3-4：小型分支站点部署RODC

Practice：windows 2008R2 server core上部署RODC - 曾垂鑫的技术专栏 - 51CTO技术博客
http://543925535.blog.51cto.com/639838/290944

RODC的特征

只读数据：RODC上包含所有ADDS的对象和属性，但是和可读写的DC不一样的是，默认情况下，RODC上不包含账户的密码。在不能保证域控制器的安全性的情况下（例如分支机构），我们通过RODC实现域信息的安全性。在分支机构如果有LDAP的应用程序需要访问活动目录并对活动目录对象作修改，则该LDAP应用程序可以重定向到中央站点的可读写DC上。

单向复制：RODC对ADDS和DFS执行的常规的入站复制。因为您不能直接在RODC上进行写的操作，所以RODC是不支持出站复制的，所以作为RODC复制伙伴的可读写DC是不会从RODC接收到数据的。RODC的单向复制也同样应用到DFS复制。

凭据缓存:在RODC上存储用户和计算机的凭据称之为credential caching（凭据缓存）。默认情况下，RODC上只存储它自己的计算机账户和一个用于这台RODC的特殊的Kerberos 票据授权票 (KRBTGT)账户，此账户是被可读写DC用来验证RODC身份的。如果您需要在RODC上存储用户凭据或者计算机凭据的话，你需要在RODC上允许这些凭据被缓存。如果您在RODC上激活了凭据缓存，它只会影响组织中计算机和与用户账户的比较小的子集，这是因为RODC一般是总是放置在比较小的分支机构，所以您允许凭据缓存的计算机和用户账户应该都不多。这样即使您的RODC被偷了，您只会丢失那些缓存在RODC上的凭据。其实在后面会说到，在RODC被偷走之后，您可以马上在可读写DC上将RODC的计算机账户删除，在删除时可以对缓存在该RODC上的凭据进行密码重设，这样丢失掉的这些凭据就没有任何作用了。

只读DNS:您可以在RODC上安装DNS服务。RODC可以复制DNS所使用的所有应用程序目录分区（Application Directory Partition），包括ForestDNSZones和DomainDNSZones。如果您在RODC上安装了DNS，则客户端可以请求RODC进行名称解析。但是，在RODC上的DNS是不支持客户端直接进行更新DNS纪录的，因此RODC不会在它所拥有的活动目录集成区域里面注册任何NS纪录。当客户端找RODC进行DNS纪录更新时，RODC将返回一个指针。然后客户端计算机将联系指针所指向的DNS服务器更新DNS纪录。在后台，在RODC上的DNS服务器将尝试从执行更新的DNS服务器上复制更新的纪录。为了提高复制效率，RODC只会请求更新的纪录。

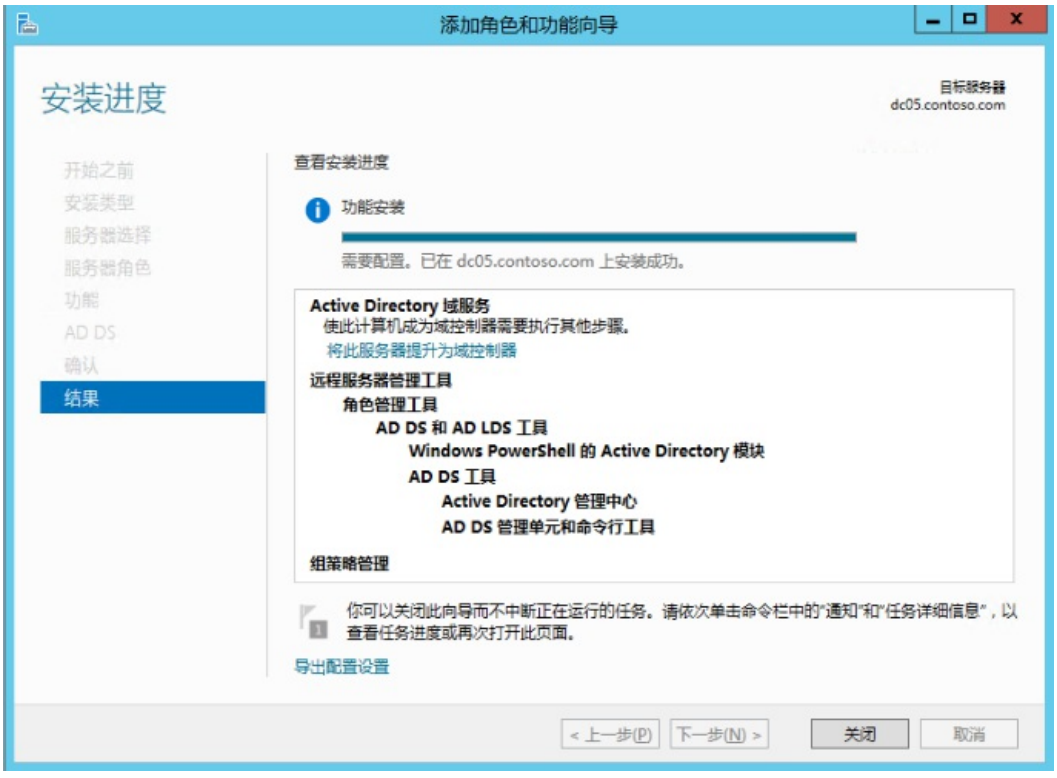
管理角色分离：您可以使用该特征来允许一个普通的域用户成为RODC的本地管理员。这样此用户可以对分支机构的RODC进行管理操作，例如安装安全更新或者驱动程序。这个特征好处在于此用用在域中或者任何可读写的域控制器上没有用户权利。而在以前都是可读写DC，DC的本地管理员和域管理员是没有区别的。这使得分支机构用户可以有效的管理RODC而不会影响整个域的安全性。

