AIX 5L V5.2

安全指南

AIX 5L V5.2

安全指南

注

在使用本信息和它支持的产品前，请阅读第 215 页的附录 E，『声明』中的信息。

第一版（2002年10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，而无需对您承担任何责任。

目录

关于本书

本书讲述向系统管理员提供有关 AIX 操作系统的用户和组、文件、系统和网络安全的信息。本指南包含关于如何执行诸如更改权限、设置认证方法、配置可信计算基环境和有 评定级别 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》*包含如下部分: 单机系统安全、网络和因特网的安全性以及附录。

- 第一部分, “单机系统安全, ”讲述了单机系统的 AIX 安全性的基线。本部分的范围包括使用可信计算基环境安装单机系统、安装 CAPP／EAL4+ 功能、控制登录、加强适当的密码规则以及监视文件和目录访问。本部分还包含有关 X11、公共桌面环境（CDE）、轻量级目录访问协议（LDAP）等更多的信息。
- 第二部分, “网络和因特网的安全性, ”提供关于网络和因特网的安全性的信息。该部分针对关于配置 TCP/IP 安全性、控制网络服务系统、审计和监视网络安全性、配置虚拟专用网、电子邮件安全性、NFS 安全性、命名服务及 Kerberos 的关注。
- 第三部分包含附录, 它包含安全性核对表、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系统和通信口的参考信息。

本书读者群

本书是为系统管理员及 IT 安全性管理员编写的。

突出显示

下列突出显示约定在本书中使用:

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先定义的项。也标识图形对象, 例如用户选择的按钮、标号及图标。
斜体	标识由用户提供实际名称或值的参数。
单空白	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 中的区分大小写

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有区别。例如, 您可使用 **ls** 命令来列出文件。如果您输入 LS, 则系统显示该命令 “未查找到”。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, 一定要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。

相关书籍

下列书籍包含相关的信息:

- *《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如何保护单机系统的信息，而不考虑网络连接性如何。这些章节描述了如何在安全性选项打开时安装您的系统，以及如何保护 AIX 免受无授权的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。

本章中的主题包括:

可信计算基

系统管理员必须决定赋予某个特定程序多大的信任。这一决定包括在决定以一定的权限安装程序需要多大信任时，考虑系统之信息资源的价值。

可信计算基（TCB）是负责实施系统级信息安全策略的系统的一部分。通过安装和使用 TCB，您可以定义对可信通信路径的用户访问权，这将允许用户和 TCB 间的通信。只有在安装操作系统时，才启用 TCB 功能。要在安装就绪的机器上安装 TCB，您必须执行“保留”（Preservation）安装。启用 TCB 允许您访问可信 shell、可信进程及“安全注意密钥”（SAK）。

本部分讨论下列主题:

安装带可信计算基的系统

TCB 是负责实施系统安全策略的系统的一部分。TCB 包含全部计算机的硬件，但系统的管理人员应主要关心 TCB 的软件组件。

如果您使用“可信计算基”选项安装系统，您就启用了可信路径、可信 shell 及系统完整性检查（**tcbck** 命令）。这些功能*只有*在基本操作系统（base operating system, BOS）安装期间启用。如果在初始安装期间未选择 TCB 选项，**tcbck** 命令将被禁用。只有重新安装系统并打开 TCB 选项，才能正确启用该命令。

要在 BOS 安装期间设置 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，**安装可信计算基**选择缺省值是 **no**。为启用 TCB，键入 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** 目录中的每一个文件。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。如果安装 TCB，安装以后立即把该文件备份到可移除的介质中，如: 磁带、CD 或者磁盘，并把介质存储在安全的地方。

检查可信计算基

tcbck 命令审计可信计算基的安全状态。当不能正确保护 TCB 文件时或当配置文件具有非安全值时，操作系统的安全性受到损害。**tcbck** 命令通过读取 **/etc/security/sysck.cfg** 文件审计这些信息。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 文件在线，黑客就有可能改变它。确保每一个 TCB 更新后，创建一个离线的只读副本。同时，做任何检查之前，把该文件从归档介质中复制到磁盘上。

安装 TCB 和使用 tcbck 命令都不能保证系统在符合受控访问保护概要文件（CAPP）和评估保险级别 4+（EAL4+）的模式下运行。有关 CAPP/EAL4+ 选项的更多信息，请参阅第 8 页的『受控的访问保护概要文件与 评定级别 4+』。

sysck.cfg 文件的结构

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

每节都有下列属性:

class
一组文件的名称。该属性允许通过给 **tcbck** 命令指定单一参数而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。

owner
文件所有者的用户标识或用户名称。如果不能和文件所有者相匹配，**tcbck** 命令把文件的所有者标识符设置成该值。

group
文件组的组标识或组名称。如果不能和文件所有者相匹配，**tcbck** 命令把文件的所有者标识设置成该值。

mode
逗号分隔值表。允许值是 SUID、SGID、SVTX 和 TCB。文件权限必须是最后的值，而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** 是有效的文件权限。如果不能和实际的文件模式匹配，**tcbck** 命令使用正确的值。

links
链接到该文件的路径名称列表，用逗号分隔。如果该表中任何路径名称不能和该文件链接，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: 有额外的链接但不能确定它们的名称。如果使用 *tree* 参数，**tcbck** 命令也打印与链接到该文件的任何附加路径名称。

symlinks
符号链接到该文件的路径名称列表，用逗号分隔。如果该表中任何路径名称和该文件不是符号链接，**tcbck** 命令创建符号连接。如果使用 *tree* 参数，**tcbck** 命令也打印出任何和该文件有符号链接的附加路径名称。

program
逗号分隔的值表。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，这取决于 **tcbck** 命令使用哪个标志。

acl
文本字符串代表文件的访问控制列表。必须和 **aclget** 命令输出有相同的格式。如果不能和实际的文件 ACL 匹配，**sysck** 命令使用 **aclput** 命令应用该值。

