

王哥哥哥哥

微软让我们一起改变世界

博客园

首页

新随笔

联系

订阅

管理

随笔 - 33 文章 - 0 评论 - 6

Windows Server 2012 R2 创建AD域

前言

我们按照下图来创建第一个林中的第一个域。创建方法为先安装一台Windows服务器，然后将其升级为域控制器。然后创建第二台域控制器，一台成员服务器与一台加入域的Win8计算机。

公告

希望能和大家一起研究微软的公有和私有云
大家一起进步，一起使用微软的技术来改变世界

昵称：王哥哥哥哥

园龄：2年6个月

粉丝：6

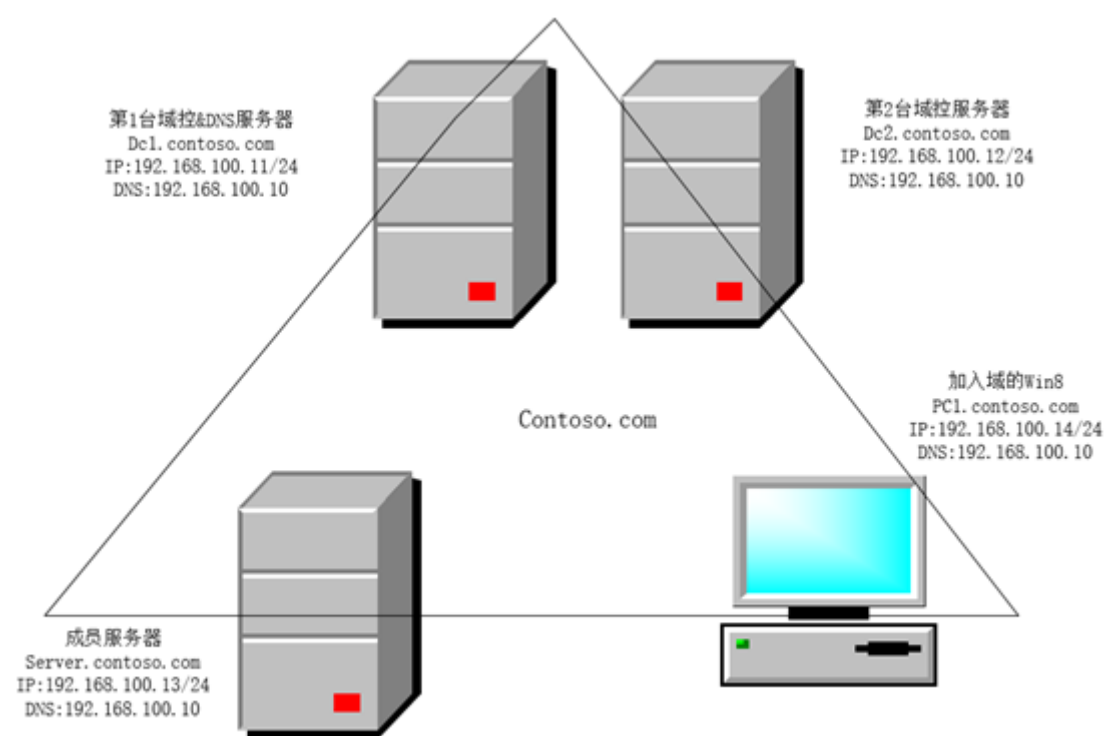
关注：1

+加关注

<	2018年1月						>
日	一	二	三	四	五	六	
31	1	2	3	4	5	6	
7	8	9	10	11	12	13	
14	15	16	17	18	19	20	
21	22	23	24	25	26	27	
28	29	30	31	1	2	3	
4	5	6	7	8	9	10	

搜索





环境

网络192.168.100.1 子网掩码 255.255.255.0 网关192.168.100.2

域名 contoso.com

DC1 192.168.100.11/24

DC2 192.168.100.12/24

Server 192.168.100.13/24

PC1 192.168.100.14/24

创建域的必备条件

- **DNS域名**：先要想好一个符合dns格式的域名，如 contoso.com
- **DNS服务器**：域中需要将自己注册到DNS服务器内，靠其他计算机通过DNS服务器来找到这台机器，因此需要一台可支持AD的DNS服务器，并且支持动态更新（如果现在没有DNS服务器，则可以在创建域的过程中，选择这台域控上安装DNS服务器）

常用链接

[我的随笔](#)
[我的评论](#)
[我的参与](#)
[最新评论](#)
[我的标签](#)

最新随笔

1. 本博客停止更新改用wordperss
2. Powershell批量安装SNMP服务
3. DELL OME监控服务器安装配置
4. 用beamoff给VMware的Mac OS X 10.10.x加速
5. VMware 12Pro 安装MACOS 10.10
6. 特别篇：Hyper-v群集模拟实战演示
7. DELL 服务器报CPU 1 has an internal error (IERR)
8. 第十章 实时迁移
9. 第九章 通过 SMB 共享虚拟机
10. 第八章 Hyper-V 2012 R2 故障转移群集

我的标签

[dell\(1\)](#)
[DELL OME\(1\)](#)
[hyper\(1\)](#)
[powershell\(1\)](#)
[windows\(1\)](#)
[windows server 2012\(1\)](#)
[故障转移群集\(1\)](#)

随笔分类

注：AD需要一个SYSVOL文件夹来存储域共享文件（例如域组策略有关的文件），该文件夹必须位于NTFS磁盘，系统默认创建在系统盘，为了性能建议按照到其他分区。

创建网络中的第一台域控制器

修改机器名和ip

先修改ip地址，并且将dns指向自己，并且修改计算机名为DC1，升级成域控后，机器名称会自动变成dc1.contoso.com

计算机名	DC1
工作组	WORKGROUP
Windows 防火墙	公用: 启用
远程管理	已启用
远程桌面	已启用
NIC 组合	已禁用
Ethernet0	192.168.100.11，IPv6 已启用

安装域功能

- DELL 服务器(2)
- Hyper-v(10)
- MAC OS(2)
- Powershell(1)
- System Center(1)
- Windows(3)
- Windows Server 2012 R2系统配置(11)
- 随便写写(2)

随笔档案

- 2015年9月 (1)
- 2015年8月 (18)
- 2015年7月 (8)
- 2015年6月 (6)

公有云

Azure Lei Zhang的博客
衡子

最新评论

- Re:VMware 12Pro 安装MACOS 10.10
博主,你的网盘链接不可用了~
--Sungeek
- Re:第三章 Hyper-V 2012 R2配置选项
我印象中,好像VMware Workstation不会产生类似的文件吧?除非挂起虚拟机,它才会保存一个虚拟机内存的文件.但为何Hyper-V在运行时 也会有这样一个bin文件?真是让人不解,本来SSD.....
--wkl17
- Re:第八章 Hyper-V 2012 R2 故障转移群集
大神有没有联系方式可以留一个 希望和你学习下
--nocoah



选择服务器

4. Re:Windows Server 2012 R2 创建AD域
谢谢分享

--server126

5. Re:特别篇：Hyper-v群集模拟实战演示
@玻璃鱼儿这倒还好，主要最近很忙，没空写我自己也在学习，感觉微软官方的东西不好，所以买书看，顺便把自己实际工作中的经验分享出来...

--王哥哥哥哥

阅读排行榜

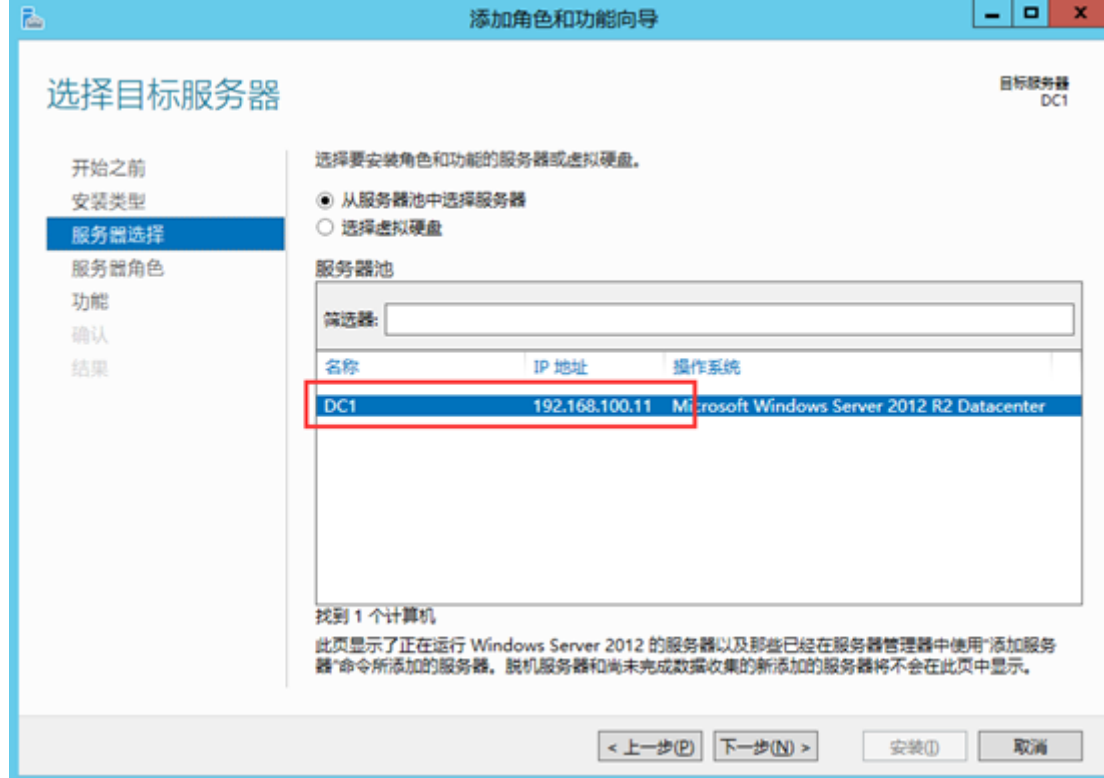
1. Windows Server 2012 R2 创建AD域 (22951)
2. VMware 12Pro 安装MACOS 10.10(10616)
3. 利用WSUS部署更新程序(8762)
4. 用beamoff给VMware的Mac OS X 10.10.x加速(3717)
5. 第四章 Hyper-V 2012 R2 网络配置 (3641)

评论排行榜

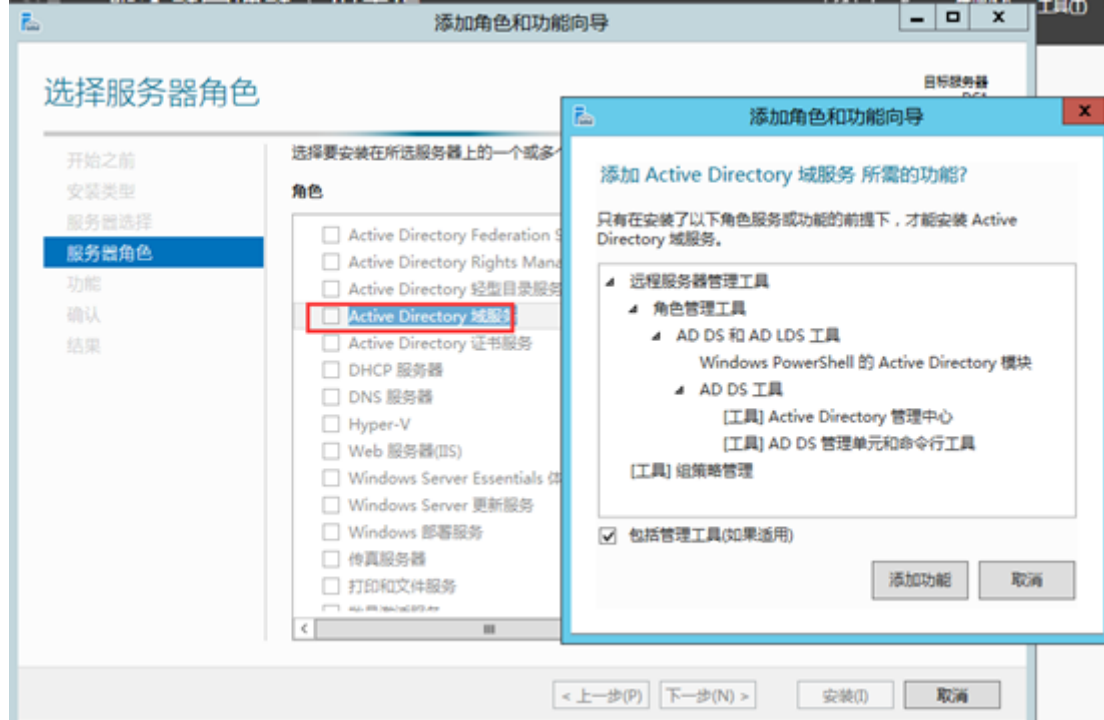
1. 特别篇：Hyper-v群集模拟实战演示(2)
2. 第八章 Hyper-V 2012 R2 故障转移群集 (1)
3. Windows Server 2012 R2 创建AD域(1)
4. 第三章 Hyper-V 2012 R2配置选项(1)
5. VMware 12Pro 安装MACOS 10.10(1)

推荐排行榜

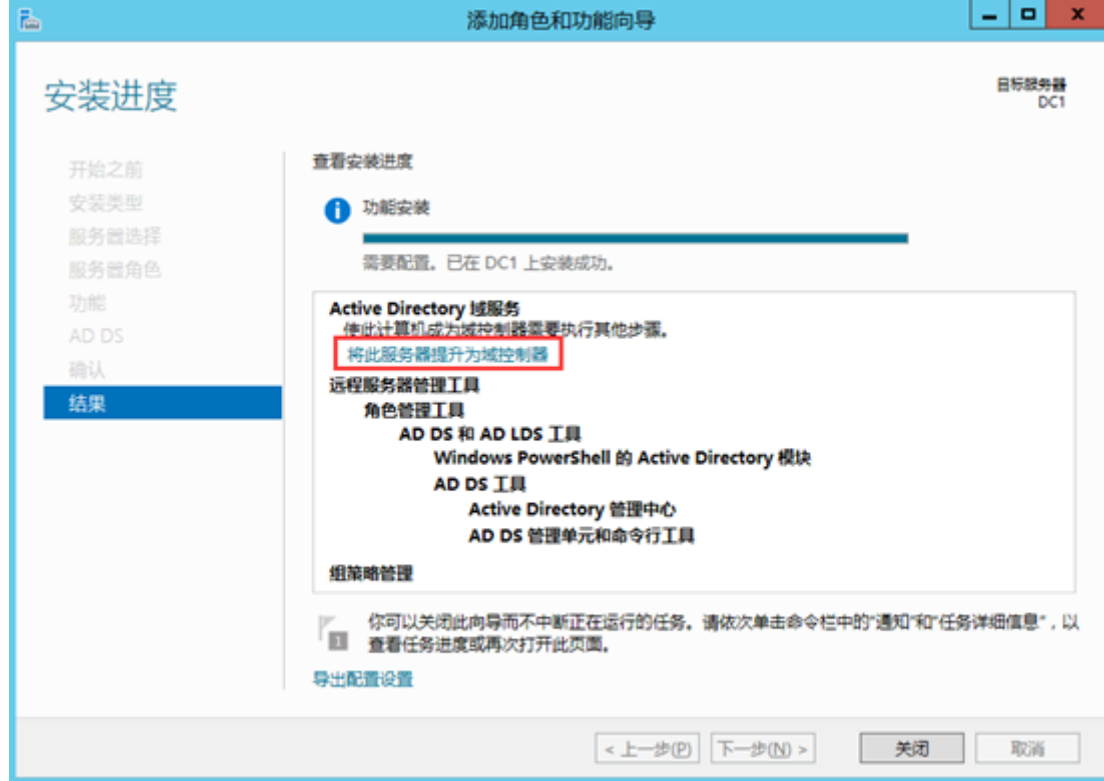
1. Windows Server 2012 R2 创建AD域(1)
2. 特别篇：Hyper-v群集模拟实战演示(1)
3. 第十章 实时迁移(1)
4. 第八章 Hyper-V 2012 R2 故障转移群集 (1)



