

安全观察Windows域密码策略Microsoft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\\_ti2020/644/2021\\_2022\\_\\_E5\\_AE\\_89\\_E5\\_85\\_A8\\_E8\\_A7\\_82\\_E5\\_c100\\_644597.htm](https://www.100test.com/kao_ti2020/644/2021_2022__E5_AE_89_E5_85_A8_E8_A7_82_E5_c100_644597.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 Windows Server 2008 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、

Windows 2000 Active Directory 或

Windows Server 2003 Active Directory)，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。图 1 显示了这些策略和设置。

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 Active Directory 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。) 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](http://www.100test.com)