AIX 5L 版本 5.2

安全指南

S152-0648-02

AIX 5L 版本 5.2

安全指南

S152-0648-02

注

在使用本资料及其支持的产品前，请阅读第 235 页的附录 E，『声明』中的信息。

第四版（2004 年 5 月）

本版本适用于 AIX 5L V5.2 和本产品的所有后续发行版，直到在新版本中另有声明为止。

本出版物的后面提供了一张读者意见表。如果该表已除去，则将意见寄往：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。要通过电子的形式提供意见，请使用此商业因特网地址：ctscrcf@cn.ibm.com。我们可能会使用您提供的任何信息，而无须对您承担任何责任。

目录

关于本书

本书向系统管理员提供关于 AIX 操作系统的用户和组、文件、系统以及网络安全的信息。本指南包含关于如何执行诸如更改权限、设置认证方法、配置可信计算库环境和有评估保证级别 4+（EAL4+）功能的受控的访问保护概要文件（CAPP）的任务的信息。

*《AIX 5L V5.2 安全指南》*包含以下部件: 单机系统安全性、网络和因特网安全性及附录。

- 第一部分, “单机系统安全”提供了单机系统的 AIX 安全性的基线。此部分的范围包括使用可信计算库环境安装单机系统、安装 CAPP/EAL4+ 功能、控制登录、实施适当的密码规则、实现恰当的用户安全性机制、启用系统审计以及监视文件和目录访问。此部分还包含关于 X11、公共桌面环境（CDE）、轻量级目录访问协议（LDAP）以及更多的安全性信息。
- 第二部分, “网络和因特网安全性”提供关于网络和因特网安全性的信息。此部分阐述了关于配置 TCP/IP 安全性、控制网络服务、审计和监视网络安全性、配置 IP 安全性、配置虚拟专用网、电子邮件安全性、NFS 安全性、名称服务及 Kerberos 的关注。
- 第三部分包含附录，它包含安全性清单、关于安全性工具的信息、联机安全性参考资料以及关于网络服务和通信端口的参考信息。

本版本支持带有 5200-03 推荐的维护软件包的 AIX 5L V5.2 的发行版。任何对该维护软件包的特定引用都显示为*带 5200-03 的 AIX5.2*。

本书适用于

本书是为系统管理员及 IT 安全性管理员准备的。

突出显示

本书中使用以下突出显示约定:

粗体	标识命令、子例程、关键字、文件、结构、目录及其它名称由系统预定义的项。也标识图形对象，例如用户选择的按钮、标签及图标。
斜体	标识将由用户提供实际名称或值的参数。
等宽字体	标识特定数据值的示例、与您可能见到的显示文本类似的示例、与您作为程序员可能编写的程序代码类似的片断示例、来自系统的信息或您应实际输入的信息。

AIX 中区分大小写

AIX 操作系统中的每一项都是区分大小写的，这意味着其大小写字母之间有区别。例如，可以使用 **ls** 命令来列出文件。如果您输入 LS，则系统响应该命令“未找到”。同样，**FILEA**、**FiLea** 和 **filea** 是三个不同的文件名，即使它们驻留在同一个目录下。为了避免引起执行不想要的操作，要始终确保使用正确的大小写字母。

ISO 9000

本产品的开发和生产中使用了 ISO 9000 质量认证体系。

相关出版物

以下出版物包含相关的信息:

- *《AIX 5L V5.2 系统管理指南: 操作系统与设备》*
- *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*
- *《AIX 5L V5.2 系统管理指南: 通信与网络》*
- *《AIX 5L V5.2 操作系统安装: 入门》*
- *《AIX 5L V5.2 安装指南与参考大全》*
- *《AIX 5L V5.2 命令参考大全》*
- *AIX 5L Version 5.2 Files Reference*
- *AIX 5L Version 5.2 General Programming Concepts: Writing and Debugging Programs*
- *《AIX 5L V5.2 系统用户指南: 操作系统与设备》*
- *《AIX 5L V5.2 系统用户指南: 通信与网络》*
- *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide*
- *AIX 5L Version 5.2 Guide to Printers and Printing*

第 1 部分 单机系统安全性

本指南的第一部分提供了有关如何保护单机系统的信息，而不考虑网络连通性。这些章节描述了如何在安全性选项打开时安装系统，以及如何保护 AIX 以免使无授权用户取得对系统的访问。

第 1 章 安装和配置安全系统

本章提供关于安装和配置安全系统的信息。

本章中的主题包含:

- 『可信计算库』
- 第 8 页的『受控的访问保护概要文件和评估保证级别 4+』
- 第 20 页的『登录控制』
- 第 23 页的『管理 X11 和 CDE 注意事项』

可信计算库

系统管理员必须确定可以赋予某个特定程序多大的信任。这一确定包含在决定以特权安装程序需要多大信任时，考虑系统上信息资源的价值。

“可信计算库”（TCB）是负责强制系统范围信息安全策略的系统的一部分。通过安装和使用 TCB，可以定义对可信通信路径的用户访问，这将允许用户和 TCB 间的安全通信。只有在安装操作系统时，才启用 TCB 功能。要在已安装的机器上安装 TCB，您将必须执行“保留”安装。启用 TCB 允许您访问可信 shell、可信进程以及“安全注意键”（SAK）。

本部分讨论以下主题:

- 『安装带有可信计算库的系统』
- 第 4 页的『检查可信计算库』
- 第 4 页的『sysck.cfg 文件的结构』
- 第 4 页的『使用 tcbck 命令』
- 第 6 页的『配置额外的可信选项』

安装带有可信计算库的系统

TCB 是负责强制系统信息安全策略的系统的一部分。TCB 包含全部计算机硬件，但管理系统的人员应该主要关心 TCB 的软件组件。

如果您安装系统时使用“可信计算库”选项，您就启用了可信路径、可信 shell 及系统完整性校验（**tcbck** 命令）。这些功能*仅*可以在基本操作系统（BOS）安装过程中启用。如果在初始安装过程中未选择 TCB 选项，**tcbck** 命令将被禁用。只有通过启用 TCB 选项来重新安装系统才可以使用该命令。

要在 BOS 安装过程中设置 TCB 选项，请从“安装和设置”屏幕选择**更多选项**。在“安装选项”屏幕，**安装可信计算库**选择的缺省值是 **no**。要启用TCB ，请输入 2 并按下 Enter 键。

由于每个设备都是 TCB 的一部分，所以 TCB 监视 **/dev** 目录中的每个文件。另外，TCB 自动监视超过 600 个附加文件，把这些文件的关键信息存储在 **/etc/security/sysck.cfg** 文件中。如果正在安装 TCB，安装以后立即把该文件备份到可移动的介质中，例如磁带、CD 或磁盘，并把介质存储在安全的地方。

检查可信计算库

tcbck 命令审计“可信计算库”的安全状态。当 TCB 文件未得到正确保护或当配置文件具有非安全值时，操作系统的安全性会受到危害。**tcbck** 命令通过读取 **/etc/security/sysck.cfg** 文件审计该信息。该文件包含所有 TCB 文件、配置文件和可信命令的描述。

/etc/security/sysck.cfg 文件并没有脱机，因此黑客就有可能改变它。确保每一个 TCB 更新后，创建一个脱机的只读副本。同时，做进行任何检查之前，把该文件从归档介质中复制到磁盘上。

安装 TCB 和使用 **tcbck** 命令不能保证系统在符合受控访问保护概要文件（CAPP）和评估保证级别 4+（EAL4+）的方式下运行。有关 CAPP/EAL4+ 选项的信息，请参阅第 8 页的『受控的访问保护概要文件和评估保证级别 4+』。

sysck.cfg 文件的结构

tcbck 命令读取 **/etc/security/sysck.cfg** 文件以确定检查哪些文件。在 **/etc/security/sysck.cfg** 文件中用节描述了系统上每一个可信程序。

每节都有以下属性:

acl
文本字符串代表文件的访问控制列表。它必须和 **aclget** 命令输出有相同的格式。如果这不能与实际文件 ACL（访问控制表）相匹配，则 **sysck** 命令使用 **aclput** 命令来应用该值。

注: 如果存在 SUID、SGID 和 SVTX 属性，它们必须和方式指定的属性相匹配。

class
一组文件的名称。该属性允许通过给 **tcbck** 命令指定单一参数来检查具有相同类名的多个文件。可以指定一个以上的类，每一个类用逗号分隔。

group
文件组的组标识或名称。如果它和文件所有者不匹配，**tcbck** 命令把文件的所有者标识符设置成该值。

links
逗号分隔的路径名称列表链接到该文件。如果该表中的任意路径名称不和该文件链接，那么 **tcbck** 命令创建链接。如果没有使用 *tree* 参数，**tcbck** 命令打印出一条消息: 有额外的链接但没有确定它们的名称。如果使用 *tree* 参数，**tcbck** 命令也同样打印与链接到该文件的任何附加路径名称。

mode
逗号分隔的值列表。允许值是 SUID、SGID、SVTX 和 TCB。文件许可权必须是最后的值，且可指定为八进制值或 9 个字符的字符串。例如，**755** 或者 **rwxr-xr-x** 是有效的文件许可权。如果它和实际的文件方式不匹配，**tcbck** 命令应用正确值。

owner
文件所有者的用户标识或用户名称。如果它和文件所有者不匹配，**tcbck** 命令把文件的所有者标识符设置成该值。

program
逗号分隔的值列表。第一个值是检查程序的路径名称。当执行程序时，附加值作为参数传给程序。

注: 第一个参数总是 **-y**、**-n**、**-p** 或 **-t** 中的一个，取决于 **tcbck** 命令使用哪个标志。

source
文件名称，在检查之前源文件要从其复制过来。如果值为空白，且它为常规文件、目录或命名管道，如果还不存在，就创建该文件新的空版本。对于设备文件，为相同类型的设备创建一个新的特殊文件。

symlinks
逗号分隔的路径名称列表链接到该文件。如果该表中的任意路径名称不是至该文件的符号链接，**tcbck** 命令创建符号链接。如果使用 *tree* 参数，**tcbck** 命令也打印出任意至该文件的符号链路的其它路径名称。

如果 **/etc/security/sysck.cfg** 文件中的节没有指定属性，就不会执行相应的检查。

使用 tcbck 命令

tcbck 命令通常用于执行以下操作:

- 确保安全性相关文件的恰当安装

- 确保文件系统树不包含明显违反系统安全性的文件
- 更新、添加或删除可信文件

可以用以下方式使用 **tcbck** 命令:

- 正常使用
  - 系统初始化时的非交互式
  - 使用 **cron** 命令
- 交互式使用
  - 检出个别文件和文件类
- 过分猜疑型使用
  - 脱机存储文件 **sysck.cfg**，并定期恢复该文件以检出机器

虽然没有加密保护，TCB 使用 **sum** 命令得到校验和。TCB 数据库可以通过不同的校验和命令进行手工设置，例如，**textutils** RPM 软件包管理器 软件包中随 *AIX Toolbox for Linux Applications CD* 一起提供的 **md5sum** 命令。

检查可信文件

要检查 **tcbck** 数据库中所有的文件，并且修正并报告所有错误，请输入:

```
tcbck -y ALL
```

这样使 **tcbck** 命令检查 **/etc/security/sysck.cfg** 文件所描述的 **tcbck** 数据库中的每一个文件的安装。

要在系统初始化过程中自动执行此操作并生成错误日志，请将先前的命令字符串添加到 **/etc/rc** 命令中。

检查文件系统树

无论何时怀疑系统的完整性是否可能已经受损，请运行 **tcbck** 命令检查文件系统树:

```
tcbck -t tree
```

当使用带有 *tree* 值的 **tcbck** 命令时，检查系统上的所有文件是否正确安装（这可能需要较长的时间）。如果 **tcbck** 命令发现任何对系统安全性有潜在威胁的文件，可以改变可疑文件以除去损坏的属性。另外，对文件系统中所有其它的文件也执行以下检查:

- 如果文件所有者是 root，且文件设置了 **SetUID** 位，那么就清除 **SetUID** 位。
- 如果文件组是一个管理组，文件是可执行的，而且文件设置了 **SetGID** 位，那么就清除 **SetGID** 位。
- 如果文件设置了 **tcb** 属性，清除该属性。
- 如果文件是一个设备（字符或块特殊文件），则除去它。
- 如果文件是 **/etc/security/sysck.cfg** 文件中所述的路径名称的附加链接，则除去该链接。
- 如果文件是 **/etc/security/sysck.cfg** 文件中所述的至路径名称的附加符号链路，则出去该符号链路。

> **注**: 在执行 **tcbck** 命令或系统变得不可用之前，必须将所有设备记录添加到 **/etc/security/sysck.cfg** 文件中。要把可信设备添加到 **/etc/security/sysck.cfg** 文件中，使用 **-l** 标志。

警告: 不要运行 **tcbck -y tree** 命令选项。该选项删除并禁用那些在 TCB 中罗列不当的设备，且可能禁用系统。

添加可信程序

要将特定程序添加到 **/etc/security/sysck.cfg** 文件中，请输入:

```
tcbck -a PathName [Attribute=Value]
```

只有其值不是从文件当前状态引出的属性才必须在命令行中进行指定。所有的属性名称都包含在 **/etc/security/sysck.cfg** 文件中。

例如，以下命令注册一个新的 SetUID 根程序，命名为 **/usr/bin/setgroups**，它有一个名为 **/usr/bin/getgroups** 的链接:

```
tcbck -a /usr/bin/setgroups links=/usr/bin/getgroups
```

要添加 jfh 和 jsl 作为管理用户并添加 developers 作为管理组以在文件 **/usr/bin/abc** 安全审查过程中进行验证，请输入:

```
tcbck -a /usr/bin/abc setuids=jfh,jsl setgids=developers
```

安装程序以后，可能不知道哪个新文件在 **/etc/security/sysck.cfg** 文件中注册。可以使用以下命令查找和添加这些文件:

```
tcbck -t tree
```

该命令字符串显示在 **/etc/security/sysck.cfg** 文件中注册的任何文件名称。

删除可信程序

如果从系统删除一个 **/etc/security/sysck.cfg** 文件中所述的文件，则还必须从 **/etc/security/sysck.cfg** 文件中除去该文件的描述。例如，如果已删除了 **/etc/cvid** 程序，则以下命令字符串产生一条错误消息:

```
tcbck -t ALL
```

产生的错误消息如下所示:

```
3001-020 The file /etc/cvid was not found.
```

该程序的描述仍保留在 **/etc/security/sysck.cfg** 文件中。要除去该程序的描述，请输入以下命令:

```
tcbck -d /etc/cvid
```

配置额外的可信选项

本节提供了有关如何为 TCB 配置其它选项的信息。

限制访问终端

getty 和 **shell** 命令更改终端的所有者和方式以防止非可信程序访问终端。操作系统提供了配置专用终端访问的方法。

使用安全注意键

> **注意**: 当使用 SAK 时要小心，因为它会杀死试图访问终端的所有进程以及任何指向它的链接（例如，**/dev/console** 可以链接到 **/dev/tty0**）。

通过按下“安全注意键”（SAK）保留按键顺序（Ctrl-X，然后 Ctrl-R），可创建可信通信路径。根据以下条件建立可信通信路径:

- 当登录到系统时

按下 SAK 之后:

- 如果显示新的登录屏幕，那么您有了安全路径。
- 如果显示可信 shell 提示符，初始登录屏幕是未授权的程序，它可能试图窃取您的密码。使用 **who** 命令确定当前是谁在使用该终端，然后注销。

- 当您希望所输入的命令产生一个可信程序运行。这样的一些示例包含:
  - 作为 root 用户运行。只有创建了可信通信路径之后，才能作为 root 用户运行。这将确保没有非可信程序使用 root 用户权限运行。
  - 运行 **su -**、**passwd** 以及 **newgrp** 命令。只有创建了可信通信路径之后，才能运行这些命令。

配置安全注意键

可以单独配置每个终端，以便在该终端上按下“安全注意键”（SAK）创建可信通信路径。这在 **/etc/security/login.cfg** 文件的 **sak_enabled** 属性中进行指定。如果该属性值是 True，启用 SAK。

如果端口用于通信，（例如，通过 **uucp** 命令），所使用的特定端口在 **/etc/security/login.cfg** 文件中的节有以下行:

```
sak_enabled = false
```

该行（或那节中没有项）禁用那个终端的 SAK。

要在终端上启用 SAK，将以下行添加到该终端的节中:

```
sak_enabled = true
```

受控的访问保护概要文件和评估保证级别 4+

在 AIX 5.2 中开始，系统管理员可以在基本操作系统（BOS）安装过程中安装带有“受控的访问保护概要文件”（CAPP）和“评估保证级别 4+”（EAL4+）选项的系统。带有该选项的系统对 BOS 安装过程中安装的软件有限制，并且对网络访问也有限制。

本节讨论以下主题:

- 『CAPP/EAL4+ 符合的系统概述』
- 第 9 页的『安装 CAPP/EAL4+ 系统』
- 第 10 页的『CAPP/EAL4+ 软件包』
- 第 11 页的『用于 CAPP/EAL4+ 系统的物理环境』
- 第 12 页的『用于 CAPP/EAL4+ 系统的组织环境』
- 第 13 页的『CAPP/EAL4+ 系统的系统配置』

CAPP/EAL4+ 符合的系统概述

CAPP 系统是依照“公共标准”的针对安全性评估设计与配置的满足 受控的访问保护概要文件（CAPP）的系统。CAPP 指定系统的性能需求，类似于较早的 TCSEC C2 标准（也称为*橙皮书*）。

“公共标准（CC）评估系统”是已依照“公共标准”（用于 IT 产品评估的 ISO 标准（ISO 15408））进行评估的系统。 符合这些需求的系统配置在本指南中是指 *CAPP/EAL4+ 系统*。

如果按 CC 标准评估系统，CC 评估只对特定的系统配置（硬件和软件）是有效的。更改相关的安全性配置会产生未评估的系统。这并不一定意味将减少系统的安全性，只表示系统不再处于已认证配置状态。CAPP 与 CC 都不涵盖所有 AIX 5.2 可能的安全性配置选项。某些功能部件（如 IPsec 或定制密码检查模块）未包括在内，但可用于增强系统的安全性。

AIX 5.2 CAPP/EAL4+ 系统包含 64 位 POWER3 与 POWER4 处理器上的基操作系统，有以下部分:

- 逻辑卷管理程序（LVM）与增强的日志文件系统（JFS2）
- 带有 CDE 界面的 X-Windows 系统
- 基本网际协议 V4（IPv4）网络功能（Telnet、FTP、rlogin 与 rsh/rcp）
- 网络文件系统（NFS）

如果符合以下条件，则认为 CAPP/EAL4+ 系统是在安全状态中:

- 如果配置了审计过程且系统是多用户方式，则审计过程必须是可运作的。
- 该系统接受用户登录与服务网络请求。
- 对于分布式系统，该管理数据库是从主控服务器进行 NFS 安装的。

提供了以下安全性功能的管理界面:

- 识别和认证措施（用户的配置、密码设置、登录配置等。）
- 审计措施（配置 bin 方式审计、选择已审计的事件、处理审计跟踪等。）
- 自主访问控制（权限位数和文件系统对象的 ACL、IPC 机制和 TCP 端口）
- 设置系统时间
- 运行 **diag** 诊断子系统
- 运行 **su** 命令以成为有特权的管理员（root 用户）

这包含了可以用来执行相应管理的配置文件和系统调用。

提供了以下安全性功能的用户界面:

- **passwd** 命令，用于更改用户的密码
- **su** 命令，用于更改用户的标识
- **at**、**batch** 和 **crontab** 工具，用于调度命令处理
- 自主访问控制（权限位数和文件系统对象的 ACL 和 IPC 机制）
- 系统控制台的登录机制（例如，识别和认证机制）和受支持的网络应用程序（比如，**telnet** 和 **ftp**）

这包含了处理用户标识或访问控制的设置的系统调用。

AIX 5.2 CAPP/EAL4+ 系统在基于使用一个和两个 POWER3-II 处理器的 IBM eServer pSeries 对称多处理器（SMP）系统（IBM eServer pSeries 610）、使用 RS64 IV 处理器的 SMP 系统（IBM eServer pSeries 660）以及使用 POWER4 处理器的 SMP 系统（IBM eServer pSeries 690）的硬件平台上运行。受支持的外围设备是作为存储设备的终端和打印机、硬盘和 CD-ROM 驱动器以及作为备份设备的磁带机和软盘驱动器。受支持的网络接口类型是以太网和令牌环。

在 带有 5200-01 推荐的维护软件包的 AIX 5L V 5.2 中开始，CAPP/EAL4+ 技术在支持逻辑分区配置的 POWER4 处理器（IBM eServer pSeries 630、IBM eServer pSeries 650 和 IBM eServer pSeries 690）硬件平台上运行。受支持的外围设备是作为存储设备的终端和打印机、硬盘和 CD-ROM 驱动器以及作为备份设备的磁带机和软盘驱动器。受支持的网络接口类型是以太网和令牌环。

注: 管理员必须通知系统的所有用户不要使用 **$HOME/.rhosts** 文件进行远程登录和运行命令。

安装 CAPP/EAL4+ 系统

要在 BOS 安装期间设置 CAPP/EAL4+ 选项，请执行以下操作:

1. 在“安装与设置”屏幕上，选择 **更多选项**。
2. 在“更多选项”屏幕中，为**启用 CAPP 与 EAL4+ 技术**输入与 Yes 或 No 选项相符的数字。缺省值设置为 No。

启用 CAPP 与 EAL4+ 技术选项只有在以下条件下才是可用的:

- 安装方法设置为新建和完全覆盖安装。
- 选择英语语言。
- 启用 64 位内核。
- 启用增强的日志文件系统（JFS2）。

当**启用 CAPP 与 EAL4+ 技术**选项设置为 **yes** 时，**可信计算基**选项也设置为 **yes** 并且唯一有效的 **Desktop** 选项为 **NONE** 或 **CDE**。

如果正用定制的 **bosinst.data** 文件执行无提示安装，INSTALL_TYPE 字段必须设置为 CC_EVAL 且以下字段必须按如下设置:

```
control_flow:
 CONSOLE = ???
 PROMPT = yes
INSTALL_TYPE = CC_EVAL
INSTALL_METHOD = overwrite
TCB = yes
 DESKTOP = NONE or CDE
 ENABLE_64BIT_KERNEL = yes
 CREATE_JFS2_FS = yes
 ALL_DEVICES_KERNELS = no
 NETSCAPE_BUNDLE = no
 HTTP_SERVER_BUNDLE = no
```

```
 KERBEROS_5_BUNDLE = no
 SERVER_BUNDLE = no
 ALT_DISK_INSTALL_BUNDLE = no

locale:
 CULTURAL_CONVENTION = en_US or C
 MESSAGES = en_US or C
```

CAPP/EAL4+ 和网络安装管理（NIM）环境

可以使用“网络安装管理”（NIM）环境来执行 CAPP/EAL4+ 技术客户机的安装。配置了 NIM 主控机以提供安装 AIX 5L 的相应 CAPP/EAL4+ 级别所需的资源。然后可以使用位于 NIM 主控机上的资源来安装 NIM 客户机。您可以通过在 **bosinst_data** 资源中设置以下字段来执行客户机的无提示 NIM 安装:

```
control_flow:
 CONSOLE = ???
 PROMPT = no
INSTALL_TYPE = CC_EVAL
INSTALL_METHOD = overwrite
TCB = yes
 DESKTOP = NONE or CDE
 ENABLE_64BIT_KERNEL = yes
 CREATE_JFS2_FS = yes
 ALL_DEVICES_KERNELS = no
 NETSCAPE_BUNDLE = no
 HTTP_SERVER_BUNDLE = no
 KERBEROS_5_BUNDLE = no
 SERVER_BUNDLE = no
 ALT_DISK_INSTALL_BUNDLE = no

locale:
 CULTURAL_CONVENTION = en_US or C
 MESSAGES = en_US or C
```

NIM 主控机不能配置为 CAPP/EAL4+ 系统且无法连接到与其它 CAPP/EAL4+ 系统相同的网络。当从 NIM 主控机启动安装时，**安装 SMIT 后保留 NIM 客户机**菜单选项必须设置为否。在安装了 NIM 客户机作为 CAPP/EAL4+ 系统后，必须从 NIM 主控机的网络除去该 NIM 客户机，并且无法使用 NIM 主控机来执行其它的软件安装和更新。

在一个示例情况中，有两种网络环境；第一个网络由 NIM 主控机和非 CAPP/EAL4+ 系统构成；第二个网络只由 CAPP/EAL4+ 系统构成。在 NIM 客户机上执行 NIM 安装。安装完成后，把新安装的 CAPP/EAL4+ 系统从 NIM 主控机的网络断开连接，再把该系统连接到评估过的网络。

另一个示例由一个网络构成。当其它系统以评估过的配置运行时，NIM 主控机未连接到网络，且 CAPP/EAL4+ 系统在 NIM 安装过程中未连接到网络。

CAPP/EAL4+ 软件包

如果选择了 CAPP/EAL4+ 选项，则安装 **/usr/sys/inst.data/sys_bundles/CC_EVAL.BOS.autoi** 安装包的内容。

通过选择 CAPP/EAL4+ 选项，可以随意选择安装图形软件包和文档服务软件包。如果选择 CAPP/EAL4+ 选项同时选择“图形软件”选项，则安装 **/usr/sys/inst.data/sys_bundles/CC_EVAL.Graphics.bnd** 软件包的内容。如果选择 CAPP/EAL4+ 选项同时选择“文档服务软件”选项，则安装 **/usr/sys/inst.data/sys_bundles/CC_EVAL.DocServices.bnd** 软件包的内容。

在安装了“许可程序产品”（LPP）后，系统更改缺省配置以符合 CAPP/EAL4+ 的要求。对缺省配置进行以下更改:

- 从 **/etc/pse.conf** 文件除去 **/dev/echo**。

- 实例化 STREAMS 设备。
- 只允许 root 用户访问可移动介质。
- 从 **inetd.conf** 文件除去非 CC 项。
- 更改不同的文件许可权。
- 在 **sysck.cfg** 文件中注册符号链接。
- 在 **sysck.cfg** 文件注册设备。
- 设置缺省用户与端口属性。
- 为浏览器的使用配置 **doc_search** 应用程序。
- 从 **inittab** 文件除去 **httpdlite**。
- 从 **inittab** 文件除去 **writesrv**。
- 从 **inittab** 文件除去 **mkatmpvc**。
- 从 **inittab** 文件除去 **atmsvcd**。
- 在 **/etc/rc.tcpip** 文件中禁用 **snmpd**。
- 在 **/etc/rc.tcpip** 文件中禁用 **hostmibd**。
- 在 **/etc/rc.tcpip** 文件中禁用 **snmpmibd**。
- 在 **/etc/rc.tcpip** 文件中禁用 **aixmibd**。
- 在 **/etc/rc.tcpip** 文件中禁用 **muxatmd**。
- NFS 端口（2049）是具有特权的端口。
- 将丢失的事件添加到 **/etc/security/audit/events** 文件。
- 确保回送接口正在运行。
- 为 **/dev/console** 创建同义词。
- 强制缺省 X-server 连接许可权。
- 更改 **/var/docsearch** 目录，这样使得全部文件是所有人可读的。
- 添加“对象数据管理器”（ODM）节以设置控制台许可权。
- 设置在 BSD 样式 ptys 上的许可权为 000。
- 禁用 **.netrc** 文件。
- 添加补丁目录处理。

用于 CAPP/EAL4+ 系统的物理环境

CAPP/EAL4+ 系统对其运行的环境有特定的要求。要求如下:

- 必须限制对系统的物理访问，这样只有授权的管理员才可使用系统控制台。
- “服务处理器”没有连接到调制解调器。
- 限制已授权用户对终端的物理访问。
- 物理网络对窃听和电子欺骗程序（也称为“特洛伊木马”程序）是安全的。当在不安全的线路上通信时，需要额外的安全措施，如加密。
- 不允许与非 AIX 5.2 CAPP/EAL4+ 系统或不处于相同管理控制下的其它系统通信。
- 当与其它 CAPP/EAL4+ 系统通信时只使用 IPv4，IPv6 尚未经过评估。
- 必须禁止用户更改系统时间。
- LPAR 环境中的系统无法共享 PHB。

用于 CAPP/EAL4+ 系统的组织环境

对于 CAPP/EAL4+ 系统，必须满足以下程序性的与组织上的需求:

- 管理员必须是训练有素的。
- 管理员被认为是可信的。
- 只有授权处理系统上的信息的用户才能授予系统上的用户标识。
- 用户必须使用高质量密码（尽可能地随机且与用户或组织无关联）。有关设置密码规则的信息，请参阅第 40 页的『密码』。
- 用户不得把他们的密码透露给其他人。
- 管理员必须有充分的管理关键系统安全性的知识。
- 管理员必须按系统文档提供的指导工作。
- 管理员必须以他们的个人标识登录并使用 **su -** 命令切换到超级用户方式以便管理。
- 由管理员为系统用户生成的密码必须安全地发送给用户。
- 那些负责系统的人必须建立并实现必要的安全系统操作的过程。
- 管理员必须确保对安全关键性系统资源的访问受到许可权位和 ACL 的相应设置保护。
- 物理网络必须由组织核准来传送系统拥有的最敏感的数据。
- 维护过程必须包含系统的常规诊断。
- 管理员必须有适当的过程以确保在系统故障后安全操作与恢复。
- 不应该更改 **LIBPATH** 环境变量，因为这可能导致可信进程装入不可信库。
- 窃听和跟踪软件（**tcpdump**、**trace**）不得在运作的系统上使用。
- 匿名协议（如 HTTP）只能用于公共信息（例如在线文档）。
- 只可使用 TCP-based NFS。
- 不要赋予用户对可移动介质的访问权。设备文件将受到适当的许可权位或 ACL 的保护。
- 管理 AIX 时仅使用 root 用户权限。所有基于角色和基于组的管理授权功能及 AIX 的特权机制都不包含在 CAPP/EAL4+ 符合性中。
- 管理员不得使用动态分区来分配和释放资源。只有在没有任何分区运行时才可以执行分区配置。

CAPP/EAL4+ 系统的操作环境

对于CAPP/EAL4+，必须满足以下操作需求和过程:

- 如果使用的是 硬件管理控制台（HMC），HMC 位于物理控制的环境中。
- 只有经过授权的人员才能访问操作环境和 HMC。
- 如果要使用 HMC，则 HMC 只能用于以下任务:
  - 分区的初始配置。在配置处理过程中，分区不能是活动的。
  - 重新启动“挂起的”分区
- 在已配置的系统的整个操作中不得使用 HMC。
- 必须禁用系统的“回呼”功能。
- 必须禁用远程调制解调器访问系统。
- 如果 AIX 在启用了 LPAR 的环境中运行，则管理员应查看 LPAR 文档以获得关于逻辑分区的 EAL4+ 操作的需求。
- 必须在逻辑分区上禁用服务权限功能。

CAPP/EAL4+ 系统的系统配置

本节提供 CAPP/EAL4+ 系统中涉及的关于子系统配置方面的信息。

管理

管理员必须用他们个人用户帐户登录，并使用 **su** 命令成为系统管理的 root 用户。要有效阻止猜测 root 帐户的密码，仅允许授权的管理员在 root 帐户上使用 **su** 命令。要确保这一点，请执行以下操作:

1. 添加项到 **/etc/security/user** 文件的 **root** 节，按如下所示:

```
root:
  admin = true
  .
  .
  .
  sugroups = SUADMIN
```

2. 在仅包含授权管理员的用户标识的 **/etc/group** 文件中定义组，如下所示:

```
system:!:0:root,paul
staff:!:1:invscout,julie
bin:!:2:root,bin
.
.
.
SUADMIN:!:13:paul
```

管理员也必须遵守以下过程:

- 建立与实现某些过程来确保组成分布式系统的硬件、软件和固件组件以安全的方式发布、安装和配置。
- 确保系统已配置使得只有管理员能把新的可信软件引入到系统。
- 实现过程以确保用户从串行登录设备（如 IBM 3151 终端）注销之前清除屏幕。

用户与端口配置

用户与端口的 AIX 配置选项必须设置为满足评估的需求。实际的需要是正确猜测到密码的概率应该至少为一百万分之一，并且在一分钟内通过反复尝试而正确猜测到密码的概率应该至少为十万分之一。

以下示例中所显示的 **/etc/security/user** 文件使用 **/usr/share/dict/words** 字典列表。**/usr/share/dict/words** 文件包含在 **bos.data** 文件集中。在配置 **/etc/security/user** 文件之前，您必须安装 **bos.data** 文件集。**/etc/security/user** 文件的推荐值如下:

```
default:
  admin = false
  login = true
  su = true
  daemon = true
  rlogin = true
  sugroups = ALL
  ttys = ALL
  auth1 = SYSTEM
  auth2 = NONE
  tpath = nosak
  umask = 077
  expires = 0
  SYSTEM = "compat"
  logintimes =
  logintimes =
  pwdwarntime = 5
  account_locked = false
  loginretries = 3
  histexpire = 52
  histsize = 20
  minage = 0
```

```
  maxage = 8
  maxexpired = 1
  minalpha = 2
  minother = 2
  minlen = 8
  mindiff = 4
  maxrepeats = 2
  dictionlist = /usr/share/dict/words
  pwdchecks =
  dce_export = false

root:
  rlogin = false
  login = false
```

不应该用单个用户的特定设置覆盖 **/etc/security/user** 文件中的缺省设置。

注: 在 root 节设置 `login = false` 阻止直接的 root 用户登录。只有对于该 root 帐户有 **su** 特权的用户帐户才能以 root 帐户登录。如果启动 “拒绝服务” 攻击对发送错误密码给用户帐户的系统发动攻击，它能锁定所有的用户帐户。此攻击可能阻止任何用户（包括管理用户）登录到该系统。一旦锁定某用户的帐户，该用户将不能登录，直到系统管理员在 **/etc/security/lastlog** 文件中重新设置该用户的 `unsuccessful_login_count` 属性小于`loginretries` 用户属性的值。如果锁定了所有的管理帐户，可能需要重新启动系统到维护方式并运行 **chsec** 命令。有关使用 **chsec** 命令的更多信息，请参阅第 30 页的『用户帐户控制』。

/etc/security/login.cfg 文件的推荐值为如下:

```
default:
  sak_enabled = false
  logintimes =
  logindisable = 4
  logininterval = 60
  loginreenable = 30
  logindelay = 5
```

资源限制

当在 **/etc/security/limits** 文件中设置资源的限制时，确保该限制符合系统上进程的需要。特别是 `stack` 与 `rss` 大小决不应该设置为 `unlimited`。不受限制的堆栈可能覆盖正运行的进程的其它段，且不受限制的 `rss` 大小允许进程使用所有的实内存，因此对其它进程造成了资源问题。`stack_hard` 和 `rss_hard` 的大小也应受到限制。

审计子系统

以下过程帮助保护审计子系统:

- 配置审计子系统来记录用户所有的相关安全性活动。要确保审计过程需要的文件空间可用并且不受文件系统空间的其他客户损坏，请为审计数据设置专用的文件系统。
- 保护审计记录（如审计跟踪、库文件与其它所有存储在 **/audit** 的数据），从而使非 root 用户不能访问。
- 对于 CAPP/EAL4+ 系统，当使用审计子系统时，必须设置 **bin** 方式审计。有关如何建立审计子系统的信息，请参考第 55 页的『设置审计』。
- 系统中至少 20% 的可用磁盘空间应该由审计跟踪专用。
- 如果启用了审计过程，则 **/etc/security/audit/config** 文件的 **start** 节中的 *binmode* 参数应该设置为 **panic**。在 *bin* 节中的 **freespace** 参数最小应配置为等于 25% 的由存储审计跟踪专用的磁盘空间值。*bytethreshold* 与 *binsize* 参数每个都应该设置为 65536 字节。
- 从系统拷贝审计记录到用于文档的永久性存储器。

网络配置

网络配置必须使用“因特网端口任意访问控制”（DACinet）来确保不能匿名使用 X 协议（X11）与 NFS。有关 **dacinet** 命令的更多信息，请参阅第 125 页的『基于用户的 TCP 端口访问控制和因特网端口的带有自主访问控制』。

dacinet 命令阻止出现以下情况:

- 用 X11 取代另一用户桌面的用户。
- 向 NFS 服务器（该服务器允许用户成为 root 用户）伪造请求的客户机上的用户。通常，用户通过发出请求到本地主机上的“逻辑文件系统”，然后该系统发出请求（以 root 用户身份）到远程服务器，从而实现访问远程 NFS 服务器。为 root 用户仅设置 ACL 且不允许绕过此端口来确保用户不能直接发送协议请求到 NFS 服务器。

系统服务

下表显示运行于 CAPP/EAL4+ 系统上的标准系统服务（如果没有图形卡）。

表 1. 标准系统服务

UID	命令	描述
root	/etc/init	初始化进程
root	/usr/sbin/syncd 60	文件系统 sync 守护程序
root	/usr/sbin/srcmstr	SRC 主守护程序
root	/usr/sbin/cron	带 AT 支持的 CRON 设备
root	/usr/ccs/bin/shlap64	共享的库支持守护程序
root	/usr/sbin/syslogd	Syslog 守护程序
root	/usr/lib/errdemon	AIX 错误日志守护程序
root	/usr/sbin/getty /dev/console	getty / TSM
root	/usr/sbin/portmap	用于 NFS 与 CDE 的端口映射程序
root	/usr/sbin/biod 6	NFS 客户程序
root	/usr/sbin/rpc.lockd	NFS 锁定守护程序
daemon	/usr/sbin/rpc.statd	NFS stat 守护程序
root	/usr/sbin/rpc.mountd	NFS 安装守护程序
root	/usr/sbin/nfsd	NFS 服务器守护程序
root	/usr/sbin/inetd	Inetd 主守护程序
root	/usr/sbin/uprintfd	内核打印守护程序
root	/usr/sbin/qdaemon	排队守护程序
root	/usr/lpp/diagnostics/bin/diagd	诊断

运行 CAPP/EAL4+ 分布式系统

要运行 CAPP/EAL4+ 相应的分布式系统，所有用户在全部系统上必须有同样的用户标识。虽然这可用 NIS 来达到，该结果对于 CAPP/EAL4+ 系统还不够安全。本节描述一个分布式的设置，它确保用户标识在 CAPP/EAL4+ 相应的全部系统上是相同的。

主控机系统存储用于整个分布式系统的识别与认证数据（用户与组的配置）。所有其它系统使用 NFS 来安装此数据。NFS 由 DACinet 保护，这样只有管理员能在主控机访问 NFS 端口。

任意系统上的任意管理员都可使用工具（如 SMIT）来更改认证数据。在主控机上以物理方式更改认证数据。

所有共享识别与认证数据来自于 **/etc/data.shared** 目录。常规的识别与认证文件由符号链接替换为 **/etc/data.shared** 目录。

分布式系统上的共享文件: 在分布式系统中以下文件是共享的。通常，它们来自于 **/etc/security** 目录。

/etc/group
/etc/group 文件

/etc/hosts
/etc/hosts 文件

/etc/passwd
/etc/passwd 文件

/etc/security/.ids
下一个可用的用户与组标识

/etc/security/.profile
用于新用户的缺省 **.profile** 文件

/etc/security/acl
/etc/security/acl 文件存储用于受保护的服务的系统范围的 ACL 定义，这些服务将由 **/etc/rc.tcpip** 文件在下一次系统引导时重新激活。

/etc/security/audit/bincmds
用于该主机的库方式审计命令

/etc/security/audit/config
本地审计配置

/etc/security/audit/events
审计事件与格式的列表

/etc/security/audit/objects
该主机上审计对象的列表

/etc/security/audit/streamcmds
用于该主机的流方式审计命令

/etc/security/environ
每个用户的环境变量

/etc/security/group
来自 **/etc/security/group** 文件的扩展组信息

/etc/security/limits
每个用户的资源限制

/etc/security/passwd
每个用户的密码

/etc/security/priv
系统启动时要指定为有特权的端口列在 **/etc/security/priv** 文件中

/etc/security/services
列在 **/etc/security/services** 文件的端口认为是免除 ACL 检查的

/etc/security/user
每个用户与缺省用户的属性

分布式系统中非共享文件: **/etc/security** 目录中的以下文件在分布式系统中是不共享的，而是保留为特定主机使用:

/etc/security/failedlogin
每台主机登录失败的日志文件

/etc/security/lastlog
有关该主机上最后一次成功与不成功登录的每个用户信息

/etc/security/login.cfg
可信路径、登录 shell 与其它登录相关信息的特定主机登录特征

/etc/security/portlog
该主机上用于锁定端口的每个端口信息

共享文件自动生成的备份文件也是非共享的。备份文件与原始文件有相同的名称，但有小写字母 o 的区别。

设置分布式系统（主系统）： 在主控机，创建新的逻辑卷，它保留用于识别与认证的数据的文件系统。该逻辑卷命名为 **/dev/hd10sec** 且它作为 **/etc/data.master** 安装在主系统。要在主控机生成必需的更改，用主控机的 IP 地址和名称运行 **mkCCadmin** 命令，如下所示:

```
mkCCadmin -m -a ipaddress hostname
```

设置分布式系统（所有系统）： 移动所有要共享的数据到 **/etc/data.shared** 目录。启动时，所有系统通过 **/etc/data.shared** 目录安装主控机的 **/etc/data.master** 目录。主控机本身使用回送安装。

客户机系统通过运行以下命令设置:

```
mkCCadmin -a ipaddress hostname
```

要更改客户机以使用不同的主控机，请使用 **chCCadmin** 命令。

系统集成到分布式识别与认证系统后，生成以下额外的 **inittab** 项:

isCChost
初始化系统为 CAPP/EAL4+ 方式。

rcCC 清除所有 DACinet ACL 并只打开端口映射程序和 NFS 所需的端口。然后它加载共享目录。

rcdacinet
装入管理员可能已定义的附加 DACinet ACL。

当运行分布式系统时，请考虑以下内容:

- 管理员必须确保在更改共享配置文件前已加载了共享的数据，以保证在所有的系统上都能看到共享的数据。
- 更改 root 用户密码是只有在未加载共享目录时才允许的管理操作。

使用 DACinet 功能以获得基于用户和基于端口的网络访问控制

DACinet 功能部件可用于限制用户对 TCP 端口的访问。需要关于 DACinet 的更多信息，请参阅第 125 页的『基于用户的 TCP 端口访问控制和因特网端口的带有自主访问控制』。例如，当使用 DACinet 来限制只带 DACinet 功能的 root 用户对 TCP/25 端口入站的访问，只有来自 CAPP/EAL4+ 相应主机的 root 用户可以访问该端口。这种情况限制了常规用户通过使用 **telnet** 连接到受害人的 TCP/25 端口来欺骗电子邮件的可能性。

要在引导时为 TCP 连接激活 ACL，从 **/etc/inittab** 运行 **/etc/rc.dacinet** 脚本。它将读取 **/etc/security/acl** 文件中的定义并装载 ACL 到内核。不应由 ACL 保护的端口应该在 **/etc/security/services** 文件中列出，该文件使用与 **/etc/services** 文件相同的格式。

假定所有已连接的系统的子网为 10.1.1.0/24，仅对于 **/etc/security/acl** 文件中的 X（TCP/6000），root 用户的限定访问 ACL 项将如下:

```
6000    10.1.1.0/24 u:root
```

在 CAPP/EAL4+ 相应的系统上安装其它的软件

管理员能在 CAPP/EAL4+ 相应的系统上安装额外的软件。如果该软件不是由 root 用户或不使用 root 用户特权运行的，这将不会使 CAPP/EAL4+ 符合性无效。典型示例包含只由常规用户运行并没有 SUID 组件的办公应用程序。

另外，安装的使用 root 用户特权运行的软件将使得 CAPP/EAL4+ 符合性无效。例如，这意味着不应该安装较旧的 JFS 的驱动程序，因为它们以内核方式运行。以 root 用户运行的其它的守护程序（例如，SNMP 守护程序）也会使 CAPP/EAL4+ 符合性无效。

CAPP/EAL4+ 相应的系统很少用于评估配置，特别在商业环境。通常需要附加服务，这样生产系统将基于评估系统，但不符合评估系统的精确规范。

登录控制

潜在的黑客能够从缺省的 AIX 登录屏幕获取宝贵的信息，例如主机名和操作系统版本。这些信息资料使他们能确定去尝试哪种探查方法。为安全性原因，您可能希望在系统安装后尽可能快地更改登录屏幕缺省值。本节讨论以下主题:

- 『设置登录控制』
- 第 21 页的『更改登录屏幕的欢迎消息』
- 第 21 页的『更改公共桌面环境的登录屏幕』
- 第 21 页的『设置系统缺省登录参数』
- 第 21 页的『保护无人照管终端』
- 第 21 页的『强制自动注销』

KDE 和 GNOME 桌面系统都有一些相同的安全性说明。有关 KDE 和 GNOME 的更多信息，请参阅《*AIX 5L V5.2 安装指南与参考大全*》。

有关用户、组和密码的信息，请参阅第 25 页的第 2 章，『用户、角色和密码』。

设置登录控制

要使得较难通过猜测密码来攻击系统，请在 **/etc/security/login.cfg** 文件中如下所示设置登录控制:

表 2. **/etc/security/login.cfg** *文件的“属性”及“建议值”。*

属性	用于 PtYs（网络）	用于 TTYs	建议值	注释
sak_enabled	Y	Y	false	很少需要“安全注意键”。请参阅第 6 页的『使用安全注意键』。
logintimes	N	Y		在此处指定允许登录的次数。
logindisable	N	Y	4	在此终端连续 4 次试图登录失败后，禁止其登录。
logininterval	N	Y	60	在 60 秒内进行了指定的无效尝试后，禁用终端。
loginreenable	N	Y	30	在自动禁用终端 30 分钟后重新启用该终端。
logindelay	Y	Y	5	在两次出现登录提示之间的以秒为单位的时间间隔。这将随着尝试失败的次数成倍地增加；例如，初始值为 5 时，该时间间隔就为 5 秒、10 秒、15 秒、20 秒。

这些端口限制主要在已连接的串行终端上发挥作用，而不是在网络登录使用的伪终端上。您可在该文件中指定显式终端，例如:

```
/dev/tty0:
        logintimes = 0600-2200
        logindisable = 5
        logininterval = 80
        loginreenable = 20
```

更改登录屏幕的欢迎消息

为防止在登录屏幕上显示某些信息，请编辑 **/etc/security/login.cfg** 文件中的 *herald* 参数。缺省的 *herald* 包含随登录提示一起显示的欢迎消息。您可用 **chsec** 命令或直接编辑文件来更改该参数。

以下示例用 **chsec** 命令更改缺省的 *herald* 参数:

```
# chsec -f /etc/security/login.cfg -a default -herald
"Unauthorized use of this system is prohibited.\n\nlogin: "
```

有关 **chsec** 命令的更多信息，请参阅《*AIX 5L V5.2 命令参考大全，卷 1*》。

要直接编辑文件，请打开 **/etc/security/login.cfg** 文件并更新 *herald* 参数如下:

```
缺省值:
herald ="禁止未授权使用本系统 \n登录: "
 sak_enable = false
 logintimes =
 logindisable = 0
 logininterval = 0
 loginreenable = 0
 logindelay = 0
```

注: 要使得该系统更安全，请将 **logindisable** 和 **logindelay** 变量的值设置为大于 0（# > 0）。

更改公共桌面环境的登录屏幕

该安全性说明也影响公共桌面环境（CDE）用户。在缺省情况下，CDE 登录屏幕也显示主机名和操作系统版本。要防止显示此信息，请编辑 **/usr/dt/config/$LANG/Xresources** 文件，其中 **$LANG** 指的是安装在您的机器上的本地语言。

在我们的示例中，假定 **$LANG** 设置为 **C**，将该文件复制到 **/etc/dt/config/C/Xresources** 目录中。然后，打开 **/usr/dt/config/C/Xresources** 文件并编辑，以除去包含主机名和操作系统版本的欢迎消息。

有关 CDE 安全性说明的更多信息，请参阅第 23 页的『管理 X11 和 CDE 注意事项』。

设置系统缺省登录参数

要为许多登录参数设置基本缺省值，例如那些可能需要为新用户设置的参数（登录重试次数、登录重新启用和登录内部），请编辑 **/etc/security/login.cfg** 文件。

保护无人照管终端

如果终端处于登录状态却无人照管，那么所有的系统都是脆弱的。当系统管理员让用超级权限启用的终端处于无人照管状态时，就会出现最严重的问题。通常，任何时候用户离开他们的终端时都应该注销。让系统终端处于非安全状态会造成潜在的安全威胁。要锁定终端，请使用 **lock** 命令。如果您的界面是 AIXwindows，请使用 **xlock** 命令。

强制自动注销

另一个要关注的有效安全性问题是用户长时间将他们的帐户置于无人照管状态造成的后果。这种情况使闯入者可以控制用户的终端，从而潜在地危及系统的安全。

要预防这类潜在的安全威胁，您可在系统中启用自动注销功能。要这样做，请编辑 **/etc/security/.profile** 文件，为*所有*用户包含自动注销值，如下例所示:

```
TMOUT=600 ; TIMEOUT=600 ; export readonly TMOUT TIMEOUT
```

在本例中，数字 600 是以秒为单位，它等于 10 分钟。但是，该方法只在 shell 中生效。

当先前的操作允许您对所有用户强制执行自动注销策略时，系统用户就能通过编辑他们各自的 **.profile** 文件来绕过一些限制。为了完全实现自动注销策略，必须采取权威的措施，即给用户提供适当的 **.profile** 文件，阻止对这些文件的写访问权。

管理 X11 和 CDE 注意事项

本节讨论了涉及 X11 X 服务器和公共桌面环境（CDE）的潜在安全弱点。

除去 /etc/rc.dt 文件

尽管用户运行 CDE 接口很方便，但是有些安全性说明与之有关。由于这个原因，请不要在需要高级别安全性的服务器上运行 CDE。最好的解决方案是避免安装 CDE（dt）文件集。如果您已经在您的系统上安装了这些文件集，那就考虑将其卸载，特别是启动 CDE 的 **/etc/rc.dt** 脚本。

更多关于 CDE 的信息，请参阅 *《AIX 5L V5.2 系统管理指南: 操作系统与设备》*。

阻止远程 X 服务器的未经授权的监视

与 X11 服务器有关的一个重要安全问题是远程服务器的未经授权的静默监视。**xwd** 和 **xwud** 命令可以用于监视 X 服务器活动，因为它们有能力捕获击键，这会暴露密码和其它敏感数据。要解决这个问题，除去这些可执行文件，除非在您的配置下它们是必要的，或者，作为备用，将对这些命令的访问权更改为只有 root 用户才能访问。

xwd 和 **xwud** 命令位于 **X11.apps.clients** 文件集。

如果您确实需要保留 **xwd** 和 **xwud** 命令，考虑使用 OpenSSH 或 MIT Magic Cookie。这些第三方应用程序帮助阻止运行 **xwd** 和 **xwud** 命令所产生的风险。

有关 OpenSSH 和 MIT Magic Cookies 的更多信息，请参考每个应用程序各自的文档。

禁用和启用访问控制

X 服务器允许远程主机使用 **xhost +** 命令来连接系统。确保使用 **xhost +** 命令指定了主机名，因为它禁用对 X 服务器的访问控制。这允许您将访问权授予特定主机，以便于监视对 X 服务器的潜在攻击。要将访问权授予特定主机，运行如下的 **xhost** 命令:

```
# xhost + 主机名
```

如果您不指定主机名，那么将访问授权予所有主机。

有关 **xhost** 命令的更多信息，请参阅*《AIX 命令参考大全，卷 6》*。

禁用运行 xhost 命令的用户许可权

确保适当地使用 **xhost** 命令的另一种方法是限制该命令仅能由具有 root 用户权限的用户执行。要做到这一点，使用 **chmod** 命令将 **/usr/bin/X11/xhost** 的许可权更改为 744，如下所示:

```
chmod 744/usr/bin/X11/xhost
```

第 2 章 用户、角色和密码

本章描述了如何管理 AIX 用户和角色。讨论以下主题:

Root 帐户

root 帐户实际上拥有对系统中所有程序、文件及资源的不受限制的访问权。root 帐户是 **/etc/passwd** 文件中用户标识（UID）为 0 的特殊用户，并且通常所给的用户名是 *root*。并不是这个用户名使得 root 帐户这么特殊，而是 UID 的值 0。这意味着拥有 UID 为 0 的任何用户也拥有与 root 用户一样的权限。并且，root 帐户总是通过本地安全性文件认证。

root 帐户应该总是有密码，该密码应该从不共享。安装系统后，应立即给 root 帐户一个密码。只有系统管理员才能知道 root 密码。系统管理员应该只在执行需要 root 权限的系统管理功能时才作为 root 用户进行操作。对于其它所有的操作，他们应该返回到他们的一般用户帐户。

警告: 因为 root 帐户覆盖许多系统安全防护，所以经常作为 root 用户操作可能会对系统产生损坏。

禁用直接 root 用户登录

潜在黑客的一个常见攻击方法是获取 root 密码。

要避免此类攻击，可以禁用直接访问 root 标识，然后要求系统管理员通过使用 **su -** 命令获取 root 权限。除了允许删除作为攻击对象的 root 用户，限制直接的 root 访问使您可以监视哪些用户获取了 root 访问权及他们操作的时间。可以查看 **/var/adm/sulog** 文件做到这一点。另一种方法是启用系统审计，这将报告此类活动。

要禁止 root 用户远程登录访问，编辑 **/etc/security/user** 文件。在 root 项中指定 **false** 作为 rlogin 的值。

在禁用远程 root 登录之前，请检查并准备可能使系统管理员用非 root 用户标识无法登录的情况。例如，如果用户的主文件系统已满，该用户将无法登录。如果禁用了远程 root 登录，而能使用 **su -** 命令更改到 root 用户的用户主文件系统已满，则 root 用户可能永远无法取得对系统的控制。系统管理员可以通过为他们自己创建比一般用户文件系统大的主文件系统绕过此问题。

有关控制 root 用户登录的更多信息，请参阅第 13 页的『CAPP/EAL4+ 系统的系统配置』。

管理角色

可以将 root 用户权限的一部分分配给非 root 用户。给不同的 root 用户任务分配不同的权限。这些权限分组成角色并指定给不同的用户。

本节涵盖以下主题:

- 『角色概述』
- 『使用 SMIT 设置和维护角色』
- 第 27 页的『理解授权』.

角色概述

角色由授权构成。这些授权允许用户运行通常需要 root 用户许可权的功能。以下是有效角色的列表:

添加与除去用户
对于此角色，允许任何用户作为 root 用户操作。它们能够添加与除去用户、更改用户信息、修改审计类、管理组和更改密码。执行用户管理的任何人必须在 **security** 组中。

更改用户密码
允许用户更改密码。

管理角色
允许用户创建、更改、除去和列出角色。用户必须在 **security** 组中。

备份与恢复
允许用户备份与恢复文件系统及目录。该角色还不足以使用 mksysb 启用系统备份和恢复，还需要适当的权限。

只备份
允许用户只备份文件系统及目录。用户必须有启用系统备份的适当权限。

运行诊断
允许用户或服务代表运行诊断及诊断任务。用户必须将 **system** 指定为主组和包含 **shutdown** 的组集合。

注: 处于运行诊断角色的用户可更改系统配置、更新微码等等。此角色的用户必须完全理解该角色所要求的职责。

系统关机
允许用户关闭、重新引导或停止系统。

使用 SMIT 设置和维护角色

以下 SMIT 快速路径可用于实现和维护角色:

表 3. 设置和维护角色任务

任务	SMIT 快速路径
添加角色	**smit mkrole**
更改角色特征	**smit chrole**
显示角色特征	**smit lsrole**
除去角色	**smit rmrole**
列出全部角色	**smit lsrole**

理解授权

授权是用户的权限属性。授权允许用户执行某些任务。现有以下授权类型:

基本授权
允许用户运行特定的命令。例如，RoleAdmin 授权是允许用户管理员运行 **chrole** 命令的基本授权。无此授权，不修改角色定义而终止命令。

授权修饰符
增加用户的能力。例如，UserAdmin 授权是增加属于 **security** 组的用户管理员的能力的授权修饰符。无此授权，**mkuser** 命令仅创建非管理员用户。有此授权，**mkuser** 命令也创建管理员用户。

授权执行以下功能:

Backup
执行系统备份。以下命令使用 Backup 授权:

Backup
备份文件和文件系统。用户管理员必须拥有 Backup 授权。

Diagnostics
允许用户运行诊断。也需要权限直接从命令行运行诊断任务。以下命令使用 Diagnostics 授权:

diag 在选定的资源上运行诊断。如果用户管理员没有 Diagnostics 权限，命令结束。

GroupAdmin
对组数据执行 root 用户功能。以下命令使用 GroupAdmin 授权:

chgroup
更改任意组信息。如果用户没有 GroupAdmin 授权，仅能更改非管理组信息。

chgrpmem
管理所有组。如果组管理员没有 GroupAdmin 授权，仅能更改所管理的组中的组成员或更改组安全性中的用户以管理任意非管理组。

chsec 修改 **/etc/group** 和 **/etc/security/group** 文件中的管理组数据。用户也能修改缺省的 **节值**。如果用户没有 GroupAdmin 授权，仅能修改 **/etc/group** 和 **/etc/security/group** 文件中的非管理组数据。

mkgroup
创建任意组。如果用户没有 GroupAdmin 授权，仅能创建非管理组。

rmgroup
除去任意组。如果用户没有 GroupAdmin 授权，仅能除去非管理组。

ListAuditClasses
查看有效审计类的列表。使用此授权的用户管理员不必是 root 用户或在**审计**组中。

使用 **smit mkuser** 或 **smit chuser** 快速路径列出产生或更改用户的可用审计类。请在 **AUDIT classes** 字段中输入审计类列表。

PasswdAdmin
对密码数据执行 root 用户功能。以下命令使用 PasswdAdmin 授权:

chsec 修改所有用户的 **lastupdate** 和 **flags** 属性。在没有 PasswdAdmin 权限的情况下，**chsec** 命令仅允许用户管理员修改非管理用户的 **lastupdate** 和 **flags** 属性。

lssec 查看所有用户的 **lastupdate** 和 **flags** 属性。无 PasswdAdmin 授权，**lssec** 命令仅允许用户管理员查看非管理用户的 **lastupdate** 和 **flags** 属性。

pwdadm

更改所有用户的密码。用户管理员必须在 **security** 组中。

PasswdManage

对非管理用户执行密码管理功能。以下命令使用 PasswdManage 授权:

pwdadm

更改非管理用户的密码。管理员必须在 **security** 组中或者拥有 PasswdManage 授权。

UserAdmin

对用户数据执行 root 用户功能。仅拥有 UserAdmin 授权的用户能修改用户的角色信息。无此授权，不能访问或修改用户审计信息。以下命令使用 UserAdmin 授权:

chfn 更改任意用户一般信息（gecos）字段。如果用户没有 UserAdmin 授权但是在 **security** 组中，则他们可以更改任何非管理用户的 gecos 字段。否则，用户仅能更改自己的 gecos 字段。

chsec 修改 **/etc/passwd**、**/etc/security/environ**、**/etc/security/lastlog**、**/etc/security/limits** 和 **/etc/security/user** 文件中的管理用户数据，包括角色属性。用户管理员也能修改缺省节值和 **/usr/lib/security/mkuser.default** 文件，不包括审计类属性。

chuser

更改除了审计类属性的任意用户信息。如果用户没有 UserAdmin 授权，仅能更改除了审计类和角色属性的非管理用户信息。

mkuser

创建除了审计类属性的任意用户。如果用户没有 UserAdmin 授权，仅能创建除了审计类和角色属性的非管理用户。

rmuser

除去任意用户。如果用户没有 UserAdmin 授权，仅能创建非管理用户。

UserAudit

允许用户修改用户审计信息。以下命令使用 UserAudit 授权:

chsec 为非管理用户修改 **mkuser.default** 文件的审计类属性。如果用户有 UserAdmin 授权，也能为管理及非管理用户修改 **mkuser.default** 文件的审计类属性。

chuser

修改非管理用户的审计类属性。如果用户管理员有 UserAdmin 授权，也能修改所有用户的审计类属性。

lsuser 如果用户是 root 用户或在 **security** 组，查看该非管理用户的审计类属性。如果用户管理员有 UserAdmin 授权，也能查看所有用户的审计类属性。

mkuser

创建新用户并允许用户管理员分配非管理用户的审计类属性。如果用户管理员有 UserAdmin 授权，也能修改所有用户的审计类属性。

RoleAdmin

对角色数据执行 root 用户功能。以下命令使用 RoleAdmin 授权:

chrole 修改角色。如果用户管理员没有 RoleAdmin 授权，命令结束。

lsrole 查看角色。

mkrole

创建角色。如果用户管理员没有 RoleAdmin 授权，命令结束。

rmrole

除去角色。如果用户管理员没有 RoleAdmin 授权，命令结束。

Restore

执行系统恢复。以下命令使用 Restore 授权:

Restore

恢复备份文件。用户管理员必须拥有 Restore 授权。

授权命令列表

下表列出了命令和它们使用的授权。

命令	许可权	授权
chfn	2555 root.security	UserAdmin
chuser	4550 root.security	UserAdmin, UserAudit
diag	0550 root.system	Diagnostics
lsuser	4555 root.security	UserAudit, UserAdmin
mkuser	4550 root.security	UserAdmin, UserAudit
rmuser	4550 root.security	UserAdmin
chgroup	4550 root.security	GroupAdmin
lsgroup	0555 root.security	GroupAdmin
mkgroup	4550 root.security	GroupAdmin
rmgroup	4550 root.security	GroupAdmin
chgrpmem	2555 root.security	GroupAdmin
pwdadm	4555 root.security	PasswdManage, PasswdAdmin
passwd	4555 root.security	PasswdManage, PasswdAdmin
chsec	4550 root.security	UserAdmin, GroupAdmin, PasswdAdmin, UserAudit
lssec	0550 root.security	PasswdAdmin
chrole	4550 root.security	RoleAdmin
lsrole	0550 root.security	RoleAdmin
mkrole	4550 root.security	RoleAdmin
rmrole	4550 root.security	RoleAdmin
backup	4555 root.system	Backup
restore	4555 root.system	Restore

用户帐户

- 第 30 页的『推荐用户属性』
- 第 30 页的『用户帐户控制』
- 第 31 页的『登录用户标识』
- 第 31 页的『使用访问控制表增强用户安全性』
- 第 31 页的『PATH 环境变量』

推荐用户属性

用户管理由创建用户和组以及定义它们的属性构成。用户的一个主要属性是如何对他们进行认证。用户是系统的主要代理。其属性控制他们的访问权、环境、如何对他们进行认证以及如何、何时、在哪里可以访问他们的帐户。

组是对保护资源共享同一访问许可权的用户集合。一个组有一个标识，且由组成员和管理员组成。组的创建者通常就是第一管理员。

可以对每个用户帐户设置多个属性，包含密码和登录属性。有关可配置属性的列表，请参阅第 45 页的『磁盘配额系统概述』。推荐以下属性:

- 每个用户应有一个不与其他用户共享的用户标识。所有安全防护措施和责任工具仅在每个用户都有唯一标识时起作用。
- 为系统用户指定一个对其有意义的用户名。最好使用实际名称，因为大多数电子邮件系统使用用户标识为接收的邮件标号。
- 使用基于 Web 的系统管理器或 SMIT 界面添加、更改和删除用户。虽然可以通过命令行来执行所有这些任务，但这些界面有助于减少小错误。
- 在用户准备好登录系统前不要为用户帐户提供初始密码。如果在 **/etc/passwd** 文件中将密码字段定义为 *（星号），虽然帐户信息得到保存，但不能登录到该帐户。
- 不要更改系统正常运行所需的由系统定义的用户标识。系统定义的用户标识罗列在 **/etc/passwd** 文件中。
- 一般情况下，不要将任何用户标识的 **admin** 参数设置为 **true**。只有 root 用户可以为在 **/etc/security/user** 文件中设置为 **admin=true** 的用户更改属性。

操作系统支持通常出现在 **/etc/passwd** 和 **/etc/group** 文件中的标准用户属性，例如:

认证信息	指定密码
凭证	指定用户标识、主体组和补充组标识
环境	指定主环境或 shell 环境。

用户帐户控制

每个用户帐户有一组相关属性。当使用 **mkuser** 命令创建用户时，这些属性根据缺省值创建。这些属性可以通过使用 **chuser** 命令来修改。以下用户属性不用于控制与密码质量无关的方面:

account_locked	如果必须明确地锁定帐户，则该属性可以设置为 *true*；缺省值是 *false*。
admin	如果设置为 true，则该用户无法更改密码。只有管理员可以更改它。
admgroups	列出此用户具有管理权限的组。对于这些组，该用户可以添加或删除成员。
auth1	用于授权用户访问的认证方法。典型地，将它设置为 *SYSTEM*，然后将使用较新的方法。
auth2	按 **auth1** 指定的无论什么对用户进行认证后运行的方法。它无法阻止对系统的访问。典型地，将它设置为 *NONE*。
daemon	此布尔参数指定是否允许用户使用 **startsrc** 命令启动守护程序或子系统。它也限制对 **cron** 和 **at** 设备的使用。
login	指定是否允许该用户登录。
logintimes	限制用户何时可以登录。例如，用户可能被限制只能在正常营业时间访问系统。
registry	指定用户注册表。可以用于告知系统用户信息的备用注册表，例如 NIS、LDAP 或 Kerberos。
rlogin	指定是否允许该用户通过使用 **rlogin** 或 **telnet** 登录。
su	指定其他用户是否可以使用 **su** 命令切换至此标识。
sugroups	指定允许哪个组切换至此用户标识。
ttys	限制某些帐户进入物理安全区域。
expires	管理学生或访客帐户；也可以用于临时关闭帐户。

loginretries 指定用户标识被系统锁定之前连续的可以尝试登录失败的最大次数。失败的尝试记录在 **/etc/security/lastlog** 文件中。

umask 指定用户的初始 **umask**。

所有的用户属性在 **/etc/security/user**、**/etc/security/limits**、**/etc/security/audit/config** 和 **/etc/security/lastlog** 文件中定义。使用 **mkuser** 命令创建的用户缺省值在 **/usr/lib/security/mkuser.default** 文件中指定。只有覆盖 **/etc/security/user** 和 **/etc/securtiy/limits** 文件中的 **default** 节中的一般缺省值的选项和审计类必须在 **mkuser.default** 文件中指定。这些属性中的一些控制用户如何可以登录，并且可以配置这些属性在指定情况下自动锁定用户帐户（阻止进一步登录）。

用户帐户由系统锁定后，用户无法登录直到系统管理员重新设置该用户在 **/etc/security/lastlog** 文件中的 **unsuccessful_login_count** 属性值小于登录重试值。可以使用以下 **chsec** 命令完成，如下所示:

```
chsec -f /etc/security/lastlog -s username -a
unsuccessful_login_count=0
```

可以使用 **chsec** 命令在相应安全性文件（例如 **/etc/security/user** 或 **/etc/security/limits** 文件）中编辑 *default* 节来更改缺省值。将许多缺省值定义为标准行为。要明确地指定每次创建新用户时要设置的属性，请更改 **/usr/lib/security/mkuser.default** 中的 *user* 项。

要了解扩展用户密码属性的信息，请参考第 40 页的『密码』。

登录用户标识

操作系统通过用户的登录用户标识来识别他们。登录用户标识允许系统可以追踪所有用户操作至它们的源。在用户登录系统后，初始用户程序运行前，系统将进程的登录标识设置为在用户数据库中找到的用户标识。登录会话过程中所有后继进程都用此标识做标记。这些标记提供登录用户标识执行的所有活动的踪迹。用户可以在会话过程中重新设置有效用户标识、真实用户标识、有效组标识、真实组标识和增补组标识，但不能更改登录用户标识。

使用访问控制表增强用户安全性

要在系统上取得安全性的相应水平，要开发一个一致的安全性策略来管理用户帐户。最常用的安全机制是访问控制表（ACL）。有关 ACL 和开发安全性策略的信息，请参阅第 36 页的『访问控制表』。

PATH 环境变量

PATH 环境变量是一个重要的安全控制。它指定搜索的目录来查找命令。缺省系统范围的 **PATH** 值在 **/etc/profile** 文件中进行指定，而且每个用户通常在自己的 **$HOME/.profile** 文件中都有一个 **PATH** 值。**.profile** 文件中的 **PATH** 值可以将系统范围 **PATH** 值覆盖，或向它添加额外的目录。

对 **PATH** 环境变量的未授权更改可能使得系统中的用户 “欺骗” 其他用户（包括 root 用户）。*电子欺骗*程序（也称为*特洛伊木马*程序）更换了系统命令，然后捕获给该命令的信息，例如用户密码。

例如，假定用户更改 **PATH** 值使系统运行命令时首先查找 **/tmp** 目录。然后该用户在 **/tmp** 目录中放置一个称为 **su** 的程序，该程序就象 **su** 命令一样要求 root 密码。接着，该 **/tmp/su** 程序将 root 密码邮寄给该用户，并在退出前调用 **su** 命令。在这种情况下，任何使用 **su** 命令的 root 用户将暴露 root 密码，而且自己甚至还未意识到。

系统管理员和用户要防止关于 **PATH** 环境变量的任何问题，请执行以下操作:

- 当感到怀疑时，请指定全路径名。如果指定了全路径名，将忽略 **PATH** 环境变量。

- 切勿将当前目录（由 **.** 指定（句点））插入为 root 用户指定的 **PATH** 值中。切勿允许在 **/etc/profile** 中指定当前目录。
- root 用户应当在其私有的 **.profile** 文件中有自己的 **PATH** 规范。通常，**/etc/profile** 中的规范列出了对于所有用户的最少标准，然而 root 用户可能需要比缺省值更多或更少的目录。
- 警告其他用户在没有咨询系统管理员的情况下，不要更改他们的 **.profile** 文件。否则，可信的用户可能做出更改允许无意识的访问。应将用户 **.profile** 文件的许可权设置为 740。
- 系统管理员不应使用 **su** 命令从用户会话中取得 root 用户特权，因为在 **.profile** 文件中指定的该用户 **PATH** 值是有效的。用户可以设置他们自己的 **.profile** 文件。系统管理员应当作为 root 用户或最好使用他们自己的标识登录到用户的机器，然后使用以下命令:

  ```
  /usr/bin/su - root
  ```

  这确保在会话过程中使用 root 环境。如果系统管理员在另一用户会话中以 root 身份操作，则在整个会话中系统管理员应当指定全路径名。
- 保护输入字段分隔符（**IFS**）环境变量以免在 **/etc/profile** 文件中更改。**.profile** 中的 **IFS** 环境变量可以用于修改 **PATH** 值。

设置带有安全用户帐户的匿名 FTP

该方案采用命令行界面和脚本设置带有安全用户帐户的匿名 **ftp**。

注: 该方案不能用在带有 受控的访问保护概要文件（CAPP）和 评估保证级别 4+（EAL4+）功能的系统中。

1. 通过输入以下命令验证 **bos.net.tcp.client** 文件集已安装到您的系统上:

