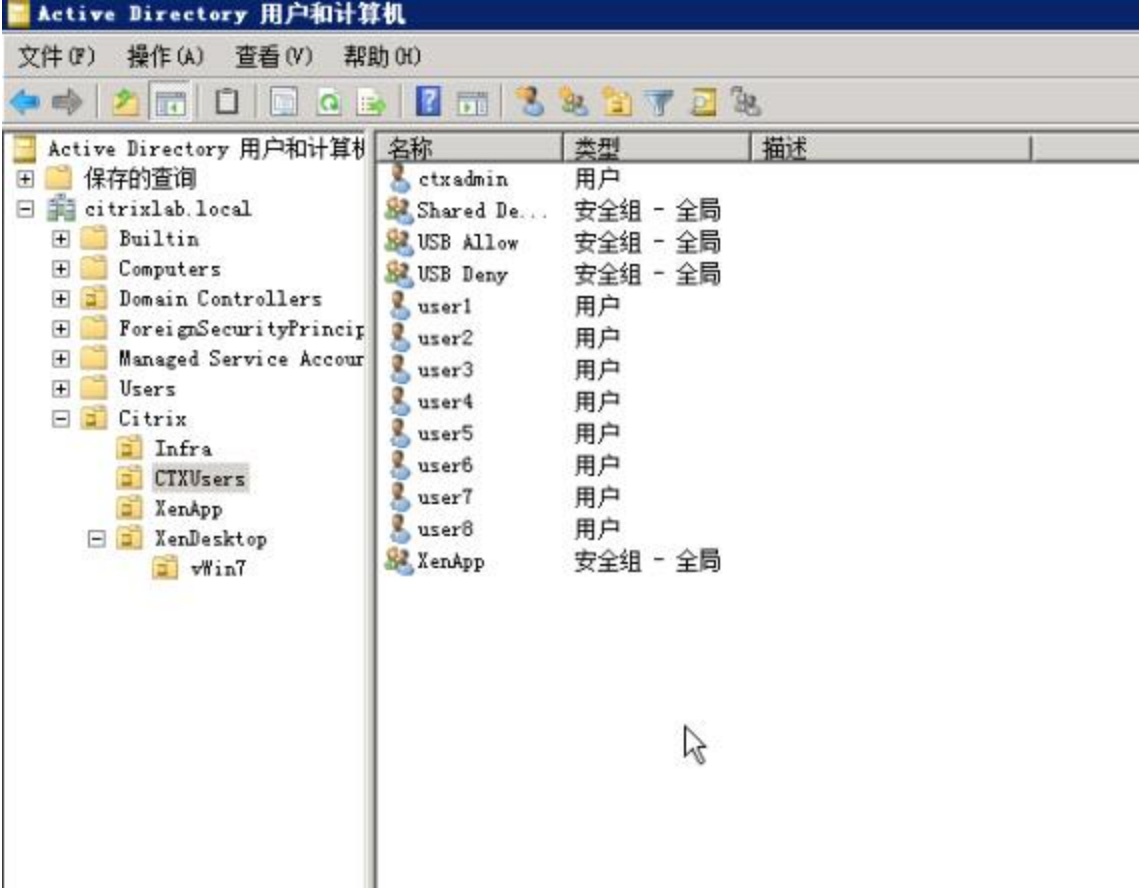
步骤	操作
1.	<p>开始-管理工具-Active Directory 用户和计算机</p>  <p>The screenshot shows the Windows Start menu with the 'Administrative Tools' folder expanded. The 'Active Directory 用户和计算机' (Active Directory Users and Computers) option is highlighted. The taskbar at the bottom shows the '开始' (Start) button and several application icons.</p>

步骤	操作
2.	<p>右击刚才所建域（此处为 citrixlab.local）-新建-组织单位</p>  <p>The screenshot shows the 'Active Directory 用户和计算机' window. The left pane shows the tree structure with 'citrixlab.local' selected. The right pane shows a list of objects. A context menu is open over 'citrixlab.local', and the 'New' option is selected, leading to a sub-menu where '组织单位' (Organizational Unit) is highlighted.</p>
3.	<p>输入组织单元名称，如 Citrix，勾选“防止容器被意外删除”，“确定”</p>  <p>The screenshot shows the '新建对象 - 组织单位' dialog box. The '创建于' (Created at) field is set to 'citrixlab.local/'. The '名称 (A):' (Name) field contains 'Citrix'. The checkbox '防止容器被意外删除 (P)' (Prevent accidental deletion of container) is checked. The '确定' (OK) button is highlighted.</p>
4.	其他组织单元可参考如上建立

