IBM

eserver

iSeries

保护 iSeries 的技巧和工具

版本 5

SB84-0175-02

IBM

@server

iSeries

保护 iSeries 的技巧和工具

版本 5

SB84-0175-02

注意

在使用本资料及其支持的产品之前，请阅读第 145 页的『声明』中的信息。

中文版（2004 年 4 月）

此版本适用 IBM Operating System/400（产品号 5722-SS1）的 V5.3.0 及所有后续发行版和修订版，直到新版本中另有声明为止。此版本不能在所有精简指令集计算机（RISC）机型上运行，也不能在 CISC 机型上运行。

此版本替换 SC41-5300-06。

目录

图

表

关于保护 iSeries 的技巧和工具（SB84-0175-02）

计算机在组织中的角色正在快速更改。IT 管理员、软件供应商、安全管理员和审计员需要重新考虑他们在过去认为理所当然的许多领域。iSeries 安全性应该在该列表中。

系统正在提供许多新的功能，它们在很大程度上不同于传统记帐应用程序。用户正以新的方式进入系统：LAN、交换线路（拨号）、无线以及所有类型的网络。通常，用户永远看不到注册屏幕。许多组织正在使用私有网络或因特网扩充成为“扩展企业”。

突然，系统好象具有一组新的门和窗。系统管理员和安全管理员当然关心如何在此快速更改的环境中保护信息资产。

本资料提供一组实用建议，有关如何使用 iSeries 的安全性功能部件和如何建立意识到安全性的操作过程。在本资料中的建议适用于具有一般安全性需求和漏洞的安装。本资料并不提供可用的 iSeries 安全性功能部件的完整描述。如果需要阅读了解附加选项或需要更完整的背景信息，查阅第 143 页的第 17 章，『相关信息』中所描述的出版物。

本资料也描述如何设置和使用属于 OS/400 一部分的安全性工具。第 25 页的第 4 章，『将 iSeries 配置为使用安全性工具』和第 26 页的『安全性命令的命令和菜单』提供关于安全性工具的参考信息。本资料提供了使用这些工具的示例。

本书的适用对象

安全主管或**安全管理员**负责系统上的安全性。该职责通常包括下列任务:

- 设置和管理用户概要文件
- 设置影响安全性的系统范围的值
- 管理对对象的权限
- 实施和监控安全策略

如果您负责一个或多个 iSeries 系统的安全性管理，则本资料适用于您。本资料中的指示信息假定以下情况:

- 您熟悉基本的 iSeries 操作过程，如注册和使用命令。
- 您熟悉 iSeries 安全性的基本元素：安全级别、安全性系统值、用户概要文件和对象安全性。

  注: 第 3 页的第 1 章，『iSeries 安全性的基本元素』复述了这些元素。如果您不熟悉这些基本元素，则阅读 iSeries 信息中心中的*基本安全性和规划*主题。有关更多详细信息，请参阅第 xii 页的『先决条件和相关信息』。
- 您已通过将安全级别（QSECURITY）系统值至少设置为 30 来激活系统上的安全性。

IBM® 不断增强 iSeries 的安全性能力。要利用这些增强功能，应该定期评估当前可用于您的发行版的累积修正软件包。查看它是否包含与安全性有关的修订。

如何使用本资料

如果您未将系统设置为使用安全性工具或如果您已安装了安全性工具箱 OS/400 版的更早发行版，执行下列操作:

1. 从第 9 页的第 2 章，『iSeries 安全性向导和 eServer Security Planner』开始。它描述如何使用这些功能部件来选择建议哪些安全性工具以及如何入门。
2. 有关更多的基本安全性信息，可以复查“安全性参考”信息，该联机信息位于“iSeries™ 信息中心”中。

注意

本资料具有*许多*用于保护 iSeries 的技巧。您的系统可能仅在某些区域需要保护。使用本资料来自学有关可能的安全性漏洞及其补救方法。然后，将您的努力集中在对您的系统最关键的区域上。

先决条件和相关信息

使用“iSeries 信息中心”作为查找 iSeries 技术信息的开始点。

可以两种方式访问“信息中心”:

- 从下列 Web 站点:

  `http://www.ibm.com/eserver/iseries/infocenter`

- 从 *《iSeries 信息中心》*，SK3T-4091-04 CD-ROM。此 CD-ROM 随新的 iSeries 硬件或 IBM Operating System/400 软件升级订单而附带。您也可以从 IBM 出版物中心（Publications Center）订购此 CD-ROM:

  `http://www.ibm.com/shop/publications/order`

“iSeries 信息中心”包含新的和更新的 iSeries 信息，例如: 软件和硬件安装、Linux、WebSphere®、Java™、High Availability、数据库、逻辑分区、CL 命令和系统应用程序编程接口（API）。另外，它提供顾问程序和查找程序以帮助计划、故障诊断和配置 iSeries 硬件和软件。

对于每份新硬件订单，您都会接收到*《iSeries 安装与操作 CD-ROM》*，SK3T-4098-02。此 CD-ROM 包含 IBM **@server** IBM e(logo)server iSeries Access for Windows 和 EZ-Setup 向导。iSeries Access Family提供一组强大的客户机和服务器功能，用于将 PC 连接至 iSeries 服务器。EZ-Setup 向导自动执行多种 iSeries 安装任务。

如何发送您的意见

您的反馈对于帮助提供最准确和高质量的信息很重要。如果您对本书或任何其它 iSeries 文档有任何意见，填写本书背面的读者意见表。

1. 如果您更喜欢通过邮件发送意见，使用本书背面印刷的带有地址的读者意见表。如果您从美国之外的国家或地区邮寄读者意见表，则可以将意见表寄往当地的 IBM 分公司或 IBM 代表，由后者支付邮资。
2. 通过电子的形式发送到以下列出的任一网络标识。如果需要答复，请务必提供您完整的网络地址。

因特网: ctscrcf@cn.ibm.com
IBMLink: ibmcn(ctscrcf)

3. 通过传真，请使用以下号码:

   中国: 021-63857881
   其它国家或地区: (86-21)63857881

4. 通过寄送普通邮件到以下地址:

   IBM 中国公司上海分公司，汉化部
   中国上海市淮海中路 333 号瑞安广场 10 楼
   邮政编码: 200021

第 1 部分 基本 iSeries 安全性

第 1 章 iSeries 安全性的基本元素

本主题简要回顾了一起工作以提供 iSeries 安全性的基本元素。在本书的其它部分，我们超出基础来提供用于使用这些安全性元素的技巧以满足您的组织的需要。

安全级别

可以通过设置安全级别（QSECURITY）系统值来选择需要系统实施多大的安全性。系统提供 5 个级别的安全性:

级别 10:

系统不实施任何安全性。不需要密码。如果当某人注册时，指定的用户概要文件在系统上不存在，则系统会创建一个用户概要文件。

注意:

从 V4R3 和以后的发行版开始，您不能将 QSECURITY 系统值设置为 10。如果您的系统当前处于安全级别 10，则当您安装 “版本 4 发行版 3” 时，它将仍处于级别 10。如果将安全级别更改为某个其它值，则您不能将它重新更改为级别 10。因为级别 10 不提供安全性保护，所以 IBM 建议不要使用安全级别 10。**IBM 将不提供对于在安全级别 10 发生的任何问题的支持，除非在更高的安全级别也会引起该问题。**

级别 20:

系统需要用户标识和密码进行注册。安全级别 20 通常称为**注册安全性**。缺省情况下，所有用户可以访问所有对象，因为所有用户都具有 *ALLOBJ 特权。

级别 30:

系统需要用户标识和密码进行注册。用户必须具有权限才能使用对象，因为用户在缺省情况下不具有任何权限。这称为**资源安全性**。

级别 40:

系统需要用户标识和密码进行注册。除资源安全性外，系统还提供**完整性保护**功能。完整性保护功能（如验证操作系统的接口的参数）将保护系统和系统上的对象免遭有经验的系统用户篡改。对于大多数安装，级别 40 是建议的安全级别。当您接收到具有 V4R5 或更高发行版的新 iSeries 系统时，安全级别已设置为 40。

级别 50:

系统需要用户标识和密码进行注册。系统实施级别 40 的资源安全性和完整性保护，但添加**增强型完整性保护**，如在系统状态程序和用户状态程序之间的消息处理的限制。安全级别 50 是为具有较高安全性需求的 iSeries 系统提供的。

注: 级别 50 是 C2 证书（和 FIPS-140 证书）的必需级别。

iSeries Security Reference 一书的 Chapter 2 提供关于安全级别的更多信息并描述如何从一个安全级别移动到另一个安全级别。

全局设置

您的系统具有全局设置，这些设置影响工作如何进入系统以及系统对其它系统用户显示的方式。这些设置包括以下各项:

安全性系统值:

安全性系统值用来控制系统中的安全性。这些值分成 4 个组:

- 一般安全性系统值
- 与安全性相关的其它系统值
- 控制密码的系统值
- 控制审计的系统值

本书中的几个主题讨论特定系统值的安全性隐含。*iSeries Security Reference* 一书中的 Chapter 3 描述所有与安全性相关的系统值。

网络属性:

网络属性控制您的系统如何参与（或选择不参与）具有其它系统的网络中。可以在 *Work Management* 一书中阅读更多关于网络属性的信息。

子系统描述和其它工作管理元素:

工作管理元素确定工作如何进入系统以及该工作在什么环境中运行。本信息中的几个主题讨论某些工作管理值的安全性隐含。*Work Management* 一书提供完整信息。

通信配置:

您的通信配置也影响工作如何进入您的系统。本信息中的几个主题提供当系统参与网络时保护系统的建议。

用户概要文件

每个系统用户**必须**具有一个用户概要文件。您必须创建用户概要文件之后，用户才能注册。用户概要文件也可以用来控制对服务工具（如 DASD 和主存储器转储）的访问。有关更多信息，请参阅第 55 页的『管理服务工具』。

用户概要文件是功能强大且灵活的工具。它控制用户可以执行的操作并定制系统对用户表现的方式。*iSeries Security Reference* 一书描述在用户概要文件中的所有参数。

组概要文件

组概要文件是一种特殊类型的用户概要文件。可以使用组概要文件来为一组用户定义权限，而不是单独对每个用户授予权限。当您通过使用复制概要文件功能来创建单个用户概要文件时，也可以使用组概要文件作为模式，或者如果您使用 “iSeries 导航器”，您可以使用安全策略菜单来编辑用户权限。

在 *iSeries Security Reference* 一书中的 Chapter 5 和 Chapter 7 提供有关计划和使用组概要文件的更多信息。

资源安全性

系统上的资源安全性允许您定义谁可以使用对象以及可以如何使用那些对象。访问对象的能力称为**权限**。当您设置对象权限时，可能需要谨慎授予您的用户足够权限来完成他们的工作，而不是授予他们权限来浏览和更改系统。对象权限给用户授予对特定对象的许可权并可以指定允许用户对对象所执行的操作。可以通过特定的详细用户权限（如添加记录或更改记录）来限制对象资源。系统资源可以用来授予用户对特定的系统定义的权限子集的访问权: *ALL、*CHANGE、*USE 和 *EXCLUDE。

文件、程序、库和目录是最普通的需要资源安全性保护的系统对象，但您可以为系统上的任何单个对象指定权限。

第 5 章，『使用对象权限保护信息资产』讨论在系统上设置对象权限的重要性。*iSeries Security Reference* 一书中的 Chapter 5 描述用于设置资源安全性的选项。

对程序功能的限制访问

当您不具有 iSeries 对象来对程序进行保护时，对程序功能的限制访问使您能够为程序提供安全性。在 V4R3 中添加对程序功能的限制访问支持之前，您可以通过创建权限列表或其它对象并检查对对象的权限以控制对程序功能的访问来实现这一点。现在您可以使用对程序功能的限制访问来更方便地控制对应用程序、应用程序的部件或程序中的功能的访问。

有两种方法可以用来管理用户通过“iSeries 导航器”对应用程序功能的访问。第一种方法使用“应用程序管理”支持:

1. 右键单击包含要更改其访问设置的功能的系统。
2. 选择**应用程序管理**。
3. 如果您位于管理系统上，选择**本地设置**。否则，继续执行下一步骤。
4. 选择一个可管理的功能。
5. 选择**缺省访问**（如果适用）。通过选择此选项，缺省情况下您允许所有用户访问该功能。
6. 选择**所有对象访问**（如果适用）。通过选择此选项，您允许具有所有对象系统特权的所有用户访问此功能。
7. 选择**定制**（如果适用）。使用**定制访问**对话框中的**添加**和**除去**按钮来在**允许的访问**和**拒绝的访问**列表中添加或除去用户或组。
8. 选择**除去定制**（如果适用）。通过选择此选项，您删除所选择功能的任何定制访问。
9. 单击**确定**来关闭**应用程序管理**对话框。

管理用户访问的第二种方法涉及“iSeries 导航器”的“用户和组”支持:

1. 在“iSeries 导航器”中，展开**用户和组**。
2. 选择**所有用户**、**组**或**不在组中的用户**来显示用户和组的列表。
3. 右键单击用户或组并选择**特性**。
4. 单击**功能**。
5. 单击**应用程序**选项卡。
6. 使用此页面来更改用户或组的访问设置。

7. 单击**确定**两次来关闭**特性**对话框。

有关 “iSeries 导航器” 安全性问题的更多信息，请参阅第 134 页的『 “iSeries 导航器” 安全性 』。

如果您是应用程序编写者，可以使用对程序功能 API 的限制访问来执行下列操作:

- 注册某个功能
- 检索关于该功能的信息
- 定义谁可以或不可以使用该功能
- 检查是否允许用户使用该功能

注: 此支持**不**是资源安全性的替代品。对程序功能的限制访问并不阻止用户从另一个接口访问资源（如文件或程序）。

要在应用程序中使用此支持，应用程序供应商在安装应用程序时必须注册功能。已注册的功能对应于应用程序中特定功能的代码块。当用户运行应用程序时，在应用程序调用该代码块之前，应用程序调用该 API。该 API 调用检查用法 API 来查看是否允许用户使用该功能。如果允许用户使用已注册的功能，则运行代码块。如果不允许用户使用该功能，则阻止用户运行代码块。

注: API 涉及在注册数据库（WRKREGINF）中注册 30 个字符的功能标识。尽管没有与由对功能 API 的限制访问所使用的功能标识相关的出口点，但它必须具有出口点。要在注册表中注册任何内容，您**必须**提供出口点格式名称。为此，“注册功能 API” 创建哑元格式名称并对注册的所有功能使用此哑元格式名称。因为这是哑元格式名称，所以未曾调用出口点程序。

系统管理员指定允许或拒绝谁访问某个功能。管理员可以使用 API 来管理对程序功能的访问或使用 “iSeries 导航器” 的 “应用程序管理” GUI。*iSeries server API Reference* 一书提供关于对程序功能 API 的限制访问的信息。有关控制对功能的访问的附加信息，请参阅第 134 页的『 “iSeries 导航器” 安全性 』。

安全性审计

由于下列几个原因，用户需要审计系统的安全性:

- 估计安全性计划是否完成。
- 确保计划的安全性控制到位，且工作正常。此类型的审计通常由安全主管作为日常安全性管理的一部分来执行。它有时也由内部或外部审计员以更详细的方式作为定期安全性复查的一部分来执行。
- 为了确保系统安全性与对系统环境的更改保持同步。影响安全性的更改的一些示例为:
  - 由系统用户创建的新对象
  - 允许进入系统的新用户
  - 对象所有权的更改（未调整权限）
  - 职责的更改（已更改用户组）
  - 临时权限（未及时撤销）
  - 安装的新产品

- 为未来的事件作准备，如安装新的应用程序、移动到更高的安全级别或设置通信网络。

此处描述的技术适合于所有这些情况。审计哪些内容和审计频率取决于您的组织的大小和安全性需求。

安全性审计涉及在您的系统上使用命令和访问作业记录和日志信息。可以创建由执行您的系统的安全性审计的某个人使用的特殊概要文件。审计员概要文件需要 *AUDIT 特权来更改系统的审计特征。在本章中建议的某些审计任务需要具有 *ALLOBJ 和 *SECADM 特权的用户概要文件。当审计周期结束时，将审计员概要文件的密码设置为 *NONE。

有关安全性审计的更多详细信息，请参阅 *Security Reference* 一书的 Chapter 9。

示例: 系统安全性属性报告

图 1 显示“打印系统安全性属性”（PRTSYSSECA）命令的输出示例。该报告显示为具有正常安全性需求的系统建议的与安全性相关的系统值和网络属性的设置。它也显示您的系统上的当前设置。

注: 报告上的*当前值*列显示系统上的当前设置。将此值与建议的值进行比较来查看您在哪里可能具有安全性漏洞。

```
系统安全性属性

系统值
名称            当前值                建议的值
QALWOBJRST      *NONE                 *NONE
QALWUSRDMN      *ALL                  QTEMP
QATNPGM         QEZMAIN   QSYS        *NONE
QAUDENDACN      *NOTIFY               *NOTIFY
QAUDFRCLVL      *SYS                  *SYS
QAUDCTL         *AUDLVL               *AUDLVL   *OBJAUD
QAUDLVL         *SECURITY             *AUTFAIL  *CREATE
                                      *DELETE   *SECURITY
                                      *SAVRST   *NOQTEMP
```

图 1. 系统安全性属性报告 - 样本 (1/4)

```
QAUTOCFG        0                     0
QAUTORMT        1                     0
QAUTOVRT        9999                  0
QCMNRCYLMT      0 0                   0 0
QCRTAUT         *CHANGE               在库级别上控制。
QCRTOBJAUD      *NONE                 在库级别上控制。
QDEVRCYACN      *DSCMSG               *DSCMSG
QDSCJOBITV      120                   120
QDSPSGNINF      1                     1
QINACTITV       60                    60
QINACTMSGQ      *ENDJOB               *ENDJOB
QLMTDEVSSN      0                     1
QLMTSECOFR      0                     1
QMAXSGNACN      2                     3
QMAXSIGN        3                     3
```

图 1. 系统安全性属性报告 - 样本 (2/4)

```
QPWDEXPITV      60                  60
QPWDLMTAJC      1                   1
QPWDLMTCHR      *NONE               AEIOU@$#
QPWDLMTREP      1                   2
QPWDLVL         0
QPWDMAXLEN      8                   8
QPWDMINLEN      6                   6
QPWDPOSDIF      1                   1
QPWDRQDDGT      1                   1
QPWDRQDDIF      0                   1
QPWDVLDPGM      *NONE               *NONE
QRETSVRSEC      0                   0
QRMTIPL         0                   0
QRMTSIGN        *FRCSIGNON          *FRCSIGNON
QSECURITY       50                  50
QSHRMEMCTL      1                   0
QSRVDMP         *DMPUSRJOB          *NONE
QUSEADPAUT      *NONE               CRTAUTL AUTL(QUSEADPAUT) AUT(*EXCLUDE)
                                    CHGOBJOWN OBJ(QUSEADPAUT) OBJTYPE(*AUTL)
                                    CHGSYSVAL SYSVAL(QUSEADPAUT) VALUE(QUSEADPAUT)
QVFYOBJRST      1                   3
```

图 1. 系统安全性属性报告 - 样本 (3/4)

系统安全性属性

网络属性

名称	当前值	建议的值
DDMACC	*OBJAUT	*REJECT
JOBACN	*FILE	*REJECT
PCSACC	*OBJAUT	*REJECT

图 1. 系统安全性属性报告 - 样本 (4/4)

第 2 章 iSeries 安全性向导和 eServer Security Planner

“iSeries 服务器安全性向导” 和 “eServer Security Planner” 工具可以帮助您确定哪些安全性值会对 iSeries 服务器生效。使用 “iSeries 导航器” 中的 “iSeries 服务器安全性向导”，将根据选择的回答产生反映安全性需要的报告。然后可以使用它来配置您的系统安全性。

使用 “iSeries 安全性向导” 或 “eServer Security Planner” 帮助您计划和实现 iSeries 服务器的基本安全策略。两个工具的目标是使您更易于在您的系统上实现和管理安全性。向导（可作为 OS/400® 的一部分获得）询问您关于您的服务器环境的几个高级别问题并根据您的回答，为您提供向导可以立即应用于您的系统的一组建议。

“eServer Security Planner” 是在线版的 “安全性向导”。它允许您根据安全性需要做出选择并提供报告，就保护站点所需的功能提出建议。

“eServer Security Planner” 是一种基于 Web 版本的向导。它提供用于在您的系统上实现安全性的建议，正如向导所完成的那样。但是，顾问程序不适用于建议。相反，根据对顾问程序的问题的回答，它输出在您的系统上应该应用的系统安全性值和其它属性的列表。

安全性向导

决定对您的企业应该使用哪些 iSeries 安全性系统值可能很复杂。如果您不熟悉 iSeries 服务器上的安全性实现，或运行 iSeries 服务器的环境最近已更改，“安全性向导” 可以帮助您做出决定。

什么是向导?

- 向导是一种工具，设计成由初学者用户运行来安装或配置系统上的某些内容。
- 向导通过询问问题来提示用户输入信息。对每个问题的响应确定下一步询问什么问题。
- 当向导询问完所有问题时，为用户提供一个完成对话框。用户然后按**完成**按钮来安装和配置该项。

安全性向导目标

“安全性向导” 的目标是根据用户的响应配置下列内容。

- 与安全性相关的系统值和网络属性。
- 用于监控系统的与安全性相关的报告。
- 生成 “管理员信息报告” 和 “用户信息报告”：
  - “管理员信息报告” 包含建议的安全性设置和在使建议生效之前应该遵循的任何过程。
  - “用户信息报告” 包含可以用于商业安全策略的信息。例如，密码组合规则包括在此报告中。
- 为系统上的各种与安全性相关的项提供建议的设置。

安全性向导目标

- “安全性向导” 的目标是:

  - 根据用户对向导的问题的回答确定系统安全性设置应该是什么，然后实现这些设置（如果合适的话）。
  - 向导生成包含下列内容的详细信息报告。
    - 说明“向导”的建议的报告。
    - 详细列举在实现之前应该遵循的过程的报告。
    - 列示要分发到系统中用户的相关信息的报告。
- 这些项使基本的安全策略在您的系统上生效。
- 向导建议您应该调度定期运行的审计日志报告。当调度时，这些报告有助于:
  - 确保遵循安全策略。
  - 确保仅具有您的批准时才更改安全策略。
  - 调度报告来监控在您的系统上与安全性相关的事件。
- 向导允许您保存建议或将某些或所有建议应用于您的系统。

注: 在同一系统上可以多次使用“安全性向导”以允许可能具有较早安装的用户复查他们的当前安全性。可以从 V3R7 系统（当引入“iSeries 导航器”时）向上使用“安全性向导”。

要使用“iSeries 导航器”，必须已将 IBM iSeries Access for Windows® 安装在您的 Windows 95/NT PC 并从此 PC 连接至 iSeries 服务器。必须将“向导”的用户连接至 iSeries 服务器。用户的用户标识必须具有 *ALLOBJ、*SECADM、*AUDIT 和 *IOSYSCFG 特权。有关将 Windows 95/NT PC 连接至 iSeries 系统的帮助，查阅在信息中心中的 IBM iSeries Access for Windows 主题（有关详细信息，请参阅第 xii 页的『先决条件和相关信息』）。

要访问“安全性向导”，执行下列操作:

1. 在“iSeries 导航器”中，展开您的服务器。
2. 右键单击**安全性**并选择**配置**。
   - 当用户启动“iSeries 导航器”的**安全性**选项时，将请求发送至 iSeries 服务器来检查用户的特权。
   - 如果用户不具有所有必需的特权（*ALLOBJ、*AUDIT、*IOSYSCFG 和 *SECADM），则他们将看不到**配置**选项并将无法访问“安全性向导”。
3. 假定用户具有必需的权限:
   - 检索先前的向导响应。
   - 检索当前的安全性设置。

“安全性向导”将为您提供三个欢迎屏幕之一：您看到哪个屏幕取决于存在下列哪种情况:

- 从未对目标 iSeries 服务器运行向导。
- 以前运行了向导但延迟了安全性更改。
- 以前运行了向导并且已使安全性更改生效。

如果您未使用“iSeries 导航器”，您仍可以在计划安全性需求时获取帮助。eServer Security Planner 是一种在线版的“安全性向导”，略有差别。顾问程序将不自动配置您的系统。然而，它将根据您的回答生成建议的安全性选项的报告。要访问“eServer Security Planner”，请访问 eServer 信息中心:

`http://publib.boulder.ibm.com/eserver/`

eServer Security Planner

“eServer Security Planner” 是一种在线版的 “安全性向导”。它询问与 “安全性向导” 相同的问题并根据您的回答生成相同的建议。这两个工具间的主要差别是:

- “eServer Security Planner” **不会** –
  - 生成报告。
  - 将当前设置与建议设置比较。
  - 自动设置任何系统值。
- 不能从 “eServer Security Planner” 获得建议。

“eServer Security Planner” 生成 CL 程序，您可以剪贴及编辑此程序供自己使用以自动实现安全性配置。您也可以从 “eServer Security Planner” 直接链接到 iSeries 服务器文档。这提供了关于系统值或报告的信息，它可以帮助您确定此设置是否适用于您的环境。

要访问 “eServer Security Planner”，将因特网浏览器指向下列 URL:

`http://publib.boulder.ibm.com/eserver/`

第 3 章 控制交互式注册

当您考虑限制您的系统的入口时，从明显的“注册”屏幕开始。以下是您可以用来使某个人很难通过使用“注册”屏幕来注册到您的系统的选项。

设置密码规则

要保护您的系统注册，执行下列操作:
- 设置一种策略，该策略表明密码不能是平常的且不得共享。
- 设置系统值来帮助您实施。表 1 显示建议的系统值设置。

在表 1 中的值的组合相当受限制，旨在显著减少平常密码的可能性。然而，您的用户可能发现选择满足这些限制的密码很难且感到灰心。

考虑为用户提供下列内容:
1. 密码的条件列表。
2. 有效密码和无效密码示例。
3. 关于如何想出好密码的建议。

运行“配置系统安全性”（CFGSYSSEC）命令来 设置这些值。使用“打印系统安全性属性”（PRTSYSSECA）命令 来打印这些系统值的当前设置。

iSeries Security Reference 一书的 Chapter 3。第 32 页的『由“配置系统安全性”命令设置的值』提供关于 CFGSYSSEC 命令的更多信息。

表 1. 密码的系统值

系统值名称	描述	建议的值
QPWDEXPITV	系统用户必须更改他们的密码的频率。可以在用户概要文件中为单个用户指定不同的值。	60（天）
QPWDLMTAJC	系统是否阻止相同的相邻字符。	1（是）
QPWDLMTCHR	在密码中不可以使用什么字符。[2]	AEIOU#$@
QPWDLMTREP	系统是否阻止相同字符在密码中出现多次。	2（不允许连续出现）
QPWDLVL	是将用户概要文件密码限制为 10 个字符还是最大值 128。	0[3]
QPWDMAXLEN	在密码中字符的最大数目。	8
QPWDMINLEN	在密码中字符的最小数目。	6
QPWDPOSDIF	在密码中的每个字符是否必须与在先前密码中的同一位置中的字符不同。	1（是）
QPWDRQDDGT	密码是否必须至少具有一个数字字符。	1（是）
QPWDRQDDIF	用户必须等待多长时间之后，才可以再次使用同一密码。[2]	5 个或更少的（到期时间间隔）[1]
QPWDVLDPGM	调用什么出口程序来验证新指定的密码。	*NONE

注:

1. QPWDEXPITV 系统值指定必须更改密码的频率，如每隔 60 天一次。这是**到期时间间隔**。QPWDRQDDIF 系统值指定必须经过多少到期时间间隔之后，才能再次使用同一密码。 *iSeries Security Reference* 一书的 Chapter 3 提供有关这些系统值如何共同起作用的更多信息。
2. 未在密码级别 2 或 3 实施 QPWDLMTCHR。有关详细信息，请参阅第 14 页的『密码级别』。
3. 参阅第 14 页的『计划密码级别更改』来确定适合于您的需求的密码级别。

密码级别

从操作系统的 V5R1 开始，QPWDLVL 系统值提供增强的密码安全性。在前发行版中，用户限制于长度不超过 10 个字符的密码，这些字符在受限制的字符范围内。现在，用户可以根据设置他们的系统的密码级别来选择具有多达 128 个字符的密码（或密码短语）。密码级别为:

- **级别 0**: 系统是在此级别交付的。在级别 0，密码长度不超过 10 个字符，仅包含 A-Z、0–9、#、@、$ 和 _ 字符。在级别 0 的密码不及在更高密码级别上的那些密码安全。
- **级别 1**: 与密码级别 0 的规则相同，但不保存 Windows 网上邻居的 “iSeries 支持”（以后称为 iSeries NetServer）的密码。
- **级别 2**: 密码在此级别上是安全的。此级别可以用于测试目的。如果密码是 10 个字符或小于 10 个字符并使用级别 0 或 1 密码的字符集，则为级别 0 或 1 的用户保存密码。在此级别的密码（或密码短语）具有下列特征:
  - 长度最多可有 128 个字符。
  - 包括任何可用的键盘字符。
  - 不可以完全由空格组成；从密码末尾除去空格。
  - 区分大小写。
- **级别 3**: 在此级别上的密码最安全并利用可用的最高级的加密算法。此级别与级别 2 的密码具有相同的特征。在此级别上不保存 iSeries NetServer 的密码。

仅当在您的网络中的每个系统满足以下条件时，才应该使用密码级别 2 和 3:

- 操作系统是 V5R1 或更高版本
- 密码级别设置为 2 或 3

同样，用户必须全部使用相同的密码级别登录。密码级别是全局的；用户不能选择他们要保护其密码的级别。

计划密码级别更改

应该仔细计划更改密码级别。如果您未充分计划密码级别更改，则其它系统的操作可能失败或用户可能无法注册到系统。在更改 QPWDLVL 系统值之前，确保您使用 SAVSECDTA 或 SAVSYS 命令保存了您的安全性数据。如果您具有当前备份，则当您需要返回至较低的密码级别时，您将能够为所有用户的概要文件复位密码。

当将密码级别（QPWDLVL）系统值设置为 2 或 3 时，在系统上和在系统所连接的客户机上使用的产品可能有问题。必须升级以加密格式而不是以用户在注册屏幕上输入的明文格式将密码发送至系统的任何产品或客户机才能使用 QPWDLVL 2 或 3 的新密码加密规则。发送加密密码称为**密码替换**。

密码替换用来阻止在通过网络传输期间捕获密码。将不接受由较早的不支持 QPWDLVL 2 或 3 的新算法的客户机生成的密码替换，即使特定的字符是正确的。这也适用于利用加密值从一个系统对另一个系统进行认证的任何 iSeries 到 iSeries 对等访问。

由于某些受影响的产品（如 Java 工具箱）是作为中间件提供的这样的事实使问题更加复杂。在使用中间件的更新版本重新构建之后，合并这些产品之一的先前版本的第三方产品才将正常工作。

给出了各种各样的方案，容易看出在更改 QPWDLVL 系统值之前为什么有必要仔细计划。

将 QPWDLVL 从 0 更改为 1 的注意事项

密码级别 1 允许不需要与 Windows 网上邻居的 “Windows 95/98/ME AS/400® 客户机支持”（iSeries NetServer）产品通信的系统从系统中删除 iSeries NetServer 密码。从系统删除不必要的加密密码会增加系统的整体安全性。

在 QPWDLVL 1 上，所有当前的 V5R1 前的密码替换和密码认证机制将继续起作用。除对需要 iSeries NetServer 密码的功能和服务之外，很少有可能破坏。

将 QPWDLVL 从 0 或 1 更改为 2 的注意事项

密码级别 2 引入长度多达 128 个字符的区分大小写密码的使用（也称为密码短语）并提供最大能力来回复到 QPWDLVL 0 或 1。

不管系统的密码级别如何，当更改密码或用户注册到系统时，会创建密码级别 2 和 3 的密码。当系统仍处于密码级别 0 或 1 时创建级别 2 和 3 的密码有助于为更改为密码级别 2 或 3 作准备。

在将 QPWDLVL 更改为 2 之前，您应该使用 DSPAUTUSR 或 PRTUSRPRF TYPE(*PWDINFO) 命令来定位不具有在密码级别 2 上可使用的密码的所有用户概要文件。根据这些命令所定位的那些概要文件，您可能需要使用下列机制之一来将密码级别 2 和 3 的密码添加至概要文件。

- 使用 CHGUSRPRF 或 CHGPWD CL 命令或 QSYCHGPW API 为用户概要文件更改密码。这将导致系统更改在密码级别 0 和 1 可使用的密码；并且系统还创建在密码级别 2 和 3 可使用的两个等价的区分大小写的密码。创建全部大写和全部小写版本的密码以供在密码级别 2 或 3 使用。

  例如，将密码更改为 C4D2RB4Y 导致系统生成 C4D2RB4Y 和 c4d2rb4y 密码级别 2 的密码。
- 通过以明文格式提供密码的机制（不使用密码替换）注册到系统。如果密码有效但用户概要文件不具有在密码级别 2 和 3 可使用的密码，则系统创建在密码级别 2 和 3 可使用的两个等价的区分大小写的密码。创建密码的全部大写和全部小写版本以供在密码级别 2 或 3 使用。

当用户概要文件也不具有在密码级别 0 和 1 可使用的密码时或当用户通过使用密码替换的产品尝试注册时，没有在密码级别 2 或 3 可使用的密码可能是一个问题。在这些情况下，当将密码级别更改为 2 时，用户将不能注册。

如果用户概要文件不具有在密码级别 2 和 3 可使用的密码，用户概要文件具有在密码级别 0 和 1 可使用的密码，该用户通过发送明文密码的产品注册，则系统根据密码级别 0 密码验证该用户并为该用户概要文件创建两个密码级别 2 密码（如上所述）。将根据密码级别 2 密码验证后续注册。

如果未将使用密码替换的任何客户机／服务更新为使用新密码（密码短语）替换方案，则该客户机在 QPWDLVL 2 上将不会正常工作。管理员应该检查未更新为新密码替换方案的客户机／服务是否是必需的。

使用密码替换的客户机 / 服务包括:

- TELNET
- iSeries Access
- iSeries 主机服务器
- QFileSrv.400
- iSeries NetServer 打印支持
- DDM
- DRDA®
- SNA LU6.2

强烈建议在更改为 QPWDLVL 2 之前，保存安全性数据。这可以有助于使转换回 QPWDLVL 0 或 1 更容易（如果这有必要）。

建议在 QPWDLVL 2 上执行某些测试之后再更改其它密码系统值，如 QPWDMINLEN 和 QPWDMAXLEN。这将使得易于转换回 QPWDLVL 1 或 0（如果有必要）。然而，在 QPWDVLDPGM 系统值必须指定 *REGFAC 或 *NONE 之后，系统才将允许将 QPWDLVL 更改为 2。因此，如果您使用密码验证程序，您可能希望为 QIBM_QSY_VLD_PASSWRD 出口点编写可以通过使用 ADDEXITPGM 命令注册的新的密码验证程序。

iSeries NetServer 密码在 QPWDLVL 2 仍受支持，因此需要 iSeries NetServer 密码的任何功能 / 服务仍可正常工作。

一旦管理员对于在 QPWDLVL 2 上运行系统感到舒适，他们就可以开始更改密码系统值来使用较长的密码。然而，管理员需要了解较长的密码将具有以下影响:

- 如果指定大于 10 个字符的密码，将清除密码级别 0 和 1。如果将系统返回至密码级别 0 或 1，此用户概要文件将无法注册。
- 如果密码包含特殊字符或不遵循简单对象名称的组合规则（不包括区分大小写），则清除密码级别 0 和 1 密码。
- 如果指定大于 14 个字符的密码，则清除用户概要文件的 iSeries NetServer 密码。
- 密码系统值仅适用于新的密码级别 2 值而不适用于系统生成的密码级别 0 和 1 密码或 iSeries NetServer 密码值（如果生成的话）。

将 QPWDLVL 从 2 更改为 3 的注意事项

在 QPWDLVL 2 上运行一段时间系统之后，管理员考虑移动至 QPWDLVL 3 来最大化他的密码安全性保护。

在 QPWDLVL 3 上，清除所有 iSeries NetServer 密码，因此在没有必要使用 iSeries NetServer 密码之前，不应该将系统移动至 QPWDLVL 3。

在 QPWDLVL 3 上，清除所有密码级别 0 和 1 密码。管理员可以使用 DSPAUTUSR 或 PRTUSRPRF 命令来定位不具有与其关联的密码级别 2 或 3 密码的用户概要文件。

更改为较低密码级别

并不期望返回至较低的 QPWDLVL 值（在可能时）是完全不费力的操作。一般情况下，想象设置应该是从较低 QPWDLVL 值到较高 QPWDLVL 值的单向操作。然而，可能有必须恢复较低的 QPWDLVL 值的情况。

以下各节讨论移动到较低密码级别所需要的工作。

从 QPWDLVL 3 更改为 2 的注意事项: 此更改相对容易。一旦将 QPWDLVL 设置为 2，管理员需要确定是否要求任何用户概要文件包含 iSeries NetServer 密码或密码级别 0 或 1 密码，如果这样，将用户概要文件的密码更改为允许的值。

此外，可能必须将密码系统值更改回与 iSeries NetServer 和密码级别 0 或 1 密码兼容的值（如果需要那些密码）。

从 QPWDLVL 3 更改为 1 或 0 的注意事项: 由于很可能为系统带来问题（类似因为清除了所有的密码级别 0 和 1 密码，用户都不可以注册），此更改不直接受支持。要从 QPWDLVL 3 更改为 QPWDLVL 1 或 0，系统必须首先进行中间更改，更改为 QPWDLVL 2。

从 QPWDLVL 2 更改为 1 的注意事项: 在将 QPWDLVL 更改为 1 之前，管理员应该使用 DSPAUTUSR 或 PRTUSRPRF TYPE(*PWDINFO) 命令来定位不具有密码级别 0 或 1 密码的任何用户概要文件。如果在更改 QPWDLVL 之后用户概要文件将需要密码，管理员应该确保使用下列机制之一为概要文件创建密码级别 0 和 1 密码:

- 使用 CHGUSRPRF 或 CHGPWD CL 命令或 QSYCHGPW API 为用户概要文件更改密码。这将导致系统更改在密码级别 2 和 3 上可使用的密码；并且系统还创建在密码级别 0 和 1 上可使用的等价大写密码。仅当满足下列条件时，系统才能够创建密码级别 0 和 1 密码。
  - 密码长度为 10 个字符或小于 10 个字符。
  - 可以将密码转换为大写 EBCDIC 字符 A-Z、0-9、@、#、$ 和下划线。
  - 密码不以数字或下划线字符开始。

  例如，将密码更改为值 RainyDay 将导致系统生成密码级别 0 和 1 密码 RAINYDAY。但是将密码值更改为 Rainy Days In April 将导致系统清除密码级别 0 和 1 密码（因为该密码太长并且它包含空格）。

  即使无法创建密码级别 0 或 1 密码，也不生成消息或指示。
- 通过以明文格式提供密码的机制（不使用密码替换）注册到系统。如果密码有效但用户概要文件不具有在密码级别 0 和 1 上可使用的密码，则系统创建在密码级别 0 和 1 上可使用的等价大写密码。仅当满足以上列示的条件时，系统才能够创建密码级别 0 和 1 密码。

管理员然后可以将 QPWDLVL 更改为 1。当 QPWDLVL 1 更改生效（下次 IPL）时，清除所有 iSeries NetServer 密码。

从 QPWDLVL 2 更改为 0 的注意事项: 除当更改生效时保留所有 iSeries NetServer 密码外，注意事项与从 QPWDLVL 2 更改为 1 相同。

从 QPWDLVL 1 更改为 0 的注意事项: 在将 QPWDLVL 更改为 0 之后，管理员应该使用 DSPAUTUSR 或 PRTUSRPRF 命令来定位不具有 iSeries NetServer 密码的任何用户概要文件。如果该用户概要文件需要 iSeries NetServer 密码，则可以通过更改用户的密码或通过以明文格式提供密码的机制注册来创建它。

管理员然后可以将 QPWDLVL 更改为 0。

更改已知密码

执行下列操作来关闭进入到在您的系统中可能存在的 iSeries 服务器的某些公认的入口。

__ 步骤 1. 确保没有用户概要文件仍具有缺省密码（等于用户概要文件名称）。可以使用“分析缺省密码”（ANZDFTPWD）命令。（请参阅第 22 页的『避免缺省密码』。）

__ 步骤 2. 尝试使用在表 2 中显示的用户概要文件和密码的组合注册到您的系统。这些密码是公开的，并且它们是尝试闯入您的系统的任何人的第一密码。如果您可以注册，使用“更改用户概要文件”（CHGUSRPRF）命令来将该密码更改为建议的值。

__ 步骤 3. 启动“专用服务工具”（DST）并尝试使用在表 2 中显示的密码注册。参阅 iSeries 信息中心—>安全性—>服务工具。有关访问“iSeries 信息中心”的信息，请参阅第 xii 页的『先决条件和相关信息』。

__ 步骤 4. 如果您可以使用这些密码中的任何一个注册到 DST，则应该更改这些密码。“iSeries 信息中心—>安全性—>服务工具”提供有关如何更改服务工具用户标识和密码的详细指示信息。有关访问“iSeries 信息中心”的信息，请参阅第 xii 页的『先决条件和相关信息』。