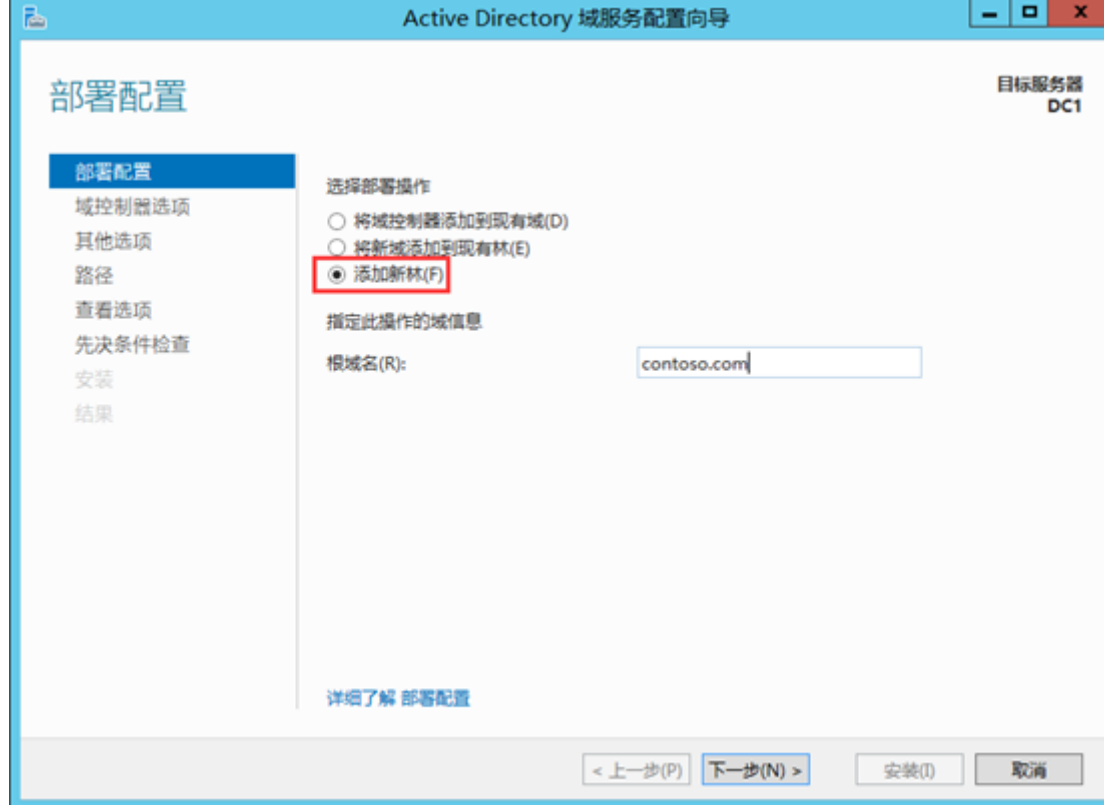
选择域服务



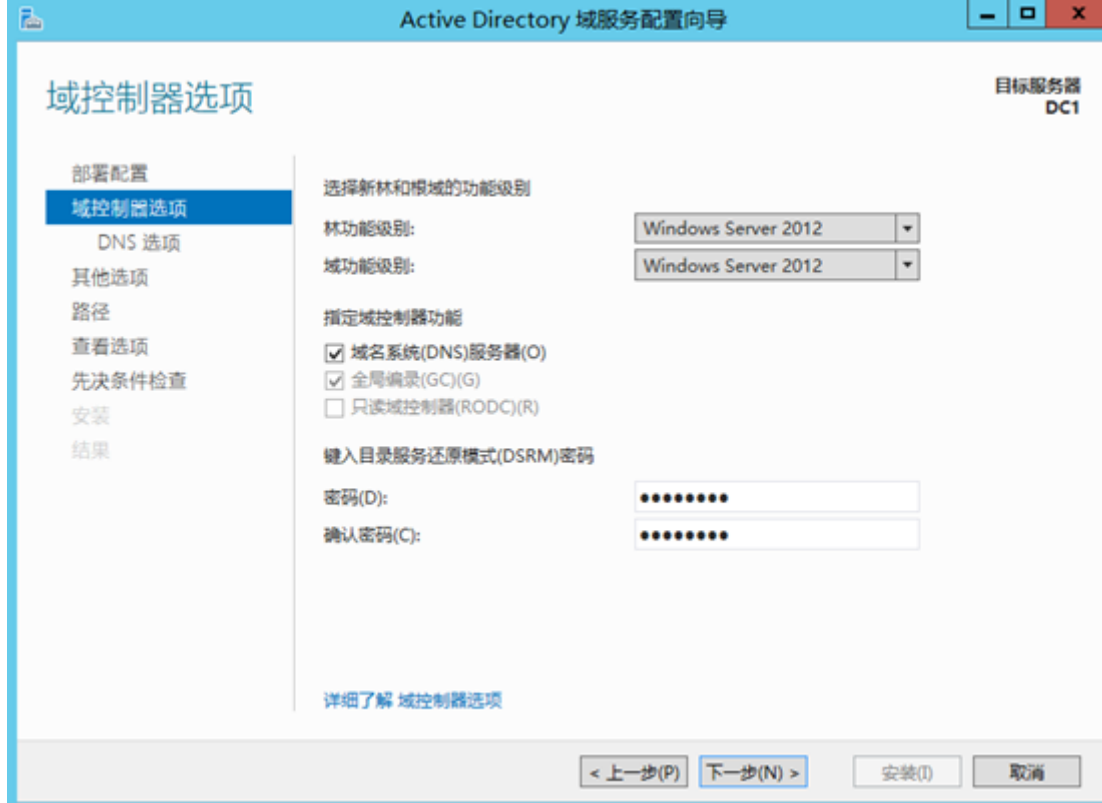
提升为域控制器



添加新林



此林根域名不要与对外服务器的DNS名称相同，如对外服务的DNS URL为<http://www.contoso.com>，则内部的林根域名就不能是contoso.com，否则未来可能会有兼容问题。



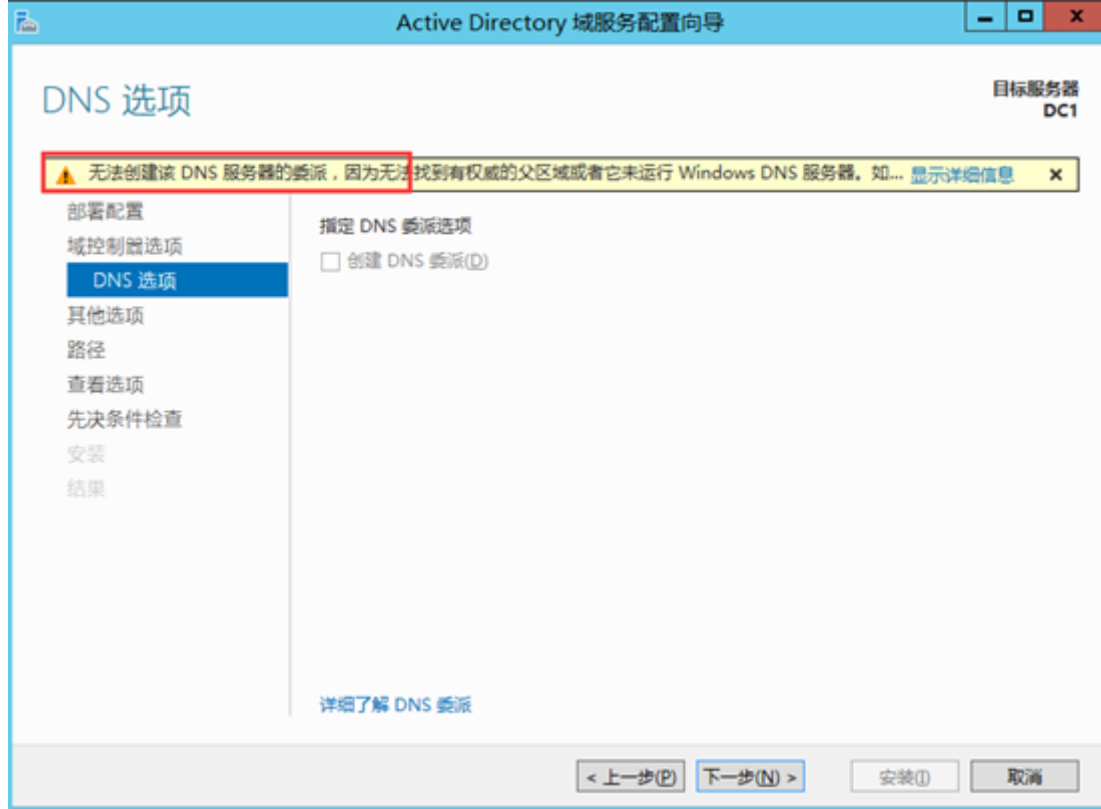
- 选择林功能级别，域功能级别。

此处我们选择的为win 2012，此时域功能级别只能是win 2012，如果选择其他林功能级别，还可以选择其他域功能级别

- 默认会直接在此服务器上安装DNS服务器
- 第一台域控制器必须是全局编录服务器的角色
- 第一台域控制器不可以是只读域控制器（RODC）这个角色是win 2008时新出来的功能
- 设置目录还原密码。

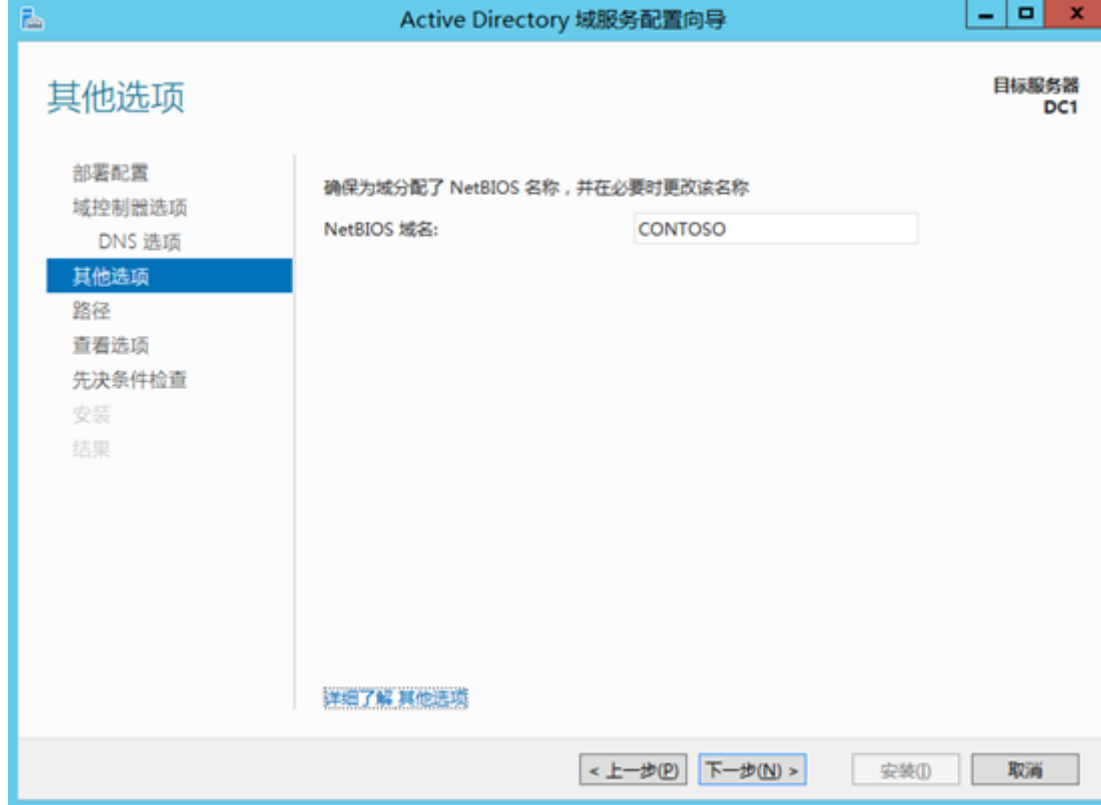
目录还原模式是一个安全模式，可以开机进入安全模式时修复AD数据库，但是必须使用此密码

出现此警告无需理会

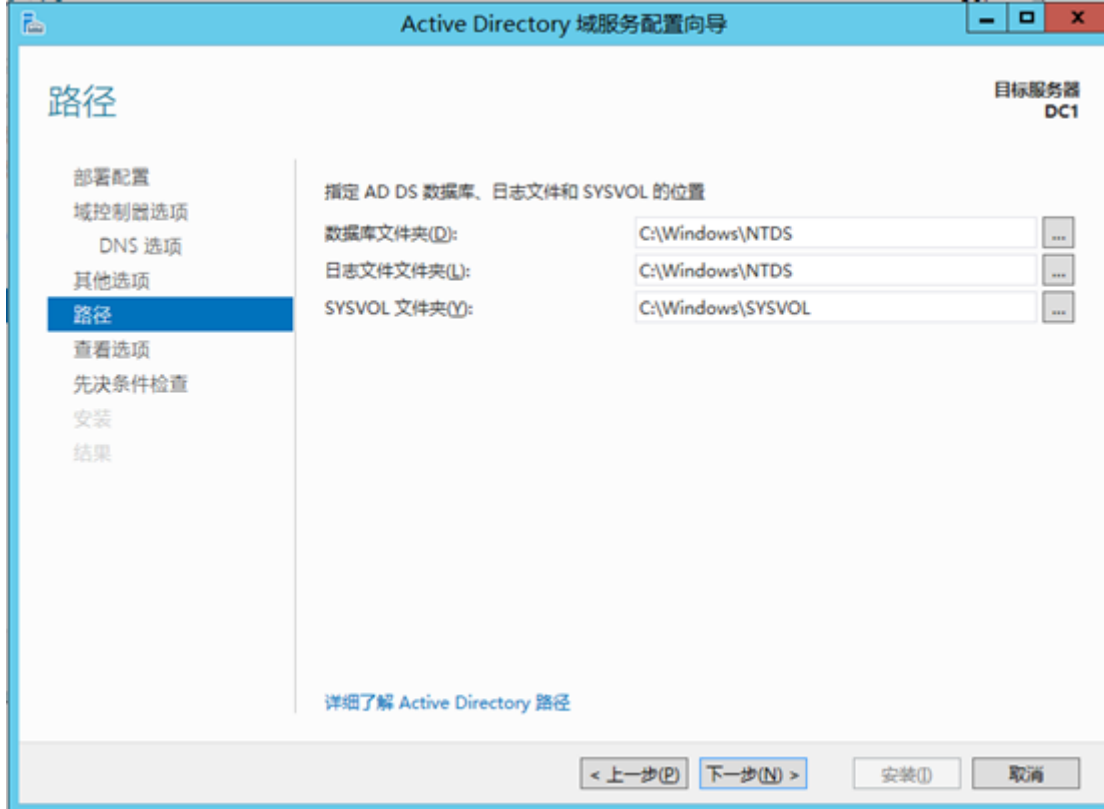


系统会自动创建一个netbios名称，可以更改。

不支持DNS域名的旧系统，如win98 winnt需要通过netbios名来进行通信

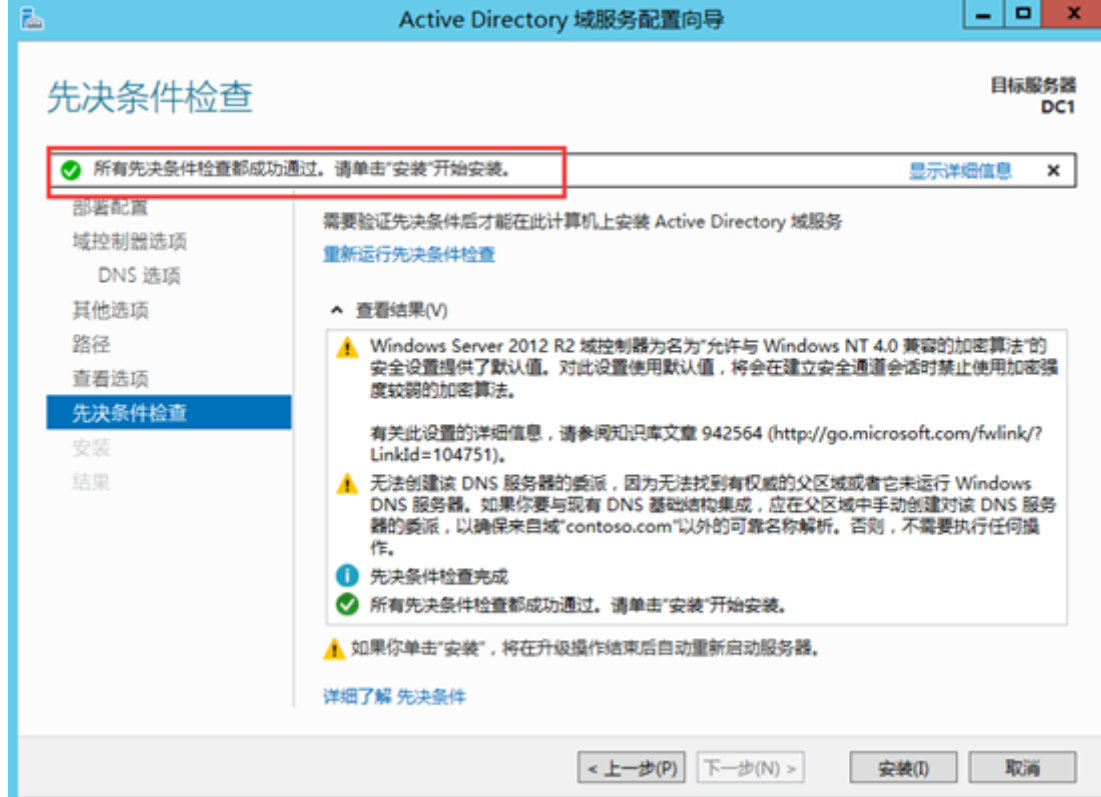


- 数据库文件夹：用了存储AD数据库
- 日志文件文件夹：用了存储AD的更改记录，此记录可以用来修复AD数据库
- SYSVOL文件夹：用了存储域共享文件（例如组策略）



如果计算机内有多个硬盘，建议将数据库与日志文件夹分别设置到不同的硬盘内，分两个硬盘可以提供运行效率，而且分开存储可以避免两份数据同时出现问题，以提高修复AD的能力。（不过我认为现在都是RAID模式了没必要分开，和操作系统分区分开就可以了）

顺利通过检查，直接安装



安装完成重启



检查DNS服务器内的记录是否完备

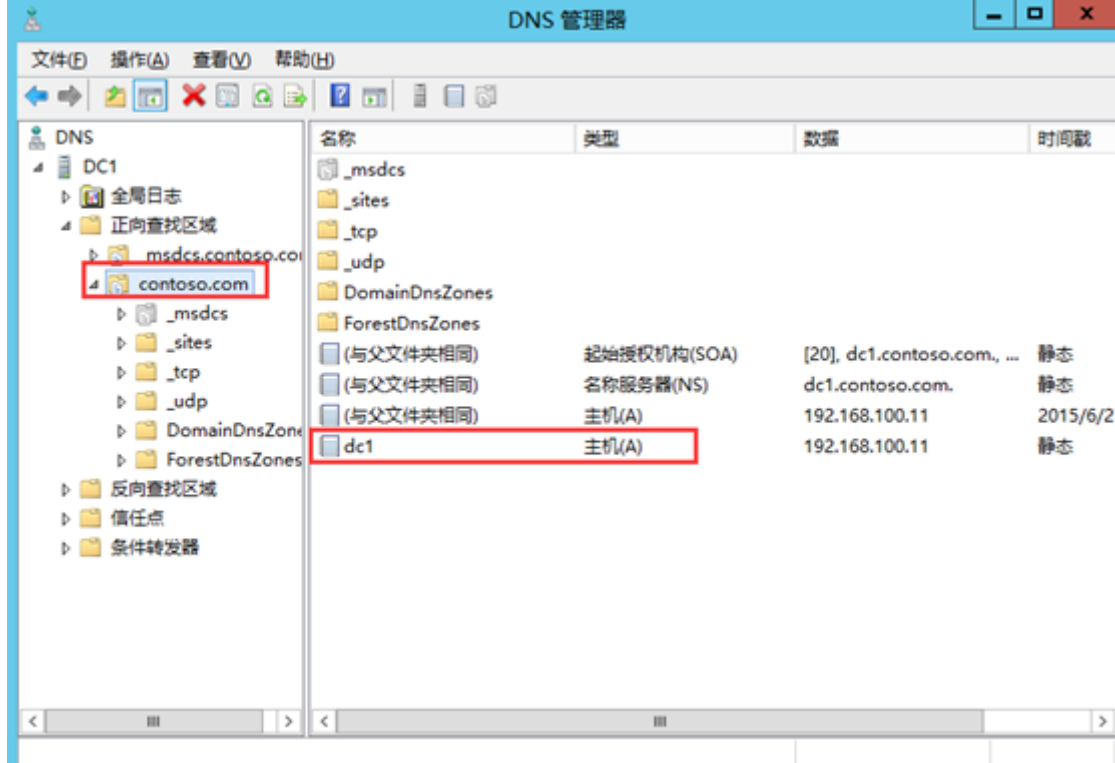
域控会将自己扮演的角色注册到DNS服务器内，以便让其他计算机能够通过DNS服务器来找到域控。因此先检查DNS服务器内是否已经存在这些记录。需要用域管理员账户来登陆contoso\administrator.

