**详解Windows Server 2008安全日志**

【IT专家网独家】为了让大家了解如何追踪计算机安全日志功能的具体方面，首先需要了解如何启动安全日志。大多数Windows计算机(除了某些**[域](http://whatis.ctocio.com.cn/searchwhatis/194/7352194.shtml" \t "_bank)**控制器版本系统)默认情况下不会向安全日志(Security Log)启动日志记录信息。这样的设置有利也有弊，弊的方面在于，除非用户强迫计算机开始日志记录安全事件，否则根本无法进行任何追踪。好的方面在于，不会发生日志信息爆满的问题以及提示日志已满的错误信息，这也是Windows [**Server**](http://whatis.ctocio.com.cn/searchwhatis/497/5948997.shtml) 2003域控制器在没有任何预警下的行为。

　　安全日志事件跟踪可以使用组策略来建立和配置，当然你可以配置本地组策略对象，但是这样的话，你将需要对每台计算机进行单独配置。另外，你可以使用Active Directory内的组策略为多台计算机设置日志记录配置。要建立安全日志追踪，首先打开连接到域的计算机上的Group [**Policy**](http://whatis.ctocio.com.cn/searchwhatis/177/6026177.shtml) Management Console (GPMC，组策略管理控制台)，并以管理员权限登录。

　　在GPMC中，你可以看到所有的组织单位(OU)(如果你事先创建了的话)以及GPO(如果你创建了两个以上)，在本文中，我们将假设你有一个OU，这个OU中包含所有需要追踪相同安全日志信息的计算机，我们将使用台式计算机OU和AuditLog GPO。

　　编辑AuditLog GPO然后展开至以下节点：

[**Computer**](http://whatis.ctocio.com.cn/searchwhatis/364/5947364.shtml)[**Configuration**](http://whatis.ctocio.com.cn/searchwhatis/388/5947388.shtml)**\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy**

　　展开此节点后，你会看到你可以配置的审核类别列表，如图1所示：

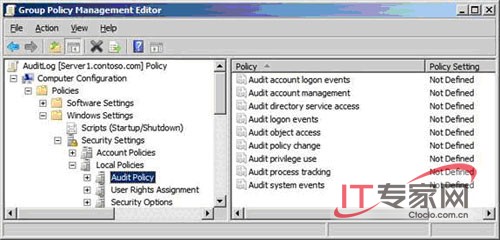


图1：Audit Policy类别可以帮助你制定想要记录日志信息的安全区域

　　每个政策设置都有两个选择：成功和/或失败，要想为任何类别配置成功或者失败，你需要勾选**Define These Policy Settings**选项框，如图2所示。



图2：每个审计政策都需要首先就进行定义，然后需要配置审计类型

　以下是关于每种类别控制范围的简要介绍：

**审计帐户登录事件**– 每次用户登录或者从另一台计算机注销的时候都会对该事件进行审计，计算机执行该审计是为了验证帐户，关于这一点的最好例子就是，当用户登录到他们的Windows XP Professional计算机上，总是由**[域](http://whatis.ctocio.com.cn/searchwhatis/194/7352194.shtml" \t "_bank)**控制器来进行身份验证。由于域控制器对用户进行了验证，这样就会在域控制器上生成事件。除了Windows [**Server**](http://whatis.ctocio.com.cn/searchwhatis/497/5948997.shtml) 2003域控制器(配置为审计这些事件的成功与否)启动了设置外，没有**[操作系统](http://whatis.ctocio.com.cn/searchwhatis/250/7333750.shtml" \t "_bank)**启动该设置。最常见以及最佳的做法就是让所有的域控制器和服务器对这些事件进行审计。我还发现，在很多环境中，客户端也会配置为审计这些事件。

**审计账户管理**–这个将对所有与管理计算机(配置了审计)的用户数据库中的帐户的用户有关的事件进行审计，这些事件的示例如下：

　　·创建一个用户帐户

　　·添加用户到一个组

　　·重命名用户帐户

　　·为用户帐户更改密码

　　对于域控制器而言，该管理政策将会对域帐户更改进行审计。对于服务器或者客户端而言，它将会审计本地安全帐户管理器(Security Accounts Manager)以及相关的帐户。除了Windows Server 2003域控制器(配置为审计这些事件的成功与否)启动了设置外，没有操作系统启动该设置。最常见以及最佳的做法就是让所有的域控制器和服务器对这些事件进行审计。对于用户帐户的审计，安全日志以及审计设置是不能捕捉的。

