eTrust® Access Control for Windows

管理员指南

r8 SP1

CA 产品引用

本文档引用以下 CA 产品 ：

- eTrust® Access Control (eTrust AC)
- 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： 简介

此部分包含以下主题：

关于本指南

本指南介绍 eTrust AC for Windows（它是为开放系统提供完整安全解决方案的产品）所使用的概念，还说明 eTrust AC，尤其是用来管理 eTrust AC for Windows 的用户界面，即策略管理器。

使用本指南的用户

本指南是为负责实施和维护受 eTrust AC 保护的环境的安全管理员和系统管理员编写的。

命令表示法约定

eTrust AC 文档在解释命令语法和用户输入时使用一些特殊约定：

格式	含义
等宽字体	代码或程序输出
斜体	必须提供信息的占位符
粗体	必须完全按照显示内容键入的元素
用方括号括起来 ([])	可选项目
用花括号括起来 ({})；竖线分隔的选项 (|)。	必需选项集，您必须从中只选择一个选项
行结尾处的空格和反斜杠 (\)	命令延续到下一行

注意：

- 粗体文本还用于简单强调。例如：

  您**决不**要将密码粘贴在显示器上。

- 有时，在本指南中，一行无法容纳一个命令。在这些情况下，行结尾处的空格加上反斜杠（ \）就表示该命令延续到下一行。

  注意：在实际的命令语法中，请避免复制不必要的反斜杠字符。

- 竖线（|）将互斥的项目分隔开。项目集用花括号（{}）括起来，在键入其中一个项目时并**不**需要键入这种花括号。例如，下面的示例**可以**表示用户名，**也可以**表示组名：

  ```
  {username|groupname}
  ```

示例：命令表示法约定

下面的代码说明了在本指南中使用命令约定的方式：

```
ruler className [props({all|{propertyName1[,propertyName2]}})
```

在该示例中：

- 命令名称 (ruler) 以粗体显示，因为必须按照显示内容键入。
- className 选项以斜体显示，因为这是一个类名（例如 USER）占位符。
- 即使没有用方括号括起来的第二部分，您也可以运行该命令，因为该部分是可选的。
- 使用可选参数 (props) 时，可以选择关键字 all，也可以指定一个或多个（以逗号分隔）的属性名。

第 2 章： 基本概念

此部分包含以下主题：

eTrust AC

eTrust AC 软件产品是用于开放系统的主动型综合性安全软件解决方案，它动态绑定到操作系统。用户每次请求有关安全的操作（例如，打开文件、替换用户 ID 或获取网络服务）时，eTrust AC 会实时截获该事件并评估其有效性，然后才将控制权转交给标准的操作系统 (OS) 功能。

访问控制的概念

eTrust AC 为您提供用来管理本地平台安全性的强大工具，从而能够实施可完全根据企业安全要求自定义的安全策略。eTrust AC 可以为本地操作系统中可用用户、组和资源之外的用户、组和资源提供安全保护，在整个组织范围内集中管理安全性，并将您的 Windows 和 UNIX 安全策略集成到一个异构环境中。

保护的对象是什么？

eTrust AC 保护下列实体：

- **文件**

  用户是否有权访问特定文件？

  eTrust AC 限制用户访问文件的能力。您可以给予用户一种或多种访问权限，如 READ、WRITE、EXECUTE、DELETE 和 RENAME。访问权限的指定可以与单个文件有关，也可以与一组名称类似的文件有关。

- **终端**

  用户是否有权使用特定终端？

  该检查是在登录过程中完成的。在 eTrust AC 数据库中，可以使用访问规则（该规则指明允许哪些用户或用户组使用终端或终端组）来定义各个终端和终端组。终端保护可确保不能使用未经授权的终端或工作站登录到拥有强大权限的用户的帐号。

- **登录时间**

  用户是否有权在特定日期的特定时间登录？

  大多数用户只在工作日和工作时间使用他们的工作站；日-内-某时和周-内-某日登录限制以及假期限制，是为了防止黑客和其他未经授权的访问者擅自登录。

- **TCP/IP**

  另一个工作站是否有权从本地计算机接收 TCP/IP 服务？另一个工作站是否有权向本地计算机提供 TCP/IP 服务？是否允许另一个工作站从本地工作站的每个用户接收服务？

  开放系统（计算机和网络都开放的系统）的优点也是缺点。一旦计算机连接到外面的世界，您就无法确保谁进入系统以及外来用户可以进行何种破坏（无论有意还是无意）。eTrust AC 提供“防火墙”，可以防止本地工作站和服务器向未知工作站提供服务。

- **多个登录权限**

  是否允许用户从第二个终端登录？

  术语“并发登录”指的是用户从多个终端登录到系统的能力。eTrust AC 可以阻止用户多次登录。这可以防止入侵者登录到已经登录的用户的帐户。

- **用户-定义的实体**

  您可以定义和保护常规实体（如 TCP/IP 服务和终端）和功能实体（也称为抽象对象，如执行事务和访问数据库中的记录）。《SDK 开发人员指南》中介绍了用于定义和保护抽象对象的应用程序编程人员接口 (API)。

- **管理员权限方面**

  eTrust AC 提供了向操作员委派管理员权限和限制根用户自身的方法。

  eTrust AC 提供了同时向操作员委派管理员权限并限制管理员自身的方法。

- **注册表键**

  用户是否有权访问特定注册表键？

  eTrust AC 限制用户访问注册表键的能力。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。

- **程序**

  特定程序是否可受托？用户是否有权调用它？用户是否可以使用程序来访问特定资源？

  安全管理员可以对程序进行测试，确保它们不包含任何可用来获得未经授权的访问的安全漏洞。通过测试并被视为安全的程序定义为受托程序。eTrust AC 自我保护模块（也称为**监视程序**）知道哪个程序在特定时间处于控制之下，检查该程序自归类为受托程序之后是否经过修改或移动。如果受托程序经过修改或移动，则不再将该程序视为受托程序，eTrust AC 将不允许它运行。

另外，eTrust AC 还可以防止各种故意的和偶然的威胁，包括：

- **终止尝试**

  eTrust AC 可以用来保护关键服务器和服务或后台程序，防止终止尝试。

- **密码攻击**

  eTrust AC 防止各种类型的密码攻击，强制您的站点实施密码-定义策略，并检测入侵-企图。

- **密码缺点**

  eTrust AC 策略描述了强制用户创建和使用高质量密码的规则。为了确保用户创建和使用合格的密码，eTrust AC 可以设置密码的最长使用期限和最短使用期限、限制某些字词、禁用重复字符，以及强制执行其他限制。不允许密码有过长的使用期限。

- **帐户管理**

  eTrust AC 策略确保正确处理睡眠帐户。

如何保护它？

<eTrust AC 服务在操作系统完成初始化后立即启动。eTrust AC 将挂钩放置在必须保护的系统服务中。这样，便可以在执行服务之前将控制传递给 eTrust AC。eTrust AC 决定是否应该将该服务授予用户。

例如，用户可以尝试访问 eTrust AC 所保护的资源。该访问请求生成了对内核的系统调用，从而可以打开资源。eTrust AC 截获系统调用，并决定是否授予访问权限。如果授予权限，则 eTrust AC 将控件传递给常规系统服务；如果 eTrust AC 拒绝权限，它会将标准权限拒绝错误代码返回到激活系统调用的程序，系统调用即结束。

授权决定基于数据库中定义的访问规则和策略。安全管理员对数据库中的大多数记录进行定义。

数据库描述了两种对象：访问者和资源。访问者是用户和组。资源是要保护的对象，例如文件和服务。数据库中的每个记录都描述了访问者或资源。

每个对象都属于一个类 - 同类对象的集合。例如，TERMINAL 是包含 eTrust AC 所保护的终端（工作站）对象的类。

类激活

数据库中保存了有关类状态的信息（即类是活动的还是非活动的）。eTrust AC 截获每次访问资源的尝试，并对数据库中的状态进行检查。如果该类是非活动的，则允许访问，无需进一步检查权限。

eTrust AC 在引擎启动和用户更改类活动状态时发布活动类的列表。如果类是非活动的，则不截获对资源的访问，从而减少了系统开销。

访问者元素

每个用户由一个访问者元素 (ACEE) 代表（该元素是数据库中的用户记录在内存中的反映）。eTrust AC 在登录进程中构建访问者元素。访问者元素与用户的进程相关。无论何时进程请求 eTrust AC 所保护的系统服务，或发出访问资源的暗示请求，eTrust AC 都会访问该资源的记录。然后，它将确定以前创建的访问者元素中的信息（例如用户的安全级别、模式和组）是否允许用户访问该资源。

组件

eTrust AC 包括一个数据库 (seosdb)、两个驱动程序（seosdrv 和 drveng）、许多服务（包括监视程序、代理、引擎 (seosd)、策略模型和任务委托）和一个图形用户界面。

数据库

数据库包含下列元素的定义：

- 组织中的用户和组
- 需要保护的系统资源
- 管理用户和组访问系统资源的规则

驱动程序

驱动程序通过执行下列任务，对所有 eTrust AC 文件和注册表键进行保护：

- 截获要打开文件或注册表键、终止进程和执行网络活动的每个请求
- 将这些请求传递给 eTrust AC 引擎，并接收引擎批准还是拒绝请求的决定。
- 将决定转发给操作系统的原始系统调用，操作系统然后根据从驱动程序收到的回答继续其处理。

服务

监视程序

监视程序会经常检查其他 eTrust AC 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

代理负责执行以下任务：

- 通过 TCP/IP 之上的专有应用程序协议与 eTrust AC 客户端进行通信
- 管理 eTrust AC 用户的安全

引擎

引擎负责执行下列任务：

- 管理数据库，包括控制所有数据库更新
- 决定是否批准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，如果发现监视程序已停止运行，则重新启动监视程序

引擎处理数据库访问请求并做出访问决定，从而创建有效服务。

策略模型

单独管理数十或数百个数据库并不现实。因此，eTrust AC 提供了策略模型服务，它是允许从一台计算机管理许多计算机的组件。虽然使用策略模型服务是可选的，但是它极大地简化了大型站点上的管理。

借助策略模型服务，可以使用策略模型数据库 (PMDB)。与其他 eTrust AC 数据库一样，PMDB 包含用户、组、受保护的资源和管理资源访问的规则。此外，PMDB 还包含一个订户工作站列表。订户工作站与 PMDB 链接，这样以来，对 PMDB 所做的任何更改都会自动发送到订户数据库。

您可以为组织创建基本安全策略，并在单一数据库（策略模型数据库）上实施所有必需的规则。订户可以同时包括 Windows 和 UNIX 工作站，从而确保以最少的管理工作执行统一规则。

系统管理员或安全管理员将更新 PMDB。然后，PMDB 会以批处理模式将所有更新从 PMDB 传播给其订户，从而将管理员解放出来执行其他工作。

PMDB 可以有两类订户：另一个 PMDB 或本地数据库。该 PMDB 还包含它将数据库更新传播到的订户的列表。您可以利用该功能生成 PMDB 的层级结构。本地数据库可用于保护在工作站上定义的用户、组和资源。

图形用户界面

策略管理器 (p. 35) 是图形用户界面 (GUI)，所有 eTrust AC 功能都可以通过该界面执行。

功能

eTrust AC 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 AC 还可以进行自我保护。下面几节介绍这些功能。

管理 Windows

在您组织中的 Windows 工作站上安装 eTrust AC 后，即可以从一个中央位置管理所有 Windows 工作站，无论它们位于哪个域中。使用策略管理器界面或称为 selang 的命令行语言，可以完成该操作。

提供自我防护

无论有意还是无意，黑客或用户实际上无法终止 eTrust AC 服务。当 eTrust AC 运行时，实际上未经授权的用户也无法更改或擦除 eTrust AC 文件和数据。

管理本机 Windows 安全性

使用 eTrust AC，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 AC 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。

Active Directory

Active Directory 是自 Windows 2000 后的 Windows 操作系统使用的目录服务；它提供了有关网络中对象（例如用户、计算机和服务）的层次结构信息库。

在 Windows 操作系统上安装 Active Directory 后，可以使用 eTrust AC 添加和修改用户和组以及扩展的用户和组属性，就像可以在本地 Windows 环境中管理用户和组一样。

在 Windows 服务器系统上安装 Active Directory 后，可以使用 OU 类在特定组织机构中创建用户、组和计算机。

文件保护

Windows 支持使用一些不同类型的文件系统。最常用的是 FAT 和 NTFS。如果使用 NTFS 文件系统，则 Windows 通过为每个文件创建和更新 ACL 来保护系统中的文件。eTrust AC 支持文件 ACL。

密码保护

本地 Windows 安全性可以通过许多方式保护密码和加强密码质量。Windows 提供下列功能：

- 强制执行密码最长时限
- 强制执行最小密码长度
- 最多保存 24 代用户密码
- 重复登录失败后锁定帐户
- 强制用户登录到 Windows 后才能更改密码

eTrust AC 还强制实施相同的规则，但是通过其自身的独特机制实施。另外，eTrust AC 还实施-了与大型计算机的双向密码同步。

扩展本地 Windows 安全性

下列 eTrust AC 功能扩展了本地 Windows 安全性。

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。每个预定义组的存在都是为了执行一组特定的系统函数。允许作为组成员的用户执行该组的所有函数。

Windows 中功能最强大的组是 Administrators 组。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。

<您可以利用 eAC> 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。

向常规用户授予管理员权限

<您可以使用 eAC> 向普通用户（即非管理员用户）授予必需的权限，以便这些用户不必成为 Administrators 组的成员即可执行管理任务。这称为任务委托。能够以这种详细方式委托任务（授予管理权限）是 eTrust AC 最重要的优点之一。

- SUDO 类中的记录存储了命令脚本，允许用户使用借来的权限运行该脚本。
- 数据属性值是命令脚本。通过将可选脚本参数值添加到该值，可以对该值进行修改。
- SUDO 类中的每个记录都标识一个命令，一个用户可以借用另一个用户的权限来执行该命令。
- SUDO 类记录的关键字是 SUDO 记录的名称。当用户执行 SUDO 记录中的命令时，会使用该名称来代替命令名称。

定义 SUDO 记录

SUDO 类中的记录将存储命令脚本，以便用户可以使用借用的权限来运行该脚本。借用权限的能力由 SUDO 记录以及执行脚本的 sesudo 命令严格控制。

注意：当 SeOS 任务委托服务在安装了终端服务的计算机上使用除 SYSTEM 帐户以外的用户帐户运行时，sesudo 命令无法执行交互式进程。

在 SUDO 记录中，comment 属性用于特殊用途，通常，它也称为 data 属性。

comment 属性的值是命令脚本，也可以在其中添加一个或多个要禁止或允许使用的脚本参数值。整个 comment 属性值必须放在单引号中，并且应该使用可执行文件的完整路径名称引用可执行文件，以防止特洛伊木马获取它们的位置。

以下是 comment 属性的格式：

```
comment('cmd[;[prohibited-values][;permitted-values]]')
```

因为禁止和允许使用的值的列表是可选的，所以简单的 comment 属性值可以是：

```
newres SUDO NET comment('net use')
```

该命令中的简单值表示命令 sesudo NET 将执行命令“net use”。不禁用特定脚本参数值；允许使用所有脚本参数值。

使用通配符和功能强大的变量，可以灵活地指定禁用的参数和允许使用的参数。可以使用的通配符是标准的 Windows 通配符。禁止使用的参数和允许使用的参数也可以包含下列变量：

变量	说明
$A	字母值
$G	现有 eTrust AC 组名

变量	说明
$H	以用户的主目录开头的参数
$N	数字值
$O	运行 sesudo 的 eTrust AC 用户的名称
$U	现有 eTrust AC 用户名
$e	空条目。 使用此变量为规则指定不带任何参数的 SUDO 命令。
$f	现有文件名
$g	现有 Windows 组名
$h	现有主机名
$r	具有 Windows 读访问权限的现有文件
$u	现有 Windows 用户名
$w	具有 Windows 写访问权限的现有文件
$x	具有 Windows 执行访问权限的现有文件

如果将禁用的参数值的列表附加到脚本中，请执行以下操作：

- 用分号分隔脚本和禁用的参数值，但将它们都保留在单引号内。例如，如果要禁止用户使用 -start，但允许用户使用所有其他参数，请输入下面的命令：

  ```
  newres SUDO scriptname comment('cmd;-start')
  ```

  其中 cmd 代表您的脚本。

  另外，如果不允许使用任何参数值，但希望默认使用所有参数，请按以下方式定义 SUDO 记录：

  ```
  newres SUDO scriptname comment('cmd;*')
  ```

- 如果脚本参数有多个禁用的值，请使用空格字符作为分隔符。例如，如果要禁止用户使用 -start 和 -stop，但却允许用户使用所有其他参数，请输入下面的命令：

  ```
  newres SUDO scriptname comment('cmd;-start -stop')
  ```

- 如果多个脚本参数有禁用值，请使用管道符 (|) 作为各组禁用值之间的分隔符。例如，如果要禁止用户将 -start 和 -stop 用作脚本的第一个参数并禁止其将任何当前的 Windows 用户名用作第二个参数（请参阅前面的变量列表），请输入下面的命令：

  ```
  newres SUDO scriptname comment('cmd;-start -stop | $u')
  ```

  如果脚本的参数多于列表中的参数，则最后一组禁用参数将适用于所有其余参数。

如果将允许使用的参数值的列表附加到脚本中，请执行以下操作：

- sesudo 实用程序检查参数值：
  - 不能与任何相应的禁用值匹配。
  - 至少与一个相应的允许值匹配。

  这意味着如果某个参数值在禁用列表中，则即使在允许使用列表中指定了该参数，也不允许使用它。

- 用分号将允许值的列表与禁用值的列表分隔开，但要将它们都保留在单引号内。即使您没有禁用值的列表，仍需要使用分号；否则，将禁用您要允许使用的值。例如，如果仅允许值 NAME 作为脚本的参数值，请输入下面的命令：

  ```
  newres SUDO scriptname comment('cmd;;NAME')
  ```

- 正如在另一个列表中一样，
  - 如果脚本参数有多个允许值，请使用空格字符作为分隔符。
  - 如果多个脚本参数具有允许值，请使用管道符 (|) 作为各组允许值之间的分隔符。

  例如，如果您有两个参数，第一个参数必须是数值而不能是 Windows 用户名，第二个参数必须是字母而不能是 Windows 组名，则请输入下面的命令：

  ```
  newres SUDO scriptname comment('cmd;$u | $g ;$N | $A')
  ```

  如果脚本的参数多于列表中的参数，则最后一组允许使用的参数将适用于所有剩余参数。

因此，comment 属性的完整格式为：首先是脚本，然后是逐个参数的禁用值，最后是逐个参数的允许值：

```
comment('cmd; \
param1_prohib1 param1_prohib2 ... param1_prohibN | \
param2_prohib1 param2_prohib2 ... param2_prohibN | \
 ...
paramN_prohib1 paramN_prohib2 ... paramN_prohibN ; \
param1_permit1 param1_permit2 ... param1_permitN | \
param2_permit1 param2_permit2 ... param2_permitN |
 ...
paramN_permit1 paramN_permit2 ... paramN_permitN')
```

sesudo 实用程序通过以下方式检查用户输入的每个参数：

1. 测试参数 N 是否与允许的参数 N 匹配。（如果允许的参数 N 不存在，则使用上一个允许的参数。）
2. 测试参数 N 是否与禁止的参数 N 匹配。（如果禁止的参数 N 不存在，则使用上一个禁止的参数。）

如果所有参数都与允许的参数匹配，但任何参数与禁止的参数都不匹配，则 sesudo 执行该命令。

任务委托示例

示例 1

1. 从“访问控制”程序栏中选择“资源”图标  。

   显示“资源”窗口。

2. 展开“任务委托资源”树，右击“任务”，然后选择“新建”。

   显示“新建 SUDO 资源 - 常规”对话框，允许您创建新的策略。

3. 在“名称”字段中，输入 SUDO 记录的名称 NET。

   在“数据”字段中，输入以下内容：

   ```
   net;start;send
   ```

   数据属性的格式如下：

   命令; 禁止值; 允许值

   例如，对于用户 any_user，要允许执行 net send 而阻止执行 net start，可以在“数据”字段中输入以下内容，将 any_user 授权该 SUDO 记录：

   ```
   net;start;send computer_name message
   ```

4. 在“所有者”字段中，单击“浏览”，从“用户”选项卡中选择“nobody”，然后单击“确定”。

5. 单击“设置默认访问权限”，选择“无”，然后单击“确定”。

6. 从对话框的左窗格中选择“授权”图标。

   出现该对话框的“授权”页。

7. 单击“插入”  以添加访问者，并单击“名称”字段旁边的“浏览”。

8. 选择要委派权限的用户或组，然后单击“确定”。

   将出现“添加/编辑 eTrust 访问者”对话框。

9. 单击“确定”。

10. 选中“执行权限”，然后单击“确定”。

    创建新的 SUDO 资源。

11. 执行 SUDO 记录测试。
    a. 以应用了 SUDO 记录的用户身份登录。
    b. 打开命令提示，执行以下命令：

       ```
       sesudo -do NET start
       ```

       此时出现以下消息：

       ```
       sesudo:不允许您将 'start' 作为参数编号 1 使用。
       ```

       注意：将不执行 net start，因为已将其定义为禁止的值。
    c. 执行以下值：

       ```
       sesudo -do NET send
       ```

       应该执行该命令。

示例 2

用户可以使用任何管理单元 MSC 模块执行高权限操作，如下例所示：

1. 在“资源”窗口中，展开“任务委托资源”树，右击“任务”，然后选择“新建”。

   显示“新建 SUDO 资源 - 常规”对话框，允许您创建新的策略。
2. 在“名称”字段中，输入“services”。
3. 在“数据”字段中，输入“c:\winnt\system32\mmc.exe”。
4. 在“所有者”字段中，选择“nobody”。
5. 选择“交互”复选框。

   “交互式”功能提供了启动服务后登录者可以使用的桌面用户界面。仅在服务作为 LocalSystem 帐户运行时，该选项才可用。
6. 单击“设置默认访问权限”，选择“无”，然后单击“确定”。
7. 从对话框的左窗格中选择“授权”图标。
   出现该对话框的“授权”页。
8. 单击“插入”  以添加访问者，并单击“名称”字段旁边的“浏览”。
9. 选择要委派权限的用户或组，然后单击“确定”。
10. 选中“执行权限”，然后单击“确定”。

    创建新的 SUDO 资源。
11. 执行 SUDO 资源测试。
    a. 以应用 SUDO 资源的用户身份登录。
    b. 打开命令提示，执行以下命令：

```
sesudo -do services
```

c. mmc.exe 将启动。

12. 要拒绝执行 SUDO 资源，请编辑 SUDO Authorize 属性，并选中“拒绝”列中的复选框。

13. 打开命令提示，输入以下命令：

```
sesudo -do services
```

此时出现以下消息：

```
sesudo:您没有获得使用 services 命令的授权。
```

注意：services 是为该示例创建的 SUDO 资源的名称。SUDO 资源应该阻止执行 services 脚本。

增强的文件保护

eTrust AC 支持逻辑文件名格式和绝对文件名格式。例如，如果文件 foo.txt 位于逻辑驱动器 D 的目录 \tmp 下，则逻辑名"D:"分配给物理磁盘 1 的分区 0。您可以使用逻辑或绝对文件名将文件定义给 eTrust AC 数据库：

```
nr file D:\tmp\foo.txt
```

或

```
nr file \Device\HardDisk1\Partition1\tmp\foo.txt
```

注意：如果使用第二个格式，则即使更改了磁盘的逻辑名称，文件仍受保护。对于 eTrust AC 常规文件保护，还支持绝对文件名格式。

eTrust AC 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 AC 还支持 CDFS（专用于 CD 的文件系统）和 HPFS（OS/2 文件系统）。

eTrust AC 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。_

普通类别文件保护

eTrust AC 支持逻辑文件名格式和绝对文件名格式。对于 eTrust AC 常规文件保护，还支持绝对文件名格式。

利用普通类别文件保护，可以保护所有符合指定的通配符模式（一般表达式）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常规访问规则的保护。<您可以利用 eAC> 对文件进行常规保护。

如果一个资源与多个常规访问规则匹配，则 eTrust AC 选择与该文件最匹配的规则。

使用普通类别文件保护，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. 18)。 但是，eTrust AC 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 AC 时，可以创建强制用户选择更安全、更可靠密码的附加规则。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。

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。程序通路大大提高了敏感文件的安全性。<eTrust AC 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 AC 包括下列 B1"橙皮书"功能：安全级别、安全类别和安全标签。

- 可以向数据库中的访问者和资源分配一个安全级别。安全级别是 1 到 255 之间的整数。只有当访问者拥有的安全级别等于或大于分配给资源的安全级别时，访问者才可以获得对资源的访问权限。
- 数据库中的访问者和资源可以属于一个或多个安全类别。只有当访问者属于分配给资源的所有安全类别时，访问者才能访问该资源。
- 安全标签是将特定安全级别与一组零或其他安全类别相关联的名称。将用户分配给某一安全标签会授予该用户与该安全标签相关联的安全级别和所有安全类别。

