eTrust® Access Control for Windows

入门指南

r8 SP1

CA 产品引用

本文档引用以下 CA 产品 ：

- eTrust® Access Control (eTrust Access Control)
- eTrust® Single Sign-On (eTrust SSO)
- eTrust® Web Access Control (eTrust Web AC)
- eTrust® CA-Top Secret®
- eTrust® CA-ACF2®
- eTrust® Audit
- Unicenter® TNG
- Unicenter® Network and Systems Management (Unicenter NSM)
- Unicenter® Software Delivery

联系客户支持

欲获取联机技术帮助以及位置、主要服务时间和电话号码的完整列表，请通过 http://www.ca.com/camap.htm 与客户支持人员联系。

目录

第 1 章： eBusiness 的多方面安全简介 9

本指南的用途 9
CA 技术服务：实现企业 IT 管理的愿景 9
教育和培训：实现 CA 技术的商业价值最大化 10
eTrust 解决方案 10
CA：eBusiness 管理软件 10
更多信息 10
您的开放式分布网络环境是否真正安全？ 11
Windows 和 UNIX 超级用户权限 11
保护环境安全 11
防止入侵主机 12
保护数据和应用程序 12
管理用户帐户和密码 12
保护多个服务器 12
提升统一的跨平台安全保护 13
特性 14
Active Directory 支持 15
策略管理系统 15
应用程序策略生成器 16

第 2 章： 增强操作系统安全性 17

组件、功能和安装注意事项 17
eTrust Access Control 的组件 18
eTrust Access Control 的功能 19
管理 eTrust Access Control 服务 26
eTrust Access Control 文档 26
后续内容 26

第 3 章： 运行管理员界面 27

实施和维护安全策略 27
菜单栏和工具栏 28
程序栏 29
selang 命令 30
设置管理员默认值 31
向导 31
后续内容 33

第 4 章： 了解强大的保护功能 35

从保护程序到监视系统文件 35
创建用户和组 36
保护文件和目录 38
文件组 39
保护程序 39
监视文件 40
保护进程不被终止 40
程序模式 41
保护其他资源 42
利用预定义的组限制访问 42
后续内容 44

第 5 章： 获得对用户帐户更多的控制 45

限制用户访问和权限 45
限制 Administrators 的使用 45
限制从终端访问 47
限制模拟请求 48
设置日内时和周内某日规则 51
后续内容 53

第 6 章： 保护网络活动 55

控制网络级访问 55
保护网络 (TCP/IP) 55
控制传出连接 59
面向服务的 TCP/IP 规则 60
后续内容 61

第 7 章： 设置密码和审核策略 63

密码、登录和审核规则 63
设置密码策略 64
更改密码 65
在本地环境中设置审核策略 65
清理 66
后续内容 66

第 8 章： 集中管理 67

创建用户、安全策略和其他 67
创建 PMDB 67

使用 PMDB 68
事务管理器 — 一种更简单的替代方法 69
后续内容 71

第 9 章： 与 Unicenter 集成 73

将 eTrust Access Control 与 Unicenter 进行集成 73
安装 Unicenter Integration 工具 74
安装说明 75
后续内容 75

第 10 章： 常见问题 77

第 1 章： eBusiness 的多方面安全简介

此部分包含以下主题：

本指南的用途 (p. 9)
CA 技术服务：实现企业 IT 管理的愿景 (p. 9)
教育和培训：实现 CA 技术的商业价值最大化 (p. 10)
eTrust 解决方案 (p. 10)
CA：eBusiness 管理软件 (p. 10)
更多信息 (p. 10)
您的开放式分布网络环境是否真正安全？ (p. 11)

本指南的用途

本指南向您介绍有关 eTrust Access Control 的信息。读完本指南后，您将对该产品的广阔范围有一个概括性的了解，并将熟悉其可用性。对我们而言，重要的是您在开始使用 eTrust Access Control 之前先有一种得心应手的感觉。

CA 技术服务：实现企业 IT 管理的愿景

CA Technology Services(tm) 提供企业 IT 管理解决方案，帮助我们的客户实现更高效率的业务运营和更好地管理 IT 基础设施，促进他们创造有意义的商业价值和财务效益。CA 技术服务部充分利用自己在企业系统管理、业务服务优化、安全管理和存储管理方面的全球专业技术和认证专家，帮助客户实现 IT 投资收益最大化。

我们荟萃了 1,000 多名技术服务专家的超过 27 年的管理软件经验和业界称道的服务提供能力，而且绝大多数专家都获得了 CISSP、ITIL 和 SNIA 认证。-行业领先的服务合作伙伴，为您提供最佳经验做法和经得起时间检验的可靠方法。

教育和培训：实现 CA 技术的商业价值最大化

CA 技术服务部的教育与培训着重帮助您实现简化实施过程、缩短创造价值的时间和提高生产效率，从而实现 CA 技术的商业价值最大化。我们为 CA 全面的、-集成化的开放式企业 IT 管理 (EIM) 解决方案提供教师引导和自学相结合且范围广泛的学习方案，并通过与领先的增值教育提供商结为合作伙伴，扩展我们在企业系统管理、安全管理、存储管理和业务服务优化方面的课程教学内容。我们由获得认证的资深专家组成的实力强大的团队将实时传授优化 CA 软件产品和充分利用可靠的 IT 处理模型的专家意见，指导您的组织如何在 IT 环境中实际应用最佳经验做法。

有关教育与培训课程的完整列表，请访问 http://ca.com/education。

eTrust 解决方案

eTrust 解决方案通过提供便于组织保护其环境安全的创新技术来促进发展 eBusiness。这个全面的安全套件以及包括风险评估、攻击检测、损失防范在内的解决方案将会增加任何 eBusiness 的回报机会。使用 eTrust，组织可以灵活地将安全解决方案作为独立产品或安全套件进行部署，或者-与 Unicenter NSM 进行全面集成。通过与 Unicenter NSM 配合使用，eTrust 解决方案将启用一致的方法来构建、部署和管理作为企业管理比较重要的任务之一的安全保护。

CA：eBusiness 管理软件

利用当前的商务基础结构并采用了新技术之后，下一代 eBusiness 将会向我们展现无限的商机。但与此同时，无论是在组织内部还是组织之间，从管理计算设备到集成与管理应用程序、数据和业务流程，极其复杂的管理工作都会在方方面面向我们提出挑战。请您从 CA 寻求答案。CA 具有可用于帮助 eBusiness 解决这些重要问题的解决方案。利用业界-领先的 eBusiness 进程管理、eBusiness 信息管理和 eBusiness 基础结构管理，CA 提供了独一无二的、全面的、最先进的解决方案，从而为那些在不断扩展的全球经济环境中勇于进取的风险投资企业提供服务。

更多信息

阅读了本《入门指南》之后，可以参阅为您提供的大量资源来了解更多信息。您的产品 CD 包含指导文档，这些文档展示您的软件，并提供有关产品的全面的、功能丰富的组件的详细说明。

For assistance, contact Technical Support at http://ca.com/support.

您的开放式分布网络环境是否真正安全?

在大多数公司，重要信息（如财务事项、客户信息和机密人事记录）都驻留在分布式服务器上。保护和控制对该数据的访问是非常重要的业务要求。遗憾的是，开放式系统服务器没有提供足够的数据安全保护。事实上，由于基础操作系统中存在的"漏洞"，分布式服务器很容易受到未经授权的访问。Windows 和 UNIX 操作系统都是围绕超级用户管理员概念构建的，这一概念创建了由对应用程序、数据和审核记录具有完全访问权限的单个特权用户帐户造成的漏洞。

注意：除非特别指定，否则，术语"Windows"是指由 eTrust Access Control 支持的任何 Microsoft Windows 操作系统。

Windows 和 UNIX 超级用户权限

这些系统中最严重的问题之一是通过系统超级用户或管理员的单点破坏。管理员是可以在系统上执行任何任务并可查看或修改任何文件的特殊的特权用户。这被认为是这些操作系统中最大的风险之一，因为该帐户可以终止系统服务、删除重要文件、访问机密信息以及消除其审核跟踪。同时，超级用户帐户经常会提供给其他系统管理操作员，以便进行数据备份、帐户创建和删除或密码重置。超级用户帐户也是黑客最主要的攻击目标，因为他们知道，一旦该帐户被破坏，他们实际上就可以随心所欲地执行任何操作。

保护环境安全

通过使用 eTrust Access Control，公司可以集中管理用户访问权限，并可快速部署预先配置的基本安全策略。eTrust Access Control 将确保合适的人对合适的信息拥有访问权限。它将主动保护对遍及整个组织的 Windows 系统服务器上的数据和应用程序的访问。

<eTrust Access Control 通过其 Dynamic Security (DSX) 技术提供了可靠的、非插入式的保护。DSX 将实时动态地截获对安全性较敏感的请求，而无须对操作系统内核进行任何永久性更改。这将在不干扰服务器处理的情况下提供级别非常高的安全。eTrust Access Control 中的高级功能（如一般文件保护）从根本上提高了 Windows 操作系统的安全性。使用普通类别文件保护，组织可以使用通配符选项来保护相关文件组或相关程序组。通过该功能可以轻松地开发功能强大的常规访问策略。

防止入侵主机

<eTrust Access Control 为基于主机的入侵防御系统 (HIPS) 提供许多关键功能，能够降低外部蠕虫攻击或恶意软件破坏的安全风险。 利用堆栈溢出保护 (STOP) 功能、特洛伊木马阻止功能、预定义的应用程序安全模板示例和应用程序行为配置程序，eTrust Access Control 为管理员提供了更强大的关键服务器保护，让他们有更多时间的时间去修复系统漏洞和分发安全修补程序。

保护数据和应用程序

组织的成功取决于其数据和应用程序的完整性和私密性。使用 eTrust Access Control，用户和程序都对他们所需的信息拥有适当的访问权限，并且所有未经授权的信息请求将受到阻止并进行记录!

eTrust Access Control 为增强的应用程序安全提供了自定义的安全策略。同时，CA 正在与重要的软件供应商进行合作，以使 eTrust Access Control 可以控制对特定应用程序的访问。这些"防护盾"解决方案为重要业务的应用程序提供了全面保护。

管理用户帐户和密码

随着企业在 eBusiness 市场中不断发展，跨不同的地域或系统域以及各种部门管理用户给系统管理员造成了大量的工作。跨各种系统或者甚至各种平台的用户帐户、密码和安全策略的同步可能是一项令人畏缩的任务，因为它容易产生错误、过程复杂、反应时间增加且成本很高。

保护多个服务器

为了解决保护网络上多个服务器的问题，eTrust Access Control 提供了策略模型数据库 (PMDB) 基础结构。PMDB 可以使帐户、密码和安全策略同步任务安全准确地执行到已订阅的分层节点。eTrust Access Control 的一个重要设计目标是，即使在网络连接没有正常工作的情况下，也应该强制实施给定服务器的安全性。这样做的结果就是规则被分散，并且每个服务器都可以单独安全地存在。

提升统一的跨平台安全保护

使用 eTrust Access Control，将提升每个系统上的安全级别，以满足整体业务要求。可以集中创建并自动分发单个 eTrust Access Control 安全策略，然后在各种 Windows 和 UNIX 操作系统上强制执行该策略。最终结果是，花费最少的时间和精力获得了一个可靠、一致的服务器安全级别。

如果不使用 eTrust Access Control，管理员必须为每个计算系统创建并维护单独的安全策略，这需要花费大量的时间和精力。此外，公司范围内的安全标准经常是基于具有最低安全级别的系统，这是一种无法满足大多数组织的安全要求的方法。

可以在企业范围内创建、管理和分发策略，或者自定义策略以满足特定应用程序的安全要求。可以在各个部门（如会计或开发部门）、最大型企业、以及介于二者规模之间的任何部门或企业中部署该完全解决方案。其增强的操作系统安全、完全审核功能和跨平台访问控制将会保护分布式系统上的关键进程和敏感信息。

由于该强大的解决方案是开放式和可扩展的，因此它支持所有行业标准的平台、数据库和应用程序，并包括允许它保护任何资源的已发布接口。eTrust Access Control 可以与 Unicenter TNG 进行通信，从而提供一种功能强大、全面的解决方案，用于构建、部署和管理作为企业管理的一个重要部分的安全保护。

特性

eTrust Access Control 提供了许多功能来管理企业安全：

集中化的管理

您可以使用 eTrust Access Control 从单点来管理管理员工作站和安装了 eTrust Access Control 的所有其他工作站。

自我-文件保护

自-卫机制将防止黑客或其他用户关闭 eTrust Access Control 服务。该机制还将保护 eTrust Access Control 文件和审核数据。

配置文件组

eTrust Access Control 允许您基于组成员资格分配安全角色。例如，它可以限制授予 Administrator 组和作为该组成员的用户的权限。

注册表保护

eTrust Access Control 可以保护注册表，以确保未经授权的用户不能更改系统参数。授权用户可以根据需要更新注册表设置。

进程保护

eTrust Access Control 将保护指定进程，以确保它们不被终止。eTrust Access Control 进程保护也有助于保护 Windows 服务和其他非交互式 Windows 应用程序。

网络保护

eTrust Access Control 通过管理传入和传出的网络连接来控制对网络服务和端口的访问。

SPECIALPGM 保护

eTrust Access Control 将保护指定程序（比如系统服务），这些程序通常必须作为 SYSTEM 帐户运行，以便仅逻辑用户可以访问它们。

登录保护

eTrust Access Control 允许您以几种方式限制用户登录 — 从帐号过期日期到日期和时间限制。

程序和文件签名

eTrust Access Control 通过为程序和文件提供签名来保护它们。如果签名已经更改，该程序或文件将变为不受信托的，并且无法进行访问。

任务委托

您可以使用 eTrust Access Control 向普通用户授予所需的权限和特权，以便这些用户可以执行管理任务。这称为任务委托。能够以这种详细方式委派任务（授予管理权限）是 eTrust Access Control 最重要的优点之一。

增强的文件保护

eTrust Access Control 将保护当前与 Windows 一起使用的所有文件系统 — Windows 文件系统 (NTFS) 和文件分配表 (FAT)。eTrust Access Control 也支持 CDFS 和 HPFS。

堆栈溢出保护 (STOP)

STOP 将防止黑客使用堆栈溢出利用，通过它黑客可以执行任意命令来入侵系统。

跨-平台支持

管理员可以为 Windows 和 UNIX 计算机创建、实施和维护类似或完全相同的安全策略。

Active Directory 支持

许多组织正在转向将它们的用户数据存储集中到 基于 Active Directory 或 LDAP 存储库中。eTrust Access Control 通过 eTrust IAM 支持外部用户（在外部存储库上定义的 用户）。也就是说，一个组织可以在外部存储库中 定义用户，然后 eTrust IAM 将这些用户与 eTrust Access Control 数据库关联。eTrust Access Control 还可以 创建、修改或删除驻留在 Active Directory 或 安全帐户管理器 (SAM) 即 Windows NT 用户帐户数据库中的原始用户。

策略管理系统

eTrust Access Control 提供一个独立的策略管理系统，帮助管理员利用策略设置版本控制、分布和远程下载功能来轻松管理部门安全策略，从而确保所有订阅服务器都能够获得最新的安全策略和易用的版本控件。

您可以使用 eTrust Access Control 以两种方式从一个中央计算机来管理多个数据库：

- 基于规则的自动策略更新

  您在中央数据库 (PMDB) 中定义的常规规则会自动传播给配置的层级结构中的数据库。

- 基于策略的高级管理和报告

  您存储在中央位置的策略（规则组）将被部署并传播给配置的层级结构中的所有数据库。您还可以删除已部署的策略版本（取消部署）和关于部署状态、部署偏差和部署层级结构的报告。要使用此功能，您需要安装并配置额外的组件。