检查主机记录

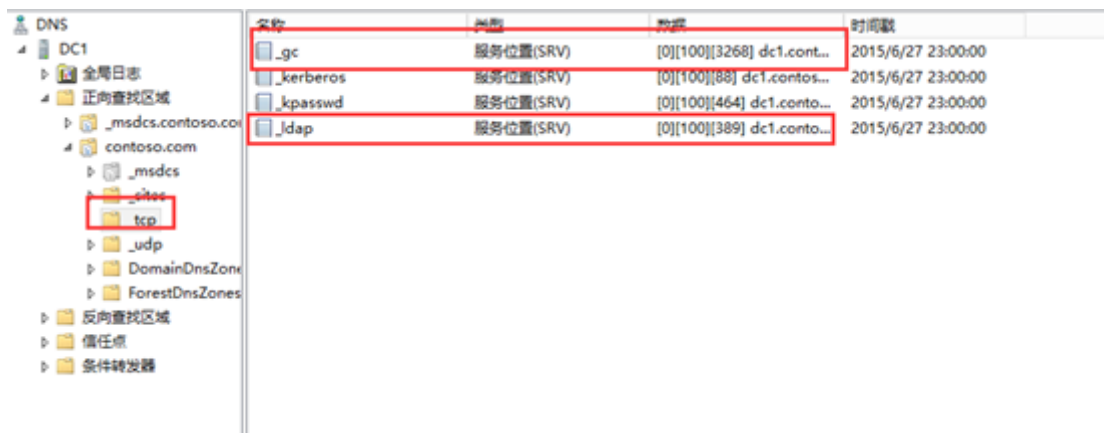
选择管理工具-dns

名称	修改日期	类型
Terminal Services	2013/8/22 23:39	文件夹
Active Directory 管理中心	2013/8/22 7:50	快捷方式
Active Directory 用户和计算机	2013/8/22 14:55	快捷方式
Active Directory 域和信任关系	2013/8/22 14:55	快捷方式
Active Directory 站点和服务	2013/8/22 14:55	快捷方式
ADSI 编辑器	2013/8/22 14:55	快捷方式
DNS	2013/8/22 14:55	快捷方式
iSCSI 发起程序	2013/8/22 14:57	快捷方式
Microsoft Azure 服务	2014/7/24 12:02	快捷方式
ODBC 数据源(32 位)	2013/8/22 7:56	快捷方式
ODBC 数据源(64 位)	2013/8/22 7:56	快捷方式
Windows PowerShell (x86)	2013/8/22 23:37	快捷方式
Windows PowerShell ISE (x86)	2013/8/22 14:55	快捷方式
Windows PowerShell ISE	2013/8/22 14:55	快捷方式
Windows Server Backup	2013/8/22 14:53	快捷方式
Windows 内存诊断	2013/8/22 14:52	快捷方式
安全配置向导	2013/8/22 14:45	快捷方式

默认会有一个contoso.com的区域，主机记录表示域控dc.contoso.com已经正确的将其主机名与IP地址注册到DNS服务器内。



如果域控制器已经正确的将家里注册到dns服务器，应该还会有_tcp _udp等文件夹。单击_tcp文件夹后可以看到数据类型为服务位置(SRV)的_lap记录，表示dc1.contoso.com已经正确的注册为域控制器。还能看到_gc记录全局编录也是由dc1.contoso.com所扮演。

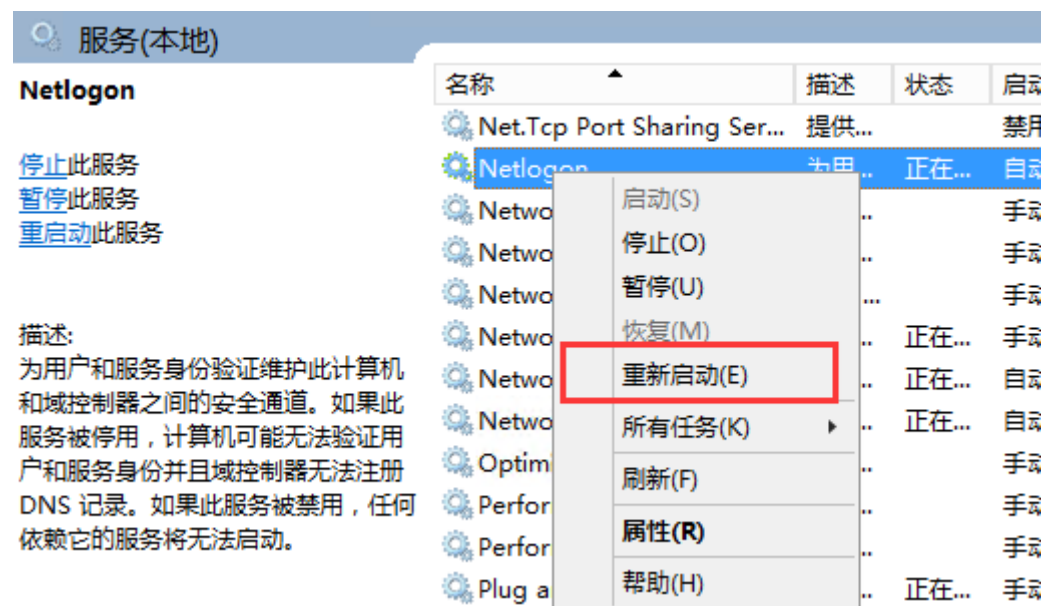


排除注册失败的问题

如果域成员本身的设置或者网络问题，会造成无法将数据注册到DNS服务器。

如果有成员计算机的主机与ip美元正确注册到DNS服务器，可以到此机器上运行ipconfig /registerdns来手动注册。完成后，到DNS服务器检查是否已有正确记录，例如server1.contoso.com，ip地址192.168.100.13则坚持区域contoso.com是否有对应的a记录和ip。

如果发现域控制器没有将其扮演的角色注册到dns服务器，也就是没有_tcp文件夹与记录，到服务器中重启netlogon服务



创建更多的域控制器

如果一个域内有多个域控制器，可以有如下好处.

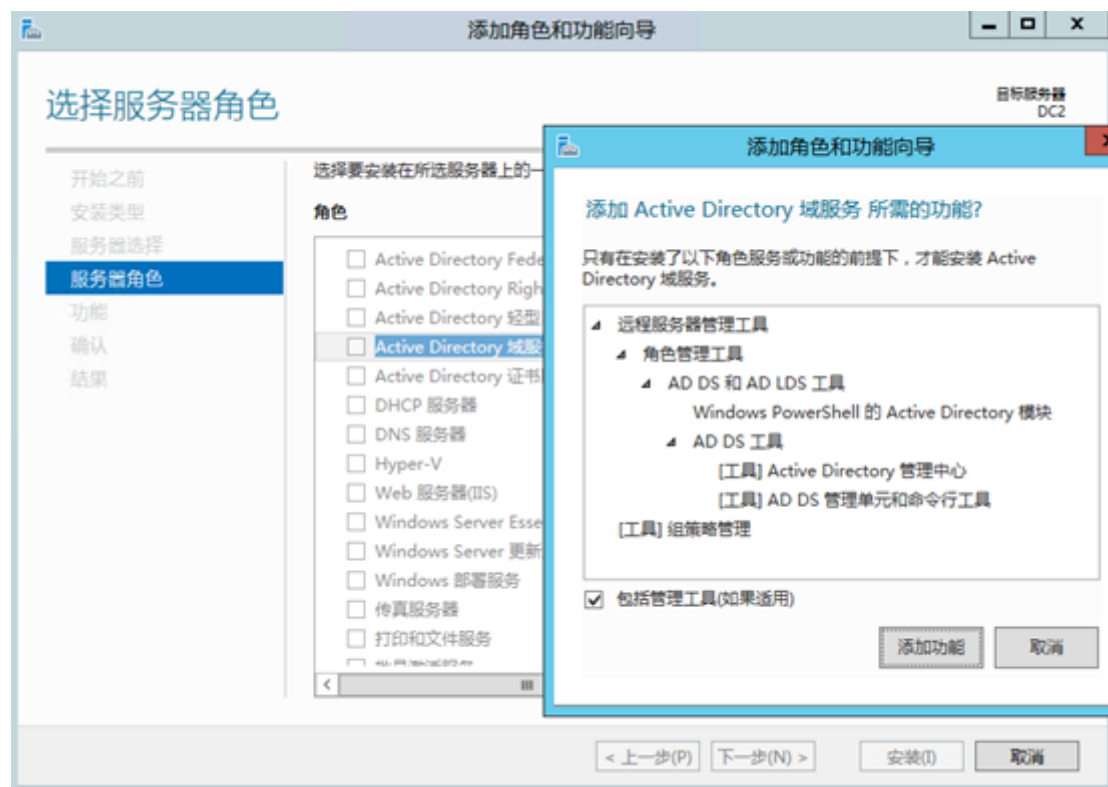
- 提高用户登录的效率：如果同时有多台域控制器对客户提供服务，可以分担审核用户登录身份（账户与密码）的负担，让用户登录效率更佳。
- 排错功能：如果有域控制器发生故障，此时依然能有其他正常的域控制器继续提供域服务器。

我们将dc2.contoso.com升级为域控制器

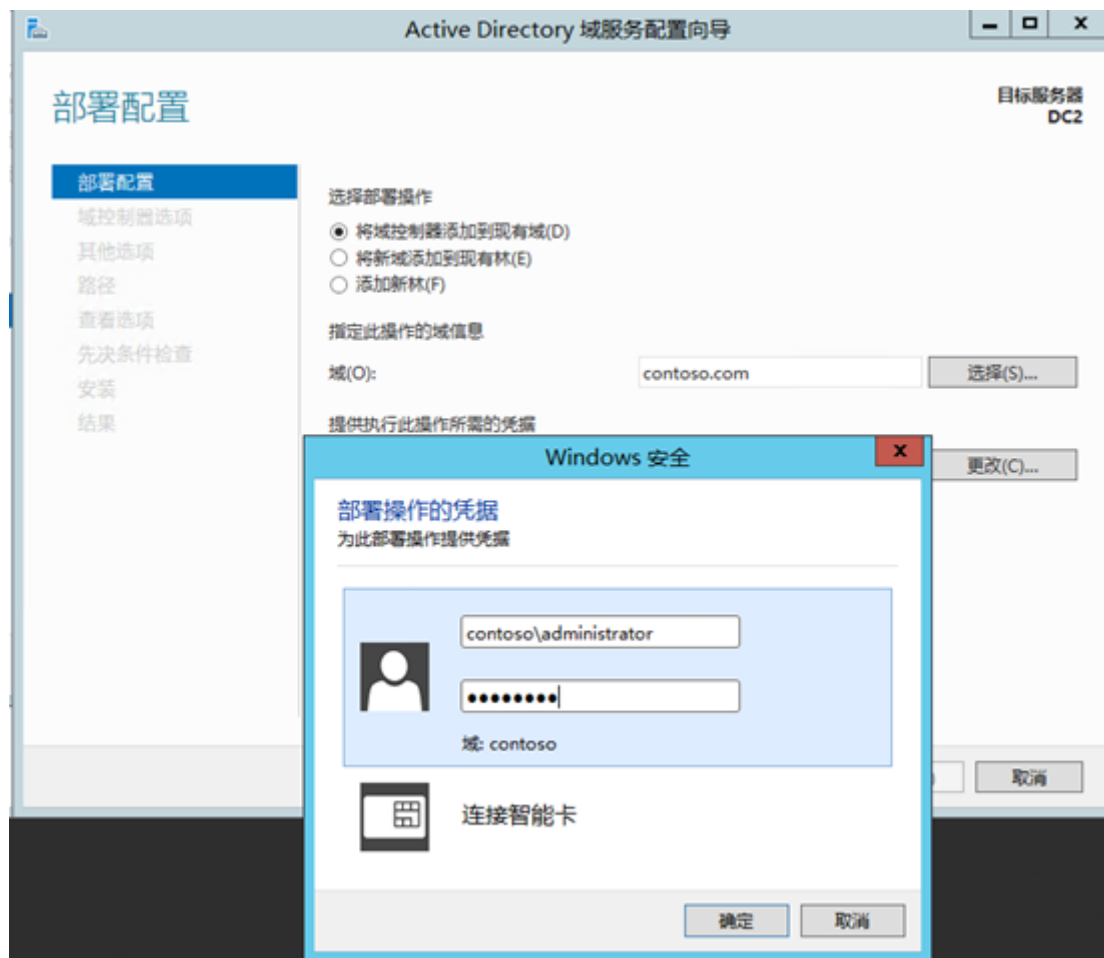
首先改名，改ip

计算机名	DC2
工作组	WORKGROUP
Windows 防火墙	专用: 启用
远程管理	已启用
远程桌面	已启用
NIC 组合	已禁用
Ethernet0	192.168.100.12 , IPv6 已启用
操作系统版本	Microsoft Windows Server 2012 R2 Datacenter
硬件信息	VMware, Inc. VMWare7,1

后面都和前面一样安装功能



这里不同，将域控添加到现有域，输入域名contoso.com，并且输入现有权限添加域控的账户contoso\administrator的密码。



只有Enterprise Admins和Domain Admins内的用户有权限创建其他域控制器。

Active Directory 域服务配置向导

域控制器选项

目标服务器
DC2

部署配置

域控制器选项

DNS 选项

其他选项

路径

查看选项

先决条件检查

安装

结果

指定域控制器功能和站点信息

☒ 域名系统(DNS)服务器(O)

☒ 全局编录(GC)(G)

☐ 只读域控制器(RODC)(R)

站点名称(S):

Default-First-Site-Name

键入目录服务还原模式(DSRM)密码

密码(P):

••••••••

确认密码(C):

••••••••

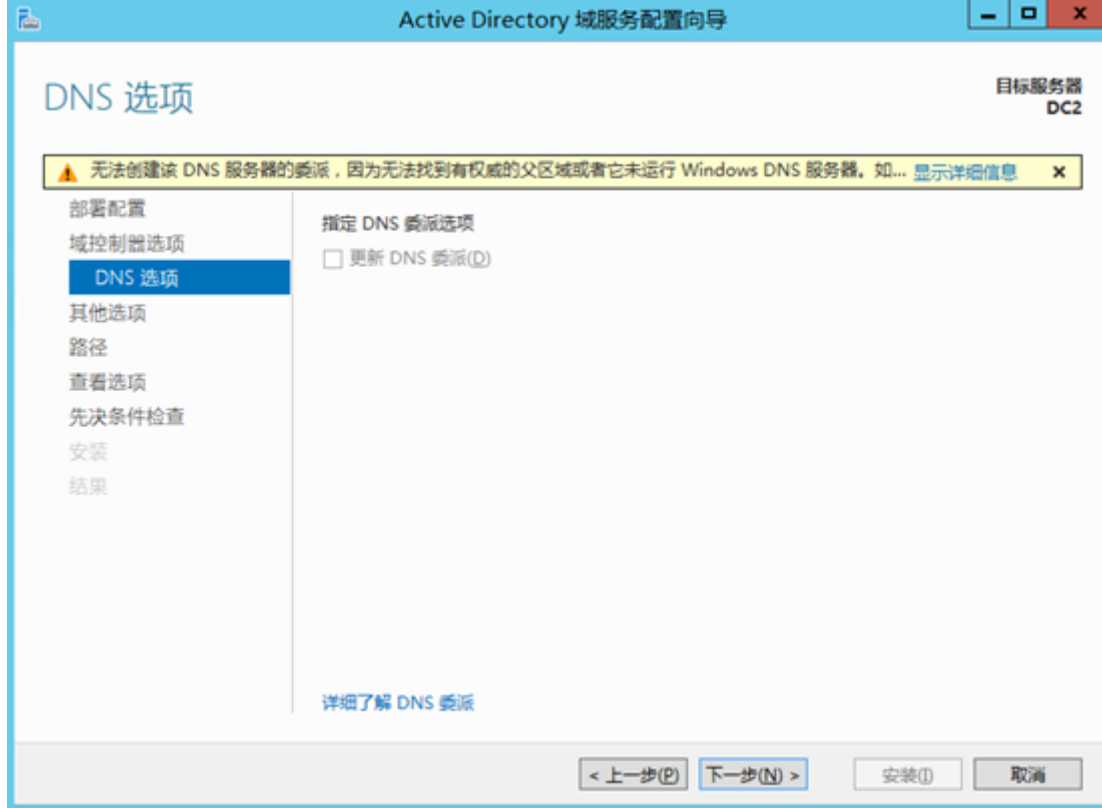
详细了解 域控制器选项

< 上一步(B)