windows 2012R2的RODC部署也分为两步：

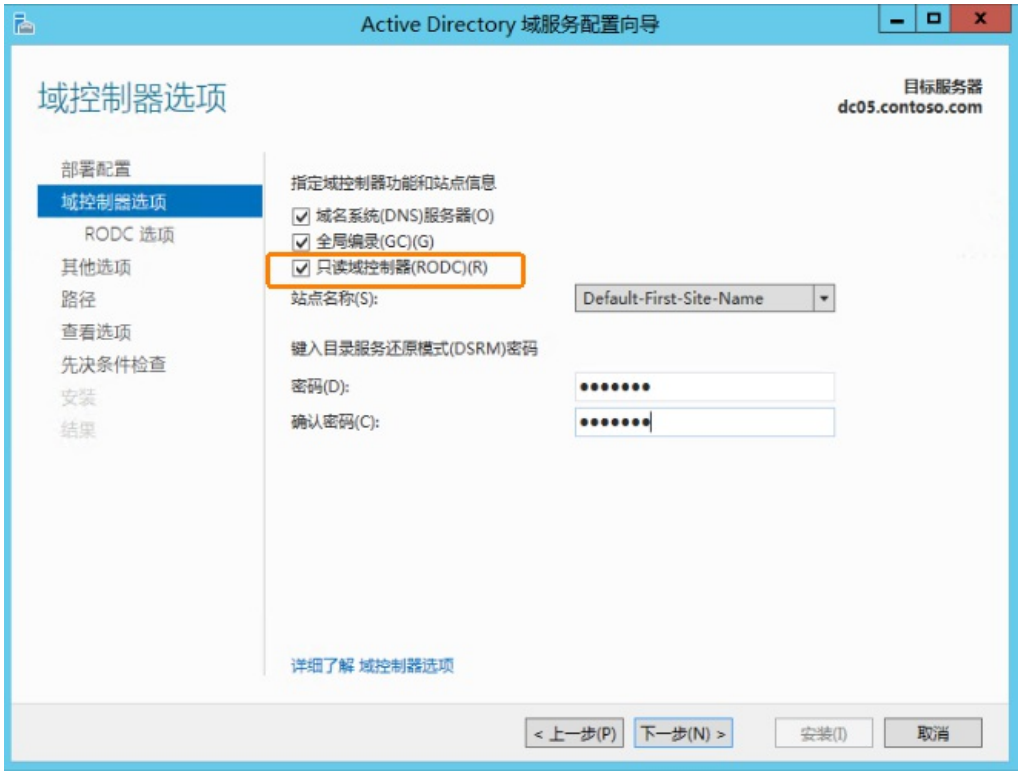
生产环境中：进行RODC的阶段式安装。

安装 Windows Server 2012 Active Directory 只读域控制器 (RODC)（级别 200） https://technet.microsoft.com/zh-cn/library/jj574152(v=ws.11).aspx