注意：有关 B1 橙皮书功能的详细信息，请参阅《实施指南》。

运行 eTrust AC

可以使用策略管理器界面或称为 selang 的命令行语言来管理 eTrust AC。通过这些工具，可以管理本地工作站以及安装了 eTrust AC 的所有其他 Windows 工作站。

策略管理器

策略管理器是 eTrust AC 的管理工具。

selang

命令行语言 selang 执行 eTrust AC 的所有功能。要使用 selang 命令，请打开命令提示窗口并启动 selang。还可以在脚本中使用 selang。

有关 selang 及其命令的详细信息，请参阅《参考指南》中的"selang 命令语言"一章。

管理 Windows 和 UNIX 的安全性

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 AC，可以执行下列所有操作：

- 开发一个适用于 UNIX 和 Windows 的通用安全策略
- 通过使用 eTrust AC 来实施该策略
- 使用一个 Windows 工作站来管理 Windows 和 UNIX 环境的安全性

进行更改并让 eTrust AC 将其传播到不同环境中的多个工作站，可以极大降低管理开销。

以下几节介绍了通用安全策略中一些非常重要的元素。

维护一组用户

在您的站点中安装 eTrust AC 后，可以维护一个包含所有用户的 eTrust AC 数据库。这意味着用户维护只能执行一次。eTrust AC 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 AC 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。

使用 eTrust AC，可以创建和维护在 UNIX 和 Windows 环境中都可以使用的一个组集。

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。PMDB 使您可以将安全数据库以及对它所做的任何更改传播给其所有订户。可以为同一 PMDB 订阅 Windows 和 UNIX 工作站。

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。这种设计将网络流量减到最少并且确保了订户的完整性。

设置管理员

安装 eTrust AC 后，系统会要求您命名一个或多个 eTrust AC 管理员。eTrust AC 管理员有权修改整个规则数据库或其中一部分。您应该至少有一个具有全部权限的管理员。该管理员可以自由修改或创建访问规则，并可以指定其他级别的管理员。

为系统定义用户后，可以通过向其他用户分配 ADMIN 属性来向他们分配管理权限。

注意：具有 ADMIN 属性的用户拥有强大的权限。因此，应该严格限制 ADMIN 用户的数量。在设置一个或多个 eTrust AC 安全管理员后，将 Windows Administrator 和 ADMIN 的角色分隔开，从 Administrator 删除 ADMIN 属性，这不失为一个好策略。

由于始终至少需要一个具有权限的用户来管理数据库，因此 eTrust AC 不允许删除最后一个具有 ADMIN 属性的用户。如果想要从 Administrator 删除 ADMIN 属性，则必须首先将 ADMIN 属性授予另一个用户。

如果希望任何 eTrust AC 管理员从该工作站管理其他主机，请确保该主机数据库中的规则向他们授予了从该工作站进行读取和写入的访问权限。

两种环境的最佳操作：创建子管理员

eTrust AC 包含子管理功能，它允许管理员授予特定权限，使常规用户可以管理特定类。这些用户则称为子管理员。

例如，可以允许特定用户只管理用户和组。

还可以通过不仅为特定类还为这些类中的特定对象授予访问权限，来指定更高级别的子管理。

设置审核过程

eTrust AC 将根据数据库中定义的审核规则保留拒绝访问和授权访问事件的审核记录。是否记录某个事件的决策基于以下规则：

- 每个访问者和资源都有 AUDIT 属性，可以设置该属性以表示访问成功还是失败或者是否应该记录成功和失败；另外，访问者的 AUDIT 属性可以表示登录成功还是失败或者是否应该记录成功和失败。
- 如果资源或访问者具有 AUDIT(ALL) 属性，则记录与 eTrust AC 所保护的资源相关的所有事件，无论访问成功还是失败。
- 如果对 eTrust AC 所保护的资源的访问成功，且用户或资源具有 AUDIT(SUCCESS)，则记录该事件。
- 如果对 eTrust AC 所保护的资源的访问失败，且用户或资源具有 AUDIT(FAIL)，则记录该事件。

只有系统审核者（向其分配了 AUDITOR 属性的用户）可以执行审核任务，例如，更改分配给用户和资源的审核属性。

如果特定资源已经设置为警告模式，则违反该资源的访问规则会生成一个审核记录，表明因为由于警告模式生效，因此允许该违反行为。

审核记录构成了称为审核日志 (seos.audit) 的文件。注册表中指定了审核日志的位置，它与错误日志在相同的位置。

在以下注册表键中指定了审核日志（以及错误日志）：

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\logmgr
```

审核日志是二进制文件，不能进行编辑或更改。但是，可以使用策略管理器查看已记录的事件、按时间限制或事件类型筛选事件等等。（还可以使用 seaudit 实用程序来完成这些相同的任务。）

如果考虑对旧的审核日志和错误日志进行存档（备份），则可以在以后扫描这些事件。

将审核事件发送到 Unicenter TNG

与 Unicenter TNG 的集成是在安装时设置的。

可以选择将审核数据发送给 Unicenter TNG，允许从 Unicenter TNG 启动 eTrust AC，或选择两者。这两个选项不相关。

选择第一个选项会在子键下设置注册表值：

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\UCTNG
```

值 Integration 设置为 1（是），值 EvtManagerServer 将 Unicenter TNG 主机的名称接收为字符串值。

传递给 Unicenter TNG 的审核事件显示在 Unicenter Enterprise Management\Enterprise Managers\Windows NT\Event 窗口的“控制台”日志中。

审核事件	显示颜色	严重性
成功	蓝色	S
已拒绝	橙色	F
失败	橙色	F
警告	蓝色	W
eTrust AC 停止（审核停止）	蓝色	I
eTrust AC 启动（审核开始）	蓝色	I

第二个选项允许从 Unicenter WorldView 菜单启动 eTrust AC，方法是指向“托管对象”窗口中代表 TCP/IP 网络的图标，然后从右键单击菜单中选择 eTrust AC。

eTrust AC 还发送以下有关事件的信息：

- 产品名称（eTrust Access Control + 版本号）
- 用户名
- 终端名称
- 类名
- 资源名称
- 进程名称
- 事件时间
- eTrust AC 审核格式的完整审核消息

并不总是发送“用户名”、“终端名称”、“类名”、“资源名称”和“进程名称”字段的信息，这取决于事件类型。

使用策略模型数据库

在拥有许多计算机和工作站的大型站点，单独管理数十或数百个 eTrust AC 数据库并不现实。当企业中大多数计算机的安全规则都相同时，管理员需要一种方法，以便只应用一次安全策略并让这些策略根据需要传播。在 eTrust AC 中，策略模型数据库 (PMDB) 提供了这一便利。

PMDB 包含与本地数据库种类相同的信息（eTrust AC 或本地操作系统）以及订阅数据库（可以是本地数据库或驻留在其他主机中的其他 PMDB）的列表。PMDB 本质上是主规则数据库或模板。在 PMDB 中定义的规则及其所有更改都应用到订阅数据库。

PMDB 工具提供了简单的层级结构模型，可用来向多个系统分发访问规则并创建对于一组主机都相同的访问规则。通过在层级结构中配置 PMDB，您可以支持多级策略，从顶级-模板（适用于企业中所有主机的访问规则）到较低级模板（定义适用于主机的子组的特定规则）。

虽然 PMDB 可以有多个订户，但是只能为了实现接收传播的规则更改这一目的而为一个父 PMDB 订阅 PMDB 或本地数据库。另外，为了传播密码更改，每个 PMDB 可以有相同的父 PMDB，也可以有不同的父 PMDB（称为密码 PMDB）。与规则更改相反，密码更改的传播是双向的，即，从启动更改的主机上的本地数据库到密码策略模型的顶端，再向下回到层级结构中的所有订户。

设置加密

如果您的网络包含多个运行 eTrust AC 的服务器，则对不同服务器上的 eTrust AC 服务之间的通信进行加密。默认情况下，eTrust AC 使用快速且有效的编码算法进行加密。

eTrust AC 还提供了在安装过程中可以选择的 AES、DES 和 3DES 加密选项。

标准加密

eTrust AC 加密形式是在动态链接库 (DLL) 中实施的。该 DLL 实施所有数据加密和解密，允许数据以安全的形式在客户端程序（selang.exe 或 SeAM.exe）和代理服务之间进行传输。可以使用 sechkey 实用程序在命令提示下或使用 ChEncKey.exe 实用程序从 Windows 中更改默认加密项。

eTrust AC 安装将名称为 defenc.dll（用于默认加密）、aes128enc.dll（用于 128 位 AES 加密）、aes192enc.dll（用于 192 位 AES 加密）、aes256enc.dll（用于 256 位 AES 加密）、desenc.dll（用于 DES 加密）和 tripledesenc.dll（用于 3DES 加密）文件安装在以下目录中：

```
eTrustACDir\bin
```

其中 eTrustACDir 为安装 eTrust AC 的目录。

defenc.dll、aesenc.dll、desenc.dll 或 tripledesenc.dll 的完整路径另存为以下注册表子键中的注册表值 Encryption Package：

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl
```

自定义加密

如果希望使用自己的加密方法，则必须写入新的 DLL。新的加密 DLL 不需要存储在以下目录中，但是您必须使用新 DLL 的完整路径目录名替换注册表值 Encryption Package：

