

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（KRBGT）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，您需要在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大的子集，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置，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：

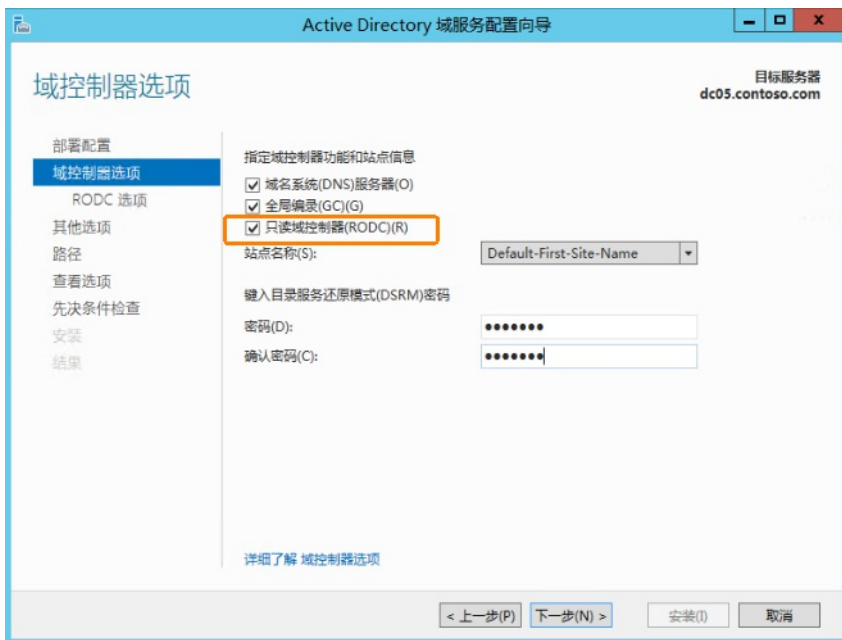
生产环境中：进行RODC的阶段式安装。

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](https://technet.microsoft.com/zh-cn/library/jj574152(v=ws.11).aspx)

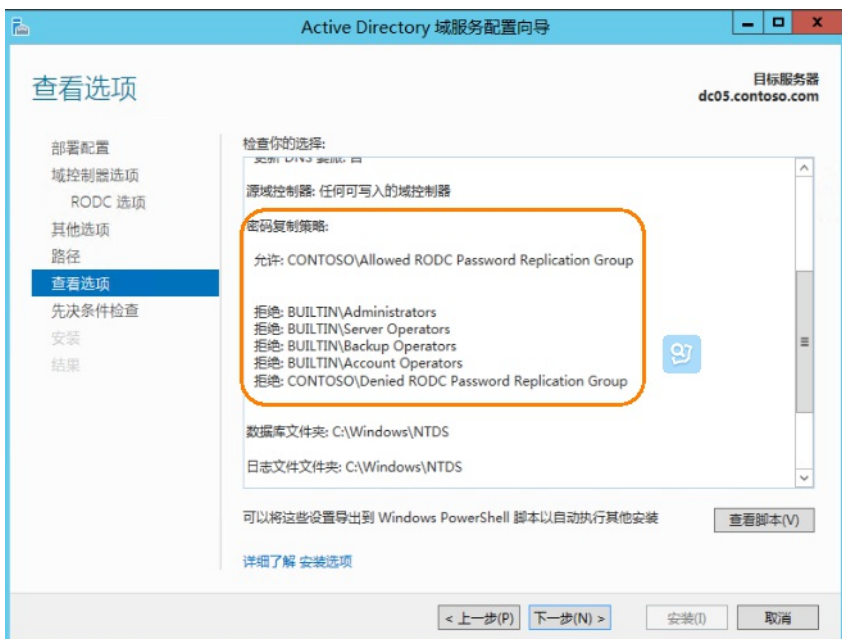
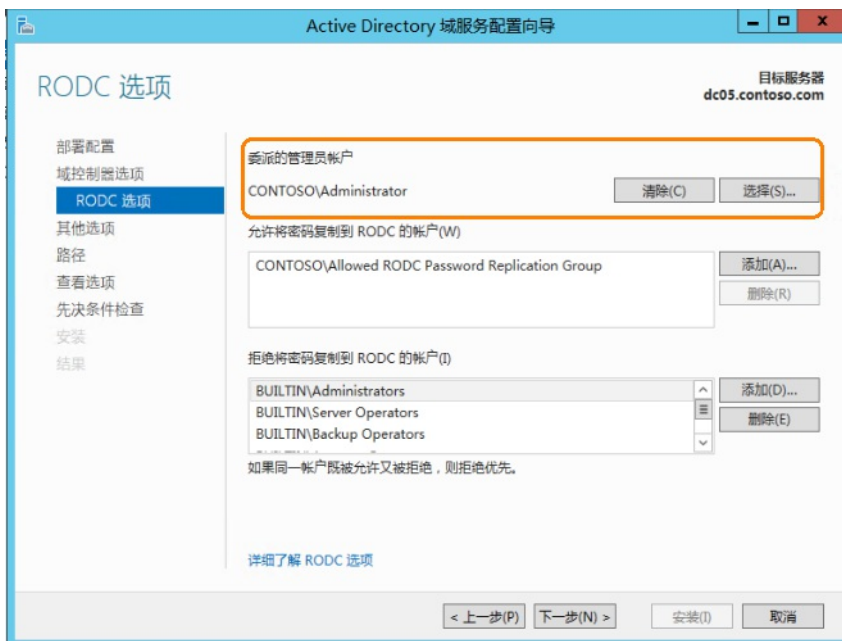
1）安装ADDS

