微软认证:安全观察Windows域密码策略Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/590/2021_2022__E5_BE_AE_E8_BD_AF_E8_AE_A4_E8_c100_590115.htm 如果您是 Windows 域的管理员，一定会非常清楚域用户帐户的密码策略的相关限制。但随着WindowsServer2008的到来，其中一些限制将不复存在。让我们来看看这个新操作系统将如何解决这样一个问题：不能实现多个密码策略。 如果您运行的是 Windows? 域当前的任意版本(Windows NT? 、Windows2000ActiveDirectory?或 WindowsServer?2003ActiveDirectory)，就会受到每个域只能有一个密码策略的限制。事实上，对您产生限制的不仅是密码策略，而且还有帐户策略涵盖的范围更广的设置。 Figure 1 Account policies 密码策略 强制密码历史 密码最长使用期限 密码最短使用期限 最短密码长度 密码必须满足复杂性要求 使用可逆加密存储密码 帐户锁定策略 帐户锁定时间 帐户锁定域值 重置帐户锁定计数器之前经过的时间... Kerberos 策略 强制用户登录限制 服务票证最长寿命 用户票证最长寿命 用户票证续订最长寿命 计算机时钟同步的最大容差 默认情况下，这些策略设置适用于与域相关联的所有域帐户和用户帐户。这是因为组策略是沿着ActiveDirectory结构向下继承的。为了更好地认识这些策略如何影响域帐户和本地用户帐户，了解以下两点非常重要：这些策略的设置位置，以及组策略的继承方式如何影响所有不同的用户帐户。(请注意，Kerberos策略设置仅适用于域用户帐户，这是因为只有域用户帐户使用Kerberos进行身份验证。本地用户帐户使用NTLMv2、NTLM 或LM 进

行身份验证。) 设置帐户策略 在 Active Directory内部，组策略建立并控制整个域的帐户策略。这是在首次安装ActiveDirectory域时发生的，并且是通过获得链接到 ActiveDirectory 中域节点的默认组策略对象 (GPO)完成的。此GPO名为默认域策略，具有帐户策略的所有三部分的默认配置。图 2显示了 WindowsServer2003域中密码策略项初始设置的完整列表。 Figure 2 Default password policies for WindowsServer2003domain(单击该图像获得较大视图) 此GPO中的设置控制所有域用户帐户以及每台域计算机的帐户策略。请记住，所有域计算机(台式机和服务器)都具有本地安全帐户管理器(SAM)，这很重要。此默认GPO中的设置控制的就是这一SAM。当然，本地 SAM 也包含每台计算机的本地用户帐户。 通过 GPO 沿着 ActiveDirectory结构向下进行的正常继承，默认域策略中的设置可影响所有域计算机。由于此GPO链接到域节点，所以它将影响此域中的所有计算机帐户。 无法对当前密码策略执行的操作 关于 Active Directory(在WindowsServer2003中)的当前实现，目前仍存在对密码控制的许多误解，尽管经过了多年的严格测试，也未找到证据证明那些误解是对的。很明显(或应该说)，策略是无法通过设计以外的其他方式起作用的。 也就是说，很多管理员都相信，可以为同一域中的多个用户设置多个密码策略。他们认为您可以创建一个GPO，并将其链接到某个组织单位(OU)。该思想是将用户帐户移到OU以使GPO影响这些对象。在GPO内部，对帐户策略进行修改以创建更安全的密码策略(可能是通过将最大密码长度设置为14实现此目的)。但是，由于一些原因，此配置永远达不到期望的结果。首先，密码策略设置是

基于计算机而非基于用户的策略。有了这种设置的前提条件之后，设置将永远无法影响用户帐户。其次，修改域用户帐户的帐户策略设置只有一种方法，即在链接到该域的GPO内部进行修改。链接到OU且被配置为更改帐户策略设置的那些GPO，会修改驻留在 OU 中(或在链接的 OU 的子OU中)计算机的本地 SAM。 另一个误解是，在根域(ActiveDirectory林的初始域)中建立的帐户策略设置将向下流动或继承到林中的子域。这同样并非事实，通过这种方式是无法使设置起作用的。链接到域和某个域中OU的GPO不会影响其他域中的对象，即使 GPO 链接到的域是根域也是一样。使 GPO 设置影响其他域中对象的唯一方法是将GPO链接到ActiveDirectory 站点。密码策略的改变 可以看到，Windows的当前版本处理用户帐户密码的方式简单直观。这包括一组适用于所有域帐户的密码规则，以及通过链接到 ActiveDirectory中域节点的组策略对象来管理帐户策略的方式。随着Windows Server2008的到来，这一切就都被判出局了。 Windows Server 2008 以及一同推出的ActiveDirectory基础结构采用了另一种方法。将帐户策略置于GPO中只允许对所有域用户帐户设置一种策略，而现在已将这些设置移到了ActiveDirectory的更深部分。此外，帐户策略也不再基于计算机帐户。现在，您可以让个人用户和用户组来控制其密码限制。对于 Windows管理员来说，这是一个全新的概念，毕竟我们长期以来一直在处理计算机帐户的帐户策略。 Windows Server 2008 中的帐户策略 在 Windows Server2008中，无需使用默认域策略建立帐户策略。实际上，您根本不会使用GPO为域用户帐户创建帐户策略。在 Windows Server2008中，会将您带到 ActiveDirectory数据库中