应用程序策略生成器

eAC 提供的自动化策略生成器程序可以描述应用程序行为并据此生成安全策略。它创建包围应用程序的安全封套，极大地减少了构建这些规则所需要的部署工作。

第 2 章： 增强操作系统安全性

此部分包含以下主题：

组件、功能和安装注意事项 (p. 17)

组件、功能和安装注意事项

新的开放式和分布式计算模式已经对计算机安全提出了越来越高的要求。不同平台间的集成任务变得更加复杂。对一种能够解决相同安全问题、适用不同系统的安全解决方案的需求，已经成为安全日程上的一项重要议题。此外大型公司的并购活动较之以往更多。这就产生了新一轮的安全要求，包括突发事件处理、销售能力、高效和集中化管理以及跨平台支持。

eTrust Access Control 具有内置基本策略，可以为组织提供直接的现成结果。由于该强大的解决方案是开放式并且可扩展的，因此它支持所有行业标准的平台、数据库和应用程序，并包括允许它保护任何资源的已发布接口。

易用优点与集中式用户和访问权限管理相结合，使得组织可以放手利用当今的电子商务商机。作为 eTrust 安全解决方案的一部分，eTrust Access Control 可以与 Unicenter NSM 进行互操作，从而为构建、部署和管理作为企业管理一个重要组成部分的安全保护提供了一套功能强大、全面的解决方案。

eTrust Access Control 的组件

eTrust Access Control 包括数据库 (seosdb)、两个驱动程序（seosdrv 和 drveng）、许多服务（包括监视程序、代理、引擎、策略模型和任务委派）以及图形用户界面。

数据库

数据库包含组织中用户和组的定义、需要保护的系统资源以及管理用户和组对系统资源进行访问的规则。

驱动程序

驱动程序将截获每个请求，以打开文件、打开注册表键、终止进程或执行网络活动。驱动程序会将这些请求传递给服务)引擎，接收引擎应该批准请求还是拒绝请求的决定，并将该决定转发给操作系统的原始系统调用，然后该系统调用将继续处理基于它从驱动程序收到的答复。

监视程序

监视程序会经常检查其他 eTrust Access Control 服务是否正在运行。偶尔，当监视程序发现另一个服务已经停止时，它会立即再次启动该服务。

代理

代理通过 TCP/IP 之上的专用应用程序协议与 eTrust Access Control 客户端进行通信，并管理 eTrust Access Control 用户的安全

引擎

引擎管理数据库，包括控制所有数据库更新、确定是否批准它从驱动程序和代理收到的访问请求、检查监视程序服务是否正在运行，以及重新启动监视程序（如果监视程序已经停止运行）。

引擎将处理数据库访问请求和决策功能，从而将进程间通信减至到最少，并可实现最大效率。

策略模型

单独地管理数十或数百个数据库是不实际的，因此 eTrust Access Control 提供了策略模型服务，它是用于从一台计算机对许多计算机进行管理的组件。使用策略模型服务是可选的，但是它将极大地简化大型站点上的管理。

任务委托

eTrust Access Control 允许您为一般用户授予必需的权限，以便这些用户可以执行管理任务。这称为任务委托。

图形用户界面

策略管理器是图形用户界面 (GUI)，所有 eTrust Access Control 功能都可以通过该界面执行。

注意：有关策略管理器的的详细信息，请参阅《管理员指南》。

eTrust Access Control 的功能

eTrust Access Control 允许您从一个中央位置来管理本地 Windows，并可显著扩展本地 Windows 安全性。eTrust Access Control 还可以进行自我保护。以下几节将介绍这些功能。

Windows 管理

将 eTrust Access Control 安装在组织的 Windows 工作站上之后，可以从一个中央工作站来管理所有这些工作站，而不管它们位于哪些域中。若要执行上述操作，请使用策略管理器，或者使用名为 selang 的命令行语言。

策略管理器

策略管理器是 eTrust Access Control 的 GUI。使用策略管理器，您可以运行所有的 eTrust Access Control 功能。

注意：有关策略管理器的的详细信息，请参阅《管理员指南》。

selang

Selang 是 eTrust Access Control 的命令行语言。也可以使用 selang 编写脚本。可以通过在命令提示符窗口中调用 selang 来运行 selang 命令，或者使用策略管理器中的命令和脚本工具来运行该命令。

注意：有关 selang 及其命令的详细信息，请参阅《参考指南》。

eTrust Access Control 自我防护

无论有意还是无意，黑客或用户实际上无法终止 eTrust Access Control 服务。当 eTrust Access Control 运行时，未经授权的用户实际上也不能更改或清除 eTrust Access Control 文件和数据，因为 eTrust Access Control 使用特殊的文件签名。

管理员帐户限制

管理 Windows 的用户通常是在系统设置期间自动创建的预定义组的成员。每个预定义组用于执行一组特定的系统功能。属于某个组的成员的用户可以执行该组的所有功能。

Windows 中功能最强大的组是 Administrators 组。Windows 会在 Administrators 组中创建一个 Administrator 帐户。Administrators 组的每个成员都可以执行多种任务，从创建、删除和修改用户到锁定、重新配置和关闭服务器。

Windows 中的主要安全风险之一是，未经授权的用户可以获得 Administrators 组中用户帐户的控制权。如果发生这种情况，未经授权的用户可能会对系统造成巨大破坏。

eTrust Access Control 允许您限制授予 Administrator 帐户的权限，以及限制作为 Administrators 组成员的用户的权限。这将会减少 Windows 系统的漏洞。

本地 Windows 安全性管理

使用 eTrust Access Control，可以管理 Windows 安全性的下列元素：

注册表保护

Windows 注册表是一个包含大多数操作系统参数的集中数据库，包括控制设备驱动程序、配置详细信息及硬件、环境和安全设置的参数。

eTrust Access Control 可以保护注册表，以确保未经授权的用户不能更改系统参数。授权用户可以根据需要更新注册表设置。

文件保护

Windows 使用几种不同类型的文件系统之一。最常用的是 FAT 和 NTFS。如果使用 NTFS 文件系统，Windows 将通过创建和更新每个文件的访问控制列表 (ACL) 来保护系统中的文件。eTrust Access Control 支持文件 ACL。

密码保护

eTrust Access Control 可以保护密码并强制执行密码质量检查，就像本地 Windows 安性全一样，但是通过其自身的机制实施的。eTrust Access Control 可以执行下列任务：

- 强制执行密码最长时限
- 强制执行最小密码长度
- 最多保存 20 代用户密码
- 重复登录失败后锁定帐户
- 强制用户在更改密码之前登录到 Windows

服务器管理器功能

eTrust Access Control 可以通过 Windows NT 程序栏上的服务器管理器来管理其他本地 Windows 资源。受保护的 Windows 资源包括：

COM

COM 类中的记录使用"控制面板"中"端口"下列出的串行端口 (COM) 或并行端口 (LPT) 来定义设备。

设备

DEVICE 类中的记录定义 Windows 硬件设备（列在"控制面板"中的"设备"下）。

磁盘

DISK 类中的记录定义系统卷。

域管理

DOMAIN 类中的记录定义共享通用数据库和安全策略（域）的计算机集合。

打印机

PRINTER 类中的记录定义连接到可以在介质上重新生成可视图像的 Windows 计算机系统的设备（列在 PRINTERS 文件夹中）。

进程

PROCESS 类中的记录定义由可执行程序、虚拟内存地址集和线程组成的对象（在"Windows 任务管理器"中列出）。

服务

SERVICE 类中的记录定义 Windows 服务（列在"控制面板"中"服务"下）。

共享

SHARE 类中的记录定义包括由网络用户使用的设备、数据或程序的共享资源，如目录、文件、打印机和命名管道。

Windows 会话

SESSION 类中的记录定义本地主机上的用户会话。该记录包括用户名、计算机名、已用的连接时间和正在使用的资源。

本地 Windows 安全性扩展

下列 eTrust Access Control 功能扩展了本地 Windows 安全性。

普通用户的管理员权限

eTrust Access Control 允许您为普通用户授予必要的权限，以便这些用户可以执行管理任务，而不必是 Administrators 组的成员。这称为任务委托。以这种详细方式委派任务（授予管理权限）的能力是 eTrust Access Control 最重要的优点之一。

增强的文件保护

eTrust Access Control 将保护当前与 Windows 一起使用的所有文件系统。两个最常用的文件系统是 Windows 文件系统 (NTFS) 和文件分配表 (FAT)。eTrust Access Control 还支持 CDFS（专用于 CD 的文件系统）和 HPFS（OS/2 文件系统）。

eTrust Access Control 还提供了文件分配表 (FAT) 的总体安全解决方案，以及包括 NTFS 和 CDFS 的其他文件系统的额外安全层。

一般文件保护

一般文件保护可以保护所有符合指定通配符模式（正则表达式）的文件。名称与指定通配符模式匹配的任何资源都受指定的一般访问规则的保护。eTrust Access Control 可以对文件进行常规保护。

如果资源与多个一般访问规则匹配，eTrust Access Control 将选择与该文件最匹配的规则。

使用一般文件保护，只须定义少数几个安全规则就可以保护需要保护的许多文件。

增强的密码保护

本地 Windows 安全性为用户密码提供了重要保护 (p. 21)。 但是，eTrust Access Control 极大扩展了密码保护，以便显著降低黑客成功偷取密码的可能性。

在使用 eTrust Access Control 时，可以创建强制用户选择更安全、更可靠密码的其他规则。例如，可以要求用户至少选择一定数目的字母、数字、特殊、小写或大写字符。也可以确保用户选择的新密码中不包含被替换的密码，并且被替换的密码中也不包含该新密码。

进程保护

<eTrust Access Control 将保护指定进程，以确保它们不被终止。eTrust Access Control 进程保护也有助于保护 Windows 服务和其他非交互式 Windows 应用程序。

SPECIALPGM 保护

eTrust Access Control 将保护指定程序，如系统服务，这些程序通常必须作为 System 帐户运行，以便仅逻辑用户可以访问它们。

程序和安全的文件保护

<eTrust Access Control 通过为程序和文件提供签名来保护它们。如果签名已经更改，该程序或文件将变为不受信托的，并且无法进行访问。

堆栈溢出保护 (STOP)

STOP 将防止黑客利用堆栈溢出功能，通过该功能黑客可以执行任意命令来入侵系统。

程序通路

程序通路是指要求只能通过特定程序访问特定文件的能力。程序通路大大增加了敏感文件的安全性。<eTrust Access Control 允许您使用程序通路来为系统中的文件提供附加保护。

B1 安全级别认证

eTrust Access Control 包括下列 B1"橙皮书"功能：安全级别、安全类别和安全标签。

Active Directory 管理

下列 eAC> 功能将扩展 Windows Active Directory 服务。

用户属性和组属性

较新版本的 Windows 使用几个唯一标识用户的属性（如全名和登录名），但管理 Windows 较旧版本中的用户属性的 Microsoft Net API 不支持这些属性。

eTrust Access Control 支持这些属性，所以您可以在用户和组的 Active Directory 记录中管理用户定义属性的值。支持这些属性同时增强了组织机构管理。

容器管理

eTrust Access Control 支持 Active Directory 组织机构 (OU) 的创建和编辑。OU 是一个逻辑容器，您可以将用户、组、计算机和其他对象类型置于其中。eAC> 支持三种常用对象类型：**User**、**Group** 和 **Computer**，并且它还通过支持对象类型 OU 来支持 OU 嵌套。这为您提供了下列功能：

- 在除默认容器 USERS 之外的 OU 或容器中新建用户和组
- 在 Active Directory 中创建或删除容器或 OU
- 将用户或组从一个容器或 OU 移动到另一个容器或 OU
- 从 eTrust Access Control 中查看分层的 Active Directory 结构（父子关系）。

可以在主域控制器上创建 OU 类中的对象。

注意：OU 类仅可用于安装了 Active Directory 的 Windows 2000 Advanced Server 工作站。如果 eTrust Access Control 正在具有其他配置的计算机上运行，则该类不适用。

Windows 和 UNIX 的安全管理

通常，大型组织都同时拥有 Windows 和 UNIX 系统。这就使得保持系统的良好安全性的任务变得复杂了。理想情况下，应该开发一个可以在两种类型的系统上实施的安全策略。

使用 eTrust Access Control，可以执行下列操作：

- 开发一个适用于 UNIX 和 Windows 的通用安全策略
- 通过使用 eTrust Access Control 来实施该策略
- 使用一个 Windows 工作站同时管理 Windows 和 UNIX 环境的安全

可以进行更改并让 eTrust Access Control 将更改传播给不同环境中的许多工作站这一功能可以大大减少管理开销。

以下几节讲述通用安全策略中一些特别重要的元素。

维护一组用户

将 eTrust Access Control 安装在站点上之后，就可以维护一个包含所有用户的 eTrust Access Control 数据库。这意味着用户维护只能执行一次。<eTrust Access Control 可以将添加、更改和删除传播到应该接收更新的所有工作站（包括 UNIX 和 Windows）。

维护一个组集

为方便起见，通常将从事特定项目或在组织特定部门中工作的用户组合在一起。Windows、UNIX 和 eTrust Access Control 都允许您定义用户组。您可以像为用户分配权限一样来为组分配权限。使用组可以减轻工作量，因为只须将权限分配给组一次，而不必重复地将相同的权限分配给各个用户。然后，每个用户将会接收到组的权限。

使用 eTrust Access Control 可以创建和维护一组在 UNIX 和 Windows 环境中都可以使用的组。

维护一组访问规则

策略模型服务允许您开发和维护一组同时适用于 Windows 和 UNIX 的访问规则。策略模型数据库 (PMDB) 允许您将安全数据库以及对它所作的任何更改传播给其所有订户。可以让 Windows 和 UNIX 工作站订阅相同的 PMDB。

PMDB 与其订户之间的通信通常是单向的：PMDB 将数据库中的更改发送给订户。只有当订户通知 PMDB 它已处于联机状态、并请求 PMDB 在关闭时发送的所有更改时，该订户才与 PMDB 进行通信。该设计将网络流量减到最少，并确保了订户的完整性。

同步密码

任何理想安全策略的主要部分之一都是强制用户选择有效的密码。如果用户必须仅记住一个可以在整个系统中使用的密码，这就更容易了。通过实施 eTrust Access Control，可以强制执行一组密码规则，并在两个系统间启用密码同步。

PMDB 可以传播定义可接受密码的规则。PMDB 也可以将新密码和更改的密码传播给所有订户工作站，包括大型计算机。

注意:有关详细信息，请参阅《实施指南》。

管理 eTrust Access Control 服务

默认情况下，所有 eTrust Access Control 服务都会自动启动。您可以将任何 eTrust Access Control 服务的启动方式从自动更改为手动，或者禁用该服务。要访问这些服务，请完成以下步骤：

1. 关闭 eTrust Access Control。
2. 从 Windows 的"控制面板"中打开"服务"。
3. 右键单击要更改或禁用的服务。
4. 在"启动类型"中选择"自动"、"手动"或"禁用"，以表明您希望服务以何种方式启动，然后单击"确定"。

eTrust Access Control 文档

eTrust Access Control 文档以 PDF 文件的形式提供。如果您的系统尚未安装 Adobe Reader，要查看 PDF 文件，就必须从 Adobe 网址下载并安装 Adobe Reader。

以下网址提供已更新的指南：http://ca.com/support。

注意：您还可以从产品 CD 中获得适合版本的 Adobe Reader。

自述文件提供 eTrust Access Control 文档的完整列表。

后续内容

由于已经较好地了解了 eTrust Access Control 的功能，接着，您就可以学习如何保护企业的系统完整性和数据的机密性。下一章将指导您保护程序和文件不受用户和组的影响。

第 3 章： 运行管理员界面

此部分包含以下主题：

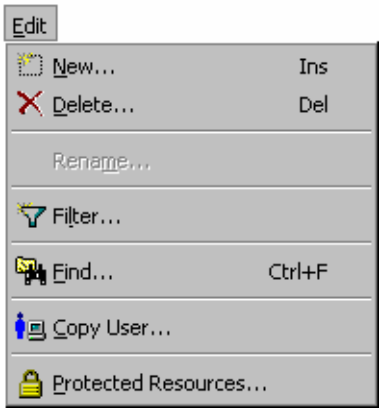
实施和维护安全策略 (p. 27)