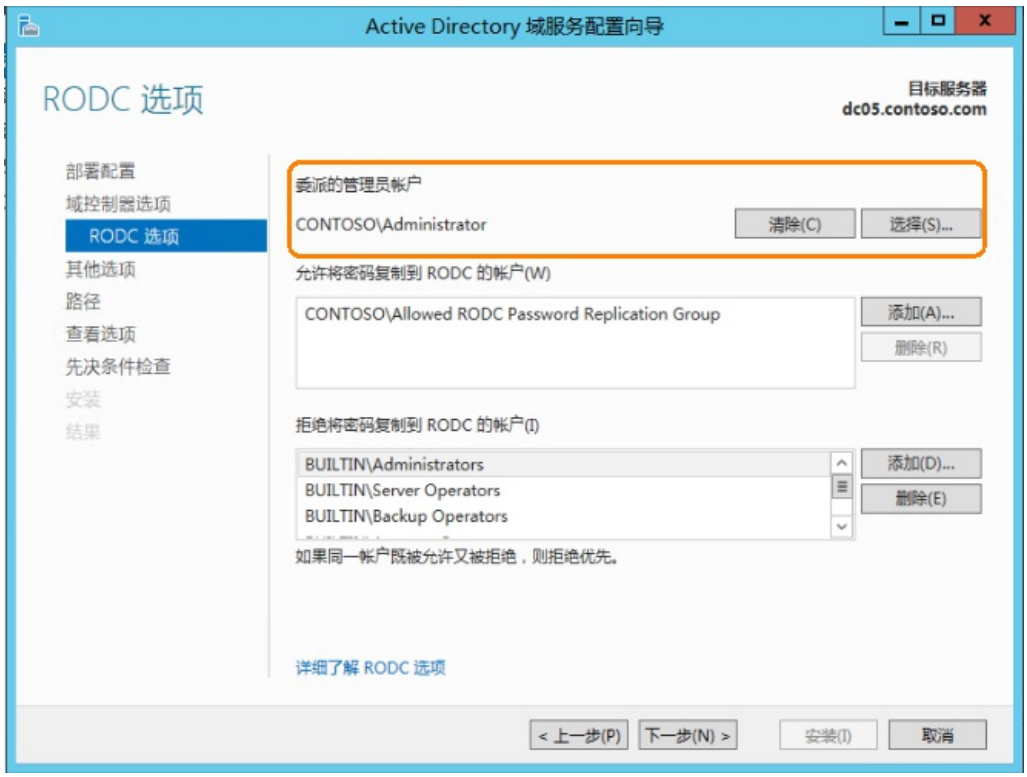
1）安装ADDS

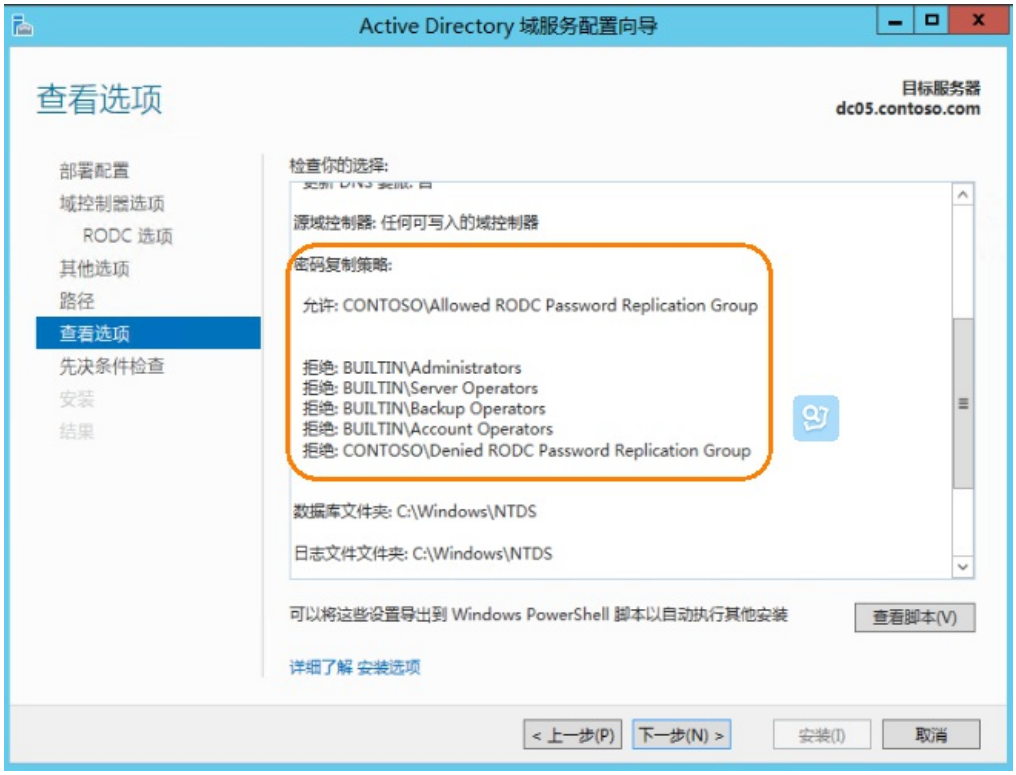


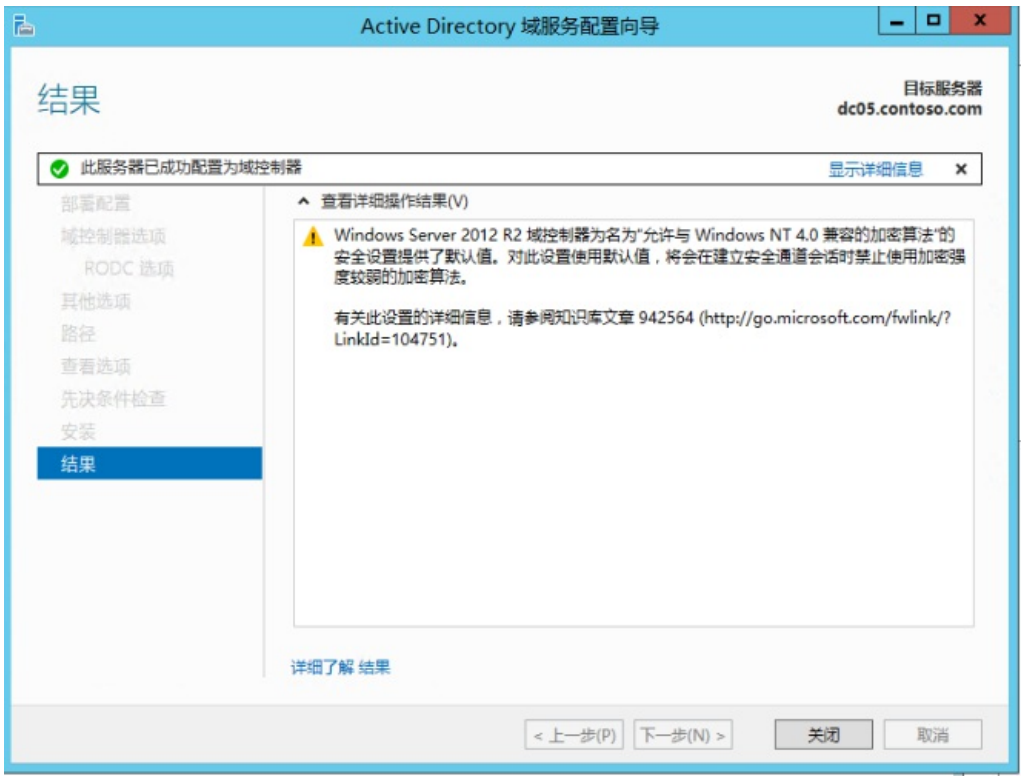
2）启用DC功能

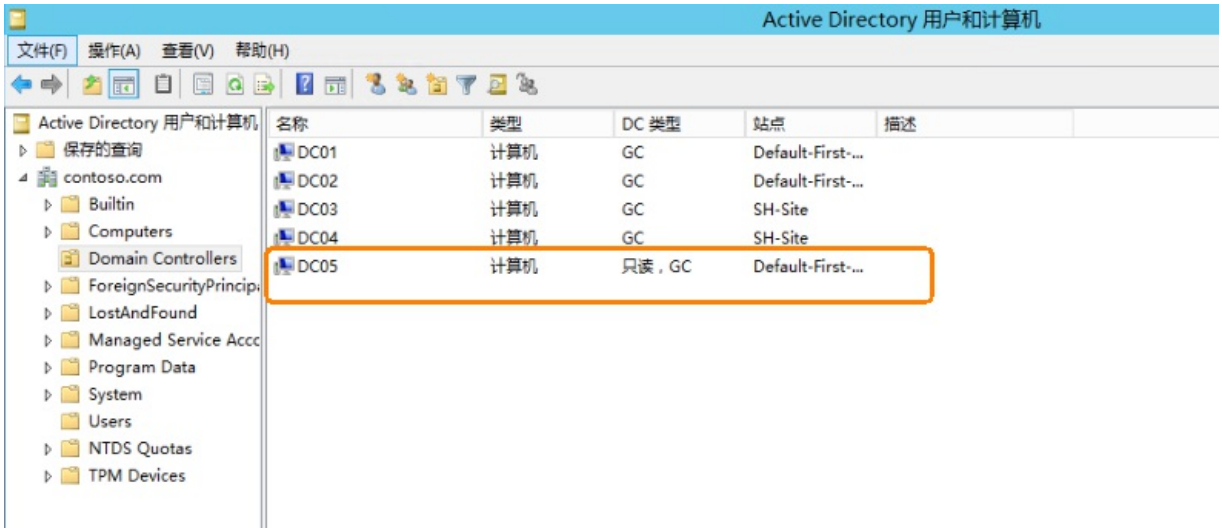


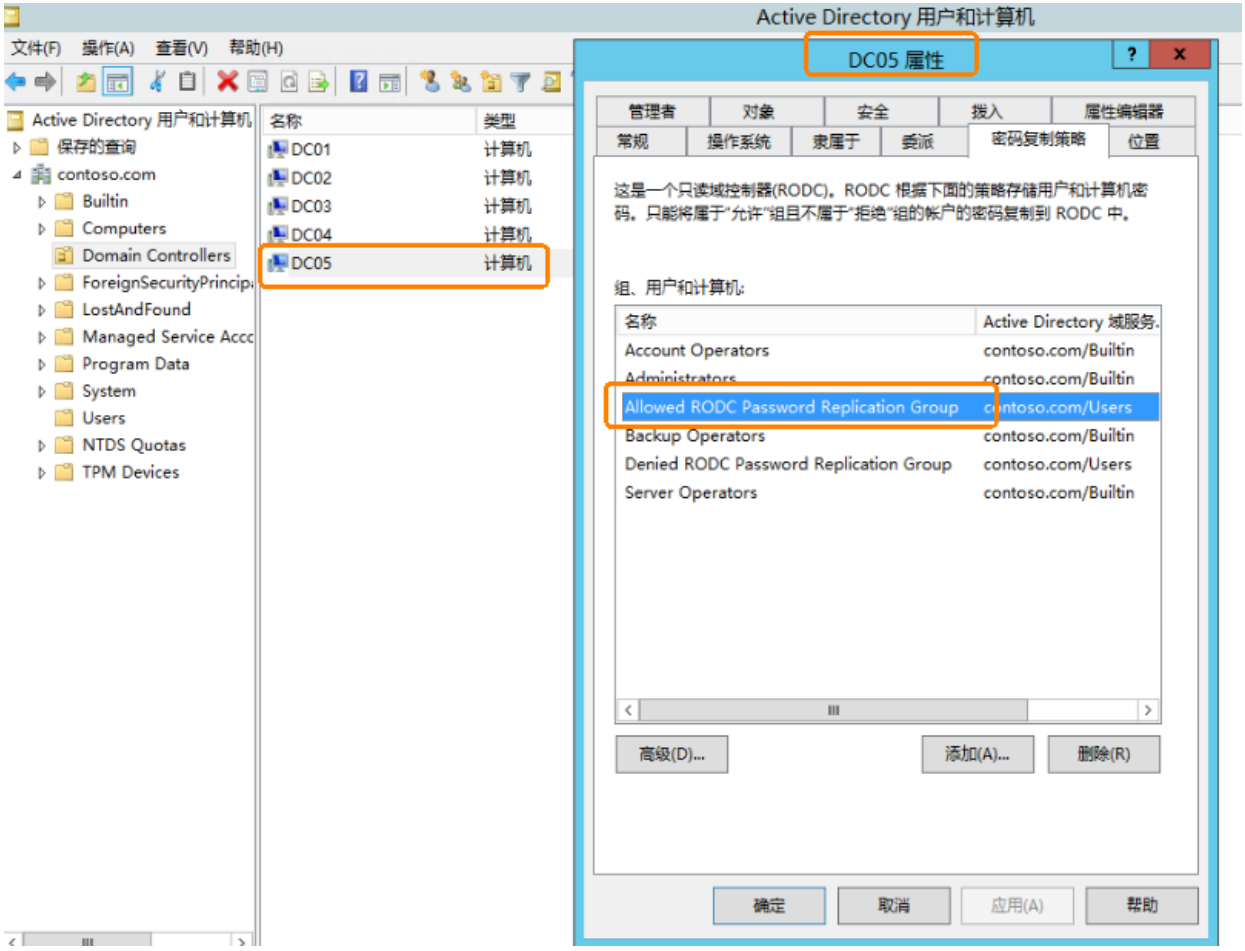
委派RODC的管理员账户，这里可以新建一个普通域账户，专门用来管理RODC。

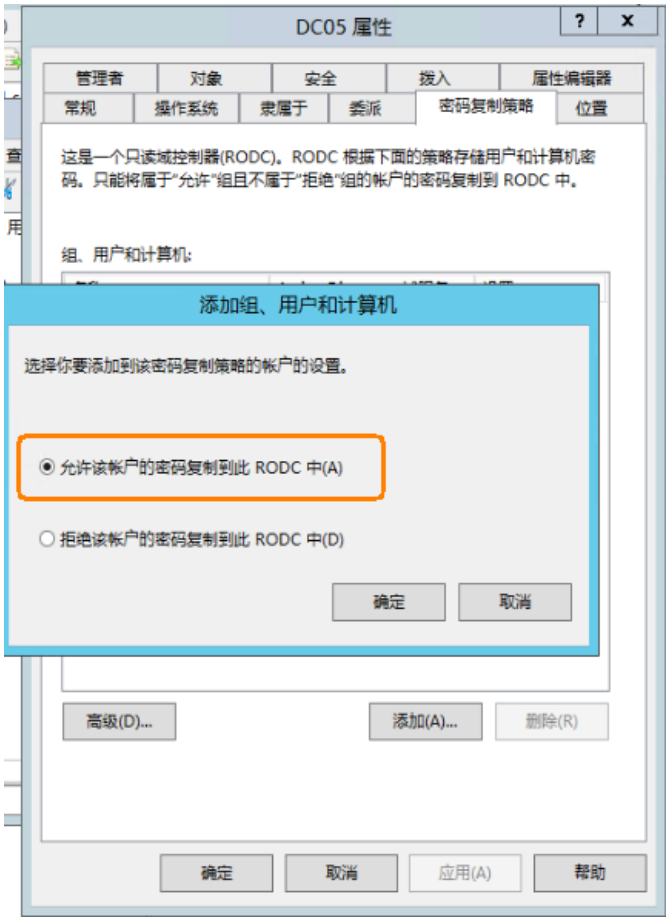


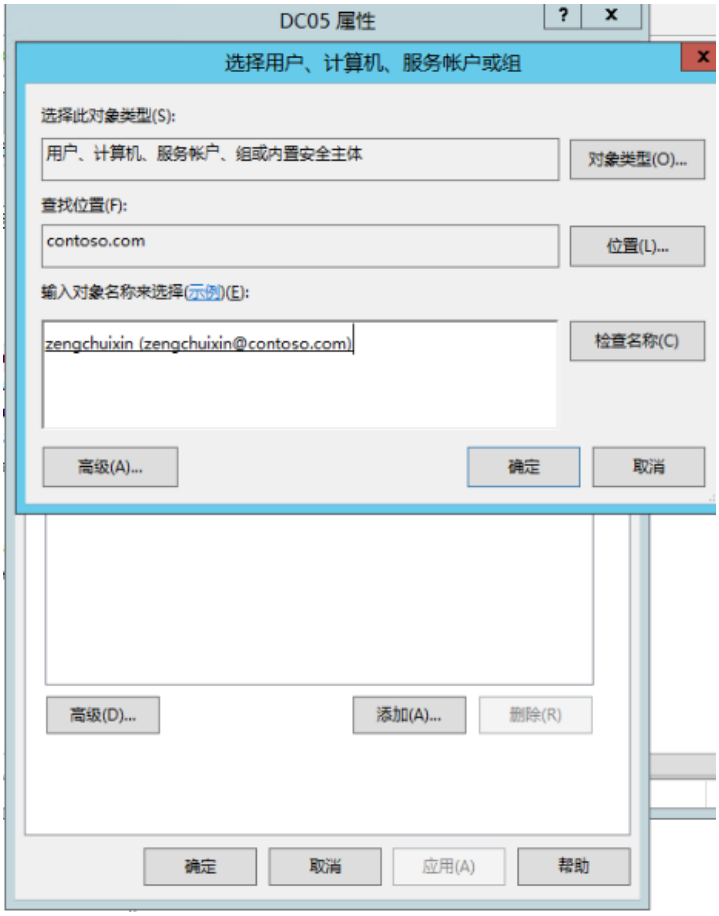

Active Directory 域服务配置向导
查看选项
目标服务器
dc05.contoso.com
部署配置
域控制器选项
RODC 选项
其他选项
路径
查看选项
先决条件检查
安装
结果
检查你的选择:
源域控制器: 任何可写入的域控制器
密码复制策略:
允许: CONTOSO\Allowed RODC Password Replication Group
