我们都知道，组策略能给我们对域内计算机和用户管理带来不可估量的好处，通过前面三次课，我们基本上对组策略有了大致的认识，在这里我总结了**组策略的20条使用规则**，相信各位应用组策略之后，读过一定会给你带来不小的收获。在后期的课程里，我会围绕着这些规则展开讲解。

1. **GPO=GPC+GPT** （理解GPO的应用过程） [见系列之二](http://jary3000.blog.51cto.com/610705/121770)

2. 当计算机开机或用户登录时，**组策略的应用顺序**：Local--->site--->domain--->OU--->子OU

3. **GPO只能链接到容器**上（即LSDOU），只能对容器里面的计算机或用户生效，而对组无效。

4. **组策略的生效原则**： [见系列之三](http://jary3000.blog.51cto.com/610705/122093)  
a.用户和计算机必须在其对应的容器下面。   
用户会应用其GPO中的用户配置，而不管用户在哪台计算机上登录。   
计算机会应用其GPO中的计算机配置，而不管哪个用户登录。   
b.默认状态下，GPO会应用在authenticated users组（即所有域用户和域计算机，默认下此组用户可以读取和应用组策略）

5. **组策略的生效时间**：   
a. 计算机策略设置：计算机启动、手动刷新（gpupdate /force)、90-120分钟后台周期刷新。   
b. 用户策略设置：用户登录、手动刷新（gpupdate /force)、90-120分钟后台刷新。   
c. DC的策略设置：5分钟后台周期刷新。   
  
6. **累加性**：如果各级容器的GPO的策略设置没有冲突，则累加。（默认状态下）

7. 如果各级容器的GPO的策略设置发生冲突，则以范围小的GPO策略为准。（默认）   
8. 若一个容器上链接多个GPO，设置不冲突，则累加;若设置冲突，则以列表中最上面的优先（即最后执行的优先）（默认）

9. 若计算机策略和用户策略冲突，则计算机设置覆盖用户设置。   
  
10. **调整组策略的应用顺序**:   
阻止继承：在子容器上启用（将阻止掉所有上级容器的策略，只应用本容器的GPO设置）   
强制（禁止替代）：在父容器的某个GPO上启用（此GPO优先级最高，如果冲突，以此为准，其它不冲突的将累加）   
“阻止继承”不能阻止上级容器所做的“强制”的GPO。（即若二者同时启用，以强制的为准）   
若多个容器的GPO设为“强制”时，以先被应用的为准。

11.查看计算机或用户应用组策略的结果：gpresult/组策略结果集（MMC、帮助中）   
12.**组策略的安全过滤**：如果一个用户帐号位于一个GPO相连的容器里，但不在security filtering里，则该用户不受到该GPO的影响。  
   
13.**WMI筛选**：如果在一个GPO上连接了一个WMI过滤器，则该GPO的设置将只能作用于所连容器中符合WMI要求的计算机。   
如：要求给所有客户机满足是winxp的机器安装软件。   
思考：图书馆或教室的计算机，要求不管什么域用户登录，将都会应用本计算机的相应策略。即原有用户设置失效！--􀃆启用回环模式。   
  
14. **LOOPBACK模式**：如果对一个容器的GPO设置了Loopback模式，则无论一个用户帐号来自何处，则只要在该容器的计算机登录到域，一定会受到该容器GPO的用户策略的影响。（replace/merge两种方式）   
  
15.**同步和异步**：默认winxp是异步处理组策略。即先登录，后刷新组策略。   
  
16.禁用GPO。可以针对一个容器禁用GPO中的计算机配置或用户配置或二者全禁。  
   
17.改变管理GPO的DC：通过GPMC.msc或传统工具完成。   
  
18.**组策略的委派管理**：（为指定的域或OU指定相应的组策略管理员）   
三种权限的管理员：   
可以为OU创建并链接，并编辑、删除（完全权限）--》domain admins   
可以为OU创建并链接、编辑、删除（自己创建的）--》将用户加入到Group Policy Creator Owners组   
可以为指定OU链接已有GPO，并可以删除GPO的链接，但不能编辑   
  
19.低速链路配置组策略：注册表策略进程、安全策略进程。仍将处理。  
   
20.组策略的复制、粘贴、备份、恢复、导入等：利用GPMC.msc   
复制、粘贴：可以在同一域内操作，也可跨域、跨林操作。   
备份、恢复：   
a. 可以执行某个GPO的备份，也可以同时执行多个GPO的备份或所有GPO的备份。   
b. 备份内容：GPO设置、名称等，但不备份GPO到某个容器的链接。   
c. 还原不可跨域操作，但导入可以跨域操作。   
\*\* 如果父子域中，子域如果要用父域的GPO，应该在父域上备份，然后导入到子域或通过复制和粘贴方式处理。不要做直接链接。   
注：   
a. 有些设置不能对低客户端生效。   
b. 有些设置不能对慢速链路用户生效。  
c. 还原默认的两条组策略对象GPO：dcgpofix