> **注:** 如果存在的话，SUID、SGID 和 SVTX 属性必须和模式指定的属性相匹配。

source
一文件名称，在检查之前源文件要从其复制过来。如果值为空，它为常规文件、目录或命名管道，如果不存在，就创建该文件的新的空版本。对于设备文件，为相同类型的设备创建一新的特殊文件。

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

一般使用 **tcbck** 命令执行以下操作:

- 确保适当安装与安全性相关的文件
- 确保文件系统树不能包含明显违反系统安全性的文件
- 更新、添加或者删除可信文件

用下列方式使用 **tcbck** 命令:

- 正常使用
  - 在系统初始化时非交互式
  - 使用 **cron** 命令
- 交互式使用
  - 对检测个别的文件和文件类很有用
- Paranoid 使用
  - 离线存储文件 **sysck.cfg** 并定期恢复该文件以检查机器。

尽管没有加密安全，TCB 依然使用 UNIX **sum** 命令检查。使用不同的 checksum 命令手工设置 TCB 数据库，例如，**md5sum** 命令（用 *AIX Toolbox for Linux Applications CD* 在 **textutils** RPM 软件包中传递）。

检查可信文件

检查 **tcbck** 数据库中所有的文件，修正并报告所有的错误，键入:

```
tcbck -y ALL
```

这样使 **tcbck** 命令检查每一个文件的安装，**/etc/security/sysck.cfg** 文件描述了 **tcbck** 数据库中的每一个文件。

为了在系统初始化时自动执行检查，并生成错误日志，把以前的命令字符串添加到 **/etc/rc** 文件中。

检查文件系统树

无论何时对约定的系统完整性有疑问，可以随时运行 **tcbck** 命令检查文件系统树。可以运行下列命令检查文件系统树:

```
tcbck -t tree
```

当用 *tree* 值使用 **tcbck** 命令时，检查系统上的所有文件是否正确安装（这需要较长的时间）。如果 **tcbck** 命令查出任何对系统安全有潜在威胁的文件，可以改变有疑问的文件以移除不合的属性。另外，对文件系统中其它的文件也执行下列检测:

- 如果文件所有者是 root，并且文件设置了 **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），移除它。
- 如果文件是 **/etc/security/sysck.cfg** 文件中描述的路径名的附加链接，那么就移除该链接。
- 如果文件是 **/etc/security/sysck.cfg** 文件中描述的路径名的附加符号链接，那么就移除该符号链接。

> **注**: 在执行 **tcbck** 命令或系统不可用之前，所有的设备记录必须添加到 **/etc/security/sysck.cfg** 文件中。为了把可信设备添加到 **/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不恰当地列在 TCB 中的设备，并且可能禁用您的系统。

添加可信程序

把特殊程序添加到 **/etc/security/sysck.cfg** 文件中，键入:

```
tcbck -a PathName [attribute=value]
```

只有值不是从文件的当前状态演绎出的属性才在命令行中指定。所有的属性名称都包含在 **/etc/security/sysck.cfg** 文件中。

例如，下列命令注册一个新的 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
```

为了添加 jfh 和 jsl 作为管理用户，developers 作为管理组，要在安全审计文件 **/usr/bin/abc** 时验证它们，键入:

```
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注册到 **/etc/security/sysck.cfg** 文件中。可以=使用下列命令查找并添加这些文件:

```
tcbck -t tree
```

该命令字符串显示注册到 **/etc/security/sysck.cfg** 文件中任何文件的名称。

删除可信程序

如果从 **/etc/security/sysck.cfg** 文件描述的系统移除一个文件，也应该从 **/etc/security/sysck.cfg** 文件中移除该文件的描述。例如，如果删除了 **/etc/cvid** 程序，下列命令字符串就会显示一条错误信息:

```
tcbck -t ALL
```

显示错误消息是:

```
3001-020 不能查找到文件 /etc/cvid。
```

该程序的描述仍然在 **/etc/security/sysck.cfg** 文件中。为了移除该程序的描述，键入下列命令:

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

配置额外的可信选项

下列各节提供关于如何给 TCB 配置附加选项。

限定访问终端

getty 和 **shell** 命令更改终端的所有者和模式以防止不可信程序访问终端。操作系统提供了注册唯一终端访问的方法。

使用安全注意密钥

通过按下安全注意密钥（SAK）保留按键序列（Ctrl-X，然后 Ctrl-R），可创建可信通信路径。根据下列条件创建可信通信路径:

- 当登录到系统时

  您按下 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，初始的登录屏幕是未授权的程序，它可能偷盗您的密码。使用 **who** 命令确定当前是谁在使用该终端，然后登出。

• 当您想要您键入的命令致使一个可信程序运行。一些例子包括:

- 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。这样确保用 root 用户权限运行可信程序。
- 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。

  注意: 当使用 SAK 时要小心，因为 SAK 会杀死试图访问终端的所有进程以及任何和它的链接（例如，**/dev/console** 可能链接到 **/dev/tty0**）。

配置安全注意密钥

独立配置每一个终端，以致在终端上按下 SAK 就创建一可信通信路径。**/etc/security/login.cfg** 文件中的 **sak_enabled** 属性指定它。如果该属性值是 True，启用 SAK。

如果通信使用端口，（例如，用 **uucp** 命令），所使用的特定端口在 **/etc/security/login.cfg** 文件中的节有下列行:

```
sak_enabled = false
```

