第 12 章　安全审核

安全审核是整体安全策略的一部分。通过对系统和用户进行充分和适当的审核，就能够在发生安全事故之后帮助发现发生事故的原因，并提供相应的证据。

Windows 2000 包含了安全审核功能，允许监视与安全性相关的事件（如失败的登录尝试），因此可以检测到入侵者和试图危害系统上数据的事件。Windows 2000 审核功能提供比在 Windows NT 4.0 上可用的相关功能更为详细的信息。在要审核的事件类型中，最常见的有：

- 访问对象（如文件和文件夹）
- 用户账户和组账户的管理
- 当用户登录到系统和从系统注销时

除了审核与安全性相关的事件外，Windows 2000 还产生安全日志并提供一个方法来查看记录中所报告的安全事件。

12.1　Windows 2000 安全审核概述

Windows 2000 中的审核是跟踪计算机上用户活动和 Windows 2000 活动的过程，称之为事件。为了便于使用，这些事件被分别记录到六种日志中去，分别是应用程序日志、系统日志、安全日志、目录服务日志、文件复制日志和 DNS 服务器日志。前三种在所有的 Windows 2000 和 Windows NT 系统中都存在，而后三种则仅当安装了相应的服务才会提供。

- 应用服务日志：记录了应用程序和系统产生的事件。任何厂商开发的应用程序都可以用审核系统将自己注册，并向应用程序日志中写入事件。
- 系统日志：含有 Windows 2000 系统自身产生的事件，以及驱动程序等组件产生的事件。
- 安全日志：含有关于安全事件的信息，其中包括与监视系统、用户和进程的活动相关的信息，以及关于启动失败等安全服务的消息。
- 目录服务日志：含有与目录服务相关的信息。
- 文件复制日志：记录了与文件复制相关的事件，这些事件含有服务已启动或停止，或者服务已成功完成等信息。
- DNS 服务日志：含有与域名系统有关的信息，包括 DNS 服务何时启动或停止这样的详细信息，以及与 DNS 区域相关的任何错误信息和消息。

审核事件可以分为两类：成功事件和失败事件。成功事件表示一个用户成功地获得了访问一种资源的权限，而失败事件则表明用户尝试过但失败了。失败事件对于跟踪企图进行的攻击非常有用，但成功事件解释起来就难得多。尽管绝大多数成功的审核事件仅表明活动是正常的，但设法获得了对系统的访问权的攻击者也会生成一个成功事件。事件发生的模式常常与事件本身同样重要。例如，一系列失败后面跟着一个成功可能表示企图进行的攻击最后是成功的。

12.2　审核策略的设置

实现安全审核的第一步是选择系统要审核的事件类型。对于每一个可审核的事件，配置设置都会指明是否要跟踪成功的尝试还是失败的尝试。通过使用“ 组策略 ”管理单元可设置审核策略。

在 Windows 2000 中可以审核的事件类型如下：

- 策略更改
- 登录事件
- 对象访问
- 过程追踪
- 目录服务访问
- 特权使用
- 系统事件
- 账户登录事件
- 审核账户管理。

1. 登录事件

如果对登录事件进行审核，那么每次用户在计算机上登录或注销时，都会在进行了登录尝试的计算机的安全日志中生成一个事件。此外，在用户连接到远程服务器之后，也会在远程服务器的安全日志中生成一个登录事件。在创建或者销毁登录会话和令牌时也会分别创建登录事件。

登录事件对于跟踪以交互方式登录服务器的尝试或者对于调查从特定计算机发动的攻击十分有用。成功审核将在登录尝试成功的情况下生成一个审核项。失败审核将在登录尝试失败的情况下生成一个审核项。

登录事件包括计算机登录事件和用户登录事件两种。在有人试图从基于 Windows NT 或 Windows 2000 的计算机上建立网络连接的情况下，就会看到针对计算机账户和用户账户的两种不同的安全事件日志项。基于 Windows 9x 的计算机在目录中没有计算机账户，因此对于网络登录事件不会生成计算机登录事件项。

作为成员服务器和域控制器基本策略的组成部分，对成功和失败登录事件的审核已启用。因此对于交互登录以及连接到运行“终端服务”的计算机的“终端服务”登录，可以看到表 12-1 所列举的事件 ID。

