活动目录在WindowsServer2008中的改进：只读域控制器(RODC) PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/245/2021_2022__E6_B4_BB_E5_8A_A8_E7_9B_AE_E5_c100_245041.htm 只读域控制器（RODC）是在Windows Server? 2008操作系统中一种新的域控制器。有了只读域控制器，组织能够容易地的物理安全得不到保证的地区部署域控制器。一台RODC包含了活动目录数据库的只读部分。 在Windows Server? 2008发布以前，如果用户不得不跨广域网连接域控制器进行身份验证的话，那也就没有其它更好的选择。在许多案例中，这不是有效的解决方法。分支机构通常无法为一台可写的域控制器提供的足够的物理安全。而且，当分支机构连接到枢纽站点时，它们的网络带宽通常比较差。这将导致登录时间变长。这也会阻碍网络资源的访问。 从Windows Server? 2008开始，组织能够部署RODC来处理这些问题。作为部署的结果，用户能够获得以下好处：改进的安全性快速登录更有效的访问网络资源RODC可以做什么？ 在考虑部署RODC时，物理安全的不足是最为寻常的理由。RODC给那些需要快速可靠的身份验证，同时对可写域控制器而言物理安全无法得到确保的地方部署域控制器提供了新的方法。 然而你的组织也可以为了特殊的管理需要选择部署RODC。比如，业务程序（line-of-business，LOB）只能被安装到域控制器上并才能得以成功运行。或者，域控制器是分支机构仅有的服务器，而不得不运行服务器应用。 在这些例子中，业务程序所有者必须经常交互式登录到域控制器或者使用终端服务来配置和管理程序。这种环境引起了在可写域控制器上不被接受的安全

风险。 RODC为在这些场景中部署域控制器提供了更安全的机械结构。你能够将登录到RODC的权利转让给没有管理权限的域用户同时最小化给互动目录森林带来的安全风险。 你也可以在其它场景中部署RODC，比如在外延网（EXTRANETS）中本地储存的所有域密码被认为是主要威胁。 还有其它要特别考虑的吗？ 为了部署RODC，域中必须至少有一台运行Windows Server 2008的可写域控制器。此外，活动目录域和森林的功能级必须是Windows Server 2003或者更高。 这项特性提供了什么新功能？ RODC处理了在分支机构中的普遍问题。这些地方也许没有域控制器。或者他们有可写的域控制器但是没有足够的物理安全，网络带宽以及专门的技术人员来提供支持。下面的RODC的功能缓解了这些问题：只读活动目录数据库单向复制凭据缓存管理员角色分割只读DNS 只读活动目录数据库除了账户密码之外，RODC拥有所有可写域控制器拥有的对象和属性。然而，无法针对储存在RODC的数据库进行任何数据上的改变。数据上的改变必须在可写域控制器上进行然后复制回RODC。 请求获得目录读取权限的本地程序能够获得访问许可。当使用轻型目录访问协议（LDAP）的程序请求写入权限时将会收到“ referral ”应答。在枢纽站点中，通常情况下这些应答将写入请求引导到可写的域控制器。 RODC已筛选属性集使用AD DS作为数据存储的某些程序，也许会将类似信任凭据的数据（诸如密码，信任凭据，加密密钥）储存在RODC上。而你不想将这些数据储存在RODC上是因为考虑到RODC受到安全威胁的情况。 为了这些程序。你可以在架构中动态配置不被复制到RODC的域对象的属性集。这个属性集被称为RODC已筛

选属性集。在RODC已筛选属性集定义的属性不允许复制到森林内的任何一台RODC。 威胁到RODC的恶意用户能够以某种途径尝试配置RODC，并尝试将RODC已筛选属性集中定义的属性复制到其它域控制器。如果RODC尝试从一台安装Windows Server 2008的域控制器上复制这些属性，那么复制请求将被拒绝。然而，如果RODC尝试从一台安装Windows Server 2003的域控制器上复制这些属性，复制请求将被接受。因此，作为安全性的预防措施，如果你想配置RODC已筛选属性集请确保森林的功能级是Windows Server 2008。如果森林的功能级是Windows Server 2008，那么收到威胁的RODC将不能被如此利用，因为运行Windows Server 2003的域控制器在森林中是不被允许的。 你无法添加系统关键属性到RODC已筛选属性集。判断是否是系统关键属性的依据是看以下服务能否正常工作，这样的服务有 AD DS、LSA、SAM（及SSPIs比如Kerberos）在Windows Server 2008 Beta3的后继版本中，系统关键属性拥有属性值等于1的schemaFlagsEx属性。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com