该行（或那节中没有记录）禁用那个终端的 SAK。

为启用终端上的 SAK，把下列行添加到终端的节中:

```
sak_enabled = true
```

受控的访问保护概要文件 与 评定级别 4+

在 AIX 5.2，系统管理员能用 受控的访问保护概要文件(CAPP）与 评定级别 4+(EAL4+）选项在 CD-ROM 基操作系统（BOS）安装期间安装系统。带此选项的系统对在 BOS 安装期间安装的软件有限制，另外网络访问也受限制。

本节讨论下列主题:

- 『CAPP/EAL4+ 符合性系统概述』
- 『安装 CAPP/EAL4+ 系统』
- 第 9 页的『CAPP/EAL4+ 软件捆绑』
- 第 10 页的『用于 CAPP/EAL4+ 系统的物理环境』
- 第 10 页的『用于 CAPP/EAL4+ 系统组织的环境』
- 第 11 页的『用于 CAPP/EAL4+ 系统的系统配置』

CAPP/EAL4+ 符合性系统概述

CAPP 系统是对于依照公共标准的安全性评估把它设计与配置为满足 受控的访问保护概要文件(CAPP）的系统。该 CAPP 指定系统的性能要求，类似于旧的 TCSEC C2 标准（大家知道的*橙皮书*）。

公共标准（CC）评估系统是已依照公共标准，一个用于 IT 产品评估的 ISO 标准（ISO 15408）评估的系统 AIX 5.2 包含满足 CAPP 与 CC 保证级别 EAL4+的要求的技术。满足这些要求的系统配置在本指南中作为 *CAPP/EAL4+ 系统* 引用。

如果按 CC 标准评估某系统，CC 评估只对特定的系统配置（硬件或软件）是有效的。更改相关的安全性配置导致未评估系统。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。本章将说明满足 CAPP 与 CC 评估要求的系统的约束。CAPP 与 CC 都不包括所有可能的 AIX 5.2 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+ 系统包括在 64 位 POWER3 与 POWER4 处理器上的基操作系统，有以下模块:

- 逻辑卷管理程序（LVM）与增强的日志文件系统（JFS2）
- 有 CDE GUI 的 X-Windows 系统
- 基本的网际协议版本 4（IPv4）网络功能（Telnet、FTP、rlogin 与 rsh/rcp）
- 网络文件系统（NFS）

如果下列条件适用，则认为 CAPP/EAL4+ 系统处于安全状态:

- 如果配置了审计技术且系统是多用户方式，则审计技术必须是可运作的。
- 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通过 NFS 安装的。

要获得在 CAPP/EAL4+ 的最新的信息，请参阅 *AIX 5.2 发行说明*。

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 **More Options**。
2. 在 More Options 屏幕，为 **启用CAPP 与 EAL4+ 技术输入相应于 Yes 或 No 选项的数字**。缺省值为 **no**。

该**启用 CAPP 与 EAL4+ 技术**选项只有在下列条件下才是可用的:

- 安装方法设置为新的和完全覆盖安装。
- 选定英语语言。
- 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，**Trusted Computing Base** 选项也设置为 **yes** 且唯一有效的 **Desktop** 选择为 **NONE** 或 **CDE**。

如果正用定制的 **bosinst.data** 文件执行无提示的安装，INSTALL_TYPE 字段必须设置为 CC_EVAL 且下列字段必须按如下设置:

```
INSTALL_TYPE = CC_EVAL
INSTALL_METHOD = overwrite
TCB = yes
DESKTOP = NONE 或 CDE
```

也能使用网络安装管理（NIM）环境安装 CAPP/EAL4+ 系统。要安装 CAPP/EAL4+ 客户机，NIM 主控机必须为 CAPP/EAL4+ 系统。尽管两个系统都能位于正构建的网络，CAPP/EAL4+ 系统只能与其它 CAPP/EAL4+ 系统通信。要安装 CAPP/EAL4+ 客户机，必须如上所示定义 **bosinst_data** 资源且编辑字段。

CAPP/EAL4+ 软件捆绑

如果选定 CAPP/EAL4+ 选项，则安装 **/usr/sys/inst.data/sys_bundles/CC_EVAL.BOS.autoi** 安装捆绑的内容。

用选定的 CAPP/EAL4+ 选项，可以随意地选择安装图形软件捆绑与文档服务软件捆绑。如果用 CAPP/EAL4+ 选项选择图形软件选项，则安装 **/usr/sys/inst.data/sys_bundles/CC_EVAL.Graphics.bnd** 软件捆绑。如果用 CAPP/EAL4+ 选项选择文档服务软件选项，则安装 **/usr/sys/inst.data/sys_bundles/CC_EVAL.DocServices.bnd** 软件捆绑。

在安装许可程序产品（LPP）后，系统更改缺省配置来遵循 CAPP/EAL4+ 要求。所做的缺省配置更改如下所示:

- 从 **/etc/pse.conf** 文件除去 **/dev/echo**。
- 实例化流设备。
- 只允许 root 用户访问可更换媒体。
- 从 **inetd.conf** 文件除去非 CC 条目。
- 更改不同的文件许可权。
- 在 **sysck.cfg** 文件登记 symlink。
- 在 **sysck.cfg** 文件登记设备。
- 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** 文件禁用 **snmpd**。
- 在 **/etc/rc.tcpip** 文件禁用 **hostmibd**。
- 在 **/etc/rc.tcpip** 文件禁用 **snmpmibd**。
- 在 **/etc/rc.tcpip** 文件禁用 **aixmibd**。