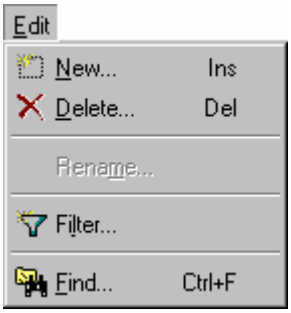
实施和维护安全策略

在本章中，您将了解策略管理器的组成部分 - eTrust Access Control 图形用户界面，您可以在该界面中管理 Windows 和 UNIX 平台上的数据库。

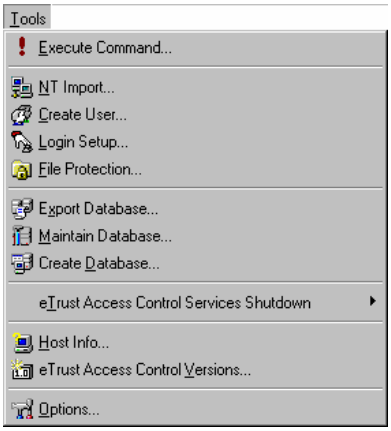
菜单栏和工具栏

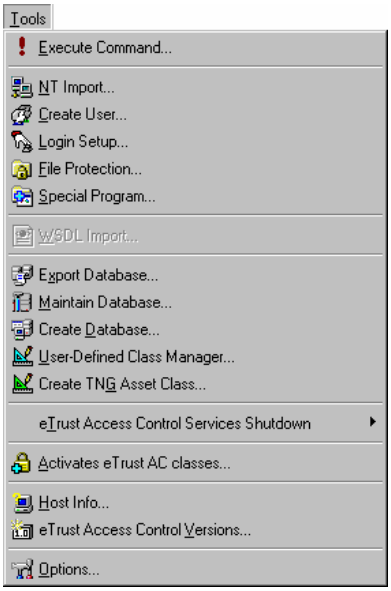
菜单将显示相关信息，具体取决于所打开的窗口。例如，您可以比较"用户"窗口和"资源"窗口的"编辑"菜单：





作为另一个示例，请查看一下"工具"菜单。此处所显示的是"用户"窗口和"资源"窗口的"工具"菜单。



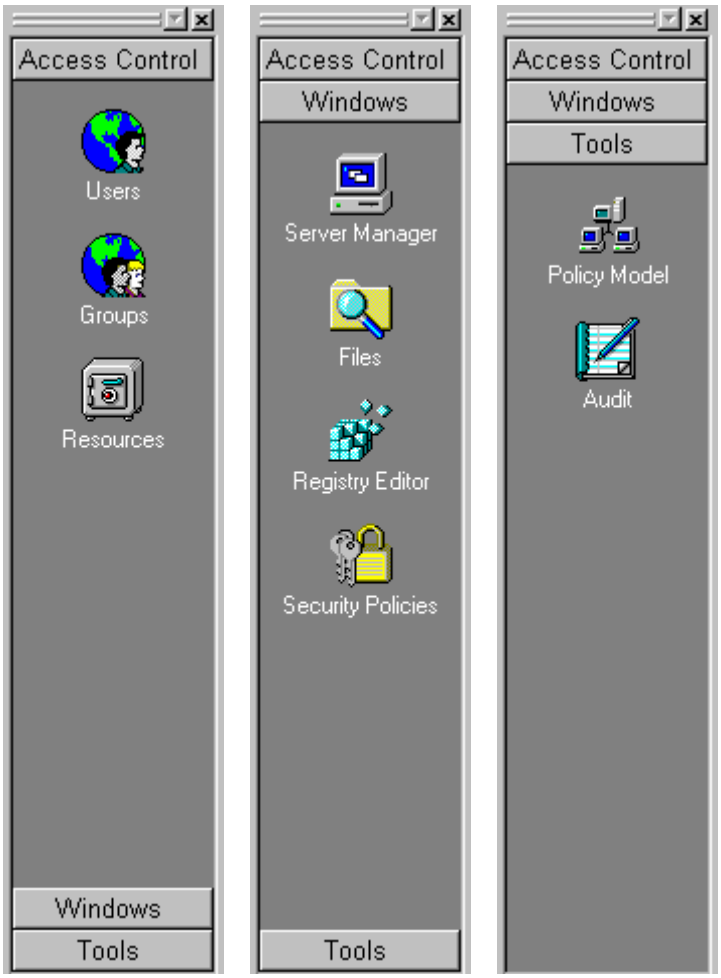


"视图"菜单用于控制工具栏和窗口显示。

程序栏

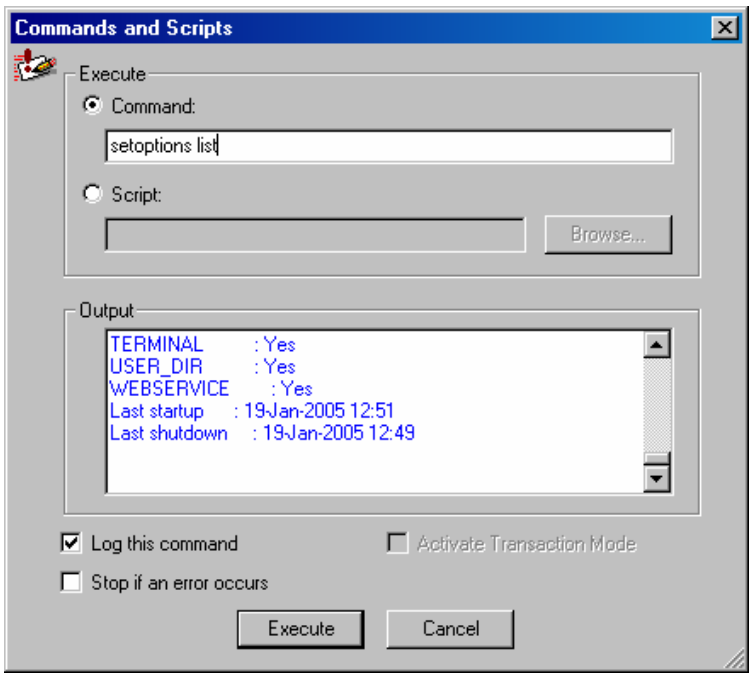
功能被划分成三个程序栏 - eTrust 访问者和资源、NT 资源和工具。使用"文件"、"打开"可以获取同样的功能。

注意:如果已经安装了 eTrust Web AC，您将会看到第四个程序栏，用于管理 eTrust Web AC 功能。这些内容将在 eTrust Web AC 的文档中进行介绍。



selang 命令

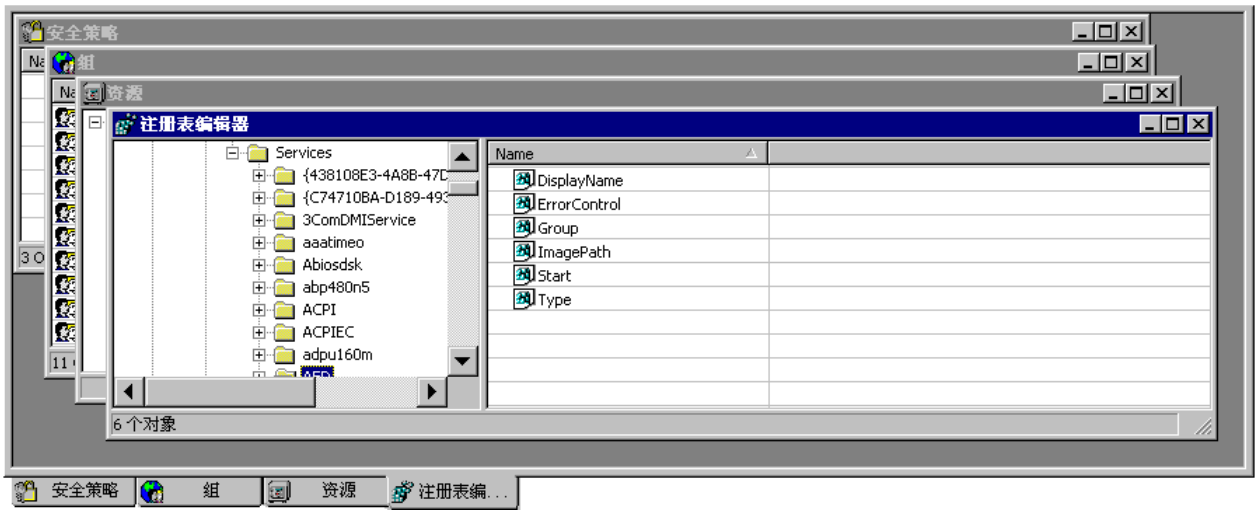
通过在"工具"菜单中选择"执行命令"，可以从策略管理器发出 selang 命令。请在随后显示的"命令和脚本"对话框的"执行命令"字段中输入该命令。



设置管理员默认值

要设置 GUI 默认值，请在"工具"菜单中选择"选项"。

您可以更改任何选项。"外观"和"格式"用于自定义界面，以使您看起来感觉更舒服。例如，工作簿模式将在窗口上放置选项卡。如果在同时打开许多窗口的情况下工作，您可能会觉得这样很方便。



"启动"选项用于设置启动默认值，并激活自定义初始屏幕。"创建"选项可以定义用于新建用户和组的默认环境。您可能希望将默认值更改为 eTrust，从而仅用于完成这些教程。（这将最小化清理）。

注意:单击"确定"后，设置将立即生效。

向导

eTrust Access Control 提供了许多有用的向导来引导您完成常见过程。

使用"登录保护设置向导"

eTrust Access Control 安全性将防止用户从未经授权的终端进行登录。尤其是，必须在 TERMINAL 类记录中定义所有终端，并且所有用户都必须拥有在他们所使用的每个终端的访问控制列表 (ACL) 中定义的访问权限。"登录保护设置向导"考虑到了这一点以及其他因素：

1. 通过单击"向导管理器工具栏"按钮来启动"登录保护设置"向导。选择"登录保护"。
2. 选择要保护的用户和组：

   注意:您可以在"受保护的用户和组"中定义多个用户和组。
3. 在"登录终端"页上，指定用户和组可以（和不能）进行登录的终端：
4. 在"限制用户帐户"页上，指定所指定的用户和组可以进行登录的日期和时间。

   注意：使用"工作日"按钮，可以通过一次单击取消选择"星期六"和"星期日"。
5. 在下一页中，指定假期的登录权限，然后单击"完成"：

注意：要允许或阻止在特定假期登录，在使用该对话框之前，您必须在以前已经在日历中定义了假期。

使用"创建用户向导"

可以使用"创建用户向导"来标识用户。请按照向导中的说明来指定用户属性（如 operator 或 administrator）、密码和组成员身份。

使用"文件保护向导"

使用"文件保护向导"可以保护指定的文件和目录。请按照向导中的说明来选择要保护的文件、可以访问该文件的用户和组以及他们所拥有的访问级别。

使用"NT 导入向导"

如果在安装期间没有导入 Windows 用户和组，请使用"NT 导入向导"：

- 从 Windows 数据库将用户导入到本地主机数据库或 PMDB 中
- 从 Windows 数据库将组导入到本地主机数据库或 PMDB 中

您无法导入到远程主机中。可以直接导入 Windows 数据库，也可以将它保存为脚本文件 (.lng)。

使用"特殊程序向导"

可以使用"特殊程序向导"来保护特殊程序。

可以设置诸如系统服务等程序的权限保护，它通常需要作为 SYSTEM 帐户来运行。可以通过使用逻辑用户或回避来限制对指定程序的访问。

该向导将创建 SPECIALPGM 资源，并在策略管理器窗口的输出栏中显示结果。

使用"复制用户向导"

使用"复制用户向导"可以执行以下操作：

- 将用户记录从一个主机复制到另一个主机，或者复制到同一主机上的 PMDB 中
- 复制用户时将它们添加到组中
- 将多个用户记录从一个主机复制到另一个主机，或者复制到同一主机上的 PMDB 中
- 使用一个用户记录作为模板在同一主机上创建另一个记录
- 创建用于复制用户记录的脚本

注意：要访问复制用户向导，请在 访问控制程序栏上单击"用户"，然后在"编辑"菜单中选择"复制用户"。

使用"复制组向导"

使用"复制组向导"可以执行以下操作：

- 将组记录从一个主机复制到另一个主机，或者复制到同一主机上的 PMDB 中
- 将组及成员用户记录从一个主机复制到另一个主机，或者复制到同一主机上的 PMDB 中
- 将多个组记录从一个主机复制到另一个主机，或者复制到同一主机上的 PMDB 中
- 使用一个组记录作为模板在同一主机上创建另一个记录
- 创建用于复制组记录的脚本

注意：要访问复制组向导，请在 访问控制程序栏上单击"组"图标之后，在"编辑"菜单中选择"复制组"。

后续内容

现在您已经很好地了解了策略管理器，下一章将指导您设置访问和帐户限制等内容，并为您提供有关如何使用新软件的建议。

第 4 章： 了解强大的保护功能

此部分包含以下主题：

从保护程序到监视系统文件 (p. 35)

从保护程序到监视系统文件

在本章中，您将了解如何注册新的用户和组、保护文件和目录、保护文件不受未经授权用户的访问，以及使用程序通路和文件名模式等保护文件，这是使 eTrust Access Control 为您服务的后续步骤。

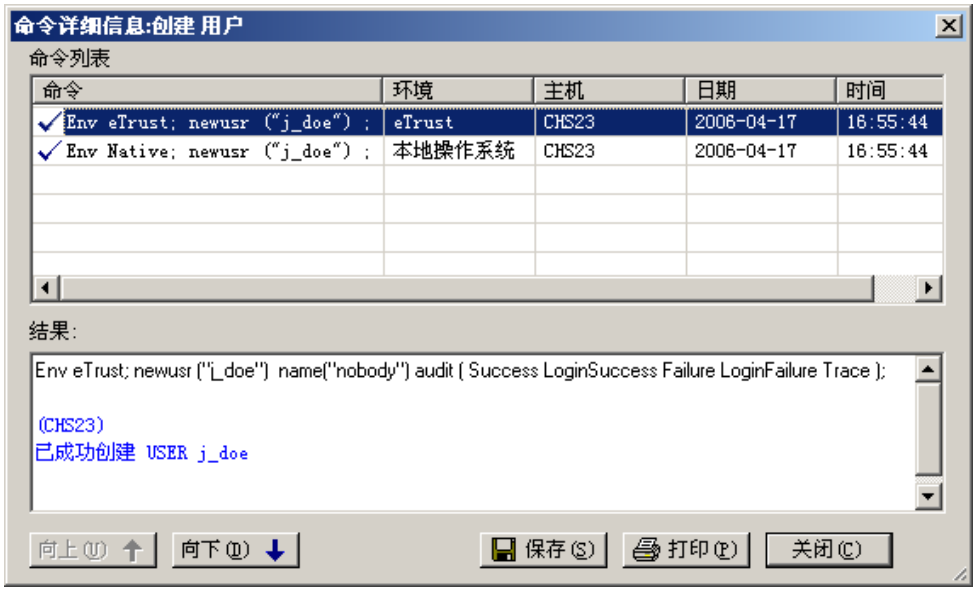
创建用户和组

要创建用户，请完成以下步骤：

1. 单击 GUI 左侧程序栏中的"用户"图标。
2. 在工具栏上，单击"新建"图标。在"用户名"文本框中输入"j_doe"。现在忽略密码选项。
3. 单击"用户属性"。在"所有者"字段中输入"**nobody**"。不要检查任何"用户类型"框，因为 j_doe 是普通用户。
4. 单击"杂项"图标，然后选择"审核信息"。

