Windows 2003 下密码策略设置和密码创建

密码对于服务器的安全是个很重要的部分，设置安全的密码策略和符合复杂度的密码是服务器安全保障的重要组成部分。在 Windows Server 2003 系统的“帐户和本地策略”中包括“帐户策略”和“本地策略”两个方面，而其中的“帐户策略”又包括：密码策略、帐户锁定策略和 Kerberos 策略三个方面，下面我们重点介绍“密码策略”的设置。

一、密码策略的设置

密码策略作用于域帐户或本地帐户，其中就包含以下几个方面：

1、密码必须符合复杂性要求

2、密码长度最小值

3、密码最长使用期限

4、密码最短使用期限

5、强制密码历史

6、用可还原的加密来存储密码

以上各项的配置方法均需根据当前用户帐户类型来选择。下面分别根据几种不同用户类型介绍相应的密码策略配置方法。下面介绍在本地计算机上配置以上密码安全策略选项的方法。对于本地计算机的用户帐户，其密码策略设置是在“本地安全设置”管理工个中进行的。下面是具体的配置方法。

第 1 步，执行【开始】→【管理工具】→【本地安全策略】菜单操作，打开“本地安全设置”界面。对于本地计算机中用户“帐户和本地策略”都查在此管理工具中进行配置的（如图 1）。

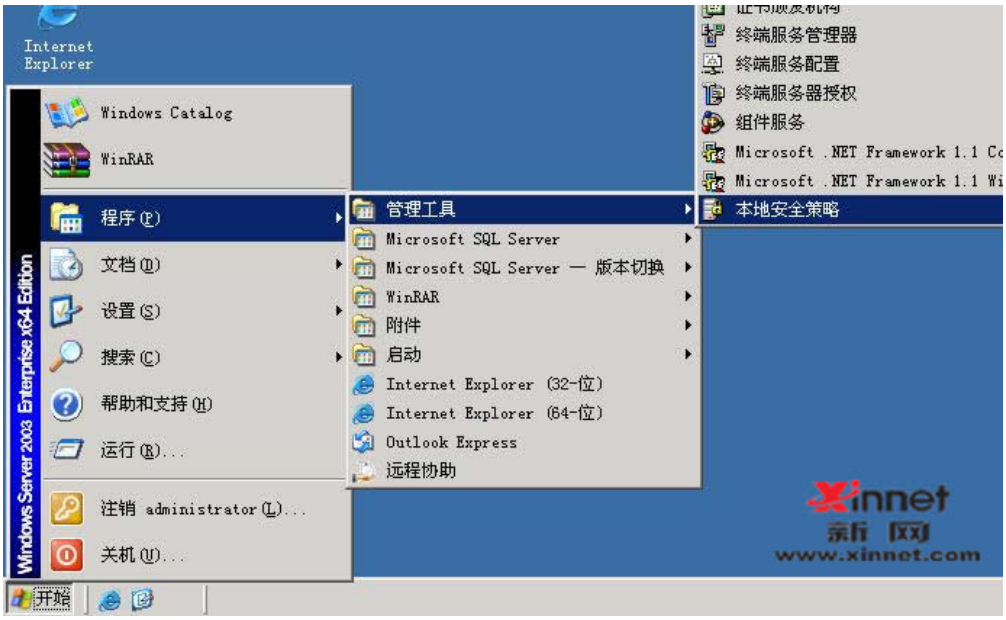

图 1

第 2 步，因密码策略是属于用户策略范畴，所以需单击选择【账户策略】选项，然后再选择【密码策略】选项，在右边详细信息窗口中将显示可配置的密码策略选项的当前配置（如图 2）。