表 12-1 登录事件的事件 ID 及其含义说明

事件 ID	说 明
528	用户成功地登录到计算机
529	有人用未知的用户名进行了登录尝试，或者用已知的用户名进行了登录尝试，但密码不正确
530	用户账户试图在不允许的时间进行登录
531	有人使用一个被禁用的账户进行登录尝试
532	有人使用一个过期的账户进行登录尝试
533	未允许该用户登录此计算机
534	用户试图用不允许使用的登录类型（如网络登录、交互登录、批登录、服务登录或远程交互登录）进行登录
535	指定账户的密码已经过期
536	“网络登录”服务没有处于活动状态
537	由于其他原因登录尝试失败
538	一个用户被注销
539	在有人进行登录尝试时账户被锁定。此事件可表明有人发动密码攻击但未成功，因而导致账户被锁定
540	网络登录成功。此事件表明远程用户从网络成功地连接到服务器上的本地资源，并为该网络用户生成了一个令牌
682	一个用户重新连接到已断开连接的终端服务会话。此事件表明有人连接到了以前的终端服务会话
683	一个用户没有注销就断开了“终端服务”会话连接。此事件在一个用户通过网络连接到终端服务会话的情况下生成。它出现在终端服务器上

可以使用登录事件的安全审核策略来诊断下面的安全事件。

- 本地登录尝试失败。下列事件 ID 中任何一个都说明失败的登录尝试：529、530、531、532、533、534 和 537。如果一个攻击者试图猜测本地账户的用户名和密码组合但未成功，就会看到事件 529 和 534。然而，这些事件也会在一个用户忘记自己的密码或者通过“ 网上邻居 ”浏览网络时发生。在大规模的环境中很难有效地解释这些事件。一般来讲，如果它们反复发生或者与其他不寻常的因素发生巧合，则应调查这些事件发生的模式。例如，如果在深夜许多 529 事件后面跟着 528 事件，则可能表明发生了一次成功的密码攻击。
- 账户误用。事件 530、531、532 和 533 都可表示用户账户误用。这些事件都表明正确地输入了账户/密码组合，但其他限制因素妨碍了登录的成功。只要有可能，都应调查这些事件以确定是否发生了误用或者是否需要修改当前的限制。例如，可能需要延长某些账户的登录时间。
- 账户锁定。事件 539 表明账户被锁定。此事件也可表明一次密码攻击失败。应当查找同一用户账户以前是否发生了 529 事件并努力分析出所尝试的登录的模式。
- 终端服务攻击。可以使终端服务会话保持连接状态，以允许进程在会话结束之后继续运行。事件 683 表明用户没有从终端服务会话注销，而事件 682 则表明有人连接到了先前断开连接的会话中。

2. 账户登录事件

在一个用户登录到域时，是在域控制器上对登录进行处理的。如果审核域控制器上的账户登录事件，那么就会看到在对账户进行验证的域控制器上记录的此登录尝试。账户登录事件是在身份验证程序包对用户的凭据进行验证时创建的。在使用域凭据的情况下，账户登录事件只在域控制器的事件日志中生成。如果出示的凭据是本地 SAM 数据库凭据，那么就会在服务器的安全事件日志中创建账户登录事件。

由于账户登录事件可以记录在域中的任何有效的域控制器上，因此应当确保将各个域控制器上的安全日志合并，再来分析域中的所有账户登录事件。

与登录事件一样，账户登录事件也包括计算机登录事件和用户登录事件两种。作为成员服务器和域控制器基本策略的组成部分，对成功和失败账户登录事件的审核已启用。因此对于网络登录和终端服务身份验证，可以看到表 12-2 列举的事件 ID：

表 12-2　账户登录事件的事件 ID 及其含义

事件 ID	说　　明
672	成功地发出并验证了身份验证服务 (AS) 票证
673	授予了票证授予服务 (TGS) 票证
674	安全主体更新了 AS 票证或 TGS 票证
675	预身份验证失败
676	身份验证票证请求失败
677	未授予 TGS 票证
678	账户已成功地映射到域账户
680	识别用于成功的登录尝试的账户。此事件还表明使用身份验证程序包对账户进行了身份验证
681	有人进行了域账户登录尝试
682	一个用户重新连接到已断开连接的“终端服务”会话
683	一个用户没有注销就断开了 “ 终端服务 ” 会话连接

对于这些事件中的每个事件，事件日志显示了有关每个特定的登录的详细信息。可以使用账户登录事件安全审核策略来诊断下面的安全事件。

- 域登录尝试失败。事件 ID 675 和 677 表明试图登录到域的失败尝试。
- 时间同步问题。如果客户计算机的时间与进行身份验证的域控制器的时间相差五分钟（默认情况下）以上，那么在安全日志中就会记录事件 ID 675。
- 终端服务攻击。可以使终端服务会话保持连接状态，以允许进程在会话结束之后继续运行。事件 ID 683 表明用户没有从终端服务会话注销，而事件 ID 682 表明有人连接到了先前断开连接的会话。若要防止断开连接或者终止这些已断开连接的会话，可以在终端服务配置控制台中 RDP-TCP 协议的属性设置对话框中定义结束已断开的会话的时间间隔。

