第 11 章　安全配置与分析

本章介绍 Windows 2000 系统中的安全配置工具集。作为 Microsoft 管理控制台（MMC）管理单元的一个集合，设计它的目的是为了减小基于 Windows NT 和 Windows 2000 操作系统的网络安全配置与分析方面的开销。

安全配置工具集允许对基于 Windows NT 或 Windows 2000 的系统安全属性进行配置，然后进行周期性的系统分析以保证配置的完整性，或者过后再进行必要的更改。在拥有大量系统的企业中，该工具集也可以同 Windows 管理更改和配置管理器集成在一起以自动配置安全组策略。

11.1　安全配置工具集概述

安全配置工具集是一组 Microsoft 管理控制台（MMC）管理单元，使用它可以为与安全性相关的管理任务提供一个中心储备库。有了安全配置工具集，可以使用集成化的工具集在网络上的一个或多个基于 Windows 2000 或 Windows NT 的机器上配置并分析安全性。

11.1.1　安全配置工具集的用途

从管理员的角度来看，Windows NT 提供了一些可单独用于配置系统安全性不同方面的图形化工具。但是，这些工具并不是集中式的，也就是说，为了配置一台计算机的安全性，管理员可能需要打开三个或四个应用程序。因此，安全配置较为复杂，而且因为在 Windows 2000 系统中增加了分布式安全功能，所以安全配置将变得更加复杂。

虽然 Windows NT 4.0 系统中提供了足够的（尽管有些不方便）的配置工具，但却缺乏用于安全分析的工具。该类别中的惟一工具就是事件查看器，但它不并是为执行企业级的审核分析而设计的。

安全配置工具集的目的是要满足集中式安全配置工具的需要，并且在以后的版本中为企业级分析功能提供框架。最重要的是，通过定义一个点（可以根据需要，在此查看、分析并调整整个系统的安全性），它将降低与安全性有关的管理费用。目标是为配置和分析系统的安全性提供一个全面、灵活、可扩展而且简单的工具集。

安全配置工具集的首要目标是为基于 Windows NT 或 Windows 2000 系统的安全性提供单点管理。为了达到这个目标，该工具必须允许管理员：

- 在一个或多个基于 Windows NT 或 Windows 2000 的计算机上配置安全性。
- 在一个或多个基于 Windows NT 或 Windows 2000 的计算机上进行安全性分析。
- 在一个集成且统一的框架内完成这些任务。

从所涉及到的系统组件与可能需要的更改级别来看，在基于 Windows NT 或 Windows 2000 的网络中配置安全性的过程不但复杂而且琐碎。因此，安全配置工具集的设计允许管理员在宏观层次上进行配置。换句话说，工具集允许定义多个配置设置，并让它们在后台实现。一旦有了这个工具，配置任务就可以分组并且自动执行。若要配置一组计算机，就不再需要多次、重复按键并对多个不同应用程序进行反复访问了。

安全配置工具集的设计并不能替代处理系统安全性的不同方面的系统工具，如用户管理器、服务器管理器、访问控制列表 (ACL) 编辑器等。相反，其目标是通过定义一个可以解释标准配置文件并可在后台自动执行所需操作的引擎，与它们互为补充。必要时，管理员可以继续使用现有工具（或其更新的版本）更改单个安全设置。 为了填补 Windows NT 安全管理中安全分析的空白，安全配置工具集提供了微观层次的分析。该工具集的设计可以提供

与安全性相关的各个系统方面的信息。

11.1.2 安全配置工具集的特性

安全配置工具集不但全面、灵活、可扩展，而且简单。

1. 全面性

不像操作系统的其他功能那样，安全性是系统作为一个整体的特征。几乎系统的每个组件都对系统安全性的某个方面负责。因此，像“我的计算机是否安全？”或“我的网络是否安全？”这样的问题变得极为难以回答。通常，系统管理员在试图回答这些问题时，必须检查许多不同的系统组件并使用许多工具。安全管理工具集的目标是成为回答与安全性有关问题的资源，不管该问题是概括的（如以上所列出的）还是非常具体的。要提供全面的安全管理与信息，安全配置工具集允许管理员配置并分析所有下列各项。

- 账户策略：可以使用该工具设置访问策略（包括域或本地密码策略）、域或本地账户锁定策略和域 Kerberos 策略。
- 本地策略：可以配置本地审核策略、用户权限分配以及各种安全选项，例如软盘、CD-ROM 等的控制。
- 受限的组：可以为内置组指派组成员身份，例如管理员、服务器操作员、备份操作员、超级用户等，以及任何想配置的其他特定组。它不应被用作常用成员身份管理工具，而只应用来控制被赋予敏感功能的特定组的成员身份。
- 系统服务：可以为系统上安装的不同服务配置安全性，包括网络传输服务，例如 TCP/IP、NetBIOS、CIFS 文件共享、打印等。可以为这些服务配置启动选项（自动、手动或禁用），或者在这些服务上设置访问控制，包括授权或拒绝其开始、停止、暂停和发出控制命令的权限。
- 文件或文件夹共享：可以配置 Windows NT 文件系统（NTFS）和重定向服务的设置。这些设置包括在访问各种网络文件共享时关闭匿名访问并启用数据包签名和安全的选项。未来的版本将包括其他服务特定的子区域，包括一些诸如 Internet Information Server（IIS）的服务。
- 系统注册表：可以设置系统注册表项的安全性。
- 系统存储：可以设置本地文件系统卷和目录树的安全性。
- 目录安全：可以管理驻留在 Windows 2000 Active Directory 中的对象的安全。

2. 灵活性

使用安全配置工具集可以定义安全配置，这包括上面所概述的每个领域中的安全属性的设置。使用这些配置，就可以配置系统。也可以以这些配置作为建议在系统上进行的安全分析。

配置保存在基于文本的.inf 文件中。配置信息将在不同的节进行说明，并且由工具集的配置引擎进行解析。随着系统的不断变化，如果需要确定新的安全配置和分析区域，体系结构足够灵活到可以支持新的部分。