**审计目录服务访问**–这个将对与访问AD对象(已经被配置为通过系统访问控制列表SACL追踪用户访问情况)的用户有关的事件进行审计，AD对象的SACL指明了以下三件事：

　　·将会被追踪的帐户(通常是用户或者组)

　　·将会被追踪的访问类型，如只读、创建、修改等

　　·对对象访问的成功或者失败情况

　　由于每个对象都有自己独特的SACL，对将被追踪的AD对象的控制级别应该是非常精确的。除了Windows Server 2003域控制器(配置为审计这些事件的成功与否)启动了设置外，没有操作系统启动该设置。最佳做法是为所有域控制器的目录服务访问启动成功和失败审计。

**审计登陆事件** –这将对与登录到、注销或者网络连接到(配置为审计登录事件的)电脑的用户相关的所有事件进行审计，一个很好的例子就是，当这些事件日志记录的时候，恰好是用户使用域用户帐户交互的登录到工作站的时候，这样就会在工作站生成一个事件，而不是执行验证的域控制器上生成。从根本上讲，追踪事件是在当尝试登录的位置，而不是在用户帐户存在的位置。除了Windows Server 2003域控制器(配置为审计这些事件的成功与否)启动了设置外，没有操作系统启动该设置。通常会对网络中所有计算机的这些事件进行日志记录。

**审计对象访问** –当用户访问一个对象的时候，审计对象访问会对每个事件进行审计。对象内容包括：文件、文件夹、打印机、注册表项和AD对象。在现实中，任何有SACL的对象丢会被涵盖到这种类型的审计中。就像对目录访问的审计一样，每个对象都有自己独特的SACL，语序对个别对象进行有针对性的审计。没有任何对象是配置为魔神进行审计的，这意味着启用这个设置并不会产生任何日志记录信息。一旦建立了该设置，对象的SACAL就被配置了，对尝试登录访问该对象时就开始出现表项。除非有特别需要对某些资源的追踪访问，通常是不会配置这种级别的审计，在高度安全的环境中，这种级别的审计通常是启用的，并且会为审计访问配置很多资源。

**审计政策更改**–这将对与计算机上三个“政策”之一的更改相关的每个事件进行审计，这些政策区域包括：

　　·用户权利分配

　　·审计政策

　　·信任关系

　　除了Windows Server 2003域控制器(配置为审计这些事件的成功与否)启动了设置外，没有操作系统启动该设置。最佳做法就是对网络中的所有计算机配置这种级别的审计。

**审计特权使用**–与执行由用户权限控制的任务的用户相关的每个事件都会被审计，用户权利列表是相当广泛的，如图3所示：

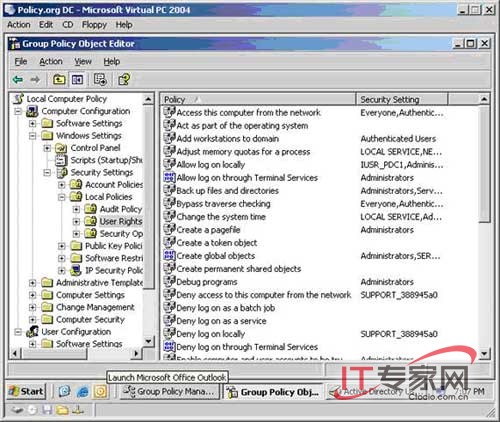


图3：计算机的用户权限列表

　　这种级别的审计不是默认配置来追踪所有操作系统的事件，最佳做法就是对网络中的所有计算机配置这种级别的审计。

**审计过程追踪** – 这将对与计算机中的**[进程](http://whatis.ctocio.com.cn/searchwhatis/292/7333792.shtml" \t "_bank)**相关的每个事件进行审计，这将包括、程序激活、进程退出、处理重叠和间接对象访问。这种级别的审计将会产生很多的事件，并且只有当应用程序正在因为排除故障的目的被追踪的时候才会配置。