   ```
   lslpp -L | grep bos.net.tcp.client
   ```

   如果没有收到输出，则该文件集未安装。有关如何安装的指示信息，请参阅《*AIX 5L V5.2 安装指南与参考大全*》。
2. 通过输入以下命令验证系统的 **/home** 目录下是否至少有 8 MB 的可用空间:

   ```
   df -k /home
   ```

   步骤 4 中的脚本需要 **/home** 目录下至少有 8 MB 可用空间来安装所需的文件和目录。如果您需要增加可用空间的数量，请参阅《*AIX 5L V5.2 系统管理指南: 操作系统与设备*》。
3. 使用 root 权限，更改为 **/usr/samples/tcpip** 目录。例如:

   ```
   cd /usr/samples/tcpip
   ```
4. 要设置帐户，请运行以下脚本:

   ```
   ./anon.ftp
   ```
5. 当提示确定要修改 /home/ftp? 时，输入 **yes**。输出类似于以下显示:

   ```
   Added user anonymous.
   Made /home/ftp/bin directory.
   Made /home/ftp/etc directory.
   Made /home/ftp/pub directory.
   Made /home/ftp/lib directory.
   Made /home/ftp/dev/null entry.
   Made /home/ftp/usr/lpp/msg/en_US directory.
   ```
6. 更改到 **/home/ftp** 目录。例如:

   ```
   cd /home/ftp
   ```
7. 通过输入以下命令创建 **home** 子目录:

   ```
   mkdir home
   ```

8. 通过输入以下命令将 **/home/ftp/home** 目录的许可权更改为 drwxr-xr-x:

   ```
   chmod 755 home
   ```

9. 通过输入以下命令更改到 **/home/ftp/etc** 目录:

   ```
   cd /home/ftp/etc
   ```

10. 通过输入以下命令创建 **objrepos** 子目录:

    ```
    mkdir objrepos
    ```

11. 通过输入以下命令将 **/home/ftp/etc/objrepos** 目录的许可权更改为 drwxrwxr-x:

    ```
    chmod 775 objrepos
    ```

12. 通过输入以下命令将 **/home/ftp/etc/objrepos** 目录的所有者和组更改为 root 用户和 system 组:

    ```
    chown root:system objrepos
    ```

13. 通过输入以下命令创建 **security** 子目录:

    ```
    mkdir security
    ```

14. 通过输入以下命令将 **/home/ftp/etc/security** 目录的许可权更改为 drwxr-x---:

    ```
    chmod 750 security
    ```

15. 通过输入以下命令将 **/home/ftp/etc/security** 目录的所有者和组更改为 root 用户和 security 组:

    ```
    chown root:security security
    ```

16. 通过输入以下命令更改为 **/home/ftp/etc/security** 目录:

    ```
    cd security
    ```

17. 通过输入以下 SMIT 快速路径来添加用户:

    ```
    smit mkuser
    ```

    在本例中，我们要添加一个名为 test 的用户。

18. 在 SMIT 字段中，输入以下值:

    ```
    用户名                                          [test]
    管理用户?                                        true
    主组                                            [staff]
    组集                                            [staff]
    另一用户可 SU 至用户?                            true
    主目录                                          [/home/test]
    ```

    输入更改之后，按下回车键创建用户。在 SMIT 过程完成后，退出 SMIT。

19. 用以下命令为该用户创建密码:

    ```
    passwd test
    ```

    当提示时，输入期望的密码。必须再一次输入新密码以确认。

20. 通过输入以下命令更改到 **/home/ftp/etc** 目录:

    ```
    cd /home/ftp/etc
    ```

21. 通过输入以下命令复制 **/etc/passwd** 文件到 **/home/ftp/etc/passwd** 文件:

    ```
    cp /etc/passwd /home/ftp/etc/passwd
    ```

22. 使用您喜欢的编辑器，编辑 **/home/ftp/etc/passwd** 文件。例如:

    ```
    vi passwd
    ```

23. 从复制的内容中删除除 root、ftp 和 test 用户以外的所有行。编辑之后，内容看起来应该与以下类似:

    ```
    root:!:0:0::/:/bin/ksh
    ftp:*:226:1::/home/ftp:/usr/bin/ksh
    test:!:228:1::/home/test:/usr/bin/ksh
    ```

24. 保存更改并退出编辑器。
25. 通过输入以下命令将 **/home/ftp/etc/passwd** 文件的许可权更改为 -rw-r--r--:

    ```
    chmod 644 passwd
    ```

26. 通过输入以下命令将 **/home/ftp/etc/passwd** 目录的所有者和组更改为 root 用户和 security 组:

    ```
    chown root:security passwd
    ```

27. 通过输入以下命令将 **/etc/security/passwd** 文件内容复制到 **/home/ftp/etc/security/passwd** 文件:

    ```
    cp /etc/security/passwd /home/ftp/etc/security/passwd
    ```

28. 使用您喜欢的编辑器，编辑 **/home/ftp/etc/security/passwd** 文件。例如:

    ```
    vi ./security/passwd
    ```

29. 从复制的内容中删去除 test 用户之外的所有节。
30. 从 test 用户节中除去 flags = ADMCHG 行。编辑之后，内容看起来应该与以下类似:

    ```
    test:
            password = 2HaAYgpDZX3Tw
            lastupdate = 990633278
    ```

31. 保存更改并退出编辑器。
32. 通过输入以下命令将 **/home/ftp/etc/security/passwd** 文件的许可权更改为 -rw-------:

    ```
    chmod 600 ./security/passwd
    ```

33. 通过输入以下命令将 **/home/ftp/etc/security/passwd** 目录的所有者和组更改为 root 用户和 security 组:

    ```
    chown root:security ./security/passwd
    ```

34. 使用您喜欢的编辑器，编辑 **/home/ftp/etc/security/group** 文件。例如:

    ```
    vi ./security/group
    ```

35. 将以下行添加到文件中:

    ```
    system:*:0:
    staff:*:1:test
    ```

36. 保存更改并退出编辑器。
37. 使用以下命令将相应的内容复制到 **/home/ftp/etc/objrepos** 目录:

    ```
    cp /etc/objrepos/CuAt ./objrepos
    cp /etc/objrepos/CuAt.vc ./objrepos
    cp /etc/objrepos/CuDep ./objrepos
    cp /etc/objrepos/CuDv ./objrepos
    cp /etc/objrepos/CuDvDr ./objrepos
    cp /etc/objrepos/CuVPD ./objrepos
    cp /etc/objrepos/Pd* ./objrepos
    ```

38. 通过输入以下命令更改到 **/home/ftp/home** 目录:

    ```
    cd ../home
    ```

39. 通过输入以下命令为您的用户新建一个主目录:

    ```
    mkdir test
    ```

    这将是新的 ftp 用户的主目录。
40. 通过输入以下命令将 **/home/ftp/home/test** 目录的所有者和组更改为 test 用户和 staff 组:

    ```
    chown test:staff test
    ```

41. 通过输入以下命令将 **/home/ftp/home/test** 文件的许可权更改为 -rwx------:

    ```
    chmod 700 test
    ```

此时，您已经在机器上设置了 ftp 子登录。您可以用以下的过程来测试它。

1. 使用 ftp，连接到您创建 test 用户的主机。例如:

   ```
   ftp MyHost
   ```

2. 以 anonymous 登录。当提示输入密码时，按下回车键。
3. 通过使用以下命令更改至新近创建的 test 用户:

   ```
   user test
   ```

   当提示输入密码时，使用您在步骤 第 33 页的 19 中创建的密码。
4. 使用 pwd 命令来验证用户的主目录是存在的。例如:

   ```
   ftp> pwd
        /home/test
   ```

   输出显示 **/home/test** 作为 **ftp** 子目录。主机上的全路径名称实际上是 **/home/ftp/home/test**。

系统特殊用户帐户

AIX 提供一组缺省的系统特殊用户帐户，以阻止 root 和系统帐户拥有所有操作系统文件和文件系统。

警告: 当除去系统特殊用户帐户时使用警告。您可以通过在 **/etc/security/passwd** 文件相应行的开头插入一个星号（*）来禁用特定帐户。然而，小心不要禁用 root 用户帐户。如果删除了系统特殊用户帐户或禁用了 root 帐户，则操作系统将不能正常运行。

以下帐户在操作系统中预定义:

adm adm 用户帐户拥有以下基本系统功能:

- 诊断，相应的工具存储在 **/usr/sbin/perf/diag_tool** 目录中。
- 记帐，相应的工具存储在以下目录中:
  - **/usr/sbin/acct**
  - **/usr/lib/acct**
  - **/var/adm**
  - **/var/adm/acct/fiscal**
  - **/var/adm/acct/nite**
  - **/var/adm/acct/sum**

bin bin 用户帐户通常拥有大多数用户命令的可执行文件。该帐户的主要用途是帮助分配重要系统目录和文件的所有权，因此所有东西都不是由 root 和 sys 用户帐户单独拥有的。

daemon

daemon 用户帐户只是为了拥有和运行系统服务器进程及其关联的文件而存在。该帐户保证这些进程使用适当的文件访问许可权运行。

nobody

nobody 用户帐户由 “网络文件系统”（NFS）用于启用远程打印。有了这个帐户，程序可以允许对 root 用户的临时 root 访问。例如，在启用 “安全 RPC” 或 “安全 NFS” 之前，请检查主 NIS 服务器上的 **/etc/public** 键以查找还未分配公用密钥和安全密钥的用户。作为 root 用户，您可以为每个未分配的用户在数据库中创建一个项，通过输入:

```
newkey -u username
```

或者，您可以为 nobody 用户帐户在数据库中创建一个项，然后任何用户都可以运行 **chkey** 程序来在数据库中创建它们自己的项而无需作为 root 登录。

root root 用户帐户，即 UID 0，通过该帐户您可以执行系统维护任务和对系统问题进行故障查找。

sys sys 用户拥有缺省的“分布式文件服务”（DFS）高速缓存的安装点，这必须在客户机上安装或配置 DFS 之前存在。**/usr/sys** 目录也可以存储安装映象。

除去不必要的缺省用户帐户

在操作系统安装过程中，会创建许多缺省用户和组标识。根据您在系统上运行的应用程序和系统在网络中所处的位置，其中某些用户和组标识可以成为安全弱点，容易被人利用。如果这些用户和组标识是不必要的，那么您可以将其除去以使跟其有关的安全风险最小化。

下表列出了您可能能够除去最常用的公共缺省用户标识:

表 4. 您可能能够除去的公共缺省用户标识。

用户标识	描述
uucp, nuucp	uucp 协议所用的隐藏文件的所有者。uucp 用户帐户是用于“UNIX 到 UNIX 复制程序”，该程序是在大多数 AIX 系统上存在的一组命令、程序和文件，它们允许用户使用专线或电话线与另一 AIX 系统进行通信。
lpd	打印子系统所使用文件的所有者
imnadm	IMN 搜索引擎（由文档库搜索使用）。
guest	允许那些无权访问帐户的用户访问

下表列出了可能不需要的公共组标识:

表 5. 可能不需要的公共组标识。

组标识	描述
uucp	uucp 和 nuucp 用户所属的组
printq	lpd 用户所属的组
imnadm	imnadm 用户所属的组

分析您的系统以确定哪些标识确实是不需要的。可能也存在其它您可能不需要的用户和组标识。在您的系统投入生产之前，执行可用标识的彻底评估。

访问控制表

访问控制由受保护的信息资源组成，其指定授予谁对这些资源的访问权。操作系统允许需要知晓或自由决定的安全性。信息资源的所有者可以授权其它用户对那些资源的读或写访问权。给予对象访问权的用户可以创建该对象的其它副本并给予第三方该新建对象的访问权。然而，只有对象所有者可以授予第三方原始对象的访问权。只有对象的所有者和 root 用户是可以更改对象的访问权的用户。

用户只有它们自己的对象的基于用户的访问权。通常，用户接收资源的组许可权或缺省许可权。管理访问控制的最主要的任务是定义用户的组员身份，因为这些组员身份决定了用户对不是他们自己的文件的访问权。

访问控制表（ACL）通过添加修改已分配给个人和组的基本许可权的扩展许可权来增加文件访问控制的质量。通过扩展许可权，可以允许或拒绝指定个人或组的文件访问而无需更改基本许可权。

注: 文件的 ACL 大小不能超出一内存页（大约 4096 字节）。

访问控制也涉及使用 **setuid** 和 **setgid** 程序和硬拷贝标签来管理受保护资源。操作系统支持几种类型的信息资源或*对象*。这些对象允许用户处理为存储或通信信息。大多数重要的对象类型如下:

- 文件和目录（用作信息存储）
- 命名管道、消息队列、共享内存段和信号（用作进程间的信息传送）

每个对象有相关的所有者、组以及方式。方式定义所有者、组和其它用户的访问许可权。以下是不同对象类型的直接访问控制属性:

所有者 特定对象的所有者控制其自由决定的访问属性。所有者的属性设置为创建进程的有效用户标识。对于文件系统对象，所有者的直接访问控制属性在没有 root 权限的情况下不能更改。

对 System V 进程间通信（SVIPC）对象，创建者或所有者都可以更改所有者。SVIPC 对象有相关的拥有所有者的所有权限的创建者（包括访问授权）。然而，即使具有 root 权限也不能更改创建者。

组 SVIPC 对象初始化为创建进程的有效组标识。对于文件系统对象，直接访问控制属性初始化为创建进程的有效组标识或父目录的组标识（这是由父目录的组继承标志确定的）。

对象的所有者可以更改组；新组必须为创建进程的有效组标识或父目录的组标识。对象的所有者可以更改组；新组必须为有效组或所有者的当前进程的副组标识中的有效组。（如上所述，SVIPC 对象有不能更改并共享对象组访问授权的相关创建组。）

维护 ACL，请使用 **aclget**、**acledit** 和 **aclput** 命令。

数字方式（用八进制记数法）的 **chmod** 命令可以设置基本许可权和属性。**chmod** 子例程（该命令调用的）禁用扩展许可权。如果对有 ACL 的文件使用 **chmod** 命令的数字方式，则禁用扩展许可权。**chmod** 命令的符号方式不禁用扩展许可权。有关数字方式和符号方式的信息，请参考 **chmod** 命令。

使用 setuid 和 setgid 程序

在多数情况下许可权位机制允许对资源的有效访问控制。但对于更精确的访问控制，操作系统提供了 **setuid** 和 **setgid** 程序。

大部分程序以调用它们的用户的用户和组访问权执行。程序所有者通过使该程序成为 **setuid** 或 **setgid** 程序可以关联调用它们的用户的访问权；就是说，程序在其许可权字段内设置了带有 setuid 或 setgid 位。当进程执行程序时，进程获取程序所有者的访问权。**setuid** 程序使用其所有者的访问权执行，而 **setgid** 程序有其组的访问权，并且两个位都可以根据许可权机制来设置。

虽然进程分配有额外的访问权，这些权限都由具有这些权限的程序控制。因此，**setuid** 和 **setgid** 程序允许间接授予访问权的用户编程的访问控制。程序作为可信子系统，保护用户的访问权。

虽然可以很有效地使用这些程序，如果不小心设计将有安全性风险。特别地，程序在它仍有其所有者的访问权时决不返回控制给用户，因为这样将允许用户无限制地使用所有者的权限。

注: 出于安全性原因，操作系统不支持在 shell 脚本内的 **setuid** 或 **setgid** 调用。

管理访问权

操作系统为系统管理提供特权访问权。系统特权是基于用户和组标识的。带有有效用户或组标识 0 的用户为特权用户。

带有效用户标识 0 的进程称为 root 用户进程，并可以:

- 读写任何对象

- 调用任何系统功能
- 通过执行 **setuid-root** 程序来执行某些子系统控制操作。

可以使用两类特权来管理系统: **su** 命令特权和 **setuid-root** 程序特权。**su** 允许您调用的所有程序具有作为 root 用户进程的功能。**su** 命令使用灵活的方法管理系统，但不是很安全。

使一个程序成为 **setuid-root** 程序意味着该程序是带 setuid 位设置的 root 用户拥有的程序。**setuid-root** 程序提供普通用户不会危及安全性就可以执行的管理功能；将特权封装在程序中而不是直接授权给用户。封装所有必要的管理功能到 **setuid-root** 程序可能比较困难，但是它提供系统管理器更高的安全性。

基本许可权

基本许可权是传统的分配到文件所有者、文件组和其它用户的文件访问方式。访问方式是: 读（r）、写（w）和执行／搜索（x）。

在 ACL 中，基本许可权为以下格式，带有表示为 rwx（将每个没有指定的许可权更换为连字符（-））的 *Mode* 参数:

```
base permissions:
   owner(name): Mode
   group(group): Mode
   others: Mode
```

属性

以下属性可以添加到 ACL:

setuid (SUID)
设置用户标识（Set-user-ID）方式位。该属性在运行时将有效的、已保存过的进程的用户标识设置为文件的所有者标识。

setgid (SGID)
设置组标识（Set-group-ID）方式位。该属性在运行时将有效的、已保存过的进程的组标识设置为文件的组标识。

savetext (SVTX)
对于目录，表示只有文件所有者能链接或取消链接指定目录中的文件。

这些属性以以下格式添加:

```
attributes: SUID, SGID, SVTX
```

扩展许可权

扩展许可权允许文件的所有者更精确地定义该文件的访问权。扩展许可权通过对指定的个人、组或组和用户的组合允许、拒绝或执行访问方式来修改基本文件许可权（所有者、组、其它）。通过使用关键字来修改许可权。

permit、**deny** 和 **specify** 关键字定义如下:

permit 授予用户或组对文件的指定访问权
deny 限制用户或组使用对文件的指定访问权
specify 为用户或组精确地定义文件访问权

如果通过 **deny** 或 **specify** 关键字来拒绝用户特定的访问权，没有任何其它的项可以覆盖该访问拒绝。

要使扩展许可权生效，**enabled** 关键字必须在 ACL 中指定。缺省值为 **disabled** 关键字。

在 ACL 中，扩展许可权为以下格式:

```
extended permissions:
  enabled | disabled
    permit   Mode  UserInfo...:
    deny     Mode  UserInfo...:
    specify  Mode  UserInfo...:
```

每一个 **permit**、**deny** 或 **specify** 项占独立的一行。*Mode* 参数表示成 **rwx**（每个没有指定的许可权用连字符（-）代替）。*UserInfo* 参数表示成 u:UserName 或 g:GroupName 或逗号隔开的 u:UserName 和 g:GroupName 的组合。

> **注**: 如果在一个项中指定多于一个的用户名，该项不能在访问控制判定中使用，因为一个进程只有一个用户标识。

访问控制列表示例

以下为 ACL 的一个示例:

```
attributes: SUID
base permissions:
      owner(frank):  rw-
      group(system): r-x
      others: ---
extended permissions:
      enabled
        permit  rw-  u:dhs
        deny    r--  u:chas, g:system
        specify r--  u:john, g:gateway, g:mail
        permit  rw-  g:account, g:finance
```

ACL 项描述如下:

- 第一行表示打开了 **setuid** 位。
- 下一行介绍了基本许可权，这是可选的。
- 下三行指定基本许可权。在括号内的所有者和组名只是信息。更改这些名称不会改变文件所有者或文件组。只有 **chown** 命令和 **chgrp** 命令可以更改这些文件属性。
- 下一行介绍扩展许可权，这是可选的。
- 下一行表示启用跟随的扩展许可权。
- 最后四行是扩展项。第一个扩展项授予用户 dhs 读（r）和写（w）文件的许可权。
- 第二个扩展项只在 chas 用户为 system 组的成员时拒绝其读（r）访问权。
- 第三个扩展项指定只要用户 john 既是 gateway 组的成员也是 mail 组的成员，则他就拥有读（r)访问权。如果用户 john 不是这两个组的成员，此扩展许可权不适用。
- 最后一个扩展项授予在 account 组和 finance 组*两个*组中的任何用户读（r）和写（w）许可权。

> **注**: 对请求访问受控对象的进程可适用多于一个扩展项，限制项优先于允许方式。

有关全部语法，请参阅《*AIX 5L V5.2 命令参考大全*》中的 **acledit** 命令。

访问授权

信息资源的所有者对管理访问权负责。资源是受*许可权位*保护的，许可权位包含在对象的方式中。许可权位定义授权给对象所有者、对象组和 others 缺省类的访问许可权。操作系统支持可独立授权的三种不同的访问方式（读、写和执行）。

当用户登录到帐户（使用 **login** 或 **su** 命令）时，关联分配到该帐户的用户标识和组标识到用户进程。这些标识确定进程的访问权。

对于文件、目录、命名管道和设备（特定文件），访问授权如下:

- 对于 ACL 中的每个访问控制项（ACE），标识列表与进程标识相比较。如果匹配，进程接受该项定义的许可权和限制。许可权和限制的逻辑并集是从 ACL 的每个匹配项计算的。如果请求进程没有匹配在 ACL 中的任何项，它接受缺省项的许可权和限制。
- 如果请求的访问方式为许可（包含在许可权并集中）且不是限制（包含在限制并集中），则授权访问。否则，拒绝访问。

具有用户标识 0 的进程称为 *root 用户进程*。这些进程通常允许所有访问许可权。但是如果 root 用户进程请求执行程序的许可权，只有在执行许可权授权到至少一个用户时才授权访问。

如果在表中的所有标识匹配请求进程相应类型的有效标识，则 ACL 的标识列表匹配进程。如果用户类型标识与进程中的有效用户标识相同则用户类型标识匹配，如果组类型标识与进程中的有效组标识或增补组标识之一相同则组类型标识匹配。例如，带有如下的标识列表的 ACE:

```
USER:fred, GROUP:philosophers, GROUP:software_programmer
```

将匹配带有有效用户标识为 fred 和组设置如下的进程:

```
philosophers, philanthropists, software_programmer, doc_design
```

但是不匹配带有有效用户标识 fred 和组设置如下的进程:

```
philosophers, iconoclasts, hardware_developer, graphic_design
```

注意，带有以下标识列表的 ACE 将匹配两个进程:

```
USER:fred, GROUP:philosophers
```

换句话说，ACE 功能中标识列表是必须为要授予的指定访问权保留的状态集。

当对象第一次访问时，在系统调用级别上进行这些对象的所有访问许可权检查。因为 System V 进程间通信（SVIPC）对象无状态访问，所以对每一个访问做检查。对于带有文件系统名称的对象，必须能够解析实际对象的名称。名称解析可以是相对的（相对于进程工作目录），也可以是绝对的（相对于进程根目录）。所有名称解析通过搜索这些目录的其中之一开始。

自由决定的访问控制机制允许信息资源的有效访问控制并提供对信息的机密性和完整性的独立保护。所有者控制的访问控制机制仅按照用户的要求有效。所有用户必须知道访问许可权如何授权和拒绝以及这些是如何设置的。

密码

猜测密码是系统最常遇到的攻击方法之一。因此，控制和监视您的密码限制策略是不可缺少的。AIX 提供机制以帮助您实施更强的密码策略，例如为以下的项建立值:

- 密码可被更改之前和之后可经过的最小和最大星期数
- 密码的最小长度

- 选择密码时，最小可使用的字母字符个数

本节讨论 AIX 如何存储和处理密码，以及您如何建立较强的密码策略。本节中的主题包括:

- 『设定良好的密码』
- 『使用 /etc/passwd 文件』
- 第 42 页的『使用 /etc/passwd 文件和网络环境』
- 第 42 页的『隐藏用户名和密码』
- 第 43 页的『设置推荐的密码选项』
- 第 44 页的『扩展密码限制』

设定良好的密码

良好的密码是抵御未授权进入系统的第一道有效防线，它们是以下类型:

- 大小写字母的混合
- 字母、数字或标点符号的组合。此外，它们可以包含特殊字符，如 `~!@#$%^&*()-_=+[]{}|\;:'",.<>?/< 空格>`
- 未写在任何地方
- 如果使用 **/etc/security/passwd** 文件，那么长度最少为 7 个字符最大 8 个字符（象 LDAP 那样使用注册表实施的认证，可以使用超出此最大长度的密码）。
- 不是在字典中可查到的真实单词
- 不是键盘上字母的排列模式，比如 *qwerty*
- 不是真实单词或已知排列模式的反向拼写
- 不包含任何与您自己、家庭或朋友有关的个人信息
- 不与从前一个密码的模式相同
- 可以较快输入，这样边上的人就不能确定您的密码

除了这些机制，您可以通过限定密码不可以包含可能猜测到的标准 UNIX 单词，从而进一步实施更严格的规则。该功能使用 **dictionlist**，它要求您首先安装 **bos.data** 和 **bos.txt** 文件集。

要实现前面定义的 **dictionlist**，请编辑 **/etc/security/users** 文件中的以下行:

```
dictionlist = /usr/share/dict/words
```

/usr/share/dict/words 文件使用 **dictionlist** 来防止使用标准 UNIX 单词作为密码。

使用 /etc/passwd 文件

传统上，**/etc/passwd** 文件是用来记录每个拥有系统访问权的注册用户。**/etc/passwd** 文件以冒号分隔，它包含以下信息:

- 用户名
- 已加密密码
- 用户标识号（UID）
- 用户的组标识号（GID）
- 用户全名（GECOS）
- 用户主目录
- 登录 shell

以下是一个 **/etc/passwd** 文件的示例:

```
root:!:0:0::/:/usr/bin/ksh
daemon:!:1:1::/etc:
bin:!:2:2::/bin:
sys:!:3:3::/usr/sys:
adm:!:4:4::/var/adm:
uucp:!:5:5::/usr/lib/uucp:
guest:!:100:100::/home/guest:
nobody:!:4294967294:4294967294::/:
lpd:!:9:4294967294::/:
lp:*:11:11::/var/spool/lp:/bin/false
invscout:*:200:1::/var/adm/invscout:/usr/bin/ksh
nuucp:*:6:5:uucp login user:/var/spool/uucppublic:/usr/sbin/uucp/uucico
imnadm:*:188:188::/home/imnadm:/usr/bin/ksh
paul:!:201:1::/home/paul:/usr/bin/ksh
jdoe:*:202:1:John Doe:/home/jdoe:/usr/bin/ksh
```

缺省情况下，AIX 没有象 UNIX 系统那样将加密密码存储在 **/etc/password** 文件内，而是在缺省情况下存储在 **/etc/security/password** 文件（仅 root 用户可读）内。AIX 使用 **/etc/passwd** 中归档的密码来表示密码是否存在或帐户是否被阻止。

/etc/passwd 文件由 root 用户拥有，且必须对所有用户都是可读的，但只有 root 用户有写许可权，显示为 `-rw-r--r--`。如果用户标识具有密码，则该密码字段中会有一个 `!`（感叹号）。如果用户标识没有密码，则该密码字段中有一个 `*`（星号）。加密的密码存储在 **/etc/security/passwd** 文件中。以下示例包含 **/etc/security/passwd** 文件（基于以上所示的 **/etc/passwd** 文件的项）中的最后四个项。

```
guest:
        password = *

nobody:
        password = *

lpd:
        password = *

paul:
        password = eacVScDKri4s6
        lastupdate = 1026394230
        flags = ADMCHG
```

用户标识 `jdoe` 在 **/etc/security/passwd** 文件中没有项，因为它在 **/etc/passwd** 文件中没有设置密码。

可使用 **pwdck** 命令来检查 **/etc/passwd** 文件的一致性。**pwdck** 命令通过检查全部用户或指定用户的定义来验证用户数据库文件中密码信息的正确性。

使用 /etc/passwd 文件和网络环境

在传统的网络环境中，用户必须在每个系统中有一个帐户才能获得对该系统的访问权。这通常意味着用户要在每个系统上的每个 **/etc/passwd** 文件中有一个项。然而，在分布式环境中，要确保每个系统都有相同的 **/etc/passwd** 文件不是件容易的事情。要解决这个问题，有若干种方法（包括网络信息系统（NIS）和 NIS+）可以使 **/etc/passwd** 文件中的信息在整个网络中可用。

有关 NIS 和 NIS+ 的更多信息，请参阅第 183 页的第 12 章，『网络信息服务（NIS）和 NIS+ 安全』。

隐藏用户名和密码

为了达到更高级别的安全性，请确保用户标识和密码在系统内是不可见的。**.netrc** 文件包含用户标识和密码。该文件未进行加密或编码保护，这样它的内容象纯文本一样清楚显示。要查找这些文件，运行以下命令:

```
# find `awk -F: '{print $6}' /etc/passwd` -name .netrc -ls
```

找到这些文件后，请删除它们。保存密码的一个更有效的方法是设置 Kerberos。有关 Kerberos 的更多信息，请参阅第 205 页的第 15 章，『Kerberos』。

设置推荐的密码选项

恰当的密码管理只有通过用户教育来实现。为提供某些额外的安全性，操作系统提供了可配置的密码限制。它们允许管理员限制用户选择的密码，并强制定期更改密码。密码选项和扩展用户属性位于 **/etc/security/user** 文件中，此文件是包含用户属性节的 ASCII 文件。每当为用户定义新密码时，这些限制就会执行。所有密码限制都是按照用户来定义的。通过在 **/etc/security/user** 文件的缺省节中保存限制，对所有用户执行相同限制。为了维护密码安全性，所有密码必须受到相似的保护。

管理员还可以扩展密码限制。使用 **/etc/security/user** 文件中的 **pwdchecks** 属性，管理员可以将新的子例程（称为*方法*）添加到密码限制代码中。这样，本地站点策略可添加到操作系统，并由操作系统执行该策略。有关更多信息，请参阅第 44 页的『扩展密码限制』。

应用密码限制要切合实际。过于限制的尝试，比如限制密码空间（这将使猜测密码更容易），或强制用户选择难以记忆的密码（用户可能选择会写下密码），都会危及密码安全性。密码安全性最终要依靠用户。简单的密码限制结合合理的指导和偶尔的审查（以验证当前密码是否唯一）是最好的策略。

下表列出与 **/etc/security/user** 文件中用户密码相关的一些安全属性的推荐值。

表 6. 用户密码的推荐安全属性值。

属性	描述	推荐值	缺省值	最大值
dictionlist	验证密码不包含标准 UNIX 单词。	**/usr/share/dict/words**	不适用	不适用
histexpire	密码可重新使用前的星期数。	26	0	260[注 1]
histsize	可允许的密码重复次数。	20	0	50
maxage	必须更改密码前的最大星期数。	8	0	52
maxexpired	超过 *maxage* 后可由用户更改到期密码的最大星期数。（root 用户例外。）	2	-1	52
maxrepeats	在密码中可重复字符的最大数目。	2	8	8
minage	密码可被更改前的最小星期数。不应设置此项为非零值，除非总是能很容易联系到管理员来对一个最近更改过的、意外泄密的密码进行重新设置。	0	0	52
minalpha	密码必须包含字母字符的最小数目。	2	0	8
mindiff	密码必须包含唯一字符的最小数目。	4	0	8

表 6. 用户密码的推荐安全属性值。 (续)

属性	描述	推荐值	缺省值	最大值
minlen	密码长度的最小值。	6（对 root 用户是 8）	0	8
minother	密码必须包含非字母字符的最小数目。	2	0	8
pwdwarntime	系统发出要求更改密码警告前的天数。	5	不适用	不适用
pwdchecks	通过使用一个检查密码质量的定制代码，该项可用来增强 **passwd** 命令。	有关更多信息，请参阅『扩展密码限制』。	不适用	不适用

注:

1. 最多保留 50 个密码。

对于受控访问保护概要文件和评定保证级别 4+（CAPP/EAL4+）系统，请使用第 13 页的『用户与端口配置』中推荐的值。

如果在系统上安装了文本处理程序，管理员可以使用 **/usr/share/dict/words**文件作为 **dictionlist** 字典文件。在这种情况下，管理员可以设置 **minother** 属性为 0。这是因为字典文件中的大多数单词不包含属于 **minother** 属性类别中的字符，把 **minother** 属性设置为 1 或更大将消除对这个字典文件中绝大多数单词的需要。

系统中密码的最小长度由 **minlen** 属性的值或 **minalpha** 属性的值中的较大者加上 **minother** 属性来设置。密码的最大长度是八个字符。**minalpha** 属性的值加上 **minother** 属性的值决不能大于 8。如果 **minalpha** 的值加上 **minother** 属性的值大于 8，则 **minother** 属性的值会减少为 8 减去 **minalpha** 属性的值。

如果 **histexpire** 属性的值和 **histsize** 属性的值都设置了，则系统保留适用于两种情况所需的密码个数，最多达系统所限制的每个用户 50 个密码。不保留空密码。

您可以编辑 **/etc/security/user** 文件，使之包含您要用来管理用户密码的任何缺省值。或者，您也可以通过使用 **chuser** 命令更改属性值。

其它可以与该文件一起使用的命令有 **mkuser**、**lsuser** 和 **rmuser** 命令。**mkuser** 命令为 **/etc/security/user** 文件中的每个新建用户创建一个项，并用 **/usr/lib/security/mkuser.default** 文件中定义的属性初始化该项的属性。要显示属性和它们的值，请使用 **lsuser** 命令。要除去一个用户，请使用 **rmuser** 命令。

扩展密码限制

密码程序接受或拒绝密码所使用的规则（密码构成限制）可由系统管理员进行扩展，以提供特定于站点的限制。通过添加方法（在更改密码过程中调用）来扩展限制。**/etc/security/user** 文件中的 **pwdchecks** 属性指定调用的方法。

AIX 5L Version 5.2 Technical Reference 包含对 **pwdrestrict_method** 的描述，它是指定的密码限制方法必须符合的子例程接口。要正确扩展密码构成限制，则系统管理员必须在编写密码限制方法时对该接口编程。请谨慎对待扩展密码设置限制。这些扩展将直接影响 **login** 命令、**passwd** 命令、**su** 命令以及其它程序。系统安全性可能被恶意的或有缺陷的代码轻易破坏。

用户认证

识别和认证建立用户身份。要求每一个用户登录到系统中。如果帐户有用户名称的话（安全系统中，所有帐户必须有密码，否则无效），用户提供帐户的用户名称和密码。如果密码正确，用户登录到该帐户；用户获取帐户的访问权限和特权。**/etc/passwd** 和 **/etc/security/passwd** 文件维护用户密码。

采用出现在 **/etc/security/user** 中的 **SYSTEM** 属性把认证的备用方法集成在系统中。例如，“分布式计算环境”（DCE）需要密码认证，但是以与 **etc/passwd** 和 **/etc/security/passwd** 中使用的加密模型不同的方式验证这些密码。通过 DCE 认证的用户可以将 **/etc/security/user** 中他们的节设置为 SYSTEM=DCE。

其它 **SYSTEM** 属性值是 **compat**、**files** 和 **NONE**。当名称解析（和后继认证）遵循本地数据库时，使用 **compat** 标记，而且如果找不到解析时，就尝试“网络信息服务”（NIS）数据库。**files** 标记指定认证过程中只能使用本地文件。最后，**NONE** 标记关闭方法认证。为了关闭所有的认证，**NONE** 标记必须出现在用户节的 **SYSTEM** 和 **auth1** 行。

可以在 **/usr/lib/security/methods.cfg** 中定义 **SYSTEM** 属性的其它可接受标记。

注: 总是采用本地系统安全文件的方式认证 root 用户。root 用户的 **SYSTEM** 属性项在 **/etc/security/user** 中被特别设置为 **SYSTEM = "compat"**。

有关保护密码的更多信息，请参阅 *《AIX 5L V5.2 系统用户指南: 操作系统与设备》*。

登录用户标识

为该用户记录的所有审计事件都标有此标识，而且当您生成审计记录时可以进行检查这些事件。关于登录用户标识的更多信息，请参阅 *《AIX 5L V5.2 系统用户指南: 操作系统与设备》*。

磁盘配额系统概述

系统管理员使用磁盘配额系统控制可以分配给用户或组的文件和数据块的数目。下面部分提供了有关磁盘配额系统、它的实现以及使用的进一步信息:

- 『理解磁盘配额系统』
- 第 46 页的『从超配额情形中恢复』
- 第 46 页的『设置磁盘配额系统』

理解磁盘配额系统

该磁盘配额系统基于 Berkeley 磁盘配额系统，它提供了控制磁盘空间使用的有效方式。可以为个人用户或组定义配额系统，并为每个日志文件系统维护配额系统。

磁盘配额系统基于以下参数建立配额，可以使用 **edquota** 命令更改这些参数:

- 用户或组的软配额
- 用户或组的硬配额
- 配额宽延时间

*软配额*定义了在此限定下用户必须保留的 1 KB 的磁盘块数或文件数。*硬配额*定义了在已建立的磁盘配额下用户可以累积的最大磁盘块或文件数量。*配额宽延时间*允许用户在短期内（缺省值是一周）超过软配额。如果在特定的时间内用户不能把使用空间降低到软配额以下，系统会把软配额解释为最大允许的分配，而不再给用户分配更多存储空间。通过除去足够的文件把使用空间减小到软配额以下，用户可以复位此条件。

磁盘配额系统在 **quota.user** 和 **quota.group** 文件中跟踪用户和组的配额，这些文件位于已启用配额的文件系统根目录下。这些文件使用 **quotacheck** 和 **edquota** 命令创建并可以用配额命令读取。

从超配额情形中恢复

在超过配额限制时为了减小文件系统使用，可以使用以下方法:

- 杀死致使文件系统达到配额的当前进程，除去过剩的文件使限制低于配额，并重试失败的程序。
- 如果正在运行编辑器（比如 vi），使用 shell 转义序列检测文件空间，除去多余文件，则不丢失已编辑文件而返回。或者，如果正在使用 C 或 Korn shell，可以用 Ctrl-Z 按键顺序暂挂编辑器，发出文件系统命令，然后用 **fg**（前台）命令返回。
- 暂时把文件写入没有超过配额限制的文件系统中，删除多余的文件，然后把文件返回到正确的文件系统中。

设置磁盘配额系统

通常，只有包含用户主目录和文件的那些文件系统才需要磁盘配额。考虑在以下条件下实现磁盘配额系统:

- 系统磁盘空间有限。
- 需要更高的文件系统安全性。
- 磁盘使用程度很高，例如在许多大学。

如果这些条件不适用于您的环境，您可能不希望执行磁盘配额系统以创建磁盘使用限制。

磁盘配额系统只能与日志文件系统一起使用。

注: 不要为 **/tmp** 文件系统创建磁盘配额。

使用以下步骤设置磁盘配额系统:

1. 用 root 权限登录。
2. 确定哪些文件系统需要配额。

   注: 由于在 **/tmp** 文件系统中许多编辑器和系统实用程序创建临时文件，因此它必须没有配额。
3. 使用 **chfs** 命令包含 **/etc/filesystems** 文件中的 **userquota** 和 **groupquota** 配额配置属性。以下示例使用 **chfs** 命令启用 **/home** 文件系统中的用户配额:

   ```
   chfs -a "quota = userquota" /home
   ```

   要启用 **/home** 文件系统的用户和组配额，输入:

   ```
   chfs -a "quota = userquota,groupquota" /home
   ```

   /etc/filesystems 文件中的相应项显示如下:

   ```
   /home:
   dev         = /dev/hd1
   vfs         = jfs
   log         = /dev/hd8
   mount       = true
   check       = true
   quota       = userquota,groupquota
   options     = rw
   ```
4. 指定备用磁盘配额文件名称（可选）。**quota.user** 和 **quota.group** 文件名称是缺省名称，在已启用配额的文件系统的根目录下。可以用 **/etc/filesystems** 文件中的 **userquota** 和 **groupquota** 属性为这些配额文件指定备用名称或目录。

以下示例使用 **chfs** 命令为 **/home** 文件系统创建用户和组配额，并且给 **myquota.user** 和 **myquota.group** 配额文件命名:

```
chfs -a "userquota = /home/myquota.user" -a "groupquota = /home
        /myquota.group" /home
```

/etc/filesystems 文件中的相应项显示如下:

```
/home:
dev         = /dev/hd1
vfs         = jfs
log         = /dev/hd8
mount       = true
check       = true
quota       = userquota,groupquota
userquota   = /home/myquota.user
groupquota  = /home/myquota.group
options     = rw
```

5. 如果以前没有安装它们，请安装指定的文件系统。
6. 为每一个用户或组设置希望的配额限制。使用 **edquota** 命令为每一个用户或组的允许磁盘空间和最大文件数量创建软配额和硬配额。

   以下示例项显示 *davec* 用户的配额限制:

   ```
   Quotas for user davec:
   /home: blocks in use: 30, limits (soft = 100, hard = 150)
           inodes in use: 73, limits (soft = 200, hard = 250)
   ```

   该用户已经使用了 100 KB 最大磁盘空间中的 30 KB。*davec* 已经创建了最多 200 个文件中的 73 个。该用户有 50 KB 磁盘空间和 50 个文件缓冲可分配作临时存储。

   当为多个用户建立磁盘配额时， 使用带 **-p** 标志的 **edquota** 命令为另一用户复制用户的配额。

   要为用户 *nanc* 复制已为用户 *davec* 建立的配额，请输入:

   ```
   edquota -p davec nanc
   ```

7. 用 **quotaon** 命令启用配额系统。**quotaon** 命令启用指定文件系统的配额，或在使用 **-a** 标志时为带有配额的所有文件系统（如 **/etc/filesystems** 文件中指定的）启用配额。
8. 使用 **quotacheck** 命令检测配额文件对于实际磁盘使用率的一致性。

   注: 建议您在每次文件系统首次启用配额时，以及每次重新引导系统之后执行此操作。

   要在系统启动过程中启用此检测并打开配额，在 **/etc/rc** 文件的结尾添加以下行:

   ```
   echo " Enabling filesystem quotas "
   /usr/sbin/quotacheck -a
   /usr/sbin/quotaon -a
   ```

第 3 章 审计

审计启用系统管理员来记录安全性相关的信息，可分析该信息来检测对系统安全性策略潜在和实际的违背。

本节讨论以下主题:

- 『审计子系统』
- 第 50 页的『事件选择』
- 第 51 页的『审计子系统配置』
- 第 52 页的『审计日志程序配置』
- 第 55 页的『设置审计』

审计子系统

审计子系统有以下功能:

- 『检测事件』
- 『收集事件信息』
- 第 50 页的『处理审计跟踪信息』

系统管理员可以配置这些功能的每一项。

检测事件

事件检测分布遍及整个可信计算库（TCB），既在内核（管理状态码）又在可信程序（用户状态码）中。在系统中发生的任何安全性相关的事件为可审计的事件。安全性相关发生是指任何系统安全性状态的更改、任何系统访问控制或责任安全策略的试图或实际的违例、或两者都是。检测可审计的事件的程序和内核模块负责报告这些事件到系统审计日志程序，它作为内核的一部分运行并可由子例程（对于可信程序审计）或在内核过程调用中（对监督状态审计）访问。报告的信息包含可审计事件的名称、该事件的成功与失败，以及任何附加的跟安全性审计有关的特定事件的信息。

事件检测配置包含打开或关闭事件检测，以及指定要审计哪个用户的哪个事件。激活事件检测，使用 **audit** 命令来启用或禁用审计子系统。**/etc/security/audit/config** 文件包含审计子系统处理的事件和用户。

收集事件信息

信息收集围绕记录选定的可审计事件。此功能由内核审计日志程序执行，内核审计日志程序提供了系统调用和记录可审计的事件的内部内核过程调用界面。

审计日志程序有责任构造完整的审计记录，由审计标题和审计跟踪组成。标题包含所有事件公用的信息（比如事件名、需负责任的用户、时间和事件的返回状态），审计跟踪包含特定事件的信息。审计日志程序将每个连续记录追加到内核审计跟踪，这可以用两种方式之一（或两者）来写:

BIN 方式
: 跟踪写入交互的文件，提供安全和长期的存储。

STREAM 方式
: 跟踪写入循环缓冲区，缓冲区通过审计伪设备同步读取。STREAM 方式提供快速响应。

可在前端（事件记录）和后端（跟踪处理）配置信息收集。事件记录在每个用户基础上是可选的。每个用户有当事件发生时登录到审计跟踪的审计事件的定义设置。在后端，逐个地配置此方式，以便管理员能使用最适合特定环境的后端处理。另外，可将 BIN 方式审计可以配置为在跟踪的可用文件系统空间太小时，生成警告。

处理审计跟踪信息

操作系统提供几种处理内核审计跟踪的选项。BIN 方式跟踪可以在审计跟踪归档存储前压缩、过滤、格式化输出、或任何这些的合理的组合（如果有的话）。通过 Huffman 编码压缩。通过类标准查询语言（SQL）审计记录选择来过滤（使用 **auditselect** 命令），该选择为选择查看和选择审计跟踪保留时间提供。审计跟踪记录格式化可以用来检查审计跟踪、生成定期安全性报告以及打印纸上的审计跟踪。

可实时监视 STREAM 方式审计跟踪，从而提供快速威胁监视能力。这些选项的配置由可作为用来过滤 BIN 或 STREAM 方式跟踪的守护程序进程调用的独立程序处理，虽然某些过滤程序更适合于某种方式或另一种。

事件选择

系统上的可审计事件设置定义了实际可审计的事件以及审计提供的粒度。如先前定义的，可审计事件必须涵盖系统上的安全性相关事件。用来定义可审计事件的详细信息级别必须在非足够详细信息（使管理员难于理解选定的信息）和足够详细信息（导致过多的信息收集）间维持平衡。利用检测事件的相似性来定义事件。对于此讨论的目的，*检测事件*是任何单个的可审计事件的实例；例如，可在不同的地方检测到给定的事件。基础原则为：选定有类似安全性属性的检测事件为相同的可审计事件。以下列表显示安全性策略事件的分类:

- 主题事件
  - 进程创建
  - 进程删除
  - 设置主题安全性属性：用户标识、组标识
  - 进程组、控制终端
- 对象事件
  - 对象创建
  - 对象删除
  - 对象打开（包括作为对象的进程）
  - 对象关闭（包括作为对象的进程）
  - 设置对象安全性属性：所有者、组、ACL
- 导入／导出事件
  - 导入或导出对象
- 责任事件
  - 在密码数据库中添加用户，更改用户属性
  - 在组数据库中添加组，更改组属性
  - 用户登录
  - 用户注销
  - 更改用户认证信息
  - 可信路径终端配置
  - 认证配置
  - 审计管理：选择事件和审计跟踪、转换打开或关闭、定义用户审计类
- 常规系统管理事件

  - 特权使用
  - 文件系统配置
  - 设备定义和配置
  - 系统配置参数定义
  - 正常系统 IPL 和关闭
  - RAS 配置
  - 其它系统配置
- 安全性违背（潜在的）
  - 访问许可权拒绝
  - 特权失败
  - 诊断检测故障和系统错误
  - 尝试变更 TCB

审计子系统配置

审计过程子系统有一个表示审计过程子系统是否打开的全局状态变量。另外，每个进程有一个表示审计过程子系统是否应该记录此进程信息的本地状态变量。这两种变量确定了是否用可信计算库（TCB）和程序来检测事件。关闭指定进程的 TCB 审计允许此进程做它自己的审计并且不忽略系统责任策略。允许可信程序自身审计允许更有效率和有效的信息收集。

收集审计子系统信息

信息收集有**事件选择**和**内核审计跟踪**两种方式。通过提供登录信息界面（检测可查的事件的 TCB 组成部分使用的）和配置界面（审计过程子系统用来控制审计记录例程的）是由内核例程完成的。

审计记录

可审计事件通过以下界面记录: 用户状态和超级用户状态。TCB 的用户状态部分使用 **auditlog** 或 **auditwrite** 子例程，而 TCB 的超级用户状态部分使用内核过程集调用。

对每个记录，审计事件日志程序附加审计报头为指定事件信息的前缀。此报头标识审计此事件用户和进程以及事件发生的时间。检测事件的代码提供事件类型并返回代码或状态以及可选的、额外的特定事件信息（事件跟踪）。特定事件信息包含对象名（例如，拒绝访问的文件或在失败的登录试图中使用的 tty）、子例程参数和其它修改的信息。

象征性地定义事件而不是用数字定义。在不使用事件注册方案时，这减少了名称冲突的可能。由于子例程是可审计的并且可扩展的内核定义没有固定的交换型虚拟电路（SVC）号，要用数字记录事件很困难。必须校对数字映射并记录每一次的内核界面扩展或重定义。

审计记录格式

审计记录由公共报头、跟有指定记录的审计事件的审计跟踪构成。在 **/usr/include/sys/audit.h** 文件中定义报头的结构。审计跟踪中的信息格式对于每个基本事件是特定的，并显示在 **/etc/security/audit/events** 文件中。

通常在审计报头中的信息由登录例程来收集以确保它的准确性，而在审计跟踪中的信息是由检测事件的代码提供的。审计日志程序并没有结构化的信息或审计跟踪的语义。例如，当 **login** 命令检测到失败登录时，它记录

在其发生的终端上的指定事件并使用 **auditlog** 子例程将记录写入审计跟踪。审计日志程序内核组件记录指定主题信息（用户标识、进程标识、时间）到报头并追加其到另外的信息。调用程序仅提供事件名称和在报头中的结果字段。

审计日志程序配置

审计日志程序负责构造完整的审计记录。必须选择想要记录的审计事件。

选择审计事件

审计事件选择有以下类型:

每个进程审计

要有效地选择进程事件，系统管理员可以定义审计类。审计类是系统中的基本审计事件的子集。审计类提供基本审计事件方便的逻辑分组。

对系统上的每个用户，系统管理员定义确定可为该用户记录的基本事件的审计类集。用户运行的每个进程标记有其审计类。

每个对象审计

操作系统提供通过名称访问对象的审计；就是说，指定对象（通常是文件）的审计。按名称的对象审计防止必须涵盖所有对象访问以审计几乎没有的相关对象。另外，可以指定审计方式，以便只记录指定方式（读 / 写 / 执行）的访问。

内核审计跟踪方式

内核记录可设置为 BIN 或 STREAM 方式以定义内核审计跟踪要写入哪里。如果使用 BIN 方式，内核审计日志程序（在启动审计前）必须给定至少一个文件描述符，记录追加于此。

BIN 方式包含写审计记录到备用文件。在审计过程启动时，内核发送两个文件描述符和一个建议的最大 bin 大小。它暂挂调用进程并开始将审计记录写到第一个文件描述符。当第一个 bin 的大小达到最大 bin 大小时，且如果第二个文件描述符有效，它切换至第二个 bin 并重新激活调用进程。内核继续写到第二个 bin 直至用另一个有效的文件描述符再次调用。如果此时第二个 bin 满了，它切换回第一个 bin 并且调用进程立即返回。否则，暂挂调用进程并且内核继续写记录到第二个 bin 直到满为止。以此方式继续处理直到关闭审计过程。请参阅下图审计 BIN 方式的说明:

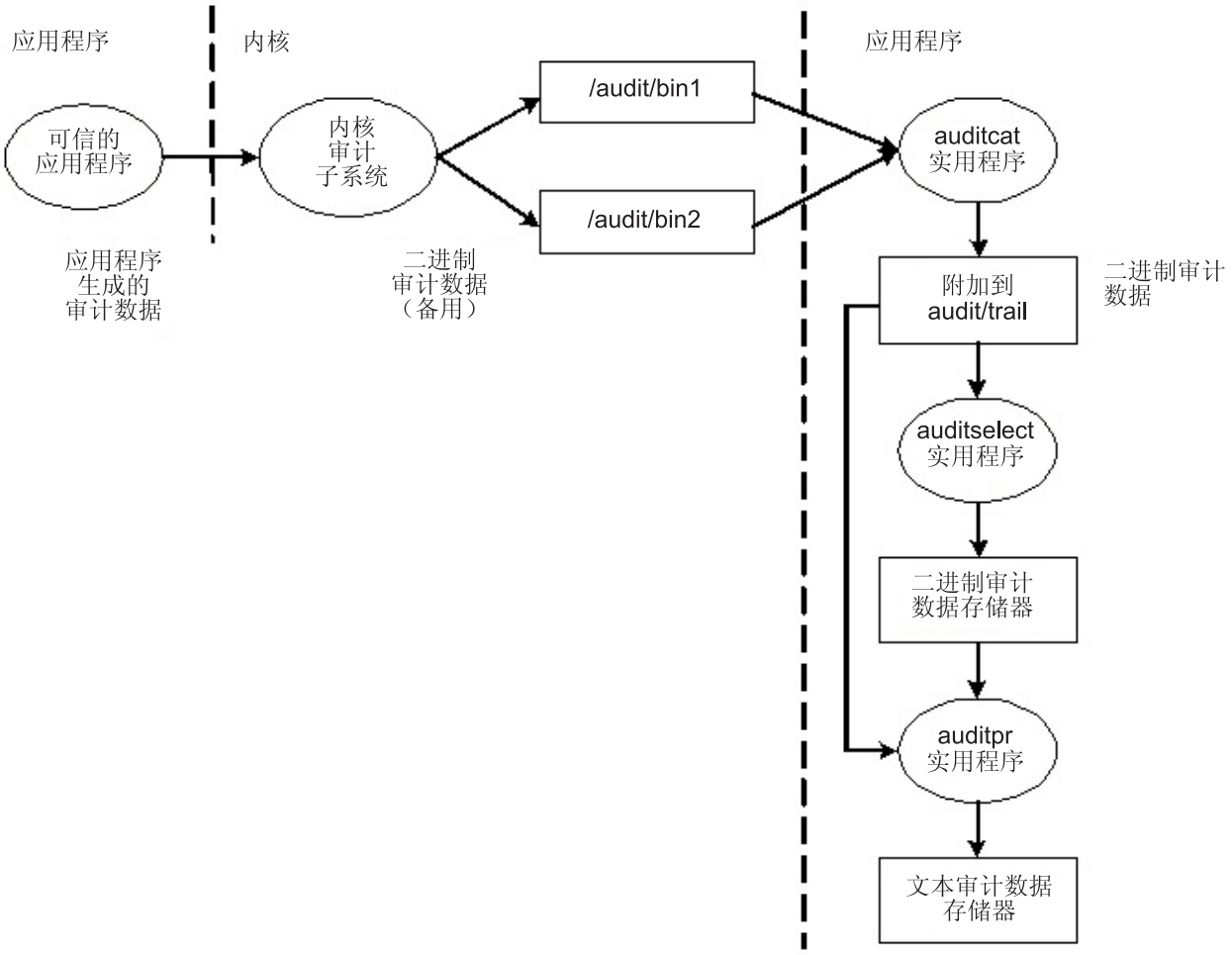


图 1. 审计 BIN 方式的过程。. 此说明显示了审计 BIN 方式的过程。

交互的 bin 机制用来确保在处理审计记录时审计子系统总有某些东西要写。当审计子系统切换至另一个 bin 时，它清空第一个 bin 的内容到**跟踪**文件。当又切换到此 bin 时，第一个 bin 已经可用了。它使数据生成的数据存储和分析分离。通常，**auditcat** 程序用来从此刻内核没有写入的 bin 读取数据。确保系统从不由于审计跟踪（**auditcat** 程序的输出）而空间耗尽，可以在 **/etc/security/audit/config** 文件中指定 **freespace** 参数。如果系统拥有小于此处指定的 512 位的块数，则它生成 **syslog** 消息。

如果启用审计，在 **/etc/security/audit/config** 中的 **start** 节中的 **binmode** 参数应该设成 **panic**。在 **bin** 节中的 **freespace** 参数应该配置成最小为磁盘空间的 25% 来存储审计跟踪。每个 **bytethreshold** 和 **binsize** 参数应该设置为 65536 字节。

在 STREAM 方式中，内核写记录到循环缓冲区。当内核达到缓冲区的限制时，它只是绕回开头。进程从名为 **/dev/audit** 的伪设备读取信息。当进程打开此设备时，就为该进程创建了一个通道。作为选择，可以将在通道上读取的事件指定为审计类的列表。请参阅下图审计 STREAM 方式的说明:

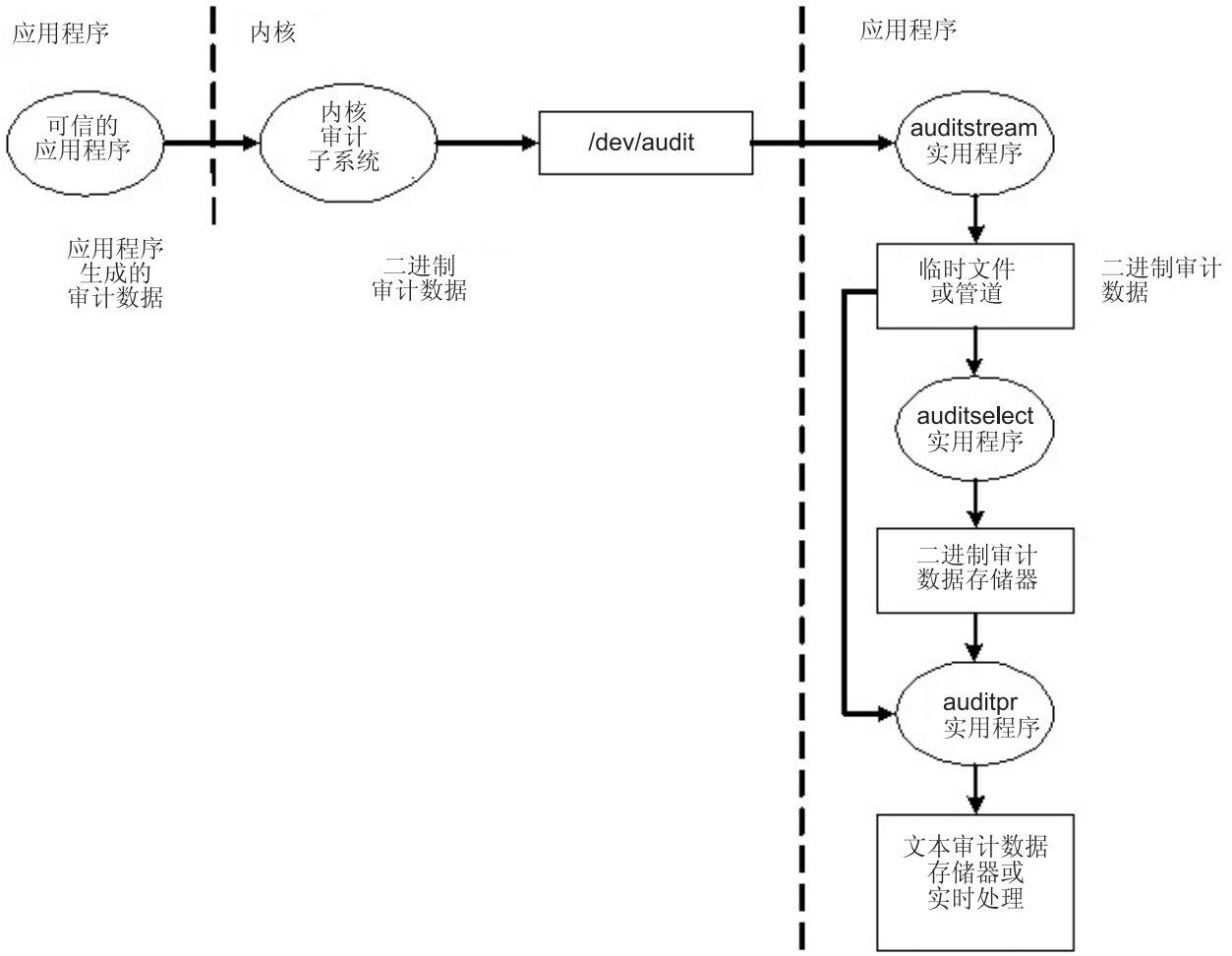


图 2. 审计 STREAM 方式的过程. 此说明显示了审计 STREAM 方式的过程。

STREAM 方式的主要目的是允许及时地读取审计跟踪，这可用来实时威胁监视。另一个用途是创建即时写的跟踪来防止任何可能的对审计的篡改（如果跟踪存储在某些可写介质上，这是可能的）。

还有一个使用 STREAM 的方法是把审计流写到在远程系统上存储审计信息的程序，这允许中央近时处理，而且同时防止审计信息在源主机的篡改。

处理审计记录

auditselect、**auditpr** 和 **auditmerge** 命令用来处理 BIN 或 STREAM 方式的审计记录。两个实用程序运行为过滤器以便它们可在管道中易使用，这特别方便于 STREAM 方式的审计过程。

auditselect

可用来用类似 SQL 的语句仅选择特定的审计记录。例如，要只选择由用户 **afx** 生成的 **exec()** 事件，则请输入以下内容:

```
auditselect -e "login==afx && event==PROC_Execute"
```

auditpr

用于将二进制审计记录转换成人类可读的格式。所显示的信息量取决于在命令行中指定的标志。要获取所有可用的信息，请如下所示运行 **auditpr** 命令:

```
auditpr -v -hhelrtRpPTc
```

当指定了 **-v** 标志时，除了内核为每个事件而发出标准审计信息外，还显示特定于事件的字符串的审计跟踪（请参阅 **/etc/security/audit/events** 文件）。

auditmerge

用来合并二进制审计跟踪。这在需要联接几个系统的审计跟踪时特别有用。**auditmerge** 命令获取命令行中跟踪的名称并将合并的二进制跟踪发送到标准输出，因此仍需要使用 **auditpr** 命令来使之可读。例如，**auditmerge** 和 **auditptr** 命令可以运行如下:

```
auditmerge trail.system1 trail.system2 | auditpr -v -hhelrRtpc
```

使用快速安全性检查的审计子系统

不安装审计子系统来监视单一的可疑程序，可以使用 **watch** 命令。它将记录指定程序生成的请求或所有事件。例如，在运行 **vi /etc/hosts** 时查看 **FILE_Open** 事件，输入以下内容:

```
watch -eFILE_Open -o /tmp/vi.watch vi /etc/hosts
```

/tmp/vi.watch 文件显示编辑器会话中的所有 **FILE_Open** 事件。

设置审计

以下过程显示如何设置审计子系统。有关更多特定信息，请参考这些步骤中注释的配置文件。

1. 从 **/etc/security/audit/events** 文件中的列表选择系统活动（事件）审计。如果已经向应用程序或内核扩展添加了新的审计事件，则必须编辑文件以添加新的事件。
   - 如果包含的代码记录应用程序（使用 **auditwrite** 或 **auditlog** 子例程）或内核扩展（使用 **audit_svcstart**、**audit_svcbcopy** 和 **audit_svcfinis** 内核服务）里的事件，添加事件到此文件。
   - 确保任何新建审计事件的格式指示信息包含在 **/etc/security/audit/events** 文件中。当格式化审计记录时，这些规范启用 **auditpr** 命令写审计跟踪。
2. 分组选定的审计事件到名为*审计类*相似项目集中。定义 **/etc/security/audit/config** 文件的类节中的审计类。
3. 指定单独用户的审计类并指定审计事件到需要审计的文件，如下:
   - 指定单独用户的审计类，添加一行到 **/etc/security/audit/config** 文件的 user 节。指定用户的审计类，可以使用 **chuser** 命令。
   - 指定对象（数据或可执行文件）的审计事件，为该文件添加节到 **/etc/security/audit/objects** 文件。
   - 还可以通过编辑 **/usr/lib/security/mkuser.default** 文件来为新的用户指定缺省的审计类。当生成新建用户标识时，文件保留要使用的用户属性。例如，为所有新建用户标识使用 **general** 审计类，如下:

     ```
     user:
         auditclasses = general
         pgrp = staff
         groups = staff
         shell = /usr/bin/ksh
         home = /home/$USER
     ```

     获取全部审计事件，指定 **ALL** 类。当甚至在适度繁忙的系统执行此操作时，将生成大量的数据。通常，更实际的做法是限制记录事件的数量。
4. 在 **/etc/security/audit/config** 文件中，使用 BIN 收集、STREAM 收集或两种方式都用来配置数据收集类型。通过为审计数据使用分离的文件系统确保审计数据不能和文件空间的其它数据竞争。这确保审计数据有足够的空间。配置数据收集类型如下:
   - 配置 BIN 收集:

     a. 通过设置 **start** 节里的 `binmode = on` 启用 BIN 方式收集。

b. 编辑 **binmode** 节配置 bin 和 trail，并指定包含 BIN 方式后端处理命令的文件路径。后端命令的缺省文件是 **/etc/security/audit/bincmds**文件。

c. 确信审计 bin 足够大能满足需要并且如果正在填充文件系统相应设置 **freespace** 参数以获取警告。

d. 包含在 **/etc/security/audit/bincmds** 文件中审计管道中处理审计 bin 的 shell 命令。

- 配置 STREAM 收集:

a. 通过设置 **start** 节中的 `streammode = on` 启用 STREAM 方式收集。

b. 编辑 streammode 节指定到包含 streammode 处理命令的文件路径。包含此信息的缺省文件是 **/etc/security/audit/streamcmds** 文件。

c. 包含在 **/etc/security/audit/streamcmds** 文件中审计管道中处理 stream 记录的 shell 命令。

5. 完成对配置文件的任何必需的更改后，准备使用 **audit start** 命令选项启用审计子系统。
6. 使用 **audit query** 命令选项查看审计哪个事件和对象。
7. 使用 **audit shutdown** 命令选项再次释放审计子系统。

选择审计事件

审计的目的是检测可能有损系统安全性的活动。当未授权用户执行时，以下活动违背系统安全性并且是审计的对象:

- 在可信计算库里从事活动
- 认证用户
- 访问系统
- 更改系统配置
- 绕过审计系统
- 初始化系统
- 安装程序
- 修改帐户
- 把信息传入到系统或从系统传出

审计系统没有要审计事件的缺省设置。必须根据您的需要选择事件或事件类。

要审计活动，必须识别启动审计事件的命令或进程并且确保事件列在系统的 **/etc/security/audit/events** 文件中。那么必须添加事件到 **/etc/security/audit/config** 文件中的相应类或到 **/etc/security/audit/objects** 文件中的对象节。请参阅系统上 **/etc/security/audit/events** 文件里的审计事件和跟踪格式化指示信息列表。有关如何写和使用审计事件格式的描述，请参阅 **auditpr** 命令。

在选定审计事件后，必须把相似事件并到审计类。然后分配审计类给用户。

选择审计类

通过把连接相似事件并入到审计类，可以简化把审计事件指定给用户。审计类定义在 **/etc/security/audit/config** 文件中的类节里。

一些可能的典型审计类如下:

常规 改变系统状态和更改用户认证的事件。审计试图绕过系统访问控制。
对象 安全性配置文件的写入权限。
内核 通过内核的进程管理功能生成内核类中的事件。

/etc/security/audit/config 中节的示例如下:

```
classes:
    general = USER_SU,PASSWORD_Change,FILE_Unlink,FILE_Link,FILE_Rename
    system = USER_Change,GROUP_Change,USER_Create,GROUP_Create
    init = USER_Login,USER_Logout
```

选择审计数据收集方法

数据收集方法的选择取决于要如何使用审计数据。如果需要大量数据的长期存储，选择 BIN 收集。如果收集时处理数据，选择 STREAM 收集。如果需要长期存储和立即处理，选择两种方法。

Bin 收集
允许大审计跟踪的长时间存储。审计记录写进作为临时的 bin 的文件保存。在文件填满后，当审计子系统写进其它 bin 文件并且把记录写到审计跟踪存储时，通过 **auditbin** 守护程序处理数据。

Stream 收集
允许在收集的同时处理审计数据。审计记录写进内核里的循环缓冲区，通过读 **/dev/audit** 检索。审计记录可以显示、打印提供纸上的审计跟踪或通过 **auditcat** 命令转换成 bin 记录。

实时文件修改监视示例

以下示例用于监控关键文件的实时文件访问:

1. 设置监控关键文件改变的列表，例如 **/etc** 中的全部文件，并且在 **objects** 文件中配置它们以获得 **FILE_Write** 事件:

   ```
   find /etc -type f | awk '{printf("%s:\n\tw = FILE_Write\n\n",$1)}' >> /etc/security/audit/objects
   ```

2. 设置 stream 审计列出全部文件写操作。(此示例列出写到控制台的全部文件，但在生产环境下可能想要有一个后端，它发送事件到入侵检测系统。) The **/etc/security/audit/streamcmds** file is similar to the following:

   ```
   /usr/sbin/auditstream | /usr/sbin/auditselect -e "event == FILE_Write" |
   auditpr  -hhelpPRtTc -v > /dev/console &
   ```

3. 在 **/etc/security/audit/config** 中设置 STREAM 方式审计，为文件写事件添加类并且配置应该用类审计的所有用户:

   ```
   start:
           binmode = off
           streammode = on

   stream:
           cmds = /etc/security/audit/streamcmds

   classes:
           filemon = FILE_write

   users:
           root = filemon
           afx = filemon
           ...
   ```

4. 现在运行 **audit start**。在控制台上显示所有 **FILE_Write** 事件。

类属审计日志方案的示例

此例中假定系统管理员要使用审计子系统监控大的多用户服务器系统。未执行直接集成到 IDS，手工检查所有审计记录的不规则性。仅记录一些实质的审计事件，保持生成数据的数量为可管理的大小。

以下是为审计检测考虑的审计事件:

FILE_Write	要知道对配置文件的文件写操作，因此此事件会用于 **/etc** 树里的全部文件。
PROC_SetUserIDs	用户标识的所有更改
AUD_Bin_Def	审计 bin 配置
USER_SU	**su** 命令
PASSWORD_Change	**passwd** 命令
AUD_Lost_Rec	万一有记录丢失的通知
CRON_JobAdd	新建 **cron** 作业
AT_JobAdd	新建 **at** 作业
USER_Login	所有登录
PORT_Locked	终端上由于太多无效尝试而全部锁定

以下是如何生成类属审计日志的示例:

1. 设置要监控关键文件改变的列表，例如 **/etc** 里全部文件，并且为 **objects** 文件里的 **FILE_Write** 事件配置它们，如下:

   ```
   find /etc -type f | awk '{printf("%s:\n\tw = FILE_Write\n\n",$1)}' >> /etc/security/audit/objects
   ```

2. 使用 **auditcat** 命令设置 BIN 方式审计。**/etc/security/audit/bincmds** 文件与以下相似:

   ```
   /usr/sbin/auditcat -p -o $trail $bin
   ```

3. 编辑 **/etc/security/audit/config** 文件并且为我们感兴趣的事件添加类。列出所有现有的用户并且为它们指定 **custom** 类:

   ```
   start:
           binmode = on
           streammode = off

   bin:
           cmds = /etc/security/audit/bincmds
           trail = /audit/trail
           bin1 = /audit/bin1
           bin2 = /audit/bin2
           binsize = 100000
           freespace = 100000

   classes:
           custom = FILE_Write,PROC_SetUser,AUD_Bin_Def,AUD_Lost_Rec,USER_SU, \
                    PASSWORD_Change,CRON_JobAdd,AT_JobAdd,USER_Login,PORT_Locked

   users:
           root = custom
           afx = custom
           ...
   ```

4. 将 **custom** 审计类添加到 **/usr/lib/security/mkuser.default** 文件，这样新的标识将自动拥有正确的相关审计调用:

   ```
   user:
       auditclasses = custom
       pgrp = staff
       groups = staff
       shell = /usr/bin/ksh
       home = /home/$USER
   ```

5. 通过使用 SMIT 或 **crfs** 命令创建名为 **/audit** 的新的文件系统。该文件系统应该足以容纳两个 bin 和一个大的审计跟踪。

6. 运行 **audit start** 命令选项并测试 **/audit** 文件。您应该可以看到两个 bin 文件和一个初始为空的 **trail** 文件。使用系统一定时间后，**trail** 文件中应该已有审计记录，可以通过以下命令读取