拒绝: BUILTIN\Administrators
拒绝: BUILTIN\Server Operators
拒绝: BUILTIN\Backup Operators
拒绝: BUILTIN\Account Operators
拒绝: CONTOSO\Denied RODC Password Replication Group
数据库文件夹: C:\Windows\NTDS
日志文件文件夹: C:\Windows\NTDS
可以将这些设置导出到 Windows PowerShell 脚本以自动执行其他安装
查看脚本(V)
详细了解 安装选项
< 上一步(P)
下一步(N) >
安装(I)
取消

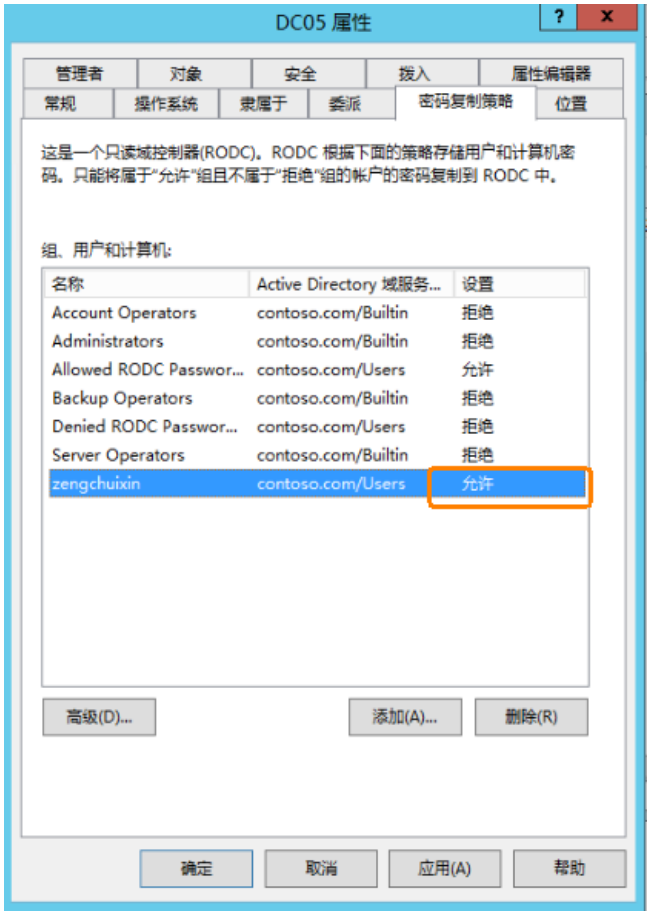

Active Directory 域服务配置向导
结果
目标服务器
dc05.contoso.com
此服务器已成功配置为域控制器
显示详细信息
部署配置
域控制器选项
RODC 选项
其他选项
路径
查看选项
先决条件检查
安装
结果
查看详细操作结果(V)
Windows Server 2012 R2 域控制器为名为"允许与 Windows NT 4.0 兼容的加密算法"的安全设置提供了默认值。对此设置使用默认值，将会在建立安全通道会话时禁止使用加密强度较弱的加密算法。
有关此设置的详细信息，请参阅知识库文章 942564 (http://go.microsoft.com/fwlink/?LinkId=104751)。
详细了解 结果
< 上一步(P)
下一步(N) >
关闭
取消


Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 帮助(H)
Active Directory 用户和计算机
保存的查询
contoso.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipa
LostAndFound
Managed Service Accc
Program Data
System
Users
NTDS Quotas
TPM Devices
名称 类型 DC 类型 站点 描述
DC01 计算机 GC Default-First-...
DC02 计算机 GC Default-First-...
DC03 计算机 GC SH-Site
DC04 计算机 GC SH-Site
DC05 计算机 只读，GC Default-First-...