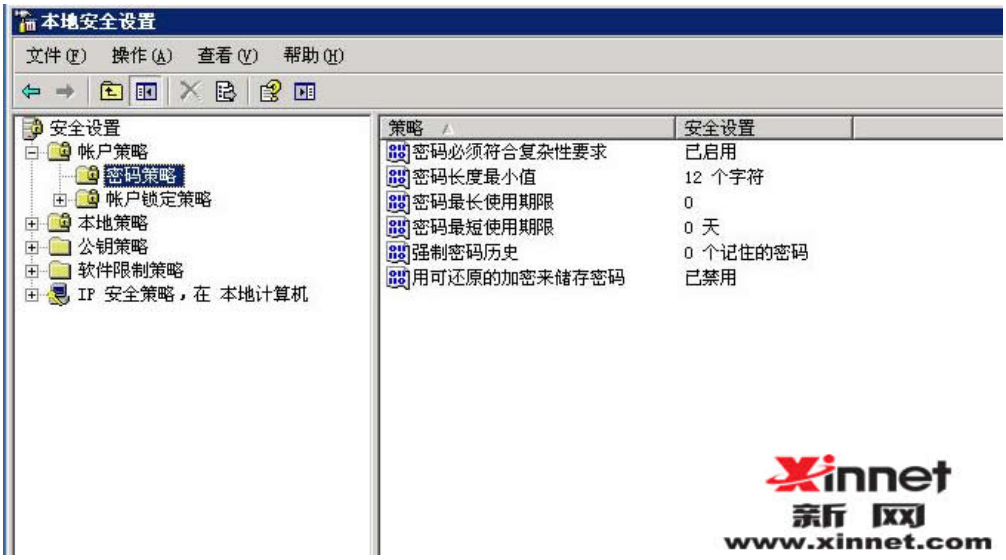

图 2

1、密码必须符合复杂性要求。

此安全设置确定密码是否必须符合复杂性要求，在更改或创建密码时执行复杂性要求。如果启用此策略，密码必须符合下列最低要求:

（1）不能包含用户的帐户名，不能包含用户姓名中超过两个连续字符的部分

（2）至少有六个字符长

（3）包含以下四类字符中的三类字符:

- 英文大写字母(A 到 Z)
- 英文小写字母(a 到 z)
- 10 个基本数字(0 到 9)
- 非字母字符(例如 !、$、#、%)

如果启用了此安全策略，而您所配置的用户密码不符合此配置要求时系统会提示错误。有时您可能百思不得其解，认为自己所设的密码已经够长，而且也是属于随机的，不全都是数字或字母，可系统为什么还是老说错误呢？一般来说是由于您所设的密码所包括的字符类型不足以上四个中的三个。通常只各个领域其中的两种，即数字和字母，而没有考虑到字母的大小写或者非字母字符，所以达不到复杂性要求。更改或创建密码时，会强制执行复杂性要求。默认情况下，在独立服务器上则默认是禁用的。

这个安全选项的配置方法是双击【密码必须符合复杂性要求】选项打开对话框。在这个对话框中就可随意启用或者禁用这个安全策略选项，配置好后单击【确定】按钮使配置更改生效（如图 3）。

图 3

2、密码长度最小值

该安全设置确定用户帐户的密码可以包含的最少字符个数。可以设置为 1 到 14 个字符之间的某个值，或者通过将字符数设置为 0，以确定不需要密码。在独立服务器上默认为 0。