安全配置工具集包括一组预定义配置。管理员可以选择这些预定义配置，或者可以将它们作为创建自定义配置的出发点。工具集的配置编辑工具（称之为“安全配置编辑器”）则提供这种功能。

3. 可扩展性

安全配置工具集的设计是可扩展的。可以添加扩展，将其作为新的安全性配置和分析区域或现有区域中的新属性。因为配置信息是以标准的 .inf 文件格式存储的，可以轻松地对其进行扩展而不会影响向后兼容性。

4. 简便性

因为使用安全工具集可以减少与在网络上管理安全性有关的费用，因此最重要的是工具应该易于学习与使用。工具集不包括复杂选项，它只有一个简单统一的图形用户界面（GUI），可以用于定义配置、将它们保存到文件中、查看存储在安全性分析数据库中的安全性分析数据。该界面使用 Microsoft 管理控制台支持的标准上下文菜单与视图。其中，没有多余的图形或统计数字，只有信息的简单列表视图（它带有标记安全问题的可视提示）。除此之外，工具集还包括一个命令行工具即 Secedit.exe，它允许管理员将配置与分析作为脚本的一部分进行运行。管理员可以使用图形界面或命令行应用已保存的配置并进行分析，这将能够很容易地将工具纳入现有的管理模式，也可以使用图形界面来定义配置并浏览分析数据。

11.2 安全配置工具组件

安全配置工具集由如图 11-1 所示的组件组成。

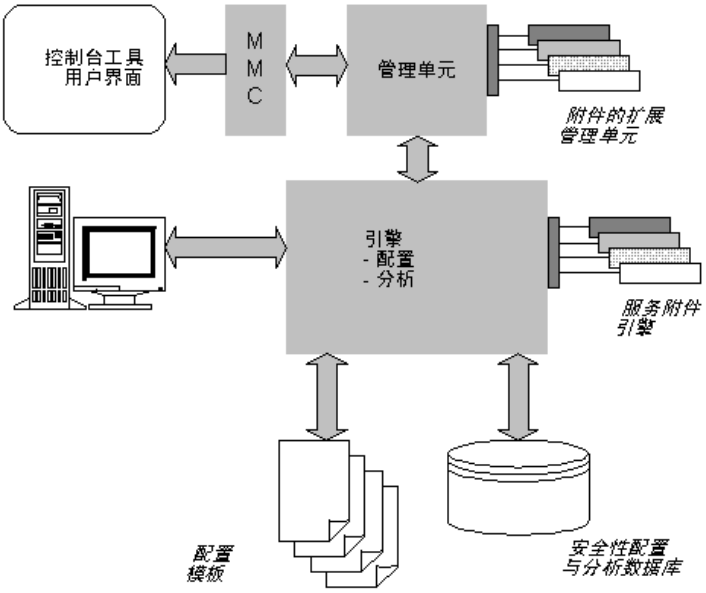

图 11-1 安全配置工具集的体系结构

- 安全配置服务：该服务是安全配置工具集的核心引擎。它运行在基于 Windows 2000 的每个系统上，并且负责由工具集提供的所有安全配置与分析的功能。该服务是整个体系结构的中枢。
- 安装安全：安装过程中所完成的初始安全性配置是由该工具集使用与系统一起发行的预定义配置完成的。这将在每个全新安装的 Windows 2000 计算机上创建一个叫做“本地计算机策略”数据库的初始安全数据库。
- 安全配置模板管理单元：这个独立的管理单元工具可以在一个安全模板中创建、编辑和保存安全配置，它在物理磁盘上存储为基于文本的.inf 文件。
- 安全配置和分析管理单元：这个独立的管理单元工具可以将一个或多个已保存的安全配置模板导入安全数据库（可以是本地计算机策略数据库或任何专用数据库）。导入的配置创建一个计算机指定的安全数据库，它存储合成配置。可以将合成配置应用于计算机，并根据数据库中存储的合成配置分析当前系统的配置。
- 组策略编辑器的安全设置扩展：这个管理单元工具扩展了组策略编辑器的功能。它允许将安全配置定义为“组策略对象”的一部分。然后可以将组策略对象分配给特定计算机，或者在 Active Directory 中的域或组织单元范围内进行分配，从而将其

应用于该范围内的所有计算机。各个组策略对象（本地、域和组织单元）的安全配置被传播到计算机并导入该计算机上的本地计算机策略数据库。来自该数据库的复合配置将周期性地应用于计算机以保证系统遵循企业策略。实际上这就是计算机的“安全策略”。

- 命令行工具 Secedit.exe：这是工具集中允许不用图形用户界面（GUI）就可以执行配置和分析功能的命令行接口。

11.3 安全模板管理单元

通过 MMC 的“安全模板”管理单元，能够定义、编辑和保存安全模板，如图 11-2 所示。

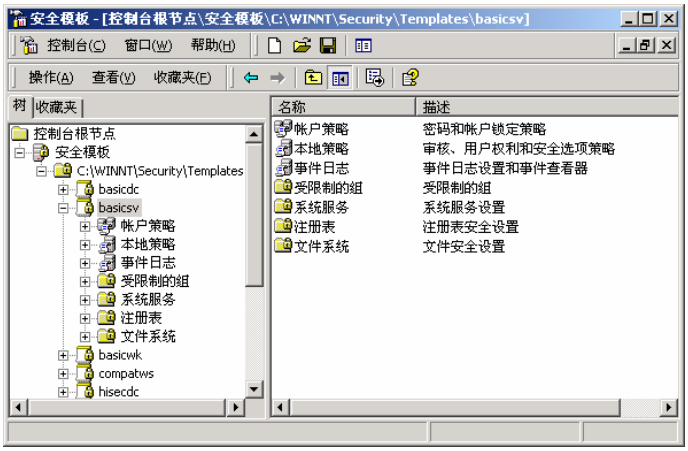

图 11-2 安全模板管理单元

虽然模板是以文本文件保存的，用任何文本编辑器都可以阅读，但是，并不推荐使用文本编辑器来修改这些模板。因为如果不小心改变了模板文件的格式，就可能会造成“安全配置服务引擎”无法对其进行解析。