```
eTrustACDir\bin
```

其中 eTrustACDir 为安装 eTrust AC 的目录。

加密 DLL 必须包含下列三个导出的函数：

1. DWORD Init(PCHAR pKey, DWORD dwLength)

   该函数初始化加密密钥。

2. DWORD Scramble(void *param, char *buffWithPlainText, int sizeofbuffWithPlainText, char *buffWithEncryptText, int *sizeofbuffWithEncryptText)

   该函数对第二个参数中收到的数据进行加密，并将加密的缓冲区保存在第四个参数中。

3. DWORD Unscramble(void *param, char *buffWithEncryptText, int sizeofbuffWithEncryptText, char *buffWithPlainText, int *sizeofbuffWithPlainText)

   该函数对第二个参数中收到的数据进行解密，并将缓冲区以纯文本的形式保存在第四个参数中。

重要！如果更改了加密密钥或加密 DLL，则必须在相互通信的所有主机中进行相同的更改。否则，会出现加密不相同且主机无法成功通信的情况。

第 3 章： 使用管理员界面

此部分包含以下主题：

策略管理器

策略管理器是用于管理和审核 Windows 和 UNIX 下 eTrust AC 本地数据库和 PMDB 的界面。本章以下几节介绍策略管理器，并说明如何使用 eTrust AC 来实施和维护安全策略。策略管理器还可以管理本地 Windows 和本地 UNIX 环境。使用策略管理器几乎可以执行可使用 Windows 用户管理器或在 UNIX 下使用命令行执行的所有操作。

策略管理器界面

所有数据管理任务都从策略管理器的主窗口开始。在您成功登录后即显示该窗口。

注意：要运行策略管理器，您的工作站必须在安装过程中定义为管理控制台。有关详细信息，请参阅《实施指南》。

菜单栏

菜单栏包含您可以与策略管理器一起使用的命令的下拉菜单。菜单栏结构是动态的，相应的命令显示您正在执行的操作。例如，只有在活动窗口包含树结构时才显示树菜单。

工具栏

工具栏提供常用命令的快捷访问。大多数命令也可以从菜单栏中访问。与菜单栏一样，工具栏是动态的，相应的命令显示您正在执行的操作。以下几节介绍通用工具。专用于特定窗口的工具在有关该功能的部分中介绍。

程序栏

您可以利用程序栏选择要保护或者要防御的特定项目。要在程序栏上显示面板，请单击标记为"访问控制"、"Windows NT"和"工具"的按钮。

工作区

工作区显示从"文件"菜单或程序栏打开的窗口。这些窗口称为应用程序窗口。

输出栏

输出栏显示命令日志，eTrust AC 在该文件中写入 selang 命令。输出栏中显示的信息是创建的命令、创建命令的主机、创建命令的环境以及执行命令的日期和时间。

每次开始策略管理器的新会话时，eTrust AC 都会创建新的命令日志。因此，如果希望从会话中保存命令，应保存或打印日志。

注意：策略管理器窗口输出栏中的每一行都可能表示命令日志中的多个 selang 命令。

注意：有关策略管理器及其使用方法的详细信息，请参阅《策略管理器联机帮助》。

管理访问者

访问者有时称作帐户，它是可以访问系统资源的实体。最常见的访问者类型是用户，通常是能够登录并应为其分配访问权限，且应检查其访问权限的人员。组、程序和终端也是访问者。

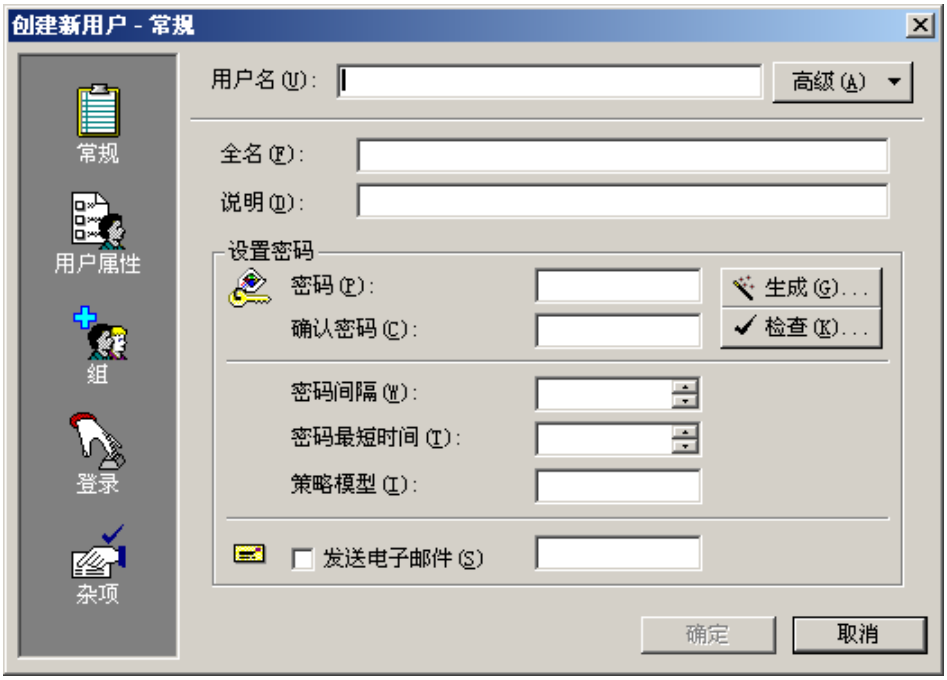
eTrust AC 可以仅使用帐户名或者使用以 Windows 域名或服务器名（当用户帐户不属于 Windows 域时）作为前缀的帐户名来标识用户，这取决于在 eTrust AC 数据库中创建用户记录时使用哪一项。

您可以管理在本地 Windows 操作系统和 eTrust AC 数据库（eTrust 环境）中定义的所有用户和组。您可以执行下列任务：

- 向一种或两种环境（Windows 和 eTrust）中添加用户或组。
- 更新一种或两种环境中的用户或组。
- 删除一种或两种环境中的用户或组。
- 重命名用户（仅适用于 Windows 环境）。
- 向组中添加用户，或者从组中删除用户。
- 向组中添加组，或者从组中删除组。
- 查看用户或组受保护的资源。

要执行这些功能，请单击  程序栏  "访问控制"面板中的"用户"或"组"，然后在工具栏上单击"新建"、"删除"或"属性"。

这是用于添加用户的对话框（单击"用户"和"新建"）：



单击左侧图标可显示不同面板。例如，显示的"常规"面板可用于输入用户名及说明，指定 eTrust AC 或 Windows 环境（"高级"按钮），并设置密码信息。

注意：eTrust AC 还为管理访问者所必需的部分任务提供向导。要访问向导，请单击"访问控制"面板中的"用户"或"组"，然后从"工具"菜单中选择或者单击"向导"工具栏按钮。

重要！我们极力建议您不要使用 Windows NT 备份域控制器 (BDC) 来定义用户。能够在本地 Windows 中使用"用户管理器"和"域用户管理器"执行的大多数功能，也都可以在程序栏的"访问控制"和 Windows 面板中执行。

使用"NT 导入向导"，您可以在安装过程中或之后将 Windows 系统中的用户和组导入到 eTrust AC 数据库。

注意：有关详细信息和详细过程，请参阅《策略管理器在线帮助》。

为访问者分配 Windows 权限

您可以为 Windows 中的用户和组分配标准和高级权限。大多数高级权限仅适用于为运行 Windows 工作站或 Windows 服务器的计算机编写应用程序的编程人员；通常不向组或终端用户授予高级权限。

注意：有关高级权限的详细信息，请参阅 Windows Server 编程文档。

限制用户登录

您可以通过几种方法限制用户的登录权限：

- 指定过期日期。
- 挂起帐户，以便它存在于 eTrust AC 数据库中，但用户却不能登录。
- 指定宽限登录的次数。
- 指定用户可以登录的最大终端数。
- 指定停用帐户之前必须经过的天数。
- 将登录权限限制为特定的工作日和小时。

默认情况下，帐户不会过期或停用，帐户不会被挂起，而用户可以没有限制地登录到任意数量的终端。

使用"登录"面板限制登录权限。

选择要审核的用户活动

对于 eTrust AC 数据库中定义的用户，您可以指定 eTrust AC 应审核的用户活动。

注意：只有在数据库中定义的、具有 AUDITOR 属性的用户才能指定审核属性。对于仅在本地环境中定义的用户，该选项将变灰。

下列审核模式指定 eTrust AC 审核日志中包含的用户活动。用于创建和编辑用户的对话框中的"杂项"面板中提供这些选项。

成功

记录对 eTrust AC 中定义的资源的成功访问。

登录成功

记录成功的登录。

登录失败

记录失败的登录尝试。

失败

记录访问数据库中定义的资源的失败尝试。

所有

记录所有用户活动，无论成功与否。

无

不记录用户活动。

输入个人信息

您可以从创建和编辑用户对话框的“杂项”面板中输入有关用户的个人信息。这些属性是可选的。

位置

最多可包含 128 个字符的字母数字字符串，指定用户的位置，如 Main Office 或 East Coast Sales。

国家 / 地区

最多可包含 19 个字符的字母数字字符串，指示用户所在的国家或地区。

组织

最多可包含 256 个字符的字母数字字符串，指示将用户分配到其中的组织。

组织部门

最多可包含 256 个字符的字母数字字符串，指示将用户分配到其中的组织部门。

电话

最多可包含 19 个字符的字母数字字符串，指示用户的电话号码。

电子邮件

最多可包含 256 个字符的字母数字字符串，指示用户的电子邮件地址。

设置帐户信息

您可以从创建和编辑用户对话框的"杂项"面板中设置有关用户的帐户信息。这些属性是可选的。

主目录

用户的主目录。用户自动登录到他们自己的主目录。

脚本

用户登录时自动运行的文件名。该登录脚本配置工作环境。

配置文件路径

包含用户配置文件的文件的完整路径。每当用户登录到任何工作站时，都在屏幕上显示相同的环境。

分配用户权限

您可以从创建和编辑用户对话框的"杂项"面板中分配用户权限。用户权限包括的项目如：

- 更改系统时间
- 加载和卸载设备驱动程序
- 本地登录
- 还原文件和目录
- 备份文件和目录

使用 B1 安全功能

您可以使用 B1 "橙皮书"安全功能来添加额外的安全保护。通过单击创建和编辑用户对话框的"杂项"面板上的"B1 功能"按钮，可以从"B1 功能"对话框中选择安全标签、类别和级别。

- 您可以为用户分配一个介于 1 至 255 之间的安全级别。只有在用户的安全级别大于或等于分配给资源的安全级别时，用户才可以访问该资源。
- 用户可以属于一个或多个安全类别。只有在用户属于分配给资源的所有安全类别时，用户才可以访问该资源。
- 安全标签将特定的安全级别与一组安全类别相关联。将用户分配给某一安全标签会授予该用户与该安全标签相关联的安全级别和所有安全类别。

分配会话组

使用创建和编辑用户的"杂项"面板上的"会话"按钮，您可以为用户分配 eTrust SSO 会话组。

将用户添加到组中

您可以将用户添加到组中，以便大大简化管理。使用用于创建和编辑用户的对话框的"组"面板：

添加嵌套组

您可以从创建和编辑组对话框的"杂项"面板添加或修改嵌套组。（单击程序栏中的"组"，然后单击工具栏上的"新建"或"属性"。）

您可以利用"嵌套组"对话框从现有组中添加和删除超级组（父项）和成员组（子项）。高级组的属性向下传递给其成员组。

设置 Active Directory 属性

如果连接至带有 Active Directory 的 Windows 2000 计算机，则可以使用"用户属性或组属性"对话框的"目录服务"面板来设置 Active Directory 用户或组属性。在 Windows NT、不含 Active Directory 的 Windows 2000 或者 eTrust AC 本地环境数据库中不支持这些属性。

只有在您连接到带有 Active Directory 的 Windows 2000 计算机时，才会出现用于激活该面板的图标。

注意：您可以使用 Active Directory 将用户组织到不同文件夹中。策略管理器在单个"用户"面板中显示所有的 Active Directory 用户。

与本地操作系统同步数据

使用 selang 命令时，您可以在数据库中更改有关访问者的数据，而不更改本地操作系统中的数据。同样，在 Windows 中使用用户管理器时，您可以在 Windows 中更改有关访问者的数据，而不更改 eTrust AC 中的数据。在使用上述方法更改数据时，在每个数据库中以不同方式定义访问者。

eTrust AC 监视 eTrust AC 和本地操作系统中的定义，并在 Windows 和 eTrust AC 中的定义不匹配时提供一个"同步"面板。如果定义匹配，则不显示"同步"图标。

管理 eTrust AC 资源

资源是用户和组可访问的实体。最常见的资源类型是文件。访问文件是指从文件读取信息或向文件写入信息。

资源按类分组，类是资源类型的名称。例如，TERMINAL 类包含作为终端的所有对象，例如 tty1、tty2 等；SHARE 类包含共享的所有对象；FILE 类包含文件和目录的定义。

注意：有关 eTrust AC 类的详细信息，请参阅《参考指南》。

受保护资源的属性存储在资源的记录中。记录是由资源的名称和属性组成的数据集合。特定类中的每条记录包含同一组属性（即该类说明的对象类型的相应属性）的值，。

属性指明定义资源的用户、定义资源的日期等等。一般情况下，资源记录中包含的最重要信息是授权访问资源的访问者列表。该列表称为访问控制列表 (ACL)。许多资源包含另一个访问者列表，拒绝其中的访问者进行访问。该列表称为否定式访问控制列表 (NACL)。

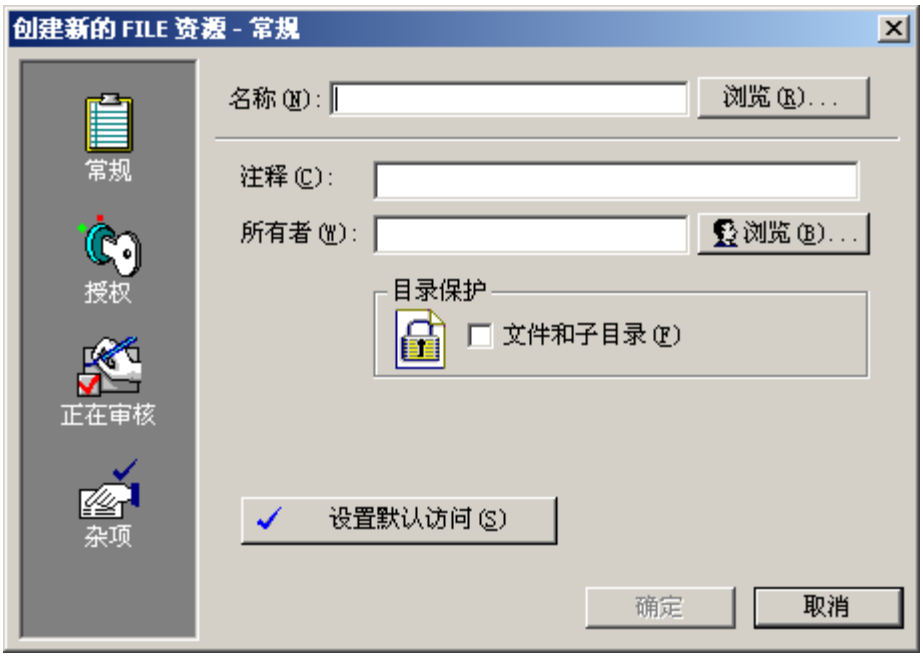
注意：您可以右键单击用户名或组名，并从显示的菜单中选择"受保护的资源"，来查看特定用户或组的 ACL 或 NACL。

通过执行下列操作，您可以管理 eTrust AC 数据库中的所有资源：

- 向 eTrust AC 数据库中的任何类添加资源
- 更新 eTrust AC 数据库中任何类的资源
- 从 eTrust AC 数据库中的任何类中删除资源
- 定义用户可以从中登录的终端和终端组
- 定义用户需要额外权限才能登录的假期
- 定义任务委托和任务组

要执行这些功能，请  在程序栏的"访问控制"面板中单击"资源"，在工作区中选择一个资源，然后单击工具栏上的"新建"、"删除"或"属性"。

下面是用于在 FILE 类中创建资源的对话框（单击"资源"和"新建"）：



单击左侧图标可显示不同面板。例如，显示的"常规"面板用于输入资源名和说明、指定所有者等等。

使用日历管理 eTrust AC 资源

eTrust AC 根据 Unicenter TNG 日历支持用户、组和资源访问实施。日历包含 15 分钟的时间间隔，您可以将其设置为 ON 或 OFF。将日历时间间隔设置为 OFF 可禁止访问资源；将日历时间间隔设置为 ON 可允许访问资源。eTrust AC 按指定的时间间隔检索 Unicenter TNG 活动日历。

您可以使用"资源"视图添加、编辑或删除日历资源。在资源树中选择"登录保护"。单击"日历"树条目，然后右键单击以选择一个选项。

管理 Windows 资源

您可以使用用于创建和编辑资源的对话框来管理本地 Windows 数据库中的资源。您可以：

- 将资源添加到 Windows 数据库中的 REGISTRY 和 SHARE 类。
- 更新包括 Active Directory 数据库在内的 Windows 数据库中的所有类中的资源。
- 从 Windows 数据库中的任何类中删除资源。

注意：有关 Windows 资源的详细信息，请参阅《参考指南》中"Windows 环境中的类和属性"一章。

管理 Windows 域

使用策略管理器，您可以：

- 显示有关 Windows 域的信息。
- 向 Windows 域中添加新的计算机。
- 删除 Windows 域中的计算机。
- 创建和删除 Windows 域之间的受托关系。

在资源树中选择"NT 指定"。单击"域"树条目，然后右键单击以选择一个选项。

当 eTrust AC 客户端（如策略管理器或 selang）执行这些操作时，eTrust AC 检查它们的有效性。检查操作的有效性时，eTrust AC 使用域控制器中存在的 eTrust AC 数据库中的授权规则。

eTrust AC 的 DOMAIN 类中的每条记录定义一个 Windows 域。对 DOMAIN 类中的记录的三种可能访问权限是：

READ

允许用户显示域的属性

CHMOD（更改委托）

允许用户创建或删除域之间的委托关系

EXEC（执行）

允许用户向域中添加成员，或者从域中删除成员

保护进程

PROCESS 类中的对象定义需要 eTrust AC 保护的进程应用程序。

要使用 eTrust AC 保护进程，请完成下列步骤：

1. 启动 eTrust AC 策略管理器。
2. 从程序栏中，选择"资源"。
3. 展开 eTrust AC 资源树，以便显示"系统资源"，然后选择"进程"。
4. 新增要保护的进程，请右键单击名称列，然后选择"新建"或者单击键盘上的 Insert 键。
5. 启动 Windows 任务管理器 (taskmgr.exe)。任务管理器必须正在运行才能执行后续步骤。
6. 单击"名称"字段旁边的"浏览"。选择要保护的进程 (taskmgr.exe)。单击"确定"。
7. 单击"所有者"字段旁边的"浏览"。
8. 选择"nobody"。单击"确定"。
9. 单击"设置默认访问权限"按钮。

   将出现"设置默认访问权限"对话框。
10. 确定选择了"无"。单击"确定"。
11. 要测试该规则，请打开任务管理器 (taskmgr.exe)，选择"进程"选项卡，选择 taskmgr.exe，然后单击"结束进程"。
12. 将出现"任务管理器警告"对话框。单击"是"。

    如果已经成功执行了该规则，则会出现"无法终止进程"对话框。
13. 要添加授权用户以结束选定的进程，请展开 eTrust AC 资源树，以显示"系统资源"，然后选择"进程"。
14. 右键单击某个进程，选择"属性"。
15. 单击"授权"。
16. 单击"插入"。
17. 单击"名称"字段旁边的"浏览"。
18. 选择"用户或组"选项卡，然后单击"确定"。
19. 选中"读取"权限，单击"确定"。
20. 要测试新规则，请作为授权用户登录以结束进程。

21. 打开任务管理器 (taskmgr.exe)，选择"进程"选项卡，选择 taskmgr.exe，然后单击"结束进程"。

    至此该进程应该结束。

注意：Windows 服务是 eTrust AC 进程保护的适合对象，因为这些服务中大部分都在后台而不是 GUI 或交互式应用程序中运行。

使用 SPECIALPGM 保护资源

SPECIALPGM 类中的对象定义需要特殊 eTrust AC 授权保护的应用程序。该类尤其适用于保护通常必须用系统帐户运行的程序，例如系统服务。要保护这类程序，请将它们定义为 SPECIALPGM 类中的记录，并将逻辑用户名（定义为 eTrust AC 数据库中的 USER 记录）与运行该程序所需的 Windows 用户名相关联，仅授权该逻辑用户运行这些程序。

在 Windows 中，可以使用“特殊程序向导”帮助设置该保护。要从 GUI 运行该向导，请单击程序栏中的“资源”按钮。然后从“工具”菜单选择“特殊程序向导”。

管理策略模型

您可以使用策略管理器管理多个 PMDB 功能。这些功能包括指定 PMDB、管理订户、管理错误日志、启动和停止策略模型后台程序（在 UNIX 中）、重新激活不可用的订户以及显示属性。

指定 PMDB

eTrust AC 支持一台主机上的多个策略模型。您可以使用策略管理器或 selang 来指定 PMDB。

显示策略模型窗口

从程序栏的"工具"面板激活的策略模型窗口列出在所连接的工作站上定义的所有 PMDB，包括可能有的订户。

策略模型窗口包括以下列：

名称

列出选定 PMDB 的订户。

类型

显示订户的类型：eTrust 数据库、PMDB 或 MF（主机）。

状态

指示订户是否可用。如果不存在等待执行的命令，则订户可用。如果订户的父 PMDB 已发送一个或多个尚未执行的命令，则订户不可用。命令保存在 updates.dat 文件中，其默认位置为 eTrustACDir\data\pmdb（其中，eTrustACDir 是安装 eTrust AC 的目录）。

下一个命令

显示等待执行的命令。

如果订户的状态为可用，则该列为空。

错误

为选定订户显示错误数。错误是指失败的命令，即它未更新订户。连接失败不包括在内。

已执行命令

显示已执行命令的百分比。如果订户的状态为可用，该列显示 100% 。

管理策略模型层级结构

PMDB 的订户可以是：

- 同一主机或远程主机上的另一个 PMDB
- 同一主机或远程主机上的 eTrust 数据库
- 大型机数据库

使用策略管理器，您可以：

- 将订户添加到 PMDB
- 从 PMDB 中删除订户
- 显示发送给订户但未能更新订户的命令，即错误日志中出现的错误
- 清除错误日志的内容

在添加订户时，确保父 PMDB 和要订阅它的所有工作站都包含在同一网络中，并可以通过名称相互进行通信。这样 eTrust AC 才可以更新订户的注册表中的 parent_pmd 键。

使用错误日志

策略模型错误日志 包含订户工作站拒绝应用的事务列表。

使用策略管理器，您可以显示 PMDB 及其所有订户的错误，或者仅显示一个订户的错误。还可以清除错误日志的内容。

"策略模型错误日志"对话框包含以下列：

主机

失败命令所在 PMDB 的全名。

命令

失败的完整 eTrust AC 命令。

错误描述

命令失败的原因。

偏移量

updates.dat 文件中命令的位置。

日期

命令失败的日期。

时间

命令失败的时间。

注意：如果单击"下一步"按钮，eTrust AC 将显示下一个记录集。query_size 注册表键定义集中的记录数。（默认值为 100。）将下一个集中的记录添加到显示。这意味着，如果您按一次"下一步"按钮（并且该键值仍然为 100），则显示 200 条记录。

显示属性

通过从"视图"菜单或右击菜单中选择"属性"，可显示 PMDB 或订户的属性。

下面说明父 PMDB 显示的属性。

策略模型名称

PMDB 的名称。

父策略模型

指示 PMDB 是否为父项。

密码文件

仅用于 UNIX，包含有关本地定义用户的信息（例如，用户的全名、ID、用户所属组的 ID、主目录以及加密密码）的文件的名称。

组文件

仅用于 UNIX，包含有关本地定义组的信息（例如，组 ID 和组中用户的列表）的文件的名称。

eTrust AC 显示"策略模型"窗口 (p. 47) 以说明订户的属性。

使用 eTrust AC for Windows 管理 UNIX

您可以使用策略管理器来管理安装了 eTrust AC 的 UNIX 计算机。您可以管理 UNIX 和 eTrust AC 环境中定义的用户、组、资源和 PMDB 层级结构。

管理员资源

ADMIN 类

通过使用策略管理器的"按类访问"功能，您可以将对象添加到 ADMIN 类中。

- ADMIN 类包含允许非 ADMIN 用户管理特定类的定义。
- ADMIN 记录表示将由授权用户管理的每个 eTrust AC 类。
- 记录包含具有每个记录的访问权限的访问者列表。
- ADMIN 类记录的关键字是将要保护的类的名称。

示例:

要定义非 ADMIN 用户执行 ADMIN 类功能，请参考以下示例：

注意：以下示例需要两个工作站才能完成。我们将本地终端称为 **computer1**，而将远程终端称为 **computer2**。计算机名因环境可能有所不同。

1. 在本地终端 (computer1) 上创建用户 sub_admin。
   a. 启动 eTrust AC。
   b. 在程序栏上单击"用户"，并创建新用户。
   c. 在"用户名"字段中输入 sub_admin。
   d. 在"全名"字段中输入 sub_admin。
   e. 在"说明"字段中输入 sub_admin。
   f. 在"密码"字段中输入您需要记住的密码。
   g. 单击"高级"下拉菜单。一定要同时选中：
      - 在本地 OS 环境中创建
      - 在 eTrust AC 环境中创建
   h. 单击"确定"
2. 在远程终端 (computer2) 上创建用户 sub_admin。
   a. 启动 eTrust AC。
   b. 在程序栏上单击"用户"，并创建新用户。

      注意：必须以下列格式输入远程访问用户名：

      `computer_name\user_name.`
   c. 在"用户名"字段中输入 computer1\sub_admin。
   d. 在"全名"字段中输入 computer1\sub_admin。
   e. 在"说明"字段中，输入 computer1\sub_admin。
   f. 单击"高级"下拉菜单。选择"仅在 eTrust AC 环境中创建"。单击"确定"。

3. 在远程终端 (computer2) 上允许本地终端 (computer1) 访问。
   a. 在远程终端 (computer2) 上，单击 eTrust AC 程序菜单，然后单击"资源"。
   b. 展开登录保护树，右键单击"名称"列中打开的字段，然后选择"新建"。
   c. 输入您的本地终端 (computer1) 信息。
   d. 在"名称"字段中输入本地终端 (Computer1) 的名称。
   e. 在"备注"字段中输入终端 (Computer1)。
   f. 在"所有者"字段中输入"nobody"。
   g. 单击"设置默认访问权限"，并确保选择"无"。
   h. 单击"确定"。
   i. 单击"授权"。
   j. 单击"插入"。
   k. 单击"名称"字段旁边的"浏览"按钮。
   l. 选择您在前面创建的 computer1\sub_admin 用户，单击"确定"以返回到"添加/编辑 eTrust 访问者"对话框。
   m. 将出现"添加/编辑 eTrust 访问者"对话框。单击"确定"。
   n. 选择您刚才添加的用户，选中"读取"权限，然后单击"确定"。

4. 在远程终端 (computer2) 上，展开管理树，选择"按类访问"，然后选择"USER 类"。

   a. 右键单击"USER 类"，选择"属性"，然后单击"授权"。

   b. 单击"插入"。

   c. 单击"名称"字段旁边的"浏览"。

   d. 选择您在前面创建的 computer1\sub_admin 用户，单击"确定"以返回到"添加/编辑 eTrust 访问者"对话框。

   e. 将出现"添加/编辑 eTrust 访问者"对话框。单击"确定"。

   f. 选择您刚才添加的用户，选中"读取"权限，然后单击"确定"。

5. 确定两台计算机的 eTrust AC 都在同一个网络上运行。

6. 在本地计算机 (computer1) 上，以 sub_admin 用户身份登录到 Windows。

7. 在本地计算机 (computer1) 上，启动 eTrust AC。单击位于左上侧的连接图标。

8. 输入远程终端主机 (computer2) 的名称，然后单击"确定"。

9. 将出现"连接信息"对话框。单击"确定"。

   单击"确定"后，将打开策略管理器。您将连接到远程终端 (computer2)。

10. 在策略管理器中，单击  "用户"。

11. 应出现下列错误消息。

12. "按类访问"也用于子管理。

    为了使子管理员可以管理管理员指定的类和资源，请仅在远程终端 (computer2) 上完成下列步骤：

    a. 选择"工具"菜单、"选项"和"启动"选项卡。

    b. 选中"启用用户和组子管理"，然后单击"确定"。

13. 再次单击 USERS。

    您将看到"用户列表"和"用户属性"。如果您试图更改任何用户属性，则将显示该状态的错误消息"不允许操作"。出现该情况是因为用户在 ADMIN/USER 类中只有"读取"访问权限。

    因为用户不是 ADMIN 类或 GROUP 类的授权用户，因此，如果您单击"组"也将出现 "不允许操作"错误消息。

14. 要浏览"组属性"对话框中的组和文件，您必须在"设置 Admin 属性"对话框中为对象组添加读取权限。

    a. 从远程终端中，展开管理资源树，选择"按类访问"，右键单击"组类"，然后选择"属性"。

    b. 单击"授权"，单击"插入"，选择您创建的终端，并设置"用户权限"。

    c. 从本地终端连接到远程终端，然后单击"组"。

    d. 您应该看到"组类"。

容器类

容器类中的每个记录定义一组来自其他资源类的对象、文件和用户。当一个规则应用于若干不同的对象类时，这可简化访问规则的定义。容器类记录的成员可以是来自任何 eTrust AC 类的对象、文件和用户。

示例:

在本示例中，在 CONTAINER 类中创建对象 MyContainer。收集该对象的两个成员，一个来自 FILE 类 (c:\winnt\notepad.exe)，另一个来自 TERMINAL 类 (MyComp.ca.com)。然后，您授权或者允许 John 对 MyContainer 的"读取"和"执行"权限。

1. 展开系统资源树，右键单击"文件"，单击"新建"，然后输入下列信息：

    a. 在"名称"字段中，输入 c:\winnt\notepad.exe。

    b. 在"备注"字段中，输入"Container Test Rule"。

    c. 在"所有者"字段中，指定"nobody"。

    d. 将"设置默认访问权限"设置为"无"。

2. 展开管理资源树，右键单击"容器"，选择"新建"，然后输入下列信息：

   a. 在"名称"字段中，输入 MyContainer。

   b. 在"备注"字段中，输入 MyContainer test。

   c. 在"所有者"字段中，指定"nobody"。

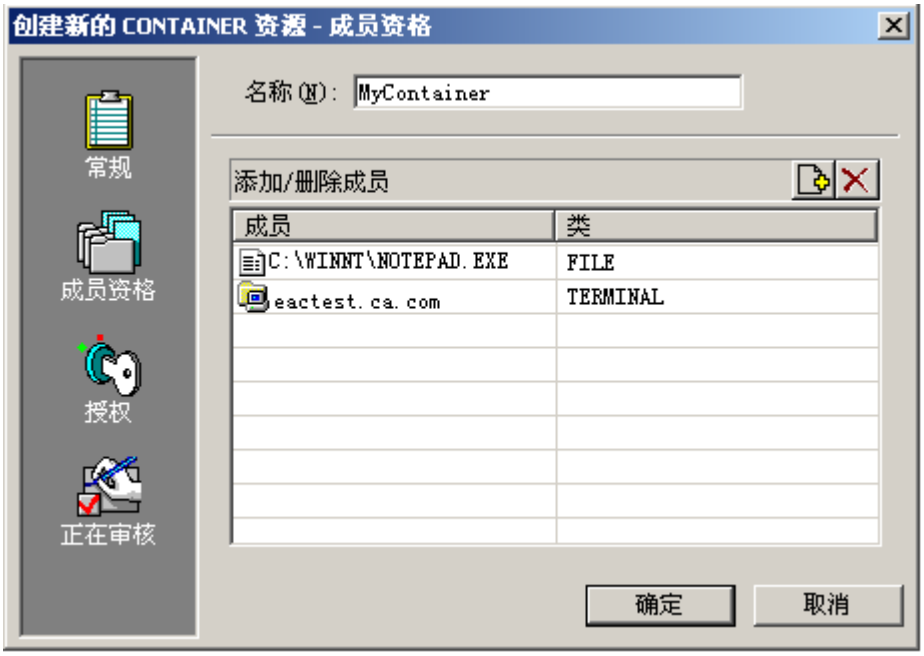
3. 单击"成员身份"，右键单击 MEMBERS 列中打开的字段，然后单击"添加"。

4. 选择 File 类，突出显示您创建的 File 规则 (c:\winnt\notepad.exe)，然后单击"确定"。

5. 右键单击"成员"列中打开的字段，然后单击"添加"。

6. 选择 Terminal 类，选择您想要添加的终端名称，然后单击"确定"。

   "容器资源"对话框如下所示：

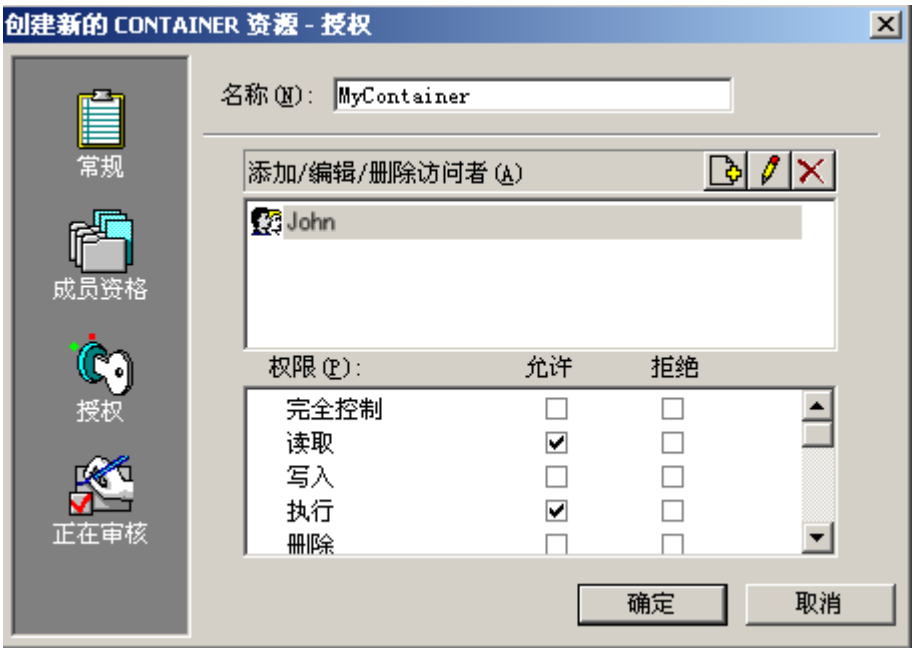


7. 单击"授权"，单击"插入"，再单击"名称"字段旁边的"浏览"，并选择"用户"。然后单击"确定"。

   将出现"添加/编辑 eTrust 访问者"。

8. 单击"确定"。

9. 为您选择的用户授予"读取"和"执行"权限。



10. 以前面指定的用户身份登录。由于在 MyContainer 中为该用户授予了"读取"访问权限，因此，您应该成功登录。
11. 运行 c:\winnt\notepad.exe，并允许它执行。
12. 尝试删除 c:\winnt\notepad.exe。该操作应该被禁止。
13. 尝试打开 eTrust AC 客户端、策略管理器或 selang 的会话。该操作应该被禁止，因为没有在 MyContainer 中为 John 授予"写入"访问权限。
14. 尝试更改您的"用户权限"，并拒绝所有项目。

    指定用户应该被拒绝登录。也应该拒绝执行 c:\winnt\notepad.exe。

创建子管理员

要通过策略管理器设置子管理员以管理用户和组，请完成下列步骤：

1. 启动策略管理器。

   注意：如果 eTrust AC 服务器安装在该计算机上，请在登录到策略服务器后关闭 eTrust AC 服务。

2. 从策略服务器工具栏中选择"工具"、"选项"。

   将显示"选项"对话框。

3. 选择"启动"选项卡，然后选中"启用用户和组子管理"。

4. 单击"确定"。

要使子管理员可从特定终端访问策略服务器，请完成下列步骤：

1. 在 eTrust AC 程序栏中选择"资源"图标以显示"资源"窗口。

2. 展开"登录保护"文件夹。

3. 选择"终端"，以显示可用终端的列表。

4. 双击您需要的终端。将显示"查看或设置终端属性 - 常规"对话框。

5. 选择"授权"图标，以便显示"查看或设置终端属性 - 授权"对话框。

6. 选择您要授权的子管理员，然后选中"读取"和"写入"权限。

7. 单击"确定"。

要定义具有管理用户权限的子管理员，请执行下列操作：

1. 在 eTrust AC 程序栏中选择"资源"图标以显示"资源"窗口。

2. 展开"管理"文件夹。

3. 选择"按类访问"，以显示可用类的列表。

4. 双击 USER 类，并选择"属性"。将显示"查看或设置 ADMIN 属性 - 常规"对话框。

   注意：要使子管理员能够管理其他类，请使用您需要的类（GROUP、USER_DIR 等等）代替 USER 类。

5. 选择"授权"图标，以显示"查看或设置 ADMIN 属性　授权"对话框。

6. 单击"添加"以显示"添加 eTrust AC 访问者"对话框。

7. 在"名称"字段中输入子管理员的名称，或者单击"浏览"以以查找名称。

8. 选中要授予子管理员的访问权限。

9. 单击"确定"，以便返回到"查看或设置 ADMIN 属性 — 授权"对话框。

10. 单击"确定"完成。

第 4 章： 管理用户密码

此部分包含以下主题：

密码管理实用程序

您可以使用下列实用程序来管理用户密码：

密码管理器

您可以使用密码管理器来设置和替换用户密码。

密码管理器是一个独立的密码管理工具，可以安装在没有运行策略管理器的计算机上。这有助于将密码管理任务分配给非管理员用户。

策略管理器

每当您创建或更新 Windows 中定义的用户时，都可以设置或替换用户密码。

还可以使用策略管理器 (p. 35) 设置密码策略。

selang 命令

selang 命令 newusr、editusr 和 chusr 设置用户的密码。

注意：有关这些命令的详细信息，请参阅《参考指南》。

Windows 实用程序

您可以使用 Windows 用户管理器或者在命令提示窗口中使用 Windows 命令来管理用户密码。

注意：有关详细信息，请参阅相关的 Windows 文档。

使用密码管理器、策略管理器或 selang 来设置或更改用户密码时，在向数据库中添加密码之前，eTrust AC 不检查它的密码规则。eTrust AC 接受您从这些工具中输入的任何密码。因此，根据 eTrust AC 中的密码规则，新密码可能无效。当使用 Windows 用户管理器或其他非 eTrust AC 软件来更改密码时，eTrust AC 会检查新密码的有效性。

管理密码和锁定策略

密码是最常用的身份验证机制，但密码保护方法却存在众所周知的问题：简易密码容易被猜中；持续使用多年的密码和循环密码最终会被破坏；而网络上明文发送的密码可能被侦听者截获。

Windows 有一套强制用户使用密码的密码规则和策略，可以避免大多数这些常见陷阱。eTrust AC 提供确保用户选择更为安全的密码的附加规则。

您可以在 eTrust AC 中指定下列规则：

- 新密码不得与以前的密码匹配。在密码策略中指定 eTrust AC 存储的以前的密码个数。
- 新密码不得包含用户名。
- 新密码不得包含正在替换的密码。
- 新密码不得与正在替换的密码相匹配。eTrust AC 不区分大小写。
- 新密码至少必须有在密码策略中指定的最低数量的字母数字字符、特殊字符、数字、小写字符和大写字符。
- 新密码中重复的字符数不得超过密码策略中指定的字符数。
- 新密码不得为 eTrust AC 包括的字典中受限制的单词之一。该字典由注册表子键中的 Dictionary 值指定：

  `HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\passwd`

每个密码必须有最长使用期限（即，它到期必须失效），从而强制用户在某一时间间隔后选择新的密码。

- 每个密码必须有一个最短使用期限。通过指定一个最短使用期限，您可以防止用户迅速频繁地更改密码。使用频繁更改的密码，他们可以溢出密码历史堆栈，然后重复使用以前的密码。

使用密码管理器

如果在工作站上安装了密码管理器，则可以使用它来设置新密码，或替换现有密码。

您可以在设置或替换密码时执行以下操作：

- 要求用户在下次登录时更改他们的密码。
- 重置已锁定的用户帐户，以便不再锁定该用户。
- 更改目标主机，以便可以为远程主机、本地主机的 PMDB 或远程主机的 PMDB 上的用户设置密码。默认情况下，eTrust AC 假定用户位于本地主机上。
- 配置 eTrust AC，以便生成符合组织密码策略的用户密码。
- 配置 eTrust AC，以便向您更改了其密码的用户发送电子邮件，通知他们新的密码。

生成密码

您可以在密码管理器中为现有用户生成密码。eTrust AC 生成的密码始终符合您为站点确立的条件。要生成密码，您必须选择"启用密码生成"作为系统选项。默认情况下，选择"密码生成"选项。

更改目标主机

您可以更改目标主机，以便为本地主机的 PMDB、远程主机或者远程主机的 PMDB 上的用户设置密码。

设置用户密码更改

在策略管理器中，您可以设置一种功能来提醒用户更改他们的密码。当用户登录到策略管理器时，将出现一个提醒更改密码的对话框。如果单击"是"，则出现"更改密码"对话框。

要设置该功能，请完成以下步骤：

1. 单击"访问控制"程序栏中的"资源"图标。
2. 在"工具"菜单中选择"激活 eTrust 类"。选中"密码"框，以及"更改自己的密码"框。
3. 单击"确定"。

解析错误消息

如果您正在为 Windows NT 系统上的用户设置密码，则可能出现下列消息：

密码太短，不符合要求。

该错误表明密码不符合策略要求。这可能是由以下任何一种原因造成的：

- 该密码短于或长于要求长度。
- 该密码最近已被使用，并存在于"Windows NT 更改历史记录"字段中。
- 该密码没有足够多的唯一字符。
- 该密码不符合其他密码策略要求（例如，使用 eTrust AC 密码策略设置的要求）。

为了避免该错误，请确保设置符合所有相关要求的密码。

第 5 章： 保护帐户

此部分包含以下主题：

保护用户模拟请求

帐户登录后，您必须监视它，以确保它在系统资源上仅执行已授权的功能。操作系统根据访问者的用户 SID 对文件提供某种程度的保护。要绕过该保护，用户必须首先把自己模拟成另一个用户 SID。操作系统防范未经授权模拟的措施是，模拟操作要求发出请求的用户指定目标用户的密码。

该方案有许多缺点。要把自己模拟成某个用户 SID 的用户必须记住目标用户的密码，记下密码，或者要求目标用户使用简易密码。这违反了一些密码策略。另外，没有有效的责任；您可能永远不知道哪个用户更改了特定用户的标识。此外，当某个用户知道超级用户的密码后，就可以绕过任何安全保护，从而无限制地访问系统。

eTrust AC 使用一种更高级的方法来保护用户模拟：只有在特定的规则允许更改时，用户才可以将用户 SID 更改为另一个用户的 SID。

例如，假设用户 X 运行一个程序，该程序以用户 Y 身份执行某些任务。如果用户 X 知道用户 Y 的密码，但没有权限替换为用户 Y，则该程序请求会被拒绝。

这样，入侵者仅知道管理员的密码还不够；在数据库中还必须有一种允许入侵者成为管理员的规则。

每个用户 SID 和组 SID 在数据库中都有访问规则。eTrust AC 已经为这种保护类型指定了 SURROGATE 类。如果在初始阶段希望授予任何模拟请求的访问权限，请使用下列命令：