   ```
   auditpr  -hhelpPRtTc -v | more
   ```

此例仅使用很少事件。要查看全部事件，您可以为所有用户指定类名 **ALL**。这个操作将生成大量的数据。您可能希望将所有有关用户更改和特权更改的事件都添加到 **custom** 类中。

第 4 章 LDAP 认证装入模块

轻量级目录访问协议（LDAP）定义了一种在客户机 – 服务器模型中本地或远程访问和更新目录（数据库）中的信息的标准方法。主机群集可以使用 LDAP 方法以允许集中式安全认证以及访问用户和组信息。此功能意在用于群集环境以使认证、用户和组信息在整个群集中公用。

安全子系统的 LDAP 开发可作为 LDAP 认证装入模块实现。概念上，它与其它装入模块（例如 NIS、DCE 和 Kerberos 5）相似。该装入模块在 **/usr/lib/security/methods.cfg** 文件中定义。LDAP 认证装入模块在低级别实现，并且由库来处理。

启用 LDAP 认证装入模块来提供用户和组信息服务后，大多数高级 API、命令和系统管理工具按照通常方式运作。引入 **-R** 标志使大多数高级命令通过不同的装入模块运作。例如，要从客户机创建名为 joe 的 LDAP 用户，请使用以下命令:

```
mkuser -R LDAP joe
```

客户机系统通过 **/etc/security/user** 文件中用户的 **SYSTEM** 属性检查用户是否是 LDAP 用户。如果用户的 **SYSTEM** 属性设置为 LDAP，则用户只能通过 LDAP 来认证。如果在缺省节中的 **SYSTEM** 属性设置为 LDAP，则所有没有 **SYSTEM** 属性设置的用户都被当作是 LDAP 用户。LDAP 关键字可以如第 45 页的『用户认证』所描述那样与其它 **SYSTEM** 属性值一起使用。客户机方通过 **secldapclntd** 守护程序与服务器进行通信。守护程序从应用程序（通过 API 库）接受请求、查询 LDAP 服务器并将数据返回到应用程序。**secldapclntd** 守护程序还负责高速缓存。

设置 LDAP 安全信息服务器

要将系统设置成 LDAP 安全信息服务器，让它能通过 LDAP 提供认证、用户和组信息服务，则必须安装 LDAP 服务器和客户机软件包。必须将 LDAP 服务器配置成为一个客户机和一个服务器。LDAP 服务器也需要有 DB2 数据库。如果需要安全套接字层（SSL），则必须安装 **GSKit** 软件包。系统管理员必须使用 **ikeyman** 命令来创建密钥。必须将服务器密钥证书传送到客户机。

mksecldap 命令可用于设置 LDAP 安全信息服务器。它建立称为 **ldapdb2** 的数据库，将来自本地主机的用户和组信息植入数据库，并设置 LDAP 服务器管理员 DN（专有名称）和密码。它可选择性地设置用于客户机／服务器通信的 SSL。**mksecldap** 命令将一个项添加到 **/etc/inittab** 文件中以在每次重新引导时启动 LDAP 服务器。通过 **mksecldap** 命令完成全部 LDAP 服务器设置，该命令更新了 **slapd.conf** 文件（SecureWay® Directory V3.2 和 4.1）或 **slapd32.conf** 文件（SecureWay Directory V3.2）。不需要配置 LDAP Web 管理接口。

在 LDAP 服务器设置过程中将所有用户和组从本地系统迁移到 LDAP 服务器。为此步骤选择以下 LDAP 模式之一:

特定于 AIX 的模式
包含 **aixAccount** 和 **aixAccessGroup** 对象类。此模式提供 AIX 用户和组的全套属性。

NIS 模式（RFC 2307）
包含 **posixAccount**、**shadowAccount** 和 **posixGroup** 对象类，并且由若干供应商目录产品使用。NIS 模式只定义了 AIX 所使用属性的一个小子集。

完全 AIX 支持的 NIS 模式
包含 **posixAccount**、**shadowAccount** 和 **posixGroup** 对象类以及 **aixAusAccount** 和 **aixAusGroup** 对象类。**aixAusAccount** 和 **aixAuxGroup** 对象类提供由 AIX 使用但没有由 NIS 模

式定义的属性。推荐使用完全 AIX 支持的 NIS 模式来设置 LDAP 服务器，除非必须设置特定于 AIX 的模式 LDAP 服务器以与现有的 LDAP 服务器兼容。

所有用户和组信息储存在公共的 AIX 目录树下（后缀）。缺省后缀是 "cn=aixdata"。**mksecldap** 命令通过 **-d** 标志来接受用户提供的后缀。如果用户提供的后缀没有将 "cn=aixdata" 作为其第一个 RDN（相对专有名称），则 **mksecldap** 命令在用户提供的后缀中添加 "cn=aixdata" 作为前缀。此 AIX 目录树是受 ACL（访问控制列表）保护的。客户机必须绑定为 LDAP 服务器管理员以能够访问 AIX 目录树。

mksecldap 命令即使在 LDAP 服务器设置为其它用途的情况下仍起作用；例如，将 LDAP 服务器设置为用作查找用户标识信息。在本例中，**mksecldap** 添加了 AIX 目录树，并将其带 AIX 安全信息植入现有数据库中。此目录树是受 ACL 保护的，并独立于其它目录树。在本例中，除了作为 AIX LDAP 安全服务器服务之外，LDAP 服务器象平常一样工作。

注: 建议运行 **mdsecldap** 命令设置安全服务器来共享同一数据库之前备份现有的数据库。

在成功设置 LDAP 安全信息服务器之后，必须将同一主机设置为客户机，以使完成 LDAP 用户和组管理，并且 LDAP 用户能够登录到该服务器。

如果设置 LDAP 安全信息服务器不成功，您可以运行带有 **-U** 标志的 **mksecldap** 命令来撤销设置。这会将 **slapd.conf**（或 **slapd32.conf**）文件恢复到它的设置前状态。在任何设置尝试失败后，在再次尝试运行 **mksecldap** 命令前，运行带有 **-U** 标志的 **mksecldap** 命令。否则，残余的设置信息会保留在配置文件中，并导致后面的设置失败。作为安全预防措施，撤销选项不会对数据库或其数据执行任何操作，因为运行 **mksecldap** 命令之前该数据库可能已经存在了。如果数据库是通过 **mksecldap** 命令创建的，那么就手工将其除去。如果 **mksecldap** 命令已经将数据添加到先前存在的数据库，那就确定应采取什么步骤从失败的设置尝试中的恢复。

关于设置 LDAP 安全信息服务器的更多信息，请参阅 **mksecldap** 命令。

设置 LDAP 客户机

每个客户机都必须安装 LDAP 客户机软件包。如果需要 SSL，那么必须安装 GSKit、创建密钥，必须将 LDAP 服务器 SSL 密钥证书添加到此密钥中。

可以使用 **mksecldap** 命令来设置客户机。要该客户机与 LDAP 安全信息服务器联系，就必须在设置过程中提供服务器名称。客户机访问服务器上的 AIX 目录树也需要服务器的管理员 DN 和密码。**mksecldap** 命令将服务器上的服务器管理员 DN、密码、服务器名、AIX 目录树 DN 以及 SSL 密钥路径和密码保存到 **/etc/security/ldap/ldap.cfg** 文件中。

在客户机设置过程中可以向 **mksecldap** 命令提供多个服务器。在本例中，客户机按照提供的次序联系服务器，并与客户机可以成功绑定的第一个服务器建立连接。如果在客户机和服务器之间发生不良连接，那么会使用同一逻辑尝试请求重新连接。安全 LDAP 开发模型不支持参照。保持复制服务器同步是很重要的。

客户机可与 LDAP 安全信息服务器通过客户机方守护程序（**secldapclntd**）进行通信。如果在该客户机上启用了装入模块，那么高级命令最终会通过 API 库找到该守护程序。守护程序查询服务器，并将信息返回给调用者。

在客户机设置过程中，可以向 **mksecldap** 命令提供其它精细调节选项，例如设置守护程序所用的线程数、高速缓存项大小以及高速缓存到期超时。这些选项仅供有经验的用户使用。对于大多数环境而言，缺省值已经足够。

在客户机设置的最后步骤中，**mksecldap** 命令启动客户机方守护程序，并在 **/etc/inittab** 文件中添加一个项，这样在每次重新引导时会启动守护程序。您可以通过检查 **secldapclntd** 进程来检查是否设置成功。假如设置并运行 LDAP 安全信息服务器，如果设置成功，那么就会运行该守护程序。

LDAP 用户管理

您可使用高级命令从任何 LDAP 客户机上管理 LDAP 安全信息服务器上的用户和组。添加到大多数高级命令的 **-R** 标志能够使用 LDAP 以及其它认证装入模块（例如 DCE、DCE 以及 Kerberos）来管理用户和组。关于涉及 **-R** 标志使用的更多信息，请参考每个用户或组管理命令。

要使用户能够通过 LDAP 认证，请运行 **chuser** 命令将用户的 **SYSTEM** 属性值更改为 LDAP。通过根据已定义的语法来设置 **SYSTEM** 属性值，用户可以通过使用多于一个的装入模块（例如，compat 和 LDAP）来认证。有关设置用户认证方法的更多信息，请参阅第 45 页的『用户认证』和 **/etc/security/user** 文件中定义的 **SYSTEM** 属性语法。

通过按下列任何一种格式运行带有 **-u** 标志的 **mksecldap** 命令，用户能够在客户机设置时成为 LDAP 用户:

1. 运行 `mksecldap -c -u user1,user2,...`，其中 **user1,user2,...** 是用户列表。该列表中的用户可以是本地定义的或远程 LDAP 定义的用户。**/etc/security/user** 文件中每个以上用户节中的 **SYSTEM** 属性都设置为 LDAP。这些用户只能通过 LDAP 来认证。该列表中的用户必须在 LDAP 安全信息服务器上存在；否则它们不能从该主机登录。运行 **chuser** 命令修改 **SYSTEM** 属性，并允许通过多种方法（例如，本地和 LDAP）进行认证。
2. 运行 "mksecldap -c -u ALL"。该命令为所有本地定义的用户将 **/etc/security/user** 文件的每一用户节中的 **SYSTEM** 属性设置为 LDAP。所有这样的用户都只能通过 LDAP 来认证。本地定义的用户必须在 LDAP 安全信息服务器上存在；否则它们不能从该主机上登录。在 LDAP 服务器上定义的而没有在本地定义的用户不能从该主机登录。要允许远程 LDAP 定义的用户从该主机登录，请运行 **chuser** 命令将该用户的 **SYSTEM** 属性设置为 LDAP。

另外，您也可以通过将 **/etc/security/user** 文件中“缺省”节的值修改为“LDAP”，从而使所有的 LDAP 用户（不管它们是否是本地定义的）都能够通过本地主机上的 LDAP 来认证。所有没有为其 **SYSTEM** 属性定义值的用户都必须遵照在缺省节中所定义的值。例如，如果缺省节有 "SYSTEM = ″compat″"，将它更改为 "SYSTEM = ″compat OR LDAP″" 允许这些用户通过 AIX 或 LDAP 进行认证。将缺省节更改为 "SYSTEM = ″LDAP″" 使这些用户只能通过 LDAP 认证。那些已定义 **SYSTEM** 属性值的用户不受缺省节影响。

LDAP 主机访问控制

AIX 为系统提供用户级主机访问（登录）控制。管理员可以通过将 LDAP 用户的 **SYSTEM** 属性设置为 LDAP 来配置 LDAP 用户以登录到 AIX 系统。**SYSTEM** 属性在 **/etc/security/user** 文件中。**chuser** 命令可用于设置它的值，与以下内容相似:

```
# chuser -R LDAP SYSTEM=LDAP registry=LDAP foo
```

注: 在这种控制类型下，不要将缺省的 **SYSTEM** 属性设置为 LDAP（这允许所有 LDAP 用户登录到系统）。这会将 LDAP 属性设置成允许用户 `foo` 登录到该系统。它还将注册表设置为 LDAP，这允许登录进程记录 `foo` 登录 LDAP 的尝试，并允许在 LDAP 上完成任何用户管理任务。

管理员需要在每个客户机系统上运行这样的设置，以使某些用户能够登录。

从 AIX 5.2 开始，AIX 已经实现了一个功能，即将 LDAP 用户限制为只能登录到某些 LDAP 客户机系统。此功能允许集中式主机访问控制管理。管理员能够对一个用户帐户指定两个主机访问控制列表: 一个允许列表和一个拒绝列表。通过用户帐户这两个用户属性存储在 LDAP 服务器中。用户可以对允许列表中指定的系统或

网络进行访问，但不能对拒绝列表中的系统或网络进行访问。如果同时在允许列表和拒绝列表中指定了一个系统，那么用户不能对该系统进行访问。有两种方法指定用户的访问列表：当创建用户时可以使用 **mkuser** 命令，或者对于现有的用户可以使用 **chuser** 命令。为向后兼容，如果用户的允许列表和拒绝列表不存在，那么缺省情况下，允许用户登录到任何 LDAP 客户机系统。从 AIX 5.2 开始，该主机访问控制功能可用。

设置用户的允许和拒绝许可权列表的示例如下:

```
# mkuser -R LDAP hostsallowedlogin=host1,host2 foo
```

这会创建用户 foo，只允许用户 foo 登录到 host1 和 host2。

```
# mkuser -R LDAP hostsdeniedlogin=host2 foo
```

这会创建用户 foo，用户 foo 可以登录到 host2 之外的任何 LDAP 客户机系统。

```
# chuser -R LDAP hostsallowedlogin=192.9.200.1 foo
```

这会将用户 foo 设置成具有登录到地址为 192.9.200.1 的客户机系统的许可权。

```
# chuser -R LDAP hostsallowedlogin=192.9.200/24 hostsdeniedlogin=192.9.200.1 foo
```

这会将用户 foo 设置成具有登录到 192.9.200/24 子网内任何客户机系统的许可权，除了地址为 192.9.200.1 的客户机系统。

有关更多信息，请参阅 **chuser** 命令。

LDAP 安全信息服务器审计

SecureWay Directory V3.2（及更新版本）提供缺省服务器审计日志功能。一旦启用，缺省的审计插件会将 LDAP 服务器活动记录到日志文件中。关于该缺省审计插件的更多信息，请参阅 *Packaging Guide for LPP Installation* 中的 LDAP 文档。

在 AIX 5.1 及更新版本中已经实现了 LDAP 安全信息服务器审计功能，称为 *LDAP 安全审计插件*。它独立于 SecureWay Directory 缺省审计服务，因此可以启用这两个审计子系统中的任何一个或同时启用两个。AIX 审计插件只记录那些在 LDAP 服务器上更新或查询 AIX 安全信息的事件。它在 AIX 系统审计的框架内运作。

要提供 LDAP，**/etc/security/audit/event** 文件中包含以下审计事件:

- **LDAP_Bind**
- **LDAP_Unbind**
- **LDAP_Add**
- **LDAP_Delet**
- **LDAP_Modify**
- **LDAP_Modifydn**
- **LDAP_Search**

ldapserver 审计类定义也在包含所有上述事件的 **/etc/security/audit/config** 文件中创建。

要审查 LDAP 安全信息服务器，将以下行添加到 **/etc/security/audit/config** 文件中每个用户的节:

```
ldap = ldapserver
```

因为 LDAP 安全信息服务器审计插件在 AIX 系统审查框架内实现，所以它是 AIX 系统审计子系统的一部分。使用系统审计命令（例如 **audit start** 或 **audit shutdown**）可以启用或禁用 LDAP 安全信息服务器审计。将所有审计记录添加到系统审计跟踪中，该跟踪能够使用 **auditpr** 命令来检查。更多信息，请参阅第 49 页的第 3 章，『审计』。

LDAP 命令

mksecldap 命令

mksecldap 命令可以用来设置安全认证和数据管理的 IBM SecureWay Directory 服务器和客户机。该命令必须在服务器和所有客户机上运行。

注:

1. 客户机（**-c** 标志）和服务器（**-s** 标志）选项不能同时运行。当设置服务器时，**mksecldap** 命令应该在该机器上运行两次。第一次运行用来设置服务器，第二次运行用来设置客户机。
2. SecureWay Directory 服务器配置文件是 AIX 3.2 或后续版本的 **/etc/slapd32.conf**。AIX 5.2 仅支持 SecureWay Directory 3.2 和后续版本。

要设置服务器，确保安装了 **ldap.server** 文件集。在安装 **ldap.server** 文件集时，也同时自动安装了 **ldap.client** 文件集和后端 DB2 软件。用该命令设置 LDAP 服务器时不需要运行任何 DB2 预配置。当运行 **mksecldap** 命令设置服务器时，命令将:

1. 创建一个 DB2 实例，将 **ldapdb2** 作为缺省的实例名。
2. 创建一个 DB2 数据库，将 **ldapdb2** 作为缺省的数据库名称。如果数据库已经存在，**mksecldap** 将绕过以上两步。（这是设置 LDAP 服务器另作它用的例子。）**mksecldap** 命令将使用现有的数据库存储 AIX 用户／组数据。
3. 创建 AIX 树 DN（后缀）。如果没有从命令行提供基本 DN，缺省的后缀设置为 **cn=aixdata** 并把用户／组组数据放置在 **cn=aixsecdb,cn=aixdata** DN。这是建议的情况。否则，**mksecldap** 命令提取用户提供的 DN 并在其上加上 **cn=aixdata** 前缀，并使新建的 DN 成为后缀。下表显示了这种行为。括号中的值代表由用户从命令行提供的可选 DN。

命令行 DN:	[o=ibm]
后缀:	cn=aixdata[,o=ibm]
安全性 DN:	cn=aixsecdb,cn=aixdata[,o=ibm]
用户 DN:	ou=aixuser,cn=aixsecdb,cn=aixdata[,o=ibm]
组 DN:	ou=aixgroup,cn=aixsecdb,cn=aixdata[,o=ibm]

如果本地系统已设置 LDAP 服务器，**mksecldap** 命令从 **slapd32.conf** 配置文件中定义的后缀和数据库中寻找 **cn=aixsecdb** 关键字。如果它找到了关键字，它假定已经运行了 **mksecldap**，并绕过基本 DN 设置步骤和用户／组迁移步骤，然后退出。

如果在后缀和数据库中没有找到 **cn=aixsecdb**，**mksecldap** 命令检查 **cn=aixdata** 关键字。**cn=aixdata** 是一个被不同 AIX LDAP 组件共享的公共基本 DN。如果 **mksecldap** 命令找到了关键字，它把关键字和用户提供的 DN 进行比较。如果它们相同的，将会把用户／组放在 **cn=aixsecdb**，**cn=aixdata**，**[userDN]**下面。如果它们不相同，**mksecldap** 命令显示一个错误消息以警告 **cn=aixdata,...** DN 的存在，而不把用户／组移到用户提供的 DN 下面。通过对该现有 DN 再次运行 **mksecldap** 命令，可以选择使用现有的 **cn=aixdata,...**。

4. 把数据从本地主机的安全数据库文件迁移到 LDAP 数据库。根据 **-S** 选项，**mksecldap** 命令迁移用户／组时使用的三个 LDAP 模式之一:
   - **AIX** – AIX 模式（**aixaccount** 和 **aixaccessgroup** 对象类）

- **RFC2307** – RFC 2307 模式（**posixaccount**、**shadowaccount** 和 **posixgroup** 对象类）
- **RFC2307AIX** – 完全支持 AIX 的 RFC 2307 模式（**posixaccount**、**shadowaccount**、**posixgroup 对象类**以及 **aixauxaccount** 和 **aixauxgroup** 对象类）。

  警告: 运行 AIX 4.3 和 AIX 5.1（它们作为 LDAP 客户机配置）的系统将只能与 AIX 类型方案的服务器一起使用。它们不与 RFC2307 或 RFC2307AIX 类型的 LDAP 服务器会话。

5. 设置 LDAP 服务器管理员 DN 和密码。该名称／密码对也用于 AIX 树的访问控制。
6. 设置在该服务器和客户机间安全传送数据的 SSL（安全套接字层）。该设置需要已安装了 **GSKIT**。

   注: 如果使用了该选项，在运行 **mksecldap** 命令之前必须创建了 SSL 密钥。否则，服务器可能无法启动。
7. 安装 **/usr/ccs/lib/libsecldapaudit.a**，一个 LDAP 服务器插件。该插件支持 LDAP 服务器的 AIX 审计。
8. 在完成了全部上述步骤后，启动／重新启动 LDAP 服务器。
9. 在重新引导后，把 LDAP 服务器进程添加到（**slapd**）**/etc/inittab** 来启动 LDAP 服务器。
10. 用 **-U** 选项，撤销早先的服务器配置文件设置。在您第一次运行 **mksecldap** 命令时，它保存了两份 **slapd32.conf** 服务器配置文件的副本。一份保存到 **/etc/security/ldap/slap32.conf.save.orig**，另一份保存到 **/etc/ security/ldap/slapd32.conf.save**。**mksecldap** 的每次后续运行，**当前 slapd32.conf** 仅保存到 **/etc/security/ldap/slapd32.conf.save** 文件。撤销选项用 **/etc/security/ ldap/slapd32.conf.save** 副本来恢复 **/etc/slapd32.conf** 服务器配置文件。

    注: 撤销选项仅适用于服务器配置文件。它不影响数据库。

注: 所有的 LDAP 配置保存到 **/etc/slapd32.conf** LDAP 服务器配置文件中。

对于设置客户机，确保设置了 LDAP 服务器且正在运行。**mksecldap** 命令在客户机设置期间做以下事情:

1. 保存 LDAP 服务器的主机名。
2. 保存服务器的用户基本 DN 和组基本 DN。如果没有从命令行提供 **-d** 选项，**mksecldap** 命令在 LDAP 服务器上搜索 **aixaccount**、**aixaccessgroup**、**posixaccount**、**posixgroup** 和 **aixauxaccount** 对象类，并设置相应的基本 DN。如果服务器有多个基本用户／组，您必须提供有 RDN 的 **-d** 选项，使 **mksecldap** 命令可以设置该 RDN 中选项的基本 DN。

   如果在设置客户机期间找到 **posixaccount** 对象类，**mksecldap** 也将尝试从服务器搜索这些实体的基本 DN: 主机、网络、服务、网络组、协议和 rpc，并保存任何找到的实体。
3. 确定 LDAP 服务器使用的模式类型 – **AIX** 特定模式、**RFC 2307** 模式或有完全 AIX 支持的 **RFC 2307** 模式（请参阅步骤 2 列出的对象类）。它在 **/etc/security/ldap/ ldap.cfg** 文件相应的设置了对象类和属性映射。**mksecldap** 命令不能识别其它模式类型，所以必须手工设置客户机。
4. 在该主机和 LDAP 服务器之间设置 SSL 以进行安全数据传输。该步骤需要预先创建客户机的 SSL 密钥和密钥密码，而且必须将服务器设置为使用 SSL 以使客户机 SSL 能起作用。
5. 保存 LDAP 服务器管理员 DN 和密码。DN／密码对必须与服务器设置期间指定的对相同。
6. 根据客户机方守护程序使用的项数目来设置高速缓存大小。对用户有效的值的范围为 100-10,000，对组有效的为 10-1,000。对用户的缺省值为 1,000，对组的缺省值为 100。
7. 设置客户机方守护程序的高速缓存超时。有效值范围为 60-3600 秒。缺省值为 300 秒。把该值设为 0 来禁用高速缓存。
8. 设置客户机方守护程序使用的线程数。有效值范围为 1-1,000。缺省值为 10。
9. 以秒为单位设置客户机守护程序检查 LDAP 服务器状态的时间间隔。有效值为 60-3,600 秒。缺省值为 300。

10. 通过修改在 **/etc/security/user** 文件中的 SYSTEM 行来选择性地设置用户列表或所有使用 LDAP 的用户。关于启用 ldap 登录的更多信息，请参阅以下注解。
11. 启动客户机守护进程（**secldapclntd**）。
12. 将客户机方守护进程添加到 **/etc/inittab** 以使该守护程序在重新引导后启动。
13. 使用 **-U** 选项，撤销 **/etc/security/ldap/ldap.cfg** 文件的先前设置。

    注: 客户机配置数据保存到 **/etc/security/ldap/ldap.cfg** 文件。设置 **/etc/security/user** 缺省节的 SYSTEM 为 LDAP，只允许 LDAP 用户登录到系统。设置 SYSTEM 为 LDAP 或 compat 允许 LDAP 用户和本地用户登录到系统。

示例

1. 要设置用户和组的特定于 AIX 模式的 LDAP 服务器，请输入:

   ```
   mksecldap -s -a cn=admin -p adminpwd -S aix
   ```

   这将设置一个 LDAP 服务器，并使 LDAP 服务器管理员 DN 为 **cn=admin**，密码为 **adminpwd**。用户和组数据从本地文件迁移到缺省的 **cn=aixdata** 后缀。
2. 要设置一个带基本 DN（除了缺省值和 SSL 安全通信之外）的 LDAP 服务器，请输入:

   ```
   mksecldap -s -a cn=admin -p adminpwd -d o=mycompany,c=us -S rfc2307 \ -k /usr/ldap/serverkey.kdb
    -w keypwd
   ```

   这将设置 LDAP 服务器，并使 LDAP 服务器管理员 DN 为 **cn=admin**，密码为 **adminpwd**。用户和组数据被从本地文件迁移到缺省的 **cn=aix-data, o=mycompany, c=us** 后缀。LDAP 服务器通过使用存储在 **/usr/ldap/serverkey.kdb** 的密钥来使用 SSL 通信。密钥的密码（**keypwd**）也必须提供。用户和组以 RFC 2307 模式迁移。
3. 要撤销先前的服务器设置:

   ```
   mksecldap -s -U
   ```

   这撤销了先前对 **/etc/slapd32.conf** 服务器配置文件的设置。由于安全原因，这不除去先前设置所创建的任何数据库项或数据库。如果不再需要数据库项 / 数据库，请手工除去它们。
4. 要设置使用 **server1.ibm.com** 和 **server2.ibm.com** LDAP 服务器的客户机，请输入:

   ```
   mksecldap -c -a cn=admin -p adminpwd -h server1.ibm.com,server2.ibm.com
   ```

   必须向该客户机提供 LDAP 服务器管理员 DN 和密码以认证到服务器。**mksecldap** 命令联系 LDAP 服务器以取得所用的模式类型，并相应地设置客户机。从命令行不带 **-d** 选项，整个服务器 DIT 搜索用户基本 DN 和组基本 DN。
5. 要设置客户机使用 SSL 和 **server3.ibm.com** LDAP 服务器会话，请输入:

   ```
   mksecldap -c -a cn=admin -p adminpwd -h server3.ibm.com -d o=mycompany,c=us -k /usr/ldap/clientkey.kdb -w keypwd -u user1,user2
   ```

   这样设置的 LDAP 客户机类似于例 3，除了使用 SSL 进行通信。**mksecldap** 命令搜索 **o=mycompany, c=us** RDN 以获得用户基本 DN 和组基本 DN。配置 user1 帐户和 user2 帐户通过 LDAP 进行认证。

   注: **-u ALL** 选项使所有 LDAP 用户能够登录到该客户机。
6. 要撤销先前的客户机设置，请输入:

   ```
   mksecldap -c -U
   ```

   这会撤销先前对 **/etc/security/ldap/ldap.cfg** 文件的设置。这并不从 **/etc/security/user** 文件中除去 **SYSTEM=LDAP** 和 **registry=LDAP**。

关于 **mksecldap** 命令的更多信息，请参阅《*AIX 5L V5.2 命令参考大全*》中的 **mksecldap**。

secldapclntd 守护程序

secldapclntd 守护程序从 LDAP 装入模块中接受请求，把请求转发到 “LDAP 安全信息服务器” 上，并把从服务器返回的结果发送到 LDAP 装入模块。该守护程序在它的启动过程中读取定义在 **/etc/security/ldap/ldap.cfg** 文件中的配置信息，并使用服务器管理员的专有名称和密码到 “LDAP 安全信息服务器” 上进行认证，并建立本地主机和服务器的连接。

如果在 **/etc/security/ldap/ldap.cfg** 文件中指定了多个服务器，**secldapclntd** 守护程序就连接到所有的服务器上。然而在特定时间，它只和它们中的一个会话。**secldapclntd** 守护程序可以检测到与它会话的服务器什么时候关闭，并自动和另一个可用服务器会话。它也能检测到什么时候服务器再次可用，并和该服务器重新建立连接（但它继续和它正在会话的服务器会话）。这种自动检测功能通过 **secldapclntd** 守护程序来完成，它定期检查每一个服务器。后继检查之间的时间间隔的缺省值为 300 秒，可以在守护程序启动时从命令行更改，或通过修改 **/etc/ security/ldap/ldap.cfg** 文件中相应的值来更改。

在启动时，**secldapclntd** 守护程序尝试与 LDAP 服务器建立连接。如果它不能连接到任何一个服务器，它将进入休眠状态，并在三十秒后再一次尝试连接。它重复该过程两次，如果它还是不能建立任何连接，**secldapclntd** 守护进程将退出。

secldapclntd 守护程序是一个多线程程序。该守护程序使用的缺省线程数是 10。管理员可以通过调整该守护程序使用的线程数来精细调节系统性能。

secldapclntd 守护程序存放从 LDAP 安全信息服务器检索到的调整性能的信息。如果在高速缓存中能找到所请求的数据并且高速缓存项没有过期，该数据就被送回到请求者。否则，**secldapclntd** 守护程序向 “LDAP 安全信息服务器” 发出一个请求来获取信息。

对于用户，高速缓存项的有效数目范围是 100-10,000，而对组的有效数目范围是 10-1,000。对用户项的缺省值是 1000，对于组是 100。

高速缓存超时或 TTL（生存时间）可以是从 60 秒到 1 小时（60*60=3600 秒）。缺省情况下，高速缓存项在 300 秒后过期。如果高速缓存超时设置为 0，高速缓存功能将被禁用。

示例

1. 要启动 **secldapclntd** 守护程序，请输入:

   ```
   /usr/sbin/secldapclntd
   ```

2. 要启动 **secldapclntd**，使用 20 个线程并且高速缓存超时值为 600 秒，请输入:

   ```
   /usr/sbin/secldapclntd -p 20 -t 600
   ```

建议您通过运行 **start-secldapclntd** 命令来启动 **secldapclntd** 守护程序。还建议您在 **/etc/security/ldap/ldap.cfg** 文件中指定这些值，使得每次启动 **secldapclntd** 进程时都可以使用这些值。

有关 **secldapclntd** 守护程序的更多信息，请参阅《*AIX 5L V5.2 命令参考大全*》中的 **secldapclntd**。

LDAP 管理命令

start-secldapclntd 命令

如果 **secldapclntd** 守护程序没有运行，可以用 **start-secldapclntd** 命令启动它。如果 **secldapclntd** 守护程序已经在运行，则不作任何操作。脚本在启动 **secldapclntd** 守护程序前还从任何先前的 **secldapclntd** 守护进程中清除端口映射程序注册（如果有的话）。该操作会防止由于端口映射程序注册失败而导致的新守护进程启动失败。

示例:

1. 要启动 **secldapclntd** 守护程序，请输入:

   ```
   /usr/sbin/start-secldapclntd
   ```

2. 要启动 **secldapclntd** 使用 20 个线程并且高速缓存超时值为 600 秒，请输入:

   ```
   /usr/sbin/start-secldapclntd -p 20 -t 600
   ```

   建议您在 **/etc/security/ldap/ldap.cfg** 文件中指定这些值，使得每次启动 **secldapclntd** 进程时都可以使用这些值。

关于 **start-secldapclntd** 命令的更多信息，请参阅《*AIX 5L V5.2 命令参考大全*》中的 **start-secldapclntd**。

stop-secldapclntd 命令

stop-secldapclntd 命令终止运行着的 **secldapclntd**守护进程。如果 **secldapclntd** 守护程序没有运行，它将返回一个错误。

示例: 要停止运行 **secldapclntd** 守护进程，请输入:

```
/usr/sbin/stop-secldapclntd
```

关于 **stop-secldapclntd** 命令的更多信息，请参阅《*AIX 5L V5.2 命令参考大全*》中的 **stop-secldapclntd**。

restart-secldapclntd 命令

如果 **secldapclntd** 守护程序在运行，那么 **restart-secldapclntd** 脚本使其停止，然后重新启动它。如果 **secldapclntd** 守护程序没有运行，该命令只是启动它。

示例:

1. 要重新启动 **secldapclntd** 守护程序，请输入:

   ```
   /usr/sbin/restart-secldapclntd
   ```

2. 要重新启动 **secldapclntd** 使用 30 个线程并且高速缓存超时值为 500 秒，请输入:

   ```
   /usr/sbin/restart-secldapclntd -p 30 -t 500
   ```

关于 **restart-secldapclntd** 命令的更多信息，请参阅《*AIX 5L V5.2 命令参考大全*》中的 **restart-secldapclntd**。

ls-secldapclntd 命令

ls-secldapclntd 命令列出了 **secldapclntd** 守护程序的状态。返回的信息包含以下内容:

- 正与 **secldapclntd** 守护程序会话的 LDAP 服务器
- LDAP 服务器端口号
- 使用的 LDAP 协议版本
- 用户基本 DN

- 组基本 DN
- 系统（标识）基本 DN
- 用户高速缓存大小
- 用户使用的高速缓存大小
- 组高速缓存大小
- 使用的组高速缓存大小
- 高速缓存超时（生存时间）值
- **secldapclntd** 到 LDAP 服务器的检测信号时间间隔
- **secldapclntd** 守护程序使用的线程数
- LDAP 服务器使用的用户对象类
- LDAP 服务器使用的组对象类

示例:

1. 要列出 **secldapclntd** 守护程序的状态，请输入:

   ```
   /usr/sbin/ls-secldapclntd
   ```

关于 **ls-secldapclntd** 命令的更多信息，请参阅《*AIX 5L V5.2 命令参考大全*》中的 **ls-secldapclntd**。

flush-secldapclntd 命令

flush-secldapclntd 命令清空 **secldapclntd** 守护进程的高速缓存。

示例: 要刷新 **secldapclntd** 守护程序的高速缓存，请输入:

```
/usr/sbin/flush-secldapclntd
```

关于 **flush-secldapclntd** 命令的更多信息，请参阅《*AIX 5L V5.2 命令参考大全*》中的 **flush-secldapclntd**。

sectoldif 命令

sectoldif 命令读取本地定义的用户和组，并以 **ldif** 格式将结果打印到标准输出。如果重定向到一个文件，可以用 **ldapadd** 命令或 **db2ldif** 命令将结果添加到 LDAP 服务器。

-S 选项指定了 ldif 输出所使用的模式类型。**sectoldif** 命令接受以下模式类型:

- **AIX** – AIX 模式（**aixaccount** 和 **aixaccessgroup** 对象类）
- **RFC2307** – RFC 2307 模式（**posixaccount**、**shadowaccount** 和 **posixgroup** 对象类）
- **RFC2307AIX** – 完全支持 AIX 的 RFC 2307 模式（**posixaccount**、**shadowaccount** 和 **posixgroup** 对象类以及 **aixauxaccount** 和 **aixauxgroup** 对象类）。

mksecldap 命令调用 **sectoldif** 命令来在 LDAP 服务器设置期间迁移用户和组。使用 **sectoldif** 输出把附加的用户和组从其它系统迁移到 LDAP 服务器时要谨慎。当使用 **sectoldif** 输出添加项、从多个系统迁移用户和组时（可能会导致多个账户共享一个数字标识，这是安全性违例），**ldapadd** 和 **db2ldif** 命令仅检查项名（用户名或组名），而不检查数字标识。

示例:

1. 要打印本地定义的所有用户和组，请输入以下命令:

   ```
   sectoldif -d cn=aixsecdb,cn=aixdata -S rfc2307aix
   ```

   这将所有本地定义的用户和组以 **ldif** 格式打印到标准输出。使用 rfc2307aix 模式类型表示用户项和组项。基本 DN 设置为 `cn=aixsecdb, cn=aixdata`。

2. 要仅打印本地定义的用户占位符，请输入以下命令:

```
sectoldif -d cn=aixsecdb,cn=aixdata -u foo
```

这将本地定义的用户占位符以 **ldif** 格式打印到标准输出。不带 **-S** 选项，使用缺省 AIX 模式类型来表示占位符的 ldif 输出。

关于 **sectoldif** 命令的更多信息，请参阅《*AIX 5L V5.2 命令参考大全*》中的 **sectoldif**。

ldap.cfg 文件格式

/etc/security/ldap/ldap.cfg 文件包含正确启动和运行了的 **secldapclntd** 守护程序的信息，也包含了精细调节守护程序性能的信息。**/etc/security/ldap/ldap.cfg** 文件在客户机安装时通过 **mksecldap** 命令来更新。

/etc/security/ldap/ldap.cfg 文件可以包含以下字段:

ldapservers	指定逗号分隔的 “LDAP 安全信息服务器”。这些服务器可以是主服务器和 / 或主服务器的副本。
ldapadmin	指定 “LDAP 安全信息服务器” 的管理员 DN。
ldapadmpwd	指定管理员 DN 的密码。
useSSL	指定是否使用 SSL 通信。有效值是 ON 和 OFF。缺省值为 OFF。 **注**: 您将需要 SSL 密钥和该密钥对应的密码来启用该功能。
ldapsslkeyf	指定到 SSL 密钥的全路径。
ldapsslkeypwd	指定 SSL 密钥的密码。 **注**: 取消对该行的注释以使用隐藏密码。密码存储文件必须与 SSL 密钥本身驻留在同一个目录，并必须与密钥文件有相同的名称，但用 **.sth** 扩展名替代了 **.kdb** 扩展名。
userattrmappath	为用户指定到 AIX-LDAP 属性映射的全路径。
groupattrmappath	为组指定到 AIX-LDAP 属性映射的全路径。
idattrmappath	为标识指定到 AIX-LDAP 属性映射的全路径。当创建 LDAP 用户时 **mkuser** 命令使用这些标识。
userbasedn	指定用户基本 DN。
groupbasedn	指定组基本 DN。
idbasedn	指定标识基本 DN。
hostbasedn	指定主机基本 DN。
servicebasedn	指定服务基本 DN。
protocolbasedn	指定协议基本 DN。
networkbasedn	指定网络基本 DN。
netgroupbasedn	指定网组基本 DN。
rpcbasedn	指定 RPC 基本 DN。
userclasses	指定用于用户项的对象类。
groupclasses	指定用于组项的对象类。
ldapversion	指定 LDAP 服务器协议版本。缺省值是 3。
ldapport	指定 LDAP 服务器侦听的端口。缺省值是 389。
ldapsslport	指定 LDAP 服务器侦听的 SSL 端口。缺省值是 636。
followaliase	指定是否跟随别名。有效值是 NEVER、SEARCHING、FINDING 和 ALWAYS。缺省值是 NEVER。
usercachesize	指定用户高速缓存大小。有效值是 100-1,000 个项。缺省值是 1,000。
groupcachesize	指定组高速缓存大小。有效值是 10-1,000 个项。缺省值是 100。
cachetimeout	指定高速缓存的 TTL（生存时间）。有效值是 60-3,600 秒。缺省值是 300。把值设为 0 来禁用高速缓存。
heartbeatinterval	以秒为单位来指定客户机联系服务器获得服务器状态的时间间隔。有效值是 60-3,600 秒。缺省值是 300。
numberofthread	指定 **secldapclntd** 守护程序所使用的线程数。有效值是 1-1,000。缺省值是 10。

有关 **/etc/security/ldap/ldap.cfg** 文件的更多信息，请参阅 *AIX 5L Version 5.2 Files Reference* 中的 **/etc/security/ldap/ldap.cfg**。

LDAP 属性的映射文件格式

/usr/lib/security/LDAP 模块和 **secldapclntd** 守护程序使用这些映射文件来将 AIX 属性名称转换为 LDAP 属性名称。映射文件的每个项代表一个属性的转换。一个项有由四个空格分隔的字段:

```
AIX_Attribute_Name AIX_Attribute_Type LDAP_Attribute_Name LDAP_Value_Type
```

AIX_Attribute_Name	指定 AIX 属性名称。
AIX_Attribute_Type	指定 AIX 属性类型。值为 SEC_HAR、SEC_INT、SEC_LIST 和 SEC_BOOL。
LDAP_Attribute_Name	指定 LDAP 属性名称。
LDAP_Value_Type	指定 LDAP 值类型。为 **s** 的值表示单值，**m** 表示多值。

有关 LDAP 属性映射文件格式的更多信息，请参阅 *AIX 5L Version 5.2 Files Reference* 中的 **LDAP attribute mapping file format**。

相关信息

mksecldap、**start-secldapclntd**、**stop-secldapclntd**、**restart-secldapclntd**、**ls-secldapclntd**、**sectoldif** 和 **flush-secldapclntd** 命令。

secldapclntd 守护程序。

/etc/security/ldap/ldap.cfg 文件。

LDAP 属性映射文件格式。

第 5 章 PKCS #11

PKCS #11 子系统为应用程序提供了以设备类型无关方式访问硬件设备（标记）的方法。本章内容符合 PKCS #11 标准 V2.01。

使用以下组件实现 PKCS #11 子系统:

- 插槽管理器守护程序（**pkcsslotd**），它为子系统提供关于可用硬件设备状态的信息。在安装过程中以及当系统重新启动时，该守护程序会自动启动。
- 为已经实现 PKCS #11 支持的适配器提供了 API 共享对象（**/usr/lib/pkcs11/pkcs11_API.so**）作为通用接口。
- 一个特定于适配器的库，它为适配器提供 PKCS #11 支持。此分层设计使用户可以在新的 PKCS #11 设备可用时不用重新编译现有应用程序就使用该新设备。

本章包含以下信息:

IBM 4758 2 型密码协处理器

IBM 4758 2 型密码协处理器提供安全的计算环境。在试图配置 PKCS #11 子系统之前，验证适配器是否已经使用支持的微码正确地配置过。

用 PKCS #11 子系统验证 IBM 4758 2 型密码协处理器的使用。

PKCS #11 子系统设计为自动检测能在安装和重新启动过程中支持 PKCS #11 调用的适配器。因此，将不能从 PKCS #11 接口访问任何没有正确配置的 IBM 4758 2 型密码协处理器，并且发送到适配器的调用会失败。要验证适配器是否设置正确，请完成以下操作:

1. 输入以下命令以确保适配器的软件安装正确:

   ```
   lsdev -Cc adapter | grep crypt
   ```

   如果 IBM 4758 2 型密码协处理器没有包含在结果列表中，则检查是否正确放置此卡以及是否正确安装了支持软件。

2. 输入以下命令以确定卡中是否装入了正确的固件:

   ```
   csufclu /tmp/l ST device_number_minor
   ```

   验证 Segment 3 Image 是否装入了 PKCS #11 应用程序。如果没有装入，参照特定适配器的文档获得最新的微码和安装说明。

   注: 如果该实用程序不可用，则没有安装支持软件。

PKCS #11 子系统配置

PKCS #11 子系统自动检测支持 PKCS #11 的设备。可是，为了一些程序能使用这些设备，一些初始的安装是必要的。这些任务包括:

- 『初始化令牌』
- 『设置安全官员 PIN』
- 『初始化用户 PIN』

通过 API（通过编写 PKCS #11 应用程序）或使用 SMIT 界面可以执行这些任务。通过主 SMIT 菜单的**管理 PKCS11 子系统**或通过使用 **smit pkcs11** 快速路径访问 PKCS #11 SMIT 选项。

初始化令牌

在成功使用每一个适配器或 PKCS #11 令牌之前，必须初始化。该初始化步骤包括为标志设置一个唯一标签。该标签允许应用程序唯一地标识令牌。因此，标签不应该重复。然而，API 不验证标签是否没有重新使用过。通过 PKCS #11 应用程序或由使用 SMIT 的系统管理员执行初始化。如果令牌有一个安全官员 PIN，其缺省值设置为 87654321。初始化之后应该更改该值，以确保 PKCS #11 子系统的安全性。

初始化令牌:

1. 输入 `smit pkcs11` 进入令牌管理屏幕。
2. 选择 **初始化令牌**。
3. 从支持的适配器列表中选择一个 PKCS #11 适配器。
4. 按下 Enter 键确认您的选择。

   注: 这样会擦除令牌上的所有信息。
5. 输入安全官员 PIN（SO PIN）和唯一的令牌标签。

如果输入了正确的 PIN，命令运行完毕以后适配器会初始化或重新初始化。

设置安全官员 PIN

如果令牌有一个 SO PIN，可以从 PIN 的缺省值更改 PIN，如下所示:

1. 输入 `smit pkcs11`:
2. 选择**设置安全官员 PIN**。
3. 选择您想设置 SO PIN 的已初始化适配器。
4. 输入当前的 SO PIN 和新的 PIN。
5. 验证新的 PIN。

初始化用户 PIN

令牌初始化以后，可能有必要设置用户 PIN 以允许应用程序访问令牌对象。参考特定设备的文档以确定在访问对象之前该设备是否要求用户登录。

初始化用户 PIN:

1. 通过输入 `smit pkcs11` 进入令牌管理屏幕。
2. 选择 **初始化用户 PIN**。
3. 从支持的适配器列表中选择一个 PKCS #11 适配器。
4. 输入 SO PIN 和用户的 PIN。

5. 验证用户的 PIN。
6. 验证时，必须更改用户 PIN。

重新设置用户 PIN

要重新设置用户 PIN，可以使用 SO PIN 重新初始化 PIN 或使用现有的用户 PIN 设置用户 PIN。要执行此操作:

1. 输入 `smit pkcs11` 进入令牌管理屏幕。
2. 选择**设置用户 PIN**。
3. 选择您想设置用户 PIN 的已初始化的适配器。
4. 输入当前的用户 PIN 和新的 PIN。
5. 验证新的用户 PIN。

设置 PKCS #11 函数控制向量

如果没有装入函数控制向量，那么令牌可能不支持强加密操作。参考特定设备的文档确定令牌是否需要函数控制向量以及在何处找到它。

如果需要函数控制向量，您应该有一个密钥文件。要加载函数控制向量:

1. 输入 `smit pkcs11` 进入令牌管理屏幕。
2. 选择 **设置函数控制向量**。
3. 为令牌选择 PKCS #11 插槽。
4. 输入函数控制向量文件的路径。

PKCS #11 使用方法

应用程序要使用 PKCS #11 子系统，子系统的插槽管理器守护程序必须正在运行，而且应用程序必须装入 API 的共享对象。

通常在引导时，**inittab** 调用 **/etc/rc.pkcs11** 脚本来启动槽管理器。在启动槽管理器守护程序前，该脚本验证系统中的适配器。因此，在用户登录系统前，插槽管理器守护程序是不可用的。守护程序启动后，在没有系统管理员干预的情况下，子系统将对支持适配器的数目和类型的所有更改进行合并。

可以通过运行时链接到对象中或使用延迟的符号解析将 API 装入。例如，应用程序可以用以下方式获取 PKCS #11 函数列表:

```
d CK_RV (*pf_init)();
void *d;
CK_FUNCTION_LIST *functs;

d = dlopen(e, RTLD_NOW);
if ( d == NULL ) {
   return FALSE;
}

pfoo = (CK_RV (*)())dlsym(d, "C_GetFunctionList");
if (pfoo == NULL) {
   return FALSE;
}

rc = pf_init(&functs);
```

第 6 章 X.509 证书认证服务和公用密钥基础结构

证书认证服务为 AIX 5.2 操作系统提供使用 X.509 公用密钥基础结构（PKI）证书认证用户和将证书与进程关联作为用户身份证明的能力。通过可装载的认证模块框架（LAMF），用于提供 DCE、Kerberos 的相同可扩展的 AIX 机制和其它认证机制提供此能力。

以下本节讨论以下主题:

证书认证服务的概述

每个参加 PKI 认证的用户帐户都有一个唯一的 PKI 证书。登录过程中将证书与密码结合起来用于认证用户。PKI 证书基于公用密钥／专用密钥技术。该技术使用两个非对称密钥来加密和解密数据。使用其中一个密钥加密的数据只能使用另一个密钥解密。用户保留一个密钥专用，叫作专用密钥，存储在专用的密钥存储器中，而以证书的形式发布另一个密钥，叫作公用密钥。证书一般在轻量级目录访问协议（LDAP）服务器上维护，在组织中公司内使用或在因特网上世界范围内使用。

名为 John 的用户要给名为 kathy 的用户发送只有她能解密的数据，John 必须从 Kathy 已发布的证书中获得公用密钥，使用 Kathy 的公用密钥加密数据，再将数据发送给她。Kathy 将使用在她专用密钥存储器中她的专用密钥解密来自 John 的数据。

此技术也用于数字签名。如果 Kathy 想发送由她数字签名的数据给 John，Kathy 将使用她的专用密钥来数字签名数据并且发送数据和数字签名给 John。John 将获得来自 Kathy 的已发布证书的公用密钥，在使用数据前用公用密钥来验证数字签名。

这两种情况下，Kathy 的专用密钥在专用的密钥存储器中维护。许多类型的专用密钥存储器包含智能卡和文件，但是所有密钥存储器类型都通过使用密码或个人识别码（PIN）来保护专用密钥。它们通常为多个专用密钥连同证书和其它 PKI 对象一起提供存储。用户通常拥有他们自己的密钥存储器。

在登录过程中，证书认证服务使用数字签名技术来认证用户。证书认证服务基于用户帐户名称找到用户的证书和密钥存储器，使用用户的密码从用户的密钥存储器中获得证书的匹配专用密钥，使用用户的专用密钥标识数据项，并用来自证书的用户的公用密钥来检查签名。用户认证后，系统在受保护的内存中存储用户的证书，将证书与用户创建的每个进程关联。对用户和操作系统内核拥有的任何进程，该内存中关联启用对用户证书的快速访问。

证书

理解证书认证服务需要对证书、证书格式和证书生命周期管理的基本理解。证书是遵循 X.509 标准的标准化对象，其中，版本 3（X.509v3）是最新版。认证中心（CA）创建、标识和发出证书，它通常是接受和处理证书请求的软件应用程序。证书由几个证书属性组成。一些属性是必要的，但许多是可选的。在此文档中通常使用和讨论的证书属性有:

- 证书版本 – X.509 版本号（即 1、2 或 3）。
- 序列号 – 一个将该证书从所有其它由相同 CA 发出的证书中唯一地区别开来的证书序列号。

- 签发者名称 – 指定证书的签发 CA 的名称。
- 有效期 – 证书的激活和到期日。
- 公用密钥 – 公用的密钥。
- 主题专有名称 – 指定证书所有者的名称。
- 主题备用名称电子邮件 – 所有者的电子邮件地址。
- 主题备用名称 URI – 所有者的 Web 站点 URI/URL。

每个证书有一个唯一的版本号来表示符合哪个版本的 X.509 标准。每个证书有一个序列号唯一地将其与同一 CA 发出的所有其它证书区别开来。序列号仅对发出 CA 是唯一的。证书的签发者名称标识发出 CA。

证书只有在两个指定的日期之间是有效的: “不早于”日期和“不晚于”日期。因此，可能在有效日期之前创建证书，在将来某个日期之前。证书有 3 个月到 5 年的生命范围是普遍的。

主题专有名称通过使用名为“专有名称”（DN）的专用的命名格式指定证书所有者。DN 考虑了国家或地区、组织、城市、州、所有者名称和其它与请求实体关联的属性（通常是人，但不限于人）的规范。主题备用名称电子邮件考虑了所有者电子邮件地址的规范，主题备用名称 URI 考虑了所有者的 Web 站点 URI/URL 的规范。

认证中心和证书

认证中心发出、存储并通常发布证书。发布证书的公共位置是在 LDAP 服务器上，因为 LDAP 允许对面向团体定向数据方便的访问。

CA 还处理证书的取消和证书撤销列表（CRL）的管理。取消证书是发布由于某些原因（除证书有效期到期之外）特定证书不再有效的事实的行为。因为证书的副本可以在发出 CA 的控制外维护和使用，CA 在 CRL 中发布已取消证书的列表使得外面的实体能查询列表。这样就让实体负责用已复制的证书来比较已复制的证书和发出 CA 的 CRL。CA 只能取消它创建或发出的证书。不能取消由其它 CA 发出的证书。

取消证书的管理原因包含:

- 证书的专用密钥的泄漏。
- 证书所有者离开公司。
- CA 的泄漏。

CA 也有它们自己的识别证书。其它使用中（例如，信任链），它允许 CA 在对等通信中互相识别。

许多 CA 支持查询和取消证书的证书管理协议（CMP）。协议支持多个方法在客户机（也称为端实体）和 CA 之间建立安全连接，虽然不是全部客户机和 CA 支持所有方法。一个公共的方法需要每个证书创建和取消请求使用引用号和 CA 识别的密码。可能也需要例如 CA 识别的特殊证书这样的其它数据。取消请求可能需要取消证书的匹配专用密钥。

虽然 CMP 为证书创建和取消请求作准备，却不支持 CRL 查询请求。实际上，经常通过带外方法访问 CRL。因为经常在 LDAP 服务器上发布 CRL，所以软件应用程序能从 LDAP 服务器中获得 CRL 并手工扫描 CRL。另一种出现的方法是联机证书状态协议（OCSP），但不是所有的 CA 都支持 OCSP。

CA 通常由政府组织或可信的私人组织拥有和操作，它们试图提供保证，使之发出的证书与申请发出证书的人相符。短语*发出证书*意味着创建证书，与请求已发布证书的副本不同。

证书存储格式

存储个别证书的最通用的格式是使用特异编码规则（DER）的抽象语法符号表示法 V1（ASN.1）格式。该格式引用为 *DER 格式*。

密钥存储器

密钥存储器（有时称为*密钥集*）包含匹配它们证书的公用密钥的用户专用密钥。为了方便地识别，通常由用户将一个唯一的密钥标签指定给每个专用密钥。密钥存储器是受密码保护的，在用户访问密钥或添加新密钥之前需要用户输入密码。通常，用户拥有他们自己的密钥存储器。密码存储器有许多不同的格式，例如：智能卡、基于 LDAP、基于文件等。不仅形式不同，还有访问它们所用的方法和存储专用密钥数据的格式也不同。证书认证服务仅支持基于文件的密钥存储器。

证书认证服务的实现

证书认证服务作为客户机 / 服务器模型运行。为创建和维护 X.509 V3 证书和证书撤销列表（CRL），服务器端包含认证中心（CA）。（通常，一个组织对整个组织使用一个 CA。）客户机包含每个加入 PKI 认证的系统需要的软件（命令、库、装入模块和配置文件）。服务器的安装软件包是 **cas.server**，客户机的安装软件包是 **cas.client**。

创建 PKI 用户帐户

创建 PKI 用户帐户，使用 AIX **mkuser** 命令。创建后，每个帐户有一个证书和一个专用的密钥存储器。（也能将现有的帐户转换为 PKI 帐户，但是需要其它步骤。）管理员将密钥存储器密码提供给新用户，新用户能登录到系统并更改他们的密钥存储器密码。

用户认证数据流

本节描述怎样认证 PKI 用户。用户可以有与他们帐户关联的多个证书。为方便认证，每个证书有与它关联的唯一的，用户定义的标记值，但只有一个证书能指定为认证证书。证书认证服务使用名为 **auth_cert** 的每个用户的属性来指定用户的哪个证书是用户的认证证书。**auth_cert** 属性的值是证书的标记值。

在每用户基础上的 LDAP 下维护证书、标记、匹配密钥存储器位置、匹配密钥标签和其它相关数据。用户名和标记的组合允许证书认证服务在 LDAP 服务器下定位证书。有关 PKI LDAP 层的更多信息，请参阅第 81 页的『PKI LDAP 层（证书存储器）』。

登录时，用户提供用户名和密码。通过用户名，系统从用户的 **auth_cert** 属性中检索用户的认证证书标记。结合用户名和标记，系统从 LDAP 中检索用户的证书、密钥存储器位置和匹配密钥标签。检查在证书中发现的有效期值来确定证书是已经到期还是未达到激活日期。接着系统根据密钥存储器位置、密钥标签和提供的密码来检索用户的专用密钥。检索专用密钥后，系统通过内部签署进程来验证专用密钥和证书匹配。如果二者匹配，用户通过登录过程的 PKI 认证步骤。（这并不意味着用户已登录。允许用户访问系统前，在用户帐户上的 AIX 执行几项其它帐户检查。）

对于用作认证证书的证书，必须使用可信签字密钥签署该证书。为了以后的引用将签名和证书一起存储在 LDAP 下。此实现需要在将标记指定给 **auth_cert** 前证书已拥有签名。

认证过程不比较证书和 CRL。这是由于性能原因（CRL 花费时间来获取和扫描，并且可能暂时不可用），但是还因为 CRL 的发布延迟（通过 CRL，使得证书取消成为禁用用户帐号的可怜的替代品，CA 在发布取消证书前可能延迟一个小时或更多时间）。

认证不需要 CA 也无关紧要。除了检索 LDAP 下存储的数据之外，证书认证服务本地执行主要的工作。

服务器实现

证书认证服务的服务器端实现 Java 编写的 CA，包含连同自审查功能的注册中心（RA）。它发布证书和为 LDAP 服务器创建的 CRL。通过配置文件集（Java 属性文件），CA 是可配置的。它包含名为 **runpki** 的管理应用程

序，该应用程序在其它功能中提供子命令来启动和停止服务器，且为创建和取消证书支持 CMP。CA 需要 Java 1.3.1、IBM DB2 7.1 数据库和 IBM Directory 4.1。因为 DB2 的需要，CA 必须在用户帐户而不是 root 用户下运行。

为帮助安装和管理 **cas.server** 组件，服务器包含以下命令:

mksecpki

安装中使用该命令来配置 AIX PKI 服务器组件。作为任务的部分，该命令为认证中心创建证书认证用户帐户。

runpki

该命令允许系统管理员启动服务器。如果 JavaPKI 守护程序正在运行，必须首先停止。**runpki** 命令通过使用 **lb** 标志组合在后台中启动守护程序。如果需要在交互方式中启动守护程序，管理员可以编辑 **runpki** 命令并使用 **l** 标志而非 **lb** 标志。

对于在其下运行认证中心的用户帐户，**runpki** 命令必须在对其执行 **su -** 操作后运行。命令定位于认证中心用户帐户主目录下的 **javapki** 目录。（**mksecpki** 命令创建认证中心用户帐户。）

例如，如果认证中心用户帐户是 **pkiinst**，那么用超级权限，输入以下内容:

1. `su - pkiinst`
2. `cd javapki`
3. `runpki`

客户机实现

证书认证服务客户机实现证书认证服务的用户认证、用户管理和用户证书管理功能。在系统上安装和配置后，通过 AIX 可装载的认证模块框架（LAMF）的使用，证书认证服务集成为现有的用户认证和管理功能（例如 **mkuser**、**chuser**、**passwd** 和 **login** 命令）。还添加命令、库和配置文件来帮助管理用户证书和密钥存储器。

为了存储标准 AIX 属性，证书认证服务能与 AIX LDAP 数据库机制或基于文件数据库机制合用。证书认证服务一直使用 LDAP 来维护用户证书，甚至在使用基于文件的数据库机制时。要获取有关使用基于文件的数据库时的限制的信息，请参阅第 88 页的『规划证书认证服务』。

证书认证服务的客户机端包含两部件中大多数面向用户的软件。因为这个原因，以下节描述证书认证服务怎样维护和使用 PKI 认证需要的数据。

常规客户机功能

以下列表描述证书认证服务的一些常规功能:

- 通过 PKI 证书提供用户认证
- 提供管理用户证书和密钥存储器的命令
- 每个用户支持多个证书
- 同时支持多个 CA
- 集成到现有的 AIX 管理命令和认证中（例如，**login**、**passwd**、**mkuser**）
- 在用户创建时生成证书或用户创建后添加证书
- 用 LDAP 用户数据库或标准 AIX 基于文件的用户数据库工作
- 配置密钥大小和算法
- 关联证书和进程认证组（PAG）。

常规客户机体系结构

证书认证服务的客户机体系结构使用分层的方法，并划分为以下组成组件:

- 『Java 守护程序』
- 『服务管理层』
- 『PKI LDAP 层（证书存储器）』
- 第 82 页的『libpki.a 库』
- 第 82 页的『可装载的认证模块框架层』
- 第 82 页的『客户机命令』
- 第 83 页的『进程认证组命令』
- 第 83 页的『用户管理命令』
- 第 84 页的『配置文件』

Java 守护程序: 在客户机的基础是使用 JCE 安全软件包的基于 Java 的守护程序。守护程序管理用户密钥存储器、创建密钥对、执行 CMP 通信，并提供全部散列和加密功能。因为 PKI 服务供应商软件包的 API 对 C 应用程序是不标准的，叫作服务管理层（SML）的包装程序层 API 向应用程序和守护程序提供规范化的 API。

服务管理层: Java 守护程序的 SML 服务名为 **/usr/lib/security/pki/JSML.sml**。SML 创建证书，并创建和管理密钥存储器，但不管理证书存储。证书存储由 PKI LDAP 层管理。

通过 SML 存储专用密钥: 为存储用户密钥，Java 守护程序使用 PKCS#12 已格式化密钥存储器文件。用来加密密钥存储器中全部密钥的单一密码保护密钥存储器。将密钥存储器的位置指定为 URI。缺省情况下，证书认证服务维护 **/var/pki/security/keys** 目录中的密钥存储器文件。

密钥存储器通常在大小上受限，包括文件密钥存储器。SML 层提供管理密钥存储器的 API。

证书认证服务仅支持文件密钥存储器。不支持智能卡或 LDAP 密钥存储器。可以通过将文件密钥存储器放置在所有系统同一安装点下的共享文件系统中来支持漫游用户。

PKI LDAP 层（证书存储器）: 证书认证服务通过 PKI LDAP 层，在 LDAP 的每个用户基础上存储证书和证书相关信息。证书认证服务维护 LDAP 服务器上每个用户基础上的证书关联。用户帐户可以有多个与其关联的证书。为了方便地识别和查询，每个关联有唯一的，用户指定的标记。证书认证服务使用用户的名称和标记的组合在 LDAP 中定位用户的证书关联。

对于性能相对磁盘空间折衷方案，证书认证服务能保存 LDAP 下的整个证书或仅仅是对证书的 URI 引用。如果 URI 引用用来代替证书，证书认证服务查询引用以获得实际的证书。引用最常与在 LDAP 服务器上发布证书的 CA 结合使用。证书认证服务当前支持的 URI 引用类型是 LDAP 引用。证书认证服务以 DER 格式存储证书并期望 URI 引用以参阅 DER 格式化的证书。

证书认证服务也存储每个证书与 LDAP 服务器关联的证书相同的记录中匹配的密钥存储器和密钥标签的类型和位置。允许用户有一个以上密钥存储器，为快速发现证书的匹配专用密钥允许证书认证服务。为支持漫游的用户，用户的密钥存储器必须驻留在所有系统上的同一位置。

证书认证服务维护以每个用户为基础的 LDAP 中的 **auth_cert** 属性。该属性指定用来认证的证书的标记。

除受限于 LDAP **ldappkiadmin** 帐户的 **auth_cert** 属性外，全部 LDAP 信息对于普通用户是可读的。既然 root 用户通过 **acct.cfg** 文件访问 LDAP **ldappkiadmin** 密码，那么以 root 的有效 UID 运行的应用程序可以访问 **auth_cert** 属性。（适用于 URI 引用值的可访问性，而不是由 URI 引用值引用的数据。通常，由 URI 引用值引用的数据是公共的。）管理证书存储的 API 包含于 **libpki.a** 库。

libpki.a 库: 除作为 SML API 和 PKI LDAP 层 API 的根服务外，**libpki.a** 库收藏几种子例程。库包含执行以下操作的 API:

- 管理新配置文件
- 访问证书特定属性
- 将多个更低层功能组合到更高级功能中
- 在 SML 服务中预期是公共的

注: 不发布 API。

可装载的认证模块框架层: SML API 和 PKI LDAP API 之上驻留可装载的认证模块框架（LAMF）层。LAMF 提供 AIX 认证和有公共认证和用户管理 API 的用户管理应用程序，不考虑下层的机制（例如 Kerberos、LDAP、DCE、文件）。LAMF 使用 SML API 和 PKI LDAP API 作为实现 PKI 认证中的构建模块。

通过将 LAMP 的 API 映射到不同认证／数据库技术的装入模块的使用来执行。象 **login**、**telnet**、**passwd**、**mkuser** 等命令使用 LAMF API 来实现它们的功能；因此，当这些技术的新装入模块添加到系统中时，这些命令自动支持新认证和数据库技术。

证书认证服务添加新 LAMF 装入模块到名为 **/usr/lib/security/PKI** 的系统。为了认证，必须在使用 PKI 前由系统管理员将模块添加到 **/usr/lib/security/methods.cfg** 文件中。模块也必须在用于认证前和 **methods.cfg** 文件中的数据库类型（例如，LDAP）是成对的。包含 LAMF 模块和数据库定义的 **methods.cfg** 文件的一个示例，可以在第 99 页的『methods.cfg 文件』中找到。

一旦将定义添加到 **methods.cfg**，管理员可以将 **registry** 和 **SYSTEM** 用户属性（在 **/etc/security/user** 文件中已定义）设置到为 PKI 认证的新节值。

客户机命令: 在全部 API 层上（LAMF、PKI LDAP 和 SML）驻留命令。除支持证书认证服务（通过 LAMF）的标准 AIX 认证和用户管理命令之外，还存在几种证书认证服务特定命令。这些命令帮助用户管理证书和密钥存储器。下面是带有简短描述的命令列表。

certadd
将证书添加到 LDAP 中的用户帐户并检查证书是否取消。

certcreate
创建证书。

certdelete
从用户帐户删除证书（即，从 LDAP）。

certget
从用户帐户检索证书（即，从 LDAP）。

certlink
将对存在于远程资源库的证书的链接添加到 LDAP 中的用户帐户并检查证书是否取消。

certlist
列出与包含于 LDAP 中的用户帐户关联的证书。

certrevoke
取消证书。

certverify
验证专用密钥匹配证书并执行可信签署。

keyadd
将密钥存储器对象添加到密钥存储器。

keydelete
从密钥存储器中删除密钥存储器对象。

keylist
列出密钥存储器中的对象。

keypasswd
更改密钥存储器上的密码。

有关这些命令的更多信息。请参阅《*AIX 5L V5.2 命令参考大全*》。

进程认证组命令: 进程认证组（PAG）命令对于 AIX 是新的。PAG 是将用户认证数据与进程关联的数据项。对于证书认证服务，如果已启用 PAG 机制，用户认证证书与用户登录 shell 关联。shell 创建子进程时，PAG 传播到每个子进程。

PAG 机制需要启用 **/usr/sbin/certdaemon** 守护程序来提供该功能。缺省情况下，该机制没有启用。证书认证服务不需要 PAG 机制是启用的，但是如果是启用的则使用该机制工作。

启用 **certdaemon** 守护程序，将以下行添加到 **/etc/inittab** 文件:

```
certdaemon:2:wait:/usr/sbin/certdaemon
```

带有简短描述的 PAG 命令列表如下:

paginit
认证用户并创建 PAG 关联。

pagdel
列出与当前进程关联的认证信息。

paglist
除去在当前进程凭证中现有的 PAG 关联。

有关这些命令的更多信息，请参阅《*AIX 5L V5.2 命令参考大全*》。

用户管理命令: 与用户认证相似，证书认证服务通过 AIX LAMF 与 AIX 用户管理功能集成。象 **chuser**、**lsuser**、**mkuser** 和 **passwd** 的命令使用 LAMF API 来实现它们的功能。因此，当将为这些技术新装入模块添加到系统时，这些命令自动地支持新认证和数据库技术。

下面子节提供了 PKI 认证如何影响用户管理命令方面的更深入的观点。

以下命令受 PKI 认证进程影响:

chuser
该命令允许管理员修改 **auth_cert** 用户属性。该属性指定用来认证的证书的标记值。为了作为认证证书使用，证书必须由可信签字密钥签署。（通过该命令，证书属性、证书存储属性和密钥存储器属性是不可用的。）

lsuser 该命令列出用户的 **auth_cert** 属性的值，以及在下面列出的证书属性。**auth_cert** 属性指定用来认证的证书的标记值。（通过该命令，其它证书属性、证书存储属性和密钥存储器属性是不可用的。）

lsuser 命令列出的证书属性如下:

subject-DN
用户的对象专有名称。

subject-alt-name
用户主题备用名称电子邮件。

valid-after
用户证书变为有效的日期。

valid-until
用户证书变为无效的日期。

issuer 发行商的专有名称。

mkuser

该命令为管理员提供在用户创建时间生成证书的选项。在为还没有认证证书的用户创建用户期间，管理员能使用 **mkuser** 命令来生成证书。任选的，如果用户已经有认证证书，但没有用户帐户，管理员能不生成证书而创建帐户，随后添加证书（和密钥存储器）。该选项的缺省值由 **cert** 属性在 newuser 节中的 **/usr/lib/security/pki/policy.cfg** 文件中指定。

当为用户使用 **mkuser** 命令自动地生成认证证书时需要许多缺省值。在 **/usr/lib/security/pki/policy.cfg** 文件的 **newuser** 节中指定许多这些值。**newuser** 节提供对这些缺省值的管理控制。一些缺省值如下:

- CA
- **auth_cert** 属性的值
- 密钥存储器的位置
- 密钥存储器的密码
- 专用密钥标签
- 主题备用名称电子邮件字段的域名

创建 PKI 用户帐户和非 PKI 用户帐户行为上的不同是: 如果 **mkuser** 命令为帐户生成认证证书，创建 PKI 用户帐户需要密码来加密专用密钥。因为 **mkuser** 命令是非交互式命令，命令从 **policy.cfg** 文件中获得密码，将密钥存储器密码（专用密钥密码）设置到该值；因此，创建后帐户立即是可访问的。创建非 PKI 用户帐户时，**mkuser** 命令将密码设置为无效值，防止可访问性。

passwd

此命令在 PKI 用户帐户上使用时修改用户密钥存储器密码。它强制在 **/etc/security/user** 文件中找到密码限制规则、它强制在 **/etc/security/passwd** 文件中找到标志属性，且它强制 PKI 服务供应商需要的任何规则。

因为基于文件的密钥存储器用用户密码加密它们的专用密钥，**root** 用户不知道密钥存储器的当前密码时不能重新设置基于文件的密钥存储器的密码。如果用户忘记其密钥存储器的密码，则 root 用户不能重新设置密码，除非 root 知道该密钥存储器的密码。如果不知道密码，可能必须给用户发布新密钥存储器和新证书。

配置文件: 证书认证服务为配置客户机使用配置文件: **acct.cfg**、**ca.cfg** 和 **policy.cfg**。SMIT 界面为这些配置文件提供支持。以下节提供关于配置文件的信息。

acct.cfg 文件: **acct.cfg** 文件由 CA 节和 LDAP 节构成。CA 节包含不适合公用可读的 **ca.cfg** 文件的专用 CA 信息，例如 CMP 引用号和密码。LDAP 节包含不适合公共访问的专用的 LDAP 信息，例如 PKI LDAP 管理名称和密码。

对 **ca.cfg** 文件中的每个 CA 节，**acct.cfg** 文件应该包含同样命名的 CA 节，全部 CA 节必须唯一命名。LDAP 节全部命名为 **ldap**，因为这个原因，CA 节不能命名为 **ldap**。同样，没有节能命名为 **default**。LDAP 节必须存在，且也必须存在至少一个名为 **local** 的 CA 节。