3. 账户管理

账户管理的审核用于确定用户或组是在何时创建、更改或删除的。该审核策略可用于确定何时创建了安全主体，以及什么人执行了该任务。

作为成员服务器和域控制器基本策略的组成部分，账户管理中的对成功和失败的审核已启用。因此可以在安全日志中看到表 12-3 所列举的事件 ID。

表 12-3 账户管理事件的事件 ID 及其含义

事件 ID	说　　明
624	创建了用户账户
625	更改了用户账户类型
626	启用了用户账户
627	尝试了密码更改
628	设置了用户账户密码
629	禁用了用户账户
630	删除了用户账户
631	创建了启用安全的全局组
632	添加了启用安全的全局组成员
633	删除了启用安全的全局组成员
634	删除了启用安全的全局组
635	创建了禁用安全的本地组
636	添加了启用安全的本地组成员
637	删除了启用安全的本地组成员
638	删除了启用安全的本地组
639	更改了启用安全的本地组
641	更改了启用安全的全局组
642	更改了用户账户
643	更改了域策略
644	用户账户被锁定

可以使用安全日志诊断下面的账户管理事件。

- 创建用户账户。事件 ID 624 和 626 识别何时创建和启用用户账户。如果仅限于为本单位中的特定个人创建账户，那么可以使用这些事件识别是否有未经授权的人员创建了用户账户。
- 更改了用户账户密码。用户本人之外的其他人对密码进行修改，可表明一个账户已经被另一个用户掌握。应查找表明进行了密码更改尝试并获得成功的事件 ID 627 和 628。查看事件的详细信息以确定是否由另一个账户进行了该更改，以及该账户

是否为可以重置用户账户密码的服务台或其他服务组的成员。

- 更改了用户账户状态。一个攻击者可能试图通过禁用或删除在发动攻击时使用的账户来掩盖他们的踪迹。应该对所有的事件 ID 629 和 630 进行调查以确保这些事件是经授权的事务。还要查找事件 ID 626 发生后较短的时间内接着发生事件 ID 629 的情况。这种情况可表明有人启用并使用了被禁用的账户然后又将该账户禁用。
- 对安全组的修改。应该检查对下列组的成员身份进行的更改：域管理员组、管理员组、任一操作员组；自定义全局组、通用组或受到委派承担管理功能的域本地组。对全局组成员身份的修改，应当查找事件 ID 632 和 633。对域本地组成员身份的修改，应当查找事件 ID 636 和 637。
- 账户锁定。在账户被锁定后，将会在 PDC 模拟器操作主机上记录两个事件。644 事件表明账户名被锁定，然后将记录一个 642 事件，该事件表明用户账户被更改以指示该账户现在被锁定。

4. 对象访问

可以用系统访问控制列表 (SACL) 对基于 Windows 2000 的网络中的所有对象启用审核。SACL 包含一个将要审核的对对象进行的操作的用户和组的列表。在 Windows 2000 中几乎任何用户可以操作的对象都有一个 SACL。这些对象包括 NTFS 驱动器上的文件和文件夹，打印机和注册表项。

SACL 由访问控制项（ACE）组成。每个 ACE 都包含三部分信息：

- 要对其进行审核的安全主体
- 要审核的特定访问类型，称为“访问掩码”
- 一个指示要审核失败访问、成功访问还是两种访问都审核的标志

如果希望让事件出现在安全日志中，则必须首先启用审核对象访问，然后对每个希望对其进行审核的对象定义 SACL。

Windows 2000 中的审核是在打开一个对象的句柄时生成的。Windows 2000 使用的是内核模式安全子系统，这种安全子系统只允许程序通过内核对对象进行访问。这样可以防止程序试图绕过安全系统。由于内核内存空间是与用户模式程序分离的，因此程序通过一种称为“句柄”的数据结构来对对象进行引用。下面是典型的访问尝试过程：

（1）一个用户命令一个程序对对象进行访问（例如打开文件打开）。

（2）该程序从系统中请求句柄，并指定需要哪一种访问（读取、写入等）。

（3）安全子系统将被请求的对象上的 DACL 与用户的令牌进行比较，在 DACL 中查找匹配该用户或匹配该用户所属的组并且具有该程序请求的访问权限的项。

（4）系统将被请求的对象上的 SACL 与用户的令牌进行比较，在 SACL 中查找匹配返回到该程序的有效权限或者该程序所请求的权限的项。如果一个匹配的失败审核 ACE 与所请求的但未允许的访问匹配，则会生成一个失败审核事件。如果一个匹配的成功审核 ACE 与允许的访问匹配，则会生成一个成功审核事件。

（5）如果任何访问都被允许，那么系统就会向该程序返回一个句柄，该程序就可以使用该句柄对对象进行访问。

需要注意的是，在进行审核并生成事件时，对于对象还没有发生任何事情。所以，写入审核是在对文件进行写入之前生成的，而读取审核是在对文件进行读取之前生成的。

与所有的审核一样，对于审核对象访问采取有针对性的方法是很重要的。在审核计划中，先要决定必须进行审核的对象的类型，然后再针对每个要审核的对象类型确定希望监视哪些访问尝试类型（成功、失败或二者）。如果对审核采取过于宽泛的方法，将会对系统的性能产生重大的影响，并将导致收集太多不需要的或没有用的数据。