```
eTrust> editres SURROGATE _default defaccess(READ)
```

该命令告知 eTrust AC：如果用户发出请求把自己模拟为另一个用户，并且数据库中的记录不明确保护该用户替代，则允许访问。

要防止尝试将 SID 替换为超级用户的 SID，请使用下列命令：

```
eTrust> newres SURROGATE USER.Administrator defaccess(NONE)
```

该命令告知 eTrust AC：Administrator 用户名是受保护的，因此没有被明确允许使用该名称的用户不能模拟 Administrator。要允许安全管理员使用 Administrator，必须使用以下命令明确进行指定：

```
eTrust> authorize SURROGATE USER.Administrator gid("Security Admins")
```

注意：

- 如果用户的 SURROGATE 记录没有特别允许某个用户进行替换，则此用户获得该记录的默认访问权限。在上一个示例中，默认值为 NONE，这意味着没有权限的用户无法模拟为 Administrator。
- 名为 USER._default 的记录代表自己没有记录的所有用户。类似地，名为 GROUP._default 的记录代表自己没有记录的所有组。如果某个访问者没有 SURROGATE 记录，则替换为该访问者的请求将以 SURROGATE USER._default 记录、SURROGATE GROUP._default 记录或者 _default 记录（用户和组）中指定的默认值结束。
- _default 记录的默认值为 READ；未定义的 SURROGATE 记录意味着允许模拟为这些用户。该默认值符合实施过程中的一般经验规则，即“只要没有在 eTrust AC 中定义，就得不到 eTrust AC 的保护”。您可以在实施阶段后将该规则修改为相反的规则，即“只要 eTrust AC 没有允许就会自动被 eTrust AC 禁止”。
- 许多 Windows 实用程序和服务（例如，Run As）标识为“NT AUTHORITY\SYSTEM”用户，而不是运行它们的原始用户。要让使用这些实用程序和服务的用户模拟其他用户，您必须在 eTrust AC 数据库中创建此 SYSTEM 用户，并授权它模拟目标用户。例如：

  ```
  auth SURROGATE USER.Administrator uid("NT AUTHORITY\SYSTEM") acc(R)
  ```

设置 Surrogate DO 工具

操作员、生产人员和最终用户通常需要执行只有超级用户才能执行的任务。

传统的解决方案是向所有这些用户提供超级用户密码，这会危及到站点的安全。安全的替代方法（即保持密码的保密性）会使系统管理员因处理用户要执行例行任务的合法请求而导致负担过重。

Surrogate DO (sesudo) 实用程序解决了这个难题。它允许用户执行 SUDO 类（其中每条记录包含一个脚本）中定义的操作，指定哪些用户和组可以运行脚本，以及基于这一目的借给他们必要的权限。

例如，就好像用户为系统一样，要定义启动“Print Spooler”服务的 SUDO 资源，请输入以下命令：

```
eTrust> newres SUDO StartSpooler data("net start spooler")
```

该 newres 命令将 StartSpooler 定义为受保护的操作，某些用户可能获得执行的系统权限。

重要！在数据属性中，请使用完整的绝对路径名。相对路径名可能会意外地执行未受保护的目录中植入的特洛伊木马程序。

此外，通过使用 authorize 命令，可以授权用户执行 StartSpooler 操作。例如，要允许用户 operator1 启动“Print Spooler”服务，请输入下列命令：

```
eTrust> authorize SUDO StartSpooler uid(operator1)
```

还可以使用 authorize 命令明确防止用户执行受保护的操作。例如，要防止用户 operator2 启动“Print Spooler”服务，请输入命令：

```
eTrust> authorize SUDO StartSpooler uid(operator2) access(None)
```

运行 sesudo 实用程序将执行受保护的操作。例如，使用下列命令，用户 operator1 将启动“Print Spooler”服务：

```
cmd> sesudo -do StartSpooler
```

sesudo 工具首先检查是否授权用户执行 SUDO 操作，然后，如果授权用户使用资源，则执行资源中定义的命令脚本。在我们的示例中，sesudo 检查是否授权 operator1 执行 StartSpooler 操作，然后使用系统凭据调用命令“net start spooler”。

注意：有关 sesudo 实用程序的详细信息，请参阅《实用程序指南》。有关格式化 SUDO 记录的数据属性的详细信息，请参阅《参考指南》中的 chres、editres 和 newres 命令。

检查用户无操作状态

无操作状态功能防止通过其所有者离开的帐户或者组织不再采用的帐户未经授权擅自访问系统。无操作日是用户未登录的日期。您可以指定在用户帐户被挂起和无法登录之前必须经过的无操作天数。一旦挂起帐户，则必须手工重新激活它。

注意：在无操作状态检查方面，会将密码更改视为活动。如果用户密码更改，则该用户不能因为无操作而被挂起。

可以使用 USER 类记录或 GROUP 类记录的无操作属性设置无操作天数。后者只影响将该组作为配置文件组的用户。您还可以使用 SEOS 类的 INACT 属性，为系统范围内的所有用户设置无操作。

selang 和安全管理器都提供了设置无操作的方法。在 selang 中，使用以下命令可以通过全局方式指定无操作状态：

```
setoptions inactive ( numdays)
```

要设置组的无操作天数（覆盖该组系统范围的无操作设置），请使用下列命令：

```
{chgrp | editgrp | newgrp} groupName inactive ( numdays)
```

要设置用户的无操作天数（覆盖该用户的组和系统范围设置），请使用下列命令：

```
{chusr | editusr | newusr} userName inactive ( numdays)
```

要重新激活挂起的用户帐户，请使用以下命令：

```
{chusr | editusr} userName resume
```

要重新激活挂起的配置文件组，请使用以下命令：

```
{chgrp | editgrp} userName resume
```

要禁用系统级的无操作登录检查，请使用下列命令：

```
setoptions inactive-
```

要禁用对组的无操作登录检查，请使用以下命令：

```
{chgrp | editgrp} groupName inactive-
```

要禁用对用户的无操作登录检查，请使用以下命令：

```
{chusr | editusr} userName inactive-
```

第 6 章： 集中管理策略

此部分包含以下主题：

策略模型数据库

单独管理数十个或数百个数据库是不切合实际的，因此 eTrust AC 提供了策略模型服务，一个允许从一个中心数据库对许多数据库进行管理的组件。使用策略模型 (PMD) 服务是可选的，但是它将极大地简化大型站点上的管理。

注意：在 Windows 任务管理器中，策略模型服务显示为 sepmdd.exe。

策略模型服务使用策略模型数据库 (PMDB)。与其他 eTrust AC 数据库一样，PMDB 包含用户、组、受保护的资源和管理资源访问的规则。此外，PMDB 还包含一个订户数据库列表。每个订户都是驻留在独立计算机上的一个 eTrust AC 数据库，或者驻留在同一或不同计算机上的其他 PMDB。更新订户的 PMDB 是订户的父项。

在管理具有类似权限限制和访问规则的多个数据库方面，PMDB 是一个非常有用的工具。

注意：有关使用 sepmd 实用程序来管理 PMDB 以及远程管理 PMDB 的信息，请参阅《参考指南》。

磁盘上的 PMDB 位置

计算机中的所有 PMDB 都驻留在一个公用目录中。在下列 Windows 注册表子键中的 _pmd_directory_ 值指定该目录的名称：

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\Pmd
```

在 NTFS 根目录中，_pmd_directory_ 的默认值为：eTrustACDir\data，其中 eTrustACDir 是您安装 eTrust AC 的目录（默认为 C:\Program Files\CA\eTrustAccessControl）。

每个 PMDB 都占用公共目录中的一个子目录。子目录中的文件包含定义策略模型必需的所有数据。策略模型配置设置存储在 eTrust AC 注册表设置的 Pmd 子键中。该子键的名称就是策略模型的名称。

管理本地 PMDB

eTrust AC 提供用于管理 PMDB 的实用程序：

sepmd

您可以使用 PMDB 管理实用程序来执行以下任务：

- 管理订户
- 截短更新文件
- 管理双重控制
- 管理策略模型日志文件
- 执行其他管理任务

注意：有关 sepmd 实用程序的全面论述，请参阅《参考指南》。

管理远程 PMDB

eTrust AC 还提供一系列可以在 pmd 环境中使用的 selang 命令。您可以使用这些命令远程管理 PMDB：

createpmd

创建 PMDB。

deletepmd

删除 PMDB。

findpmd

显示计算机上所有 PMDB 的名称。

listpmd

列出以下关于 PMDB 的信息：

- 订户及其状态
- PMDB 描述及其状态
- 更新文件中的命令及其偏移量
- 错误日志的内容

pmd

您可以使用 PMDB 管理命令来执行以下任务：

- 从不可用订户列表中删除订户
- 清除策略模型错误日志
- 启动和停止策略模型服务
- 截短更新文件
- 重新加载注册表设置

subs

您可以使用 PMDB 订阅命令执行以下任务：

- 向父 PMDB 添加订户
- 为数据库（eTrust AC 或另一个 PMDB）指定父 PMDB

subspmd

为本地数据库指定父 PMDB。

unsubs

从 PMDB 中删除订户。

注意：有关可以在 pmd 环境中使用的 selang 命令的全面论述，请参阅《参考指南》。

体系结构相关性

部署 eTrust AC 时，您应当考虑环境的层级结构。在许多站点上，网络都包括各种体系结构。有些策略规则（例如受托程序列表）与体系结构密切相关。另一方面，大多数规则都与系统体系结构无关。

您可以使用层级结构来包括这两种规则。您可以为与体系结构无关的规则定义一个全局数据库，向它提供订户 PMDB，从而定义与体系结构相关的规则。

注意：根 PMBD 及其所有订户可以驻留在同一计算机或不同计算机上，这取决于您的环境的实际需要。

示例：一个两层的部署层级结构

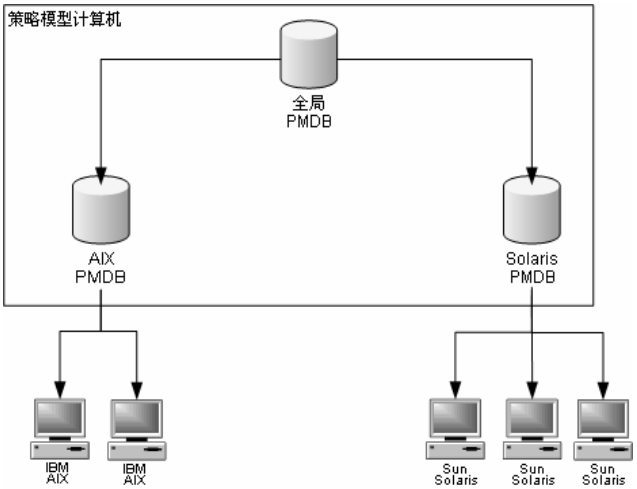
下面的 UNIX 示例也适用于 Windows 体系结构，不过需要做一些小修改。

在该示例中，站点包括 IBM AIX 和 Sun Solaris 系统。由于 IBM AIX 上的受托程序列表与 Sun Solaris 上的列表不同，因此，PMDB 需要考虑体系结构的依赖性。

要设置多体系结构 PMDB，请按以下步骤设置 PMDB：

1. 定义名为 whole_world 的 PMDB，以包含用户、组和所有其他与体系结构无关的策略。
2. 定义名为 pm_aix 的 PMDB，以包含所有特定于 IBM AIX 的规则。
3. 定义名为 pm_sol 的 PMDB，以包含所有特定于 Sun Solaris 的规则。

   名为 pm_aix 和 pm_solaris 的 PMDB 是名为 whole_world 的 PMDB 的订户。站点上的所有 IBM AIX 计算机都是 pm_aix 的订户者。站点上的所有 Sun Solaris 计算机都是 pm_sol 的订户。下面以图表说明该概念。



4. 当您在 whole_world 中输入与平台无关的命令，例如添加用户或设置 SURROGATE 规则，则自动更新站点上的所有数据库。
5. 当您向 pm_aix 中添加受托程序时，只更新 IBM AIX 计算机，而不会影响 Sun Solaris 系统。

集中管理策略的方法

您可以使用 eTrust AC 以两种方式从一个计算机中管理多个数据库：

- 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。

  注意：仅此方法提供双重控制，并且仅在 UNIX 中可用。

- 高级策略管理和报告

  您部署的策略（规则组）将被传播给配置的层级结构中的所有数据库。您还可以取消部署（删除）策略和关于部署状态、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。

注意：高级策略管理和报告功能提供基于规则的自动策略更新所没有的附加功能。但是，要使用高级策略管理，您首先需要为基于规则的自动策略更新配置环境。

基于规则的自动策略更新

您在中央数据库中进行的单一规则策略更新（常规 selang 规则）将自动传播给订户数据库。通过为同一数据库订阅几个计算机，并为一个数据库订阅另一个数据库，您可以创建层级结构。您可以为基于规则的自动策略更新配置环境。

注意：这种管理策略的方法限制于让您在整个层级结构进行单一策略更新。其他功能只能通过实施高级策略管理和报告 (p. 80)来提供。

基于规则的自动策略更新原理

为基于规则的自动策略更新配置环境时，您在中心数据库中定义的每条规则自动通过以下方式传播给它的所有订户：

1. 必须为至少有一个订户的任何 PMDB 定义一条规则。
2. PMDB 向所有订户数据库发送命令。
3. 订户数据库应用传播的命令。
   a. 如果订户数据库没有响应，则 PMDB 按规定时间间隔（默认情况下为每隔 30 分钟）发送命令，直到更新了订户数据库为止。
   b. 如果订户数据库正在响应，但拒绝应用命令，则 PMDB 会将命令放在策略模型错误日志 (p. 78)中。
4. 如果订户数据库是其他订户的父项，则将命令发送给它的订户。

示例:从层级结构中的所有计算机上删除用户

如果使用 rmusr 命令删除 PMDB 中的用户，则将相同的 rmusr 命令发送给所有订户数据库。这样一来，一个 rmusr 命令就可以从不同计算机上的许多数据库中删除用户。

如何能够设置层级结构

eTrust AC 使用策略模型服务在配置的层级结构中传播基于规则的策略更新。通过为同一个 PMDB 订阅几个 eTrust AC 计算机，并通过为一个 PMDB 订阅另一个 PMDB，您可以创建层级结构。

设置 PMDB 层级结构的最简单方式是在安装 eTrust AC 时进行设置，因此，在开始安装之前，有必要考虑要如何构建层级结构。由于父 PMDB 及其订户必须能够相互通讯，因此必须确保 PMDB 层级结构中的所有主机都属于同一个网络。也就是说，父 PMDB 必须能够按名称连接它的每个订户，而每个订户必须能够按名称连接到父 PMDB。

注意：有关安装 eTrust AC 的详细信息，请参阅《实施指南》。

如果您想要更改在安装期间创建的配置，或者如果您在安装期间没有创建 PMDB 结构，您可以随时更改或创建 PMDB 配置。您可以使用下列方式之一来执行该操作：

- 利用策略管理器
- 利用 sepmd 实用程序

要创建 PMDB 层级结构并在安装后启用基于规则的自动策略更新，请执行以下操作：

1. 创建和配置主 PMDB。
2. （可选）创建和配置订户 PMDB。
3. 定义订阅计算机的父 PMDB，称为端点。

更新订户

更新订户时，策略模型执行以下操作：

1. 当向策略模型中添加订户名称，或者从中删除订户名称时，策略模型将试图对其进行完全限定。
2. PMDB 服务即 sepmdd 尝试更新订户数据库。
3. 如果超出最长等待时间，但该服务无法成功更新某个订户，则它会忽略该订户，并尝试更新列表中的其余订户。
4. 完成订户列表的首次扫描后，sepmdd 会接着执行第二次扫描，在这次扫描期间，它会尝试更新在第一次扫描期间未成功更新的订户。

注意：每次 PMDB 在将更新传播到订户的过程中遇到错误时，sepmdd 服务都会在策略模型错误日志文件 (p. 78)中创建一个条目。文件 ERROR_LOG 位于 PMDB 目录 (p. 68)中。

更新策略模型数据库

在 PMDB 驻留的计算机上工作不会自动更新 PMDB 本身。要更新 PMDB，您需要将其指定为目标数据库。

您可以使用 selang 或策略管理器来指定 PMDB。要使用 selang 来指定目标数据库，请使用 selang 命令 shell 中的 hosts 命令：

```
eTrustAC> hosts <pmd_name>@<pmd_host>
```

所有 selang 命令立即更新指定的策略模型数据库。这些命令然后自动传播到此计算机和所有订户计算机上的活动数据库中。

注意：有关策略管理器的详细信息，请参阅《策略管理器联机帮助》。

示例:指定目标 PMDB

要将目标数据库设置为 myPMD_host 上的 policy1，请使用以下命令：

```
eTrustAC> hosts policy1@myPMD_host
```

如果您现在输入 newusr 命令，则新用户将被添加到 policy1 数据库以及此计算机和所有订户计算机上的活动数据库中。

清理更新文件

sepmd 实用程序自动写入它在 updates.dat 文件中接收到的每项更新。为了防止该文件变得过大，建议您定期删除文件中已处理过的更新。

要清理更新文件，请使用以下命令：

```
<eTrustAC_InstallDir>/bin sepmd-t pmdbName auto
```

sepmd 计算尚未传播的第一个更新条目的偏移量，并删除在它之前的所有更新条目。

传播并同步密码

设置 PMDB 层级结构后，当使用 Windows 用户管理器或 eTrust AC 以外的软件更改用户密码时，您可以使用 PMDB 层级结构使用户密码在系统中保持同步。

注意： eTrust AC 也支持大型机密码同步 (p. 133)。

传播并同步密码

1. 创建 PMDB 层级结构。
2. 在用户或管理员可以更改密码的每个工作站上，输入适当的父 PMDB 的名称作为注册表中的 passwd_pmd 项值。

   ```
   HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\
   eTrustAccessControl\passwd_pmd
   ```

   PMDB 然后将密码更改传播到它的所有订户。如果 passwd_pmd 值为空，则 eTrust AC 将检查 secondary_pmd 值，除非该值也为空，否则将新的和更新的密码发送到该值中列出的 PMDB。

注意：如果 PMDB 将用户密码发送到没有定义用户的订户，则不会更改设置，并且一直不定义订户的用户。

删除订户

如果您不再希望将更新传播给某个订户，则应当将其删除。

删除订户

1. 将计算机从订阅列表中删除：

   ```
   sepmd-u <PMDB_name> <computer_name>
   ```

   从策略模型订阅列表中删除计算机。

2. 关闭在您从订阅列表中删除的计算机上的 seosd：

   ```
   secons -s
   ```

   seosd 服务被关闭。

3. 在您从订阅列表中删除的计算机上删除以下注册键中的 parent_pmd 注册表值：

   ```
   HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\
   eTrustAccessControl
   ```

   计算机将停止接受来自 PMDB 的更新。

4. 重新启动 seosd。

   在您从订阅列表中删除的计算机上的活动数据库不再是指定 PMDB 的订户。

注意：从 PMDB 取消订阅数据库后，PMDB 不再发送命令。

筛选更新

如果希望 PMDB 更新不同订户数据库上的不同数据子集，您需要定义向订户数据库发送哪些记录。

筛选更新

1. 配置 PMDB 以便用作订户子集的父集。
2. 修改父 PMDB 的注册表键中的 Filter 注册表项，以指明要在同一计算机上设置的筛选器文件。

   然后将对订户数据库的更新限于通过该筛选器的记录。

策略模型筛选器文件

筛选器文件由每行具有六个字段的行组成。字段包含如下信息：

- 允许或禁用的形式。

  例如，EDIT 或 MODIFY

- 受影响的环境：

  eTrust、UNIX 或 Native

- 记录的类。

  例如，USER 或 TERMINAL

- 规则涵盖的类中的对象。

  例如：User1、AuditGroup 或 COM2

- 记录授予或取消的属性。

  例如，筛选行中的 OWNER 和 FULL_NAME 意味着具有这些属性的任何命令都会被筛选。您必须按照《参考指南》中所示的方式准确地输入每个属性。

- 这类记录是否应该转发到订户数据库：

  PASS 或 NOPASS

以下规则适用于筛选器文件中的每一行：

- 可以使用星号 (*) 表示任意字段中的所有可能值。
- 如果不止一行包括相同的记录，则使用适用的第一行。
- 用空格分隔字段。
- 在具有多个值的字段中，使用分号分隔值。
- 任何以 # 开始的行都被视为注释行。
- 不允许有空行。

示例:筛选器文件

以下示例介绍筛选器文件中的行：

CREATE	eTrust	USER	*	FULL_NAME;OBJ_TYPE	NOPASS
↑	↑	↑	↑	↑	↑
访问形式	环境	类	记录名 （* =全部）	属性	处理

在此示例中，如果我们将具有该行的文件命名为 Printer1_Filter.flt 并编辑 PMDB PM-1 的注册表，以便筛选 =C:\Program Files\CA\eTrustAccessControl\Printer1_Filter.flt，则 PMDB PM-1 不会向其订户发送使用 FULL_NAME 和 OBJ_TYPE 创建新用户的记录。

策略模型错误日志文件

按时间先后顺序组织的策略模型错误日志看上去与以下内容类似：

错误文本	错误类别
20 Nov 03 11:56:07 (pmdb1): fargo nu u5 0 Retry ERROR: 登录过程失败 (10068) ERROR: 无法接受来自非-父 PMDB 的更新 (pmdb1@name.company.com) (10104)	配置错误
20 Nov 03 19:53:17 (pmdb1): fargo nu u5 0 Retry ERROR: 连接失败 (10071) 主机不可访问 (12296)	连接错误
20 Nov 03 11:57:06 (pmdb1): fargo nu u5 560 Cont ERROR: 创建 USER u5 失败 (10028) 已存在 (-9) 20 Nov 03 11:57:06 (pmdb1): fargo nu u5 1120 Cont ERROR: 创建 USER u5 失败 (10028) 已存在 (-9)	数据库更新错误

