活动目录在WindowsServer2008中的改进：审核策略 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/245/2021_2022__E6_B4_BB_E5_8A_A8_E7_9B_AE_E5_c100_245044.htm 在Windows Server 2008中，你现在能够建立AD DS审核通过使用新的审核策略的子类（目录服务变化）来记录新旧属性值，当活动目录对象及它们的属性发生变化时。 审核策略的变化也同样可以应用到活动目录轻量目录服务（Active Directory Lightweight Directory Services 以下简称AD LDS） AD DS审核能干什么？ 全局审核策略审核对目录服务的访问控制，无论针对目录服务事件的审核是被启用或被禁用。这个安全设定决定了当确定的操作被应用到目录对象时事件将被记录到安全日志中。你能控制什么样的操作被审核通过修改一个对象上的系统访问控制列表（SACL）。在Windows Server 2008中这项策略默认被启用。 你能够定义本策略设定（通过修改默认域控制器安全策略），你能够指定审核成功的事件，失败的事件，或者什么也不审核。你能够在AD DS对象的属性对话框中的安全选项卡中设置系统访问控制列表。针对目录服务的审核也同样如此。但只适用与AD DS对象上而不是文件对象或注册表对象。 现存的功能发生了什么变化？ Windows Server 2008增加了AD DS审核策略对某一属性新老值的记录，当一个成功的属性变化时间发生时。先前AD DS的审核策略只记录发生变化的属性名称，而不记录以前及现在的属性值。 审核AD DS访问 在Windows 2000 Server和Windows Server 2003中只有一种审核策略（目录服务访问审核）, 用来控制审核目录服务事件是被启用或者禁用。在Windows Server 2008，本策略被划分

成四个子类：目录服务访问（Directory Service Access） 目录服务变化（Directory Service Changes） 目录服务复制（Directory Service Replication） 详细的目录服务复制（Detailed Directory Service Replication） 正因为新的审核子类（目录服务变化）因此AD DS对象属性的变化才能被审核。你能够审核的变化类型有创建，修改，移动以及反删除。这些事件将被记录在安全日志中。 在AD DS中新的审核策略子类（目录服务变化）增加了以下的功能：当对对像的属性修改成功时，AD DS会纪录先前的属性值以及现在的属性值。如果属性含有一个以上的值时，只有作为修改操作结果变化的值才会被记录。 如果新的对像被创建，属性被赋予的时间将会被记录，属性值也会被记录，在多数情景中，AD DS分配缺省属性给诸如sAMAccountName等系统属性，这些系统属性值将不被记录。 如果一个对像被移动到同一个域中，那么先前的以及新的位置（以distinguished name [比如cn=anna,ou=test,dc=contoso,dc=com]形式）将被记录。当对象被移动到不同域时，一个创建事件将会在目标域的域控制器上生成。 如果一个对象被反删除，那么这个对象被移动到的位置将会被记录。另外如果在反删除操作中属性被增加，修改或者删除，那么这些属性的值也会被记录。 注意：如果一个对象被删除，将不产生任何审核事件。然而，如果启用了Directory Service Access审核子类，那么审核事件将被创建。当Directory Service Changes启用以后，AD DS会在安全日志中记录事件当对象属相的变化满足管理员指定的审核条件。下面的这张表格描述了这些事件。 事件号 事件类型 事件描述 5136 修改 这个事件产生于成功的修改目录对象属性 5137 创建

这个事件产生于新的目录对象被创建 5138 反删除 这个事件产生于目录对象被反删除时 5139 移动 这个事件产生于对象在同一域内移动时 建立审核策略的步骤 这部分将包括以下这两个步骤： 步骤一：启用审核策略 步骤二：使用活动目录用户与计算机来说明如何通过对象的SACL来启用对象审核。 步骤一：启用审核策略 本步骤包含了使用图形界面及命令行来启用审核。 默认情况下组策略管理并没有安装，你可以通过服务器管理里的添加部件（Add Features）进行安装。 通过使用命令行工具Auditpol，你能启用独立的子项目。 通过图形界面启用全局审核策略 1. 单击开始按钮，指向管理工具，再指向组策略管理。 2. 在控制台树，双击林名称，双击域，双击你的域名称，双击域控制器，右键单击默认域控制器策略然后点击编辑。 3. 在计算机配置下，双击Windows设置，双击安全设置，双击本地策略，再双击审核策略 4. 在审核策略中，右键单击审核目录服务访问，然后点击属性 5. 选择定义这些这些策略的复选框 6. 选择成功复选框，单击确定 使用命令行工具Auditpol启用审核策略 1. 单击开始按钮，右键单击命令提示符，再单击以管理员运行 2. 输入以下命令并回车auditpol /set /subcategory:"directory service changes" /success:enable 步骤二：在对象SACL列表中创建审核策 1. 单击开始按钮，指向管理工具，再单击活动目录用户与计算机 2. 右键单击你想启用审核组织单位（OU）或者其它对象，再单价属性 3. 单价安全选项卡，单击高级，再单击审核选项卡 4. 单击添加，在输入对象名称进行选择对话框中，输入Authenticated Users（或者其它安全主体），然后单击确定。 5. 在应用到下拉框中选择子用户对象（Descendant User objects）或者其它对象 6. 在“ 访

问”中勾选“写入所有属性”的成功复选框 7. 单击确定，直到对象的属性页完全关闭。 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