CA 节包含以下属性:

capasswd
指定 CA 的 CMP 密码。密码的长度由 CA 指定。

carefnum
指定 CA 的 CMP 引用号。

keylabel
指定在可信密钥存储器中用来签署证书申请的专用密钥的标签。

keypasswd
指定可信密钥存储器密码。

rvpasswd
指定用于 CMP 的取消密码。密码的长度由 CA 指定。

rvrefnum
指定用于 CMP 的取消引用号。

LDAP 节包含以下属性:

ldappkiadmin
指定在 **ldapservers** 中列出的 LDAP 服务器的帐户名称。

ldappkiadmpwd
指定 LDAP 服务器帐户的密码。

ldapservers
指定 LDAP 服务器名称。

ldapsuffix
指定由 **mkuser** 命令添加到用户证书 DN 的 DN 属性。

以下是 **acct.cfg** 文件示例:

```
local:
 carefnum = 12345678
 capasswd = password1234
 rvrefnum = 9478371
 rvpasswd = password4321
 keylabel = "Trusted Key"
 keypasswd = joshua

ldap:
 ldappkiadmin = "cn=admin"
 ldappkiadmpwd = secret
 ldapservers = "ldap.server.austin.ibm.com"
 ldapsuffix = "ou=aix,cn=us"
```

有关更多信息，请参阅 *AIX 5L Version 5.2 Files Reference*。

ca.cfg 文件: **ca.cfg** 文件由 CA 节构成。CA 节包含为生成证书申请和证书撤销申请，证书认证服务使用的公共 CA 信息。

对于 **ca.cfg** 文件中的每个 CA 节，**acct.cfg** 文件应该包含一个同样命名的 CA 节。**ca.cfg** 文件中的每个 CA 节名称必须是唯一的。必须存在至少一个名为 **local** 的节。节不能命名为 **ldap** 或 **default**。

CA 节包含以下属性:

algorithm
指定公用密钥算法（例如，RSA）。

crl 指定 CA 的 CRL URI。

dn 指定创建证书时使用的基本 DN。

keysize
指定以位计算的最小的密钥大小。

program
指定 PKI 服务模块文件名称。

retries
指定联系 CA 时重试次数。

server 指定 CA 的 URI。

signinghash
指定用于签署证书的散列算法（例如，MD5）。

trustedkey
指定包含用于签署认证证书的可信签字密钥的可信密钥存储器。

url 为主题备用名称 URI 指定缺省值。

缺省 CA 节命名为 local。以下是 **ca.cfg** 文件的一个示例:

```
local:
 program = /usr/lib/security/pki/JSML.sml
 trustedkey = file:/usr/lib/security/pki/trusted.p15
 server = "cmp://9.53.230.186:1077"
 crl = "ldap://dracula.austin.ibm.com/o=aix,c=us"
 dn = "o=aix,c=us"
 url = "http://www.ibm.com/"
 algorithm = RSA
 keysize = 512
 retries = 5
 signinghash = MD5
```

有关更多信息，请参阅 *AIX 5L Version 5.2 Files Reference*。

policy.cfg 文件: **policy.cfg** 文件由四个节构成: **newuser**、**storage**、**crl** 和 **comm**。这些节修改一些系统管理命令的行为。**mkuser** 命令使用 **newuser** 节。**certlink** 命令使用 **storage** 节。**certadd** 和 **certlink** 命令使用 **comm** 和 **crl** 节。

newuser 节包含以下属性:

ca 指定生成证书时 **mkuser** 命令使用的 CA。

cert 指定缺省情况下 **mkuser** 命令是生成证书（new）还是不生成（get）。

domain
指定生成证书时 **mkuser** 命令使用的证书的主题备用名称电子邮件值的域部分。

keysize
指定生成证书时 **mkuser** 命令使用的以位计算的最小的加密密钥大小。

keystore
指定生成证书时 **mkuser** 命令使用的密钥存储器 URI。

keyusage
指定生成证书时 **mkuser** 命令使用的证书的密钥使用值。

label 指定生成证书时 **mkuser** 命令使用的专用密钥标签。

passwd
指定生成证书时 **mkuser** 命令使用的密钥存储器的密码。

subalturi
指定生成证书时 **mkuser** 命令使用的证书的主题备用名称 URI 值。

tag 指定 cert=new 创建用户时 **mkuser** 命令使用的 **auth_cert** 标记值。

validity
指定生成证书时 **mkuser** 命令使用的证书的有效期值。

version
指定要创建的证书的版本号。支持的值仅有 3。

storage 节包含以下属性:

replicate
指定 **certlink** 命令是保存证书的副本（**yes**），还是只是链接（**no**）。

crl 节包含 **check** 属性，该属性指定 **certadd** 和 **certlink** 命令是否应该检查 CRL（**yes**），或不检查（**no**）。

comm 节包含 **timeout** 属性，该属性指定当使用 HTTP（例如，正在检索 CRL）请求证书信息时，**certadd** 和 **certlink** 使用的以秒计算的超时周期。

以下是 **policy.cfg** 文件的一个示例:

```
newuser:
 cert = new
 ca = local
 passwd = pki
 version = "3"
 keysize = 512
 keystore = "file:/var/pki/security/keys"
 validity = 86400

storage:
 replicate = no

crl:
 check = yes

comm:
 timeout = 10
```

有关更多信息，请参阅 *AIX 5L Version 5.2 Files Reference*。

审计日志事件: 证书认证服务客户机生成以下审计日志事件:

- CERT_Create
- CERT_Add
- CERT_Link
- CERT_Delete
- CERT_Get
- CERT_List
- CERT_Revoke
- CERT_Verify
- KEY_Password

- KEY_List
- KEY_Add
- KEY_Delete

跟踪事件: 证书认证服务客户机在 3B7 和 3B8 范围内生成几个新的跟踪事件。

规划证书认证服务

以 AIX 5.2 开始的证书认证服务是可用的。对证书认证服务的最小软件需求是一台 DB2 服务器、一台 IBM 目录服务器和一台证书认证服务服务器。全部能安装在一个系统或一个系统组合上。每个企业必须为他们的环境确定最好选项。

本节提供规划证书认证服务的信息，如下:

- 『证书注意事项』
- 『密钥存储器注意事项』
- 『用户注册表注意事项』
- 第 89 页的『配置注意事项』
- 第 89 页的『安全性注意事项』
- 第 89 页的『其它证书认证服务注意事项』

证书注意事项

证书认证服务支持 X.509 V3 证书。还支持几个 V3 证书属性，但不是全部证书属性。获取受支持的证书属性的列表，请参阅 **certcreate** 命令和 **ca.cfg** 文件。证书认证服务包含受限的 Teletex 字符集的支持。特定地，证书认证服务只支持 7 位（ASCII 子集）Teletex。

密钥存储器注意事项

证书认证服务支持密钥存储器文件。不支持智能卡、LDAP 密钥存储器和其它类型的密钥存储器。

缺省情况下，将用户密钥存储器保留在本地文件系统的 **/var/pki/security/keys** 目录下。因为密钥存储器对于系统是本地的，其它系统不能访问它们；因而，用户认证将限制在包含用户的密钥存储器的系统中。考虑到漫游用户，将用户的密钥存储器以相同的密钥存储器名称复制到其它系统的同一位置，或者将密钥存储器放置在分布式文件系统上。

注: 必须谨慎来确保对用户密钥存储器的访问许可权没有改变。（在 AIX 中，LDAP 中的每个证书包含到包含证书专用密钥的专用密钥存储器的路径名称。为了用于认证，密钥存储器必须存在于 LDAP 中指定的路径名称。）

用户注册表注意事项

证书认证服务支持 LDAP 用户注册表。LDAP 也是推荐的和证书认证服务一同使用的用户注册表类型。

证书认证服务也支持基于文件的用户注册表。为了基于文件的 PKI 正确工作，管理员必要强制某些限制。特定地，加入 PKI 认证的不同系统上同样命名的用户帐户必须指向同一帐户。

例如，*系统 A* 上的用户 *Bob* 和*系统 B* 上的用户 *Bob* 必须指向同一用户 *Bob*。这是因为证书认证服务使用 LDAP 在每个用户基础上存储证书信息。用户名作为索引密钥来访问该信息。因为基于文件的注册表对于每个系统是本地的，LDAP 对于所有系统是全局的，加入 PKI 认证的所有系统上用户名必须映射到 LDAP 名称空

间中唯一的用户名。如果系统 *A* 上的用户 *Bob* 与系统 *B* 上的用户 *Bob* 不同，或者只有 *Bob* 中的一个能加入 PKI 认证，或者每个 *Bob* 帐户必须使用不同的 LDAP 名称空间／服务器。

配置注意事项

为了配置简单，考虑维护在分布式文件系统上的三个配置文件（**acct.cfg**、**ca.cfg** 和 **policy.cfg**），使用符号链接来避免必须在每个系统上修改配置文件。在这些文件上维护正确的访问控制设置。因为在这些文件中的信息将跨网络传送，所以该情况可能增加安全漏洞。

安全性注意事项

acct.cfg 文件

acct.cfg 文件包含敏感的 CA 引用号和密码（请参阅 **acct.cfg** 的 **carefnum**、**capasswd**、**rvrefnum** 和 **rvpasswd** 属性描述）。当分别创建证书和取消证书时为了 CMP 与 CA 通信，单独使用这些值。如果遭受破坏，入侵者可能能够随意创建证书以及随意取消任何人的证书。

为了限制风险，考虑将证书创建或取消限制到少量的系统。仅在创建证书的系统上需要 **carefnum** 和 **capasswd** 属性（通过 **certcreate** 或 **mkuser** 命令）。这可能意味着限制用户帐户创建到同样的系统设置。

注: 用户创建过程中可以配置 **mkuser** 命令以自动创建证书，或它可以创建账户而无需证书，由此管理员必须随后创建和添加证书。

同样地，仅在取消证书（通过 **certrevoke** 命令）的系统上，才需要 **rvrefnum** 和 **rvpasswd** 属性值。

acct.cfg 文件也包含敏感可信签字密钥信息（请参阅 **acct.cfg** 文件的 **keylabel** 和 **keypasswd** 属性描述）。为特殊的证书验证操作单独使用这些值。如果遭受破坏，入侵者可能能够伪造已验证的证书。

为了限制风险，考虑限制证书验证到少量系统。只有在需要证书验证的系统上，才需要 **acct.cfg** 文件的 **keylabel** 和 **keypasswd** 属性，以及 **ca.cfg** 文件的 **trustedkey** 属性。特定地，在需要 **mkuser**（启动了自动创建证书）和 **certverify** 命令的系统上。

激活新帐户

创建 PKI 用户帐户时，如果将 **policy.cfg** 文件中 **newuser** 节的 **cert** 属性设置为 **new**，**mkuser** 命令创建活动的 PKI 帐户并完全具有工作的证书和密码。**newuser** 节中的 **passwd** 属性指定帐户上的密码。因为密钥存储器需要密码以存储专用密钥。这与用户帐户创建的其它类型的不同在于管理员必须首先创建帐户，然后在帐户激活前设置密码。

root 用户和密钥存储器密码

不象其它帐户类型，**root** 用户不知道帐户的密码就能更改帐户的密码，PKI 帐户不允许这样。这是因为帐户密码用来加密密钥存储器，而不知道密码就不能解密密钥存储器。当用户忘记密码时，必须发出新证书并创建新的密钥存储器。

其它证书认证服务注意事项

规划证书认证服务时其它的注意事项包含如下内容:

- 证书认证服务包含自己的认证中心（CA）。证书认证服务不支持其他 CA 实现。
- 密钥大小越大，生成密钥对和加密数据所需的时间越多。不支持基于硬件的加密。
- 证书认证服务为 LDAP 使用 IBM 目录。证书认证服务不支持其他 LDAP 实现。
- 证书认证服务为数据库支持使用 DB2。证书认证服务不支持其他数据库实现。
- 证书认证服务需要所有命令、库和守护程序运行在 Unicode 环境中。

证书认证服务的封装

证书认证服务的软件包组件有以下内容:

表 7. 证书认证服务的封装

软件包名称	文件集	内容	相关性	安装
cas.server	cas.server.rte	认证中心（CA）	• AIX 5.2 • Java131（随 AIX 基介质一起提供） • Java131 安全性扩展（随扩展包一起提供） • IBM 目录服务器（LDAP） • DB2 7.1	手册
cas.client	cas.client.rte	• Cert 命令 • PKI Auth 装入模块 • libpki.a • SML 模块 • 配置文件 • Java 守护程序	• AIX 5.2 • Java131（随 AIX 基介质一起提供） • Java131 安全性扩展（随扩展包一起提供） • IBM 目录客户机（LDAP） • PAG（设想）	手册
cas.msg	cas.msg.[lang].client	消息编目	cas.client	手册
bos	bos.security.rte	PAG 命令和守护程序	不适用	和内核一起安装

cas.server 软件包包含 CA，在 **/usr/cas/server** 和 **/usr/cas/client** 目录中安装。通常，一个组织仅使用一个 CA，因此，手工安装该软件包。该软件包在 IBM 目录服务器端的先决条件是 **db2_07_01.client**、**Java131.rte** 和 **Java131.ext.security**。安装 AIX 5.2 操作系统时，缺省情况下安装 **Java131.rte 软件包**，但是手工安装其它软件包。

为了 **db2_07_01.client** 软件包工作，**db2_07_01.server** 软件包必须安装在网络上的系统上。

cas.client 软件包包含支持证书认证服务的每个客户机系统所需的文件。没有该软件包，系统不能加入 AIX PKI 认证。

安装和配置证书认证服务

证书认证服务的安装由执行以下过程构成:

- 第 91 页的『安装和配置 LDAP 服务器』
- 第 93 页的『安装和配置证书认证服务服务器』
- 第 94 页的『为证书认证服务服务器配置 LDAP』
- 第 96 页的『配置证书认证服务客户机』
- 第 99 页的『管理配置示例』

安装和配置 LDAP 服务器

当为 PKI 用户证书数据安装和配置 LDAP 时可能发生以下情况。

- 如果没有安装 LDAP 服务器软件，执行以下过程:
  1. 『LDAP 服务器安装』
  2. 『LDAP 服务器配置』
  3. 第 92 页的『为 PKI 配置 LDAP 服务器』
- 如果已安装和配置 LDAP 服务器软件，但没有为 PKI 配置，执行第 92 页的『为 PKI 配置 LDAP 服务器』。

LDAP 服务器安装

有关安装 IBM 目录服务器软件的详细说明能在 **ldap.html.en_US.config** 文件集中包含的产品文档中找到。安装 **ldap.html.en_US.config** 文件集后，可以使用以下 URL 上的 web 浏览器查看文档: **file:/usr/ldap/web/C/getting_started.htm**。

LDAP 服务器安装过程如下:

1. 作为 **root** 用户登录。
2. 将 AIX 基本操作系统 CD 的卷 1 放入 CD-ROM 驱动器。
3. 在命令行输入 **smitty install_latest** 并按下 Enter 键
4. 选择 **Install Software**。
5. 选择输入设备或包含 IBM 目录服务器软件的软件目录，按下 Enter 键。
6. 使用 **F4** 键来列出在 **Software to Install** 字段中的安装软件包。
7. 选择 **ldap.server** 软件包，按下 Enter 键。
8. 验证 **AUTOMATICALLY install requisite software** 选项已设置为 **YES**，并按下 Enter 键。这将安装 LDAP 服务器和客户机文件集以及 DB2 后端数据库文件集。

   安装的文件集包含以下内容:

   - **ldap.client.adt**（目录客户机 SDK）
   - **ldap.client.dmt**（目录客户机 DMT）
   - **ldap.client.java**（目录客户机 Java）
   - **ldap.client.rte**（目录客户机运行时环境）
   - **ldap.server.rte**（目录服务器运行时环境）
   - **ldap.server.admin**（目录服务器）
   - **ldap.server.cfg**（目录服务器配置）
   - **ldap.server.com**（目录服务器框架）
   - **db2_07_01.***（DB2 运行时环境和关联的文件集）

   DB2 软件包，**db2_07_01.jdbc**，也必须安装。DB2 软件包，**db2_07_01.jdbc**，位于 Expansion Pack CD。使用以上列出的安装过程安装 **db2_07_01.jdbc** 软件包。

LDAP 服务器配置

安装 LDAP 和 DB2 文件集后，必须配置 LDAP 服务器。即使通过命令行和文件编辑能执行配置，为了减轻管理和配置，推荐 LDAP Web 管理员。该工具需要 Web 服务器。

Apache Web 服务器应用程序位于 LINUX Applications CD 的 AIX Toolbox 中。使用 SMIT 界面或 **geninstall** 命令来安装 Apache Web 服务器。也能使用其它 Web 服务器，要获取详细信息请参阅 LDAP 文档。

配置 LDAP 的详细说明能在产品 HTML 文档中找到。下面是配置步骤的简明描述:

1. 使用 **ldapcfg** 来设置 LDAP 数据库的 admin DN 和密码。管理员是 LDAP 数据库的 **root** 用户。用密码 **secret** 配置 **cn = admin** 的管理员 DN，输入以下内容:

   ```
   # ldapcfg -u cn=admin -p secret
   ```

   稍后配置每个客户机时将需要 DN 和密码。特定地，将 DN 和密码用作 **acct.cfg** 文件中 **ldap** 节的 **ldappkiadmin** 和 **ldappkiadmpwd** 属性。
2. 使用 Web 服务器配置文件的位置配置 Web 管理员工具，如下:

   ```
   # ldapcfg -s apache -f /etc/apache/httpd.conf
   ```
3. 重新启动 Web 服务器。对于 Apache 服务器，使用命令:

   ```
   # /usr/local/bin/apachectl restart
   ```
4. 用 URL **http:// hostname/ldap** 来访问 Web 管理员。然后使用在步骤 2 中配置的 LDAP 管理员 DN 和密码登录。
5. 使用 Web 管理员工具，遵循配置 DB2 数据库后端的指导，重新启动 LDAP 服务器。

为 PKI 配置 LDAP 服务器

证书认证服务需要两个分离的 LDAP 目录信息树。CA 使用一个树发布证书和 CRL。每个客户机使用另一个树存储和检索每个用户 PKI 数据。以下步骤配置用于存储和检索每个用户 PKI 数据的 LDAP 目录信息树。

1. **添加 LDAP 配置后缀项**。PKI 数据的缺省后缀是 **cn=aixdata**。对所有的 AIX 数据，将 PKI 证书数据放置在缺省后缀下。PKI 数据的缺省数据 root 是 **ou=pkidata**，**cn=aixdata**。所有 PKI 数据放置在该位置。

   PKI 数据后缀

   cn=aixdata

   对于所有 AIX 数据的公共后缀。如果其它 AIX 数据正在使用 LDAP 服务器，则可能已经存在。

   后缀配置项可通过 Web 管理员工具，或直接编辑 LDAP 服务器配置文件进行添加。

   使用 Web 管理员添加后缀配置项，请执行以下操作:

   a. 从左边的菜单中选择 **Settings**。
   b. 选择 **Suffixes**。
   c. 为 PKI 数据输入必要的后缀，然后单击 **Update** 按钮。
   d. 成功添加后缀后，重新启动 LDAP 服务器。

   通过编辑 LDAP 服务器配置文件添加后缀配置项，执行以下内容:

   a. 在 **/usr/ldap/etc/slapd32.conf** 文件中，定位包含以下内容的行

      ```
      ibm-slapdSuffix: cn=localhost
      ```

      这是缺省系统后缀。
   b. 为 PKI 数据添加必要的 `ibm-slapdSuffix` 项。例如，能添加与以下内容相似的后缀项:

      ```
      ibm-slapdSuffix: cn=aixdata
      ```
   c. 保存配置文件更改。
   d. 重新启动 LDAP 服务器。
2. **添加 PKI 数据后缀、Root 和 ACL 数据库项**。数据 Root 是 LDAP 目录结构中的点，其下驻留所有的 PKI 数据。对于为所有 PKI 数据设置访问规则的数据 Root，ACL 是访问控制列表。提供 **pkiconfig.ldif**

文件将后缀、root 和 ACL 项添加到数据库中。首先，添加后缀和 root 数据库项和 PKI 数据管理员密码。文件的第一个部分将缺省后缀项添加到数据库中，设置密码如下:

```
dn: cn=aixdata
objectclass: top
objectclass: container
cn: aixdata

dn: ou=pkidata,cn=aixdata
objectclass: organizationalUnit
ou: cert
userPassword: <<password>>
```

编辑 **pkiconfig.ldif** 文件，对于 PKI 数据管理器用您的密码替换 **userPassword** 属性后的 <<password>> 字符串。

稍后配置每个客户机时将需要 DN 和 **userPassword** 值。特定地，将 DN（`ou=pkidata, cn=aixdata`）和 *password* 的值用作 **acct.cfg** 文件中的 **ldap** 节中的 **ldappkiadmin** 和 **ldappkiadmpwd** 属性。

文件的第二部分更改所有权并为 PKI 数据添加 ACL，如下:

```
dn: ou=pkidata,cn=aixdata
changetype: modify
add: entryOwner
entryOwner: access-id:ou=pkidata,cn=aixdata
ownerPropagate: true

dn: ou=pkidata,cn=aixdata
changetype: modify
add: aclEntry
aclEntry: group:cn=anybody:normal:grant:rsc:normal:deny:w
aclEntry: group:cn=anybody:sensitive:grant:rsc:sensitive:deny:w
aclEntry: group:cn=anybody:critical:grant:rsc:critical:deny:w
aclEntry: group:cn=anybody:object:deny:ad aclPropagate: true
```

注: 要避免危害到 PKI 实现的完整性，请不要对 ACL 设置作任何更改。

pkiconfig.ldif 文件可以编辑以使用除了缺省值以外的文件后缀，然而只对有经验的 LDAP 管理员推荐使用。然后可以使用下面的 **ldapadd** 命令使 **ldif** 文件适用于数据库。用本地 LDAP 管理员 DN 和密码替换 **-D** 和 **-w** 选项的值，如下:

```
# ldapadd -c -D cn=admin -w secret -f pkiconfig.ldif
```

3. **重新启动 LDAP 服务器**。使用 web 管理器工具，或通过杀死和重新启动 **slapd** 进程来重新启动 LDAP 服务器。

安装和配置证书认证服务服务器

安装和配置证书认证服务，请执行以下操作:

1. 从 Expansion Pack CD 中安装 Java 安全性文件集（**Java131.ext.security.***）。所需的软件包如下:
   - **Java131.ext.security.cmp-us**（Java 证书管理）
   - **Java131.ext.security.jce-us**（Java 密码术扩展）
   - **Java131.ext.security.jsse-us**（Java 安全套接字扩展）
   - **Java131.ext.security.pkcs-us**（Java 公用密钥密码术）
2. 从 **/usr/java131/jre/lib/ext** 中将 **ibmjcaprovider.jar** 文件移动到另一个目录中。该文件与 Java 安全性文件集冲突，为了证书认证服务的正确运行必须移动该文件。
3. 从 Expansion Pack CD 中安装证书认证服务服务器文件集（**cas.server.rte**）。

为证书认证服务服务器配置 LDAP

通过执行以下步骤配置证书认证服务服务器来与 LDAP 一同工作:

1. 如果还没有安装，那么在支持 **cas.server** 软件包的系统上安装 IBM 目录客户机软件包。
2. 如果还没有配置，那么配置 IBM 目录客户机，如下:

   ```
   # ldapcfg -l /home/ldapdb2 -u "cn=admin" -p secret -s apache \
             -f /usr/local/apache/conf/httpd.conf
   ```

   设想 Web 服务器是以上配置命令中的 Apache Web 服务器。
3. 将以下后缀添加到 **slapd.conf** 文件中，如下:

   ```
   ibm-slapdSuffix: o=aix,c=us
   ```

   可以指定不同的专有名称代替 o=aix,c=us。
4. 运行 **slapd** 命令，如下:

   ```
   # /usr/bin/slapd -f /etc/slapd32.conf
   ```
5. 添加对象类，如下:

   ```
   # ldapmodify -D cn=admin -w secret -f setup.ldif
   ```

   其中 **setup.ldif** 包含以下内容:

   ```
   dn: cn=schema
   changetype: modify
   add: objectClasses
   objectClasses: ( 2.5.6.21 NAME 'pkiuser' DESC 'auxiliary class for non-CA certificate owners'
     SUP top AUXILIARY MAY userCertificate )

   dn: cn=schema
   changetype: modify
   add: objectClasses
   objectClasses: ( 2.5.6.22 NAME 'pkiCA' DESC 'class for Cartification Authorities' SUP top
     AUXILIARY MAY ( authorityRevocationList $ caCertificate $ certificateRevocationList $
     crossCertificatePair ) )

   dn:cn=schema
   changetype: modify
   replace: attributetypes
   attributetypes: ( 2.5.4.39 NAME ( 'certificateRevocationList'
     'certificateRevocationList;binary' ) DESC '  ' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
     SINGLE-VALUE )

   replace:ibmattributetypes
   ibmattributetypes:( 2.5.4.39 DBNAME ( 'certRevocationLst' 'certRevocationLst' )
     ACCESS-CLASS NORMAL)
   ```
6. 添加项:

   ```
   # ldapadd -D cn=admin -w secret -f addentries.ldif
   ```

   addentries.ldif 包含以下内容:

   ```
   dn: o=aix,c=us
   changetype: add
   objectclass: organization
   objectclass: top
   objectclass: pkiCA
   o: aix
   ```

   注: **cas.server** 软件包中提供样本 **addentries.ldif** 和 **setup.ldif** 文件。
7. 停止并启动 **slapd** 守护程序。

创建认证中心

创建认证中心如下:

1. 创建引用文件。引用文件包含一个或多个证书创建引用号和密码对。当证书创建期间证书认证服务客户机试图对服务器认证时，一个密码对表示证书认证服务服务器接受的认证信息。文件的格式是后跟密码的引用号，都在独立的行上。例如:

   ```
   12345678
   password1234
   87654321
   password4321
   ```

   其中 12345678 和 87654321 是引用号，password1234 和 password4321 是它们各自的密码。不允许空白行。空格字符不能在引用号或密码前后。文件中必须至少存在一个引用号和密码。在 **/usr/cas/server/iafile** 中能查找到示例文件。每次设置客户机需要引用这些值。

2. 使用 **mksecpki** 命令配置 CA，如下:

   ```
   # mksecpki -u pkiuser -f /usr/cas/server/iafile -p 1077 -H ldap.cert.mydomain.com \
              -D cn=admin -w secret -i o=aix,c=us
   ```

   mksecpki 标志上的信息如下:

   -u 指定安装证书认证服务服务器所在的用户帐户名称。

   -f 指定在之前步骤中创建的引用文件。

   -p 指定 LDAP 服务器的端口号。

   -H 指定 LDAP 服务器主机名或 IP 地址。

   -D 指定 LDAP 管理器的公共名称。

   -w 指定 LDAP 管理密码。

   -i 指定用户证书数据驻留其中的 LDAP 分支。

   mksecpki 命令自动生成连同 **TrustedKey** 密钥标签的可信签字密钥和 CA 用户帐户的密码，将它放置在 **/usr/lib/security/pki/trusted.pkcs12** 密钥存储器文件中。没有必要执行『创建可信签字密钥』中的步骤，除非需要生成多个密钥或想要带有不同密钥标签和／或密码的可信签字密钥。

创建可信签字密钥

mksecpki 命令自动生成连同 **TrustedKey** 密钥标签的可信签字密钥和 CA 用户帐户的密码，并将它放置在 **/usr/lib/security/pki/trusted.pkcs12** 密钥存储器文件中。如果需要生成新的可信签字密钥或多个可信签字密钥，那么本节提供生成可信签字密钥需要的步骤。

所有允许证书创建和取消的证书认证服务客户机为了签署用户认证证书需要可信签字密钥。在独立的密钥存储器中保存密钥，对于能在其中创建证书的所有系统成为可用的。所有系统能使用单一密钥，或者为了更安全的方法，能创建和分布多个密钥。

为创建可信密钥，使用 **/usr/java131/bin/keytool** 命令。使用不存在的文件的文件名。**keytool** 命令提示输入密钥存储器密码和密钥密码。为了访问密钥存储器中的密钥，对于证书认证服务，密钥存储器密码和密钥密码必须是相同的。运行 **keytool** 命令，如下:

```
keytool -genkey -dname `cn=trusted key' -alias `TrustedKey' -keyalg RSA \
        -keystore filename.pkcs12 -storetype pkcs12ks
```

在该示例中，可信密钥标签是 **TrustedKey**，且可信密钥存储器密码是用户提供的。记住这些值，因为在配置证书认证服务客户机时需要它们。当配置证书认证服务客户机时，**acct.cfg** 文件中的 **keylabel** 和 **keypasswd** 属性需要分别设置到可信密钥标签和可信密钥存储器密码。

为了安全性原因，确保密钥存储器文件（*filename*.pkcs12）是读和写保护的。只有 root 用户会有到该文件的访问权。可信密钥应该是密钥存储器中唯一的对象。

配置证书认证服务客户机

在证书认证服务的客户机端有许多配置选项。以下节提供加入 PKI 认证的每个系统所需的配置过程。

安装可信签字密钥

将包含可信签字密钥的可信密钥存储器复制到本地系统。有关创建可信签字密钥的信息，请参阅第 95 页的『创建可信签字密钥』。可信密钥存储器的缺省位置是在 **/usr/lib/security/pki** 目录中。

因为安全性原因，确保密钥存储器文件是读和写保护的。只有 root 用户会有到该文件的访问权。

编辑 acct.cfg 文件

使用象 **vi** 命令一样的基于文本的编辑器，除去可能存在于 **/usr/lib/security/pki/acct.cfg** 文件中的所有 **ldap** 节。

配置认证中心

最低限度，必须配置本地 CA 帐户。缺省情况下，存在本地 CA 帐户，但必须将其修改以匹配您的环境。

通过基于节的配置文件的单一系统，证书认证服务支持多个 CA 的使用。当用户或软件指定 CA 时，使用缺省 CA 节名称 **local**。在适当的证书认证服务配置文件中所有系统必须有一个有效的 local 节定义。只有一个 CA 有 **local** 的节名称。所有其它 CA 必须有一个唯一的节名称。CA 节名称不能是 **ldap** 或 **default**。

以下节通过 SMT 配置屏幕指导您配置本地 CA。

更改／显示认证中心:

1. 运行 PKI SMIT，如下:

   ```
   smitty pki
   ```

2. 选择**更改／显示认证中心**。
3. 对认证中心名称字段，输入 `local`，按下 Enter 键。
4. 将 **Service Module Name** 字段设置为 **/usr/lib/security/pki/JSML.sml**。这是缺省 SML 装入模块。该字段映射到 **/usr/lib/security/pki/ca.cfg** 文件中的 **program** 属性。
5. 忽略 **CA 的证书路径名**字段。该字段映射到 **/usr/lib/security/pki/ca.cfg** 文件中的 **certfile** 属性。
6. 将 **CA 的可信密钥路径名**字段设置为本地系统上可信密钥存储器的位置的 URI。仅支持基于文件的密钥存储器。可信密钥存储器的典型的位置是在 **/usr/lib/security/pki** 目录中。（请参阅『安装可信签字密钥』。）该字段映射到 **/usr/lib/security/pki/ca.cfg** 文件中的 **trustedkey** 属性。
7. 将 **URI of the Certificate Authority Server** 字段设置为 CA 位置（**cmp://myserver:1077**）的 URI。该字段映射到 **/usr/lib/security/pki/ca.cfg** 文件中的 **server** 属性。
8. 忽略**证书分布点**字段。该字段映射到 **/usr/lib/security/pki/ca.cfg** 文件中的 **cdp** 属性。
9. 设置**证书撤销表（CRL）URI** 字段。该字段为该 CA 指定应该设置为证书撤销表的位置的 URI。通常，这是 LDAP URI，例如:

   ```
   ldap://crlserver/o=XYZ,c=us
   ```

   该字段映射到 **/usr/lib/security/pki/ca.cfg** 文件中的 **crl** 属性。
10. **缺省证书专有名称**字段指定创建证书时所用的基线 DN（例如，`o=XYZ`，`c=us`）。该字段是不需要的。该字段映射到 **/usr/lib/security/pki/ca.cfg** 文件中的 **dn** 属性。

11. 如果在创建时没有提供主题备用名称 URI，**缺省证书主题备用名称 URI** 字段指定创建证书时使用的缺省主题备用名称 URI。该字段是不需要的。该字段映射到 **/usr/lib/security/pki/ca.cfg** 文件中的 **url** 属性。
12. **公用密钥算法**字段指定创建证书时使用的公用密钥算法。选项是 **RSA** 和 **DSA**。如果两者都不指定，系统缺省值为 **RSA**。该字段映射到 **/usr/lib/security/pki/ca.cfg** 文件中的 **algorithm** 属性。
13. **公用密钥大小（以位为单位）**字段指定公用密钥算法的位大小。该字段是以位，不是字节为单位，为支持下一可行的字节大小，基础的公用密钥机制可能将该值四舍五入。（通常，当位数不是 8 的偶倍数时四舍五入）。示例值是 512、1024 和 2048。如果不指定该字段，系统缺省为 1024 位。该字段映射到 **/usr/lib/security/pki/ca.cfg** 文件中的 **keysize** 属性。
14. **最大通信重试**字段指定系统放弃前试图联系 CA（当创建或取消证书时）的次数。系统缺省为 5 次。该字段映射到 **/usr/lib/security/pki/ca.cfg** 文件中的 **retries** 属性。
15. **签署散列算法**字段指定签署认证证书时使用的散列算法。选项是 **MD2**、**MD5** 和 **SHA1**。系统的缺省为 **MD5**。该字段映射到 **/usr/lib/security/pki/ca.cfg** 文件中的 **signinghash** 属性。
16. 按下 Enter 键提交更改。

更改／显示 CA 帐户:

1. 运行 PKI SMIT，如下:

   ```
   smitty pki
   ```

2. 选择**更改／显示 CA 帐户**。
3. 对**认证中心名称**字段，输入 local，按下 Enter 键。
4. **证书创建引用号**字段指定创建证书中所用的 CA 引用号。创建引用号必须由所有数字组成，且长度上至少 7 个数字。CA 定义引用号。（请参阅第 95 页的『创建认证中心』。）该字段映射到 **/usr/lib/security/pki/acct.cfg** 文件中的 **carefnum** 属性。
5. **证书创建密码**字段指定创建证书时使用的 CA 的引用密码。创建密码必须由 7 位 ASCII 码的字母和数字组成，长度上至少 12 个字符。在 CA 中定义创建密码，且必须是以上创建引用号的匹配密码。（请参阅第 95 页的『创建认证中心』。）该字段映射到 **/usr/lib/security/pki/acct.cfg** 文件中的 **capasswd** 属性。
6. **证书取消引用号**字段指定当取消证书时使用的引用号。取消引用号必须由所有数字组成，长度上至少 7 个数字。在每个证书创建期间将取消引用号发送给 CA，并通过 CA 与证书关联。要取消证书，取消过程中必须发送和创建证书时发送的相同的取消引用号（和取消密码）。该字段映射到 **/usr/lib/security/pki/acct.cfg** 文件中的 **rvrefnum** 属性。
7. **证书取消密码**字段指定当取消证书时使用的引用密码。取消密码必须由 7 位 ASCII 码的字母和数字组成，长度上至少 12 个字符。每个证书创建过程中将取消密码发送给 CA，并通过 CA 与证书关联。要取消证书，取消过程中必须发送和创建证书时发送的相同的取消密码（和取消引用号）。该字段映射到 **/usr/lib/security/pki/acct.cfg** 文件中的 **rvpasswd** 属性。
8. **可信密钥标签**字段指定定位于可信密钥存储器的可信签字密钥的标签（有时称为 *alias*）。可信密钥标号值是来自第 95 页的『创建可信签字密钥』的值。该字段映射到 **/usr/lib/security/pki/acct.cfg** 文件中的 **keylabel** 属性。
9. **可信密钥密码**字段指定定位于可信密钥存储器的可信签字密钥的密码。可信密钥密码值是来自第 95 页的『创建可信签字密钥』的值。该字段映射到 **/usr/lib/security/pki/acct.cfg** 文件中的 **keypasswd** 属性。
10. 按下 Enter 键提交更改。

添加 CA LDAP 帐户:

1. 运行 PKI SMIT，如下:

   ```
   smitty pki
   ```

2. 选择**添加 LDAP 帐户**。

3. **管理用户名**字段指定 LDAP 管理帐户 DN。CA LDAP 帐户的管理用户名与第 91 页的『LDAP 服务器配置』和第 94 页的『为证书认证服务服务器配置 LDAP』使用的名称相同。该值应为 cn=admin。访问 CA LDAP 数据时为了与 LDAP 服务器通信客户机使用它。该字段映射到 **/usr/lib/security/pki/acct.cfg** 文件中的 **ldappkiadmin** 属性。例如:

   ```
   ldappkiadmin = "cn=admin"
   ```

4. **管理密码**字段指定 LDAP 管理帐户密码。管理密码与第 91 页的『LDAP 服务器配置』和第 94 页的『为证书认证服务服务器配置 LDAP』使用的密码相同。该字段映射到 **/usr/lib/security/pki/acct.cfg** 文件中的 **ldappkiadmpwd** 属性。例如:

   ```
   ldappkiadmpwd = secret
   ```

5. **服务器名称**字段指定 LDAP 服务器的名称，且必须在每个 LADP 节中定义。该值是单一的 LDAP 服务器名称。该字段映射到 **/usr/lib/security/pki/acct.cfg** 文件中的 **ldapservers** 属性。例如:

   ```
   ldapservers = ldapserver.mydomain.com
   ```

6. **后缀**字段指定数据驻留在其中的目录信息树的 DN 后缀。该后缀是用在第 94 页的『为证书认证服务服务器配置 LDAP』中的 **ibm-slapdSuffix** 属性的值。该属性必须在每个 LDAP 节中定义。该字段映射到 **/usr/lib/security/pki/acct.cfg** 文件中的 **ldapsuffix** 属性。例如:

   ```
   ldapsuffix = "ou=aix,cn=us"
   ```

7. 按下 Enter 键提交更改。

添加 PKI 每个用户 LDAP 帐户: 执行和第 97 页的『添加 CA LDAP 帐户』中同样的步骤，除了使用在第 92 页的『为 PKI 配置 LDAP 服务器』中的**添加 PKI 后缀**和 **ACL 数据库项**步骤中使用的值。使用以下值:

- 管理用户名（ou=pkidata，cn=aixdata），
- 管理密码（*password*），
- 服务器名称（*site specific*），
- 后缀（ou=pkidata，cn=aixdata）。

按下 Enter 键提交更改。

更改／显示策略:

1. 运行 PKI SMIT，如下:

   ```
   smitty pki
   ```

2. 选择**更改／显示策略**。

- **为新用户创建证书**字段指定 **mkuser** 命令是为新用户生成证书和密钥存储器（**new**），还是如果创建用户后管理员提供证书和密钥存储器（**get**）。该字段映射到 **/usr/lib/security/pki/policy.cfg** 文件中的 **newuser** 节的 **cert** 属性。
- **认证中心名称**字段指定生成证书时 **mkuser** 命令使用的 CA。字段值必须是 **ca.cfg** 文件中找到的节名称; 例如，**local**。该字段映射到 **/usr/lib/security/pki/policy.cfg** 文件中的 **newuser** 节的 **ca** 属性。
- **初始用户密码**字段指定创建用户密钥存储器时 **mkuser** 命令使用的密码。该字段映射到 **/usr/lib/security/pki/policy.cfg** 文件中的 **newuser** 节的 **passwd** 属性。
- **证书版本**字段指定生成证书时 **mkuser** 命令使用的证书版本。通常地，仅支持值 3，它代表 X.509v3。该字段映射到 **/usr/lib/security/pki/policy.cfg** 文件中的 **newuser** 节的 **version** 属性。
- **公用密钥大小**字段指定生成证书时 **mkuser** 命令使用的公用密钥的大小（以位为单位）。该字段映射到 **/usr/lib/security/pki/policy.cfg** 文件中的 **newuser** 节的 **keysize** 属性。
- **密钥存储器位置**字段指定创建密钥存储器时 **mkuser** 命令使用的 URI 格式的密钥存储器目录。该字段映射到 **/usr/lib/security/pki/policy.cfg** 文件中的 **newuser** 节的 **keystore** 属性。

- **有效期**字段指定生成证书时 **mkuser** 命令使用的证书要求的有效期。要求的有效期可能是或可能不是创建证书时 CA 授予的。周期能以秒、天或年为单位来指定。如果只提供一个数字，则认为是以秒为单位。如果数字后立即是字母 d，则解释为天。如果数字后立即是字母 y，则解释为年。示例值是:
  - 1y（即 1 年）
  - 30d（即 30 天）
  - 2592000（即以秒为单位表示为 30 天）

  该字段映射到 **/usr/lib/security/pki/policy.cfg** 文件中的 **newuser** 节的 **validity** 属性。
- **复制非本地证书**字段指定 **certlink** 命令是保存证书的副本（**yes**），还是只是到证书的链接（**no**）。该字段映射到 **/usr/lib/security/pki/policy.cfg** 文件中的 **storage** 节的 **replicate** 属性。
- **检查证书撤销列表**字段指定 **certadd** 和 **certlink** 命令在执行它们的任务前是检查 CRL（**yes**）还是不检查（**no**）。该字段映射到 **/usr/lib/security/pki/policy.cfg** 文件中的 **crl** 节的 **check** 属性。
- **缺省通信超时**字段指定使用 HTTP（例如，检索 CRL）请求证书信息时 **certadd** 和 **certlink** 命令使用的以秒为单位的超时周期。该字段映射到 **/usr/lib/security/pki/policy.cfg** 文件中的 **comm** 节的 **timeout** 属性。

methods.cfg 文件

methods.cfg 文件指定 **registry** 和 **SYSTEM** 属性使用的认证语法的定义。特定地，这就是对于 **PKILDAP**（即使用 LDAP 的 PKI）和 **FPKI**（*文件* PKI）的认证语法必须由系统管理员定义和添加的位置。

下面是典型的 **methods.cfg** 定义。节名称 **PKI**、**LDAP** 和 **PKILDAP** 为任意的名称，可以由管理员更改。本节为了一致性始终使用这些节名称。

```
PKI:
  program = /usr/lib/security/PKI
  options = authonly

LDAP:
  program = /usr/lib/security/LDAP

PKILDAP:
  options = auth=PKI,db=LDAP
```

为支持漫游用户，在支持漫游用户的所有系统中使用相同的 **methods.cfg** 节名称和属性值。

管理配置示例

创建新 PKI 用户帐户

为创建新 PKI 用户帐户，使用 **mkuser** 命令和适当的 **/usr/lib/security/methods.cfg** 节名称（**PKILDAP**）。取决于在 **/usr/lib/security/pki/policy.cfg** 文件中的属性设置，**mkuser** 命令能为用户自动创建证书。下面是创建用户帐户 bob 的 **mkuser** 示例:

```
mkuser -R PKILDAP SYSTEM="PKILDAP" registry=PKILDAP bob
```

将非 PKI 用户帐户转换为 PKI 用户帐户

将非 PKI 用户帐户转换为 PKI 用户帐户有一对不同的方法。第一个方法最初允许系统管理员初始地访问用户专用密钥存储器，这在给出的环境中可能或可能不是可接受的，但却是转换用户的最快的方法。第二种方法需要在用户和系统管理员之间的交互作用，这可能花更多的时间设置。

两个示例都使用以下假设:

- 已经安装、配置及运行 **cas.server** 和 **cas.client**。
- 在 **methods.cfg** 中将 **PKILDAP** 定义为『methods.cfg 文件』中显示的那样。

示例 1:

通过超级权限，系统管理员对用户帐户 bob 执行以下命令:

```
certcreate -f cert1.der -l auth_lbl1 cn=bob bob  # Create & save cert in cert1.der.
certadd -f cert1.der -l auth_lbl1 auth_tag1 bob  # Add cert to LDAP as auth_tag1.
certverify auth_tag1 bob                         # Verify & sign the cert in LDAP.
chuser SYSTEM="PKILDAP" registry=PKILDAP bob     # Change account type to PKILDAP.
chuser -R PKILDAP auth_cert=auth_tag1 bob        # Set the user's auth certificate.
```

那么，让用户 bob 使用 **keypasswd** 命令更改他在密钥存储器上的密码。

示例 2:

让用户 bob 执行上面示例 1 的前 3 个命令（**certcreate**、**certadd**、**certverify**），创建他自己的证书和密钥存储器。然后让系统管理员执行上面示例 1 的最后两个 **chuser** 命令。

创建和添加认证证书

如果 PKI 用户需要创建认证证书，用户可以创建新证书，且让系统管理员使该证书成为用户的认证证书。下面是用户 bob 创建证书，系统管理员使该证书成为认证证书的示例。

```
# Logged in as user account bob:
certcreate -f cert1.der -l auth_lbl1 cn=bob  # Create & save cert in cert1.der.
certadd -f cert1.der -l auth_lbl1 auth_tag1  # Add cert to LDAP as auth_tag1.
certverify auth_tag1                         # Verify & sign the cert in LDAP.
# As the system adminstrator:
chuser -R PKILDAP auth_cert=auth_tag1 bob    # Set the user's auth certificate.
```

更改缺省新密钥存储器密码

编辑 **/usr/lib/security/pki/policy.cfg** 文件中的 **newuser** 节的 **passwd** 属性值以修改用来创建新 PKI 用户的密钥存储器的密码。

处理已损坏的可信签字密钥

包含可信签字密钥的文件需要替换，且用户认证证书需要重新签署。

处理已损坏的用户专用密钥

如果用户的专用密钥已损坏，用户或管理员应该使用适当的原因码取消该证书，应该将损坏通知使用公用密钥的其它用户，且视专用／公用密钥的目的而定，应该发布新证书。如果证书用作用户的认证证书，那么另一个证书（属于用户的新证书或现有的未损坏的证书）应该添加为新认证证书。

处理已损坏的密钥存储器或密钥存储器密码

更改密钥存储器的密码。取消所有用户的证书。为用户创建创建证书，包含新认证证书。为了访问以前的加密数据，已损坏的专用密钥可能对于用户仍然是有用的。

移动用户的密钥存储器或更改用户的密钥存储器的名称

如果用户的专用密钥已损坏，用户或管理员应该使用适当的原因码取消该证书，应该将损坏通知使用公用密钥的其它用户，且视专用／公用密钥的目的而定，应该发布新证书。如果该证书用作用户的认证证书，那么另一个证书（属于用户的新证书或现有的未损坏的证书）应该添加为新认证证书。

移动用户的密钥存储器或更改用户的密钥存储器的名称

每个维护在 LDAP 中的用户证书包含它的匹配专用密钥的密钥存储器位置。要从一个目录中将用户的密钥存储器移动到另一个，或更改密钥存储器的名称，需要更改与用户的证书关联的 LDAP 密钥存储器的位置和名称。如果用户使用多个密钥存储器，那么必须特别注意只更改密钥存储器更改影响的证书的 LDAP 信息。

将密钥存储器从 **/var/pki/security/keys/user1.p12** 移动到 **/var/pki/security1/keys/user1.p12**:

```
# As root...

cp /var/pki/security/keys/user1.p12 /var/pki/security1/keys/user1.p12

# Retrieve a list of all the certificates associated with the user.
certlist ALL user1

# For each certificate associated with the keystore, do the following:
# A) Retrieve the certificate's private key label and its "verified" status.
# B) Retrieve the certificate from LDAP.
# C) Replace the certificate in LDAP using the same private key label,
# but the new keystore path name.
# D) If the certificate was previously verified, it must verified again.
# (Step D requires the password to the keystore.)

# Example modifying one certificate.
# Assume:

# username: user1

# cert tag: tag1

# key label: label1

# Retrieve the certificate's private key label.
certlist -a label tag1 user1

# Retrieve the certificate from LDAP and place it in file cert.der.
certget -f cert.der tag1 user1

# Replace the certificate in LDAP.
certadd -r -f cert.der -p /var/pki/security1/keys/user1.p12 -l label1 tag1 user1

# Re-verify the certificate if it was previously verified.
# (Need to know the keystore password.)
certverify tag1 user1
```

第 7 章 可插入认证模块

可插入认证模块（PAM）结构为系统管理员提供通过可插入模块将多个认证机制结合进现有系统的能力。支持使用 PAM 的应用程序能够不更改现有的应用程序就*插入*到新的技术中。这种灵活性允许管理员执行以下操作:

- 为应用程序选择系统中的任意认证服务
- 对给定的服务使用多个认证机制
- 不修改现有的应用程序而添加新的认证服务模块
- 使用以前输入的密码来用于多模块认证

PAM 结构由库、可插入模块以及配置文件组成。PAM 库实现了 PAM 应用程序编程接口（API）并为管理 PAM 事务和调用在可插入模块中定义的 PAM 服务编程接口（SPI）提供服务。可插入模块根据调用服务及其在配置文件中的项而由库动态装入。成功不但取决于可插入模块，也取决于为服务所定义的行为。通过*堆栈*的概念，可以将服务配置为通过多个认证方法认证。如果得到支持，那么模块也可配置为使用先前提交的密码，而不是提示另外输入。

下图显示了应用程序、PAM 库、配置文件以及 PAM 模块间的交互作用。假定的 PAM 应用程序（pam_login、pam_su 以及 pam_passwd）调用 PAM 库中的 PAM API。库根据配置文件中的应用程序项确定装入适当的模块，并调用在该模块中的 PAM SPI。通过使用在 PAM 模块中实现的对话功能，可以在 PAM 模块和库之间通信。然后，模块的成功或失败与配置文件中定义的行为确定是否需要装入另一个模块。如果是，进程继续；否则，会将数据发送回应用程序。

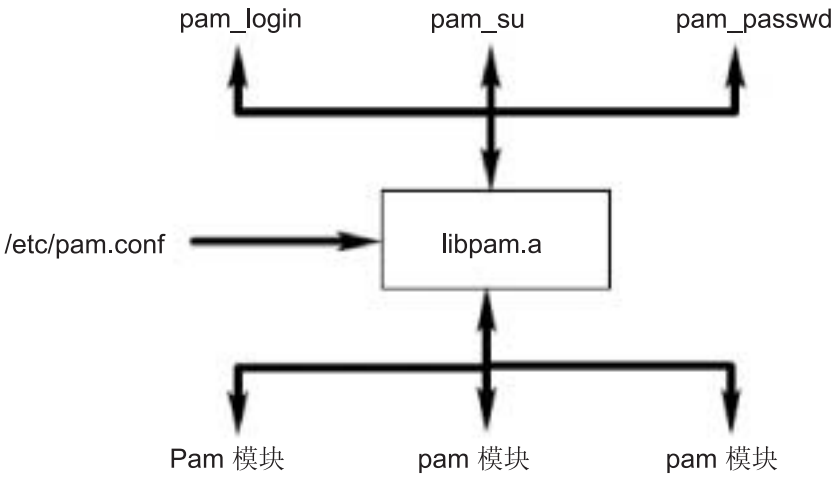


图 3. PAM 框架和实体. 本图显示了假定的应用程序命令如何使用 PAM 库来访问适当的 PAM 模块。

PAM 库

PAM 库 **/usr/lib/libpam.a** 包含 PAM API，它作为所有 PAM 应用程序的公共接口并且还控制模块装入。PAM 库根据在 **/etc/pam.conf** 文件中定义的堆栈行为装入模块。

以下的 PAM API 功能调用由 PAM 模块提供的相应 PAM SPI。例如，**pam_authenticate** API 调用在 PAM 模块中的 **pam_sm_authenticate** SPI。

- **pam_authenticate**
- **pam_setcred**
- **pam_acct_mgmt**
- **pam_open_session**
- **pam_close_session**
- **pam_chauthtok**

同时在 PAM 库中也提供了几个功能，这些功能启用应用程序来调用 PAM 模块和将信息发送到 PAM 模块。以下的 PAM 结构 API 在 AIX 中实现:

pam_start	建立 PAM 会话
pam_end	终止 PAM 会话
pam_get_data	检索特定于模块的数据
pam_set_data	设置特定于模块的数据
pam_get_item	检索公共 PAM 信息
pam_set_item	设置公共 PAM 信息
pam_get_user	检索用户名
pam_strerror	获取 PAM 标准错误信息

PAM 模块

PAM 模块允许在系统上合并或分别使用多个认证机制。给定的 PAM 模块必须至少实现四种模块类型之一。模块类型以及要求与模块类型一致的相应的 PAM SPI 描述如下。

认证模块

认证用户以及设置、刷新或破坏凭证。这些模块根据它们的认证和凭证识别用户。

认证模块功能:

- **pam_sm_authenticate**
- **pam_sm_setcred**

帐户管理模块

确定用户帐户的有效性以及从认证模块识别后的后继访问。这些模块执行的检查通常包含帐户到期和密码限制。

帐户管理模块功能:

- **pam_sm_acct_mgmt**

会话管理模块

启动和终止用户会话。此外，可能提供会话审计支持。

会话管理模块功能:

- **pam_sm_open_session**
- **pam_sm_close_session**

密码管理模块

执行密码修改以及相关的属性管理。

密码管理模块功能:

- **pam_sm_chauthtok**

PAM 配置文件

/etc/pam.conf 配置文件由每个 PAM 模块类型的服务项组成，并通过已定义的模块路径提供路由服务。此文件中的项由以下空白分隔的字段组成:

service_name module_type control_flag module_path module_option

其中:

service_name	指定服务的名称。关键字 OTHER 用于定义项中没有指定的应用程序所用的缺省模块。
module_type	为服务指定模块类型。有效模块类型是 auth、account、session 或 password。
control_flag	为模块指定堆栈行为。支持的控制标志是 required、sufficient 或 optional。
module_path	指定实现服务功能的库对象的路径名。*module_path* 项应该从根（**/**）目录开始。如果该项不以 **/** 开始，那么会将 **/usr/lib/security** 预设为文件名。
module_option	指定能够发送到服务模块的选项列表。该字段的值取决于在 *module_path* 字段中定义的模块支持的选项。

所有的先行字段对于每个项都是必要的，除了 *module_options* 字段，它是可选的。PAM 库会忽略格式错误的项以及 *module_tyep* 或 *control_flag* 字段具有无效值的项。行起始以数字符号（#）开头的项也会被忽略，因为这表示注释。

通过使用相同的 *module_type* 字段创建多个项在配置文件中实现堆栈。以文件中列出的顺序调用模块，并由每个项指定的 *control_flag* 字段确定最终结果。*control_flag* 字段的有效值和在堆栈中的相应的行为如下:

required	所有堆栈中 required 模块必须通过才能得到成功的结果。如果一个或多个 required 模块失败，那么会尝试堆栈中所有 required 模块，但返回第一个失败的 required 模块的错误。
sufficient	如果一个标志为 sufficient 的模块成功，之前没有 required 或 sufficient 的模块失败，那就会忽略堆栈中所有剩余的模块，并返回成功。
optional	如果堆栈中没有模块是 required，并且没有 sufficient 模块成功，那么至少有一个对于服务的 optional 模块必须成功。如果在堆栈中的另一个模块成功了，那么就会忽略 optional 模块中的失败。

以下是 **/etc/pam.conf** 文件示例，它能够在安装了其它的 PAM 模块的系统上使用:

```
#
# PAM configuration file /etc/pam.conf
#

# Authentication Management
login   auth     required       /usr/lib/security/pam_aix
login   auth     required       /usr/lib/security/pam_verify
login   auth     optional       /usr/lib/security/pam_test      use_first_pass
su      auth     sufficient     /usr/lib/security/pam_aix
su      auth     required       /usr/lib/security/pam_verify
OTHER   auth     required       /usr/lib/security/pam_aix

# Account Management
OTHER   account  required       /usr/lib/security/pam_aix

# Session Management
OTHER   session  required       /usr/lib/security/pam_aix

# Password Management
OTHER   password required       /usr/lib/security/pam_aix
```

此示例配置文件包含登录服务的三个项。将 **pam_aix** 和 **pam_verify** 指定为 required 之后，用户必须输入两个密码用于认证，而且用户要认证的话两个密码必须都成功。**pam_test** 模块的第三个项是可选的，它的成功或失败不会影响用户是否能够登录。**pam_test** 模块的 `use_first_pass` 选项允许使用以前输入的密码，而不是提示输入一个新的密码。

su 命令的运行方式使得如果 **pam_aix** 成功了，那么认证也成功了。如果 **pam_aix** 失败了，那么必须通过 **pam_verify** 方可成功认证。

将 **OTHER** 关键字用作服务名称为配置文件中没有明确声明的任何其它服务启用了一个缺省值。设置缺省值确保给定的模块类型在所有情况下都至少有一个模块适用。

添加 PAM 模块

要添加 PAM 模块，使用以下过程:

1. 将模块安装在 **/usr/lib/security** 目录中。
2. 将文件所有权设置为 root，并将许可权设置为 555。PAM 库不装入任何不是 root 用户拥有的模块。
3. 更新 **/etc/pam.conf** 配置文件，使其在项中包含用于期望的服务名称的模块。
4. 测试受影响的服务以确保其功能。在执行完登录测试前不要从系统注销。

更改 /etc/pam.conf 文件

更改 **/etc/pam.conf** 配置文件时，考虑以下的内容:

- AIX 不提供缺省的 **/etc/pam.conf** 文件，因此必须在使用 PAM 之前创建此文件。创建此文件时，将文件所有权设置为 root，并将基本许可权设置为 644。然后 root 用户就可以对它进行手工编辑，以进行期望的更改。
- 确定每个模块类型要使用的缺省模块，然后使用 **OTHER** 关键字来阻止对每个服务指定该模块。
- 阅读给选定的模块提供的任何文档，并确定支持哪个控制标志和选项以及它们的效果如何。
- 仔细选择模块的顺序和控制标志，牢记堆栈模块中 **required**、**sufficient** 以及 **optional** 控制标志的行为。

注: PAM 配置文件的不正确配置会导致系统无法登录。更改文件后，请总是在从系统注销之前测试受影响的应用程序。不能登录的系统可以通过以维护方式重新引导系统并更正 **/etc/pam.conf** 配置文件来恢复。

启用 PAM 调试

PAM 库能在执行过程中提供调试信息。启用系统收集调试输出后，收集的信息可用于跟踪 PAM-API 调用并确定当前 PAM 安装失败点。要启用 PAM 调试输出，请遵循以下步骤:

1. 在 **/etc/pam_debug** 创建一个空文件。PAM 库检查 **/etc/pam_debug** 文件的存在，如果找到此文件，就启用 syslog 输出。
2. 编辑 **/etc/syslog.conf** 文件，使其包含信息的期望级别的相应项。
3. 重新启动 **syslogd** 守护程序以便配置更改能被识别。
4. 重新启动 PAM 应用程序时，调试信息会收集在 **/etc/syslog.conf** 配置文件里定义的输出文件中。

在 AIX 中的集成 PAM

可以通过使用 AIX 可装入的认证模块 PAM 和 **pam_aix** 模块把 PAM 集成到 AIX 中。这些模块提供 PAM 集成的以下独立路径:

- 通过 PAM 模块提供从 AIX 安全服务到 PAM 的访问
- 通过 PAM 模块（**pam_aix**）提供从 PAM 应用程序到 AIX 安全服务的访问

PAM 模块

可将 AIX 安全服务配置成通过使用现有的 AIX 可装入认证模块结构调用 PAM 模块。当正确设置了 **/usr/lib/security/methods.cfg** 文件后，PAM 装入模块把 AIX 安全服务（**passwd**、**login** 等）路由到 PAM 库。PAM 库检查 **/etc/pam.conf** 文件以确定使用哪个 PAM 模块，然后进行相应的 PAM SPI 调用。从 PAM 返回的值映射为 AIX 错误代码，并返回到调用的程序。

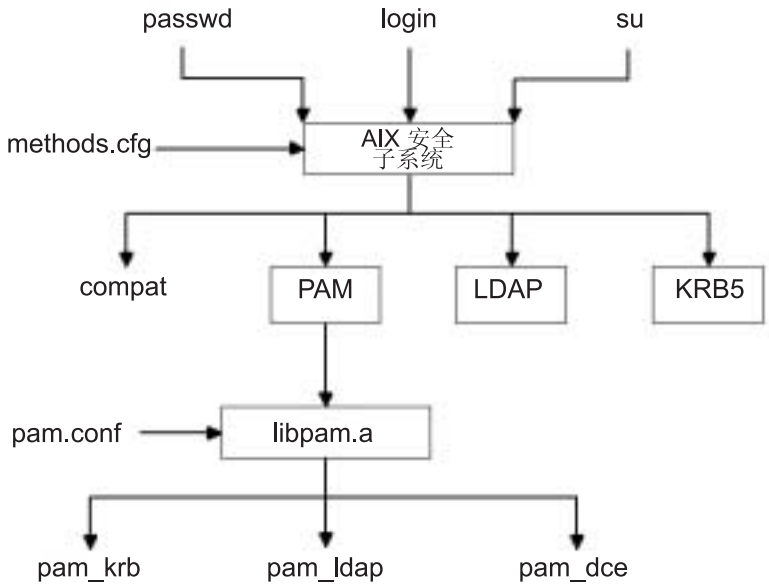


*图 4. 到 PAM 模块路径的 AIX 安全服务. 此插图显示当正确配置了 PAM 后，AIX 安全服务调用所采用的路径。显示的 PAM 模块（**pam_krb**、**pam_ldap** 和 **pam_dce**）作为第三方解决方案的示例列出。*

PAM 装入模块安装在 **/usr/lib/security** 目录中并且是仅用于认证的模块。PAM 模块必须与数据库结合以形成复合的装入模块。以下的示例显示了一些节，可以添加这些节到 **methods.cfg** 文件中以形成带有被**文件**调用的数据库的复合 PAM 模块。**db** 属性的 **BUILTIN** 关键字将把数据库指定为 UNIX 文件。

```
PAM:
        program = /usr/lib/security/PAM

PAMfiles:
        options = auth=PAM,db=BUILTIN
```

然后通过使用 **-R** 选项和管理命令并通过创建用户时设置 **SYSTEM** 属性来创建和修改用户。例如:

```
mkuser -R PAMfiles SYSTEM=PAMfiles registry=PAMfiles pamuser
```

此操作把进一步的调用通知 AIX 安全服务（**login**、**passwd** 等）以使用 PAM 装入模块进行认证。当**文件**数据库在本例中用于复合模块时，如果安装了其它数据库（比如 LDAP），则也可以使用它。如前面描述那样创建用户会导致 AIX 安全到 PAM API 调用的如下映射:

```
 AIX                     PAM API
=====                    =========
authenticate       -->   pam_authenticate
chpass             -->   pam_chauthtok
passwdexpired      -->   pam_acct_mgmt
passwdrestrictions -->   不存在可比映射，返回成功
```

定制 **/etc/pam.conf** 文件允许为了认证将 PAM API 调用定向到期望的 PAM 模块。要进一步优化该认证机制，可以实现堆栈。

AIX 安全服务提示的数据通过 **pam_set_item** 功能传递到 PAM，因为不可能容纳来自 PAM 的用户对话。为和 PAM 模块集成所写的 PAM 模块应通过 **pam_get_item** 调用检索所有数据并且不应试图提示用户输入数据，因为这都是由安全服务来处理的。

提供了循环检测以捕获可能的配置错误，这些错误可能发生在 AIX 安全服务路由到 PAM，然后反过来，PAM 模块试图调用 AIX 安全服务以执行该操作的过程中。此循环事件的检测会导致期望操作的立即失败。

注: 当使用从 AIX 安全服务到 PAM 模块的 PAM 集成时，不应该写 **/etc/pam.conf** 文件以利用 **pam_aix** 模块，因为这将导致产生循环条件。

pam_aix 模块

pam_aix 模块是提供启用 PAM 的应用程序对 AIX 安全服务访问的 PAM 模块。这是通过提供调用其所在位置的对等 AIX 服务的接口实现的。这些服务由可装入认证模块或 AIX **内置**函数轮流执行，该函数是基于用户定义和 **methods.cfg** 文件中的对应设置。在执行 AIX 服务过程中生成的任何错误代码映射为相应的错误代码。

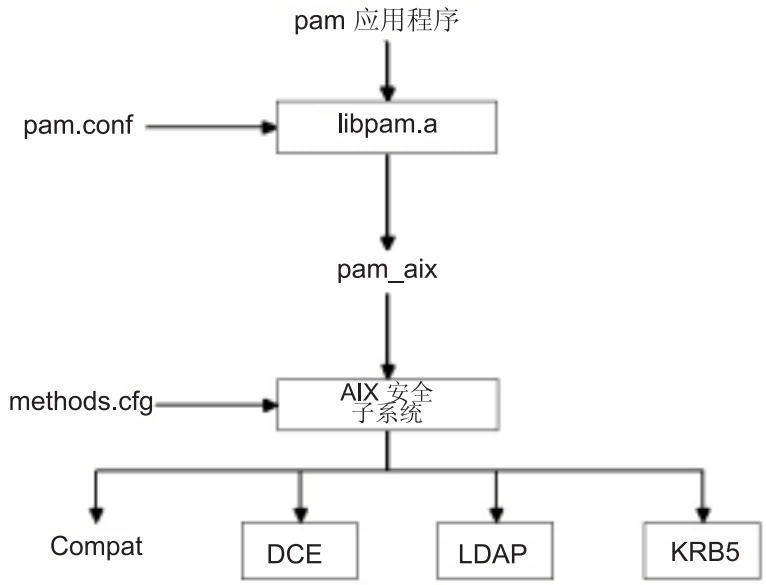


*图 5. PAM 应用程序到 AIX 安全子系统路径. 此插图显示了如果配置 **/etc/pam.conf** 文件以利用 **pam_aix** 模块，则 PAM 应用程序 API 调用将要遵循的路径。如图表所示，该集成允许用户由任一可装入的认证模块（DCE、LDAP 或 KRB5）或在 AIX 文件中（compat）进行认证。*

pam_aix 模块安装在 **/usr/lib/security** 目录中。**pam_aix** 模块的整合要求将 **/etc/pam.conf** 文件配置为使用该模块。堆栈仍然是可用的，但是不在以下 **/etc/pam.conf** 文件的示例中显示:

```
#
# Authentication management
#
OTHER   auth     required       /usr/lib/security/pam_aix

#
# Account management
#
OTHER   account  required       /usr/lib/security/pam_aix

#
# Session management
#
OTHER   session  required       /usr/lib/security/pam_aix

#
# Password management
#
OTHER   password required       /usr/lib/security/pam_aix
```

pam_aix 模块实现了 **pam_sm_authenticate**、**pam_sm_chauthok** 和 **pam_sm_acct_mgmt** 的 SPI 功能。**pam_sm_setcred**、**pam_sm_open_session** 和 **pam_sm_close_session** SPI 也在 **pam_aix** 模块中实现，但是这些 SPI 功能返回 PAM_SUCCESS 调用。

以下是 PAM SPI 调用到 AIX 安全子系统的大致映射:

```
 PAM SPI                    AIX
=========                  =====
pam_sm_authenticate   -->  authenticate
pam_sm_chauthtok      -->  passwdexpired, chpass
                           注: 仅在 PAM_CHANGE_EXPIRED_AUTHTOK
                           标志通过时检查 passwdexpired。
pam_sm_acct_mgmt      -->  loginrestrictions, passwdexpired
pam_sm_setcred        -->  不存在可比映射，返回 PAM_SUCCESS
pam_sm_open_session   -->  不存在可比映射，返回 PAM_SUCCESS
pam_sm_close_session  -->  不存在可比映射，返回 PAM_SUCCESS
```

要传递到 AIX 安全子系统的数据可以在使用模块前用 **pam_set_item** 功能来设置，或者如果该功能还未存在，则可以对数据使用 **pam_aix** 模块。

第 8 章 OpenSSH 软件工具

OpenSSH 软件工具支持 SSH1 和 SSH2 协议。该工具为加密和认证网络流量提供 shell 功能。OpenSSH 是基于客户机和服务器体系结构。OpenSSH 在 AIX 主机上运行 **sshd** 守护程序并等待客户机连接。它支持用于通道认证和加密的公用密钥和专用密钥对以保证安全网络连接和基于主机的认证。有关 OpenSSH（包括手册页）的更多信息，请参阅以下 Web 站点:

```
http://www.openssh.org
```

有关 AIX 上 OpenSSH 的更多信息，请参阅以下 Web 站点，它有 AIX 5L 的最新 **installp** 格式软件包:

```
http://oss.software.ibm.com/developerworks/projects/opensshi
```

本节说明了如何在 AIX 上安装并配置 OpenSSH。

OpenSSH 软件在 AIX 5.2 Expansion Pack 上提供。使用 **openssh-3.7.1p2** 级别的源代码将本版本的 OpenSSH 编译并封装成为 **installp** 软件包。**installp** 软件包包括手册页和已翻译的消息文件集。 Expansion Pack CD-ROM 介质中包含的 OpenSSH 程序是按照 “IBM 国际软件许可协议”（IPLA）中无保证程序的条款和条件授权的。

在安装 OpenSSH **installp** 格式软件包之前，必须安装包含加密的库的 “开放安全安全套接字层（OpenSSL）软件。OpenSSL 在 *AIX Toolbox for Linux Applications* CD 上的 RPM 软件包中可用，或者还可以从以下 *AIX Toolbox for Linux Applications* Web 站点下载软件包:

```
http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
```

由于 OpenSSL 软件包包含隐藏图片的内容，所以必须在 Web 站点上注册以下载软件包。可以通过完成以下步骤下载软件包:

1. 在 *AIX Toolbox for Linux Applications* Web 站点的右面单击 **AIX 工具箱隐藏图形的内容**链路。
2. 单击**之前未注册**。
3. 填充表格中需要的字段。
4. 读许可证，然后单击**接受许可证**。浏览器自动重定向到下载页面。
5. 向下滚动隐藏图形的内容软件包的列表知道看见” OpenSSL — SSL 隐藏图形库 “下面的 **openssl-0.9.6k-1.aix4.3.ppc.rpm**。
6. 单击**现在下载**！按钮以获取 **openssl-0.9.6k-1.aix4.3.ppc.rpm**。

在下载 OpenSSL 软件包后，可以安装 OpenSSL 和 OpenSSH。

1. 使用如下 **geninstall** 命令安装 OpenSSL RPM 软件包:

   ```
   # geninstall -d/dev/cd0 R:openssl-0.9.6g
   ```

   输出与以下显示相似:

   ```
   SUCCESSES
   ---------
   openssl-0.9.6g-3
   ```

2. 使用 **geninstall** 命令来安装 OpenSSH **installp** 软件包，如下:

   ```
   # geninstall -I"Y" -d/dev/cd0 I:openssh.base
   ```

   在查看过 OpenSSH 许可证协议后，使用 **Y** 标志以接受该许可证协议。

   输出与以下显示相似:

```
安装摘要
--------------------
名称                         级别           部分        事件        结果
-------------------------------------------------------------------------------
openssh.base.client          3.6.0.5200     USR         APPLY       SUCCESS
openssh.base.server          3.6.0.5200     USR         APPLY       SUCCESS
openssh.base.client          3.6.0.5200     ROOT        APPLY       SUCCESS
openssh.base.server          3.6.0.5200     ROOT        APPLY       SUCCESS
```