策略模型错误日志采用二进制格式，您只有通过输入以下命令才能查看它：

```
<eTrustAC_InstallDir>/bin sepmd-e pmdname
```

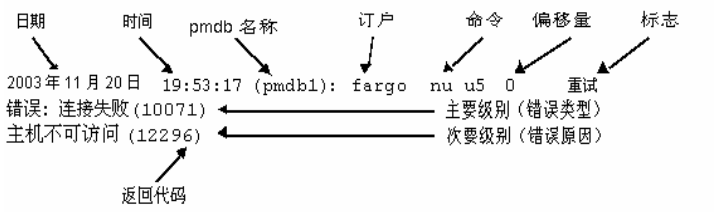
注意：不要手动删除错误日志（例如，使用 UNIX rm 命令）。只能使用以下命令删除日志：

```
<eTrustAC_InstallDir>/bin sepmd-c pmdname
```

重要！ eTrust AC r5.1 及更高版本的错误日志的格式与以前版本的格式不兼容。sepmd 无法处理以前版本的错误日志。当您升级到具有该格式的版本时，旧的错误日志被复制到 ERROR_LOG.bak 中；在您启动 sepmdd 时将创建新的日志文件。

示例:PMDB 更新错误消息

以下示例显示典型的错误消息：



- 第一行总是包括日期、时间和订户。接下来显示产生错误的命令，然后是偏移量（十进制格式），指示更新文件中失败更新的位置。最后，标志指示 PMDB 是自动重试更新，还是忽略该命令而继续。
- 第二行显示主要级别消息（发生的错误类型）的示例及消息的返回代码。
- 第三行显示次要级别消息（发生错误的原因）示例及消息的返回代码。

示例:错误消息

一个命令可能会产生并显示多个错误。而且，一个错误可能包括主要级别消息、次要级别消息或同时包括这两种消息。

下列错误只有一个消息级别：

```
Fri Dec 29 10:30:43 2003 CIMV_PROD:Release failed. Return code = 9241
```

sepmd pull 尝试释放可用的订户时出现该消息。

本地策略模型存储库

您可以在 PMDB 中存储所有的本地环境用户和组对象类型。通过在 PMDB 中存储该信息，您可以使用 show 命令（例如 show user 或 show group）接收有关对象的信息。返回的对象是在 Windows 或 UNIX 订户中定义的实际对象的映像。

在连接到策略模型之后，用户可以选择下列环境：

- eTrust
- 本地
- NT
- UNIX

注意：当您在 Windows 操作系统上工作时，本地完全与 Windows 一样运行，或者，当您在 UNIX 操作系统上工作时，则本地完全与 UNIX 一样运行。

要使用本地环境存储库，请使用下列命令：

- 在 selang 提示符后输入下列命令：

  ```
  env NT; find
  ```

  您的结果将列出所有的本地环境对象类型。

  注意：有关这些对象类型的说明，请参阅《参考指南》中的“Windows 环境中的类和属性”一章。

- 输入下列命令以接收 NT 和 Active Directory USER 属性列表：

  ```
  env NT; ruler user
  ```

- 输入下列命令以接收 NT 和 Active Directory GROUP 属性列表：

  ```
  env NT; ruler group
  ```

如果某个策略模型是另一个（父）策略模型的订户，它则通过传播接收父策略模型的数据，并在数据库中保存所有的用户和组属性，因此，您可以查看并更改这些属性。

注意：有关详细信息，请参阅《参考指南》中的“sepmd 实用程序”一节。

高级策略管理和报告

您创建的多规则策略可以存储并部署在配置的层级结构中。使用这种基于策略的模型，您可以存储策略版本，然后部署和取消部署策略。您还可以创建有关部署状态、部署偏差和部署层级结构的报告。

注意：此方法不提供双重控制，该控制仅在 UNIX 中可用。

环境体系结构

要使用高级策略管理和报告功能，您需要安装和配置以下附加组件：

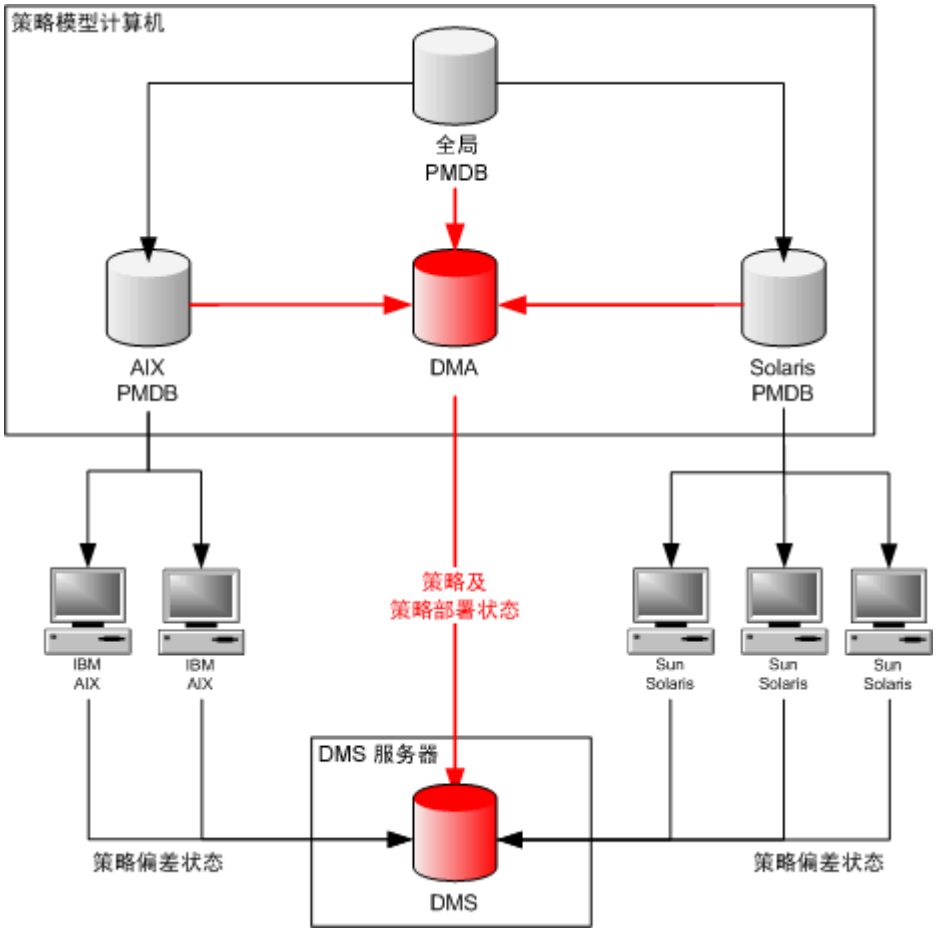
- 在用于此用途的中央计算机上的部署映射服务器 (DMS) (p. 82)。
- 在每台包含至少一个 PMDB 的计算机上的部署映射代理 (DMA) (p. 82)。

注意：高级策略管理和报告功能要求为基于规则的自动策略更新设置环境。在适当的计算机上安装 DMS 和 DMA 后，请配置父数据库和订户数据库 (p. 73)。

示例:一个具有中央 DMS 的两层层级结构

注意：下面的 UNIX 示例也适用于 Windows 体系结构，不过需要做一些小修改。

在该示例中，站点包括 IBM AIX 和 Sun Solaris 系统。由于 IBM AIX 上的受托程序列表与 Sun Solaris 上的列表不同，因此，PMDB 需要考虑体系结构的依赖性。出于管理和报告的目的，我们设置 DMS 和 DMA 支持在配置多 PMDB 环境 (p. 70)时创建环境。DMS 存储所有策略部署和偏差信息，eTrust AC 允许您利用这些信息来创建报告。



部署映射服务器 (DMS)

DMS 居于高级策略管理和报告的核心。DMS 的目的是保持 eTrust AC 部署层级结构的最新映射和每台计算机上部署的策略的状态。将此数据存放在中心位置（而不是以分层方式连接每个数据库）将减少生成报告所需要的时间。此外，DMS 存储您可以在以后根据要求部署和取消部署的策略的版本。

DMS 是一个 PMD 节点，并将 PMDB 作为其数据存储库。DMS 收集了它从由每个为其自身配置的 PMD 节点发出的通知中接收到的数据。

部署映射代理 (DMA)

DMA 是负责 PMD 与 DMS 通信的代理。您应当在每个 PMD 节点（至少一个 PMDB）上安装一个 DMA。父 PMDB 上的 DMA 通知 DMS 有关策略部署状态和层级结构变化的情况。端点只将策略偏差状态直接发送到 DMS。

注意：不要在端点计算机上安装 DMA。

DMA 使用标准的 eTrust AC 通信和加密机制来与 DMS 通信。

注意：您不需要为启用 DMA\DMS 通信而将 DMA 定义为 DMS 的父项。

高级策略管理类

DMS 的目的是保持 eTrust AC 部署层级结构的最新映射和每台计算机上部署的策略的状态，它使用特定的 eTrust AC 类。

HNODE

每个 HNODE 对象都代表层级结构中的一个节点。它保留关于其所代表的某个节点、其订户和父 PMDB 的信息。另外，每个 HNODE 对象还保留关于要在其所代表的节点上部署的策略以及每个策略的状态（已部署、部署出错，等等）的信息。

HNODE 对象的名称与其代表的节点的类型有关：

- 端点的实际主机名。

  例如，myhost.mydomain.com

- PMDB 的策略模型名称。

  例如，mypmd@hostB.domain.com

POLICY

每个 POLICY 对象代表可以在 HNODE 层级结构的任意部分上部署的策略的版本。它包含关于存储关联策略脚本的位置（在 RULESET 对象中）和要部署策略的节点的信息。

对象名称由策略名称和版本号后缀组成（即 policy_name#xx）。

RULESET

每个 RULESET 对象保留与策略版本关联的部署和取消部署（删除）脚本。

该对象名称基于各自的 POLICY 对象名称。

注意：有关这些类的详细信息，请参阅《参考指南》。

如何设置基于策略的高级管理和报告的层级结构

eTrust AC 使用 DMS 来保持 eTrust AC 部署层级结构的最新映射和每台计算机上部署的策略的状态。通过在层级结构中的每台计算机上安装和配置适当的组件，您可以启用基于策略的管理和报告功能。

要启用基于策略的管理和报告功能，请执行以下操作：

1. 在中央计算机上安装 DMS。

   DMS 可以在 eTrust AC 安装期间进行安装，或通过 dmsmgr 实用程序来安装。

2. 在每个 PMD 节点上安装一个 DMA。

   DMA 可以在 eTrust AC 安装期间进行安装，或通过 dmsmgr 实用程序来安装。

3. 在每个 eTrust AC 计算机上安装高级管理和报告功能。

   该功能配置偏差计算，以便将策略偏差状态发送到 DMS。

4. 设置层级结构 (p. 73)。

   设置层级结构时，在 DMS 中添加代表层级结构中每个节点的 HNODE 对象。

   重要！当您从计算机中卸载 eTrust AC 或删除 PMDB 时，HNODE 对象保留在计算机上。您需要删除弃用的对象节点 (p. 86)。如果您取消从层级结构中订阅数据库，则 HNODE 对象保留，但将删除其指向父节点的链接。您虽然不需要删除此对象，但它将保持指向以前在节点上创建的策略对象的链接。

注意：有关安装 DMS 和 DMA 以及配置高级策略管理和报告功能的信息，请参阅《实施指南》。

DMS 通知

当您配置配置高级策略管理和报告的环境时，层级结构中的组件将通知 DMS 以下三个方面的状态变化：

- 层级结构变化。

  添加或删除订户（PMD 节点或端点）时发送通知。

- 策略部署和取消部署。

  当对订户（PMD 节点或端点）部署或取消部署策略时发送通知。然后根据操作结果（成功、失败，等等）更新策略详细信息和部署状态。

- 偏差状态。

  当 eTrust AC 端点计算策略偏差并发送结果（发现或未发现偏差）时发送通知。

注意：层级结构变化以及策略部署和取消部署通知只能由 DMA 通过 PMD 节点发送。偏差状态通知只能由偏差计算器通过 eTrust AC 端点发送。

层级结构和策略状态通知的工作原理

DMA 将层级结构变化和策略状态通知发送给 DMS。以下列方式对 DMA 通知进行处理：

1. DMA 将通知消息存储在更新文件中。

   这些通知包括层级结构变化通知以及策略部署和取消部署通知。

2. DMA 与 DMS 联系：

   - 如果 DMS 不可用，则 DMA 尝试定期与 DMS 通信，直至所有消息都成功发送出去。
   - 如果 DMS 可用，则 DMA 发送存储的通知。

   注意：每个 DMA 直接与 DMS 通信，绕过层级结构并降低依赖性。

3. DMS 存储从每个 DMA 接收到的信息以供将来使用。

   每次创建报告时，eTrust AC 都会在 DMS 上检索信息。

偏差通知的工作原理

偏差计算器随 eTrust AC 一起安装，并在其计算偏差的端点上本地运行。偏差计算器执行以下操作并向 DMS 发送偏差通知：

1. 通过向端点发送一个 selang 命令 (start devcalc) 触发偏差计算过程。

   建议您按自定义脚本规定执行计划来计算偏差。

2. 完成计算后，偏差计算器将结果存储在一个数据文件中。

   该文件是 <eTrustAC_Dir>\data\devcalc\deviation.dat

   注意：报告实用程序可以检索偏差详细信息（使用 -dev 选项）。另外，您可以在端点上使用 get devcalc 命令来检索数据文件的内容。

3. 偏差计算器然后将偏差状态（发现偏差或未发现偏差）发送到 DMS。

   偏差本身（即数据文件的内容）不随状态通知一起发送。

从层级结构中删除弃用节点

DMS 存储关于层级结构的信息。如果您在从计算机中卸载 eTrust AC 时将计算机从层级结构中删除，则 DMS 仍然保留对该节点的引用。作为常规维护过程，您应当将这些弃用节点从 DMS 中清理掉。

要从层级结构中删除弃用节点，请在 DMS 计算机上运行 dmsmgr 实用程序来执行常规清理：

```
dmsmgr -dms -cleanup <number_of_days>
```

其中，<number_of_days>是 eTrust AC 节点不可用后的最少天数。

注意：您可以通过在 DMS 计算机上发出以下命令手动删除特定节点：

```
rr HNODE <HNODE_name>
```

基于策略的高级管理的工作原理

您可以利用基于策略的高级管理来存储、部署和取消部署策略版本，并在以后创建有关部署状态、部署偏差和部署层级结构的报告。每个策略都是一对您创建的 selang 脚本文件。第一个脚本文件称为部署脚本，它包含一组构建策略的 selang 命令。第二个脚本文件是取消部署脚本，它包含从端点数据库取消部署（删除）策略所需的命令。

每个策略都分两个阶段应用到您指定的目标数据库：

1. 您可以将策略详细信息存储在 DMS 中。

   策略详细信息包括部署和取消部署脚本以及自动创建的策略签名（用于检测相同策略的变化）。

   如果未将策略详细信息存储在 DMS 中，则确保您：

   - 从对 DMS 拥有 TERMINAL 权限的计算机中存储策略。
   - 拥有对 DMS 中的 POLICY 和 RULESET 类子管理权限。
   - 没有包含语法错误的部署或取消部署脚本。

2. 此实用程序使用自动版本控制来存储策略。

   根据策略是否已经在 DMS 中存在，此实用程序执行以下任务之一：

   - 如果策略名称在 DMS 中并不存在，则它创建该策略的第一个版本 (policy_name#01)。
   - 如果策略名称已存在于 DMS 中，则它通过在找到的最高策略版本号基础上加 1，创建新的策略版本。

3. 您可向目标数据库部署存储的策略版本。

   如果未在目标层级结构中部署存储的策略，则确保您：

   - 从对目标根策略模型拥有 TERMINAL 权限的计算机中部署。
   - 拥有对 DMS 和您要部署策略的层级结构中的每个数据库里的 POLICY、RULESET 和 HNODE 类的子管理权限。
   - 在目标策略模型根计算机上拥有子管理权限。
   - 没有已经部署在组成部署层级结构的主机上的相同策略版本。

4. 每个规则 — 即在部署脚本中指定 selang 命令 — 在目标数据库上运行。

   如果不能在某个数据库上部署规则，则视为策略部署失败（已失败状态）。

   如果尝试在主机上部署策略并且部署脚本包含以下内容，就会出现这一情况：

   - 对不存在的对象的引用。例如：

     ```
     cr FILE /does_not_exist comment(123)
     ```

     由于这个原因，策略部署脚本必须是独立的。也就是说，必须构建部署脚本，以便其创建自己使用的所有资源。

   - 导致错误的命令。
   - 没有执行子管理权限的命令。

5. 策略状态可以记录下来。

   状态状态包括已部署 (Deployed)、已取消部署 (Undeployed)、已传输 (Transferred)、已失败 (Failed)（部署失败）、已排队 (Queued)、TransferFailed、SigFailed（签名失败）、UndeployFailed（取消部署失败）和未知 (Unknown)。

   注意：如果策略部署出错，您需要查看发生部署出错的计算机上的日志文件。

在 DMS 上存储并在目标数据库上部署策略详细信息后，如果目标数据库是 PMDB，则使用基于规则的自动策略更新机制在整个层级结构中传播该策略。

将新订户添加到层级结构中时，所有策略将通过层级结构传播，并通知 DMS 已经向层级结构添加节点。

管理要求

您可以从安装了 eTrust AC 的任何计算机中运行策略部署实用程序。要在 DMS 中存储策略，或在层级结构中的数据库上部署和取消部署策略，您及您使用的计算机必须拥有适当的权限。

要在 DMS 中存储策略，请执行以下操作：

- 您运行 policydeploy 实用程序的计算机必须拥有对 DMS 的终端访问权限（TERMINAL 类）。
- 您必须拥有对 DMS 中的 POLICY 和 RULESET 类的子管理权限。

要在整个层级结构中部署和取消部署策略，请执行以下操作：

- 您运行 policydeploy 实用程序的计算机必须拥有对作为目标根策略模型的计算机的终端访问权限（TERMINAL 类）。
- 您必须拥有：
  - 对 DMS 中的 POLICY 和 RULESET 类的读权限，以及对 HNODE 类的子管理权限。
  - 对您要部署策略的层级结构上的每个数据库中的 POLICY、HNODE 和 RULESET 类的子管理权限。
  - 在您要部署策略的层级结构上的每个数据库中的适当子管理权限。

    这些是在每台计算机上部署构成策略的 selang 命令必需的权限。

    例如，如果您要创建新的文件资源，则需要拥有对 FILE 类的子管理权限。

    ```
    nr FILE /inetpub/* defaccess(none)
    ```

如何部署审批过的策略版本

使用基于策略的高级管理，您可以存储策略的草稿版本，然后按照要求进行审查和修改，然后部署审批过的策略版本。

要部署审批过的策略版本，请执行以下操作：

1. 在 DMS 中存储某个策略版本。

   有了存储的策略版本后，可以对策略进行审查和部署。

2. 审查策略 (p. 91)。

   任何对 POLICY 和 RULESET 类拥有读权限的用户都可以查看策略及其关联规则。

3. 必要时，存储策略的新版本，其中包含审批更改。

   每当您需要更新某个策略时，您必须存储该策略的新版本，其中包含已做必要修改的策略部署和取消部署规则。

4. 向层级结构部署审批过的策略版本 (p. 92)。

存储策略版本

您存储在 DMS 中的每个策略都会自动获得一个版本号。当您第一次存储策略时，它将收到版本号“01”。例如，当您第一次存储策略 myPolicy 时，policydeploy 实用程序就会创建一个名为 myPolicy#01 的 POLICY 对象。每次您存储已经在 DMS 中存在的策略时，该策略的最新存储版本将按 1 递增，以创建新的策略版本。例如，当您存储了某个版本的 myPolicy 策略 28 次时，policydeploy 实用程序就会创建一个名为 myPolicy#28 的 POLICY 对象。

您可以查看存储的策略，并按要求向您的层级结构部署这些策略。

存储策略版本

1. 用 selang 部署命令创建新的脚本文件。

   这些是构建您想要在层级结构中的每个计算机上部署的策略必需的命令。

   重要！策略部署不支持设置用户密码的命令。不要将这类命令包含在您的部署脚本文件中。Windows（本地）selang 命令虽然受支持，但这些命令不会在偏差报告中出现。

2. 用 selang 取消部署命令创建新的脚本文件。

   这些是在层级结构中的计算机上取消部署（删除）策略必需的命令。

   注意：当您从目标层级结构取消部署策略时，默认情况下将使用这些命令，除非您在取消部署策略时提供新的策略取消部署脚本。

3. 使用 -store 选项运行 policydeploy 实用程序：

   ```
   policydeploy -store name -ds file1 -uds file2 [-dms list]
   ```

   其中，name 是您要存储的策略的名称，file1 是部署脚本文件的完整路径和名称，file2 是取消部署脚本文件的完整路径和名称，而 list 是可选的用逗号分隔的 DMS 节点列表。

   policydeploy 实用程序提示您是否要在 DMS 中创建策略的新版本。

   注意： 策略名称不能包含井号 (#) 字符，该字符已为用来表示策略版本号而保留，并自动进行添加。

4. 输入 y 确认此操作。

   policydeploy 实用程序在 DMS 中创建策略的新版本。

示例：存储 IIS 5 保护策略

下例说明如何存储用于保护 Internet 信息服务 Services (IIS) 5 Web 服务器的策略。这是我们第一次在 DMS 上存储该策略。

我们将在策略模型层级结构中部署 IIS5 策略，在该层级结构中 iis5@host.company.com 是根 PMDB。

1. 用以下 IIS 脚本保存名为 IIS5.selang 的文件：

   ```
   nu inet_pers owner(nobody)
   ```

```
nr FILE c:\InetPub\wwwroot\* defaccess(none) owner(nobody)
authorize FILE c:\InetPub\wwwroot\* uid(inet_pers) access(all)
nr FILE c:\InetPub\wwwroot\scripts defaccess(none) owner(nobody)
nr FILE *.asp defaccess(none) owner(nobody)
authorize FILE *.asp uid(inet_pers) via(pgm(inetinfo.exe)) access(read, execute)
```

这些是部署 IIS 5 保护策略必需的命令。

2. 用以下脚本保存名为 IIS5_rm.selang 的文件：

```
ru inet_pers
rr FILE c:\InetPub\wwwroot\*
rr FILE c:\InetPub\wwwroot\scripts
rr FILE *.asp
```

这些是取消部署我们在步骤 1 中创建的 IIS 5 保护策略必需的命令。

3. 运行 policydeploy 实用程序：

```
policydeploy -store IIS5 -ds IIS5.selang -uds IIS5_rm.selang
```

这将按 DMS 中 IIS5.selang 和 IIS5_rm.selang 定义的方式存储 IIS5 策略 (IIS5#01) 的第一个版本。

查看与策略关联的规则

在 DMS 中存储某个策略后，任何对 POLICY 和 RULESET 类拥有读权限的用户都可以查看该策略及其关联规则。如果不知道哪个是已存储策略的最新版本，您可以先把它找出来。

查看与策略关联的规则

1. 通过 selang 连接到 DMS：

```
hosts dms_name@hostname
```

您可以通过 selang 查询 DMS。

2. 如果您想要知道哪个是策略的最新版本，请发出以下 selang 命令找到策略的所有版本：

```
find POLICY policy_name#*
```

selang 窗口列出 policy_name 策略的所有版本。

3. 发出以下 selang 命令查看策略部署和取消部署脚本：

```
sr RULESET policy_name#xx
```

其中，xx 是您要查看其规则的策略的编号。

selang 窗口显示 policy_name#xx RULESET 对象，包括与 xx 版的 policy_name 策略相关的部署和取消部署规则。

部署存储的策略版本

您可以在层级结构中采用某种便利方式部署已存储的多规则策略的版本：允许您以后取消部署该策略，并创建有关部署状态、部署偏差和部署层级结构的报告。

部署存储的策略版本

请执行下面的操作之一：

- 如果您要部署已存储的策略的最新版本，请运行 policydeploy 实用程序，并指定策略名称和目标层级结构：

  ```
  policydeploy -deploy name -root db1[,db2] [-dms list]
  ```

  该实用程序用您提供的名称在 DMS 上查找策略的最新版本，并尝试在目标数据库上部署该版本。然后向预订数据库（如果存在）传播策略命令。

- 如果您要部署已存储的策略的特定版本，请运行 policydeploy 实用程序，并指定策略名称、策略版本和目标层级结构：

  ```
  policydeploy -deploy name#xx -root db1[,db2] [-dms list]
  ```