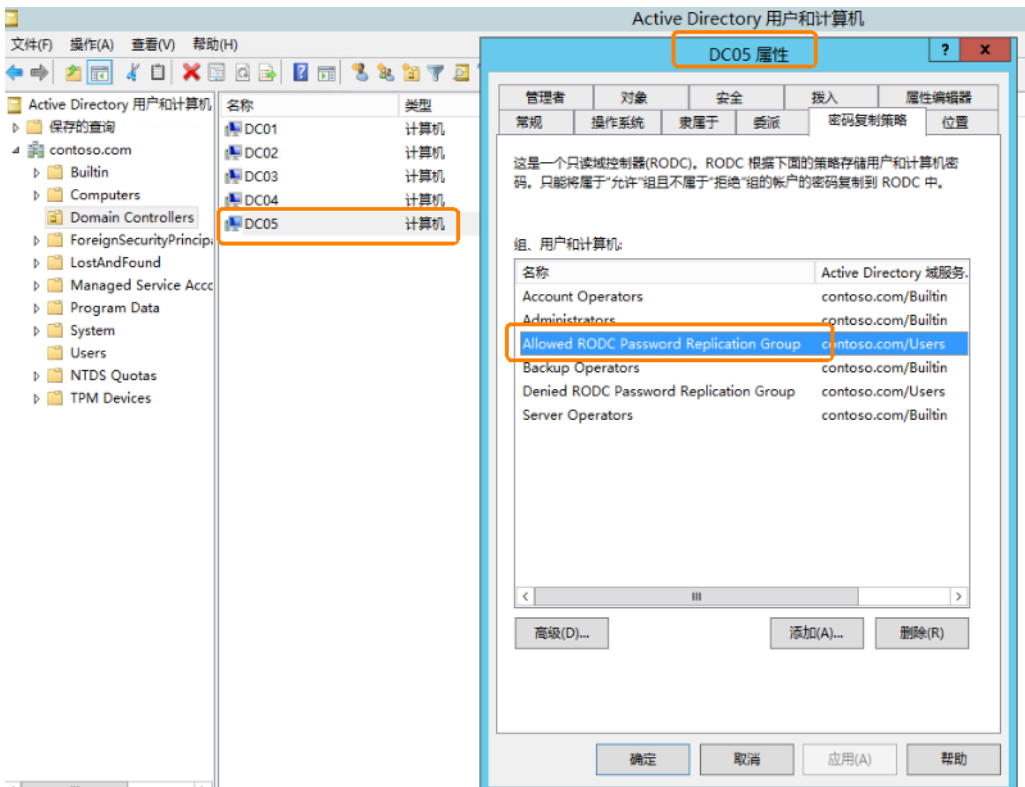
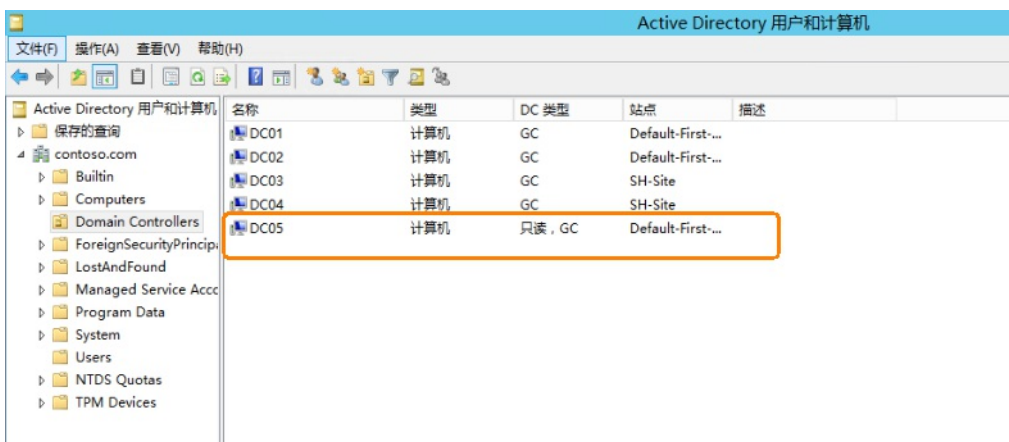
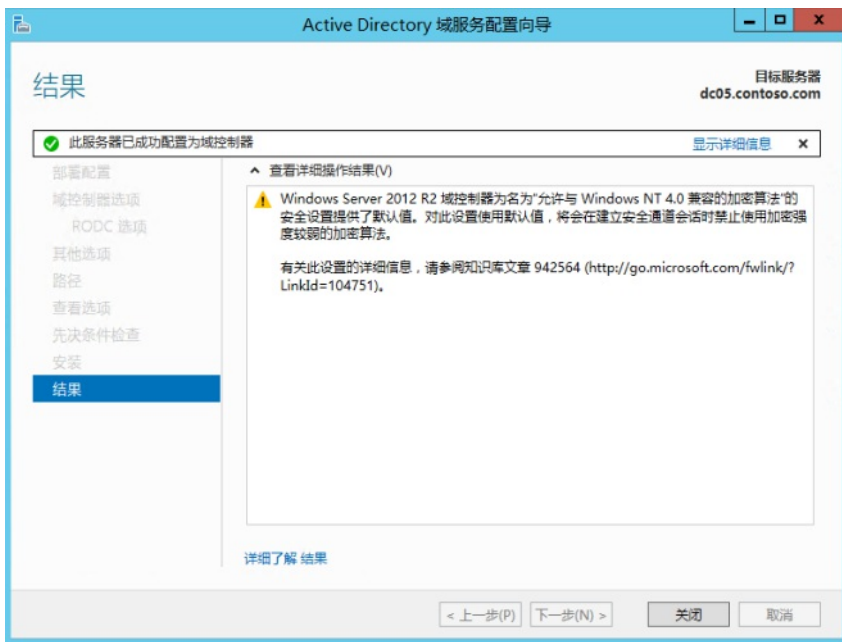