- 在 **/etc/rc.tcpip** 文件禁用 **muxatmd**。
- NFS 端口（2049）是有特权的端口。
- 添加丢失的事件到 **/etc/security/audit/events** 文件。
- 确保回送接口在运行。
- 为 **/dev/console** 创建同义词。
- 强迫缺省 X-server 连接许可权。
- 更改 **/var/docsearch** 目录，这样使得全部文件是全局可读的。
- 添加 ODM 节来设置控制台许可权。
- 设置在 BSD 样式 ptys 的许可权为 000。
- 禁用 **.netrc** 文件。
- 添加补丁程序目录处理。

用于 CAPP/EAL4+ 系统的物理环境

CAPP/EAL4+ 系统对它运行的环境有特定的要求。要求如下:

- 实际访问必须受限制，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调制解调器。
- 限制已授权用户对终端的实际访问。
- 物理网络对窃听与电子欺骗是安全的。当在不安全的线路上通信时，需要额外的安全性措施，如加密。
- 与非 AIX 5.2 CAPP/EAL4+ 系统或不处于相同管理控制的其它系统通信，是不允许的。
- 当与其它 CAPP/EAL4+ 系统通信时只使用 IPv4，尚未评估 IPv6。
- 应该不允许用户更改系统时间。

用于 CAPP/EAL4+ 系统组织的环境

对 CAPP/EAL4+ 系统下列的程序上的与组织的要求必须满足:

- 只有授权可处理系统信息的用户才授予其用户标识。
- 用户必须使用高质量密码（尽可能地随意且与用户或组织无关连）。要获得设立密码的规则，请参阅第 37 页的『密码』。
- 用户不该把他们的密码透露给其他人。
- 管理员必须有管理关键系统安全性的充足的知识。
- 管理员必须按系统文档提供的指导工作。
- 管理员必须用他们个人的标识登录并使用 **su -** 来切换至超级用户模式以便管理。
- 由管理员为系统用户生成的密码必须安全地发送到用户。
- 那些负责系统的人必须建立与实现必要的系统的安全操作的过程。
- 管理员必须确保对安全关键性系统资源的访问受相应的许可权位和 ACL 的设置保护。
- 物理网络必须由组织核准来运送系统拥有的极其敏感数据。
- 维护过程必须包括系统的定期的诊断。
- 管理员必须有确保在系统故障后安全操作与恢复的适当的过程。
- 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。
- 窃听并跟踪软件（**tcpdump**、**trace**）不应该在运作的系统上使用。
- 匿名协议如 HTTP 可能只用于公共信息（例如在线文档）。

- 只有基于 TCP 的 NFS 能用于 CAPP/EAL4+ 系统。
- 不要给用户对可更换介质的访问。设备文件要得到适当的许可权位或 ACL 的保护。
- 只在管理 AIX 时使用超级权限。所有基于角色与基于组的管理授权功能部件，与 AIX 的特权机制一样，不包括在 CAPP/EAL4+ 符合性。

用于 CAPP/EAL4+ 系统的系统配置

本节提供包含于 CAPP/EAL4+ 系统的子系统配置方面的信息。

管理

管理员必须用他们个人的帐户登录，并使用 **su** 命令来变为系统管理的 root 用户。要有效阻止猜测 root 帐户的密码，只允许授权的管理员在 root 帐户使用 **su** 命令。要确保这一点，请执行以下操作:

1. 按如下所示，添加条目到 **/etc/security/user** 文件的 **root** 节:

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

2. 必须按如下所示，在只包含已授权的管理员的用户标识的 **/etc/group** 文件定义一个组:

```
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步骤:

- 建立与实现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。
- 确保系统配置成只有一个管理员能把新的可信软件引进到系统。
- 实现过程来确保用户在注销串行登录设备（例如，IBM 3151 终端）前清屏。

用户与端口配置

用于用户与端口的 AIX 配置选项必须设置为满足评估的要求。实际的需要是正确地猜测到密码的概率应该至少为 1,000,000 分之一，并且在一分钟内反复尝试正确猜测到密码的概率应该至少为 100,000 分之一。

用于 **/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 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。如果拒绝服务攻击对发送不正确的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（包括管理的用户）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模式并运行 **chsec** 命令。要获得更多的使用 **chsec** 命令的信息，请参阅第 26 页的『用户帐户控制』。

对于 **/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
```

资源的限制

当在 **/etc/security/limits** 文件设置资源的限制时，确保该限制符合系统上的进程的需要。特别是，`stack` 与 `rss` 大小应该决不设置为 `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，从而对其它进程造成了资源问题。`stack_hard` 与 `rss_hard` 大小也同样应受限制。

审计子系统

下列过程帮助保护审计子系统:

- 配置审计子系统来记录用户的所有相关安全性活动。要确保审计过程需要的文件空间可用，设立用于审计数据的专用的文件系统。
- 保护审计记录（如审计跟踪、库文件与所有其它存储在 **/audit** 的数据），使非 root 用户不能访问。
- 对于 CAPP/EAL4+ 系统，当使用审计子系统时，必须建立 **bin** 方式审计过程。要获得如何建立审计子系统的信息，请参阅第 51 页的『设置启动审计过程』。
- 至少系统中百分之二十的可用磁盘空间应该专用于审计跟踪。
- 如果启用审计过程，在 **/etc/security/audit/config** 的 **start** 节中的 **binmode** 参数应该设置为 **panic**。在 **bin** 节中的 **freespace** 参数应该配置为至小等于 25% 的专用于存储审计跟踪的磁盘空间的值。**bytethreshold** 与 **binsize** 参数应该每个都设置为 65536 字节。
- 从系统拷贝审计记录到用于文档的永久存储器。