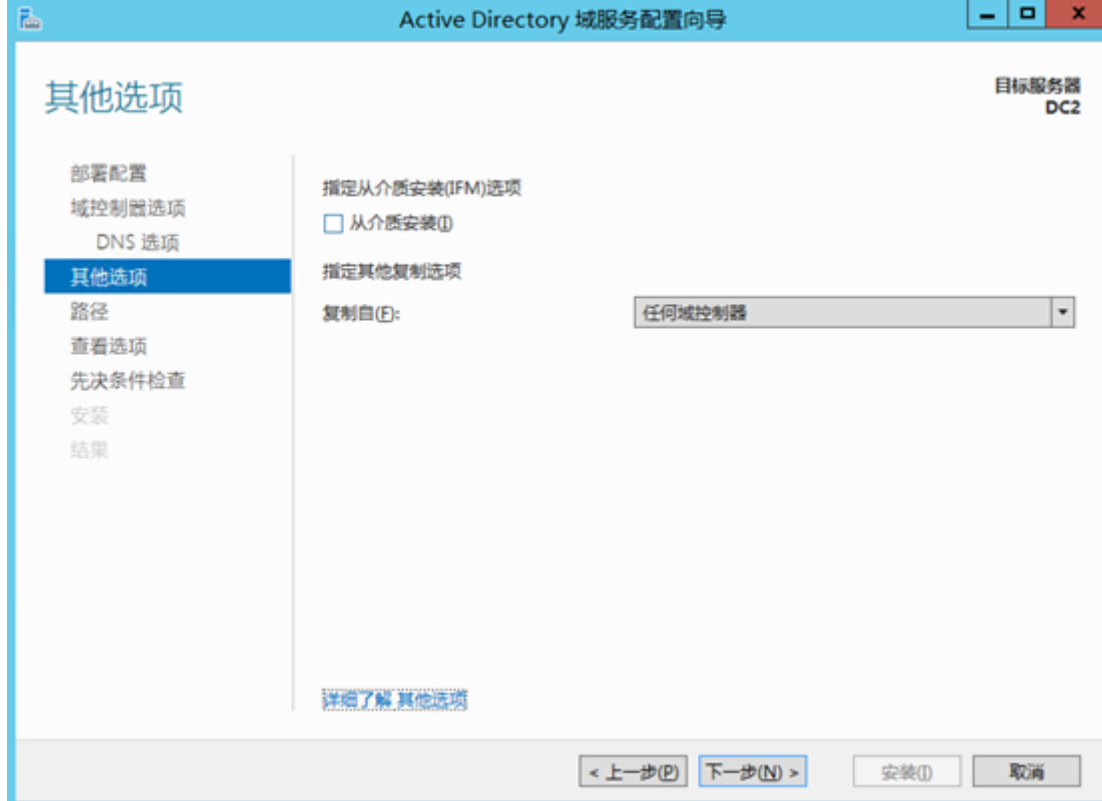
下一步(N) >

安装(I)

取消



选择从其他域控复制



安装完成后机器会重启，然后在检查DNS记录。

修改dns指向

修改dc1和dc2的dns互相将各自的首选dns指向对方域控

● 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P):	192 . 168 . 100 . 12
备用 DNS 服务器(A):	192 . 168 . 100 . 11

将windows计算机加入或脱离域

Windows加入域后，就可以访问ad数据库和其他域资源。可以被加域的计算机：

Windows server 2012(R2)

Windows server 2008(R2)

Windows server 2003(R2)

Windows 8

Windows 7

Windows vista

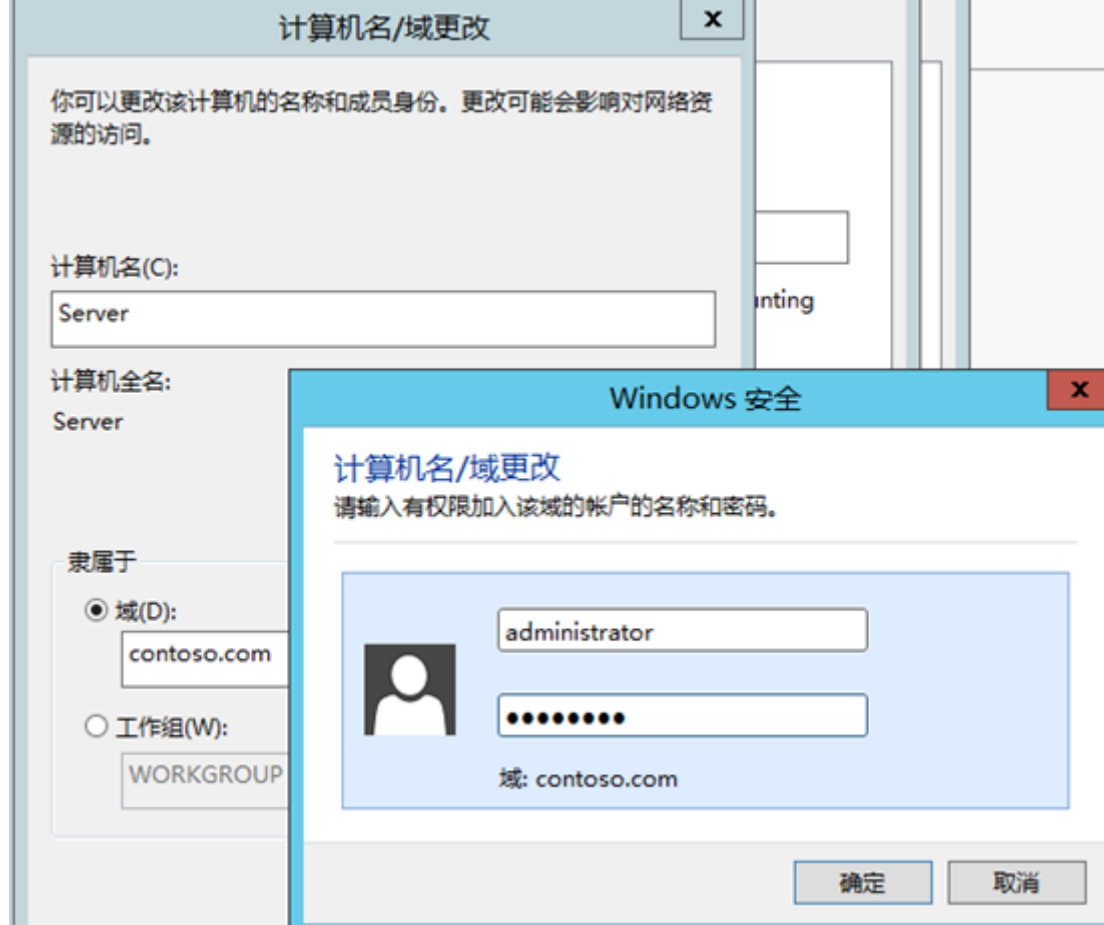
Windows xp

将windows计算机加入域

我们要将server.contoso.com机器加入域。

先将机器改名改ip。

输入域名和域账户密码

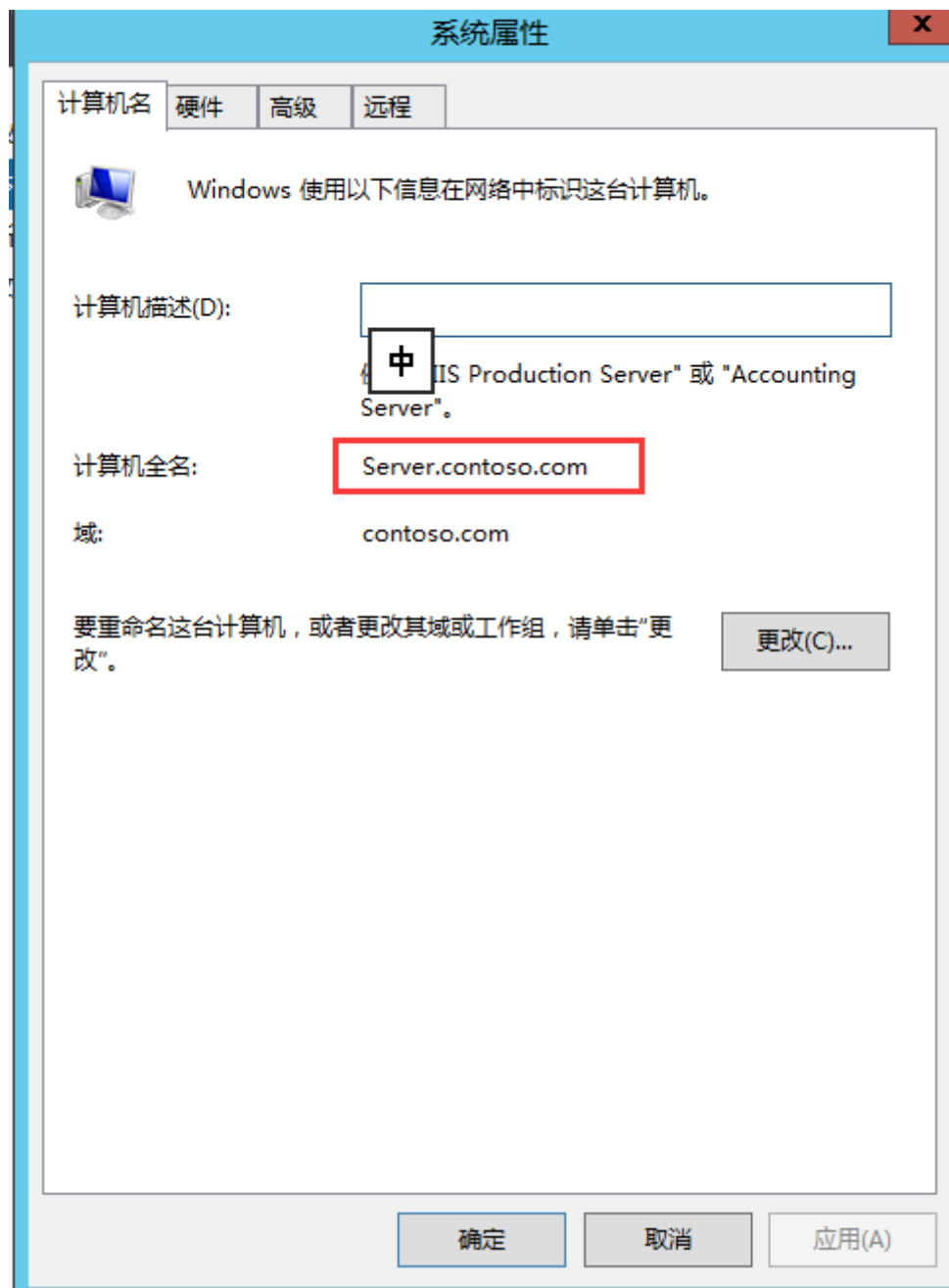


如果报错，请检查dns是否指向域控。

完成后我们可以使用域账户登录此台服务器



计算机名后已自动加上域名



脱离域

只要输入工作组并点击确定

计算机名/域更改

你可以更改该计算机的名称和成员身份。更改可能会影响对网络资源的访问。

计算机名(C):
Server

计算机全名:
Server.contoso.com

其他(M)...

隶属于

☐ 域(D):
contoso.com

☒ 工作组(W):
WORK

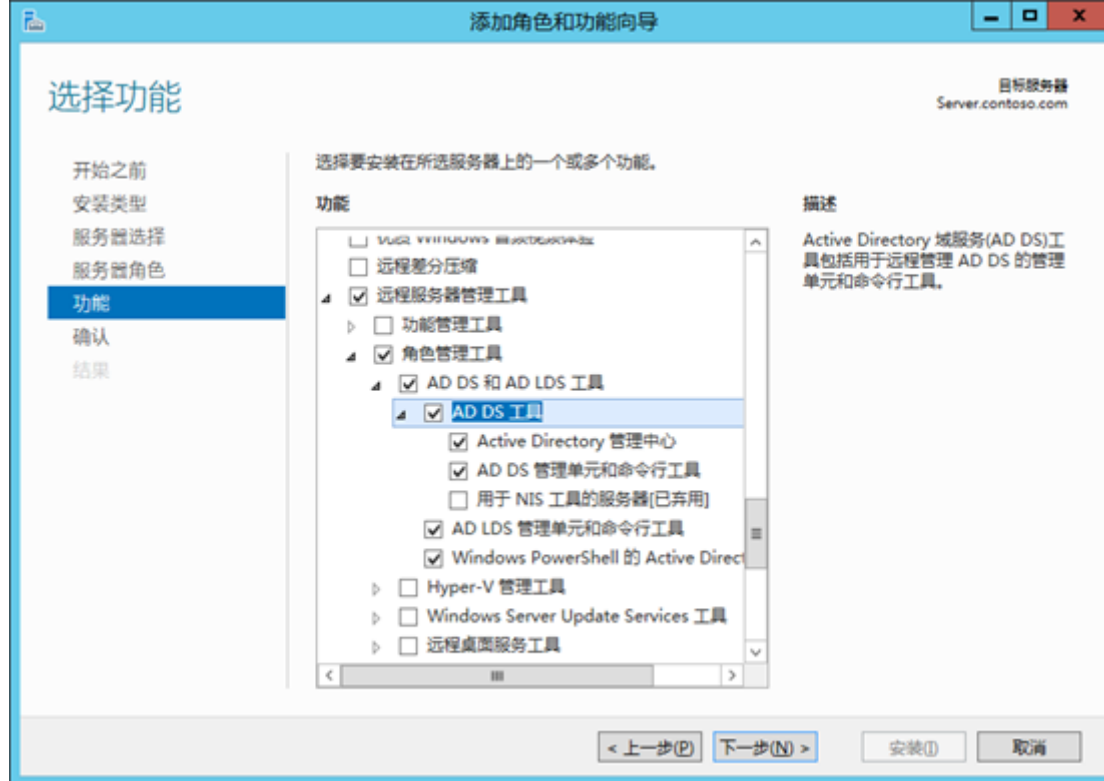
确定 取消

成员计算机内的ad管理工具

我们有时管理员管理不过来是可以将开账户的权限委派改其他各个部门的行政，委派给他们后，他们当然是不能登陆域控的，这时就要在他们的计算机上安装ad管理工具

Windows server 2012

添加功能中，添加远程服务器管理工具



Windows8 和Windows7

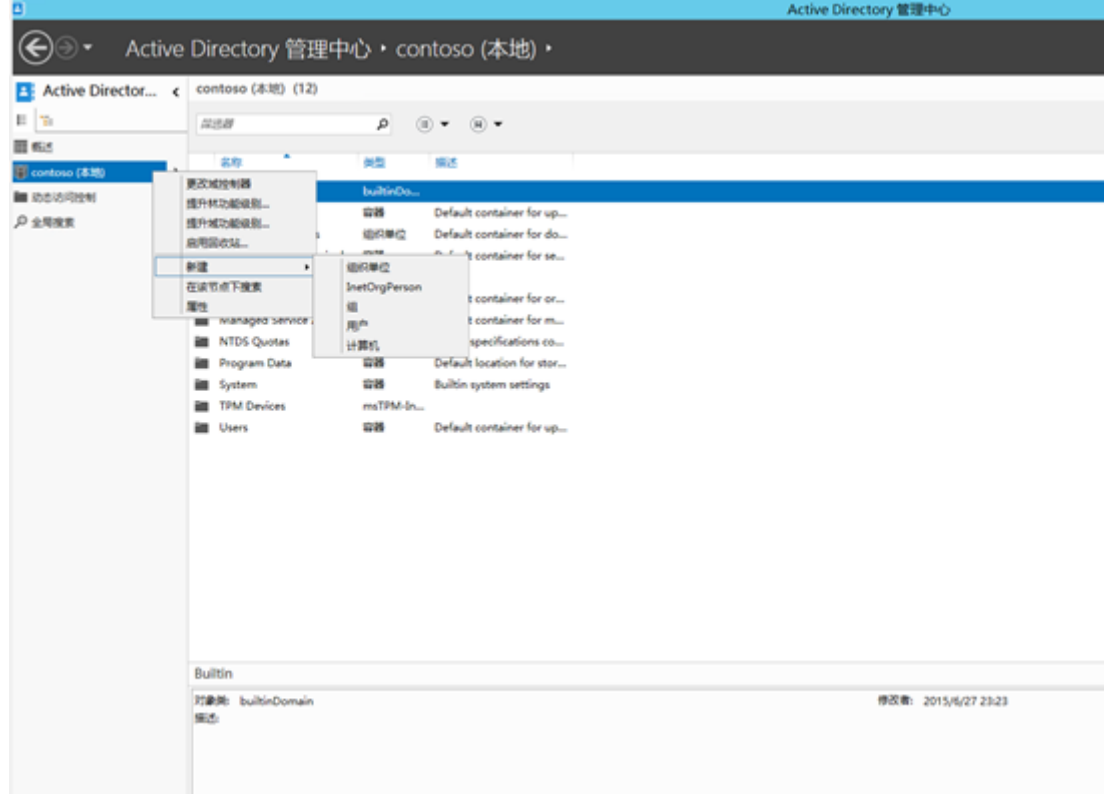
都去官网下载Remote Server Administration Tools for Windows8/7

创建组织单位与域用户账户

可以将用户账户创建到任何一个容器或组织单位（OU）内。先创建业务部的OU,然后再创建用户。

创建组织单位

点击 Active Directory管理中心



输入名称

创建 组织单位: 业务部

任务 节

组织单位(O) 组织单位

管理者(B)

名称: * 业务部

地址: 街道

城市 省/市/自... 邮政编码

国家/地区:

创建位置: DC=contoso,DC=com

描述: 更改...