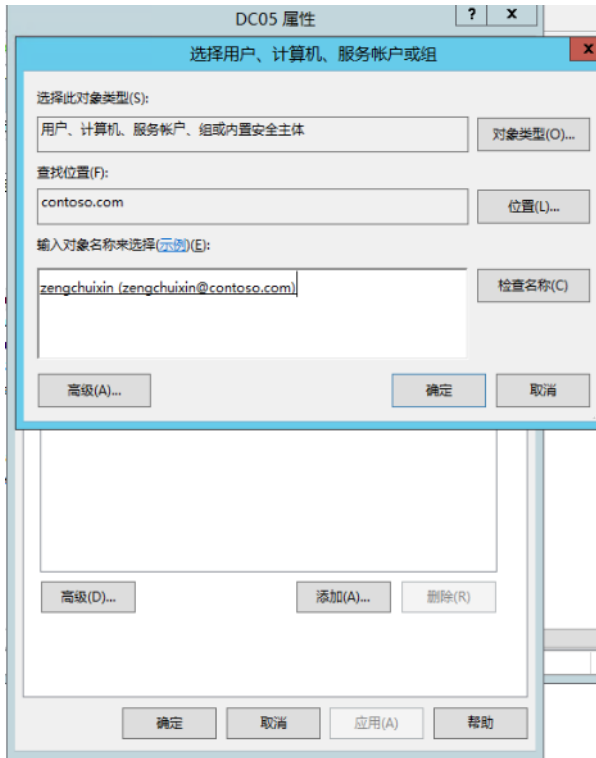
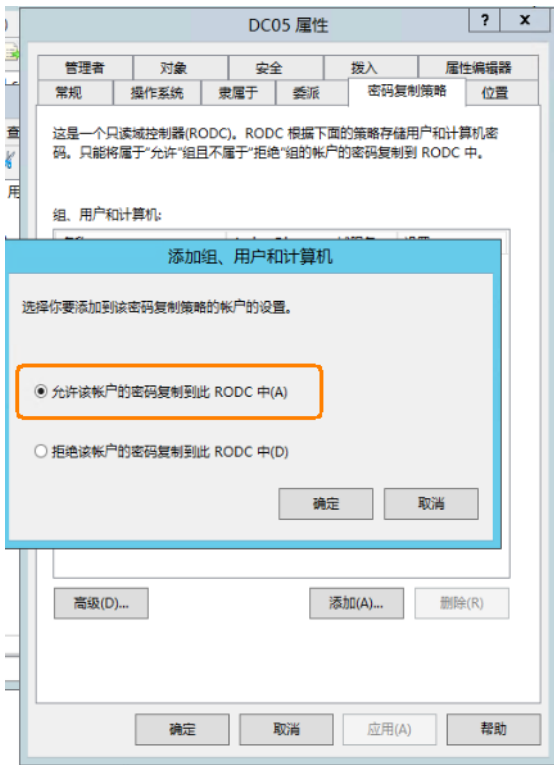
2）启用DC功能