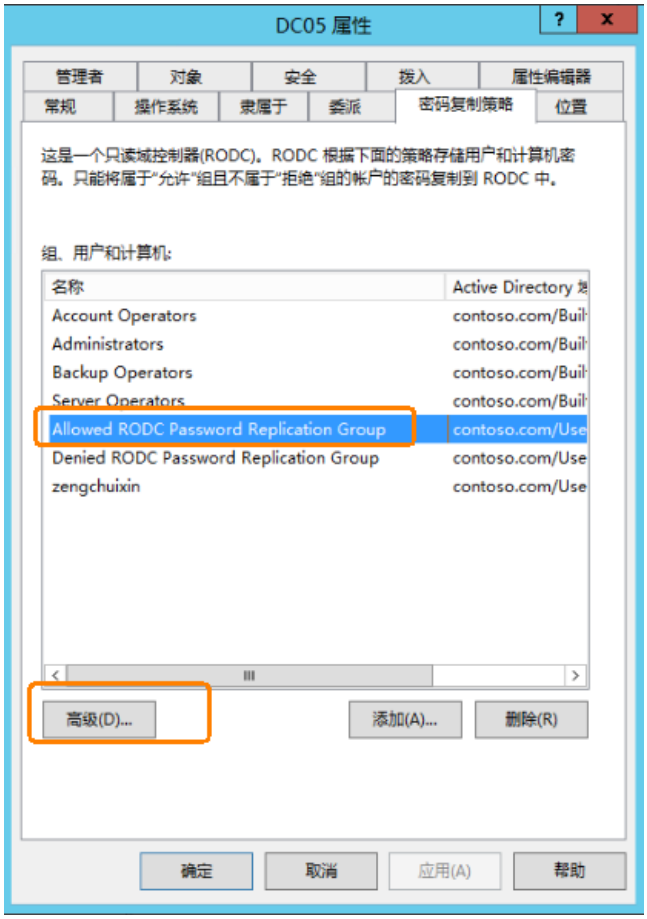

Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 帮助(H)
DC05 属性
管理者 对象 安全 拨入 属性编辑器
常规 操作系统 隶属于 委派 密码复制策略 位置
这是一个只读域控制器(RODC)。RODC 根据下面的策略存储用户和计算机密码。只能将属于"允许"组且不属于"拒绝"组的帐户的密码复制到 RODC 中。
组、用户和计算机:
名称 Active Directory 域服务...
Account Operators contoso.com/Builtin
Administrators contoso.com/Builtin
Allowed RODC Password Replication Group contoso.com/Users
Backup Operators contoso.com/Builtin
Denied RODC Password Replication Group contoso.com/Users
Server Operators contoso.com/Builtin
高级(D)...
添加(A)...
删除(R)
确定
取消
应用(A)
帮助

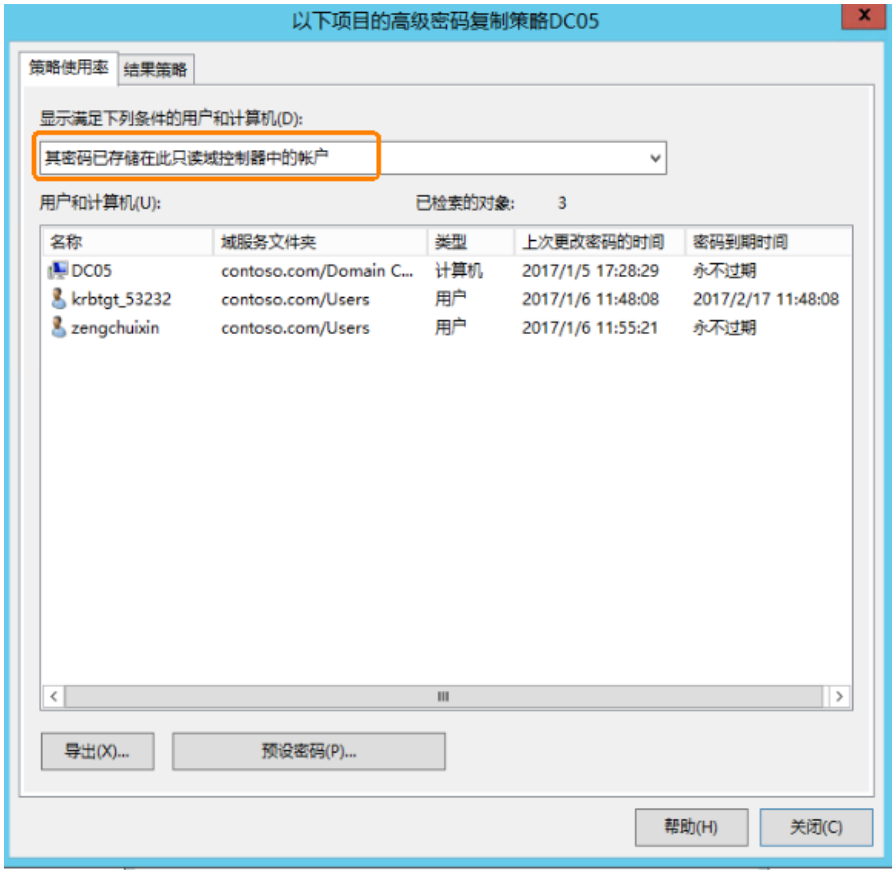

DC05 属性
管理者
对象
安全
拨入
属性编辑器
常规
操作系统
隶属于
委派
密码复制策略
位置
这是一个只读域控制器(RODC)。RODC 根据下面的策略存储用户和计算机密码。只能将属于"允许"组且不属于"拒绝"组的帐户的密码复制到 RODC 中。
组、用户和计算机:
添加组、用户和计算机
选择你要添加到该密码复制策略的帐户的设置。
允许该帐户的密码复制到此 RODC 中(A)
拒绝该帐户的密码复制到此 RODC 中(D)
确定
取消
高级(D)...
添加(A)...
删除(R)
确定
取消
应用(A)
帮助