   注意:标题将显示您正在使用的面板。
5. 单击"全部"，然后单击每个窗口上的"确定"关闭它们。

如果查看该界面的下半部分，您会看到输出栏中显示您已成功地新建了用户。双击条目行可以查看"详细信息"窗口。



该窗口的上半部分显示由策略管理器生成的 selang 命令；下半部分显示结果。选择每个命令可以查看该命令的结果。

您可能已经注意到，该示例非常简单。您可以轻松地将许多其他参数添加到 eTrust Access Control 数据库的用户记录中。

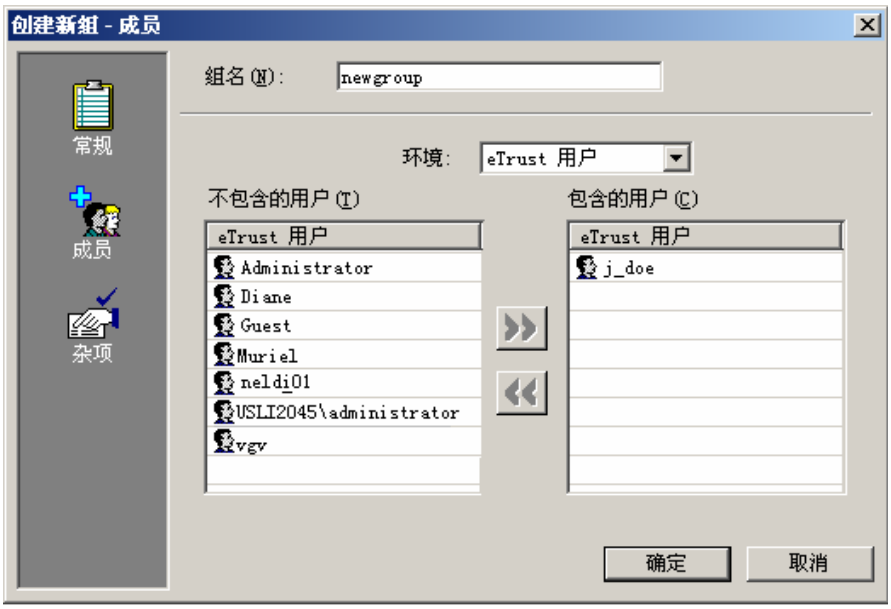
此处为另一个示例。这次将创建一个组。

1. 在程序栏上单击"组"图标，然后单击工具栏上的"新建"图标。"新建组"窗口与"新建用户"窗口非常相似。

   注意：您也可以将鼠标指向"组"窗口中的任何位置，然后单击鼠标右键。"新建组"是您单击鼠标右键时所显示的快捷菜单上的选项之一。

2. 为该组提供一个名称，并指定所有者"**nobody**"。也可以指定超级组。这样，新组将成为子组；它将继承超级组的所有属性，除了您在创建该组时更改或添加的那些属性。

3. 单击 "成员"图标，然后向新组添加某些成员。

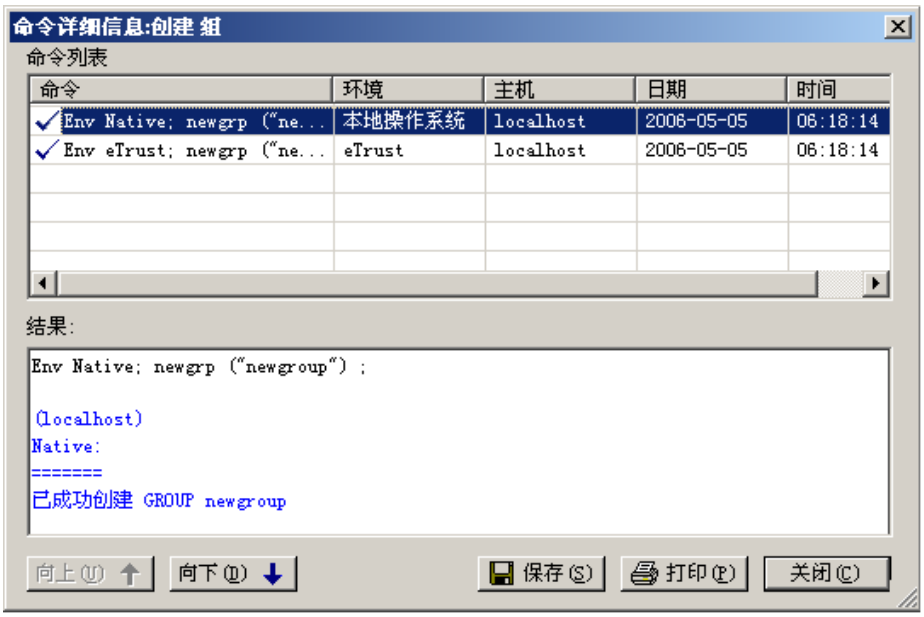


   在该示例中仅添加了一个用户。您可以添加更多用户。选择组时按住 Shift 或 Ctrl 键，可以一次添加几个用户。

4. 将用户添加到组之后，单击"杂项"图标。添加日期和时间限制，然后单击"确定"以创建新组。

   注意:指定给用户的限制优先于指定给组的限制。

5. 现在，请阅读命令详细信息，以查看发生了什么情况。



保护文件和目录

任何计算机系统都至少有两类文件。系统文件是操作系统正常运行所必需的。应用程序文件由站点上的应用程序和用户创建和使用。

您应该确定每类文件应该拥有哪一类保护，然后实施该保护。eTrust Access Control 的主要优点是它可以保护文件和目录免受不必要的访问，甚至免受系统管理员的访问；它还可以将保护扩展到非 NTFS 文件系统。

让我们为该练习创建一个虚拟文件。

1. 单击"程序"栏中的"资源"图标，以打开"资源"窗口。在"系统资源"下，单击"文件"。
2. 单击工具栏上的"新建"图标，使用"浏览"按钮找到该文件，然后定义所有者"**nobody**"。
3. 为某些用户或组授予访问该文件的权限。要执行此操作，请单击"授权"，然后单击"添加访问者"列表框旁边的"添加"按钮。选择用户或组，然后单击"确定"。您所添加的名称会显示在"添加访问者"列表框中。

4. 依次选择每个用户或组，以便为他们选择权限。

   对于管理员 adm1，我们仅选择了"删除"。这是限制管理员访问权限的一个极端示例。

   我们为用户 p_jones 授予了完全权限。（p_jones 的权限如上图中所示）。但 Jones 也是 Newgroup 的成员，该组只有读取权限。由于规则是这些权限是添加的，因此 Jones 不受 Newgroup 成员身份的限制。

   请注意，我们已为该组选择了程序 (Word)。这称为程序通路，意味着这些用户只能使用该特定程序访问文件。程序通路大大提高了敏感文件的安全性。在这种情况下，该组中的任何人都无法使用读取元数据的应用程序打开该文件。

5. 通过指定审核模式并单击"确定"创建文件资源来结束操作。

6. 检查命令详细信息，以查看发出了哪些 selang 命令。

注意:有关文件保护的详细信息，请参阅《参考指南》中的 FILE 类。

文件组

一旦在数据库中定义了文件，就可以对它们进行分组并为组分配权限。例如，可以将财务部门的所有文件放到一个称为 Finance 的组中，然后仅允许高层管理和财务部门的员工进行访问。

基于部门内个人或组对访问文件的需求，组中的各个文件或模式都可以有一组不同的访问者权限。也可以在文件组内嵌套文件组，以获得对文件权限层级结构的详细控制。

保护程序

eTrust Access Control 定义被视为受托计算存储库的一部分的程序。该类中的程序被认为是没有安全漏洞的，因为监视程序会监视这些程序以确保它们未被修改。如果受托程序被更改，eTrust Access Control 会自动将该程序标记为不受托的，并阻止该程序执行。

注意:在 PROCESS 类中定义程序时，还必须为其创建 FILE 类记录。创建这些记录的顺序并不重要。

要保护程序，请查看"资源"窗口的"系统资源"部分。

1. 单击"程序"。

   请注意，数据库已经包含 Microsoft Word 的记录。当您在上一个练习中为 NewGroup 实施程序通路时，eTrust Access Control 就自动创建了该记录。

2. 右键单击 Microsoft Word 的条目，然后选择"属性"。

   您只能为访问者分配"执行"权限。"拒绝"权限将阻止访问该程序。

3. 单击"常规"图标。

   "常规"面板中有一个标记为"托管"的复选框。当您创建程序记录时，eTrust Access Control 会设置该属性。如果程序已被修改，eTrust Access Control 会将该属性重置为"不受托"，并阻止该程序执行。问题修复后，您可以在该窗口中重置托管属性。

监视文件

eTrust Access Control 可以监视重要的系统文件。通过在 SECFILE 类（具有代表安全文件的对象的类）中创建记录，您可以验证未经授权的用户没有更改经常被修改的敏感系统文件。监视程序将扫描这些文件，并确保有关这些文件的已知信息未被修改。

下面是要包括的文件类型的一些示例：

- \Winnt\system32\drivers\etc\hosts
- *\etc\services
- *\etc\protocol
- *\etc\networks

保护进程不被终止

在其自身的地址空间中运行的可执行文件可能需要保护，以防被终止或"绝杀"。主要的实用程序和数据库服务器是 eTrust Access Control 进程保护的理想对象，因为这些进程是拒绝服务攻击的主要目标。eTrust Access Control 进程保护也有助于保护 Windows 服务和其他非交互式 Windows 应用程序。

eTrust Access Control 可以防止三种绝杀信号：常规终止信号 (TERM) 和两种应用程序无法屏蔽的信号（Terminate Process 和 STOP）。

作为一个示例，我们将保护任务管理器 (Taskmgr.exe)。

1. 选择"进程"，然后单击"新建"。
2. 为 Taskmgr.exe（位于 \system32 子目录中）新建一个记录。

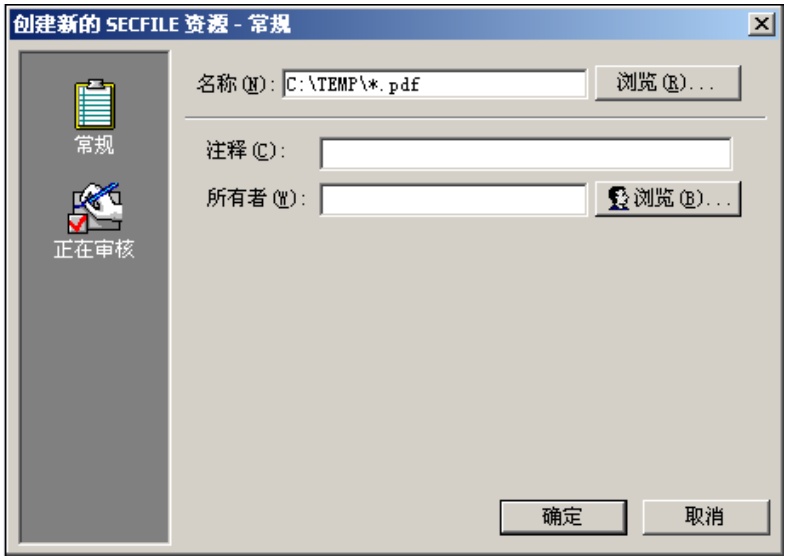
   注意：Taskmgr.exe 必须处于活动状态（即，显示在 Windows 任务栏上），以便在使用"浏览"按钮时显示为选中内容。
3. 授权用户终止该进程。"读取"权限意味着用户可以终止该进程；"拒绝"权限意味着用户无法终止该进程。

程序模式

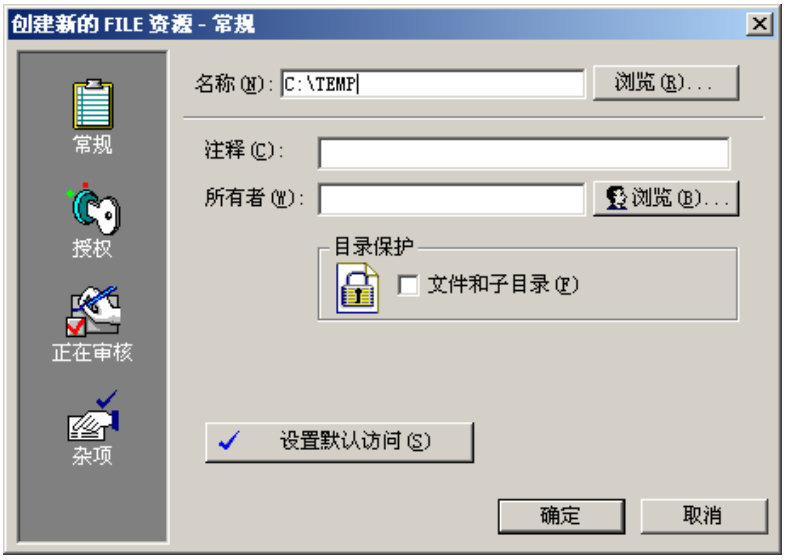
定义系统中每个文件的文件资源可能非常繁琐。eTrust Access Control 提供了可以加速这一过程的工具。

以下示例描述了保护文件组的快速方法。通过指定模式，而不是特定名称，您可以对适合该模式的所有文件强制执行相同的访问限制。

在"资源"窗口中选择"监控的文件"，并单击"新建"。



您也可以保护目录。



请注意用于保护文件和子目录的复选框。尝试在选中和未选中该复选框的情况下创建文件资源。您将在资源列表中看到差异。检查命令详细信息，以查看发出的不同命令。

保护其他资源

注意 eTrust Access Control 可以保护的其他资源类型。在"资源"窗口中展开树，您会看到 eTrust Access Control 可以监视重要系统组件，如您的网络和 Windows 注册表。

利用预定义的组限制访问

eTrust Access Control 包含四个预定义的组，可以用来限制对文件的访问：

- _abspath
- _interactive
- _network
- _restricted

使用 _restricted 组

将用户添加到 _restricted 组中将阻止他们访问没有明确为其授予访问权限的任何文件。这包括未在数据库中列出的文件。这些文件由 FILE 类的默认访问值控制。安装时，该默认值会自动设置为"none"。

注意:如果将用户添加到 _restricted 组，并且数据库中包含极少的 FILE 访问规则，_restricted 用户可能无法执行任何操作。如果您计划将用户添加到 _restricted 组，并使用 NONE 作为 FILE 类的默认访问权限，请考虑使用警告模式。然后，审核事件将显示 _restricted 用户工作时所需的文件。稍后，您可以授予适当的权限并关闭 WARNING 模式。

您已经了解了如何将用户添加到组。将用户添加到 _restricted 组的过程完全相同。

要提升安全性，请重置 FILE 类的审核模式。

1. 在"资源"窗口中，打开"管理"文件夹，然后单击"按类访问"。双击"FILE"。

   注意:如果将光标停留在"设置默认访问权限"按钮上，工具提示将显示当前的默认访问。

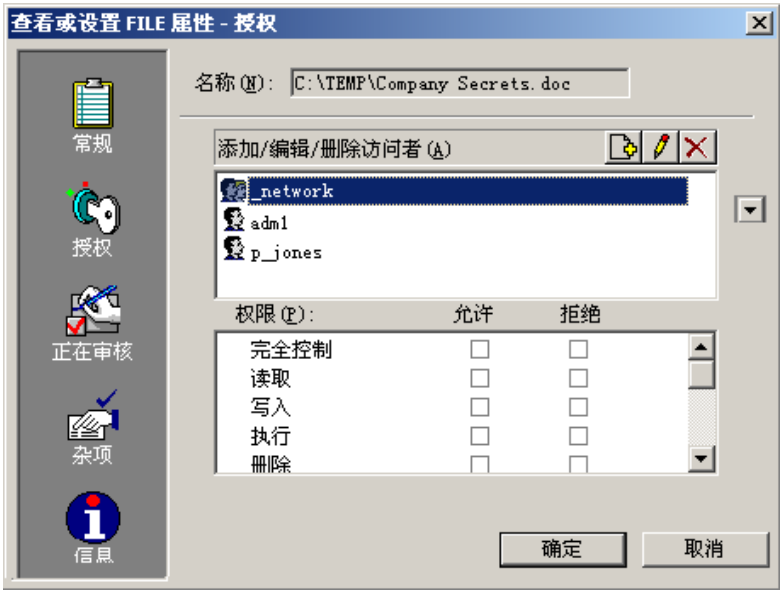
2. 打开"审核"面板。清除"失败"，并选择"警告模式"。
3. 现在，您可以测试将用户添加到 _restricted 组的结果。