也可以使用 SMIT **install_software** 快速路径安装 OpenSSL 和 OpenSSH。

作为之前安装步骤的结果，以下的 OpenSSH 二进制文件也都安装了:

scp	类似 **rcp** 的文件复制程序
sftp	类似 **FTP** 的程序，通过 SSH1 和 SSH2 协议工作
sftp-server	SFTP 服务器子系统（由 **sshd** 守护程序自动启动）
ssh	类似 **rlogin** 和 **rsh** 客户机程序
ssh-add	添加密钥到 **ssh-agent** 的工具
ssh-agent	可以存储专用密钥的代理
ssh-keygen	密钥生成工具
ssh-keyscan	从一些主机中收集公共主机密钥的实用程序
ssh-keysign	基于主机认证的实用程序
ssh-rand-helper	由 OpenSSH 使用的程序，用来收集随机数。它只能在 AIX 5.1 安装上使用。
sshd	允许登录的守护程序

以下的一般信息包含了 OpenSSH:

- **/etc/ssh** 目录包含 **sshd** 守护程序和 **ssh** 客户机命令的配置文件。
- **/usr/openssh** 目录包含自述文件和 OpenSSH 开放源许可证原始文本文件。此目录还包含 **ssh** 协议和 Kerberos 许可证文本。
- **sshd** 守护程序受 AIX SRC 控制。可以发出以下命令启动、停止以及查看守护程序的状态:

  ```
  startsrc -s sshd   或 startsrc -g ssh  （组）
  stopsrc -s sshd    或 stopsrc -g ssh
  lssrc -s sshd      或 lssrc -s ssh
  ```

  也可以发出以下命令启动和停止守护程序:

  ```
  /etc/rc.d/rc2.d/Ksshd start
  ```

  或

  ```
  /etc/rc.d/rc2.d/Ssshd start
  ```

  ```
  /etc/rc.d/rc2.d/Ksshd stop
  ```

  或

  ```
  /etc/rc.d/rc2.d/Ssshd stop
  ```

- 当安装了 OpenSSH 服务器文件集后，就有一项添加到 **/etc/rc.d/rc2.d** 目录。有一项在 inittab 中以执行运行级别 2 过程（`l2:2:wait:/etc/rc.d/rc 2`），以便 **sshd** 守护程序将在引导时自动启动。要防止守护程序在引导时启动，请删除 **/etc/rc.d/rc2.d/Ksshd** 和 **/etc/rc.d/rc2.d/Ssshd** 文件。
- OpenSSH 软件把信息记录到 SYSLOG 中。

- IBM 红皮书 *Managing AIX Server Farms* 提供有关在 AIX 中配置 OpenSSH 的信息，可以在以下 Web 站点中可以得到:

  http://www.redbooks.ibm.com

OpenSSH 编译的配置

本节提供有关在 AIX 中如何编译 OpenSSH 代码的信息。

当配置 AIX 5.1 版的 OpenSSH 时，输出的内容与以下相似:

```
OpenSSH 已配置带有以下选项:
                     用户二进制文件: /usr/bin
                   系统二进制文件: /usr/sbin
               配置文件: /etc/ssh
                   Askpass 程序: /usr/sbin/ssh-askpass
                      手册页: /usr/man
                          PID 文件: /etc/ssh
  特权分离 chroot 路径: /var/empty
            sshd 缺省用户路径: /usr/bin:/bin:/usr/sbin:/sbin:/usr/local/bin

                    联机帮助页: man
                       PAM 支持: no
                 KerberosIV 支持: no
                  KerberosV 支持: yes
                  智能卡支持: no
                        AFS 支持: no
                      S/KEY 支持: no
              TCP 包装程序支持: no
              MD5 密码支持: no
       $DISPLAY 黑客攻击中的 IP 地址: no
          在缺省的攻击时使用 IPv4: no
           在 v6 攻击中转换 v4: no
                 BSD 认证支持: no
              随机数来源: ssh-rand-helper
     ssh-rand-helper 收集位置: Command hashing (timeout 200)

              主机: powerpc-ibm-aix5.1.0.0
           编译器: cc
    编译器标志: -O -D__STR31__
预处理器标志: -I. -I$(srcdir) -I/home/BUILD/test2debug/zlib-1.1.3/ -I/o
pt/freeware/src/packages/SOURCES/openssl-0.9.6g/include -I/usr/include -I/usr/in
clude/gssapi -I/usr/include/ibm_svc -I/usr/local/include $(PATHS) -DHAVE_CONFIG_
H
      链接程序标志: -L. -Lopenbsd-compat/ -L/opt/freeware/lib/ -L/usr/local/lib
-L/usr/krb5/lib -blibpath:/opt/freeware/lib:/usr/lib:/lib:/usr/local/lib:/usr/kr
b5/lib
         库:    -lz  -lcrypto -lkrb5 -lk5crypto -lcom_err

警告: 您正在使用内置的随机数收集服务。请阅读 WARNING.RNG 并请求您的 OS
供应商在该 OS 的以后版本中包含基于内核的随机数集合。
```

当配置 AIX 5.2 版的 OpenSSH 时，输出的内容与以下相似:

```
OpenSSH 已配置带有以下选项:
                     用户二进制文件: /usr/bin
                   系统二进制文件: /usr/sbin
               配置文件: /etc/ssh
                   Askpass 程序: /usr/sbin/ssh-askpass
                      手册页: /usr/man
                          PID 文件: /etc/ssh
  特权分离 chroot 路径: /var/empty
            sshd 缺省用户路径: /usr/bin:/bin:/usr/sbin:/sbin:/usr/local/bin

                    联机帮助页: man
                       PAM 支持: no
```

```
                KerberosIV 支持: no
                 KerberosV 支持: yes
                 智能卡支持: no
                       AFS 支持: no
                    S/KEY 支持: no
               TCP 包装程序支持: no
               MD5 密码支持: no
        $DISPLAY 黑客攻击中的 IP 地址: no
           在缺省的攻击时使用 IPv4: no
            在 v6 攻击中转换 v4: no
                  BSD 认证支持: no
              随机数来源: OpenSSL 仅对于内部

              主机: powerpc-ibm-aix5.2.0.0
           编译器: cc
     编译器标志: -O -D__STR31__
     预处理器标志: -I/opt/freeware/src/packages/BUILD/openssl-0.9.6g/includ
e  -I/usr/local/include -I/usr/local/include
       链接程序标志: -L/opt/freeware/src/packages/BUILD/openssl-0.9.6g  -L/usr/lo
cal/lib -L/usr/local/lib -blibpath:/usr/lib:/lib:/usr/local/lib:/usr/local/lib
          库:    -lz  -lcrypto -lkrb5 -lk5crypto -lcom_err
```

OpenSSH 和 Kerberos V5 支持

Kerberos 是一种认证机制，它为网络用户提供了一种安全的认证方法。它通过加密客户机和服务器之间的认证消息来阻止通过网络传送明文密码。另外，Kerberos 提供了一个系统用于以管理令牌或凭证的形式进行授权。

要使用 Kerberos 来认证用户，该用户运行 **kinit** 命令从中心 Kerberos 服务器，即 KDC（密钥分发中心）获得初始凭证。KDC 将验证该用户并把他的初始凭证，即 TGT（授予凭单的凭单）发送回给他。然后该用户可以使用一个服务（比如 Kerberized Telnet 或 OpenSSH）来启动远程登录会话，而 Kerberos 通过从 KDC 获得用户凭证来认证该用户。Kerberos 执行此认证不需要任何用户交互，因此用户不需要输入密码来登录。IBM 版本的 Kerberos 称为“网络认证服务”（NAS）。NAS 可以从“AIX 扩展包 CD”安装。它可以在 **krb5.client.rte** 和 **krb5.server.rte** 软件包中获得。从 OpenSSH 3.6 的 2003 年 7 月发行版开始，OpenSSH 通过 NAS V1.3 支持 Kerberos 5 认证和授权。

AIX 已创建了带有 Kerberos 认证的 OpenSSH 作为可选的方法。如果未在系统上安装 Kerberos 库，则当 OpenSSH 运行时，将跳过 Kerberos 认证而 OpenSSH 尝试下一个已配置的认证方法（比如 AIX 认证）。

安装了 Kerberos 后，建议您先阅读 Kerberos 文档再去配置 Kerberos 服务器。有关如何安装和管理 Kerberos 的更多信息，请参考 *IBM Network Authentication Service Version 1.3 for AIX : Administrator's and User's Guide*，它位于 **/usr/lpp/krb5/doc/html/***lang***/ADMINGD.htm** 路径。

使用带有 Kerberos 的 OpenSSH

以下步骤提供了关于为使用带有 Kerberos 的 OpenSSH 所需的初始设置的信息:

1. 在您的 OpenSSH 客户机和服务器上，**/etc/krb5.conf** 文件必须存在。该文件告诉 Kerberos 使用哪个 KDC、给每个凭单的生命期多长，等等。以下是一个 **krb5.conf** 示例文件:

```
[libdefaults]
ticket_lifetime = 600
default_realm = OPENSSH.AUSTIN.XYZ.COM
default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc
default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc

[realms]
OPENSSH.AUSTIN.xyz.COM = {
```

```
    kdc = kerberos.austin.xyz.com:88
    kdc = kerberos-1.austin.xyz.com:88
    kdc = kerberos-2.austin.xyz.com:88
    admin_server = kerberos.austin.xyz.com:749
    default_domain = austin.xyz.com
}

[domain_realm]
    .austin.xyz.com = OPENSSH.AUSTIN.XYZ.COM
    kdc.austin.xyz.com = OPENSSH.AUSTIN.XYZ.COM
```

2. 同时，您必须把以下 Kerberos 服务添加到每个客户机的 **/etc/services** 文件中:

```
kerberos      88/udp    kdc    # Kerberos V5 KDC
kerberos      88/tcp    kdc    # Kerberos V5 KDC
kerberos-adm  749/tcp          # Kerberos 5 admin/changepw
kerberos-adm  749/udp          # Kerberos 5 admin/changepw
krb5_prop     754/tcp          # Kerberos slave
                               #  propagation
```

3. 如果您的 KDC 正在使用 LDAP 作为注册表以存储用户信息，则建议阅读第 61 页的第 4 章，『LDAP 认证装入模块』 和 Kerberos 出版物。另外，请确保执行了以下操作:
   - KDC 正在运行 LDAP 客户机。您可以用 **secldapclntd** 命令启动 LDAP 客户机守护程序。
   - LDAP 服务器正在运行 **slapd** LDAP 服务器守护程序。
4. 在 OpenSSH 服务器上，编辑 **/etc/ssh/sshd_config** 文件以包含以下行:

```
KerberosAuthentication yes
KerberosTicketCleanup yes
GssapiAuthentication yes
GssapiKeyExchange yes
GssapiCleanupCreds yes
```

5. 在 SSH 服务器上，运行 **startsrc -g ssh** 命令以启动 ssh 服务器守护程序。
6. 在 SSH 客户机上，运行 **kinit** 命令以获得初始凭证（TGT）。可以通过运行 **klist** 命令来验证是否接收到了 TGT。这将显示属于您的所有凭证。
7. 通过运行 **ssh** *username@servername* 命令来连接到服务器。
8. 如果正确配置了 Kerberos 以认证用户，则将不会显示要求密码的提示，且用户将自动登录到 SSH 服务器。

第 2 部分 网络和因特网的安全性

本指南的第二部分提供关于网络和因特网安全性措施的信息。这几章描述了如何安装和配置“IP 安全性”；如何识别必要和不必要的网络服务；审计和监视网络安全性及更多内容。

第 9 章 TCP/IP 安全性

如果安装了“传输控制协议／网际协议”（TCP/IP）和“网络文件系统”（NFS）软件，您可以对您的系统进行配置，使之通过网络进行通信。本指南不对 TCP/IP 基本概念进行描述，而描述 TCP/IP 的安全相关注意事项。关于 TCP/IP 安装及初始配置的信息，请参考 *《AIX 5L V5.2 系统管理指南: 通信与网络》* 中的『传输控制协议／网际协议』章节。

不管有多少理由，系统管理员都可能不得不遇到一定级别的安全问题。例如，安全级别可能是公司策略方面的事。或系统可能需要访问政府系统，因而要求以一定安全级别进行通信。这些安全标准可能适用于网络、操作系统、应用软件，甚至系统管理员写的程序。

本章描述 TCP/IP 以标准方式和作为安全系统所提供的安全特性，并讨论了一些网络环境中适当的安全注意事项。

安装了 TCP/IP 及 NFS 软件后，使用基于 Web 的系统管理器或系统管理界面工具（SMIT）**tcpip** 快速路径来配置系统。

本章讨论以下主题:

特定于操作系统的安全性

许多 TCP/IP 可用的安全特性是基于那些通过操作系统可用的安全特性。以下几节略述 TCP/IP 的安全性。

网络访问控制

联网的安全策略是操作系统安全策略的扩展，且它由以下主要部分组成:

- 与用户登录本地系统的方式相同，通过用户名称和密码在远程主机上提供**用户认证**。可信 TCP/IP 命令，例如 **ftp**、**rexec** 和 **telnet** 有相同的要求，并象操作系统中的可信命令一样经历相同的验证过程。
- 为确保远程主机有预期的“网际协议”（IP）地址及名称，提供**连接认证**。这防止远程主机伪装成另一个远程主机。
- **数据导入与导出安全性**允许具有指定安全级别的数据流入和流出具有同样的安全性和权限级别的网络接口适配器。例如，绝密数据仅可以在设置为绝密安全级的适配器之间流动。

网络审计

TCP/IP 提供网络审计，使用审计子系统来审计内核网络例程及应用程序。审计的目的是记录那些影响系统安全性的操作及对这些操作有责任的用户。

审计以下类型事件:

内核事件

- 更改配置
- 更改主机标识
- 更改路由
- 连接
- 创建套接字
- 导出对象
- 导入对象

应用程序事件

- 访问网络
- 更改配置
- 更改主机标识
- 更改静态路由
- 配置邮件
- 连接
- 导出数据
- 导入数据
- 将邮件写入文件

操作系统审计对象的创建及删除。应用程序审计记录暂挂并恢复审计以避免内核的冗余审计。

可信路径、可信 shell 和安全注意键（SAK）

操作系统提供*可信路径*以预防未授权程序读取用户终端数据。当需要同系统的安全通信路径，例如更改密码或登录系统时，使用此路径。操作系统也提供*可信 shell*（**tsh**），它只执行已经过测试并验证为安全的可信程序。TCP/IP 支持所有这些特性及*安全注意键*（SAK），它将在您与系统之间建立安全通信的必要环境。每当使用 TCP/IP 时，本地 SAK 可用。通过 **telnet** 命令，远程 SAK 也可用。

本地 SAK 在 **telnet** 中具有在其它操作系统应用程序中相同的功能：它结束 **telnet** 进程及所有与正在运行 **telnet** 的终端相关的其它进程。然而，在 **telnet** 程序中您可使用 **telnet send sak** 命令（此时以 **telnet** 命令方式）向远程系统发送对可信路径的请求。您也可以用 **telnet set sak** 命令定义一个单独键启动 SAK 请求。

关于可信计算库的更多信息，请参阅第 3 页的『可信计算库』。

TCP/IP 命令安全性

TCP/IP 中的一些命令提供操作过程中的安全环境。这些命令是 **ftp**、**rexec** 和 **telnet**。**ftp** 功能提供文件传送过程中的安全性。**rexec** 命令为在外部主机上运行命令提供安全环境。**telnet** 功能为登录外部主机提供安全性。

ftp、**rexec** 和 **telnet** 命令仅在它们操作过程中提供安全性。也就是说，它们并不建立与其它命令一起使用的安全环境。为了保护系统进行其它操作，使用 **securetcpip** 命令。此命令通过禁用非可信守护程序和应用程序，及提供保护 IP 层网络协议的选项，提供您保护系统安全的能力。

ftp、**rexec**、**securetcpip** 和 **telnet** 命令提供以下形式的系统及数据安全性:

ftp

ftp 命令提供传送文件的安全环境。当用户对外部主机调用 **ftp** 命令时，提示用户输入登录标识。显示的缺省登录标识为: 用户在本地主机的当前登录标识。提示用户输入远程主机的密码。

自动登录过程搜索本地用户的 **$HOME/.netrc** 文件以获取用于外部主机的用户标识及密码。对于安全性，**$HOME/.netrc** 文件的许可权必须设置为 600 （只能由所有者读写）。否则，自动登录失败。

> **注:** 因为 **.netrc** 文件的使用需要将密码存储在非加密文件中，当系统配置了 **securetcpip** 命令时，**ftp** 命令的自动登录功能不可用。通过将 **ftp** 命令从 **/etc/security/config** 文件的 tcpip 节中除去可以重新启用此功能。

要使用文件传送功能， **ftp** 命令需要两个 TCP/IP 连接，一个用于“文件传输协议”（FTP），另一个用于数据传输。协议连接是主要的而且是安全的，因为它建立在可靠的通信端口上。第二连接是实际数据传输所必需的，且本地及远程主机都验证了此连接的另一端由与主要连接相同的主机建立的。如果主要连接和第二连接不是由相同主机建立，**ftp** 命令首先显示错误消息，指出数据连接未认证，然后退出。第二连接的这种验证防止第三主机拦截要送至另一主机的数据。

rexec

rexec 命令为在外部主机上执行命令提供安全环境。提示用户输入登录标识及密码。

自动登录功能引起 **rexec** 命令搜索本地用户的 **$HOME/.netrc** 文件以获取外部主机上的用户标识及密码。对于安全性，**$HOME/.netrc** 文件的许可权必须设置为 600（只能由所有者读写）。否则，自动登录失败。

> **注:** 因为 **.netrc** 文件的使用需要将密码存储在非加密文件中，当系统在安全状态下操作时，**rexec** 的自动登录功能不可用。通过将 **rexec** 项从 **/etc/security/config** 文件中的 tcpip 节除去可以重新启用此功能。

securetcpip

securetcpip 命令启用 TCP/IP 安全功能。发出此命令时，从系统中除去对非可信命令的访问。通过运行 **securetcpip** 命令来除去以下每一个命令:

- **rlogin** 和 **rlogind**
- **rcp**、**rsh** 和 **rshd**
- **tftp** 和 **tftpd**
- **trpt**

使用 **securetcpip** 命令将系统从标准安全性级别转换为更高安全性级别。系统转换后，除非重装了 TCP/IP，否则不必再次发出 **securetcpip** 命令。

telnet 或 **tn**

telnet（TELNET）命令提供登录到外部主机的安全环境。提示用户输入登录标识及密码。将用户终端看作直接与主机连接的终端。即访问终端受控于许可位。其它用户（组及其它）没有对终端的读访问权，但如果所有者给予它们写许可权，它们就可以对终端写消息。**telnet** 命令也通过 SAK 提供对远程系统上可信 shell 的访问。此按键顺序不同于调用本地可信路径的顺序，并可以在 **telnet** 命令中定义。

远程命令执行的访问权（**/etc/hosts.equiv**）

列在 **/etc/hosts.equiv** 文件中的主机上的用户，无需提供密码就可以在系统上运行某些命令。下表中提供有关如何使用基于 Web 的系统管理器、SMIT 或命令行列出、添加和除去远程主机的信息。

远程命令执行的访问权任务

任务	SMIT 快速路径	命令或文件	基于 Web 的系统管理器 管理环境
列出具有命令执行的访问权的远程主机	**s m i t lshostsequiv**	查看 **/etc/hosts.equiv** 文件	软件 —> 网络 —> **TCPIP (IPv4 and IPv6)** —> **TCPIP** 协议配置 —> **TCP/IP** —> 配置 **TCP/IP** —> 高级方法 —> 主机文件 —> **/etc/hosts** 文件的内容。
为命令执行的访问权添加远程主机	**s m i t mkhostsequiv**	编辑 **/etc/hosts.equiv** 文件[注 1]	软件 —> 网络 —> **TCPIP (IPv4 and IPv6)** —> **TCPIP** 协议配置 —> **TCP/IP** —> 配置 **TCP/IP** —> 高级方法 —> 主机文件。在**添加 / 更改主机项**中，完成以下字段: **IP 地址**、**主机名**、**别名**和**注释**。单击**添加 / 更改项**，再单击**确定**。
从命令执行的访问权中除去远程主机	**s m i t rmhostsequiv**	编辑 **/etc/hosts.equiv** 文件[注 1]	软件 —> 网络 —> **TCPIP (IPv4 and IPv6)** —> **TCPIP** 协议配置 —> **TCP/IP** —> 配置 **TCP/IP** —> 高级方法 —> 主机文件。在 **/etc/host 文件内容**中选择主机。单击**删除项** —> **确定**。

注: 有关这些文件过程的更多信息，请参阅 *AIX 5L Version 5.2 Files Reference* 中的 “hosts.equiv File Format for TCP/IP” 。

限制文件传送程序用户（/etc/ftpusers）

/etc/ftpusers 文件中列出的用户受到保护，不允许远程 FTP 访问。例如，假设用户 A 登录到远程系统，而且他知道系统上用户 B 的密码。如果用户 B 列在 **/etc/ftpusers** 文件中，即使用户 A 知道用户 B 的密码，用户 A 也不能用 FTP 对用户 B 的帐户上传或下载文件。

下表提供有关如何使用基于 Web 的系统管理器、SMIT 或命令行列出、添加及除去受限用户的信息。

远程 FTP 用户任务

任务	SMIT 快速路径	命令或文件	基于 Web 的系统管理器 管理环境
列出受限 FTP 用户	**smit lsftpusers**	查看 **/etc/ftpusers** 文件	软件 —> 用户 —> 所有用户。
添加受限用户	**smit mkftpusers**	编辑 **/etc/ftpusers** 文件[注 1]	软件 —> 用户 —> 所有用户—> 选定 —> 将该用户添加到组。选择组，并单击**确定**。
除去受限用户	**smit rmftpusers**	编辑 **/etc/ftpusers** 文件[注 1]	软件 —> 用户 —> 所有用户 —> 选定 —> 删除。

注: 有关这些文件过程的更多信息，请参阅 *AIX 5L Version 5.2 Files Reference* 中的 “ftpusers File Format for TCP/IP” 。

可信进程

可信程序或可信进程是满足特定安全标准的 shell 脚本、守护程序或程序。这些安全标准由美国国防部设置并维护，美国国防部也认证一些可信程序。

可信程序在不同级别可信。安全级别包括 A1、B1、B2、B3、C1、C2 和 D，A1 级提供最高安全性级别。每个安全性级别必须满足一定的要求。例如，C2 安全性级别可具体说明以下标准:

程序完整性 确保完全按计划执行进程。

模块性
将进程源代码分隔成不会直接受其它模块影响或访问的模块。

最少特权原则
说明用户一直以授予的最低级特权操作。即如果用户只能有权查看某些文件，那么用户也就无权意外地改变此文件。

对象重用的限制
例如，防止用户意外地找到已标出要覆盖而还未清除的可能包含敏感资料的内存区域。

TCP/IP 包含几个可信守护程序及许多非可信守护程序。

可信守护程序的示例如下:

- **ftpd**
- **rexecd**
- **telnetd**

非可信守护程序的示例如下:

- **rshd**
- **rlogind**
- **tftpd**

对于可信系统，必须用可信计算库操作，即对于单独主机，机器必须安全。对于网络，全部文件服务器、网关和其它主机必须安全。

网络可信计算库

“网络可信计算库”（NTCB）由硬件和软件构成并确保网络安全性。本节定义与 TCP/IP 有关的 NTCB 组件。

网络的硬件安全特性由与 TCP/IP 一起使用的网络适配器提供。这些适配器通过只接收目的地为本地系统的数据和所有系统都可接收的广播数据来控制进入的数据。

NTCB 的软件组件仅由那些已认为可信的程序构成。作为安全系统的一部分的程序及相关文件基于目录到目录在下表中列出。

/etc 目录

名称	所有者	组	方式	许可权
gated.conf	root	system	0664	rw-rw-r—
gateways	root	system	0664	rw-rw-r—
hosts	root	system	0664	rw-rw-r—
hosts.equiv	root	system	0664	rw-rw-r—
inetd.conf	root	system	0644	rw-r—r—
named.conf	root	system	0644	rw-r—r—
named.data	root	system	0664	rw-rw-r—
networks	root	system	0664	rw-rw-r—
protocols	root	system	0644	rw-r—r—
rc.tcpip	root	system	0774	rwxrwxr—
resolv.conf	root	system	0644	rw-rw-r—
services	root	system	0644	rw-r—r—
3270.keys	root	system	0664	rw-rw-r—

/etc 目录

名称	所有者	组	方式	许可权
3270keys.rt	root	system	0664	rw-rw-r—

/usr/bin 目录

名称	所有者	组	方式	许可权
host	root	system	4555	r-sr-xr-x
hostid	bin	bin	0555	r-xr-xr-x
hostname	bin	bin	0555	r-xr-xr-x
finger	root	system	0755	rwxr-xr-x
ftp	root	system	4555	r-sr-xr-x
netstat	root	bin	4555	r-sr-xr-x
rexec	root	bin	4555	r-sr-xr-x
ruptime	root	system	4555	r-sr-xr-x
rwho	root	system	4555	r-sr-xr-x
talk	bin	bin	0555	r-xr-xr-x
telnet	root	system	4555	r-sr-xr-x

/usr/sbin 目录

名称	所有者	组	方式	许可权
arp	root	system	4555	r-sr-xr-x
fingerd	root	system	0554	r-xr-xr—
ftpd	root	system	4554	r-sr-xr—
gated	root	system	4554	r-sr-xr—
ifconfig	bin	bin	0555	r-xr-xr-x
inetd	root	system	4554	r-sr-xr—
named	root	system	4554	r-sr-x—
ping	root	system	4555	r-sr-xr-x
rexecd	root	system	4554	r-sr-xr—
route	root	system	4554	r-sr-xr—
routed	root	system	0554	r-xr-x—-
rwhod	root	system	4554	r-sr-xr—
securetcpip	root	system	0554	r-xr-xr—
setclock	root	system	4555	r-sr-xr-x
syslogd	root	system	0554	r-xr-xr—
talkd	root	system	4554	r-sr-xr—
telnetd	root	system	4554	r-sr-xr—

/usr/ucb 目录

名称	所有者	组	方式	许可权
tn	root	system	4555	r-sr-xr-x

/var/spool/rwho 目录

名称	所有者	组	方式	许可权
rwho（目录）	root	system	0755	drwxr-xr-x

数据安全性及信息保护

TCP/IP 的安全功能并没有加密通过网络传送的用户数据。因此，建议用户识别通信中任何可能导致密码及其它敏感信息泄露的风险，并基于该风险应用相应的对策。

在“国防部”（DOD）环境中使用 TCP/IP 安全功能可能需要遵守关于通信安全性的 DOD 5200.5 和 NCSD-11。

基于用户的 TCP 端口访问控制和因特网端口的带有自主访问控制

“因特网端口（DACinet）的自主访问控制”是某种基于用户的访问控制的特征，该访问控制应用于 AIX 5.2 主机之间通信的 TCP 端口。AIX 5.2 可以使用附加的 TCP 头传送系统之间的用户及组信息。DACinet 特性允许目标系统上的管理员控制基于目标端口、始发用户标识及主机的访问。

另外，DACinet 特性允许管理员限制本地端口只能由 root 用户使用。象 AIX 这样的 UNIX 系统将 1024 以下的端口视为只能由 root 用户打开的特权端口。AIX 5.2 允许您指定 1024 以上只能由 root 用户打开的附加端口，因此防止用户在熟知的端口上运行服务器。

视设置而定，非 DACinet 系统可能可以或无法连接至 DACinet 系统。DACinet 特性的初始状态拒绝访问。一旦启用了 DACinet，就无法禁用 DACinet。

dacinet 命令接受被指定为主机名、点分十进制主机地址或后面跟有网络前缀长度的网络地址的地址。

以下示例指定一个单一主机，已知它的全限定主机名为 *host.domain.org*:

```
host.domain.org
```

以下示例指定一个单一主机，已知它的 IP 地址为 10.0.0.1:

```
10.0.0.1
```

以下示例指定具有 10.0.0.0 值的前 24 位（网络前缀长度）的整个网络:

```
10.0.0.0/24
```

此网络包括 10.0.0.1 与 10.0.0.254 之间的所有 IP 地址。

基于 TCP 的服务的访问控制

DACinet 使用 **/etc/rc.dacinet** 启动文件，且使用的配置文件是 **/etc/security/priv**、**/etc/security/services** 和 **/etc/security/acl**。

列于 **/etc/security/services** 的端口视为免于 ACL 检查。此文件具有与 **/etc/services** 相同的格式。对其进行初始化最简便的方式就是将文件从 **/etc** 复制到 **/etc/security**，然后删除所有应该应用 ACL 的端口。ACL 存储在两个地方。当前活动的 ACL 存储在内核，而且可以通过运行 **dacinet aclls** 来读取。将在下一次系统引导时通过 **/etc/rc.tcpip** 来重新激活的 ACL 存储在 **/etc/security/acl** 中。使用以下格式:

```
service host/prefix-length [user|group]
```

这里可用数字或 **/etc/services** 中所列的方式指定服务，可用主机名或具有子网掩码规范的网络地址给出主机，而且用 **u:** 或 **g:** 前缀指定用户或组。当没有指定用户或组时，那么 ACL 只考虑发送主机。给服务加上前缀 **-** 将显式地禁用访问。根据第一个匹配评估 ACL。因而您可以为一组用户指定访问，但也可以通过将组中某用户的规则置于组规则之前来显式地拒绝此用户。

/etc/services 文件包含两个项，它们具有 AIX 5.2 中不支持的端口号值。系统管理员必须在执行 **mkCCadmin** 命令前除去文件中的这两行。从 **/etc/services** 文件中除去以下行:

```
sco_printer     70000/tcp     sco_spooler    # For System V print IPC
sco_s5_port     70001/tcp     lpNet_s5_port  # For future use
```

DACinet 使用示例

例如，使用 DACinet 将端口 TCP/25 的入站访问限定于只具有 DACinet 特性的 root 用户时，那么只有其它 AIX 5.2 主机的 root 用户能访问此端口，因此，限制了常规用户仅通过远程登录到该主机的端口 TCP/25 就能欺骗电子邮件的可能性。以下示例显示如何为只能访问的 root 用户配置 X 协议（X11）。确保将 **/etc/security/services** 中的 X11 项已除去，以使 ACL 应用于此服务。

假定一个所有连接系统的 10.1.1.0/24 子网，将访问限定于 root 用户（仅对 **/etc/security/acl** 中的 X（TCP/6000））的 ACL 项如下:

```
      6000    10.1.1.0/24 u:root
```

限制 **friends** 组中用户的 Telnet 服务时，不管它们来自哪个系统，从 **/etc/security/services** 除去 telnet 项后，使用以下 ACL 项:

```
telnet    0.0.0.0/0   g:friends
```

禁止用户 fred 访问 Web 服务器，但允许其他人访问:

```
-80     0.0.0.0/0 u:fred
80      0.0.0.0/0
```

运行本地服务的特权端口

通常任何用户可以打开 1024 以上的任何端口。例如，用户可在端口 8080 放置常用于运行 Web 代理的服务器，或通常在 1080 位置放置 SOCKS 服务器。要防止常规用户在指定端口运行服务器，可将这些端口指定为具有特权。**dacinet setpriv** 命令可以用于向正在运行的系统添加特权端口。系统启动时，指定为具有特权的端口必须列在 **/etc/security/priv** 中。

用 **/etc/services** 中定义的符号名称或通过指定端口号将端口列在此文件中。以下项将禁止非 root 用户在通常的端口运行 SOCKS 服务器或 Lotus Notes 服务器。

```
1080
lotusnote
```

注: 此功能不能防止**用户**运行程序。它只能防止用户在熟知的端口运行服务，而这些端口通常正需要这些服务。

关于 **dacinet** 命令的更多信息，请参阅 *《AIX 5L V5.2 命令参考大全》*。

第 10 章 网络服务

本章提供有关识别和保护打开通信端口的网络服务的信息

识别打开通信端口的网络服务

客户机服务器应用程序在服务器上打开通信端口，允许应用程序侦听接收到的客户机请求。因为打开的端口易受潜在的安全攻击，所以要识别打开端口的这些应用程序并关闭那些没有必要打开的端口。这种习惯很有用，因为它使您知道什么系统对从因特网上访问的人来说是可用的。

要确定打开的端口，请执行以下操作:

1. 使用如下的 **netstat** 命令来识别服务:

   ```
   # netstat -af inet
   ```

   下面是该命令输出的例子。**netstat** 命令输出的最后一列表示每种服务的状态。等待进入连接状态的服务处于 LISTEN 状态。

活动的因特网连接（包括服务器）

Proto	Recv-Q	Send-Q	本地地址	外部地址	（状态）
tcp4	0	0	*.echo	*.*	LISTEN
tcp4	0	0	*.discard	*.*	LISTEN
tcp4	0	0	*.daytime	*.*	LISTEN
tcp	0	0	*.chargen	*.*	LISTEN
tcp	0	0	*.ftp	*.*	LISTEN
tcp4	0	0	*.telnet	*.*	LISTEN
tcp4	0	0	*.smtp	*.*	LISTEN
tcp4	0	0	*.time	*.*	LISTEN
tcp4	0	0	*.www	*.*	LISTEN
tcp4	0	0	*.sunrpc	*.*	LISTEN
tcp	0	0	*.smux	*.*	LISTEN
tcp	0	0	*.exec	*.*	LISTEN
tcp	0	0	*.login	*.*	LISTEN
tcp4	0	0	*.shell	*.*	LISTEN
tcp4	0	0	*.klogin	*.*	LISTEN
udp4	0	0	*.kshell	*.*	LISTEN
udp4	0	0	*.echo	*.*	
udp4	0	0	*.discard	*.*	
udp4	0	0	*.daytime	*.*	
udp4	0	0	*.chargen	*.*	

活动的因特网连接（包括服务器）

Proto	Recv-Q	Send-Q	本地地址	外部地址	（状态）
udp4	0	0	*.time	*.*	
udp4	0	0	*.bootpc	*.*	
udp4	0	0	*.sunrpc	*.*	
udp4	0	0	255.255.255.255.ntp	*.*	
udp4	0	0	1.23.123.234.ntp	*.*	
udp4	0	0	localhost.domain.ntp	*.*	
udp4	0	0	name.domain..ntp	*.*	

.....

2. 打开 **/etc/services** 文件因特网号码分配管理局（IANA）服务从而在操作系统中将服务映射到把端口号。

下面是 **/etc/services** 文件的样本片段:

```
tcpmux                          1/tcp                   # TCP Port Service Multiplexer
tcpmux                          1/tcp                   # TCP Port Service Multiplexer
Compressnet                     2/tcp                   # Management Utility
Compressnet                     2/udp                   # Management Utility
Compressnet                     3/tcp                   # Compression Process
Compressnet                     3/udp                   Compression Process
Echo                            7/tcp
Echo                            7/udp
discard                         9/tcp                   sink null
discard                         9/udp                   sink null
..............
rfe                             5002/tcp                # Radio Free Ethernet
rfe                             5002/udp                # Radio Free Ethernet
rmonitor_secure                 5145/tcp
rmonitor_secure                 5145/udp
pad12sim                        5236/tcp
pad12sim                        5236/udp
sub-process                     6111/tcp                # HP SoftBench Sub-Process Cntl.
sub-process                     6111/udp                # HP SoftBench Sub-Process Cntl.
xdsxdm                          6558/ucp
xdsxdm                          6558/tcp
afs3-fileserver                 7000/tcp                # File Server Itself
```

```
afs3 文件服务器                  7000/udp            # File Server Itself
af3-callback                     7001/tcp            # Callbacks to Cache Managers
af3-callback                     7001/udp            # Callbacks to Cache Managers
```

3. 通过除去正在运行的服务来关闭不必要的端口。

识别 TCP 和 UDP 套接字

识别处在 LISTEN 状态的 TCP 套接字和等待数据到达的空闲 UDP 套接字。使用 **lsof** 命令，它是 **netstat -af** 命令的变体。在 AIX 5.1 开始，**lsof** 命令包含在 *AIX Toolbox for Linux Applications* CD 中。

例如，要显示处在 LISTEN 状态的 TCP 套接字和等待数据到达的空闲 UDP 套接字，请如下运行 **lsof** 命令:

```
# lsof -i | egrep "COMMAND|LISTEN|UDP"
```

输出结果与以下类似:

Command	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
dtlogin	2122	root	5u	IPv4	0x70053c00	0t0	UDP	*:xdmcp
dtlogin	2122	root	6u	IPv4	0x70054adc	0t0	TCP	*:32768(LISTEN)
syslogd	2730	root	4u	IPv4	0x70053600	0t0	UDP	*:syslog
X	2880	root	6u	IPv4	0x70054adc	0t0	TCP	*:32768(LISTEN)
X	2880	root	8u	IPv4	0x700546dc	0t0	TCP	*:6000(LISTEN)
dtlogin	3882	root	6u	IPv4	0x70054adc	0t0	TCP	*:32768(LISTEN)
glbd	4154	root	4u	IPv4	0x7003f300	0t0	UDP	*:32803
glbd	4154	root	9u	IPv4	0x7003f700	0t0	UDP	*:32805
dtgreet	4656	root	6u	IPv4	0x70054adc	0t0	TCP	*:32768(LISTEN)

在确定进程标识后，您可以运行以下命令获取有关应用程序的更多信息:

```
" # ps -fp PID#"
```

输出包含命令名称的路径，您可以用它来访问该程序的联机帮助页。

第 11 章 网际协议（IP）安全性

IP 安全性通过在 IP 层的安全数据流量来启用因特网和公司网络内的安全通信。它允许个别的用户或组织对于所有应用程序保护流量，而不必对应用程序进行任何修改。因此，可以安全的传送任何数据，例如电子邮件或特定应用程序的公司数据。

本章讨论以下主题:

IP 安全性概述

本节讨论以下主题:

- IP 安全性和操作系统
- IP 安全功能
- 安全性关联
- 隧道和密钥管理
- 本地过滤器能力
- 数字证书支持
- 虚拟专用网的好处

IP 安全性操作系统

操作系统使用 IP 安全（IPsec）技术，该技术是一开放的、标准的安全技术，是由因特网工程任务组织（IETF）开发的。IPsec 对在通信堆栈内 IP 层的所有数据提供基于密码系统的保护。不需要更改现有的应用程序。IPsec 是 IETF 为 IP V4 和 V6 环境选择的工业标准网络安全框架。

IPsec 使用以下密码技术保护您的数据通信:

认证 决定要验证哪个主机或端点的身份的进程

完整性检查
确保在跨越网络传输时没有修改数据的进程

加密 确保在网络上传输的“隐藏”数据和私有 IP 地址保密性的进程

认证算法证实发送方的标识和数据完整性，通过使用密码散列函数来处理使用密钥产生唯一摘要的数据信息包（包含固定的 IP 报头字段）。在接收方，用相同的函数和密钥处理数据。如果任何一方更改了数据，或者发送方密钥无效，则废弃该数据报。

加密使用一个密码算法修改并使数据随机化，该过程使用特定算法和密钥产生称为*加密文本*的加密数据。加密使数据在传输时无法破解。在接收到加密数据之后，使用相同算法和密钥（对称的加密算法）重新获得该数据。加密必需同认证同时发生来验证加密数据的数据完整性。

这些基本服务是在 IPsec 中执行的，该执行过程使用封装安全性有效负载（ESP）和认证标题（AH）。ESP 通过加密原始的 IP 信息包、构建 ESP 报头、将翻译文本放入 ESP 有效负载来提供机密性。

如果机密性没有问题，可以单独使用 AH 来进行认证和一致性检查。使用 AH，IP 报头和数据的静态字段有一个适用于计算键控摘要的散列算法。接收方使用它的密钥计算并比较摘要以确保信息包没有改变以及发送方是已认证身份。

IP 安全功能

该操作系统的 IP 安全功能提供以下功能:

- 10/100 Mbps 以太网 PCI 适配器 II 的硬件加速。
- AH 支持使用 RFC 2402，ESP 支持使用 RFC 2406。
- “证书撤销列表”支持使用 HTTP 或者 LDAP 服务器检索。
- 隧道的自动密钥刷新使用 IETF 因特网密钥交换（IKE）协议。
- 在密钥协商期间 IKE 协议支持 X.509 数字证书和预共享密钥。
- 手工隧道可以配置为提供同其它系统的互操作性，该其它系统不支持自动 IKE 密钥刷新方法，用于 IP V6 隧道。
- 主机或网关隧道的隧道方式和传输方式。
- HMAC（散列消息认证代码）、MD5（消息摘要 5）和 HMAC SHA（安全散列算法）认证算法。
- 加密算法包含 56 位数据加密标准（DES）带有64 位初始向量（VI）的密码分组链接（CBC），三重 DES，DES CBC 4（32 位IV）。
- 双 IP 堆栈支持（IP V4 和 IP V6）。
- 可以封装和过滤 IP V4 和 IP V6 的流量。因为 IP 堆栈是分离的，每个堆栈的“IP 安全性”函数可以独立配置。
- IKE 隧道可以用 Linux 配置文件（AIX 5.1 和后续版本）来创建。
- 通过多种 IP 特征，比如源和目标 IP 地址、接口、协议、端口号等，过滤安全和不安全的流量。
- 自动创建和删除多数隧道类型的过滤规则。
- 当定义隧道和过滤规则时用于目的地址的主机名的使用。主机名自动地转换成 IP 地址（只要 DNS 可用）。
- 将“IP 安全性”事件记录到 **syslog**。
- 使用系统跟踪和统计学来进行问题确定。
- 用户定义的缺省操作允许用户指定是否允许与定义的隧道不匹配的流量。

因特网密钥交换（IKE）特征

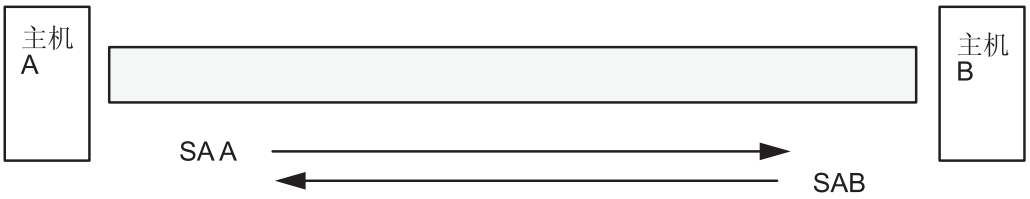
因特网密钥交换（从 AIX 4.3.2 开始）可用以下功能:

- 有预共享的密钥和 X.509 数字签名的认证。
- 使用的主要方式（身份保护方式）和进攻方式。

- 支持 Diffie Hellman 1、2 和 5 组。
- ESP 加密支持数据加密标准（DES）、三重 DES、Null 加密; ESP 认证支持 HMAC MD5 和 HMAC SHA1。
- AH 支持 HMAC MD5 和 HMAC SHA1。
- 支持 IP V4 和 V6。

安全性关联

安全通信所构建的构建模块称为*安全性关联*的概念。安全性关联使一个安全参数的特定设置关联到一个流量类型。通过 “IP 安全性” 保护的数据，每个方向、每个报头类型、AH 或 ESP 都存在一个分离的安全性关联。在安全性关联中包含的信息包括通信各方的 IP 地址、一个称作安全性参数索引（SPI）的唯一标识符、为认证或加密选定的算法、认证和加密密钥和密钥生命期。以下数字显示了在主机 A 和主机 B 之间的安全性关联。



SA = 安全性关联，由下列项组成：

目标地址
SPI
密钥
加密算法和格式
认证算法
密钥生命期

图 6. 在主机 A 和 B 之间安全隧道的建立. 本插图显示运行在主机 A 和主机 B 间的虚拟隧道。安全性关联 A 是从 A 指向 B 的箭头。安全性关联 B 是从主机 B 指向主机 A 的箭头。一个安全性关联由目标地址、SPI、密钥、加密器算法和格式、认证算法及密钥生命期构成。

密钥管理的目标是协商和计算保护 IP 流量的安全性关联。

隧道和密钥管理

要在两个主机间安装安全通信，在使用隧道期间必须协商和管理安全性关联。以下是支持的隧道类型，每个类型使用一个不同的密钥管理技术:

- IKE 隧道（动态更改密钥，IETF 标准）
- 手工隧道（静态、持久密钥，IETF 标准）

IKE 隧道支持

IKE 隧道是基于 IETF 开发的 ISAKMP/Oakley（因特网安全性关联和密钥管理协议）标准。使用此协议，协商和刷新安全性参数，并安全地交换密钥。以下认证类型支持: 预共享密钥和 X.509v3 数字证书签名。

协商使用一个两阶段方案。第一阶段认证通信的各方，并为第二阶段的安全通信指定使用的算法。在第二阶段期间，协商数据传输过程将使用的 “IP 安全性” 参数，并创建和交换安全性关联和密钥。

以下表显示的认证算法可以用于使 AH 和 ESP 安全协议支持 IKE 隧道。

算法	AH IP V4 & 6	ESP IP V4 & 6
HMAC MD5	X	X
HMAC SHA1	X	X
DES CBC 8		X
三重 DES CBC		X
ESP Null		X

手工隧道支持

手工隧道提供向后兼容性，它们与不支持 IKE 密钥管理协议的机器互操作。手工隧道的缺点是密钥值是静态的。加密和认证密钥对于隧道的生命周期是相同的，而且必需手工更新。

以下表显示的认证算法可以用于使 AH 和 ESP 安全协议支持手工隧道。

算法	AH IP V4	AH IP V6	ESP IP V4	ESP IP V6
HMAC MD5	X	X	X	X
HMAC SHA1	X	X	X	X
三重 DES CBC			X	X
DES CBC 8			X	X
DES CBC 4			X	X

因为 IKE 隧道提供更有效的安全性，IKE 是首选的密钥管理方法。

本机过滤能力

*过滤*是一个基本功能，基于它的各种特征传入和发送可以接受或拒绝的信息包。这允许用户或系统管理员配置主机来控制该主机和其它主机之间的流量。过滤是在各种信息包属性上完成的，例如源和目标地址、IP 版本（4 或者 6）、子网掩码、协议、端口、路由特征、分解片段、接口和隧道定义。

称为*过滤规则*的规则用于关联某种具有特殊隧道的流量。在手工隧道的基本配置中，当用户定义了主机到主机的隧道时，过滤规则自动生成指导从该主机来的所有流量通过安全隧道。如果期望更多特定类型流量（例如子网到子网），可以编辑或替换过滤规则来允许对使用特殊隧道的流量进行精确控制。

对于 IKE 隧道，一旦激活隧道，过滤规则也将自动生成并插入到过滤表中。

相似地，当修改了或删除了隧道，则自动删除该隧道的过滤规则，这将简化 “IP 安全性” 配置并减少人为错误。隧道定义可以使用导入和导出实用程序在机器和防火墙间传播和共享，这对于大量机器的管理是有很帮助的。

过滤规则关联隧道的特殊类型的流量，但过滤的数据未必需要在隧道中传送。过滤规则的这个方面让操作系统为一些人提供基本的防火墙功能，这些人想限制从没有真正的防火墙保护的内部网或外部网络上往返于他们机器的流量。在本方案中，过滤规则在一组机器外提供第二层保护屏障。

在生成过滤规则后，它们被存储在一个表中，并装入内核。当准备从网络发送或接收信息包，在列表中从头到尾检查过滤规则以确定信息包是否许可、拒绝或通过隧道发送。规则准则同信息包特征比较，直到找到匹配或达到缺省规则。

“IP 安全性”功能同样实现非安全信息包过滤，该过滤是基于小包的、用户定义标准的过滤，这允许在不需要认证或“IP 安全性”的加密属性的网络和机器间控制流量。

数字证书支持

“IP 安全性”支持使用 X.509 V3 数字证书。“密钥管理器”工具管理证书申请，维护密钥数据库，并进行其它的管理功能。

数字证书描述在数字证书配置中。“密钥管理器”和它的功能描述在使用 IBM 密钥管理器工具中。

虚拟专用网和 IP 安全性

一个虚拟专用网（VPN），通过如因特网一样的公用网络安全地扩展一个专用内部网。VPN 通过本质上是在因特网上的专用隧道，在远程用户、分公司和商务伙伴／供应商之间往返传递信息。公司可以选择通过因特网服务供应商（ISP）的因特网访问，使用直接线路或本地电话号码，排除更贵的租用线路、长距离呼叫和免费电话号码。VPN 解决方案可以使用 IPsec 安全性标准，因为 IPsec 是 IETF 选择的工业标准网络安全框架，适用于 IP V4 和 6 的环境，不需要改变现有的应用程序。

对在 AIX 中规划和实现 VPN 的建议资源是 *A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management* 的第 9 章，ISBN SG24-5309-00。该指南也可以在因特网的万维网中得到 http://www.redbooks.ibm.com/redbooks/SG245309.html。

安装 IP 安全性功能

AIX 中的 IP 安全性功能是独立安装并且可载入的。需要安装的文件集如下:

- **bos.net.ipsec.rte**（用于内核 IP 安全性环境和命令的运行时环境）
- **bos.msg.***LANG***.net.ipsec**（其中 *LANG* 是想期望的语言，例如 **en_US**）
- **bos.net.ipsec.keymgt**
- **bos.net.ipsec.websm**
- **bos.crypto-priv**（DES 和三重 DES 加密的文件集合）

bos.crypto-priv 文件集位于“扩展包”中。对于 IKE 数字签名支持，您必须也安装 **gskit.rte** 文件集（AIX V4）或者“扩展包”中的 **gskkm.rte**（AIX 5.1）。

要在 基于 Web 的系统管理器 中支持 IP 安全，必须安装 **Java131.ext.xml4j** 文件集，级别 1.3.1.1 或后续版本。

安装后，对于 IP V4 和 IP V6，可以独立装入 IP 安全性，使用『装入 IP 安全性』中提供的推荐过程或者使用 **mkdev** 命令。

装入 IP 安全性

> **注**: 装入 IP 安全性启用过滤功能。装入之前，确保创建了正确的过滤器规则是很重要的。否则，所有外界通信可能都受阻塞。

在启动 IP 安全性时，使用 SMIT 或者基于 Web 的系统管理器自动地装入 IP 安全性模块。同样的，SMIT 和基于 Web 的系统管理器确保按照正确的顺序装入内核扩展和 IKE 守护程序。

如果装入成功完成，**lsdev** 命令将显示 IP 安全性设备为Available。

```
lsdev -C -c ipsec

  ipsec_v4 Available IP Version 4 Security Extension
  ipsec_v6 Available IP Version 6 Security Extension
```

装入了 IP 安全性内核扩展之后，准备配置报文封装和过滤器。

规划 IP 安全性配置

要配置“IP 安全性”，必须配置隧道和过滤器。当定义全部流量使用简单隧道时，可以自动地生成过滤规则。如果期望更复杂的过滤，可以个别地配置过滤规则。

配置“IP 安全性”，使用基于 Web 的系统管理器网络插件、虚拟专用网插件或系统管理接口工具（SMIT）。如果使用 SMIT，可用以下快速路径:

smit ips4_basic
IP V4 的基本配置

smit ips6_basic
IP V6 的基本配置

在配置站点“IP 安全性”之前，必须决定意在用什么方法；例如，是否更想使用隧道或过滤器（或两个都使用），哪一种类型的隧道最符合需要等等。以下部分提供了在做出这些决定之前必须理解的信息:

- 硬件加速
- 隧道与过滤器
- 隧道和安全性关联
- 选择隧道类型
- 带 DHCP 或动态分配地址使用 IKE

硬件加速

10/100 Mbps 以太网 PCI 适配器 II（功能代码 4962）提供基于标准的“IP 安全性”，以及设计为从 AIX 操作系统中卸载“IP 安全性”功能。当 AIX 系统中有 10/100 Mbps 以太网 PCI 适配器 II，“IP 安全性”堆栈使用适配器的以下能力:

- 使用 DES 或三重 DES 算法加密和解密
- 使用 MD5 或 SHA-1 算法进行认证
- 存储安全性关联信息。

使用适配器上的功能而不是软件算法。10/100 Mbps 以太网 PCI 适配器 II 也可用于手工和 IKE 隧道。

“IP 安全性”硬件加速功能在 **bos.net.ipsec.rte** 和 **devices.pci.1410ff01.rte** 文件集的 **5.1.0.25** 或更新级别中可用。

对于安全性关联的数量有一个限制，这样可以卸载到接收方（入站流量）的网络适配器上。在发送方（出站流量），所有使用支持配置的信息包卸载到适配器上。某个隧道配置不能卸载到适配器上。

10/100 Mbps 以太网适配器 II 支持以下内容:

- 通过 ESP 加密 DES、3DES 或 NULL
- 通过 ESP 或 AH 认证 HMAC-MD5 或 HMAC-SHA-1，但不能同时。（如果 ESP 和 AH 同时使用，ESP 必须首先执行。这对于 IKE 隧道始终是正确的，但用户可以选择手工隧道的订单。）
- 传输和隧道方式
- 卸载 IPV4 信息包

注: 10/100 Mbps 以太网 PCI 适配器 II 不能用 IP 选项处理信息包。

要为“IP 安全性”启用 10/100 Mbps 以太网 PCI 适配器，必须拆离网络接口，然后启用“IPsec 卸载”功能。

要拆离网络接口，请使用 SMIT 接口执行以下操作:

1. 作为 **root** 用户登录。
2. 在命令行中输入 `smitty inet` 并按 Enter 键。
3. 选择**除去网络接口**选项并按 Enter 键。
4. 选择与 10/100 Mbps 以太网 PCI 适配器 II 相对应的网络接口并按 Enter 键。

要启用 “IPsec 卸载” 功能，请用 SMIT 接口执行以下操作:

1. 作为 **root** 用户登录。
2. 在命令行中输入 `smitty eadap` 并按 Enter 键。
3. 选择**更改 / 显示以太网适配器的特征**选项并按 Enter 键。
4. 选择 10/100 Mbps 以太网 PCI 适配器 II 并按 Enter 键。
5. 更改 **IPsec 卸载**字段为**是**并按 Enter 键。

要拆离网络接口，请在命令行中输入以下内容:

```
# ifconfig enX detach
```

要启用 IPsec 卸载属性，请在命令行中输入以下内容:

```
# chdev -l entX -a ipsec_offload=yes
```

要验证 IPsec 卸载属性已启用，请在命令行中输入以下内容:

```
# lsattr -El entX detach
```

要禁用 IPsec 卸载属性，请在命令行中输入以下内容:

```
# chdev -l entX -a ipsec_offload=no
```

使用 **enstat** 命令来确保隧道配置正在使用 IPsec 卸载属性。当 IPsec 卸载特征启用时，**enstat** 命令显示了发送和接收的 IPsec 信息包的全部的统计信息。例如，如果以太网接口是 *ent1*，请输入以下内容:

```
# entstat -d ent1
```

输出与以下内容相似:

```
.
.
.
10/100 Mbps 以太网 PCI 适配器 II (1410ff01) 详尽统计:
---------------------------------------------
.
.
.
发送 IPsec 信息包: 3
删除的发送 IPsec 信息包: 0
接收 IPsec 信息包: 2
删除的接收 IPsec 信息包: 0
```

隧道与过滤器

“IP 安全性” 的两个不同的部分是*隧道*和*过滤器*。隧道需要过滤器，但过滤器不需要隧道。

- *过滤*是一种功能，它可以基于称为*规则*的多种特征来接受或拒绝接收和发送的信息包。这个功能允许系统管理员配置主机来控制该主机与其它主机之间的流量。过滤是基于多种信息包属性完成的，例如源地址和目标地址，IP 版本（4 或 6）、子网掩码、协议、端口、路由特征、分解片段、接口和隧道定义。该过滤是在 IP 层完成的，所以无须更改应用程序。

- *隧道*定义了两个主机间的安全性关联。该安全性关联涉及特定的安全参数，该参数由隧道的端点共享。

以下插图显示了信息包是如何从网络适配器到 IP 堆栈中的。从那里调用过滤器模块以确定是否允许或拒绝该信息包。如果指定了隧道标识，信息包会检查现有的隧道定义。如果从隧道中成功解封，则将信息包传递到上层协议。该功能在发送信息包的倒序时发生。隧道依赖于过滤规则来将信息包与特定的信息包关联，但是过滤功能可以在不将信息包发送到隧道的情况下发生。

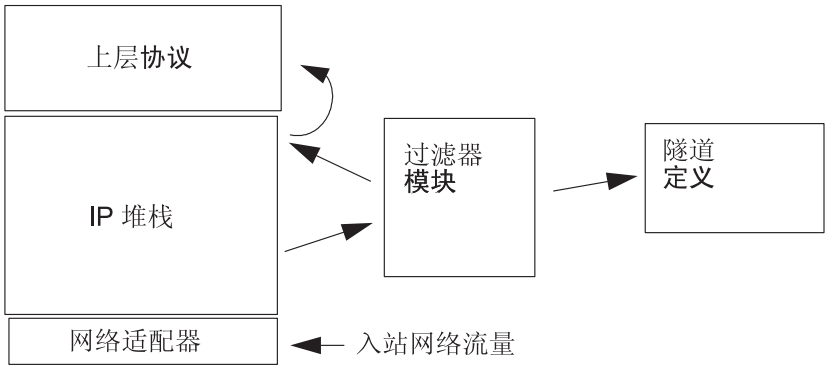
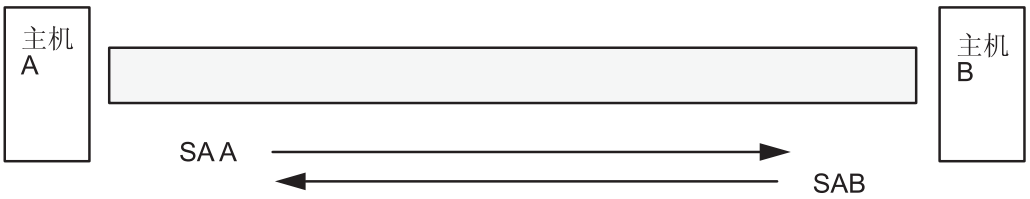


图 7. 网络信息包路由. 该插图显示了网络信息包采用的路由。从网络入站，信息包进入网络适配器。从那里，它到达 IP 堆栈，在堆栈中再发送到过滤器模块。从过滤器模块，或者将信息包发送到隧道定义，或者将其返回到 IP 堆栈，在堆栈中将其转发到上层协议。

隧道和安全性关联

不管在什么时候需要，隧道都必须将数据认证过或认证过并加密过。隧道通过指定两个主机之间的安全性关联来定义。安全性关联定义了一些为加密、认证算法和隧道特征的参数。以下插图显示了主机 A 和主机 B 之间的虚拟隧道。



SA = 安全性关联，由下列项组成：

目标地址
SPI
密钥
加密算法和格式
认证算法
密钥生命期

图 8. 在主机 A 和主机 B 之间建立安全隧道. 该插图显示了在主机 A 和主机 B 之间运行的虚拟隧道。安全性关联 A 的箭头方向是从主机 A 到主机 B。安全性关联 B 的箭头方向是从主机 B 到主机 A。A 安全性关联由目的地址、SPI、KEY、Crypto 算法和格式、认证算法以及密钥生命期组成。

安全性参数索引（SPI）和目的地址识别一个唯一的安全性关联。为了唯一指定隧道，这些参数是必需的。其它参数，例如密码算法、认证算法、密钥和生命期，可以指定或使用缺省值。

隧道注意事项

IKE 隧道与手工隧道不同，因为安全性策略的配置是一个与定义隧道端点分离的过程。在 IKE 中，有一个两步的协商过程。每一步的协商过程叫做一个*阶段*，每一阶段可以有不同的安全性策略。

当启动因特网密钥协商，它必须为协商设置一个安全信道。这称为*密钥管理*阶段或*阶段 1*。在该阶段期间，每一方使用预共享密钥或数字证书来认证其它方并传递标识信息。该阶段安装了安全性关联，在该关联期间双方确定它们如何规划安全的通信以及在第二阶段期间，用哪个保护来进行通信。该阶段的结果是 *IKE* 或*阶段 1* 隧道。

第二阶段称为*数据管理*阶段或*阶段 2*，它使用 IKE 隧道来创建 AH 和 ESP 实际保护流量的安全性关联。第二阶段还要确定“IP 安全性”隧道将要使用的数据。例如，它可以指定以下内容:

- 子网掩码
- 地址范围
- 协议和端口号组合

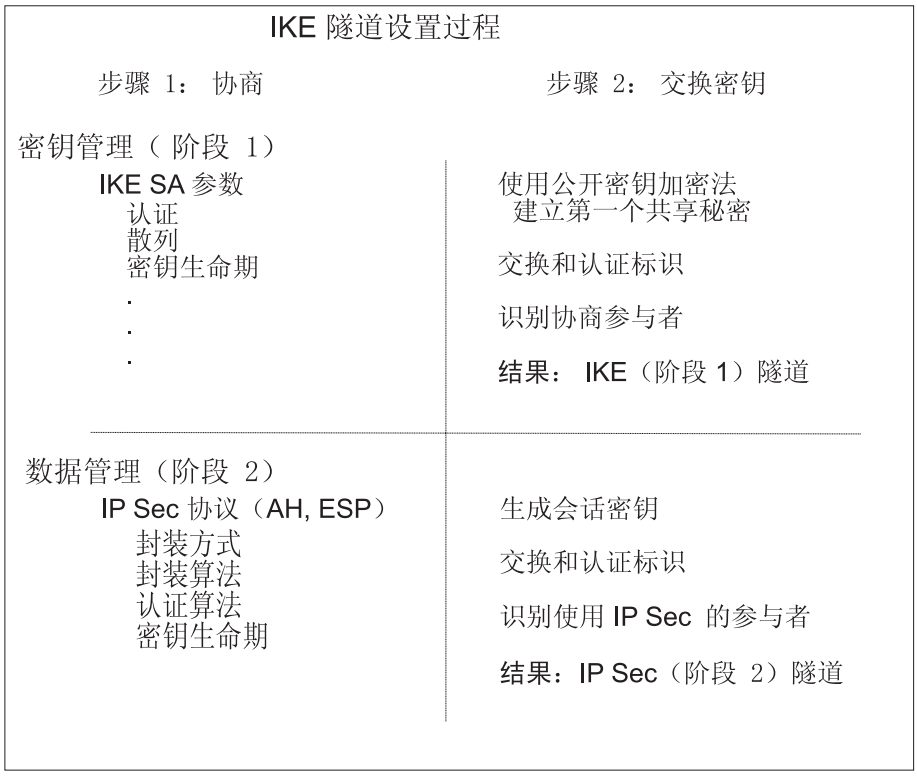


图 9. IKE 隧道设置过程. 该插图显示了设置 IKE 隧道的两步骤、两阶段过程。

在很多情况下，密钥管理（IKE）隧道的端点将与数据管理（ “IP 安全性” ）隧道的端点相同。IKE 隧道端点是执行协商的机器的标识。 “IP 安全性”隧道端点描述了将要使用 “IP 安全性”隧道的流量的类型。对于简单的主机到主机的隧道，其中两隧道之间的全部流量用相同的隧道保护，阶段 1 和阶段 2 的隧道端点是相同的。当协商双方是两个网关，IKE 隧道端点是两个网关， “IP 安全性”隧道端点是机器或子网（在网关之后）或隧道用户的地址范围（在网关之后）。

密钥管理参数和策略

阶段 1（密钥管理阶段）用以下参数来设置 IKE 隧道配置。

密钥管理（阶段 1）隧道	IKE 隧道的名称。对于每个隧道，必须指定协商的端点。有两个计划来发送和验证 IKE 信息的机器。隧道的名称可能描述了隧道端点，例如 `VPN Boston` 或 `VPN Acme`。
主机识别类型	将用于 IKE 交换的标识类型。为了确保执行正确的密钥查询，标识类型和值必须与预共享密钥的值相匹配。如果用单一标识搜索预共享密钥的值，则*主机标识*是密钥的标识，其*类型*是 KEY_ID。如果单一主机有多于一个预共享密钥值，则 KEY_ID 类型就很有用了。
主机标识	主机标识的值表示为一个 IP 地址、一个全限定域名（FQDN）或一个在全限定域名中的用户（*user@FQDN*）。例如，jdoe@studentmail.ut.edu。
IP 地址	远程主机的 IP 地址。当主机标识类型是 KEY_ID 或无论什么时候主机标识类型不能由IP 地址解析时，这个值是必需的。例如，如果用户名不能通过本地名称服务器解析，则必须输入远程方的 IP 地址。

不能通过指定那些在 IKE 协商期间使用过的参数定制密钥管理策略。例如，有为预共享密钥或签名方式认证的密钥管理策略。对于阶段 1，用户必须确定某个密钥管理安全性属性，用该属性来执行交换。

数据管理参数和策略

数据管理建议参数在 IKE 隧道配置的阶段 2 期间设置。在手工隧道中使用时，它们是相同的“IP 安全性”参数，并描述了用于在隧道中保护数据流量的保护类型。可以在同一个阶段 1 隧道下启动多于一个阶段 2 隧道。

以下的端点标识类型描述了那些使用“IP 安全性”数据隧道的数据类型:

主机、子网或范围	描述在隧道中流通的数据流量可以是属于一个特定的主机、子网或地址范围。
主机／子网标识	包含通过该隧道传递流量的本地和远程系统主机或子网的识别。确定在阶段 2 协商发送的标识和如果协商成功将构建的过滤规则。
子网掩码	描述子网内的全部 IP 地址（例如，主机 9.53.250.96 和掩码 255.255.255.0）
起始 IP 地址范围	为地址范围提供起始 IP 地址，它们将使用隧道（例如，9.53.250.96 到 9.53.250.93 的 9.53.250.96）
结束 IP 地址范围	为地址范围提供结束 IP 地址，它们将使用隧道（例如，9.53.250.96 到 9.53.250.93 的 9.53.250.93）
端口	用于特定端口号（例如，21 或 23）的描述数据
协议	描述正用特定协议传送的数据（例如，TCP 或 UDP）。确定在阶段 2 协商发送的协议和如果协商成功将构建的过滤规则。本地端点的协议必须与远程端点的协议匹配。

选择隧道类型

判定使用手工隧道或 IKE 隧道取决于远程终端支持的隧道和期望的密钥管理类型。建议用 IKE 隧道（当可用时），因为它们提供了工业标准的安全密钥协商和密钥更新。它们也利用 IETF ESP 和 AH 头类型并支持反重放保护。有选择地配置签名方式以允许数字证书。

如果远程端使用需要手工隧道的其中一个算法，则应该使用手工隧道。手工隧道确保了大量主机的互操作性。因为密钥是静态的且很难改变，更新起来可能很麻烦，它们也不安全。手工隧道可以用于运行该操作系统的主机和任何其它运行 IP 安全并且有公共加密和认证算法设置的机器。大多数供应商提供带 DES 的键控 MD5，或带 DES 的 HMAC MD5。该子集几乎可以与全部“IP 安全性”实现一起工作。

安装手工隧道使用的过程取决于是否安装隧道的第一个主机或安装第二个主机，第二个主机设置的参数要与第一个匹配。当安装第一主机时，密钥可以自动产生，算法可以是默认的。当安装第二主机，如果可能，从远程端导入隧道信息。

另一个重要的注意事项是确定远程系统是否在防火墙之后。如果是，则设置必须包含插入防火墙的信息。

使用 IKE 和 DHCP 或动态的指定地址

一个通过操作系统来使用“IP 安全性”的普通方案是当远程系统在用服务器启动 IKE 会话时，它们的标识不能依赖于特定的 IP 地址。在本地局域网（LAN）环境下可以发生这种情况，比如使用“IP 安全性”连接到 LAN 上的一个服务器并等待加密数据。其它公共使用涉及远程客户机向服务器拨号，并且使用全限定域名（FQDN）或电子邮件地址（*user@FQDN*）来标识远程标识。

为了制定基于明确的关于远程标识的策略决策，必须使用主动方式。在这种情况下，在协商的第一消息中发送标识，并且可以用于在安全策略数据库中进行策略查询。这将确保仅指定命名的远程标识可以使用 IKE 协议协商。

对于“数据管理”阶段（阶段 2），当创建“IP 安全性”关联来加密 TCP 或 UDP 流量，一般可以配置数据管理器隧道。因此，如果 IP 地址没有在数据库中明确地配置，阶段 1 期间的任何认证了的请求将使用类属隧道来定义“数据管理”阶段。这允许任何地址匹配类属隧道，只要严格公共的基于密钥的安全性验证在阶段 1 是成功的，那么就可以使用。

使用 XML 来定义一个类属数据管理隧道

定义类属“数据管理”隧道，使用 **ikedb** 可以理解的 XML 格式。有关 IKE XML 接口和 **ikedb** 命令的更多信息，请参阅标题为第 146 页的『IKE 报文封装配置的命令行界面』的一节。“类属数据管理”隧道与 DHCP 一起使用。XML 格式使用标记名称基于 Web 的系统管理器调用“数据管理”隧道。这也是参考了其它上下文中*阶段 2 隧道*。*类属数据管理隧道*不是真正的隧道，而是一个 **IPSecProtection**，它在接收的“数据管理”消息（在特定“密钥管理”隧道下）与任何为“密钥管理”隧道定义的“数据管理”隧道不匹配时使用。它仅在响应程序是 AIX 系统的情况下使用。指定一个类属数据管理隧道 **IPSecProtection** 是可选的。

类属数据管理隧道定义在 **IKEProtection** 元素中。有两个 XML 属性，称为 **IKE_IPSecDefaultProtectionRef** 和 **IKE_IPSecDefaultAllowedTypes**，它们是为此所用的。

首先，如果没有匹配的 **IPSecTunnels**（“数据管理”隧道），则需要定义一个您想用作缺省值的 **IPSecProtection**。用作缺省值的 **IPSecProtection** 必须有以 `_defIPSprot_` 开始的 **IPSec_ProtectionName**。

现在请转至您要使用 **IPSecProtection** 这个缺省值的 **IKEProtection**。指定 **IKE_IPSecDefaultProtectionRef** 属性，它包含缺省值 **IPSec_Protection** 的名称。

还必须在该 **IKEProtection** 中为 **IKE_IPSecDefaultAllowedTypes** 属性指定一个值。它可以有一个或多个以下的值（如果有多个值，它们应该空格分开）：

```
Local_IPV4_Address
Local_IPV6_Address
Local_IPV4_Subnet
Local_IPV6_Subnet
Local_IPV4_Address_Range
Local_IPV6_Address_Range
Remote_IPV4_Address
Remote_IPV6_Address
Remote_IPV4_Subnet
Remote_IPV6_Subnet
Remote_IPV4_Address_Range
Remote_IPV6_Address_Range
```

这些值与启动程序指定的标识类型相符。在 IKE 协商中，忽略了实际的标识。如果 **IKE_IPSecDefaultAllowedTypes** 属性包含一个以 Local_ 开始的字符串，该字符串与启动程序的本地标识类型相符，同时包含一个以 Remote_ 开始的字符串，该字符串与启动程序的远程标识类型相符，那么将使用指定的 **IPSecProtection**。换句话说，在任何 **IKE_IPSecDefaultAllowedTypes** 属性中至少有一个 **Local_** 值和至少一个 **Remote_** 值，这是为了与要使用的 **IPSec_Protection** 相符。