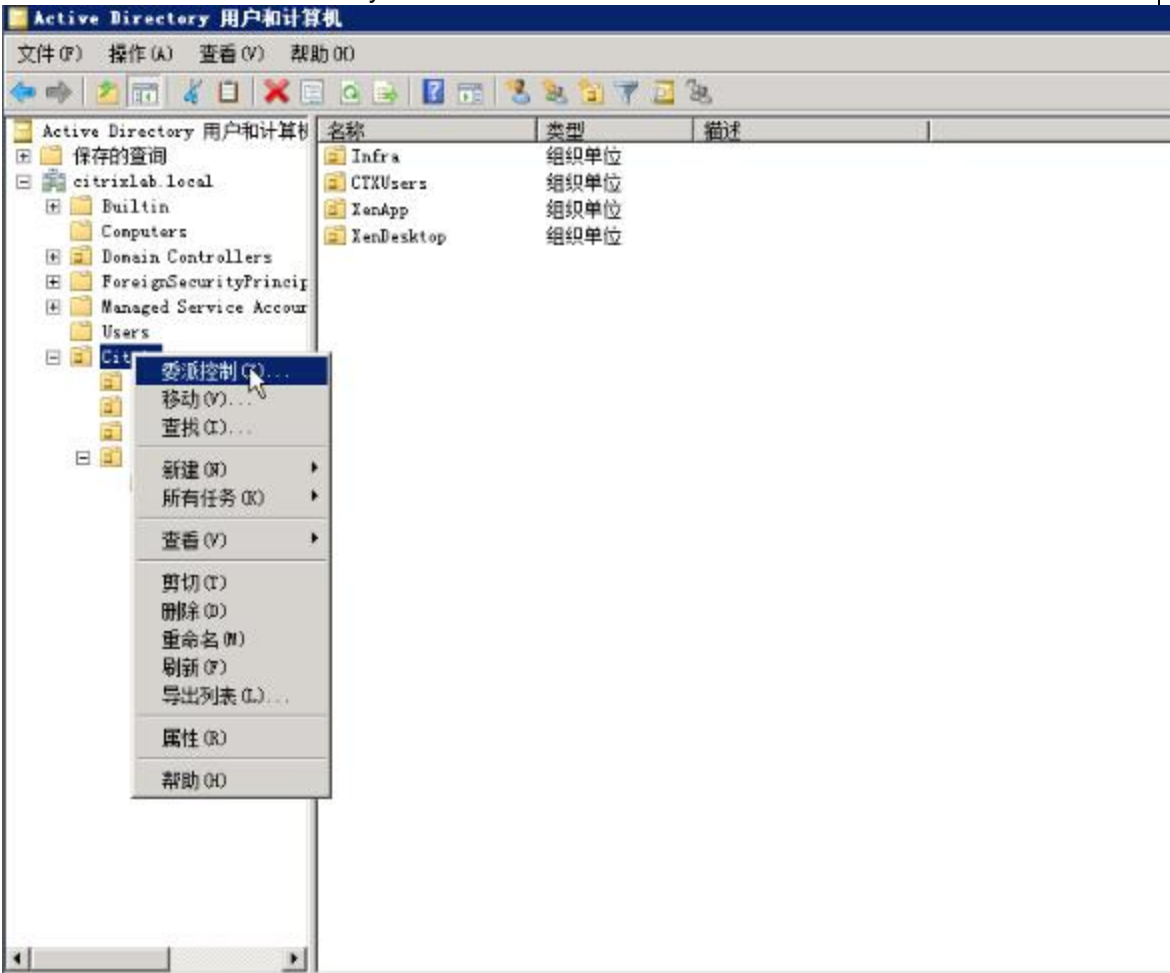
步骤	操作															
5.	<p>可查看在 Citrix 下所建立所有组织单元信息</p>  <p>The screenshot shows the 'Active Directory 用户和计算机' window. The left pane displays a tree view of the directory structure. Under 'citrixlab.local', the 'Citrix' organizational unit is expanded, showing sub-units: 'Infra', 'CTXUsers', 'XenApp', and 'XenDesktop'. The right pane shows a list of these sub-units with columns for '名称' (Name), '类型' (Type), and '描述' (Description). All listed sub-units are of type '组织单位' (Organizational Unit).</p> <table><tr><th>名称</th><th>类型</th><th>描述</th></tr><tr><td>Infra</td><td>组织单位</td><td></td></tr><tr><td>CTXUsers</td><td>组织单位</td><td></td></tr><tr><td>XenApp</td><td>组织单位</td><td></td></tr><tr><td>XenDesktop</td><td>组织单位</td><td></td></tr></table>	名称	类型	描述	Infra	组织单位		CTXUsers	组织单位		XenApp	组织单位		XenDesktop	组织单位	
名称	类型	描述														
Infra	组织单位															
CTXUsers	组织单位															
XenApp	组织单位															
XenDesktop	组织单位															
6.	<p>右击 CTXUsers-新建-用户，填写用户名，用户登录名</p>  <p>The screenshot shows the '新建对象 - 用户' dialog box. It contains fields for creating a new user. The '创建于' (Created by) field is set to 'citrixlab.local/Citrix/CTXUsers'. The '姓' (Surname) field is 'ctxadmin'. The '名' (Given name) field is empty, and the '英文缩写' (Initials) field is also empty. The '姓名' (Full name) field is 'ctxadmin'. The '用户登录名' (User logon name) field is 'ctxadmin', and the domain dropdown is set to '@citrixlab.local'. The '用户登录名 (Windows 2000 以前版本)' (User logon name (Windows 2000 and earlier versions)) field is 'CITRIXLAB\ctxadmin'. At the bottom, there are buttons for '< 上一步' (Previous), '下一步 >' (Next), and '取消' (Cancel).</p>															