☒ 防止意外删除

管理者

管理者: 编辑... 清除

电话号码: 主要电话号... 移动电话号... 传真:

办公室: 地址: 街道

城市 省/市/... 邮政编码

国家/地区:

详细信息

确定 取消

创建用户

业务部-新建用户

Active Director...

contoso (本地) (13)



概述

contoso (本地)

动态访问控制

全局搜索

筛选器

名称	类型	描述
Builtin	builtinDo...	
Computers	容器	Default container for up...
Domain Controllers	组织单位	Default container for do...
ForeignSecurityPrincipals	容器	Default container for se...
Infrastructure	infrastruct...	
LostAndFound	lostAndFo...	Default container for or...
Managed Service Accou...	容器	Default container for m...
NTDS Quotas	msDS-Qu...	Quota specifications co...
Program Data	容器	Default location for stor...
System	容器	Builtin system settings
TPM Devices	msTPM-In...	
Users	容器	Default container for up...

业务单元

新建

删除

移动...

在该节点下搜索

属性

组织单位

InetOrgPerson

组

用户

计算机

- **用户UPN登录**：用户可以利用这个域电子邮箱格式相同的名称（wang@contoso.com）来登录域，此名称被称为User Principal Name（UPN）。此名在林中是唯一的。
- **用户名SamAccountName登录**：用户也可以利用此名称（contosolwang）来登录。其中wang是NetBios名。同一个域中此名称必须是唯一的。Windows NT Windows 98等旧版系统不支持UPN，因此在这些计算机上登录时，只能使用此登录名。

使用新账户登录域

我们使用2种方法来登录域



其他用户

contoso\wang



登录到: contoso

[如何登录到其他域?](#)



 Windows Server 2012 R2



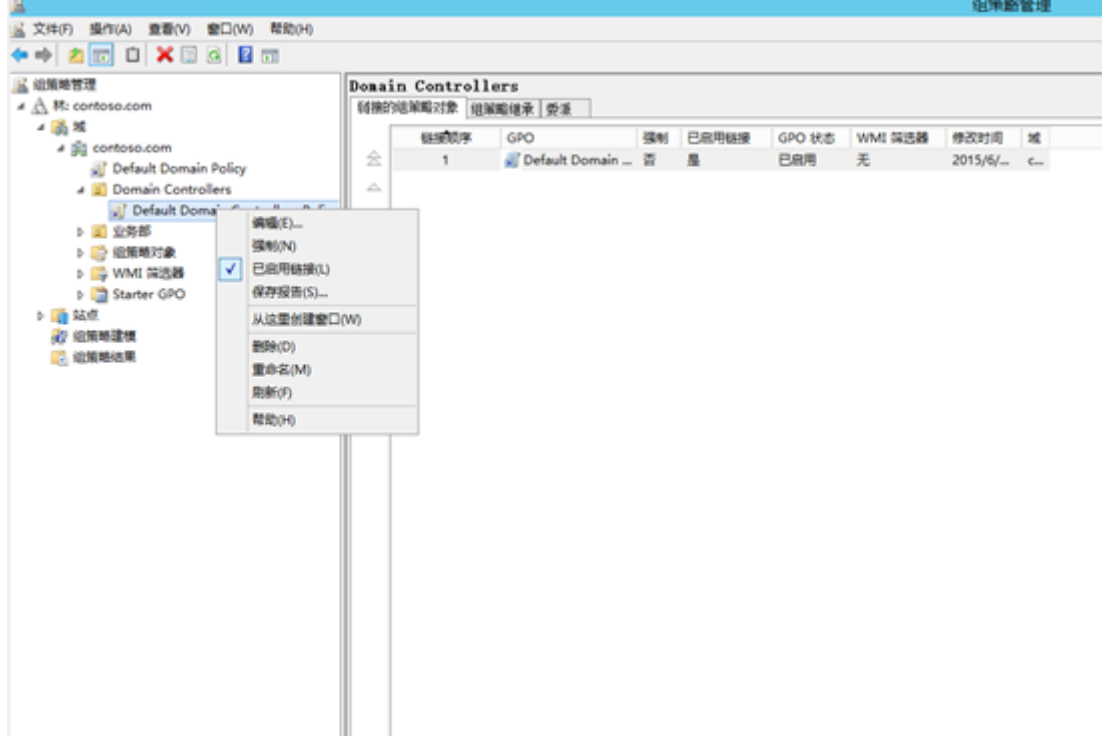
利用新用户账户登录域控

除了域Administrators等少数组内的成员外，其他一般域账户默认无法登陆到域控上，除非另外开放。

赋予用户在域控登录权限

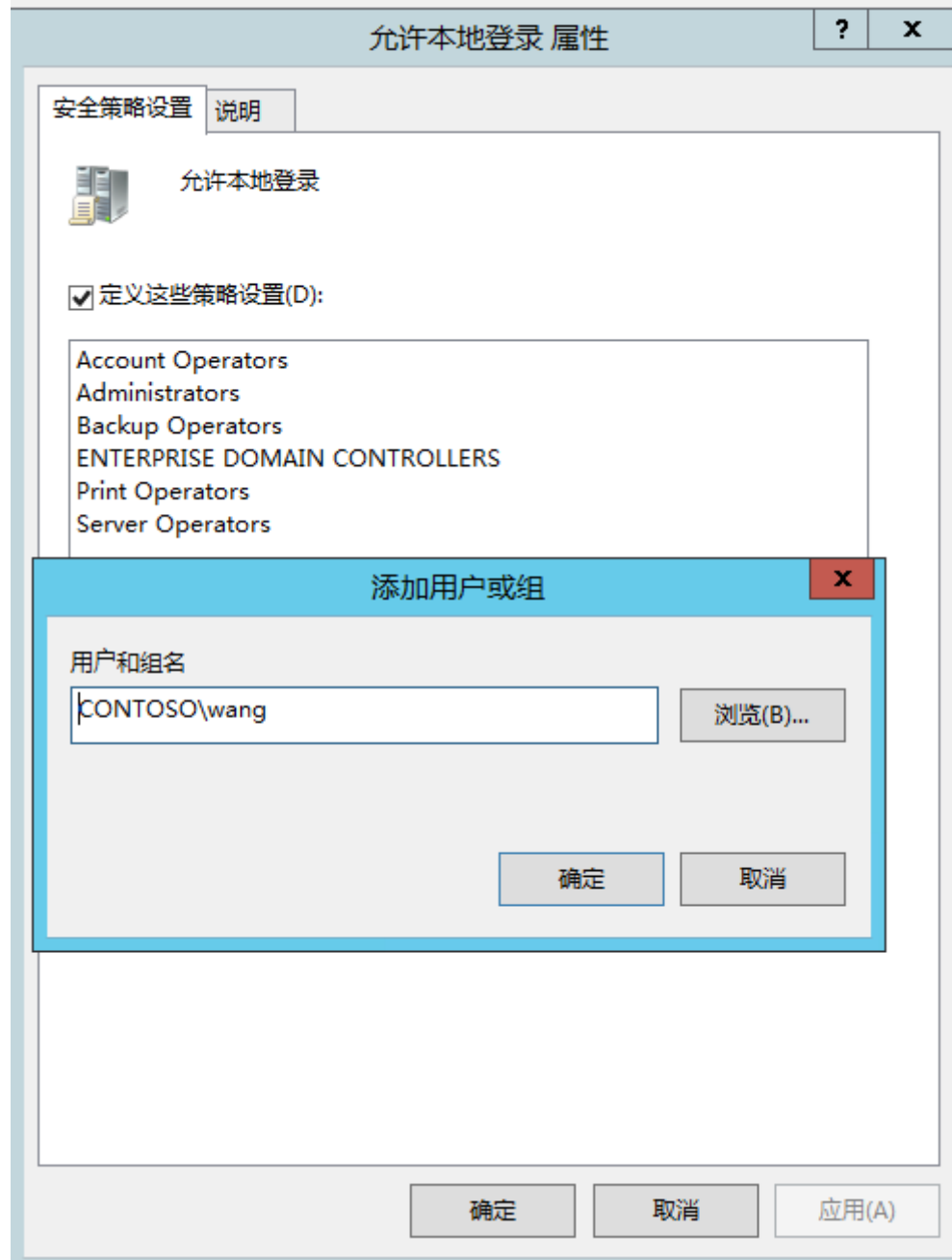
一般用户必须在域控上拥有**允许本地登录**的权限，才能在域控上登录。此权限可以用过组策略来开放。

系统管理工具-组策略管理



计算机配置-策略-windows设置-安全设置-本地策略-用户权限分配-允许本地登录，然后将用户或组加入到列表内

fault Domain Controllers Policy ^	策略	策略设置
计算机配置		
策略		
软件设置		
Windows 设置		
域名解析策略		
脚本(启动/关机)		
安全设置		
帐户策略		
本地策略		
审核策略		
用户权限分配		
安全选项		
事件日志		
受限制的组		
系统服务		
注册表		
文件系统		
有线网络(IEEE 802.3)		
高级安全 Windows 防火墙		
网络列表管理器策略		
无线网络(IEEE 802.11)		
公钥策略		
软件限制策略		
网络访问保护		
应用程序控制策略		
IP 安全策略, 在本地计算机上		
高级审核策略配置		
基于策略的 QoS		
管理模板: 从本地计算机中		
首选项		
用户配置		
策略		
	还原文件和目录	Administrators,Backup Oper...
	加载和卸载设备驱动程序	Administrators,Print Operators
	将工作站添加到域	Authenticated Users
	拒绝本地登录	没有定义
	拒绝从网络访问这台计算机	没有定义
	拒绝通过远程桌面服务登录	没有定义
	拒绝以服务身份登录	没有定义
	拒绝作为批处理作业登录	没有定义
	配置文件单一进程	Administrators
	配置文件系统性能	Administrators,NT SERVICE\...
	取得文件或其他对象的所有权	Administrators
	绕过遍历检查	Everyone,LOCAL SERVICE,NE...
	身份验证后模拟客户端	没有定义
	生成安全审核	LOCAL SERVICE,NETWORK S...
	锁定内存页	没有定义
	提高计划优先级	Administrators
	替换一个进程级令牌	LOCAL SERVICE,NETWORK S...
	调试程序	Administrators
	同步目录服务数据	没有定义
	为进程调整内存配额	LOCAL SERVICE,NETWORK S...
	信任计算机和用户帐户可以执行委派	Administrators
	修改固件环境值	Administrators
	修改一个对象标签	没有定义
	以操作系统方式执行	没有定义
	允许本地登录	Administrators,Backup Oper...
	允许通过远程桌面服务登录	没有定义
	增加进程工作集	没有定义
	执行卷维护任务	没有定义
	作为服务登录	没有定义
	作为批处理作业登录	Administrators,Backup Oper...
	作为受信任的呼叫方访问凭据管理器	没有定义



组策略配置完成需要应用到域控才有效，应用方法有三种：

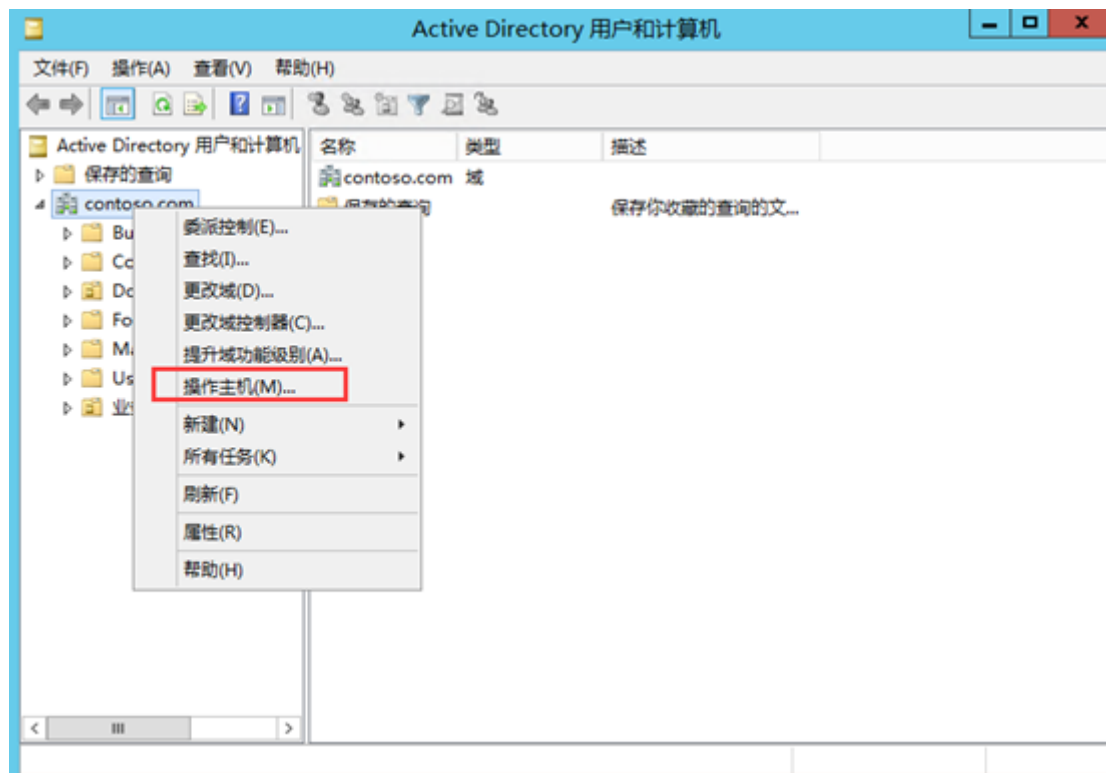
- 将域控制器重启
- 等域控制器自动应用此策略，可能需要等待5分钟或更久

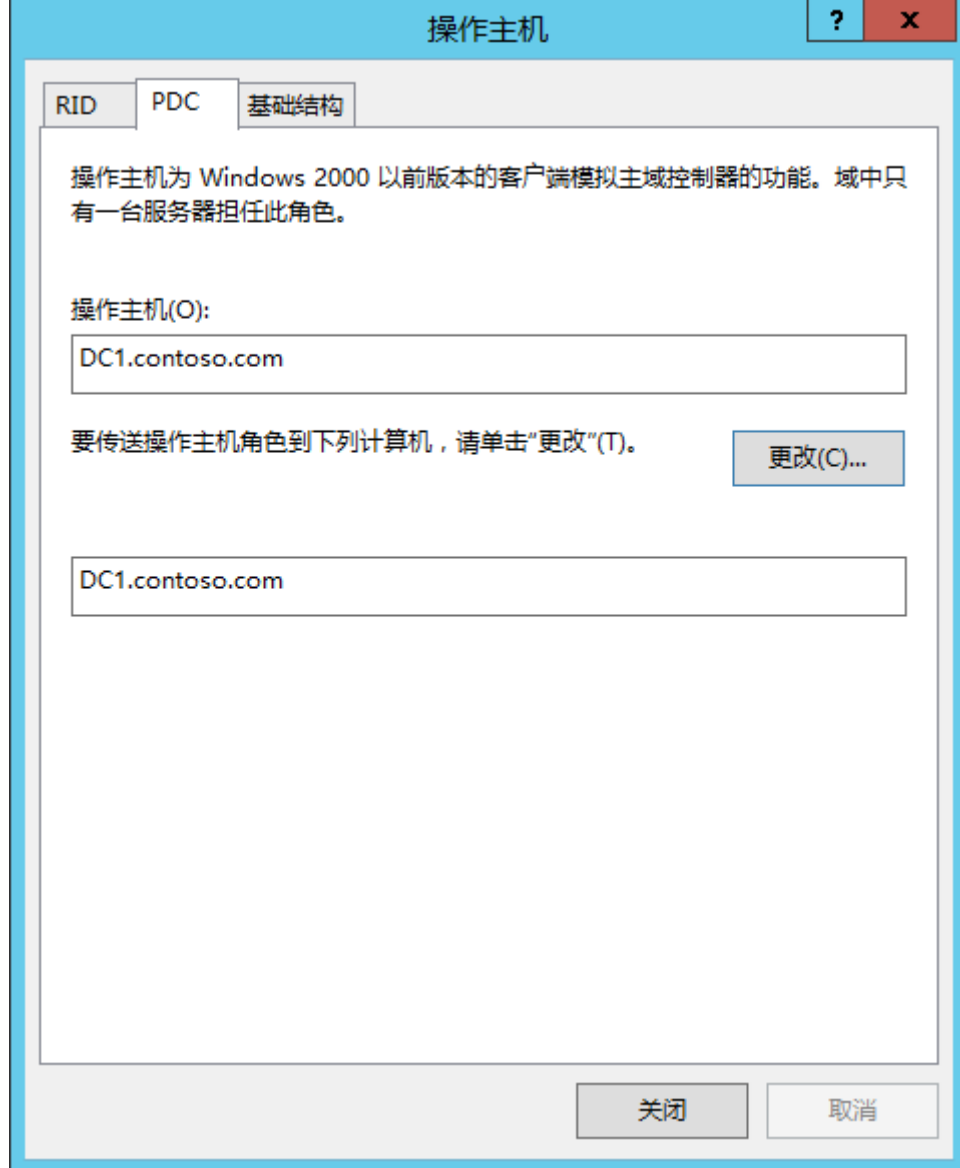
- 手动应用：到域控制器上运行gpupdate或gpupdate\force

多台域控制器的情况

如果域内有多台域控制器，则设置的安全设置值，先被存储到**PDC操作主机**角色的域控制器内，默认由第一台域控制器扮演。

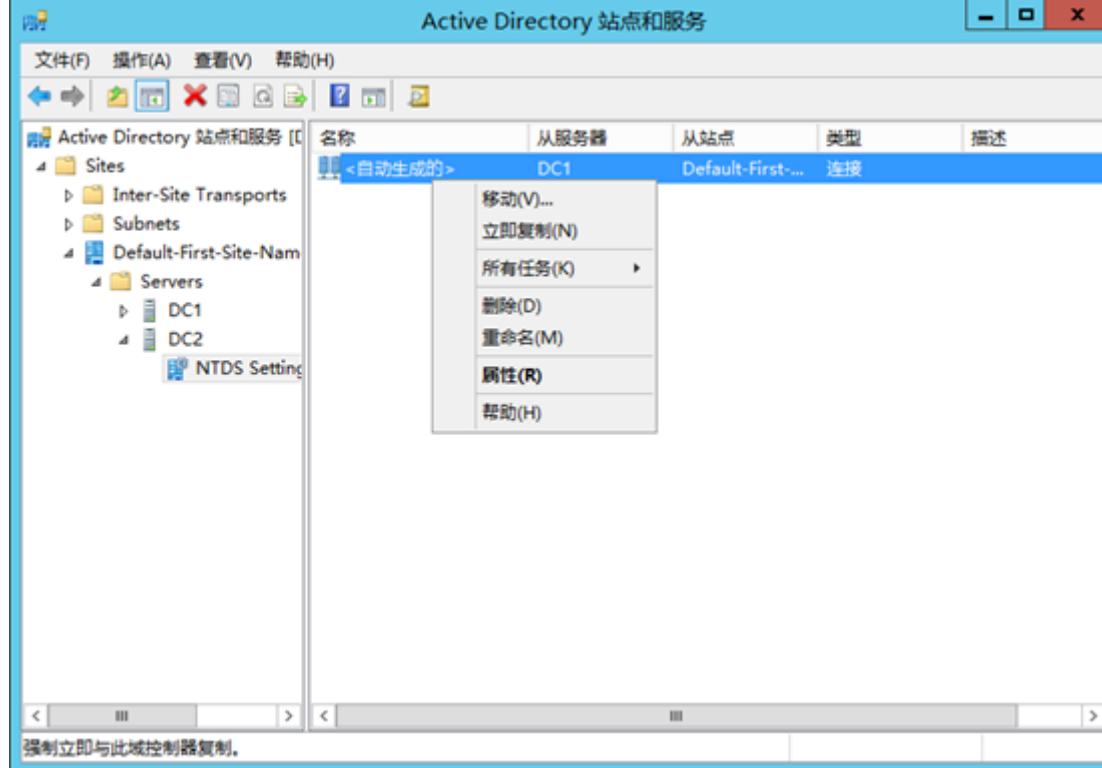
Active Directory用户和计算机-选择contoso.com右键操作主机