  该实用程序尝试在目标数据库上部署此策略的指定版本。然后向预订数据库（如果存在）传播策略命令。

注意：有关 policydeploy 实用程序的详细信息，请参阅《实用程序指南》（UNIX 版）或《参考指南》（Windows 版）。

重要!如果已经在部署层级结构包含的任何主机上部署了某个策略版本，则您无法部署相同的策略。

示例：部署 IIS 5 保护策略

下例说明如何部署用于保护 Internet 信息服务 (IIS) 5 Web 服务器安全的策略。我们将审查 IIS5 策略的第四个版本，然后在策略模型层级结构中部署它，在该层级结构中 iis5@host1.company.com 是根 PMDB。IIS5 策略存储在 crDMS@cr_host.company.com DMS 节点上。

1. 通过 selang 连接到 DMS：

   ```
   hosts crDMS@cr_host.company.com
   ```

   您可以通过 selang 查询 DMS。

2. 如果您不确定哪个是策略的最新可用版本，请发出以下 selang 命令找到该策略的所有版：

   ```
   find POLICY IIS5#*
   ```

   selang 窗口列出 IIS5 策略的所有版本。

3. 发出以下 selang 命令查看策略部署和取消部署脚本：

   ```
   sr RULESET IIS5#04
   ```

selang 窗口显示 IIS5#04 RULESET 对象，包括与第四版的 IIS5 策略相关的部署和取消部署规则。

4. 在命令行窗口中，运行 policydeploy 实用程序：

```
policydeploy -deploy IIS5#04 -root iis5@host1.company.com
```

这就会在 PMD 层级结构的 iis5@host.company.com 之下部署 IIS5 策略的第四个版本

取消部署策略

如果您不再希望在计算机上部署多规则策略，则可以从目标层级结构中取消部署该策略。如果您想要删除某个策略（创建该策略的更新版本），也需要取消部署该策略。

取消部署策略

1. （可选）用 selang 取消部署命令创建新的脚本文件。

   这些是在层级结构中的计算机上取消部署（删除）策略必需的命令。

   如果您没有创建和指定新的取消部署脚本，则取消部署命令使用部署时为策略指定的脚本。

   重要！即使您指定了策略取消部署脚本，DMS 仍记录您在存储策略时提供的原始规则，而不是用于取消部署策略的新脚本。

2. 请执行下面的操作之一：

   - 如果您要取消部署策略的最新版本，请运行 policydeploy 实用程序，并指定策略名称和目标层级结构：

     ```
     policydeploy -undeploy name -root db1[,db2] [-dms list] [-uds file2]
     ```

     该实用程序用您提供的名称在 DMS 上查找策略的最新版本，并尝试在目标数据库上取消部署该版本。然后向预订数据库（如果存在）传播策略取消部署命令。

     重要！如果层级结构中任意端点上的策略版本包含在 DMS 上找到的非最新版本，那么您必须明确取消部署这些特定版本。

   - 如果您要取消部署策略的特定版本，请运行 policydeploy 实用程序，并指定策略名称、策略版本和目标层级结构：

     ```
     policydeploy -undeploy name#xx -root db1[,db2] [-dms list] [-uds file2]
     ```

     该实用程序尝试从目标数据库中取消部署此策略的指定版本 (xx)。然后向预订数据库（如果存在）传播策略取消部署命令。

   注意：有关 policydeploy 实用程序的详细信息，请参阅《实用程序指南》（UNIX 版）或《参考指南》（Windows 版）。

注意：当您取消部署策略时，DMS 报告该策略的状态是已取消部署。POLICY 和 RULESET 对象始终保留在部署该策略版本的所有主机（包括 DMS）上，以便以后可以对它们进行重新部署或查询。

修改部署的策略

要修改部署的策略，您首先需要取消部署已部署的策略版本，存储包含修改过的部署和取消部署脚本的新版本策略，然后使用新版本重新部署策略。

修改部署的策略

1. 存储新的策略版本。。

   新的策略版本存储在 DMS 中。

2. 取消部署策略 (p. 94)。

   从目标层级结构中取消部署策略。

3. 部署策略的新版本 (p. 92)。

   将策略部署到包含修改策略的目标层级结构中。

高级策略报告的工作原理

您可以使用高级策略报告功能为配置的层级结构和使用基于策略的高级管理方法创建的策略创建有关部署状态、部署偏差和部署层级结构的报告。报告生成实用程序 (policyreport) 生成某个时间点（静态）的基于 DMS 内容的 HTML 报告。

policyreport 实用程序通过执行以下操作创建层级结构和策略报告：

1. 该实用程序查询 DMS 以获得请求的信息。

   检索到的信息取决于所生成的报告类型。

2. 如果请求了偏差计算，则该实用程序向端点查询策略偏差结果。

   虽然偏差状态在 DMS 中存在，但是必须从每个端点检索实际偏差。

3. 该实用程序生成一组 XML 文档。

   这是一个 XML 报告。

4. 该实用程序将 XML 报告的格式转换为 HTML。

   现在就可以在浏览器中查看报告了。

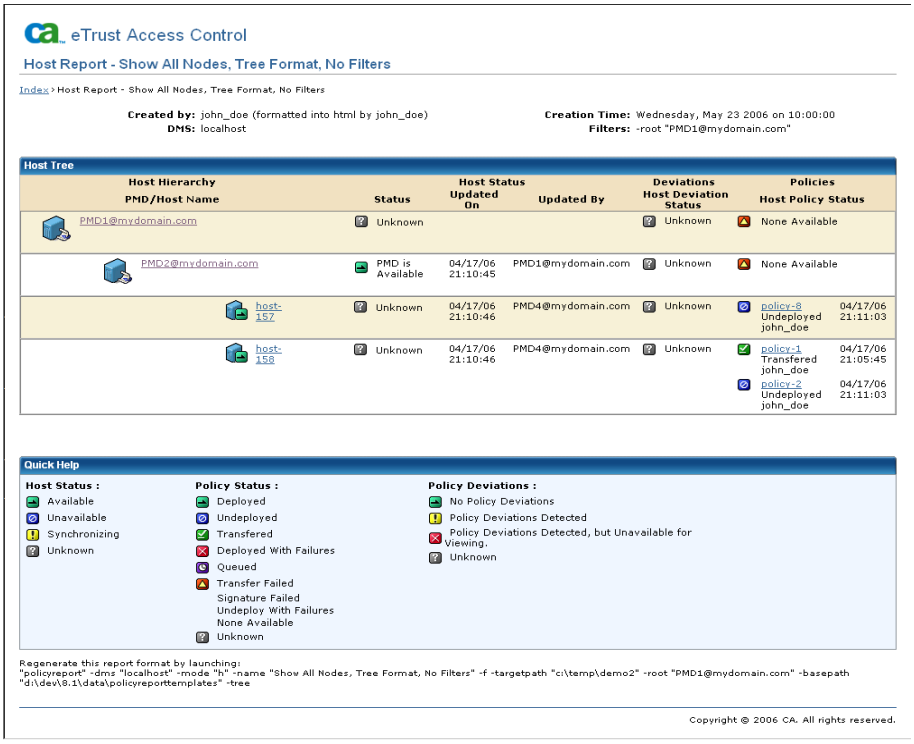
注意：policyreport 实用程序将报告存储在您使用 -name 选项指定的子目录中，而该子目录位于您使用 -targetpath 选项指定的目录下。

报告类型

您可以使用报告生成实用程序查看以两种模式在层级结构中部署的策略：

- 主机模式

  主机报告提供以计算机为主的信息。如果您要查看主机支持的环境，请使用此模式。在此模式中，您可以查看计算机的配置方式和层级结构中每台计算机的状态，还可以了解有哪些计算机部署了什么样的策略及其状态如何、实际部署的规则与应当在每台计算机部署的规则存在多大偏差。



eTrust Access Control

Host Report - Show All Nodes, Tree Format, No Filters

Index › Host Report - Show All Nodes, Tree Format, No Filters

Created by: john_doe (formatted into html by john_doe)
DMS: localhost
Creation Time: Wednesday, May 23 2006 on 10:00:00
Filters: -root "PMD1@mydomain.com"

Host Tree

Host Hierarchy PMD/Host Name	Status	Host Status Updated On	Updated By	Deviations Host Deviation Status	Policies Host Policy Status
PMD1@mydomain.com	Unknown			Unknown	None Available
PMD2@mydomain.com	PMD is Available	04/17/06 21:10:45	PMD1@mydomain.com	Unknown	None Available
host-157	Unknown	04/17/06 21:10:46	PMD4@mydomain.com	Unknown	policy-8 Undeployed john_doe 04/17/06 21:11:03
host-158	Unknown	04/17/06 21:10:46	PMD4@mydomain.com	Unknown	policy-1 Transfered john_doe 04/17/06 21:05:45 policy-2 Undeployed john_doe 04/17/06 21:11:03

Quick Help

Host Status :
- Available
- Unavailable
- Synchronizing
- Unknown

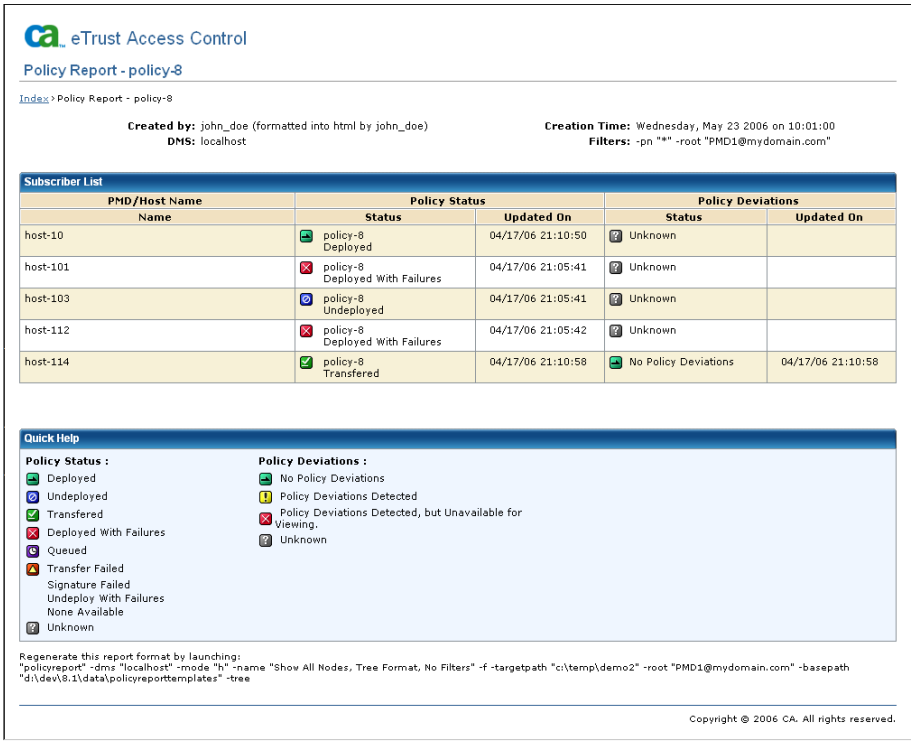
Policy Status :
- Deployed
- Undeployed
- Transfered
- Deployed With Failures
- Queued
- Transfer Failed
- Signature Failed
- Undeploy With Failures
- None Available
- Unknown

Policy Deviations :
- No Policy Deviations
- Policy Deviations Detected
- Policy Deviations Detected, but Unavailable for Viewing.
- Unknown

Regenerate this report format by launching:
"policyreport" -dmz "localhost" -mode "h" -name "Show All Nodes, Tree Format, No Filters" -f -targetpath "c:\temp\demo2" -root "PMD1@mydomain.com" -basepath "d:\dev\8.1\data\policyreporttemplates" -tree

- 策略模式

  策略报告提供以策略为主的信息。如果您要查看整个环境中一个或多个策略的状态，请使用此模式。



eTrust Access Control

Policy Report - policy-8

Index › Policy Report - policy-8

Created by: john_doe (formatted into html by john_doe)
DMS: localhost

Creation Time: Wednesday, May 23 2006 on 10:01:00
Filters: -pn "*" -root "PMD1@mydomain.com"

Subscriber List

PMD/Host Name	Policy Status		Policy Deviations	
Name	Status	Updated On	Status	Updated On
host-10	policy-8 Deployed	04/17/06 21:10:50	Unknown	
host-101	policy-8 Deployed With Failures	04/17/06 21:05:41	Unknown	
host-103	policy-8 Undeployed	04/17/06 21:05:41	Unknown	
host-112	policy-8 Deployed With Failures	04/17/06 21:05:42	Unknown	
host-114	policy-8 Transfered	04/17/06 21:10:58	No Policy Deviations	04/17/06 21:10:58

Quick Help

Policy Status :
Deployed
Undeployed
Transfered
Deployed With Failures
Queued
Transfer Failed
Signature Failed
Undeploy With Failures
None Available
Unknown

Policy Deviations :
No Policy Deviations
Policy Deviations Detected
Policy Deviations Detected, but Unavailable for viewing.
Unknown

Regenerate this report format by launching:
"policyreport" -dms "localhost" -mode "h" -name "Show All Nodes, Tree Format, No Filters" -f -targetpath "c:\temp\demo2" -root "PMD1@mydomain.com" -basepath "d:\dev\8.1\data\policyreporttemplates" -tree

除报告类型外，您还可以通过以下方式影响输出：

- 选择您要生成报告的层级结构部分。
- 生成单个计算机的报告。
- 按主机名、状态或状态更新时间进行筛选，也可以按策略名称或状态（支持通配符）进行筛选。
- 包含或排除偏差计算结果。
- 选择树形格式。
- 隐藏报告列。

创建主机报告

您可以通过主机报告查看计算机在层级结构中的配置方式、每台计算机在层级结构中的状态或计算机部署的策略以及这些策略的状态。

要创建主机报告，请在 h 模式下运行 policyreport 实用程序：

```
policyreport -name <name> -mode h -dms <dms_name> -root <pmd1>[,<pmd>] -tree \
-targetpath <path>
```

注意：您还可以利用附加的可选标志来调整报告。有关 policyreport 实用程序的详细信息，请参阅《参考指南》。

示例：为主机名与指定掩码匹配的计算机创建报告

下例说明如何使用 policyreport 实用程序来执行以下任务：

- 在以下目录中生成主机报告：

  C:\eac_data\reports\production_March2006

- 从 DMS 检索信息：

  mainDMS（在 **mainhost.domain.com** 计算机上）。

- 只包含在层级结构中处于下列 PMDB 之下的计算机：

  rootPMD@root.domain.com

- 只包含主机名称以下列字符开头的计算机：

  prod

```
policyreport -name production_March2006 -mode h \
-dms mainDMS@mainhost.domain.com -root rootPMD@root.domain.com -hn prod* \
-targetpath C:\eac_data\reports
```

policyreport 实用程序将报告存储在我们使用 (-name production_March2006) 选项指定的子目录中，而该子目录位于我们使用 -targetpath 选项 (C:\eac_data\reports) 指定的目录之下。即使在输出目录中已经存在一个报告，我们稍后也可以通过添加创建报告的 -f 选项来更新报告。

注意：如果您还指定了 **-tree** 标志，则报告将显示层级结构的图形说明。这包括报告中的所有父计算机，即使父计算机的主机名称与指定掩码不匹配也不受影响。

示例：为在某个日期范围内最后一次更改状态的计算机创建报告

下例说明如何使用 policyreport 实用程序来执行以下任务：

- 在以下目录中生成主机报告：

  C:\eac_data\reports\Feb06-Mar06

- 从 DMS 检索信息：

mainDMS（在 **mainhost.domain.com** 计算机上）。

- 只包含在层级结构中处于下列 PMDB 之下的计算机：

  rootPMD@root.domain.com

- 只包含主机状态最后一次更新日期在 2006 年 2 月的计算机。

```
policyreport -name Feb06-Mar06 -mode h \
-dms mainDMS@mainhost.domain.com -root rootPMD@root.domain.com \
-sd 01-02-2006 -ed 28-02-2006 -targetpath C:\eac_data\reports
```

示例：创建重新计算策略偏差结果并将结果存储在当前工作目录中的报告

下例说明如何使用 policyreport 实用程序来执行以下任务：

- 在以下目录中生成主机报告：

  <working_directory>**/hierarchy_20March06**

- 从 DMS 检索信息：

  mainDMS（在 **mainhost.domain.com** 计算机上）。

- 只包含在层级结构中处于下列 PMDB 之下的计算机：

  rootPMD@root.domain.com

- 包含偏差计算结果。
- 使用缩进以图形方式表示层级结构。

```
policyreport -name hierarchy_20March06 -mode h -dms mainDMS@mainhost.domain.com \
-root rootPMD@root.domain.com -targetpath -dev -tree
```

创建策略报告

您可以通过策略报告查看在哪些计算机上部署了什么策略。

要创建策略报告，请在 p 模式下运行 policyreport 实用程序：

```
policyreport -name <name> -mode p -dms <dms_name> -root <pmd1>[,<pmd>] \
-targetpath <path>
```

注意：您还可以利用附加的可选标志来调整报告。有关 policyreport 实用程序的详细信息，请参阅《参考指南》。

示例：为指定策略的所有版本创建报告

下例说明如何使用 policyreport 实用程序来执行以下任务：

- 在以下目录中生成策略报告：

  C:\eac_data\reports\iis5Policies_March2006

- 从以下 DMS 中检索信息：

  mainDMS（在 **mainhost.domain.com** 计算机上）。

- 只包含在层级结构中处于下列 PMDB 之下的计算机（订户）：

  rootPMD@root.domain.com

- 只包含以下策略的版本：

  iis5

```
policyreport -name prodPolicies_March2006 -mode p \
-dms mainDMS@mainhost.domain.com -root rootPMD@root.domain.com -pn iis5#* \
-targetpath C:\eac_data\reports
```

policyreport 实用程序将报告存储在我们使用 -name 选项 (iis5Policies_March2006) 指定的子目录中，而该子目录位于我们使用 -targetpath 选项 (C:\eac_data\reports) 指定的目录之下。即使在输出目录中已经存在一个报告，我们稍后也可以通过添加创建报告的 -f 选项来更新报告。

示例：为部署出错的策略创建报告

下例说明如何使用 policyreport 实用程序来执行以下任务：

- 在以下目录中生成策略报告：

  C:\eac_data\reports\policyErrors

- 从 DMS 检索信息：

  mainDMS（在 **mainhost.domain.com** 计算机上）。

- 只包含在层级结构中处于下列 PMDB 之下的计算机（订户）：

  rootPMD@root.domain.com

- 只包含部署出错（失败）的策略

```
policyreport -name policiesErrors -mode p \
-dms mainDMS@mainhost.domain.com -root rootPMD@root.domain.com \
-pstat "Failed" -targetpath C:\eac_data\reports
```

查看策略或主机报告

生成报告后，您需要导航到存储报告的文件夹，并在浏览器中打开报告进行查看。

查看策略或主机报告

1. 导航到存储报告的文件夹。

   它在以下路径中：<target_path>/<report_name>/html

   其中，<target_path> 是您使用 -targetpath 标志指定的目录，<report_name> 是您在生成报告时使用 -name 标志指定的报告名称。

2. 在浏览器中打开 **index.html** 文件进行查看。

   浏览器上显示报告的主页。

策略偏差计算器的工作原理

您可以利用高级策略管理和报告功能查看要在端点上部署的策略规则之间的差异，以及在该端点上实际应用的策略规则。您可以利用这些信息处理与策略部署关联的问题。

策略偏差计算在每个端点上运行，并执行以下任务：

1. 从本地主机中检索应当在端点上部署的规则的列表。

   它们是按本地 RULESET 对象中定义的方式为每个部署的策略指定的规则，而本地 RULESET 对象与每个部署的策略的 POLICY 对象关联。

2. 请检查是否已将每个策略应用于端点。

   重要！ 偏差计算不会检查是否应用了 Windows（本地）规则。它还忽略从数据库中删除对象（用户或对象属性、用户或资源授权，或者实际用户或资源）的规则。例如，计算无法验证是否应用了以下规则：
   rr FILE C:\tmp\tmp.txt

3. （可选）。将与本地 HNODE 对象关联的策略与第一个可用 DMS 上的策略进行比较。

   正常情况下，偏差计算器只检查本地主机上的偏差。如果您指定了 -strict 选项，则偏差计算器还将本地策略与列表中第一个可用 DMS 上的策略进行比较。它比较以下方面：

   a. 与代表本地主机的 HNODE 对象相关联的策略列表。

   b. 每个与 HNODE 对象关联的 POLICY 对象的策略状态。

   c. 每个与 HNODE 对象关联的 POLICY 对象的策略签名。

4. 输出以下两个文件：

   - <eTrustACDir>\data\devcalc\deviation.log

     记录在最后一次偏差计算过程收集到的错误消息。

   - <eTrustACDir>\data\devcalc\deviation.dat

     策略及其偏差的列表。

   注意： eTrust AC 还发送可以使用 **seaudit -a** 查看的审核事件。有关 seaudit 实用程序的详细信息，请参阅《参考指南》。

5. 把找到的任何偏差通知一个或多个 DMS。

   要通知的 DMS 可以手动指定（使用 -dms 选项），或者，如果没有指定 DMS，则偏差计算器使用为本地 eTrust AC 数据库指定的 DMS 列表。

为策略偏差计算配置端点

当您使用自定义安装来安装或升级 eTrust AC 时，如果您选择了“高级策略管理”选项，则安装过程配置策略偏差计算器。您还可以配置要计算的数据库并将偏差状态通知发送到指定的 DMS 数据库后续安装中。

为策略偏差计算配置端点

注意：如果您没有使用所选的“高级策略管理”选项来安装或升级此 eTrust AC 计算机，则才需要执行上述操作。有关 eTrust AC 安装的详细信息，请参阅《实施指南》。

1. 打开 selang 命令窗口。

   selang 命令窗口打开，允许您输入 selang 命令。

2. 输入下面的命令：

   ```
   nu ("+devcalc") admin auditor
   ```

   这将创建名称为 +devcalc 且具有 ADMIN 属性的新用户。eTrust AC 使用该用户来运行偏差计算器。

3. 输入下面的命令：

   ```
   nr SPECIALPGM ("<devcalc.exe_path>") seosuid("+devcalc") nativeuid("SYSTEM")
   ```

   其中，<devcalc.exe_path> 是 devcalc.exe 应用程序的完整路径，该程序驻留在 eTrust AC 安装目录的二进制目录中。

   这将为偏差计算器创建新的特殊程序资源，并指定授权运行该特殊程序的逻辑用户和本地 Windows 用户。

4. 输入下面的命令：

   ```
   so dms+(<DMS1>[,<DMS2>)
   ```

   其中 <DMSx> 是您希望偏差计算向其发送策略偏差状态通知的 DMS 的名称。必须按以下格式指定每个 DMS：DMS_name@hostname。

示例：配置一个端点以将策略偏差状态发送给中心 DMS

下例说明您需要在端点上运行的命令，该端点是为执行以下任务使用典型安装（和默认的安装目录）进行安装的：

- 配置能够执行偏差计算的端点。
- 将策略偏差状态发送到 DMS：

  prodDMS（在 **centralhost.com** 计算机上）。

```
nu ("+devcalc") admin auditor
nr SPECIALPGM ("C:\Program Files\eTrustAccessControl\bin\devcalc.exe") \
seosuid("+devcalc") nativeuid("SYSTEM")
so dms+(prodDMS@centralhost.com)
```

策略偏差日志和错误文件

在每次偏差计算过程中，策略偏差计算都会编写新的日志。该日志还包含错误消息，存储在 <eTrustACDir>\data\devcalc\deviation.log 中。

如果您在报告中看到的偏差结果（从 DMS 检索得到）不是从最后一次运行偏差计算得到的，请使用该日志。它可以帮助您诊断为什么偏差计算结果没有发送到 DMS 的原因。

重要！如果偏差日志包含错误消息“ERROR：初始化 DB 库失败，数据库已打开”，那么您需要重新创建数据库的索引文件。为此，请退出 selang 并从 <eTrustACDir>\data\devcalc\init_ac_db 目录运行以下命令，然后重新运行偏差计算 (p. 105)：
selang -l -d .