步骤	操作
7.	<p>输入密码，可选择密码设置，此处为便于操作，选择“密码永不过期” “下一步”</p> 


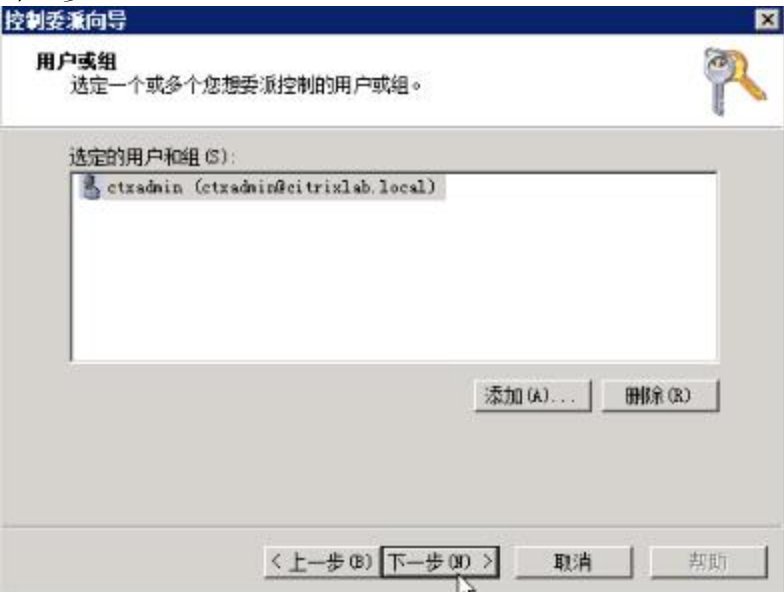
步骤	操作
8.	<p>右击属性-隶属于-添加 将 ctxadmin 加入 Account Operators 组中 注：Account Operators，可以管理域内的帐号、组。无特殊情况请勿加入 Domain Admin 组。</p> 
9.	<p>创建普通用户，操作和前面基本一致 右击 CTXUsers-新建-用户，填写用户名，用户登录名</p> 