需要等待设置值从PDC操作主机复制到其他域控制器后，他们才会应用这些设置值。什么时候应用分两种情况：

- **自动复制**：PDC操作主机默认15秒后会自动将其复制出去，因此其他域控制器可能需要等15秒或更久才能接受到此设置值。
- **手动复制**：到任何一台域控制器上选择Active Directory站点和服务-Sites-Default-First-Name Servers单击要接收设置的域控制器-NTDS Settings-立即复制。如下图DC1是操作主机，DC2是需要接收的域控



如果是组策略设置，则他先辈存储在PDC操作主机内，但如果Active Directory用户账户或其他对象有改动，则这些改动会先被存储在所连接的域控制器，同时系统默认会在15秒后自动将此改动数据复制到其他域控制器。

如果要查询目前连接的域控制器，可以如下图在**Active Directory管理中心**控制台中将鼠标指针对着图中的contoso，他就会显示所连接的域控制器。如果要更改连接其他控制器，单击**更改域控制器**。



Active Director... <



contoso (本地)

业务

动态访问控制

全局搜索

DN: DC=contoso,DC=com
已连接的 DC: DC1.contoso.com
登录身份: CONTOSO\administrator

欢迎使用 Active Directory 管理中心



了解有关 Active Directory 管理中心的更多

使用 Active Directory 管理中心管理 IT 任务

使用 Windows PowerShell 的 Active Directory 模块

在 Active Directory 论坛上查找答案

部署动态访问控制

获取 Microsoft 解决方案加速器以帮助配置动态访问控

部署身份验证策略和接收器

重置密码

用户名:

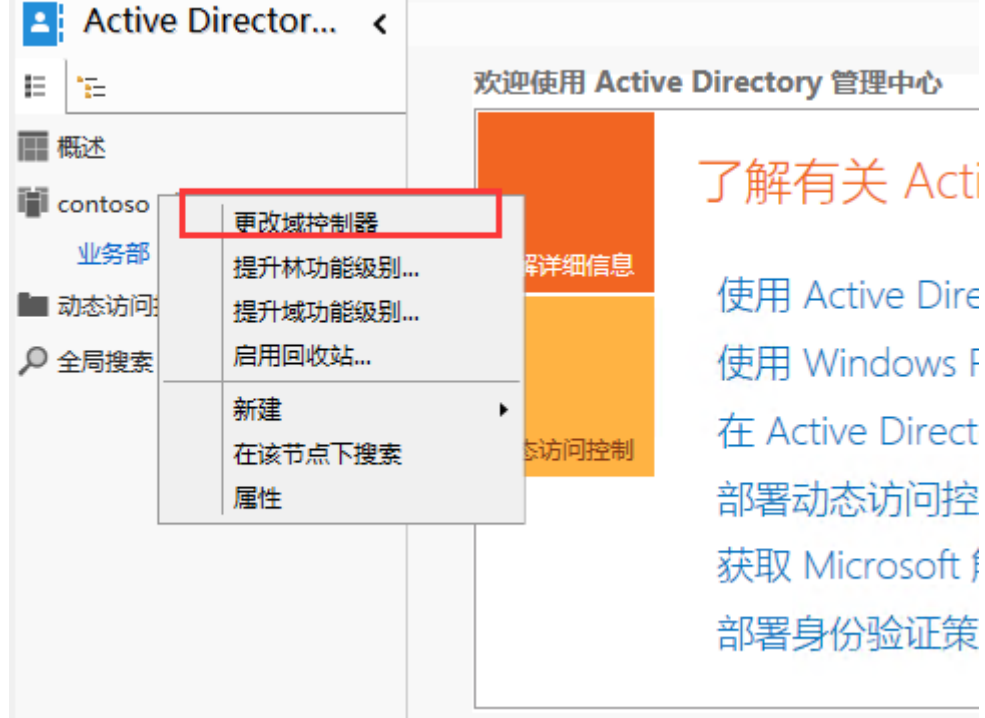
域\用户名

密码:

确认密码:

☒ 用户下次登录时须更改密码

☐ 解锁帐户



域用户个人数据的设置

每个域用户账户内部都有一些相关的属性数据，例如地址 电话等，域用户可以通过这些属性来查找Active Directory内的用户，因此这些数据越完整越好。

王哥哥

任务节

帐户(A)

组织(O)

成员(F)

密码设置(S)

配置文件(P)

扩展(E)

组织

显示名称:

办公室:

电子邮件:

网页:

其他网页...

电话号码:

主要电话号码:

主页:

移动电话号码:

传真:

寻呼机:

IP 电话:

其他电话号码...

描述:

职务:

部门:

公司:

管理者:

直接报告:

地址:

街道:

城市:

省/市/自治区:

邮政编码:

国家/地区:

编辑...

清除

添加...

删除

成员

筛选器

添加

详细信息

确定取消

限制登录时间与登录计算机

我们可以限制用户的登录时间已经能用使用某些计算机来登录域。

王哥哥

任务 节

帐户(A)

组织(O)

成员(F)

密码设置(S)

配置文件(P)

扩展(E)

帐户

名字:

中间名首字母缩写:

姓氏:

全名: * 王哥哥

用户 UPN 登录: wang @ contoso.co

用户 SamAccountName: contoso \ * wang

☒ 防止意外删除

帐户过期: ☒ 从不 ☐ 结束日期

密码选项: ☐ 用户下次登录时须更改密码 ☒ 其他密码选项

☐ 交互式登录时需要智能卡

☒ 密码永不过期

☐ 用户不能更改密码

加密选项:

其他选项:

登录小时... 登录到...

组织

显示名称:

办公室:

电子邮件:

网页:

其他网页: [其他网页...](#)

电话号码:

主联系号码:

职务:

部门:

公司:

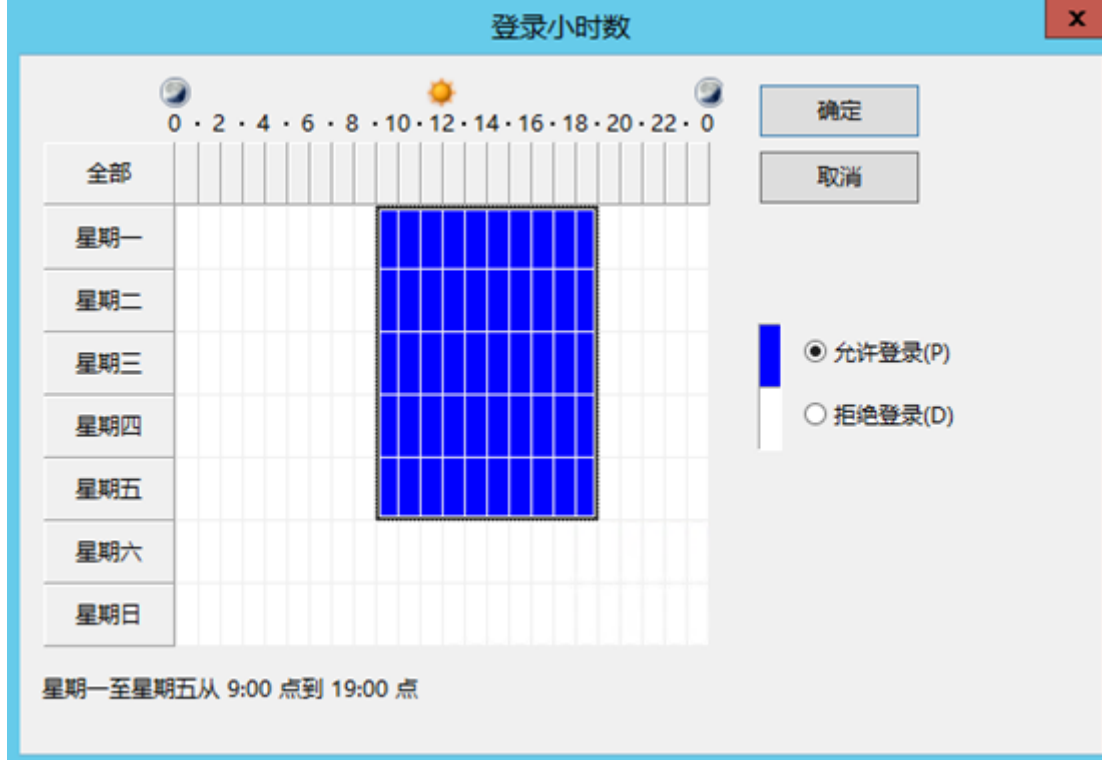
管理者: 编辑... 清除...

直接报告: 添加...

详细信息

确定 取消

如下图只能允许用户在正常上班时间内登录电脑

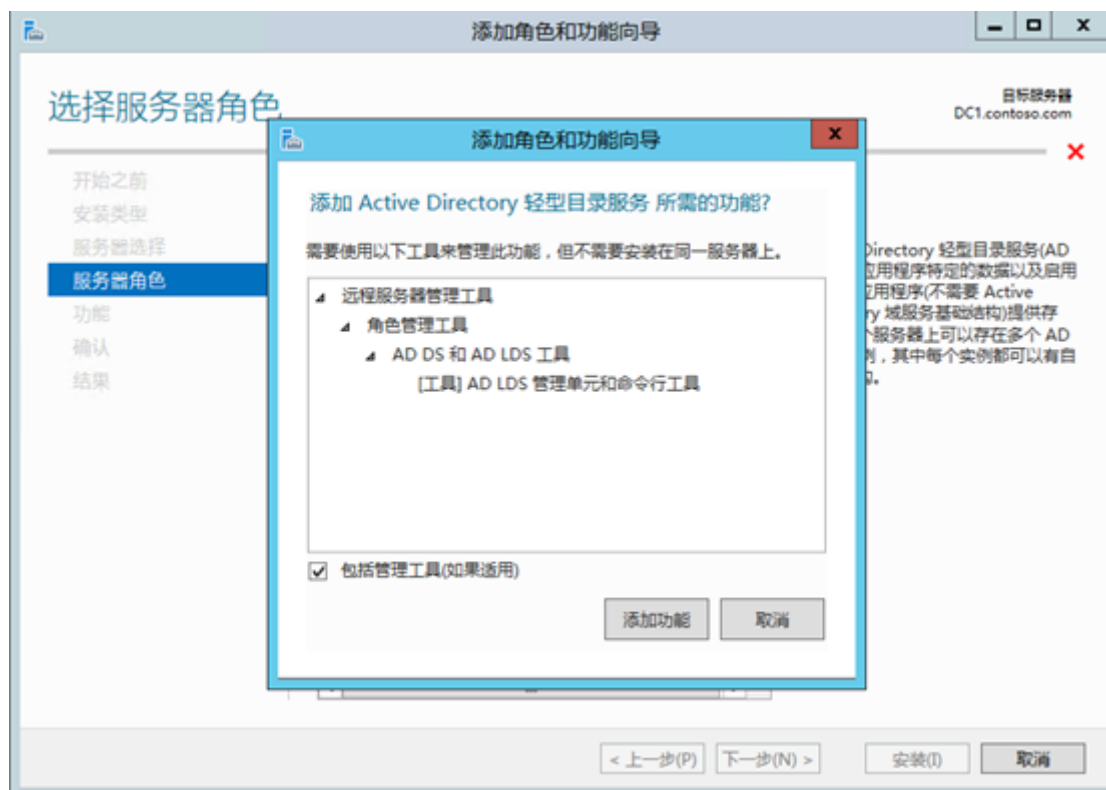


默认用户可以登录所有非域控制器的成员计算机，不过可以限制他们只能利用某些特定计算机来登录域。如下图限制只能登录server计算机。



Active Directory轻型目录服务

为了让支持目录访问的应用程序，可以在没有域的环境内享有目录服务的好处，Windows Server 2012内提供了Active Directory轻型目录服务 AD LDS,它可以让你在计算机内创建多个目录服务器的环境，每个环节被称为一个AD LDS实例，每个实例拥有独立的目录设置，架构，数据库。



Active Directory回收站

在旧版的操作系统中，如果系统管理员误将ad对象删除，就需要进入目录服务还原模式。还原麻烦，并且在还原好重启时，域无法提供服务。

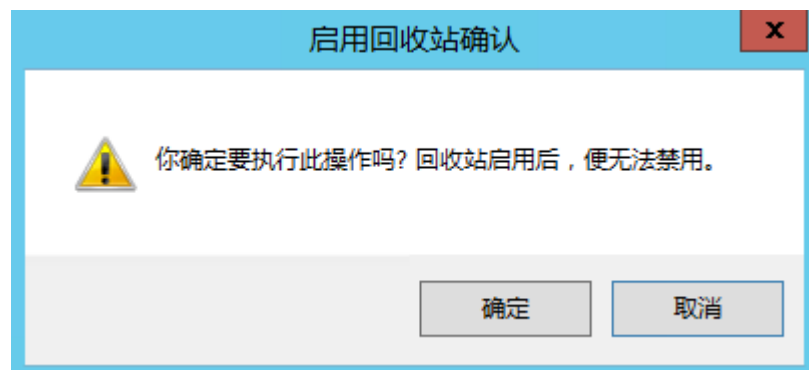
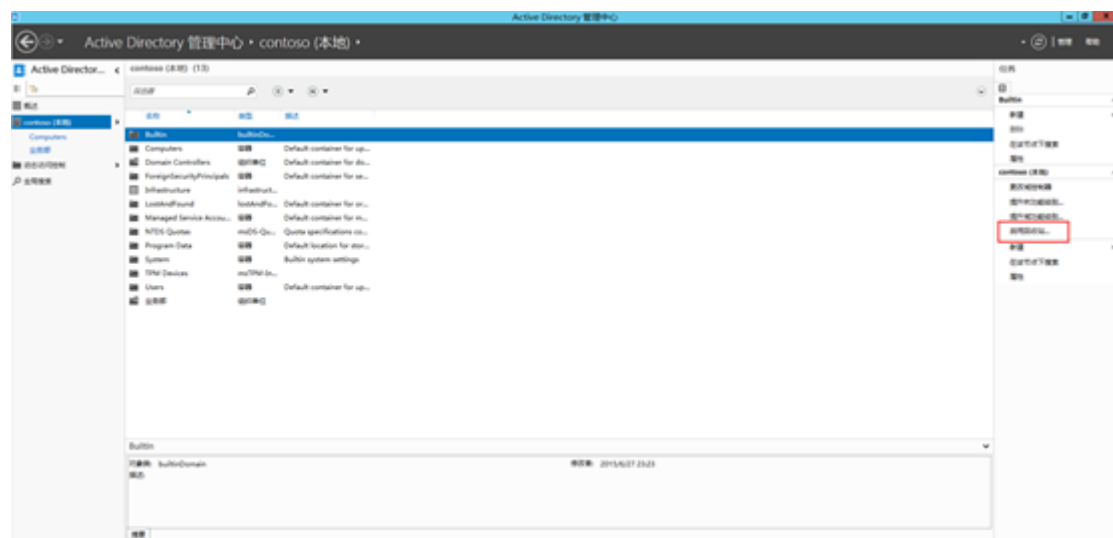
虽然windows server 2008 R2新增了ad回收站，让系统管理员不需要进入目录服务还原模式，就可以救回被删除的对象，但是却不是很好用，例如需要通过复杂的命令与步骤。

Windows server 2012 的ad回收站又有了进一步的改良，他提供容易使用的图像界面管理工具。

要启用ad回收站，林与域功能级别必须是Windows Server 2008 R2（含）以上的级别。**注意，一旦启用回收站，就无法在禁用，因此域与林功能基本也无法在被降级。**