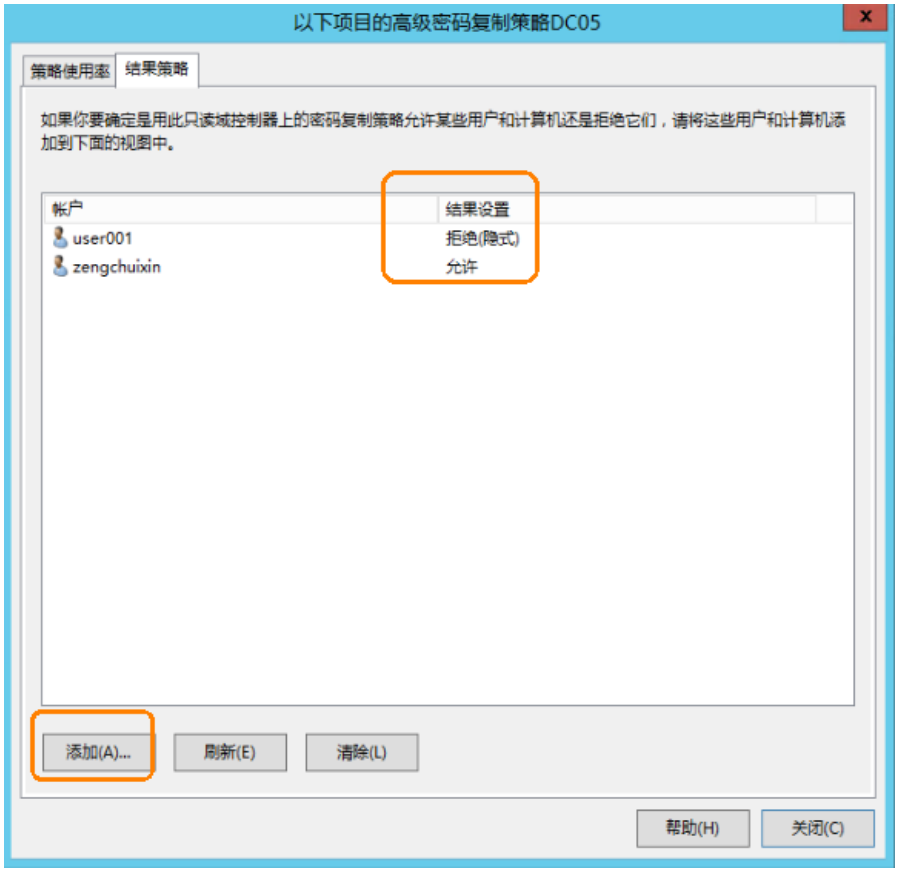

DC05 属性
选择用户、计算机、服务帐户或组
选择此对象类型(S):
用户、计算机、服务帐户、组或内置安全主体
对象类型(O)...
查找位置(F):
contoso.com
位置(L)...
输入对象名称来选择(示例)(E):
zengchuixin (zengchuixin@contoso.com)
检查名称(C)
高级(A)...
确定
取消
高级(D)...
添加(A)...
删除(R)
确定
取消
应用(A)
帮助



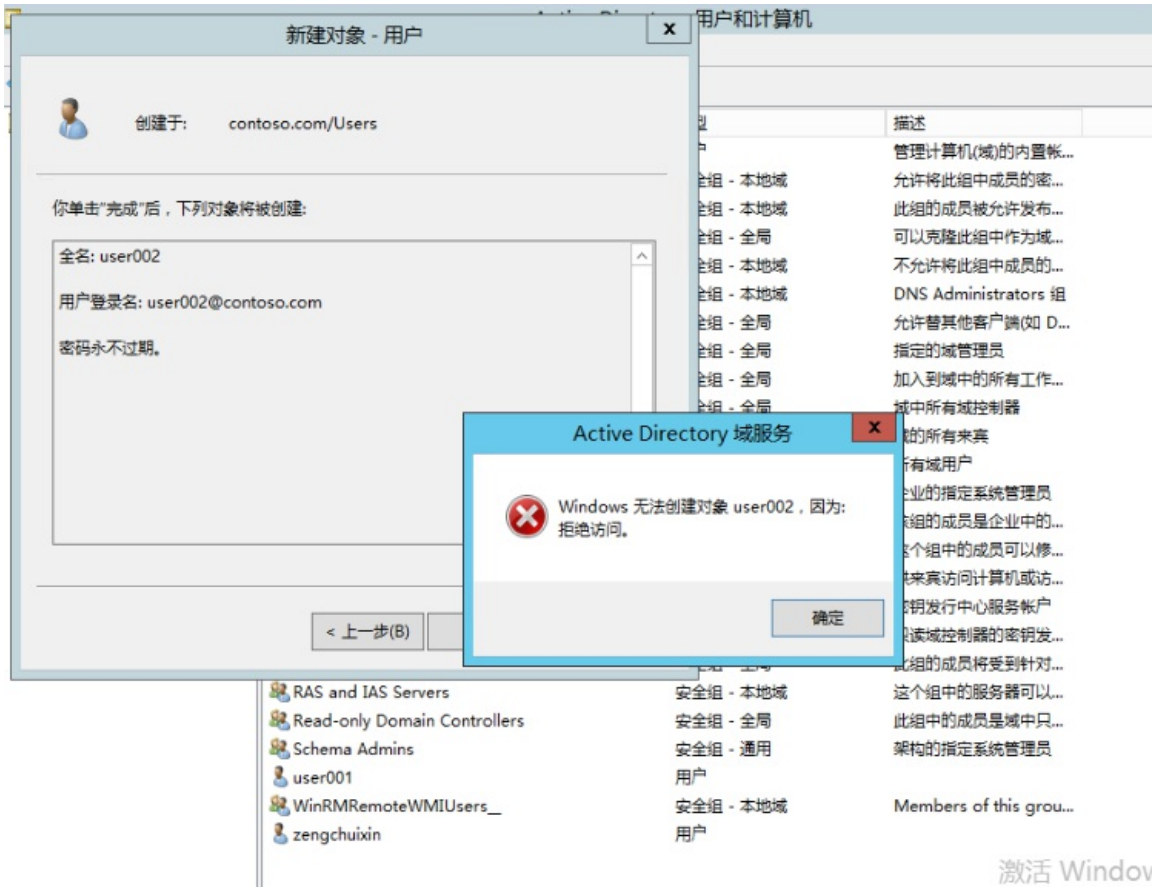
将zengchuixin设置为RODC的管理者。注意设置完成后，如果无法登录RODC，可以尝试手动复制站点或者等待一段时间之后再尝试登录。