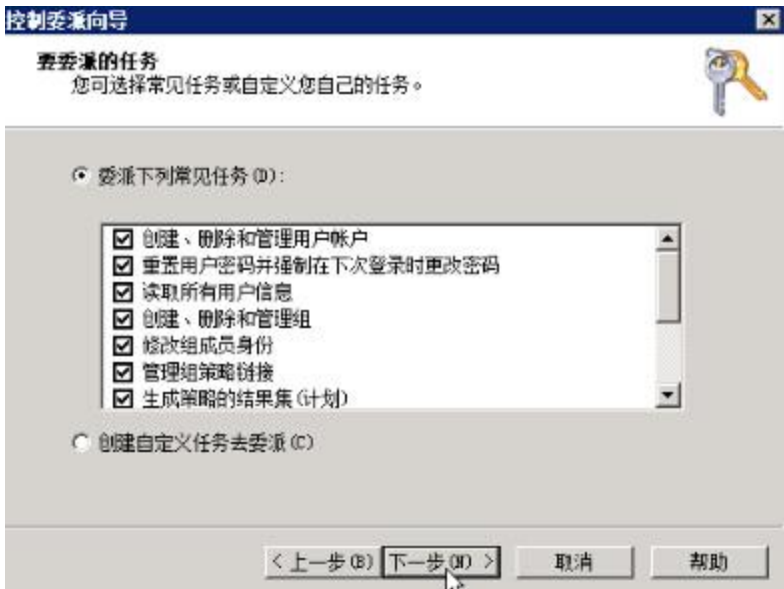
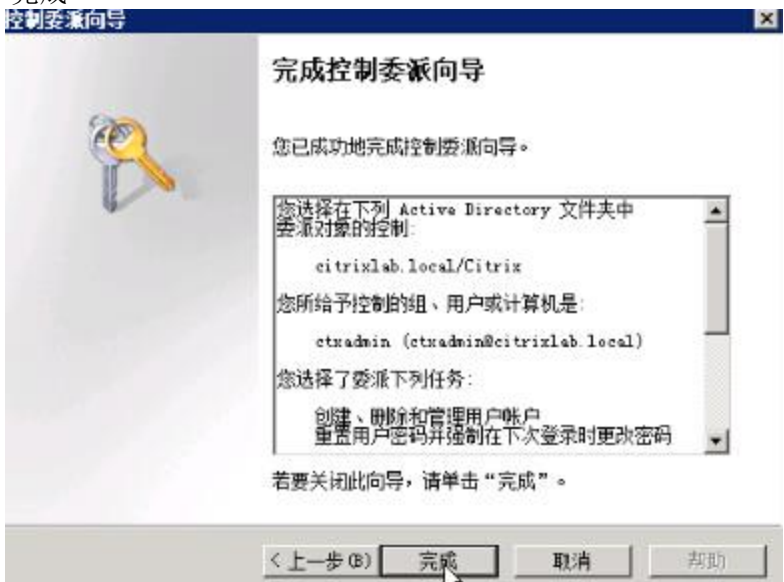
步骤	操作																																										
10.	<p>输入密码，可选择密码设置，此处为便于操作，选择“密码永不过期” “下一步”</p> 																																										
11.	<p>可查看建立所有用户信息</p>  <table><thead><tr><th>名称</th><th>类型</th><th>描述</th></tr></thead><tbody><tr><td>ctxadmin</td><td>用户</td><td></td></tr><tr><td>Shared De...</td><td>安全组 - 全局</td><td></td></tr><tr><td>USB Allow</td><td>安全组 - 全局</td><td></td></tr><tr><td>USB Deny</td><td>安全组 - 全局</td><td></td></tr><tr><td>user1</td><td>用户</td><td></td></tr><tr><td>user2</td><td>用户</td><td></td></tr><tr><td>user3</td><td>用户</td><td></td></tr><tr><td>user4</td><td>用户</td><td></td></tr><tr><td>user5</td><td>用户</td><td></td></tr><tr><td>user6</td><td>用户</td><td></td></tr><tr><td>user7</td><td>用户</td><td></td></tr><tr><td>user8</td><td>用户</td><td></td></tr><tr><td>XenApp</td><td>安全组 - 全局</td><td></td></tr></tbody></table>	名称	类型	描述	ctxadmin	用户		Shared De...	安全组 - 全局		USB Allow	安全组 - 全局		USB Deny	安全组 - 全局		user1	用户		user2	用户		user3	用户		user4	用户		user5	用户		user6	用户		user7	用户		user8	用户		XenApp	安全组 - 全局	
名称	类型	描述																																									
ctxadmin	用户																																										
Shared De...	安全组 - 全局																																										
USB Allow	安全组 - 全局																																										
USB Deny	安全组 - 全局																																										
user1	用户																																										
user2	用户																																										
user3	用户																																										
user4	用户																																										
user5	用户																																										
user6	用户																																										
user7	用户																																										
user8	用户																																										
XenApp	安全组 - 全局																																										

第7章 组织单位（Citrix）委派

步骤	操作															
1.	<div>开始-管理工具-Active Directory 用户和计算机-citrixlab.local-右击 Citrix-委派控制</div> <div><p>The screenshot shows the 'Active Directory 用户和计算机' console for the 'citrixlab.local' domain. The left pane shows the tree structure with 'Citrix' selected under 'Users'. The right pane displays a table of objects in the 'Citrix' OU:</p><table><tr><th>名称</th><th>类型</th><th>描述</th></tr><tr><td>Infra</td><td>组织单位</td><td></td></tr><tr><td>CTXUsers</td><td>组织单位</td><td></td></tr><tr><td>XenApp</td><td>组织单位</td><td></td></tr><tr><td>XenDesktop</td><td>组织单位</td><td></td></tr></table><p>A context menu is open over the 'Citrix' folder, with '委派控制 (C)...' highlighted. Other menu items include '移动 (M)...', '查找 (F)...', '新建 (N)', '所有任务 (O)', '查看 (V)', '剪切 (T)', '删除 (D)', '重命名 (R)', '刷新 (F)', '导出列表 (L)...', '属性 (R)', and '帮助 (H)'.</p></div> <div>在此文件夹的委派对象控制</div>	名称	类型	描述	Infra	组织单位		CTXUsers	组织单位		XenApp	组织单位		XenDesktop	组织单位	
名称	类型	描述														
Infra	组织单位															
CTXUsers	组织单位															
XenApp	组织单位															
XenDesktop	组织单位															