注意:eTrust Access Control 仅在启动时才会读取 _restricted 用户列表。如果用户已经加入或离开 _restricted 组，则仅当重新启动 eTrust Access Control 时，更改才生效。

使用 _network 和 _interactive 组

_network 组定义从网络到特定资源的访问权限。_interactive 组定义允许从特定资源所驻留的计算机上访问该资源的权限。这些组适用于所有资源，而不仅仅是文件。它们也适用于所有用户；任何用户都不必显式添加到这些组中。

现在来看一个示例。



此处，我们已经添加了 _network，它对文件 Company Secrets.doc 的访问控制列表 (ACL) 没有任何权限。这意味着无法从网络访问该文件。_interactive 在本地主机上以相同方式运行。请记住，不要将用户添加到这些组中。

注意:在 eTrust Access Control 中，_network 和 _interactive 组之间没有连接。您可以将它们添加到相同的资源中。

后续内容

现在，您已经对如何创建用户和组以及保护文件、目录和程序有了很好的了解。下一章将指导您了解管理员界面。

第 5 章： 获得对用户帐户更多的控制

此部分包含以下主题：

限制用户访问和权限 (p. 45)

限制用户访问和权限

在本章中，您将设置管理员权限、限制从终端访问、设置日内某时和周内某日规则，以及设置条件访问权限等，这是使 eTrust Access Control 为您服务的后续步骤。

限制 Administrators 的使用

计算机网络的主要安全风险之一在于未经授权的用户可能会获得对 Administrators 组用户帐户的控制。如果发生这种情况，未经授权的用户可能会对系统造成巨大破坏。

eTrust Access Control 允许您限制授予 Administrator 帐户的权限，以及限制作为 Administrators 组成员的用户的权限。然后，您可以将管理员类型的权限分发给一般用户，使他们不必成为 Administrators 组的成员即可执行管理任务。该功能称作任务委托，它是 eTrust Access Control 最重要的优点之一。

用户类型

eTrust Access Control 提供了许多用户类型，它们都具有部分管理员权限。为用户分配这些属性通常是分发管理员权限的第一步。

下面是 eTrust Access Control 的一些用户类型：

组管理员

可以执行某个特定组内大多数管理功能的用户。

子管理员

可以管理管理员所指定的类与资源的用户。

密码管理员

具有修改其他用户密码设置的权限的用户。

组密码管理员

具有修改某个特定组内其他用户密码设置的权限的用户。

审核员

具有读取审核日志权限的用户。他们还可以确定在每次登录和每次尝试访问资源时要执行的审核类型。

组审核员

可以读取特定组的审核日志的用户。他们还具有确定该组内要执行的审核类型的权限。

操作员

可以显示（读取）数据库中所有信息的用户。

组操作员

可以显示其自身定义所在的组的数据库中所有信息的用户。

注意:请不要混淆 Administrators 组（是本地 Windows 的一部分）与组管理员（不是本地 Windows 的一部分）。

您可以在本地环境中和 eTrust 环境中定义这些特殊的用户类型。但他们的特殊权限是 eTrust 的一部分，而不是 Windows 的一部分。

新建用户或修改当前用户记录时，您可以分配用户属性。策略管理器支持分配 eTrust 数据库中的属性。

要将用户属性分配给当前用户，请单击"用户"图标。在结果列表中选择该用户名，然后单击"用户属性"。

要分配仅应用于组内的属性，请单击"组"图标。在"成员属于"列下选择该组名，然后单击"组属性"。

该属性为用户 j_doe 授予审核访问者和组管理员所拥有的资源的权限。

注意:当您指定组为访问者或资源的所有者时，该组的管理员、审核者和其他成员都将对该访问者或组拥有相应的管理权限。

限制从终端访问

eTrust Access Control 提供了几种限制用户访问权限的方法。这些方法包括设置帐户的截止日期、设置宽限登录、限制在特定日期和时间登录，以及控制用户登录的终端。我们将在本节中对终端进行说明，而在下一节中讨论时间限制。

使用向导新建用户之后，我们使用登录设置向导为该用户定义了终端。请记住，如果不将该用户与某个终端匹配，将会阻止该用户登录或访问受保护的资源。现在来详细了解一下"终端"资源。

首先，您需要在本地环境中定义一对用户。如果尚未定义，请现在定义。为了节约时间，请将当前的 eTrust 用户添加到本地环境中：

1. 选择一个用户，单击工具栏上的"属性"图标，然后使用"高级"按钮添加本地环境。

   注意：您还可以右键单击用户，然后在快捷菜单中选择"属性"。

2. 将终端权限分配给该用户：

   a. 单击程序栏上的"资源"图标，然后单击"登录保护"旁边的加号来打开树。

   b. 选择"终端"，然后双击您的本地主机。

   c. 打开"授权"面板，然后为"添加访问者"单击"插入"图标。

   d. 使用浏览按钮添加用户，然后单击"确定"。

   e. 选中"读取"和"写入"权限的"拒绝"框。

   用户 j_doe 现在已被阻止使用名为 workstation1 的终端。

3. 现在对其他用户重复以上授权，这次分配"读取"权限。

   注意:要允许用户管理终端，请分配"读取"和"写入"权限。

4. 注销计算机，然后分别尝试用每个用户身份进行登录。用户 j_doe 应该收到登录错误消息，但用户 b_raines 可以访问该终端。

重要！此练习完成后进行清理时，**请勿**删除您计算机的终端资源。（您可以删除远程计算机的终端资源）。**请勿**在您的计算机上删除或更改您自己的读取和写入权限。否则，您将无法管理 eTrust Access Control。您可能将无法还原，除非重新安装该软件。

终端组

如果您要对几台计算机指定相似的限制，则可将它们放在一个终端组中，然后一次为所有计算机授权。

1. 在"资源"窗口中选择"终端组"，然后单击工具栏上的"新建"图标。
2. 为该组提供名称和所有者。
3. 打开"成员身份"面板。单击"添加/删除成员"的"新建"图标，然后选择终端。

   注意:按住 Ctrl 键或 Shift 键可以同时选择多个终端。
4. 如前面所述完成授权和审核。
5. 检查命令详细信息以查看生成了哪些 selang 命令。

限制模拟请求

当用户尝试从其用户名切换到其他用户名时，将生成模拟请求。模拟请求可以直接来自 RunAs 命令，或来自任何使用合适的 Win32 API 的程序。

eTrust Access Control 通过对模拟请求强制实施限制来保护管理员和其他用户。作为示范，请按以下步骤进行操作：

1. 选择一个您已知其密码的用户名。在以下命令中，user001 代表您所选择的用户名。

   在"资源"窗口中，选择"用户标识控制"、"用户 ID 替换"，然后单击工具栏上的"新建"。
2. 在策略管理器中定义以下规则：

该规则告诉 eTrust Access Control 阻止用户 user001 的模拟请求，除非经过明确授权，否则不允许任何人模拟 user001。

您可以按照以下步骤测试 surrogate 规则。

- 在 windows shell 中，输入以下命令：

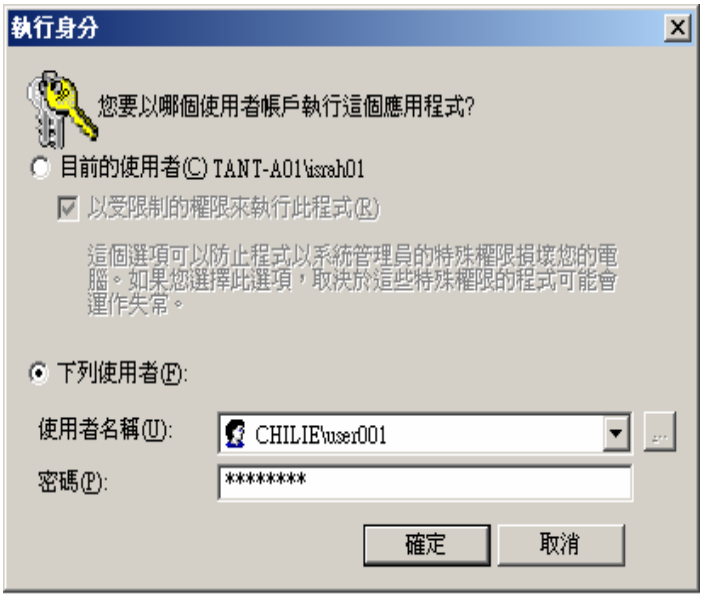
  ```
  cmd> RunAs /profile /USER:CHILE\user001 cmd.exe
  ```

  - 输入 CHILE\user001 的密码

    系统将返回以下消息：

    ```
    Attempting to start "cmd.exe" as user "CHILE\user001"...
    RUNAS ERROR:Unable to run - cmd.exe
    5: Access is denied.
    ```

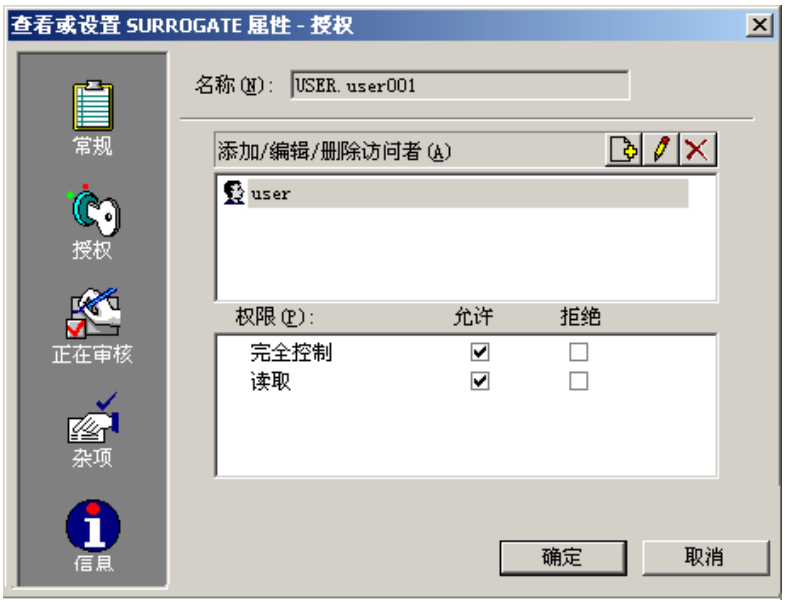
- 在 Windows 的"以其它用户身份运行"对话框中，输入：



系統將返回以下消息：

在审核窗口中，您可以发现模拟事件遭到了拒绝，原因是没有规则为您授予访问权限。

如果您希望让 eTrust Access Control 允许您模拟 user001，请在 eTrust 策略管理器窗口中指定以下规则。如果您希望成为唯一可以对 usr001 进行模拟的用户，则可以指定自己的用户名。如果您希望允许所有 eTrust Access Control 定义的用户都可以对 usr001 进行模拟，则可以使用星号 (*) 作为用户。



注意：如果不使用授权命令明确授权这种模拟请求，即使是超级用户也无法模拟 user001 。

设置日内时和周内某日规则

系统最容易遭受攻击的时间通常在夜间和周末，因为这些时候几乎没有审核者或其他职员在场。使用 eTrust Access Control，您可以限制用户只能在一天的特定时间和一周的特定日子登录，从而提供了更高的安全级别。

可以通过向用户添加时间限制开始设置。

1. 选择一个用户，然后打开"用户属性"窗口。通过在"杂项"面板上单击"时间/日期限制"按钮来设置时间限制。

   默认值为一天 24 小时，一周 7 天。您可以根据需要取消选择任意日期。时间适用于所有选定日；不能为每天设置不同的时间。

   您还可以选择 Unicenter TNG 日历来使用"日历"功能。

2. 完成设置限制后，单击"确定"。
3. 尝试在授权时间和未授权时间内作为该用户登录以查看结果。

帐户锁定

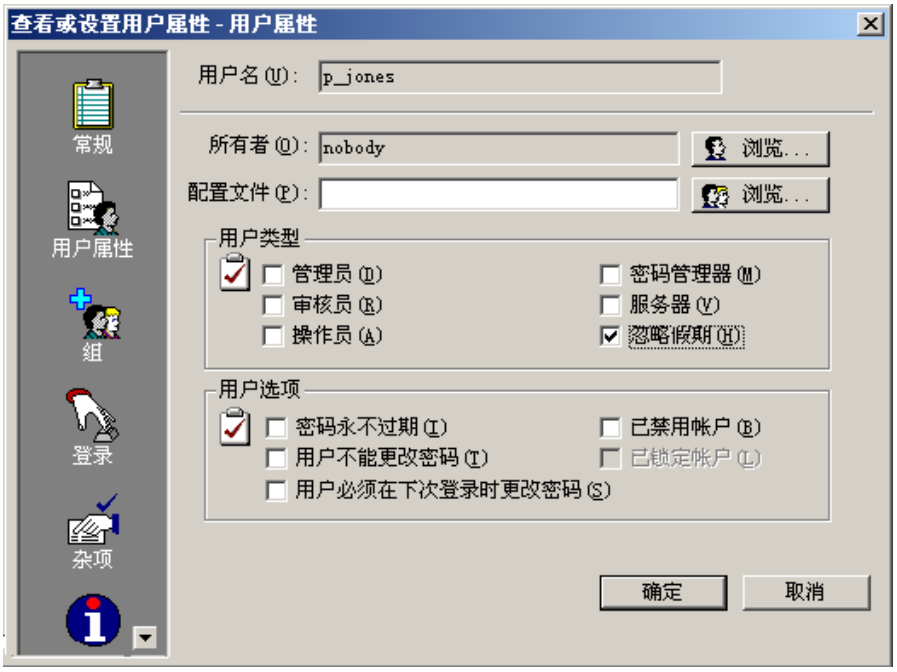
在前面的示例中，我们为 Peter Jones 授予了额外的登录访问权限，大约是标准的每天上午 9 点至下午 5 点。。这些时间仅与登录相关。一旦登录之后，他可以在网络上停留任意长的时间。如果希望从下午 6 时起阻止 Peter 停留在网络上，则必须执行下列步骤来进行相应设置：

在"策略"菜单中选择"帐户"。"帐户锁定"选项卡的底部有一个复选框用于强制注销。

设置假期信息

限制用户可以访问系统的时间的另一种方法是定义假期。假期将阻止所有未被授予特殊权限的用户访问系统。

注意:确保您自己没有被锁定于系统之外的最佳方法是，在开始本练习之前更改您的用户属性，使之包括"忽略假期"。这将为您授予在所有假期登录的权限。请查看下面的插图。



要设置假期，请完成以下步骤：

1. 再次打开"资源"窗口。
2. 在"登录保护"下选择"假期"。
3. 单击工具栏上的"新建"图标以新建一个"假期"资源。

   选择"假期"图标后可以添加日期。在单个"假期"资源中，可以根据需要添加任意多个假期，如果您希望对权限进行更多的控制，还可以定义单独的假期。
4. 输入开始日期和结束日期，或单击日期字段旁边的箭头下拉日历，然后指向并通过单击来选择日期。默认情况下将全年的每一天都设置为假期，但您可以通过取消选中相应的复选框来更改设置。
5. 接下来分配授权权限。每个授予了"读取"权限的用户或组都可以在指定假期登录。

6. 创建今天作为一个假期资源。为某些用户授予"读取"权限，为另一些用户授予"无"权限，而其他用户则根本不保留在列表中。
7. 现在，尝试用每个用户的身份进行登录。