一般来讲，如果需要审核所选择的对象的所有访问，包括来自不受信任的账户的访问，应当将 Everyone 组添加到希望审核的对象上的 SACL。对于对象访问成功的审核应该谨慎使用，因为这会导致在安全日志中生成大量的审核项。不过，假设正在调查对重要文件的删除事件，就需要检查成功审核事件以确定哪一个用户账户删除了该文件。

Windows 2000 已将成员服务器和域控制器基本策略设置为对成功和失败的对象访问进行审核。然而，在对象上却没有设置 SACL，所以应当根据实际来设置 SACL。可以直接在对象上定义 SACL，也可以使用组策略管理单元进行定义。如果需要审核的对象在多台计算机上都存在，那么就应当在组策略中定义 SACL。

审核对象访问将使表 12-4 所列出的事件出现在安全日志中。

表 12-4　对象访问事件的事件 ID 及其含义

事件 ID	说　明
560	授予了对现有的对象的访问权
562	关闭了一个对象的句柄
563	进行了一次打开一个对象以便将它删除的尝试。（这在指定了 FILE_DELETE_ON_CLOSE 标志的情况下供文件系统使用）
564	删除了一个受保护的对象
565	授予了对现有的对象类型的访问权

若要查找特定的对象访问事件，那么就主要需要调查事件 ID 560 事件。有用的信息位于事件详细信息内，应当搜索事件详细信息来发现所搜索的特定事件。

5. 目录服务访问

Active Directory 对象具有与它们关联的 SACL，因此也可以对它们进行审核。如前所述，通过审核账户管理来审核 Active Directory 用户账户和组账户。然而，如果要审核对其他名称上下文（如配置和架构名称上下文）中的对象的修改，则必须审核对象访问，然后为希望审核的特定容器定义 SACL。审核项是在 Active Directory 对象的 SACL 列出的用户试图访问该对象时生成的。

由于会发生大量的（一般来讲是无害的）事件，因此很难找到与目录服务访问相关的特定事件。因此，对于目录服务访问，成员服务器和域控制器基本策略只审核失败的事件。这将有助于识别一个攻击者试图对 Active Directory 进行未经授权的访问。

尝试的目录访问将在安全日志中显示为 ID 为 565 的目录服务事件。只有通过查看安全事件的详细信息才能确定该事件对应于哪一个对象。

6. 特权使用

用户在系统和网络环境中工作时，就会行使所规定的用户权限。如果对特权使用的成功和失败进行审核的话，那么每次一个用户尝试行使用户权限时都会生成一个事件。

即使审核特权使用，也并非对所有用户权限进行审核。默认情况下，下列用户权限被排除在外：

- 绕过遍历检查
- 调试程序
- 创建令牌对象
- 替换进程级别的令牌
- 生成安全审核
- 备份文件和目录
- 还原文件和目录

可以通过在组策略中启用对备份和还原权限的使用进行审核安全选项，来重写不审核备

份和还原用户权限这一默认行为。

对特权使用成功的审核将会在安全日志中生成大量的日志项。因此，成员服务器和域控制器基本策略只对特权使用失败进行审核。如果启用了对特权使用的审核，则会生成表 12-5 所列举的事件：

表 12-5　特权使用事件的事件 ID 及其含义

事件 ID	说　明
576	向用户的访问令牌中添加了指定的特权。（在用户登录时生成此事件）
577	一个用户试图执行一个特权系统服务操作。
578	有人在受保护对象的已打开句柄上使用了特权。

下面是在使用特定的用户权限时会存在的一些事件日志项的示例。

- 充当操作系统的一部分。应查找带有用户权限 SeTcbPrivilege 的事件 ID 577 或 578。在事件详细信息中标出了使用该用户权限的用户账户。此事件表明有一个用户通过充当操作系统的一部分来试图提升安全特权。例如，一个用户试图将其账户添加到管理员组的 GetAdmin 攻击就使用了此特权。此事件的日志项只能属于系统账户以及授予了这一用户权限的任何服务账户。
- 更改系统时间。应查找带有用户权限 SeSystemtimePrivilege 的事件 ID 577 或 578。在事件详细信息中标出了使用该用户权限的用户账户。此事件可以表明有一个用户尝试更改系统时间以隐藏事件发生的真实时间。
- 从远程系统强制关闭。应查找带有用户权限 SeRemoteShutdownPrivilege 的事件 ID 577 和 578。在事件详细信息中会包括给其授予该用户权限的特定安全标识符（SID）和授予了该权限的安全主体的用户名。
- 加载和卸载设备驱动程序。应查找带有用户权限 SeLoadDriverPrivilege 的事件 ID 577 或 578。在事件详细信息中标出了使用该用户权限的用户账户。此事件表明有一个用户试图加载一个设备驱动程序的未经授权版本或特洛伊木马版本。
- 管理审核和安全日志。应查找带有用户权限 SeSecurityPrivilege 的事件 ID 577 或 578。在事件详细信息中标出了使用该用户权限的用户账户。在清除事件日志以及向安全日志写入有关特权使用的事件时都将会发生此事件。
- 关闭系统。应查找带有用户权限 SeShutdownPrivilege 的事件 ID 577。在事件详细信息中标出了使用该用户权限的用户账户。在有人尝试关闭计算机时将会发生此事件。
- 取得文件或其他对象的所有权。应查找带有用户权限 SeTakeOwnershipPrivilege 的事件 ID 577 或 578。在事件详细信息中标出了使用该用户权限的用户账户。此事件表明有一个攻击者正在通过取得一个对象的所有权来尝试绕过当前的安全设置。