启用Active Directory回收站

打开Active Directory管理中心，单击左侧的域名contoso，单击右侧的**启用回收站**

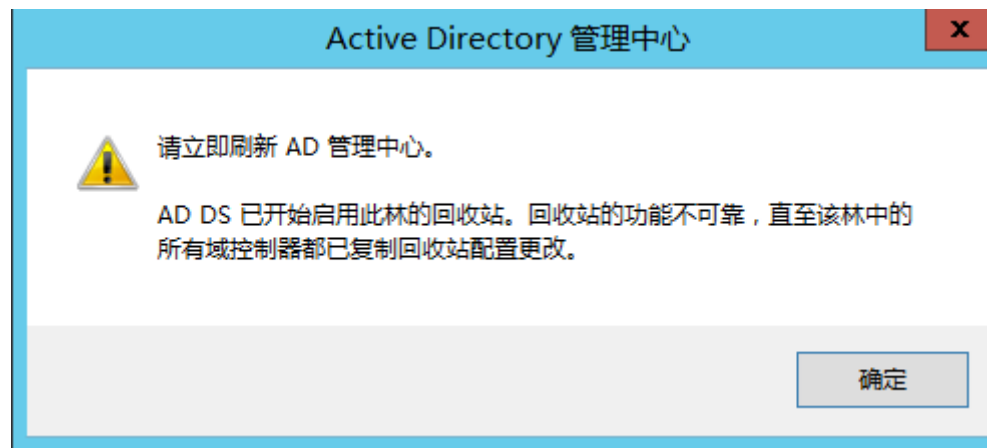


报错了



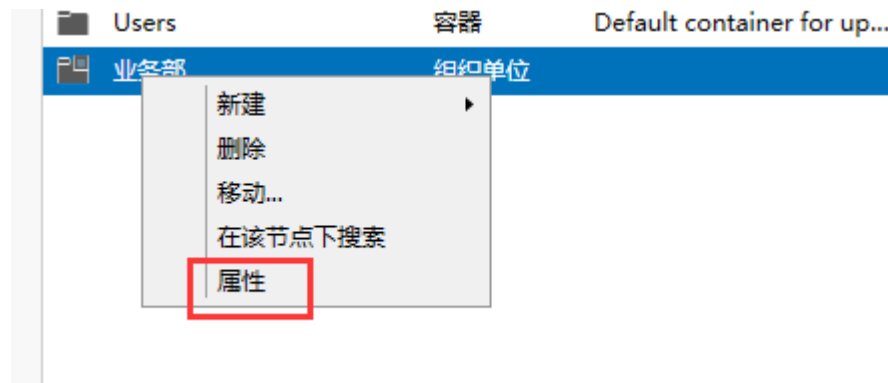
因为域内有多个域控制器，需要等设置值被复制到所有的域控制器后，ad回收站功能才会完全正常。（我做实验，节约性能还有一台辅助域控没有打开）

开启辅助域控并复制设置值后再次开启回收站。



删除组织单位

试着将业务部删除，但是先将防止删除的选项删除



取消勾选防止意外删除。

业务部

任务 节

组织单位(O) 组织单位

管理者(M) 扩展(E)

名称: * 业务部 描述:

地址: 街道

☐ 防止意外删除

城市 省/市/自治区 邮政编码

国家/地区:

管理者

管理者: 编辑... 清除 办公室:

电话号码: 地址: 街道

主要电话号码: 城市 省/市/自治区 邮政编码

移动电话号码: 国家/地区:

传真:

扩展

COM+ 安全 属性编辑器

此组织单位是以下 COM+ 分区集的成员:

详细信息 确定 取消

接着删除业务部

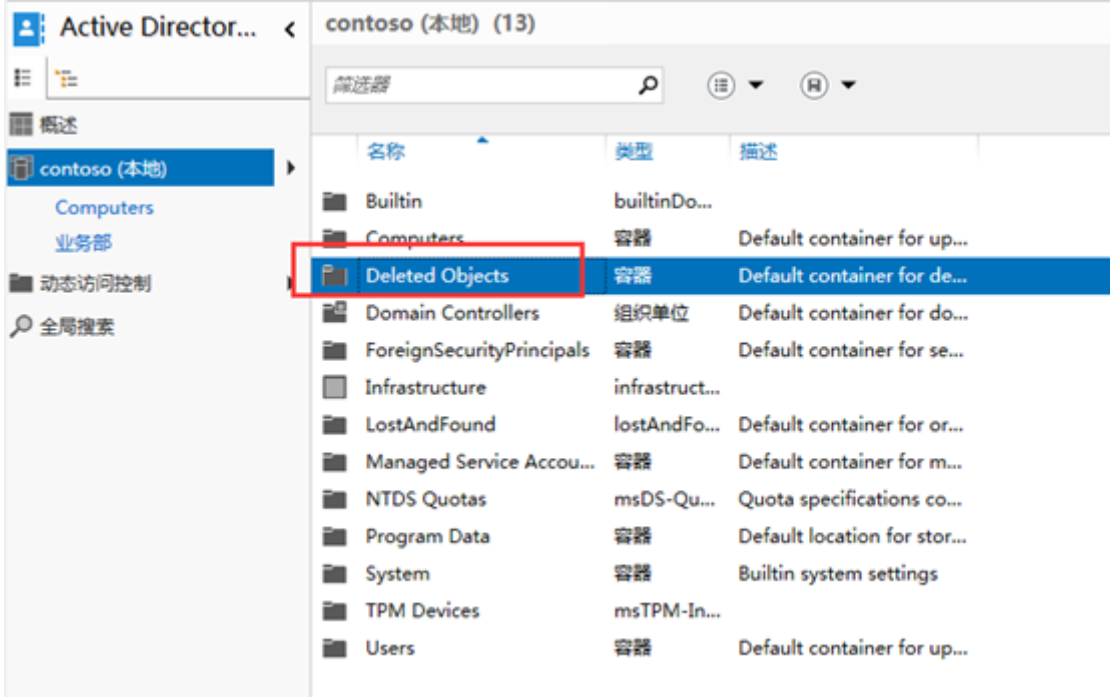
删除确认

你确实要删除 组织单位 业务部 吗?

是(Y) 否(N)

还原组织单位

接下来，要通过回收站来救回组织单位，双击deleted objects。



选择要救回的组织单位，单击还原



删除域控制器与域

可以通过降级的方式来删除域控制器，也就是将Active Directory从域控制器删除。在降级前先注意以下事项：

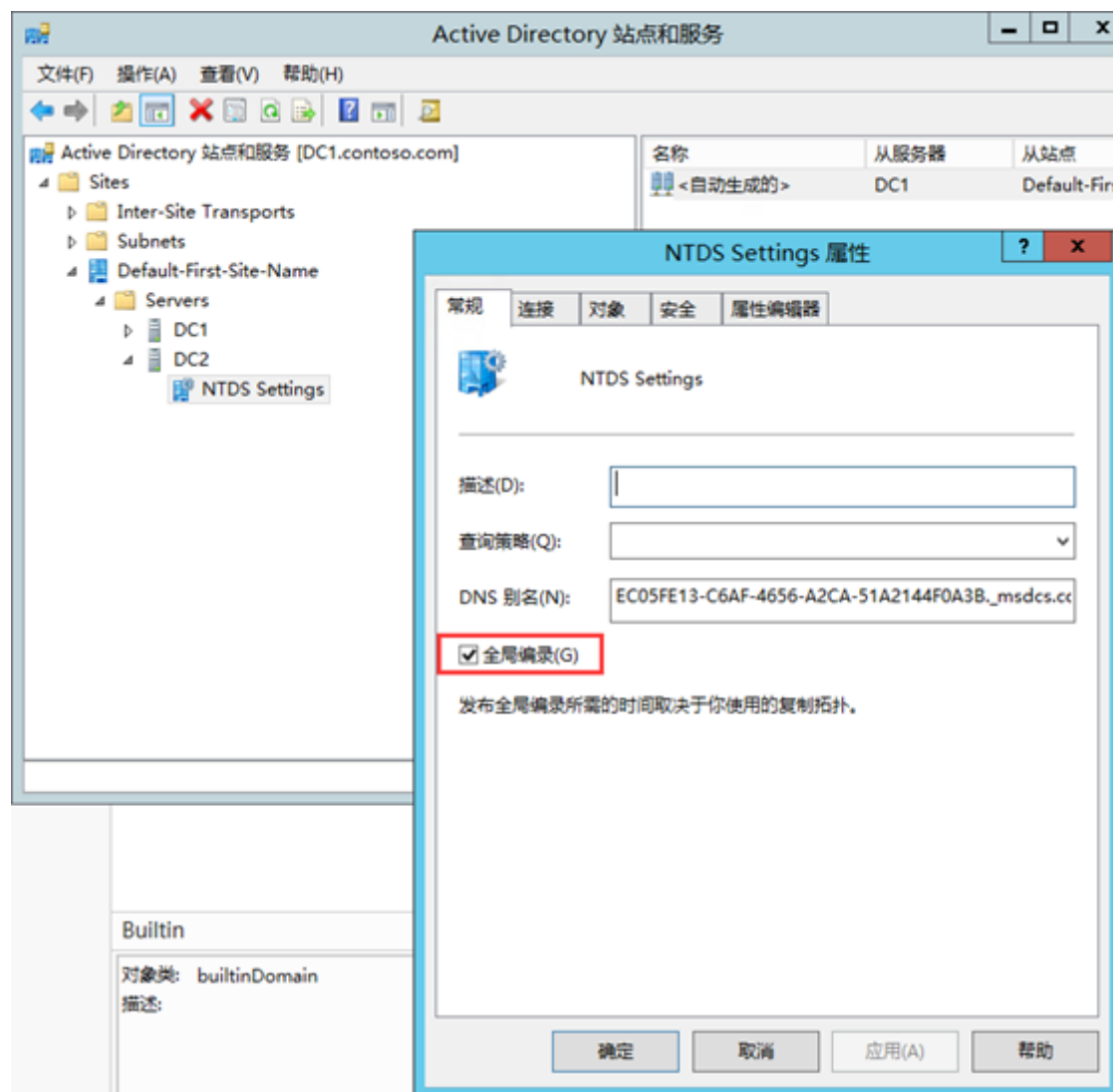
如果域内还有其他域控制器存在，则它会被降级为该域的成员服务器。

如果这台域控制器是此域内的最后一台域控制器，域内也没有其他的域控制器存在了，因此域将被删除，而域控制器也将会被降级为独立的服务器。

注：建议先将成员服务器server.contoso.com脱离域，因为在域删除后，这台服务器的账户就无法登陆域了（域删除后，也可以再将成员服务器脱离域）。

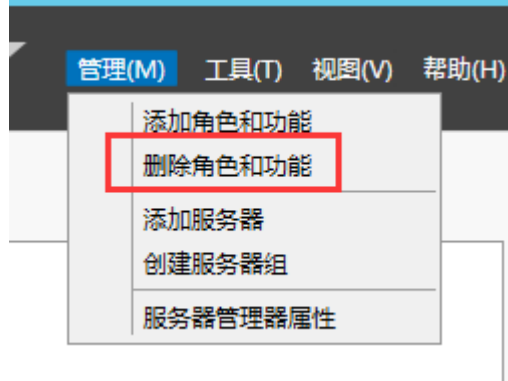
必须是Enterprise Admins组的成员，才能有权删除域内的最后一台域控制器。如果此域之下还有子域，请先删除子域。

- 如果此域控制器是全局编录服务器，请检查其所在站点内是否还有其他全局编录服务器，如果没有，请先指定另一台域控制器来扮演全局编录服务器，否则将影响用户登录。**Active Directory站点和服务-Site-Defalut-First-Site-Name – Server-NTDS Setting**并单击鼠标右键-属性-勾选全局编录