资源

也可以在资源上应用时间限制。对于终端、文件、网络保护对象、容器对象和注册表对象，实际上对于任何资源，您都可以限制只能在特定日期和时间访问它们。

上述限制过程与对用户进行时间限制完全相同。选择一个资源，打开"属性"窗口，然后在"杂项"面板中输入限制。

后续内容

现在您已经对如何限制用户访问和权限有了很好的了解，这将有助于您控制网络安全。请阅读下一章，它将指导您保护网络、控制传出连接以及其他操作。

第 6 章： 保护网络活动

此部分包含以下主题：

控制网络级访问 (p. 55)

控制网络级访问

在本章中，您将练习保护网络的 TCP/IP 连接访问 - 这是使 eTrust Access Control 为您服务的后续步骤。

保护网络 (TCP/IP)

TCP/IP 网络的开放性既是其最具吸引力的功能，但就安全而言，也是它的一个主要缺点。作为网络保护程序，eTrust Access Control 提供了防火墙功能，不必使用专用计算机。使用 eTrust Access Control，可以允许特定客户端向特定主机发送特定 TCP/IP 服务，但仅允许某些主机向本地主机发送特定 TCP/IP 服务。

控制传入连接

要查看 eTrust Access Control 如何防止计算机受到来自网络的未授权访问，请执行以下步骤：

1. 检查是否激活了 HOST 类。
   a. 在"工具"菜单中选择"激活 eTrust Access Control 类"。

      此时将显示"激活 eTrust 类"对话框。

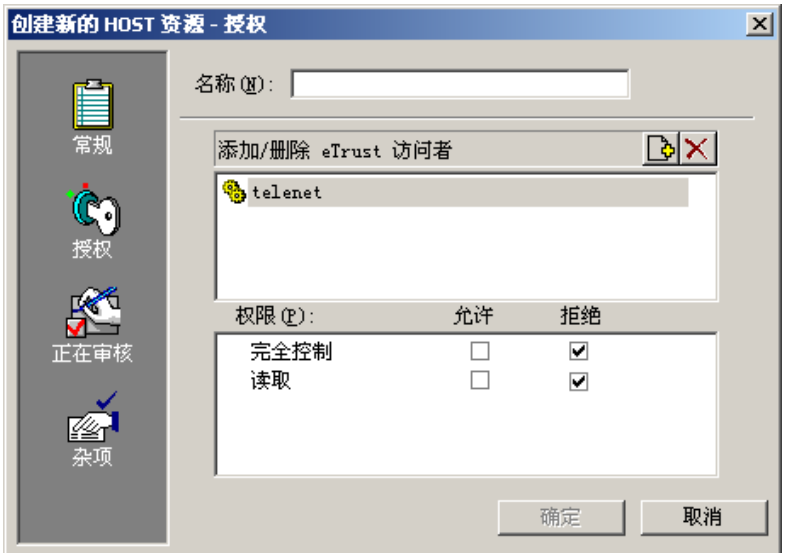
   b. 滚动直至找到 HOST。如果未选中"HOST"框，请选中它并单击"确定"。
2. 选择另一台计算机（与正在运行 eTrust Access Control 的计算机相连）并定义为主机。在下面的示例中，workstation2 代表您已经选择的计算机。

3. 将 workstation2 定义为主机。

   在"访问控制"程序栏上，单击"资源"图标，展开"网络保护"并选择"主机"。然后单击工具栏上的"新建"图标。此时将显示"新建 HOST 资源 - 常规"对话框：

   使用左侧的图标，输入新 HOST 记录的信息。使用"授权"图标输入授权信息，包括服务（如 TCP/IP）或端口：

4. 为本地主机授予权限，以接收来自 workstation2 的所有 TCP/IP 服务（Telnet 除外）。为此，请拒绝 Telnet 权限：



5. 尝试从 workstation2 进行 telnet 登录。您的尝试应该被拒绝。

6. 尝试从 workstation2 进行 ftp 登录。由于 ftp 是非 telnet 的 TCP 服务，ftp 请求应被接受。

注意：另外，也可以在主机组级、网络级和名称模式级指定 TCP/IP 访问规则。

在主机组级别保护

要定义主机组，请在 GHOST 类中创建数据库记录。该主机组接收授权的方式与单个主机相同。

注意：正如对单个用户一样，单个主机的任何一个特定规则都将覆盖组规则。

要在"访问控制"程序栏中对资源设置 TCP/IP 访问规则，请单击"资源"图标展开"网络保护"，并选择"主机组"。然后单击工具栏上的"新建"图标。

在网络级别保护

另外，还可以在网络级别指定 eTrust Access Control 访问规则。要定义网络，请在类 HOSTNET 中创建数据库记录。然后，该网络将以与单个 HOST 记录相同的方式接收授权。

注意:主机组级别上的任何规则都将覆盖网络级别规则。

要从"访问控制"程序栏中对资源设置 TCP/IP 访问规则，请单击"资源"图标展开"网络保护"，并选择"主机网络"。然后单击工具栏上的"新建"图标：

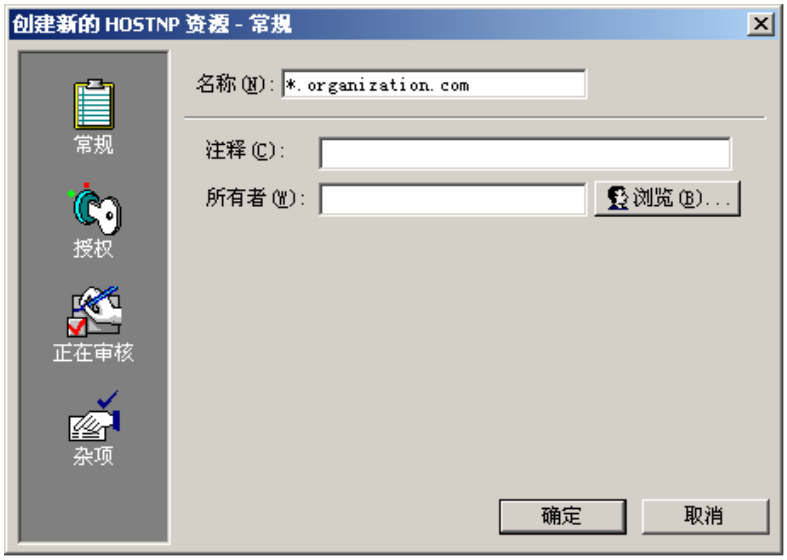
使用名称模式保护

定义 TCP/IP 访问规则的另一种方法是通过使用 HOSTNP（主机名称模式）类的名称模式服务。网络接收授权的方式与单个 HOST 记录相同。

注意:网络级别的任何规则都将覆盖名称模式级别规则。

要对资源设置 TCP/IP 访问规则，请单击"访问控制"程序栏上的"资源"图标展开"网络保护"，并选择"根据名称进行主机保护的模式"。然后单击工具栏上的"新建"图标。

此时将显示"新建 HOSTNP 资源"对话框：



控制传出连接

可以将每个计算机的传出连接作为另一种资源类型进行管理。

通过在网络中限制传出连接，可以将设法穿过防火墙入侵的破坏者所造成的损失降至最低。也可以将合法的 Internet 访问者限制在网络中特定一组服务和系统内。例如，您可以只允许电子邮件和几种必要形式的数据库访问。

要查看 eTrust Access Control 如何限制传出连接，请执行以下步骤：

1. 检查是否激活了 CONNECT 类。
   a. 在"工具"菜单中选择"激活 eTrust Access Control 类"。

      此时将显示"激活 eTrust 类"对话框。

   b. 滚动直至找到 CONNECT。如果未选中 CONNECT 框，请选中它并单击"确定"。
2. 选择另一台计算机（与正在运行 eTrust Access Control 的计算机相连）并定义为连接资源。在下面的示例中，workstation2 代表您已经选择的计算机。
3. 将 workstation2 定义为连接资源。为此，请在"访问控制"程序栏中单击"资源"图标展开"通用"和"网络保护"文件夹，并选择"主机的传出连接"。然后单击"新建"按钮。
4. 在您的计算机上，尝试使用 telnet 或 FTP 连接 workstation2。您的尝试应该被拒绝。
5. 向用户 j_doe 分配连接权限：
   a. 单击程序栏上的"资源"图标，并单击"网络保护"旁边的加号以打开树。
   b. 选择"主机的传出连接"，然后双击 workstation2。
   c. 单击"授权"图标以打开"授权"页，然后单击"添加访问者"的"插入"图标。
   d. 使用"浏览"按钮添加用户 j_doe，然后单击"确定"。
   e. 选中"读取"权限的"允许"框。

   现在，虽然所有用户的访问规则均为"拒绝"，但却允许用户 j_doeis 使用 telnet 或 FTP 连接到 workstation2。

面向服务的 TCP/IP 规则

eTrust Access Control 还提供面向服务的 TCP/IP 访问规则（除本章前面提到的面向主机之类的规则之外）：

这几类访问规则可以通过特定 TCP 服务（端口）管理传入和传出连接。要定义这种规则，请使用 TCP 类。

要查看 eTrust Access Control 如何使用面向服务的 TCP/IP 规则保护计算机，请执行以下步骤：

1. 停止 HOST 和 CONNECT 类。
   a. 在"工具"菜单中选择"激活 eTrust Access Control 类"。

      此时将显示"激活 eTrust 类"对话框。

   b. 滚动直至找到 HOST。确保未选中"主机"框。

   c. 滚动直至找到 CONNECT。确保未选中 CONNECT 框。

   d. 单击"确定"。

2. 将 Telnet 定义为 TCP 服务：

   在"资源"窗口中，选择"网络保护"、"TCP 保护"，然后单击工具栏上的"新建"。

   为本地主机授予与所有计算机进行 Telnet 活动的权限，但不包括从 workstation2 接收 Telnet 通信。要执行该操作，请在"新建 TCP 资源 - 常规"对话框中单击"设置默认访问权限"按钮，并选择"全部"。 单击"确定"。

3. 单击"权限"图标以输入授权信息。在"新建 TCP 资源 - 授权"对话框中单击"插入"图标，接着在"添加/编辑 eTrust 访问者"对话框中单击"浏览"按钮，选择"主机"，然后选择"workstation2"。

   确保未选中 workstation2 的"读取"和"写入"权限。

4. 尝试从 workstation2 进行 telnet 登录。您的尝试应该被拒绝。

5. 为所有计算机授予与本地主机进行 Telnet 活动的权限，但不包括用户 p_jones 向 workstation2 发送 Telnet 通信。

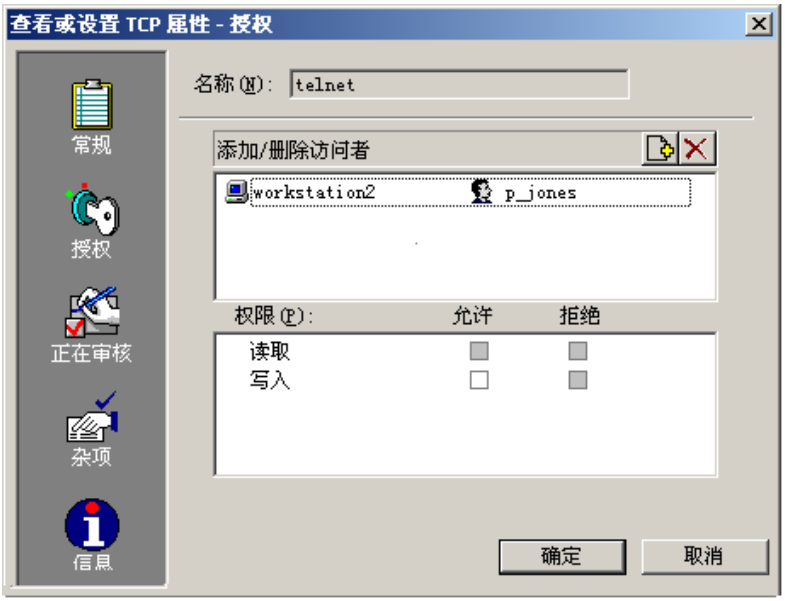
   注意:您已经为所有主机设置了 Telnet 资源的默认访问权限。

   a. 单击"查看或设置 TCP 资源"对话框上的"权限"图标。

   b. 单击"插入"图标，在"添加/编辑 eTrust 访问者"对话框上单击"浏览"按钮，然后选择"主机"，再选择"workstation2"。

   c. 选中"传出的连接"框，在"名称"字段中输入 p_jones。

   d. 单击"确定"。您的对话框应类似如下显示：



6. 作为用户 p_jones 登录，并尝试使用 Telnet 连接到 workstation2。您的尝试应该被拒绝。

后续内容

现在您已经详细了解了如何保护网络，下一章将指导您设置密码策略。

第 7 章： 设置密码和审核策略

此部分包含以下主题：

密码、登录和审核规则 (p. 63)

密码、登录和审核规则

在本章中，您将定义密码策略、更改密码、激活策略检查、审核策略以及执行其他更多操作。策略管理器则简化了默认安全策略的设置。

安全策略包括密码规则、登录规则和审核规则。可以为用户设置一个通用策略，也可以在逐一为各个组设置不同策略。有些设置是全局的，但其他设置（例如，最小与最大时限和宽限期）可以被单个用户设置覆盖。

设置密码策略

在定义密码策略之前，请检查是否激活了密码策略检查。（这是新安装的默认设置。）

1. 在"工具"菜单中选择"激活 eTrust Access Control 类"。

   此时将显示"激活 eTrust 类"对话框。

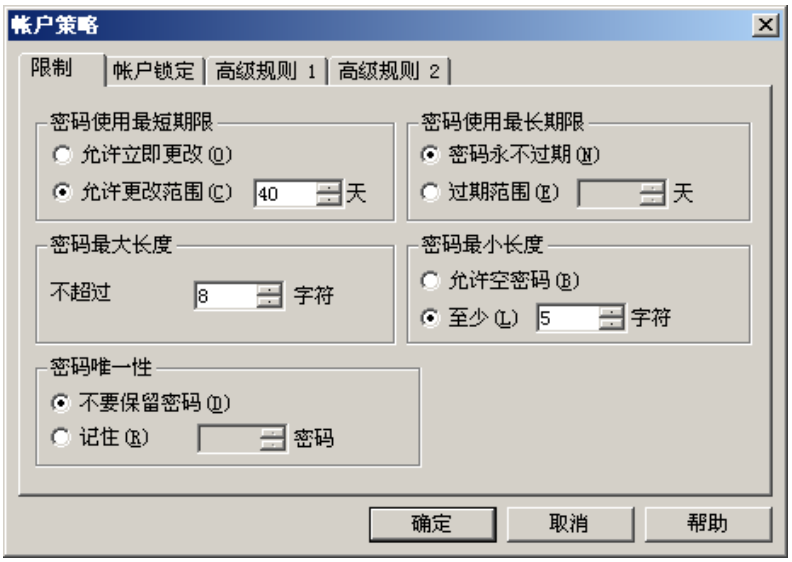
2. 滚动直至找到 PASSWORD。如果 PASSWORD 框没有选中，请选中它并单击"确定"。