示例: 在阶段 2（数据管理）的消息中启动程序向 AIX 系统发送以下信息:

```
本地标识类型:      IPV4_Address
本地标识:          192.168.100.104

远程标识类型:      IPV4_Subnet
远程标识:          10.10.10.2
远程网掩码:        255.255.255.192
```

AIX 系统没有与这些标识匹配的“数据管理”隧道。但是它的确有一个有以下定义的属性 **IPSecProtection**:

```
IKE_IPSecDefaultProtectionRef="_defIPSprot_protection4"
IKE_IPSecDefaultAllowedTypes="Local_IPV4_Address
                              Local_IPV4_Address_Range
Local_IPV6_Address_Range
                              Remote_IPV6_Address
                              Remote_IPV4_Address_Range"
```

进入消息的本地标识类型（**IPV4_Address**）与所允许类型 **Local_** 值中的一个匹配，**Local_IPV4_Address**。同时，消息的远程标识（**IPV4_Subnet**）与值 **Remote_IPV4_Subnet** 匹配。因此“数据管理”隧道协商将继续进行 _defIPSprot_protection4 作为 **IPSecProtection**。

/usr/samples/ipsec/default_p2_policy.xml 文件是一个完全的 XML 文件，它定义了一个类属 **IPSecProtection**，它可作为示例使用。

使用基于 Web 的系统管理器定义类属数据管理隧道

要使用基于 Web 的系统管理器接口定义类属“数据管理”隧道，请执行以下操作:

1. 在“IKE 隧道”容器中选择一个“密钥管理”隧道，然后选择“定义数据管理隧道”操作。
2. 选择类属“数据管理”隧道。配置面板类似于用于定义“数据管理”隧道的面板。然而，标识类型的选项是不同的。不需要指定显式标识。标识类型（IP v4 或 v6 Address Only、IP v4 或 v6 Subnet Only 和 IP v4 或 v6 Address 或 Subnet）涵盖所允许的所有标识情况。
3. 用与“数据管理隧道”设置中一样的方式来设置剩余信息，并单击“确定”。每个“密钥管理”隧道仅能有一个关联的“类属隧道”。

注: “类属数据管理”隧道只能用于 AIX 系统是响应程序的情况。

配置因特网密钥交换报文封装

本节提供关于如何使用基于 Web 的系统管理器界面、系统管理界面程序（SMIT）或命令行来配置网际密钥交换（IKE）报文封装的信息。

使用基于 Web 的系统管理器配置 IKE 报文封装

『使用基本配置向导』提供了一种简单的方式来定义带有预共享密钥的 IKE 报文封装。有关更多高级选项，请参阅『高级 IKE 报文封装配置』。

使用基本配置向导

您可以通过基于 Web 的系统管理器定义 IKE，使用预共享密钥或者证书作为认证方法。基于 Web 的系统管理器添加新的密钥管理和数据管理 IKE 报文封装到 IP 安全子系统，允许您输入极小数据并选择一些选项，对于报文封装生命期这样的参数，使用公共缺省值。

当使用基本配置向导时，以下的要记住:

- 向导只可用于初始报文封装配置。要修改、删除或激活报文封装，请使用 **IKE 报文封装**插件或任务栏。
- 系统中报文封装的名称是唯一的，但您可以在远程系统中使用相同的名称。例如，在本地和远程系统中，报文封装的名称可以是 *hostA_to_hostB*，但本地 IP 地址和远程 IP 地址字段（端点）是交换的。
- 阶段 1 和阶段 2 的报文封装用相同的加密和认证算法来定义。
- 预共享密钥必须以十六进制（不带 `0x` 前导）或 ASCII 文本输入。
- 如果选择数字证书作为认证方法，则您必须使用密钥管理器来创建数字证书。
- 主机标识类型只能是 `IP` 地址.
- 您创建的转换和提议是以用户定义的报文封装名称结尾的指定名称。您可以通过 **VPN** 和 **IKE 报文封装**插件在基于 Web 的系统管理器中查看转换与提议。

通过向导使用以下过程来配置新的报文封装:

1. 在命令行中使用 **wsm** 命令打开基于 Web 的系统管理器。
2. 选择网络插件
3. 选择**虚拟专用网（IP 安全性）**。
4. 从控制台区域，选择**概述与任务**文件夹。
5. 选择**配置基本报文封装配置向导**。
6. 在步骤 1 介绍面板中单击**下一步**，然后按照步骤配置 IKE 报文封装。

   如果需要的话可以使用联机帮助。

   在使用向导定义了报文封装之后，报文封装的定义就显示在基于 Web 的系统管理器 IKE 报文封装列表中，并且可以激活或修改。

高级 IKE 报文封装配置

您可以分别配置密钥管理和数据管理报文封装，采用以下的过程。

配置密钥管理报文封装: 采用基于 Web 的系统管理器配置 IKE 报文封装。使用以下过程来添加密钥管理报文封装:

1. 使用 **wsm** 命令打开基于 Web 的系统管理器。
2. 选择网络插件。
3. 选择**虚拟专用网（IP 安全性）**。

4. 从控制台区域，选择**概述与任务**。
5. 选择**启动 IP 安全性**。该操作装入“IP 安全性”内核扩展并启动 **isakmpd**、**tmd** 和 **cpsd** 守护程序。

   通过定义密钥管理和数据管理端点及其有关的安全性转换和提议来创建报文封装。
   - 密钥管理是认证阶段。它在计算最终的“IP 安全性”参数和密钥之前，设置了协商部分之间的安全信道。
   - 数据管理描述了使用特殊报文封装的流量类型。对于单独的主机或主机组（使用子网或 IP 范围）连同指定的协议和端口号一起配置。

   可以使用相同的密钥管理报文封装来保护多个数据管理协商和密钥刷新，只要它们位于相同的两个端点之间；例如，在两个网关之间。
6. 要定义密钥管理报文封装端点，单击“识别”选项卡中的**网际密钥交换（IKE）报文封装**。
7. 输入信息以描述参与协商的系统的身份。大部分情况下使用 IP 地址，并且必须创建与远程方兼容的策略。

   在“转换”选项卡中，双方都使用匹配转换，或者联系远程端管理员来定义匹配转换。可以创建包含几个选项的转换以提供当提议或匹配转换时的灵活性。
8. 如果对于认证使用预共享密钥，在**密钥**选项卡下输入预共享密钥。在远程和本地机器上该值必须匹配。
9. 使用“转换”选项卡上的**添加**按钮来创建与该报文封装关联的转换。

   要启用数字证书和签名方式支持，选择 **RSA 签名** 或**带有 RCL 校验的 RSA 签名认证方法**。

   关于数字证书的更多信息，请参阅第 150 页的『处理数字证书和密钥管理器』。

配置数据管理报文封装: 要设置数据管理报文封装端点及提议并完成 IKE 报文封装设置，打开基于 Web 的系统管理器，如第 144 页的『配置密钥管理报文封装』中所述。数据管理报文封装按照以下步骤创建:

1. 选择密钥管理报文封装并定义任意唯一的选项。大多数数据管理选项可以按照缺省定义保留。
2. 在“端点”选项卡下指定端点类型（例如IP 地址、子网或 IP 地址范围）。您可以选择端口号和协议或者接受缺省值。
3. 在提议面板中，您可以创建一个新的提议，通过单击**添加**按钮或者单击**确定**来创建提议。如果有多个提议，您可以使用“上移”或“下移”按钮来更改搜索顺序。

分组支持: 从 AIX 5.1 开始，IP 安全性在报文封装定义中支持 IKE 标识分组，以使多个标识与单一的安全性策略相关联，而不需要创建单独的报文封装定义。当设置连接到几个远程主机时，分组尤其有用，因为您可以避免设置或管理多个报文封装定义。同样，如果必须要更改安全性策略，您不必更改多个报文封装定义。

在使用报文封装定义中的组名之前，必须先定义一个组。组的大小限制为 1 KB。在协商的启动程序一方，可以将组仅用作数据管理报文封装定义中的远程标识。在协商的响应程序一方，可以将组作为键管理和数据管理报文封装定义中的远程标识。

组是由组名和 IKE 标识及标识类型列表组成的。标识可以是相同的类型或者以下的组合:

- IPv4 地址
- IPv6 地址
- FQDN
- user@FQDN
- X500 DN 类型

在“安全性关联协商”期间，线性搜索组中的标识以获得第一个匹配。

基于 Web 的系统管理器可以用来定义用于“密钥管理”报文封装的远程端点的组。要用基于 Web 的系统管理器来定义一个组，请使用以下过程:

1. 在 **IKE 报文封装**容器中选择”键管理“报文封装。
2. 打开**属性**对话。
3. 选择**标识**选项卡。
4. 对于远程主机身份类型选择**组标识定义**。
5. 选择**配置组定义**按钮，在窗口中输入组成员。

关于从命令行定义组的信息，请参考『IKE 报文封装配置的命令行界面』节。

使用 IKE 报文封装配置的 SMIT 界面

您可以使用 SMIT 界面来配置 IKE 报文封装并执行基本的 IKE 数据库功能。SMIT 使用基础的 XML 命令函数来执行对 IKE 报文封装定义的添加、删除和修改。IKE SMIT 用在快速配置 IKE 报文封装并提供用于创建 IKE 报文封装定义的 XML 语法。IKE SMIT 菜单也允许您备份、修复和初始化 IKE 数据库。

要配置 IPv4 IKE 报文封装，请使用 **smitty ike4** 快速路径。要配置 IPv6 IKE 报文封装，请使用 **smitty ike6** 快速路径。IKE 数据库函数可以在“高级 IP 安全性配置”菜单中找到。

通过 SMIT 添加的所有的 IKE 数据库项都可以通过基于 Web 的系统管理器工具查看或修改。

IKE 报文封装配置的命令行界面

ikedb 命令（在 AIX 5.1 及以后版本中可用）允许用户使用 XML 界面检索、更新、删除、导入和导出 IKE 数据库中的信息。**ikedb** 命令允许用户写入（放入）或者读取（获取）IKE 数据库。输入输出格式是“可扩展标记语言”（XML）文件。XML 文件的格式是由它的“文档类型定义”（DTD）指定的。**ikedb** 命令允许用户参阅 DTD，它用于在写入时验证 XML 文件。尽管可以使用 **-e** 标志将实体声明添加到 DTD 中，这是对 DTD 唯一能做的修改。将忽略任何输入 XML 文件中的外部 DOCTYPE 声明，任何内部 DOCTYPE 声明都可能导致出错。使用 DTD 分析 XML 文件所遵循的规则在 XML 标准中指定。**/usr/samples/ipsec** 文件有个典型的 XML 文件样本，它定义了公共报文封装方案。关于语法的详细信息，请参阅《*AIX 5L V5.2 命令参考大全*》中的 **ikedb** 命令描述。

您可以使用 **ike** 命令来启动、停止和监视 IKE 报文封装。**ike** 命令也可用于激活、除去或者列出 IKE 和 IP 安全性报文封装。关于语法的详细信息，请参阅《*AIX 5L V5.2 命令参考大全*》中的 **ike** 命令描述。

以下示例显示了如何使用 **ike**、**ikedb** 和其它几个命令来配置和检查 IKE 报文封装的状态。

1. 要启动报文封装协商（*激活*报文封装）或者允许进入的系统充当响应程序（取决于指定的角色），使用带有报文封装号的 **ike** 命令，如下所示:

   ```
   # ike cmd=activate numlist=1
   ```

   您也可以使用远程标识或者 IP 地址，如以下的例子所示:

   ```
   # ike cmd=activate remid=9.3.97.256
   # ike cmd=activate ipaddr=9.3.97.100, 9.3.97.256
   ```

   由于可能需要几秒钟来完成命令，命令在启动协商后返回。
2. 要显示报文封装状态，请使用 **ike** 命令，如下所示:

   ```
   # ike cmd=list
   ```

   输出类似于以下的显示:

```
Phase 1 Tunnel ID       [1]
Phase 2 Tunnel ID       [1]
```

输出显示了当前激活的阶段 1 和阶段 2 报文封装。

3. 要获得报文封装的详细列表，请使用 **ike** 命令，如下所示:

```
# ike cmd=list verbose
```

输出类似于以下的显示:

```
Phase 1 Tunnel ID       1
Local ID Type:          Fully_Qualified_Domain_Name
Local ID:               bee.austin.ibm.com
Remote ID Type:         Fully_Qualified_Domain_Name
Remote ID:              ipsec.austin.ibm.com
Mode:                   Aggressive
Security Policy:        BOTH_AGGR_3DES_MD5
Role:                   Initiator
Encryption Alg:         3DES-CBC
Auth Alg:               Preshared Key
Hash Alg:               MD5
Key Lifetime:           28800 Seconds
Key Lifesize:           0 Kbytes
Key Rem Lifetime:       28737 Seconds
Key Rem Lifesize:       0 Kbytes
Key Refresh Overlap:    5%
Tunnel Lifetime:        2592000 Seconds
Tunnel Lifesize:        0 Kbytes
Tun Rem Lifetime:       2591937 Seconds
Status:                 Active

Phase 2 Tunnel ID       1
Local ID Type:          IPv4_Address
Local ID:               10.10.10.1
Local Port:             any
Local Protocol:         all
Remote ID Type:         IPv4_Address
Remote ID:              10.10.10.4
Remote Subnet Mask:     N/A
Remote Port:            any
Remote Portocol:        all
Mode:                   Oakley_quick
Security Policy:        ESP_3DES_MD5_SHA_TUNNEL_NO_PFS
Role:                   Initiator
Encryption Alg:         ESP_3DES
AH Transform:           N/A
Auth Alg:               HMAC-MD5
PFS:                    No
SA Lifetime:            600 Seconds
SA Lifesize:            0 Kbytes
SA Rem Lifetime:        562 Seconds
SA Rem Lifesize:        0 Kbytes
Key Refresh Overlap:    15%
Tunnel Lifetime:        2592000 Seconds
Tunnel Lifesize:        0 Kbytes
Tun Rem Lifetime:       2591962 Seconds
Assoc P1 Tunnel:        0
Encap Mode:             ESP_tunnel
Status:                 Active
```

4. 要显示动态过滤器表中的过滤器规则以获取最近激活的 IKE 报文封装，使用 **lsfilt** 命令，如下所示:

```
# lsfilt -d
```

输出类似于以下的显示:

```
1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no udp eq 4001 eq 4001 both both no all
  packets 0 all
2 *** Dynamic filter placement rule *** no
0 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 yes all any 0 any 0 both both no all
  packets 0 all

*** Dynamic table ***

0 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no udp eq 500 eq 500 local both no all
  packets 0
0 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no ah any 0 any 0 both inbound no all
  packets 0
0 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no esp any 0 any 0 both inbound no all
  packets 0
1 permit 10.10.10.1 255.255.255.255 10.10.10.4 255.255.255.255 no all any 0 any
  0 both outbound yes all packets 1
1 permit 10.10.10.4 255.255.255.255 10.10.10.1 255.255.255.255 no all any 0 any
  0 both inbound yes all packets 1
```

该示例显示了有一个 IKE 报文封装而无其它报文封装的机器。用户可以移动动态过滤布局规则（在静态表的示例输出中的规则 #2）来控制与所有其他用户定义的规则有关的布局。当协商报文封装时动态表中的规则自动构造，并且把相应的规则插入到过滤器表中。这些规则可以显示，但不能编辑。

5. 要打开动态过滤器规则记录，将规则 #2 的记录选项设置为是，使用 **chfilt** 命令，如以下示例所示:

   ```
   # chfilt -v 4 -n 2 -l y
   ```

   需要 IKE 流量记录的更多详细信息，请参阅第 168 页的『记录设备』。

6. 要取消激活报文封装，使用 **ike** 命令，如下所示:

   ```
   # ike cmd=remove numlist=1
   ```

7. 要查看报文封装定义，使用 **ikedb** 命令，如下所示:

   ```
   # ikedb -g
   ```

8. 要从同级设备上生成的 XML 文件中写入定义到 IKE 数据库并覆盖数据库中现有的任意同名对象，使用 **ikedb** 命令，如下所示:

   ```
   # ikedb -pFs peer_tunnel_conf.xml
   ```

   peer_tunnel_conf.xml 是在同级设备上生成的 XML 文件。

9. 要获取命名为 *tunnel_sys1_and_sys2* 的阶段 1 的报文封装的定义和所有带有各自提议和保护的相关阶段 2 报文封装，请使用 **ikedb** 命令，如下所示:

   ```
   # ikedb -gr -t IKETunnel -n tunnel_sys1_and_sys2
   ```

10. 要从数据库中删除所有预共享密钥，使用 **ikedb** 命令，如下所示:

    ```
    # ikedb -d -t IKEPresharedKey
    ```

关于 IKE 报文封装组支持的一般信息，请参阅第 145 页的『分组支持』节。您可以从命令行使用 **ikedb** 命令来定义组。

AIX IKE 与 Linux 的相似性

要通过使用 Linux 配置文件（AIX 5.1 及后续版本）来配置 AIX IKE 报文封装，请使用带有 **-c** 标志（转换选项）的 **ikedb**命令，它可以让您将 **/etc/ipsec.conf** 和 **/etc/ipsec.secrets** Linux 配置文件用作 IKE 报文封装定义。**ikedb** 命令分析 Linux 配置文件、创建 XML 文件并选择性的把 XML 报文封装定义添加到 IKE 数据库中。然后您可以使用 **ikedb -g** 命令或基于 Web 的系统管理器来查看报文封装定义。

IKE 报文封装配置方案

以下方案描述了大多数客户试图设置报文封装时遇到的情况的类型。这些方案可以描述为分公司、业务伙伴和远程访问情况。

- 在分公司情况下，客户有两个想连接在一起的可信网络（一个位置的工程组到另一位置的工程组）。本示例中，有互相连接的网关，并且所有网关之间的流量使用相同的报文封装。报文封装任意端的流量解包并传送到公司内部网的空白区。

  在 IKE 协商的第一个阶段，在两个网关之间创建 IKE 安全性关联。通过 “IP 安全性” 报文封装的流量是两个子网之间的流量，该子网标识用于阶段 2 协商。在输入报文封装的安全性策略和报文封装参数之后，创建报文封装号。使用 **ike** 命令启动报文封装。
- 在业务伙伴方案中，网络是不可信的，网络管理员可能想要限制安全性网关之后少量主机的访问。在这种情况下，主机之间的报文封装运载流量，该流量受 “IP 安全性” 保护并用于两台特定主机之间。阶段 2 报文封装的协议是 AH 或 ESP。这种主机到主机的报文封装在网关到网关报文封装内是安全的。
- 在远程访问情况下，报文封装按照要求设置并且应用高级安全性。IP 地址可能没有意义，因此，全限定域名或 *user@* 全限定域名作为首选。您可以选择性的使用 KEYID 将密钥与主机标识相关联。

处理数字证书和密钥管理器

数字证书将身份绑定到公用密钥上，通过它您可以验证加密传送的发送方或接收方。从 AIX 4.3.3 开始，IP 安全性使用数字证书以启用公*用密钥密码术*，也称为*非对称密码术*，它采用只有用户知道的专用密钥来加密数据，并采用来自于给定的公用 – 专用密钥对的相关公用（共享）密钥来解密数据。*密钥对*是长串数据，这些数据充当用户加密方案的密钥。

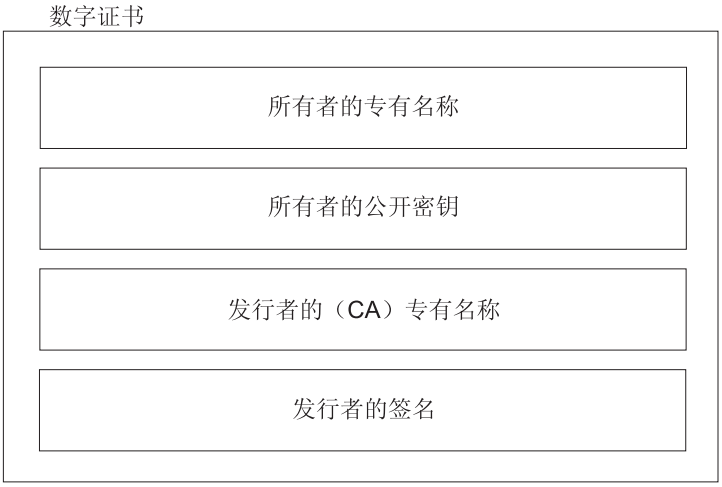
在公用密钥密码术中，公用密钥交给用户想要与之通信的任何人。发送方以数字化方式为其指定的密钥对签署所有带有相应的专用密钥的安全通信。接收方使用公用密钥来验证发送方的签名。如果用公用密钥成功的对消息进行解密，则接收方可以验证发送方是经过认证的。

公用密钥密码术依赖于可信的称为*认证中心*（*CA*）的第三方，从而发出可靠的数字证书。接收方指定哪些发布组织或权限是认为可信的。针对特定的时间量发出证书；当超过到期日时，必须替换它。

AIX 4.3.3 及后继版本提供“密钥管理器”工具，它管理数字证书。以下部分提供关于证书本身的概念性信息。这些证书的管理任务在『处理数字证书和密钥管理器』中描述。

数字证书的格式

数字证书包含了关于证书所有者的身份和认证中心的特定信息片断。请参阅下图以获得数字证书的说明。



数字证书的内容

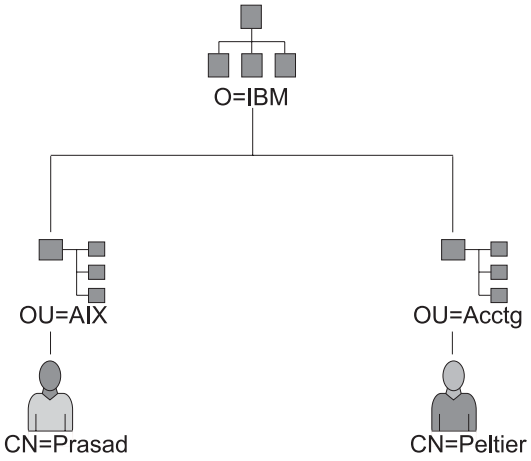
图 10. 数字证书的内容. 该插图显示了数字证书的四个实体。从上向下依次是: 所有者专有名称、所有者公用密钥、发行商（CA）专有名称和发行商签名。

以下的列表进一步描述了数字证书的内容:

所有者专有名称

目录树中的所有者公共名和上下文（位置）的组合。例如，在以下的简单目录树图中，Prasad 是所有者的普通名，上下文是: 国家 = US，组织 = ABC，下级组织 = SERV；因此，专有名称为:

```
/C=US/O=ABC/OU=SERV/CN=prasad.austin.ibm.com
```



从目录树派生专有名称的示例

图 11. 从目录树派生专有名称的示例. 该插图是一个目录树，0 = ABC 在顶级，第二级分支出两个实体。二级包含单独的分支上的 OU=AIX 和 OU=Acctg；每个都有导向上一级单独实体的分支。上一级分别包含 CN=Prasad 和 CN=Peltier。

所有者公用密钥
接收方用来解密数据

主题备用名称
可以是标识符，例如 IP 地址、电子邮件地址、全限定域名等等。

发出日期
发出数字证书的日期。

到期日 数字证书的到期日。

发行商专有名称
认证中心的专有名称。

发行商数字签名
用于验证证书的数字签名。

数字证书的安全性注意事项

单独的数字证书不能证明身份。数字证书只允许通过提供检查所有者的数字签名所需的公用密钥来验证数字证书所有者的身份。您可以安全地发送公用密钥给另一方，因为没有密钥对的另一部分（您的专用密钥），数据是无法解密的。因此，所有者必须保护好专用密钥，它属于数字证书中的公用密钥。如果知道了专用密钥，则数字证书所有者的全部通信都可以译码。没有专用密钥，不能滥用数字证书。

认证中心和信任层次结构

数字证书仅像发布它的认证中心（CA）一样值得信任。作为这种信任的一部分，应该理解发布出证书的策略。每个组织或用户必须确定可作为值得信任的可以接受的认证中心。

“密钥管理器”工具也允许组织创建自签署证书，这可能对测试或在少数用户或机器的环境中有用。

作为安全性服务的用户，您需要知道它的公用密钥来获取和验证任何数字证书。而且，简单地接收数字证书不确保它的可靠性。要验证其可靠性，您需要发布数字证书的认证中心的公用密钥。如果您没有保留 CA 公用密钥的确保的副本，则可能需要其它的数字证书来获得 CA 的公用密钥。

证书撤销列表（CRL）

数字证书预期用于它的整个有效期中。然而，如果需要的话，证书可能在它的实际到期日之前就到期了。使证书无效可能是必要的，例如，如果雇员离开公司或者证书的专用密钥已经泄漏。要使证书无效，您必须通知相应的环境认证中心（CA）。当 CA 取消证书时，它将无效的证书序列号添加到“证书撤销列表”（CRL）中。

CRL 是签署的数据结构，它是周期性发布的并在公共资源库中可用。CRL 可以从 HTTP 或 LDAP 服务器上检索。每个 CRL 包含当前时间戳记和 **nextUpdate** 时间戳记。列表中每个取消的证书由其证书序列号识别。

配置 IKE 报文封装和使用数字证书作为您的认证方法时，可以通过选择带有 CRL 校验的 RSA 签名来确认证书是否还未取消。如果启用 CRL 校验，在协商过程期间找到并检查列表来建立密钥管理报文封装。

> **注**: 要使用“IP 安全性”的这个功能，必须配置您的系统以使用 SOCKS 服务器（HTTP 服务器版本 4）或 LDAP 服务器或同时使用二者。如果您知道正在使用哪个 SOCKS 或 LDAP 服务器来获取 CRL，您可以通过使用基于 Web 的系统管理器来进行必要的配置选择。从“数字证书”菜单中选择 **CRL 配置**。

因特网应用程序中数字证书的使用

使用公用密钥密码术系统的因特网应用程序必须使用数字证书来获取公用密钥。有许多使用公用密钥密码术的应用程序，包含以下这些:

虚拟专用网（VPN）

虚拟专用网，也称为*安全报文封装*，可以在系统（例如防火墙）之间设置来启用通过不安全通信链路的安全网络之间的受保护连接。所有通往这些网络的流量都在参与的系统之间加密。

用于报文封装的协议遵循 IP 安全性和 IKE 标准，它允许对于远程客户机（例如，在家里工作的雇员）和安全主机或网络之间的安全加密连接。

安全套接字层（SSL）

SSL 是一个协议，它为通信提供保密性和完整性。Web 服务器将它用于 Web 服务器和 Web 浏览器之间的安全连接，轻量级目录访问协议（LDAP）将它用于 LDAP 客户机和 LDAP 服务器之间的安全连接，Host-on-Demand V.2 将它用于客户机和主机系统之间的连接。SSL 将数字证书用于密钥交换、服务器认证，以及可供选择的用于客户机认证。

安全电子邮件

许多使用 PEM 或 S/MIME 作为安全电子邮件标准的电子邮件系统将数字证书用于数字签名和加密解密邮件信息的密钥交换。

数字证书和证书申请

签署的数字证书包含所有者专有名称、所有者公用密钥、CA 专有名称和 CA 签名等字段。自签署数字证书包含所有者专有名称、公用密钥和签名。

必须创建*证书申请*并发送给 CA 以申请数字证书。证书申请包含申请者专有名称、公用密钥和签名等字段。CA 用数字证书中的公用密钥验证申请者的签名以确保:

- 证书申请在申请者和 CA 之间传送过程中未经修改。
- 对于证书申请中的公用密钥，申请者拥有相应的专用密钥。

CA 也负责验证申请者身份的某个级别。这种验证的要求范围从用户身份的极小证据到完全确信。

密钥管理器工具

密钥管理器工具管理数字证书，它位于扩展包的 **gskkm.rte** 文件集中。

本节描述了如何使用密钥管理器执行以下操作:

1. 创建密钥数据库
2. 添加 CA 根数字证书
3. 建立信任设置
4. 删除 CA 根数字证书
5. 申请数字证书
6. 添加（接收）新的数字证书
7. 删除数字证书
8. 更改数据库密码
9. 使用数字证书创建 IKE 报文封装

要设置数字证书和签名支持，您最少必须执行任务 1、2、3、4、6 和 7。然后，使用基于 Web 的系统管理器来创建 IKE 报文封装并将策略和使用 RSA 签名作为认证方法的报文封装相关联。

您可以从基于 Web 的系统管理器的 VPN 概述窗口中创建和配置密钥数据库，通过选择**管理数字证书**选项，或者使用 **certmgr** 命令从命令行中打开密钥管理器工具。

创建密钥数据库

密钥数据库采用有效的数字证书来启用要连接的 VPN 端点。密钥数据库（*.kdb）跟 IP 安全性 VPN 一起使用。

密钥管理器提供以下 CA 数字证书类型:

- RSA 安全服务器认证中心
- Thawte 个人收费认证中心
- Thawte 个人免费邮件认证中心
- Thawte 个人基本认证中心
- Thawte 个人服务器认证中心
- Thawte 服务器认证中心
- Verisign 类 1 公共基本认证中心
- Verisign 类 2 公共基本认证中心
- Verisign 类 3 公共基本认证中心
- Verisign 类 4 公共基本认证中心

这些签名数字证书启用客户机连接到具有来自这些签发者的有效数字证书的服务器。在创建了密钥数据库之后，您可以把它用作已创建的密钥数据库来连接到具有来自签发者之一的有效的数字证书的服务器。

要使用该表中未列出的签名数字证书，您必须从 CA 中申请并把它添加到您的密钥数据库。请参阅第 154 页的『添加 CA 根数字证书』。

要使用 **certmgr** 命令创建密钥数据库，请使用以下过程:

1. 启动密钥管理器工具，输入:

   ```
   # certmgr
   ```

2. 从密钥数据库文件下拉菜单中选择**新建**。
3. 对于**密钥数据库类型**字段，接受缺省值，**CMS 密钥数据库文件**。
4. 在**文件名**字段中输入以下文件名:

   ```
   ikekey.kdb
   ```

5. 在**位置**字段中输入以下数据库的位置:

   ```
   /etc/security
   ```

   注: 密钥数据库必须命名为 **ikekey.kbd** 并且必须放在 **/etc/security** 目录中。否则，IP 安全性不能正确运转。

6. 单击**确定**。显示**密码提示**屏幕。
7. 在**密码**字段中输入密码，在**确认密码**字段中再次输入一遍。
8. 如果想要更改密码到期天数，在**设置到期时间?** 字段输入想要的天数。该字段的缺省值为 60 天。如果不想要密码到期，则清除**设置到期时间?** 字段。
9. 要在存储文件中保存密码的加密版本，选择**密码存储到文件?** 字段并输入**是**。

   注意: 您必须存储密码以启用带有 IP 安全性的数字证书的使用。

10. 单击**确定**。显示确认屏幕，验证您已创建密钥数据库。
11. 再次单击**确定**，返回 IBM 密钥管理屏幕。您可以执行其它任务或者退出工具。

添加 CA 根数字证书

从 CA 中申请并接收到根数字证书之后，可以把它添加到数据库中。大多数根数字证书具有 *.arm 格式，如下所示:

```
cert.arm
```

要添加一个 CA 根数字证书到数据库中，使用以下过程:

1. 除非您已经在使用密钥管理器，否则启动该工具，通过输入:

   ```
   # certmgr
   ```

2. 从主屏幕中，选择密钥数据库文件下拉菜单中的**打开**。
3. 突出显示您想要添加 CA 根数字证书到其中的密钥数据库文件，单击**打开**。
4. 输入密码，单击**确定**。密码接受时，返回 IBM 密钥管理屏幕。这时，标题栏将显示您选定的密钥数据库文件名称，表示文件现在打开并准备处理了。
5. 从个人／自签署证书下拉菜单中选择**自签署证书**。
6. 单击**添加**。
7. 从数据类型下拉菜单中选择数据类型，例如:

   ```
   Base64 编码的 ASCII 数据
   ```

8. 输入 CA 根数字证书的证书文件名和位置，或者单击**浏览**选择名称和位置。
9. 单击**确定**。
10. 输入 CA 根数字证书的标签，例如测试 CA 根证书，单击**确定**。返回到密钥管理屏幕。**自签署证书**字段现在显示刚刚添加的 CA 根数字证书的标签。您可以执行更多任务或者退出工具。

建立信任设置

安装的 CA 证书缺省情况下设置为**可信的**。要更改信任设置，请执行以下操作:

1. 除非您已经在使用密钥管理器，否则通过输入以下内容启动该工具:

```
# certmgr
```

2. 从主屏幕中，选择密钥数据库文件下拉菜单中的**打开**。
3. 突出显示您想要更改其中的缺省数字证书的密钥数据库文件，单击**打开**。
4. 输入密码，单击**确定**。密码接受以后，返回 IBM 密钥管理屏幕。标题栏显示您选定的密钥数据库文件名称，表示文件现在打开了。
5. 从个人／自签署证书下拉菜单中选择**自签署证书**。
6. 突出显示您想更改的证书，单击**查看／编辑**，或者双击条目。显示证书条目的密钥信息屏幕。
7. 要使该证书成为可信根证书，选择**设置证书为可信根**之后的框，单击**确定**。如果证书不可信，清除复选框，单击**确定**。
8. 在自签署证书屏幕中单击**确定**。返回 IBM 密钥管理屏幕。您可以执行其它任务或者退出工具。

删除 CA 根数字证书

如果不再想支持签名数字证书列表中的 CA 之一，必须删除该 CA 根数字证书。

注意: 在删除 CA 根数字证书之前，创建备份副本，以防止以后想要重新创建 CA 根。

要从数据库中删除 CA 根数字证书，使用下面的过程:

1. 除非您已经在使用密钥管理器，否则启动该工具，通过输入:

```
# certmgr
```

2. 从主屏幕中，选择**打开**，在密钥数据库文件下拉菜单中。
3. 突出显示您想要删除 CA 根数字证书的密钥数据库文件，单击**打开**。
4. 输入密码，单击**确定**。密码接受以后，返回到**密钥管理**屏幕。这时，标题栏将显示您选定的密钥数据库文件名称，表示文件现在打开并准备编辑了。
5. 选择**自签署证书**，从个人／自签署证书下拉菜单中。
6. 突出显示您想删除的证书，单击**删除**。显示确认屏幕。
7. 单击**是**。返回 IBM 密钥管理屏幕。**自签署证书**字段不再出现 CA 根数字证书的标签。您可以执行其它任务或者退出工具。

申请数字证书

要获取数字证书，使用密钥管理器生成申请，并把申请提交给 CA。生成的申请是以 PKCS#10 的格式。然后 CA 验证您的身份，给您发送数字证书。

要申请数字证书，采用以下过程:

1. 除非您已经在使用密钥管理器，否则启动该工具，通过输入:

```
# certmgr
```

2. 从主屏幕中，选择密钥数据库文件下拉菜单中的**打开**。
3. 突出显示您想要从中生成申请的 **/etc/security/ikekey.kdb** 密钥数据库文件，单击**打开**。
4. 输入密码，单击**确定**。密码接受以后，返回 IBM 密钥管理屏幕。标题栏将显示您选定的密钥数据库文件名称，表示文件现在打开并准备编辑了。
5. 从“个人／签署人证书”下拉菜单中（在 AIX V4 中）选择**个人证书申请**或者选择**创建 —> 新的证书申请**（从 AIX 5.1 开始）。
6. 单击**新建**。
7. 从以下的屏幕中，输入自签署数字证书的**密钥标签**，例如:

keytest

8. 输入**普通名称**（缺省值为主机名）和**组织**，然后选择**国家或地区**。对于剩下的字段，接受缺省值或者选择新值。
9. 定义**主题备用**名称。与**主题备用**相关联的可选字段为电子邮件地址、IP 地址和 DNS 名称。对于 IP 地址的报文封装类型，输入相同的 IP 地址，在 IKE 报文封装中将该地址配置到 IP 地址字段。对于 *user@FQDN* 的报文封装标识类型，完成电子邮件地址字段。对于 FQDN 报文封装标识类型，在 DNS 名称字段输入全限定域名（例如，*hostname.companyname*.com）。
10. 在屏幕底端，输入文件名称，例如:

    certreq.arm

11. 单击**确定**。显示确认屏幕，验证您是否已为新的数字证书创建申请。
12. 单击**确定**。返回 “IBM 密钥管理” 屏幕。**个人证书申请**字段现在显示创建的新的数字证书申请的密钥标签（PKCS#10）。
13. 发送文件给 CA 以申请新的数字证书。您可以执行其它任务或者退出工具。

添加（接收）新的数字证书

从 CA 接收新数字证书之后，必须把它添加到生成申请的密钥数据库中。

要添加（接收）新的数字证书，使用以下过程:

1. 除非您已正在使用 “密钥管理器”，否则启动该工具，请输入:

   # certmgr

2. 从主屏幕中，从 “密钥数据库文件” 下拉菜单中选择**打开**。
3. 突出显示生成证书申请的密钥数据库文件并单击**打开**。
4. 输入密码并单击**确定**。密码接受以后，返回 “IBM 密钥管理” 屏幕。标题栏将显示您选择的密钥数据库文件名称，表示文件现在已打开并准备编辑。
5. 从 “个人／签名人证书” 下拉菜单中选择**个人证书申请**。
6. 单击**接收**（以添加新近接收的数字证书到数据库中）。
7. 从**数据类型**下拉菜单中选择新数字证书的数据类型。缺省值为 **Base64 编码的 ASCII 数据**。
8. 为新数字证书输入证书文件名和位置，或者单击**浏览**来选择名称和位置。
9. 单击**确定**。
10. 输入新建数字证书的描述性标签，例如:

    VPN 分支证书

11. 单击**确定**。返回 “IBM 密钥管理” 屏幕。**个人证书**字段现在显示您刚刚添加的新数字证书的标签。您可以执行其它任务或者退出工具。

    如果装入证书出错，请检查证书文件是否起始于文本 ——-BEGIN CERTIFICATE——-，结束于文本 ——-END CERTIFICATE——-。

    例如:

    ```
    -----BEGIN CERTIFICATE-----
    ajdkfjaldfwwwwwwwwwwadafdw
    kajf;kdsajkflasasfkjafdaff
    akdjf;ldasjkf;safdfdasfdas
    kaj;fdljk98dafdas43adfadfa
    -----END CERTIFICATE-----
    ```

    如果文本不匹配，编辑证书文件从而使它适当地开始和结束。

删除数字证书

注: 在删除数字证书之前，为以后您万一想要重新创建它创建备份副本。

要从数据库中删除数字证书，请使用下面的过程:

1. 除非您已正在使用“密钥管理器”，否则启动该工具，请输入:

   ```
   # certmgr
   ```

2. 从主屏幕中，从“密钥数据库文件”下拉菜单中选择**打开**。
3. 突出显示您想要从中删除数字证书的密钥数据库文件，并单击**打开**。
4. 输入密码并单击**确定**。密码接受以后，返回“IBM 密钥管理”屏幕。标题栏将显示您选择的密钥数据库文件名称，表示文件现在已打开并准备编辑。
5. 从“个人／签名人证书”下拉菜单中选择**个人证书申请**。
6. 突出显示您想删除的数字证书并单击**删除**。显示“确认”屏幕。
7. 单击**是**。返回“IBM 密钥管理”屏幕。**个人证书**字段中不再显示您刚才删除的数字证书标签。您可以执行其它任务或者退出工具。

更改数据库密码

要更改密钥数据库，请使用以下过程:

1. 除非您已正在使用“密钥管理器”，否则启动该工具，请输入:

   ```
   # certmgr
   ```

2. 从主屏幕中，从“密钥数据库文件”下拉菜单中选择**更改密码**。
3. 在**密码**字段中输入新密码，并且在**确认密码**字段中再输入一遍。
4. 如果想要更改密码到期天数，在**设置到期时间?** 字段输入想要的天数。该字段的缺省值为 60 天。如果不想要密码到期，则清除**设置到期时间?** 字段输入想要的天数。
5. 要在存储文件中保存密码的加密版本，选择**密码存储到文件?** 字段并输入**是**。

   注: 您必须存储密码以启用带有“IP 安全性”的数字证书的使用。
6. 单击**确定**。状态栏中的消息表示成功完成申请。
7. 再次单击**确定**并返回到“IBM 密钥管理”屏幕。您可以执行其它任务或者退出工具。

使用数字证书创建 IKE 报文封装

要创建使用数字证书的 IKE 报文封装，必须使用基于 Web 的系统管理器和“密钥管理器”工具。

定义密钥管理 IKE 报文封装策略时要启用数字证书的使用，必须配置使用签名方式的转换。 *签名方式*针对认证使用 RSA 签名算法。 “IP 安全性”提供基于 Web 的系统管理器对话框“添加／更改转换”以允许您选择 RSA 签名或带有 CRL 校验的 RSA 签名的认证方法。

报文封装至少一个端点必须具有定义使用签名方式转换的策略。您也可以通过基于 Web 的系统管理器使用签名方式来定义其他的转换。

“IP 安全性”支持的 IKE 密钥管理报文封装类型（ “识别”选项卡上的**主机身份类型**字段）如下:

- IP 地址
- 全限定域名（FQDN）
- *user@FQDN*

- X.500 专有名称
- 密钥标识符

使用**基于 Web 的系统管理器**在“密钥管理报文封装属性 – 识别”选项卡中选择主机身份类型。如果选择 **IP 地址**、**FQDN** 或 **user@FQDN**，则必须在基于 Web 的系统管理器中输入值，然后把这些值提供给 CA。该信息用作个人数字证书中的“主题备用名称”。

例如，如果您在**识别**选项卡上从基于 Web 的系统管理器下拉列表中选择主机身份类型为 **X.500 专有名称**，并且输入 **Host identity** 为 **/C=US/O=ABC/OU=SERV/CN=*name*.austin.ibm.com**，则以下就是当创建数字证书申请时您必须在“密钥管理器”中输入的精确值:

- Common name: ***name*.austin.ibm.com**
- Organization: **ABC**
- Organizational unit: **SERV**
- Country : **US**

输入的 **X.500 专有名称**是由您的系统或 LDAP 管理员设置的名称。输入组织单位值是可选的。然后在创建数字证书时，CA 使用该信息。

另一个示例，如果从下拉列表中选择主机身份类型为 **IP 地址**，并输入主机身份为 **10.10.10.1**，下面是您在数字证书申请中必须输入的精确值:

- Common name: ***name*.austin.ibm.com**
- Organization: **ABC**
- Organizational unit: **SERV**
- Country : **US**
- Subject alternate IP address field: **10.10.10.1**

在创建了具有该信息的数字证书申请之后，CA 使用该信息创建个人数字证书。

当申请个人数字证书时，CA 需要以下信息:

- 您正在申请 X.509 证书。
- 签名格式为带有 RSA 加密算法的 MD5。
- 您是否指定“主题备用名称”。备用名称类型为:
  - IP 地址
  - 全限定域名（FQDN）
  - *user@FQDN*

  以下的主题备用名称信息包含在证书申请文件中。
- 计划密钥使用（必须选择数字签名位）。
- “密钥管理器”数字证书申请文件（以 PKCS#10 的形式）。

对于特定步骤使用“密钥管理器”来创建证书申请，请参阅第 155 页的『申请数字证书』。

在激活 IKE 报文封装之前，必须把从 CA 接收到的个人数字证书添加到“密钥管理器”数据库（**ikekey.kdb**）中。需要更多信息，请参阅第 156 页的『添加（接收）新的数字证书』。

“IP 安全性”支持以下的个人数字证书类型:

主题 DN

"主题专有名称"必须按照下面的格式和顺序:

/C=US/O=ABC/OU=SERV/CN=*name*.austin.ibm.com

"密钥管理器"工具只允许一个 **OU** 值。

作为 IP 地址的主题 DN 和主题备用名称

"主题专有名称"和"主题备用名称"可以指定为 IP 地址，如下所示:

/C=US/O=ABC/OU=SERV/CN=*name*.austin.ibm.com 和 10.10.10.1

作为 FQDN 的主题 DN 和主题备用名称

"主题专有名称"和"主题备用名称"可以指定为全限定域名，如下所示:

/C=US/O=ABC/OU=SERV/CN=*name*.austin.ibm.com 和 bell.austin.ibm.com。

作为 *user@FQDN* 的"主题 DN"和"主题备用名称"

"主题专有名称"和"主题备用名称"可以指定为用户地址（*user_ID@fully_qualified_domain_name*），如下所示:

/C=US/O=ABC/OU=SERV/CN=*name*.austin.ibm.com 和 *name*@austin.ibm.com。

主题 DN 和多个主题备用名称

"主题专有名称"可以与多个"主题备用名称"相关联，如下所示:

/C=US/O=ABC/OU=SERV/CN=*name*.austin.ibm.com 和 bell.austin.ibm.com、10.10.10.1 和 *user*@*name*.austin.ibm.com。

配置人工报文封装

以下过程配置 IP 安全性以使用人工报文封装。

设置报文封装和过滤器

要设置人工报文封装，不必单独配置过滤规则。只要两台主机之间的所有流量都经过报文封装，就会自动生成必要的过滤器规则。设置报文封装的过程是为了在一端定义报文封装，在另一端导入定义，并在两端激活报文封装和过滤器规则。然后报文封装就准备使用。

如果没有明确提供，则必须产生关于报文封装的信息用于双方的匹配。例如，如果目标值没有指定的话，针对源指定的加密和认证算法将用作目标位置。

在第一台主机上创建人工报文封装

您可以使用基于 Web 的系统管理器网络应用程序、SMIT **ips4_basic** 快速路径（对于 IP V4）或者 SMIT **ips6_basic** 快速路径（对于 IP V6）来配置报文封装。您也可以使用以下过程手工创建报文封装。

下面是一个用于创建人工报文封装的 **gentun** 命令的示例:

```
gentun -v 4 -t manual -s 5.5.5.19 -d 5.5.5.8 \
   -a HMAC_MD5 -e DES_CBC_8 -N 23567
```

您可以使用 **lstun -v 4** 命令列出由前面的示例创建的人工报文封装的特征。输出类似于以下的显示:

```
Tunnel ID            : 1
IP Version           : IP Version 4
Source               : 5.5.5.19
Destination          : 5.5.5.8
Policy               : auth/encr
Tunnel Mode          : Tunnel
Send AH Algo         : HMAC_MD5
Send ESP Algo        : DES_CBC_8
Receive AH Algo      : HMAC_MD5
Receive ESP Algo     : DES_CBC_8
Source AH SPI        : 300
Source ESP SPI       : 300
Dest AH SPI          : 23576
Dest ESP SPI         : 23576
Tunnel Life Time     : 480
Status               : Inactive
Target
Target Mask          : -
Replay               : No
New Header           : Yes
Snd ENC-MAC Algo     : -
Rcv ENC-MAC Algo     : -
```

要激活报文封装，请输入如下命令:

```
mktun -v 4 -t1
```

将会自动生成与报文封装有关的过滤器规则。

要查看过滤规则，使用 **lsfilt -v 4** 命令。输出类似于下面的显示:

```
Rule 4:
Rule action          : permit
Source Address       : 5.5.5.19
Source Mask          : 255.255.255.255
Destination Address  : 5.5.5.8
Destination Mask     : 255.255.255.255
Source Routing       : yes
```

```
Protocol              : all
Source Port           : any 0
Destination Port      : any 0
Scope                 : both
Direction             : outbound
Logging control       : no
Fragment control      : all packets
Tunnel ID number      : 1
Interface             : all
Auto-Generated        : yes

Rule 5:
Rule action           : permit
Source Address        : 5.5.5.8
Source Mask           : 255.255.255.255
Destination Address   : 5.5.5.19
Destination Mask      : 255.255.255.255
Source Routing        : yes
Protocol              : all
Source Port           : any 0
Destination Port      : any 0
Scope                 : both
Direction             : inbound
Logging control       : no
Fragment control      : all packets
Tunnel ID number      : 1
Interface             : all
Auto-Generated        : yes
```

要激活过滤规则，包含缺省的过滤规则，请使用 **mktun -v 4 -t 1** 命令。

要设置另一边（当它是使用该操作系统的另一台机器时），可以从主机 A 上导出报文封装定义，然后将其导入到主机 B。

以下命令将报文封装定义导出到一个名为 **ipsec_tun_manu.exp** 的文件中，并且目录中任何与文件 **ipsec_fltr_rule.exp** 有关的过滤规则都由 **-f** 标志表示:

```
exptun -v 4 -t 1 -f /tmp
```

在第二台主机上创建人工报文封装

要创建报文封装的匹配端，使用如下的命令将导出的文件复制并导入远程机器:

```
imptun -v 4 -t 1 -f /tmp
```

其中

1 是要导入的报文封装

/tmp 是导入文件驻留的目录

系统生成报文封装号。您可以从 **gentun** 命令的输出来获得，或者使用 **lstun** 命令列出报文封装并确定导入的正确的报文封装数。如果在导入文件中只有一个报文封装，或者所有的报文封装都要导入，则不需要 **-t** 选项。

如果远程机器不在运行该操作系统，导出文件可以用作设置报文封装另一端的算法、密钥和安全性参数索引（SPI）值的参考。

可以导入从防火墙产品中引出的文件来创建报文封装。要这样做，在导入文件时使用 **-n** 选项，如下:

```
imptun -v 4 -f /tmp -n
```

设置过滤器

采用大部分自动生成过滤器规则可以很容易地设置过滤器，或者可以根据 IP 信息包的属性定义极特别的过滤器功能来定制过滤器。通过比较源地址和 SPI 值从而将进入信息包匹配到过滤器表中所列出的源地址和 SPI 值。因此，这种配对必须是唯一的。

过滤器表中的每行看作是一个*规则*。规则集合确定接受什么信息包出入机器以及它们如何指向。过滤器规则可以控制通信的许多方面，包括源地址和目标地址及掩码、协议、端口号、方向、分段控制、源路由、报文封装和接口类型。

过滤器规则的类型如下:

- 在过滤器表中创建『静态过滤器规则』，用于流量的常规过滤器或人工报文封装的关联。它们可以添加、删除、修改和移动。可以添加可选的描述文本字段来标识特定规则。
- 第 165 页的『自动生成过滤器规则和用户指定过滤器规则』（也称为*自动生成*过滤器规则）是为了使用 IKE 报文封装而创建的特定的规则集合。静态和动态过滤器规则都是基于数据管理报文封装信息和数据管理报文封装协商来创建的。
- 第 166 页的『预定义的过滤器规则』是通用过滤器规则，它不可以修改、移动或删除，例如 `all traffic` 规则、`ah` 规则和 `esp` 规则。它们指所有流量。

与这些过滤器规则有关的是*子网掩码*，它把与过滤器规则以及主机 – 防火墙 – 主机配置选项有关的标识分组。以下几节描述不同类型的过滤器规则和它们的相关功能。

静态过滤器规则

每个静态过滤器规则包含几个空格分隔的字段。以下列表提供了每个字段的名称（来自规则 1 的每个字段的示例显示在圆括号中）:

- Rule_number (`1`)
- Action (`permit`)
- Source_addr (`0.0.0.0`)
- Source_mask (`0.0.0.0`)
- Dest_addr (`0.0.0.0`)
- Dest_mask (`0.0.0.0`)
- Source_routing (`no`)
- Protocol (`udp`)
- Src_prt_operator (`eq`)
- Src_prt_value (`4001`)
- Dst_prt_operator (`eq`)
- Dst_prt_value (`4001`)
- Scope (`both`)
- Direction (`both`)
- Logging (`no`)
- Fragment (`all packets`)
- Tunnel (`0`)
- Interface (`all`).

静态过滤器规则的进一步解释按照这个示例:

```
1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no udp eq 4001 eq 4001 both both no all
   packets 0 all

2 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no ah any 0 any 0 both both no all packets
   0 all

3 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no esp any 0 any 0 both both no all packets
   0 all

4 permit 10.0.0.1 255.255.255.255 10.0.0.2 255.255.255.255 no all any 0 any 0 both
   outbound no all packets 1 all outbound traffic

5 permit 10.0.0.2 255.255.255.255 10.0.0.1 255.255.255.255 no all any 0 any 0 both
   inbound no all packets 1 all


6 permit 10.0.0.1 255.255.255.255 10.0.0.3 255.255.255.255 no tcp lt 1024 eq 514 local
   outbound yes all packets 2 all


7 permit 10.0.0.3 255.255.255.255 10.0.0.1 255.255.255.255 no tcp/ack eq 514 lt 1024
   local inbound yes all packets 2 all


8 permit 10.0.0.1 255.255.255.255 10.0.0.3 255.255.255.255 no tcp/ack lt 1024 lt 1024
   local outbound yes all packets 2 all


9 permit 10.0.0.3 255.255.255.255 10.0.0.1 255.255.255.255 no tcp lt 1024 lt 1024 local
   inbound yes all packets 2 all


10 permit 10.0.0.1 255.255.255.255 10.0.0.4 255.255.255.255 no icmp any 0 any 0 local
   outbound yes all packets 3 all


11 permit 10.0.0.4 255.255.255.255 10.0.0.1 255.255.255.255 no icmp any 0 any 0 local
   inbound yes all packets 3 all


12 permit 10.0.0.1 255.255.255.255 10.0.0.5 255.255.255.255 no tcp gt 1023 eq 21 local
   outbound yes all packets 4 all


13 permit 10.0.0.5 255.255.255.255 10.0.0.1 255.255.255.255 no tcp/ack eq 21 gt 1023 local
   inbound yes all packets 4 all


14 permit 10.0.0.5 255.255.255.255 10.0.0.1 255.255.255.255 no tcp eq 20 gt 1023 local
   inbound yes all packets 4 all


15 permit 10.0.0.1 255.255.255.255 10.0.0.5 255.255.255.255 no tcp/ack gt 1023 eq 20 local
   outbound yes all packets 4 all


16 permit 10.0.0.1 255.255.255.255 10.0.0.5 255.255.255.255 no tcp gt 1023 gt 1023 local
   outbound yes all packets 4 all


17 permit 10.0.0.5 255.255.255.255 10.0.0.1 255.255.255.255 no tcp/ack gt 1023 gt 1023 local
   inbound yes all packets 4 all
```

```
18 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no all any 0 any 0 both both yes all
   packets
```

前面示例中的每个规则描述如下:

规则 1

用于 “会话密钥” 守护程序。该规则只出现在 IP V4 过滤器表中。它使用端口号 4001 来控制用于刷新会话密钥的信息包。规则 1 是如何能将端口号用于特定用途的一个示例。

注: 除记录用途以外，不要修改该过滤器规则。

规则 2 和 规则 3

允许处理认证头部分（AH）和封装安全性有效负载（ESP）头部分。

注: 除记录用途以外，不要修改过滤器规则 2 和 规则 3。

规则 4 和规则 5

自动生成的规则的集合，它过滤器通过报文封装 1 的地址 10.0.0.1 和 10.0.0.2 之间的流量。规则 4 用于出站流量，规则 5 用于入站流量。

注: 规则 4 有用户定义的 *outbound traffic* 描述。

规则 6 到规则 9

用户定义的规则集合，它过滤通过报文封装 2 的地址 10.0.0.1 和 10.0.0.2 之间的出站 **rsh**、**rcp**、**rdump**、**rrestore** 和 **rdist** 服务。在本示例中，记录设置为是，从而管理员可以监视这类流量。

规则 10 和规则 11

用户定义的规则集合，它过滤通过报文封装 3 的地址 10.0.0.1 和 10.0.0.4 之间的任意类型的入站和出站 **icmp** 服务。

规则 12 到规则 17

用户定义的过滤器规则，它是过滤通过报文封装 4 的从 10.0.0.1 和 10.0.0.5 之间的出站文件传输协议（FTP）。

规则 18

自动生成的总是置于表末的规则。在本示例中，它允许与其它过滤规则不匹配的所有的信息包。可以设置它来拒绝所有与其它过滤规则不匹配的流量。

可以单独查看每个规则（使用 **lsfilt**）并列出每个字段及其值。例如:

```
Rule 1:
Rule action          : permit
Source Address       : 0.0.0.0
Source Mask          : 0.0.0.0
Destination Address  : 0.0.0.0
Destination Mask     : 0.0.0.0
Source Routing       : yes
Protocol             : udp
Source Port          : eq  4001
Destination Port     : eq  4001
Scope                : both
Direction            : both
Logging control      : no
Fragment control     : all packets
Tunnel ID number     : 0
Interface            : all
Auto-Generated       : yes
```

以下的列表包含了在过滤器规则中可以指定的所有参数:

-v IP 版本: 4 或 6。

-a 操作:

- **d** 拒绝
- **p** 允许

-s 源地址。可以是 IP 地址或主机名。

-m 源子网掩码。

-d 目标地址。可以是 IP 地址或主机名。

-M 目标子网掩码。

-g 源路由控制: y 或 n。

-c 协议。值可以是 udp、icmp、tcp、tcp/ack、ospf、pip、esp、ah 和 all。

-o 源端口或 ICMP 类型操作。

-p 源端口或 ICMP 类型值。

-O 目标端口或 ICMP 代码操作。

-P 目标端口或 ICMP 代码值。

-r 路由:

- **r** 转发的信息包
- **l** 本地目标 / 源信息包
- **b** 二者

-l 日志控制。

- **y** 包含在日志中
- **n** 不包含在日志中。

-f 分段。

- **y** 应用到分段头部分、分段部分和非分段部分
- **o** 只应用于分段部分和分段头部分
- **n** 只应用于非分段部分
- **h** 只应用于非分段部分和分段头部分

-t 报文封装标识。

-i 接口, 如 tr0 或 en0。

需要更多信息, 请参阅 **genfilt** 和 **chfilt** 命令描述。

自动生成过滤器规则和用户指定过滤器规则

自动为 “IP 安全性” 过滤器和报文封装代码生成某些规则。自动生成的规则包含:

- 更新 IKE（AIX 4.3.2 及后续版本）中 IP 版本 4 的会话密钥守护程序的规则。
- 处理 AH 和 ESP 信息包的规则。

当定义报文封装时, 也会自动生成过滤器规则。对于人工报文封装, 自动生成的规则指定源地址、目标地址、掩码值和报文封装标识。那些地址间的所有流量都将流过报文封装。

对于 IKE 报文封装, 自动生成的规则确定 IKE 协商期间的协议和端口号。IKE 过滤器规则保存在单独的表中, 在静态过滤器规则之后和自动生成的规则之前搜索此表。插入 IKE 过滤器规则到静态过滤器表中的缺省位置, 但用户不能移动它们。

自动生成的规则允许通过报文封装的所有流量。用户定义的规则可以对某些类型的流量加以限制。在自动生成的规则之前放置这些用户定义的规则，因为“IP 安全性”使用查找到的适用于信息包的第一个规则。以下是一个用户定义的规则的示例，它过滤基于 ICMP 操作的流量。

```
1 permit 10.0.0.1 255.255.255.255 10.0.0.4 255.255.255.255 no icmp any 8 any 0
   local outbound no all packets 3 all
2 permit 10.0.0.4 255.255.255.255 10.0.0.1 255.255.255.255 no icmp any 0 any 0 local
   inbound no all packets 3 all
3 permit 10.0.0.4 255.255.255.255 10.0.0.1 255.255.255.255 no icmp any 8 any 0 local
   inbound no all packets 3 all
4 permit 10.0.0.1 255.255.255.255 10.0.0.4 255.255.255.255 no icmp any 0 any 0 local
   outbound no all packets 3 all
```

为简化单一报文封装的配置，在定义报文封装时自动生成过滤器规则。该功能可以通过在 **gentun** 中指定 **-g** 标志从而禁止。您可以用 **genfilt** 命令查找样本过滤器文件，从而为 **/usr/samples/ipsec/filter.sample** 中不同的 TCP/IP 服务生成过滤器规则。

预定义的过滤器规则

用某些事件自动生成几种预定义的过滤器规则。装入 ipsec_v4 或者 ipsec_v6 设备时，将预定义的规则插入过滤器表并激活该规则。缺省情况下，这个预定义规则允许所有信息包，但它是用户可配置的，您可以设置它来拒绝所有信息包。

> **注**: 远程配置时，请确保配置完成之前拒绝规则不启用，以防止您的会话锁定在机器之外。这种情况可以避免，可以在激活“IP 安全性”之前通过设置缺省操作或者配置报文封装到远程机器来实现。

IPv4 和 IPv6 过滤器表都有预定义规则。可以独立地改变二者中的任何一个来拒绝全部信息包。这样将阻止流量通过，除非该流量是由附加过滤器规则特别定义的。改变预定义规则的唯一其它选项是带有 **-l** 选项的 **chfilt**，它允许将与该规则匹配的信息包记录到日志。

为了支持 IKE 报文封装，在 IPv4 过滤器表中安置动态过滤器规则。这就是动态过滤器规则插入到过滤器表中的位置。该位置可以由用户通过向上和向下移动过滤器表的位置来控制。初始化报文封装管理器守护程序和 **isakmpd** 守护程序（以允许 IKE 报文封装协商）之后，在动态过滤器表中就会自动地创建规则，从而处理 IKE 消息以及 AH 和 ESP 信息包。

子网掩码

子网掩码用于分组与过滤器规则关联的标识集合。掩码值和过滤器规则中的标识进行“与”运算，并与信息包中指定的标识相比较。例如，源 IP 地址为 10.10.10.4 而子网掩码为 255.255.255.255 的过滤器规则指定必须存在十进制 IP 地址的精确匹配，如下所示:

	二进制	十进制
源 IP 地址	1010.1010.1010.0100	10.10.10.4
子网掩码	1111.1111.1111.1111	255.255.255.255

10.10.10.x 子网指定为 1111.1111.1111.0 或者 255.255.255.0。进入的地址应该附带子网掩码，这样可以将这个组合与过滤器规则中的标识相比较。例如，在应用了子网掩码之后，地址 10.10.10.100 成为 10.10.10.0，它与过滤器规则相匹配。

子网掩码为 255.255.255.240 允许地址中的最后四位为任意值。

主机 – 防火墙 – 主机配置

报文封装的主机 – 防火墙 – 主机配置选项允许您在主机和防火墙之间创建报文封装，然后自动生成必需的过滤器规则，用于主机和防火墙后的主机之间的正确通信。自动生成的过滤器规则允许通过指定报文封装的两台无防火墙主机之间的所有规则。缺省规则（用于用户数据报协议（UDP）、认证头部分（AH）和封装安全性有效负载（ESP））应该已经处理了主机到防火墙通信。必须适当的配置防火墙来完成设置。应该使用来自创建的报文封装导出的文件来输入防火墙需要的 SPI 值和密钥。

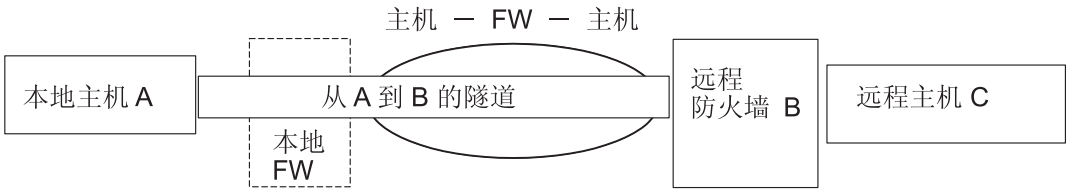


图 12. 主机 – 防火墙 – 主机. 该插图显示了主机 – 防火墙 – 主机配置。主机 A 有一个运行的报文封装，它通过本地防火墙并进入因特网。然后它转到远程防火墙 B，然后再到远程主机 C。

记录设备

本节描述与“IP 安全性”有关的系统日志配置和格式。主机间相互通信时，传送的信息包会记录在日志守护程序（**syslogd**）中。其它关于 IP 安全性重要信息也显示出来。管理员也许会为流量分析和调试助手选择监视记录信息。下面是设置记录设施的步骤。

1. 编辑 **/etc/syslog.conf** 文件添加以下项:

   ```
   local4.debug var/adm/ipsec.log
   ```

   使用 local4 设备记录流量和“IP 安全性”事件。标准操作系统优先级别应用。在通过“IP 安全性”报文封装和过滤器显示稳定性和正确活动之前，应该设置 debug 的优先级别。

   注: 过滤器事件的记录能够在“IP 安全性”主机创建大量的活动，并消耗大量的存储器。

2. 保存 **/etc/syslog.conf**。
3. 转至您为日志文件指定的目录，并用相同的名称创建一个空文件。在上面的情况，您更改为 **/var/adm** 目录，并发出命令:

   ```
   touch ipsec.log
   ```

4. 发出 **refresh** 命令到 **syslogd** 子系统:

   ```
   refresh -s syslogd
   ```

5. 如果使用 IKE 报文封装，确保 **/etc/isakmpd.conf** 文件指定想要的 **isakmpd** 记录级别。（请参阅第 172 页的『IP 安全性问题确定』以获得关于 IKE 记录的更多信息。）
6. 当为您的主机创建过滤器规则时，如果您希望记录匹配特定规则的信息包，请设置 **-l** 参数为 **Y**（是），使用 **genfilt** 或者 **chfilt** 命令。
7. 打开信息包记录，启动 **ipsec_logd** 守护程序，使用以下命令:

   ```
   mkfilt -g start
   ```

   可以通过发出以下命令停止信息包的记录:

   ```
   mkfilt -g stop
   ```

以下样本日志文件包含流量项和其它“IP 安全日志”项:

```
1. Aug 27 08:08:40 host1 : Filter logging daemon ipsec_logd (level 2.20)
   initialized at 08:08:40 on 08/27/97A
2. Aug 27 08:08:46 host1 : mkfilt: Status of packet logging set to Start
   at 08:08:46 on 08/27/97
3. Aug 27 08:08:47 host1 : mktun: Manual tunnel 2 for IPv4, 9.3.97.244, 9.3.97.130
   activated.
4. Aug 27 08:08:47 host1 : mkfilt: #:1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   udp eq  4001 eq  4001  both both l=n f=y t=0 e= a=
5. Aug 27 08:08:47 host1 : mkfilt: #:2 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   ah any 0 any 0  both both l=n f=y t=0 e= a=
6. Aug 27 08:08:47 host1 : mkfilt: #:3 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   esp any 0 any 0  both both l=n f=y t=0 e= a=
7. Aug 27 08:08:47 host1 : mkfilt: #:4 permit 10.0.0.1 255.255.255.255 10.0.0.2
   255.255.255.255 icmp any 0 any 0  local outbound l=y f=y t=1 e= a=
8. Aug 27 08:08:47 host1 : mkfilt: #:4 permit 10.0.0.2 255.255.255.255 10.0.0.1
   255.255.255.255 icmp any 0 any 0  local inbound l=y f=y t=1 e= a=
9. Aug 27 08:08:47 host1 : mkfilt: #:6 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
    all any 0 any 0  both both l=y f=y t=0 e= a=
10. Aug 27 08:08:47 host1 : mkfilt: Filter support (level 1.00) initialized at
    08:08:47 on 08/27/97
11. Aug 27 08:08:48 host1 : #:6 R:p  o:10.0.0.1 s:10.0.0.1 d:10.0.0.20 p:udp
    sp:3327 dp:53 r:l a:n f:n T:0 e:n l:67
12. Aug 27 08:08:48 host1 : #:6 R:p  i:10.0.0.1 s:10.0.0.20 d:10.0.0.1 p:udp
    sp:53 dp:3327 r:l a:n f:n T:0 e:n l:133
```

```
13. Aug 27 08:08:48 host1 : #:6 R:p  i:10.0.0.1 s:10.0.0.15 d:10.0.0.1 p:tcp
    sp:4649 dp:23 r:l a:n f:n T:0 e:n l:43
14. Aug 27 08:08:48 host1 : #:6 R:p  o:10.0.0.1 s:10.0.0.1 d:10.0.0.15 p:tcp
    sp:23 dp:4649 r:l a:n f:n T:0 e:n l:41
15. Aug 27 08:08:48 host1 : #:6 R:p  i:10.0.0.1 s:10.0.0.15 d:10.0.0.1 p:tcp
    sp:4649 dp:23 r:l a:n f:n T:0 e:n l:40
16. Aug 27 08:08:51 host1 : #:4 R:p  o:10.0.0.1 s:10.0.0.1 d:10.0.0.2 p:icmp
    t:8 c:0 r:l a:n f:n T:1 e:n l:84
17. Aug 27 08:08:51 host1 : #:5 R:p  i:10.0.0.1 s:10.0.0.2 d:10.0.0.1 p:icmp
    t:0 c:0 r:l a:n f:n T:1 e:n l:84
18. Aug 27 08:08:52 host1 : #:4 R:p  o:10.0.0.1 s:10.0.0.1 d:10.0.0.2 p:icmp
    t:8 c:0 r:l a:n f:n T:1 e:n l:84
19. Aug 27 08:08:52 host1 : #:5 R:p  i:10.0.0.1 s:10.0.0.2 d:10.0.0.1 p:icmp
    t:0 c:0 r:l a:n f:n T:1 e:n l:84
20. Aug 27 08:32:27 host1 : Filter logging daemon terminating at 08:32:27 on
    08/27/97l
```

以下段落解释日志项。

1 激活的过滤器记录守护程序。

2 通过使用 **mkfilt -g start** 命令将过滤器信息包记录设置为打开。

3 报文封装激活，显示报文封装标识、源地址、目的地址和时间戳记。

4-9 已激活过滤器。记录显示全部装入的过滤器规则。

10 消息显示过滤器的激活。

11-12 这些项显示对主机的 DNS 查询。

13-15 这些项显示部分的 Telnet 连接（由于空间原因，已从本例中除去其他项）。

16-19 这些项显示两个 ping。

20 过滤器记录守护程序关闭。

以下示例从启动主机的角度显示两个协商阶段 1 和阶段 2 报文封装的主机。（指定 **isakmpd** 记录级别为 **isakmp_events**。）

```
1. Dec  6 14:34:42 host1 Tunnel Manager: 0: TM is processing a
   Connection_request_msg
 2. Dec  6 14:34:42 host1 Tunnel Manager: 1: Creating new P1 tunnel object (tid)
 3. Dec  6 14:34:42 host1 isakmpd: 192.168.100.103 >>> 192.168.100.104 ( SA PROPOSAL
    TRANSFORM  )
 4. Dec  6 14:34:42 host1 isakmpd: ::ffff:192.168.100.103 <<< 192.168.100.104 ( SA
    PROPOSAL TRANSFORM  )
 5. Dec  6 14:34:42 host1 isakmpd: Phase I SA Negotiated
 6. Dec  6 14:34:42 host1 isakmpd: 192.168.100.103 >>> 192.168.100.104 ( KE NONCE  )
 7. Dec  6 14:34:42 host1 isakmpd: ::ffff:192.168.100.103 <<< 192.168.100.104 ( KE
    NONCE  )
 8. Dec  6 14:34:42 host1 isakmpd: Encrypting the following msg to send: ( ID HASH
     )
 9. Dec  6 14:34:42 host1 isakmpd: 192.168.100.103 >>> 192.168.100.104 ( Encrypted
    Payloads )
10. Dec  6 14:34:42 host1 isakmpd: ::ffff:192.168.100.103 <<< 192.168.100.104 (
    Encrypted Payloads )
11. Dec  6 14:34:42 host1 Tunnel Manager: 1: TM is processing a P1_sa_created_msg
    (tid)
12. Dec  6 14:34:42 host1 Tunnel Manager: 1:   Received good P1 SA, updating P1
    tunnel (tid)
13. Dec  6 14:34:42 host1 Tunnel Manager: 0: Checking to see if any P2 tunnels need
    to start
14. Dec  6 14:34:42 host1 isakmpd: Decrypted the following received msg: ( ID HASH
     )
15. Dec  6 14:34:42 host1 isakmpd:  Phase I Done !!!
16. Dec  6 14:34:42 host1 isakmpd: Phase I negotiation authenticated
```

```
17. Dec  6 14:34:44 host1 Tunnel Manager: 0: TM is processing a
    Connection_request_msg
18. Dec  6 14:34:44 host1 Tunnel Manager: 0: Received a connection object for an
    active P1 tunnel
19. Dec  6 14:34:44 host1 Tunnel Manager: 1: Created blank P2 tunnel (tid)
20. Dec  6 14:34:44 host1 Tunnel Manager: 0: Checking to see if any P2 tunnels need
    to start
21. Dec  6 14:34:44 host1 Tunnel Manager: 1: Starting negotiations for P2 (P2 tid)
22. Dec  6 14:34:45 host1 isakmpd: Encrypting the following msg to send: ( HASH SA
    PROPOSAL TRANSFORM NONCE ID ID  )
23. Dec  6 14:34:45 host1 isakmpd: 192.168.100.103 >>> 192.168.100.104 ( Encrypted
    Payloads )
24. Dec  6 14:34:45 host1 isakmpd: ::ffff:192.168.100.103 <<< 192.168.100.104 (
    Encrypted Payloads )
25. Dec  6 14:34:45 host1 isakmpd: Decrypted the following received msg: ( HASH SA
    PROPOSAL TRANSFORM NONCE ID ID  )
26. Dec  6 14:34:45 host1 isakmpd: Encrypting the following msg to send: ( HASH  )
27. Dec  6 14:34:45 host1 isakmpd: 192.168.100.103 >>> 192.168.100.104 ( Encrypted
    Payloads )
28. Dec  6 14:34:45 host1 isakmpd: Phase II SA Negotiated
29. Dec  6 14:34:45 host1 isakmpd: PhaseII negotiation complete.
30. Dec  6 14:34:45 host1 Tunnel Manager: 0: TM is processing a P2_sa_created_msg
31. Dec  6 14:34:45 host1 Tunnel Manager: 1: received p2_sa_created for an existing
    tunnel as initiator (tid)
32. Dec  6 14:34:45 host1 Tunnel Manager: 1: Filter::AddFilterRules: Created filter
    rules for tunnel
33. Dec  6 14:34:45 host1 Tunnel Manager: 0: TM is processing a List_tunnels_msg
```