这个安全选项的配置方法是双击【密码长度最小值】选项打开对话框。在这个对话框中就可随意选择 0~14 数字，配置好后单击【确定】按钮使配置更改生效（如图 4）。

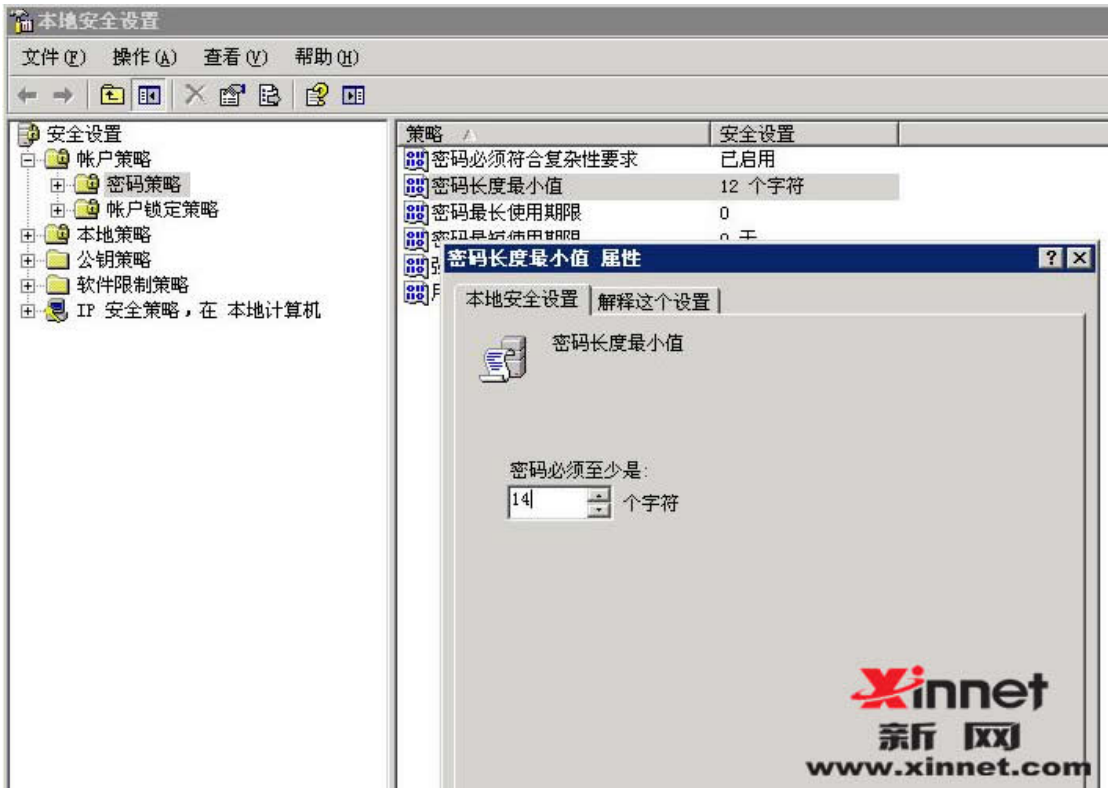

图 4

3、密码最长使用期限

此安全设置确定在系统要求用户更改某个密码之前可以使用该密码的期间(以天为

单位)。可以将密码设置为在某些天数(介于 1 到 999 之间)后到期，或者将天数设置为 0，指定密码永不过期。如果密码最长使用期限介于 1 和 999 天之间，密码最短使用期限必须小于密码最长使用期限。如果将密码最长使用期限设置为 0，则可以将密码最短使用期限设置为介于 0 和 998 天之间的任何值。

注意: 安全最佳操作是将密码设置为 30 到 90 天后过期，具体取决于您的环境。这样，攻击者用来破解用户密码以及访问网络资源的时间将受到限制。默认值: 42。

这个安全选项的配置方法是双击【密码最长使用期限】选项打开对话框。在这个对话框中就可随意输入 0~998 中的数字，配置好后单击【确定】按钮使配置更改生效（如图 5）。