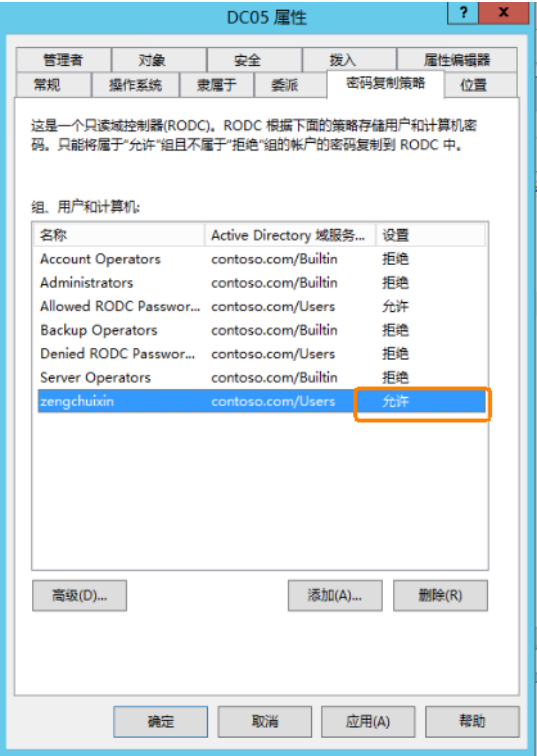


委派RODC的管理员账户，这里可以新建一个普通域账户，专门用来管理RODC。

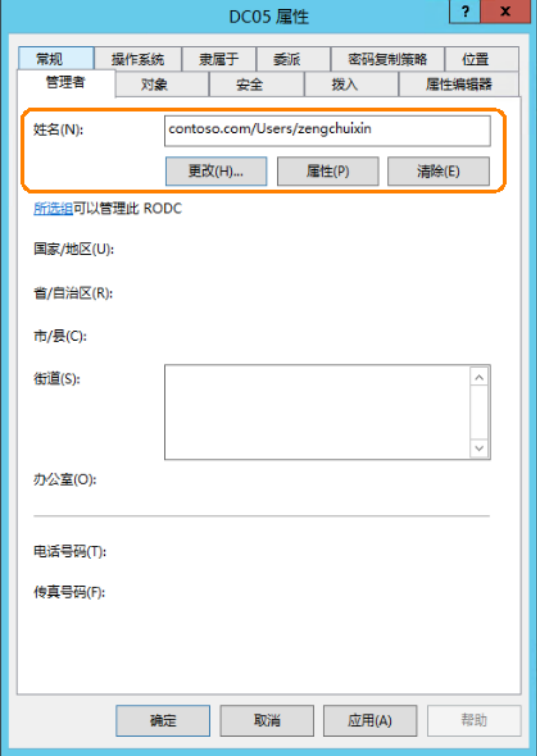


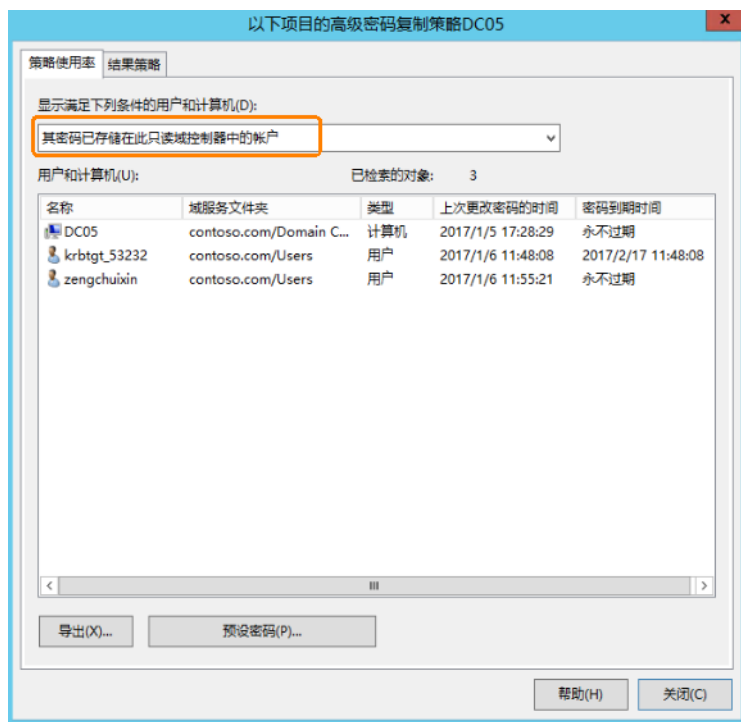