步骤	操作
2.	<p>“下一步”</p> 
3.	<p>“添加”</p> 

步骤	操作
4.	<p>填写用户名 ctxadmin</p> 
5.	<p>“下一步”</p> 

步骤	操作
6.	<p>根据实际情况，选择委派的权限。 本次实验全选</p> 
7.	<p>“完成”</p> 

第8章 环境完成确认检查

本 LAB 结束后，请确认以下事项以：

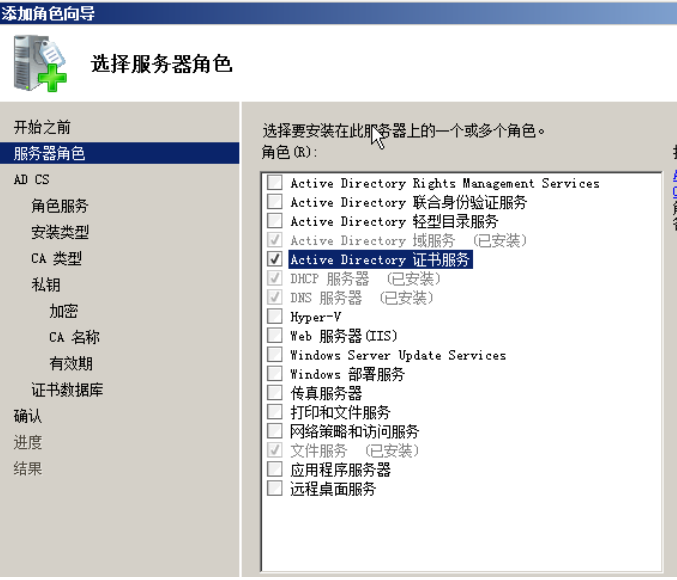
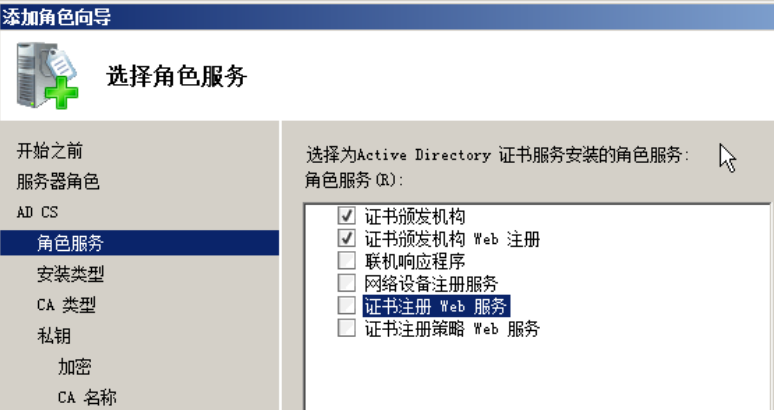
- 活动目录环境建立完毕。DNS、DHCP 服务配置完毕，工作正常。
- IP 地址主机名等配置均按表格配置，并且加入活动目录，登录域正常。
- 相应的 OU，用户账号在活动目录内建立完毕。


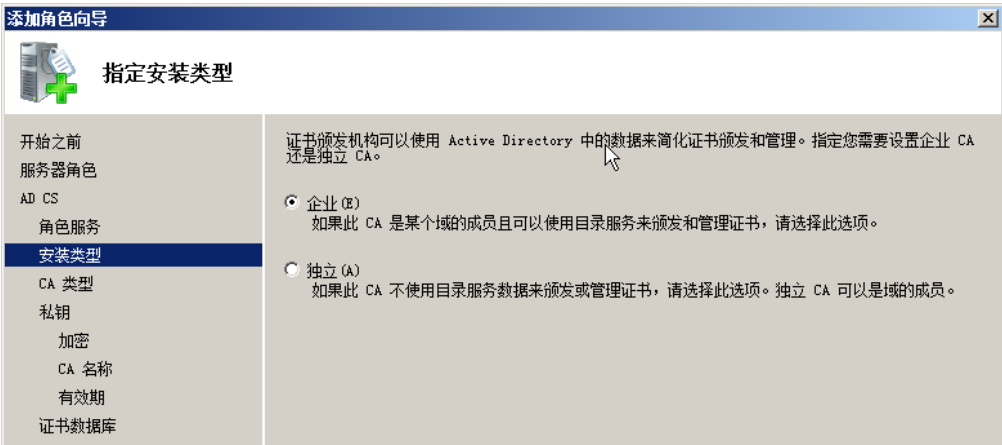
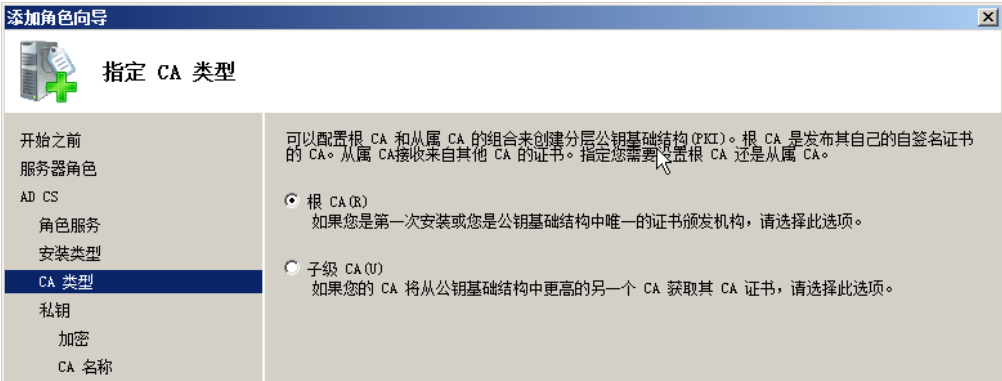
第9章 Windows CA 服务器安装配置