7. 进程跟踪

如果在基于 Windows 2000 的计算机上审核运行的进程的详细跟踪信息，那么事件日志将显示创建进程和结束进程的尝试。事件日志还会记录一个进程尝试生成一个对象的句柄或尝试获取对一个对象的间接访问权的时间。

由于会产生大量的审核项，因此成员服务器和域控制器基本策略不启用对进程跟踪的审核。不过，如果选择审核成功和失败的进程跟踪，将会在事件日志中记录表 12-6 所列举的事件 ID。

表 12-6　进程跟踪事件的事件 ID 及其含义

事件 ID	说　明
592	创建了一个新进程

593	一个进程已退出
594	复制了一个对象的句柄
595	获得了对一个对象的间接访问权

8. 系统事件

在一个用户或进程改变计算机环境的某些方面时会生成系统事件。可以审核对系统进行更改的尝试，如关闭计算机或更改系统时间。如果审核系统事件，则也要审核清除安全日志的时间。这是很重要的，因为攻击者往往试图在对环境进行更改之后清除他们的踪迹。

成员服务器和域控制器基本策略对成功和失败的系统事件进行审核，这就会导致在事件日志中出现表 12-7 所列举的事件 ID。

表 12-7　系统事件的事件 ID 及其含义

事件 ID	说　　明
512	Windows 正在启动。
513	Windows 正在关闭。
514	本地安全机构加载了一个身份验证程序包。
515	一个受信任的登录进程已向本地安全机构注册。
516	为了对安全事件消息进行排队而分配的内部资源已经用尽，导致一些安全事件消息丢失。
517	安全日志被清除。
518	安全账户管理器加载了一个通知程序包。

可以使用这些事件 ID 来捕获下面众多的安全问题。

- 计算机关闭/重新启动。事件 ID 513 表明 Windows 正在关闭。知道关闭或重新启动服务器的时间是很重要的。有许多合法的原因，比如安装驱动程序或应用程序时需要重新启动，或者在进行维护时关闭或重新启动服务器。不过，攻击者也可能强制服务器重新启动以便在启动过程中获取对系统的访问权。应该将所有的关闭计算机的情况都记录下来，以便与事件日志进行比较。许多攻击都涉及计算机的重新启动。通过研究事件日志，可以确定服务器重新启动的时间，以及重新启动是计划中的重新启动还是未计划的重新启动。事件 ID 513 表明 Windows 正在启动，在系统日志中自动生成的一系列其他事件也表明 Windows 正在启动。这些事件中包括事件 ID 6005，该事件表明启动了事件日志服务。除了这一日志项外，还应查找在系统日志中是否存在另外两个不同的事件日志项之一。如果前一次关机是完全的，如在管理员重新启动计算机时，那么在系统日志中会记录事件 ID 6006（事件日志服务已停止）。通过检查该日志项的详细信息，就可以确定是哪一个用户进行了该关机操作。如果重新启动是由意外的重新启动造成的，那么事件 ID 6008 表明重启（发生在<日期><时间>的前一次系统关闭）是意外的。这也可表明有一个导致计算机关闭的拒绝服务攻击。但是请记住，也有可能是由电源故障或者设备驱动程序故障造成的。如果重新启动是由蓝屏造成的，那么在系统日志中就会记录一个具有“保存转储源”的事件 ID 1001。可以在事件详细信息中检查实际的蓝屏错误消息。
- 修改或清除安全日志。攻击者可能试图修改安全日志，或者在实施攻击过程中禁用审核功能，或者清除安全日志以防止被检测到。如果发现安全日志中很多时间段内没有日志项，则应查找事件 ID 612 和 517 以确定哪个用户修改了审核策略。应该将所有的事件 ID 517 与表明清除安全日志的所有时间的物理日志进行比较。一次未经授权的安全日志清除，可能是一次隐藏以前的安全日志中存在的事件的企图。在事件详细信息中包括了清除该日志的用户的名称。