11.3.1 安全模板

安全模板是文本文件，其中包含的安全性配置被细分为安全区域。Microsoft 已经确定了几个安全区域，但是，也可以添加新的区域以支持增强型系统功能而无须破坏与现有配置文件和数据库的向后兼容性。现在所支持的安全区域包括：

- 账户策略 该区域允许设置密码、账户锁定以及 Kerberos 策略。Kerberos 策略只和 Windows 2000 域控制器有关。
- 本地策略 该区域允许配置审核策略、用户权利分配与计算机安全选项。
- 事件日志 :该区域允许配置包括日志文件最大值和日志覆盖策略在内的事件日志配置。
- 受限组 该区域允许设置一个给定组的成员身份。当一个受限组策略应用到计算机之后，就只对该计算机的本地受限组进行配置。
- 系统服务 该区域包括所有的本地或网络系统服务。允许控制每个服务的启动模式（自动、手工还是禁用）以及用户可用的的访问级别。
- 注册表 该区域允许对授予注册表键的权限进行配置，也可以指定审核所需的访问权限。
- 文件系统 该区域允许对授予文件系统对象（文件、目录和子目录）的权限进行配置，也可以指定审核所需的访问类型。

- 目录对象　该区域仅在 Windows 2000 域控制器中存在。

11.3.2 预定义的安全模板

Windows 2000 提供了许多预定义的安全模板，如图 11-3 所示。默认情况下，这些模板存放在计算机上的%SYSTEMROOT%\Security\Templates 目录中。

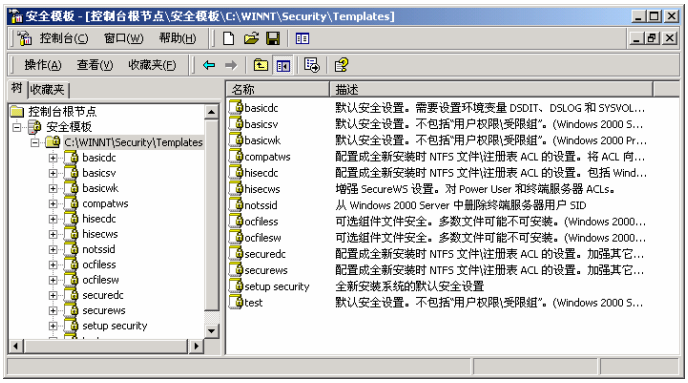

图 11-3 预定义的安全模板

可以使用 MMC 的“安全模板”管理单元自定义这些模板并将其导入到“组策略”管理单元的“安全设置”扩展中。

这些安全模板的构建基于这样一种假设，即它们将被应用于使用默认的 Windows 2000 安全设置的 Windows 2000 计算机。也就是说，在使用默认安全模板的计算机上，这些模板将对默认的安全设置进行增量修改。但它们不会先安装默认安装模板，然后再进行修改。安装在 FAT 文件系统上的 Windows 2000 系统不会得到有效保护。

预定义的安全模板包括：

- 默认工作站（basicwk.inf）
- 默认服务器（basicsv.inf）
- 默认域控制器（basicdc.inf）
- 兼容工作站或服务器（compatws.inf）
- 安全工作站或服务器（securews.inf）
- 高度安全工作站或服务器（hisecws.inf）
- 专用域控制器（dedicadc.inf）
- 安全域控制器（securedc.inf）
- 高度安全域控制器（hisecdc.inf）

这些模板被设计成含有五个公用安全要求，不同的安全要求就分别对应以下五种不同的安全等级。

（1）基本（basic*.inf）

基本配置的模板可以作为一种方法提供以反转不同安全配置的应用程序。除了这些属于用户的权限之外，基本配置可以将 Windows 2000 默认的安全设置应用于所有安全区域。因为应用程序安装程序通常会修改用户权限以成功地使用应用程序，所以不在基本模板中进行修改。撤消这些修改并不是基本配置文件的目的。

（2）兼容（compat*.inf）

Windows 2000 默认的安全配置为本地 Users 组成员设置了严格的安全性，而本地 Power Users 组的安全设置与 Windows NT 4.0 兼容。 这一默认配置允许在提供给 Users 的标准 Windows 环境中运行经 Windows 2000 验证过的应用程序，同时还允许在提供给 Power Users 的安全性稍低的环境下运行未经 Windows 2000 验证的应用程序。但是，如果为了运行未经 Windows 2000 验证过的程序而让用户成为 Power Users 组的成员，这对某些环境就太不安全

了。有的时候，一种较好的解决方法是：在默认情况下，只将用户指派为 Users 组的成员，然后将 Users 组的安全性特权级降至 Windows 2000 未验证的应用程序也可以运行。Windows 2000 系统则为其设计了兼容模板。通过降低通常由应用程序访问的特定文件、文件夹和注册表项的安全级别，兼容模板允许大多数的应用程序成功运行。此外，由于假定应用兼容模板的管理员不需要用户成为 Power Users，因此将删除 Users 组的所有成员。

（3）安全（secure*.inf）

除文件、文件夹和注册表项之外，安全模板是对所有的安全区域执行推荐的安全设置。因为默认情况下将安全地配置文件系统和注册表权限，所以这些都不会被修改。

（4）高度安全（hisec*.inf）

高度安全模板定义 Windows 2000 网络通信的安全设置。设置安全区域以便为用于运行 Windows 2000 的计算机间的网络通信和协议请求最大限度的保护。它们不能与运行 Windows 9x 或 Windows NT 的计算机进行通信。

（5）专用域控制器（dedica*.inf）

在默认情况下，运行 Windows 2000 域控制器上的本地用户安全并不理想。这允许管理员以向后兼容的方式运行域控制器上现有的基于服务器的应用程序（不推荐）。如果不运行域控制器上基于服务器的应用程序（推荐），默认的本地用户组文件系统和注册表权限可以按与 Windows 2000 工作站和独立服务器默认定义相同的方式定义。通过执行专用安全模板，这些理想的本地用户安全设置可以在 Windows 2000 域控制器上应用。