示例：偏差日志和错误文件

下面是一个偏差日志和错误文件示例：

```
start time: Mon Jan 23 13:04:48 2006
WARNING, \"检索 DMS 主机名失败，将在本地存储偏差\"
found deviation(s) for policy 'iis8#02'
end time: Mon Jan 23 13:05:04 2006
```

策略偏差数据文件

策略偏差计算编写一个包含策略及其偏差的列表的数据文件。该数据文件存储在 <eTrustACDir>\data\devcalc\deviation.dat 中。

注意：该数据文件包含的策略列表与用于计算偏差的策略有关（默认情况下，所有策略和所有策略版本都在端点上）。

重要！偏差计算不会检查是否应用了 Windows（本地）规则。它还忽略从数据库中删除对象（用户或对象属性、用户或资源授权，或者实际用户或资源）的规则。例如，计算无法验证是否应用了以下规则：
rr FILE C:\tmp\tmp.txt

偏差状态发送到 DMS（无论是否存在偏差），但实际偏差在本地存储。创建报告时，可以从此文件中检索实际偏差结果，并将其添加到报告中。

在策略偏差数据文件中包含以下行：

Date

偏差计算的日期

格式： DATE, DDD MMM DD hh:mm:ss YYYY

Strict

指定用 -strict 选项运行偏差计算。

格式： STRICT, DMS@hostname, policy_name#xx, {1|0}

其中，{1|0} 表示是否在与本地 HNODE 对象关联的策略以及与 DMS@hostname（第一个可用 DMS）上的 HNODE 对象关联的策略之间找到偏差，(1) 表示找到，(0) 表示没有找到。

Policy Start

启动定义该策略的偏差的策略块。

格式： POLICYSTART, policy_name#xx

Difference

说明为策略找到的偏差。与偏差对应的策略的名称出现在此行上面的最近的**策略行**中。

下表说明四种类型的偏差：

偏差类型	格式
未找到类	DIFF, (<class_name>), (*), (*), (*)
未找到对象	DIFF, (<class_name>), (<object_name>), (*), (*)

偏差类型	格式
属性未找到	DIFF, (<class_name>), (<object_name>), (<property_name>), (*)
属性值不匹配	DIFF, (<class_name>), (<object_name>), (<property_name>), (<expected_value>)

Policy End

结束定义该策略的偏差的策略块。

格式： POLICYEND, policy_name#xx, {1|0}

其中，{1|0} 表示是否找到偏差，(1) 表示找到，(0) 表示没有找到。

Warning

说明警告。

格式： WARNING, "warning_text"

示例：偏差数据文件

```
Date, Sun Mar 19 08:30:00 2006
WARNING, "检索 DMS 主机名失败，将在本地存储偏差"
POLICYSTART, iis8#02
DIFF, (USER), (am), (*), (*)
POLICYEND, iis8#02, 1
```

执行偏差计算

应当定期执行偏差计算，以使 DMS 包含关于策略偏差状态的最新信息。我们建议您安排按符合您的报告要求的时间间隔执行策略偏差计算。

要在端点执行偏差计算，请在 selang 窗口中输入以下命令：

```
start DEVCALC
```

示例：安排日常偏差计算

下例说明如何在 Solaris 上创建按下列要求执行的偏差计算任务：

- 每天午夜运行。
- 向 DMS 发送偏差状态：

  mainDMS（在 **mainhost.domain.com** 计算机上）。

为此，请执行以下步骤：

1. 用以下行创建批处理文件：

   ```
   selang -c "start DEVCALC params('-dms mainDMS@mainhost.domain.com')"
   ```

2. 添加执行以下选项的计划任务：
   - 浏览并选择新批处理文件。
   - 每天执行此任务。
   - 开始时间：12:00 AM

将 PMDB 与 Unicenter 集成

将 PMDB 与 Unicenter TNG 集成使您可以使用 PMDB 来创建规则，以防止 Unicenter TNG 对象被各种 Unicenter TNG 组件操纵（例如，命令处理器、事件管理和工作量管理）。

您必须手动执行集成。

将 PMDB 与 Unicenter TNG 集成

1. 创建 PMDB。
2. 使用以下命令，将 Unicenter Security 选项迁移到 PMDB 中：

   ```
   MigOpts pmdb-name
   ```

   其中 pmdb-name 是 PMDB 的名称。

   注意:只要您使用了 Unicenter Security，并在安装 eTrust AC 期间选择了“在 Unicenter Integration 下的安全数据迁移”选项，则该步骤就是必需的。如果您没有使用 Unicenter Security，而且从未建立任何安全选项，则没有内容要迁移到您的 PMDB 中。
3. 使用以下命令，为用户-定义的任何 Unicenter TNG 资产类型定义类：

   ```
   defclass.bat.pmdb-name
   ```

   其中 pmdb-name 是 PMDB 的名称。

   注意：只要您使用了 Unicenter Security，并创建了用户-定义的资产类型，则该步骤是必需的。如果您在 eTrust AC 安装期间选择了 Unicenter 集成，则在每个新的 PMDB 中自动定义 Unicenter TNG 资产类型。

第 7 章： 使用事务管理器

此部分包含以下主题：

事务管理器

事务管理器是管理 eTrust AC、UNIX 和 Windows 安全的工具。它自动将在本地主机上执行的 eTrust AC 事务发送到多个主机上。该事务模式旨在快速有效地替代或者附属于策略模型。它并不对将修改传播到每个订户的安全数据库提供相同的保证，但却更易于使用，而且，在想要更改没有定义为策略模型层级结构一部分的多个数据库时尤其有用。

设置事务管理器

在使用事务管理器之前，请执行以下操作：

1. 请确保您在每台访问的远程主机及本地主机上都有 ADMIN 权限。

   在访问的每台主机上为管理计算机创建一个 TERMINAL 记录。

   以上要求与管理远程主机的要求相同。

   启用事务管理器。从策略管理器中，选择"工具"、"选项"，并打开"事务管理器"选项卡。选中"启用多主机事务"。还可以选择您想要激活的"事务管理器"选项。

2. 创建"目标主机"文件。

多主机事务选项

除了"安全策略"和"审核"以外，可以在从程序栏打开的任何窗口中使用事务管理器。默认情况下选中"用户"、"组"和"资源"。

"事务管理器"选项允许您自定义事务模式操作的方式。选项如下：

常规选项

在第一次出错时停止发送数据

默认操作是即使发生错误也继续发送事务，使您可以尽可能多地传播事务，并在稍后处理错误。不过，通过在第一次发生错误时便终止传播可以节约您的时间，例如，您正在向许多主机发送事务，而您预计在某一台主机上发生的错误会在其他主机上发生。

退出时关闭事务管理器

选中该复选框会导致事务管理器与策略管理器同时退出，而不管它是否已完成队列事务的发送。该选项的默认值是关闭策略管理器时继续运行事务管理器。

注意：事务管理器的内存不稳定；当事务管理器退出时，其事务日志将丢失。

启动时激活事务模式

在启动策略管理器时始终启动事务管理器。但在默认情况下，单击工具栏上的事务模式按钮后才能处于事务模式。选中该复选框可以在启动策略管理器时自动进入事务模式。

目标主机文件

您可以使用该选项为目标主机文件设置目录路径。默认路径为 eTrustACDir\data\hosts.txt（其中，eTrustACDir 是安装 eTrust AC 的目录）。

刷新的时间间隔（秒）...

该选项控制 TM 状态窗口监视事务管理器的紧密程度。默认值为 10 秒，如果事务较短，则可能不会显示任何进程。

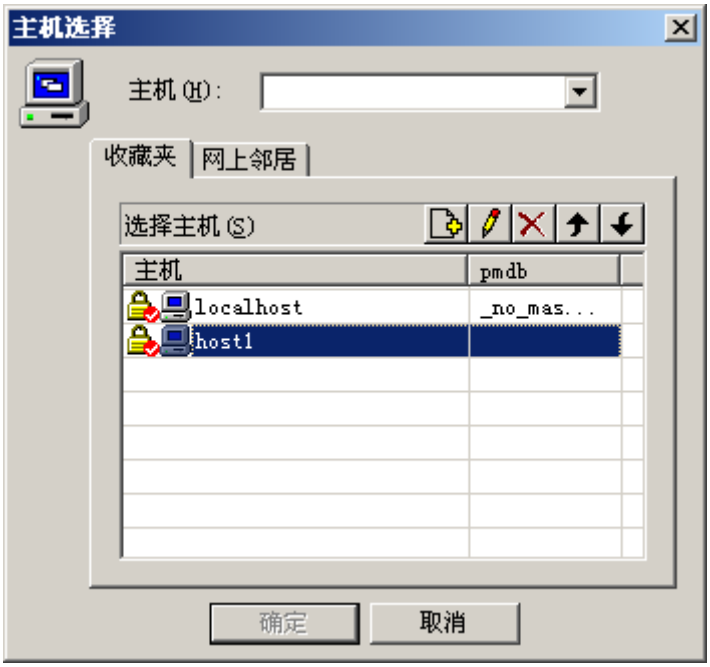
命令和脚本

通常情况下，事务模式与策略管理器事务一起使用。您还可以用它来将 selang 命令或脚本发送到多台主机。选中这些复选框，可以同时使用事务模式与"命令和脚本"对话框（"工具"、"执行命令"）向多台主机发送 selang 命令。

设置目标主机文件

目标主机文件控制在事务模式下工作时接收事务的主机或主机组。

添加"收藏夹"列表或"网上邻居"中的主机。



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。这些选择会在单击"确定"后立即生效，并一直到被更改后为止。每次要向不同的主机组发送事务时，您必须手动重置目标主机文件。

注意：启用"事务模式"后，"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。

在事务模式下工作

在启用了事务管理器并创建了目标主机文件后，请单击工具栏上的"事务模式"图标。在本地数据库上执行的任何事务也会传播到选定主机。例如，当通过选择"用户"窗口中的某个名称，并单击工具栏上的"删除"删除用户时，该事务立即在本地主机数据库中发生（和往常一样），然后自动传播到目标主机文件中的主机。

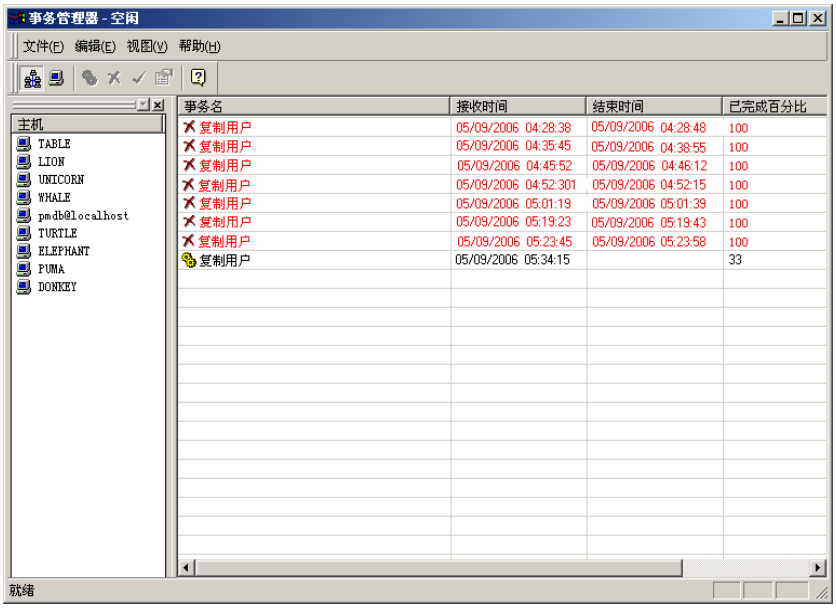
您可以借助"任务管理器状态"窗口来跟踪传播的进度。要挂起长事务，请右键单击任务栏中的"事务管理器"图标，然后选择"挂起事务管理器"。如果选择"恢复事务管理器"，则会继续传播。关闭事务管理器窗口，甚至单击右上角的关闭按钮都不会终止应用程序。要退出事务管理器，请在任务栏中右键单击该图标，然后选择"退出"。请切记，如果执行该操作，将会清除日志中的所有事务。

事务管理器窗口

双击 Windows 任务栏中的事务管理器图标可以激活事务管理器窗口。该窗口包含传播到多台主机的所有事务的日志。任务管理器的内存不稳定，因此仅显示当前会话中的事务。您可以从"视图"菜单，或者通过单击工具栏上的某个主机图标来选择"主机状态"或"主机栏"视图。请注意，这两个图标是等效的；单击任一个图标都会切换视图。工具栏上的按钮选择视图，使您可以再次运行事务，删除或取消删除事务，或者显示其属性。当删除队列中的事务时，事务管理器将忽略该事务，并跳至队列中的下一个事务。您可以随时取消删除事务以继续传播该事务。不能删除当前事务。

主机状态栏视图

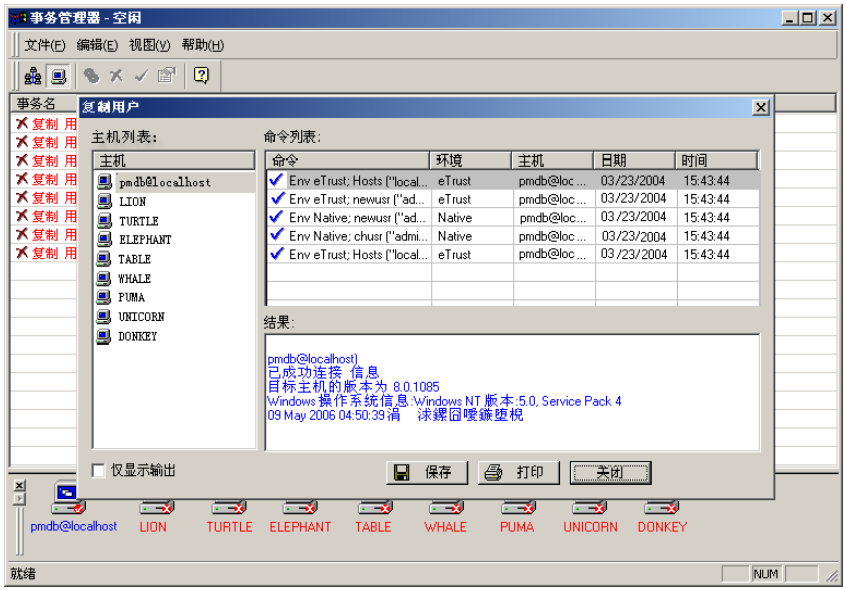
在"主机状态栏"视图中，每台选定主机的图标都显示在窗口左侧的状态栏中。单击图标可将事务列表关联到该主机。双击事务将显示一个包含"命令列表"文本框和"结果"文本框的"更新"对话框。选择"命令列表"文本框中的命令会在"结果"文本框中显示该命令的结果。您可以选择打印该结果或者将其保存到某个文件。



主机栏视图

在"主机栏"视图中，事务行将占用窗口的整个宽度，而选定主机的图标显示在底部。双击事务将打开一个包含"主机"列表栏、"命令列表"文本框和"结果"文本框的"更新"对话框。当选择某个主机图标时，"命令列表"与该主机关联。当选择某个命令时，"结果"与该命令关联。

或者，您可以选择一个事务，然后双击窗口底部的主机图标。将显示"更新"对话框。



第 8 章： 监视和审核

此部分包含以下主题：

安全审核者

安全审核者和系统管理员的最重要的任务之一就是审核或监视系统活动，从而发现可疑或恶意的活动。安全审核在安全环境中是一项必不可少的任务，eTrust AC 中的安全审核功能包括以下几个方面：

- 确切指出访问过系统的用户、已被访问的资源及访问的时间
- 在有人尝试进行安全破坏活动（即使尝试失败）时，通知相关的用户并发出警报
- 指明对安全规则做出的更改及更改者
- 提供在执行访问规则之前测试该规则效果的方式

eTrust AC 审核模仿真实审核：安全审核者的操作独立于系统和安全管理员，但如果某种其他模型更适合于您的环境，则可以更改实施方式，以便进行相应的更改。

安全审核者就是为其分配了 AUDITOR 属性的用户。定义为安全审核者的用户可以执行审核任务，例如，更改为用户和资源分配的审核规则。此外，他们还授权使用 eTrust AC 审核实用程序，而无须拥有 ADMIN 属性。

监视访问控制活动

eTrust AC 跟踪是实时日志，可以显示 eTrust AC 执行的每项操作。跟踪记录汇集在 eTrustACDir\log\seosd.trace（其中 eTrustACDir 是 eTrust AC 的安装目录）中。

或者汇集在指定为注册表子键中的 trace_file 值的任何文件中：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrustAccessControl\SeOSD\
```

尽管您可以从跟踪文件中筛选记录，但是跟踪机制是为系统监视而设计的，而不是为安全审核而设计的。

默认情况下，eTrust AC 仅在初始化 eTrust AC 期间生成跟踪消息。eTrust AC 完成初始化之后，它将停止跟踪机制，而且不会生成跟踪消息。

筛选跟踪记录

使用跟踪筛选文件，可以指定不应在跟踪文件中显示的某些活动类型。跟踪筛选文件是使用注册表键中的 trace_filter 值指定的：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrustAccessControl\SeOSD
```

默认值为 eTrustACDir\log\trcfilter.ini（其中 eTrustACDir 是 eTrust AC 的安装目录）。

重要！eTrust AC 将在安装时创建跟踪筛选文件，该文件中只有一行：*seosd.trace*。请勿删除该记录。

跟踪筛选文件中的每一行都表示一种不应跟踪的访问或活动。例如，要消除对用户访问 Microsoft Word 的跟踪，请在跟踪筛选文件中添加以下行：

```
*winword.exe*
```

筛选审核记录

您可以使用 audit.cfg 文件（在 eTrustACDir\data 中）通过定义不应生成的审核记录来筛选主机上的审核记录。每一行都代表一条用于筛选审核信息的规则（即，与行中条件匹配的审核记录将不出现在审核文件中）。该筛选器可以只保留需要的记录，从而有助于限制 seos.audit 文件的大小。您可以为类名、对象名、用户名、组名、程序名、访问权限和授权结果设置筛选规则。eTrust AC 引擎 (seosd) 在启动时读取此文件。

语法

```
<class>;登录信息;<user>;<program-path>;<access-mode>;<auth-result>
```

注意：任何列中 * 是表示任意值的通配符。

当向审核文件发送消息时，seosd 会检查该消息是否与 audit.cfg 文件中的下列项之一匹配：

字段	Rule
类	应该以大写形式写入的类名
对象	可以使用模式 (*) 写入的资源名称
用户	可以使用模式 (*) 写入的用户名
程序路径	可以使用模式 (*) 写入的正在使用的程序
访问模式	访问权限必须符合规则
授权结果	授权结果必须是 P（允许）或 D（拒绝） **注意：**值"P"还会筛选针对警告模式中的资源生成的审核记录。

TCP 类的语法

```
<class>;登录信息;<host>;<program-path>;<access-mode>;<auth-result>
```

示例：审核访问筛选器

在以下示例中，如果 Administrator 成功读取文件，seosd 将不会向审核文件发送消息。如果 Administrator 无法读取该文件，则 seosd 会向审核文件发送一条消息。

```
FILE;*;Administrator;*;R;P
```

设置审核规则

对于安全审核，eTrust AC 将根据在数据库中定义的审核规则，保留拒绝访问事件或授权访问事件的审核记录。

每个访问者和每种资源都具有 AUDIT 属性，可以设置为以下一个或多个值：

FAIL

记录访问者对资源的访问失败。

SUCCESS

记录访问者对资源的成功访问。

LOGINFAIL

记录访问者的每一次登录失败。（该值不适用于资源。）

LOGINSUCCESS

记录访问者的每一次成功登录。（该值不适用于资源。）

ALL

记录与访问者的 FAIL、SUCCESS、LOGINFAIL 和 LOGINSUCCESS 或资源的 FAIL 和 SUCCESS 相同的信息。

NONE

不记录任何有关访问者或资源的信息。

无论您何时在数据库中创建或更新访问者或资源记录，都可以指定 AUDIT 属性。此外，您还可以指定是否应该发送以及向何人发送记录事件的电子邮件通知。（您可以按照"使用管理员界面"一章中的说明使用策略管理器，或按照《参考指南》的"selang 命令语言"一章中的说明使用 selang 命令来创建和更新数据库中的记录。）

审核日志中的记录将根据这些审核规则进行汇集。是否记录某个事件的决策基于以下情况：

- 如果资源或访问者拥有 AUDIT(ALL)，则将记录访问者的所有登录事件以及与受 eTrust AC 保护的资源有关的所有事件，无论访问失败还是成功。
- 如果对 eTrust AC 所保护的资源的访问成功，且访问者或资源具有 AUDIT(SUCCESS)，则记录该事件。
- 如果访问受 eTrust AC 保护的资源失败，并且访问者或资源拥有 AUDIT(FAIL)，则将记录该事件。

在 Windows 中设置审核策略

除了设置访问者和资源的访问规则以外，您还可以指定要写入审核日志中的 Windows 事件。您可以为整个组织或逐个为用户指定此类审核策略。

审核日志

由审核规则和审核策略中定义的事件或访问创建的审核记录，构成了名为"审核日志"的文件。以下 Windows 注册表子键中的值 audit_log 指定了审核日志的位置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrustAccessControl\logmgr
```

该键的默认值为：

```
*\Program Files\CA\eTrustAccessControl\log\seos.audit
```

默认情况下，eTrust AC 在达到 1024 KB 时，会重命名该审核日志文件，并新建一个审核日志文件，从而自动对其进行备份。您可以通过更改该子键中的值 audit_size 来更改触发备份的审核日志大小：

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\logmgr
```

您还可以选择通过更改 Windows 注册表子键中的值 BackUp_Date 来定期（每天、每周或每月）备份审核日志：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrustAccessControl\logmgr
```

注意：有关这些注册表子键的详细信息，请参阅《参考指南》。

您应该考虑将旧的审核日志存档在磁带中，以便以后对事件进行扫描。

使用审核日志

eTrust AC 提供两种嵌入式工具，用于查看、筛选和搜索审核日志：

- 策略管理器
- seaudit 实用程序

您可以显示审核日志中的每条记录，也可以使用筛选器从审核日志中选择特定记录。

本章的其余部分介绍在使用策略管理器中的审核筛选器时，如何查看审核日志中的记录。

审核筛选器

审核日志中的记录数目可能会非常庞大。要减少 eTrust AC 显示的记录数目，请使用筛选器选择要显示的某些类型的记录。您可以依据各种条件（包括时间或事件类型）来筛选事件。

通过指定名称并至少选择一个必选项，可以在策略管理器中创建筛选器。您可以选择其他开关参数，并同时选择零个、一个或多个选项。还可以使用 seaudit 工具来筛选记录。

策略管理器提供了几个预定义的筛选器，并且您可以创建自己的筛选器。

默认情况下，eTrust AC 会将所有的审核筛选器都存储到 eTrustACDir\data\AuditFilters.flt（其中 eTrustACDir 是 eTrust AC 的安装目录）中。

您可以选择将创建的筛选器保存到该文件中，也可以将筛选器保存到其他文件中。

开关参数

INet host service

列出从指定服务的指定主机接收的 TCP 请求的 INET 审核记录。主机 (host) 和服务 (service) 是标识搜索的主机和服务集的掩码。

LOGON user terminal

显示以下内容：

- 指定用户在指定终端上的 LOGIN 记录。user 和 terminal 都是掩码。
- 多次输入无效密码时由授权引擎创建的记录。

Resource class resource user

列出资源记录。可以指定以下内容：

- Class - 标识被访问资源所属类的掩码。
- Resource - 标识被访问资源的名称的掩码。
- User - 标识访问资源的用户名的掩码。

Start

列出来自 eTrust AC 服务的启动和关闭消息。

Update (cmd, class, object, user)

显示数据库更新审核记录。可以指定以下内容：

- Cmd - 标识要搜索的 selang 命令集的掩码。
- Class - 标识要搜索的类的掩码。
- Object - 标识要搜索的记录的掩码。
- User - 标识已执行这些命令的用户的掩码。

Watchdog

列出监视程序审核记录。

All

列出除通过跟踪工具发送至审核日志的记录以外的所有记录。

选项

结束日期

指定结束日期。不列出该指定日期之后的记录。

结束时间

指定结束时间。不列出该指定时间之后的记录。

无错误

指定不列出故障。

无授权

指定不列出成功（授权）访问。

无注销

指定不列出注销记录。

Internet 地址

指定列出 Internet 地址，而不是 TCP/IP 记录中的主机名。

无通知

指定不列出 NOTIFY 审核记录。

无密码

指定不列出密码尝试记录。

来源主机

指定仅列出来源于指定主机的记录。该选项仅在连接至 UNIX 工作站时适用。

开始日期

指定开始日期。不列出该指定日期之前的记录。

开始时间

指定开始时间。不列出该指定时间之前的记录。

显示端口号

指定列出端口号，而不是服务名。

无警告

指定不列出警告记录。

预定义筛选器

eTrust AC 附带了下列预定义筛选器：

所有

显示审核日志中的每条记录。不执行任何筛选。

今日

显示今天创建的每条记录。

最后两天的记录

显示昨天和今天创建的每条记录。

最后七天的记录

显示过去七天期间创建的记录。

访问控制服务的连接

显示指明用户何时连接至 eTrust AC 服务（例如策略管理器或 selang）的记录。

注意：连接至 UNIX 工作站时，该筛选器的名称将变成为"登录记录"。该记录表示用户登录。

管理活动

显示更新 eTrust AC 或操作系统数据库的所有记录。数据库更新包括添加、删除和更改所有类型的记录。

用户定义的筛选器

您可以根据需要创建任意数目的筛选器。您应该选择重要的字段并命名筛选器。eTrust AC 会自动保存筛选器，以便您可以在调用策略管理器时随时重用该筛选器。

警告模式

随着您逐步采用安全策略，您可能会发现检查某些资源访问限制的行为非常有用，而无须实际执行限制。这种做法在以下情况下特别有用：

- 确定要设置的规则是否太严格或太宽松，以便相应地修改安全策略
- 您怀疑某些限制可能会对系统应用程序的执行产生不利影响时

eTrust AC 可以指定限制并替换用于执行限制的警告消息。

实施警告模式

要实施警告模式，请完成以下步骤：

- 在受要测试的规则影响的所有资源记录中设置 WARNING 参数。
- 在策略管理器中，在创建或修改资源时选择"审核"，并选中"警告"框。
- 在 selang 中，将 warning 参数与 newres、editres 或 chres 命令一起使用。

  注意：有关详细信息，请参阅《参考指南》中的 chres/editres/newres 命令。

当为资源打开警告模式，但未授权访问者以所请求的方式访问资源时，eTrust AC 会发出警告消息、记录访问（由于警告模式已生效，因此允许声明该违规）并允许访问资源。

注意：

- 注意：在警告模式中，eTrust AC 不为资源组创建警告消息。
- 如果您在实施 eTrust AC 期间使用警告模式，请确保有足够的磁盘空间来存储审核日志，并确保审核日志的大小限制足够大。

第 9 章： Unicenter 迁移和集成

此部分包含以下主题：

安装 Unicenter Integration 工具

<eTrust AC 完全集成到 Unicenter 企业管理环境中。以下各节介绍 eTrust AC 如何处理集成。

重要！要将 Unicenter TNG 与 eTrust AC 集成，必须将 Unicenter TNG 与 eTrust AC 安装在同一台计算机上。

注意：有关 Windows 环境的完整安装说明，请参阅《实施指南》。

Unicenter Integration 功能

下面几节将说明 eTrust AC 如何与 Unicenter TNG 集成。

SSF/EMSec API 支持

Windows 通道的 EMSec API 可以调入单个 DLL。EMSec 对 Unicenter Integration 的支持包括替换 CAUSECR.DLL。该 DLL 将接收对 EMSec API 的调用，然后重新格式化这些请求，并将它们重定向到等效的 eTrust AC API。从 eTrust AC API 返回的代码会被转换回对应的 EMSec API 返回代码，并且将控制权返回 EMSec API 的调用者。这种方法可以保护当前正在使用 EMSec API 的应用程序的完整性。

Unicenter Integration 设置过程完成后，便会激活 EMSec 支持。Unicenter Integration 设置将替换 Unicenter 安装路径（CAIGLBL0000 目录）中的当前 CAUSECR.DLL。此时，替换 CAUSER.DLL 会截获传入的 EMSec API 请求，并且将通过 eTrust AC API 无缝检索请求的信息。

Unicenter Security 数据迁移功能

下面几节将说明如何将 Unicenter Security 数据迁移到 eTrust AC。

Unicenter Security 选项迁移

eTrust AC 程序 MigOpts.exe 将提取选定的 Unicenter Security 选项，并根据这些选项自定义目标 eTrust AC 数据库。要激活该功能，必须运行 Unicenter Integration 和 Unicenter Security 数据迁移设置过程。该设置过程会自动运行 MigOpts.exe。

注意：下列 Unicenter Security 选项可以被**完全**迁移到 eTrust AC 环境中。

- AUDIT_LOGIN
- MODIFY_PWDNEVEREXP
- PWDQUEUESIZE
- SEC_AUDIT_DBUPDATE
- SEC_AUDIT_SEND
- SEC_PASSWORD_ALPHA
- SSF_MAXPWDVIO
- SSF_MINPWDLEN
- SSF_SECPWEXCL
- USER_DEFSESID
- USER_PWDCHANGE
- USER_PWDCHGMAXDAYS
- USER_PWDCHGMINDAYS
- USER_PWDMAINT

注意：USER_PWDMAINT 将迁移到特定于现有 Unicenter Security 数据的 eTrust AC 环境中。eTrust AC 会维护密码信息，但此过程不会自动完成。将现有的 Unicenter TNG 用户从 Unicenter Security 中导出到 eTrust AC 数据库时，如果 USER_PWDMAINT 选项的值为"yes"，则将自动执行该手动过程。但是迁移完成后，如果必须跟踪管理员添加的新用户的密码信息，则该管理员必须同时确保"__workload__"应用程序对象存在。例如：