**审计系统事件** – 与计算机重新启动或者关闭相关的事件都会被审计，与系统安全和安全日志相关的事件同样也会被追踪(当启动审计的时候)。这是必要的计算机审计配置，不仅当发生的事件需要被日志记录，而且当日志本身被清除的时候也有记录。除了Windows Server 2003域控制器(配置为审计这些事件的成功与否)启动了设置外，没有操作系统启动该设置。最佳做法就是对网络中的所有计算机配置这种级别的审计。

**每个审计类型的Event ID**

　　在安全日志中可能会产生成千上万的事件，所以你需要要秘密解码器环来找出寻找的事件，以下是每种类别最重要的事件(你可能想要在安全日志中跟踪的)：

　　审计帐户登录事件

**Event ID 描述**

　　4776 - [**域**](http://whatis.ctocio.com.cn/searchwhatis/194/7352194.shtml)控制器试图验证帐户凭证信息

　　4777 -域控制器未能验证帐户凭证信息

　　4768 -要求有Kerberos验证票(TGT)

　　4769 -要求有Kerberos验证票(TGT)

　　4770 - Kerberos服务票被更新

　　审计帐户管理

**Event ID 描述**

　　4741 - 计算机帐户已创建

　　4742 – 计算机帐户已更改

　　4743 – 计算机帐户已删除

　　4739 – 域政策已经更改

　　4782 - 密码hash帐户被访问

　　4727 - 安全全局组已经创建

　　4728 – 一名用户被添加到安全全局组

　　4729 – 一名用户从安全全局组解除

　　4730 – 安全全局组已经删除

　　4731 - 安全本地组已经创建

　　4732 -一名用户被添加到安全本地组

　　4733 -一名用户被安全本地组解除

　　4734 -安全本地组已经删除

　　4735 - 安全本地组已经更改

　　4737 -安全全局组已经更改

　　4754 -安全通用组已创建

　　4755 -安全通用组已创建更改

　　4756 -一名用户被添加到安全通用组

　　4757 -一名用户被安全通用组解除

　　4758 -安全本地组已经删除

　　4720 – 用户帐户已创建

　　4722 – 用户帐户已启用

　　4723 - 试图更改帐户密码

　　4724 – 试图重置帐户密码

　　4725 – 用户帐户被停用

　　4726 -用户帐户已删除

　　4738 -用户帐户已被改变

　　4740 -用户帐户被锁定

　　4765 - SID历史记录被添加到一个帐户

　　4766 -尝试添加SID历史记录到帐户失败

　　4767 -用户帐户被锁定

　　4780 -对管理组成员的帐户设置了ACL

　　4781 -帐户名称已经更改

审计目录服务访问

　　4934 - Active Directory 对象的属性被复制

　　4935 -复制失败开始

　　4936 -复制失败结束

　　5136 -目录服务对象已修改

　　5137 -目录服务对象已创建

　　5138 -目录服务对象已删除

　　5139 -目录服务对象已经移动

　　5141 -目录服务对象已删除

　　4932 -命名上下文的AD的副本同步已经开始

　　4933 -命名上下文的AD的副本同步已经结束

**审计登录事件**

　　4634 - 帐户被注销

　　4647 - 用户发起注销

　　4624 - 帐户已成功登录

　　4625 - 帐户登录失败

　　4648 - 试图使用明确的凭证登录

　　4675 - SID被过滤

　　4649 - 发现重放**[攻击](http://whatis.ctocio.com.cn/searchwhatis/308/7333808.shtml" \t "_bank)**

　　4778 -会话被重新连接到Window Station

　　4779 -会话断开连接到Window Station

　　4800 – 工作站被锁定

　　4801 - 工作站被解锁

　　4802 - 屏幕保护程序启用

　　4803 -屏幕保护程序被禁用

　　5378 所要求的凭证代表是政策所不允许的

　　5632 要求对无线网络进行验证

　　5633 要求对有线网络进行验证

**审计对象访问**

　　5140 - 网络共享对象被访问

　　4664 - 试图创建一个硬链接

　　4985 - 交易状态已经改变

　　5051 - 文件已被虚拟化

　　5031 - Windows防火墙服务阻止一个应用程序接收网络中的入站连接

　　4698 -计划任务已创建

　　4699 -计划任务已删除

　　4700 -计划任务已启用

　　4701 -计划任务已停用

　　4702 -计划任务已更新

　　4657 -注册表值被修改

　　5039 -注册表项被虚拟化

　　4660 -对象已删除

　　4663 -试图访问一个对象

**审计政策变化**

　　4715 - 对象上的审计政策(SACL)已经更改

　　4719 - 系统审计政策已经更改

　　4902 - Per-user审核政策表已经创建

　　4906 - CrashOnAuditFail值已经变化

　　4907 - 对象的审计设置已经更改

　　4706 - 创建到**[域](http://whatis.ctocio.com.cn/searchwhatis/194/7352194.shtml" \t "_bank)**的新信任