以下段解释日志项。

1-2 **ike cmd=activate phase=1** 命令启动一个连接。

3-10 **isakmpd** 守护程序协商阶段 1 报文封装。

11-12 “报文封装管理器”从响应程序接收有效的阶段 1 安全关联。

13 “报文封装管理器”检查是否 **ike cmd=activate** 具有更多工作的阶段 2 值。它没有。

14-16 **isakmpd** 守护程序完成阶段 1 协商。

17-21 **ike cmd=activate phase=2** 命令启动阶段 2 报文封装。

22-29 **isakmpd** 守护程序协商阶段 2 报文封装。

30-31 “报文封装管理器”从响应程序接收有效的阶段 2 安全关联。

32 “报文封装管理器”写入动态过滤器规则。

33 **ike cmd=list** 命令查看 IKE 报文封装。

字段项中的标签

简化日志项中的字段以减少 DASD 空间需求:

引起信息包记录的规则号码。

R 规则类型

- **p** 允许
- **d** 拒绝

i/o 当信息包由过滤器支持代码截获时的移动方向。标识同信息包关联的适配器的 IP 地址。

- 对于入站（i）信息包，这就是信息包到达的适配器。
- 对于出站（o）信息包，这就是 IP 层决定的应该处理信息包传送的适配器。

s 指定信息包发送方（从 IP 报头抽取）的 IP 地址。

d 指定信息包接收方（从 IP 报头抽取）的 IP 地址。

p 指定用于在信息包的数据部分中创建消息的高级协议。或许是数字或名称，例如: udp、icmp、tcp、tcp/ack、ospf、pip、esp、ah 或 all。

sp/t 指定同信息包发送方（从 TCP/IP 报头抽取的）相关联的的协议端口号。当协议是 ICMP 或者 OSPF 时，该字段用 **t** 替换，它指定 IP 类型。

dp/c 指定同信息包接收方（从 TCP/IP 报头抽取的）相关联的的协议端口号。当协议是 ICMP 或 OSPF 时，该字段用 **c** 替换，它指定 IP 代码。

- 指定无信息可用。

r 表示信息包是否有本地联系。

- **f** 转发信息包
- **l** 本地信息包
- **o** 发送
- **b** 二者

l 以字节方式指定特定信息包的长度。

f 识别信息包是否是分段。

T 表示报文封装标识。

i 指定信息包进入的接口。

IP 安全性问题确定

本节包含一些提示和技巧，在遇到问题时它们可能会对您有所帮助。建议在第一次配置 IPSec 时安装日志。在确定过滤器及隧道发生了什么问题时，日志是非常有用的。（有关日志的详细信息，请参阅第 168 页的『记录设备』。）

手工隧道错误故障查找

错误: 发出 **mktun** 命令产生以下错误:

`insert_tun_man4()`: 写失败: 所请求的资源正忙。

问题: 请求激活的隧道已经是活动的，或有 SPI 值冲突。

修订: 发出 **rmtun** 命令来取消激活，然后发出 mktun 命令来激活。检查以确定发生故障的隧道的 SPI 值是否与任何其它激活的隧道匹配。每个隧道有它自己唯一的 SPI 值。

错误: 发出 **mktun** 命令产生了以下错误:

`设备 ipsec_v4 处于“已定义”状态。`

`没有执行 IP V4 的隧道激活。`

问题: 没有使“IP 安全性”设备可用。

修订: 发出以下命令:

```
mkdev -l ipsec -t 4
```

如果对于 IP V6 隧道激活的也得到相同的错误，可能只好将 **-t** 选项更改为 6。设备必须在可用状态。要检查“IP 安全性”设备状态，发出以下命令:

```
lsdev -Cc ipsec
```

错误: 发出 **gentun** 命令产生了以下错误:

`源 IP 地址无效`

问题: 没有输入源地址的有效 IP 地址。

修订: 对于 IP V4 隧道，检查以确认已为本地机器输入了可用的 IP V4 地址。在生成隧道时不能使用主机名作为源，仅可以使用主机名作为目的。

对于 IP V6 隧道，检查以确认您输入了可用的 IP V6 地址。如果输入 `netstat -in` 同时不存在 IP V6 地址，运行 **/usr/sbin/autoconf6**（接口）获得一个本地自动生成地址（使用 MAC 地址）的链接，或使用 **ifconfig** 命令来手工指定一个地址。

错误: 发出 **gentun** 命令产生了以下错误:

`源 IP 地址无效`

问题: 没有输入源地址的有效 IP 地址。

修订: 对于 IP V4 隧道，检查以确认已为本地机器输入了可用的 IP V4 地址。不能在生成隧道时使用源主机名，只能使用目的主机名。

对于 IP V6 隧道，检查以确认您输入了可用的 IP V6 地址。如果输入 `netstat -in` 时不存在 IP V6 地址，运行 **/usr/sbin/autoconf6**（接口）获得一个本地自动生成地址（使用 MAC 地址）的链接，或使用 **ifconfig** 命令来手工指定一个地址。

错误: 发出 **mktun** 命令产生了以下错误:

`insert_tun_man4()`: 写失败: 系统调用收到了一个无效的参数。

问题: 隧道生成于无效的 ESP 和 AH 组合，或在必要时没有使用新的头格式。

修订: 检查以确定有问题的特定隧道正在使用什么认证算法。请记住 HMAC_MD5 和 HMAC_SHA 算法需要新的头格式。新的头格式可以使用 SMIT 快速路径 **ips4_basic** 或带 **-z** 参数的 **chtun** 命令来更改。还有要记住 DES_CBC_4 不能与头格式一起使用。

错误: 从基于 Web 的系统管理器开始“IP 安全性”导致了一个失败消息。

问题: “IP 安全性”守护程序没在运行。

修订: 通过输入 `ps -ef` 命令查看哪个守护程序正在运行。以下守护程序与“IP 安全性”有关:

- **tmd**
- **isakmpd**
- **cpsd**

cpsd 守护程序仅在安装数字证书代码（文件集叫作 **gskit.rte** 或 **gskkm.rte**）并且已经配置了“密钥管理器”工具来包含数字证书时是激活的。

如果守护程序不是激活的，使用基于 Web 的系统管理器来停止“IP 安全性”，然后重新启动它，这会自动地启动适当的守护程序。

错误: 尝试使用“IP 安全性”产生了以下错误:

所安装的 `bos.crypto` 级别低，必须进行更新。

问题: **bos.net.ipsec.*** 文件已经更新为一个新版本，但是对应的 **bos.crypto.*** 文件没有更新。

修订: 将 **bos.crypto.*** 文件更新为与已更新的 **bos.net.ipsec.*** 文件相应的版本。

IKE 隧道错误故障查找

以下各节描述在使用 IKE 隧道过程中可发生的错误。

IKE 隧道过程流程

IKE 隧道由 **ike** 命令或基于 Web 的系统管理器 VPN 面板与以下守护程序的通信来安装:

表 8. IKE 隧道使用的守护程序。

tmd	“隧道管理器”守护程序
isakmpd	IKE 守护程序
cpsd	证书代理守护程序

为了使 IKE 隧道正确安装，要运行 **tmd** 和 **isakmpd** 守护程序。如果“IP 安全性”设置成重新引导时启动，这些守护程序会自动地启动。否则，它们必须使用基于 Web 的系统管理器启动。

“隧道管理器”向 **isakmpd** 命令发出请求来启动隧道。如果隧道已经存在或者无效（例如，有一个无效的远程地址），它会报告错误。如果协商已启动，可能要花一些时间来完成协商，主要取决于网络传输时间。**ike cmd=list** 命令列出隧道的状态以确定协商是否成功。而且，“隧道管理器”将事件记录到 **syslog** 中，它根据 **debug**、**event** 和 **information** 级别来记录，这可以用作监视协商进度。

按以下顺序:

1. 使用基于 Web 的系统管理器或 **ike** 命令来启动隧道。

2. **tmd** 守护程序向 **isakmpd** 守护程序发出一个密钥管理（阶段 1）的连接请求。
3. **isakmpd** 守护程序响应 SA 已创建或一个错误。
4. **tmd** 守护程序向 **isakmpd** 守护程序发出一个数据管理隧道（阶段 2）连接请求。
5. **isakmpd** 守护程序响应 SA created 或一个错误。
6. 隧道参数插入内核隧道高速缓存。
7. 将过滤规则添加进内核动态过滤表。

当机器充当响应程序时，**isakmpd** 守护程序通知 “隧道协商管理器” **tmd** 守护程序，隧道已经协商成功，并且有一个新的隧道插入到内核中。在这种的情况下，该过程从步骤 3 开始直到步骤 7 结束，在此过程中 **tmd** 守护程序不发出连接请求。

IKE 记录

isakmpd、**tmd** 和 **cpsd** 守护程序把事件记录到 **syslog** 中。对于 **isakmpd** 守护程序，使用 **ike cmd=log** 命令启用日志记录。可设置 **/etc/isakmpd.conf** 配置文件来指定记录级别。级别可以设置成 **none**、**error**、**isakmp_events** 或 **information**。

> **注**: 在比 AIX 5.1 更早的版本中，**isakmpd** 守护程序将日志记录到一个单独文件中，该文件也在 **/etc/isakmpd.conf** 文件中指定。

可以为日志记录设置的配置文件参数是 log_level。IKE 守护程序使用以下级别的记录:

none 无记录（缺省值）

error 只记录协议和 API 错误

isakmp_events
只记录 IKE 协议事件和错误

information
记录协议和实现信息（建议用于调试）。

该选项的语法象下面这样简单:

```
log_level
```

isakmpd 守护程序代码或者通过发送建议来启动，或者通过评估建议来响应。如果接受建议，则创建安全性的关联并安装隧道。如果没有接受建议或在协商完成前连接超时，**isakmpd** 守护程序会显示错误。在 **tmd** 的 **syslog** 中的项表明是否协商成功。将由无效的证书引起的失败记录到 **syslog** 中。要确定协商失败的准确原因，检查指定在 **/etc/syslog.conf** 文件中的日志文件。

syslog 工具给每个日志行添加了一个前缀，来标出数据、时间、机器和程序。以下示例使用 googly 作为机器名称，使用 isakmpd 作为程序名:

```
Nov 20 09:53:50 googly isakmpd: ISAKMP_MSG_HEADER
Nov 20 09:53:50 googly isakmpd:  Icookie : 0xef06a77488f25315, Rcookie :0x0000000000000000
Nov 20 09:53:51 googly isakmpd:  Next Payload : 1(SA), Maj Ver : 1, Min Ver : 0
Nov 20 09:53:51 googly isakmpd:  Xchg Type : 2 (ID protected), Flag= 0, Encr : No,COMMIT : No
Nov 20 09:53:51 googly isakmpd:  Msg ID  : 0x00000000
```

为了更加清楚，**grep** 命令可以用来抽取所感兴趣的日志行（例如所有 **isakmpd** 记录），而且 **cut** 命令可以用来从每行中除去前缀。在本节剩余部分的 **isakmpd** 日志示例是用相似方法制做的。

解析有效负载记录功能

通过交换 IKE 消息建立两端点之间的安全性关联（SA）。“解析有效负载”功能以人可读的格式解析消息。通过编辑 **/etc/isakmpd.conf** 文件，可以启用日志记录。**/etc/isakmpd.conf** 文件中的记录项与以下内容相似:

```
information
```

“解析有效负载”记录的 IKE 有效负载类型取决于 IKE 消息的内容。示例包含“SA 有效负载”、“密钥交换有效负载”、“证书申请有效负载”、“证书有效负载”以及“签名有效负载”。以下是一个“解析有效负载”日志的例子，其中 ISAKMP_MSG_HEADER 后面跟有五个有效负载:

```
ISAKMP_MSG_HEADER
        Icookie : 0x9e539a6fd4540990, Rcookie : 0x0000000000000000
        Next Payload : 1(SA), Maj Ver : 1, Min Ver : 0
        Xchg Type : 4 (Aggressive), Flag= 0, Encr : No,COMMIT : No
        Msg ID  : 0x00000000
        len     : 0x10e(270)
SA Payload:
        Next Payload : 4(Key Exchange), Payload len : 0x34(52)
        DOI          : 0x1(INTERNET)
        bitmask      : 1(SIT_IDENTITY_ONLY
   Proposal Payload:
        Next Payload : 0(NONE), Payload len : 0x28(40)
        Proposal # : 0x1(1), Protocol-ID : 1(ISAKMP)
        SPI size : 0x0(0), # of Trans : 0x1(1)
   Transform Payload:
        Next Payload : 0(NONE), Payload len : 0x20(32)
        Trans # : 0x1(1), Trans.ID : 1(KEY_IKE)
        Attr : 1(Encr.Alg     ), len=0x2(2)
        Value=0x1(1),(DES-cbc)
        Attr : 2(Hash Alg     ), len=0x2(2)
        Value=0x1(1),(MD5)
        Attr : 3(Auth Method  ), len=0x2(2)
        Value=0x3(3),(RSA Signature)
        Attr : 4(Group Desc   ), len=0x2(2)
        Value=0x1(1),(default 768-bit MODP group)
        Attr : 11(Life Type    ), len=0x2(2)
        Value=0x1(1),(seconds)
        Attr : 12(Life Duration), len=0x2(2)
        Value=0x7080(28800)
Key Payload:
        Next Payload : 10(Nonce), Payload len : 0x64(100)

        Key Data :
        33 17 68 10 91 1f ea da 38 a0 22 2d 84 a3 5d 5d
        a0 e1 1f 42 c2 10 aa 8d 9d 14 0f 58 3e c4 ec a3
        9f 13 62 aa 27 d8 e5 52 8d 5c c3 cf d5 45 1a 79
        8a 59 97 1f 3b 1c 08 3e 2a 55 9b 3c 50 cc 82 2c
        d9 8b 39 d1 cb 39 c2 a4 05 8d 2d a1 98 74 7d 95
        ab d3 5a 39 7d 67 5b a6 2e 37 d3 07 e6 98 1a 6b

Nonce Payload:
        Next Payload : 5(ID), Payload len : 0xc(12 )
        Nonce Data:
        6d 21 73 1d dc 60 49 93
ID Payload:
        Next Payload : 7(Cert.Req), Payload len : 0x49(73)
        ID type      : 9(DER_DN), Protocol : 0, Port = 0x0(0)
Certificate Request Payload:
        Next Payload : 0(NONE), Payload len : 0x5(5)
        Certificate Encoding Type: 4(X.509 Certificate - Signature)
```

在每一个有效负载中，Next Payload 字段指向紧跟当前有效负载的有效负载。如果当前的有效负载是 IKE 消息中的最后一个，那么 Next Payload 字段有为零的值（无）。

示例中的“每个有效负载”有指向现在正在执行的协商的信息。例如，SA 有效负载有“协议和转换有效负载”，该有效负载依次显示加密算法、认证方式、散列算法、SA 生命类型和发起者建议的对响应程序的 SA 持续时间。

而且，“SA 有效负载”由一个或多个“建议有效负载”和一个或多个“转换有效负载”构成。“建议有效负载”的 Next Payload 字段有一个或者是 0 或者是 2 的值，如果它是唯一的“协议有效负载”时值是 0，如果它是带有多于一个的“协议有效负载”时值是 2。类似地，“转换有效负载”的 Next Payload 字段，当它是唯一的“转换有效负载”时值是 0，或者当跟有多于一个的“转换有效负载”时值是 3，如以下例子中所显示:

```
ISAKMP_MSG_HEADER
        Icookie : 0xa764fab442b463c6, Rcookie : 0x0000000000000000
        Next Payload : 1(SA), Maj Ver : 1, Min Ver : 0
        Xchg Type : 2 (ID protected), Flag= 0, Encr : No,COMMIT : No
        Msg ID  : 0x00000000
        len     : 0x70(112)
SA Payload:
        Next Payload : 0(NONE), Payload len : 0x54(84)
        DOI          : 0x1(INTERNET)
        bitmask      : 1(SIT_IDENTITY_ONLY
   Proposal Payload:
        Next Payload : 0(NONE), Payload len : 0x48(72)
        Proposal # : 0x1(1), Protocol-ID : 1(ISAKMP)
        SPI size : 0x0(0), # of Trans : 0x2(2)
   Transform Payload:
        Next Payload : 3(Transform), Payload len : 0x20(32)
        Trans # : 0x1(1), Trans.ID : 1(KEY_IKE)
        Attr : 1(Encr.Alg     ), len=0x2(2)
        Value=0x5(5),(3DES-cbc)
        Attr : 2(Hash Alg     ), len=0x2(2)
        Value=0x1(1),(MD5)
        Attr : 3(Auth Method  ), len=0x2(2)
        Value=0x1(1),(Pre-shared Key)
        Attr : 4(Group Desc   ), len=0x2(2)
        Value=0x1(1),(default 768-bit MODP group)
        Attr : 11(Life Type    ), len=0x2(2)
        Value=0x1(1),(seconds)
        Attr : 12(Life Duration), len=0x2(2)
        Value=0x7080(28800)
   Transform Payload:
        Next Payload : 0(NONE), Payload len : 0x20(32)
        Trans # : 0x2(2), Trans.ID : 1(KEY_IKE)
        Attr : 1(Encr.Alg     ), len=0x2(2)
        Value=0x1(1),(DES-cbc)
        Attr : 2(Hash Alg     ), len=0x2(2)
        Value=0x1(1),(MD5)
        Attr : 3(Auth Method  ), len=0x2(2)
        Value=0x1(1),(Pre-shared Key)
        Attr : 4(Group Desc   ), len=0x2(2)
        Value=0x1(1),(default 768-bit MODP group)
        Attr : 11(Life Type    ), len=0x2(2)
        Value=0x1(1),(seconds)
        Attr : 12(Life Duration), len=0x2(2)
        Value=0x7080(28800)
```

“解析有效负载”日志的“IKE 消息头”显示了交换类型（“主方式”或“主动方式”）、整个消息长度、消息标识等等。

“证书申请有效负载”从响应程序请求证书。响应程序在不同的报文中发送证书。以下示例显示了“证书有效负载”和“签名有效负载”，它们作为 SA 协商的一部分送到了对等点。证书数据和签名数据以十六进制格式显示。

```
ISAKMP_MSG_HEADER
        Icookie : 0x9e539a6fd4540990, Rcookie : 0xc7e0a8d937a8f13e
        Next Payload : 6(Certificate), Maj Ver : 1, Min Ver : 0
        Xchg Type : 4 (Aggressive), Flag= 0, Encr : No,COMMIT : No
        Msg ID  : 0x00000000
        len     : 0x2cd(717)
Certificate Payload:

        Next Payload : 9(Signature), Payload len : 0x22d(557)
        Certificate Encoding Type: 4(X.509 Certificate - Signature)
        Certificate: (len 0x227(551) in bytes
        82 02 24 30 82 01 8d a0 03 02 01 02 02 05 05 8e
        fb 3e ce 30 0d 06 09 2a 86 48 86 f7 0d 01 01 04
        05 00 30 5c 31 0b 30 09 06 03 55 04 06 13 02 46
        49 31 24 30 22 06 03 55 04 0a 13 1b 53 53 48 20
        43 6f 6d 6d 75 6e 69 63 61 74 69 6f 6e 73 20 53
        65 63 75 72 69 74 79 31 11 30 0f 06 03 55 04 0b
        13 08 57 65 62 20 74 65 73 74 31 14 30 12 06 03
        55 04 03 13 0b 54 65 73 74 20 52 53 41 20 43 41
        30 1e 17 0d 39 39 30 39 32 31 30 30 30 30 30 30
        5a 17 0d 39 39 31 30 32 31 32 33 35 39 35 39 5a
        30 3f 31 0b 30 09 06 03 55 04 06 13 02 55 53 31
        10 30 0e 06 03 55 04 0a 13 07 49 42 4d 2f 41 49
        58 31 1e 30 1c 06 03 55 04 03 13 15 62 61 72 6e
        65 79 2e 61 75 73 74 69 6e 2e 69 62 6d 2e 63 6f
        6d 30 81 9f 30 0d 06 09 2a 86 48 86 f7 0d 01 01
        01 05 00 03 81 8d 00 30 81 89 02 81 81 00 b2 ef
        48 16 86 04 7e ed ba 4c 14 d7 83 cb 18 40 0a 3f
        55 e9 ad 8f 0f be c5 b6 6d 19 ec de 9b f5 01 a6
        b9 dd 64 52 34 ad 3d cd 0d 8e 82 6a 85 a3 a8 1c
        37 e4 00 59 ce aa 62 24 b5 a2 ea 8d 82 a3 0c 6f
        b4 07 ad 8a 02 3b 19 92 51 88 fb 2c 44 29 da 72
        41 ef 35 72 79 d3 e9 67 02 b2 71 fa 1b 78 13 be
        f3 05 6d 10 4a c7 d5 fc fe f4 c0 b8 b8 fb 23 70
        a6 4e 16 5f d4 b1 9e 21 18 82 64 6d 17 3b 02 03
        01 00 01 a3 0f 30 0d 30 0b 06 03 55 1d 0f 04 04
        03 02 07 80 30 0d 06 09 2a 86 48 86 f7 0d 01 01
        04 05 00 03 81 81 00 75 a4 ee 9c 3a 18 f2 de 5d
        67 d4 1c e4 04 b4 e5 b8 5e 9f 56 e4 ea f0 76 4a
        d0 e4 ee 20 42 3f 20 19 d4 25 57 25 70 0a ea 41
        81 3b 0b 50 79 b5 fd 1e b6 0f bc 2f 3f 73 7d dd
        90 d4 08 17 85 d6 da e7 c5 a4 d6 9a 2e 8a e8 51
        7e 59 68 21 55 4c 96 4d 5a 70 7a 50 c1 68 b0 cf
        5f 1f 85 d0 12 a4 c2 d3 97 bf a5 42 59 37 be fe
        9e 75 23 84 19 14 28 ae c4 c0 63 22 89 47 b1 b6
        f4 c7 5d 79 9d ca d0
Signature Payload:
        Next Payload : 0(NONE), Payload len : 0x84(132)

        Signature: len 0x80(128) in bytes
        9d 1b 0d 90 be aa dc 43 95 ba 65 09 b9 00 6d 67
        b4 ca a2 85 0f 15 9e 3e 8d 5f e1 f0 43 98 69 d8
        5c b6 9c e2 a5 64 f4 ef 0b 31 c3 cb 48 7c d8 30
        e3 a2 87 f4 7c 9d 20 49 b2 39 00 fa 8e bf d9 b0
        7d b4 8c 4e 19 3a b8 70 90 88 2c cf 89 69 5d 07
        f0 5a 81 58 2e 15 40 37 b7 c8 d6 8c 5c e2 50 c3
        4d 19 7e e0 e7 c7 c2 93 42 89 46 6b 5f f8 8b 7d
        5b cb 07 ea 36 e5 82 9d 70 79 9a fe bd 6c 86 36
```

数字证书和签名方式问题

错误: **cpsd**（“认证代理服务器”守护程序）没有启动。与以下内容相似的项出现在日志文件中:

```
Sep 21 16:02:00 ripple CPS[19950]: Init():LoadCaCerts() failed, rc=-12
```

问题: 证书数据库还没有打开或者还没有创建。

修订: 确保“密钥管理器”证书数据库出现在 **/etc/security** 中。以下文件可以弥补数据库: **ikekey.crl**、**ikekey.kdb**、**ikekey.rdb**、**ikekey.sth**。

如果仅丢失 **ikekey.sth** 文件，则当“密钥管理器”数据库创建时，不选中隐藏密码选项。必须隐藏密码来启用使用带有“IP 安全性”的数字证书。（请参阅创建密钥数据库以获得更多信息。）

错误: “密钥管理器”在接收到证书时给出以下错误:

```
发现无效的 Base64 解码数据
```

问题: 在证书文件中找到多余数据或其它数据丢失或损坏。

修订: ‘DER’ 已编码证书应该包含于以下字符串中（在下面显示的）。除了 BEGIN 和 END CERTIFICATE 字符串以外，之前或之后应该没有其它的字符。

```
-----BEGIN CERTIFICATE-----
MIICMTCCAZqgAwIBAgIFFKZtANowDQYJKoZIhvcNAQEFBQAwXDELMAkGA1UEBhMC
RkkxJDAiBgNVBAoTG1NTSCBDb21tdW5pY2F0aW9ucyBTZWN1cml0eTERMA8GA1UE
CxMIV2ViIHRlc3QxFDASBgNVBAMTC1Rlc3QgUlNBIENBMB4XDTk5MDkyMTAwMDAw
MFoXDTk5MTAyMTIzNTk1OVowOzELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lCTTEe
MBwGA1UEAxMVcmlwcGxlLmF1c3Rpbi5pYm0uY29tMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQC5EZqo6n7tZrpAL6X4L7mf4yXQSm+m/NsJLhp6afbFpPvXgYWC
wq4pvOtvxgum+FHrE0gysNjbKkE4Y6ixC9PGGAKHnhM3vrmvFjnl1G6KtyEz58Lz
BWW39QS6NJ1LqqP1nT+y3+Xzvfv8EonqzNo8mglCWMX09SguLmWoU1PcZQIDAQAB
oyAwHjALBgNVHQ8EBAMCBaAwDwYDVR0RBAgwBocECQNhhzANBgkqhkiG9w0BAQUF
AOBgQA6bgp4Zay34/fyAlyCkNNAYJRrN3Vc4NHN7IGjUziN6jK5UyB5zL37FERW
hT9ArPLzK7yEZs+MDNvB0bosyGWEDYPZr7EZHhYcoBP4/cd0V5rBFmA8Y2gUthPi
Ioxpi4+KZGHYyLqTrm+8Is/DVJaQmCGRPynHK35xjT6WuQtiYg==
-----END CERTIFICATE-----
```

以下选项能够帮助诊断和解决该问题。

- 如果数据丢失或毁坏的，重新创建证书
- 使用 ASN.1 解析器（在因特网万维网中可用的），通过成功地解析证书来检查证书是否是有效的。

错误: “密钥管理器”在接收到个人证书时给出以下错误:

```
未找到该证书的请求密钥
```

问题: 不存在正在接收的个人证书的“个人证书申请”。

修订: 再次创建“个人证书申请”并请求一个新的证书。

错误: 当您配置 IKE 隧道时，基于 Web 的系统管理器给出以下错误:

```
Error 171 in the Key Management (Phase 1) Tunnel operation:
PUT_IRL_FAILED
```

问题: 该错误的一个原因是主机识别类型无效，该类型是在 IKE 对话框（标识表格）中配置的。当从下拉列表选择的主机识别类型不与在 Host Identity 字段中输入的类型匹配时，会发生这样的问题。例如，如果选择 **X500 专有名称**的主机标识类型，则必须在 Host Identity 字段中恰当地输入一个格式化专有名称。

修订: 确保所输入的专有名称对于在主机标识下拉列表中选定的类型是正确的。

错误: IKE 协商失败并在日志文件中出现一个与以下内容相似的项:

```
inet_cert_service::channelOpen():clientInitIPC():error,rc =2
（没有这样的文件或目录）
```

问题: **cpsd** 没有运行或已终止。

修订: 使用基于 Web 的系统管理器启动 “IP 安全性”。该操作也启动适当的守护程序。

错误: IKE 协商失败并在日志文件中出现与以下内容相似的项:

```
CertRepo::GetCertObj: DN Does Not Match: ("/C=US/O=IBM/CN=ripple.austin.ibm.com")
```

问题: 当定义的 IKE 隧道与在个人证书中的 X.500 DN 不匹配时输入 X.500 专有名称（DN）。

修订: 更改在基于 Web 的系统管理器中的 IKE 隧道定义来匹配在证书中的专有名称。

错误: 当定义在基于 Web 的系统管理器中的 IKE 隧道时，禁用在 “认证方法” 标签下的数字证书复选框。

问题: 与该隧道关联的策略没有使用 RSA 签名方式认证。

修订: 更改相关策略的转换以使用 RSA 签名认证方法。例如，当定义 IKE 隧道时，可以选择 *IBM_low_CertSig* 作为密钥管理策略。

跟踪工具

跟踪是一种用于跟踪内核事件的调试工具。跟踪用来获取关于在内核过滤器和隧道代码中发生的事件或错误的更多特定信息。

SMIT “IP 安全性” 跟踪工具可以在 “高级 IP 安全性配置” 菜单中得到。通过该跟踪工具捕获的包含关于错误、过滤器、过滤器信息、隧道、隧道信息、捕获／释放捕获、捕获信息、加密器和加密器信息的信息。通过设计，错误跟踪挂钩提供了最严重的信息。信息跟踪挂钩可以生成严重信息，并可能对系统性能产生影响。该跟踪将提供确定是什么问题的线索。当与服务技术人员谈话时，也需要跟踪信息。要访问跟踪工具，请使用 SMIT 快速路径 **smit ips4_tracing**（为 IP V4 使用）或 **smit ips6_tracing**（为 IP V6 使用）。

ipsecstat

可以发出 **ipsecstat** 命令来生成以下样本报告。该样本报告显示了 “IP 安全性” 设备在可用状态，在该状态安装了三个认证算法、三个加密算法以及一个信息包活动的当前报告。如果进行 “IP 安全性” 流量故障查找时，该信息在确定问题在哪里时会有用的。

```
IP Security 设备:
ipsec_v4 可用
ipsec_v6 可用

认证算法:
HMAC_MD5 -- Hashed MAC MD5 Authentication Module
HMAC_SHA -- Hashed MAC SHA Hash Authentication Module
KEYED_MD5 -- Keyed MD5 Hash Authentication Module

加密算法:
CDMF -- CDMF Encryption Module
DES_CBC_4 -- DES CBC 4 Encryption Module
DES_CBC_8 -- DES CBC 8 Encryption Module
3DES_CBC -- Triple DES CBC Encryption Module

IP 安全性统计信息 -
接收的信息包总计: 1106
接收的 AH 信息包: 326
接收的 ESP 信息包: 326
允许的 Srcrte 信息包: 0
发送的信息包总计: 844
```

```
发送的 AH 信息包: 527
发送的 ESP 信息包: 527
删除的接收信息包总计: 12
  过滤器拒绝的输入: 12
  AH 未计算: 0
  ESP 未计算: 0
  AH 重放违例: 0
  ESP 重放违例: 0
删除的发送信息包总计: 0
  过滤器拒绝输入: 0
添加的隧道高速缓存项: 7
到期的隧道高速缓存项: 0
删除的隧道高速缓存项: 6
```

注: 从 AIX 4.3.3 开始，已除去 CDMF 支持，因为 DES 现在在全球都可用。重新配置任何使用 CDMF 的隧道来使用 DES 或三重 DES。

IP 安全性参考

命令列表

ike cmd=activate	启动因特网密钥交换（IKE）协商（AIX 4.3.2 和后续版本）。
ike cmd=remove	取消激活 IKE 隧道（AIX 4.3.2 和后续版本）
ike cmd=list	列出 IKE 隧道（AIX 4.3.2 和后续版本）
ikedb	提供接口给 IKE 隧道数据库（AIX 5.1 和后续版本）
gentun	创建隧道定义
mktun	激活隧道定义
chtun	更改隧道定义
rmtun	除去隧道定义
lstun	列出隧道定义
exptun	导出隧道定义
imptun	导入隧道定义
genfilt	创建过滤器定义
mkfilt	激活过滤器定义
mvfilt	移动过滤规则
chfilt	更改过滤器定义
rmfilt	除去过滤器定义
lsfilt	列出过滤器定义
expfilt	导出过滤器定义
impfilt	导入过滤器定义
ipsec_convert	列出“IP 安全性”状态
ipsecstat	列出“IP 安全性”状态
ipsectrcbuf	列出“IP 安全性”跟踪缓冲区的内容
unloadipsec	卸装加密器模块

方法列表

defipsec	定义 IP V4 或 IP V6 的“IP 安全性”实例
cfgipsec	配置和装入 **ipsec_v4** 或 **ipsec_v6**
ucfgipsec	对 **ipsec_v4** 或者 **ipsec_v6** 取消配置

第 12 章 网络信息服务（NIS）和 NIS+ 安全

本章提供了 NIS+ 如何保护其名称空间的概述，包含以下部分:

操作系统安全机制

操作系统安全性是通过用户在进入操作系统环境之前必须通过的门，以及确定用户进入系统环境后能够做什么的许可权矩阵来提供的。在某些上下文中，*安全 RPC 密码*被称为*网络密码*。

整个系统由四个门和两个许可权矩阵组成:

拨号门 要通过调制解调器和电话线从外部访问给定操作系统环境，您必须提供有效的登录标识和拨号密码。

登录门 要进入给定操作系统环境，您必须提供有效的登录标识和用户密码。

root 用户门

要取得超级权限，您必须提供有效的 root 用户密码。

安全 RPC 门

在以安全级别 2（缺省值）运行的 NIS+ 环境中，当您尝试使用 NIS+ 服务以及取得对 NIS+ 对象（服务器、目录、表、表项等）的访问时，NIS+ 使用安全 RPC 进程确认您的身份。

要进入安全 RPC 门，您必须出示安全 RPC 密码。您的安全 RPC 密码和您的登录密码通常是相同的。在这种情况下，您将自动通过门，而不需要重新输入您的密码。（在某些上下文中，*安全 RPC 密码*称为*网络密码*。要了解关于处理两个不同一密码的信息，请参阅 *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide* 中的 Secure RPC Password versus Login Password 部分。）

一套*凭证*被用来通过安全 RPC 门自动传递您的请求。生成、出示并验证您的凭证的过程称为*认证*，因为它确认您的身份并确认您有有效的安全 RPC 密码。每次您要求 NIS+ 服务时，该认证过程自动执行。

在 NIS 兼容方式下运行的 NIS+ 环境中，安全 RPC 门提供的保护大大减弱，因为人人都有对所有 NIS+ 对象的读取权，以及对适用于各项的修改权，不管他们是否拥有有效的凭证（也就是说，不管认证进程是否已确认了他们的身份并验证了他们的安全 RPC 密码）。由于这种情况允许*任何*人拥有对 NIS+ 全部对象的读取权以及对适用于各项的修改权，在兼容性方式下运行的 NIS+ 网络比在正常方式下运行的同样网络更不安全。（在安全 RPC 术语中，任何没有有效凭证的用户被认为是属于 **nobody** 类的成员。要了解关于四个类的描述，请参阅第 190 页的『授权类』。）

有关如何管理 NIS+ 认证和凭证的详细信息，请参阅 *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide* 中的 Administering NIS+ Credentials 部分。

文件和目录矩阵

一旦您取得对操作系统环境的访问权，您读取、执行、修改、创建以及销毁文件和目录的能力就由适用的许可权来管理。

NIS+ 对象矩阵

一旦您取得对于 NIS+ 的恰当认证，您读取、修改、创建以及破坏 NIS+ 对象的能力就由适用的许可权管辖。这个过程称为 *NIS+ 授权*。

有关 NIS+ 许可权和授权的详细信息，请参阅 *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide* 中的 Administering NIS+ Access Rights 部分。

NIS+ 安全机制

NIS+ 安全性是 NIS+ 名称空间整体的一部分。不可能独立于名称空间之外来设置安全性。因此，设置安全性的指示信息与设置名称空间的其它组件所使用的步骤交织在一起。一旦设置了 NIS+ 安全性环境，您可以添加和除去用户、更改许可权、重新分配组成员以及执行管理一个发展中的网络所需的所有其它日常管理任务。

NIS+ 的安全性功能保护名称空间中的信息以及名称空间结构本身免受未授权的访问。没有这些安全性功能，任何 NIS+ 客户机可以获得、更改甚至损坏名称空间中存储的信息。

NIS+ 安全性起到两个用途:

认证 认证是用来识别 NIS+ 主体的。每次一个主体（用户或机器）尝试访问 NIS+ 对象，都要进行用户的身份和安全 RPC 密码确认和验证。（作为认证过程的一部分，您不一定非要输入密码。然而，如果由于某种原因，您的安全 RPC 密码不同于您的登录密码，则您必须在第一次尝试访问 NIS+ 对象或服务时，执行 **keylogin**。要执行 **keylogin**，您必须提供有效的安全 RPC 密码。请参阅 *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide* 中的 Secure RPC Password versus Login Password 部分。）

授权 授权是用来指定访问权的。每次 NIS+ 主体尝试访问 NIS+ 对象时，它们将被归入四个授权类（owner、group、world、nobody）之一。NIS+ 安全系统允许 NIS+ 管理员指定每个类对 NIS+ 对象的不同的读取、修改、创建或破坏权限。例如，一个给定类可允许修改 passwd 表中的特定列，但不能读取该列，或另一类可允许读取一个特定表中的某些项，但不能读取其它项。

例如，一个给定的 NIS+ 表也许允许一个类读取和修改表中的信息，但另一个类只允许读取信息，而第三个类甚至连读取也不被允许。这在概念上与操作系统的文件和目录许可权系统是类似的。（有关类的更多信息，请参阅第 190 页的『授权类』。）

认证和授权防止拥有机器 A root 特权的某人使用 **su** 命令来冒充另一个用户的身份，（那个用户或者根本未登录，或在机器 B 上登录，）然后使用那个用户的 NIS+ 访问特权来访问 NIS+ 对象。

但请注意，NIS+ 不能防止知道另一个用户登录密码的某人冒充那个用户的身份以及他的 NIS+ 访问权限。NIS+ 也不能防止拥有 root 特权的用户冒充从*相同*机器上登录的另一个用户的身份。

下图详细解释了这个过程。

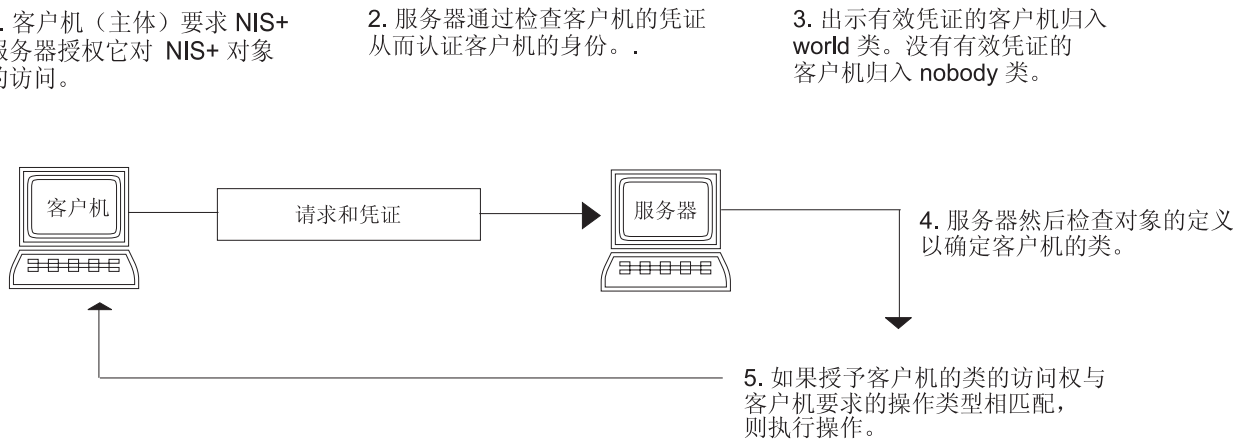


图 13. NIS+ 安全性过程的总结. 这个插图显示了对 NIS+ 安全性过程的陈述。

1. *客户机／主体请求 NIS+ 服务器授权对 NIS+ 对象的访问。*
2. *服务器检查客户机的凭证，以认证客户机的身份。*
3. *拥有有效凭证的客户机被归入 world 类中。*
4. *没有有效凭证的客户机被归入 nobody 类中。*
5. *服务器检查对象的定义，以确定客户机的类。*
6. *如果授权给客户机的类的访问权与所请求的操作类型相匹配，则执行该操作。*

NIS+ 主体

NIS+ 主体是那些提交 NIS+ 服务请求的实体（客户机）。NIS+ 主体可以是作为常规用户登录到客户机上的某人、作为 root 用户登录的某人或任何在 NIS+ 客户机上运行的拥有 root 用户许可权的进程。这样，NIS+ 主体可以是客户机用户或是客户机工作站。

NIS+ 主体也可以是从 NIS+ 服务器上提供 NIS+ 服务的实体。由于所有 NIS+ 服务器也是 NIS+ 客户机，本讨论的许多部分也适用于服务器。

NIS+ 安全级别

NIS+ 服务器在两个安全级别中的一个上操作。这些级别决定了为了认证主体的请求而必须提交的凭证类型。NIS+ 是设计成在最安全的级别上运行，即安全级别 2。级别 0 只是为了测试、设置以及调试用途而提供的。以下表格总结了这些安全级别。

注: 不论安全级别或凭证状态如何，请使用基于 Web 的系统管理器、SMIT 或 **passwd** 命令来更改您自己的密码。

NIS+ 安全级别

严重性级别	描述
0	设计安全级别 0 是为了测试和设置初始的 NIS+ 名称空间设计的。在安全级别 0 上运行的 NIS+ 服务器授予任何 NIS+ 主体对域中所有 NIS+ 对象的完全访问权。级别 0 只用于设置目的，只应该由管理员为此目的使用。级别 0 不应该由常规用户在网络上进行正常操作时使用。
1	安全级别 1 使用 AUTH_SYS 安全性。NIS+ 不支持该级别，不应该使用该级别。

NIS+ 安全级别

严重性级别	描述
2	安全级别 2 是缺省值。作为 NIS+ 目前提供的最高安全级别，它只认证使用数据加密标准（DES）凭证的请求。没有凭证的请求被指定为 nobody 类，并拥有授权给那个类的任何访问权。使用无效的 DES 凭证的请求被重试。在重复的获取有效 DES 凭证的尝试接连失败后，使用无效凭证的请求失败并返回认证错误。（凭证可能会因为不同的原因而无效，比如发送请求的主体未通过 **keylogin** 登录在那台机器上、时钟不同步、密钥不匹配等原因。）

NIS+ 认证和凭证

NIS+ 凭证认证每个请求 NIS+ 服务或请求对 NIS+ 对象进行访问的主体的身份。NIS+ 凭证/授权进程是对安全 RPC 系统的实现。

凭证/认证系统防止某人冒充另一人的身份。也就是说，它防止拥有一台机器超级权限的某人使用 **su** 命令来冒充另一个用户的身份（那个用户或者根本未登录，或者是在另一台机器上登录），然后使用那个用户的 NIS+ 访问特权来访问 NIS+ 对象。

> **注**: NIS+ 不能防止知道另一个用户登录密码的某人冒充那个用户的身份以及他的 NIS+ 访问权限。NIS+ 也不能防止拥有超级权限的用户冒充目前登录在*相同*机器上的另一个用户的身份。

服务器认证了主体后，它将检查主体想要访问的 NIS+ 对象以验证授权主体执行哪些操作。（有关授权的进一步信息，请参阅第 190 页的『NIS+ 授权与访问』。）

用户和机器凭证

对于主体的基本类型，*用户*和*机器*存在以下不同类型的凭证:

用户凭证
当某人作为常规用户登录到 NIS+ 客户机上，对 NIS+ 服务的请求包含此人的用户凭证。

机器凭证
当用户作为 root 用户登录到 NIS+ 客户机上，服务的请求使用客户机工作站的凭证。

DES 凭证与本地凭证

NIS+ 主体可以拥有 DES 或本地凭证。

DES 凭证

数据加密标准（DES）凭证提供安全认证。当本指南提到 NIS+ 检查凭证以认证 NIS+ 主体，NIS+ 所验证的是 DES 凭证。

注: 使用 DES 凭证只是获得认证的一种方法。不要将 DES 凭证与 NIS+ 凭证等同起来。

每次一个主体请求 NIS+ 服务或对 NIS+ 对象的访问，软件使用为该主体存储的凭证信息来为该主体生成凭证。DES 凭证是由 NIS+ 管理员为每个主体创建的信息生成的，*AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide* 中的 Administering NIS+ Credentials 部分对此作了解释。

- 当 NIS+ 确认了主体的 DES 凭证的有效性，该主体就是被*认证*了。
- 在一个主体归入 owner、group 或 world 授权类之前，该主体必须被认证。换句话说，为了归入这些类之一，您必须有有效的 DES 凭证。（没有有效 DES 凭证的主体被自动归入 nobody 类。）
- DES 凭证信息总是存储在主体的主域中的 cred 表中，不论该主体是客户机用户或是客户机工作站。

本地凭证

本地凭证是用户的用户标识号和他们的 NIS+ 主体名称（包含他们主域名）之间的映射。当用户登录时，系统查找他们的本地凭证，该凭证识别存储他们 DES 凭证的主域。系统使用这个信息来获取用户的 DES 凭证信息。

用户登录到远程域时，那些请求使用他们的本地凭证,这些本地凭证指回其主域。NIS+ 然后查询用户的主域，以得到用户的 DES 凭证信息。这就允许用户在远程域中被认证，即使该用户的 DES 凭证信息未存储在那个域中。下图说明了这个概念。

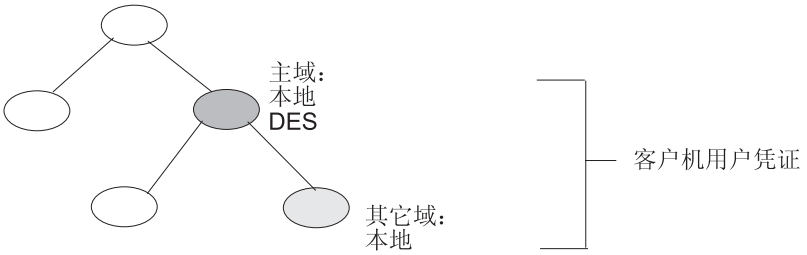


图 14. 凭证和域. 这个插图显示一个域的层次结构。用户的主域有本地和 DES 凭证。子域只有本地凭证。主域和子域标有客户机用户凭证。

本地凭证信息可存储于任何域。要登录到远程域并通过认证，客户机用户*必须*在远程域的 cred 表中拥有本地凭证。如果用户在他尝试访问的远程域中没有一个本地凭证，NIS+ 无法定位该用户的主域来获得他的 DES 凭证。在这种情况下，用户将不被认证，并将被归入 nobody 类。

用户类型和凭证类型

用户可以同时拥有两种类型的凭证，但机器只能拥有 DES 凭证。

root 用户不能作为 root 用户拥有对其它机器的 NIS+ 访问权，因为每台机器的 root 用户 UID 总是零。如果机器 A 的 root 用户（UID=0）尝试以 root 用户的身份访问机器 B，这与机器 B 中现有的 root（UID=0）相冲突。这样，本地凭证对于客户机*工作站*是不适当的；它只允许客户机*用户*拥有。

NIS+ 授权与访问

NIS+ 授权的基本目的是指定每个 NIS+ 主体对每个 NIS+ 对象与服务具有的访问权。

提出 NIS+ 请求的主体得到认证后，NIS+ 将该主体放入授权类中。在类的基础上分配访问权（许可权），这些访问权指定主体可以对给定的 NIS+ 对象进行哪项操作。换句话说，一个授权类可能有某种访问权，而一个不同的类则有不同的权限。

授权类 现有以下授权类: owner、group、world 和 nobody。（详细信息请参阅『授权类』）。

访问权 现有以下类型的访问权（许可权）: 创建、破坏、修改和读取。（详细信息请参阅第 192 页的『NIS+ 访问权限』）。

授权类

NIS+ 对象并非直接向 NIS+ 主体授予访问权。相反，它们向以下主体的类授予访问权:

Owner
恰好是对象所有者的主体获取向 owner 类授予的权限。

Group 每个 NIS+ 对象都有一个与其关联的组。由 NIS+ 管理员指定对象组的成员。属于对象 group 类的主体获取授予 group 类的权限。（在此上下文中，*组*指 NIS+ 组，而非操作系统或网络组。）有关 NIS+ 组的描述，请参阅第 191 页的『group 类』。

World world 类包含服务器可认证的全部 NIS+ 主体。（也就是说，既不在 owner 类又不在 group 类的每个已认证的主体。）

Nobody
所有主体属于 nobody 类，包括那些未认证的主体。

下图说明了类的关系:

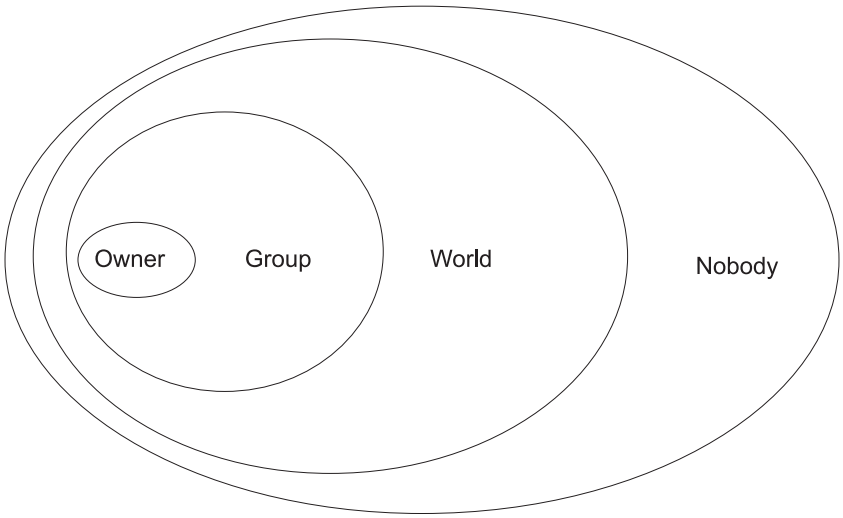


图 15. 授权类. 此图显示一系列表示授权类之间关系的椭圆。最小的椭圆是 owner，外面包围着较大的标为 group 的椭圆，再外面包围着标为 world 的椭圆，最外面包围着标为 nobody 的椭圆。

对于任何 NIS+ 请求，系统确定请求主体属于哪一类，然后此主体可用属于此类的任何访问权。

对象可向这些类中的每一类授予访问权限的任意组合。但是，通常分配给较高类的权限与分配给所有较低类的相同，可能附加的权限也是如此。

例如，对象可能向 nobody 和 world 类授予读取访问权，向 group 类授予读取和修改访问权，并向 owner 类授予读取、修改、创建及破坏访问权。

以下对授权类进行了详细的描述:

owner 类

所有者是*单一* NIS+ 主体。

向 NIS+ 对象提出访问请求的主体，必须在授予所有者访问权限前得到认证（出示有效 DES 凭证）。

缺省情况下，对象的所有者是创建此对象的主体。但是，对象的所有者可通过两种不同的方法让出所有权给另一个主体:

- 创建对象时，主体指定另一个的所有者（请参阅 *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide* 中 Specifying Accesss Rights in Commands 一节）。
- 创建对象后，主体更改对象的所有权（请参阅 *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide* 中 Changing Ownership of Objects and Entries 一节）。

主体让出所有权后，该主体就让出了一切 owner 对该对象的访问权，仅保留该对象分配给 group、world 或 nobody 的权限。

group 类

对象的组是*单一* NIS+ 组。（在此上下文中，*组*指 NIS+ 组，而非操作系统或网络组。）

向 NIS+ 对象提出访问请求的主体必须在被授予组访问权限前得到认证（出示 DES 有效凭证），并必须属于该组。

NIS+ 组是 NIS+ 主体的集合，以便于访问名称空间。向 NIS+ 组授予的访问权适用于是该组成员的所有主体。（但是，对象的所有者不必属于此对象组。）

创建对象时，创建者可选择缺省组。可在创建对象时或之后的任何时候指定非缺省组。

有关 NIS+ 组的信息存储在 NIS+ 组**对象**（在每个 NIS+ 域的 **groups_dir** 子目录下）中。（注意有关 NIS+ 组的信息未存储在 NIS+ 组表中。此表储存有关操作系统组的信息。）有关管理 NIS+ 组的指示信息在 *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide* 的 Administratering NIS+ Groups 一节中提供。

world 类

world 类包含 NIS+ 认证的所有 NIS+ 主体，即 owner 及 group 类的全部成员以及出示 DES 有效凭证的所有其它主体。

授予 world 类的访问权适用于所有已认证的主体。

noboday 类

noboday 类包含全部主体，甚至那些没有 DES 有效凭证的主体。

授权类及 NIS+ 对象层次结构

NIS+ 安全性将授权类单独应用于对象层次结构。目录对象是缺省层次结构的顶层，然后是组或表对象，然后是列，然后是项。以下定义提供有关每个级别的更多信息:

目录级别
每个 NIS+ 域包含两个 NIS+ 目录对象: **groups_dir** 和 **org_dir**。每个 **groups_dir** 目录对象包含各种组。每个 **org_dir** 目录对象包含各种表。

组或表的级别
组包含各个项和可能的其它组。表包含列及各个项。

列级 每个表有一个或多个列。

项（行）级
每组或表都有一个或多个项。

四种授权类应用于每一级。这样，目录对象有一个所有者和一个组。目录对象中的每个表有其自己的所有者和组，它们可不同于目录对象的所有者和组。在表内部，列或项可有其自己的所有者或组，它们可不同于表整体或目录对象整体的所有者和组。

NIS+ 访问权限

NIS+ 对象以操作系统文件为操作系统用户指定许可权的相同方式为 NIS+ 主体指定访问权限。访问权指定允许 NIS+ 主体在 NIS+ 对象上执行的操作类型。（您可以用 **niscat -o** 命令对这些进行检查。）

在不同类型的对象中，NIS+ 的操作不同，但是所有的操作都属于以下访问权类别之一: 读取、修改、创建和破坏。

读取 具有读取对象权限的主体可查看此对象的内容。

修改 具有修改对象权限的主体可更改此对象的内容。

破坏 具有破坏对象权限的主体可破坏或删除此对象。

创建 具有对较高级别对象的创建权限的主体可以在该级别中创建新对象。如果您对 NIS+ 目录对象有创建权限，您可在此目录内创建新表。如果您对 NIS+ 表有创建权限，您可在此表内创建新列及新项。

从 NIS+ 客户到 NIS+ 服务器的每次通信都是请求在特定的 NIS+ 对象上执行其中一种操作。例如，当 NIS+ 主体请求另一个工作站的 IP 地址时，它实际上是在请求对存储此类信息的 **hosts** 表对象的读取权。当主体要求服务器向 NIS+ 名称空间添加目录时，它实际上是在请求对该目录的父对象的**修改**访问。

这些权限合乎逻辑的向下展开，从目录到表、到表列及项级。例如，为了创建新表，您必须有创建 NIS+ 目录对象（用于存储表）的权限。当您创建此表时，您就成为其缺省的所有者。作为所有者，您可以给自己分配创建表的权限，此权限允许您在表中创建新的项。如果您在表中创建新项，您就成为这些项的缺省所有者。作为表所有者，您也可对其它类授予表级创建权。例如，您可以将表级创建权赋予表的 group 类。在这种情况下，表的组中任一成员都可在此表中创建新项。创建新表项的各个组成员成为此项的缺省所有者。

NIS+ 安全性和管理权限

NIS+ 不执行任何只许有一个 NIS+ 管理员的要求。任何对对象拥有管理权限（也就是，创建、破坏权限以及对某些对象的修改权限）的人都被认为是该对象的 NIS+ 管理员。

任何创建一个 NIS+ 对象的人设置对那个对象的初始访问权。如果创建者对对象的所有者（初始创建者）限制管理权限，则只有所有者拥有对象的管理权限。另一方面，如果创建者将管理权授权给对象的组，则组中的每个人拥有对该对象的管理权。

理论上，您可以将管理权授权给 world 类、甚至 nobody 类。软件允许您这样做。但将管理权限授权给 group 类以外的人，实际上使得 NIS+ 安全性失效。因此，如果将管理权限授予给 world 或 nobody 类，您实际上是在废除 NIS+ 安全性的目的。

NIS+ 安全性参考

请使用以下命令来管理密码、凭证和密钥（有关更多信息，请参阅相应的命令描述）：

chkey 更改主体的安全 RPC 密钥对。除非您要用新密码来重新加密您当前的专用密钥，请使用 **passwd** 命令。**chkey** 命令不影响 passwd 表中或 **/etc/passwd** 文件中的主体项。

keylogin
用 **keyserv** 解密并存储主体的保密密钥。

keylogout
从 **keyserv** 中删除存储的保密密钥。

keyserv
使服务器能够存储专用加密密钥。

newkey
在公用密钥数据库中创建新的密钥对。

nisaddcred
为 NIS+ 主体创建凭证。

nisupdkeys
更新目录对象中的公用密钥。

passwd
更改并管理主体的密码。

第 13 章 网络文件系统（NFS）安全性

除了标准 UNIX 认证系统外，网络文件系统（NFS）提供了以逐条消息为基础认证网络中用户和机器的方法。这种额外的认证系统使用数据加密标准（DES）加密和公开密钥加密法。

本章讨论以下主题:

NFS 认证

NFS 为不同目的使用 DES 算法。NFS 使用 DES 来加密远程过程调用（RPC）消息的时间戳记，这些消息在 NFS 服务器和客户机之间发送。此加密的时间戳记认证机器，就像“标记”认证发送方一样。

由于 NFS 能认证在 NFS 客户机和服务器间交换的每条 RPC 消息，这为每个文件系统提供了额外的、可选的安全级别。缺省情况下，文件系统导出时带有标准 UNIX 认证。要利用该额外的安全级别，您可以在导出文件系统时指定 **secure** 选项。

用于安全 NFS 的公开密钥加密法

用户的公用密钥和秘密密钥都以其网络名称在 **publickey.byname** 映射中存储和索引。秘密密钥使用用户登录密码进行了 DES 加密。**keylogin** 命令使用加密的秘密密钥，用登录密码解密它，再将它交给一个安全的本地密钥服务器保存，以备将来 RPC 事务使用。用户不会注意到他们的公用和秘密密钥，因为 **yppasswd** 命令除了更改登录密码，还自动生成公用和秘密密钥。

keyserv 守护程序是在每个 NIS 和 NIS+ 机器上运行的 RPC 服务。要了解关于 NIS+ 如何使用 **keyserv** 的信息，请参阅 *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide*。在 NIS 中，**keyserv** 执行以下公用密钥子例程:

- **key_setsecret** 子例程
- **key_encryptsession** 子例程
- **key_decryptsession** 子例程

key_setsecret 子例程告诉密钥服务器存储用户的秘密密钥（SK_A）以备将来使用；它通常由 **keylogin** 命令调用。客户机程序调用 **key_encryptsession** 子例程生成加密的对话密钥，该密钥在第一个 RPC 事务中被传递给一个服务器。密钥服务器查找服务器公用密钥，并将它与客户机的秘密密钥（由一个先前的 **key_setsecret** 子例程设置）结合，以生成公共密钥。服务器通过调用 **key_decryptsession** 子例程，要求密钥服务器解密对话密钥。

调用程序的名称在这些子例程调用中是隐式的，必须用某种方式认证。密钥服务器不能使用 DES 认证来进行上述认证，因为这将产生一个死锁。密钥服务器解决该问题的方法是通过按用户标识（UID）存储秘密密钥，并只授权给本地 root 进程的请求。然后客户机进程执行 root 用户拥有的 **setuid** 子例程，该子例程以客户机名义提出请求，告知密钥服务器客户机的真正 UID。

NFS 认证要求

安全 NFS 认证是基于发送方加密当前时间的能力，接收方可以再解密此当前时间，并与自己的时钟检查对照。该过程有以下要求:

- 双方的当前时间必须一致。
- 发送方和接收方必须使用相同的 DES 加密密钥。

协调当前时间

如果网络使用时间同步，则 **timed** 守护程序保持客户机和服务器的时钟同步。否则，客户机根据服务器时钟计算恰当的时间戳记。要做到这点，客户机在开始 RPC 会话之前确定服务器时间，再计算其本身时钟与服务器时钟之间的时差。然后客户机相应调整其时间戳记。如果在 RPC 会话过程中，客户机与服务器的时钟变得不同步，以至服务器开始拒绝客户机请求，则客户机将重新确定服务器时间。

使用相同 DES 密钥

客户机与服务器使用公开密钥加密法计算相同的 DES 加密密钥。对于任何客户机 A 和服务器 B，一个称为*公共密钥*的密钥只能由 A 和 B 推导出。该密钥是。客户机通过计算以下公式得出公共密钥:

$$K_{AB} = PK_B^{SK}A$$

其中 *K* 是公共密钥，*PK* 是公用密钥，而 *SK* 是秘密密钥，这些密钥的每一个都是一个 128 位的数字。服务器通过计算以下公式得出相同的公共密钥:

$$K_{AB} = PK_A^{SK}B$$

只有服务器与客户机可以计算出此公共密钥，因为要做到这点，需要知道一个或另一个的秘密密钥。由于公共密钥有 128 位，而 DES 使用 56 位密钥，客户机与服务器从公共密钥中抽取 56 位以形成 DES 密钥。

NFS 认证过程

当客户机想要与服务器谈话时，它随机生成一个密钥，用于加密时间戳记。此密钥称为*对话密钥*（*conversation key, CK*）。客户机使用 DES 公共密钥加密对话密钥（在认证要求中描述述）并在第一个 RPC 事务中将它发送至服务器。下图说明了此过程:

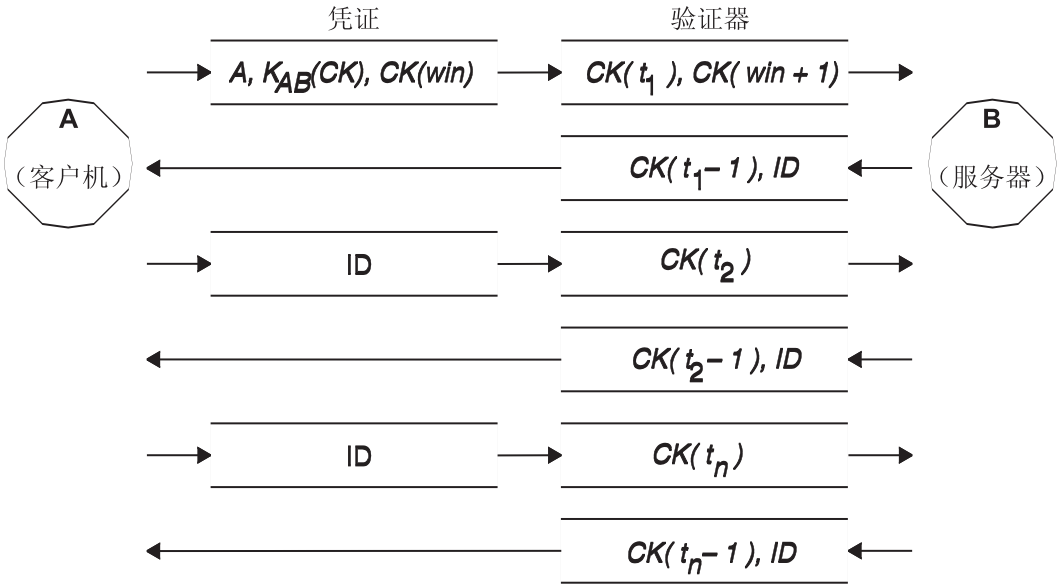


图 16. 认证过程. 此图说明了认证过程。

此图显示客户机 A 连到服务器 B。术语 *K*（*CK*）表示 *CK* 由 DES 公共密钥 *K* 加密。在它第一次的请求中，客户机 RPC 凭证包含客户机名称（*A*）、对话密钥（*CK*）以及由 *CK* 加密的称为 *win*（窗口）的变量。（缺省窗口大小是 30 分钟。）第一次请求中的客户机验证符包含加密的时间戳记和指定窗口的加密验证符，*win* + 1。该窗口验证符使猜测正确的凭证尤其困难，增加了安全性。

认证客户机之后，服务器将以下各项存储在一个凭证表中:

- 客户机名称，*A*
- 对话密钥，*CK*
- 窗口
- 时间戳记

服务器只接受按时序上大于上次见到的时间戳记的一个时间戳记，因此任何重放事务一定会被拒绝。服务器在验证符中向客户机返回一个凭证表的索引标识，还有客户机时间戳记减 1（用 *CK* 加密）。客户机知道只有服务器才能发送这样一个验证符，因为只有服务器知道客户机发送的时间戳记是什么。从时间戳记中减去 1 的原因是确保它无效且不能作为客户机验证符再次使用。在首次 RPC 事务后，客户机仅发送其标识和加密的时间戳记到服务器，而服务器返回由 *CK* 加密的减去 1 后的客户机时间戳记。

为 DES 认证命名网络实体

DES 认证使用网络名称进行命名。有关 NIS+ 如何处理 DES 认证的信息，请参阅 *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide*。

*网络名称*是要认证的一串可打印字符。公共和秘密密钥按每个网络名称而不是按每个用户名称为基础进行存储。**netid.byname** NIS 映射将网络名称映射到一个本地 UID 和组访问列表。

用户名在每个域中是唯一的。网络名是通过用 NIS 连接操作系统和用户标识以及因特网域名来分配的。一个命名域的较好约定是将因特网域名（com、edu、gov、mil）附加到本地域名上。

对用户和机器都分配网络名。机器网络名的形成很像用户网络名的形成。例如，eng.xyz.com 域中名为 hal 的机器具有网络名 unix.hal@eng.xyz.com。正确的机器认证对于需要通过网络对主目录有完全访问权的无盘机器是非常重要的。

要从任何远程域认证用户，请在两个 NIS 数据库中为其设立条目。一个条目是为其公用和秘密密钥设立的；另一个是为其本地 UID 和组访问列表映射设立的。这样远程域的用户就可以访问所有本地网络服务，例如 NFS 和远程登录。

/etc/publickey 文件

/etc/publickey 文件包含名称和公用密钥，NIS 和 NIS+ 使用它们来创建 **publickey** 映射。**publickey** 映射是用来保护联网。文件中的每个条目都由网络用户名（指用户名或主机名）构成，后跟用户的公用密钥（使用十六进制符号表示法）、冒号和用户加密秘密密钥（也使用十六进制符号表示法）。缺省情况下，**/etc/publickey** 文件中的唯一用户是用户 nobody。

请不要使用文本编辑器更改 **/etc/publickey** 文件，因为该文件包含加密密钥。要更改 **/etc/publickey** 文件，请使用 **chkey** 或 **newkey** 命令。

公用密钥系统的引导注意事项

当掉电故障之后重新启动机器时，所有存储的秘密密钥都丢失，也没有进程可以访问安全网络服务，例如安装 NFS。如果有人可以输入解密 root 用户秘密密钥的密码，root 进程则可继续。解决方案是将 root 用户的已解密的秘密密钥存储在密钥服务器可以读取的文件中。

不是所有的 **setuid** 子例程调用都能正确执行。例如，如果一个 **setuid** 子例程由所有者 A 调用，而所有者 A 自从启动后还未登录到机器上，则子例程不能作为 A 访问任何安全网络服务。然而，大多数 **setuid** 子例程调用由 root 用户拥有，而 root 用户的秘密密钥总是在启动时存储。

安全 NFS 的性能注意事项

安全 NFS 以下列方式影响系统性能:

- 客户机和服务器都必须计算公共密钥。计算公共密钥的时间大约是一秒钟。因此，建立初始 RPC 连接大约需要两秒钟，因为客户机和服务器都必须执行此操作。初始 RPC 连接之后，密钥服务器存储先前计算的结果，这样它就不需要每次都重新计算公共密钥。
- 每个 RPC 事务都要求以下 DES 加密操作:
  1. 客户机加密请求时间戳记。
  2. 服务器将它解密。
  3. 服务器加密应答时间戳记。
  4. 客户机将它解密。

由于系统性能可能因为安全 NFS 而降低，所以请在增加安全性获得的收益和系统性能要求间进行权衡。

管理安全 NFS 的核对表

使用以下核对表帮助确保安全 NFS 正常运行:

- 当使用 **-secure** 选项在客户机上安装文件系统时，服务器名称必须与 **/etc/hosts** 文件中的服务器主机名相匹配。如果名称服务器正用于主机名解析中，则请确保名称服务器返回的主机信息与 **/etc/hosts** 文件中的条目相匹配。如果这些名称不匹配，则产生认证错误。因为机器的网络名称是基于 **/etc/hosts** 文件中的主要条目，并且 **publickey** 映射中的密钥是由网络名称访问的。
- 请不要混淆安全和非安全的导出和安装。否则，文件访问权确定可能会不正确。例如，如果客户机未使用 **secure** 选项安装安全文件系统，或使用 **secure** 选项安装非安全系统，用户将作为 nobody 拥有访问权，而不是作为他们自己。如果一个 NIS 或 NIS+ 未知的用户试图创建或修改安全文件系统上的文件，这种情况也会发生。
- 由于 NIS 必须在每次使用 **chkey** 和 **newkey** 命令后传播新的映射，所以请只在网络负载轻时才使用这些命令。
- 请不要删除 **/etc/keystore** 文件或 **/etc/.rootkey** 文件。如果您重新安装、移动或升级一个机器，请保存 **/etc/keystore** 和 **/etc/.rootkey** 文件。
- 请指示用户使用 **yppasswd** 命令，而不是 **passwd** 命令来更改密码。这样做使密码和专用密钥保持同步。
- 由于 **login** 命令不从 **keyserv** 守护程序的 **publickey** 映射中检索密钥，所以用户必须执行 **keylogin** 命令。您也许想将 **keylogin** 命令放在每个用户的**概要**文件中，从而以在登录时自动执行该命令。**keylogin** 命令要求用户再次输入其密码。
- 当您使用 **newkey -h** 或 **chkey** 命令位为每个主机的 root 用户生成密钥时，您必须运行 **keylogin** 命令将新的密钥传递到 **keyserv** 守护程序。这些密钥存储在 **/etc/.rootkey** 文件中，每次 **keyserv** 守护程序启动时都会读取此文件。
- 请定期验证 **yppasswdd** 和 **ypupdated** 守护程序是否正在 NIS 主控服务器上运行。这些守护程序对维护 **publickey** 映射是必需的。
- 定期验证 **keyserv** 守护程序是否正在所有使用安全 NFS 的机器上运行。