网络配置

网络必须对于因特网端口（DACinet）使用任意的访问控制来确保 X 协议（X11）与 NFS 不能匿名地使用。要获得 **dacinet** 命令的更多信息，请参阅第 119 页的『为网际端口所设的基于用户的 TCP 端口访问控制以及自主访问控制』。

dacinet 命令阻止出现下列情况:

- 一用户用 X11 接管另一用户的桌面。
- 客户机上的一个用户伪造对 NFS 服务器的请求，该请求将允许该用户成为 root 用户。通常，用户通过发出请求到本地主机的逻辑文件系统，然后该系统发出请求（以 root 用户身份）到远程服务器，来达到访问远程 NFS 服务器的目的。设置只用于 root 用户的一个 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（如果这里无图形卡）。

表 1. 标准系统服务

UID	命令	描述
root	/init	Init 进程
root	/usr/sbin/syncd 60	文件系统同步守护程序
root	/usr/sbin/srcmstr	SRC 主控机守护程序
root	/usr/sbin/cron	带 AT 支持的 CRON 设施
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 错误记录守护程序
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 客户机
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 主控机守护程序
root	/usr/sbin/uprintfd	内核打印守护程序
root	/usr/sbin/qdaemon	队列守护程序
root	/usr/lpp/diagnostics/bin/diagd	诊断

运行 CAPP/EAL4+ 分布式系统

要运行遵循 CAPP/EAL4+ 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，它确保用户标识在遵循 CAPP/EAL4+ 的全部系统上是同样的。

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。

任何管理员在任何系统上都可使用工具（如 SMIT）来更改认证数据。在主控机上物理更改认证数据。

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

分布式系统上的共享文件: 在分布式系统下列文件是共享的。通常，它们来自于 **/etc/security** 目录。

表 2. 分布式系统上的共享文件

文件	描述
/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/audit/bincmds	用于主机的 Bin 模式审计命令
/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	此主机上审计对象的列表
/etc/security/audit/streamcmds	用于此主机流模式审计命令
/etc/security/environ	每个用户的环境变量
/etc/group	**/etc/group** 文件
/etc/passwd	**/etc/passwd** 文件
/etc/security/group	来自 **/etc/security/group** 文件的扩展组信息
/etc/hosts	**/etc/hosts** 文件
/etc/security/limits	每用户的资源限制
/etc/security/passwd	每用户的密码
/etc/security/user	每个用户与缺省用户的属性
/etc/security/priv	系统启动时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** 文件的端口免除 ACL 检查
/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。

分布式系统中非共享的文件: 下列在 **/etc/security** 目录的文件在分布式系统是不共享的，而是保留为特定主机使用:

表 3. 分布式系统上的非共享文件

文件	描述
/etc/security/failedlogin	每台主机登录失败的日志文件
/etc/security/lastlog	有关最后一次成功与不成功登录到此主机的每个用户信息
/etc/security/portlog	用于此主机锁定端口的每个端口信息
/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

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，但有一小写字母 o 区别。

建立分布式系统（主控系统）: 在主控机，创建新的逻辑卷，它包含用于识别与认证的数据的文件系统。该逻辑卷命名为 **/dev/hd10sec** 且它以 **/etc/data.master** 安装在主控机系统。要在主控机生成必需的更改，用主控机的 IP 地址和名称按如下所示运行 **mkCCadmin** 命令:

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

建立分布式系统（所有系统）: 所有要共享的数据移动到 **/etc/data.shared** 目录。在启动时所有系统将在 **/etc/data.shared** 目录之上安装主控机的 **/etc/data.master** 目录。主控机自己使用回送安装。

客户机系统通过运行如下命令建立:

```
mkCCadmin -a ipaddress hostname
```

要更改客户机来使用不同的主控机，使用 **chCCadmin** 命令。

在一系统并入分布式识别与认证系统后，生成下列额外的 **inittab** 条目:

isCChost
初始化系统为 CAPP/EAL4+ 模式。

rcCC 这全部清除全部 DACinet ACL 并且只打开端口映射程序与 NFS 需要的端口。然后它安装共享目录。

rcdacinet
这装入管理员可能已定义的额外的 DACinet ACL。

考虑下列情况: 当运行分布式系统时

- 管理员必须确保在更改共享配置文件之前，安装共享数据以确保共享数据在所有的系统都可见。
- 当共享目录未安装时，更改 root 用户密码是唯一允许的管理行为。

使用 DACinet 功能以获得基于用户和端口的网络访问控制

DACinet 功能部件能用于限制用户对 TCP 端口的访问。要获得更多关于 DACinet 的信息，请参阅第 119 页的『为网际端口所设的基于用户的 TCP 端口访问控制以及自主访问控制』。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，只有来自遵循 CAPP/EAL4+ 主机的 root 用户可以访问该端口。这种情况限制常规用户通过 **telnet** 连接到受害者的 TCP/25 端口来欺骗电子邮件。

要为 TCP 连接在引导时激活 ACL，**/etc/rc.dacinet** 脚本从 **/etc/inittab** 运行。它将读取在 **/etc/security/acl** 文件的定义并装载 ACL 到内核。该受 ACL 保护的端口应该列在 **/etc/security/services**。此文件使用与 **/etc/services** 文件相同的格式。

假定用于所有连接的系统的 10.1.1.0/24 子网，ACL 的限制对 root 用户访问以在 **/etc/security/acl** 得到 X（TCP/6000）的条目将如下所示:

```
6000    10.1.1.0/0xFFFFFF00 u:root
```