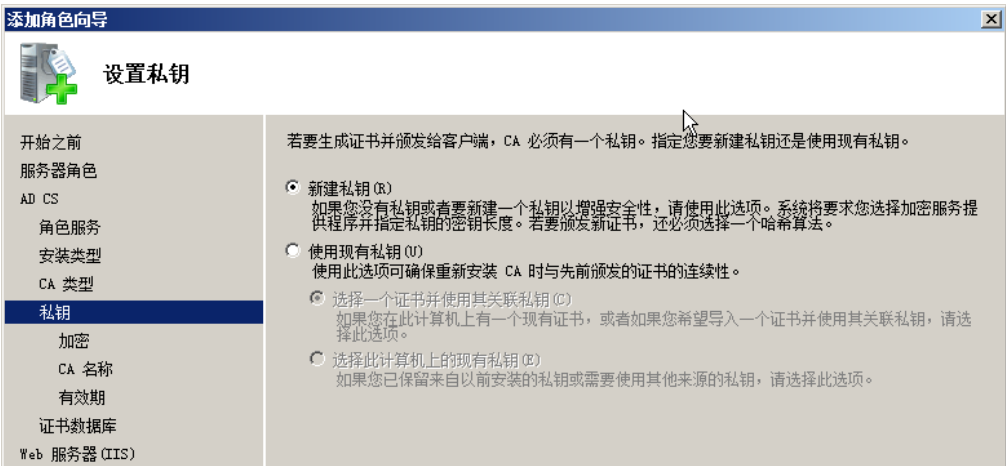
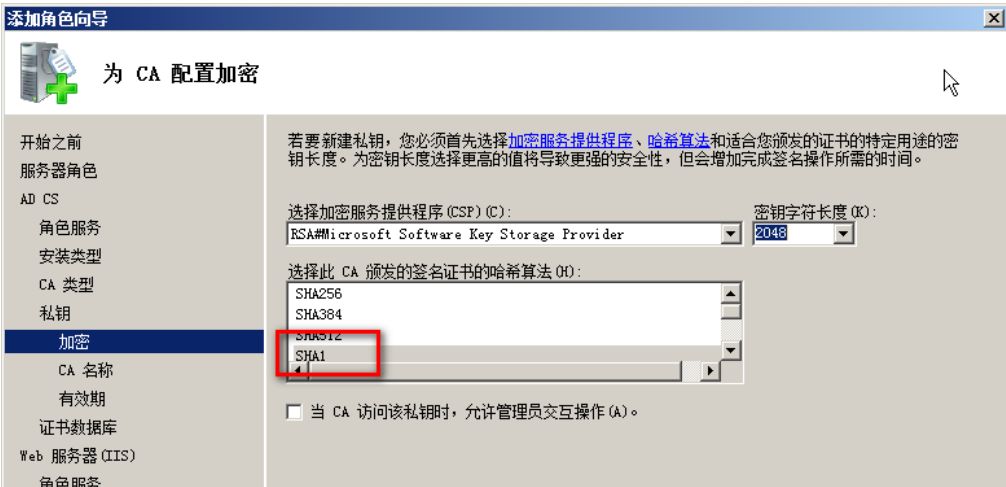
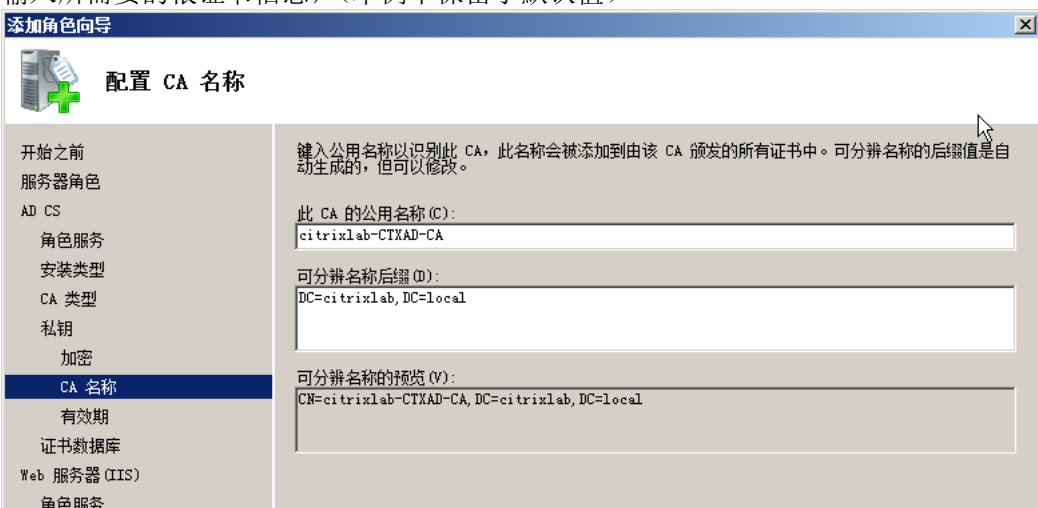
为了在域中实现 HTTPS 安全通信，我们需要为主机提供服务器证书。鉴于 Android 设备对于 NetScaler 自建证书识别不正常的情况，以后 PoC 项目所需要使用的证书都请通过 Windows Certificate Authority (CA) 服务来创建。