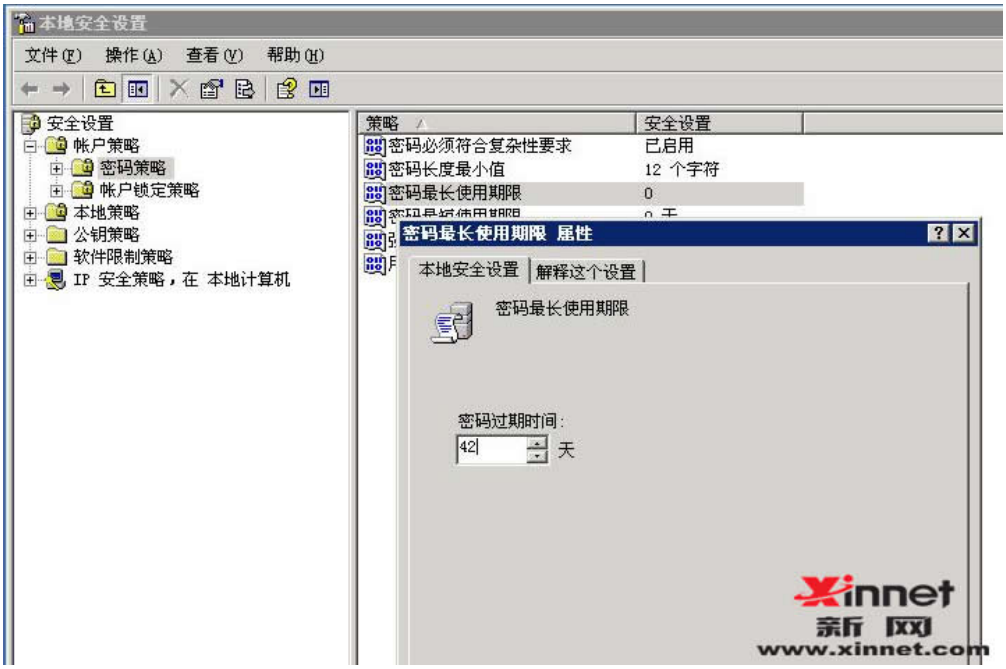

图 5

4、密码最短使用期限

此安全设置确定在用户更改某个密码之前必须使用该密码一段时间(以天为单位)。可以设置一个介于 1 和 998 天之间的值，或者将天数设置为 0，允许立即更改密码。

密码最短使用期限必须小于密码最长使用期限，除非将密码最长使用期限设置为 0，指明密码永不过期。如果将密码最长使用期限设置为 0，则可以将密码最短使用期限设置为介于 0 和 998 之间的任何值。默认情况下，在独立服务器上设置为 0。

如果希望“强制密码历史”有效，则需要将密码最短使用期限设置为大于 0 的值。如果没有设置密码最短使用期限，用户则可以循环选择密码，直到获得期望的旧密码。默认设置没有遵从此建议，以便管理员能够为用户指定密码，然后要求用户在登录时更改管理员定义的密码。如果将密码历史设置为 0，用户将不必选择新密码。因此，默认情况下将“强制密码历史”设置为 1。

这个安全选项的配置方法是双击【密码最短使用期限】选项打开对话框。在这个对话框中就可随意输入 0~998 中的数字，配置好后单击【确定】按钮使配置更改生效（如图 6）。

图 6

5、强制密码历史

此安全设置确定再次使用某个旧密码之前必须与某个用户帐户关联的唯一新密码数。该值必须介于 0 个和 24 个密码之间。

此策略使管理员能够通过确保旧密码不被连续重新使用来增强安全性。独立服务器默认情况下为 0 成员计算机沿用各自域控制器的配置。

若要维护密码历史的有效性，还要同时启用密码最短使用期限安全策略设置，不允许在密码更改之后立即再次更改密码。有关密码最短使用期限安全策略设置的信息，请参阅“密码最短使用期限”。

这个安全选项的配置方法是双击【强制密码历史】选项打开对话框。在这个对话框中就可随意输入 0~24 中的数字，配置好后单击【确定】按钮使配置更改生效（如图 7）。

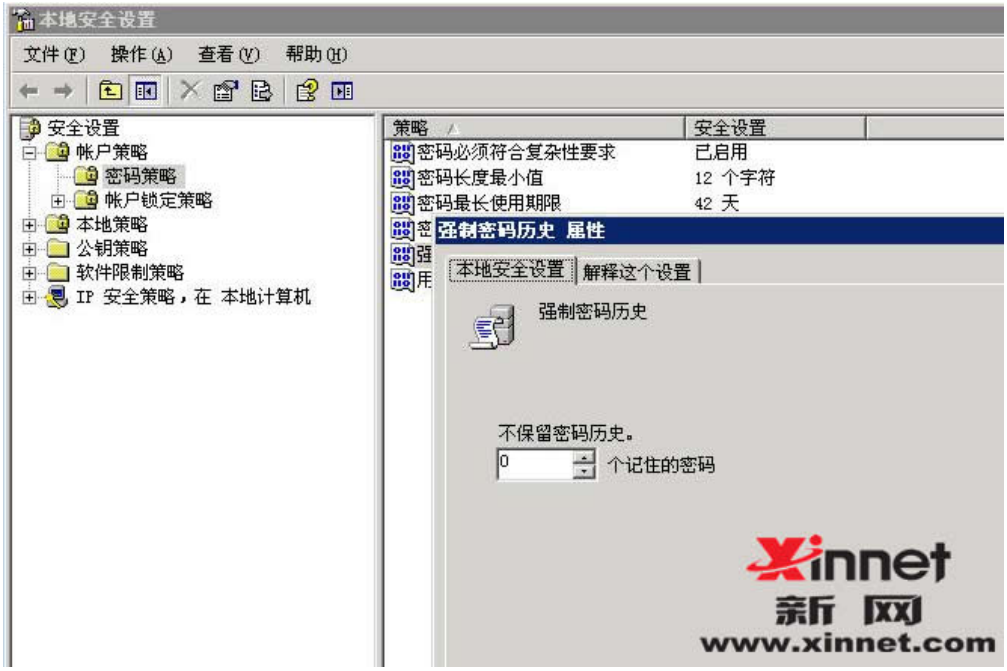

图 7

6、用可还原的加密来储存密码

使用此安全设置确定操作系统是否使用可还原的加密来储存密码。

此策略为某些应用程序提供支持，这些应用程序使用的协议需要用户密码来进行身份验证。使用可还原的加密储存密码与储存纯文本密码在本质上是相同的。因此，除非应用程序需求比保护密码信息更重要，否则绝不要启用此策略。系统默认设置为“禁用”。