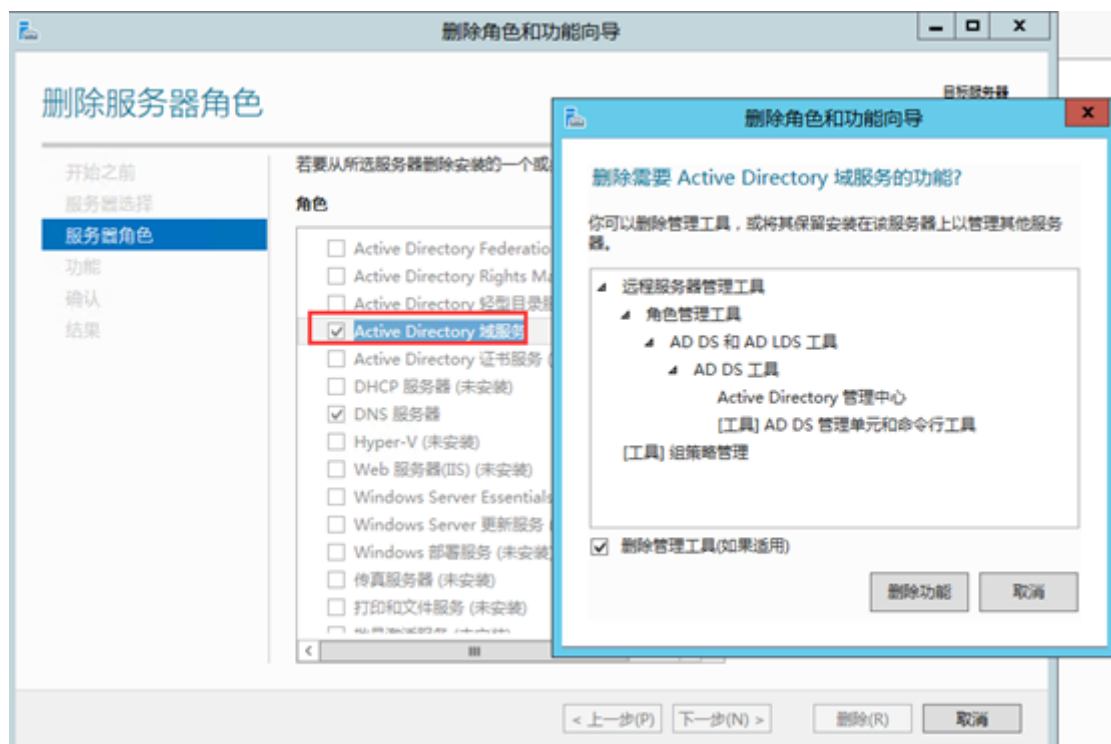


- 如果删除的域控制器是林内最后一台域控制器，则林辉被一起删除。Enterprise Admins组的成员才有限删除这台域控制器与林。

删除域控制器步骤：



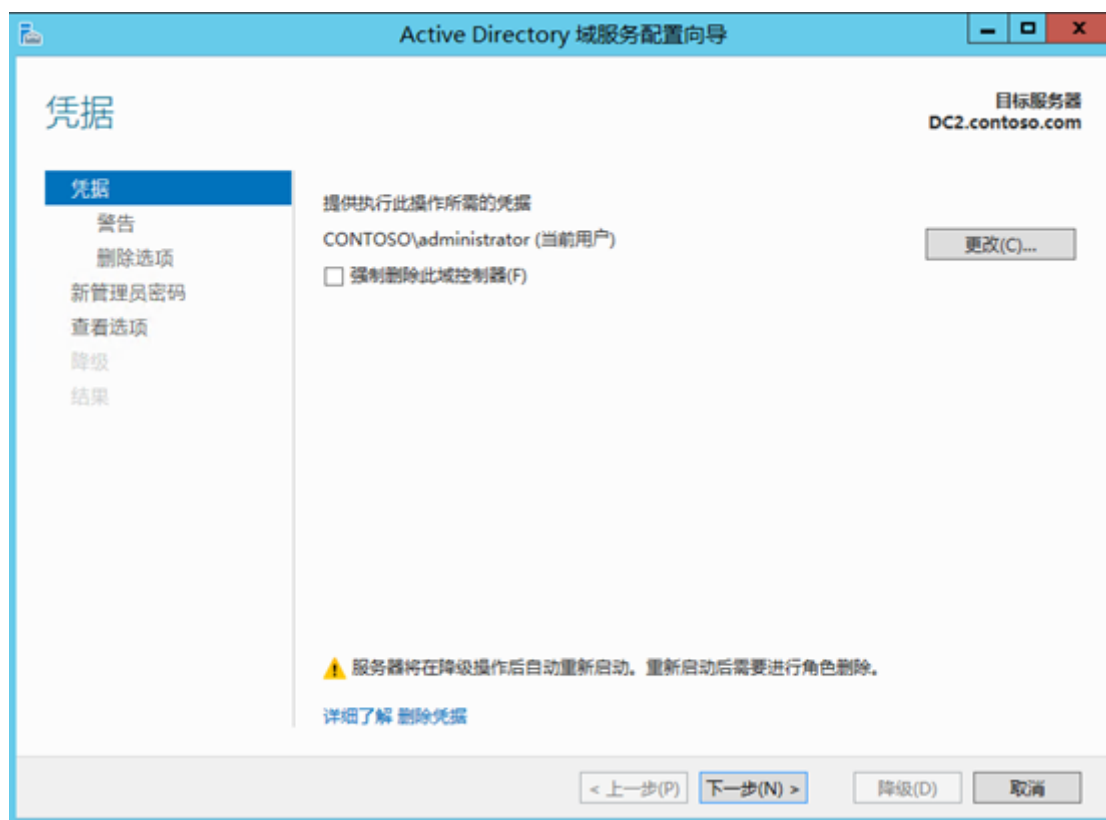
取消勾选



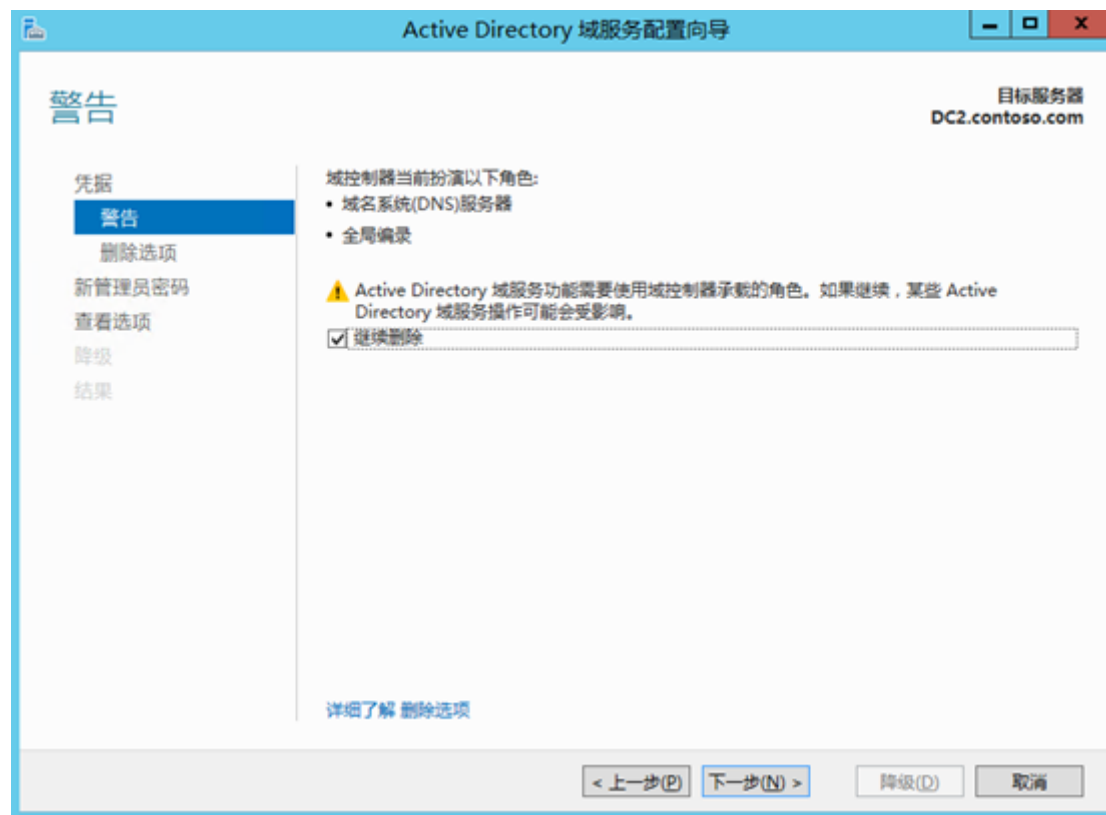
先降级

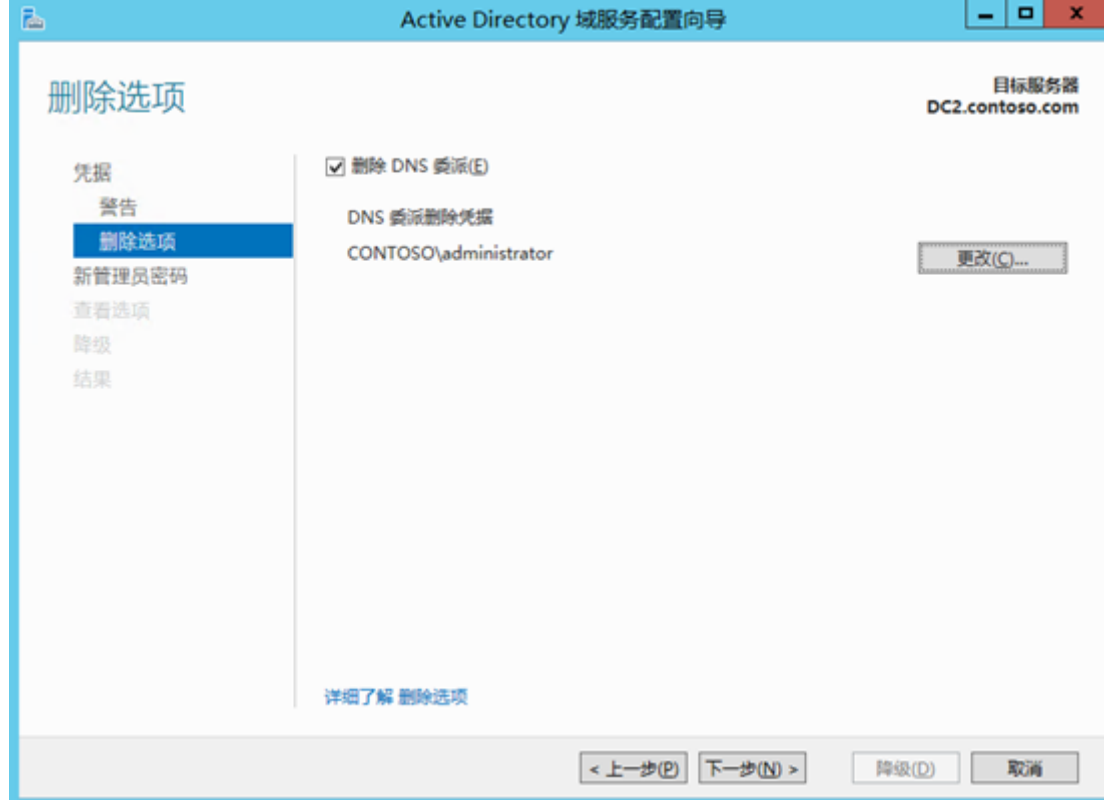


选择拥有权限的账户



如因为故障无法删除此域控制器(如，在删除时，需要能够连接企图域控制器，但是一直无法连接)此时可以勾选强制删除此域控制器。





属于降级后的本地administrator密码

Active Directory 域服务配置向导

新管理员密码

目标服务器
DC2.contoso.com

凭据
警告
删除选项
新管理员密码
查看选项
降级
结果

密码(P):
确认密码(C):

.....
.....

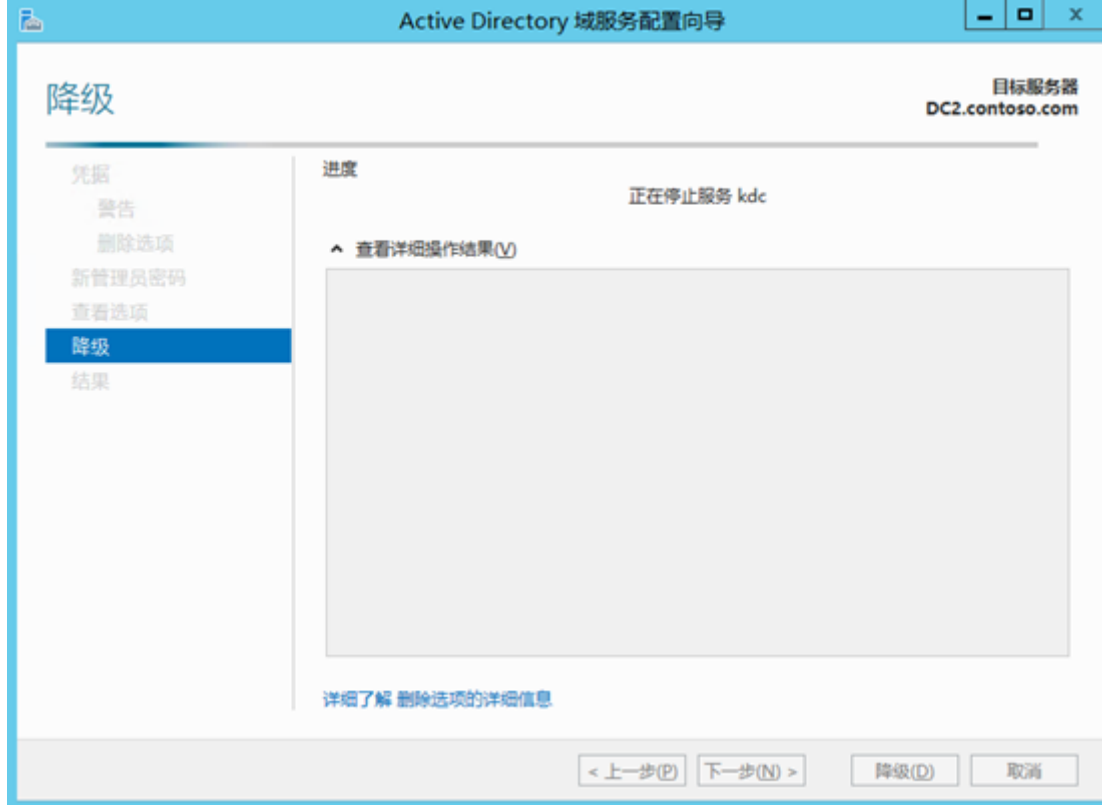
详细了解 删除管理员密码

< 上一步(B)

下一步(N) >

降级(D)

取消

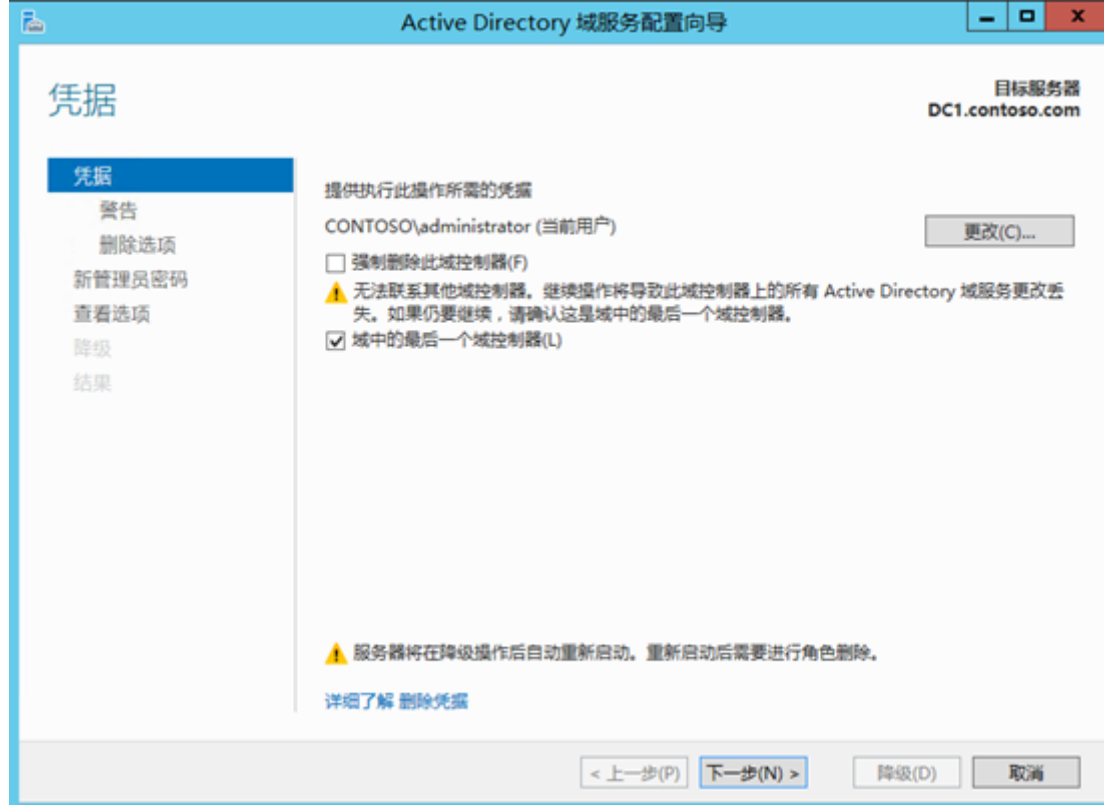


降级后服务器会重启，并重新登陆

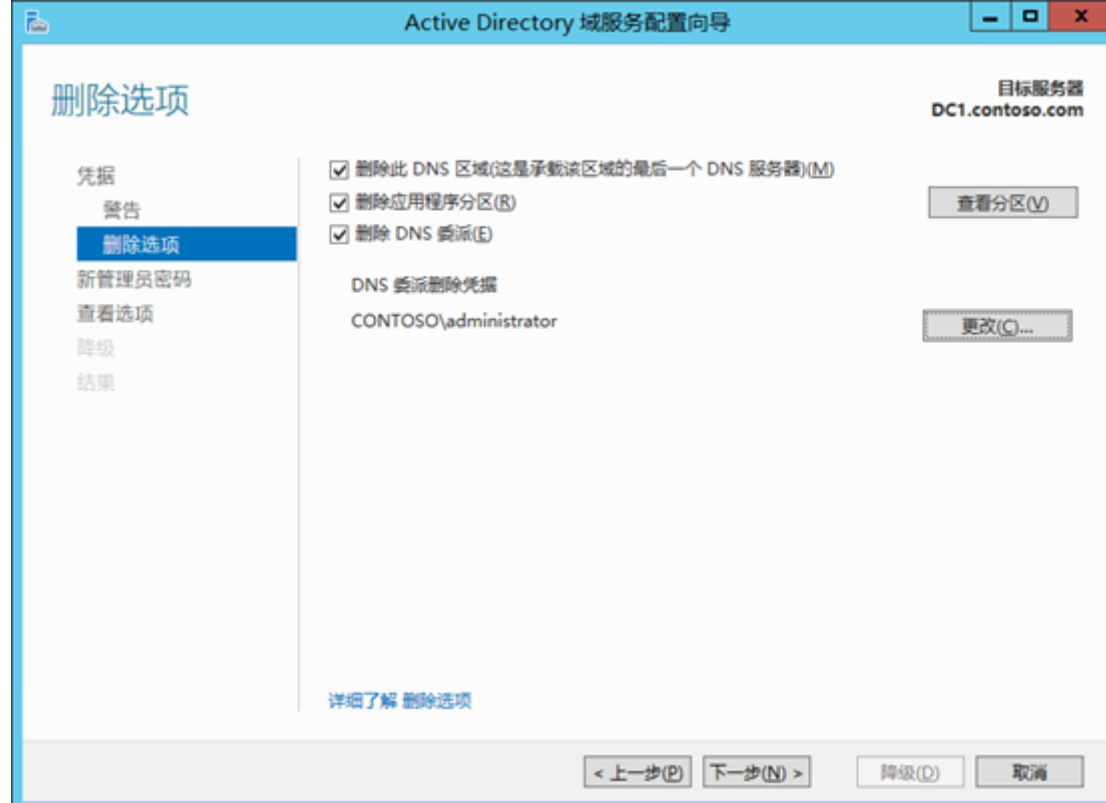
虽然这台服务器已经不再是域控了，不过此时域服务组件依然存在还是要继续去删除。

删除最后一台域控

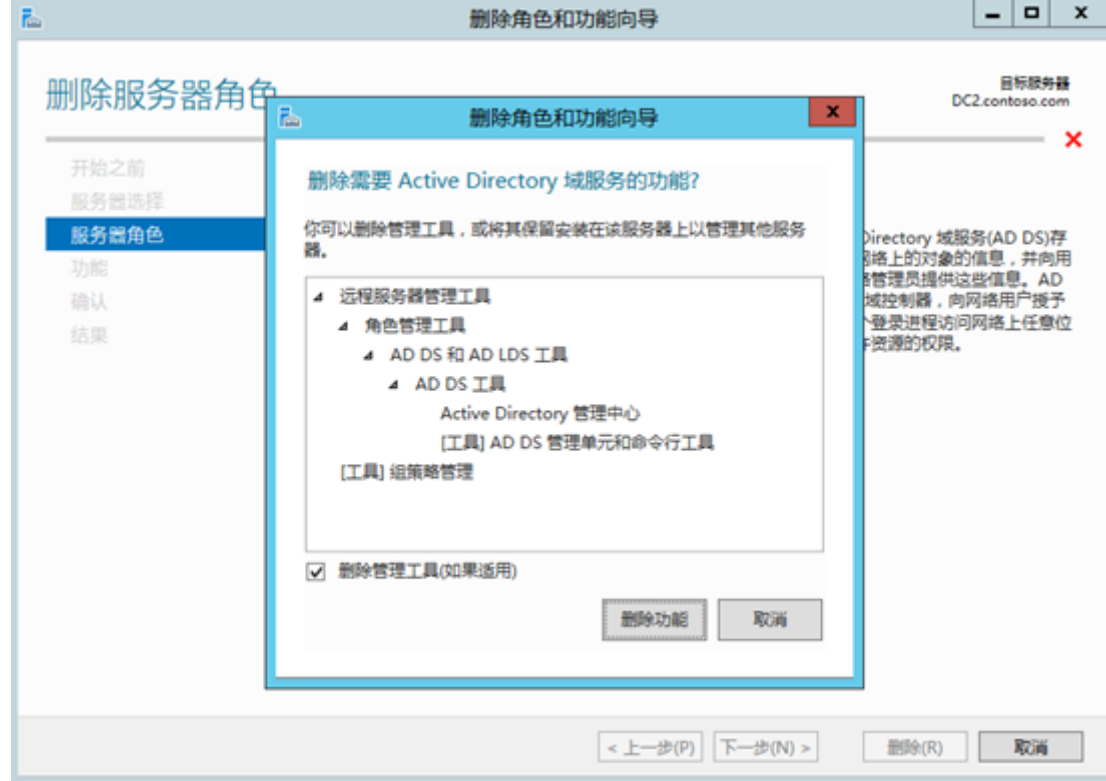
当域中已经没有其他域控制器时，最后一台删除时会多此选项。



删除dns区域和应用程序分区



完成后将管理工具删除



改变世界

分类: Windows Server 2012 R2系统配置



王哥哥哥哥
关注 - 1
粉丝 - 6

+加关注

1
推荐

0
反对

« 上一篇: [如何用vmware workstation来做虚拟化实验](#)

» 下一篇: [Bitlocker驱动器加密使用](#)


posted @ 2015-06-28 15:56 王哥哥哥哥 阅读(22952) 评论(1) 编辑 收藏

评论列表

谢谢分享

支持(0) 反对(0)

[刷新评论](#) [刷新页面](#) [返回顶部](#)

 注册用户登录后才能发表评论，请 [登录](#) 或 [注册](#)，[访问网站首页](#)。

【推荐】超50万VC++源码: 大型工控、组态\仿真、建模CAD源码2018！

【推荐】腾讯云如何购买服务器更划算？



最新IT新闻:

- UC回应裁员传闻：岗位调整一直在进行，欢迎新人加入
 - 拍拍贷宣布未来3年投入10亿加速科技金融进化
 - 在投资这件事上，印度本土巨头能从BAT学到什么？
 - 嘀嗒出行CEO宋中杰：我们为什么要把嘀嗒拼车升级为嘀嗒出行
 - 社交VR的成功取决于人，而不是VR头显
- » 更多新闻...



最新知识库文章:

- 步入云计算
- 以操作系统的角度述说线程与进程
- 软件测试转型之路

· 门内门外看招聘
· 大道至简，职场上做人做事做管理
» 更多知识库文章...