9. 策略更改

一个高级攻击者将会设法修改审核策略本身，以使他们进行的任何更改不会被审核到。如果审核策略更改，就将会发现修改审核策略的企图以及对其他策略和用户权限的更改。成员服务器和域控制器基本策略对成功和失败的审核策略更改进行审核。可以在事件日志中看到记录的下列事件，如表 12-8 所示：

表 12-8　策略更改事件的事件 ID 及其含义

事件 ID	说　明
608	授予了用户权限
609	删除了用户权限
610	与另一个域建立了信任关系
611	删除了与另一个域的信任关系
612	更改了审计策略
768	在一个目录林中的命名空间元素和另一个目录林中的命名空间元素之间检测到了冲突（在一个目录林中的命名空间元素与另一个目录林中的命名空间元素重叠时发生）

这里应查找的两个最重要事件是事件 ID 608 和 609。许多攻击企图都可能导致在日志中记录这些事件。下面的示例都将在授予用户权限时生成事件 ID 608 或者在删除用户权限时生成事件 609。在每一种情况下，事件详细信息中都会包括给其授予用户权限的特定 SID 和授予了该权限的安全主体的用户名。

- 充当操作系统的一部分。应在事件详细信息中查找带有用户权限 SeTcbPrivilege 的事件 ID 608 和 609。
- 将工作站添加到域中。应在事件详细信息中查找带有用户权限 SeMachineAccountPrivilege 的事件。
- 备份文件和目录。应在事件详细信息中查找带有用户权限 SeBackupPrivilege 的事件。
- 绕过遍历检查。应在事件详细信息中查找带有用户权限 SeChangeNotifyPrivilege 的事件。此用户权限允许用户即使在没有访问目录树的其他权限的情况下遍历该目录树。
- 更改系统时间。应在事件详细信息中查找带有用户权限 SeSystemtimePrivilege 的事件。此用户权限允许一个安全主体更改系统时间，潜在地掩盖事件发生的时间。
- 创建永久共享对象。应在事件详细信息中查找带有用户权限 SeCreatePermanentPrivilege 的事件。此用户权限的拥有者可以创建文件和打印共享。
- 调试程序。应在事件详细信息中查找带有用户权限 SeDebugPrivilege 的事件。此用户权限的拥有者可以附加到任何进程。默认情况下，只将此权限授予管理员。
- 从远程系统强制关闭。应在事件详细信息中查找带有用户权限 SeRemoteShutdownPrivilege 的事件。
- 增加调度优先级。应在事件详细信息中查找带有用户权限 SeIncreaseBasePriorityPrivilege 的事件。具有此权限的用户可以修改进程优先级。
- 加载和卸载设备驱动程序。应在事件详细信息中查找带有用户权限 SeLoadDriverPrivilege 的事件。具有此用户权限的用户可以加载设备驱动程序的特洛伊木马版本。
- 管理审核和安全日志。应在事件详细信息中查找带有用户权限 SeSecurityPrivilege 的事件。具有此用户权限的用户可以查看和清除安全日志。
- 替换进程级别的令牌。应在事件详细信息中查找带有用户权限 SeAssignPrimaryTokenPrivilege 的事件。具有此用户权限的用户可以更改与已启动

的子进程关联的默认令牌。

- 还原文件和目录。应在事件详细信息中查找带有用户权限 SeRestorePrivilege 的事件。
- 关闭系统。应在事件详细信息中查找带有用户权限 SeShutdownPrivilege 的事件。具有此用户权限的用户可以关闭系统以初始化新设备驱动程序的安装。
- 取得文件或其他对象的所有权。应在事件详细信息中查找带有用户权限 SeTakeOwnershipPrivilege 的事件。具有此用户权限的用户可以通过取得对象或文件的所有权来访问 NTFS 磁盘上的任何对象或文件。

这些审核事件仅表明给特定的安全主体授予了用户权限，并不意味着该安全主体使用该用户权限执行了某一项任务。审核事件确实可以确定修改用户权限策略的时间。

12.3 事件日志的管理

通过审核生成的每一个事件都可在事件查看器中查看，如图 12-1 所示。

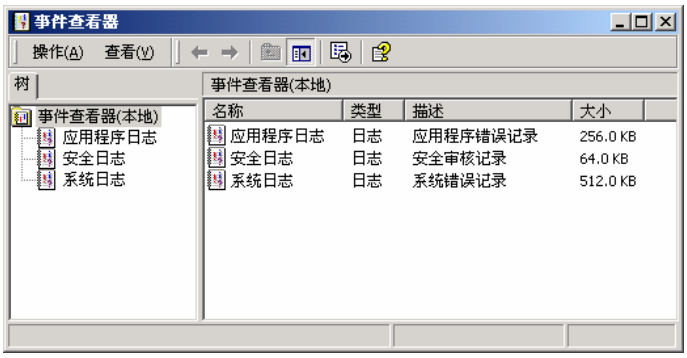

图 12-1 通过“事件查看器”查看事件

12.3.1 事件日志属性设置

若要设置事件日志在存储所生成的事件时所采用的方式，可以直接在事件查看器窗口中进行设置，也可以在组策略中对其中的每一个设置进行定义。可以设置的参数（用于应用程序、系统和安全事件）如下：