在遵循 CAPP/EAL4+ 的系统安装额外的软件

管理员能在遵循 CAPP/EAL4+ 的系统安装额外的软件。如果该软件不由 root 用户或不带 root 用户特权运行，这不会使 CAPP/EAL4+ 符合性无效。典型示例包括只由常规用户运行并没有 SUID 组件的办公应用程序。

另外，安装用 root 用户特权运行的软件，使 CAPP/EAL4+ 符合性无效。这意味着，例如，不应该安装较旧的 JFS 的驱动程序，因为它们以内核模式运行。附加的以 root 用户运行的守护程序（例如，SNMP 守护程序）也使 CAPP/EAL4+ 符合性无效。

CAPP/EAL4+ 符合性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，这样生产系统为基于评估系统，但不符合评估系统的严格规范。

登录控制

潜在的黑客从缺省的 AIX 登录屏幕可以获取宝贵的信息资料，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。为了安全性的原因，您可能想在安装系统后尽快地更改登录屏幕缺省值。本节讨论下列主题:

- 『更改登录屏幕欢迎消息』
- 第 18 页的『更改公共桌面系统环境登录屏幕』
- 第 18 页的『固定系统缺省登录参数』
- 第 18 页的『保护无人照管终端』
- 第 18 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问题。有关 KDE 和 GNOME 的更多信息，请参照 *《AIX 5L V5.2 安装指南与参考大全》*。

有关用户、组及密码的信息，请参照第 21 页的第 2 章，『用户、角色和密码』章节。

设置登录控制

在 **/etc/security/login.cfg** 文件中设置下列登录控制，使得用密码猜解难以攻击系统。

表 4. **/etc/security/login.cfg** *文件的属性及推荐值。*

属性	用于 PtY（网络）	用于 TTY	推荐值	注释
sak_enabled	Y	Y	false	很少需要安全注意密钥。请参阅第 6 页的『使用安全注意密钥』。
logintimes	N	Y		指定这里允许登录的次数。
logindisable	N	Y	4	连续 4 次尝试失败后，禁止在此终端登录。
logininterval	N	Y	60	60 秒内进行了指定的无效尝试时，禁用终端。
loginreenable	N	Y	30	30 分钟后对自动禁用的终端重启用。
logindelay	Y	Y	5	出现登录提示符的间隔时间（秒）。这可随失败尝试次数成倍增加，例如，初始值是 5，随失败次数增加，出现登录提示符的间隔就是 5 秒、10 秒、15 秒、20 秒。

要明白，这些端口限制主要对连接的串行终端而不是网络登录使用的伪终端发挥作用。您可在此文件中指定显式终端，例如:

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

更改登录屏幕欢迎消息

为预防在登录屏幕上显示某些信息，在 **/etc/security/login.cfg** 文件中编辑 *herald* 参数。缺省的 *herald* 包含随登录提示符显示的欢迎信息。您可用 **chsec** 命令或直接编辑文件来更改这个参数。

下列示例用 **chsec** 命令更改缺省的 *herald* 参数:

```
# chsec -f /etc/security/login.cfg -a default -herald
"未经授权，禁止使用本系统。 \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，就打开 **/etc/security/login.cfg** 文件并更新 *herald* 参数，如下:

```
default:
herald = "未经授权，禁止使用本系统。 \nlogin: "
 sak_enable = false
 logintimes =
 logindisable = 0
 logininterval = 0
 loginreenable = 0
 logindelay = 0
```

注: 将 logindisable 和 logindelay 变量值设置为大于 0 （# > 0）以使系统更安全。

更改公共桌面系统环境登录屏幕

此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及操作系统版本。为防止显示此信息，编辑 **/usr/dt/config/$LANG/Xresources** 文件，这里 **$LANG** 指您的机器上安装的本地语言。

在我们的示例中，假设 **$LANG** 设置为 **C**，将此文件复制到 **/etc/dt/config/C/Xresources** 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信息。

有关 CDE 安全性说明的更多信息，请参阅第 20 页的『管理 X11 和 CDE 注意事项』。

固定系统缺省登录参数

编辑 **/etc/security/login.cfg** 文件设置许多登录参数的缺省基数，例如您可能为新用户设置的那些参数（登录重试次数、登录重启用数及登录间隔时间）。

保护无人照管终端

如果终端处于登录状态却无人照管，那么所有的系统容易受到攻击。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，用户任何时候离开终端时都应当退出系统。让系统终端处于非安全状态，会造成安全隐患。为了锁定您的终端，使用 **lock** 命令。如果您的界面是 AIXwindows，使用 **xlock** 命令。

强制自动注销

另一个要关注的安全性问题是由于用户长期将他们的帐户置于无人照管状态造成的后果。这种状况使入侵者可以控制用户的终端，从而潜在地危及系统的安全。

为了预防这类安全隐患，您可在系统中启用自动退出系统功能。要做到这一点，编辑 **/etc/security/.profile** 文件，对*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，600 是秒数，等于 10 分钟。但是，此方法只在 shell 中生效。如果用户在应用程序中，例如 **vi**，这将不起作用。

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，那么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，必须采取权威措施，给用户提供适当的 **.profile** 文件，防止

对这些文件的写访问权。

管理 X11 和 CDE 注意事项

本节讨论涉及 XII 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

虽然运行 CDE 图形用户界面（GUI）对用户来说是方便的，但是安全问题也随之而来。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

关于 X11 服务器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，就要除去这些可执行文件，除非在您的配置下它们是必要的，或者另外一种方法是，将对这些命令的访问权更改为只有 root 用户才能访问。

可以在 **X11.apps.clients** 文件集中找到 **xwd** 和 **xwud** 命令。

如果您需要保留 **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由运行 **xwd** 和 **xwud** 命令所造成的风险。

更多关于 OpenSSH 和 MIT Magic Cookie 的信息，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 +** 命令来连接您的系统。确保您使用 **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，从而使对 X 服务器的潜在攻击的监视变得轻松。要授权对特定主机的访问，运行如下的 **xhost** 命令:

```
# xhost + hostname
```

更多关于 **xhost** 命令的信息，请参阅 *《AIX 命令参考》，第 6 卷*。

禁用运行 xhost 命令的用户许可权

确保适当使用 **xhost** 命令的另一种方法是将对这个命令的执行仅限为超级用户权限。要做到这一点，使用 **chmod** 命令将 **/usr/bin/X11/xhost** 的许可权更改为 744。

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

确保您使用 **xhost** 命令指定了主机名，因为它禁用对 X 服务器的访问控制。这允许您授权对特定主机的访问，从而使对 X 服务器的潜在攻击的监视变得轻松。

如果您不指定主机名，那么会将访问权授予所有的主机。

第 2 章 用户、角色和密码

本章描述了管理 AIX 用户和角色的方面。讨论下列问题:

root 帐户

root 帐户实际上可以不受限制地访问系统上所有的程序、文件和资源。**root** 帐户是更适合称为超级用户。超级用户是带有用户标识（UID）0 的 **/etc/passwd** 中的特殊用户。该用户一般被授予用户名 **root**。因此，不是用户名称而是 0 的用户标识值使得 **root** 帐户这么特殊。同时，总是运用本地安全文件认证 **root** 帐户。

root 帐户应该总是有密码，而且该密码不能共享。安装系统后，会立即给 **root** 帐户一个密码。只有系统管理员才能知道 **root** 密码。系统管理员只能作为 **root** 操作执行 **root** 需要的系统管理功能。关于其它所有的操作，应该返回它们的一般用户帐户。因为 **root** 帐户覆盖许多系统安全防护，经常作为 **root** 操作可能导致系统损坏。

禁用直接根登录

潜在黑客的一般攻击方式是获得超级用户或 root 用户密码。

为了避免这种类型的攻击，可以禁止直接访问 root ID 然后使用 **su -** 命令要求系统管理员获得超级用户特权。另外，允许移除作为攻击点的 root 用户，禁止直接访问 root 允许您监视哪些用户获得超级用户访问以及他们的操作时间。这样做，可以查看 **/var/adm/sulog** 文件。另一种方法是启用系统审计，它能汇报该类型的活动。

要禁止 root 用户远程登录访问，编辑 **/etc/security/user** 文件。在记录中为 root 指定 **false** 作为登录值。

在禁用远程 root 登录之前，检查并计划以防止系统管理员用非 root 用户 ID 登录的情况。例如，用户的主文件系统已满，用户就不能登录。如果禁用远程 root 登录，并且用户 **su -** 到 root 有一个满的主文件系统，那么 root 就永远不能控制系统。系统管理员可以通过为他们自己创建主文件系统绕过这个问题，该主文件系统比一般用户文件系统大。

有关控制 root 登录的更多信息，请参阅第 11 页的『管理』和第 11 页的『用户与端口配置』。

管理角色

分配部分 root 用户权限给非 root 用户。不同的 root 用户任务指定不同的权限。这些权限分组成角色并指定给不同的用户。

本节覆盖下列主题:

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

角色概述

角色由允许用户运行函数的权限构成，运行函数通常需要 root 用户的权限。

以下是合法角色的列表:

添加与删除用户
对于此角色，允许任何用户作为 root 用户操作。它们能够添加与删除用户、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是 **security** 组的成员。

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、删除和列出角色。用户必须是 **security** 组成员。

备份与恢复
允许用户备份与恢复文件系统及目录。此角色需要启用系统备份与恢复的授权。

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授权。

运行诊断
允许用户或服务代表运行诊断及诊断任务。用户必须让 **system** 指定为主组，还要有包含 **shutdown** 的组设置。
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。此角色的用户必须理解角色所要求的职责。

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

实现和维护角色可使用 SMIT 快速路径（如下列表格显示）。

表 5. 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。授权允许用户执行特定的任务。例如，拥有 UserAdmin 授权的用户可以通过运行 **mkuser** 命令创建管理员用户。无此权限的用户不能创建管理员用户。

授权有两种类型:

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。

授权执行下列功能:

备份 执行系统备份。

下列命令使用备份授权:

Backup

备份文件和文件系统。用户管理员必须拥有备份授权。

诊断 允许用户运行诊断。要求权限直接从命令行运行诊断任务。

下列命令使用诊断授权:

diag 在选定的资源上运行诊断。如果用户管理员没有诊断权限，结束命令。

GroupAdmin

对组数据执行 root 用户功能。

下列命令使用 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里的组成员或更改组安全性里用户以管理任意非管理组。

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

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**组里。

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。输入 AUDIT 类字段里的审计类列表。

PasswdAdmin

对密码数据执行 root 用户功能。

下列命令使用 PasswdAdmin 授权:

chsec 修改所有用户的 **lastupdate** 和 **flags** 属性。无 PasswdAdmin 授权，**chsec** 命令仅允许用户管理员修改非管理员用户的 **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员用户的 **lastupdate** 和 **flags** 属性。

pwdadm
更改所有用户的密码。用户管理员必须在组安全性中。

PasswdManage
对非管理员用户执行密码管理功能。

下列命令使用 PasswdManage 授权:

pwdadm
更改非管理员用户的密码。管理员必须在组安全性里或有 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，不能访问用户审计信息。

下列命令使用 UserAdmin 授权:

chfn 更改任意用户一般信息（gecos）字段。如果用户在组安全性中但没有 UserAdmin 授权，能更改任意非管理员用户 gecos 字段。否则，用户仅更改自己的 gecos 字段。