通过远程访问或 Internet 身份验证服务(IAS)使用质询握手身份验证协议(CHAP)验证时需要设置此策略。在 Internet 信息服务(IIS)中使用摘要式身份验证时也需要设置此策略。

这个安全选项的配置方法是双击【用可还原的加密来储存密码】选项打开对话框。在这个对话框中就可随意输入 0~24 中的数字，配置好后单击【确定】按钮使配置更改生效（如图 8）。

图 8

二、密码设置和修改

上面介绍的是在本地计算机上配置以上密码安全策略选项的方法，下面介绍本地计算机密码的配置方法。创建密码和修改密码方法相同，在此只介绍

第 1 步，右键单击【我的电脑】然后选择【管理】（如图 9）。

图 9

第 2 步，打开“计算机管理”对话框后，选择左侧【本地用户和组】选项，点击【用户】选项（如图 10）。

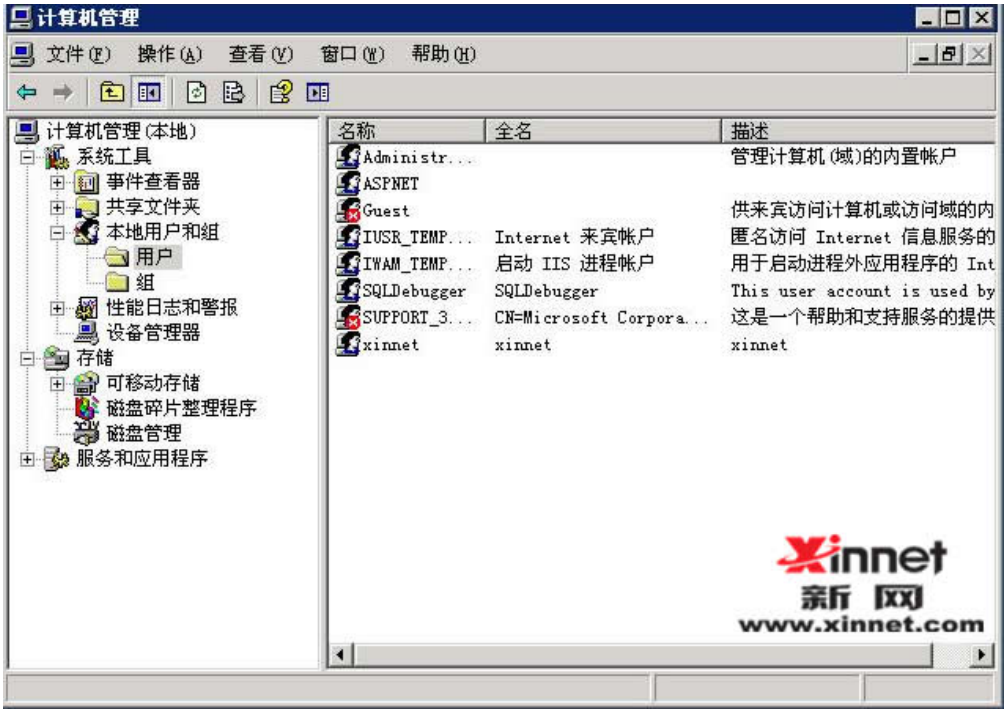

图 10

第 3 步，找到“Administrator”用户并右键单击【Administrator】用户，然后选择【设置密码】（如图 11）。

图 11

第 4 步，出现设置对话框后点击【继续】选项，然后在密码设置对话框中输入新的密码，然后点击【确定】密码创建完毕（如图 12）。

图 12

修改密码方法和创建密码方法相同，故在此不过多赘述。

三、注意事项

1、请在得到服务器开通信后及时登陆服务器修改密码策略和密码；

2、建议使用密码复杂性要求，来提高服务器的安全度；

3、主机租用、托管和 VPS 服务器用户都可以进行密码策略的设置；

4、如果用户使用 VPS 服务器，服务器密码修改的同时控制面板的密码也随之修改。