- 最大值 设置日志可以达到的最大容量。这个数值的效果实际上依赖于日志检查过程以及在日志被填满时的操作。表 12-9 列出了推荐的日志容量。

表 12-9 日志容量的推荐设置

日志类型	域控制器	文件和打印服务器	数据库服务器	Web 服务器	工作站
安全日志	5 ~ 10MB	2 ~ 4MB	2 ~ 4MB	1 ~ 2MB	1MB
系统日志	1 ~ 2MB	1 ~ 2MB	1 ~ 2MB	1 ~ 2MB	1MB
应用程序日志	1 ~ 2MB	1 ~ 2MB	1 ~ 2MB	1 ~ 2MB	1MB

- 保留方法 确定当前事件已满时将如何处理日志。表 12-10 指定了保留方法和时间。

表 12-10 日志保留时间的推荐设置

日志	覆盖策略设置
安全日志	覆盖 21 天以前的事件
系统日志	覆盖 14 天以前的事件
应用程序日志	按需要覆盖事件

- 按天数改写事件 覆盖所保留时间之前的事件。如果日志在还没有达到保留时间之

前就以填满，则不会记录日志，直到超过这个时间为止，这时服务将覆盖以前的日志。应该注意，除非拥有足够大的日志文件来适应所设置的保留时间，否则将错过重要的审核事件。

- 按需要改写事件　不管保留时间的要求如何都覆盖以前的事件。这是最安全的方法，但是攻击者可以利用这个设置来填满日志，从而覆盖潜在的重要信息。只有在没有任何合适的日志维护计划时才使用这个设置。
- 不改写事件　需要手工清除日志。这将确保记录的任何信息在管理员清除日志之前都一直存在。它具有与“ 按天数改写事件 ”相同的问题，即一旦日志以满，不会在清除日志之前记录事件。如果存在定期的检查方法及入侵侦测系统，则将在日志即将被填满时发出警告，那么这种方法会运行的很好。
- 限制来宾的日志的访问　删除 Everyone 组访问日志的能力。通常情况下，任何用户都可以访问应用程序日志和系统日志。通常只有管理员账号才能查看安全日志。
- 安全审核日志满后关闭计算机　日志文件已满并且不能覆盖事件，系统就会关闭。如果发生了这种情况，那么只有管理员用户才能登录。对于可用性要求很高的系统来说，不推荐设置该选项。