配置安全 NFS

要在 NIS 主控和从属服务器上配置安全 NFS，请使用基于 Web 的系统管理器网络应用程序或使用以下步骤。有关一起使用 NFS 和 NIS+ 的信息，请参阅 *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide*。

1. 在 NIS 主控服务器上，通过使用 **newkey** 命令在 NIS **/etc/publickey** 文件中为每个用户创建一个条目，如下所示:
   - 对于常规用户，请输入:

     ```
     smit newkey
     ```

     或

     ```
     newkey -u username
     ```

     对于主机上的 root 用户，请输入:

     ```
     newkey -h hostname
     ```

   - 或者，用户也可以通过使用 **chkey** 或 **newkey** 命令建立他们自己的公用密钥。
2. 请按照 *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide* 中的指示信息创建 NIS **publickey** 映射。相应的 NIS **publickey.byname** 映射只驻留在 NIS 服务器上。
3. 取消 **/etc/rc.nfs** 文件中以下节的注解:

   ```
   #if [ -x /usr/sbin/keyserv ]; then
   #  startsrc -s keyserv
   #fi
   #if [ -x /usr/lib/netsvc/yp/rpc.ypupdated -a -d /etc/yp/`domainname` ]; then
   ```

```
#  startsrc -s ypupdated
#fi
#DIR=/etc/passwd
#if [ -x /usr/lib/netsvc/yp/rpc.yppasswdd -a -f $DIR/passwd ]; then
#  startsrc -s yppasswdd
#fi
```

4. 请通过使用 **startsrc** 命令启动 **keyserv**、**ypupdated** 和 **yppasswdd** 守护程序。

要在 NIS 客户机上配置安全 NFS，请通过使用 **startsrc** 命令来启动 **keyserv** 守护程序。

使用安全 NFS 导出文件系统

可以使用基于 Web 的系统管理器网络应用程序或使用以下步骤之一来导出安全 NFS。

- 要使用 SMIT 导出安全 NFS 文件系统，请执行以下操作:
  1. 通过运行 **lssrc -g nfs** 命令验证 NFS 是否已经在运行。输出表示 **nfsd** 和 **rpc.mountd** 守护程序是活动的。
  2. 验证 **publickey** 映射是否存在，以及 **keyserv** 守护程序是否正在运行。有关更多信息，请参阅第 199 页的『配置安全 NFS』。
  3. 运行 **smit mknfsexp** 快速路径。
  4. 为以下选项指定适当的值: 导出目录的 PATHNAME、导出目录的 MODE以及现在或系统重新启动（或同时指定两个字段）时 EXPORT。将“用户安全”选项字段指定为 yes。
  5. 指定任何其它可选的特征或接受缺省值。
  6. 退出 SMIT。如果 **/etc/exports** 文件不存在，则将创建该文件。
  7. 对您想要导出的每个目录，重复步骤 3 到 6。
- 要通过使用文本编辑器来导出安全 NFS 文件系统，请执行以下操作:
  1. 用您喜爱的文本编辑器打开 **/etc/exports** 文件。
  2. 使用目录的全路径名，为每个要导出的目录创建一个条目。从左边界开始，列出要导出的每个目录。目录不应包含任何其它已导出的目录。请参阅 **/etc/exports** 文件文档，以了解 **/etc/exports** 文件中条目的完整语法描述，包括如何指定**安全**选项。
  3. 保存并关闭 **/etc/exports** 文件。
  4. 如果 NFS 当前正在运行，请输入:

     ```
     /usr/sbin/exportfs -a
     ```

     将 **-a** 选项和 **exportfs** 命令一起使用，把 **/etc/exports** 文件中的所有信息发送到内核。
- 要临时导出 NFS 文件系统（即不更改 **/etc/exports** 文件），请输入:

  ```
  exportfs -i -o secure /dirname
  ```

  其中，*dirname* 是您要导出的文件系统名称。**exportfs -i** 命令指定对于指定目录不检查 **/etc/exports** 文件，并且所有选项都从命令行直接获得。

使用安全 NFS 安装文件系统

要显式地安装安全 NFS 目录，请执行以下操作:

1. 通过运行此命令验证 NFS 服务器是否已导出目录:

   ```
   showmount -e ServerName
   ```

其中，*ServerName* 是 NFS 服务器名称。此命令显示当前从 NFS 服务器中导出的目录名称。如果您要安装的目录没有列出，请从服务器中导出目录。

2. 通过使用 **mkdir** 命令建立本地安装点。为了 NFS 成功完成安装，必须提供充当 NFS 安装的安装点（或占位符）的目录。此目录必须是空的。可以像创建任何其它目录一样创建此安装点，并且不需要特殊属性。
3. 验证 **publickey** 映射存在，并且 **keyserv** 守护程序正在运行。要了解更多信息，请参阅第 199 页的『配置安全 NFS』。
4. 请输入:

   ```
   mount -o secure ServerName:/remote/directory /local/directory
   ```

   其中，*ServerName* 是 NFS 服务器名称，*/remote/directory* 是您希望安装的 NFS 服务器上的目录，而 */local/directory* 是 NFS 客户机上的安装点。

   注: 只有 root 用户可以安装安全 NFS。

第 14 章 企业身份映射

今天的网络环境是由复杂的一组系统和应用程序构成的，这导致必须管理多个用户注册表。迅速处理多个用户注册表引出一个重大的管理问题，它影响到用户、管理员和应用程序开发人员。“企业身份映射”（EIM）允许管理员和应用程序开发者找到该问题。

本章描述了这些问题，概述了当前工业方案，并解释了 EIM 方案。

管理多个用户注册表

许多管理员管理包含不同系统和服务器的网络，每一个都通过不同的用户注册表采用唯一的管理用户方式。在这些复杂的网络中，管理员负责管理整个复杂系统中每个用户的身份和密码。此外，管理员必须经常同步这些身份和密码。用户要承担起记住多个身份和密码并保持它们同步的重任。因为用户和管理员在该环境中的开销是昂贵的，管理员经常花费宝贵的时间对失败的登录尝试进行故障诊断并重新设置遗忘的密码，而不是管理企业。

管理多个用户注册表的问题也影响应用开发人员，他们想要提供多层或者不同种类的应用程序。客户有重要的业务数据分布在多个不同类型的系统中，每个系统处理它自己的用户注册表。因此，开发者必须为其应用程序创建专有的用户注册表及有关的安全性语义。尽管这解决了应用开发人员的问题，但它增加了用户和管理员的开销。

当前方案

解决管理多个用户注册表问题的几个当前业界途径是可用的，但它们都提供不完全的解决方案。例如，轻量级目录访问协议（LDAP）提供一种分布式用户注册表解决方案。然而，要使用 LDAP 这样的解决方案，管理员必须还要管理另一个用户注册表和安全性语义，或者替换为使用那些注册表而构建的现有应用程序。

使用这类解决方案，管理员针对个别的资源必须管理多个安全机制，从而增加了管理开销，并潜在的增加了安全性泄漏的可能性。当多个机制支持单独的资源时，通过一种机制更改权限并忘记更改一个或更多的其它机制权限的机会就会更高。例如，当用户适当地拒绝通过一个接口的访问但允许通过一个或更多个其它接口的访问时，就会导致安全性泄漏。

完成该工作后，管理员会发现并没有完全解决问题。通常，企业在当前用户注册表中以及有关的安全性语义中投入了太多资金以使用这类实际的解决方案。创建另一个用户注册表及有关的安全性语义可以为应用程序供应商解决问题，但不能为用户或管理员解决问题。

另一个解决方案是使用单签名的方案。有几个产品是可用的，它们允许管理员管理包含用户的所有身份和密码的文件。然而，该方案有几个弱点:

- 它只解决用户面临的问题中的一个。尽管它允许用户通过提供一个身份和密码注册到多个系统中，但用户仍然需要在其他的系统中有密码，或者需要管理这些密码。
- 它引入了一个产生安全性泄漏的新问题，因为明文或可以解密的密码保存在这些文件中。密码绝不可以保存在明文文件或容易受任何人（包括管理员）访问的文件中。
- 它没有解决第三方应用开发人员的问题，他们提供不同种类的、多层的应用程序。他们仍需为应用程序提供专有用户注册表。

尽管有这些弱点，一些企业仍使用这些解决方案，因为它们为多个用户注册表问题提供了一些缓解。

使用企业身份映射

EIM 体系结构描述企业中个人和实体之间的关系（例如文件服务器和打印服务器）以及企业内部很多代表他们的身份。此外，EIM 提供 API 集，允许应用程序查询关于这些关系的问题。

例如，在一个用户注册表中给出一个人的用户身份，您可以确定在另一个用户注册表中哪一个身份代表同一个用户。如果用户用一个身份认证，您可以把该身份映射到另一个用户注册表中相应的身份，用户不需要再次提供认证凭证。您只需要知道在另一个用户注册表中哪个身份代表该用户。因此，EIM 为企业提供概括的身份映射功能。

在不同注册表的用户身份之间映射的能力提供了许多益处。首先，应用程序具有这样的灵活性，它可以使用一个注册表来认证而使用一个完全不同的注册表来授权。例如，管理员可以将 SAP 身份映射到访问 SAP 资源。

身份映射需要管理员请执行以下操作:

1. 创建 EIM 标识符来表示企业中的人或实体。
2. 创建描述企业中现有用户注册表的 EIM 注册表定义。
3. 把那些注册表中用户身份之间的关系定义为他们创建的 EIM 标识符。

不需要更改现有注册表的代码。针对用户注册表中所有的用户不需要映射。EIM 允许一到多映射（换言之，一个单独的用户在一个单独的用户注册表中具有一个以上的身份）。EIM 也允许多到一映射（换言之，在一个单独的用户注册表中多个用户共享一个单独的身份，尽管支持该功能，但是为了安全性原因不建议使用）。在 EIM 中管理员可以提供任意类型的任意用户注册表。

EIM 不需要把现有的数据复制到新建的资源库并尝试保持两个副本同步。EIM 引入的唯一的新数据是关系信息。管理员在 LDAP 目录中的这些数据提供了这样的灵活性，可以在一个地方管理数据并在任何使用该信息的地方有副本。

有关“企业身份映射”的更多信息，请访问以下 Web 站点:

- http://publib.boulder.ibm.com/eserver/
- http://www.ibm.com/servers/eserver/security/eim/

第 15 章 Kerberos

Kerberos 是一种提供验证物理不安全网络上主体身份方法的网络认证服务。Kerberos 提供相互认证、数据完整性和保密性，是基于网络流量易受攻击以导致被捕获、检查和替换的情况下的现实假设。

Kerberos 凭单是验证身份的凭证。有两种类型的凭单: *授予凭单的凭单*和*服务凭单*。授予凭单的凭单针对的是初始标识请求。登录到主机系统时，需要能验证您的身份的凭证，例如密码或标记。具有授予凭单的凭单后，就可以使用授予凭单的凭单来为特定的服务请求服务凭单。这种两种凭单的方法称为 Kerberos 的*可信任第三方*。授予凭单的凭单向 Kerberos 服务器认证您的身份，而服务凭单是向服务安全地介绍您。

Kerberos 中的可信任第三方或媒介称为*密钥分发中心*（KDC）。KDC 向客户机发出所有 Kerberos 票据。

Kerberos 数据库保留每个主体的记录；记录包含关于每个主体的名称、专用密钥、主体的到期日及某些管理信息。主 KDC 包含数据库的主要副本，并将其发送到从属 KDC。

本章包含以下 Kerberos 信息:

- 『理解安全远程命令』
- 第 207 页的『使用 Kerberos 进行 AIX 认证』
- 第 211 页的『KRB5A 认证装入模块问题和故障查找信息』

理解安全远程命令

注:

1. 从“分布式计算环境”（DCE）V2.2 开始，DCE 安全服务器可以返回 Kerberos V5 票据。
2. 从 AIX 5.2 开始，所有安全远程命令（rcmds）使用由“网络认证服务”（NAS）V1.3 提供的 Kerberos V5 库。在 DCE 域中，**ftp** 命令使用 **libdce.a** DCE 库中的 GSSAPI 库，而在本地域中，**ftp** 命令使用 NAS V1.3 中的 GSSAPI 库。NAS V1.3 位于“扩展包 CD”中。唯一需要的 LPP 是 **krb5.client.rte** 文件集。
3. 如果迁移到 AIX 5.2，并且安装了 Kerberos V5 或 Kerberos V4，则安装脚本提示用户安装 **krb5.client.rte**。

安全 rcmds 是 **rlogin**、**rcp**、**rsh**、**telnet** 和 **ftp**。这些命令是大家共同所知的*标准 AIX* 方法。（该方法指 AIX 4.3 和更早发行版使用的认证方法。）所提供的其它方法是 Kerberos V5 和 Kerberos V4。

当使用 Kerberos V5 认证方法时，客户机从 DCE 安全服务器或 Kerberos 服务器获取 Kerberos V5 票据。该票据是用户当前 DCE 或本地凭证（对于所要连接的 TCP/IP 服务器是加密的）的一部分。TCP/IP 服务器上的守护程序对此票据解密。此操作允许 TCP/IP 服务器完全标识用户。如果允许票据中所述的 DCE 或本地主体访问操作系统用户帐户，则连接开始。安全 rcmds 支持 Kerberos V5 和 DCE 的 Kerberos 客户机和服务器。

除了认证客户机，Kerberos V5 将当前用户凭证转发到 TCP/IP 服务器。如果凭证标记成可转发的，客户机将它们作为 Kerberos 授予票据的票据（TGT）发送到服务器。在 TCP/IP 服务器端，如果用户正和 DCE 安全服务器通信，则守护程序使用 **k5dcecreds** 命令将 TGT 升级到完全的 DCE 凭证。

ftp 命令使用与其它安全 rcmds 不同的认证方法。它使用 GSSAPI 安全机制在 **ftp** 命令和 **ftpd** 守护程序之间传递认证。使用 **clear**、**safe** 和 **private** 子命令，**ftp** 客户机支持数据加密。

在操作系统客户机和服务器之间，**ftp** 命令允许加密数据连接的多字节传输。标准仅定义了加密数据连接的单字节传输。当连接到第三方机器并使用数据加密时，**ftp** 命令遵循单字节传输限制。

系统配置

对于所有安全 rcmds，系统级配置机制确定该系统中允许何种认证方法。配置控制输出和输入连接。

认证配置由 **libauthm.a** 库和 **lsauthent** 以及 **chauthent** 命令构成，提供对 **get_auth_methods** 和 **set_auth_methods** 库例程的命令行访问。

认证方法定义了何种方法用于通过网络认证用户。系统支持以下认证方法:

- Kerberos V5 是最普遍的方法，因为它是 DCE 的基础。
- Kerberos V4 仅由 **rlogin**、**rsh** 和 **rcp** 安全 rcmds 使用。它仅在 SP 系统中提供支持向后兼容性。Kerberos V4 票据不能升级到 DCE 凭证。
- 标准 AIX 是由 AIX 4.3 及更早发行版使用的认证方法。

如果配置了多于一个的认证方法，而第一个方法无法连接，则客户机尝试使用所配置的下一个认证方法来认证。

认证方法可以配置为任何次序。唯一的例外是标准 AIX 必须是所配置的最后的认证方法，因为没有后退选项。如果标准 AIX 不是所配置的认证方法，则不尝试密码认证，并且任何使用该方法的连接尝试都被拒绝。

可以不使用任何认证方法对系统进行配置。在这种情况下，机器拒绝所有使用安全 rcmds 来自和到达任何机器的连接。并且，因为 Kerberos V4 仅支持 **rlogin**、**rsh** 和 **rcp** 命令，所以配置为仅使用 Kerberos V4 的系统不允许使用 **telnet**、**ftp** 的连接。

Kerberos V5 用户验证

当使用 Kerberos V5 认证方法时，TCP/IP 客户机获取为 TCP/IP 服务器加密的服务票据。当服务器解密票据时，它具有识别用户的安全方法（通过 DCE 或本地主体）。然而，服务器仍然需要确定是否允许该 DCE 或本地主体访问本地帐户。将 DCE 或本地主体映射到本地操作系统帐户是由共享库 **libvaliduser.a**（它具有单独子例程，称为 kvalid_user）来处理的。如果首选了不同的映射方法，则系统管理员必须提供 **libvaliduser.a** 库的备用选择。

DCE 配置

要使用安全 rcmds，对于可以连接到的每个网络接口，必须存在两个 DCE 主体。它们是:

```
host/FullInterfaceName
ftp/FullInterfaceName
```

其中:

FullInterfaceName
接口名称和域名

本地配置

要使用安全 rcmds，对于可以连接到的每个网络接口，必须存在两个本地主体。它们是:

```
host/FullInterfaceName@Realmname
ftp/FullInterfaceName@Realmname
```

其中:

FullInterfaceName
接口名称和域名

RealmName

本地 Kerberos V5 域的名称

相关信息

- *AIX 5L Version 5.2 Technical Reference: Communications Volume 2* 中的 get_auth_method 和 set_auth_method 子例程
- *《AIX 5L V5.2 命令参考大全，卷 1》*中的 chauthent 命令
- *《AIX 5L V5.2 命令参考大全，卷 3》*中的 lsauthent 命令

使用 Kerberos 进行 AIX 认证

AIX 提供以下 Kerberos 认证装入模块: **KRB5** 和 **KRB5A**。尽管两种模块都进行 Kerberos 认证，但是 **KRB5** 装入模块执行 Kerberos 主体管理，而 **KRB5A** 装入模块不执行。**KRB5** 装入模块使用 IBM 网络认证服务的 Kerberos 数据库接口来操作 Kerberos 身份和主体。使用 **KRB5** 装入模块，AIX 系统管理员可以通过使用现有的 AIX 用户管理命令（而不需要任何更改）来管理 Kerberos 认证的用户及他们所关联的 Kerberos 主体。例如，要创建一个 AIX 用户和与该用户关联的 Kerberos 主体，请运行 **mkuser** 命令。

KRB5A 装入模块仅执行认证。Kerberos 主体管理是通过使用 Kerberos 主体管理工具分别完成。**KRB5A** 装入模块使用在这样一个环境下，在该环境中 Kerberos 主体存储在非 AIX 系统中并无法通过使用 Kerberos 数据库接口从 AIX 进行管理。例如，可以拥有一个 “Windows 2000 活动目录” 服务器，在该服务器中 Kerberos 主体管理是使用 “活动目录” 帐户管理工具和 API 来执行的。

使用 KRB5 安装和配置 Kerberos 集成登录系统

“网络认证服务”（IBM Kerberos 实现）是随 “扩展包” 一起提供的。要安装 Kerberos V5 客户机软件包，请安装 **krb5.client.rte** 文件集。要安装 Kerberos V5 服务器软件包，请安装 **krb5.server.rte** 文件集。要安装整个 Kerberos V5 软件包，请安装 **krb5** 软件包。

要避免 DCE 和 Kerberos 命令之间（即 **klist**、**kinit** 和 **kdestroy** 命令之间）的名称空间冲突，请将 Kerberos 命令安装在 **/usr/krb5/bin** 和 **/usr/krb5/sbin** 目录下。您可以将这些目录添加到 **PATH** 定义中。否则，要执行 Kerberos 命令，则必须指定全限定命令路径名。

“网络认证服务” 文档在 **krb5.doc.***lang.pdf|html* 软件包中提供，其中 *lang* 代表所支持的语言。

配置 Kerberos V5 KDC 和 kadmin 服务器

注:

1. 不推荐在同一物理系统中同时安装 DCE 和 Kerberos 服务器软件。如果必须这样做，则必须更改 DCE 客户机和服务器或 Kerberos 客户机和服务器的缺省可选互连网端口号。不论是在哪种情况下，这样的更改都可以影响环境中现有的 DCE 和 Kerberos 部署的互操作性。有关 DCE 和 Kerberos 共存的信息，请参考 “网络认证服务” 文档。
2. Kerberos V5 设置成拒绝从任何其时钟不在所指定的 KDC 最大时钟偏移内的主机来的凭单请求。最大时钟偏移的缺省值是 300 秒（5 分钟）。Kerberos 需要配置在服务器和客户机间的几种格式的时间同步。建议您用 **xntpd** 或 **timed** 守护程序使时间同步。要使用 **timed** 守护程序，请执行以下操作:
   a. 通过启动 **timed** 守护程序来将 KDC 服务器设置为时间服务器，如下所示:
      ```
      timed -M
      ```
   b. 在每个 Kerberos 客户机上启动 **timed** 守护程序。
      ```
      timed -t
      ```

要配置 Kerberos KDC 和 **kadmin** 服务器，请运行 **mkkrb5srv** 命令。例如，要为 MYREALM 域、sundial 服务器和 xyz.com 域配置 Kerberos，请输入以下内容:

```
mkkrb5srv -r MYREALM -s sundial.xyz.com -d xyz.com -a admin/admin
```

等待几秒钟，以使 **kadmind** 和 **krb5kdc** 命令从 **/etc/inittab** 启动。

运行 **mkkrb5srv** 命令产生以下操作:

1. 创建 **/etc/krb5/krb5.conf** 文件。域名值、Kerberos 管理服务器和域名都根据命令行中所指定的来设置。**/etc/krb5/krb5.conf** 文件还设置 **default_keytab_name**、**kdc** 和 **admin_server** 日志文件的路径。
2. 创建 **/var/krb5/krb5kdc/kdc.conf** 文件。**/var/krb5/krb5kdc/kdc.conf** 文件设置 **kdc_ports**、**kadmin_port**、**max_life**、**max_renewable_life**、**master_key_type** 和 **supported_enctypes** 变量的值。该文件还设置 **database_name**、**admin_keytab**、**acl_file**、**dict_file** 和 **key_stash_file** 变量的路径。
3. 创建 **/var/krb5/krb5kdc/kadm5.acl** 文件。设置 **admin**、**root** 和 **host** 主体的访问控制。
4. 创建数据库和一个 **admin** 主体。要求设置 Kerberos 主密钥并命名和设置 Kerberos 管理主体标识的密码。对于灾难恢复用途，安全地存储主密钥和管理主体标识及密码是很关键的。

有关更多信息，请参考第 209 页的『样本运行』和『错误消息和恢复操作』。

配置 Kerberos V5 客户机

Kerberos 安装完成后，不对常规用户显示正在使用 Kerberos 技术。操作系统的登录过程仍保持未更改。然而，现在用户可以拥有与他们所运行的过程关联的 Kerberos 授予凭单的凭单（TGT）。要配置系统使用 Kerberos 作为用户认证的主要方法，则请运行带有以下参数的 **mkkrb5clnt** 命令:

```
mkkrb5clnt -c KDC -r realm -a admin -s server -d domain -A -i database -K -T
```

例如，要配置 MYREALM 域、sundial.xyz.com 管理服务器、xyz.com 域和 files 数据库的 sundial.xyz.com KDC，请输入以下内容:

```
mkkrb5clnt -c sundial.xyz.com -r MYREALM -s sundial.xyz.com -d xyz.com -A -i files -K -T
```

先前的示例产生以下操作:

1. 创建 **/etc/krb5/krb5.conf** 文件。域名值、Kerberos 管理服务器和域名都与在命令行中所指定的一样。而且，更新 **default_keytab_name**、**kdc** 和 **kadmin** 日志文件的路径。
2. **-i** 标志配置完全集成登录。所进入的数据库是 Kerberos 主体所存储的位置。
3. **-K** 标志将 Kerberos 配置为缺省认证方案。这允许用户在登录时已经过 Kerberos 认证。
4. **-A** 标志在 “Kerberos 数据库” 中添加了一项，为 Kerberos 建立 root 管理用户。
5. **-T** 标志获取基于 TGT 管理凭单的服务器管理。

如果系统已安装，并位于与 KDC 不同的 DNS 域中，则必须执行以下的附加操作:

1. 编辑 **/etc/krb5/krb5.conf** 文件并在 **[domain realm]** 后添加另一项。
2. 将不同的域映射到您的域。

例如，如果希望将 abc.xyz.com 域中的客户机包含在您的 MYREALM 域中，则 **/etc/krb5/krb5.conf** 文件包含以下的附加项:

```
[domain realm]
     .abc.xyz.com = MYREALM
```

错误消息和恢复操作

使用 **mkkrb5srv** 命令时可能发生的错误包含以下这些:

- 如果 **krb5.conf**、**kdc.conf** 或 **kadm5.acl** 文件已经存在，则 **mkkrb5srv** 命令不修改该值。您将接收到一条文件已经存在的消息。通过编辑 **krb5.conf**、**kdc.conf** 或 **kadm5.acl** 文件可以更改任一配置值。
- 如果误输入并且没有创建数据库，则除去已创建的配置文件并重新运行该命令。
- 如果数据库和配置值不一致，则从 **/var/krb5/krb5kdc/*** 目录除去数据库并重新运行该命令。
- 请确保 **kadmind** 和 **krb5kdc** 守护程序已在机器上启动。使用 **ps** 命令来验证守护程序是否在运行。如果没有启动这些守护程序，请检查日志文件。

使用 **mkkrb5clnt** 命令时可能发生的错误包含以下这些:

- **krb5.conf** 的错误值可以通过编辑 **/etc/krb5/krb5.conf** 文件来修正。
- **-i** 标志的错误值可以通过编辑 **/usr/lib/security/methods.cfg** 文件来修正。

已创建的文件

mkkrb5srv 命令创建以下文件:

- **/etc/krb5/krb5.conf**
- **/var/krb5/krb5kdc/kadm5.acl**
- **/var/krb5/krb5kdc/kdc.conf**

mkkrb5clnt 命令创建以下文件:

- **/etc/krb5/krb5.conf**

mkkrb5clnt -i *文件*选项将以下节添加到 **/usr/lib/security/methods.cfg** 文件:

```
KRB5:
  program =
  options =
KRB5files:
  options =
```

样本运行

以下是 **mkkrb5srv** 命令的一个示例:

```
# mkkrb5srv -r MYREALM -s sundial.xyz.com -d xyz.com -a admin/admin
```

显示与以下内容相似的输出:

```
  文件集                          级别  状态       描述
  ----------------------------------------------------------------------------
路径: /usr/lib/objrepos
  krb5.server.rte            1.3.0.0  COMMITTED  网络认证服务
                                                 服务器

路径: /etc/objrepos
  krb5.server.rte            1.3.0.0  COMMITTED  网络认证服务
                                                 服务器

不支持 -s 选项。
管理服务器将是本地主机。
正在初始化配置...
正在创建 /etc/krb5/krb5.conf...
正在创建 /var/krb5/krb5kdc/kdc.conf...
正在创建数据库文件...
正在初始化“MYREALM”域的数据库“/var/krb5/krb5kdc/principal”
主密钥名称“K/M@MYREALM”
将提示您输入数据库的“主密码”。
注意一定不要忘记该密码。
输入数据库“主密码”:
```

```
重新输入数据库“主密码”以验证:
警告: 不要为 admin/admin@MYREALM; 指定策略
  缺省值为没有策略。注意策略可能会被
  ACL 限制覆盖。
输入主体“admin/admin@MYREALM”的密码:
重新输入主体“admin/admin@MYREALM”的密码:
主体“admin/admin@MYREALM”已创建。
正在创建密钥表...
正在创建 /var/krb5/krb5kdc/kadm5.acl...
正在启动 krb5kdc...
krb5kdc 已成功地启动。
正在启动 kadmind...
kadmind 已成功地启动。
命令成功地完成。
重新启动 kadmind and krb5kdc
```

以下是 **mkkrb5clnt** 命令的一个示例:

```
mkkrb5clnt -r MYREALM -c sundial.xyz.com -s sundial.xyz.com \
           -a admin/admin -d xyz.com -i files -K -T -A
```

显示与以下内容相似的输出:

```
正在初始化配置...
正在创建 /etc/krb5/krb5.conf...
命令成功完成。
admin/admin@MYREALM 的密码:
正在配置完全集成登录
正在将 admin/admin 主体与现有的凭证进行认证。
警告: 没有指定 host/diana.xyz.com@MYREALM 的策略;
  缺省值为没有策略。注意策略可能会被
  ACL 限制覆盖。
主体“host/diana.xyz.com@MYREALM”已经创建。

管理凭证“没有销毁”。
正在将 admin/admin 主体与现有的凭证进行认证。

管理凭证“没有销毁”。
正在将 admin/admin 主体与现有的凭证进行认证。
主体“kadmin/admin@MYREALM”已修改。

管理凭证“没有销毁”。
正在将 Kerberos 配置为缺省认证方案。
正在使 Kerberos 管理员成为 root 用户。
正在将 admin/admin 主体与现有的凭证进行认证。
警告: 没有指定 root/diana.xyz.com@MYREALM 的策略;
  缺省值为没有策略。注意策略可能被
  ACL 限制覆盖。
输入主体“root/diana.xyz.com@MYREALM”的密码:
重新输入主体“root/diana.xyz.com@MYREALM”的密码:
主体“root/diana.xyz.com@MYREALM”已创建。

管理凭证“没有销毁”。
正在清除管理员凭证并退出。
```

使用 KRB5A 安装和配置 Kerberos 集成登录系统

KRB5A 装入模块用于认证时，必须执行一系列步骤（如 Kerberos 主体的创建）。

以下部分解释了如何对“活动目录”KDC 进行“AIX 网络认证服务”客户机认证。

从“扩展包”安装 **krb5.client.rte** 文件集。

配置“Windows 2000 活动目录”服务器的 AIX Kerberos V5 客户机

使用 **config.krb5** 命令配置 AIX Kerberos 客户机。配置客户机需要 Kerberos 服务器信息。如果选择了 Windows 2000“活动目录”作为 Kerberos 服务器，则以下选项可以与 **config.krb5** 命令一起使用:

```
-r realm = Windows 2000“活动目录”服务器域名-d domain = 主管 Windows 2000 活动目录服务器机器的域名
-c KDC = KDC 服务器的主机名
-s server = Windows 2000 服务器的主机名
```

1. 如以下示例显示的来使用 **config.krb5** 命令:

   ```
   config.krb5 -C -r MYREALM -d xyz.com -c w2k.xyz.com -s w2k.xyz.com
   ```

2. Windows 2000 支持 DES-CBC-MD5 和 DES-CBC-CRC 加密类型。更改 **krb5.conf** 文件，使之包含类似于以下内容的信息:

   ```
   [libdefaults]
        default_realm = MYREALM
        default_keytab_name = FILE:/etc/krb5/krb5.keytab
        default_tkt_enctypes = des-cbc-crc des-cbc-md5
        default_tgs_enctypes = des-cbc-crc des-cbc-md5
   ```

3. 将以下节添加到 **methods.cfg** 文件:

   ```
   KRB5A:
     program = /usr/lib/security/KRB5A
     options = authonly
   KRB5Afiles:
     options = db=BUILTIN,auth=KRB5A
   ```

4. 请在 Windows 2000“活动目录”服务器上执行以下操作:
   a. 使用“活动目录管理”工具来为 *krbtest* AIX 主机创建新的用户帐户，如下所示:
      1) 选择“用户”文件夹。
      2) 使用鼠标右击**新建**。
      3) 选择**用户**。
      4) 输入名称 krbtest。
   b. 从命令行使用 **Ktpass** 命令创建键表文件并为 AIX 主机设置帐户。例如，要创建名为 **krbtest.keytab** 的键表文件，请输入:

      ```
      Ktpass -princ host/krbtest.xyz.com@MYREALM -mapuser krbtest -pass password -out krbtest.keytab
      ```

   c. 将键表文件复制到 AIX 主机系统。
   d. 如下所示将键表文件合并到 **/etc/krb5/krb5.keytab** 文件:

      ```
      $ ktutil
      ktutil: rkt krbtest.keytab
      ktutil: wkt /etc/krb5/krb5.keytab
      ktutil: q
      ```

   e. 使用“活动目录”用户管理工具创建 Windows 2000 域帐户。
   f. 如下创建与 Windows 2000 域帐户相符的 AIX 帐户，使得登录过程使用 Kerberos 认证:

      ```
      mkuser registry=KRB5Afiles SYSTEM=KRB5Afiles user0
      ```

KRB5A 认证装入模块问题和故障查找信息

以下节提供了 KRB5A“认证装入模块”问题和故障查找信息的答案。

如何配置 AIX Kerberos 客户机对活动目录服务器 KDC 进行认证

使用 **config.krb5** 命令配置 AIX Kerberos 客户机。配置客户机需要 Kerberos 服务器信息。如果选择了 Windows 2000“活动目录”服务器作为 Kerberos 服务器，则以下选项可以与 **config.krb5** 命令一起使用:

-r realm

“活动目录”域名

-d domain

主管“活动目录”目录服务的机器的域名

-c KDC

KDC 服务器的主机名

-s server

Windows 2000 服务器的主机名

如以下示例显示的内容来使用 **config.krb5** 命令:

```
config.krb5 -C -r MYREALM -d xyz.com -c w2k.xyz.com -s w2k.xyz.com
```

Windows 2000 支持 DES-CBC-MD5 和 DES-CBC-CRC 加密类型。更改 **krb5.conf** 文件使之包含与以下内容类似的信息:

```
 [libdefaults]
      default_realm = MYREALM
      default_keytab_name = FILE:/etc/krb5/krb5.keytab
      default_tkt_enctypes = des-cbc-crc des-cbc-md5
      default_tgs_enctypes = des-cbc-crc des-cbc-md5
```

将以下节添加到 **methods.cfg** 文件:

```
KRB5A:
  program = /usr/lib/security/KRB5A
  options = authonly
KRB5Afiles:
  options = db=BUILTIN,auth=KRB5A
```

请在“活动目录”服务器上执行以下操作:

1. 使用“活动目录管理”工具为 *krbtest* AIX 主机创建新的用户帐户。
   - 选择“用户”文件夹。
   - 用鼠标右键单击，并选择“新建”。
   - 选择用户。
   - 输入名称 *krbtest*。
2. 从命令行使用 **Ktpass** 命令创建 krbtest.keytab 文件并为 AIX 主机设置帐户，如下所示:

   ```
   Ktpass -princ host/krbtest.xyz.com@MYREALM -mapuser krbtest -pass password \
          -out krbtest.keytab
   ```
3. 将 krbtest.keytab 文件复制到 AIX 主机系统。
4. 将 krbtest.keytab 文件合并到 **/etc/krb5/krb5.keytab** 文件中，如下所示:

   ```
   $ ktutil
   ktutil: rkt krbtest.keytab
   ktutil: wkt /etc/krb5/krb5.keytab
   ktutil: q
   ```
5. 使用“活动目录”用户管理工具创建 Windows 2000 域帐户。
6. 创建与 Windows 2000 域帐户相符的 AIX 帐户，使得登录过程知道使用 Kerberos 认证，如下所示:

   ```
   mkuser registry=KRB5Afiles SYSTEM=KRB5Afiles user0
   ```

如何修改 Kerberos 集成登录的 AIX 配置

要启用 Kerberos 集成登录，请修改 **methods.cfg** 文件。必须将复合装入模块项添加到 **methods.cfg** 文件中。认证方是 KRB5A。数据库方可以选择 BUILTIN 或 LDAP 其中之一。BUILTIN 是使用 ASCII 文件的标准 AIX 用户帐户库。例如，如果选择 BUILTIN 作为 AIX 用户帐户库，则如下所示修改 **methods.cfg** 文件:

示例: 选择本地文件系统作为 AIX 用户帐户库。

```
KRB5A:
 program = /usr/lib/security/KRB5A
 options=authonly

KRB5Afiles:
 options = db=BUILTIN,auth=KRB5A
```

示例: 选择 LDAP 作为 AIX 用户帐户库。

```
KRB5A:
 program = /usr/lib/security/KRB5A
 options=authonly

LDAP:
  program = /usr/lib/security/LDAP

KRB5ALDAP:
 options = auth=KRB5A,db=LDAP
```

如何创建带有 KRB5A 装入模块的 Kerberos 集成登录的 AIX 用户

要创建带有 KRB5A 装入模块的 Kerberos 集成登录的 AIX 用户，请如下使用 **mkuser** 命令:

```
mkuser registry=KRB5Afiles SYSTEM=KRB5Afiles auth_domain=MYREALM foo
```

有关 **auth_name** 和 **auth_domain** 属性的使用信息，请参考第 214 页的『auth_name 和 auth_domain 属性的用途』。

如何在活动目录上创建 Kerberos 主体

正在创建的 Windows 2000 用户帐户隐含地创建了主体。例如，如果在“活动目录”上创建名为 foo 的用户帐户，则也创建了与 foo 关联的主体 foo@MYREALM。有关在“活动目录”上创建用户的信息，请参阅“活动目录”用户管理文档。

如何更改 Kerberos 认证用户的密码

要更改 Kerberos 认证用户的密码，请如下使用 **passwd** 命令:

```
passwd -R KRB5Afiles foo
```

如何除去 Kerberos 认证用户

要除去 Kerberos 认证用户，请使用 **rmuser** 命令。然而，这仅从 AIX 中除去用户。还必须使用“活动目录”用户管理工具将该用户从“活动目录”中除去。

```
passwd -R KRB5Afiles foo
```

如何将 AIX 用户迁移到 Kerberos 认证用户

如果用户已在“活动目录”上有一个帐户，则 **chuser** 命令将该用户转换成 Kerberos 认证用户，如以下示例所示:

```
chuser registry=KRB5Afiles SYSTEM=KRB5Afiles auth_domain=MYREALM foo
```

如果用户在“活动目录”中没有帐户，则在“活动目录”中创建一个帐户。然后使用 **chuser** 命令。“活动目录”帐户可能有（也可能没有）相同的 AIX 用户名。如果选择了不同的名称，则使用 **auth_name** 属性来映射到“活动目录”名。例如，要将 chris AIX 用户名映射到 christopher“活动目录”用户名，请输入以下内容:

```
chuser registry=KRB5Afiles SYSTEM=KRB5Afiles auth_name=christopher auth_domain=MYREALM chris
```

如果忘记了密码该怎样做

在“活动目录”上，密码必须由管理员更改。在 AIX 上，root 用户不能设置 Kerberos 主体的密码。

auth_name 和 auth_domain 属性的用途

auth_name 和 **auth_domain** 属性用于将 AIX 用户名映射到“活动目录”上的 Kerberos 主体名称。例如，如果 chris AIX 用户具有 auth_name=christopher 和 auth_domain=SOMEREALM，则 Kerberos 主体名称是 christopher@SOMEREALM。SOMEREALM 域名和 MYREALM 缺省域名不相同。这允许 chris 用户进行 SOMEREALM 域的认证，而不是进行 MYREALM 域的认证。

Kerberos 认证过的用户是否可以变成使用标准 AIX 认证的认证

答案是肯定的。执行以下操作使用 AIX 认证来认证 Kerberos 认证用户:

1. 用户使用 **passwd** 命令设置 AIX 密码（**/etc/security/passwd**），如下所示:

   ```
   passwd -R files foo
   ```

2. 更改用户的 **SYSTEM** 属性，如下所示:

   ```
   chuser -R KRB5Afiles SYSTEM=compat foo.
   ```

   这将认证从 Kerberos 更改到 crypt。

如果希望使用 crypt 认证作为备份机制，请如下更改 **SYSTEM** 属性:

```
chuser -R KRB5Afiles SYSTEM="KRB5Afiles or compat" foo.
```

使用 Windows 2000 活动目录服务器时是否需要在 AIX 上设置 Kerberos 服务器（KDC）

不需要，因为用户对“活动目录”KDC 是经认证的，所以没有必要配置 AIX 上的 KDC。相反，如果希望更改“AIX 网络认证服务 KDC”作为 Kerberos 服务器使用，则需要配置 Kerberos 服务器。

AIX 不接受我的密码

检查密码是否符合 AIX 和 Kerberos 的要求。KDC 还必须正确配置并正常运行。

不能登录到系统

- 验证 KDC 是否已启动并正在运行。
  - 在 AIX 系统中，输入以下内容:

    ```
    ps -ef | grep krb5kdc
    ```

  - 在 Windows 2000 系统中，请执行以下操作:
    1. 在“控制面板”中，双击“管理工具”图标
    2. 双击“服务”图标。
    3. 验证“Kerberos 密钥分发中心”是否在已启动状态。

- 在 AIX 系统中，验证 **/etc/krb5/krb5.conf** 文件是否指向正确的 KDC，并且是否具有有效的参数。
- 在 AIX 系统中，验证客户机键表文件是否包含主机凭单。例如，假定您已有 **/etc/krb5/krb5.keytab** 缺省键表文件。输入以下内容:

```
$ ktutil
ktutil: rkt /etc/krb5/krb5.keytab
ktutil: l

槽     KVNO   主体
------ ------ --------------------------------------------------------
     1      4 host/krbtest.xyz.com@MYREALM

ktutil: q
```

- 如果设置了 **auth_name** 和 **auth_domain** 属性，则验证它们是否引用 ADS KDC 上有效的主体名称。
- 验证 **SYSTEM** 属性是否设置为 Kerberos 登录（**KRB5Afiles** 或 **KRB5ALDAP**）。
- 验证密码没有到期。

第 3 部分 附录

附录 A. 安全性核对表

本附录提供一份在新安装或现有系统上执行的安全性操作核对表。尽管本列表不是一份完整的安全性核对表，它可以作为基础来为环境构建安全性核对表。

- 当安装新系统时，从安全基本介质来安装 AIX。安装时执行以下步骤:
  - 不要在服务器上安装桌面软件，例如 CDE、GNOME 或 KDE。
  - 安装必要安全性修正和任何推荐的维护级修正。要了解最新的服务公告、安全性建议和修正信息，请参阅 eServer pSeries Support Fixes Web 站点（http://techsupport.services.ibm.com/server/fixes?view=pSeries）。
  - 初始安装后备份系统，并将系统备份存储在安全位置。
- 为受限制的文件和目录建立访问控制列表。
- 禁用不需要的用户帐户和系统帐户，例如 daemon、bin、sys、adm、lp 和 uucp。不推荐删除帐户，因为这将删除帐户信息，例如用户标识和用户名，它们也许仍与系统备份中的数据相关联。如果使用先前已删除的用户标识创建一个用户，并且在系统上恢复了系统备份，新建用户可能拥有对已恢复的系统的意外访问权。
- 定期检查 **/etc/inetd.conf**、**/etc/inittab**、**/etc/rc.nfs** 和 **/etc/rc.tcpip** 文件，并除去所有不必要的守护程序和服务。
- 验证以下文件的许可权设置正确:

```
-rw-rw-r-- root     system  /etc/filesystems
-rw-rw-r-- root     system  /etc/hosts
-rw------- root     system  /etc/inittab
-rw-r--r-- root     system  /etc/vfs
-rw-r--r-- root     system  /etc/security/failedlogin
-rw-rw---- root     audit   /etc/security/audit/hosts
```

- 禁止 root 帐户使其不能远程登录。root 帐户应该只能从系统控制台登录。
- 启用系统审计过程。要了解更多信息，请参阅第 49 页的第 3 章，『审计』。
- 启用登录控制策略。要了解更多信息，请参阅第 20 页的『登录控制』。
- 禁止运行 **xhost** 命令的用户许可权。要了解更多信息，请参阅第 23 页的『管理 X11 和 CDE 注意事项』。
- 防止对 **PATH** 环境变量的未授权更改。要了解更多信息，请参阅第 31 页的『PATH 环境变量』。
- 禁用 telnet、rlogin 和 rsh。要了解更多信息，请参阅第 119 页的第 9 章，『TCP/IP 安全性』。
- 建立用户帐户控制。要了解更多信息，请参阅第 30 页的『用户帐户控制』。
- 强制严格的密码策略。要了解更多信息，请参阅第 40 页的『密码』。
- 为用户帐户建立磁盘配额。要了解更多信息，请参阅第 46 页的『从超配额情形中恢复』。
- 仅允许管理帐户使用 **su** 命令。监视 **/var/adm/sulog** 文件中 **su** 命令的记录。
- 使用 X-Windows 时启用屏幕锁定。
- 限制对 **cron** 和 **at** 命令的访问，只给那些需要访问它们的帐户访问权。
- 使用 **ls** 命令的别名以显示隐藏文件和文件名中的隐藏字符。
- 使用 **rm** 命令的别名以避免从系统中意外删除文件。
- 禁用不必要的网络服务。要了解更多信息，请参阅第 127 页的第 10 章，『网络服务』。
- 执行常见的系统备份并验证备份的完整性。
- 订阅安全相关的电子邮件分发列表。

附录 B. 安全性参考资料

本附录提供多方面的安全相关的参考资料信息。

安全性 Web 站点

AIX Virtual Private Networks: http://www-1.ibm.com/servers/aix/products/ibmsw/security/vpn/index.html

CERIAS（Center for Education and Research in Information Assurance and Security）: http://www.cerias.purdue.edu/

CERT（Computer Emergency Response Team, 在 Carnegie Mellon University 中）: http://www.cert.org

CIAC（Computer Incident Advisory Capability）: http://ciac.llnl.gov

Computer Security Resource Clearinghouse: http://csrc.ncsl.nist.gov/

FIRST（Forum of Incident Response and Security Teams）: http://www.first.org/

IBM eServer Security Planner: http://www-1.ibm.com/servers/security/planner/

IBM Security Solutions: http://www-3.ibm.com/security/index.shtml

OpenSSH: http://www.openssh.org/

安全性邮递列表

CERT: http://www.cert.org/contact_cert/certmaillist.html

IBM eServer pSeries Support Subscription Service: https://techsupport.services.ibm.com/server/pseries.subscriptionSvcs

comp.security.unix: news:comp.security.unix

安全性联机参考资料

Common Criteria Concepts FAQ: http://www.radium.ncsc.mil/tpep/process/faq-sect3.html

Rainbow Series Library: http://www.radium.ncsc.mil/tpep/library/rainbow/

faqs.org: http://www.faqs.org/faqs/computer-security/

IBM eServer pSeries 信息中心: http://publib16.boulder.ibm.com/pseries/zh_CN/infocenter/base

附录 C. 普通 AIX 系统服务摘要

下表列出 AIX 中更加普通的系统服务。使用此表来识别保护系统的启动点。

在进行保护系统之前，备份所有的原始配置文件，特别是:

- **/etc/inetd.conf**
- **/etc/inittab**
- **/etc/rc.nfs**
- **/etc/rc.tcpip**

服务	守护程序	如下启动	功能	注释
inetd/bootps	inetd	/etc/inetd.conf	用于无盘客户机的 bootp 服务	• 对于“网络安装管理”（NIM）和系统远程引导是必需的 • 与 tftp 一起工作 • 在大多数情况下禁用
inetd/chargen	inetd	/etc/inetd.conf	字符发生器（仅测试）	• 可用作 TCP 与 UDP 服务 • 为“拒绝服务”攻击提供机会 • 除非正在测试网络，否则禁用
inetd/cmsd	inetd	/etc/inetd.conf	日历服务（CDE 使用）	• 以 root 用户身份运行，因此涉及安全性 • 除非用 CDE 申请该服务，否则禁用 • 在库房数据库服务器上禁用
inetd/comsat	inetd	/etc/inetd.conf	通知接收的电子邮件	• 以 root 用户身份运行，因此涉及安全性 • 很少需要的 • 禁用
inetd/daytime	inetd	/etc/inetd.conf	废弃时间服务（仅测试）	• 以 root 用户身份运行 • 可用作 TCP 与 UDP 服务 • 为“拒绝服务 PING”攻击提供机会 • 废弃服务并仅对测试使用 • 禁用
inetd/discard	inetd	/etc/inetd.conf	/dev/null service（仅测试）	• 可用作 TCP 与 UDP 服务 • 在“拒绝服务攻击”中使用 • 废弃服务并仅对测试使用 • 禁用

服务	守护程序	如下启动	功能	注释
inetd/dtspc	inetd	/etc/inetd.conf	CDE 子过程控制	• 此服务由 **inetd** 守护程序自动启动以响应 CDE 客户机，该客户机请求在守护程序的主机上启动进程。这使它易受攻击 • 在没有 CDE 的库房数据库服务器上禁用 • 没有该服务 CDE 可能会起作用 • 除非绝对需要，否则禁用
inetd/echo	inetd	etc/inetd.conf	回传服务（只测试）	• 可用作 TCP 与 UDP 服务 • 可用于“拒绝服务或 Smurf”攻击 • 用于回送信号给其他人从而穿过防火墙或启动数据传输 • 禁用
inetd/exec	inetd	/etc/inetd.conf	远程执行服务	• 以 root 用户身份运行 • 要求输入无保护传递的用户标识和密码 • 该服务是非常容易遭到监听的 • 禁用
inetd/finger	inetd	/etc/inetd.conf	在用户处进行取数	• 以 root 用户身份运行 • 给出有关您的系统与用户的信息 • 禁用
inetd/ftp	inetd	/etc/inetd.conf	文件传输协议	• 以 root 用户身份运行 • 用户标识与口令未加保护地传送，因此易受监听 • 禁用此服务并使用公共安全 shell 套件
inetd/imap2	inetd	/etc/inetd.conf	因特网邮件访问协议	• 确保您正使用该服务器的最新版本 • 只当您运行邮件服务器时才必需。否则，禁用 • 用户标识与密码未加保护地传递
inetd/klogin	inetd	/etc/inetd.conf	Kerberos 登录	• 如果您的站点使用 Kerberos 认证则启用
inetd/kshell	inetd	/etc/inetd.conf	Kerberos shell	• 如果您的站点使用 Kerberos 认证则启用
inetd/login	inetd	/etc/inetd.conf	rlogin 服务	• 易于遭受 IP 欺骗与 DNS 欺骗 • 数据（包括用户标识与密码）未加保护地传递 • 以 root 用户身份运行 • 使用安全 shell 代替该服务

服务	守护程序	如下启动	功能	注释
inetd/netstat	inetd	/etc/inetd.conf	当前网络状态报告	• 如在您的系统上运行，可能潜在地把网络信息给黑客 • 禁用
inetd/ntalk	inetd	/etc/inetd.conf	允许用户相互交谈	• 以 root 用户身份运行 • 不需要产品或库房服务器 • 除非绝对需要，否则禁用
inetd/pcnfsd	inetd	/etc/inetd.conf	PC NFS 文件服务	• 如果不是当前在使用则禁用服务 • 如果需要与此类似的服务，考虑 Samba，pcnfsd 守护程序早于 Microsoft 的 SMB 规范的发行版
inetd/pop3	inetd	/etc/linetd.conf	邮局协议	• 用户标识与密码未加保护地发送 • 如果您的系统是邮件服务器并且拥有使用仅支持 POP3 的应用程序的客户机时才需要 • 如果您的客户机使用 IMAP，则用其作为替代，或使用 POP3 服务。该服务有安全套接字层（SSL）报文封装 • 如果您不在运行邮件服务器或有需要 POP 服务的客户机，则禁用
inetd/rexd	inetd	/etc/inetd.conf	远程执行	• 以 root 用户身份运行 • 用 **on** 命令监视 • 禁用的服务 • 使用 **rsh** 与 **rshd** 作为替代
inetd/quotad	inetd	/etc/inetd.conf	文件限额的报告（对于 NFS 客户机）	• 如果您正在运行 NFS 文件服务才需要 • 除非需要对 **quota** 命令提供应答，否则禁用该服务 • 如果需要使用该服务，保持该服务的所有的补丁和修正包为最新的
inetd/rstatd	inetd	/etc/inetd.conf	内核统计信息服务器	• 如果需要监视系统，使用 SNMP 并禁用该服务 • 需要使用 **rup** 命令
inetd/rusersd	inetd	/etc/inetd.conf	关于用户登录的信息	• 这不是基本的服务。禁用 • 以 root 用户身份运行 • 给出系统上当前用户的列表并用 **rusers** 监视

服务	守护程序	如下启动	功能	注释
inetd/rwalld	inetd	/etc/inetd.conf	写给所有用户	• 以 root 用户身份运行 • 如果系统有交互式用户，可能需要保持该服务 • 如果系统为产品或数据库服务器，这就不需要 • 禁用
inetd/shell	inetd	/etc/inetd.conf	rsh 服务	• 如可能则禁用该服务。使用“安全 shell”作为替代 • 如果必须使用该服务，则使用 TCP 护封来停止电子欺骗与限制暴露 • 需要 **Xhier** 软件分布程序
inetd/sprayd	inetd	/etc/inetd.conf	RPC 喷射测试	• 以 root 用户身份运行 • 可能不需要 NFS 网络问题的诊断 • 如果不在运行 NFS 则禁用
inetd/systat	inetd	/etc/inted.conf	“ps -ef”状态报告	• 允许远程站点察看系统上的进程状态 • 该服务缺省情况下禁用。必须周期性地检查来确保未启用该服务
inetd/talk	inetd	/etc/inetd.conf	在网上两个用户间建立分区屏幕	• 不是必需服务 • 与 **talk** 命令一起使用 • 在端口 517 提供 UDP 服务 • 除非对于 UNIX 用户您需要多个交互式交谈会话，否则禁用
inetd/ntalk	inetd	/etc/inetd.conf	“new talk”在网上两个用户间建立分区屏幕	• 不是必需服务 • 与 **talk** 命令一起使用 • 在端口 517 提供 UDP 服务 • 除非对于 UNIX 用户您需要多个交互式交谈会话，否则禁用
inetd/telnet	inetd	/etc/inetd.conf	telnet 服务	• 支持远程登录会话，但未加保护地传递密码和标识 • 如果可能，禁用该服务并使用远程访问“安全 shell”作为替代
inetd/tftp	inetd	/etc/inetd.conf	琐碎文件传送	• 在端口 69 提供 UDP 服务 • 以 root 用户身份运行并且可能危及安全 • 由 NIM 使用 • 除非您正使用 NIM 或必须引导无盘工作站，否则禁用

服务	守护程序	如下启动	功能	注释
inetd/time	inetd	/etc/inetd.conf	废弃时间服务	• 由 **rdate** 命令使用的 **inetd** 的内部功能。 • 可用作 TCP 与 UDP 服务 • 有时在引导时用于同步时钟 • 该服务是过时的。使用 **ntpdate** 作为替代 • 只有在您禁用该服务来测试系统而未发现问题之后，才能禁用该服务
inetd/ttdbserver	inetd	/etc/inetd.conf	工具 - 交谈数据库服务器（用于 CDE）	• **rpc.ttdbserverd** 以 root 用户身份运行，且可能危及安全 • 为 CDE 规定作为需要的服务，但 CDE 没有它也能工作 • 不应该在库房服务器或涉及安全性的任何系统上运行
inetd/uucp	inetd	/etc/inetd.conf	UUCP 网络	• 除非有使用 UUCP 的应用程序，否则禁用
inittab/dt	init	/etc/rc.dt script in the /etc/inittab	桌面登录到 CDE 环境	• 在控制台启动 X11 服务器 • 支持 “X11 显示管理员控制协议”（xdcmp），这样其它 X11 站能登录到同一机器 • 应该只在个人工作站使用服务。避免把它用于库房系统
inittab/dt_nogb	init	/etc/inittab	桌面登录到 CDE 环境（无图形引导）	• 直到系统充分地启动后才有图形显示 • 与 **inittab/dt** 涉及内容相同
inittab/httpdlite	init	/etc/inittab	用于 **docsearch** 命令的 Web 服务器	• 文档搜索引擎的缺省 Web 服务器 • 除非您的机器是文档服务器，否则禁用
inittab/i4ls	init	/etc/inittab	许可证管理员服务器	• 针对开发机器启用 • 针对生产机器禁用 • 针对有许可证需要的库房数据库机器启用 • 为编译器、数据库软件或任何其它得到许可的产品提供支持
inittab/imnss	init	/etc/inittab	**docsearch** 命令的搜索引擎	• 用于文档搜索引擎的缺省 Web 服务器的一部分 • 除非您的机器是文档服务器，否则禁用

服务	守护程序	如下启动	功能	注释
inittab/imqss	init	/etc/inittab	用于“文档搜索”的搜索引擎	• 用于文档搜索引擎的缺省 Web 服务器的一部分 • 除非您的机器是文档服务器，否则禁用
inittab/lpd	init	/etc/inittab	BSD 行式打印机界面	• 从其它的系统接受打印作业 • 可以禁用该服务但仍然发送作业到打印服务器 • 在确认打印不受影响后，禁用该服务
inittab/nfs	init	/etc/inittab	网络文件系统/网络信息服务	• 基于建立在 UDP/RPC 上的 NFS 与 NIS 服务 • 认证是最小的 • 对库房机器禁用此项
inittab/piobe	init	/etc/inittab	打印机 I/O 后端（用于打印）	• 处理由 **qdaemon** 提交的作业的调度、假脱机与打印 • 如果因为您正发送打印作业到服务器而不从您的系统打印，则禁用
inittab/qdaemon	init	/etc/inittab	将守护程序排入队列（用于打印）	• 提交打印作业到 **piobe** 守护程序 • 如果不从系统打印则禁用
inittab/uprintfd	init	/etc/inittab	内核消息	• 通常不是必需的 • 禁用
inittab/writesrv	init	/etc/inittab	写注释到 ttys	• 只由交互式的 UNIX 工作站用户使用 • 对服务器、库房数据库与开发机器禁用该服务 • 对工作站启用该服务
inittab/xdm	init	/etc/inittab	传统的“X11 显示管理”	• 请不要在库房生产或数据库服务器上运行 • 请不要在开发系统上运行，除非 X11 显示管理是需要的 • 如果需要图形，则可以在工作站上运行
rc.nfs/automountd		/etc/rc.nfs	自动文件系统	• 如果使用 NFS，为工作站启用该服务 • 不要把自动安装器用于开发或库房服务器
rc.nfs/biod		/etc/rc.nfs	阻拦 IO 守护程序（NFS 服务器所必需的）	• 只为 NFS 服务器启用 • 如果不是 NFS 服务器，连同 **nfsd** 与 **rpc.mountd** 禁用该服务

服务	守护程序	如下启动	功能	注释
rc.nfs/keyserv		/etc/rc.nfs	安全 RPC 密钥服务器	• 管理安全 RPC 所需要的密钥 • 对 NIS+ 来说很重要 • 如果您不在使用 NFS、NIS 与 NIS+，则禁用此服务
rc.nfs/nfsd		/etc/rc.nfs	NFS 服务（NFS 服务器所所必需的）	• 认证为弱 • 能提供其本身堆栈帧崩溃 • 如果在 NFS 文件服务器上则启用 • 如果禁用该服务，那么一起禁用 **biod**、**nfsd** 与 **rpc.mountd**
rc.nfs/rpc.lockd		/etc/rc.nfs	NFS 文件锁定	• 如果不在使用 NFS，禁用此服务 • 如果不通过网络使用文件锁定则禁用此服务 • 在 “SANS 十种最大安全性威胁” 中提到 **lockd** 守护程序
rc.nfs/rpc.mountd		/etc/rc.nfs	NFS 文件安装（NFS 服务器所必需的）	• 认证为弱 • 能提供其本身堆栈帧崩溃 • 应该仅在 NFS 文件服务器上启用 • 如果禁用该服务，那么一起禁用 **biod** 与 **nfsd**
rc.nfs/rpc.statd		/etc/rc.nfs	NFS 文件锁定（来恢复它们）	• 通过 NFS 实现文件锁定 • 除非在使用 NFS 否则禁用该服务
rc.nfs/rpc.yppasswdd		/etc/rc.nfs	NIS 密码守护程序（用于 NIS 主控机）	• 用来操作本地密码文件 • 只有当有问题的机器是 NIS 主控机时才是必需的，在所有其它情况下禁用
rc.nfs/ypupdated		/etc/rc.nfs	NIS 更新守护程序（用于 NIS 从属机）	• 接收由 NIS 主控机推进的 NIS 数据库映射 • 只有当有问题的机器是主 NIS 服务器的 NIS 从属机时才是必需的
rc.tcpip/autoconf6		/etc/rc.tcpip	IPv6 界面	• 除非在运行 IPV6，否则禁用
rc.tcpip/dhcpcd		/etc/rc.tcpip	动态主机配置协议（客户机）	• 库房服务器不应该依赖于 DHCP。禁用该服务 • 如果主机不在使用 DHCP，则禁用
rc.tcpip/dhcprd		/etc/rc.tcpip	动态主机配置协议（中继	• 夺取 DHCP 广播并发送它们到另一网络的服务器 • 在路由器上查找到的服务的副本 • 如果不在使用 DHCP 或依赖于在网络间发送信息，则禁用

服务	守护程序	如下启动	功能	注释
rc.tcpip/dhcpsd		/etc/rc.tcpip	动态主机配置协议（服务器	• 在引导时从客户机应答 DHCP 请求；给予客户机信息，例如 IP 名称、号码、网掩码、路由器与广播地址 • 如果不在使用 DHCP ，则禁用该服务 • 在生产与库房服务器连同不在使用 DHCP 的主机上禁用
rc.tcpip/dpid2		/etc/rc.tcpip	过期的 SNMP 服务	• 除非需要 SNMP，否则禁用
rc.tcpip/gated		/etc.rc.tcpip	接口间控制的路由	• 仿真路由器功能 • 禁用该服务并使用 RIP 或路由器替代
rc.tcpip/inetd		/etc/rc.tcpip	inetd 服务	• 彻底地保护系统则可以禁用该服务，但这通常是不实际的 • 禁用该服务会禁用一些邮件与 Web 服务器需要的远程 shell 服务
rc.tcpip/mrouted		/etc/rc.tcpip	多播路由	• 仿真路由器在网段间发送多点广播信息包的功能 • 禁用此服务。使用路由器替代
rc.tcpip/names		/etc/rc.tcpip	DNS 名称服务器	• 只有如果您的机器是 DNS 名称服务器的话，使用此项 • 对工作站、开发与生产机器禁用
rc.tcpip/ndp-host		/etc/rc.tcpip	IPv6 主机	• 禁用，除非使用 IPV6
rc.tcpip/ndp-router		/etc/rc.tcpip	IPv6 路由	• 禁用，除非使用 IPV6。考虑使用路由器替代 IPv6
rc.tcpip/portmap		/etc/rc.tcpip	RPC 服务	• 必需的服务 • RPC 服务器用 **portmap** 守护程序注册。需要定位 RPC 服务的客户机要求 **portmap** 守护程序告诉它们特定的服务位于何处 • 只有当您已成功减少 RPC 服务，从而唯一剩余的是 **portmap** 时，禁用
rc.tcpip/routed		/etc/rc.tcpip	接口间的 RIP 路由	• 仿真路由器功能 • 禁用如果您有用于网络间的信息包的路由器
rc.tcpip/rwhod		/etc/rc.tcpip	远程 “who” 守护程序	• 收集并广播数据来监视同一网络上的服务器 • 禁用该服务

服务	守护程序	如下启动	功能	注释
rc.tcpip/sendmail		/etc/rc.tcpip	邮件服务	• 以 root 用户身份运行 • 禁用该服务，除非该机器用作邮件服务器 • 如果禁用，那么做以下的一项: – 在 crontab 放置一项来清除队列。使用 **/usr/lib/sendmail -q** 命令 – 配置 DNS 服务器，从而传送服务器的邮件到某些其它的系统
rc.tcpip/snmpd		/etc/rc.tcpip	简单网络管理协议	• 如果您不在通过 SNMP 工具监视该系统，则禁用 • 在关键服务器上可能需要 SNMP
rc.tcpip/syslogd		/etc/rc.tcpip	事件的系统日志	• 不建议禁用该服务 • 倾向于拒绝服务攻击 • 任何系统必需
rc.tcpip/timed		/etc/rc.tcpip	旧的时间守护程序	• 禁用该服务并使用 xntp 代替
rc.tcpip/xntpd		/etc/rc.tcpip	新的时间守护程序	• 在 sync 中保持系统上的时钟 • 禁用该服务。 • 配置其它系统为时间服务器并通过使用调用 ntpdate 的 cron 作业让其它系统与其同步
dt login		/usr/dt/config/Xaccess	未限制的 CDE	• 如果不提供 CDE 登录到 X11 站的组，可以限制 dtlogin 到控制台。
匿名 FTP 协议服务		user rmuser -p <username>	匿名 FTP 协议	• 匿名 FTP 协议能力使您不能跟踪某个特定用户 FTP 的使用 • 如果用户帐户存在，则除去用户 ftp，按如下操作: **rmuser -p ftp** • 通过将 **/etc/ftpusers** 文件（带有那些不可以使用 ftp 的用户的列表）植入系统可以获得更高的安全性

服务	守护程序	如下启动	功能	注释
匿名 FTP 写入			匿名 ftp 上载	• 没有文件属于 ftp。 • FTP 匿名上载允许在系统上安置处理不当代码的潜能。 • 把那些您想要禁止的用户的名称放到 **/etc/ftpusers** 文件 • 一些系统创建的用户（您可能想要禁止通过 FTP 匿名上载到系统的用户）的示例是： root、daemon、bin.sys、 admin.uucp、guest、nobody、 lpd、nuucp、ladp、 imnadm • 更改 **ftpusers** 文件的所有者和组权限，按如下所示：**chown root:system /etc/ftpusers** • 更改 **ftpusers** 文件的许可权，使之为更严格的设置，如下所示：**chmod 644 /etc/ftpusers**
ftp.restrict			ftp 到系统帐户	• 不应该允许外部用户通过 **ftpusers** 文件替换 root 文件
root.access		/etc/security/user	rlogin/telnet 到 root 帐户	• 在 **etc/security/user** 文件设置 rlogin 选项为 false • 以 root 用户身份登录的任何人应该先以自己的名称登录，然后将 **su** 改为 root；这提供了审计跟踪
snmpd.readWrite		/etc/snmpd.conf	SNMP 读写团体	• 如果不在使用 SNMP，则禁用 SNMP 守护程序。 • 在 **/etc/snmpd.conf** 文件中禁用团体 private 与团体 system • 对那些正监视您系统的 IP 地址限制 “public” 团体
syslog.conf			配置 syslogd	• 如果还未配置 **/etc/syslog.conf**，则禁用该守护程序 • 如果正使用 **syslog.conf** 来记录系统信息，则保持它是启用的

附录 D. 网络服务选项摘要

为使系统安全性达到较高级别，可以使用 0 禁用和 1 启用来更改几个网络选项。以下列表标识了这些可以与 **no** 命令一起使用的参数。

参数	命令	用途
bcastping	/usr/sbin/no -o bcastping=0	允许以广播地址响应 ICMP 回送信息包。禁用它来防止 Smurf 攻击。
clean_partial_conns	/usr/sbin/no -o clean_partial_conns=1	指定是否要避免 SYN（同步序列号）攻击。
directed_broadcast	/usr/sbin/no -o directed_broadcast=0	指定是否允许对网关进行定向广播。设置为 0 有助于防止定向信息包到达远程网络。
icmpaddressmask	/usr/sbin/no -o icmpaddressmask=0	指定系统是否响应 ICMP 地址掩码请求。禁用它可以防止通过源路由攻击进行访问。
ipforwarding	/usr/sbin/no -o ipforwarding=0	指定内核是否应转发信息包。禁用它可以防止重定向的信息包到达远程网络。
ipignoreredirects	/usr/sbin/no -o ipignoreredirects=1	指定是否处理收到的重定向。
ipsendredirects	/usr/sbin/no -o ipsendredirects=0	指定内核是应该否发送重定向信号。禁用它可以防止重定向的信息包到达远程网络。
ip6srcrouteforward	/usr/sbin/no -o ip6srcrouteforward=0	指定系统是否转发源路由 IPv6 信息包。禁用它可以防止通过源路由攻击进行访问。
ipsrcrouteforward	/usr/sbin/no -o ipsrcrouteforward=0	指定系统是否转发源路由信息包。禁用它可以防止通过源路由攻击进行访问。
ipsrcrouterecv	/usr/sbin/no -o ipsrcrouterecv=0	指定系统是否接受源路由信息包。禁用它可以防止通过源路由攻击进行访问。
ipsrcroutesend	/usr/sbin/no -o ipsrcroutesend=0	指定应用程序是否能够发送源路由信息包。禁用它可以防止通过源路由攻击进行访问。
nonlocsroute	/usr/sbin/no -o nonlocsrcroute=0	告诉“网际协议”严格源路由信息包可以对本地网络以外的主机寻址。禁用它可以防止通过源路由攻击进行访问。
tcp_pmtu_discover	/usr/sbin/no -o tcp_pmtu_discover=0	禁用它可以防止通过源路由攻击进行访问。
udp_pmtu_discover	/usr/sbin/no -o udp_pmtu_discover=0	启用或禁用 TCP 应用程序的路径 MTU 发现。禁用它可以防止通过源路由攻击进行访问。

关于可调网络选项的更多信息，请参阅《*AIX 5L V5.2 性能管理指南*》。

附录 E. 声明

本信息是为在美国提供的产品和服务编写的。

IBM 可能在其他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。您可以用书面方式将许可查询寄往:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

本条款不适用英国或任何这样的条款与当地法律不一致的国家或地区: International Business Machines Corporation “按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。某些国家或地区在某些交易中不允许免除明示或暗含的保证。因此本条款可能不适用于您。

本信息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他程序（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，请与以下地址联系:

IBM Corporation
Dept. LRAS/Bldg. 003
11400 Burnet Road
Austin, TX 78758-3498
U.S.A.

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，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 国际软件许可协议或任何同等协议中的条款提供。

有关双字节（DBCS）信息的许可查询，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

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须对您承担任何责任。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他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、兼容性或任何其他关于非 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。

本信息中对非 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。

该信息包含了日常商业操作中使用的数据和报告示例。请尽可能完整地说明这些数据和报告，示例中包含个人、公司、商标和产品的名称。所有这些名称都是虚构的，如果与实际公司企业的名称和地址有任何类似则纯属巧合。

商标

以下术语是 International Business Machines Corporation 在美国和／或其他国家或地区的商标:

AIX

AIX 5L

DB2

IBM

Lotus Notes

POWER3

POWER4

RS/6000

SecureWay

UNIX 是 The Open Group 在美国和其他国家或地区的注册商标。

Java 和所有基于 Java 的商标和徽标是 Sun Microsystems, Inc. 在美国和／或其他国家或地区的注册商标。

Microsoft、Active Directory 和 Windows 是 Microsoft Corporation 在美国和／或其他国家或地区的商标。

其他公司、产品或服务名称可能是其他公司的商标或服务标记。

索引

[T]

[W]

[X]

[Y]

[Z]

C

D

E

F

I

K

L

M

N

O

P

R

S

T

V

X

[特别字符]

读者意见表

AIX 5L 版本 5.2
安全指南

S152-0648-02

姓名

地址

单位及部门

电话号码

读者意见表
S152-0648-02

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

S152-0648-02

请沿此线
撕下或折起

中国印刷

S152-0648-02