   在进行该更改或任何其他更改之前，请检查密码规则默认值。记录下这些设置，以便在完成本节中的练习之后可以将其还原。

3. 检查 eTrust Access Control 中的当前值后，可以根据您站点的需要来更改这些值。有关详细信息，请参阅《管理员指南》。

4. 要设置一般用户帐户策略，请激活"用户"窗口。在程序栏中选择"用户"图标。然后在菜单栏中选择"策略"。可在该菜单中设置"帐户"或"审核"策略。

   "帐户策略"窗口有四个选项卡。前两个选项卡设置同时适用于本地操作系统和 eTrust 数据库的规则。"高级规则"选项卡仅设置 eTrust 策略。



5. 更改某些参数。可以通过测试系统上的各种限制来检查结果。

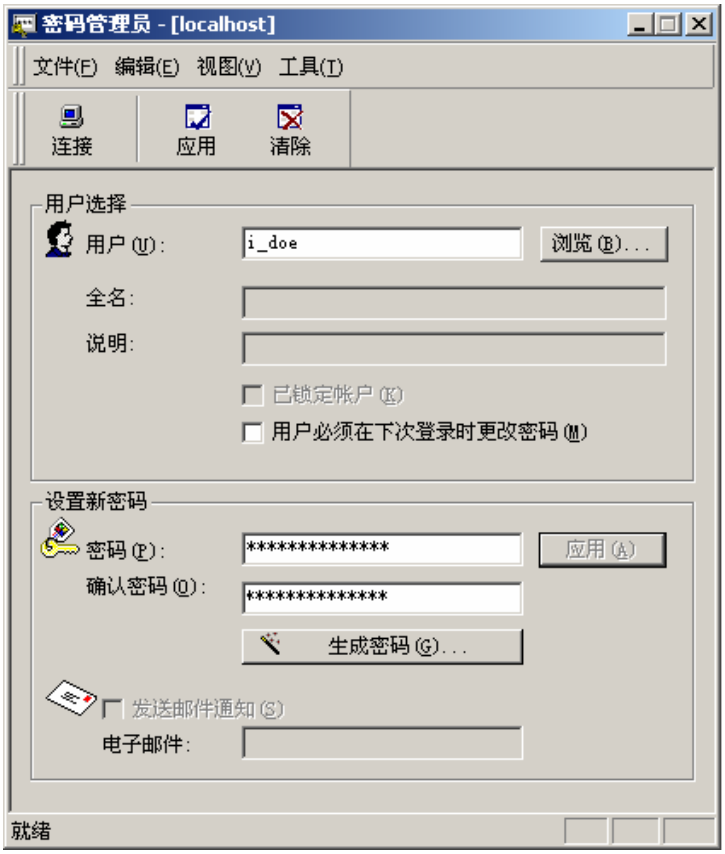
   高级规则设置 eTrust 密码策略。"登录次数"字段代表宽限登录参数。

   注意:有关宽限登录的详细信息，请参阅《管理员指南》。

更改密码

更改用户密码时不需要使用策略管理器。在数据库中指定为密码管理员的用户只须在其工作站上安装密码工具 (SetPwd.exe) 即可，可以通过任务栏上的"开始"按钮找到该工具。

依次选择"开始"、"程序"、"CA"、"eTrust Access Control"、"密码管理器"。密码管理员工具可以更改所有用户在本地环境中定义的密码。



在本地环境中设置审核策略

在"策略"菜单中选择"审核"可以设置审核策略。

尝试更改一些参数。查看命令行详细信息可以检查结果。

打开 Windows 事件查看器可以看到更改结果。

清理

请务必将密码和审核策略重置为最初的默认值。

后续内容

现在您已经对 eTrust Access Control 中的密码和审核策略有了很好的了解，下一章将指导您管理多个主机。您将创建策略模型数据库、将工作站指向 PMDB、使用策略模型以及执行其他操作。

第 8 章： 集中管理

此部分包含以下主题：

创建用户、安全策略和其他 (p. 67)

创建用户、安全策略和其他

在本章中，您将创建策略模型数据库 (PMDB)，并注册用户、权限和密码。事务管理器自动将在本地主机上执行的 eTrust Access Control 事务发送给多个主机。

创建 PMDB

在下面的示例中，我们创建一个名为 policy1 的 PMDB，并将 PMDB 的 workstat1 和 workstat2 注册为其订户。为了简化该示例，我们在同一主机上创建订户。

要注册两个授权管理 PMDB 的用户 adm1 和 adm2，请执行以下步骤：

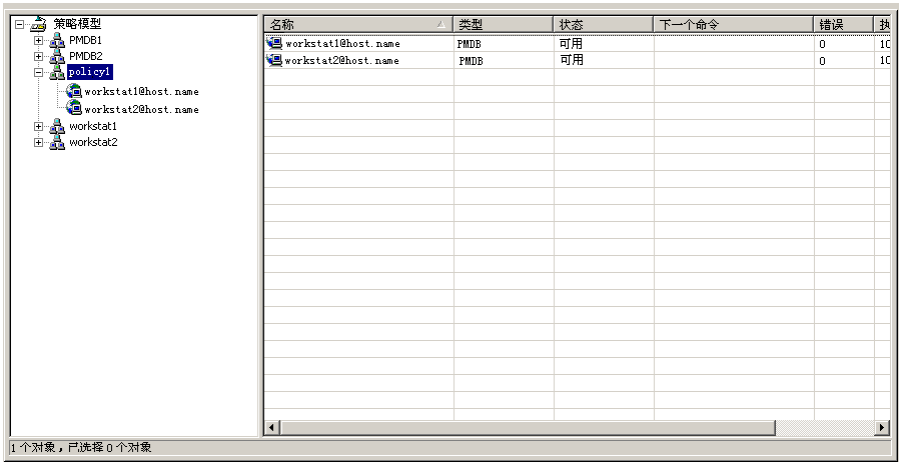
1. 连接 bighost。为管理员创建用户帐号。
   - PMDB 的管理员是经过授权可以更改 PMDB 属性的用户。
   - PMDB 的审核者是授权查看 PMDB 审核日志文件的用户。
   - PMDB 的密码管理员是授权更改 PMDB 中的密码的用户。
2. Create the user with all three attributes.
3. 授予管理员终端权限，使其可以在工作站上进行管理。
4. 现在注销，并以某个管理员身份再次登录。
5. 单击程序栏上的"工具"，然后选择"策略模型"。
6. 选择工具栏上的"新建"图标以新建 PMDB。输入 PMDB 的名称，然后选择"管理员"图标。
7. 选择"新建"，然后输入名称或使用"浏览"按钮。重复以上步骤创建第二个管理员。
8. 现在选择"终端"。单击"新建"，然后输入主机名称或使用"浏览"按钮。

9. 创建了 PMDB 之后，即可添加订户。订户可以是任何当前 PMDB 或 eTrust 数据库。在该示例中，我们已在 bighost 上创建了订户 PMDB，但实际上可以在企业中的任意位置创建它们。

   右-click the PMDB policy1.

10. 选择"添加订户"。以　格式输入名称。

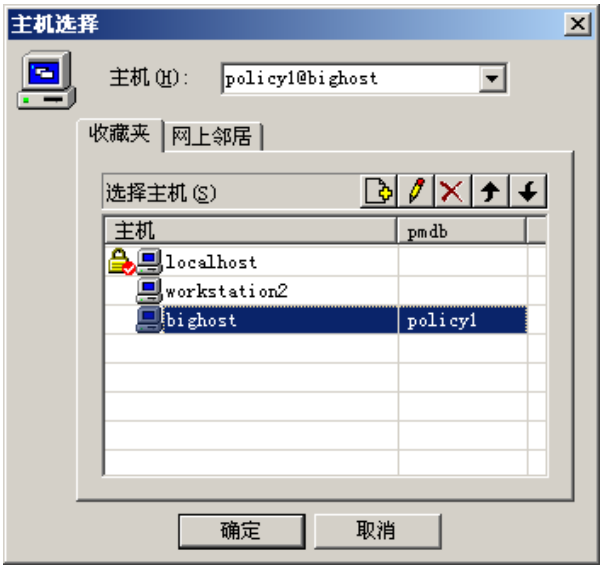
11. 重复以上步骤添加第二个订户。树显示了策略模型层次。



使用 PMDB

现在，我们将新建一个用户，并观察更改如何通过模型传播。

1. 首先，连接策略模型。



2. 创建用户 jsmith (Jennifer Smith)。
3. 连接到某个订户。

   注意：请记住，如果某个主机不在您的收藏夹列表中，您可以在连接对话框的顶部输入该主机的名称。

4. 打开"用户"窗口。

   列表中将显示新用户 jsmith。

事务管理器 — 一种更简单的替代方法

事务管理器自动将在本地主机上执行的 eTrust Access Control 事务发送给多个主机。该事务模式是策略模型的一种快速而有效的替代方法。虽然它不能确保可以传播到每个订户的安全数据库中，但它简单易用，尤其适用于更改多个未在策略模型层次中定义的数据库的情况。

设置事务管理器

在使用事务管理器之前，请验证下列事项：

- 您在要访问的每个远程主机以及本地主机上都拥有 ADMIN 权限。
- 在您要访问的每个主机上都为管理计算机创建了 TERMINAL 记录。

以上要求与管理远程主机的要求相同。事务管理器必须在启用以后才能使用。

1. 从策略管理器中，选择"工具"、"选项"，并单击"事务管理器"选项卡。
2. 选中列表上方的"启用-多主机事务"框。

   还可以选择要激活的其他事务管理器选项。
3. 单击"文件"、"目标主机"以创建目标主机文件。
4. 向目标主机列表中添加主机 workstat1 和 workstat2。

   选择要向其传播命令的主机。

主机可以是本地数据库或 PMDB。可以创建主机组以加快选择速度。单击组名称可以激活该组的所有成员。您还可以选择或取消选择任意单个主机。单击"确定"后，选择立即生效，并在下次更改前一直保持有效。每次要向不同组主机发送事务时必须手工重置 Target Host 文件。

注意：启用"事务模式"时，"主机选择"设置适用于"复制用户向导"和"复制组向导""以及事务管理器。

5. 在继续执行操作之前，再次连接 bighost。现在，单击工具栏上的"事务模式"图标。

   您所执行的所有事务还将传播到选定主机上。再次单击"事务模式"图标时，将不再传播命令。

现在，删除刚刚创建的用户。

1. 选择用户 jsmith，然后单击工具栏上的"删除"。

   要查看内部结果，请右键单击 Windows 任务栏中的"事务管理器"图标，然后选择"打开事务管理器"。下面的对话框显示了 workstat1 的结果。

2. 选择 workstat2 以查看该主机上的结果。

   在本示例中，该日志以红色显示，表示命令未成功传播。

3. 双击所选项查看命令详细信息，以获取更多信息。

注意：更正问题之后，还可以通过选择该事务并单击"再次运行"图标再次进行传播。（"再次运行"图标看似一组齿轮）。

后续内容

现在您已经对策略模型、PMDB 和事务管理器有了很好的了解。下一章将指导您对 eTrust Access Control 和 Unicenter TNG 进行集成。

第 9 章： 与 Unicenter 集成

此部分包含以下主题：

将 eTrust Access Control 与 Unicenter 进行集成 (p. 73)

将 eTrust Access Control 与 Unicenter 进行集成

eTrust Access Control 完全与 Unicenter TNG 企业管理环境集成。本章说明 eTrust Access Control 如何处理集成。

注意：要进行集成，Unicenter TNG 必须与 eTrust Access Control 安装在同一台计算机上，且必须使用下面的命令激活 Unicenter TNG Security：

```
SETOPT CA_ROUTER_CAUSECU 1
SETLOCAL CAIACTSECSV YES
```

安装 Unicenter Integration 工具

完成以下步骤可以在 Windows 环境中设置 Unicenter Integration。在 eTrust Access Control 安装过程中，请在**每个**节点上执行下列操作：

1. 在"安装向导"的"选择组件"对话框中，选择"Unicenter Integration"并单击"下一步"。
2. eTrust Access Control 向 Unicenter TNG 的配置参数所指定的主机或您选择的主机发送审核数据。要进行集成，请指定"应将审核数据发送至 Unicenter TNG"，然后选择 eTrust Access Control 应将审核数据发送到的主机。
3. 如果您要将用户和访问权限与 Unicenter TNG 日历集成，请指定从 Unicenter 日历主机服务器检索更新的频率，然后单击"下一步"。（默认值为每 10 分钟检索一次。）
4. 如果您要迁移 Unicenter Security 数据，请在"安装向导"的"Unicenter 迁移"对话框中选择"将 Unicenter 安全数据迁移到 eTrust Access Control"，然后单击"下一步"。

   注意：如果您不希望迁移 Unicenter Security 数据，**请勿**选择"将 Unicenter 安全数据迁移到 eTrust Access Control"。

   如果您没有选择该选项，将不执行从 Unicenter Security 到 eTrust Access Control 的迁移，eTrust Access Control 中的用户名将显示为完全限定名（即 DOMAINNAME\USERNAME）。迁移之后，用户名是不受限定的（即 USERNAME）。
5. 继续执行其余的安装步骤。
6. 如果显示"数据库导入"对话框，请选择"是"或"否"，以表明是否将 Windows NT 数据导入数据库中。

   注意:如果您**没有**选择"将 Unicenter 安全数据迁移到 eTrust Access Control"选项，则不会显示"数据库导入"对话框。

安装说明

- 建议在运行 Unicenter Integration and Migration Installation 进程之后不要运行 Unicenter TNG 登录截获。成功运行了 Unicenter Integration and Migration Installation 进程后，应验证 Unicenter TNG 登录截获是否已禁用。
- eTrust Access Control 迁移进程不支持 Unicenter 数据范围规则（使用 -DT 后缀确定 Unicenter TNG 资产类型目标的规则）。在迁移过程中将忽略该类规则。
- 由于不再使用 Unicenter Security，因此针对以下任何 Unicenter Security 资产类型实施的 Unicenter Security 规则都将失效：CA-USER、CA-ACCESS、CA-USERGROUP、CA-ASSETGROUP、CA-ASSETTYPE 和 CA-UPSNODE。迁移进程将忽略以任何上述资产类型或其派生资产类型为目标的规则。
- 如果您在运行 Unicenter Integration 进程后升级 Unicenter TNG 或应用 Unicenter TNG 修补程序，则必须确保 %CAIGLBL000%\BIN 目录中的 CAUSECR.DLL 文件未被替换，并且与 eTrustACDir\bin 目录中的 CAUSECR.DLL.EAC 文件相同。
- 如果卸载了 eTrust Access Control，CA_ROUTER_CAUSECU Unicenter Security 选项将被重置为"One"，SETLOCAL CAIACTSECSV Unicenter Security 选项将被重置为"Yes"，而 %CAIGLBL000%%\BIN 目录中的 CAUSECR.DLL 文件将被替换为 Unicenter 默认值。完成卸载进程后，您可能需要自定义这些选项。

注意:要获得 Unicenter Integration 功能及其工作方式的完整列表，请参阅《管理员指南》。

后续内容

下一章将提供关于 eTrust Access Control 的常见问题解答。请抽些时间通读该内容，因为它言简意赅地提供了有价值的信息，可以使您进一步了解新软件。

第 10 章： 常见问题

在本章中，我们着重讲述大家共同关注的一些安全策略问题，以及 eTrust Access Control 是如何简化 UNIX、Linux 和 Windows 安全管理与实施的。图形用户界面集中控制安全策略以及用户、组和系统资源的管理。

问：什么是 eTrust Access Control?

答：eTrust Access Control 是为 UNIX、Linux 和 Windows 服务器提供保护并为系统管理员提供访问管理的一种软件程序包。

大多数保护 UNIX 和 Linux 系统的传统方法都侧重于对威胁做出反应、评估漏洞或是尝试限制各种变成 root 用户的方式。所采取的措施包括频繁运行审核报告、使用共享件工具暴露系统漏洞和安装供应商提供的 CERT-推荐修补程序。

eTrust Access Control 的设计是基于对以下事实的认识：更可靠的 UNIX 或 Linux 安全要求从根本上改变 UNIX 或 Linux 系统资源访问权限的授予方式。eTrust Access Control 让您根据简单和易于配置的访问规则，来控制对不同操作系统资源的访问。这样就恰好在受保护数据的旁边增加了一个安全层。这个解决方案没有改变 UNIX 或 Linux 的运行方式或管理员的工作方式。

问：每个支持平台上的 eTrust Access Control 都是一样的吗？

答：是。eTrust Access Control 的功能在所有支持平台上都是一样的。所有 eTrust Access Control 界面都提供跨-平台管理，其对底层 OS 差别（初始配置中除外）是透明的。自然，当 OS 具有不同的资源名称时，eTrust Access Control 将保持与本地 OS 一致。

问：什么是 eTrust Access Control Dynamic Security Extension (DSX) 技术?

