说明

因为CIS Benchamrk中的条目太多，所以有必要单开一页来记录 Benchmark的基准OS版本是Windows 11 23H2 而我的VMware中的虚拟机服务器则是Window Server 2022. 共有19章节，一一列举如下。

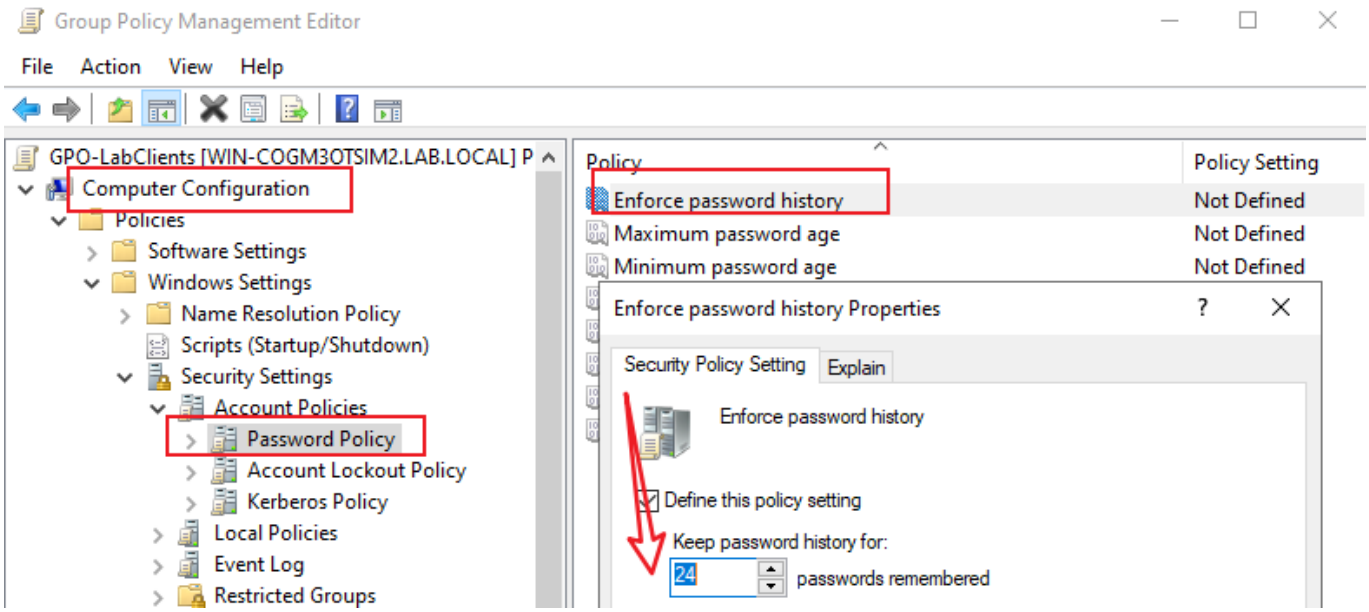
1.Account Policies

1.1 Password Policy

1.1.1 Ensure 'Enforce password history' is set to '24 or more password(s)

微软对于Win11系统的最长密码记录就是24世代。当用户长时间使用同一密码，攻击者使用暴力破解获取密码的可能性就越大。如果公司要求员工定期进行密码更换，但却未禁止用户复用密码，则定期变更密码的效果会大打折扣。 而且用户会倾向于设置新密码为增量形式，比如password01,password02,易记但容易被猜到。 **设置方法**

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history
```



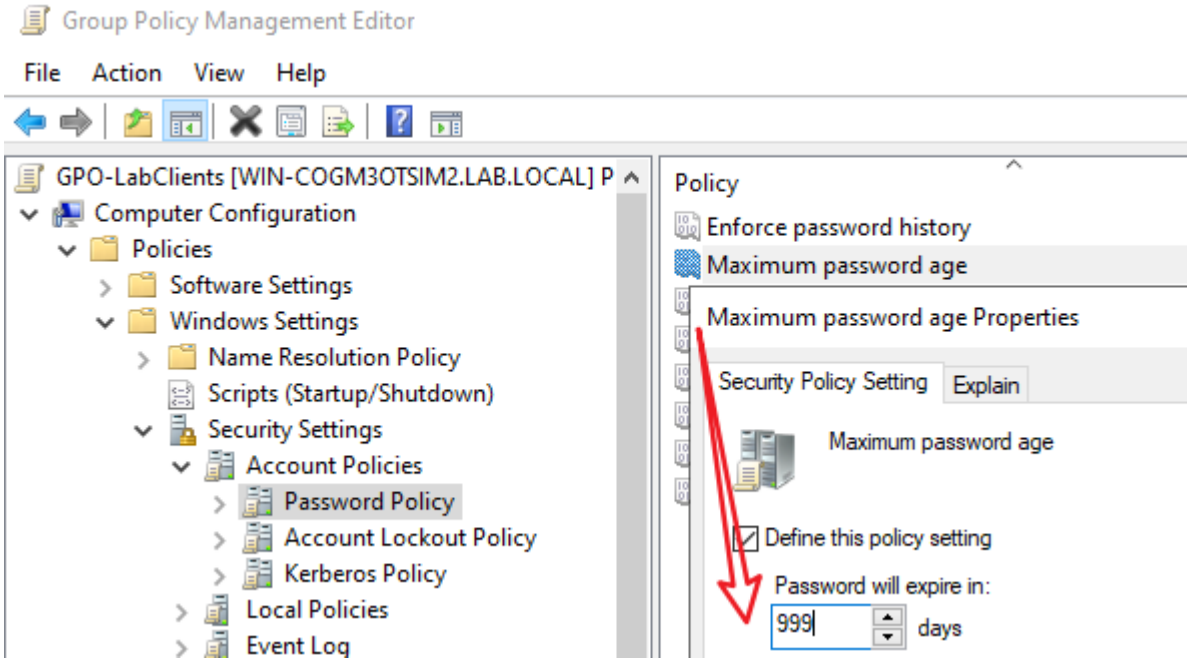
1.1.2 Ensure 'Maximum password age' is set to '365 or fewer days, but not 0

这个用于设置每一个密码可以用多久。如果设置为0，则密码永不过期。在1.1 Password Policy的设置和1.2 Account Lockout Policy的设置必须在**Default Domain Policy**中的GPO里修改，以对全Domain生效。如果是在其他GPO里修改，则只影响该GPO对应的用户账户或计算机。当然，添加其他Password Policy到特定用户或用户组也是OK的，一般是通过Active Directory Administrative Center. 参考期限 60Days

目前美国NISC已经提倡不需要定期修改密码，而是应该提高密码的复杂度以降低被攻破的风险。现在的最佳实践(BestPractice)是只在确认密码已泄露的情况下，强制要求用户修改密码。

设置方法

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age
```

