全面解析Windows密码安全问题计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022__E5_85_A8_E9_9D_A2_E8_A7_A3_E6_c98_645028.htm Windows默认密码 当你试图登录到Active Directory域的时候，你将需要输入三项内容：用户名、密码和域名。 当域控制器收到这些信息后，会根据列在Active Directory数据库的用户名和密码对信息进行分析。如果密码是相符合的，那么域控制器就会通过验证用户，然后为用户提供验证令牌以获取访问网络/域中其他资源的访问权。 当用户试图更改其帐户密码时，这种信息也会被发送至域控制器。当用户输入新密码并将新密码发送至域控制器时，会有相应的政策来确保密码符合最低安全标准。以下是一些基本的密码政策(针对域和所有本地用户帐户的)：Windows 密码(Windows Server 2003域或者更高版本)要求至少有7个字符长度 密码必须包含以下四种类型字符中的三种字符类型：大写字母、小写字母、数字、特殊符号。 新密码必须在42天前生成的，以保持帐户的有效性。 在创建24个独特密码前，密码不可以重复使用。 所有这些设置都是在GPO的电脑配置部分进行设置的，位于密码政策列表下。图1显示的是如何设置这些密码政策。 什么在控制着域密码政策? 尽管距离微软公司首次发布Active Directory已经过去9年了，很多IT专业人士仍然搞不清楚密码政策是如何被控制的以及如何修改这些政策等问题，下面是关于Windows 密码政策和功能的一些事实： 首先，Default Domain Policy GPO(默认域政策GPO)控制着整个域中所有计算机的密码政策，这包括域控制器、服务器和整个Active Directory的桌面(已经加入域中)

。Default Domain Policy是与域节点相关的，这当然包括域中的所有计算机。 其次，任何连接到域的GPO都可以用于建立和控制密码政策设置，GPO在域级别拥有最高优先权，这使其在任何与密码政策设置相冲突的设置中都能起决定作用。第三，如果GPO连接到组织单位(OU)，它将不能控制位于OU内的用户帐户。这是目前IT专业人士最常犯的错误。密码政策设置不是基于用户的，而是基于计算机的，正如图1所示。 第四，如果GPO链接到OU，GPO中创建的密码政策设置将会影响位于OU的任何计算机上的本地SAM，这将使链接到该域的GPO中配置的密码政策设置发挥主导作用，但是仅限于存储在这些计算机的本地SAM的本地用户帐户。 第五，如果GPO链接到默认域控制器OU，它将不会控制存储在域控制器的用户Active Directory数据库。修改域用户帐户的密码政策设置的唯一途径位于链接到该域的GPO内。 第六，大多数现有的Windows Active Directory企业版都支持LanManager(LM)功能，LM是一个非常旧的验证协议，不太能保证密码和生成的密码hash(用于支持该协议的验证)的安全性，有两种GPO设置(实际上是注册表设置)可以控制是否支持LM以及是否存储LM hash，这将在接下来的文章中进行探讨。 总结 Active Directory域的默认密码政策设置并不可怕，不过仍然需要改进。默认设置是最初设置的，并被保存在默认域政策GPO中，而这是与域节点相连的。对于 windows 2000和Server 2003域而言，只能有一个密码政策，这意味着所有的用户(IT人员、开发人员、管理人员、人力资源等)都拥有相同的密码政策控制，这是非常不安全的。可以通过链接到OU(这些计算机帐户位于AD中)的GPO对服务器和桌面的本地SAM进行修改，

这些GPO设置只能控制本地用户帐户，而不是域用户帐户。LM是一种旧的不安全的验证协议，尽可能禁用这种协议。下文中我们将讨论密码攻击以及预防攻击等问题。 编辑特别推荐: windows自带记事本实用技巧 快速处理Word表格的实用技巧 躲避老板教你用Excel来聊天 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