答：DSX 技术是与安全相关的 syscall 的动态截获。系统调用（或系统矢量）表中存储指向系统调用内核代码的内存地址指针。eTrust Access Control 存储这些地址指针，然后将它们更改为指向相应的 eTrust Access Control 代码。

如果访问得到批准，请求将继续原来的系统调用代码，如果访问遭到拒绝，则终止该请求。

问：eTrust Access Control 将截获系统中的每个事件吗？

答：不是。eTrust Access Control 只截获某些系统调用。一旦截获到系统调用，eTrust Access Control 引擎将根据数据库中定义的 eTrust Access Control 规则来确定是否允许或禁止对已截获资源的访问。

eTrust Access Control 只截获对文件或设备的初次访问，但不截获在该文件上执行的后续 I/O 事件（如读和写）。

对网络连接也是一样。eTrust Access Control 截获网络套接字的建立（即，端口-IP 地址配对），但不截获后续的数据传输。

eTrust Access Control 不截获为进程分配内存的例程。

问：运行 eTrust Access Control 过程中，需要哪些 CPU 开销？

答：这因主机自身功能而异。通常邮件服务器的性能损失低于数据库服务器的宿主系统。

客户经验（包括对性能要求较高的系统）已显示一般性能范围会造成-15% 的 CPU 额外开销。

问：访问规则存储在什么位置？

答：eTrust Access Control 的访问规则存储在本地主机上的受保护数据库中。

问：eTrust Access Control 是否包含 API？

答：是。事实上，eTrust Access Control 包含大量用于构建 eTrust Access Control 开放式体系结构的 API。API 可以用于任何用途，从访问控制到报警通知管理。eTrust Access Control 文档中详细说明了每个 API 的用法，同时，使用 C 语言编写的样例程序将随软件附送。eTrust Access Control API 包括：

- **授权 API**，应用程序可使用它来检查用户对任意资源的访问权限。该 API 调用集能使站点能够通过 eTrust Access Control 集中管理安全，甚至是自己开发的应用程序。
- **管理 API**，应用程序使用它来像 eTrust Access Control 一样管理 Windows UNIX 或 Linux 安全的各个方面。
- **审核 API**，用于自定义 eTrust Access Control 审核。
- **密码 API**，用于自定义除产品中所提供的密码质量检查之外的密码质量检查。

问：eTrust Access Control 是否提供网络进程通信加密？

答：是，eTrust Access Control 对所有与 eTrust Access Control 相关的网络通信进行加密。

问：什么是 eTrust Access Control 保护？

答：eTrust Access Control 将保护操作系统和驻留于受保护主机上的应用程序资源。这可以通过控制对系统资源的访问实现。下面是 eTrust Access Control 可以保护的资源类型以及可以控制的访问类型的简要列表：

文件（一般和离散）

增强的文件访问控制能够突破操作系统限制来保护文件。例如，对于某个文件，没有访问权限的用户不可以访问该文件，即使是 root 用户也不例外。eTrust Access Control 还能控制用户访问文件方式（即，使用哪个程序或应用程序）。

网络连接

eTrust Access Control 通过管理传入和传出的网络连接来控制对网络服务和端口的访问。

进程

eTrust Access Control 保护进程不被未经授权的用户终止。Windows 服务是该保护的最佳候选。

Userids 和 groupids (su)

仅限 UNIX。eTrust Access Control 可以控制替代 userids 和 groupids。仅知道其他用户的密码还不足以代替该用户的 uid。

特权程序

经特权授权的程序是后门以及对系统资源的未授权访问的主要来源。eTrust Access Control 防止对特权程序的可信任基础的修改，并防止执行新的、未识别的特权程序。

SPECIALPGM

某些应用程序（如程序或系统服务）需要特殊的 eTrust Access Control 授权保护。SPECIALPGM 通过以下方式来保护指定程序：将逻辑用户名（定义为 eTrust Access Control 数据库中的 USER 记录）与运行该程序所需的用户名关联，仅授权该逻辑用户运行这些程序。

堆栈溢出保护 (STOP)

STOP 将防止黑客使用堆栈溢出利用，通过它黑客可以执行任意命令来入侵系统。

终端

eTrust Access Control 通过定义-从哪个终端和在什么条件下登录来控制系统访问的入口点。

用户-定义的资源

管理员可以使用 eTrust Access Control 的授权 API 和数据库工具来定义站点-专用规则，以保护对挂入 eTrust Access Control 服务器的应用程序的数据的访问。

用户和组模拟

仅限 Windows。eTrust Access Control 控制用户和组的模拟。知道其他用户的密码不足以模仿该用户。

Windows 注册表

仅限 Windows。eTrust Access Control 限制用户访问注册表键。您可以授予用户一种或多种访问权限，例如读取 (READ)、写入 (WRITE) 和删除 (DELETE)。可以指定与单个注册表键或一组命名相似的注册表键相关的访问权限。

问：eTrust Access Control 是否可以防止资源免遭获得 root 用户访问权限的攻击者的攻击？

答：是。事实上，这是 eTrust Access Control 增强 UNIX 和 Linux 安全的主要方式之一。在本地 UNIX 中，使用零 (0) 作为 ID 的用户可以有效地访问所有系统资源。不仅用户密码和文件权限无力防范已成功攻击 root 用户的用户，而且规则也会遭到修改且不留下任何审核痕迹。

问：eTrust Access Control 如何管理 root 用户功能？

答：UNIX 和 Linux 的最大安全威胁是存在超级用户 (root)，-它是拥有全部权利的用户标识，-组织中各种人员均可能获得该用户标识。eTrust Access Control：

- 监管对超级用户的访问。
- 定义和限制超级用户可以执行的操作。
- 更正 root 用户暴露的不受限制的权限。
- 将特权转移到可以承担责任的个人。
- 限制攻击者通过超级用户访问可能造成的损失。
- 目前市场中尚未有任何其他安全解决方案能够提供此创新功能。

问：如何根据需要来指派-到 -root 用户的责任？

答：管理员和操作员需要有特权的 root 用户访问权限，以便履行他们的工作职责。如果没有使用 eTrust Access Control，则向他们提供 root 用户密码时，便授予了全部权利，否则不授予任何权限。使用 eTrust Access Control 可以轻松地将规则应用到定义的"角色"上。这些角色将 root 用户功能指派给能够承担责任的用户。

问：eTrust Access Control 文件访问控制能否替代 UNIX 或 Linux 文件权限？

答：否，它增强了这种文件权限的功能。对于拥有 root 用户访问权限的攻击者，本地 UNIX 不提供任何文件安全，也不提供使用一般通配符定义，以确定和维护对文件组的访问来保护文件。

eTrust Access Control 通过截获每个文件访问请求，并根据其 ACL 确定用户是否拥有授权能够以请求的方式访问文件，从而提供全面的文件保护。

eTrust Access Control 可以保护整个目录的内容，例如，/etc/* 或 $DIR/webserver/ht-docs/*。eTrust Access Control 规则还可以保护诸如 $HOME/*/.rhosts 的文件，从而保护所有用户的 .rhosts 文件。您还可以设置一个规则来保护具有以下名称的文件集：/app/config*。这样，诸如 /app/config.dat 和 /app/config.tar 这类的文件都可以得到保护。

如果需要保护没有映射到目录或通用命名约定的文件，则可以使用 GFILE 类。您可以通过该类定义特定的文件，对所有这些文件应用一组常用访问控制规则。

另外，使用程序 ACL (PACL)，您可以确保只有使用经过认可的程序才可以访问敏感资源。（例如，人事数据库文件只能使用该数据库的应用程序才可以写入。）对于支持本地 UNIX ACL 的操作系统（Solaris 和 HP-UX），eTrust Access Control 可以使 eTrust Access Control ACL 与操作系统同步。

问：如何判断规则是否具有过度的限制性？

答：只须实施该规则以观察"命中"或拒绝的访问是否切合实际。因此，eTrust Access Control 包括一种-"只监视"的模式，称作警告模式。假设用户尝试访问他们无权访问的资源。如果资源处于警告模式，则未实施访问规则（即，如果操作系统允许，用户可以访问该资源），但将创建特定的审核日志条目，该条目指明在"实施模式"下该访问必将被拒绝。

通过检查受警告的资源访问的审核日志条目，而不必实际实施规则，就可以判断出该规则是否存在过度限制。这在开发新规则时尤其有用，因为可以不必承担由于中断应用程序而在 OS 内引起异常的风险。

问：是否可能既使用界面又使用批处理来管理 eTrust Access Control?

答：是。selang 命令行界面既可以用于策略管理器（管理界面），又可以用于批处理。

问：什么是策略模型？

答：策略模型是一种简单的层级结构机制，可以将访问规则传播到多个系统上，可以创建访问规则集的模型，各种主机都可以订阅这种模型。每个 PMDB 都是一个独立的-eTrust Access Control 数据库，它包含相同类型的规则，作为与特定主机系统关联的 eTrust Access Control 数据库。当规则应用于 master PMDB 时，这些规则将传播到为该 master PMDB 定义的所有已订阅数据库上。

问：eTrust Access Control 是否既管理 Windows 操作系统又管理 UNIX 操作系统？

答：是。eTrust Access Control 提供强大的、直观的 GUI，使管理员能够从一个中央位置管理 Windows 与 UNIX 中的用户帐户和资源。

问：是否需要添加两次用户：一次添加到 UNIX 或 Linux，一次添加到 eTrust Access Control?

答：不需要。但是，需要具有明确的资源访问控制的用户则必须在两个环境中都出现。也就是说，他们必须在本地 UNIX 和 eTrust Access Control 数据库中都得到定义。使用策略管理器界面，可以定义或更改 UNIX 和 eTrust Access Control 用户和组的定义。

问：eTrust Access Control 是否可以用于管理 Windows 操作系统以及 UNIX 和 Linux 操作系统？

答：是。eTrust Access Control 提供强大的、直观的 GUI，使管理员能够从一个中央位置管理多个操作系统中的用户帐户和资源。

问：eTrust Access Control 是否支持基于硬件-的身份认证（例如 SecureID）吗？

答：eTrust Access Control 兼容所有身份验证软件，因为它不干涉身份验证过程。

问：eTrust Access Control 与防火墙有什么区别呢？

答：防火墙用于限制使用网络、主机、用户、协议、服务和应用程序对通往外部资源以及来自外部资源的网络访问。当企业提高了网络连接的-级别时，越来越多的数据需要通过防火墙。

但在防火墙后，服务器和数据很容易易受攻击。eTrust Access Control 既保护防火墙之后系统上的资源，也保护 DMZ 中的资源。

问：如果我已安装了防火墙，为什么还需要 eTrust Access Control 呢？

答：防火墙对于过滤传入和传出的网络流量是很重要的。配置良好-的防火墙能够在很大程度上减少可能尝试潜入系统的好奇用户的数量，而且能够保护信息资产不被通过 Internet 发送出去。

但是，一旦用户位于网络内部，则防火墙无力提供任何保护。另外，聪明的黑客还可以（并曾经成功）绕开防火墙。

问：应该如何理解 eTrust Access Control 提供主动的安全保护？

答：大多数安全解决方案提供的方法在本质上都趋于被动。计算机安全的历史已证明了，这些被动的方法只是暂时的解决办法，因为它们只解决应用层处理的安全问题。eTrust Access Control 是用于解决系统和系统调用层的安全事件。

采用这种方法是因为所有的资源访问请求（应用或其他）都由系统处理，并且必须通过内核。当出现安全敏感请求时，eTrust Access Control 可以截获请求，并在请求变成威胁之前禁止它。

问：一般说来，与其他免费软件的安全解决方案相比，eTrust Access Control 有哪些优势？

答：免费软件的解决方案在本质上都趋向于被动反应。它们处理症状而不是原因，提供没有超级用户或系统攻击保护的工作区。

以下是 eTrust Access Control 与免费软件相比较的优势的简要列表：

- 自我-保护
- 自我-检查（规则数据库和服务\后台程序）。
- 在运行时保护配置文件。
- 安装和维护的管理性开销较小。
- 供应商支持。
- 提供逐步实现的方法。eTrust Access Control 具有警告模式概念。不必实施也可以应用规则，不会影响正常业务。
- 提供了通用的解决方案，是各种免费解决方案的超级集合，并且可从单点管理多个计算机和平台。

一些比较知名的基于主机的-解决方案是 SUDO、审计、Tripwire 和 TCP 包装程序。eTrust Access Control 在单个软件包中提供了这些解决方案的功能超集，从而通过提供内核中的主动安全保护，解决核心问题而不是表面症状。

也许有人会问，"如果泄露了 root 用户的帐户，免费软件解决方案还能继续提供保护吗？"答案是不能。这些工具只是给用户一种错误的安全感。如果使用 eTrust Access Control，则可以继续提供保护，因为 eTrust Access Control 能保护关键资源。

问：eTrust Access Control 与本机文件权限有什么区别？

答：本机文件权限只能向所有者、组和全体用户统一提供"读取"、"写入"和"执行"的访问权限。Root 用户的访问或文件的所有者可以-以任何文件覆盖本机文件的访问权限。

eTrust Access Control 扩展了一般操作系统的访问模式，并提供其他访问权限，如"更新"、"删除"和"创建"等。eTrust Access Control 访问模式不受文件所有者或 root 用户帐户的影响。UNIX 或 Linux 只允许一个组访问，但 eTrust Access Control 可用于为不同的组分配不同的访问权限。

eTrust Access Control 还基于允许哪些程序访问文件来扩展文件访问，这是本地 UNIX 或 Linux 无法提供的。

问：eTrust Access Control 能否提供万无一失的安全解决方案？

答：任何解决方案都不能提供万无一失的安全性。然而，eTrust Access Control 能提供综合的且更合理的软件解决方案，这在以前处理操作系统安全问题的原因时并不存在。安全方面超出了软件控制的范围，它是通过建立并执行关于和包括物理访问和帐户共享的常识性策略来解决的。

问：听说黑客可以使用诸如"rootkit"此类的工具访问计算机。eTrust Access Control 能防范这些工具吗？

答：rootkit 已经存在一段时间了，是用来获得计算机未授权访问的众多工具之一。它既不是第一个，当然也不是最后一个。要了解 eTrust Access Control 如何解决这些问题，不妨分析一下黑客及其工具的目标和一般特征，以及 eTrust Access Control 的处理方法。

黑客的目标是通过截获 root 用户帐户而获得对系统的完全控制。对于此问题，eTrust Access Control 可以限制谁可以成为 root 用户以及如何成为 root 用户。一旦发生未授权的 root 用户访问，eTrust Access Control 可以控制它访问的内容。

下表有助于说明如何防范黑客威胁：

攻击方式	黑客攻击	eTrust Access Control 防护
A) 渗透	A1) 已知的服务缺陷	A1a) 禁用或限制访问有效的远程资源
	A2) 密码无效的帐户	A2a) 禁用遭到反复攻击的帐户
		A2b) 对敏感帐户的访问仅限于本地
		A2c) 实施密码质量控制
B) 获得超级用户身份	B1) 有缺陷的程序	B1a) 限制允许超级用户访问的程序
	B2) 猜测超级用户密码	B2a) 限制超级用户只可以本地访问
		B2b) 限制谁可以成为超级用户（即使已知密码）
C) 保留超级用户身份	C1) 改变现有的特权程序	C1a) 防止篡改特权程序
	C2) 引入新特权程序	C2a) 防止系统引入未授权的特权程序。
	C3) 改变系统日志以隐藏渗透	C3a) 防止篡改系统日志
		C3b) 提供与系统分离的日志记录。

另外，eTrust Access Control 采用一种新的 eTrust 技术，称作"堆栈溢出保护"(STOP)，它可以防止堆栈溢出或缓冲溢出的攻击，进一步增强了 eTrust Access Control 保护系统的能力。