　　4707 - 到域的信任已经删除

　　4713 - Kerberos政策已更改

　　4716 - 信任域信息已经修改

　　4717 - 系统安全访问授予帐户

　　4718 - 系统安全访问从帐户移除

　　4864 - 名字空间碰撞被删除

　　4865 - 信任森林信息条目已添加

　　4866 - 信任森林信息条目已删除

　　4867 - 信任森林信息条目已取消

　　4704 - 用户权限已分配

　　4705 - 用户权限已移除

　　4714 - 加密数据复原政策已取消

　　4944 - 当开启Windows [**Firewall**](http://whatis.ctocio.com.cn/searchwhatis/419/5947919.shtml)时下列政策启用

　　4945 - 当开启Windows Firewall时列入一个规则

　　4946 - 对Windows防火墙例外列表进行了修改，添加规则

　　4947 - 对Windows防火墙例外列表进行了修改，规则已修改

　　4948 - 对Windows防火墙例外列表进行了修改，规则已删除

　　4949 - Windows防火墙设置已恢复到默认值

　　4950 - Windows防火墙设置已更改

　　4951 - 因为主要版本号码不被Windows防火墙承认，规则已被忽视

　　4952 - 因为主要版本号码不被Windows防火墙承认，部分规则已被忽视，将执行规则的其余部分

　　4953 - 因为Windows防火墙不能解析规则，规则被忽略

　　4954 - Windows防火墙组政策设置已经更改，将使用新设置

　　4956 - Windows防火墙已经更改主动资料

　　4957 - Windows防火墙不适用于以下规则

　　4958 - 因为该规则涉及的条目没有被配置，Windows防火墙将不适用以下规则：

　　6144 - 组策略对象中的安全政策已经成功运用

　　6145 - 当处理组策略对象中的安全政策时发生一个或者多个错误

　　4670 - 对象的权限已更改

**审计特权使用**

　　4672 - 给新登录分配特权

　　4673 - 要求特权服务

　　4674 - 试图对特权对象尝试操作

**审计系统事件**

　　5024 - Windows防火墙服务已成功启动

　　5025 - Windows防火墙服务已经被停止

　　5027 - Windows防火墙服务无法从本地存储检索安全政策，该服务将继续执行目前的政策

　　5028 - Windows防火墙服务无法解析的新的安全政策，这项服务将继续执行目前的政策

　　5029 - Windows防火墙服务无法初始化的驱动程序，这项服务将继续执行目前的政策

　　5030 - Windows防火墙服务无法启动

　　5032 - Windows防火墙无法通知用户它阻止了接收入站连接的应用程序

　　5033 - Windows防火墙驱动程序已成功启动

　　5034 - Windows防火墙驱动程序已经停止

　　5035 - Windows防火墙驱动程序未能启动

　　5037 - Windows防火墙驱动程序检测到关键运行错误，终止。

　　4608 -Windows正在启动

　　4609 - Windows正在关机

　　4616 - 系统时间被改变

　　4621 - 管理员从CrashOnAuditFail回收系统，非管理员的用户现在可以登录，有些审计活动可能没有被记录

　　4697 - 系统中安装服务器

　　4618 - 监测安全事件样式已经发生

　　想查看所有事件的完整列表，请访问微软网站：http://[**support**](http://whatis.ctocio.com.cn/searchwhatis/446/6026446.shtml).microsoft.[**com**](http://whatis.ctocio.com.cn/searchwhatis/307/5947307.shtml)/default.aspx?scid=kb;EN-US;947226

**总结**

　　微软将继续涵盖事件查看器内的安全日志中显示的额外事件，只要你使用组策略建立了你想要审计和跟踪的类别，就可以使用上述解码的事件来跟踪环境需要的事件。如果你将事件与其他技术相结合(例如订阅)，你可以创建事件的微调谐日志，以保证网络的安全。