11.4 安全配置和分析管理单元

通过 MMC 的“安全配置和分析”管理单元，能够完成以下几项功能：

- 分析系统安全性
- 查看安全性分析数据
- 配置系统安全性

该管理单元的目标是为了允许管理员把安全配置加载到计算机中，并检查系统以找出实际的系统设置与那些设置之间的差别。这种分析之所以有用，是因为：

- 它可以确定当前配置可能存在的安全漏洞。
- 可以在实际部署策略之前，确定潜在的安全策略可能会对系统做出什么样的改动。
- 可以确定与系统当前所用策略相背离的地方。

11.4.1 安全配置和分析数据库

因为所有的安全配置和分析都是由数据库驱动的，所以有必要介绍一下“安全配置和分析数据库”。

安全配置和分析数据库（“安全数据库”）是计算机中特定的数据存储区，它是在将一个或多个配置导入至特定计算机时生成的。计算机进行 Windows 2000 全新安装时可能创建一个初始数据库。这个数据库被称为本地计算机策略数据库。最初，它包括系统的默认安全性配置。安装完毕之后可以立即将该配置导出到一个安全配置文件中并保存它。如果在以后的任何时间因为任何原因希望恢复最初的安全配置，这将是很有用的。

安全性配置和分析数据库是对系统所进行的所有配置与分析的起点。数据库是从上述与计算机无关的配置文件中初始创建的。无须改写整个配置，可以将新的配置增量地添加至数据库。

安全数据库的另一个重要方面是它在执行分析时对它的使用。可以使用安全配置和分析对当前系统的配置和在数据库中存储的配置做一个比较。执行分析可以提供有关在何处系统

可能背离了特定配置的信息。这有助于解答疑难问题、调整安全策略，而且最重要的是：检测一段时间后系统中可能出现安全缺陷。

在对系统进行安全性配置和分析之前，首先需要打开一个安全数据库，如果没有则必须首先创建一个数据库。如图 11-4 所示。

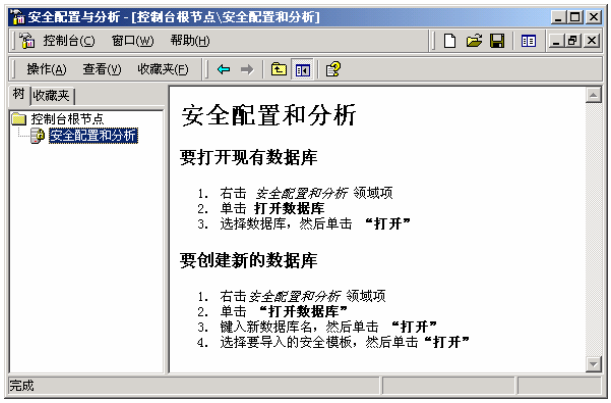

图 11-4　打开和创建安全配置和分析数据库

若要打开现有数据库，则右击“ 安全配置和分析 ”节点，在弹出的菜单中选择“ 打开数据库 ”命令，然后选择数据库，单击“ 打开 ”按钮。

若要创建新的数据库，则右击“ 安全配置和分析 ”节点，在弹出的菜单中选择“ 打开数据库 ”命令，然后输入新数据库名，单击“ 打开 ”按钮，最后选择要导入的安全模板，单击“ 打开 ”按钮。

11.4.2　分析系统安全性

通过执行安全性分析，可以把系统的当前状态与所导入的安全模板进行比较。如果当前的系统设置与基本设置匹配，则被认为是正确的；否则，那些不匹配的设置都会被标记出来。

对系统进行安全性分析可参照如下步骤：

（1）确认已经打开了一个数据库，并导入了一个基准配置模板。

（2）右击“ 安全配置和分析 ”节点。

（3）在弹出的菜单中选择“ 立即分析计算机 ”命令。

（4）选择“ 错误日志文件路径 ”，单击“ 确定 ”按钮。

（5）开始分析系统，并显示如图 11-5 所示的进度条。

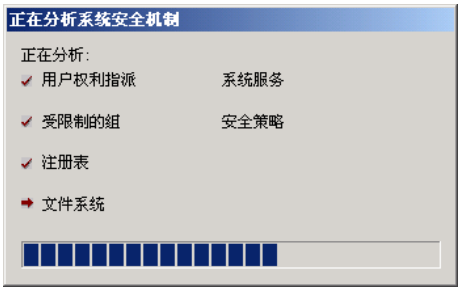

图 11-5　正在分析系统安全性

11.4.3　查看安全性分析结果

在完成安全性分析之后，就会在“ 安全配置和分析 ”节点下面出现可用的安全区域。它们是按照安全区域进行组织的，含有把有问题的区域高亮显示的标记。每个属性的当前系统设置和基本配置设置都会显示出来。

若要查看分析结果，只须展开“ 安全配置和分析 ”节点，选中其中具体的某个安全区域，

如“账户策略”下的“密码策略”，如图 11-6 所示。

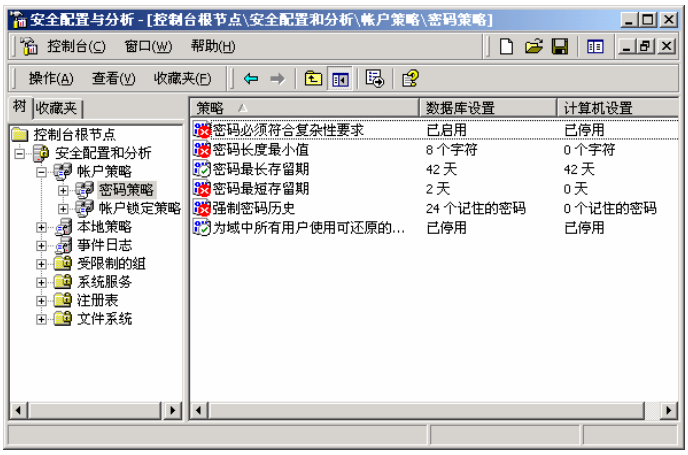

图 11-6　查看安全性分析结果

在右边的窗格中同时显示了每个对象的数据库设置和实际的系统设置。用红色标记高亮显示不一致的地方，而用绿色标记高亮显示相一致的地方。如果没有标记或者检查记号，就表明在数据库中没有指定该安全设置（即在导入的安全模板中没有对该项安全设置进行过配置）。

