活动目录在WindowsServer2008中的改进：颗粒化密码策略

 Windows Server 2008 为组织提供了一种方法，使得组织能在某一域中针对不同的用户集来定义不同的密码和账号锁定策略。在Windows 2000及Windows Server 2003的活动目录域中，只有一种密码和账户锁定策略能被应用到域中的所有用户。这些策略被定义在默认的域策略中。因此，希望针对不同的用户集采取不同的密码及账户锁定组织不得不建立密码策略筛选器或者部署多个域。这些选择会因为不同的原因而照成高昂的代价。 颗粒化的密码策略能干什么？ 你能够使用颗粒化的密码策略在同一个域内指定多样化的密码策略。你能够使用颗粒化的密码策略对同一域内的不同用户集应用不同的密码和账号锁定策略限制。 举例来说，你能够针对特权账号使用严密的设定，而对其它用户使用不太严密的设定。在其他场景中，比如你希望对密码与其它数据源同步的账号应用特殊的策略。 还有其它要特别考虑的吗？ 颗粒化的密码策略值应用于用户对象（或者用来替代用户对象的inetOrgPerson对象）以及全局安全组。在默认情况下，只有Domain Admins组的成员才能设置本策略。然而，你也能够委派其他用户来设置此策略。但是域功能级必须是Windows Server 2008。 颗粒化的密码策略不能被直接应用到OU。但是为了达到此目的，你可以使用影子组。 影子组实质上是全局安全组，在逻辑上被映射到OU，用来强化颗粒化密码策略。你向OU添加用户就好像向影子组添加成员一样，随后将颗粒化密码策略应用到影子组。你

能够根据你的需要为其它OU创建偶外的影子组。如果你从一个OU向另一个OU移动用户，那么你必须将账户组成员属性更新到对应的影子组。 颗粒化的密码策略不受你必须在同一域中应用的自定义的密码策略筛选器的影响。将自定义的密码策略筛选器部署到使用Windows 2000 or Windows Server 2003作为域控制器的组织，能够继续使用这些筛选器来强化额外的密码限制。 这项特性提供了什么新功能？ 储存颗粒化密码策略 为了储存颗粒化密码策略，Windows Server 2008在AD DS架构中包含了两个新的对象类： 密码设置容器（Password Settings Container） 密码设置（Password Settings） 密码设置容器默认被创建在域的系统容器下。你能够通过使用活动目录用户与计算并启用高级特性来查看。它为域储存了密码设置对象（Password Settings objects 一下简称PSOs）。 你不能够重命名，移动，或者删除这个容器。尽管你能够创建额外的自定义的密码设置容器，他们不被针对一个对象计算的组策略结果集计算在内。因此创建额外的自定义的密码设置容器不被推荐。 密码设置对像包含了能在默认域策略中定义的所有属性设置（除了Kerberos设置）。这些设置包含了以下密码设置属性： 强制密码历史 密码最长使用期限 密码最短使用期限 密码长度最小值 密码必须符合复杂性要求 用可还原的加密来储存密码 这些设定也包含了以下的账户锁定设置 账户锁定时间 账户锁定阈值 复位账户锁定计数器 另外，PSO也包含了以下两个新属性： PSO链接：这是链接到用户或者组对象的多值属性 优先：这是一个用来解决多个PSO被应用到一个单个用户或组对象产生冲突的整数值 这九个属性值必须被定义，缺一不可。来自多个PSO的设置不能被合并。 定义颗粒化密

码策略的范围 PSO能够被链接到和PSO在同一域中的用户（或者inetOrgPerson）或者组对象。 PSO包含了描述PSO正向链接的属性值，msDS-PSOApplies。msDS-PSOApplies是一个多值属性。因此你能够将一个PSO链接到多个用户或组。 称为msDS-PSOApplied的新属性值在2008中被添加到用户和组对象。这个属性包含了PSO的反向链接。因为msDS-PSOApplied属性有反向链接，因此一个用户或组可以被多个PSO应用。 你能够将PSO链接除了全局安全组之外的其它类型的组。 使用图形界面（adsiedit.msc）建立PSO 1. 单击开始按钮，单击运行，输入 adsiedit.msc ，单击确定 *如果你是在DC上第一次运行adsiedit.msc，请继续看第二步，不是的话跳到第四步。 2. 在ADSI EDIT界面中，右击ADSI Edit，再单击连接到 3. 在Name属性框中输入你想要创建PSO的域的完全合格域名（FQDN），然后单击确定 4. 双击域 5. 双击DC= 6. 双击CN=System 7. 双击密码设置 8. 右击 CN=Password Settings Container，单击新建，再单击对象 9. 在建立对象对话框中，选择msDS-PasswordSettings，单击下一步 10. 输入PSO的名称，单击下一步 11. 根据向导，输入必备属性 msDS-PasswordReversibleEncryptionEnabled 属性名称 描述 例值 msDS-PasswordSettingsPrecedence 密码设置优先级 10 msDS-PasswordReversibleEncryptionEnabled 用可还原的加密来储存密码 FALSE msDS-PasswordHistoryLength 历史密码长度 24 msDS-PasswordComplexityEnabled 用户密码复杂程度 TRUE msDS-MinimumPasswordLength 用户密码长度最小值 8 msDS-MinimumPasswordAge 密码最短使用期限 (只允许负值，计算方法见文末) -864000000000 (1 day)

msDS-MaximumPasswordAge 密码最长使用期限 (只允许负值，计算方法见文末) -172800000000000 (20 days) msDS-LockoutThreshold 账户锁定阈值 0 msDS-LockoutObservationWindow 复位账户锁定计数器的时间 (只允许负值，计算方法见文末) -18000000000 (30 minutes) msDS-LockoutDuration 账户锁定时间 (只允许负值，计算方法见文末) -18000000000 (30 minutes) msDS-PSOAppliesTo PSO被应用到(正向连接) CN=u1,CN=Users, 12. 在向导的最后一页，单击更多属性 13. 在选择查看何种属性菜单中，单击可选或者两者 14. 在选择一种属性进行查看的下拉菜单中，选择msDS-PSOAppliesTo 15. 在编辑属性中，添加需要应用PSO的用户和全局安全组的相对可分辨名称 16. 重复第15步，如果你需要将PSO应用到多个用户和全局安全组 17. 单击完成 附：某些涉及时间属性值的确定 时间单位 运算方法 m minutes -60*(10^7) = - 600000000 h hours -60*60* (10^7) = -36000000000 d days -24*60*60*(10^7) = -864000000000 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