__ 步骤 5. 最后，确保仅通过在“注册”屏幕上按“执行”键而不输入用户标识和密码无法注册。尝试几种不同的屏幕。如果您可以注册而不需要在“注册”屏幕上输入信息，则执行下列操作之一：

- 更改为安全级别 40 或 50（QSECURITY 系统值）。

  注: 当您将安全级别增加至 40 或 50 时，您的应用程序可能以不同方式运行。

- 将交互子系统的所有工作站输入更改为指向指定 USER(*RQD) 的作业描述。

表 2. IBM 提供的概要文件的密码

用户标识	密码	建议的值
QSECOFR	QSECOFR[1]	仅安全管理员知道的非平常的值。**写下您选择的密码并将它存储在安全位置。**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2, 3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

注:

1. 系统到达时，QSECOFR 的“*将密码设置为到期*”值设置为 *YES。第一次注册到新系统时，必须更改 QSECOFR 密码。
2. 系统需要这些用户概要文件以获取系统功能，但您不应该允许用户使用这些概要文件注册。对于安装了 V3R1 或更高发行版的新系统，此密码的出厂交付值为 *NONE。

   当您运行 CFGSYSSEC 命令时，系统将这些密码设置为 *NONE。
3. 要使用 TCP/IP 运行 iSeries Access for Windows，必须启用 QUSER 用户概要文件。

表 3. 专用服务工具的密码

DST 级别	用户标识[1]	密码	建议的值
基本能力	11111111	11111111	仅安全管理员知道的非平常的值。[2]
全部能力	22222222	22222222[3]	仅安全管理员知道的非平常的值。[2]
安全性能力	QSECOFR	QSECOFR[3]	仅安全管理员知道的非平常的值。[2]
服务能力	QSRV	QSRV[3]	仅安全管理员知道的非平常的值。[2]

注:

1. 用户标识仅对于操作系统的 PowerPC® AS（RISC）发行版是必需的。
2. 如果您的硬件服务代表需要使用此用户标识和密码注册，则在硬件服务代表离开后将密码更改为新值。
3. 服务工具用户概要文件将在第一次使用它时到期。

注: 只能通过已认证的设备更改 DST 密码。这对于相同的所有密码和对应的用户标识也是如此。有关已认证的设备的更多信息，请参阅 “iSeries 信息中心” 中的 “操作控制台” 设置信息。

设置注册值

表 4 显示几个值，您可以设置它们来使未授权用户更加难以注册到您的系统。如果您运行 CFGSYSSEC 命令，它将这些系统值设置为建议的设置。您可以在 *iSeries Security Reference* 一书的 Chapter 3 中阅读有关这些系统值的更多信息。

表 4. 注册系统值

系统值名称	描述	建议的设置
QAUTOCFG	系统是否自动配置新设备。	0（否）
QAUTOVRT	如果没有设备可用，系统将自动创建的虚拟设备描述数。	0
QDEVRCYACN	当设备在发生错误之后重新连接时系统执行的操作。[1]	*DSCMSG
QDSCJOBITV	在结束已断开连接的作业之前系统等待的时间。	120
QDSPSGNINF	当用户注册时，系统是否显示关于先前注册活动的屏幕信息。	1（是）
QINACTITV	当交互式作业不活动时，在执行操作之前系统等待的时间。	60
QINACTMSGQ	当达到 QINACTITV 时间周期时系统执行的操作。	*ENDJOB
QLMTDEVSSN	系统是否阻止一个用户同时在多个工作站上注册。	1（是）
QLMTSECOFR	具有 *ALLOBJ 或 *SERVICE 特权的用户是否只能在特定工作站上注册。	1（是）[2]
QMAXSIGN	连续不正确注册的最大尝试次数（用户概要文件或密码不正确）。	3
QMAXSGNACN	当达到 QMAXSIGN 限制时，系统执行的操作。	3（禁用用户概要文件和设备）

表 4. 注册系统值 (续)

系统值名称	描述	建议的设置
注: 1. 当显式指定 TELNET 会话的设备描述时，系统可以断开连接并重新连接 TELNET 会话。 2. 如果将系统值设置为 1（是），将需要显式授权对设备具有 *ALLOBJ 或 *SERVICE 特权的用户。执行此操作的最简单的方法是授予 QSECOFR 用户概要文件对特定设备的 *CHANGE 权限。		

更改注册错误消息

黑客想知道他们何时能够对闯入系统取得进步。当“注册”屏幕上的错误消息显示密码不正确时，黑客可以假定该用户标识是正确的。可以通过使用“更改消息描述”（CHGMSGD）命令更改两个注册错误消息的文本来阻止黑客。表 5 显示建议的文本。

表 5. 注册错误消息

消息标识	交付的文本	建议的文本
CPF1107	CPF1107 - 用户概要文件的密码不正确。	注册信息不正确 **注:** 不要在消息文本中包括消息标识。
CPF1120	CPF1120 - 用户 XXXXX 不存在。	注册信息不正确。 **注:** 不要在消息文本中包括消息标识。

调度用户概要文件的可用性

您可能想要某些用户概要文件仅在一天的某些时间或一周的某些天中可用于注册。例如，如果您为安全性审计员设置了概要文件，您可能想要仅在安排审计员工作的时间期间启用该用户概要文件。也可能想要在业余时间期间禁用具有 *ALLOBJ 特权的用户概要文件（包括 QSECOFR 用户概要文件）。

可以使用“更改激活调度项”（CHGACTSCDE）命令来将用户概要文件设置为自动启用和 禁用。对于需要调度的每个用户概要文件，创建一个定义该用户概要文件的调度的项。

例如，如果需要 QSECOFR 概要文件仅在上午 7 点和晚上 10 点之间可用，您将在 CHGACTSCDE 屏幕上输入下列内容:

```
                更改激活调度项（CHGACTSCDE）

输入选项并按“执行”键。

用户概要文件 . . . . . > QSECOFR       名称
启用时间 . . . . . > '7:00'        时间，*NONE
禁用时间 . . . . . > '22:00'       时间，*NONE
星期几 . . . . . > *MON          *ALL，*MON，*TUE，*WED...
                                > *TUE
                                > *WED
                                > *THU
                      + 获取更多值 > *FRI
```

图 2. 调度概要文件激活屏幕 – 样本

实际上，您可能需要让 QSECOFR 概要文件仅在每天的很有限的几个小时内可用。可以使用具有 *SECOFR 类的另一个用户概要文件来执行大多数系统功能。因此，应避免将公认的用户概要文件暴露在攻击之下。

可以定期使用“显示审计日志项”（DSPAUDJRNE）命令来打印 CP （更改概要文件）审计日志项。使用这些项来验证系统是否根据您计划的调度来启用和禁用用户概要文件。

检查以确保正在根据您计划的调度禁用用户概要文件的另一个方法是使用“打印用户概要文件”（PRTUSRPRF）命令。当为报告类型指定 *PWDINFO 时，报告包括每个所选用户概要文件的状态。例如，如果您定期禁用具有 *ALLOBJ 特权的所有用户概要文件，则在禁用概要文件之后，您可以调度下列命令来立即运行:

```
PRTUSRPRF TYPE(*PWDINFO) SELECT(*SPCAUT) SPCAUT(*ALLOBJ)
```

除去不活动用户概要文件

您的系统应该仅包含需要的用户概要文件。如果由于用户已离开或在组织中执行另一个作业，所以不再需要用户概要文件，则除去该用户概要文件。如果某个人长期从组织离开，则禁用（取消激活）该用户的概要文件。不必要的用户概要文件可能提供对您的系统的未授权的入口。

自动禁用用户概要文件

可以使用“分析概要文件活动”（ANZPRFACT）命令来定期禁用在指定的天数中已不活动的用户概要文件。当您使用 ANZPRFACT 命令时，指定系统查找的不活动天数。系统查看用户概要文件的上次使用日期、恢复日期和创建日期。

一旦您为 ANZPRFACT 命令指定了某个值，系统就在每周下午 1 点调度一个作业来运行（从您第一次指定了值之后的那一天开始）。该作业检查所有概要文件并禁用不活动概要文件。您不需要再次使用 ANZPRFACT 命令，除非您需要更改不活动天数。

可以使用“更改活动概要文件列表”（CHGACTPRFL）命令来使某些概要文件免除 ANZPRFACT 处理。CHGACTPRFL 命令创建 ANZPRFACT 命令将不禁用的用户概要文件列表，不管那些概要文件已多长时间不活动。

当系统运行 ANZPRFACT 命令时，它在禁用的每个用户概要文件的审计日志中写入一个 CP 项 。可以使用 DSPAUDJRNE 命令来列示最近禁用的用户概要文件。

注: 仅当 QAUDCTL 值指定 *AUDLVL 且 QAUDLVL 系统值指定 *SECURITY 时，系统才写入审计项。

检查以确保正在根据您计划的调度禁用用户概要文件的另一个方法是使用“打印用户概要文件”（PRTUSRPRF）命令。当为报告类型指定 *PWDINFO 时，报告包括每个所选用户概要文件的状态。

自动除去用户概要文件

可以使用“更改到期调度项”（CHGEXPSCDE）命令来管理用户概要文件的除去或禁用 。如果您知道某个用户将长期离开，您可以调度除去或禁用该用户概要文件。

第一次使用 CHGEXPSCDE 命令时，它创建一个作业调度项，它在每天的午夜后 1 分钟运行。该作业查看 QASECEXP 文件来确定是否调度任何用户概要文件以用于在那天除去。

使用 CHGEXPSCDE 命令，可禁用或删除用户概要文件。如果您选择删除用户概要文件，则您必须指定系统将对该用户拥有的对象执行什么操作。在调度用户概要文件以用于删除之前，需要研究该用户拥有的对象。例如，如果该用户拥有沿用权限的程序，您是否要那些程序沿用新所有者的所有权？或者，新的所有者是否比必需的具有更多权限（如特权）？或许，您需要创建具有特定权限的新用户概要文件来拥有需要沿用权限的程序。

也需要研究如果删除用户概要文件，是否将发生任何应用程序问题。例如，是否任何作业描述指定该用户概要文件作为缺省用户？

可以使用“显示到期调度”（DSPEXPSCD）命令来显示调度要禁用或除去的概要文件列表。

可以使用“显示授权用户”（DSPAUTUSR）命令来列示您的系统上的所有用户概要文件。使用“删除用户概要文件”（DLTUSRPRF）命令来删除过期的概要文件。

安全性注意: ： 您通过将用户概要文件的状态设置为 *DISABLED 来禁用用户概要文件。当禁用用户概要文件时，您使它不可用于交互式使用。不能使用禁用的用户概要文件注册或将您的作业更改到禁用的用户概要文件。批处理作业可以在禁用的用户概要文件之下运行。

避免缺省密码

当您创建新的用户概要文件时，缺省值是使密码与用户概要文件名称相同。如果某个人了解用于指定概要文件名称的策略并知道新的用户正在加入您的组织，这为某个人进入您的系统提供了机会。

当您创建新的用户概要文件时，考虑指定唯一的非平常的密码，而不要使用缺省密码。将该密码秘密告诉新用户，如在概述您的安全策略的“欢迎使用系统”的信中。通过将用户概要文件设置为 PWDEXP(*YES) 来要求用户在第一次用户注册时更改密码。

可以使用“分析缺省密码”（ANZDFTPWD）命令来检查在系统上的所有用户概要文件以获取缺省密码。 当您打印报告时，您可以选择指定如果密码与用户概要文件名称相同，则系统应该执行操作（如禁用用户概要文件）。ANZDFTPWD 命令打印它找到的概要文件列表和它执行的任何操作。

注: 密码以单向加密格式存储在您的系统中。不能解密它们。系统加密指定的密码并将它与存储的密码比较，正如它在您注册系统时将检查密码一样。如果您正在审计权限故障（*AUTFAIL），则系统将为不具有缺省密码的每个用户概要文件写入 PW 审计日志项（对于运行 V4R1 或更早发行版的系统）。从 V4R2 开始，当您运行 ANZDFTPWD 命令时，系统不写入 PW 审计日志项。

监控注册和密码活动

如果您关心进入您的系统的未授权尝试，可以使用 PRTUSRPRF 命令来帮助您 监控注册和密码活动。

以下是使用此报告的几个建议:

- 确定某些用户概要文件的密码到期时间间隔是否比系统值长以及是否调整较长的到期时间间隔。例如，在报告中，USERY 具有 120 天的密码到期时间间隔。
- 定期运行此报告来监控未成功的注册尝试。正尝试闯入您的系统的某个人可能知道系统在一定数量的未成功的尝试之后执行操作。每天晚上，准备闯入系统的闯入者可能尝试比您的 QMAXSIGN 值少的次数以免提醒您注意这些尝试。然而，如果您在每天早晨早点运行此报告并注意到某些概要文件经常具有未成功的注册尝试，则您可以怀疑您遇到了问题。
- 标识长时间未使用或其密码长时间未更改的用户概要文件。

存储密码信息

要支持某些网络功能和通信需求，iSeries 服务器提供一种安全方法来存储可以解密的密码。例如，系统使用这些密码来建立与另一系统的 SLIP 连接。（第 111 页的『安全性和拨出会话』描述了这种存储密码的用法。）

iSeries 服务器将这些特殊密码存储在任何用户程序或接口都不可访问的安全区域内。仅显式授权的系统功能可以设置这些密码并检索它们。

例如，当将存储的密码用于拨出 SLIP 连接时，用创建配置概要文件（WRKTCPPTP）的系统命令设置密码。您必须具有 *IOSYSCFG 才能使用该命令。在拨出过程期间，一个特别编码的连接脚本检索密码并将它解密。用户和任何作业记录内都见不到解密的密码。

作为安全管理员，需要决定是否允许在系统上存储可以解密的密码。使用“保留服务器安全性数据”（QRETSVRSEC）系统值来指定此决定。缺省值是 0（否）。因此，除非显式地设置此系统值，否则系统将不存储可以解密的密码。

如果具有存储密码的网络或通信需求，应设置正确的策略、了解策略并进行与伙伴的通信。例如，当使用 SLIP 与另一个 iSeries 服务器通信时，两个系统都应考虑设置特殊用户概要文件以建立会话。该特殊概要文件在系统上应具有受限制的权限。这可以限制当合作系统上损害了存储密码时对系统的影响。

第 4 章 将 iSeries 配置为使用安全性工具

此信息描述如何设置您的系统来使用安全性工具，它是 OS/400 的一部分。当您安装 OS/400 后，安全性工具就可以使用了。以下主题提供使用安全性工具的操作过程的建议。

安全地操作安全性工具

当您安装 OS/400 时，与安全性工具关联的对象是安全的。要安全地操作安全性工具，避免对任何安全性工具对象进行权限更改。

以下是对于安全性工具对象的安全性设置和需求:

- 安全性工具程序和命令位于 QSYS 产品库中。这些命令和程序在交付时公共权限为 *EXCLUDE。许多安全性工具命令在 QUSRSYS 库中创建文件。当系统创建这些文件时，这些文件的公共权限是 *EXCLUDE。

  包含关于生成已更改的报告的信息的文件具有以 QSEC 开始的名称。包含关于管理用户概要文件的信息的文件具有以 QASEC 开始的名称。这些文件包含关于您的系统的机密信息。因此，您不应该更改这些文件的公共权限。
- 安全性工具使用正常系统设置来定向已打印的输出。这些报告包含关于您的系统的机密信息。要将输出定向至保护输出队列，对将运行安全性工具的用户的用户概要文件或作业描述进行适当的更改。
- 由于他们的安全性 功能以及由于他们访问系统中的许多对象，安全性工具命令需要 *ALLOBJ 特权。其中某些命令也需要 *SECADM、*AUDIT 或 *IOSYSCFG 特权。要确保命令成功运行，当您使用安全性工具时，您应该作为安全主管注册。因此，您应该不需要对任何安全性工具命令授予专用权限。

避免文件冲突

许多安全性工具报告命令都会创建一个数据库文件，您可以使用该文件来打印报告的已更改版本。第 26 页的『安全性命令的命令和菜单』告诉每个命令的文件名。您每次从一个作业只能运行一个命令。大多数命令现在具有实施这一点的检查。如果您在另一个作业尚未完成运行某个命令时运行该命令，您将接收到错误消息。

许多打印作业是运行时间较长的作业。当您将报告提交至批处理或将它们添加至作业调度程序时，您需要小心以避免文件冲突。例如，您可能要用不同的选择标准打印 PRTUSRPRF 报告的两个版本。如果您将报告提交至批处理，则应该使用每次仅运行一个作业的作业队列来确保报告作业按顺序运行。

如果您使用作业调度程序，则需要将两个作业调度分开得足够远，以使第一个版本完成之后，第二个作业才启动。

保存安全性工具

每当您运行“保存系统”（SAVSYS）命令或“保存”菜单中运行 SAVSYS 命令的某个选项时，就会保存安全性工具程序。

安全性工具文件位于 QUSRSYS 库中。您应该已经将保存此库作为您的正常操作过程的一部分。QUSRSYS 库包含系统上许多许可程序的数据。有关哪些命令和选项保存 QUSRSYS 库的更多信息，请参阅“信息中心”。

安全性命令的命令和菜单

本节描述安全性工具的命令和菜单。本资料中包括关于如何使用这些命令的示例。

有两个菜单可用于安全性工具:

- 用于以交互式方式运行命令的 SECTOOLS（安全性工具）菜单。
- 用于以批处理方式运行报告命令的 SECBATCH（将安全性报告提交或调度至批处理）菜单。SECBATCH 菜单具有两个部分。该菜单的第一部分使用“提交作业”（SBMJOB）命令来提交报告以便以批处理方式立即进行处理。

  该菜单的第二部分使用“添加作业调度项”（ADDJOBSCDE）命令。使用它来调度将在指定日期和时间定期运行的安全性报告。

“安全性工具”菜单选项

表 6 描述以下菜单选项和关联的命令:

表 6. 用户概要文件的工具命令

菜单[1]选项	命令名称	描述	使用的数据库文件
1	ANZDFTPWD	使用“分析缺省密码”命令来报告用户概要文件并对其执行操作，这些用户概要文件的密码等于用户概要文件名称。	QASECPWD[2]
2	DSPACTPRFL	使用“显示活动概要文件列表”命令来显示或打印免于 ANZPRFACT 处理的用户概要文件列表。	QASECIDL[2]
3	CHGACTPRFL	使用“更改活动概要文件列表”命令来向 ANZPRFACT 命令的免除列表中添加和从中除去用户概要文件。活动用户概要文件列表中的用户概要文件是永久活动的（直到您从列表中除去该概要文件为止）。ANZPRFACT 命令不禁用活动概要文件列表中的概要文件，不管该概要文件已多长时间不活动。	QASECIDL[2]
4	ANZPRFACT	使用“分析概要文件活动”命令来禁用在指定的天数中未使用过的用户概要文件。在使用 ANZPRFACT 命令指定天数后，系统每夜运行 ANZPRFACT 作业。 可以使用 CHGACTPRFL 命令来免除禁用用户概要文件。	QASECIDL[2]
5	DSPACTSCD	使用“显示概要文件激活调度”命令来显示或打印关于用于启用和禁用特定用户概要文件的调度的信息。应使用 CHGACTSCDE 命令创建调度。	QASECACT[2]

表 6. 用户概要文件的工具命令 (续)

菜单[1]选项	命令名称	描述	使用的数据库文件
6	CHGACTSCDE	使用“更改激活调度项”命令来使用户概要文件仅在每天或每周的某些时间可用于注册。对于您调度的每个用户概要文件，系统为启用和禁用次数创建作业调度项。	QASECACT[2]
7	DSPEXPSCD	使用“显示到期调度”命令来显示或打印在将来要被调度至禁用或从系统中除去的用户概要文件列表。使用 CHGEXPSCDE 命令来将用户概要文件设置为到期。	QASECEXP[2]
8	CHGEXPSCDE	使用“更改到期调度项”命令来调度要除去的用户概要文件。可以临时除去它（通过禁用它）或从系统中删除它。此命令使用每天在 00:01（午夜后 1 分钟）运行的作业调度项。该作业查看 QASECEXP 文件来确定是否将任何用户概要文件设置为在那天到期。 使用 DSPEXPSCD 命令来显示调度为到期的用户概要文件。	QASECEXP[2]
9	PRTPRFINT	使用“打印概要文件内部信息”命令来打印包含关于在用户概要文件中包含的项数的信息的报告。项数确定用户概要文件的大小。	

注:

1. 选项来自 SECTOOLS 菜单。
2. 此文件位于 QUSRSYS 库中。

可以在菜单中向下翻页来查看附加选项。表 7 描述安全性审计的菜单选项和关联的命令:

表 7. 安全性审计的工具命令

菜单[1]选项	命令名称	描述	使用的数据库文件
10	CHGSECAUD	使用“更改安全性审计”命令来设置安全性审计和更改控制安全性审计的系统值。当您运行 CHGSECAUD 命令时，如果安全性审计（QAUDJRN）日志不存在，系统创建它。 CHGSECAUD 命令提供使设置 QAUDLVL（审计级别）系统值更简单的选项。可以指定 *ALL 来激活所有可能的审计级别设置。或者，可以指定 *DFTSET 来激活最常用的设置（*AUTFAIL、*CREATE、*DELETE、*SECURITY 和 *SAVRST）。 **注**: 如果使用安全性工具来设置审计，确保计划您的审计日志接收器的管理。否则，您可能很快遇到磁盘利用率的问题。	
11	DSPSECAUD	使用“显示安全性审计”命令来显示关于安全性审计日志的信息和控制安全性审计的系统值。	

表 7. 安全性审计的工具命令 (续)

菜单[1]选项	命令名称	描述	使用的数据库文件
注: 1. 选项来自 SECTOOLS 菜单。			

使用“安全性批处理”菜单

以下是 SECBATCH 菜单的第一部分:

```
SECBATCH          将安全性报告提交或调度至批处理
                                                        系统:
选择下列其中之一:

  将报告提交至批处理
     1. 沿用对象
     2. 审计日志项
     3. 权限列表权限
     4. 命令权限
     5. 命令专用权限
     6. 通信安全性
     7. 目录权限
     8. 目录专用权限
     9. 文挡权限
    10. 文挡专用权限
    11. 文件权限
    12. 文件专用权限
    13. 文件夹权限
```

当从此菜单选择一个选项时，将看到“提交作业”（SBMJOB）屏幕。如果要更改命令的缺省选项，可以在*运行的命令*行中按 F4（提示）。

要查看“调度批处理报告”，在 SECBATCH 菜单中向下翻页。通过使用在菜单的此部分中的选项，您可以执行某些操作，例如将您的系统设置为定期运行已更改版本的报告。可以向下翻页以获取附加菜单选项。当从菜单的此部分选择一个选项时，将看到“添加作业调度项”（ADDJOBSCDE）屏幕。

可以将光标定位在*运行的命令*行并按 F4（提示）来为报告选择不同设置。应该指定有意义的作业名称以便您可以在显示作业调度项时识别该项。

“安全性批处理”菜单选项

第 29 页的表 8 描述安全性报告的菜单选项和关联的命令:

当您运行安全性报告时，系统仅打印同时满足您指定的选择标准和工具的选择标准的信息。例如，指定用户概要文件名称的作业描述是与安全性相关的。因此，仅当作业描述的公共权限不是 *EXCLUDE *并且*当作业描述在 USER 参数中指定用户概要文件名称时，作业描述（PRTJOBDAUT）报告才打印在指定库中的作业描述。

同样，当您打印子系统信息（PRTSBSDAUT 命令）时，仅当子系统描述具有指定用户概要文件的通信项时，系统才打印关于该子系统的信息。

如果某个特定报告打印的信息比您期望的少，则查阅联机帮助信息来找出报告的选择标准。

表 8. 安全性报告的命令

菜单[1]选项	命令名称	描述	使用的数据库文件
1 和 40	PRTADPOBJ	使用“打印沿用对象”命令来打印沿用指定的用户概要文件的权限的对象列表。可以指定单个概要文件、类属概要文件名称（如以 Q 开始的所有概要文件）或在系统上的所有用户概要文件。 此报告具有两个版本。完整报告列示满足选择标准的所有沿用对象。更改报告列示当前在系统上的沿用对象和上次运行报告时在系统上的沿用对象之间不同的部分。	QSECADPOLD[2]
2 和 41	DSPAUDJRNE	使用“显示审计日志项”命令来显示或打印关于在安全性审计日志中的项的信息。可以选择特定的项类型、特定的用户和某个时间段。	QASYxxJ4[3]
3 和 42	PRTPVTAUT *AUTL	当对 *AUTL 对象使用“打印专用权限”命令时，将接收到在系统上所有权限列表的列表。报告包括对每个列表授权的用户和用户对列表具有什么权限。使用此信息来帮助您分析您的系统上的对象权限的源。 此报告具有三个版本。完整报告列示在系统上的所有权限列表。更改报告列示自上次运行报告以来对权限的附加和更改。删除的报告列示自上次运行报告以来已删除其对权限列表的权限的用户。 当您打印完整报告时，可以选择打印每个权限列表保护的对象列表。系统将为每个权限列表创建单独的报告。	QSECATLOLD[2]
6 和 45	PRTCMNSEC	使用“打印通信安全性”命令来打印您的系统上影响通信的对象的与安全性相关的设置。这些设置影响用户和作业可以如何进入您的系统。 此命令生成两个报告：一个报告显示系统上的配置列表的设置，另一个报告列示线路描述、控制器和设备描述的与安全性相关的参数。每个报告具有完整版本和更改版本。	QSECCMNOLD[2]
15 和 54	PRTJOBDAUT	使用“打印作业描述权限”命令来打印指定用户概要文件和具有不是 *EXCLUDE 的公共权限的作业描述列表。报告显示在作业描述中指定的用户概要文件的特权。 此报告具有两个版本。完整报告列示满足选择标准的所有作业描述对象。更改报告列示当前在系统上的作业描述对象和上次运行报告时在系统上的作业描述对象之间不同的部分。	QSECJBDOLD[2]

表 8. 安全性报告的命令 (续)

菜单[1]选项	命令名称	描述	使用的数据库文件
请参阅注释 4	PRTPUBAUT	使用“打印公共授权对象”命令来打印其公共权限不是 *EXCLUDE 的对象列表。当您运行该命令时，指定报告的对象类型和库。使用 PRTPUBAUT 命令来打印关于系统上的每个用户可以访问的对象的信息。 此报告具有两个版本。完整报告列示满足选择标准的所有对象。更改报告列示当前在系统上的指定对象和上次运行报告时在系统上的对象（具有在同一库中相同类型）之间不同的部分。	QPBxxxxxx[5]
请参阅注释 5。	PRTPVTAUT	使用“打印专用权限”命令来打印对在指定库中具有指定类型的对象的专用权限列表。使用此报告来帮助您确定对对象的权限源。 此报告具有三个版本。完整报告列示满足选择标准的所有对象。更改报告列示当前在系统上的指定对象和上次运行报告时在系统上的对象（具有在同一库中相同类型）之间不同的部分。删除的报告列示自上次打印报告以来已删除其对对象的权限的用户。	QPVxxxxxx[5]
24 和 63	PRTQAUT	使用“打印队列报告”来打印系统上的输出队列和作业队列的安全性设置。这些设置控制谁可以查看和更改在输出队列或作业队列中的项。 此报告具有两个版本。完整报告列示满足选择标准的所有输出队列和作业队列对象。更改报告列示当前在系统上的输出队列和作业队列对象和上次运行报告时在系统上的输出队列和作业队列对象之间不同的部分。	QSECQOLD[2]
25 和 64	PRTSBSDAUT	使用“打印子系统描述”命令来打印系统上子系统描述的与安全性相关的通信项。这些设置控制工作可以如何进入您的系统以及作业如何运行。仅当报告具有指定用户概要文件名称的通信项时，报告才打印子系统描述。 此报告具有两个版本。完整报告列示满足选择标准的所有子系统描述对象。更改报告列示当前在系统上的子系统描述对象和上次运行报告时在系统上的子系统描述对象之间不同的部分。	QSECSBDOLD[2]
26 和 65	PRTSYSSECA	使用“打印系统安全性属性”命令来打印与安全性相关的系统值和网络属性列表。报告显示当前值和建议的值。	
27 和 66	PRTTRGPGM	使用“打印触发器程序”命令来打印与您的系统上的数据库文件关联的触发器程序列表。 此报告具有两个版本。完整报告列示指定的并满足您的选择标准的每个触发器程序。更改报告列示自上次运行报告以来指定的触发器程序。	QSECTRGOLD[2]

表 8. 安全性报告的命令 (续)

菜单[1]选项	命令名称	描述	使用的数据库文件
28 和 67	PRTUSROBJ	使用“打印用户对象”命令来打印在库中的用户对象（不是由 IBM 提供的对象）列表。可以使用此报告来打印位于在库列表的系统部分中的库（如 QSYS）中的用户对象列表。 此报告具有两个版本。完整报告列示满足选择标准的所有用户对象。更改报告列示当前在系统上的用户对象和上次运行报告时在系统上的用户对象之间不同的部分。	QSECPUOLD[2]
29 和 68	PRTUSRPRF	使用“打印用户概要文件”命令来分析满足指定条件的用户概要文件。可以根据特殊权限、用户类或在特殊权限和用户类之间的不匹配来选择用户概要文件。可以打印权限信息、环境信息、密码信息或密码级别信息。	
30 和 69	PRTPRFINT	使用“打印概要文件内部信息”命令来打印关于项数的信息的报告。	
31 和 70	CHKOBJITG	使用“检查对象完整性”命令来确定是否更改了可操作的对象（如程序）而未使用编译器。此命令可以帮助您检测在您的系统上引入病毒程序或将程序更改为执行未授权指示信息的尝试次数。*iSeries Security Reference* 一书提供了关于 CHKOBJITG 命令的更多信息。	

注:

1. 选项来自 SECBATCH 菜单。
2. 此文件位于 QUSRSYS 库中。
3. xx 是两个字符的日志项类型。例如，AE 日志项的模型输出文件是 QSYS/QASYAEJ4。在 *iSeries Security Reference* 一书的 Appendix F 中描述了模型输出文件。
4. SECBATCH 菜单包含一般对安全管理员重要的对象类型的选项。例如，使用选项 11 或 50 来对 *FILE 对象运行 PRTPUBAUT 命令。使用一般选项（18 和 57）来指定对象类型。
5. SECBATCH 菜单包含一般对安全管理员重要的对象类型的选项。例如，选项 12 或 51 对 *FILE 对象运行 PRTPVTAUT 命令。使用一般选项（19 和 58）来指定对象类型。
6. 在文件的名称中的 xxxxxx 代表对象类型。例如，程序对象的文件对于公共权限称为 QPBPGM，而对于专用权限称为 QPVPGM。文件位于 QUSRSYS 库中。

   文件包含您打印其报告的每个库的一个成员。成员名称与库名称相同。

用于定制安全性的命令

第 32 页的表 9 描述可以用来定制您的系统上的安全性的命令。这些命令位于 SECTOOLS 菜单中。

表 9. 用于定制您的系统的命令

菜单[1]选项	命令名称	描述	使用的数据库文件
60	CFGSYSSEC	使用“配置系统安全性”命令来将与安全性相关的系统值设置为其建议的设置。该命令也设置您的系统上的安全性审计。『由“配置系统安全性”命令设置的值』描述该命令执行的操作。 **注**: 要获取对于您的情况定制的安全性建议，运行“iSeries 安全性向导”或“iSeries 安全性顾问程序”，而不是运行此命令。有关这些工具的信息，请参阅第 9 页的第 2 章，『iSeries 安全性向导和 eServer Security Planner』。	
61	RVKPUBAUT	使用“撤销公共权限”命令的方式将您的系统上对一组安全性敏感的命令的公共权限设置为 *EXCLUDE。第 34 页的『“撤销公共权限”命令的功能』列示 RVKPUBAUT 命令执行的操作。	

注:

1. 选项来自 SECTOOLS 菜单。

由“配置系统安全性”命令设置的值

表 10 列示运行 CFGSYSSEC 命令时设置的系统值。CFGSYSSEC 命令运行称为 QSYS/QSECCFGS 的程序。

表 10. 由 CFGSYSSEC 命令设置的值

系统值名称	设置	系统值描述
QALWOBJRST	*NONE	是否可以恢复系统状态程序和沿用权限的程序
QAUTOCFG	0（否）	新设备的自动配置
QAUTOVRT	0	如果没有设备可用，系统将自动创建的虚拟设备描述数。
QDEVRCYACN	*DSCMSG（与消息断开连接）	重新建立通信时的系统操作
QDSCJOBITV	120	系统对断开连接的作业执行操作之前的时间周期
QDSPSGNINF	1（是）	用户是否看到注册信息屏幕
QINACTITV	60	系统对不活动的交互式作业执行操作之前的时间周期
QINACTMSGQ	*ENDJOB	系统对不活动的作业执行的操作
QLMTDEVSSN	1（是）	是否将用户限制为一次在一个设备上注册
QLMTSECOFR	1（是）	用户将 *ALLOBJ 和 *SERVICE 用户限制于特定设备
QMAXSIGN	3	允许多少次连续的失败注册尝试
QMAXSGNACN	3（两者）	当达到 QMAXSIGN 限制时，系统是禁用工作站还是禁用用户概要文件。
QRMTSIGN	*FRCSIGNON	系统如何处理远程（传递或 TELNET）注册尝试。
QRMTSVRATR	0（关闭）	允许以远程方式分析系统。
QSECURITY 第 33 页的 1	50	实施的安全级别
QVFYOBJRST	3（恢复时验证签名）	恢复时验证对象
QPWDEXPITV	60	用户必须更改其密码的频率

表 10. 由 CFGSYSSEC 命令设置的值 (续)

系统值名称	设置	系统值描述
QPWDMINLEN	6	密码的最小长度
QPWDMAXLEN	8	密码的最大长度
QPWDPOSDIF	1（是）	新密码中的每个位置是否都必须与上一个密码中的相同位置不同
QPWDLMTCHR	请参阅注释 2	密码中不允许的字符
QPWDLMTAJC	1（是）	密码中是否禁止相邻数字
QPWDLMTREP	2（不能连续地重复）	密码中是否禁止重复字符
QPWDRQDDGT	1（是）	密码是否必须至少具有一个数字
QPWDRQDDIF	1（32 唯一密码）	需要多少唯一密码才可重复密码
QPWDVLDPGM	*NONE	系统调用以验证密码的用户出口程序

注:

1. 如果当前在用 40 或更低的 QSECURITY 值运行，在更改为更高的安全级别之前，确保复查 *iSeries Security Reference* 一书的 Chapter 2 中的信息。
2. 限制的字符以消息标识 CPXB302 存储在消息文件 QSYS/QCPFMSG 中。它们是作为 AEIOU@$# 交付的。可以使用“更改消息描述”（CHGMSGD）命令来更改限制的字符。在密码级别 2 或 3 未实施 QPWDLMTCHR 系统值。

CFGSYSSEC 命令也对下列 IBM 提供的用户概要文件将密码设置为 *NONE:

QSYSOPR

QPGMR

QUSER

QSRV

QSRVBAS

最后，CFGSYSSEC 命令通过使用“更改安全性审计过程”（CHGSECAUD）命令设置安全性审计过程。 CFGSYSSEC 命令打开操作和对象审计并同时，指定操作的缺省设置以在 CHGSECAUD 命令上审计。

定制程序

如果其中某些设置不适于您的安装，可以创建处理该命令的程序的自己的版本。执行下列操作:

__ 步骤 1. 使用“检索 CL 源”（RTVCLSRC）命令来复制当使用 CFGSYSSEC 命令时运行的程序的源。要检索的程序是 QSYS/QSECCFGS。当检索它时，给予它一个*不同的名称*。

__ 步骤 2. 编辑程序以进行更改。然后编译它。编译它时，确保*未*替换 IBM 提供的 QSYS/QSECCFGS 程序。您的程序应具有不同的名称。

__ 步骤 3. 使用“更改命令”（CHGCMD）命令来更改 CFGSYSSEC 命令的“处理命令的程序”（PGM）参数。将 PGM 值设置为您的程序的名称。例如，如果在称为 MYSECCFG 的 QGPL 库中创建程序，必须输入以下命令:

```
CHGCMD CMD(QSYS/CFGSYSSEC) PGM(QGPL/MYSECCFG)
```

注: 如果更改 QSYS/QSECCFGS 程序，IBM 不能保证或默示程序的可靠性、适用性、性能或功能。明示的不保证声明包括适销性和适用于某特定用途的默示保证。

“撤销公共权限”命令的功能

可以使用“撤销公共权限”（RVKPUBAUT）命令将一组命令和程序的公共权限设置为 *EXCLUDE。RVKPUBAUT 命令运行称为 QSYS/QSECRVKP 的程序。当交付 QSECRVKP 时，它撤销表 11 中列示的命令和表 12 中列示的应用程序编程接口（API）的公共权限（通过将公共权限设置为 *EXCLUDE）。当系统到达时，这些命令和 API 的公共权限已设置为 *USE。

表 11 中列示的命令和表 12 中列示的 API 都会在系统上执行可能提供恶作剧机会的功能。作为安全管理员，您应显式地授权用户运行这些命令和程序，而不是使它们对于所有系统用户都可用。

当运行 RVKPUBAUT 命令时，指定包含命令的库。缺省值是 QSYS 库。如果系统上有多种本地语言，则需要对每个 QSYSxxx 库运行该命令。

表 11. 公共权限由 RVKPUBAUT 命令设置的命令

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

表 12 中的 API 都在 QSYS 库中:

表 12. 公共权限由 RVKPUBAUT 命令设置的程序

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

运行 RVKPUBAUT 命令时，系统将根目录的公共权限设置为 *USE（除非它已是 *USE 或更低权限）。

定制程序

如果其中某些设置不适于您的安装，可以创建处理该命令的程序的自己的版本。执行下列操作:

__ 步骤 1. 使用“检索 CL 源”（RTVCLSRC）命令来复制当使用 RVKPUBAUT 命令时运行的程序的源。要检索的程序是 QSYS/QSECRVKP。当检索它时，给予它一个*不同的名称*。

__ 步骤 2. 编辑程序以进行更改。然后编译它。编译它时，确保未替换 IBM 提供的 QSYS/QSECRVKP 程序。您的程序应具有不同的名称。

__ 步骤 3. 使用“更改命令”（CHGCMD）命令来更改 RVKPUBAUT 命令的“处理命令的程序”（PGM）参数。将 PGM 值设置为您的程序的名称。例如，如果在称为 MYRVKPGM 的 QGPL 库中创建程序，必须输入以下命令:

```
CHGCMD CMD(QSYS/RVKPUBAUT) PGM(QGPL/MYRVKPGM)
```

注: 如果更改 QSYS/QSECRVKP 程序，IBM 不能保证或默示程序的可靠性、适用性、性能或功能。明示的不保证声明包括适销性和适用于某特定用途的默示保证。

第 2 部分 高级 iSeries 安全性

第 5 章 使用对象权限保护信息资产

您作为安全管理员所面临的挑战就是在不破坏系统上的用户的情况下保护贵组织的信息资产。需要确保用户具有足够的权限来完成他们的作业，而无需授予他们浏览整个系统和进行未授权更改的权限。

安全性技巧

太严格的权限可能造成相反的结果。用户有时通过彼此共享密码对太严格的权限限制作出反应。

OS/400 操作系统提供集成对象安全性。用户 必须使用系统提供的接口来访问对象。例如，如果您要访问数据库文件，必须使用专门用于访问数据库文件的命令或程序。不能使用专门用于访问消息队列或作业记录的命令。

每当您使用系统接口来访问对象时，系统验证您是否具有该接口所需要的访问该对象的权限 该接口。对象权限是用于保护您的系统上的资产的功能强大且灵活的工具。您作为安全管理员的挑战就是设置您可以管理和维护的有效的对象安全性方案。

对象权限实施

每当您尝试访问对象时，操作系统检查您对该对象的权限。然而，如果将您的系统上的安全级别（QSECURITY 系统值）设置为 10 或 20，则每个用户自动具有访问每个对象的权限，因为每个用户概要文件具有 *ALLOBJ 特权。

对象权限技巧: 如果您不确信您是否正在使用对象安全性，检查 QSECURITY（安全级别）系统值。如果 QSECURITY 是 10 或 20，则您未在使用对象安全性。

在更改为安全级别 30 或更高级别之前，必须计划和准备。否则，您的用户可能不能访问他们需要的信息。

在信息中心中的**基本系统安全性和计划**主题提供了一种方法，该方法用于分析您的应用程序和决定应该如何设置对象安全性。如果您尚未使用对象安全性或如果您的对象安全性方案已过期或很复杂，阅读此主题来帮助您入门。

菜单安全性

iSeries 服务器最初设计成 S/36 和 S/38 的后续产品。许多 iSeries 服务器安装曾经是 S/36 安装或 S/38 安装。为了控制用户可以执行的操作，在那些早期系统上的安全管理员常常使用称为**菜单安全性**或**菜单访问控制**的技术。

菜单访问控制指的是当用户注册时，该用户看到一个菜单。用户只能执行菜单中的功能。用户不能获取系统上的命令行来执行不在菜单中的任何功能。在理论上，安全管理员不必担心对象的权限，因为菜单和程序控制用户可以执行的操作。

iSeries 服务器提供几个用户概要文件选项来帮助菜单访问控制，您可以使用:

- **初始菜单**（INLMNU）参数来控制在用户注册之后首先看到什么菜单。
- **初始程序**（INLPGM）参数来在用户看到菜单之前运行设置程序。或者，您可以使用 INLPGM 参数来将用户限制于运行单个程序。
- **限制功能**（LMTCPB）参数来将用户限制于有限的一组命令。它也阻止用户在“注册”屏幕上指定不同的初始程序或菜单 （LMTCPB 参数仅限制从命令行输入的命令。）

菜单访问控制的限制

计算机和计算机用户在过去的几年中已更改了许多。有许多工具可用（如查询程序和电子表格），这样用户可以进行他们自己的编程来减轻 IS 部门的负担。某些工具（如 SQL 或 ODBC）提供查看信息和更改信息的功能。在菜单结构中启用这些工具是很困难的。