双击右边窗格中的任何设置，就可以进一步查看不一致的地方，如有需要还可以修改数据库中的设置（不是本地计算机的设置）。如图 11-7 所示。

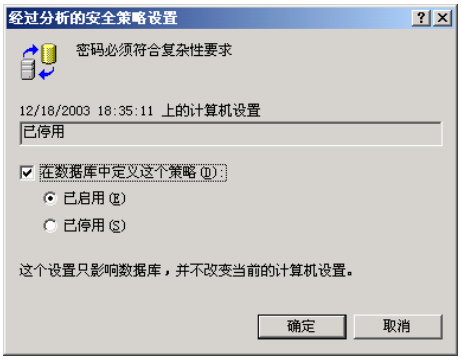

图 11-7　修改基本分析设置

11.4.4　配置系统安全性

在根据模板分析了当前的系统设置之后，如果对该模板所指示的安全性变化（标记为不匹配的地方）认可的话，就可以使用这些新的安全设置来配置系统。

对系统的安全性进行配置可参照如下步骤：

（1）右击“安全配置和分析”节点。

（2）在弹出的菜单中选择“立即配置计算机”命令。

（3）选择“错误日志文件路径”，单击“确定”按钮。

（4）开始配置系统，并显示配置进度条。

11.5　组策略管理单元的安全设置扩展

安全配置工具集中的一个重要部分就是与组策略管理单元集成的安全设置扩展。除了在“安全模板”中所描述的那些安全区域外，组策略的安全设置扩展还提供了更多的安全区域，如 IPSec 策略、公钥策略、加密密钥恢复代理、根证书和证书信任列表等。

下面详细介绍通过组策略管理单元的安全设置扩展，可以设置的基于 Windows 2000 系统的各个安全方面。

11.5.1 账户策略

在 Windows 2000 中有两种账户：域账户和本地账户。域账户的账户策略是在域中配置的，本地账户的账户策略是在本地计算机上的配置。

域的账户策略定义密码的强壮程度、密码历史、Kerberos 票据的生存时间、账户锁定等，而在本地计算机上，可以为本地账户指定除 Kerberos 策略之外完全相同的策略。因为本地账户不使用 Kerberos 进行身份验证。如图 11-8 所示。

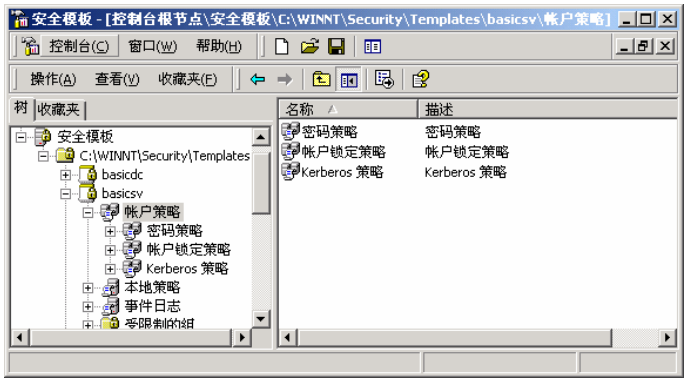

图 11-8 账户策略

1. 密码策略

密码策略包含用来限制用户密码的策略。

- 密码必须符合复杂性要求。该策略强迫用户选择包含大小写字符、数字、符号的混合密码，以增强密码的复杂性。
- 密码长度最小值。该策略指定密码可包含的最少字符的数目。
- 密码最长存留期。该策略指定密码过期之前的有效天数，可用来强制用户定期更改他们的密码。
- 密码最短存留期。该策略指定用户更改密码之前密码仍然保持有效的天数，可用来防止用户通过更改密码然后又将密码改回来而绕过“密码最长存留期”策略。
- 强制密码历史。该策略指定 Windows 2000 应为每个用户记住的密码数量。当与“密码最长存留期”策略和“密码最短存留期”结合使用时，该策略可以防止用户连续重复使用几个密码。
- 为域中所有用户使用可还原的加密来储存密码。该策略修改用来存储用户密码的加密算法，来增强密码被破解的难度。

2. 账户锁定策略

账户锁定策略可通过在规定的失败登录尝试次数之后锁定用户账户来防止暴力猜解用户密码。

- 复位账户锁定计数器。该策略指定记录失败登录尝试次数的计数器自动重设为 0 之前的时间（单位为分钟）。
- 账户锁定时间。该策略指定达到“账户锁定阀值”后用户账户仍然锁定的时间长度（单位为分钟）。
- 账户锁定阀值。该策略指定锁定用户账户之前所允许的失败登录尝试次数。

3. Kerberos 策略

对于域用户账户，该策略决定与 Kerberos 有关的设置，如账户有效期和强制性等。

- 服务票证最长寿命。该策略指定 KDC（密钥分发中心）所分发的票据保持活动状态的时间长度（单位为分钟）。
- 计算机时钟同步的最大容差。该策略指定客户机时钟和服务器时钟之间 Kerberos 所容许的最大时间差（单位为分钟）。
- 强制用户登录限制。该策略使得 KDC 通过检查目标计算机上的用户权限策略以核实是否有“本地登录”权限或者“从网络上访问这台计算机”的权限来验证每个请求的会话票据。
- 用户票证续订最长寿命。该策略指定 Windows 2000 可使用一个重复更新的 TGT（票据授予票据）的时间长度（单位为天数）。
- 用户票证最长寿命。该策略指定 KDC 所分发 TGT 保持活动状态的时间长度（单位为分钟）。