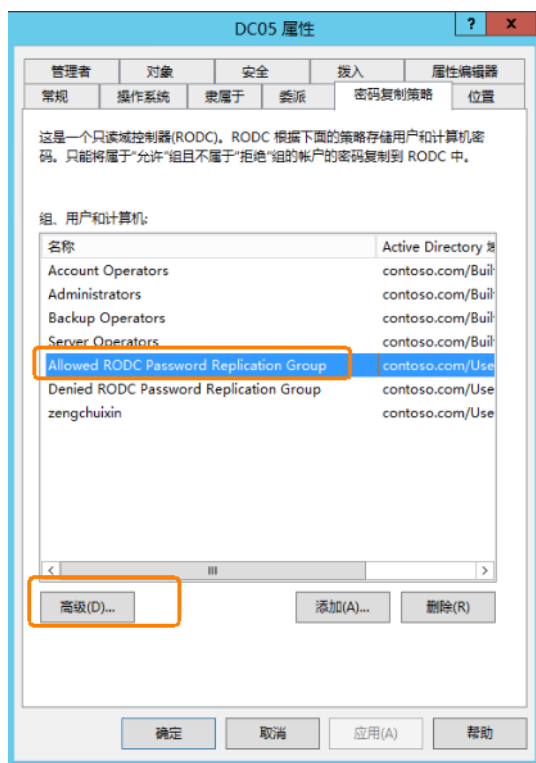


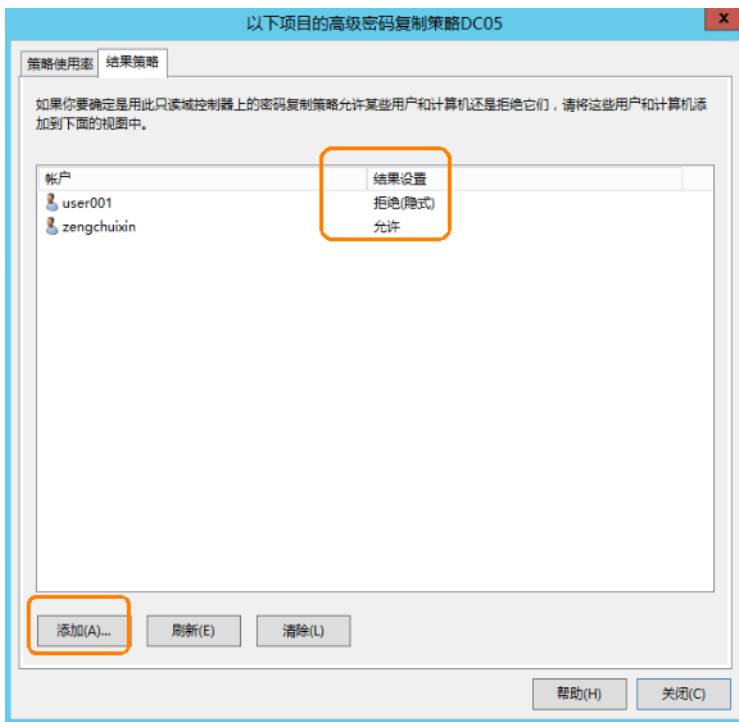




将zengchuxin设置为RODC的管理者。注意设置完成后，如果无法登录RODC，可以尝试手动复制站点或者等待一段时间之后再尝试登录。







以zengchuixin身份登录RODC，可以看到能管理的东西是有限的。