```
eTrust> na __workload__;
```

然后，管理员必须更新用户的登录信息，以包括"__workload__"应用程序对象。例如：

```
eTrust> el (Username) appl('__workload__');
```

此外，ExportTngDb.exe 在将作为 **SSF_AUTH** Unicenter Security 选项成员的 Unicenter TNG 用户添加到 eTrust AC 之前，将通过设置这些用户的 Admin 属性将它们迁移到 eTrust AC 环境中。

Unicenter Security 数据库迁移

eTrust AC 调用的 ExportTngDb.exe 从 Unicenter Security 数据库提取数据，并将其转换成 eTrust AC 命令以装载 eTrust AC 数据库。ExportTngDb.exe 将迁移以下各项：

- Unicenter Security 用户
- Unicenter Security 用户组
- Unicenter Security 规则

注意：

- 建议在运行 Unicenter Integration and Migration Installation 进程之后不要运行 Unicenter TNG 登录截获。成功执行 Unicenter Integration and Migration Integration 过程后，应验证是否已禁用 Unicenter TNG 登录截获。
- eTrust AC 迁移进程不支持 Unicenter TNG 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。

要激活 ExportTngDb.exe，必须运行 Unicenter Integration 和 Unicenter Security 数据迁移设置过程。该设置过程将自动执行 Unicenter Security 数据迁移过程。

注意：在迁移进程中，所有 Unicenter TNG 对象的创建和修改统计信息都会丢失。

由于 Unicenter TNG 和 eTrust AC 产品的差异，无法将 Unicenter Security **用户**的下列属性迁移到 eTrust AC：

统计信息

eTrust AC 不支持下列用户统计信息：

- 上次登录统计信息（日期和时间以及上次登录的节点）
- 密码更改统计信息（日期和时间、节点、更改上一个密码的用户以及密码的过期日期）
- 密码违规统计信息（日期和时间、上次失败登录的节点以及自上次成功登录后失败登录的次数）
- 访问违规统计信息（日期和时间、上次访问违规的节点以及访问违规的次数）
- 挂起统计信息（挂起的日期和时间）

PWDCHANGE VALUE (RANDOM)

随机密码生成

UPSSTATGROUP

UPS 工作站组

- eTrust AC 不受支持

USERORIGIN

用户来源（NIS 或本地）

VIOLMODE

违规模式（FAIL、MONITOR、WARN、QUIET）

- eTrust AC 仅支持 FAIL 模型。

VIOLACTION

违规操作 (CANUSER, CANU&LOG, CANU&LOG&SUS)

- eTrust AC 仅支持 CANUSER 操作。

由于 Unicenter TNG 和 eTrust AC 产品的差异，无法将 Unicenter Security **规则**的下列属性迁移到 eTrust AC：

EXPIRES

eTrust AC 不支持规则截止日期。

Unicenter 用户出口支持

要帮助迁移，可以通过 eTrust AC 来运行在 eTrust AC 环境中未更改的当前 Unicenter Security 用户出口。您不必将所有的用户出口都作为迁移的一部分重新写入。

在 Unicenter Security 和 eTrust AC 中仅使用现有用户出口，安装的每个组件被注册为标准 eTrust AC 用户出口，然后会生成对应的 Unicenter Security 出口。

要启动该功能，请运行 Unicenter Integration 和 Unicenter Security 数据迁移设置过程。设置过程完成后，将立即激活该功能。

注意：因为 Unicenter TNG 和 eTrust AC 使用不同体系结构，所以仅支持 Unicenter Security 和 eTrust AC 之间兼容的出口点和数据项。支持下列 Unicenter Security 出口点：

EmSec_CredExit()

向 Unicenter 凭据验证出口 EmSec_CredExit() 输入的内容由 EMSECSIGNON 映射。使用 eTrust AC，只有该结构中的用户和节点成员包含有意义的数据。用户成员设置为要进行身份验证的用户名，而节点成员设置为当前的本地节点名。EMSECSIGNON 结构的所有其他成员均设置为二进制零。将忽略其他参数、详细的返回代码和从 Unicenter 资源检查出口传递回的消息。

EmSec_PwExitNew()

向 Unicenter 密码验证出口 EmSec_PwExitNew 输入的内容包含用户（要更改其密码的用户）、密码（新的密码）和节点名（在 eTrust AC 支持下，这始终为本地节点名）。如果该出口失败，则将使用旧的出口 EmSec_PwExit。它仅包含作为输入内容的用户名和密码，并且在 eTrust AC 下受到完全支持。

EmSecSSFResCheck()

向资源检查出口 EmSecSSFResCheck() 输入的内容由 EMSECRESCHECK 映射。EMSECRESCHECK 中的用户成员将设置为访问用户的值。EMSECRESCHECK 中的类成员将设置为访问的资源类的值。EMSECRESCHECK 中的实体成员将设置为对象名的值。eTrust AC 访问信息将转换为 Unicenter 样式的访问权限，并且将被置于 EMSECRESCHECK 的属性成员中。EMSECRESCHECK 的所有其他成员将设置为二进制零。将忽略其他参数、详细的返回代码和从 Unicenter 资源检查出口传递回的消息。Unicenter Integration 设置完成后，将立即激活该功能。

Unicenter 日历

使用 UnicenterTNG 提供的日历工具，可以设置用户、组和资源的时间限制。日历包含 15 分钟的时间间隔，您可以将其设置为 ON 或 OFF。如果将日历时间间隔设置为 OFF，就会阻止资源访问；如果将日历时间间隔设置为 ON，便可以对资源进行访问。

在 Windows 中，管理员只能在启动安全机制之前设置日历用法。

注意：必须将 Unicenter TNG 安装在本地计算机上。eTrust AC 使用本地 Unicenter TNG 服务检索日历设置。

1. 停止 eTrust AC 安全保护。输入：

   ```
   secons -s
   ```

2. 在 Windows 注册表中，转至以下子键：

   ```
   HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\UCTNG
   ```

   在该子键中，将 TNG_calendars 值设置为"yes"。将 TNG_refresh_interval 值设置为相应的时间值（以分钟计）。

3. 启动 eTrust AC 安全保护。输入：

   ```
   seosd -start
   ```

要将 eTrust AC 资源与日历链接在一起，必须在提示符处执行以下数据库命令：

```
eTrust> nr CALENDAR calendar_name
eTrust> nr file C:\myfile.txt calendar (calendar_name) defaccess (a)
```

Unicenter TNG 日历访问控制列表 (ACL) 是附加的安全约束功能。常规的 Unicenter TNG 日历属性可以根据相应的 Unicenter TNG 日历状态限制当前资源。Unicenter TNG 日历 ACL 属性可以根据 Unicenter TNG 日历状态限制特定用户和组对当前资源的访问权限（或为其授予访问权限）。

ACL Unicenter TNG 日历的两类属性为常规属性和限制性属性。

- 常规日历 ACL 属性允许用户或组根据 ACL 访问权限访问资源。
- 限制性（被拒绝的）日历 ACL 属性拒绝用户或组根据 ACL 访问权限访问资源。

要将用户或组添加到常规日历 ACL (CALACL) 中，请在 selang 中输入下列命令：

```
eTrust> auth resource_class_name object_name uid_or_gid_name calendar(calendar name)
access(access_value)
```

例如：

```
eTrust> auth file file1 uid(george) calendar(basecalendar) access(r w)
```

要将用户或组添加到拒绝日历 ACL 中，请在 selang 中输入以下命令：

```
eTrust> auth resource_class_name object_name uid_or_gid_name
calendar(TNG_calendar_name) deniedaccess(access_value)
```

例如：

```
eTrust> auth file file2 uid(george) calendar(holidays) access(r w)
```

您可以为同一资源（例如日历和 uid）同时使用常规和限制性属性。以下命令将拥有读取权限的用户 George 添加到 file1 的被拒绝的日历 ACL 中。

```
eTrust> auth file file1 uid(george) calendar(holidays) deniedaccess(r)
```

要从 Unicenter TNG 日历 ACL 属性中删除用户或组，请使用-：

```
eTrust> auth- file file2 uid(george) calendar(holidays)
```

使用 Show Resource (sr) 命令查看分配给特定资源的所有 Unicenter TNG 日历 ACL：

```
eTrust> sr file file1
```

Unicenter 认证

- 下列功能遵循 Unicenter TNG 2.2 SP1、Unicenter TNG 2.4 或 Unicenter NSM 3.0：
  - 发送"事件"
  - 同步大型机密码
  - 使用 Unicenter TNG 日历

附录 A: 将密码与大型机同步

This section contains the following topics:

密码同步支持

eTrust AC 支持在运行 eTrust CA-Top Secret Security、eTrust CA-ACF2 Security 或 RACF 安全产品的大型机与运行 eTrust AC 的 Windows 或 UNIX 计算机中执行密码同步。同步是使用标准的 eTrust AC 密码策略模型方法完成的。

密码策略模型方法

要在网络中实现密码与大型机同步，请选择运行 eTrust AC 的 Windows 计算机作为大型机的父项，并确保安装大型机密码同步选项。接下来，对 eTrust AC 定义该大型机，并为大型机订阅来自该 Windows 计算机的密码策略模型。完成该操作后，大型机用户执行的任何密码更改都将传播至该密码策略模型层级结构中的所有计算机。

当您向大型机管理员授予更改密码的 eTrust AC 权限时，管理员在大型机上执行的任何用户密码更改、挂起操作或恢复用户操作，都会从大型机传播至整个密码策略模型层级结构结构。同样，在密码策略模型层级结构中的任何位置执行的管理密码更改和挂起或恢复用户操作，也都将传播至该大型机。

密码同步的安装要求

在大型机中

必须在计算机上安装 Unicenter TNG 2.2 SP1、Unicenter TNG 2.4、Unicenter NSM 3.0 或 CA Common Services。密码同步实用程序依赖于 Unicenter TNG 的内置 CAICCI（公用通信接口）。

您可以在下列位置找到有关为密码同步配置大型机的说明：

- 对于 eTrust CA-ACF2 Security，请参阅《eTrust CA-ACF2 Security 管理员指南》
- 对于 eTrust CA-Top Secret Security，请参阅《eTrust CA-Top Secret Security 用户指南》
- 对于 RACF，请访问 CA Common Services 的安装 CD

在 Windows 中

在要用作大型机的父项以执行密码同步的每台 Windows 计算机上，必须在安装 eTrust AC 时选择"大型机密码同步"选项。

注意：如果已安装 eTrust AC，则可以再次运行安装程序，以选择 "大型机密码同步"选项。重新安装不会改变您当前的数据库或设置。

开始安装之前，您可能需要从此计算机中获取要订阅策略模型的每台大型机的主机名、SYSID 和管理员名称。如果在安装时没有访问该信息的权限，则可以跳过这部分安装并在以后为大型机订阅（策略模型）。

要启动 eTrust AC 安装程序，请选择"自定义安装"，然后选中"大型机密码同步"选项。安装向导使用 Unicenter CAICCI 软件包，但是您必须重新启动 Unicenter TNG 才能更新 CAICCI 配置。

安装程序允许您为主机订阅策略模型。如果您有了大型机的主机名和 SYSID，则可以立即为它们订阅（策略模型）。否则，可以跳过该步骤并且在以后为这些主机订阅（策略模型）。

检查安装

完成 eTrust AC 安装后，您可以检查它是否已成功安装必要的服务和进程，如下所示：

1. 使用 Windows 服务小程序（对于 Windows NT，请依次单击"开始"、"设置"、"控制面板"、"服务"，或者对于 Windows 2000，请依次单击"开始"、"设置"、"控制面板"、"管理工具"、"服务"）查看服务列表。

   服务列表中应显示下列服务：

   - Unicenter (NR-Server)
   - Unicenter (Remote)
   - Unicenter (Transport)

   eTrust AC 主机同步

2. 打开 Windows 任务管理器，选择"进程"选项卡。

   列表中应显示下列进程：

   - mfscpfd.exe
   - mfsd.exe
   - eacmfs.exe

如果在安装期间已为大型机主机订阅策略模型，请按如下所示验证它们是否显示在订户列表中：

1. 在"开始"菜单中，依次选择"程序"、"CA"、"eTrust Access Control"、"策略管理器"。
2. 单击左侧面板底部的"工具"按钮。
3. 单击"策略模型"图标。
4. 在树视图中，选择在安装期间已为大型机订阅的策略模型。
5. 验证您为其订阅策略模型的大型机主机是否显示在右侧的列表中。

完成策略模型配置

在大型机和父 Windows 系统中安装相应的软件后，必须在 Windows 系统中执行下列操作，以完成密码同步所需的配置：

- 在 PMDB 中为计划为策略模型订阅的每台大型机创建一条 MFTERMINAL 记录。

  在 PMDB（而不是本地数据库）中创建记录时，该记录将传播至策略模型层级结构中的所有主机。

- 在 PMDB 和本地 Windows 环境中，为执行密码更改的每个大型机管理员创建一条 USER 记录，为这些用户授予管理员或密码管理员权限，以便 eTrust AC 可以识别出他们进行密码更改的权限。
- 在 PMDB 中，再次为这些大型机管理员授予 Windows 计算机的 TERMINAL 记录的完全访问权限（读取和写入），以及可从中执行密码更改的任何大型机的 MFTERMINAL 记录的读取权限。
- 为这些大型机管理员授予在本地 Windows 环境中进行本地登录的权限。来自大型机的密码更改，必须能够通过相应大型机管理员用户的授权，在本地计算机的 eTrust AC 中执行。
- 为大型机订阅策略模型（如果未在安装期间执行此操作）。
- 检查 Windows 注册表中的 passwd_pmd 键，确保它指定了用于本地计算机的密码更改的密码策略模型及其订户。如有必要，请更新该注册表键。

这些项目不需要按照任何特定顺序执行（当然，以下情况除外，即您在创建管理员的用户记录和大型机的 MFTERMINAL 记录之前，无法为大型机管理员授予 MFTERMINAL 记录的访问权限）。

以下过程是完成这些步骤的一种方法。

1. 在"开始"菜单中，依次选择"程序"、"CA"、"eTrust"、"eTrust Access Control"、"策略管理器"。
2. 如果未在安装期间为大型机订阅策略模型，请执行以下步骤。否则，跳至步骤 3。
   a. 单击左侧程序栏中的"工具"按钮。
   b. 单击"策略模型"图标。
   c. 选择相应的策略模型。
   d. 在"编辑"菜单中，选择"添加订户"。
   e. 在"订户名称"中，输入大型机的完全限定主机名。
   f. 选中"大型机订户"框。
   g. 为该大型机选择主机类型（ACF、ACF2、RACF、TNG 或 TSS），然后输入该大型机的 SYSID 和管理员名称。
   h. 单击"确定"。
   i. 对要添加的每个大型机订户重复以上步骤。

3. 按如下所示检查 passwd_pmd 项：
   a. 单击左侧程序栏中的"Windows NT"按钮。
   b. 单击"注册表编辑器"图标。
   c. 从树视图中，导航至以下目录：

      HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\eTrustAccessControl

   d. 双击右侧列表中的 passwd_pmd 键。
   e. 在"值"区域中，选择"字符串"按钮，并键入本地计算机的父项在密码策略模型层级结构中的完全限定名称（如果尚未正确指定这些项目）。
   f. 单击"确定"。
4. 为大型机管理员创建 USER 记录，为他们授予在 eTrust AC 中更改密码的权限，并且为他们授予在 Windows 中进行本地登录的用户权限，如下所示：
   a. 依次选择"文件"、"连接"或单击工具栏上的"连接"按钮。
   b. 在"主机选择"对话框中选择 localhost pmdb，或者在"主机"文本框中输入 pmdbName@localhost，其中 pmdbName 为相应的策略模型。
   c. 单击"确定"。
   d. 单击左侧程序栏中的"访问控制"按钮。
   e. 单击"用户"图标。
   f. 单击工具栏上的"新建"按钮。
   g. 在"新建用户 - 常规"对话框中，输入大型机管理员的名称。
   h. 单击"用户属性"图标。
   i. 在"用户属性"对话框中，根据希望向该用户授予的权限，选中"管理员"或"密码管理员"。
   j. 单击"杂项"图标。
   k. 在"杂项"对话框中，单击"用户权限"按钮。
   l. 从可用用户权限列表中，选择"本地登录"，然后单击">>"按钮，将该用户权限移至"授予的权限"列表中。
   m. 单击"确定"关闭"用户权限"对话框。
   n. 单击"确定"添加该用户。
   o. 对每个大型机管理员重复步骤 e 到 n。
   p. 单击"资源"图标。
   q. 从树视图中，选择"登录保护"、"终端"。
   r. 从 TERMINAL 记录列表中，选择本地计算机的记录。

s. 在"查看或设置 TERMINAL 属性"对话框中，单击左侧的"授权"图标。

t. 单击"添加访问者"右侧的"新建"按钮。

u. 浏览访问者列表，并从列表中选择大型机管理员。

v. 单击"确定"。

w. 在"权限"区域中，选择"全部"按钮。

x. 对每个大型机管理员重复步骤 e 到 i。

y. 单击"确定"。

5. 关闭策略管理器并启动 selang。

6. 连接至策略模型：

```
eTrust> host pmd@localhost
```

7. 使用以下命令为每台大型机创建 MFTERMINAL 记录：

```
eTrust> newres MFTERMINAL mfSYSID defaccess (none) owner (userName)
```

其中，mfSYSID 是大型机的 SYSID，userName 是拥有该 MFTERMINAL 记录的用户。

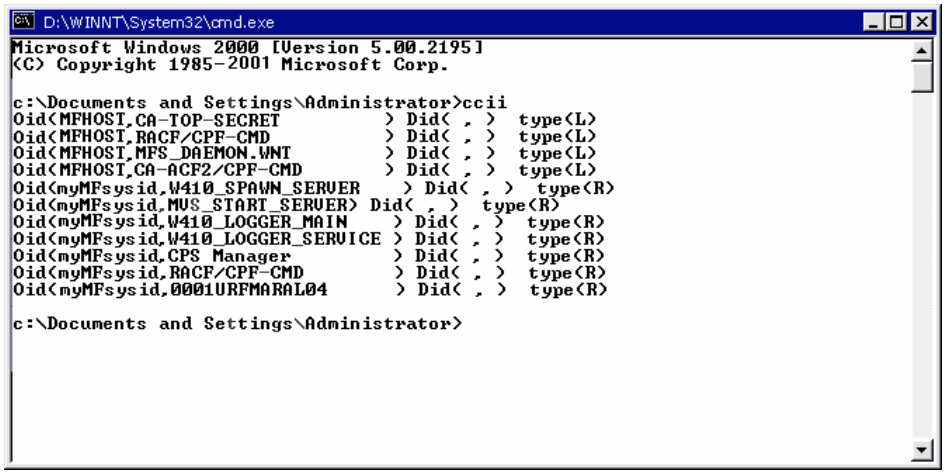
8. 使用以下命令向每个大型机管理员授予相应 MFTERMINAL 记录的访问权限：

```
eTrust> authorize MFTERMINAL mfSYSID uid (mfAdmin) access (read)
```

其中，mfSYSID 为大型机的 SYSID，mfAdmin 为大型机管理员用户。

启动大型机同步

要确保已建立通信，请在命令提示符处运行 ccii 实用程序。



CAICCI 配置文件

安装期间以及在为大型机订阅策略模型时，eTrust AC 会自动更新 CAICCI 配置文件。

如果出于某些原因您需要手动执行这些更新，请使用以下过程：

1. 在记事本中，打开 CAICCI 配置文件 (cciDirectory\tng\caiuser\ccirmtd.rc)。
2. 添加以下行：

   ```
   REMOTE = mfName mfSYSID 1024 startup port 1721
   ```

   其中，mfName 是大型机名称，mfSYSID 是大型机 SYSID。
3. 保存该文件。
4. 停止远程 CAICCI 服务：

   ```
   ccicntrl stop rmt
   ```
5. 重新启动远程 CAICCI 服务：

   ```
   ccicntrl start rmt
   ```

设置 Active Directory 用户或组属性

如果连接至带有 Active Directory 的 Windows 2000 计算机，则可以使用"用户属性或组属性"对话框的"目录服务"面板，设置 Active Directory 用户或组属性。在本地 Windows NT、不含 Active Directory 的 Windows 2000 或 eTrust AC 数据库环境中，不支持这些属性。

如果您的计算机中没有 Active Directory，请连接至一台具有该组件的计算机。（该计算机必须安装了 eTrust AC。）

1. 新建一个用户，然后打开"目录服务"面板。

   注意：只有在您连接到安装了 Active Directory 的 Windows 2000 计算机时，才会出现用于激活该面板的图标。

2. 向下滚动该列表。如果您要创建条目，请在该表的"值"（右）侧上双击。单元格周围将显示一个框，您可以在其中键入内容。

   注意：如果双击单词 Array 显示的位置，则将显示一个对话框，其中包含一个可填写内容的表。

索引

W

三划

四划

五划

六划

五划

六划

七划

八划

九划

八划

九划

十划

十一划

十二划

十三划

十四划

十六划

十九划