11.5.2 本地策略

本地策略方面的设置属于应用程序或用户所使用的计算机上的安全设置。本地策略基于已登录的计算机以及在此特殊的计算机上的权限。如图 11-9 所示。

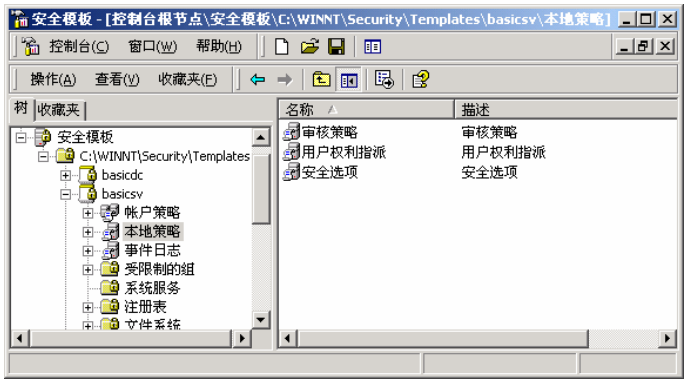

图 11-9 本地策略

根据定义，本地策略对计算机的影响是局部的。当这些设置被导入到 Active Directory 中的组策略对象时，它们将影响应用组策略对象的任何计算机账户上的本地安全设置。在任意情况下，如果有替代这些特权的本地策略设置，则将不再应用用户账户权限。

本地策略的安全区域包含下列内容的属性。

1. 审核策略

审核策略是一个可选的特性，它决定记录计算机需要捕获到安全日志中的安全事件，以便日后在事件查看器中显示。 当启用事件的日志记录时，可以指定是否需要 Windows 2000 维护一个有关成功的尝试、失败的尝试还是两者都包括在内的日志。可审核的事件类型如下。

- 策略更改。对用户安全选项、用户权限或审核策略所作的更改。
- 登录事件。用户登录或注销、或者用户建立或取消了与计算机的网络连接。
- 对象访问。用户获得对文件、文件夹或打印机的访问。
- 过程追踪。
- 目录服务访问。用户获得对特定 Active Directory 对象的访问。
- 特权使用。用户行使权限，如更改系统时间等。
- 系统事件。用户重新启动或关闭计算机，或者发生了一个影响到系统安全性或安全性日志的事件。

- 账户登录事件。域控制器接收到一个要求验证用户账户的请求。
- 审核账户管理。管理员创建、更改或删除一个用户或组。用户账户被重命名、禁用或启用、或者设置或更改了一个密码。

2. 用户权利指派

用户权利指派可以用来决定在计算机上有登录或任务特权的用户或组。它包括如下策略内容。

- 备份文件和目录。该权利可让用户回避文件和目录权限，以对系统进行备份。
- 产生安全审核。该权利可让一个进程在安全日志中生成对象访问审核项。
- 创建记号对象。该权利可让进程创建一个记号，然后该进程可使用这个记号访问任何一个本地资源。需要拥有该权利的进程应使用 LocalSystem 账户（该账户已包括了这个权利），而不是使用一个单独的用户账户，再特别分配这个权利。
- 创建全局对象。
- 创建页面文件。该权利可让用户通过指定“ 性能选项 ”对话框中特定驱动器的分页文件的大小来创建并更改一个分页文件。
- 创建永久共享对象。该权利可让进程在 Windows 2000 对象管理器中创建对象目录。该权利对于计划扩展 Windows 2000 对象名称空间的核心模式组件非常有用。因为以 Kernel 模式运行的组件以被分配有该权利，因此就不必再特别分配该权利了。
- 从插接工作站中取出计算机。该权利可让用户使用 Windows 2000 用户界面移去一台计算机。
- 从网络访问此计算机。该权利使用户能够通过网络连接到计算机。默认情况下，该权利授予给 Administrators 组、Everyone 组和 Power Users 组。
- 从远端系统强制关机。该权利可让用户从网络上的远程位置关闭一台计算机。
- 调试程序。该权利可让用户将一个调试程序与任何一个进程连接，从而提供对敏感和关键的系统操作组件的高效访问。
- 更改系统时间。该权利可让用户设置计算机内部时钟上的时间。
- 关闭系统。该权利可让用户关闭系统。
- 管理审核和安全日志。该权利可让用户指定单个资源（如文件、活动目录对象和注册表键）的对象访问审核选项。对象访问审核实际上不会被执行，除非在组策略下的整个计算机的审核策略 Active Directory 服务中定义的组策略下启用了对象访问审核：该权利不授予对计算机审核策略的访问。拥有该权利的用户还可从事件查看器中查看和清除安全日志。
- 还原文件和目录。该权利可让用户在恢复备份文件和目录时回避文件和目录权限，并将任何一个有效的安全负责人设置为对象的所有者。
- 拒绝本地登录。该权利禁止用户或组本地登录。默认情况下，该权利不会被授予给任何人。
- 拒绝从网络访问这台计算机。该权利禁止用户或组通过网络连接到本机。默认情况下，该权利不会被授予给任何人。
- 拒绝作为服务登录。该权利禁止用户或组作为服务登录。默认情况下，该权利不会被授予任何人。
- 拒绝作为批作业登录。该权利禁止用户或组通过一个批队列设备登录。默认情况下，该权利不会被授予任何人。
- 内存中锁定页。该权利可让进程保存物理内存中数据，防止系统将数据存入磁盘上的虚拟内存中。行使该权利可大大影响系统性能。该权利已经废弃，因此从来不会