1. 通过“ 事件查看器 ”窗口设置

按照下列步骤进行操作：

（1）打开“ 事件查看器 ”窗口。

（2）在控制树中，选择其中特定类型的事件日志，然后右击。

（3）选择“ 属性 ”命令，打开相应类型事件日志的属性设置对话框，如图 12-2 所示。

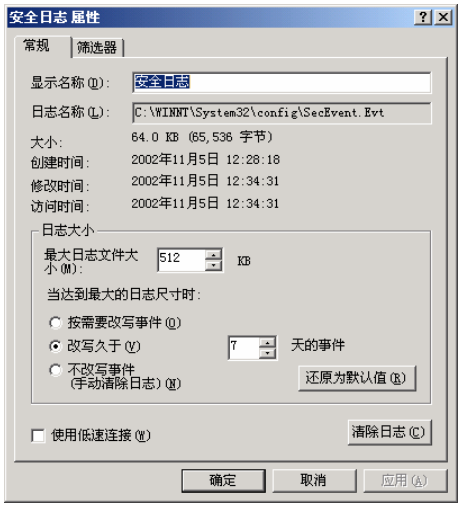

图 12-2　设置事件日志属性设置对话框

2. 通过组策略设置

若要在组织单元（OU）上的组策略中修改安全日志设置，可按照下列步骤操作：

（1）在“ 开始 ”菜单中，选择“ 管理工具 ”→“ Active Directory 用户和计算机 ”。

（2）在控制台树中，右击希望更改审核策略的 OU，然后选择“ 属性 ”命令。

（3）打开“ 组策略 ”选项卡，选择希望编辑的组策略对象，然后单击“ 编辑 ”按钮。

（4）在组策略编辑器中，定位到“ 计算机配置\Windows 设置\安全设置\事件日志\事件日志设置 ”，如图 12-3 所示。

（5）根据需要对设置进行修改。

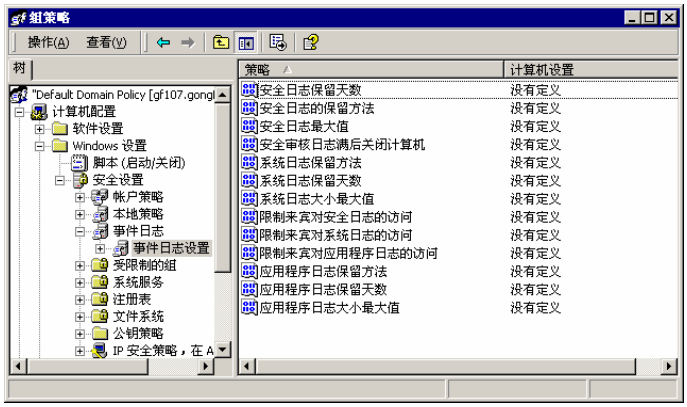

图 12-3　通过“组策略”设置事件日志属性

虽然可以直接在“事件查看器”中对事件日志的属性进行设置。但是，在组策略中定义事件日志的设置可以确保类似的计算机之间的设置一致。

12.3.2　事件日志的筛选

可以在事件查看器中定义筛选器以查找特定的事件。若要在事件查看器中定义筛选器可参照如下操作：

（1）打开“事件查看器”窗口。

（2）在控制树中，选择其中特定类型的事件日志，然后右击。

（3）选择“属性”命令。

（4）切换到“筛选器”选项卡，如图 12-4 所示。

（5）选择用于筛选的参数。

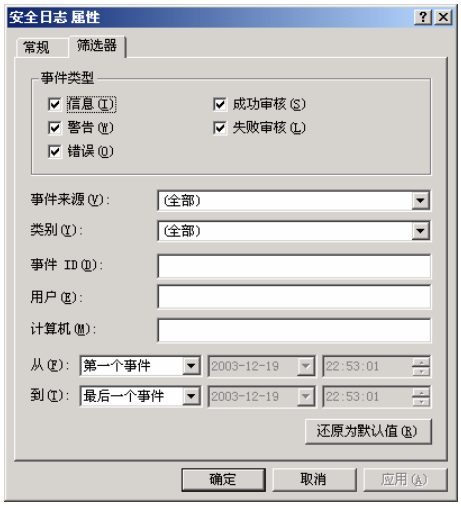

图 12-4　设置事件日志的筛选器

在这里可以定义下列属性以筛选事件项。

- 事件类型。可以将该筛选器限制为用于信息、警告、错误、成功审计、失败审计这些事件类型或其任意组合。
- 事件来源。生成该事件的特定服务或驱动程序。
- 类别。可以将该筛选器限制为用于特定的事件类别。
- 事件 ID。如果知道所要搜索的特定事件 ID，那么该筛选器可以将列表限制为该特定事件 ID。
- 用户。可以将事件显示限制为由特定用户生成的事件。
- 计算机。可以将事件显示限制为由特定计算机生成的事件。

- 日期间隔。可以将显示限制为在特定的开始日期和结束日期之间发生的事件。

在应用该筛选器之后，可以将筛选出的事件列表导出到逗号分隔列表或制表符分隔的列表中，以便导入到数据库应用程序中。

12.3.3 事件日志的转储

Microsoft 的 Resource kit 工具包中包含有一个转储事件日志的工具 Dumpel.exe（Dump Event Log Tool）。它可将本地或远程系统的事件日志转储到一个制表符分隔的文本文件中，然后可以将此文件导入到电子表格或数据库中以便进行进一步的研究。该工具还可以用于筛选或过滤掉某些事件类型。

Dumpel.exe 工具使用的语法为：

```
dumpel -f file [-s \\server] [-l log [-m source]] [-e n1 n2 n3...][-r] [-t] [-d x]
```

其中各参数的含义如下。

- -f：指定输出文件的文件名。-f 没有默认值，因此必须指定文件。
- -s：指定要为其转储事件日志的服务器。服务器名的前导反斜杠是可选的。
- -l：指定要转储哪一种日志（系统日志、应用程序日志还是安全日志）。如果指定了无效的日志名称，则会转储应用程序日志。
- -m：指定在哪个源中（如重定向器、串口等）转储记录。只能提供一个源。如果未使用该参数，则会转储所有事件。如果使用了未在注册表中注册的源，则会在应用程序日志中搜索这种类型的记录。
- -e n1 n2 n3：事件 ID nn 的筛选器（最多可以指定 10 个）。如果未使用-r 参数，则只转储这些类型的记录；而如果使用了-r 参数，则转储除这些类型的记录以外的所有记录。如果未使用此参数，则会选中指定的源名称中的所有事件。使用此参数时必须同时使用-m 参数。
- -r：指定是要筛选特定的源或记录还是将它们筛选掉。
- -t：指定各个字符串由制表符分隔。如果未使用-t，则字符串由空格分隔。
- -d x：转储在过去的 x 天内发生的事件。