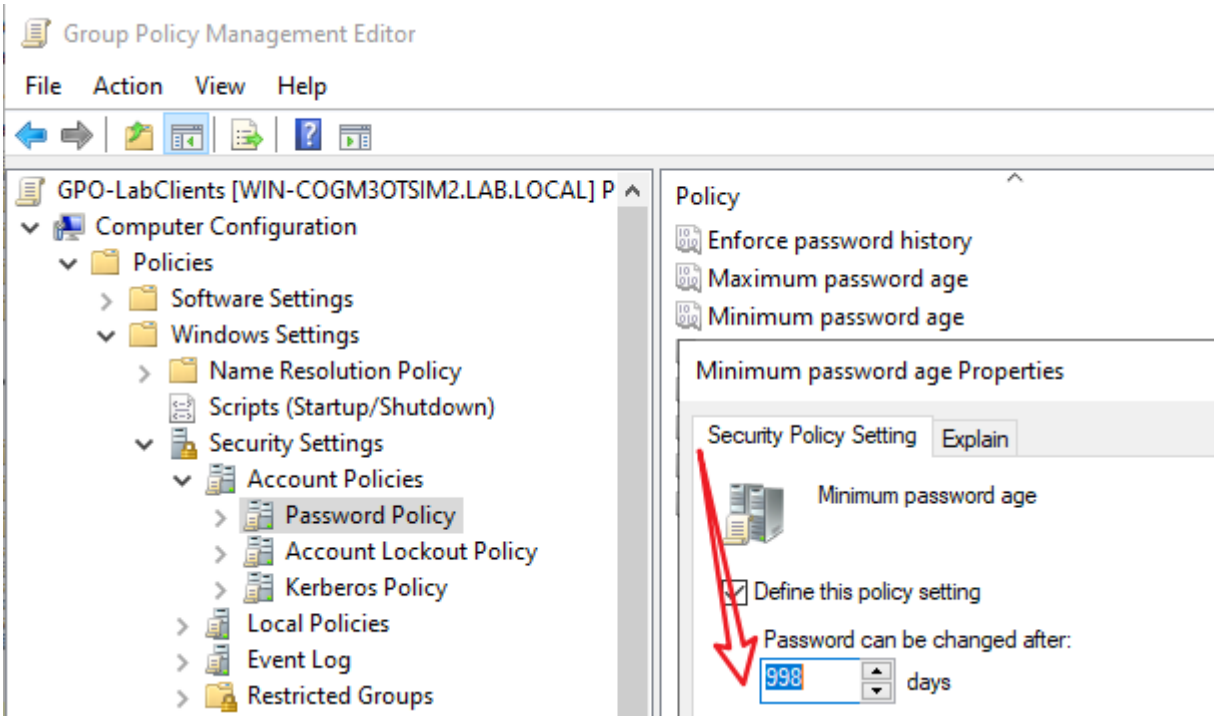


Max的设置范围是1-999天，Mix的设置范围是0-998天。

1.1.3 Ensure 'Minimum password age' is set to '1 or more day(s)

同上，设置的是最小值，默认是1天。

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age
```



设置方法

###1.1.4 Ensure 'Minimum password length' is set to '14 or more character(s) 在Windows Server2016版或之前GPO不允许将最短密码长度设为≥ 14,但是在2019版之后，微软允许将最小密码长度设置为20. 长密码可以降低风险，因为密码如果多次输错会导致账户被锁定。（用户自己多次输错则会增加Helpdesk的负担，即重置密码等 ###1.1.5 Ensure 'Password must meet complexity requirements' is set to 'Enabled' 确保密码满足复杂度要求Enabled之后，则密码必须符合以下要求：

- 不包含用户名或全名中的2个连续或以上字符
- 密码长度为6或以上
- 包含至少3种类型的字符（大小写字母A-Za-z,数字0-9以及特殊符号），或是其他Unicode字符

要知道，每增加一个字符，密码的复杂度就会呈指数级增长。 而且要对全体用户生效，必须在Default Domain Policy中设置。



特别地，我们还可以自定义密码复杂度要求，具体方法为设置Passfilt.dll文件，比如要求使用Shift+1~0字符，或是使用Alt+0128-0159的字符

设置方法 Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements ###1.1.6 Ensure 'Relax minimum password length limits' is set to 'Enabled' 是否允许最小密码长度值被发动，这一设置只会影响Local Account与Domain accounts无关。 **设置方法** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Relax minimum password length limits

From:
https://trident365.com/ - **三叉戟**

Permanent link:
https://trident365.com/doku.php?id=resources:os:windows_11:baseline

Last update: **2024/11/18 23:41**