进行修改。具体来说，您将使用一个类似于 ADSIEdit的工具来修改ActiveDirectory对象及其关联的属性。 进行此更改的原因是组策略并非针对同一域中的多个密码而设计。

在WindowsServer2008中，每个域实现多个密码的功能非常棒，但并非每个人都觉得该功能使用起来很方便。不过，随着时间的推移，用于配置设置的界面将越来越易于访问。现在，您需要采用ActiveDirectory数据库设置工具对系统进行更改。 如果您倾向于使用其他方法来修改帐户策略设置，则不必使用ADSIEdit。您可以使用能够访问ActiveDirectory数据库的任何其他 LDAP 编辑工具，甚至可以使用脚本。

在WindowsServer2008中实现密码策略后，就需要使用与过去截然不同的方法了。使用新功能意味着您需要考虑哪些用户和组要接受哪些密码设置。 您不但要考虑密码长度，还要考虑密码策略设置附带的其他一些限制，包括最短和最长使用期限、历史等。其他注意事项包括如何控制用户锁定策略设置和Kerberos设置。当前的帐户策略设置与在WindowsServer 2008中的ActiveDirectory数据库中配置的帐户策略设置存在一对一关系。但请注意，既然这些策略设置已是ActiveDirectory对象和属性，那么每个策略设置的名称也会与以前不同，这很重要。 要实现新密码设置，必须在密码设置容器下创建一个名为msDS-PasswordSettings的密码设置对象(PSO)，该容器的LDAP 路径为

“ cn=PasswordSettings,cn=System,dc=domainname,dc=com ”。请注意，所用域的域功能级别必须设置为WindowsServer2008。在此新对象下，您需要填写若干属性信息，如图3 所示。

Figure 3 Password attributes in Active Directory Active Directory 属

性名属性描述 msDS-PasswordSettingsPrecedence当同一用户在使用不同密码策略的多个组中具有成员资格时，建立优先次序。 msDS-PasswordReversibleEncryptionEnabled在是否启用可逆加密之间切换。 msDS-PasswordHistoryLength确定中间必须隔有多少个不重复的密码后，才能重用某个密码。 msDS-PasswordComplexityEnabled确定密码要求使用的字符数目和字符类型。 msDS-MinimumPasswordLength确定最短密码长度。 msDS-MinimumPasswordAge确定用户密码最短使用多久后才可更改。 msDS-MaximumPasswordAge确定密码最长使用多久后会要求用户更改密码。 msDS-LockoutThreshold确定锁定用户帐户前允许的密码尝试失败次数。 msDS-LockoutObservationWindow确定密码计数器出现错误后多长时间进行重置。 msDS-LockoutDuration确定密码尝试失败次数过多导致帐户锁定后，帐户的锁定时长。 可以看到，与帐户策略设置相关的所有组策略设置都会作为属性复制。请注意，还存在一个优先设置.这对于在同一域中实现多个密码至关重要，这是因为必然会产生一些冲突，需要有处理这些冲突的机制。 目标帐户策略设置 对于创建的每个对象，都需要填写所有的属性才能针对每位用户创建帐户策略。这里有个新属性msDS-PSOAppliesTo，用于确定哪些对象将接收这组策略设置。这是关键属性，通过它可以将特定设置分配给特定用户。此属性下的列表可以是用户也可以是组，但对于建立访问控制列表的情形而言，则最好使用组，而不是用户。因为组更稳定，更容易找到，而且处理起来通常容易得多。 起立欢呼 数年来，我们一直希望能够在同一ActiveDirectory域中使用多个密码，现在终于实现了。从密

码的角度而言，整个域中的每一个用户都处于同一安全级别的情形已经一去不复返了。例如，现在您能够为普通用户设置8个字符的密码，而为IT专业人员(可能具有管理员权限)设置复杂一些的 14 个字符的密码。 要想习惯使用ActiveDirectory数据库建立或修改帐户策略设置，会花费一些时间。但值得庆幸的是，新设置仿效了您熟悉的设置。当您开始使用WindowsServer2008后，请务必立即研究这些新设置，因为这些肯定是属于您首先完成的配置。 