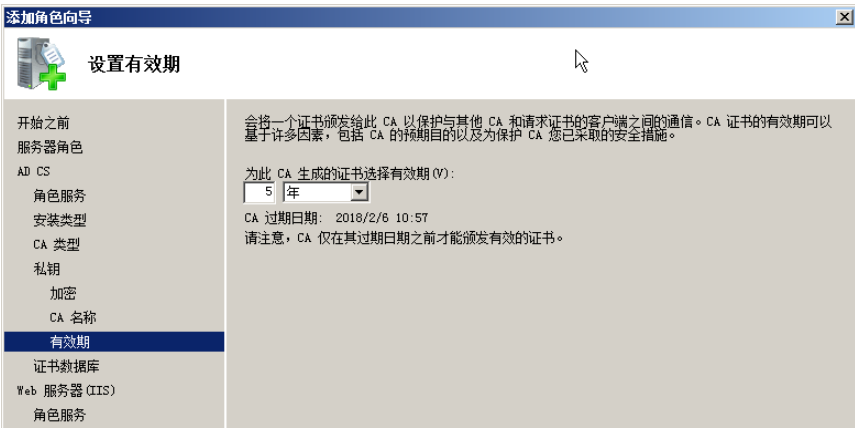

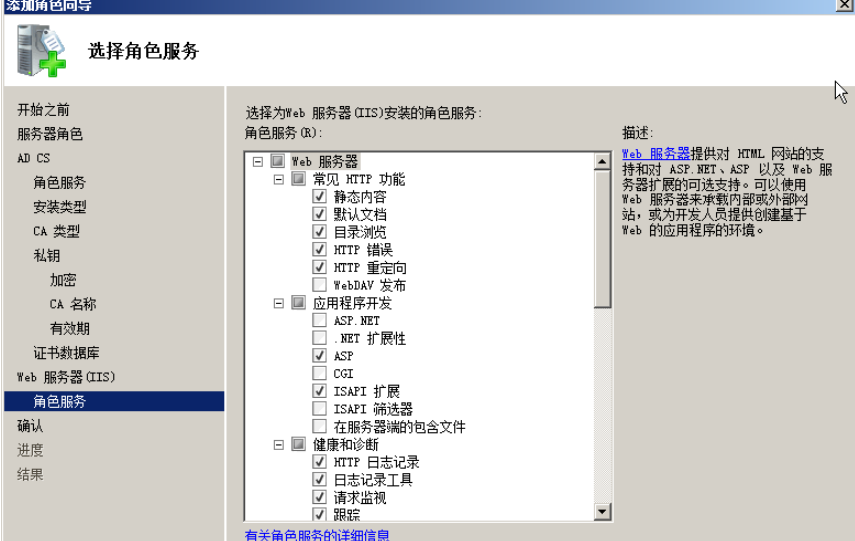
本例中，我们将 Windows CA 搭建在域控制器 CTXAD 上。



关于数字证书的概念，请参考：<http://baike.baidu.com/view/16501.htm>

步骤	操作
1.	登陆 CTXAD，打开“服务器管理器”->“添加角色”
2.	<p>勾选“Active Directory 证书服务”，点击 下一步，</p>  <p>添加角色向导</p> <p>选择服务器角色</p> <p>开始之前</p> <p>服务器角色</p> <p>AD CS</p> <p>角色服务</p> <p>安装类型</p> <p>CA 类型</p> <p>私钥</p> <p>加密</p> <p>CA 名称</p> <p>有效期</p> <p>证书数据库</p> <p>确认</p> <p>进度</p> <p>结果</p> <p>选择要安装在此服务器上的一个或多个角色。</p> <p>角色(R):</p> <ul style="list-style-type: none"> <input type="checkbox"/> Active Directory Rights Management Services <input type="checkbox"/> Active Directory 联合身份验证服务 <input type="checkbox"/> Active Directory 轻型目录服务 <input checked="" type="checkbox"/> Active Directory 域服务 (已安装) <input checked="" type="checkbox"/> Active Directory 证书服务 <input checked="" type="checkbox"/> DHCP 服务器 (已安装) <input checked="" type="checkbox"/> DNS 服务器 (已安装) <input type="checkbox"/> Hyper-V <input type="checkbox"/> Web 服务器 (IIS) <input type="checkbox"/> Windows Server Update Services <input type="checkbox"/> Windows 部署服务 <input type="checkbox"/> 传真服务器 <input type="checkbox"/> 打印和文件服务 <input type="checkbox"/> 网络策略和访问服务 <input checked="" type="checkbox"/> 文件服务 (已安装) <input type="checkbox"/> 应用程序服务器 <input type="checkbox"/> 远程桌面服务
3.	<p>选择“证书颁发机构”、“证书颁发机构 Web 注册”</p>  <p>添加角色向导</p> <p>选择角色服务</p> <p>开始之前</p> <p>服务器角色</p> <p>AD CS</p> <p>角色服务</p> <p>安装类型</p> <p>CA 类型</p> <p>私钥</p> <p>加密</p> <p>CA 名称</p> <p>选择为Active Directory 证书服务安装的角色服务：</p> <p>角色服务(R):</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> 证书颁发机构 <input checked="" type="checkbox"/> 证书颁发机构 Web 注册 <input type="checkbox"/> 联机响应程序 <input type="checkbox"/> 网络设备注册服务 <input checked="" type="checkbox"/> 证书注册 Web 服务 <input type="checkbox"/> 证书注册策略 Web 服务

步骤	操作