被选中。

- 配置单一进程。该权利可让用户使用 Windows 2000 和 Windows NT 的性能监视工具来监控非系统进程的性能。
- 配置系统性能。该权利可让用户使用 Windows 2000 和 Windows NT 的性能监视工具来监控系统进程的性能。
- 取得文件或其他对象的所有权。该权利可让用户接管系统中任何一个安全对象的所有权，包括 Active Directory 对象、文件和文件夹、打印机、注册表监、进程和线程。
- 身份验证后模拟客户端。
- 替换进程级记号。该权利可让一个进程更换与已启动进程相关的默认记号。
- 添加配额。该权利可让一个拥有另一进程写入属性访问权限的进程增量分配给另一进程的处理器配额。该权利对于系统调整非常有用，但像拒绝服务攻击一样会被滥用。
- 跳过遍历检查。该权利可让用户在任何一个 Windows 文件系统或注册表中浏览的同时绕过它不拥有访问权限的目录。该权利不能让用户列出一个目录的内容，只能遍历目录。
- 同步目录服务数据。该权利可让进程提供目录同步服务，只在域控制器上相关。默认情况下，该权利被分配给域控制器上的 Administrator 和 Local System 账户。
- 修改固件环境值。该权利可让用户通过修改系统属性或让进程修改系统环境变量。
- 以操作系统方式操作。该权利可让一个进程作为任何一位用户进行身份验证，因此该进程就可作为任何一位用户获得对相同资源的访问。只有较低级别的身份验证服务应使用该权利。
- 域中添加工作站。该权利可让用户将一台计算机添加到特定的域中。用户通过所要添加的计算机上的管理性用户界面指定域，在 Active Directory 计算机容器中创建一个对象。该权利的特性被附在计算机容器或组织单元的权限在 Windows 2000 复制。
- 允许计算机和用户账户被信任以便用于委托。该权利可让用户设置用户或计算机对象上的“可信委托”设置。被授予该权利的用户或对象必须拥有对用户或计算机对象上账户控制标记的写访问权限。信任委托的计算机上运行的服务器进程或用户运行的服务器进程都可访问另一台计算机上的资源。
- 在本地登录。该权利可让用户在本地计算机上登录。
- 增加进度优先级。该权利可让一个拥有另一进程的写入属性访问权限的进程提高另一进程的执行优先级。
- 装载和卸载设备驱动程序。该权利可让用户安装和卸载即插即用设备驱动程序。非即插即用的设备驱动程序不受该权利的影响，并且只可由管理员安装。因为设备驱动程序作为信任（高度特权）程序运行，该权利可能会被误用于安装破坏性程序并给予这些程序对资源的破坏性访问。
- 作为服务登录。该权利可让安全负责人作为一个服务登录，作为建立安全环境的一个方式。Local System 账户始终保留作为服务登录的权利。在单独账户下运行的任何一个服务都需被授予此权利。默认情况下，该权利不会被授予给任何人。
- 作为批处理作业登录。该权利可让一个用户使用批队列设备登录。默认情况下，该权利被授予 Administrators 组。

3. 安全选项

“安全选项”可用来启用或禁用计算机的安全设置，例如数据数字签名、Administrator 和 Guest 的账户名称、软盘驱动器和光盘的访问、驱动程序的安装以及登录提示等。

11.5.3 事件日志

事件日志方面的设置只包含有一个子项，即“事件日志设置”，可以用来定义与应用程序、安全性和系统日志相关的属性，如图 11-10 所示。

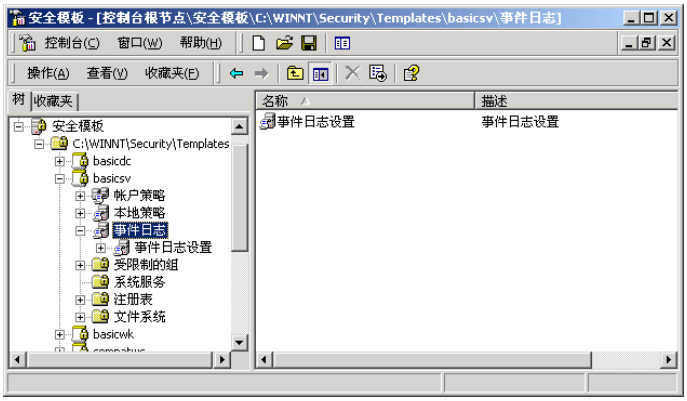

图 11-10 事件日志

这些策略为三种默认的日志（分别是应用程序、安全和系统）定义了如下一些设置。

- 日志的最大值。该策略指定日志的最大容量（单位为 KB）。
- 日志的保留天数。该策略指定事件被覆盖之前可保留在日志中的最长时间（单位为天）。
- 日志的保留方法。该策略可决定日志中的事件是否应单个覆盖还是按日期覆盖，还是根本不覆盖。
- 限制来宾对日志的访问。该策略只允许经过身份验证的用户访问日志。

11.5.4 受限制的组

受限制的组提供了一个重要的充当组成员管理者的安全新特性。它为拥有预定义功能的 Windows 2000 默认组（如 Administrators 组、Guests 组等）自动提供安全成员身份。一般将一个敏感组或特权组添加到受限制的组安全列表上，并指定哪些用户应当是该组的成员，也可指定所添加的其他组中哪一个应当是成员。从图 11-11 中可以看出，受限制的组部分的目的是防止已添加到组中的用户因疏漏而暂时留在组中，从而带来安全隐患。

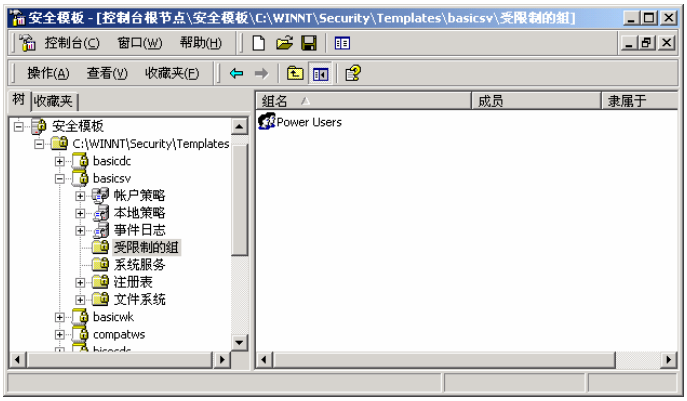

图 11-11 受限制的组

添加到受限制组的用户将被假定为允许成为该组永久成员的惟一用户。如果在添加新的组成员时没有将它们添加到这个策略中去，那么下一次应用这些组策略时，这些成员将会被

从组中删除。

例如，Power Users 组是 Windows 2000 的一个默认组，也自动成为受限组的一部分。假设 Power Users 组包含两个用户：A 和 B。后来由于 B 临时有事，所以它添加了用户 C 到该组中，以便暂时取代 B 执行职务。但是，当 B 回来之后却忘记了将 C 从组中删除。在实际管理工作中，这种情况时有可能发生，导致不应再拥有相关特权的用户仍然拥有额外的组成员资格。为了避免这种情况，就可以通过“受限制的组”来进行配置。如果设置只有 A 和 B 在受限组中被列为 Power Users 组的成员，那么当管理员下一次应用组策略设置时，C 就会被自动从组中删除了。