固定功能（“绿色屏幕”）工作站很快被个人计算机和计算机到计算机的网络替换。如果您的系统参与到网络中，用户可以进入您的系统，而未曾看到注册屏幕或菜单。

作为正在尝试实施菜单访问控制的安全管理员，您遇到了两个基本问题:

- 如果您成功将用户限制于菜单，则您的用户将可能不愉快，因为限制了他们使用现代工具的能力。
- 如果您不成功，则您可能使菜单访问控制应该保护的关键的机密信息遭到危险。当您的系统参与到网络中时，您实施菜单访问控制的能力降低了。例如，LMTCPB 参数仅适用于在交互式会话中从命令行输入的命令。LMTCPB 参数对来自通信会话的请求（如 PC 文件传送、FTP 或远程命令）没有影响。

使用对象安全性提高菜单访问控制

对于可用于连接至系统的许多新选项，将来的可行的 iSeries 服务器安全性方案不能只依赖于菜单访问控制。此主题提供用于向对象安全性环境移动来补充您的菜单访问控制的建议。

在信息中心中的*基本系统安全性和计划*主题描述用于分析权限的技术，用户必须对对象具有该权限才能运行您的当前应用程序。然后您将用户指定给组并授予组适当的权限。此方法合理且合乎逻辑。然而，如果您的系统已运行了许多年且具有许多应用程序，则分析应用程序和设置对象权限的任务可能是艰巨的。

对象权限技巧: 与沿用程序所有者的权限的程序组合的当前菜单可以提供跨越菜单访问控制的过渡。确保保护沿用权限的程序和拥有它们的用户概要文件。

当您逐步分析您的应用程序和对象时，您可能能够使用您的当前菜单来帮助您设置过渡环境。以下是使用“订单输入”（OEMENU）菜单以及关联的文件和程序的示例。

示例: 设置过渡环境

此示例从下列假设和需求开始:

- 所有文件都位于库 ORDERLIB 中。
- 您并非知道所有文件的名称。您也不知道菜单选项对不同的文件需要什么权限。
- 菜单和它调用的所有程序都位于称为 ORDERPGM 的库中。
- 想要可以注册到您的系统的每个人能够查看所有订单文件、客户文件和商品文件中的信息（例如，使用查询或电子表格）。

- 只有其当前注册菜单是 OEMENU 的用户应该能够更改文件。而且，他们必须使用在菜单中的程序来执行此操作。
- 非安全管理员的系统用户不具有 *ALLOBJ 或 *SECADM 特权。

执行下列步骤来更改此菜单访问控制环境以适应查询的需要:

__ 步骤 1. 生成其初始菜单是 OEMENU 的用户的列表。

可以使用“打印用户概要文件”（PRTUSRPRF *ENVINFO）命令来列示您的系统上的每个用户概要文件的环境。该报告包括初始菜单、初始程序和当前库。第 55 页的图 7 显示该报告的一个示例。

__ 步骤 2. 确保 OEMENU 对象（它可以是 *PGM 对象或 *MENU 对象）是由不用于注册的用户概要文件所有。应该禁用该用户概要文件或它具有密码 *NONE。对于此示例，假定 OEOWNER 拥有 OEMENU 程序对象。

__ 步骤 3. 确保拥有 OEMENU 程序对象的用户概要文件不是组概要文件。可以使用下列命令:

```
DSPUSRPRF USRPRF(OEOWNER) TYPE(*GRPMBR)
```

__ 步骤 4. 更改 OEMENU 程序来沿用 OEOWNER 用户概要文件的权限。（使用 CHGPGM 命令来将 USRPRF 参数更改为 *OWNER。）

注: *MENU 对象不能沿用权限。如果 OEMENU 是一个 *MENU 对象，您可以通过执行下列操作之一来修改此示例:

- 创建显示该菜单的程序。
- 使用当用户从 OEMENU 菜单中选择选项时运行的程序的沿用权限。

__ 步骤 5. 通过输入下列两个命令将在 ORDERLIB 中的所有文件的公共权限设置为 *USE:

```
RVKOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
     AUT(*ALL)
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
   AUT(*USE)
```

记住，如果您选择 *USE 权限，则用户可以通过使用 PC 文件传送或 FTP 来复制文件。

__ 步骤 6. 通过输入以下命令来授予拥有菜单程序的概要文件对文件的 *ALL 权限:

```
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(OEOWNER)
     AUT(*ALL)
```

对于大多数应用程序，对文件的 *CHANGE 权限已足够。然而，您的应用程序可能执行需要比 *CHANGE 更多权限的功能，如清除物理文件成员。最后，您应该分析您的应用程序并仅提供应用程序所需要的最小权限。然而，在过渡期间，通过沿用 *ALL 权限避免了可能由于权限不足引起的应用程序故障。

__ 步骤 7. 通过输入下列命令来限制对在订单库中的程序的权限:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(*PUBLIC)
   AUT(*EXCLUDE)
```

__ 步骤 8. 通过输入下列命令来授予 OEOWNER 概要文件对在库中的程序的权限:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(OEOWNER)
   AUT(*USE)
```

__ 步骤 9. 通过为每个用户输入下列命令来授予在步骤 1 中标识的用户对菜单程序的权限:

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
    USER(user-profile-name) AUT(*USE)
```

当您完成这些步骤时，未显式排除的所有系统用户都将能够访问（但不能更改）在 ORDERLIB 库中的文件。对 OEMENU 程序具有权限的用户将能够使用位于菜单中的程序来更新在 ORDERLIB 库中的文件。只有对 OEMENU 程序具有权限的用户现在将能够更改在此库中的文件。对象安全性和菜单访问控制的组合保护文件。

当您对包含用户数据的所有库完成类似的步骤时，您就创建了用于控制数据库更新的一个简单方案。此方法阻止系统用户更新数据库文件，在他们使用批准的菜单和程序时除外。同时，您生成了可用于具有决定支持工具或具有来自另一个系统或 PC 的链接的用户查看、分析和复制的数据库文件。

对象权限技巧: 当您的系统参与到网络中时，*USE 权限可以提供比您期望的更多权限。例如，使用 FTP，如果您对某个文件具有 *USE 权限，则可以将该文件复制到另一个系统（包括 PC）。

使用库安全性来补充菜单安全性

要访问在某个库中的某个对象，您必须对该对象和该库同时具有权限。大多数操作需要对库的 *EXECUTE 权限或 *USE 权限。

根据您的情况，您可能能够使用库权限作为保护对象的简单方法。例如，假定对于“订单输入”菜单示例，对“订单输入”菜单具有权限的每个人都可以使用在 ORDERPGM 库中的所有程序。不是保护单个程序，而是您可以将对 ORDERPGM 库的公共权限设置为 *EXCLUDE。然后，您可以将对库的 *USE 权限授予特定的用户概要文件，这将允许它们使用该库中的程序。（这假定对程序的公共权限是 *USE 或更大。）

库权限可能是用于管理对象权限一种简单有效的方法。然而，您必须确保您了解您正在保护的库的内容以使您不提供对对象的无意访问。

配置对象所有权

在您的系统上对象的所有权是您的对象权限方案的一个重要部分。缺省情况下，某个对象的所有者对该对象具有 *ALL 权限。在 *iSeries Security Reference* 一书中的 Chapter 5 提供了用于计划对象所有权的建议和示例。以下是几个技巧:

- 通常，组概要文件不应该拥有对象。如果组概要文件拥有某个对象，则所有组成员对该对象具有 *ALL 权限，除非显式排除该组成员。
- 如果您使用沿用权限，考虑拥有程序的用户概要文件是否也应该拥有应用程序对象，如文件。您可能不希望运行沿用权限的程序的用户对文件具有 *ALL 权限。

如果您正在使用“iSeries 导航器”，可以通过使用安全性**策略**功能完成更改来实现它。有关更多信息，参阅 iSeries 信息中心（有关详细信息，请参阅第 xii 页的『先决条件和相关信息』）。

对系统命令和程序的对象权限

以下是在您限制对 IBM 提供的对象的权限时的几个建议:

- 当您的系统上具有多种本地语言时，您的系统具有多个系统（QSYS）库。您的系统上的每种本地语言具有一个 QSYSxxxx 库。如果您正在使用对象权限来控制对系统命令的访问，记住要保护您的系统上的 QSYS 库中和每个 QSYSxxx 库中的命令。
- System/38™ 库有时为命令提供等价于您要使用的命令的功能 限制。确保您限制 QSYS38 库中的等价命令。
- 如果您具有 System/36™ 环境，则您可能需要限制附加程序。例如，QY2FTML 程序提供 System/36 文件传送。

审计安全性功能

本章描述用于审计您的系统上的安全性的有效性的技术。由于下列几个原因，用户需要审计系统的安全性:

- 估计安全性计划是否完成。
- 确保计划的安全性控制到位，且工作正常。此类型的审计通常由安全主管作为日常安全性管理的一部分来执行。它有时也由内部或外部审计员以更详细的方式作为定期安全性复查的一部分来执行。
- 为了确保系统安全性与对系统环境的更改保持同步。影响安全性的更改的一些示例为:
  - 由系统用户创建的新对象
  - 允许进入系统的新用户
  - 对象所有权的更改（未调整权限）
  - 职责的更改（已更改用户组）
  - 临时权限（未及时撤销）
  - 安装的新产品
- 为未来的事件作准备，如安装新的应用程序、移动到更高的安全级别或设置通信网络。

本章描述的技术适合于所有这些情况。审计哪些内容和频率如何取决于您的组织的大小和安全性需求。本章的目的是讨论什么信息可用、如何获取以及为什么需要，而不是给出审计频率的准则。

此信息具有三个部分:

- 可以计划和审计的安全性项的核对表。
- 有关设置和使用由系统提供的审计日志的信息。
- 可用来收集有关系统的安全性信息的其它技术。

安全性审计涉及在 iSeries 系统上使用命令和在系统上访问作业记录和日志信息。您可能需要创建由执行您的系统的安全性审计的某个人使用的特殊概要文件。审计员概要文件将需要 *AUDIT 特权才能够更改系统的审计特征。在本章中建议的某些审计任务需要具有 *ALLOBJ 和 *SECADM 特权的用户概要文件。确保当审计周期结束时，将审计员概要文件的密码设置为 *NONE。

有关安全性审计的更多详细信息，请参阅 *Security Reference* 一书的 Chapter 9。

分析用户概要文件

可以使用“显示授权用户”（DSPAUTUSR）命令来显示或打印在系统中的所有用户的完整列表。可以按概要文件名称或组概要文件名称排序列表。以下是组概要文件顺序的示例:

显示授权用户

组概要文件	用户概要文件	密码上次更改	无密码	文本
DPTSM				
	ANDERSOR	08/04/0x		Roger Anders
	VINCENTM	09/15/0x		Mark Vincent
DPTWH				
	ANDERSOR	08/04/0x		Roger Anders
	WAGNERR	09/06/0x		Rose Wagner
QSECOFR				
	JONESS	09/20/0x		Sharon Jones
	HARRISOK	08/29/0x		Ken Harrison
*NO GROUP				
	DPTSM	09/05/0x	X	销售和市场营销
	DPTWH	08/13/0x	X	仓库
	RICHARDS	09/05/0x		Janet Richards
	SMITHJ	09/18/0x		John Smith

打印所选择的用户概要文件

可以使用“显示用户概要文件”（DSPUSRPRF）命令来创建输出文件，并可以使用查询工具来处理该文件。

```
DSPUSRPRF USRPRF(*ALL) +
          TYPE(*BASIC) OUTPUT(*OUTFILE)
```

可以使用查询工具来创建输出文件的各种分析报告，例如:

- 具有 *ALLOBJ 和 *SPLCTL 特权的所有用户列表。
- 按某个用户概要文件字段（如初始程序或用户类）排序的所有用户列表。

可以创建查询程序来从输出文件产生不同的报告。例如:

- 通过选择字段 UPSPAU 不等于 *NONE 所在的记录来列示具有任何特权的所有用户概要文件。
- 通过选择*限制能力*字段（在模型数据库输出文件中称为 UPLTCP）等于 *NO 或 *PARTIAL 所在的记录来列示允许其输入命令的所有用户。
- 列示具有特定初始菜单或初始程序的所有用户。
- 通过查看日期上次注册字段列示不活动用户。

检查大的用户概要文件

具有大量权限的用户概要文件，看起来随机地分布在大多数系统上，可以反映缺乏安全性计划。以下是用于找到大的用户概要文件并评估它们的一个方法:

1. 使用“显示对象描述”（DSPOBJD）命令来创建包含关于系统中所有用户概要文件的信息的输出文件:

```
DSPOBJD OBJ(*ALL) OBJTYPE(*USRPRF) +
        DETAIL(*BASIC) OUTPUT(*OUTFILE)
```

2. 创建查询程序来按大小的递降顺序列示每个用户概要文件的名称和大小。
3. 打印关于最大的用户概要文件的详细信息并评估权限和拥有的对象以查看它们是否合适:

```
DSPUSRPRF USRPRF(user-profile-name) +
          TYPE(*OBJAUT) OUTPUT(*PRINT)
DSPUSRPRF USRPRF(user-profile-name) +
          TYPE(*OBJOWN) OUTPUT(*PRINT)
```

某些 IBM 提供的用户概要文件由于它们拥有的对象数目而很大。通常没有必要列示和分析它们。然而，应该检查沿用 IBM 提供的具有 *ALLOBJ 特权的用户概要文件（如 QSECOFR 和 QSYS）的权限的程序。

有关安全性审计的更多详细信息，请参阅 *Security Reference* 一书的 Chapter 9。

分析对象权限

可以使用下列方法来确定对在系统中的库具有权限的用户:

1. 使用 DSPOBJD 命令来列示在系统中的所有库:

```
DSPOBJD OBJ(QSYS/*ALL) OBJTYPE(*LIB) ASPDEV(*ALLAVL) OUTPUT(*PRINT)
```

注: 此命令将不显示独立辅助存储池中未处于“可用”状态的库。

2. 使用“显示对象权限”（DSPOBJAUT）命令来列示对特定库的权限:

```
DSPOBJAUT OBJ(QSYS/library-name) OBJTYPE(*LIB) +
          ASPDEV(asp-device-name) OUTPUT(*PRINT)
```

3. 使用“显示库”（DSPLIB）命令来列示在库中的对象:

```
DSPLIB LIB(QSYS/library-name) ASPDEV(asp-device-name) OUTPUT(*PRINT)
```

使用这些报告可以确定在某个库中的内容和对该库具有访问权的用户。如果有必要，也可以使用 DSPOBJAUT 命令来查看对于在该库中所选择的对象的权限。

检查变更的对象

可以使用“检查对象完整性”（CHKOBJITG）命令来查看已变更的对象。已变更的对象通常指示某个用户正在尝试干预您的系统。在某个用户已经执行下列操作之后，可能需要运行此命令:

- 将程序恢复至您的系统
- 使用专用服务工具（DST）

当运行该命令时，系统创建包含有关任何可能的完整性问题的信息的数据库文件。可以检查由一个概要文件、几个不同的概要文件或所有概要文件拥有的对象。可以查找已变更其域的对象。也可以重新计算程序验证值来查找类型为 *PGM、*SRVPGM、*MODULE 和 *SQLPKG 的已变更的对象。

运行 CHKOBJITG 程序需要 *AUDIT 特权。该命令由于它执行的扫描和计算而可能需要长时间来运行。应该在您的系统不忙时运行它。

注: 拥有许多具有许多专用权限的对象的概要文件会变得很大。所有者概要文件的大小影响在显示和处理对所拥有的对象的权限时以及在保存或恢复概要文件时的性

能。也会影响系统操作。要防止对性能或系统操作的影响，将对象的所有权分布至多个概要文件。**不要将所有（或几乎所有）对象仅指定给一个所有者概要文件。**

分析沿用权限的程序

沿用具有 *ALLOBJ 特权的用户的权限的程序会引起安全性漏洞。下列方法可以用来查找和检查那些程序:

1. 对于具有 *ALLOBJ 特权的每个用户，使用“显示沿用的程序”（DSPPGMADP）命令来列示沿用该用户的权限的程序:

   ```
   DSPPGMADP USRPRF(user-profile-name) +
             OUTPUT(*PRINT)
   ```

   注: 主题第 44 页的『打印所选择的用户概要文件』显示如何列示具有 *ALLOBJ 权限的用户。

2. 使用 DSPOBJAUT 命令来确定已授权其使用每个沿用的程序的用户以及对程序的公共权限是什么:

   ```
   DSPOBJAUT OBJ(library-name/program-name) +
           OBJTYPE(*PGM) ASPDEV(library-name/program-name) +
             OUTPUT(*PRINT)
   ```

3. 检查源代码和程序描述来评估:
   - 当在沿用的概要文件之下运行时，是否阻止程序的用户使用过多的能力，如使用命令行。
   - 程序是否沿用为打算的功能所需要的最低权限级别。使用程序故障的应用程序可以设计成使用对象和程序的同一所有者概要文件。当沿用程序所有者的权限时，用户对应用程序对象具有 *ALL 权限。在许多情况下，所有者概要文件不需要任何特权。

4. 使用 DSPOBJD 命令验证上次更改程序的时间:

   ```
   DSPOBJD OBJ(library-name/program-name) +
           OBJTYPE(*PGM) ASPDEV(library-name/program-name) +
           DETAIL(*FULL)
   ```

管理审计日志和日志接收器

审计日志 QSYS/QAUDJRN 只用于安全性审计。不应该将对象记入该审计日志。提交控制不应该使用该审计日志。不应该使用“发送日志项”（SNDJRNE）命令或“发送日志项”API 将用户项发送至此日志。

特殊锁定保护用来确保系统可以将审计项写入审计日志。当审计活动（QAUDCTL 系统值不是 *NONE）时，系统仲裁程序作业（QSYSARB）保持对 QSYS/QAUDJRN 日志的锁定。当审计活动时，不能执行对审计日志执行某些操作，如:

- DLTJRN 命令
- ENDJRNxxx 命令
- APYJRNCHG 命令
- RMVJRNCHG 命令
- DMPOBJ 或 DMPSYSOBJ 命令
- 移动日志
- 恢复日志

- 使用权限的操作，如 GRTOBJAUT 命令
- WRKJRN 命令

在 *Security Reference* 一书中描述了记录在安全性日志项中的信息。在审计日志中的所有安全性项都具有日志码 T。除安全性项外，系统项也显示在日志 QAUDJRN 中。它们是具有日志码 J 的项，这些项与初始程序装入（IPL）和对日志接收器执行的一般操作（例如，保存接收器）相关。

如果日志或其当前接收器损坏以致不能将审计项记入日志，QAUDENDACN 系统值确定系统执行的操作。从已损坏的日志或日志接收器的恢复与其它日志的恢复相同。

可能需要让系统管理日志接收器的更改。在创建 QAUDJRN 日志时指定 MNGRCV(*SYSTEM)，或将日志更改为该值。如果指定 MNGRCV(*SYSTEM)，系统在达到其阈值大小时自动拆离接收器并创建和连接新的日志接收器。这称为**系统更改日志管理**。有关更多信息，请参阅 iSeries 信息中心 —> 系统管理 –> 日志管理 –> 本地日志管理 –> 管理日志。有关访问 “iSeries 信息中心” 的信息，请参阅第 xii 页的『先决条件和相关信息』。

第 6 章 管理权限

一组安全性报告可用来帮助您跟踪系统上权限是如何设置的。当您最初运行这些报告时，可以打印所有内容（例如，对所有文件或所有程序的权限）。

在建立了信息库之后，可以定期运行报告的更改版本。更改版本有助于您标识系统上需要您注意的与安全性相关的更改。例如，您可以每周运行一次显示文件的公共权限的报告。您只能请求报告的更改版本。它将为您显示在系统上对每个人都可用的新文件和自上次报告以来其公共权限已更改的现有文件。

有两个菜单可用来运行安全性工具:

- 使用 SECTOOLS 菜单以便以交互式方式运行程序。
- 使用 SECBATCH 菜单以便以批处理方式运行程序。SECBATCH 菜单具有两个部分: 一个用于将作业立即提交至作业队列，而另一个用于将作业放置在作业调度程序中。

如果您正在使用“iSeries 导航器”，则遵循以下步骤来运行安全性工具:

1. 在“iSeries 导航器”中，展开您的服务器 —> **安全性**。
2. 右键单击**策略**并选择**资源管理**来显示您可以创建和管理的策略列表。

监控对象的公共权限

为了简单性和性能，设置大多数系统以便大多数对象对于大多数用户可用。显式拒绝用户访问对安全性敏感的某些机密对象，而不必显式授权来使用每个对象。具有高安全性需求的几个系统采用相反的方法并根据“需要知道”来授权对象。在那些系统上，大多数对象是在公共权限设置为 *EXCLUDE 的情况下创建的。

iSeries 是基于对象的系统，具有许多不同类型的对象。大多数对象类型不包含敏感信息或不执行与安全性相关的功能。作为在具有一般安全性需求的 iSeries 系统上的安全管理员，您可能想将您的注意力集中在要求保护的对象上，如数据库文件和程序。对于其它对象类型，您可以只设置对于您的应用程序已足够的公共权限，它对于大多数对象类型是 *USE 权限。

可以使用“打印公共权限”（PRTPUBAUT）命令来打印有关公共用户可以访问的对象的信息。（**公共用户**是具有注册权限但对对象不具有显式权限的任何人。）当使用 PRTPUBAUT 命令时，可以指定您要检查的对象类型和库或目录。在 SECBATCH 和 SECTOOLS 菜单中有一些选项可用来打印对象类型的“公共授权对象报告”，这些对象类型一般都具有安全性隐含。可以定期打印此报告的更改版本来查看哪些对象可能需要您的注意。

管理新对象的权限

OS/400 提供了一些功能来帮助您管理系统上新对象的权限和所有权。当用户创建新对象时，系统确定以下项:

- 谁将拥有该对象
- 对象的公共权限是什么

- 对象是否具有任何专用权限
- 在哪里放置对象（什么库或目录）
- 是否将审计对对象的访问

系统使用系统值、库参数和用户概要文件参数来作出这些决定。在 *iSeries Security Reference* 一书的 chapter 5 中的 Assigning Authority and Ownership to New Objects 提供了可用的选项的几个示例。

可以使用 PRTUSRPRF 命令来打印影响新对象的所有权和权限的用户概要文件参数。第 54 页的图 5 显示此报告的一个示例。

监控授权列表

可以通过使用权限列表来将具有相似安全性需求的对象分为一组。在概念上，权限列表包含用户列表和用户对由列表保护的对象具有的权限。权限列表提供了管理对系统上相似对象的权限的一种有效方法。然而，在某些情况下，它们使得难以跟踪对对象的权限。

可以使用“打印专用权限”（PRTPVTAUT）命令来打印关于权限列表权限的信息。图 3 显示该报告的一个样本。

专用权限（完整报告）

SYSTEM4

权限列表	所有者	主组	用户	权限	列表管理	对象 操作	对象 管理	对象 存在	对象 变更	对象 引用	数据 读	数据 添加	数据 更新	数据 删除	数据 执行
LIST1	QSECOFR	*NONE	*PUBLIC	*EXCLUDE											
LIST2	BUDNIKR	*NONE	BUDNIKR	*ALL	X	X	X	X	X	X	X	X	X	X	X
			*PUBLIC	*CHANGE		X					X	X	X	X	X
LIST3	QSECOFR	*NONE	*PUBLIC	*EXCLUDE											
LIST4	CJWLDR	*NONE	CJWLDR	*ALL	X	X	X	X	X	X	X	X	X	X	X
			GROUP1	*ALL		X	X	X	X	X	X	X	X	X	X
			*PUBLIC	*EXCLUDE											

图 3. 权限列表的专用权限报告

此报告显示您在“编辑权限列表”（EDTAUTL）屏幕上看到的相同信息。该报告的优点是它在一个位置提供关于所有权限列表的信息。例如，如果您正在为一组新对象设置安全性，则可以快速浏览该报告来查看现有权限列表是否满足您对于那些对象的需要。

可以打印报告的更改版本来查看新的权限列表或自上次打印报告以来权限已更改的权限列表。也可以选择打印每个权限列表所保护的对象列表。图 4 显示一个权限列表的报告示例:

显示权限列表对象

```
权限列表 . . . . . :   CUSTAUTL
库 . . . . . :   QSYS
所有者 . . . . . :   AROWNER
主组 . . . . . :   *NONE
```

对象	库	类型	所有者	主组	文本
CUSTMAS	CUSTLIB	*FILE	AROWNER	*NONE	
CUSTORD	CUSTORD	*FILE	OEOWNER	*NONE	

图 4. 显示权限列表对象报告

例如，可以使用此报告来了解将新用户添加至权限列表的结果（该用户将接收到什么权限）。

使用权限列表

“iSeries 导航器”提供一些安全性功能部件，该功能部件设计成帮助您开发安全性计划和策略并将您的系统配置为满足您公司的需要。其中一项可用的功能是使用权限列表。

权限列表具有下列功能部件。

- 权限列表根据相似安全性需求将对象分组。
- 权限列表在概念上包含用户和组的列表以及每个用户和组对由列表保护的对象所具有的权限。
- 每个用户和组对于列表保护的对象集可以具有不同的权限。
- 可以通过列表给出权限，而不是对单独的用户和组给出权限。

使用权限列表可以执行的任务包括以下任务。

- 创建权限列表
- 更改权限列表。
- 添加用户和组。
- 更改用户许可权。
- 显示受保护的对象。

要使用此功能，执行下列步骤:

1. 从“iSeries 导航器”，展开您的服务器 —> 安全性。您将看到**权限列表**和**策略**。
2. 右键单击**权限列表**并选择**新建权限列表**。**新建权限列表**允许您执行下列操作。
   - **使用**: 允许访问对象属性和使用对象。公众可以查看但不能更改这些对象。
   - **更改**: 允许更改对象的内容（具有某些例外）。
   - **全部**: 允许对对象执行所有操作，除了那些限制于所有者的操作。用户或组可以控制对象的存在、指定对象的安全性、更改对象以及对对象执行基本功能。用户或组也可以更改对象的所有权。
   - **排除**: 禁止对对象执行所有操作。对于具有此许可权的用户和组，不允许对对象进行任何访问或操作。指定不允许公众使用该对象。

当使用权限列表时，您将要对对象和数据授予许可权。以下列示了您可以选择的对象许可权。

- **操作**: 提供查看对象的描述和使用对象的许可权，它由用户或组对对象所具有的数据许可权确定。
- **管理**: 提供指定对象的安全性、移动或重命名对象以及将成员添加至数据库文件的许可权。
- **存在**: 提供控制对象的存在和所有权的许可权。用户或组可以删除对象、释放对象的存储器、对对象执行保存和恢复操作和转移对象的所有权。如果用户或组具有特殊保存许可权，则该用户或组不需要对象存在许可权。
- **变更**（仅用于数据库文件和 SQL 程序包）: 提供变更对象的属性所需要的许可权。如果用户或组对数据库文件具有此许可权，则该用户或组可以添加和除去触发器，添加和除去引用和唯一约束以及更改该数据库文件的属性。如果用户或组对 SQL 程序包具有此许可权，则用户或组可以更改该 SQL 程序包的属性。此许可权当前仅用于数据库文件和 SQL 程序包。

- **引用**（仅用于数据库文件和 SQL 程序包）：提供从另一个对象引用某个对象以使对那个对象的操作可以受其它对象限制所需要的许可权。如果用户或组对物理文件具有此许可权，则该用户或组可以添加引用约束，其中该物理文件是父代。此许可权当前仅用于数据库文件。

以下列示您可以选择的数据许可权。

- **读**：提供获取和显示对象的内容（如查看某个文件中的记录）所需要的许可权。
- **添加**：提供将项添加至对象（如将消息添加至消息队列或将记录添加至文件）的许可权。
- **更新**：提供更改对象中的项（如更改文件中的记录）的许可权。
- **删除**：提供从对象除去项（如从消息队列除去消息或从文件删除记录）的许可权。
- **执行**：提供运行程序、服务程序或 SQL 程序包所需要的许可权。用户也可以定位在库或目录中的对象。

有关当您在创建或编辑权限列表时的每个进程的更多信息，使用在“iSeries 导航器”中可获得的联机帮助。

在“iSeries 导航器”中访问策略

可以使用“iSeries 导航器”来查看和管理 iSeries 服务器的策略。“iSeries 导航器”具有 5 个策略区域:

- **审计策略**
  此策略允许您对特定操作和系统上特定资源的访问设置监控。
- **安全策略**
  此策略允许您指定安全性的级别以及与系统安全性相关的附加选项。
- **密码策略**
  此策略允许您为系统指定密码级别。
- **恢复策略**
  此策略允许您指定如何在系统上恢复某些对象。
- **注册策略**
  此策略允许您指定用户可以如何注册到系统。

要使用“iSeries 导航器”查看或更改策略，遵循以下步骤:

1. 在“iSeries 导航器”中，展开您的服务器 —> **安全性**。
2. 右键单击**策略**并选择**资源管理**来显示您可以创建和管理的策略列表。有关这些策略的详细信息，请参阅“iSeries 导航器”帮助。

监控对象的专用权限

SECBATCH 菜单选项:

12（*立即提交*）**41**（*使用作业调度程序*）

可以使用“打印专用权限”（PRTPVTAUT）命令来打印在指定的库中指定类型的对象的所有专用权限列表。

可以使用此报告来帮助您检测对对象的新权限。它也可以帮助您防止专用权限方案变得复杂和难以管理。

监控对输出队列和作业队列的访问

有时安全管理员执行保护对文件的访问的大型作业，而接着在打印文件的内容时忘记所发生的事情。iSeries 服务器为您提供了一些功能来保护敏感的输出队列和作业队列。例如，您可以保护输出队列以使未授权用户不能查看或复制正在等待打印的机密假脱机文件。您可以保护作业队列以使未授权用户不能将机密作业重定向至非机密的输出队列或完全取消该作业。

SECBATCH 菜单选项:

24（**立即提交**）**63**（*使用作业调度程序*）

在“信息中心”中的 *Basic system security and planning* 和 *iSeries Security Reference* 这两本书描述如何保护输出队列和作业队列。

您可以使用“打印队列权限”（PRTQAUT）命令来打印系统上作业队列和输出队列的安全性设置。然后可以评估打印机密信息的打印作业并确保将它们发送至受保护的输出队列和作业队列。

对于您认为是安全性敏感的输出队列和作业队列，您可以将您的安全性设置与 *iSeries Security Reference* 一书的 Appendix D 中的信息进行比较。在 Appendix D 中的表指示执行不同的输出队列和作业队列功能需要哪些设置。

监控特权

当系统上的用户具有不必要的特权时，可能会浪费您开发良好对象权限方案的努力。当用户概要文件具有 *ALLOBJ 特权时对象权限无意义。无论您怎样努力来保护您的输出队列，具有 *SPLCTL 特权的用户均可以查看系统上的任何假脱机文件。具有 *JOBCTL 特权的用户可以影响系统操作和重定向作业。具有 *SERVICE 特权的用户可能能够使用服务工具来存取数据，而不必通过操作系统。

SECBATCH 菜单选项:

29（立即提交）68（*使用作业调度程序*）

可以使用“打印用户概要文件”（PRTUSRPRF）命令来打印有关系统上的用户概要文件的特权和用户类的信息。当您运行报告时，您具有几个选项:

- 所有用户概要文件
- 具有特定特权的用户概要文件
- 具有特定用户类的用户概要文件
- 在用户类和特权之间具有不匹配的用户概要文件

图 5 显示报告的一个示例，该报告显示所有用户概要文件的特权:

```
                                        用户概要文件信息
报告类型 . . . . . :   *AUTINFO
  选择条件 . . . . . :   *SPCAUT
  特权 . . . . . :   *ALL
                    ----------------特权----------------
                                *IO                                                          组
用户      组        *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL   用户                 组          权限        限制
概要文件  概要文件   OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL   类          所有者  权限        类型        能力
USERA     *NONE      X     X     X    X     X     X     X     X    *SECOFR     *USRPRF  *NONE       *PRIVATE    *NO
USERB     *NONE                       X     X                       *PGMR       *USRPRF  *NONE       *PRIVATE    *NO
USERC     *NONE      X     X     X    X     X     X     X     X    *SECOFR     *USRPRF  *NONE       *PRIVATE    *NO
USERD     *NONE                                                     *USER       *USRPRF  *NONE       *PRIVATE    *NO
```

图 5. 用户信息报告: 示例 1

除特权外，报告还显示下列内容:

- 用户概要文件是否具有限制能力。
- 用户或用户的组是否拥有用户创建的新对象。
- 用户的组自动接收对用户创建的新对象的什么权限。

图 6 显示不匹配的特权和用户类的报告示例:

```
用户概要文件信息
报告类型 . . . . . :   *AUTINFO
选择条件 . . . . . :   *MISMATCH
------------------------------特权----------------
                                *IO                                                          组
用户      组        *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL   用户                 组          权限        限制
概要文件  概要文件   OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL   类          所有者  权限        类型        能力
USERX     *NONE      X                 X     X                 X    *SYSOPR     *USRPRF  *NONE       *PRIVATE    *NO
USERY     *NONE                                    X               *USER       *USRPRF  *NONE       *PRIVATE    *NO
USERZ                                              X               *USER       *USRPRF  *NONE       *PRIVATE    *NO
          QPGMR                       X     X
```

图 6. 用户信息报告: 示例 2

在图 6 中，注意下列情况:

- USERX 具有系统操作员（*SYSOPR）用户类但具有 *ALLOBJ 和 *SPLCTL 特权。
- USERY 具有用户（*USER）用户类但具有 *SECADM 特权。
- USERZ 也具有用户（*USER）类和 *SECADM 特权。您也可以查看到 USERZ 是 QPGMR 组的成员，该组具有 *JOBCTL 和 *SAVSYS 特权。

可以定期运行这些报告来帮助您监控用户概要文件的管理。

监控用户环境

用户概要文件的一个作用是定义用户的环境，包括输出队列、初始菜单和作业描述。用户的环境影响用户如何查看系统并在某种程序上影响允许用户执行什么操作。用户必须对用户概要文件中指定的对象具有权限。然而，如果您的权限方案仍在进行中或限制不是很严格，则在用户概要文件中定义的用户环境可能会产生您不想要的结果。以下是几个示例:

SECBATCH 菜单选项:

29（*立即提交*）**68**（*使用作业调度程序*）

- 用户的作业描述可能指定比用户具有更多权限的用户概要文件。
- 用户可能具有不带命令行的初始菜单。然而，用户的注意键处理程序可以提供命令行。
- 可能授权用户来运行机密报告。然而，可以将用户的输出定向至对不应该看到报告的用户可用的输出队列。

可以使用“打印用户概要文件”（PRTUSRPRF）命令的 *ENVINFO 选项来帮助您监控为系统用户定义的环境。图 7 显示报告的示例:

```
                                  用户概要文件信息
  报告类型 . . . . . :   *ENVINFO
  选择条件 . . . . . :   *USRCLS
                          初始          初始          作业          消息          输出          辅助操作请求
用户          当前        菜单 /        程序 /        描述 /        队列 /        队列 /        程序 /
概要文件      库          库            库            库            库            库            库
AUDSECOFR     AUDITOR     MAIN          *NONE         QDFTJOBD      QSYSOPR       *WRKSTN       *SYSVAL
                          *LIBL                       QGPL           QSYS
USERA         *CRTDFT     OEMENU        *NONE         QDFTJOBD      USERA         *WRKSTN       *SYSVAL
                          *LIBL                       QGPL           QUSRSYS
USERB         *CRTDFT     INVMENU       *NONE         QDFTJOBD      USERB         *WRKSTN       *SYSVAL
                          *LIBL                       QGPL           QUSRSYS
USERC         *CRTDFT     PAYROLL       *NONE         QDFTJOBD      USERC         PAYROLL       *SYSVAL
                          *LIBL                       QGPL           QUSRSYS        PRPGMLIB
```

图 7. 打印用户概要文件 – 用户环境示例

管理服务工具

服务工具用来配置、管理和维护服务器。可以从专用服务工具（DST）或系统服务工具（SST）来访问服务工具。需要服务工具用户标识来访问 DST、SST 和使用“iSeries 导航器”功能进行逻辑分区（LPAR）管理和磁盘机管理。

当启动了“许可内码”时，DST 就可用，即使尚未装入 OS/400。SST 可从 OS/400 获得。下表概述 DST 和 SST 之间的基本差别。

特征	DST	SST

如何访问	在手工 IPL 期间通过控制台物理访问或通过在控制面板上选择选项 21。	使用通过 QSRV 或下列权限注册的能力通过交互式作业访问: • 已授权的对 STRSST（启动 SST）CL 命令的权限。 • 服务特权（*SERVICE）或所有对象特权（*ALLOBJ）。 • 使用 SST 的功能特权。
何时可用	甚至当服务器具有限制能力也可用。不需要 OS/400 来访问 DST。	当启动了 OS/400 时可用。需要 OS/400 才能访问 SST。
如何认证	需要服务工具用户标识和密码。	需要服务工具用户标识和密码。

有关使用“服务工具”来执行下列任务的信息，请参阅 iSeries 信息中心 —> 安全性 —> 服务工具:

- 使用 DST 访问服务工具
- 使用 SST 访问服务工具
- 使用“iSeries 导航器”访问服务工具
- 创建服务工具用户标识
- 更改服务工具用户标识的功能特权
- 更改服务工具用户标识的描述
- 显示服务工具用户标识
- 启用或禁用服务工具用户标识
- 删除服务工具用户标识
- 使用 SST 或 DST 更改服务工具用户标识和密码
- 使用 STRSST 更改服务工具用户标识密码
- 使用工具来更改服务工具用户标识和密码
- 更改服务工具用户标识（QSYCHGDS）API
- 复位 QSECOFR OS/400 用户概要文件密码
- 复位 QSECOFR 服务工具用户标识和密码
- 保存服务工具安全性数据和恢复服务工具安全性数据
- 创建您自己的 QSECOFR 服务工具用户标识的版本
- 为 DST 配置服务工具服务器
- 为 OS/400 配置服务工具服务器
- 通过 DST 监控服务功能使用
- 通过 OS/400 安全性审计日志监控服务工具使用

有关访问“iSeries 信息中心”的信息，请参阅第 xii 页的『先决条件和相关信息』。

第 7 章 使用逻辑分区安全性（LPAR）

可以在下列方案中证明在一个 iSeries 服务器上建立多个逻辑分区是有益的。

- **维护独立系统**: 将资源（磁盘存储单元、处理器、内存和 I/O 设备）的一部分专门用于分区可以实现软件的逻辑隔离。如果正确配置逻辑分区，则逻辑分区也具有某些硬件容错能力。可以隔离交互式和批处理工作量，这些工作量在一个机器上可能不能一起很好地运行，而可以在单独的分区中有效地运行。
- **合并**: 逻辑上分区的系统可以减少企业内所需要的 iSeries 服务器系统的数目。可以将几个系统合并为单个逻辑上分区的系统。消除了对附加设备的需要及其费用。当需求更改时，可以将资源从一个逻辑分区移动到另一个分区。
- **创建混合的生产和测试环境**: 可以创建生产和测试组合式环境。可以在主分区中创建单个生产分区。有关多个生产分区，请参阅以下的*创建多个生产分区环境*。

  逻辑分区是测试或生产分区。生产分区运行您的主要商业应用程序。生产分区中的故障会显著妨碍商业运作并花费您的时间和金钱。测试分区测试软件。测试分区中的故障（当不必计划时）将不会破坏正常的商业运作。
- **创建多个生产分区环境**: 仅在辅助分区中应该创建多个生产分区。在此情况下，将主分区专门用于分区管理。
- **热备份**: 当辅助分区复制至同一系统中的另一个逻辑分区时，可以将分区故障期间切换至备份带来的不便减少至最小。此配置也最小化长时间保存窗口的影响。可以使备份分区脱机并保存，而其它逻辑分区继续执行生产工作。将需要特殊软件来使用此热备份策略。
- **集成群集**: 当使用 OptiConnect/400 以及高可用性应用软件时，已分区的系统可以作为集成群集运行。可以使用集成群集来保护系统，使其不受辅助分区内的大多数意外故障的影响。

注: 设置次分区时，需要特别注意卡的位置。如果为控制台选择的“输入／输出处理器”（IOP）具有 LAN 卡而该 LAN 卡不打算用于“操作控制台”，则也将激活它以供控制台使用，这样就不能如您所愿使用它了。有关使用“操作控制台”的更多信息，请参阅 第 59 页的第 8 章，『iSeries 操作控制台』。

有关此主题的更多详细信息，参阅 iSeries 信息中心中的“逻辑分区”。

管理逻辑分区的安全性

在已分区的系统上执行的与安全性相关的任务与在没有逻辑分区的系统上执行的任务相同。然而，当创建逻辑分区时，可以使用多个独立系统。因此，将必须在每个逻辑分区上执行同样的任务，而不是在没有逻辑分区的系统上仅执行一次任务。

此处是在逻辑分区上处理安全性时要记住的一些基本规则。

- 每次将用户添加至系统的一个逻辑分区。需要将用户添加至想要他们访问的每个逻辑分区。
- 限制有权转至主分区上的专用服务工具（DST）和系统服务工具（SST）的用户数。有关 DST 和 SST 的更多信息，请参阅“iSeries 信息中心”中的“使用 iSeries 导航器、DST 和 SST 管理逻辑分区”主题。有关使用服务工具用户概要文件来控制对分区活动的访问的信息，参阅第 55 页的『管理服务工具』。

注: 使用“iSeries 导航器”访问 LPAR 功能之前，必须初始化“服务工具服务器”（STS）。请参阅 iSeries 信息中心 —> 安全性 —> 服务工具以获取相关信息。有关访问“iSeries 信息中心”的信息，请参阅第 xii 页的『先决条件和相关信息』。

- 辅助分区无法看到或使用主存储器和另一个逻辑分区的磁盘机。
- 辅助分区只能看到它们自己的硬件资源。
- 主分区可以看到 DST 和 SST“使用系统分区”屏幕中的所有系统硬件资源。
- 主分区操作系统仍然只能看到它可用的资源。
- 系统控制面板控制主分区。当将面板方式设置为“安全”时，在 SST 的“使用分区状态”屏幕上不能执行任何操作。要从系统控制面板强制实施 DST，必须将该方式更改为“手工”。
- 当将辅助分区的操作方式设置为安全时，以下列方式限制“使用分区状态”的用法:
  - 只能在辅助分区中使用 DST 来更改分区状态；不能使用 SST 来更改分区状态。
  - 只能使用 DST 或 SST 从主分区“使用分区状态”屏幕强制在辅助分区中的 DST。
  - 只能在主分区中使用 DST 来将辅助分区方式从安全更改为任何其它值。

一旦辅助分区的方式不再是安全时，就可以在该辅助分区中使用 DST 和 SST 来更改分区状态。

有关在 iSeries 服务器上的安全性的更多信息，参阅 Security Reference 一书和 iSeries 信息中心的“基本系统安全性和计划”页面。

第 8 章 iSeries 操作控制台

“操作控制台”允许您使用 PC 来访问和控制 iSeries 服务器。“操作控制台”包含对没有控制台设备的 iSeries 服务器的远程 PC 拨入支持，从而允许远程 PC 成为控制台。当使用“操作控制台”时，注意下列事项:

- 可以从“操作控制台”执行任何可以从传统控制台执行的任务。例如，具有 *SERVICE 或 *ALLOBJ 特权的用户概要文件能够注册到“操作控制台”会话，即使已禁用它们。
- “操作控制台”使用“服务工具用户概要文件”和密码来启用与 iSeries 服务器的连接。这使得更改“服务工具用户概要文件”和密码特别重要。黑客可能熟悉缺省“服务工具用户概要文件”用户标识和密码，并且可能会使用它们尝试与 iSeries 服务器的远程控制台会话。请参阅第 18 页的『更改已知密码』和第 22 页的『避免缺省密码』以获取有关密码的技巧。
- 使用“远程控制台”时要保护信息，使用 Windows“拨号网络”的回拨选项。
- 设置次分区时，需要特别注意卡的位置。如果为控制台选择的“输入／输出处理器”（IOP）也具有 LAN 卡且不打算将该 LAN 卡用于“操作控制台”，则将激活它以供控制台使用，您可能无法将它用于预期的目的。

在 V5R1 中，增强了“操作控制台”以允许在局域网（LAN）上执行控制台活动。增强的认证和数据加密为控制台过程提供了网络安全性。要使用具有 LAN 连接性的操作控制台，强烈鼓励您安装下列产品:

- 加密访问提供程序 5722–AC2 或 5722–AC3（在 iSeries 服务器上）。
- Client Encryption 5722–CE2 或 5722–CE3（在“操作控制台”PC 上）。

为了加密控制台数据，iSeries 服务器必须已安装一个“加密访问提供程序”产品**且** PC 必须已安装一个 Client Encryption 产品。

注: 如果未安装加密产品，则将没有任何数据加密。

下表总结了可用产品的加密结果:

表 13. 加密结果

iSeries 服务器上的“加密访问提供程序”	**“操作控制台”PC 的 Client Encryption**	**产生的数据加密**
无	无	无
5722–AC2	5722–CE2	56 位
5722–AC2	5722–CE3	56 位
5722–AC3	5722–CE2	56 位
5722–AC3	5722–CE3	128 位

有关设置和管理 iSeries“操作控制台”的附加信息，请参阅“iSeries 信息中心”。

操作控制台安全性概述

“操作控制台”安全性包含:

- 控制台设备认证
- 用户认证
- 数据保密
- 数据完整性

具有直接连接性的“操作控制台”由于它的点到点连接而具有隐式设备认证、数据保密和数据完整性。用户认证安全性是注册到控制台显示器所必需的。

控制台设备认证

控制台设备认证确保哪个物理驱动器是控制台。具有直接连接性的“操作控制台”使用类似于双轴电缆控制台的物理连接。类似于双轴电缆连接，使用直接连接的“操作控制台”在物理上可能受到保护，以控制对物理控制台设备的访问。

具有 LAN 连接性的操作控制台使用的安全套接字层（SSL）版本支持设备和用户认证但不使用证书。对于此格式的连接，设备认证基于服务工具设备概要文件。有关更多详细信息，参阅 61。

用户认证

用户认证提供关于谁在使用控制台设备的保证。与用户认证相关的所有问题都相同而与控制台类型无效。

数据保密

数据保密提供只能由期望的收件人读取控制台数据的信用。具有直接连接性的“操作控制台”使用类似于双轴电缆控制台或安全网络连接的物理连接来获取 LAN 连接性以保护控制台数据。使用直接连接的“操作控制台”具有与双轴电缆连接相同的数据保密。如果物理连接是安全的，则控制台数据仍是受保护的。

如果安装了适当的加密产品（ACx 和 CEx），则具有 LAN 连接性的操作控制台使用安全网络连接。取决于安装在 iSeries 服务器和运行“操作控制台”的 PC 上的加密产品，控制台会话使用可能的最强加密。

注: 如果未安装加密产品，则将没有任何数据加密。

数据完整性

数据完整性提供将控制台数据路由到接收方的途中不发生任何更改的信用。具有直接连接性的“操作控制台”使用类似于双轴电缆控制台或安全网络连接的物理连接来获取 LAN 连接性以保护控制台数据。使用直接连接的“操作控制台”与双轴电缆连接具有相同的数据完整性。如果物理连接是安全的，则控制台数据仍是受保护的。

如果安装了适当的加密产品（ACx 和 CEx），则具有 LAN 连接性的操作控制台使用安全网络连接。取决于安装在 iSeries 服务器和运行“操作控制台”的 PC 上的加密产品，控制台会话使用可能的最强加密。

注: 如果未安装加密产品，则将没有任何数据加密。

使用具有 LAN 连接性的操作控制台

注: 任何“操作控制台”设备都可以是控制台，但只有基于 LAN 的配置使用服务工具用户概要文件。

iSeries 服务器在交付时具有缺省服务工具设备概要文件 QCONSOLE 和缺省密码 QCONSOLE。在每次成功的连接期间，具有 LAN 连接性的操作控制台都将更改密码。有关更多信息，请参阅『使用操作控制台安装向导』。

有关具有 LAN 连接性的“iSeries 操作控制台”的附加信息，参阅“信息中心”中的主题“配置具有 LAN 连接性的操作控制台”。

保护具有 LAN 连接性的操作控制台

使用具有 LAN 连接性的操作控制台时，建议以下各项:

- 创建另一个具有控制台属性的服务工具设备概要文件并将概要文件信息存储在安全位置。
- 在 iSeries 服务器上安装“加密访问提供程序”5722–AC2 或 5722–AC3，在“操作控制台”PC 上安装 Client Encryption 5722–CE2 或 5722–CE3。
- 选择非平常服务设备信息密码。
- 以保护双轴电缆控制台或具有直接连接性的“操作控制台”的相同方式保护“操作控制台”PC。

使用操作控制台安装向导

安装向导将在使用具有 LAN 连接性的操作控制台时将必要的信息添加到 PC。安装向导需要服务工具设备概要文件、服务工具设备概要文件密码和密码来保护服务工具设备概要文件信息。

注: 服务工具设备概要文件信息密码用于锁定和解锁 PC 上的服务工具设备概要文件信息（服务工具设备概要文件和密码）。

建立网络连接时，“操作控制台”安装向导将提示您输入服务设备信息密码以访问加密服务工具设备概要文件和密码。也将提示您输入有效的服务工具用户标识和密码。

第 9 章 检测可疑程序

计算机使用中的最新趋势增加了您的系统具有来自不可信源的程序或具有执行未知功能的程序的可能性。以下是一些示例:

- 个人计算机用户有时从其它 PC 用户获取程序。如果将该 PC 连接至您的 iSeries 系统，则该程序会影响您的 iSeries 服务器。
- 连接至网络的用户也可以获取程序，例如从公告牌获取程序。
- 黑客已变得更活跃和有名。他们经常发布他们的方法和他们的结果。这会导致正常守法的程序员进行模仿。

这些趋势已导致计算机安全性中的问题，称为**计算机病毒**。病毒是可以更改其它程序来包括它本身的副本的一种程序。则称其它程序为受病毒传染。此外，病毒可以执行可占用系统资源或破坏数据的其它操作。

iSeries 服务器的体系结构提供某些保护，以防止计算机病毒的传染特征。『预防计算机病毒』描述了此问题。iSeries 服务器安全管理员需要更加注意执行未授权功能的系统。本章中剩余的主题描述了不怀好意的某人可能设置有害程序在您的系统上运行的方式。这些主题提供防止程序执行未授权功能的技巧。

安全性技巧

对象权限始终是第一道防线。如果没有保护对象的良好计划，则系统无防御。本资料讨论授权用户可能尝试利用对象权限方案中的环路漏洞的方法。

预防计算机病毒

具有病毒传染的计算机具有可以更改其它程序的程序。iSeries 基于对象的体系结构比具有其它计算机体系结构更使恶作剧制造者难以生成和传播此类型的病毒。在 iSeries 服务器上，对各种类型的对象使用特定命令和指示信息工作。不能使用文件指令来更改可操作的程序对象（这是大多数病毒创建者执行的操作）。也不能轻易地创建更改另一个程序对象的程序。执行此操作需要相当多的时间、努力和专门知识，并且它需要访问并非一般可用的工具和文档。

然而，当新的 iSeries 服务器功能可用来参与到开放式系统环境中时，iSeries 服务器的某些基于对象的保护功能不再适用。例如，对于集成文件系统（IFS），用户可以直接操作目录中的某些对象，如流文件。

此外，尽管 iSeries 服务器体系结构使病毒难以在 iSeries 服务器程序中传播，但是它的体系结构不能阻止 iSeries 服务器成为病毒载体。作为文件服务器，iSeries 服务器可以存储许多 PC 用户共享的程序。这些程序中的任何一个可以包含 iSeries 服务器检测不到的病毒。要防止此类型的病毒传染连接至 iSeries 服务器的 PC，必须使用 PC 病毒扫描软件。

在 iSeries 服务器上存在几个功能以防止某个人将低级语言与指针能力一起使用来变更可操作的对象程序:

- 如果您的系统在安全级别 40 或更高级别上运行，则完整性保护包括防止更改程序对象的保护。例如，您不能成功地运行包含有阻塞的（保护的）机器指令的程序。
- 当您恢复在另一个系统上保存（并且可能已更改）的程序时，程序验证值也将保护您。 *iSeries Security Reference* 一书中的 Chapter 2 描述安全级别 40 或更高级别的完整性保护功能，包括程序验证值。

  注: 程序验证值不是防错误操作的，并且在评估恢复到系统的程序时，它不是警戒的替代。

几个工具也可用来帮助您检测将变更的程序引入到系统中:

- 可以使用“检查对象完整性”（CHKOBJITG）命令 来扫描满足搜索值的对象（可操作的对象）来确保尚未变更那些对象。它类似于病毒扫描功能。
- 可以使用安全性审计功能来监控更改或恢复的程序。 权限级别系统值的 *PGMFAIL、*SAVRST 和 *SECURITY 值提供审计记录，这些记录可以帮助您检测到将病毒类型的程序引入到您的系统中的尝试。在 *iSeries Security Reference* 一书中的 Chapter 9 和 Appendix F 提供有关审计值和审计日志项的更多信息。
- 可以使用“更改 程序”（CHGPGM）命令的强制创建（FRCCRT）参数来重新创建已恢复到系统的任何程序。系统使用程序模板来重新创建程序。如果编译程序对象之后已更改了它，则系统重新创建已更改的对象并替换它。如果程序模板包含阻塞（保护）的指令，系统将不能成功重新创建程序。
- 当程序恢复到系统时，可以使用 QFRCCVNRST（在恢复时强制转换）系统值来重新创建程序。系统使用程序模板来重新创建程序。此系统值提供关于重新创建哪些程序的几个选项。
- 可以使用 QVFYOBJRST（在恢复时验证对象）系统值来防止恢复不具有数字签名或不具有有效数字签名的程序。当数字签名无效时，它表示自程序的开发者签署程序以来已更改程序。存在允许您签署您自己的程序、保存文件和流文件的 API。

有关签署和可以如何使用它来保护系统以免受到攻击的更多信息，请参阅第 74 页的『对象签名』。

监控沿用权限的使用

在 iSeries 服务器上，您可以创建沿用程序的所有者的权限的程序。这表示运行程序的任何用户与拥有程序的用户概要文件具有相同的权限（专用权限和特权）。

当正确使用沿用权限时，它是一个重要的安全性工具。例如，第 40 页的『使用对象安全性提高菜单访问控制』描述如何组合沿用权限和菜单来帮助您扩展为超过菜单访问控制。可以使用沿用权限来保护重要文件，以免当您仍然允许对文件的查询时在您批准的应用程序之外更改文件。

作为安全管理员，您应该确保正确使用沿用权限:

- 程序应该沿用用户概要文件的权限，该概要文件只具有执行必要功能的足够权限，而不是过多权限。应该特别小心沿用具有 *ALLOBJ 特权或拥有重要对象的用户概要文件的权限的程序。
- 沿用权限的程序应该具有特定的限制功能，而不应该提供命令输入能力。
- 应该正确保护沿用权限的程序。

- 沿用权限的过多使用可能对系统性能具有负面影响。为了帮助您避免性能问题，复查在 *iSeries Security Reference* 一书的 Chapter 5 中使用沿用权限的权限检查流程图和建议。

SECBATCH 菜单选项:
1（*立即提交*）**40**（**使用作业调度程序**）

可以使用“打印沿用对象”（PRTADPOBJ）命令（在 SECTOOLS 菜单中的选项 21）来帮助您监控在系统上沿用权限的使用。

报告显示指定用户概要文件的特权、沿用用户概要文件的权限的程序以及使用概要文件的权限的 ASP 设备。在建立了信息库之后，可以定期打印沿用对象报告的更改版本。它列示沿用权限的新程序和自上次运行报告以来已更改为沿用权限的程序。

如果您怀疑在系统上错用了沿用权限，则可以将 QAUDLVL 系统值设置为包括 *PGMADP。 当此值活动时，每当某个人启动或结束沿用权限的程序时系统创建审计日志项。该项包括启动程序的用户的名称和程序的名称。

限制沿用权限的使用

当 iSeries 程序运行时，程序可以用两种不同的方法来使用沿用权限以获取对对象的访问权:

- 程序自己可以沿用它自己的权限。在程序或服务程序的用户概要文件（USRPRF）参数中指定它。
- 程序可以使用（继承）仍在作业的调用堆栈中的先前程序的沿用权限。程序可以继承先前程序的沿用权限，即使该程序本身不沿用权限。程序或服务程序的“使用沿用权限”（USEADPAUT）参数控制程序是否继承程序堆栈中先前程序的沿用权限。

以下是使用先前程序的沿用权限如何工作的示例。

假定 ICOWNER 用户概要文件对 ITEM 文件具有 *CHANGE 权限并且 ITEM 文件的公共权限是 *USE。没有其它的用户概要文件对 ITEM 文件具有任何显式定义的权限。表 14 显示使用 ITEM 文件的三个程序的属性:

表 14. 使用沿用权限（USEADPAUT）示例

程序名	程序所有者	USRPRF 值	USEADPAUT 值
PGMA	ICOWNER	*OWNER	*YES
PGMB	ICOWNER	*USER	*YES
PGMC	ICOWNER	*USER	*NO

示例 1 - 沿用权限:
1. USERA 运行 PGMA 程序。
2. PGMA 程序尝试用更新能力打开 ITEM 文件。

结果: 尝试成功。因为 PGMA 沿用 ICOWNER 的权限，所以 USERA 对 ITEM 文件具有 *CHANGE 访问权。

示例 2 – 使用沿用权限:

1. USERA 运行 PGMA 程序。
2. PGMA 程序调用 PGMB 程序。
3. PGMB 程序尝试用更新能力打开 ITEM 文件。

结果: 尝试成功。尽管 PGMB 程序未沿用权限（*USRPRF 是 *USER），但它允许使用先前的沿用权限（*USEADPAUT 是 *YES）。PGMA 程序仍在程序堆栈中。因为 PGMA 沿用 ICOWNER 的权限，因此，USERA 获取对 ITEM 文件的 *CHANGE 访问权。

示例 3 – 不使用沿用权限:

1. USERA 运行 PGMA 程序。
2. PGMA 程序调用 PGMC 程序。
3. PGMC 程序尝试用更新能力打开 ITEM 文件。

结果: 权限故障。PGMC 程序不沿用权限。PGMC 程序也不允许使用先前程序的沿用权限。尽管 PGMA 仍在调用堆栈中，但不使用它的沿用权限。

防止新程序使用沿用权限

将沿用权限传送到堆栈中后面的程序为在行的程序员提供了创建“特洛伊木马”程序的机会。“特洛伊木马”程序 可以依靠堆栈中的先前程序来获取它进行捣乱所需要的权限。要防止这一点，您可以限制允许哪些用户创建使用先前程序的沿用权限的程序。

您创建新程序时，系统自动将 USEADPAUT 参数设置为 *YES。如果不想程序继承沿用权限，必须使用“更改程序”（CHGPGM）命令或“更改服务程序”（CHGSRVPGM）来将 USEADPAUT 参数设置为 *NO。

可以使用权限列表和“使用沿用权限”（QUSEADPAUT）系统值来控制谁可以创建继承沿用权限的程序。当在 QUSEADPAUT 系统值内指定权限列表名称时，系统使用此权限列表来确定如何创建新程序。

当用户创建程序或服务程序时，系统检查用户对权限列表的权限。如果用户具有 *USE 权限，则新建程序的 USEADPAUT 参数设置为 *YES。如果用户不具有 *USE 权限，则 USEADPAUT 参数设置为 *NO。用户对权限列表的权限不能来自沿用权限。

在 QUSEADPAUT 系统值中指定的权限列表也控制用户是否可以使用 CHGxxx 命令来为程序或服务程序设置 USEADPAUT 值。

注:

1. 不必将您的权限列表称为 QUESADPAUT。可以用不同的名称创建权限列表。然后指定 QUSEADPAUT 系统值的权限列表。在此示例的命令中，替换上您的权限列表的名称。
2. QUSEADPAUT 系统值不会影响系统上现有的程序。使用 CGHPGM 命令或 CHGSRVPGM 命令来对现有程序设置 USEADPAUT 参数。

有更多限制的环境: 如果想要多数用户在创建新程序时将 USEADPAUT 参数设置为 *NO，执行下列操作:

1. 要将权限列表的公共权限设置为 *EXCLUDE，输入下列命令:

```
CHGAUTLE AUTL(QUSEADPAUT) USER(*PUBLIC)
   AUT(*EXCLUDE)
```

2. 要设置特定用户来创建使用先前程序的沿用权限的程序，输入下列命令:

```
ADDAUTLE AUTL(QUSEADPAUT) USER(user-name)
   AUT(*USE)
```

具有较少限制的环境: 如果想要多数用户在创建新程序时将 USEADPAUT 参数设置为 *NO，执行下列操作:

1. 将权限列表的公共权限设置为 *USE。
2. 要防止特定用户创建使用先前程序的沿用权限的程序，输入下列命令:

```
ADDAUTLE AUTL(QUSEADPAUT)
   USER(user-name) AUT(*EXCLUDE)
```

监控触发器程序的使用

DB2® UDB 提供将触发器程序与数据库文件关联的能力。触发器程序能力在高功能数据库管理器的产业中是常见的。

当将触发器程序与数据库文件关联时，指定该触发器程序何时运行。例如，可以将客户定单文件设置为每当将新记录添加至该文件时运行触发器程序。当客户的未付余额超过信贷限额时，触发器程序可以向客户打印警告信函并将消息发送给信贷经理。

触发器程序是一种提供应用程序功能和管理信息的有效方法。触发器程序也为具有不正当目的的某个人提供在您的系统上创建“特洛伊木马程序”的能力。破坏性的程序可能正在坐着等待当系统上的数据库文件中发生某个事件时运行。

注: 在历史上，“特洛伊木马”是一个大的空心木马，里面装满了希腊士兵。在将该木马送进特洛伊的围墙内后，士兵从木马中爬出并与特洛伊人战斗。在计算机领域中，常常将隐藏破坏功能的程序称为“特洛伊木马”。

SECBATCH 菜单选项:

27（*立即提交*）**66**（*使用作业调度程序*）

当系统交付时，限制将触发器程序添加至数据库文件的能力。如果您正在认真管理对象权限，一般用户将不具有足够的权限来将触发器程序添加至数据库文件。（在 *iSeries Security Reference* 一书中的 Appendix D 告诉需要的权限或所有命令，包括“添加物理文件触发器”（ADDPFTRG）命令。

可以使用“打印触发器程序”（PRTTRGPGM）命令来打印特定库中或所有库中的所有触发器程序的列表。

可以使用初始报告作为基础来评估在系统上已经存在的任何触发器程序。然后，可以定期打印更改的报告来查看是否已将新的触发器程序添加至系统。

当您评估触发器程序，考虑以下情况:

- 谁创建了触发器程序？可以使用“显示对象描述”（DSPOBJD）命令来确定它。
- 该程序执行什么操作？您将必须查看源程序或与程序创建者交谈来确定它。例如，触发器程序是否查看用户是谁？或许触发器程序正在等待特定用户（QSECOFR）以便获取对系统资源的访问。

在建立了信息库后，可以定期打印更改的报告来监控已添加至系统的新触发器程序。

检查隐藏的程序

触发器程序不是将“特洛伊木马”程序引进系统的唯一可能的方法。触发器程序是**出口程序**的示例。当发生某些事件（如在触发器程序的情况下文件更新）时，系统运行与此事件相关的出口程序。

表 15 描述可能在系统上的其它出口程序的示例。应使用相同的方法评估这些用于触发器程序的出口程序的使用和内容。

注: 表 15 不是可能的出口程序的完整列表。

.

表 15. 系统提供的出口程序

程序名	当程序运行时
DDMACC 网络属性上用户定义的名称。	当用户试图打开系统上的 DDM 文件或进行 DRDA 连接时。
PCSACC 网络属性上用户定义的名称	当用户通过使用“原始客户机”试图使用 Client Access™ 功能来访问系统上的对象时。
QPWDVLDPGM 系统值上的用户定义的名称。	当用户运行“更改密码”功能时。
QRMTSIGN 系统值中用户指定的名称。	当用户试图从远程系统交互式注册时。
QSYS/QEZUSRCLNP	当自动清除功能运行时。
CHGBCKUP 命令的 EXITPGM 参数上用户定义的名称。	当使用“操作助手”备份功能时。
CRTPRDLOD 命令上用户定义的名称。	在保存、恢复或删除用该命令创建的产品之前和之后。
CHGMSGD 命令的 DFTPGM 参数上用户定义的名称。	如果对消息指定了缺省程序，则当发出消息时系统运行该程序。因为标准系统上有很大数量的消息描述，所以监控缺省程序的使用是困难的。要防止公共用户对消息添加缺省程序，考虑将消息文件（*MSGF 对象）的公共权限设置为 *USE。
STREML3270 命令的 FKEYPGM 参数上用户定义的名称。	当用户在 3270 设备仿真会话期间按功能键时。当出口程序结束时，系统将控件返回到 3270 设备仿真会话。
性能监视器命令的 EXITPGM 参数上用户指定的名称。	要处理由下列命令收集的数据: STRPFRMON、ENDPFRMON、ADDPFRCOL 和 CHGPFRCOL。当数据收集结束时该程序运行。
RCVJRNE 程序的 EXITPGM 参数中的用户指定的名称。	对于从指定的日志和日志接收器中读取的每个日志项或日志项组。
QTNADDCR API 上用户指定的名称。	COMMIT 或 ROLLBACK 操作期间。
QHFRGFS API 上用户指定的名称。	要执行文件系统功能。
打印机设备描述的 SEPPGM 参数上用户指定的名称	在假脱机文件或打印作业之前或之后，要确定在分隔符页面上打印什么。
QGPL/QUSCLSXT	当关闭数据库文件以允许捕获文件使用信息时。
逻辑文件的 FMTSLR 参数上用户指定的名称。	当记录写入到数据库文件且记录格式名未包含在高级语言程序中时。选择器程序作为输入接收记录、确定使用的记录格式并将它返回到数据库。
在 QATNPGM 系统值、用户概要文件中 ATNPGM 参数或 SETATNPGM 命令的 PGM 参数中指定的用户定义的名称。	当用户按“辅助操作请求”键时。

表 15. 系统提供的出口程序 (续)

程序名	当程序运行时
TRCJOB 命令的 EXITPGM 参数上用户指定的名称。	启动“跟踪作业”过程之前。

对于允许您指定出口程序的命令，应确保命令缺省值尚未更改为指定出口程序。也应确保这些命令的公共权限不够更改命令缺省值。CHGCMDDFT 命令需要对该命令的 *OBJMGT 权限。不需要 *OBJMGT 权限来运行命令。

评估已注册的出口程序

可以使用系统注册功能来注册应在某些事件发生时运行的出口程序。要列示有关系统的注册信息，输入 WRKREGINF OUTPUT(*PRINT)。图 8 显示报告示例:

```
                使用注册信息
出口点 . . . . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
出口点格式 . . . . . . . . . . . . :   NJEO0100
已注册的出口点 . . . . . . . . . . :   *YES
允许注销 . . . . . . . . . . . . . :   *YES
出口程序的最大数目 . . . . . . . . :   *NOMAX
出口程序的当前数目 . . . . . . . . :   0
添加的预处理 . . . . . . . . . . . :   *NONE
  库 . . . . . . . . . . . . . . . :
  格式 . . . . . . . . . . . . . . :
除去的预处理 . . . . . . . . . . . :   *NONE
  库 . . . . . . . . . . . . . . . :
  格式 . . . . . . . . . . . . . . :
检索的预处理 . . . . . . . . . . . :   *NONE
  库 . . . . . . . . . . . . . . . :
```

图 8. 使用注册信息 - 示例

对于系统上的每个出口点，报告显示任何出口程序当前是否已注册。当出口点具有当前已注册的程序时，可以从 WRKREGINF 的显示版本选择选项 8（显示程序）来显示有关程序的信息:

```
                        使用注册信息

输入选项，按“执行”键。
5= 显示出口点    8= 使用出口程序

                          出口
     出口                 点
选项 点                   格式        已注册    文本
     QIBM_QGW_NJEOUTBOUND NJEO0100     *YES     网络作业项出站出口
8    QIBM_QHQ_DTAQ        DTAQ0100     *YES     原始数据队列服务器
     QIBM_QLZP_LICENSE    LICM0100     *YES     原始许可证管理服务器
     QIBM_QMF_MESSAGE     MESS0100     *YES     原始消息服务器
     QIBM_QNPS_ENTRY      ENTR0100     *YES     网络打印服务器 - 项
     QIBM_QNPS_SPLF       SPLF0100     *YES     网络打印服务器 - 假脱机
     QIBM_QNS_CRADDACT    ADDA0100     *YES     添加 CRQ 描述活动
     QIBM_QNS_CRCHGACT    CHGA0100     *YES     更改 CRQ 描述活动
```

使用与对其它出口程序和触发器程序使用的相同的方法来评估这些出口程序。

检查已调度的程序

iSeries 对稍后将运行的调度作业提供几种方法，包含作业调度程序。一般情况下，这些方法不会引起安全性漏洞，因为调度作业的用户必须具有与将作业提交至批处理所需要的相同权限。

然而，以后应定时检查调度的作业。不再是组织内的不满用户可能会使用此方法计划制造灾难。

限制保存和恢复能力

多数用户不必在系统上保存和恢复对象。保存命令提供将组织的重要资产复制到介质或其它系统的可能。多数保存命令支持可发送到另一个系统的保存文件（通过使用 SNDNETF 文件命令）而没有对介质或保存 / 恢复设备的访问权。

恢复命令对系统提供恢复未授权的对象如，程序、命令和文件的机会。通过使用保存文件，也可以恢复信息而没有对介质或保存 / 恢复设备的访问权。通过使用 SNDNETF 命令或使用 FIP 功能，可以从另一个系统发送保存文件。

以下是在系统上限制保存和恢复操作的建议:

- 控制哪些用户具有 *SAVSYS 特权。*SAVSYS 特权允许用户保存和恢复对象，即使当用户不具有对对象的必要权限时也是如此。
- 控制保存和恢复设备的物理访问权。
- 限制保存和恢复命令的访问权。安装 OS/400 许可程序时，RSTxxx 命令的公共权限是 *EXCLUDE。SAVxxx 命令的公共权限是 *USE。考虑将 SAVxxx 命令的公共权限更改为 *EXCLUDE。谨慎地限制您授权使用 RSTxxx 命令的用户。
- 使用 QALWOBJRST 系统值来限制系统状态程序、沿用权限的程序和具有验证错误的对象的恢复。
- 使用 QVFYOBJRST 系统值来控制恢复系统上已签名的对象 .
- 使用 QFRCCVNRST 系统值以控制重新创建正在系统上恢复的某些对象。
- 使用安全性审计过程来监控操作。包括 QAUDLVL 系统值中的 *SAVRST，且定期打印由恢复操作创建的审计过程记录。（*iSeries Security Reference* 一书中的 Chapter 9 和 Appendix F 提供有关审计项操作的更多信息。）

检查受保护的库中的用户对象

每个 iSeries 服务器作业都具有一个库列表。如果对于某个对象名称未指定库名称，则该库列表确定系统搜索该对象的顺序。例如，若您调用某个 程序而未指定程序所在的位置，则系统按顺序搜索您的库列表并运行它找到的程序的第一个副本。

iSeries Security Reference 一书提供关于库列表和没有库名称的调用程序（称为**未限定的调用**）的安全性漏洞的更多信息。它也提供关于控制库列表的内容和更改系统库列表的能力的建议 。

为了系统正常运行，某些系统库（如 QSYS 和 QGPL）必须位于每个作业的库列表中。您应该使用对象权限来控制谁可以将程序添加至这些库。这有助于防止有人将冒充程序放置在具有与稍后在库列表中的库中出现的程序相同的名称的这些库之一。

还应该评估谁对 CHGSYSLIBL 命令具有权限并监控安全性审计日志中的 SV 记录。不正当的用户可能将某个库放在库列表中的 QSYS 之前并导致其它用户运行与 IBM 提供的命令具有相同名称的未授权的命令。

SECBATCH 菜单选项:

28（*立即提交*）**67**（*使用作业调度程序*）

可以使用“打印用户对象”（PRTUSROBJ）命令来打印位于指定库中的用户对象（不是由 IBM 创建的对象）列表。然后可以评估该列表中的程序来确定谁创建了它们以及它们执行什么功能。

程序以外的用户对象当它们位于系统库中时也可以表现出有安全性漏洞。例如，如果程序将机密数据写入未限定其名称的文件，则可能骗该程序打开在系统库中该文件的冒充版本。

第 10 章 防止和检测攻击尝试

本资料是各种技巧的集合，用于帮助您检测可能的安全性漏洞和捣乱者。

物理安全性

系统部件是重要的商业资产，也是进入系统的潜在门户。系统中的某些系统组件体积小巧且价格昂贵。您应将系统部件放在受控的位置，以便防止他人除去贵重的系统组件。

系统部件附带的控制面板提供了无需工作站即可执行基本功能的能力。例如，可以使用控制面板来执行下列操作:

- 停止系统。
- 启动系统。
- 装入操作系统。
- 启动服务功能。

所有这些活动都能够使您的系统用户中断。它们也会对系统造成潜在的安全性漏洞。可以使用系统附带的键锁来控制何时允许这些活动。要防止使用控制面板，将键锁置于“安全”位置，卸下钥匙并将它存储在安全位置。

注:

1. 如果需要在系统上执行远程 IPL 或执行远程故障诊断，则需要为键锁选择另一设置。“iSeries 信息中心”中的“入门”主题提供关于键锁设置的更多信息（请参阅第 xii 页的『先决条件和相关信息』以获取详细信息）。
2. 并非所有系统型号都附带键锁作为标准功能部件。

监控用户概要文件活动

用户概要文件提供进入系统的通道。用户概要文件中的参数确定用户的环境和用户的安全性特征。作为安全管理员，您需要控制和审计系统上对用户概要文件所进行的更改。

可以设置安全性审计以便系统将更改记录写入用户概要文件。可以使用 DSPAUDJRNE 命令来打印那些更改的报告。

可以创建出口程序来评估对用户概要文件所请求的操作。表 16 显示可用于用户概要文件命令的出口点。

表 16. 用户概要文件活动的出口点

用户概要文件命令	出口点名称
创建用户概要文件（CRTUSRPRF）	QIBM_QSY_CRT_PROFILE
更改用户概要文件（CHGUSRPRF）	QIBM_QSY_CHG_PROFILE
删除用户概要文件（DLTUSRPRF）	QIBM_QSY_DLT_PROFILE
恢复用户概要文件（RSTUSRPRF）	QIBM_QSY_RST_PROFILE

例如，出口程序可以查找可能导致用户运行未授权版本程序的更改。这些更改可能指定不同的作业描述或新的当前库。根据出口程序接收到的信息，出口程序可以通知消息队列或执行某个操作（如更改或禁用用户概要文件）。

iSeries Security Reference 一书提供了关于用户概要文件操作的出口程序的更多信息。

对象签名

如果某人可以通过将窜改的数据引入您的系统来绕过您采取的所有安全性预防措施，则这些措施都没有意义。iSeries 服务器具有许多内置功能部件，您可以使用它们来阻止将已窜改的软件装入到您的系统上并检测已经装入系统的任何这种软件。在 V5R1 中添加的技术之一是对象签名。

对象签名是称为“数字签名”的加密概念的 iSeries 服务器实现。该概念相对简单：一旦软件制作者准备好将软件交付给客户，则该制作者“签名”该软件。此签名并不保证该软件执行任何特定的功能。然而，它提供了一种方法来证明软件是来自签署它的制作者并证明该软件自制作和签署以来尚未更改过。如果已通过因特网传送了该软件或将它存储在您认为可能已修改的介质上，则这一点特别重要。

使用数字签名给了您对可以将哪个软件装入到您的系统上的更大控制，而且一旦装入了它，您更有可能检测到更改。新的系统值“验证对象恢复”（QVFYOBJRST）提供了用于设置限制性策略的一种机制，该策略要求所有装入到系统上的软件由已知软件源签署。您也可以选择更开放的策略并且只验证签名（如果签名存在）。

所有 OS/400 软件以及选项和 iSeries 服务器许可程序的软件已经由系统可信源签署。这些签名有助于系统保护其完整性，并且当将修订应用于系统时检查这些签名，以确保该修订来自系统可信源并且在传送时未更改。也可以在软件位于系统上时检查这些签名。已扩展了 CHKOBJITG（检查对象完整性）命令，以便在除了检查系统上对象的其它完整性功能部件之外，还检查签名。而且，“数字证书管理器”具有一些面板，您可以使用这些面板来检查对象上的签名，包括在操作系统中的对象。

正如签署操作系统那样，您可以使用数字签名来保护对您的公司关键的软件的完整性。您可以购买已由软件供应商签署的软件，您也可以签署您已购买或编写的软件。然后，作为安全策略的一部分，可以定期使用 CHKOBJITG 或“数字证书管理器”来验证该软件上的签名仍然有效 – 自签署对象以来，对象尚未更改。您可能进一步要求由您或已知源签署系统上恢复的所有软件。然而，由于当前未签署的大多数 iSeries 服务器软件不是由 IBM 制作的，所以这可能对您的系统的限制太严格。新的数字签名支持使您可以灵活地决定保护软件完整性的最佳方式。

用于保护软件的数字签名仅是数字证书的用途之一。有关管理数字证书的附加信息可以在“信息中心”中的“数字证书管理”主题中找到（请参阅第 xii 页的『先决条件和相关信息』以获取详细信息）。

监控子系统描述

在 iSeries 服务器上启动子系统时，系统创建进入系统并运行的工作环境。子系统描述定义了环境的外观。因此，子系统描述可以为不合法的用户提供机会。捣乱者可以使用子系统描述来自动启动程序或使其不需要用户概要文件也能注册。

当运行“撤销公共权限”（RVKPUBAUT）命令时，系统将子系统描述命令的公共权限设置为 *EXCLUDE。这可以防止没有特别授权的用户（和没有 *ALLOBJ 特权的用户）更改或创建子系统描述。

下列主题提供关于复查当前系统上存在的子系统描述的建议。可以使用“使用子系统描述”（WRKSBSD）命令来创建所有子系统描述的列表。当从列表选择 5（显示）时，对所选的系统描述显示一个菜单。该菜单显示子系统环境的部件列表。

选择选项来查看有关部件的详细信息。使用“更改子系统描述”（CHGSBSD）命令来更改菜单上的前两个项。要更改其它项，对项类型使用相应的添加、除去或更改命令。例如，要更改工作站项，请使用“更改工作站项”（CHGWSE）命令。

Work Management 一书提供有关使用子系统描述的更多信息。它也列示了 IBM 提供的子系统描述的交付值。

自动启动作业项

自动启动作业项包含作业描述的名称。作业描述可以包含导致程序或命令运行的请求数据（RQSDTA）。例如，RQSDTA 可以是 `CALL LIB1/PROGRAM1`。无论子系统何时启动，系统都将运行库 LIB1 中的程序 PROGRAM1。

查看自动启动作业项和相关的作业描述。确保了解子系统启动时自动运行的任何程序的功能。

工作站名称和工作站类型

当子系统启动时，它分配所有未分配的工作站。工作站名称和工作站类型的项中列示了这些工作站（特别列示或按常规列示）。当用户注册时，用户在已分配工作站的子系统上注册。

在工作站上启动作业时，工作站项指示将使用哪一个作业描述。作业描述可能包含导致程序或命令运行的请求数据。例如，RQSDTA 参数可以为 `CALL LIB1/PROGRAM1`。无论用户何时注册到该子系统中的工作站，系统将运行 LIB1 中的 PROGRAM1。

查看工作站项和相关作业描述。确保没有用户已添加或更新任何项来运行您不知道的程序。

工作站项也可以指定缺省用户概要文件。对于某些子系统配置，它允许某些用户通过按“执行”键就可以注册。如果系统上的安全级别（QSECURITY 系统值）小于 40，应复查缺省用户的工作站项。

作业队列项

子系统启动时，它分配子系统描述中列示的任何未分配作业队列。作业队列项不会引起任何直接的安全性漏洞。然而，它们确实为某些用户提供了一个机会，使其通过在非计划环境中运行作业，从而损害系统性能。

应定期复查子系统描述中的作业队列项，以确保批处理作业在计划的环境中运行。

路由项

路由项定义作业进入子系统时所执行的操作。子系统对所有作业类型使用路由项：批处理、交互式和通信作业。路由项指定下列各项:

- 作业的类。与作业队列项相似，作业关联的类可以影响作业的性能，但并不会引起安全性漏洞。
- 当作业启动时运行的程序。检查路由项并确保没有用户已添加或更新任何项来运行您不知道的程序。

通信项和远程位置名称

通信作业进入系统时，系统使用活动子系统中的通信项和远程位置名称项来确定通信作业将如何运行。查看这些项的下列内容:

- 所有子系统都能够运行通信作业。如果您计划用于通信的子系统处于非活动状态，则正在尝试进入系统的作业可以在另一个子系统描述中查找满足其需要的项。您需要查看所有子系统描述中的项。
- 通信项包含作业描述。作业描述可以包含运行命令或程序的请求数据。查看通信项及其相关的作业描述，以确保了解作业将如何启动。
- 通信项也指定系统在某些情况下使用的缺省用户概要文件。确保了解缺省概要文件的作用。如果系统包含缺省概要文件，应确保它们是具有最小权限的概要文件。有关缺省用户概要文件的更多信息，请参阅第 12 章，『保护 APPC 通信』。

  可以使用“打印子系统描述”（PRTSBSDAUT）命令，来标识用于指定用户概要文件名称的通信项。

预启动作业项

可以使用预启动作业项来使子系统准备好执行某些类型的作业，以便这些作业启动更迅速。预启动作业可以在子系统启动时或在需要时启动。预启动作业项指定下列内容:

- 要运行的程序
  缺省用户概要文件
  作业描述

它们都可能引起安全性漏洞。您应确保预启动作业项仅执行已授权的期望功能。

作业和作业描述

作业描述包含当使用作业描述时可以导致特定程序运行的请求数据和路由数据。当作业描述在请求数据参数中指定了某个程序时，系统即运行该程序。当作业描述指定路由数据时，系统运行在与该路由数据匹配的路由项中指定的程序。

系统对交互式和批处理作业使用作业描述。对于交互式作业，工作站项指定作业描述。工作站项值一般为 *USRPRF，所以系统使用在用户概要文件中指定的作业描述。对于批处理作业，在提交作业时指定作业描述。

应定期复查作业描述，以确保它们没有运行非计划的程序。还应使用对象权限来防止对作业描述进行更改。*USE 权限足够运行具有作业描述的作业。标准用户不需要针对作业描述的 *CHANGE 权限。

SECBATCH 菜单选项:

15（*立即提交*）**54**（*使用作业调度程序*）

作业描述也可以指定作业应在哪一用户概要文件下运行。使用安全级别 40 和更高级别时，必须对作业描述和在作业描述中指定的用户概要文件具有 *USE 权限。使用低于 40 的安全级别时，仅需要对作业描述的 *USE 权限。

可以使用“打印作业描述权限”（PRTJOBDAUT）命令来打印一组作业描述的列表，这些作业描述用于指定用户概要文件且具有 *USE 公共权限。

该报告显示作业描述中指定的用户概要文件的特权。该报告包含用户概要文件具有的任何组概要文件的特权。您可以使用下列命令来显示用户概要文件的专用权限:

```
DSPUSRPRF USRPRF(profile-name) TYPE(*OBJAUT)
```

作业描述指定当作业运行时使用的库列表。如果某人可以更改用户的库列表，则该用户可以运行不同库中程序的非计划版本。您应定期地复查系统上的作业描述中指定的库列表。

最后，应确保“提交作业”（SBMJOB）命令和“创建用户概要文件”（CRTUSRPRF）命令的缺省值尚未更改为指向非计划的作业描述。

体系结构化事务程序名称

某些通信请求对系统发送特定类型的信号。因为事务程序的名称是系统 APPC 体系结构的一部分，所以此请求被称为**体系结构事务程序名（TPN）**。用于显示站联通请求的请求为体系结构 TPN 的示例。体系结构 TPN 是通信工作的正常方式，不一定会引起安全性漏洞。然而，体系结构 TPN 可能提供进入系统的意外入口。

某些 TPN 不会在请求中传送概要文件。如果请求与某一通信项（其缺省用户为 *SYS）关联，就可在系统上启动请求。然而，*SYS 概要文件仅可以运行系统功能，而不能运行用户应用程序。

如果不想体系结构 TPN 运行时使用缺省概要文件，可以在通信项中将缺省用户从 *SYS 更改为 *NONE。第 78 页的『体系结构化 TPN 请求』列示体系结构 TPN 和相关的用户概要文件。

如果根本不想在系统上运行特定 TPN，请执行以下操作:

1. 创建可接受几个参数的 CL 程序。该程序应未执行功能。它仅具有参数的“声明”（DCL）语句，然后结束。
2. 将 TPN 的路由项添加到具有通信项或远程位置名称项的每个子系统。路由项应指定下列内容:
   - *比较值*（CMPVAL 值），与起始位置为 37 的 TPN（请参阅体系结构化 TPN 请求）的程序名相等。

- *要调用的程序*（PGM）值与在第 77 页的 1步中创建的程序名称相等。这防止 TPN 定位另一个路由项，如 *ANY。

几个 TPN 在 QCMN 子系统中已具有它们自己的路由项。由于性能原因已添加了它们。

体系结构化 TPN 请求

表 17. TPN 请求的程序和用户

TPN 请求	程序	用户概要文件	描述
X'30F0F8F1'	AMQCRC6A	*NONE	消息队列
X'06F3F0F1'	QACSOTP	QUSER	APPC 注册事务程序
X'30F0F2D1'	QANRTP	QADSM	ADSM/400 APPC 配置
X'30F0F1F9'	QCNPCSUP	*NONE	共享文件夹
X'07F0F0F1'	QCNTEDDM	QUSER	DDM
X'07F6C4C2'	QCNTEDDM	QUSER	远程 SQL–DRDA1
X'30F0F7F7'	QCQNRBAS	QSVCCS	SNA CC_Server
X'30F0F1F4'	QDXPRCV	QUSER	DSNX–PC 接收器
X'30F0F1F3'	QDXPSEND	QUSER	DSNX–PC 发送器
X'30F0F2C4'	QEVYMAIN	QUSER	ENVY**/400 服务器
X'30F0F6F0'	QHQTRGT	*NONE	PC 数据队列
X'30F0F8F0'	QLZPSERV	*NONE	Client Access 许可证管理器
X'30F0F1F7'	QMFRCVR	*NONE	PC 消息接收器
X'30F0F1F8'	QMFSNDR	*NONE	PC 消息发送器
X'30F0F6F6'	QND5MAIN	QUSER	APPN 5394 工作站控制器
DB2DRDA	QCNTEDDDM	QUSER	DB2DRDA
APINGD	QNMAPINGD	QUSER	APINGD
X'30F0F5F4'	QNMEVK	QUSER	系统管理实用程序
X'30F0F2C1'	QNPSERVR	*NONE	PWS-I 网络打印服务器
X'30F0F7F9'	QOCEVOKE	*NONE	跨系统日历
X'30F0F6F1'	QOKCSUP	QDOC	目录影像
X'20F0F0F7'	QOQSESRV	QUSER	DIA 版本 2
X'20F0F0F8'	QOQSESRV	QUSER	DIA 版本 2
X'30F0F5F1'	QOQSESRV	QUSER	DIA 版本 2
X'20F0F0F0'	QOSAPPC	QUSER	DIA 版本 1
X'30F0F0F5'	QPAPAST2	QUSER	S/36—S/38 传递
X'30F0F0F9'	QPAPAST2	QUSER	打印机传递
X'30F0F4F6'	QPWFSTP0	*NONE	共享文件夹类型 2
X'30F0F2C8'	QPWFSTP1	*NONE	Client Access 文件服务器
X'30F0F2C9'	QPWFSTP2	*NONE	Windows** Client Access 文件服务器
X'30F0F6F9'	QRQSRVX	*NONE	远程 SQL – 一体化服务器
X'30F0F6F5'	QRQSRV0	*NONE	不提交的远程 SQL
X'30F0F6F4'	QRQSRV1	*NONE	不提交的远程 SQL
X'30F0F2D2'	QSVRCI	QUSER	SOC/CT

表 17. TPN 请求的程序和用户 (续)

TPN 请求	程序	用户概要文件	描述
X'21F0F0F8'	QS2RCVR	QGATE	SNADS FS2 接收器
X'21F0F0F7'	QS2STSND	QGATE	SNADS FS2 发送器
X'30F0F1F6'	QTFDWNLD	*NONE	PC 传送功能
X'30F0F2F4'	QTIHNPCS	QUSER	TIE 功能
X'30F0F1F5'	QVPPRINT	*NONE	PC 虚拟打印
X'30F0F2D3'	QWGMTP	QWGM	Ultimedia Mail/400 服务器
X'30F0F8F3'	QZDAINIT	QUSER	PWS-I 数据访问服务器
X'21F0F0F2'	QZDRCVR	QSNADS	SNADS 接收方
X'21F0F0F1'	QZDSTSND	QSNADS	SNADS 发送方
X'30F0F2C5'	QZHQTRG	*NONE	PWS-I 数据队列服务器
X'30F0F2C6'	QZRCSRVR	*NONE	PWS-I 远程命令服务器
X'30F0F2C7'	QZSCSRVR	*NONE	PWS-I 中央服务器

监控安全性事件的方法

设置安全性不是一劳永逸的。需要不断评估系统上的更改和安全性故障。然后对安全性环境进行调整以响应您所发现的问题。

安全性报告帮助您监控系统上发生的与安全性相关的更改。以下是可用来帮助您检测安全性故障或暴露的其它系统功能:

- 安全性审计是一个功能强大的工具，您可以使用它来观察系统上发生的许多不同类型的与安全性相关的事件。例如，可以将系统设置为在每次用户打开特定数据库文件进行更新时写一条审计记录。可以审计系统值的所有更改。可以审计当用户恢复对象时发生的操作。

  iSeries Security Reference 一书中的 Chapter 9 提供有关安全性审计功能的完整信息。可以使用“更改安全性审计”（CHGSECAUD）命令来在系统上设置安全性审计。 您也可以使用“显示审计日志项”（DSPAUDJRNE）命令来打印安全性审计日志中的所选择的信息。

- 可以创建 QSYSMSG 消息队列来捕获关键的系统操作员消息。QSYSOPR 消息队列在整个典型的营业日中都接收到不同重要性的许多消息。由于 QSYSOPR 消息队列中的消息非常多，您可能会忽略掉与安全性相关的关键消息,

  如果在系统上的 QSYS 库中创建 QSYSMSG 消息队列，系统自动将某些关键消息定向至 QSYSMSG 消息队列而不是 QSYSOPR 消息队列。

  可以创建程序来监控 QSYSMSG 消息队列，也可以以中断方式将该队列指定给自己或指定给另一个可信用户。

第 3 部分 应用程序和网络通信

第 11 章 使用“集成文件系统”来保护文件

集成文件系统为您提供了在 iSeries 服务器上存储和查看信息的多种方法。集成文件系统是支持流输入和输出操作的 OS/400 操作系统的一部分。它提供与个人计算机操作系统和 UNIX® 操作系统相似（并兼容）的存储管理方法。

使用集成文件系统，可以从分层目录结构的角度查看系统上的所有对象。然而，在大多数情况下，用户以对于特定文件系统最常用的方法查看对象。例如，“传统的” iSeries 对象位于 QSYS.LIB 文件系统中。一般情况下，用户从库的角度查看这些对象。用户通常从文件夹中文档的的角度查看 QDLS 文件系统中的对象。根（/）、QOpenSys 和用户定义的文件系统提供一种分层（嵌套）目录结构。

作为安全管理员，您需要了解下列内容:

- 在系统上使用哪些文件系统
- 每个文件系统的独特的安全性特征

以下主题提供了集成文件系统安全性的某些一般注意事项。

“集成文件系统”的安全性方法

根文件系统充当 iSeries 服务器上所有其它文件系统的根基（或基础）。在高级别，它提供系统上所有对象的集成视图。在 iSeries 服务器上可以存在的其它文件系统提供对象管理和集成的各种方法，这取决于每个文件系统的基本用途。例如，QOPT（光盘）文件系统使 iSeries 应用程序和服务器（包括 iSeries Access for Windows 文件服务器）能够访问 iSeries 服务器上的 CD-ROM 驱动器。同样，QFileSvr.400 文件系统使应用程序能够访问远程 iSeries 服务器上的集成文件系统数据。QLANSrv 文件服务器允许访问存储在 Integrated xSeries Server for iSeries 上或在网络中其它已连接的服务器上的文件。

每个文件系统的安全性方法取决于该文件系统使之可用的数据。例如，QOPT 文件系统不提供对象级别的安全性，因为不存在将权限信息写入 CD-ROM 的技术。对于 QFileSvr.400 文件系统，访问控制发生在远程系统（在物理上存储和管理文件所在的系统）上。对于象 QLANSrv 的文件系统，Integrated xSeries Server for iSeries 提供访问控制。尽管安全性模型不同，但许多文件系统通过集成文件系统命令（如“更改权限”（CHGAUT）和“更改所有者”（CHGOWN））支持访问控制的一致管理。

此处是与集成文件系统安全性的冷僻角落相关的一些技巧。集成文件系统设计尽可能遵循 POSIX 标准。这导致一些引起注意的行为，其中，iSeries 服务器权限和 POSIX 许可权“混合”在一起:

1. 不要除去用户对该用户所拥有的目录的专用权限，即使通过公共权限、组或权限列表授权该用户。当使用标准 iSeries 服务器安全性模型中的库或文件夹时，除去所有者的专用权限将会减少为用户概要文件存储的权限信息量而不会影响其它操作。但是，因为 POSIX 标准定义目录的许可权继承的方法，所以新创建的目录的所有者对该目录具有的对象权限将与父的所有者对父具有的权限相同，即使新创建的目录的所有者对父具有其它专用权限。这可能很难理解，因此，此处是一个示例: USERA 拥有目录 /DIRA，但已除去 USERA 的专用权限。USERB 对 /DIRA 具有专用权

限。USERB 创建目录 /DIRA/DIRB。由于 USERA 对 /DIRA 没有对象权限，所以 USERB 将对 /DIRA/DIRB 没有对象权限。如果没有进一步的操作来更改 USERB 的对象权限，USERB 将不能重命名或删除 /DIRA/DIRB。这也在使用带 O_INHERITMODE 标志的 open() API 来创建文件时开始起作用。如果 USERB 创建了文件 /DIRA/FILEB，USERB 将对它没有对象权限和数据权限。USERB 无法写入新文件。

2. 大多数物理文件系统不支持沿用权限。它包括根（/）、QOpenSys、QDLS 和用户定义的文件系统。
3. 创建对象的用户概要文件拥有该对象，即使将用户概要文件的 OWNER 字段设置为 *GRPPRF。
4. 许多文件系统操作需要对路径的每个组成部分（包括根（/）目录）的 *RX 数据权限。当遇到权限问题时，确保检查用户对根本身的权限。
5. 显示或检索当前工作目录（DSPCURDIR 或 getcwd() 等）需要对路径中的每个组成部分的 *RX 数据权限。然而，更改当前工作目录（CD 或 chdir() 等）只需要对每个组成部分的 *X 数据权限。因此，用户可能将当前工作目录更改为某个路径而无法显示该路径。
6. COPY 命令的目的是复制对象。对新文件的权限设置除所有者不同外将与原始文件相同。然而，CPYTOSTMF 命令的目的只是复制数据。用户不能控制对新文件的权限设置。创建者／所有者将具有 *RWX 数据权限，但组和公共权限将是 *EXCLUDE。用户必须使用别的方法（CHGAUT 或 chmod() 等）来指定所需要的权限。
7. 用户必须是对象的所有者或对对象具有 *OBJMGT 对象权限才能检索关于该对象的权限信息。这出现在某些意外的地方（如 COPY），必须检索关于源对象的权限信息才能对目标对象设置等效权限。
8. 当更改对象的所有者或组时，用户不仅必须对该对象具有适当的权限，而且必须对新的所有者／组用户概要文件具有 *ADD 数据权限以及对旧的所有者／组概要文件具有 *DELETE 数据权限。这些数据权限与文件系统数据权限不相关。可以使用 DSPOBJAUT 命令显示这些数据权限以及使用 EDTOBJAUT 命令更改它们。当 COPY 试图设置新对象的组标识时，这也意外出现在 COPY 中。
9. MOV 命令易于产生令人费解的权限错误，特别是当从一个物理文件系统移动至另一个物理文件系统时或当执行数据转换时，更是如此。在这些情况下，移动操作实际上变成了复制和删除操作。因此，除其它特定的 MOV 注意事项外，所有与 COPY 命令（请参阅以上 7 和 8）和 RMVLNK 命令相同的权限注意事项也会影响 MOV 命令。

以下节为您提供几个代表性的文件系统的一些注意事项。有关在您的 iSeries 服务器上的特定文件系统的更多信息，您将需要查阅使用该文件系统的许可程序的文档。

根（/）、QOpenSys 和用户定义的文件系统

以下是根、QOpenSys 和用户定义的文件系统的安全性注意事项。

权限如何工作

根、QOpenSys 和用户定义的文件系统为对象管理和安全性提供了 iSeries 服务器、PC 和 UNIX** 功能的一种混合。当从 iSeries 服务器会话使用集成文件系统命令（WRKAUT 和 CHGAUT）时，可以设置所有正常的 iSeries 服务器对象权限。这包括与 Spec 1170（UNIX 类型的操作系统）兼容的 *R、*W 和 *X 权限。

注: 根、QOpenSys 和用户定义的文件系统在功能上等效。QOpenSys 文件系统区分大小写。根文件系统不区分大小写。用户定义的文件系统可以定义为区分大小写。因为这些文件系统具有相同的安全性特征，所以在以下主题中可以假定可交替使用它们的名称。

当作为管理员从 PC 会话访问根文件系统时，可以设置该 PC 使用的对象属性来限制某些类型的访问:

- 系统
- 隐藏
- 归档
- 只读

这些 PC 属性是对 iSeries 服务器对象权限值的补充而不是替换。

当用户尝试访问根文件系统中的某个对象时，OS/400 实施该对象的所有对象权限值和属性，而不管那些权限从用户界面是否“可视”。例如，假定将对象的只读属性设置为打开。PC 用户不能通过 iSeries Access 接口删除对象。具有固定功能的工作站的 iSeries 服务器用户也不能删除该对象，即使该 iSeries 服务器用户具有 *ALLOBJ 特权。授权用户必须使用 PC 功能将该只读值复位为关闭之后，才能删除该对象。同样，PC 用户可能不具有足够的 OS/400 权限来更改对象的与 PC 有关的安全性属性。

在 iSeries 服务器上运行的 UNIX 类型的应用程序使用 UNIX 风格的应用程序编程接口（API）来访问根文件系统中的数据。使用 UNIX 风格的 API，应用程序可以识别和维护下列安全性信息:

- 对象所有者
- 组所有者（iSeries 服务器主组权限）
- 读（文件）
- 写（更改内容）
- 执行（运行程序或搜索目录）

系统将这些数据权限映射至现有的 iSeries 服务器对象和数据权限:

- 读（*R）= *OBJOPR 和 *READ
- 写（*W）= *OBJOPR、*ADD、*UPD 和 *DLT
- 执行（*X）= *OBJOPR 和 *EXECUTE

在 UNIX 类型的环境中，不存在其它对象权限（*OBJMGT、*OBJEXIST、*OBJALTER 和 *OBJREF）的概念。

然而，对于根文件系统中的所有对象，存在这些对象权限。当使用 UNIX 风格的 API 创建某个对象时，该对象从父目录继承这些权限，结果如下:

- 新对象的所有者与父目录的所有者具有相同的对象权限。
- 新对象的主组与父目录的主组具有相同的对象权限。
- 新对象的公众与父目录的公众具有相同的对象权限。

在 API 中使用方式参数指定新对象对于所有者、主组和公众的数据权限。当将所有的对象权限设置为“打开”时，可以获取在 UNIX 类型的环境中期望的权限行为。最好将它们的设置保留为“打开”，除非您不需要 POSIX 风格的行为。

当运行使用 UNIX 风格的 API 的应用程序时，系统实施全部对象权限，而不管它们对于 UNIX 类型的应用程序是否“可视”。例如，尽管在 UNIX 类型的操作系统中不存在权限列表的概念，但系统将实施权限列表的权限。

当具有混合的应用程序环境时，需要确保在一个环境中不进行权限更改，这些权限更改将会中断另一个环境中的应用程序。

使用根（*/*）、QOpenSys 和用户定义的文件系统的安全性

由于集成文件系统的引入，iSeries 服务器也提供了使用多个文件系统中的对象的一组新命令。此命令集包括使用安全性的命令:

- 更改审计（CHGAUD）
- 更改权限（CHGAUT）
- 更改所有者（CHGOWN）
- 更改主组（CHGPGP）
- 显示权限（DSPAUT）
- 使用权限（WRKAUT）

这些命令将基本数据和对象权限分组成 UNIX 风格的权限子集:

***RWX** 读 / 写 / 执行
***RW** 读 / 写
***R** 读
***WX** 写 / 执行
***W** 写
***X** 执行

此外，UNIX 风格的 API 可用来使用安全性。

对根目录的公共权限

当系统交付时，对根目录的公共权限是 *ALL（全部对象权限和所有数据权限）。此设置提供具有 UNXI 风格的应用程序期望的和一般的 iSeries 服务器用户期望的灵活性和兼容性。具有命令行能力的 iSeries 服务器用户可以仅通过使用 CRTLIB 命令来在 QSYS.LIB 文件系统中创建新库。通常，在一般的 iSeries 服务器上的权限允许这样做。同样，使用根文件系统的交付设置，一般用户可以在根文件系统中创建新目录（正如可以在 PC 上创建新目录一样）。

作为安全管理员，您必须教育您的用户有关充分保护他们创建的对象的事情。当用户创建库时，很可能对该库的公共权限不应该是 *CHANGE（缺省值）。该用户应该将公共权限设置为 *USE 或 *EXCLUDE，这取决于该库的内容。

如果您的用户需要在根（/）、QOpenSys 或用户定义的文件系统中创建新目录，您有几个安全性选项:

- 可以教育您的用户在他们创建新目录时覆盖缺省权限。缺省值是从最近的父目录继承权限。就在根目录中新创建的目录来说，缺省情况下公共权限将是 *ALL。
- 可以在根目录下创建“主控”子目录。将对该主控目录的公共权限设置为对于您的组织适当的设置。然后，指示用户在此主控子目录中创建任何新的个人目录。他们的新目录将继承它的权限。

- 可以考虑更改根目录的公共权限来阻止用户在该目录中创建对象。（除去 *W、*OBJEXIST、*OBJALTER、*OBJREF 和 *OBJMGT 权限。）然而，需要评估此更改是否将引起您的任何应用程序的问题。例如，您可能具有 UNIX 风格的应用程序，该程序期望能够从根目录删除对象。

打印专用权限对象（PRTPVTAUT）命令

“打印专用权限”（PRTPVTAUT）命令使您能够打印指定库、文件夹或目录中具有指定类型的对象的所有专用权限的报告。该报告列示具有指定类型的所有对象和对对象授权的用户。这是检查对对象的不同权限源的一种方法。

此命令打印所选择的对象的三个报告。第一个报告（完整报告）包含每个所选择的对象的所有专用权限。如果先前对指定库、文件夹或目录中的指定对象运行 PRTPVTAUT 命令，则第二个报告（更改报告）包含对所选择的对象的专用权限的补充和更改。所选择类型的任何新对象、对现有对象的新权限或对现有对象的现有权限的更改都列示在“更改报告”中。如果先前未对指定库、文件夹或目录中的指定对象运行 PRTPVTAUT 命令，则将没有“更改报告”。如果先前已运行该命令但未对对象的权限进行更改，则打印“更改报告”，但没有列示的对象。

第三个报告（删除报告）包含自先前运行 PRTPVTAUT 命令以来从指定对象删除的任何专用授权用户。删除的任何对象或作为专用授权用户除去的任何用户列示在“删除报告”中。如果先前未运行 PRTPVTAUT 命令，则将没有“删除报告”。如果先前运行了该命令但未对对象执行删除操作，则打印“删除报告”，但没有列示的对象。

限制: 您必须具有 *ALLOBJ 特权才能使用此命令。

示例:

此命令为 PAYROLLLIB 中的所有文件对象创建完整的、已更改的和删除的报告:

```
PRTPVTAUT OBJTYPE(*FILE) LIB(PAYROLLLIB)
```

此命令为目录 garry 中的所有流文件对象创建完整的、已更改的和删除的报告:

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*NO)
```

此命令为从目录 garry 开始的子目录结构中的所有流文件对象创建完整的、已更改的和删除的报告:

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*YES)
```

打印公共授权对象（PRTPUBAUT）命令

“打印公共授权对象”（PRTPUBAUT）命令使您能够打印不具有公共权限 *EXCLUDE 的指定对象的报告。对于 *PGM 对象，只有不具有公共权限 *EXCLUDE 的用户可以调用的程序（程序是用户域或系统安全级别（QSECURITY 系统值）为 30 或低于 30）才将包括在该报告中。这是检查授权系统上的每个用户访问的对象的一种方法。

此命令将打印两个报告。第一个报告（完整报告）将包含不具有公共权限 *EXCLUDE 的所有指定对象。第二个报告（更改报告）将包含先前运行 PRTPUBAUT 命令时具有公共权限 *EXCLUDE 或不存在但现在不具有公共权限 *EXCLUDE 的对象。如果先前

未对指定对象和库、文件夹或目录运行 PRTPUBAUT 命令，则将没有“更改报告”。如果先前已运行该命令，但附加对象都具有公共权限 *EXCLUDE，则将打印“更改报告”，但没有列示的对象。

限制: 您必须具有 *ALLOBJ 特权才能使用此命令。

示例:

此命令为库 GARRY 中不具有公共权限 *EXCLUDE 的所有文件对象创建完整的和已更改的报告: :

```
PRTPUBAUT OBJTYPE(*FILE) LIB(GARRY)
```

此命令为从目录 garry 开始的子目录结构中不具有公共权限 *EXCLUDE 的所有流文件对象创建完整的、已更改的和删除的报告:

```
PRTPUBAUT OBJTYPE(*STMF) DIR(GARRY) SCHSUBDIR(*YES)
```

限制对 QSYS.LIB 文件系统的访问

因为根文件系统是根基文件系统，所以 QSYS.LIB 文件系统表现为根目录中的子目录。因此，对您的 iSeries 服务器具有访问权的任何 PC 用户都可以使用正常的 PC 命令和操作来操作存储在 iSeries 服务器库（QSYS.LIB 文件系统）中的对象。例如，PC 用户可以将 QSYS.LIB 对象（如具有关键数据文件的库）拖动至碎纸机。

正如您在第 84 页的『根（/）、QOpenSys 和用户定义的文件系统』中所了解的，系统实施全部对象权限而不管它对于界面是否可视。因此，用户不能撕碎（删除）对象，除非该用户对该对象具有 *OBJEXIST 权限。然而，如果您的 iSeries 取决于菜单访问安全性而不是对象安全性，则 PC 用户可能很容易发现 QSYS.LIB 文件系统中可用于撕碎的对象。

随着您扩展系统的使用和提供的不同的访问方法时，将会立即发现菜单访问安全性不够。第 39 页的第 5 章，『使用对象权限保护信息资产』讨论使用对象安全性补充菜单访问控制的策略。然而，iSeries 服务器也为您提供了一种简单方法，以防止通过根文件系统目录结构访问 QSYS.LIB 文件系统。可以使用 QPWFSERVER 权限列表来控制哪些用户可以通过根目录访问 QSYS.LIB 文件系统。

当用户对 QPWFSERVER 权限列表的权限是 *EXCLUDE 时，该用户不能从根目录结构进入 QSYS.LIB 目录。当用户的权限是 *USE 时，该用户可以进入该目录。一旦该用户具有权限进入该目录，对于该用户尝试对 QSYS.LIB 文件系统中的对象执行的任何操作，正常对象权限都适用。换句话说，对 QPWFSERVER 权限列表的权限起类似进入整个 QSYS.LIB 文件系统的门户的作用。对于具有 *EXCLUDE 权限的用户，该门户是锁定的。对于具有 *USE 权限（或任何更大权限）的用户，该门户是打开的。

对于大多数情况，用户不需要使用目录界面来访问 QSYS.LIB 文件系统中的对象。很可能您将要把 QPWFSERVER 权限列表的公共权限设置为 *EXCLUDE。记住，权限列表的该权限打开或关闭进入 QSYS.LIB 文件系统中的所有库（包括用户库）的门户。如果遇到反对此排除的用户，可以单独评估他们的需求。如果适当的话，可以为单个用户显式授予对权限列表的权限。然而，需要确保该用户对 QSYS.LIB 文件系统中的对象具有适当的权限。否则，该用户可能会无意地删除对象或整个库。

注:

1. 当系统交付时，对 QPWFSERVER 权限列表的公共权限是 *USE。

2. 如果显式授权单个用户，权限列表仅通过 iSeries Access 文件服务、NetServer 文件服务和 iSeries 服务器之间的文件服务控制访问。这并不阻止通过 FTP、ODBC 和其它网络对相同目录的访问。

保护目录

要访问根文件系统中的对象，应阅读一遍该对象的整个路径。要搜索某个目录，您必须对该目录具有 *X（*OBJOPR 和 *EXECUTE）权限。例如，假定要访问下列对象:

```
/companya/customers/custfile.dat
```

您必须对 companya 目录和 customers 目录具有 *X 权限。

使用根文件系统，可以创建至某个对象的符号链接。在概念上，符号链接是路径名称的别名。通常，它比全路径名称短且易于记忆。然而，符号链接不创建该对象的另一个物理路径。用户仍需要对象的物理路径中的每个目录和子目录的 *X 权限。

对于根文件系统中的对象，可以使用目录安全性，正如可以在 QSYS.LIB 文件系统中使用库安全性一样。例如，可以将某个目录的公共权限设置为 *EXCLUDE 来防止公共用户访问该树中的任何对象。

新对象的安全性

当在根文件系统中创建新对象时，用来创建它的接口确定它的权限。例如，如果使用 CRTDIR 命令及其缺省值，则新目录继承其父目录的所有权限特征，包括专用权限、主组权限和权限列表关联。以下节描述如何为每个类型的接口确定权限。

权限来自直接父目录，而不是来自树中上面更高的目录。因此，作为安全管理员，您需要从两种观点查看指定给层次结构中的目录的权限:

- 权限如何影响对树中的对象的访问（类似库权限）。
- 权限如何影响新创建的对象（类似库的 CRTAUT 值）。

建议: 您可能要给予在集成文件系统中工作的用户一个主目录（例如，/home/usrxxx），然后适当地设置安全性（如 PUBLIC *EXCLUDE）。用户在他们的主目录下创建的任何目录将接着继承该权限。

以下是对于不同接口的权限继承的描述:

使用“创建目录”命令

当您通过使用 CRTDIR 命令来创建新的子目录时，您有两个用于指定权限的选项:

- 可以指定公共权限（数据权限或／和对象权限）。
- 可以对数据权限或／和对象权限指定 *INDIR。当对数据权限和对象权限指定 *INDIR 时，系统将所有权限信息从父目录完全复制到新对象，包括权限列表、主组、公共权限和专用权限。（系统不复制 QSYS 概要文件或 QSECOFR 概要文件对对象具有的专用权限。）

使用 API 创建目录

当您通过使用 mkdir() API 创建目录时，可以为所有者、主组和公众指定数据权限（使用 *R、*W 和 *X 的权限映射）。系统使用父目录中的信息来为所有者、主组和公众设置对象权限。

因为 UNIX 类型的操作系统不具有对象权限的概念，所以 mkdir() API 不支持指定对象权限。如果您需要不同的对象权限，可以使用 iSeries 服务器命令（CHGAUT）。然而，当您除去某些对象权限时，UNIX 风格的应用程序可能不象您期望它工作的那样来工作。

使用 open() 或 creat() API 创建流文件

当您使用 creat() API 来创建流文件时，可以为所有者、主组和公众指定数据权限（使用 UNIX 风格的权限 *R、*W 和 *X）。系统使用父目录中的信息来为所有者、主组和公众设置对象权限。

您也可以在使用 open() API 创建流文件时指定这些权限。或者，当您使用 open() API 时，可以指定对象应该从父目录继承所有权限。这称为继承方式。当指定继承方式时，系统创建父权限的完整匹配，包括权限列表、主组、公共权限和专用权限。此选项的工作与在 CRTDIR 命令中指定 *INDIR 相似。

通过使用 PC 接口创建对象

当使用 PC 应用程序在根文件系统中创建对象时，系统自动从父目录继承所有权限。这包括权限列表、主组、公共权限和专用权限。PC 应用程序不具有任何等效于在创建对象时指定权限的操作。

QFileSvr.400 文件系统

使用 QFileSvr.400 文件系统，在一个 iSeries 系统（SYSTEMA）上的用户（USERX）可以访问另一个已连接的 iSeries 系统（SYSTEMB）上的数据。USERX 具有一个正如 Client Access 接口那样的接口。远程 iSeries 服务器（SYSTEMB）表现为一个目录，而它的所有文件系统作为子目录。

当 USERX 尝试使用此接口访问 SYSTEMB 时，SYSTEMA 将 USERX 的用户概要文件名称和加密密码发送至 SYSTEMB。在 SYSTEMB 中必须存在相同的用户概要文件和密码，否则 SYSTEMB 拒绝该请求。

如果 SYSTEMB 接受该请求，USERX 出现在 SYSTEMB 中，正如任何 Client Access 用户。相同的权限检查规则适用于 USERX 尝试的任何操作。

作为安全管理员，您需要了解 QFileSvr.400 文件系统代表进入您的系统的另一个可能的门户。您不能假定将您的远程用户限制于具有显示站联通的交互式注册。如果您正在运行 QSERVER 子系统且您的系统已连接至另一个 iSeries 系统，则远程用户可以访问您的系统，好象他们位于运行 Client Access 的本地 PC 上一样。更可能的是，您的系统将具有需要运行 QSERVER 子系统的连接。这也是需要一个良好的对象权限方案的另一个原因。

网络文件系统

“网络文件系统”（NFS）提供对具有 NFS 实现的系统的访问和来自该系统的访问。NFS 是网络系统中的用户之间共享信息的一种业界标准方法。大多数主要操作系统（包括 PC 操作系统）都提供 NFS。对于 UNIX 系统，NFS 是存取数据的主要方法。iSeries 服务器可以充当 NFS 客户机和 NFS 服务器。

当您成为充当 NFS 服务器的 iSeries 系统的安全管理员时，需要了解和管理 NFS 的安全性方面。以下是建议和注意事项:

- 必须通过使用 STRNFSSVR 命令显式启动 NFS 服务器功能。控制谁具有权限使用此命令。
- 通过导出目录或对象，建立可用于 NFS 客户机的目录或对象。因此，对于您的系统中的哪些部分可用于您的网络中的 NFS 客户机，您具有非常明确的控制。
- 在导出时，您可以指定哪些客户机对对象具有访问权。可以按系统名称或 IP 地址标识客户机。客户机可以是一个单独的 PC 或整个 iSeries 服务器或 UNIX 系统。在 NFS 术语中，该客户机（IP 地址）称为机器。
- 在导出时，可以为每个机器指定只读访问或读／写访问，该机器对导出的目录或对象具有访问权。在大多数情况下，将可能需要提供只读访问。
- NFS 不提供密码保护。它设计成并打算用于系统的可信团体中的数据共享。当用户请求访问时，服务器接收用户的 uid。以下是某些 uid 注意事项:
  - iSeries 服务器尝试定位具有相同 uid 的用户概要文件。如果它找到匹配的 uid，则使用该用户概要文件的凭证。凭证是描述使用用户的权限的一个 NFS 术语。它类似于其它 iSeries 服务器应用程序中的概要文件交换。
  - 当您导出目录或对象时，可以指定是否将允许由具有根权限的概要文件来访问。在 iSeries 服务器上的 NFS 服务器把根权限与 *ALLOBJ 特权等同起来。如果您指定将不允许根权限，则映射到具有 *ALLOBJ 特权的用户概要文件的具有 uid 的 NFS 用户将不能访问该概要文件下的对象。相反，如果允许匿名访问，将会把请求者映射到匿名概要文件。
  - 当您导出目录或对象时，可以指定是否将允许匿名请求。匿名请求是具有与系统上的任何 uid 不匹配的 uid 的请求。如果您选择允许匿名请求，系统将匿名用户映射到 IBM 提供的 QNFSANON 用户概要文件。此用户概要文件不具有任何特权或显式权限。（在导出时，如果您愿意，可以为匿名请求指定另一个用户概要文件。）
- 当您的 iSeries 服务器参与到 NFS 网络（或具有依赖于 uid 的 UNIX 系统的任何网络）时，可能需要管理您自己的 uid，而不是让系统自动指定它们。将需要使 uid 与网络中的其它系统协调。

  您可能会发现需要更改 uid（甚至对于 IBM 提供的用户概要文件）来获得与网络中的其它系统的兼容性。程序可用来使更改用户概要文件的 uid 更简单。（当您更改用户概要文件的 uid 时，也需要更改在根目录中或 QOpenSrv 目录中该概要文件拥有的所有对象的 uid。） QSYCHGID 程序自动更改用户概要文件中和所有拥有的对象中的 uid。有关如何使用此程序的信息，请参阅 *iSeries System API Reference* 一书。

第 12 章 保护 APPC 通信

当您的系统参与具有其它系统的网络时，至您的系统的新的一组门户和窗口成为可用的。作为安全管理员，应该了解可以用来控制在 APPC 环境中进入您的系统的入口的选项。

高级程序间通信（APPC）是计算机（包括个人计算机）互相通信的一种方式。显示站联通、分布式数据管理和 iSeries Access for Windows 都可以使用 APPC 通信。

以下主题提供关于 APPC 通信如何工作和您可以如何设置适当的安全性的某些基本资料。这些主题主要集中在 APPC 配置中与安全性相关的元素上。要使此示例适应于您的情况，将需要与管理您的通信网络的人以及或许是您的应用程序供应商一起工作。使用此信息作为基础来帮助您理解可用于 APPC 的安全性问题和选项。

安全性从来不是“免费的”。使网络安全性更方便的某些建议可能使网络管理更困难。例如，此信息不强调 APPN®（Advanced Peer-to-Peer Networking®），因为如果没有 APPN，安全性更易于理解和管理。然而，如果没有 APPN，网络管理员必须手工创建 APPN 自动创建的配置信息。

PC 也使用通信

将 PC 连接至您的 iSeries 服务器的许多方法取决于通信，如 APPC 或 TCP/IP。当您阅读以下主题时，确保考虑连接至其它系统和连接至 PC 的安全性问题。当计划您的网络保护时，确保您不会对连接至您的系统的 PC 产生不利的影响。

APPC 术语

APPC 提供在一个系统上的用户在另一个系统上执行工作的能力。请求从中启动的系统称为以下任何一个:

- **源系统**
- **本地系统**
- **客户机**

接收请求的系统称为以下任何一个:

- **目标系统**
- **远程系统**
- **服务器**

APPC 通信的基本元素

从安全管理员的角度在一个系统（SYSTEMA）上的用户在另一个系统上（SYSTEMB）上执行有意义的工作之前，必须有以下情况发生:

- 源系统（SYSTEMA）必须提供目标系统（SYSTEMB）的路径。此路径称为 **APPC 会话**。

- 目标系统必须标识用户并使该用户与一个用户概要文件关联。目标系统必须支持源系统的加密算法（有关更多信息，请参阅第 14 页的『密码级别』）。
- 目标系统必须使用适当的环境（工作管理值）为该用户启动一个作业。

以下主题讨论这些元素以及它们如何与安全性相关。在目标系统上的安全管理员具有确保 APPC 用户不违背安全性的主要职责。然而，当两个系统上的安全管理员一起工作时，管理 APPC 安全性的作业非常容易。

示例: 基本 APPC 会话

在 APPC 环境中，当在一个系统上的用户或应用程序请求对另一个系统访问时，两个系统建立一个会话。要建立该会话，系统必须链接两个匹配的 APPC 设备描述。 在 SYSTEMA 设备描述中的远程位置名称（RMTLOCNAME）参数必须与在 SYSTEMB 设备描述中的本地位置名称（LCLLOCNAME）参数匹配，反之亦然。

为了两个系统建立 APPC 会话，在 SYSTEMA 和 SYSTEMB 上 APPC 设备描述中的位置密码必须相同。两者都必须指定 *NONE，或两者都必须指定相同的值。

如果密码是 *NONE 以外的值，则以加密格式存储和传送它们。如果密码匹配，则系统建立会话。如果密码不匹配，则拒绝用户的请求。当系统指定位置密码来建立会话时，这称为**安全绑定**。

注: 并非所有计算机系统都提供对安全绑定功能的支持。

限制 APPC 会话

作为在源系统上的安全管理员，可以使用对象权限来控制谁可以尝试访问其它系统。将 APPC 设备描述的公共权限设置为 *EXCLUDE 并将 *CHANGE 权限授予特定用户。使用 QLMTSECOFR 系统值来阻止具有 *ALLOBJ 特权的用户使用 APPC 通信。

作为在目标系统上的安全管理员，也可以使用对 APPC 设备的权限来阻止用户在您的系统上启动 APPC 会话。然而，您需要了解什么用户标识将尝试访问 APPC 设备描述。第 95 页的『APPC 用户对目标系统的访问』描述 iSeries 服务器如何使用户标识与对 APPC 会话的请求关联。

注: 可以使用“打印公共授权对象”（PRTPUBAUT *DEVD）命令和“打印专用权限”（PRTPVTAUT *DEVD）命令来找出谁对您的系统上的设备描述具有权限。

当您的系统使用 APPN 时，它自动创建新的 APPC 设备 （当现有设备不可用于系统选择的路由时）。限制对正在使用 APPN 的系统上 APPC 设备的访问的一种方法是创建权限列表。权限列表包含应该对 APPC 设备授权的用户的列表。然后可以使用“更改命令缺省值”（CHGCMDDFT）命令来更改 CRTDEVAPPC 命令。对于 CRTDEVAPPC 命令中的权限（AUT）参数，将缺省值设置为已创建的权限列表。

注: 如果您的系统具有英语以外的语言，则需要为系统上的每种本地语言更改 QSYSxxxx 库中的命令缺省值。

可以在 APPC 设备描述中使用位置密码（LOCPWD）参数来验证正在您的系统上请求会话的另一个系统的身份（代表用户或应用程序）。位置密码可以帮助您检测冒充系统。

当使用位置密码时，必须与在网络中的其它系统的安全管理员协调。也必须控制谁可以创建或更改 APPC 设备描述和配置列表。系统需要 *IOSYSCFG 特权来使用处理 APPC 设备和配置列表的命令。

注: 当您使用 APPN 时，位置密码存储在 QAPPNRMT 配置列表中，而不是存储在设备描述中。

APPC 用户对目标系统的访问

当系统建立 APPC 会话时，它们创建一条路径以用于发出请求的用户到达目标系统的门户。几个其它元素确定用户要进入其它系统必须执行的操作。

以下主题描述确定 APPC 用户如何获得进入目标系统的元素。

用于发送关于用户的信息的系统方法

APPC 体系结构提供了三种用于将关于用户的安全性信息从源系统发送至目标系统的方法。这些方法称为**体系结构化安全性值**。表 18 显示这些方法:

注: *APPC Programming* 一书提供关于体系结构化安全性值的更多信息。

表 18. 在 APPC 体系结构中的安全性值

体系结构化安全性值	发送至目标系统的用户标识	发送至目标系统的密码
None	否	否
Same	是[1]	请参阅注 2。
Program	是	是[3]

注:

1. 如果目标系统指定 SECURELOC(*YES) 或 SECURELOC(*VFYENCPWD)，源系统发送用户标识。
2. 用户未在请求中输入密码，因为源系统已经验证该密码。对于 SECURELOC(*YES) 和 SECURELOC(*NO)，源系统不发送该密码。对于 SECURELOC(*VFYENCPWD)，源系统检索存储的加密密码并发送它（以加密格式）。
3. 如果源和目标系统都支持密码加密，系统以加密格式发送密码。否则，不加密密码。

用户请求的应用程序确定体系结构化安全性值。例如，SNADS 始终使用 SECURITY(NONE)。 DDM 使用 SECURITY(SAME)。使用显示站联通，用户通过在 STRPASTHR 命令中使用参数来指定安全性值。

在所有情况下，目标系统选择是否接受具有在源系统上指定的安全性值的请求。在某些情况下，目标系统可能完全拒绝请求。在其它情况下，目标系统可能强制另一个安全性值。例如，当用户在 STRPASTHR 命令中同时指定用户标识和密码时，该请求使用 SECURITY(PGM)。然而，如果 QRMTSIGN 系统值在目标系统上是 *FRCSIGNON，则用户仍看到“注册”屏幕。对于 *FRCSIGNON 设置，系统始终使用 SECURITY(NONE)， 它等价于用户在 STRPASTHR 命令中未输入用户标识和密码。

注:

1. 在发送数据之前，源和目标系统协商安全性值。例如，在目标系统指定 SECURELOC(*NO) 而请求是 SECURITY(SAME) 的情况下，目标系统告诉源系统使用 SECURITY(NONE)。源系统不发送用户标识。

2. 当在目标系统上用户的密码到期时，目标系统拒绝会话请求。这仅适用于发送密码的连接请求，包括以下请求:
   - 类型为 SECURITY(PROGRAM) 的会话请求。
   - 当 SECURELOC 值为 *VFYENCPWD 的类型为 SECURITY(SAME) 的会话请求。

用于划分网络安全性职责的选项

当您的系统参与网络时，必须决定是否信任其它系统来验证正尝试进入您的系统的用户的身份。您将信任 SYSTEMA 来确保 USERA 确实是 USERA（或者 QSECOFR 确实是 QSECOFR）吗？或者您将要求用户再次提供用户标识和密码吗？

在目标系统上 APPC 设备描述中的安全位置（SECURELOC）参数指定 源系统是否是一个安全（可信）位置。

当两个系统都运行支持 *VFYENCPWD 的发行版时，SECURELOC(*VFYENCPWD) 在应用程序使用 SECURITY(SAME) 时提供附加保护。尽管请求者在请求时未输入密码，但源系统检索用户的密码并将它与请求一起发送。为了使请求成功，用户必须在两个系统上具有相同的用户标识和密码。

当目标系统指定 SECURELOC(*VFYENCPWD) 而源系统不支持此值时，目标系统将请求作为 SECURITY(NONE) 处理。

表 19 显示体系结构化安全性值和 SECURELOC 值如何一起工作:

表 19. APPC 安全性值和 SECURELOC 值如何一起工作

源系统	目标系统	
体系结构化安全性值	**SECURELOC 值**	**作业的用户概要文件**
无	任何值	缺省用户[1]
Same	*NO	缺省用户[1]
	*YES	与源系统中的请求者相同的用户概要文件名称。
	*VFYENCPWD	与源系统中的请求者相同的用户概要文件名称。在两个系统上用户必须具有相同的密码。
程序	任何值	在从源系统的请求上指定的用户概要文件。

注:

1. 在子系统描述中的通信项确定缺省用户。 『作业的用户概要文件的目标系统分配』描述这一点。

作业的用户概要文件的目标系统分配

当用户在另一个系统上请求 APPC 作业时，该请求具有与之关联的方式名称。该方式名称可以来自用户的请求，或它可以是来自源系统的网络属性的缺省值。

目标系统使用该方式名称和 APPC 设备名称来确定作业将如何运行。目标系统搜索活动子系统，以获取对于 APPC 设备名称和方式名称的最佳匹配的通信项。

通信项指定系统将为 SECURITY(NONE) 请求使用什么用户概要文件。以下是在子系统描述中通信项的一个示例:

```
                                显示通信项

子系统描述:  QCMN                状态:  活动

                                  作业                                缺省          最大
设备            方式              描述              库                用户          活动
*ALL            *ANY              *USRPRF                             *SYS          *NOMAX
*ALL            QPCSUPP           *USRPRF                             *NONE         *NOMAX
```

表 20 显示在通信项中缺省用户参数的可能值:

表 20. 对于缺省用户参数的可能值

值	结果
***NONE**	无缺省用户可用。如果源系统在请求中未提供用户标识，则作业将不运行。
***SYS**	只有 IBM 提供的程序（系统作业）将运行。将不运行用户应用程序。
用户名	如果源系统未发送用户标识，则作业在此用户概要文件之下运行。

可以使用“打印子系统描述”（PRTSBSDAUT）命令来打印具有与缺省用户概要文件的通信项的所有子系统列表。

显示站联通选项

显示站联通是使用 APPC 通信的应用程序示例。可以使用显示站联通来注册到通过网络连接至您的系统的另一个系统。

表 21 显示传递请求的示例（STRPASTHR 命令）和目标系统如何处理它们。对于显示站联通，系统使用 APPC 通信的基本元素和远程注册（QRMTSIGN）系统值。

注: “显示站联通”请求不再通过 QCMN 或 QBASE 子系统进行路由选择。从 V4R1 开始，它们通过 QSYSWRK 子系统进行路由选择。在 V4R1 之前，您可以假定，如果不启动 QCMD 或 QBASE 子系统，“显示站联通”将不起作用。这不再为真。可以通过将 QPASTHRSVR 系统值更改为 0 来强制“显示站联通”转至 QCMN（或 QBASE（如果它活动的话））。

表 21. 样本传递注册请求

在 STRPASTHR 命令中的值		**目标系统**		
用户标识	**密码**	**SECURELOC 值**	**QRMTSIGN 值**	**结果**
*NONE	*NONE	任何值	任何值	用户必须在目标系统上注册。
用户概要文件名称	未输入	任何值	任何值	请求失败。

表 21. 样本传递注册请求 (续)

在 STRPASTHR 命令中的值		目标系统		
用户标识	密码	SECURELOC 值	QRMTSIGN 值	结果
*CURRENT	未输入	*NO	任何值	请求失败。
		*YES	*SAMEPRF	交互式作业以与源系统上的用户概要文件名相同的用户概要文件名启动。没有任何密码传送到远程系统。用户概要文件名必须在目标系统上存在。
			*VERIFY	
			*FRCSIGNON	用户必须在目标系统上注册。
		*VFYENCPWD	*SAMEPRF	交互式作业以与源系统上的用户概要文件名相同的用户概要文件名启动。源系统检索用户密码并将它发送到远程系统。用户概要文件名必须在目标系统上存在。
			*VERIFY	
			*FRCSIGNON	用户必须在目标系统上注册。
*CURRENT（或作业的当前用户概要文件的名称）	已输入	任何值	*SAMEPRF	交互式作业以与源系统上的用户概要文件名相同的用户概要文件名启动。密码被发送到远程系统。用户概要文件名必须在目标系统上存在。
			*VERIFY	
			*FRCSIGNON	用户必须在目标系统上注册。
用户概要文件名称（不同于作业的当前用户概要文件的名称）	已输入	任何值	*SAMEPRF	请求失败。
			*VERIFY	交互式作业以与源系统上的用户概要文件名相同的用户概要文件名启动。密码被发送到远程系统。用户概要文件名必须在目标系统上存在。
			*FRCSIGNON	交互式作业从指定的用户概要文件名称开始。将密码发送至目标系统。用户概要文件名称必须在目标系统上存在。

避免意外的设备分配

当在活动设备上发生故障时，系统会尝试恢复。在某些情况下，当连接中断时，另一个用户可能会无意地重新建立有故障的会话。例如，假定 USERA 关闭了工作站的电源而没有注销。USERB 可以打开工作站的电源并重新启动 USERA 的会话而不必注册。

要防止这种可能性，将“设备 I/O 错误操作”（QDEVRCYACN）系统值设置为 *DSCMSG。当设备发生故障时，系统将结束用户的作业。

控制远程命令和批处理作业

几个选项可用于帮助您控制哪些远程命令和作业可以在您的系统上运行，包括以下内容:

- 如果您的系统使用 DDM，则可以限制对 DDM 文件的访问，以防止用户从另一个系统使用“提交远程命令”（SBMRMTCMD）命令。要使用 SBMRMTCMD，用户必须能够打开 DDM 文件。您还需要限制创建 DDM 文件的能力。
- 可以对 DDM 请求访问（DDMACC）系统值指定一个出口程序。在出口程序中，您可以先评估所有 DDM 请求，然后再允许它们。
- 可以使用网络作业操作（JOBACN）网络属性来防止提交网络作业或防止它们自动运行。
- 可以通过从子系统描述中除去 PGMEVOKE 路由项来显式指定哪些程序请求可以在通信环境中运行。PGMEVOKE 路由项使请求者能够指定运行的程序。当从子系统描述（如 QCMN 子系统描述）中除去此路由项时，必须为需要成功运行的通信请求添加路由项。

  第 78 页的『体系结构化 TPN 请求』列示通过 IBM 提供的应用程序的通信请求的程序名称。对于要允许的每个请求，可以添加使比较值和程序名称都等于程序名称的路由项。

  当使用此方法时，需要了解您的系统上的工作管理环境和您的系统上发生的通信请求的类型。如果可能的话，在更改路由项之后，应该测试所有类型的通信请求来确保它们工作正常。当通信请求未找到可用的路由项时，将接收到 CPF1269 消息。另一个替代方法（错误较少但可能有效性较差）是对于不需要在您的系统上运行的事务程序将公共权限设置为 *EXCLUDE。

  注: *Work Management* 一书提供了关于路由项和系统如何管理程序启动请求的更多信息。

评估 APPC 配置

可以使用“打印通信安全性”（PRTCMNSEC）命令或菜单选项来打印 APPC 配置中与安全性相关的值。以下主题描述有关报告的信息。

APPC 设备的相关参数

图 9 显示设备描述的“通信信息报告”的示例。第 100 页的图 10 显示配置列表的报告示例。报告后面是报告中的字段的解释。

通信信息（完整报告）

SYSTEM4

对象类型 . . . . . : *DEVD

对象名称	对象类型	设备类别	安全位置	位置密码	APPN 功能	单一会话	预先建立会话	SNUF 程序启动
CDMDEV1	*DEVD	*APPC	*NO	*NO	*NO	*YES	*NO	
CDMDEV2	*DEVD	*APPC	*NO	*NO	*NO	*YES	*NO	

图 9. APPC 设备描述 - 样本报告

```
                显示配置列表                          第 1 页
                            SYSTEM4  12/17/95  07:24:36
配置列表 . . . . . . . . . . . . . :   QAPPNRMT
配置列表类型 . . . . . . . . . . . :   *APPNRMT
文本 . . . . . . . . . . . . . . . :
----------------APPN 远程位置------------------
          远程                 远程       控制
远程      网络       本地      控制       点          安全
位置      标识       位置      点         网络标识    位置
SYSTEM36  APPN       SYSTEM4   SYSTEM36   APPN        *NO
SYSTEM32  APPN       SYSTEM4   SYSTEM32   APPN        *NO
SYSTEMU   APPN       SYSTEM4   SYSTEM33   APPN        *YES
SYSTEMJ   APPN       SYSTEM4   SYSTEMJ    APPN        *NO
SYSTEMR2  APPN       SYSTEM4   SYSTEM1    APPN        *NO
-------------------------APPN 远程位置---------------------------
          远程                                              本地        预先
远程      网络       本地      单一                        控制        建立
位置      标识       位置      会话          对话数        点          会话
SYSTEM36  APPN       SYSTEM4    *NO            10          *NO          *NO
SYSTEM32  APPN       SYSTEM4    *NO            10          *NO          *NO
```

图 10. 配置列表报告 - 示例

安全位置字段

安全位置（SECURELOC）字段指定本地系统是否信任远程系统代表它进行密码验证。SECURELOC 字段仅适用于使用 SECURITY(SAME) 值的应用程序，如 DDM 和使用 CPI 通信 API 的应用程序。

SECURELOC(*YES) 使本地系统对远程系统中可能的弱点敏感。在两个系统上存在的任何用户都可以调用本地系统上的程序。这一点特别危险，因为 QSECOFR（安全主管）用户概要文件在所有 iSeries 系统上都存在且具有 *ALLOBJ 特权。如果网络中的系统没有做好 QSECOFR 密码的保护工作，则将该系统当作安全位置的其它系统就会有风险。

使用 SECURELOC(*VFYENCPWD) 时，您的系统要比未适当保护密码的其它系统更安全。请求使用 SECURITY(SAME) 的应用程序的用户必须在两个系统上具有相同的用户标识和密码。SECURELOC(*VFYENCPWD) 要求在网络上使用密码管理策略，以便用户在所有系统上都有相同密码。

注: 仅在运行 V3R2、V3R7 或 V4R1 的系统之间支持 SECURELOC(*VFYENCPWD)。如果目标系统指定 SECURELOC(*VFYENCPWD) 而源系统不支持此功能，则以 SECURITY(NONE) 的形式处理该请求。

如果系统指定 SECURELOC(*NO)，使用 SECURITY(SAME) 的应用程序将需要缺省用户来运行程序。缺省用户取决于与请求相关联的设备描述和方式。（请参阅第 96 页的『作业的用户概要文件的目标系统分配』。）

位置密码字段

位置密码字段确定两个系统是否将交换密码以验证作出请求的系统不是冒充系统。第 94 页的『示例: 基本 APPC 会话』提供有关位置密码的更多信息。

“支持APPN”字段

“支持 APPN”（APPN）字段指定远程系统是否可以支持高级联网功能或是否限制为单中继段连接。APPN(*YES) 意味着:

- 如果远程系统是网络节点，远程系统可以将本地系统连接至其它系统。这称为**中间节点路由**。它意味着系统上的用户可能能够将远程系统用作较大网络的路由。
- 如果本地系统是网络节点，远程系统可以使用本地系统来与其它系统连接。远程系统上的用户可能能够将系统用作为较大网络的路由。

注: 可以使用 DSPNETA 命令来确定系统是网络节点还是终端节点。

“单个会话”字段

“单个会话”（SNGSSN）字段指定远程系统是否可以通过使用相同的 APPC 设备描述同时运行多个会话。通常使用 SNGSSN(*NO)，因为它消除了创建远程系统的多个设备描述的需要。例如，PC 用户经常需要多个 5250 仿真会话和文件服务器和打印服务器功能的会话。使用 SNGSSN(*NO)，可以为此功能提供 iSeries 系统上的 PC 的一个设备描述。

SNGSSN(*NO) 意味着必须依靠 PC 用户和其它 APPC 用户的有安全性意识的操作过程。系统易受在远程系统上启动未授权会话的人的攻击，该未授权会话使用与现有会话相同的设备描述。（此过程有时称为 **piggy-backing**。）

“预先建立会话”字段

当远程系统首次联系本地系统时，单个会话设备的“预先建立会话”（PREESTSSN）字段控制本地系统是否启动与远程系统的会话。PREESTSSN(*NO) 意味着本地系统等待应用程序请求与系统的会话之后才启动会话。PREESTSSN(*YES) 对于使应用程序完成连接的时间最小化是有用的。

PREESTSSN(*YES) 防止系统与不再使用的交换式（拨号）线路断开连接。应用程序或用户必须显式地使该线路脱机。PREESTSSN(*YES) 可能会增加本地系统在会话时受到 piggy-backing 攻击的时间。

“SNUF 程序启动”字段

“SNUF 程序启动”字段指定是否允许远程系统启动本地系统上的程序。*YES 意味着当远程系统上的用户启动作业并运行本地系统上的程序时，本地系统上的对象权限模式必须足够保护对象。

APPC 控制器的参数

图 11 显示控制器描述的“通信信息报告”的示例。在报告下面，将找到报告上字段的解释。

```
                          通信信息（完整报告）
                                                                  SYSTEM4
对象类型  . . . . . :   *CTLD

对象      对象      控制器      自动      交换式      调用      支持      CP        断开计时器      删除      设备
名称      类型      类别        创建      控制器      方向      APPN      会话      连接            秒数      名称
CTL01     *CTLD     *APPC       *YES       *YES       *DIAL     *YES      *YES        0             1440      AARON
CTL02     *CTLD     *APPC       *YES       *YES       *DIAL     *YES      *YES        0             1440      BASIC
CTL03     *CTLD     *APPC       *YES       *YES       *DIAL     *YES      *YES        0             1440      *NONE
```

图 11. APPC 控制器描述 - 样本报告

“自动创建”字段

在线路描述中，自动创建（AUTOCRTCTL）字段指定当入局请求找不到匹配的控制器描述时，本地系统是否自动创建控制器描述。在控制器描述中，自动创建（AUTOCRTDEV）字段指定当入局请求找不到匹配的设备描述时，本地系统是否自动创建设备描述。

对于支持 APPN 的控制器，自动创建字段无效。无论您已如何设置自动创建字段，系统在必要时会自动创建设备描述。

当对线路描述指定 *YES 时，具有对线路的访问权的任何用户都可以连接到您的系统。这包含由网桥和路由器连接的站点。

控制点会话字段

对于支持 APPN 的控制器，控制点会话（CPSSN）字段控制系统是否自动建立与远程系统的 APPC 连接。系统使用 CP 会话来与远程系统交换网络信息和状态。APPN 网络节点之间的最新信息的交换对于网络平稳地运行非常重要，

当指定 *YES 时，空闲的交换线路不会自动断开连接。这使系统对 piggy-back 会话更敏感。

断开计时器连接字段

对于 APPC 控制器，断开计时器连接字段指定，在系统断开至远程系统的连接线路之前，控制器必须有多长的时间处于未使用的状态（没有活动的会话）。此字段有两个值。第一个值指定自首次联系后控制器将保持活动的时间长度。第二个值确定最后的会话在控制器上结束后系统断开线路之前系统等待的时间长度。

仅当交换式断开连接（SWTDSC）字段是 *YES 时，系统才使用断开计时器连接。

如果使这些值较大，系统对 piggy-back 会话更敏感。

线路描述的参数

图 12 显示线路描述的“通信信息报告”的示例。在报告下面，将找到报告上字段的解释。

```
                    通信信息（完整报告）

对象类型  . . . . . :   *LIND
自动
对象          对象          线路          自动       删除       自动       自动
名称          类型          类别          创建       秒数       应答       拨号
LINE01        *LIND         *SDLC         *NO        0          *NO        *NO
LINE02        *LIND         *SDLC         *NO        0          *YES       *NO
LINE03        *LIND         *SDLC         *NO        0          *NO        *NO
LINE04        *LIND         *SDLC         *NO        0          *YES       *NO
```

图 12. APPC 线路描述 – 样本报告

自动应答字段

自动应答（AUTOANS）字段指定交换线路是否将接收没有操作员介入的入局呼叫。

当指定 *YES 时，系统不太安全，因为可以更容易地访问它。指定 *YES 时，要使安全性漏洞最小化，应在不需要线路时使线路脱机。

自动拨号字段

自动拨号（AUTODIAL）字段指定交换线路是否能进行出局呼叫而不需要操作员介入。当指定 *YES 时，允许对通信线路和调制解调器没有物理访问权的本地用户连接到其它系统。

第 13 章 保护 TCP/IP 通信

TCP/IP（传输控制协议／网际协议）是所有类型的计算机互相通信的一种常用方法。TCP/IP 应用程序是公认的并广泛用于『信息高速公路』.

本章提供以下方面的技巧:

- 防止 TCP/IP 应用程序在您的系统上运行。
- 当允许 TCP/IP 应用程序在您的系统上运行时，保护系统资源。

iSeries 信息中心 —> 联网 —> TCP/IP Web 站点是有关所有 TCP/IP 应用程序的完整信息源。*SecureWay®: iSeries 和因特网*（iSeries 信息中心 —> 安全性 —> SecureWay）描述当您将 iSeries 服务器连接至因特网（一个很大的 TCP/IP 网络）或内部网时的安全性注意事项。有关访问 “iSeries 信息中心” 的信息，请参阅第 xii 页的『先决条件和相关信息』。

记住，iSeries 服务器支持许多可能的 TCP/IP 应用程序。当您决定在您的系统中允许某个 TCP/IP 应用程序时，您也可能正在启用其它 TCP/IP 应用程序。作为安全管理员，您需要知道 TCP/IP 应用程序的范围和这些应用程序的安全性隐含。

防止 TCP/IP 处理

TCP/IP 服务器作业在 QSYSWRK 子系统中运行。可以使用 “启动 TCP/IP”（STRTCP）命令来在您的系统上启动 TCP/IP。如果您不想运行任何 TCP/IP 处理或应用程序，则不要使用 STRTCP 命令。您的系统在交付时将 STRTCP 命令的公共权限设置为 *EXCLUDE。

如果您怀疑对该命令具有访问权的某个人正在启动 TCP/IP（例如，在下班期间），则可以在 STRTCP 命令中设置对象审计。无论何时用户运行该命令，系统将写入一条审计日志项。

TCP/IP 安全性组件

可以利用几个 TCP/IP 安全性组件来提高您的网络安全性并增加灵活性。尽管也可以在防火墙产品中找到这些技术中的其中一部分，但 OS/400 的这些 TCP/IP 安全性组件并不打算用作防火墙。然而，在某些实例中也许能够使用这些功能部件的其中一部分来消除对单独防火墙产品的需要。也可能能够使用这些 TCP/IP 功能部件来在已经使用防火墙的环境中提供附加安全性。

可以利用下列组件来提高 “TCP/IP 安全性”:

- 信息包规则
- HTTP 代理服务器
- VPN（虚拟专用网络）
- SSL（安全套接字层）

使用信息包规则来保护 TCP/IP 流量

信息包规则是 IP 过滤和网络地址转换（NAT）的组合，它的作用类似防火墙，用来保护您的内部网络免遭闯入者的攻击。IP 过滤使您可以控制允许什么 IP 流量进出您的网络。基本上，它根据您定义的规则过滤信息包来保护您的网络。另一方面，NAT 使您能够将您的未注册的专用 IP 地址隐藏在一组已注册的 IP 地址后面。这有助于保护您的内部网络免受外部网络的影响。NAT 也有助于减轻 IP 地址耗尽问题，因为许多专用地址可以由较小的一组已注册的地址来表示。有关更多详细信息，请参阅 “iSeries 信息中心”。

HTTP 代理服务器

HTTP 代理服务器与 IBM HTTP Server for iSeries 服务器一起提供。HTTP Server 是 OS/400 的一部份。代理服务器接收来自 Web 浏览器的 HTTP 请求并将它们再发送到 Web 服务器。接收请求的 Web 服务器只知道代理服务器的 IP 地址，不能确定发出请求的 PC 的名称或地址。代理服务器可以处理 HTTP、FTP、Gopher 和 WAIS 的 URL 请求。

代理服务器高速缓存从所有代理服务器用户发出的请求所返回的 Web 页面。因此，当用户请求某个页面时，代理服务器检查该页面是否在高速缓存中。如果该页面在高速缓存中，则代理服务器返回高速缓存的页面。通过使用高速缓存的页面，代理服务器能够更快地处理 Web 页面，这消除了有可能对 Web 服务器的费时请求。

代理服务器也可以记录所有 URL 请求以进行跟踪。然后您可以复查记录以监控网络资源的使用和错误使用。

可以使用 IBM HTTP Server 中的 HTTP 代理支持来合并 Web 访问。PC 客户机的地址对于它们所访问的 Web 服务器是隐藏的；仅代理服务器的 IP 地址是已知的。Web 页面高速缓存也能够减小通信带宽需求和防火墙工作量。有关更多信息，访问 IBM HTTP Server for iSeries 主页: http://www-1.ibm.com/servers/eserver/iseries/software/http/index.html

虚拟专用网络（VPN）

虚拟专用网络（VPN）使您的公司能够基于公用网络（如因特网）的现有框架安全地扩展其专用内部网。使用 VPN，您的公司可以在提供重要的安全性功能部件（如认证和数据保密性）的同时控制网络流量。

OS/400 VPN 是 “iSeries 导航器” 的一种选择性安装的组件，“iSeries 导航器” 是 OS/400 的图形用户界面（GUI）。它使您能够在主机和网关的任何组合之间创建安全的端到端路径。OS/400 VPN 使用认证方法、加密算法和其它预防措施确保在其连接的两个端点之间发送的数据保持安全。

VPN 在 TCP/IP 分层通信堆栈模型的网络层上运行。特别地，VPN 使用 “IP 安全性体系结构”（IPSec）开放框架。IPSec 为因特网提供基本安全性功能并提供灵活的构件，您可以从这些构件创建健壮且安全的虚拟专用网络。

VPN 也支持 “第 2 层隧道协议”（L2TP）VPN 解决方案。L2TP 连接（也称为虚拟线路）通过允许公司的网络服务器管理指定给其远程用户的 IP 地址来为远程用户提供节省成本的访问。而且，当您使用 IPSec 保护 L2TP 连接时，L2TP 连接提供对您的系统或网络的安全访问。

了解 VPN 将对您的整个网络具有的影响是很重要的。正确的计划和实现是成功的基本条件。应该复查 “iSeries 信息中心” 中的 VPN 主题来确保您了解 VPN 如何工作以及您可以如何使用它们。有关更多信息，请参阅 iSeries 信息中心 —> 安全性 —> 虚拟专用网络。有关访问 “iSeries 信息中心” 的信息，请参阅第 xii 页的『先决条件和相关信息』。

安全套接字层（SSL）

“安全套接字层”（SSL）已成为一种业界标准，它用于在未保护的网络（如因特网）上启用安全通信会话的应用程序。SSL 协议在客户机和服务器应用程序之间建立安全连接，提供通信会话的一个或两个端点的认证。SSL 还提供客户机和服务器应用程序所交换的数据的保密性和完整性。有关更多信息，请参阅 iSeries 信息中心 –> 安全性 —> 安全套接字层（SSL）。有关访问 “iSeries 信息中心” 的信息，请参阅第 xii 页的『先决条件和相关信息』。

保护 TCP/IP 环境

此主题提供对在系统上 TCP/IP 环境中减少安全性漏洞的步骤的常规建议。这些技巧适用于整个 TCP/IP 环境而不是适用于下列主题中讨论的特定应用程序。

- 编写用于 TCP/IP 端口的应用程序时，确保正确地保护了应用程序。应假定外来者可以尝试通过该端口访问该应用程序。内行的外来者可能尝试 TELNET 至该应用程序。
- 监控系统上 TCP/IP 端口的使用。与 TCP/IP 端口相关联的用户应用程序可以对系统提供 “后门” 项，而没有用户标识和密码。系统上具有足够权限的人可以使应用程序与 TCP 或 UDP 端口相关联。
  - 作为安全管理员，应了解黑客使用的称为 *IP 欺骗*的技巧。TCP/IP 网络中的每个系统都具有 IP 地址。使用 IP 欺骗的某人设置了一个系统（通常是一台 PC）以假装是现有的 IP 地址或可信的 IP 地址。因此，通过假装是您通常与其连接的系统，冒充者可以建立与您的系统的连接。

    如果在您的系统上运行 TCP/IP，并且您的系统加入了物理上未受保护的网络（所有非交换式线路和预定义链接），您就很容易受到 IP 欺骗的攻击。要保护系统不受 “欺骗者” 损害，从本章中的建议开始，如注册保护和对象安全性。您也应确保系统具有合理的辅助存储量限制设置。这防止欺骗者用大量邮件或假脱机文件来攻击系统使系统变为不可操作。

    另外，应定期监控系统上 TCP/IP 的活动。如果检测到 IP 欺骗，可以尝试发现 TCP/IP 设置中的弱点并进行调整。
  - 对于内部网（不需要直接连接到外部的系统网络），使用可再用的 IP 地址。可再用的地址用于专用网络。因特网的骨干网不路由具有可再用的 IP 地址的信息包。因此，可再用的地址在防火墙内部提供添加的保护层。

    “iSeries 信息中心” —> 联网 —> TCP/IP Web 站点提供有关如何指定 IP 地址和 IP 地址的范围的更多信息以及有关 TCP/IP 的安全性信息。
  - 如果考虑将系统连接到因特网或内部网，复查 *SecureWay: iSeries 和因特网*（iSeries 信息中心 —> 安全性 —> SecureWay）的安全性信息。有关访问 “iSeries 信息中心” 的信息，请参阅第 xii 页的『先决条件和相关信息』。

控制要自动启动哪些 TCP/IP 服务器

作为安全管理员，当启动 TCP/IP 时，需要控制要自动启动哪些 TCP/IP 应用程序。两个命令都可用于启动 TCP/IP。对于每个命令，系统都使用不同的方法确定要启动哪些应用程序（服务器）。

表 22 显示两个命令和对它们的安全性建议。表 23 显示服务器的缺省自动启动值。要更改服务器的自动启动值，对服务器使用 CHGxxxA（更改 xxx 属性）命令。例如，TELNET 的命令 CHGTELNA。

表 22. TCP/IP 命令如何确定要启动哪些服务器

命令	服务器启动什么	安全性建议
启动 TCP/IP（STRTCP）	系统启动指定 AUTOSTART(*YES) 的每个服务器。表 23 显示每个 TCP/IP 服务器的交付值。	• 谨慎地指定 *IOSYSCFG 特权以控制可以更改自动启动设置的用户。 • 谨慎地控制具有使用 STRTCP 命令的权限的用户。命令的缺省公共权限是 *EXCLUDE。 • 对“更改*服务器名*属性”命令（如 CHGTELNA）设置对象审计以监控试图更改服务器的 AUTOSTART 值的用户。
启动 TCP/IP 服务器（STRTCPSVR）	使用参数指定要启动哪些服务器。此命令在交付时的缺省值是要启动所有服务器。	• 使用“更改命令缺省值”（CHGCMDDFT）命令将 STRTCPSVR 命令设置为仅启动指定服务器。这不会防止用户启动其它服务器。然而，通过更改命令缺省值，使用户将偶然启动所有服务器的可能性变小。例如，使用下列命令将缺省值设置为只启动 TELNET 服务器：`CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)')` **注**：更改缺省值时，只可以指定单个服务器。选择定期使用的服务器或最不可能导致安全性漏洞的服务器（如 TFTP）。 • 谨慎地控制哪些用户具有使用 STRTCPSVR 命令的权限。命令的缺省公共权限是 *EXCLUDE。

下表包含 TCP/IP 服务器的自动启动值。有关每个这些服务器的更多信息，访问“iSeries 信息中心”（**联网 —> TCP/IP**）。有关访问“iSeries 信息中心”的详细信息，请参阅第 xii 页的『先决条件和相关信息』。

表 23. TCP/IP 服务器的自动启动值

服务器	缺省值	您的值
TELNET	AUTOSTART(*YES)	
FTP（文件传输协议）	AUTOSTART(*YES)	
BOOTP (引导协议)	AUTOSTART(*NO)	
TFTP（次要文件传输协议）	AUTOSTART(*NO)	
REXEC（远程执行服务器）	AUTOSTART(*NO)	
RouteD（路由守护程序）	AUTOSTART(*NO)	
SMTP（简单电子邮件传输协议）	AUTOSTART(*YES)	
POP（邮局协议）	AUTOSTART(*NO)	
HTTP（超文本传输协议）[1]	AUTOSTART(*NO)	
ICS（因特网连接服务器）[1]	AUTOSTART(*NO)	
LPD（行式打印机守护程序）	AUTOSTART(*YES)	

表 23. TCP/IP 服务器的自动启动值 (续)

服务器	缺省值	您的值
SNMP（简单网络管理协议（SNMP））	AUTOSTART(*YES)	
DNS（域名系统）	AUTOSTART(*NO)	
DDM	AUTOSTART(*NO)	
DHCP（动态主机配置协议）	AUTOSTART(*NO)	
NSMI	AUTOSTART(*NO)	
INETD	AUTOSTART(*NO)	
注: 1. 使用 IBM HTTP Server for iSeries 服务器，使用 CHGHTTPA 命令来设置 AUTOSTART 值。		

使用 SLIP 的安全性注意事项

iSeries 服务器 TCP/IP 支持包含串行接口线协议（SLIP）。 SLIP 提供低成本的点到点连接性。通过建立与作为 LAN 或 WAN 的一部分的系统的点到点连接，SLIP 用户可以连接到 LAN 或 WAN。

SLIP 在异步连接上运行。可以将 SLIP 用于与 iSeries 服务器的拨号连接。例如，可以使用 SLIP 从 PC 拨入 iSeries 系统。在建立连接之后，可以使用 PC 上的 TELNET 应用程序来连接到 iSeries TELNET 服务器。或者，可以使用 FTP 应用程序在两个系统之间传送文件。

您的系统在交付时不存在 SLIP 配置。因此，如果不想要 SLIP（和拨号 TCP/IP）在系统上运行，不要为 SLIP 配置任何配置概要文件。使用“使用 TCP/IP 点到点”（WRKTCPPTP）命令来创建 SLIP 配置。必须具有 *IOSYSCFG 特权才能使用 WRKTCPPTP 命令。

如果想要 SLIP 在系统上运行，创建一个或多个 SLIP（点到点）配置概要文件。可以使用以下操作方式创建配置概要文件:

- 拨入（*ANS）
- 拨出（*DIAL）

下列主题讨论如何可以设置 SLIP 配置概要文件的安全性。

注: **用户概要文件**是允许注册的 iSeries 服务器对象。每个 iSeries 服务器作业都必须具有要运行的用户概要文件。**配置概要文件**存储用于建立与 iSeries 系统的 SLIP 连接的信息。当启动与 iSeries 服务器的 SLIP 连接时，就简单地建立了链接。您尚未注册和启动 iSeries 服务器作业。因此，您未必需要用户概要文件来启动与 iSeries 服务器的 SLIP 连接。然而，您将在以下讨论中看到，SLIP 配置概要文件可能需要用户概要文件来确定是否允许连接。

控制拨入 SLIP 连接

必须启动 SLIP *ANS 配置概要文件，才能使用 SLIP 建立与您的系统的拨入连接。要创建或更改 SLIP 配置概要文件，使用“使用 TCP/IP 点到点”（WRKTCPPTP）命令。要启动配置概要文件，使用“启动 TCP/IP 点到点”（STRTCPPTP）命令或 WRKTCPPTP 屏幕中的选项。交付系统时，STRTCPPTP 和 ENDTCPPTP 命令的公共

权限是 *EXCLUDE。仅当具有 *IOSYSCFG 特权时，添加、更改和删除 SLIP 配置概要文件的选项才可用。作为安全管理员，您可以使用命令权限和特权来确定谁可以将系统设置为允许拨入连接。

保护拨入 SLIP 连接

如果要验证拨入您的系统的系统，则您希望作出请求的系统发送用户标识和密码。然后您的系统可以验证用户标识和密码。如果用户标识和密码无效，您的系统可以拒绝会话请求。

要设置拨入验证，执行下列操作:

__ 步骤 1. 创建作出请求的系统可以用来建立连接的用户概要文件。请求者发送的用户标识和密码必须与此用户概要文件名和密码匹配。

注: 要系统执行密码验证，必须将 QSECURITY 系统值设置为 20 或更高。

作为附加保护，可能要特别地创建用户概要文件以建立 SLIP 连接。该用户概要文件在系统上应具有限制权限。如果不计划对建立 SLIP 连接以外的任何功能使用概要文件，可以在用户概要文件中设置下列值:

- *SIGNOFF 的初始菜单（INLMNU）
- *NONE 的初始程序（INLPGM）。
- *YES 的限制能力（LMTCPB）

这些值防止任何人使用用户概要文件交互式地注册。

__ 步骤 2. 创建系统的权限列表，以便当请求者尝试建立 SLIP 连接时进行检查。

注: 当创建或更改 SLIP 概要文件时，在*系统访问权限列表*字段中指定此权限列表。（请参阅步骤 4。）

__ 步骤 3. 使用 “添加授权项”（ADDAUTLE）命令将步骤 1 中创建的用户概要文件添加到权限列表。可以为每个点到点配置概要文件都创建一个唯一的权限列表，也可以创建几个配置概要文件共享的权限列表。

__ 步骤 4. 使用 WRKTCPPTP 命令来设置具有以下特征的 TCP/IP 点到点 *ANS 概要文件:

- 配置概要文件必须使用包含用户验证功能的连接对话框脚本。用户验证包括接受来自请求者的用户标识和密码并验证它们。系统交付了几个提供此功能的样本对话框脚本。
- 配置概要文件必须指定您在步骤 2 中创建的权限列表的名称。连接对话框脚本接收的用户标识必须在权限列表中。

记住，设置拨入安全性的值受所拨入的系统的安全性习惯和能力的影响。如果需要用户标识和密码，则作出请求的系统上的连接对话框脚本必须发送用户标识和密码。某些系统（如 iSeries 服务器）提供了存储用户标识和密码的安全方法。（第 111 页的『安全性和拨出会话』描述了该方法。）其它系统将用户标识和密码存储在脚本中，知道系统上何处可以找到该脚本的任何人都可以访问该脚本。

因为通信伙伴的不同安全性习惯和能力，可能要对不同的请求环境创建不同的配置概要文件。使用 STRTCPPTP 命令来将系统设置为接受特定配置概要文件的会话。例如，仅可在一天的某些时间启动某些配置概要文件的会话。可以使用安全性审计来记录相关联用户概要文件的活动。

防止拨入用户访问其它系统

取决于系统和网络配置，启动 SLIP 连接的用户可能能够访问网络中的另一系统而不必注册到您的系统。例如，用户能够建立与系统的 SLIP 连接。然后，用户能够建立与网络中不允许拨入的另一个系统的 FTP 连接。

通过对配置概要文件中的*允许 IP 数据报转发*字段指定 N（否），可以防止 SLIP 用户访问网络中的其它系统。这防止用户在注册到系统之前访问网络。然而，在用户成功地注册到系统之后，数据报转发值无效。它不限制用户在 iSeries 系统上使用 TCP/IP 应用程序（FTP 或 TELNET）来建立与网络中另一系统的连接的能力。

控制拨出会话

必须启动 SLIP *DIAL 配置概要文件，才可以使用 SLIP 来建立与系统的拨出连接。要创建或更改 SLIP 配置概要文件，使用 WRKTCPPTP 命令。要启动配置概要文件，使用“启动 TCP/IP 点到点”（STRTCPPTP）命令或 WRKTCPPTP 屏幕中的选项。交付系统时，STRTCPPTP 和 ENDTCPPTP 命令的公共权限是 *EXCLUDE。仅当具有 *IOSYSCFG 特权时，添加、更改和删除 SLIP 配置概要文件的选项才可用。作为安全管理员，您可以使用命令权限和特权来确定谁可以将系统设置为允许拨出连接。

安全性和拨出会话

iSeries 系统上的用户可能要建立与要求用户验证的系统的拨出连接。iSeries 服务器上的连接对话框脚本必须将用户标识和密码发送到远程系统。iSeries 服务器提供存储该密码的安全方法。密码不需要存储在连接对话框脚本中。

注:

1. 即使系统以加密形式存储连接密码，系统会在发送密码之前解密它。与 FTP 和 TELNET 密码一样，将 SLIP 密码以未加密（“以明文”）的形式发送。然而，与 FTP 和 TELNET 不同，系统在建立 TCP/IP 方式之前发送 SLIP 密码。

   因为 SLIP 以异步方式使用点到点连接，发送未加密的密码时的安全性漏洞与 FTP 和 TELNET 密码的漏洞不同。未加密的 FTP 和 TELNET 密码可以作为网络上的 IP 流量发送，因此易受到电子窃听。SLIP 密码的传输与两个系统之间的电话连接一样安全。
2. 存储 SLIP 连接对话框脚本的缺省文件是 QUSRSYS/QATOCPPSCR。此文件的公共权限是 *USE，它防止公共用户更改缺省连接对话框脚本。

当为要求验证的远程会话创建连接概要文件时，请执行以下操作:

__ 步骤 1. 确保“保留服务器安全性数据”（QRETSVRSEC）系统 值是 1（是）。此系统值确定您是否允许将可以解密的密码存储在系统上受保护的区域。

__ 步骤 2. 使用 WRKTCPPTP 命令来创建具有下列特征的配置概要文件:

- 对于配置概要文件的方式，指定 *DIAL。
- 对于*远程服务访问名称*，指定远程系统期望的用户标识。例如，如果正在连接到另一个 iSeries 服务器，指定该 iSeries 服务器上的用户概要文件名称。
- 对于*远程服务访问密码*，指定远程系统对此用户标识期望的密码。在您的 iSeries 服务器上，此密码以可以解密的形式存储在受保护的区域中。对配置概要文件指定的名称和密码与 QTCP 用户概要文件相关联。不能用任何用户命令和接口访问这些名称和密码。仅已注册的系统程序可以访问此密码信息。

注: 记住，当保存 TCP/IP 配置文件时，未保存连接概要文件的密码。要保存 SLIP 密码，需要使用“保存安全性数据”（SAVSECDTA）命令来保存 QTCP 用户概要文件。

- 对于连接对话框脚本，指定发送用户标识和密码的脚本。系统交付了几个提供此功能的样本对话框脚本。当系统运行该脚本时，系统检索密码，解密它并将它发送到远程系统。

点到点协议的安全性注意事项

点到点协议（PPP）可用作 TCP/IP 的一部分。PPP 是点到点连接的业界标准，它提供可与 SLIP 一起使用的附加功能。

使用 PPP，iSeries 服务器可以具有与“因特网服务提供商”或与内部网或外部网中的其它系统的直接高速连接。远程 LAN 可以实际地建立与您的 iSeries 服务器的拨入连接。

记住，与 SLIP 一样，PPP 也提供与 iSeries 服务器的网络连接。PPP 连接主要将请求者带到系统的门户。请求者仍需要用户标识和密码才能进入系统并连接到与 TELNET 或 FTP 类似的 TCP/IP 服务器。以下是此新连接能力的安全性注意事项:

注: 通过使用 IBM iSeries Access for Windows 工作站上的“iSeries 导航器”配置 PPP。

- PPP 提供具有专用连接的能力（其中相同用户总是具有相同的 IP 地址）。使用专用地址，具有 IP 欺骗（假装是具有已知 IP 地址的可信系统的冒充系统）的可能性。然而，PPP 提供的增强型认证能力帮助保护防止 IP 欺骗。
- 与 SLIP 一样，使用 PPP 创建具有用户名和相关联的密码的连接概要文件。然而，与 SLIP 不同，用户不必具有有效的用户概要文件和密码。用户名和密码与用户概要文件不关联。相反，验证列表用于 PPP 认证。另外，PPP 不需要连接脚本。认证（用户名和密码的交换）是 PPP 体系结构的一部分，且以比使用 SLIP 更低级别发生。
- 使用 PPP，具有使用 CHAP（询问握手认证协议）的选项。因为 CHAP 加密用户名和密码，您将不再需要担心偷听者窃听密码。

  仅当两边都具有 CHAP 支持时，PPP 连接才使用 CHAP。交换信号以在两个调制解调器之间设置通信期间，两个系统协商。例如，如果 SYSTEMA 支持 CHAP 而 SYSTEMB 不支持，SYSTEMA 可以拒绝会话或同意使用解密用户名和密码。同意使用解密用户名和密码称为纵向协商。纵向协商的决定是配置选项。在内部网上，例如，其中您知道所有系统都具有 CHAP 能力，应配置连接概要文件以便它将不会纵向协商。在系统拨出的公共连接上，您可能愿意纵向协商。

  PPP 连接概要文件提供指定有效的 IP 地址的能力。例如，您可以指示对特定用户期望特定地址或地址范围。此能力与加密密码的能力一起提供防止电子欺骗的进一步的保护。

  作为在活动会话上防止电子欺骗或 piggy-backing 的附加保护，可以将 PPP 配置为以指定的时间间隔重新提问。例如，当 PPP 会话处于活动状态时，iSeries 服务器可能会提问其它系统以获取用户和密码。它每 15 分钟进行一次，以确保它是同一连接概要文件。（最终用户将不知道此重新提问活动。系统在最终用户见到的级别以下交换名称和密码。）

  使用 PPP，期望远程 LAN 可以建立到 iSeries 服务器和到扩展的网络的拨入连接。在此环境中，使 IP 转发打开可能是需要。IP 转发具有允许闯入者通过网络漫游的潜在可能。然而，PPP 具有更强的保护（如密码的加密和 IP 地址验证）。它使闯入者可以首先建立网络连接的可能性变小。

有关 PPP 的更多信息，请参阅 “iSeries 信息中心”。

使用引导协议服务器的安全性注意事项

引导协议（BOOTP）提供使工作站与服务器相关联并指定工作站 IP 地址和初始程序装入（IPL）源的动态方法。

BOOTP 是一种 TCP/IP 协议，用于允许无介质工作站（客户机）从网络上的服务器请求包含初始代码的文件。BOOTP 服务器在公认 BOOTP 服务器端口 67 上侦听。当接收到客户机请求时，服务器查找对客户机定义的 IP 地址并用客户机的 IP 地址和装入文件的名称对客户机返回一个应答。然后客户机对服务器启动对装入文件的 TFTP 请求。客户机硬件地址和 IP 地址之间的映射保存在 iSeries 服务器上的 BOOTP 表中。

防止 BOOTP 访问

如果没有任何瘦客户机连接到网络，不需要在系统上运行 BOOTP 服务器。它可用于其它设备，但这些设备的首选解决方案是使用 DHCP。执行下列操作来防止 BOOTP 服务器运行:

__ 步骤 1. 要防止当启动 TCP/IP 时 BOOTP 服务器作业自动启动，输入以下命令:

```
CHGBPA AUTOSTART(*NO)
```

注:

a. AUTOSTART(*NO) 是缺省值。

b. 第 108 页的『控制要自动启动哪些 TCP/IP 服务器』提供有关控制哪些 TCP/IP 服务器自动启动的更多信息。

__ 步骤 2. 要防止他人将用户应用程序（例如套接字应用程序）与系统通常用于 BOOTP 的端口相关联，执行下列操作:

注: 因为 DHCP 和 BOOTP 使用相同的端口号，这将也禁止由 DHCP 使用的端口。如果要使用 DHCP，不要限制端口。

__ 步骤 a. 输入 GO CFGTCP 以显示 “配置 TCP/IP” 菜单。

__ 步骤 b. 选择选项 4（使用 TCP/IP 端口限制）。

__ 步骤 c. 在 “使用 TCP/IP 端口限制” 屏幕上，指定选项 1（添加）。

__ 步骤 d. 对于端口范围下限，指定 67。

__ 步骤 e. 对于端口范围上限，指定 *ONLY。

注:

1) 端口限制在下次启动 TCP/IP 时生效。如果设置端口限制时 TCP/IP 是活动的，应结束 TCP/IP 并重新启动它。

2) RFC1700 提供有关公共端口号指定的信息。

__ 步骤 f. 对于协议，指定 *UDP。

__ 步骤 g. 对于用户概要文件字段，指定系统上受保护的用户概要文件名称。（受保护的用户概要文件是不拥有沿用权限的程序且不具有其它用户知道的密码的用户概要文件。）通过将端口限制于特定的用户，自动排除所有其它用户。

保护 BOOTP 服务器

BOOTP 服务器不提供对 iSeries 系统的直接访问权，因此会引起限制的安全性漏洞。作为安全管理员，主要关注确保正确的信息与正确的瘦客户机相关联。即，捣乱者可以变更 BOOTP 表并导致瘦客户机工作不正常或根本不工作。

要管理 BOOTP 服务器和 BOOTP 表，必须具有 *IOSYSCFG 特权。需要谨慎地控制在系统上具有 *IOSYSCFG 特权的用户概要文件。

使用 DHCP 服务器的安全性注意事项

动态主机配置协议（DHCP）提供用于将配置信息传送到 TCP/IP 网络上的主机的框架。对于客户机工作站，DHCP 可以提供类似于自动配置的功能。客户机工作站上启用了 DHCP 的程序广播配置信息请求。如果 DHCP 服务器正在 iSeries 服务器上运行，该服务器通过发送客户机工作站正确配置 TCP/IP 所需要的信息响应该请求。

可以使用 DHCP 使用户第一次连接到 iSeries 服务器更简单。这是因为用户不需要输入 TCP/IP 配置信息。也可以使用 DHCP 来减少在子网中需要的内部 TCP/IP 地址的数目。DHCP 服务器可以临时将 IP 地址分配给活动用户（从 IP 地址池）。

对于瘦客户机，可以使用 DHCP 代替 BOOTP。DHCP 提供比 BOOTP 更多的功能，它可以支持瘦客户机和 PC 的动态配置。

防止 DHCP 访问

如果不想让任何人使用系统上的 DHCP 服务器，执行下列操作:

1. 要防止当启动 TCP/IP 时 DHCP 服务器作业自动启动，输入以下命令:

   ```
   CHGDHCPA AUTOSTART(*NO)
   ```

   注:

   a. AUTOSTART(*NO) 是缺省值。

   b. 第 108 页的『控制要自动启动哪些 TCP/IP 服务器』提供有关控制哪些 TCP/IP 服务器自动启动的更多信息。

2. 要防止他人将用户应用程序（例如套接字应用程序）与系统通常用于 DHCP 的端口相关联，执行下列操作:

   a. 输入 GO CFGTCP 以显示“配置 TCP/IP”菜单。

   b. 选择选项 4（使用 TCP/IP 端口限制）。

   c. 在“使用 TCP/IP 端口限制”屏幕上，指定选项 1（添加）。

   d. 对于端口范围下限，指定 67。

   e. 对于端口范围上限，指定 68。

      注:

      1) 端口限制在下次启动 TCP/IP 时生效。如果设置端口限制时 TCP/IP 是活动的，应结束 TCP/IP 并重新启动它。

      2) RFC1700 提供有关公共端口号指定的信息。

   f. 对于协议，指定 *UDP。

   g. 对于用户概要文件字段，指定系统上受保护的用户概要文件名称。（受保护的用户概要文件是不拥有沿用权限的程序且不具有其它用户知道的密码的用户概要文件。）通过将端口限制于特定的用户，自动排除所有其它用户。

保护 DHCP 服务器

以下是当您选择在 iSeries 系统上运行 DHCP 时的安全注意事项:

- 限制具有管理 DHCP 的权限的用户的数目。管理 DHCP 需要下列权限:
  - *IOSYSCFG 特权
  - 对下列文件的 *RW 权限:

    ```
    /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
    /QIBM/UserData/OS400/DHCP/dhcprd.cfg
    ```
- 评估 LAN 的物理上的可访问性。外来者能够容易地携带膝上型计算机走入您的位置并物理地连接到您的 LAN 吗？如果这是一种漏洞，则 DHCP 提供创建 DHCP 服务器将配置的客户机（硬件地址）列表的能力。当使用此功能部件时，您除去 DHCP 对网络管理员提供的生产益处。然而，应防止系统配置未知工作站。
- 如果可能，使用可再用的（对于因特网未体系结构化的）IP 地址池。这帮助防止来自网络外的工作站从服务器获取可用的配置信息。
- 如果需要附加安全性保护，使用 DHCP 出口点。以下是出口点和它们能力的概述。*iSeries System API Reference* 描述如何使用这些出口点。

  端口项 无论系统何时从端口 67（DHCP 端口）读数据包，它都调用出口程序。出口程序接收完整的数据包。它能够确定系统应处理还是应废弃该数据包。当现有的 DHCP 屏幕功能部件不够使用时，可以使用此出口点。

  地址指定
  无论 DHCP 何时对客户机正式指定地址，系统都调用出口程序。

  地址释放
  无论 DHCP 形式上何时释放地址并将它放回地址池中，系统都调用出口程序。

使用 TFTP 服务器的安全性注意事项

次要文件传输协议（TFTP）提供没有用户认证的基本文件传送。TFTP 使用“引导协议”（BOOTP）或“动态主机配置协议”（DHCP）。

客户机最初连接到 BOOTP 服务器或 DHCP 服务器。BOOTP 服务器或 DHCP 服务器用客户机的 IP 地址和装入文件的名称应答。然后客户机对服务器启动对装入文件的 TFTP 请求。当客户机结束装入文件的下载时，它结束 TFTP 会话。

防止 TFTP 访问

如果没有任何瘦客户机连接到网络，可能不需要在系统上运行 TFTP 服务器。执行下列操作来防止 TFTP 服务器运行:

__ 步骤 1. 要防止当启动 TCP/IP 时 TFTP 服务器作业自动启动，输入以下命令:

```
CHGTFTPA AUTOSTART(*NO)
```

注:

a. AUTOSTART(*NO) 是缺省值。

b. 第 108 页的『控制要自动启动哪些 TCP/IP 服务器』提供有关控制哪些 TCP/IP 服务器自动启动的更多信息。

__ 步骤 2. 要防止他人将用户应用程序（例如套接字应用程序）与系统通常用于 TFTP 的端口相关联，执行下列操作:

__ 步骤 a. 输入 GO CFGTCP 以显示“配置 TCP/IP”菜单。

__ 步骤 b. 选择选项 4（使用 TCP/IP 端口限制）。

__ 步骤 c. 在“使用 TCP/IP 端口限制”屏幕上，指定选项 1（添加）。

__ 步骤 d. 对于端口范围下限，指定 69。

__ 步骤 e. 对于端口范围上限，指定 *ONLY。

注:

1) 端口限制在下次启动 TCP/IP 时生效。如果设置端口限制时 TCP/IP 是活动的，应结束 TCP/IP 并重新启动它。
2) RFC1700 提供有关公共端口号指定的信息。

__ 步骤 f. 对于协议，指定 *UDP。

__ 步骤 g. 对于用户概要文件字段，指定系统上受保护的用户概要文件名称。（受保护的用户概要文件是不拥有沿用权限的程序且不具有其它用户知道的密码的用户概要文件。）通过将端口限制于特定的用户，自动排除所有其它用户。

保护 TFTP 服务器

缺省情况下，TFTP 服务器提供对 iSeries 系统的非常有限的访问权。明确地配置它以对瘦客户机提供初始代码。作为安全管理员，应了解 TFTP 服务器的下列特征:

- TFTP 服务器不需要认证（用户标识和密码）。所有 TFTP 作业都在 QTFTP 用户概要文件下运行。QTFTP 用户概要文件不具有密码。因此，它对交互式注册不可用。QTFTP 用户概要文件不具有任何特权，也不显式地授权给系统资源。它使用公共权限来访问对瘦客户机需要的资源。
- 当 TFTP 服务器到达时，配置它以访问包含瘦客户机信息的目录。必须已授予 *PUBLIC 或 QTFTP 权限来读取或写入到该目录。要写入到该目录，必须已在 CHGTFTPA 命令的“允许文件写”参数上指定 *CREATE。要写入到现有的文件，必须已在 CHGTFTPA 的“允许文件写”参数上指定 *REPLACE。 *CREATE 允许替换现有的文件或创建新文件。 *REPLACE 仅允许您替换现有文件。

  TFTP 客户机不能访问任何其它目录，除非明确地用“更改 TFTP 属性”（CHGTFTPA）命令定义目录。因此，如果本地或远程用户试图启动对系统的 TFTP 会话，则用户访问信息或导致损害的能力受到极度地限制。
- 如果选择配置 TFTP 服务器来提供除处理瘦客户机以外的其它服务，可以将出口程序定义为评估并认证每个 TFTP 请求。TFTP 服务器提供类似于可用于 FTP 服务器的出口的请求验证出口。有关更多信息，请参阅 iSeries 信息中心 —> 联网 —> TCP/IP —> TFTP。有关访问 “iSeries 信息中心” 的信息，请参阅第 xii 页的『先决条件和相关信息』。

使用 REXEC 服务器的安全性注意事项

远程执行服务器（REXEC）接收并运行来自 REXEC 客户机的命令。REXEC 客户机一般是支持发送 REXEC 命令的 PC 或 UNIX 应用程序。此服务器提供的该支持类似于当使用 FTP 服务器的 RCMD（远程命令）子命令时可用的能力。

防止 REXEC 访问

如果不想 iSeries 服务器接受来自 REXEC 客户机的命令，执行下列操作来防止 REXEC 服务器运行:

__ 步骤 1. 要防止当启动 TCP/IP 时 REXEC 服务器作业自动启动，输入以下命令:

```
CHGRXCA AUTOSTART(*NO)
```

注:

a. AUTOSTART(*NO) 是缺省值。

b. 第 108 页的『控制要自动启动哪些 TCP/IP 服务器』提供有关控制哪些 TCP/IP 服务器自动启动的更多信息。

__ 步骤 2. 要防止他人将用户应用程序（例如套接字应用程序）与系统通常用于 REXEC 的端口相关联，执行下列操作:

__ 步骤 a. 输入 GO CFGTCP 以显示“配置 TCP/IP”菜单。

__ 步骤 b. 选择选项 4（使用 TCP/IP 端口限制）。

__ 步骤 c. 在“使用 TCP/IP 端口限制”屏幕上，指定选项 1（添加）。

__ 步骤 d. 对于端口范围下限，指定 512。

__ 步骤 e. 对于端口范围上限，指定 *ONLY。

__ 步骤 f. 对于协议，指定 *TCP。

__ 步骤 g. 对于用户概要文件字段，指定系统上受保护的用户概要文件名称。（受保护的用户概要文件是不拥有沿用权限的程序且不具有其它用户知道的密码的用户概要文件。）通过将端口限制于特定的用户，自动排除所有其它用户。

注:

a. 端口限制在下次启动 TCP/IP 时生效。如果设置端口限制时 TCP/IP 是活动的，应结束 TCP/IP 并重新启动它。

b. RFC1700 提供有关公共端口号指定的信息。

保护 REXEC 服务器

以下是选择在系统上运行“远程执行服务器”时的注意事项:

- REXCD 请求包含用户标识、密码和运行的命令。正常 iSeries 服务器认证和权限检查适用于:
  - 用户概要文件和密码联合必须有效。
  - 系统对用户概要文件实施*限制能力*（LMTCPB）值。
  - 必须已对用户授予对该命令和该命令使用的所有资源的权限。
- REXEC 服务器提供的出口点类似于可用于 FTP 服务器的出口点。可以使用“验证”出口点来评估该命令并决定是否允许它。有关更多信息，请参阅 iSeries 信息中心 —> 联网 —> TCP/IP —> REXEC。有关访问“iSeries 信息中心”的信息，请参阅第 xii 页的『先决条件和相关信息』。
- 选择运行 REXEC 服务器时，您将在系统上具有的任何菜单访问控制以外运行。必须确保对象权限模式足够保护资源。

使用 RouteD 的安全性注意事项

路由守护程序（RouteD）服务器提供对 iSeries 服务器上的“路由信息协议”（RIP）的支持。RIP 是使用最广泛的路由协议。它是帮助自治系统内的 IP 信息包路由中的 TCP/IP 的“内部网关协议”。

通过允许可信网络内的系统互相用当前路由信息更新，RouteD 用于增加网络流量的效率。当运行 RouteD 时，系统可以接收来自其它参与系统的有关应如何路由选择传输（信息包）的更新。因此，如果 RouteD 服务器对于黑客是可访问的，黑客可以使用它重新路由您的信息包，使其通过可以窃听或修改那些信息包的系统。以下是 RouteD 安全性的建议:

- iSeries 服务器使用 RIPv1，它未提供认证路由器的任何方法。它用于可信网络内。如果系统是在您不“信任”的其它系统的网络内，则您不应该运行 RouteD 服务器。要确保 RouteD 服务器不自动启动，输入下列命令:

  ```
  CHGRTDA AUTOSTART(*NO)
  ```

  注:

  1. AUTOSTART(*NO) 是缺省值。
  2. 第 108 页的『控制要自动启动哪些 TCP/IP 服务器』提供有关控制哪些 TCP/IP 服务器自动启动的更多信息。
- 确保控制谁可以更改 RouteD 配置，它需要 *IOSYSCFG 特权。
- 如果系统参与了多个网络（例如，内部网和因特网），可以将 RouteD 服务器配置为仅使用安全网络发送和接收更新。

使用 DNS 服务器的安全性注意事项

“域名系统”（DNS）服务器提供主机名到 IP 地址的转换，反之亦然。在 iSeries 服务器上，DNS 服务器用于为内部的安全网络（内部网）提供地址转换。

防止 DNS 访问

如果不想让任何人使用系统上的 DNS 服务器，执行下列操作:

1. 要防止当启动 TCP/IP 时 DNS 服务器作业自动启动，输入以下命令:

   ```
   CHGDNSA AUTOSTART(*NO)
   ```

   注:

   a. AUTOSTART(*NO) 是缺省值。

   b. 第 108 页的『控制要自动启动哪些 TCP/IP 服务器』提供有关控制哪些 TCP/IP 服务器自动启动的更多信息。
2. 要防止他人将用户应用程序（例如套接字应用程序）与系统通常用于 DNS 的端口相关联，执行下列操作:

   a. 输入 GO CFGTCP 以显示“配置 TCP/IP”菜单。

   b. 选择选项 4（使用 TCP/IP 端口限制）。

   c. 在“使用 TCP/IP 端口限制”屏幕上，指定选项 1（添加）。

   d. 对于端口范围下限，指定 53。

   e. 对于端口范围上限，指定 *ONLY。

注:

1) 端口限制在下次启动 TCP/IP 时生效。如果设置端口限制时 TCP/IP 是活动的，应结束 TCP/IP 并重新启动它。
2) RFC1700 提供有关公共端口号指定的信息。

f. 对于协议，指定 *TCP。

g. 对于用户概要文件字段，指定系统上受保护的用户概要文件名称。（受保护的用户概要文件是不拥有沿用权限的程序且不具有其它用户知道的密码的用户概要文件。）通过将端口限制于特定的用户，自动排除所有其它用户。

h. 对 *UDP（用户数据报）协议重复步骤 2c 到 2g。

保护 DNS 服务器

以下是当您选择在 iSeries 系统上运行 DNS 时的安全注意事项:

- DNS 服务器提供的功能是 IP 地址转换和名称转换。它不提供对 iSeries 系统上对象的任何访问。当外来者访问 DNS 服务器时您的风险是服务器提供容易的方法来查看网络的拓扑结构。DNS 可能使黑客不要费多少力气就能确定潜在目标的地址。然而，DNS 不提供将有助于中断这些目标系统的信息。
- 一般情况下，对内部网使用 iSeries DNS 服务器。因此，您可能不需要限制查询 DNS 的能力。然而，例如，您可以在内部网内具有几个子网。您可能不希望来自不同子网的用户能够查询 iSeries 服务器中的 DNS。DNS 的安全性选项使您可以限制对主域的访问。使用 “iSeries 导航器” 来指定 DNS 服务器应响应的 IP 地址。

  另一个安全选项使您可以指定哪些辅助服务器可以从主 DNS 服务器复制信息。当使用此选项时，服务器将仅从显式列示的辅助服务器接受区域传输请求（复制信息的请求）。
- 一定要小心限制更改 DNS 服务器的配置文件的能力。例如，不怀好意的人能够将 DNS 文件更改为指向网络外部的 IP 地址。他们能够模拟网络中的服务器，并且可能从访问服务器的用户获取对机密信息的访问权。

使用 HTTP Server for iSeries 的安全性注意事项

HTTP Server 为 “万维网” 浏览器客户机提供对 iSeries 服务器多媒体对象（如 HTML（超文本标记语言）文档）的访问权。它也支持*公共网关接口（CGI）*规范。应用程序员可以编写 CGI 程序来扩展服务器的功能。

管理员可以使用因特网连接服务器或 IBM HTTP Server for iSeries 以在同一 iSeries 服务器上同时运行多个服务器。每个运行中的服务器都称为**服务器实例**。每个服务器实例都具有唯一的名称。管理员控制启动哪些实例和每个实例可以执行哪些操作。

注: 当使用 Web 浏览器配置或管理下列任何项时，您必须使 HTTP Server 的 *ADMIN 实例运行:

- iSeries 的防火墙
- 因特网连接服务器
- 因特网连接安全服务器
- IBM HTTP Server for iSeries

用户（Web 站点访问者）永远不会看到 iSeries 服务器“注册”屏幕。然而，iSeries 服务器管理员必须通过在 HTTP 伪指令中定义所有 HTML 文档和 CGI 程序，明确地对它们授权。另外，管理员可以对某些或所有请求设置资源安全性和用户认证（用户标识和密码）。

黑客的攻击可以导致 Web 服务器拒绝服务。通过评测一些客户机请求的超时，服务器可以检测拒绝服务攻击。如果服务器未接收来自客户机的请求，那么服务器确定拒绝服务攻击正在进行。它是通过初始客户机连接至服务器而进行的。服务器在缺省情况下，可以执行攻击检测和处罚。

防止 HTTP 访问

如果不想让任何人使用程序来访问系统，应防止 HTTP Server 运行。执行下列操作:

__ 步骤 1. 要防止当启动 TCP/IP 时 HTTP Server 作业自动启动，输入以下命令:

```
CHGHTTPA AUTOSTART(*NO)
```

注:

a. AUTOSTART(*NO) 是缺省值。

b. 第 108 页的『控制要自动启动哪些 TCP/IP 服务器』提供有关控制哪些 TCP/IP 服务器自动启动的更多信息。

__ 步骤 2. 缺省情况下，HTTP Server 作业使用 QTMHHTTP 用户概要文件。要防止 HTTP Server 启动，将 QTMHHTTP 用户概要文件的状态设置为 *DISABLED。

控制对 HTTP Server 的访问权

运行 HTTP Server 的主要目的是为访问者提供对 iSeries 系统上的 Web 站点的访问权。您可以将访问 Web 站点的人当成查看行业杂志中广告的人。访问者不了解在 Web 站点上运行的硬件和软件，如您使用的服务器类型以及服务器的存放位置。通常，您不想在潜在访问者和 Web 站点之间放置任何屏障（如“注册”屏幕）。然而，可能要限制对 Web 站点提供的一些文档或 CGI 程序的访问权。

可能也需要单个 iSeries 系统来提供多个逻辑 Web 站点。例如，iSeries 系统可以支持具有不同客户集的各类分公司。对于这些公司的每一个分支，您需要提供唯一的 Web 站点，该站点完全与访问者无关。另外，可能要提供具有关于商务机密信息的内部 Web 站点（内部网）。

作为安全管理员，需要保护 Web 站点的内容。同时，需要确保安全性操作未对 Web 站点的值产生消极影响。另外，需要确保 HTTP 活动未危害系统或网络的完整性。下列主题提供使用程序时的安全性建议。

管理注意事项

以下是管理因特网服务器的一些安全性注意事项。

- 通过使用 Web 浏览器和 *ADMIN 实例，执行设置和配置功能。对于某些功能，如在服务器上创建附加实例，*必须*使用 *ADMIN 服务器。
- 管理主页的缺省 URL（ *ADMIN 服务器的主页）发布在提供浏览器管理功能的产品的文档中。因此，缺省 URL 可能会被黑客知晓并发布在黑客户论坛中，就像 IBM 提供的用户概要文件缺省密码被知晓和发布一样。可以通过几种方法保护自己免于这种漏洞的攻击:

- 仅当需要执行管理功能时，才运行 HTTP Server 的 *ADMIN 实例。不要一直运行 *ADMIN 实例。
- 为 *ADMIN 实例激活 SSL 支持（通过使用“数字证书管理器”）。*ADMIN 实例使用 HTTP 保护伪指令来要求输入用户标识和密码。当使用 SSL 时，用户标识和密码已加密（连同有关管理表单上出现的其它配置信息）。
- 使用防火墙可防止从因特网访问 *ADMIN 服务器并同时隐藏系统名和域名（它们是 URL 的一部分）。

• 当执行管理功能时，必须用具有 *IOSYSCFG 特权的用户概要文件注册。可能也需要对系统上特定对象的权限，如下所示:
  - 包含 HTML 文档和 CGI 程序的库或目录。
  - 您计划要交换到服务器伪指令内的任何用户概要文件。
  - 伪指令使用的任何目录的“访问控制表”（ACL）。
  - 用于创建及维护用户标识和密码的验证列表对象。

  使用 *ADMIN 服务器和 TELNET，您能够远程执行管理功能（可能要通过因特网连接）。注意: 如果通过公共链接（因特网）执行管理，您可能会将有效的用户标识和密码暴露给窃听者。然后，“窃听者”可以使用此用户标识和密码，尝试通过诸如 TELNET 或 FTP 的方式来访问系统。

  注:

  1. 使用 TELNET，会象任何其它屏幕一样处理“注册”屏幕。尽管当输入密码时不显示密码，系统传送密码时没有任何加密或编码。
  2. 使用 *ADMIN 服务器，密码已编码而没有加密。编码方案是一种业界标准，因而在黑客团体中广为人知。尽管普通的“窃听者”很难了解编码，但老练的窃听者可能具有工具来尝试解开密码。

  安全性技巧

  如果计划通过因特网执行远程管理，应使用具有 SSL 的 *ADMIN 实例，以便对传输加密。不要使用不可靠的应用程序，如 TELNET 的 V4R4 以前的版本（TELNET 从 V4R4 开始支持 SSL）。如果要在*可信*用户的内部网中使用 *ADMIN 服务器，您也许能够安全地使用它进行管理。

• HTTP 伪指令为服务器上所有活动提供基础。交付使用的配置可用于处理缺省“欢迎”页面。在服务器管理员定义服务器的伪指令之后，客户机才能查看除“欢迎”页面以外的任何文档。要定义伪指令，请使用 Web 浏览器和 *ADMIN 服务器，或“使用 HTTP 配置（WRKHTTPCFG）”命令。两种方法都需要 *IOSYSCFG 特权。当将 iSeries 服务器连接到因特网时，则评估和控制组织中具有 *IOSYSCFG 特权的用户数目更加重要。

保护资源

IBM HTTP Server for iSeries 包含一些 HTTP 伪指令，它们可以对服务器使用的信息资产提供详细控制。可以使用伪指令来控制 Web 服务器从哪些目录对 HTML 文件和 CGI 程序的 URL 提供服务，来交换到其它用户概要文件，以及来要求对某些资源进行认证。

注: “信息中心”中“Web 服务”下的文档提供可用 HTTP 伪指令和如何使用它们的完整描述。以下是使用此支持的某些建议和注意事项:

- HTTP Server 基于“显式权限”启动。该服务器不接受请求，除非该请求是在伪指令中显式定义。即，服务器立即拒绝对 URL 的任何请求，除非 URL 已在伪指令中定义（以名称或类属方式）。
- 接受对某些或所有资源的请求之前，可以使用保护伪指令来要求输入用户标识和密码。
  - 当用户（客户机）请求受保护的资源时，服务器要求在浏览器中输入用户标识和密码。浏览器提示用户输入用户标识和密码，然后将该信息发送到服务器。一些浏览器存储用户标识和密码并与后继的请求一起自动发送。这避免用户对每个请求重复地输入相同的用户标识和密码。

    因为某些浏览器存储用户标识和密码，因此您需要承担与用户通过 iSeries 服务器“注册”屏幕或通过路由器进入系统时所要承担的相同用户教育任务。无人照管浏览器会话会引起潜在的安全性漏洞。
  - 对于系统如何处理用户标识和密码有三个选项（在保护伪指令中指定）:
    1. 可以使用正常的 iSeries 服务器用户概要文件和密码验证。这大多常用于保护内部网（安全网络）中的资源。
    2. 可以创建“因特网用户”: 可在 iSeries 服务器上验证但不具有用户概要文件的用户。通过称为“验证列表”的 iSeries 服务器对象实现因特网用户。验证列表对象包含经特别定义以用于特殊应用程序的用户和密码列表。

       决定如何提供因特网用户标识和密码（如通过应用程序，或通过响应电子邮件请求的管理员）以及如何管理因特网用户。使用 HTTP Server 的基于浏览器的界面来进行设置。

       对于非安全网络（因特网），使用因特网用户可比使用一般用户概要文件和密码提供更为全面的保护。用户标识和密码的唯一集合创建有关这些用户可执行任务的内置限制。用户标识和密码不可用于正常注册（例如使用 TELNET 或 FTP）。另外，您未暴露正常的用户标识和密码给窃听者。
    3. 轻量级目录访问协议（LDAP）是一种目录服务协议，它基于“传输控制协议”（TCP）提供对目录的访问。它允许您存储目录服务中的信息并进行查询。现在，LDAP 作为用户认证的一个选项受到支持。

    注:

    1. 当浏览器发送用户标识和密码时（无论是对用户概要文件还是对因特网用户），它们被编码而不加密。编码方案是一种业界标准，因而在黑客团体中广为人知。尽管普通的“窃听者”很难了解编码，但老练的窃听者可能具有工具来尝试解开密码。
    2. iSeries 服务器将验证对象存储在受保护的系统区域。可以仅用定义的系统界面（API）和相应的认证对其进行访问。
  - 可以使用“数字证书管理器”（DCM）来创建自己的内部网“认证中心”。“数字证书”自动将证书与自己的用户概要文件关联。证书具有与关联的概要文件相同的权限和许可权。
- 当服务器接收请求时，常规 iSeries 服务器资源安全性会接管。请求资源的用户概要文件必须具有对资源（如包含 HTML 文档的文件夹或源物理文件）的权限。缺省情况下，作业在 QTMHHTTP 用户概要文件下运行。可以使用伪指令来交换到不同用户概要文件。然后，系统使用该用户概要文件的权限来访问对象。以下是此支持的某些注意事项:

- 当服务器提供多个逻辑 Web 站点时，交换用户概要文件特别有用。可以将不同的用户概要文件与每个 Web 站点的伪指令关联，因此使用常规 iSeries 服务器资源安全性来保护每个站点的文档。
- 可以使用该功能来结合验证对象交换用户概要文件。服务器使用唯一的用户标识和密码（区别于常规用户标识和密码）来评估初始请求。服务器认证用户之后，系统交换到不同用户概要文件并因此利用资源安全性。因此用户不了解真实的用户概要文件名并不能试图以另一个方法使用它（如 FTP）。

• 某些 HTTP Server 请求需要在 HTTP Server 上运行程序。例如，程序可以访问系统上的数据。服务器管理员必须将请求（URL）映射到符合 CGI 用户界面标准的特定用户定义的程序，程序才可以运行。以下是 CGI 程序的某些注意事项:
  - 可以象处理 HIML 文档一样，对 CGI 程序使用保护伪指令。因此，运行程序之前，可以要求输入用户标识和密码。
  - 缺省情况下，CGI 程序在 QTMHHTP1 用户概要文件下运行。运行该程序之前，可以交换到不同用户概要文件。因此，可以对 CGI 程序访问的资源设置常规 iSeries 服务器资源安全性。
  - 作为安全管理员，授权任何 CGI 程序在系统上使用之前，应执行安全性复查。应知道程序来自何处和 CGI 程序执行什么功能。您也应监控在其下运行 CGI 程序的用户概要文件的能力。也应使用 CGI 程序执行测试来确定，例如是否能获取对命令行的访问权。以与对待沿用权限的程序相同的警戒来对待 CGI 程序。
  - 另外，确保评估哪些敏感对象可能具有不相称的公共权限。在少数情况下，设计不好的 CGI 程序可能允许内行老练的用户试图漫游整个系统。
  - 使用特定用户库（如 CGILIB）来保留所有 CGI 程序。使用对象权限来控制谁可以将新对象放置到此库中，以及谁可以在此库中运行程序。使用伪指令来将 HTTP Server 限制于运行此库中的 CGI 程序。

    注: 如果服务器提供多个逻辑 Web 站点，可能要对每个站点的 CGI 程序都设置一个单独的库。

其它安全性注意事项

以下是附加安全性注意事项:

- HTTP 提供对 iSeries 系统的只读访问权。HTTP Server 请求不能直接更新或删除系统上的数据。然而，您可能具有更新数据的 CGI 程序。另外，可以启用 Net.Data® CGI 程序来访问 iSeries 服务器数据库。系统使用脚本（类似于出口程序）来评估对 Net.Data 程序的请求。因此，系统管理员可以控制 Net.Data 程序可以执行哪些操作。
- HTTP Server 提供访问日志，您可以用来监控访问和通过服务器试图进行的访问。

将 IBM HTTP Server for iSeries 与 SSL 一起使用的安全性注意事项

IBM HTTP Server for iSeries 可以提供与 iSeries 服务器的安全 Web 连接。**安全 Web 站点**意味加密客户机和服务器之间（两个方向）的传输。这些加密的传输可以防止窃听者和试图捕获或变更传输的人的推敲。

注: 记住，安全 Web 站点绝对适用于客户机和服务器之间传送的信息的安全性。它的本意并不是减少服务器对于黑客的脆弱性。然而，它确实限制了黑客通过窃听可以容易获取的信息。

信息中心中有关 SSL 和 Web 服务（HTTP）的主题提供了关于安装、配置和管理加密过程的完整信息。这些主题既提供了服务器功能部件的概述，也提供了使用服务器的一些注意事项。

当安装了下列其中一项许可程序时，因特网连接服务器提供 HTTP 和 HTTPS 支持:

- 5722–NC1
- 5722–NCE

当安装了这些选项时，产品称为“因特网连接安全服务器”。

IBM HTTP Server for iSeries（5722–DG1）提供 http 和 https 支持。必须安装下列其中一项加密产品才能启用 SSL:

- 5722–AC2
- 5722–AC3

取决于加密的安全性有几个要求:

- 发送方和接收方（服务器和客户机）必须“了解”加密机制并能够执行加密和解密。HTTP Server 需要启用了 SSL 的客户机。（大多数流行的 Web 浏览器都启用了 SSL。）iSeries 加密许可程序支持几个业界标准加密方法。当客户机试图建立安全会话时，服务器和客户机进行协商以找到双方都支持的最安全的加密方法。
- 传输必须使偷听者无法解密。因此，加密方法要求双方具有只有他们知道的加密／解密**专用密钥**。如果要具有安全的*外部* Web 站点，应使用独立的认证中心（CA）来创建数字证书并颁发给用户和服务器。认证中心被认为是可信方。

加密可以保护传送信息的机密性。然而，对于敏感信息，如金融信息，除机密性以外您还需要完整性和可靠性。即，客户机和（可选）服务器必须信任另一端的对方（通过独立的引用）且他们必须确信传输尚未变更。由认证中心（CA）提供的数字签名提供这些可靠性和完整性保证。SSL 协议通过验证服务器证书（和可选客户机证书）的数字签名来提供认证。

加密和解密需要处理时间且将影响传输性能。因此，iSeries 服务器提供同时运行安全和不安全的服务程序的能力。可以使用不安全的 HTTP Server 来处理不需要安全性的文档，如产品目录。这些文档将具有以 `http://` 开始的 URL。可以对敏感信息（如客户输入信用卡信息的表单）使用安全的 HTTP Server。该程序可以处理其 URL 以 `http://` 或以 `https://` 开始的文档。

提醒信息

当传输安全和不安全时，特别是当 Web 站点仅对某些文档使用安全服务器时，这是通知客户机的很好的因特网礼节。

记住，加密既需要安全客户机也需要安全服务器。安全浏览器（HTTP 客户机）已变得相当普通。

LDAP 的安全性注意事项

“轻量级目录访问协议”（LDAP）安全性功能部件包括“安全套接字层”（SSL）、“访问控制表”和 CRAM-MD5 密码加密。在 V5R1 中，添加了 Kerberos 连接和“安全性”审计支持来增强 LDAP 安全性。

有关这些主题的更多信息，参阅 iSeries 信息中心 —> 联网 –> TCP/IP –> 目录服务（LDAP）。有关访问 “iSeries 信息中心”的信息，请参阅第 xii 页的『先决条件和相关信息』。

LPD 的安全性注意事项

LPD（行式打印机守护程序）提供分发 系统的打印机输出的能力。系统不执行 LPD 的任何注册处理。

防止 LPD 访问

如果不想让任何人使用 LPD 来访问您的系统，应防止 LPD 服务器运行。执行下列操作:

__ 步骤 1. 要防止当启动 TCP/IP 时 LPD 服务器作业自动启动，输入以下命令:

```
CHGLPDA AUTOSTART(*NO)
```

注:

a. AUTOSTART(*YES) 是缺省值。

b. 第 108 页的『控制要自动启动哪些 TCP/IP 服务器』提供有关控制哪些 TCP/IP 服务器自动启动的更多信息。

__ 步骤 2. 要防止他人将用户应用程序（例如套接字应用程序）与系统通常用于 LPD 的端口相关联，执行下列操作:

__ 步骤 a. 输入 GO CFGTCP 以显示“配置 TCP/IP”菜单。

__ 步骤 b. 选择选项 4（使用 TCP/IP 端口限制）。

__ 步骤 c. 在“使用 TCP/IP 端口限制”屏幕上，指定选项 1（添加）。

__ 步骤 d. 对于端口范围下限，指定 515。

__ 步骤 e. 对于端口范围上限，指定 *ONLY。

注:

1) 端口限制在下次启动 TCP/IP 时生效。如果设置端口限制时 TCP/IP 是活动的，应结束 TCP/IP 并重新启动它。

2) RFC1700 提供有关公共端口号指定的信息。

__ 步骤 f. 对于协议，指定 *TCP。

__ 步骤 g. 对于用户概要文件字段，指定系统上受保护的用户概要文件名称。（受保护的用户概要文件是不拥有沿用权限的程序且不具有其它用户知道的密码的用户概要文件。）通过将端口限制于特定的用户，自动排除所有其它用户。

__ 步骤 h. 对 *UDP 协议重复步骤 2c 到 2g。

控制 LPD 访问

如果要允许 LPD 客户机访问您的系统，应了解下列安全性问题:

- 要防止用户用不需要的对象淹没系统，确保已对辅助存储池（ASP）设置了适当的阈值限制。通过使用系统服务工具（SST）或专用服务工具（DST），可以显示并设置 ASP 的阈值。*Backup and Recovery* 一书提供有关 ASP 阈值的更多信息。
- 可以使用对输出队列的权限来限制哪些用户可以将假脱机文件发送到系统。没有用户标识的 LPD 用户使用 QTMPLPD 用户概要文件。可以授予此用户概要文件只对少数输出队列的访问权。

SNMP 的安全性注意事项

iSeries 服务器可以用作网络中的简单网络管理协议（SNMP）代理程序。 SNMP 提供在网络环境中管理网关、路由器和主机的方法。SNMP 代理程序收集有关系统的信息并执行远程 SNMP 网络管理器所请求的功能。

防止 SNMP 访问

如果不想让任何人使用 SNMP 来访问您的系统，应防止 SNMP 服务器运行。执行下列操作:

__ 步骤 1. 要防止当启动 TCP/IP 时 DNS 服务器作业自动启动，输入下列命令:

```
CHGSNMPA AUTOSTART(*NO)
```

注:

a. AUTOSTART(*YES) 是缺省值。

b. 第 108 页的『控制要自动启动哪些 TCP/IP 服务器』提供有关控制哪些 TCP/IP 服务器自动启动的更多信息。

__ 步骤 2. 要防止他人将用户应用程序（例如套接字应用程序）与系统通常用于 SNMP 的端口相关联，执行下列操作:

__ 步骤 a. 输入 GO CFGTCP 以显示“配置 TCP/IP”菜单。

__ 步骤 b. 选择选项 4（使用 TCP/IP 端口限制）。

__ 步骤 c. 在“使用 TCP/IP 端口限制”屏幕上，指定选项 1（添加）。

__ 步骤 d. 对于端口范围下限，指定 161。

__ 步骤 e. 对于端口范围上限，指定 *ONLY。

注:

1) 端口限制在下次启动 TCP/IP 时生效。如果设置端口限制时 TCP/IP 是活动的，应结束 TCP/IP 并重新启动它。

2) RFC1700 提供有关公共端口号指定的信息。

__ 步骤 f. 对于协议，指定 *TCP。

__ 步骤 g. 对于用户概要文件字段，指定系统上受保护的用户概要文件名称。（受保护的用户概要文件是不拥有沿用权限的程序且不具有其它用户知道的密码的用户概要文件。）通过将端口限制于特定的用户，自动排除所有其它用户。

__ 步骤 h. 对 *UDP 协议重复步骤 2c 到 2g。

控制 SNMP 访问

如果要允许 SNMP 管理器访问您的系统，应了解下列安全性问题:

- 可以使用 SNMP 访问网络的人可以收集有关网络的信息。通过使用别名和域名服务器隐藏的信息通过 SNMP 变得可用于冒充闯入者。另外，闯入者可以使用 SNMP 变更网络配置并破坏通信。
- SNMP 依靠共用名进行访问。在概念上，共用名类似于密码。共用名是未加密的。因此，它容易被窃听。使用“为 SNMP 添加共用”（ADDCOMSNMP） 命令来将管理器因特网地址（INTNETADR）参数设置为一个或多个特定 IP 地址代替 *ANY。也可以将 ADDCOMSNMP 或 CHGCOMSNMP 命令的 OBJACC 参数设置为 *NONE，以防止团体内的管理器访问任何 MIB 对象。只是临时这样做，以拒绝对共用中的管理器的访问，而不必除去共用。

INETD 服务器的安全性注意事项

与大多数 TCP/IP 服务器不同，INETD 服务器不提供对客户机的单一服务。而是提供管理员可以定制的各种杂项服务。由于该原因，INETD 服务器有时称为“超级服务器”。INETD 服务器具有下列内置服务:

- 时间
- 日间
- 回送
- 废弃
- 已更改

TCP 和 UDP 都支持这些服务。对于 UDP，回送、时间、日间和已更改的服务接收 UDP 信息包，然后将信息包发送回始发者。回送服务器回送它接收到的信息包，时间和日间服务器生成以特定格式表示的时间并将它发送回去，已更改服务器生成可打印 ASCII 字符的信息包并将它发送回去。

这些 UDP 服务的特性使系统易受拒绝服务攻击。例如，假定具有两个 iSeries 服务器: SYSTEMA 和 SYSTEMB。有恶意的程序员可以使用 SYSTEMA 的源地址和时间服务器的 UDP 端口号来伪造 IP 头和 UDP 头。然后他可以将该信息包发送至 SYSTEMB 上的时间服务器，SYSTEMB 将时间发送至 SYSTEMA，SYSTEMA 将对 SYSTEMB 作出响应等等，以致生成连续循环并消耗两个系统上的 CPU 资源以及网络带宽。

因此，您应该考虑在您的 iSeries 系统上这种攻击的风险，并且仅在安全网络中运行这些服务。交付 INETD 服务器时是当您启动 TCP/IP 时不自动启动它。您可以配置在启动 INETD 时是否启动服务。缺省情况下,当启动 INETD 服务器时启动 TCP 和 UDP 时间服务器。

对于 INETD 服务器有两个配置文件:

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

这些文件确定当 INETD 服务器启动时哪些程序启动。它们也确定当 INETD 启动这些程序时，这些程序在什么用户概要文件下运行。

注: 从不应该修改 proddata 中的配置文件。每次重新装入系统时替换该文件。只应该将客户配置更改放在 userdata 目录树中的此文件中，因为在发行版升级期间**不**更新此文件。

如果有恶意的程序员获取对这些文件的访问权，他可以配置它们来在 INETD 启动时启动任何程序。因此，保护这些文件是很重要的。缺省情况下，它们需要 QSECOFR 权限才能进行更改。您不应该减少访问它们所需要的权限。

注: 不要修改 ProdData 目录中的配置文件。每次重新装入系统时，都替换该文件。只应该将客户配置更改放在 UserData 目录树中的文件中，因为在发行版升级期间不更新该文件。

限制 TCP/IP 漫游的安全性注意事项

如果系统连接到网络，可能要限制用户利用 TCP/IP 应用程序漫游网络的能力。执行它的一个方法是限制对下列客户机 TCP/IP 命令的访问权:

注: 这些命令可能在系统上的几个库中存在。它们至少都在 QSYS 库和 QTCP 库中。确保定位和保护所有出现。

- STRTCPFTP
- FTP
- STRTCPTELN
- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD（REXEC 客户机）

由下列各项确定用户可能的目的地:

- TCP/IP 主机表中的项。
- TCP/IP 路由表中的 *DFTROUTE 项。当用户的目的地是未知网络时，这允许他们输入下一个中继段系统的 IP 地址。通过使用缺省路由，用户可以到达或与远程网络联系。
- 远程名称服务器配置。此支持允许网络中的其它服务器为用户定位主机名。
- 远程系统表。

需要控制哪些用户可以将项添加到这些表和更改配置。也需要了解表项和配置的意义。

应知道具有对 ILE C 编译器的访问权的内行用户可以创建可以连接到 TCP 或 UDP 端口的套接字程序。通过限制对 QSYSINC 库中的下列套接字接口文件的访问权，可以使创建更困难。

- SYS
- NETINET
- H
- ARPA
- 套接字和 SSL

对于服务程序，可以限制套接字和 SSL 应用程序的使用，它们已通过限制这些服务程序的使用而被编译:

- QSOSRV1
- QSOSRV2
- QSOSKIT（SSL）
- QSOSSLSR（SSL）

服务程序在交付时具有公共权限 *USE，但可以将该权限更改为 *EXCLUDE（或需要的其它值）。

第 14 章 保护工作站访问

许多系统用户把他们办公桌上的个人计算机（PC）作为他们的工作站。他们使用在 PC 上运行的工具，并且使用 PC 连接至 iSeries 服务器。

将 PC 连接至 iSeries 服务器的大多数方法比工作站仿真提供更多功能。该 PC 对 iSeries 可能看起来象一个显示器并为用户提供交互式注册会话。此外，该 PC 对 iSeries 服务器可能看起来象另一个计算机并提供诸如文件传送和远程过程调用之类的功能。

作为 iSeries 服务器安全管理员，您需要了解以下内容:

- 对连接至您的系统的 PC 用户可用的功能
- PC 用户可以访问的 iSeries 服务器资源。

如果尚未对高级 PC 功能（如文件传送和远程过程调用）准备您的 iSeries 服务器安全性方案，可能需要阻止那些功能。很可能您的长远目标是允许高级 PC 功能，尽管您仍要保护您的系统上的信息。以下主题讨论与 PC 访问关联的某些安全性问题。

预防工作站病毒

本资料建议安全管理员可以防止 PC 病毒的方法。

保护工作站数据访问

某些 PC 客户机软件使用共享文件夹来存储服务器上的信息。要访问 iSeries 数据库文件，PC 用户应具有限制的明确定义的一组接口。使用文件传送功能（大多数客户机／服务器软件具有这个功能），PC 用户可以在服务器和 PC 之间复制文件。使用数据库访问功能（如 DDM 文件、远程 SQL 或 ODBC 驱动程序），PC 用户可以访问服务器上的数据。

在此环境中，您可以创建程序来拦截并评估要访问服务器资源的 PC 用户请求。当请求使用 DDM 文件时，您可以在分布式数据管理访问（DDMACC）网络属性中指定出口程序。 对于 PC 文件传送的某些方法，您可以在客户机请求访问（PCSACC）网络属性中指定出口程序。或者， 您可以指定 PCSACC (*REGFAC) 来使用注册功能。当请求使用其它服务器功能来存取数据时，您可以使用 WRKREGINF 命令来为那些服务器功能注册出口程序。

然而，出口程序可能难以设计，它们很少是极简单的。出口程序不是对象权限的替代口，对象权限设计成保护您的对象以防止来自任何源的未授权访问。

某些客户机软件（如 IBM iSeries Access for Windows）使用集成文件系统来存储和访问 iSeries 服务器上的数据。 使用集成文件系统，整个服务器更便于 PC 用户使用。对象权限变得更加必要。通过集成文件系统，具有足够权限的用户可以查看服务器库，好象它是一个 PC 目录一样。简单的移动和复制命令可以立即将数据从 iSeries 服务器库移动到 PC 目录，反之亦然。系统自动对数据的格式进行适当的更改。

注:

1. 可以使用权限列表来控制 QSYS.LIB 文件系统中的对象的使用。有关更多信息，请参阅第 88 页的『限制对 QSYS.LIB 文件系统的访问』。
2. 第 83 页的第 11 章，『使用“集成文件系统”来保护文件』提供关于使用集成文件系统的安全性问题的更多信息。

对于用户和开发者，集成文件系统的优点是它的简单性。使用一个接口，用户就可以使用多个环境中的对象。PC 用户不需要特殊软件或 API 来访问对象。相反，PC 用户可以使用熟悉的 PC 命令或“指向并单击”来直接使用对象。

对于连接了 PC 的所有系统，但特别对于具有使用集成文件系统的客户机软件的系统，良好的对象权限方案很关键。因为安全性已集成到 OS/400 产品中，所以存取数据的任何请求都必须通过权限检查进程。权限检查适用于来自任何源的请求和使用任何方法的数据访问。

使用工作站访问的对象权限

当设置对象的权限时，您需要评估该权限为 PC 用户提供什么操作。例如，当用户对某个文件具有 *USE 权限时，该用户可以查看或打印该文件中的数据。该用户不能更改该文件中的信息或删除该文件。对于 PC 用户，查看等效于“阅读”，它为用户提供了足够的权限来在 PC 上复制文件。这可能不是您希望的。

对于某些关键文件，您可能需要将公共权限设置为 *EXCLUDE 来防止下载。然后，您可以提供另一种方法来“查看”服务器上的文件，如使用菜单和沿用权限的程序。

防止下载的另一个选项是使用出口程序，每当 PC 用户启动服务器功能（而不是交互式注册）时该程序运行。您可以通过使用“更改网络属性”（CHGNETA）命令来在 PCSACC 网络属性中指定出口程序。或者，您可以通过使用“使用注册信息”（WRKREGINF）命令注册出口程序。您使用的方法取决于 PC 在您的系统上如何存取数据和该 PC 使用哪个客户机程序。出口程序（QIBM_QPWFS_FILE_SERV）适用于 iSeries Access 和 Net Server 对 IFS 访问。它不阻止 PC 使用其它机制（如 FTP 或 ODBC）进行访问。

PC 软件一般也提供上载功能，因此用户可以将数据从 PC 复制到服务器数据库文件。如果未正确设置您的权限方案，PC 用户可能会使用来自 PC 的数据覆盖某个文件中的所有数据。您需要小心地指定 *CHANGE 权限。复查 *iSeries Security Reference* 一书中的 Appendix D 来了解文件操作所需要的权限。

“iSeries 信息中心”提供关于 PC 功能的权限和关于使用出口程序的更多信息。有关详细信息，请参阅第 xii 页的『先决条件和相关信息』。

应用程序管理

“应用程序管理”是“iSeries 导航器”（iSeries 服务器的图形用户界面（GUI））的一个可选择安装的组件。“应用程序管理”使系统管理员能够控制特定服务器上的用户和组可用的功能或应用程序。这包括控制通过客户机访问他们的服务器的用户可用的功能。注意：如果您从 Windows 客户机访问服务器，则 iSeries 服务器用户而不是 Windows 用户确定哪些功能可用于管理。

有关“iSeries 导航器应用程序管理”的完整文档，请参阅 iSeries 信息中心 –> 连接到 iSeries —> 连接对象 —> iSeries 导航器（../html/as400/v5r2/ic2924/info/rzaj3/rzaj3overview.htm）。

策略管理

策略是管理员配置他们的客户机 PC 上的软件时使用的工具。策略可以限制用户在 PC 上对哪些功能和应用程序具有访问权。策略也可以建议或要求某些用户或某些 PC 使用的配置。

注: 策略不提供对服务器资源的控制。策略不是服务器安全性的替代品。特定用户可以使用策略来影响 iSeries Access 如何能够从特定 PC 访问服务器。然而，它们并不更改可以如何通过其它机制访问服务器资源。

策略存储在文件服务器中。每次在用户注册到他们的 Windows 工作站时，从该文件服务器下载适用于该 Windows 用户的策略。用户在工作站上执行任何操作前，将策略应用于注册表。

Microsoft® 策略与应用程序管理

iSeries Access Express 支持在网络中实现管理控制的两种不同的策略: Microsoft 系统策略和 “ iSeries 导航器应用程序管理”。当决定哪个策略最适合于您的需要时，考虑以下情况。

Microsoft 系统策略

策略是 PC 驱动的，不取决于特定的 OS/400 发行版。策略可以应用于 PC 以及 Windows 用户。这表示用户引用 Windows 用户概要文件，而不是服务器用户概要文件。策略可以用来“配置”，也可以用来限制。策略通常比“应用程序管理”提供更多粒度并可以提供更广的功能。这是因为不需要与服务器连接就能确定用户是否可以使用功能。实现策略比实现“应用程序管理”更复杂，因为需要使用 Microsoft 系统策略编辑器且必须单独配置 PC 来下载策略。

“iSeries 导航器”应用程序管理

“应用程序管理”使数据与用户概要文件关联，而不是与 Microsoft 系统策略与之关联的 Windows 概要文件关联。尽管需要运行 OS/400 产品的 V4R3 或更高版本的 iSeries 服务器才能使用“应用程序管理”，但某些功能仅在 V4R4 或更高版本上可用。“应用程序管理”使用“iSeries 导航器”的图形用户界面来管理，这比策略编辑器更易于使用。“应用程序管理”信息适用于用户，而不管他从哪个 PC 注册。可以限制“iSeries 导航器”中的特定功能。如果要限制的所有功能都启用了“应用程序管理”，并且如果正在使用的 OS/400 的版本支持“应用程序管理”，则“应用程序管理”更合适。

将 SSL 与 iSeries Access for Windows 一起使用

有关使用 iSeries Access Express 与 SSL 的信息，请复查 Java 主题下的“iSeries 信息中心”主题 *Secure Sockets Layer Administration, Securing iSeries Access Express and iSeries Navigator, iSeries Developer Kit for Java , and iSeries Java Toolbox*。也可以在随系统提供给您的 CD 上复查此信息。

“iSeries 导航器”安全性

“iSeries 导航器”为拥有 iSeries Access 的用户提供了易于使用的与服务器的接口。对于 OS/400 产品的每个新发行版，通过“iSeries 导航器”可提供更多服务器功能。易于使用的界面提供了许多益处，包括减少了技术支持成本和改进了系统的图像。它也存在安全性难题。

作为安全管理员，您不能再依赖于您的用户的无知来保护资源。“iSeries 导航器”您的用户提供了许多简便和显而易用的功能。您需要确保为用户概要文件和对象权限设计并实现了安全策略来满足您的安全性需要。

V4R4 和更高版本的 IBM e(logo)server iSeries Access for Windows 提供下列方法来控制用户可以通过“iSeries 导航器”执行的功能:

- 选择性安装
- 应用程序管理
- Windows NT® 系统策略支持

“iSeries 导航器”封装到您可以单独安装的多个组件中。这使您能够仅安装您需要的功能。“应用程序管理”使管理员能够控制用户或组可以通过“iSeries 导航器”访问的功能。“应用程序管理”将应用程序分成下列类别:

iSeries 导航器
包括“iSeries 导航器”和任何插件。

客户机应用程序
包括其它任何客户机应用程序（包括 iSeries Access），这些程序为通过“应用程序管理”进行管理的客户机提供多种功能。

主机应用程序
包括完全驻留在您的服务器上并提供通过“应用程序管理”管理的功能的所有应用程序。

可以使用选择性安装、应用程序管理和策略来限制用户可以访问的“iSeries 导航器”功能。然而，所有这些方法都不应该用于资源安全性。

从 V4R4 开始，IBM e(logo)server iSeries Access for Windows 也支持使用“Windows NT 系统策略编辑器”来控制从特定的 PC 客户机可以执行哪些功能，而不管谁正在使用该 PC。

有关选择性安装、“应用程序管理”和“策略管理”的附加信息，请参阅“iSeries 信息中心”。本书的第 5 页的『对程序功能的限制访问』一节也包含应用程序管理的一些讨论。

防止 ODBC 访问

开放式数据库连接 （ODBC）是一种工具，PC 应用程序可以使用它来访问 iSeries 数据，就好象数据是 PC 数据一样。ODBC 程序员可以使数据的物理位置对 PC 应用程序的用户是透明的。有关 ODBC 安全性注意事项的更多信息，转至“iSeries Access Windows 版 ODBC 安全性”（/rzaii/rzaiiodbc09.HTM），它位于“iSeries 信息中心”。

工作站会话密码的安全性注意事项

通常，当 PC 用户启动连接软件时（如 iSeries Access），该用户为服务器输入一次用户标识和密码。将密码加密并将它存储在 PC 内存中。每当该用户与同一服务器建立新的会话时，该 PC 自动发送用户标识和密码。

某些客户机／服务器软件也提供绕过交互式会话的“注册”屏幕的选项。当用户启动交互式（5250 仿真）会话时，该软件将发送用户标识和加密的密码。要支持此选项，必须将服务器上的 QRMTSIGN 系统值设置为 *VERIFY。

当您选择允许绕过“注册”屏幕时，需要考虑安全性折衷方案。

安全性漏洞: 对于 5250 仿真或任何其它类型的交互式会话，“注册”屏幕与任何其它屏幕相同。尽管输入密码时在屏幕上不显示密码，但正如任何其它数据字段那样，密码以未加密的格式通过链接发送。对于某些类型的链接，这可能为冒充的闯入者提供监控链接并检测用户标识和密码的机会。通过电子设备监控链接通常称为**窃听**。从 V4R4 开始，可以使用安全套接字层（SSL）对 iSeries Access 和 iSeries 服务器之间的通信进行加密。这就保护了您的数据（包括密码）免遭窃听。

当您选择绕过“注册”屏幕的选项时，PC 加密密码之后，才发送密码。加密避免了通过窃听偷取密码的可能性。然而，您必须确保您的 PC 用户实行可行的安全性措施。与 iSeries 系统具有活动会话的无人照管 PC 为某个人提供了启动另一个会话的机会，而不需要知道用户标识和密码。当系统长期不活动时，应该将 PC 设置为锁定，并且这些 PC 应该需要密码才能恢复会话。

即使您不选择绕过“注册”屏幕，具有活动会话的无人照管 PC 也会引起安全性漏洞。通过使用 PC 软件，某个人可以启动服务器会话并存取数据，而不必知道用户标识和密码。5250 仿真的漏洞要稍微严重一些，因为它不需要太多的知识就能启动会话并开始存取数据。

还需要告知用户断开其 iSeries Access 会话连接的影响。许多用户假定（逻辑上，但不正确），断开连接选项完全停止他们与服务器的连接。事实上，当用户选择该选项以断开连接时，服务器使用户的会话（许可证）对另一个用户可用。然而，客户机与服务器的连接仍是打开的。另一个用户可以接近未保护的 PC 并获取对服务器资源的访问，而未曾输入用户标识和密码。

您可以对需要使他们的会话断开连接的用户建议两个选项:

- 确保他们的 PC 具有需要密码的锁定功能。这使无人照管 PC 对不知道该密码的任何人都不可用。
- 要完全使会话断开连接，注销 Windows 或重新启动（重新引导）该 PC。这就结束了与 iSeries 的会话。

您也需要教育您的用户关于在他们使用 iSeries Access for Windows 时的可能的安全性漏洞。当用户指定 UNC（通用命名约定）来标识 iSeries 资源时，Win95 或 NT 客户机构建链接至服务器的网络连接。因为该用户指定 UNC，所以该用户不将此网络连接看作是映射的“网络驱动器”。通常，用户甚至意识不到网络连接的存在。然而，此网络连接会引起无人照管 PC 上的安全性漏洞，因为服务器出现在该 PC 上的目录树中。如果该用户的会话具有功能强大的用户概要文件，在无人照管 PC 上可能暴露服务器资源。正如先前的示例，补救方法是确保用户了解漏洞和确保他们使用其 PC 的锁定功能。

保护服务器以免远程命令和过程运行

对软件（如 iSeries Access）很在行的 PC 用户可以运行服务器上的命令而不需要通过“注册”屏幕。以下是 PC 用户可用来运行服务器命令的几种方法。您的客户机／服务器软件确定您的 PC 用户对服务器可用的方法。

- 用户可以打开 DDM 文件并使用远程命令功能来运行命令。
- 某些软件（如 iSeries Access 优化的客户机）通过“分布式程序调用”（DPC）API 提供远程命令功能，而不需要使用 DDM。
- 某些软件（如远程 SQL 和 ODBC）提供远程命令功能，而不需要 DDM 或 DPC。

对于使用 DDM 获取远程命令支持的客户机／服务器软件，您可以使用 DDMACC 网络属性来完全阻止远程命令 。对于使用其它服务器支持的客户机／服务器软件，您可以为服务器注册出口程序。如果要允许远程命令，必须确保您的对象权限方案可以充分保护您的数据。远程命令能力等价于给予用户命令行。此外，当 iSeries 通过 DDM 接收远程命令时，系统不实施用户概要文件“限制”功能（LMTCPB）设置。

保护工作站以免远程命令和过程运行

IBM iSeries Access for Windows 提供接收 PC 上的远程命令的功能。可以在服务器上使用“运行远程命令”（RUNRMTCMD）命令来运行连接的 PC 上的过程。RUNRMTCMD 功能是系统管理员和帮助桌面人员的有用工具。然而，它也提供了有意地或意外地损坏 PC 数据的机会。

PC 与 iSeries 服务器不具有相同的对象权限功能。对使用 RUNRMTCMD 命令的问题的最佳保护是仔细限制对该命令具有访问权的系统用户。IBM iSeries Access for Windows 提供注册哪些用户可以在特定 PC 上运行远程命令的功能。当通过 TCP/IP 连接时，您可以使用客户机上的特性控制面板来控制远程命令访问。可以通过用户标识或远程系统名称来授权用户。当通过 SNA 连接时，某些客户机软件提供设置对话的安全性的功能。使用其它客户机软件，您可以只选择是否设置入局命令功能。

对于客户机软件和连接类型（如 TCP/IP 或 SNA）的每种组合，您需要复查至连接的 PC 的入局命令的可能性。通过搜索“入局命令”或“RUNRMTCMD”来查阅客户机文挡。准备向您的 PC 用户和网络管理员建议有关将客户机配置为允许或阻止此功能的正确（安全）方法。

网关服务器

您的系统可以使用 iSeries 系统和 PC 之间的中间或网关服务器参与到网络中。例如，可以将您的 iSeries 系统使用一个 PC 服务器连接至 LAN，该 PC 服务器具有连接至该服务器的 PC。在此情况下的安全性问题取决于在网关服务器上运行的软件的能力。第 137 页的图 13 显示网关服务器配置示例:

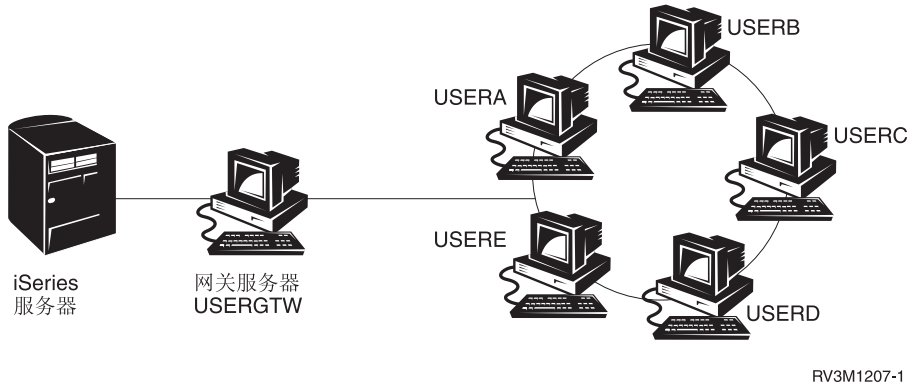

图 13. 使用网关服务器的 iSeries 系统

使用某些软件，您的 iSeries 系统将不了解来自网关服务器的下游的任何用户（如 USERA 或 USERC）。该服务器将作为单个用户（USERGTW）注册到系统上。它将使用 USERGTW 用户标识来处理来自下游用户的所有请求。来自 USERA 的请求对服务器看起来象来自用户 USERGTW 的请求。

如果是这样的话，您必须依靠网关服务器以获取安全性实施。必须了解和管理网关服务器的安全性功能。从 iSeries 服务器的角度每个用户与网关服务器用来启动会话的用户标识具有相同的权限。您可以将它看作是等价于运行沿用权限和提供命令行的程序。

使用其它软件，网关服务器将请求从单个用户传送至 iSeries 服务器。iSeries 服务器知道 USERA 正在请求访问特定对象。网关对系统几乎是透明的。

如果您的系统位于具有网关服务器的网络中，您需要评估将多大权限提供给网关服务器使用的用户标识。您也需要了解以下内容:

- 网关服务器实施的安全性机制。
- 对您的 iSeries 系统，下游用户将如何出现。

无线局域网通信

某些客户机可以使用 “iSeries 无线局域网” 来与系统进行无线通信。 “iSeries 无线局域网” 使用射频通信技术。作为安全管理员，应了解 “iSeries 无线局域网” 产品的下列安全性特征:

- 这些无线局域网产品使用扩展频谱技术。过去由政府使用此相同技术来保护无线电传输。对于试图以电子方式监控数据传输的用户，传输似乎是噪声而不是实际的传输。
- 无线连接具有三个与安全性相关的配置参数:
  - 数据率（两个可能的数据率）
  - 频率（两个可能的频率）
  - 系统标识符（8 百万个可能的标识符）

  这些配置元素组合来提供 8 千万个可能的配置，它使黑客猜中正确的配置的可能性大大地降低。
- 正如使用其它通信方法，客户机设备的安全性影响无线通信的安全性。系统标识信息和其它配置参数都在客户机设备上的文件中，且应该受到保护。

- 如果无线设备丢失或被偷，正常服务器安全性措施（如注册密码和对象安全性）在未授权的用户试图使用丢失或被偷的部件来访问系统时提供保护。
- 如果无线客户机部件丢失或被偷，应考虑更改所有用户、访问点和系统的系统标识信息。将它想象为当一串钥匙被偷时更换门上的锁。
- 可能要将服务器划分为具有唯一系统标识的客户机组。这可以限制部件丢失或被偷时的影响。仅当可以将一组用户限制为安装的特定分区时此方法才适用。
- 与有线局域网技术不同，无线局域网技术是私有的。因此，没有公然提供这些无线局域网产品的电子窃听器。窃听器是对传输执行未授权监控的电子设备。

第 15 章 安全性出口程序

某些 iSeries 服务器功能提供出口以便您的系统可以运行用户创建的程序来执行附加检查和验证。例如，可以将您的系统设置为每当有人试图打开您的系统上的 DDM（分布式数据管理）文件时运行出口程序。可以使用注册功能来指定在某些条件下运行的出口程序。

几个 iSeries 出版物包含执行安全性功能的出口程序示例。表 24 提供这些出口程序和示例程序的源的列表。

表 24. 样本出口程序的源

出口程序的类型	用途	查找示例的位置
密码验证	QPWDVLDPGM 系统值可以指定程序名称或指示使用为 QIBM_QSY_VLD_PASSWRD 出口点注册的验证程序来检查新密码以获取 QPWDxxx 系统值不处理的附加需求。应该小心监控此程序的使用，因为它接收未加密的密码。此程序**不应该**将密码存储在文件中或将它们传送至另一个程序。	• *An Implementation Guide for iSeries Security and Auditing, GG24–4200* • *iSeries Security Reference*, SC41-5302-07
PC Support/400 或 Client Access 访问[1]	可以在网络属性的“客户机请求访问”（PCSACC）参数中指定此程序名来控制以下功能: • 虚拟打印机功能 • 文件传送功能 • 共享文件夹“类型 2”功能 • Client access 消息功能 • 数据队列 • 远程 SQL 功能	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
“分布式数据管理”（DDM）访问	可以在网络属性的“DDM 请求访问”（DDMACC）参数中指定此程序名来控制以下功能: • 共享文件夹“类型 0 和 1”功能 • “提交远程命令”功能	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
远程注册	可以在 QRMTSIGN 系统值中指定某个程序来控制可以从哪些位置自动注册哪些用户（传递）。	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
具有 iSeries Access[1] 的“开放式数据库连接性”（ODBC）	控制 ODBC 的以下功能: • 是否完全允许 ODBC。 • 对于 iSeries 数据库文件允许什么功能。 • 允许什么 SQL 语句。 • 可以检索有关数据库服务器对象的什么信息。 • 允许什么 SQL 编目功能。	都不可用。

表 24. 样本出口程序的源 (续)

出口程序的类型	用途	查找示例的位置
QSYSMSG 中断处理程序	可以创建程序来监控 QSYSMSG 消息队列并根据消息的类型执行适当的操作（如通知安全管理员）。	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
TCP/IP	几个 TCP/IP 服务器（如 FTP、TFTP、TELNET 和 REXEC）提供出口点。可以添加出口程序来处理登录以及验证用户请求，如获取或放置特定文件的请求。也可以使用这些出口来在您的系统上提供匿名 FTP。	*iSeries System API Reference* 一书中的 TCP/IP User Exits
用户概要文件更改	可以为下列用户概要文件命令创建出口程序: CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• *iSeries Security Reference*, SC41-5302-07 • *iSeries System API Reference* 一书中的 TCP/IP User Exits

注:

1. 可以在 “iSeries 信息中心” 中找到关于此主题的附加信息。有关更多详情，请参阅第 xii 页的『先决条件和相关信息』。

第 16 章 因特网浏览器的安全性注意事项

您的组织中的许多 PC 用户在他们的工作站上具有浏览器。它们可能连接至因特网。它们也可能连接至您的服务器。以下是 PC 和您的服务器的某些安全性注意事项。

风险: 工作站损坏

您的用户访问的 Web 页面可能具有关联的“程序”，如 Java applet（一种 Active-X 控件）或某些其它类型的插件。尽管此类型的“程序”很少，但当它们在 PC 上运行时有可能损坏 PC 上的信息。作为安全管理员，考虑以下内容以保护您的组织中的 PC:

- 了解您的用户具有的不同浏览器的安全性选项。例如，对于某些浏览器，您可以控制 Java applet 在浏览器之外具有的访问权（Java 的受限制的操作环境称为*沙箱*）。这可以防止 applet 破坏 PC 数据。

  注: 沙箱概念及其关联的安全性限制对于 Active-X 和其它插件不存在。
- 向您的用户提出关于他们的浏览器设置的建议。您可能没有时间或资源来确保用户遵循您的建议。因此，您必须教育他们关于不正确的设置可能带来的风险。
- 考虑在提供您需要的安全性选项的 Web 浏览器上标准化。
- 指示您的用户通知您可能与特定 Web 站点关联的任何可疑行为或症状。

风险: 通过映射驱动器访问 iSeries 目录

假定使用 IBM iSeries Access for Windows 会话将 PC 连接至您的服务器。该会话设置映射驱动器来链接至 iSeries 集成文件系统。例如，PC 的 **G** 驱动器可能映射到网络中 SYSTEM1 服务器的集成文件系统。

现在假定同一 PC 用户具有浏览器并可以访问因特网。该用户请求某个 Web 页面，该页面运行有害“程序”，如 Java applet 或 Active-X 控件。可以想象，该程序可能尝试擦除在该 PC 的 G 驱动器中的所有内容。

有几个保护方法可防止对映射驱动器的破坏:

- 最重要的保护方法是您的服务器上的资源安全性。Java applet 或 Active-X 控件对服务器看起来象建立该 PC 会话的用户。您需要小心管理在您的服务器上授权 PC 用户执行的操作。
- 建议您的 PC 用户设置他们的浏览器以阻止试图访问映射驱动器。这对于 Java applet 起作用，但对于 Active-X 控件不起作用，这些控件不具有沙箱概念。
- 教育您的用户关于在同一会话中连接至您的服务器和因特网的危险。此外，确保您的 PC 用户（例如，具有 Windows 95 客户机）了解驱动器保持映射，即使当 iSeries Access 会话看来已结束。

风险: 可信的已签署的 applet

您的用户可能已遵循您的建议并设置他们的浏览器来防止 applet 写入任何 PC 驱动器。然而，您的 PC 用户需要知道*已签署的 applet* 可以覆盖他们的浏览器的设置。

已签署的 applet 具有关联的数字签名以建立其可靠性。当用户访问具有已签署的 applet 的 Web 页面时，该用户看到一条消息。该消息指示该 applet 的签名（谁签署了它和何时签署了它）。当您的用户接受该 applet 时，该用户授权该 applet 对浏览器的安全性设置的覆盖。已签署的 applet 可以写入 PC 的本地驱动器，即使浏览器的缺省设置阻止它。已签署的 applet 也可以写入在您的服务器上的映射驱动器，因为它们对 PC 看来是本地驱动器。

对于来自您的服务器的您自己的 Java applet，您可能需要使用已签署的 applet。然而，您应该指示您的用户通常不要从未知源接受已签署的 applet。

第 17 章 相关信息

手册

- *APPC Programming*, SC41-5443-00 描述 iSeries 系统的高级程序间通信（APPC）支持。此书指导开发使用 APPC 的应用程序和定义 APPC 通信的通信环境。它包括应用程序注意事项、配置需求和命令、APPC 的问题管理以及一般联网注意事项。请参阅 iSeries 信息中心 CD-ROM。
- *AS/400 因特网安全性: 在因特网中保护 AS/400 免受危害*红皮书 SG24-4929 讨论了将您的 iSeries 连接到因特网时与之相关联的安全性问题和风险。它提供 TCP/IP 应用程序的示例、建议、技巧和技术。
- *Backup and Recovery*, SC41-5304-07 提供关于计划备份与恢复策略、从系统保存信息以及恢复系统的信息。请参阅 iSeries 信息中心。也可以在 “iSeries 信息中心” 中找到关于这些主题的附加信息。有关更多详细信息，请参阅第 xii 页的『先决条件和相关信息』。
- *CL Programming*, SC41-5721-06 为可以在外部描述的文件提供了编码数据描述规范（DDS）的详细描述。这些文件是物理文件、逻辑文件、显示文件、打印文件和系统间通信功能（ICF）文件。请参阅 iSeries 信息中心。
- “信息中心” 中的 CL 主题（有关更多详细信息，请参阅第 xii 页的『先决条件和相关信息』。）提供所有 iSeries 控制语言（CL）及其 OS/400 命令的描述。OS/400 命令用来请求 Operating System/400®（5722-SS1）许可程序的功能。所有非 OS/400 CL 命令（与其它许可程序关联的那些命令，包括所有不同语言和实用程序）在支持那些许可程序的其它书籍中描述。
- *Implementing iSeries Security, 3rd Edition*, 由 Wayne Madden 和 Carol Woodbury 编写。由 Loveland, Colorado: 29th Street 出版社（Duke Communications International 的分部）于 1998 年出版。提供用于计划、设置和管理 iSeries 安全性的指导和实用建议。

  ISBN 订单号码:

  1-882419-78-2
- 有关 HTTP Server 的更多信息，访问下列 URL:

  `http://www.ibm.com/eserver/iseries/software/http/docs/doc.htm`
- *iSeries Security Reference*, SC41-5302-07 提供了关于安全性系统值、用户概要文件、资源安全性和安全性审计的完整信息。此手册并不描述特定许可程序、语言和实用程序的安全性。请参阅 iSeries 信息中心。
- “信息中心” 中的 “基本系统操作” 主题提供关于 iSeries 基本操作所需要的某些关键概念和任务的信息。有关更多详细信息，请参阅第 xii 页的『先决条件和相关信息』。
- “信息中心” 描述如何使用和配置 TCP/IP 和几个 TCP/IP 应用程序，如 FTP、SMTP 和 TELNET。有关更多详细信息，请参阅第 xii 页的『先决条件和相关信息』。
- *TCP/IP File Server Support for OS/400 Installation and User's Guide*（SC41-0125）提供 “文件服务器支持” 许可程序产品的介绍性信息、安装指示信息和设置过程。它说明使用该产品可获得的功能并包括将该产品与其它系统一起使用的示例和提示。

- *Trusted Computer Systems Evaluation Criteria* DoD 5200.28.STD 描述计算机系统的可信级别的条件。TCSEC 是美国政府的出版物。可以从下列位置获取副本:

  Office of Standards and Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 USA
  Attention: Chief, Computer Security Standards

- “信息中心”包含 iSeries 中有关“系统管理”和“工作管理”的几个主题。其中有些主题包括性能数据收集、系统值管理和存储管理。有关访问“信息中心”的详细信息，请参阅第 xii 页的『先决条件和相关信息』。Work Management(SC41-5306-03) 提供关于如何创建和更改工作管理环境的信息。请参阅 iSeries 信息中心。

除这些“信息中心”主题和“补充手册”之外，还可以使用下列资源来获取帮助:

- **IBM SecureWay**
  IBM SecureWay 为 IBM 广泛的安全性产品（硬件、软件、咨询和服务）提供一种公共品牌，以帮助客户保护他们的信息技术。无论是满足单独需要还是创建总的企业解决方案，IBM SecureWay 产品都为公司提供了规划、设计、实现和操作安全解决方案所需要的专门技术。有关 IBM SecureWay 产品的更多信息，请访问 IBM SecureWay 主页:

  `http://www.ibm.com/secureway`

- **服务提供**
  安装新的硬件或软件最终可以提高效率和商业运作。但是，它也造成商业中断和停机时间的威胁，并且可能使您宝贵的内部资源的负担加重。IBM 全球服务提供与 iSeries 安全性有关的服务。下列 Web 站点使您能够搜索对于您的 iSeries 的服务的完整列表:

  `http://www.as.ibm.com/asus`

声明

本信息是为在美国提供的产品和服务编写的。

IBM 可能在其它国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可证。您可以用书面方式将许可证查询寄往:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

有关双字节（DBCS）信息的许可证查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

本条款不适用于英国或任何这样的条款与当地法律不一致的国家或地区: 国际商业机器公司以“按现状”的基础提供本出版物，不附有任何形式的（无论是明示的，还是默示的）保证，包括（但不限于）对非侵权性、适销性和适用于某特定用途的默示保证。某些国家或地区在某些交易中不允许免除明示或默示的保证。因此，本条款可能不适用于您。

本资料中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本资料的新版本中。IBM 可以随时对本资料中描述的产品和／或程序进行改进和／或更改，而不另行通知。

本资料中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。该 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无需对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的: （i）允许在独立创建的程序和其它程序（包括本程序）之间进行信息交换，以及（ii）允许对已经交换的信息进行相互使用，请与下列地址联系:

IBM Corporation
Software Interoperability Coordinator, Department 49XA

3605 Highway 52 N
Rochester, MN 55901
U.S.A.

只要遵守适当的条件和条款，包括某些情形下一定数量的付费，都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、 IBM 国际程序许可证协议或任何同等协议中的条款提供。

此处包含的任何性能数据都是在受控环境中测得的。因此，在其它操作环境中获取的数据可能会有明显的不同。有些测量可能是在开发级的系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此外，有些测量是通过推算而估计的。实际结果可能会有差异。本文档的用户应当验证其特定环境的适用数据。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其它可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其它关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

所有关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

本资料仅用于规划目的。在所述产品上市之前，可以更改此处的信息。

本资料可能包含日常商业运作所使用的数据和报告的示例。为了尽可能全面地作举例说明，这些示例包含个人、公司、商标和产品的名称。所有这些名称都是虚构的，如与实际商业企业所使用的名称和地址有任何类似，纯属巧合。

版权许可证:

本资料可能包含源语言的样本应用程序，它们举例说明各种操作平台上的编程技术。您可以以任何形式复制、修改和分发这些样本程序，以开发、使用、市场营销或分发与编写样本程序所面向的操作平台的应用程序编程接口相符合的应用程序，而不必向 IBM 付费。并未在所有环境下完全测试这些示例。因此，IBM 不能保证或默示这些程序的可靠性、可服务性或功能。您可以以任何形式复制、修改和分发这些样本程序，以开发、使用、市场营销或分发与 IBM 的应用程序编程接口相符合的应用程序，而不必向 IBM 付费。

如果您查看的是本资料的软拷贝，可能没有图片和彩色插图。

商标

以下术语是国际商业机器公司在美国和 / 或其它国家或地区的商标:

Advanced Peer-to-Peer Networking
APPN
AS/400
DB2
DRDA
e（徽标）

IBM
iSeries
Net.Data
Operating System/400
OS/400
PowerPC
SecureWay
System/36
System/38
400

ActionMedia、LANDesk、MMX、Pentium 和 ProShare 是 Intel Corporation 在美国和／或其它国家或地区的商标或注册商标。

Microsoft、Windows、Windows NT 和 Windows 徽标是 Microsoft Corporation 在美国和／或其它国家或地区的商标。

Java 和所有基于 Java 的商标是 Sun Microsystems Inc. 在美国和／或其它国家或地区的商标。

UNIX 是 The Open Group 在美国和其它国家或地区的注册商标。

其它公司、产品和服务名称可能是其它公司的商标或服务标记。

索引

[D]

[E]

[F]

[G]

[H]

[J]

[K]

[L]

[M]

[N]

[P]

[Q]

[R]

[S]

[T]

[W]

[X]

[Y]

[Z]

[特别字符]

[数字]

A

B

C

D

E

F

I

J

L

O

P

Q

R

S

T

U

W

读者意见表

iSeries
保护 **iSeries** 的技巧和工具
版本 **5**

SB84-0175-02

姓名

地址

单位及部门

电话号码

读者意见表
SB84-0175-02

请沿此线
撕下或折起

折起并封口　　**请勿使用钉书机**　　折起并封口

在此
贴上
邮票

IBM 中国公司上海分公司，汉化部
中国上海市淮海中路 333 号
瑞安广场 10 楼
邮政编码：200021

折起并封口　　**请勿使用钉书机**　　折起并封口

SB84-0175-02

请沿此线
撕下或折起

中国印刷

SB84-0175-02