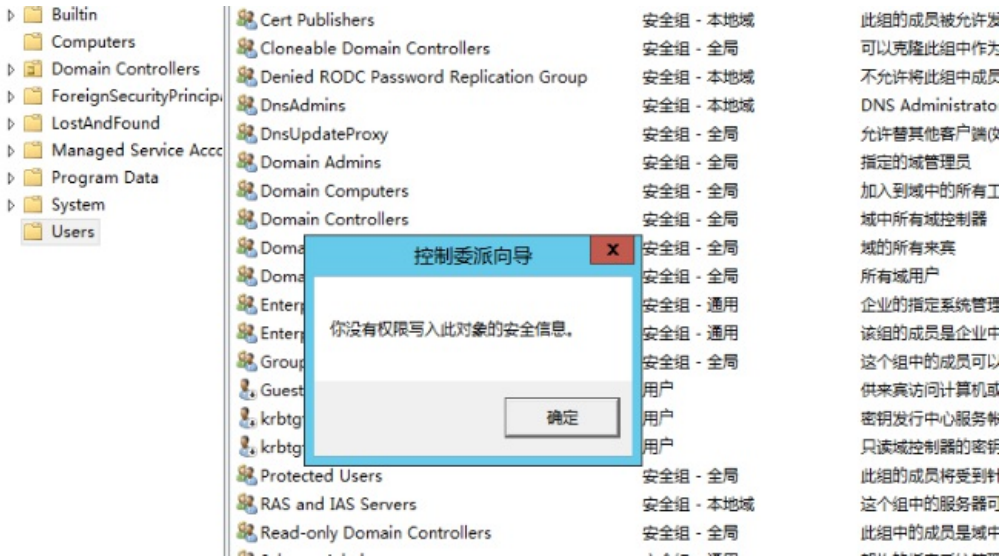

DC05 属性
管理者
对象
安全
拨入
属性编辑器
常规
操作系统
隶属于
委派
密码复制策略
位置
这是一个只读域控制器(RODC)。RODC 根据下面的策略存储用户和计算机密码。只能将属于"允许"组且不属于"拒绝"组的帐户的密码复制到 RODC 中。
组、用户和计算机:
名称
Active Directory
Account Operators
contoso.com/Buil
Administrators
contoso.com/Buil
Backup Operators
contoso.com/Buil
Server Operators
contoso.com/Buil
Allowed RODC Password Replication Group
contoso.com/Use
Denied RODC Password Replication Group
contoso.com/Use
zengchuixin
contoso.com/Use
高级(D)...
添加(A)...
删除(R)
确定
取消
应用(A)
帮助


以下项目的高级密码复制策略DC05
策略使用率
结果策略
显示满足下列条件的用户和计算机(D):
其密码已存储在此只读域控制器中的帐户
用户和计算机(U):
已检索的对象:
3
名称
域服务文件夹
类型
上次更改密码的时间
密码到期时间
DC05
contoso.com/Domain C...
计算机
2017/1/5 17:28:29
永不过期
krbtgt_53232
contoso.com/Users
用户
2017/1/6 11:48:08
2017/2/17 11:48:08
zengchuixin
contoso.com/Users
用户
2017/1/6 11:55:21
永不过期
导出(X)...
预设密码(P)...
帮助(H)
关闭(C)



以zengchuixin身份登录RODC，可以看到能管理的东西是有限的。




Builtin
Computers
Domain Controllers
ForeignSecurityPrincipa
LostAndFound
Managed Service Acc
Program Data
System
Users
Cert Publishers 安全组 - 本地域 此组的成员被允许发
Cloneable Domain Controllers 安全组 - 全局 可以克隆此组中作为
Denied RODC Password Replication Group 安全组 - 本地域 不允许将此组中成员
DnsAdmins 安全组 - 本地域 DNS Administrato
DnsUpdateProxy 安全组 - 全局 允许替其他客户端(
Domain Admins 安全组 - 全局 指定的域管理员
Domain Computers 安全组 - 全局 加入到域中的所有工
Domain Controllers 安全组 - 全局 域中所有域控制器
安全组 - 全局 域的所有来宾
安全组 - 全局 所有域用户
安全组 - 通用 企业的指定系统管理
安全组 - 通用 该组的成员是企业中
安全组 - 全局 这个组中的成员可以
用户 供来宾访问计算机或
用户 密钥发行中心服务帐
用户 只读域控制器的密钥
Protected Users 安全组 - 全局 此组的成员将受到针
RAS and IAS Servers 安全组 - 本地域 这个组中的服务器可
Read-only Domain Controllers 安全组 - 全局 此组中的成员是域中
控制委派向导
你没有权限写入此对象的安全信息。
确定