4.	<p>跳出如下提示，选择“添加所需的角色服务”</p> 
5.	<p>选择“企业”</p> 
6.	<p>选择“根 CA”</p> 

步骤	操作
7.	<p>选择“新建私钥”</p> 
8.	<p>选择“SHA1”哈希算法</p> 
9.	<p>输入所需要的根证书信息，（本例中保留了默认值）</p> 

步骤	操作
10.	<p>证书有效期选择默认的“5 年”</p> 
11.	<p>接下去一路下一步，完成证书服务的安装</p> 
12.	

步骤	操作
13.	 <p>The screenshot shows the 'Add Role Wizard' window with the 'Results' (结果) tab selected. It lists the successfully installed roles and features:</p> <ul style="list-style-type: none"> Active Directory 证书服务 (Active Directory Certificate Services): 安装成功 (Installed successfully). Sub-features include: 证书颁发机构 (Certificate Authority), 证书颁发机构 Web 注册 (Certificate Authority Web Enrollment). Web 服务器 (IIS) (Web Server (IIS)): 安装成功 (Installed successfully). Sub-features include: Web 服务器 (Web Server), 常见 HTTP 功能 (Common HTTP Features), 静态内容 (Static Content), 默认文档 (Default Document), 目录浏览 (Directory Browsing), HTTP 错误 (HTTP Errors), HTTP 重定向 (HTTP Redirect), 应用程序开发 (Application Development), ASP, ISAPI 扩展 (ISAPI Extensions), 健康和诊断 (Health and Diagnostics), HTTP 日志记录 (HTTP Logging), 日志记录工具 (Logging Tools), 请求监视 (Request Monitoring). <p>Buttons at the bottom include: < 上一步(B) (Previous), 下一步(N) > (Next), 关闭(O) (Close), and 取消 (Cancel).</p>
14.	<p>打开浏览器，输入 http://localhost/certsrv/，确认证书服务工作正常</p>  <p>The screenshot shows the Microsoft Active Directory Certificate Services website in Internet Explorer. The address bar shows http://localhost/certsrv/. The page title is 'Microsoft Active Directory 证书服务 - citrixlab-CTXAD-CA'. The main content area includes a '欢迎使用' (Welcome) section and instructions on how to use the website for certificate management.</p> <p>有关 Active Directory 证书服务的详细信息，请参阅 Active Directory 证书服务文档.</p> <p>选择一个任务：</p> <ul style="list-style-type: none"> 申请证书 查看挂起的证书申请的状态 下载 CA 证书、证书链或 CRL

产品版本

产品	版本
XenDesktop	7.5
XenApp	7.5
XenServer	6.2 SP1
NetScaler	10.1