11.5.5 系统服务

在系统服务中，可以为 Windows 2000 计算机上运行的服务配置安全性权限和启动设置，如图 11-12 所示。这些参数可用“服务”控制台进行调整的参数相同。服务的安全性属性可用来确定哪些用户或组对象拥有权限读取、写入、删除和执行该服务。

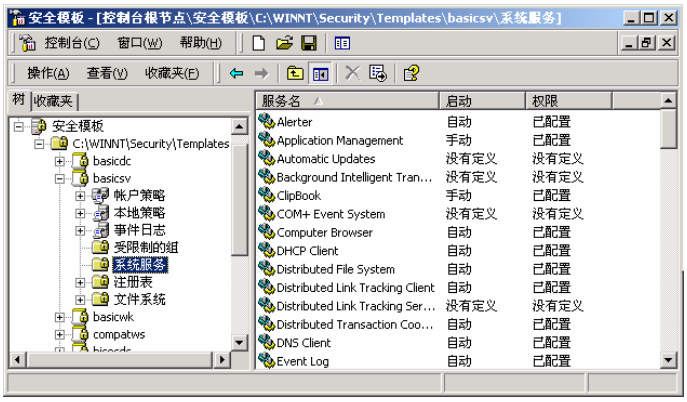

图 11-12 系统服务

11.5.6 注册表和文件系统

通过“注册表”和“文件系统”可为注册表键和文件系统元素（如文件和目录）设置访问权限。可以编辑注册表键或文件路径的安全属性，来指定哪些用户或组对象拥有访问键或文件路径的权限，并配置继承设置、审核和所有权权限。

11.6 Secedit 命令

图 11-13 显示了安全配置命令行工具 Secedit 可用的参数。

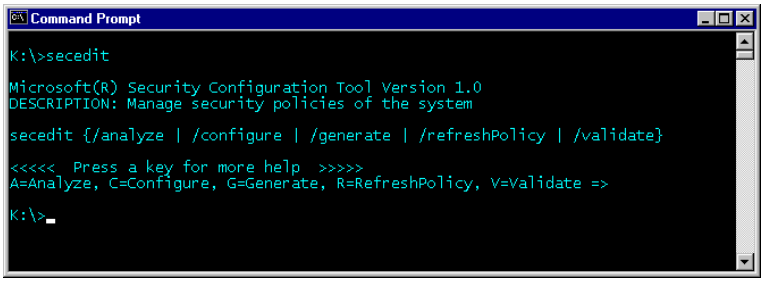

图 11-13 Secedit.exe 命令

该命令的语法如下：

secedit {/analyze | /configure | /generate | /refreshPolicy | /validate}

下面描述每个 Secedit 选项的详细语法：

1. Secedit analyze（Secedit 分析）

下面是分析系统安全的用法。

secedit /analyze [/scppath scppath] [/sadpath sadpath] [/log logpath] [/verbose] [/quiet]

- /sadpath：sadpath 是 Secedit 执行分析的数据库的路径。分析结果与已经在那里的配置信息一起保存在数据库中。如果没有指明 sadpath，则使用默认数据库。对于管理员来说，默认的数据库是%windir%\security\database\secedit.sdb，而对于用户来说则是%userprofile%\secedit.sdb 。如果 sadpath 是新数据库，那么必须指定 scppath。
- /scppath：scppath 是在进行分析之前必须加载到新数据库中的配置文件的路径。如果没有指定 scppath，则根据已包含在 sadpath 数据库中的配置信息进行分析。只有当 sadpath 是新数据库时 scppath 才有效。
- /log：logpath 是用于该过程的日志文件的路径。如果未提供该路径，则使用默认的 %windir%\security\logs\scesrv.log 路径。
- /verbose：提供详细的进度信息。
- /quiet：禁止屏幕与日志输出。

2. Secedit configure（Secedit 配置）

下面是为系统配置安全性的语法：

secedit /configure [/scppath scppath] [/areas areas] [/overwrite][/sadpath sadpath] [/log logpath] [/verbose] [/quiet]

- /areas：areas 指定要处理的安全区域。
  - SECURITYPOLICY：系统的本地策略和域策略。
  - USER_MGMT　每个用户的账户设置。
  - GROUP_MGMT　受限组设置（仅用于配置文件中指定的组）。
  - USER_RIGHTS　用户登录权限和特权授予。
  - DSOBJECTS　目录对象的安全。
  - REGKEYS　本地注册表项的安全。
  - FILESTORE　本地文件存储的安全。
  - SERVICES　所有定义过的服务的安全配置。
  - 默认区域是所有区域。每个区域应该用空格隔开。
- /overwrite：指定从 scppath 加载的配置信息应该覆盖当前数据库中保留的任何现有配置信息。将来使用该数据库的任何配置都将完全依据 scppath 文件中指定的信息。如果没有指定 overwrite，scppath 文件中的信息被附加到 sadpath 数据库中的现有信息中。只有在指定 scppath 时 Overwrite 才是有效的。

3. Secedit generate（Secedit 生成）

下面是从数据库中生成配置文件的语法：

secedit /generate /scppath scppath [/areas areas][/sadpath sadpath] [/log logpath] [/verbose] [/quiet]

4. Secedit refreshpolicy（Secedit 刷新策略）

下面是在后台开始安全策略传播的语法：

secedit /RefreshPolicy {MACHINE_POLICY | USER_POLICY}

其中 RefreshPolicy 指定 Secedit 按下列方式刷新安全策略：

- MACHINE_POLICY　刷新本地机器的策略。
- USER_POLICY　刷新有该登录 ID 的用户的策略。

5. Secedit validate（Secedit 验证）

下面是验证安全配置和分析配置文件的语法：

secedit /validate filename

其中 filename 指定要验证的配置文件。