chsec 修改包含角色属性的 **/etc/passwd**、**/etc/security/environ**、**/etc/security/lastlog**、**/etc/security/limits** 和 **/etc/security/user** 文件里的管理员用户数据。用户管理员也能修改缺省节值和不包括审计类属性的 **/usr/lib/security/mkuser.default** 文件。

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员用户信息。

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员用户。

rmuser
除去任意用户。如果用户没有 UserAdmin 授权，仅能创建非管理员用户。

UserAudit
允许用户修改用户审计信息。

下列命令使用 UserAudit 授权:

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

chuser
修改非管理员用户的审计类属性。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 如果是 root 用户或组安全性中的用户，可以查看非管理员的审计类属性。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
创建新用户并且允许用户管理员分配非管理员用户的审计类属性。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。

下列命令使用 RoleAdmin 授权:

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

lsrole 查看角色。

mkrole
创建角色。如果用户管理员没有 RoleAdmin 授权，结束命令。

rmrole
除去角色。如果用户管理员没有 RoleAdmin 授权，结束命令。

恢复 执行系统恢复。

下列命令使用 Restore 授权:

Restore
恢复备份文件。用户管理员必须拥有备份授权。

授权命令列表

下表列出了使用的命令和授权。

Command	Permissions	Authorizations
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	
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	
chsec	4550 root.security	UserAdmin, GroupAdmin, PasswdAdmin, UserAudit
lssec	0550 root.security	PasswdAdmin
chrole	4550 root.security	RoleAdmin
lsrole	0550 root.security	
mkrole	4550 root.security	RoleAdmin
rmrole	4550 root.security	RoleAdmin
backup	4555 root.system	Backup
restore	4555 root.system	Restore

用户帐户

- 『用户属性建议』
- 『用户帐户控制』
- 第 27 页的『登录用户标识』
- 第 27 页的『使用访问控制表增强用户安全性』
- 第 27 页的『PATH 环境变量』

用户属性建议

用户管理包括创建用户和组以及定义它们的属性。用户的一个主要属性是怎样对他们进行认证。用户是系统的主要代理。其属性控制访问权、环境、如何对他们进行认证以及怎样、什么时候、在哪里可以访问他们的帐户。

组是共享同一个访问许可权对受保护资源进行访问的用户的集合。一个组有一个 ID，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的许多属性，包括密码和登录属性进行设置。可以到第 42 页的『磁盘限额系统概述』中查看可配置属性列表。建议指定以下属性:

- 每个用户应有一个专属于自己的用户标识。所有安全防护措施和追溯工具只有在每个用户都有唯一的标识时才能起作用。
- 为系统用户指定一个对其有意义的用户名。最好使用实际的名字，因为大多数电子邮件系统使用用户标识为进来的邮件标号。
- 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之前不要将初始密码给用户帐户。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，但不能登录该帐户。
- 不要更改系统正常运作所需的由系统定义的用户标识。系统定义的用户标识列在 **/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 用户才能更改 **/etc/security/user** 文件中设置为 **admin=true** 的用户的属性。

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、补充组标识。
环境	指定主环境或 shell 环境。

用户帐户控制

每个用户帐户有一套相关属性。当使用 **mkuser** 命令创建用户时，这些属性根据缺省值创建。可以使用 **chuser** 命令对它们进行更改。下列用户属性只用于控制密码质量:

account_locked	如果需要对帐户进行明确的锁定，可以将此属性设置为 *true*，缺省值是 *false*。
admin	如果此属性设置为“true”，则该用户不能更改自己的密码。只有管理员才可以更改它。
admgroups	列出此用户对它具有管理权限的组。对于这些组，此用户可以添加或删除组成员。
auth1	授予用户访问权限的认证方法。一般将它设置为“SYSTEM”，这样它将使用较新的方法。
auth2	按 *auth1* 指定的内容对用户进行认证之后运行的方法。它不能阻止对系统的访问。一般将它设置为 **NONE**。

daemon	此布尔参数指定是否允许用户使用 **startsrc** 命令启动守护进程或子系统。它也限制对 **cron** 和 **at** 的使用。
login	指定是否允许该用户登录。
logintimes	限制用户什么时候可以登录。例如，可以限制用户只能在正常办公时间访问系统。
registry	指定用户注册表。可以用它来告诉系统备用用户信息注册表，如 NIS、LDAP 或 Kerberos。
rlogin	指定是否允许该用户通过 **rlogin** 或 **telnet** 登录。
su	指定其它用户是否可以使用 **su** 命令切换到此标识。
sugroups	指定允许哪个组切换到此用户标识。
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；也可以用来对帐户进行临时性关闭。
loginretries	指定系统锁定某个用户标识之前允许最多连续登录失败次数。失败登录尝试是记录在 **/etc/security/lastlog** 中。
umask	指定用户的初始 **umask**。

在 **/etc/security/user**、**/etc/security/limits**、**/etc/security/audit/config** 和 **/etc/security/lastlog** 文件中对整套用户属性进行定义。使用 **mkuser** 命令进行用户创建的缺省值由 **/usr/lib/security/mkuser.default** 文件指定。只有那些将 **/etc/security/user** 和 **/etc/securtiy/limits** 的 **default** 节的一般缺省值覆盖掉的选项以及审计类必须在 **mkuser.default** 文件中进行指定。这些属性中有几个属性控制用户要怎样才可以登录，可以对这几个属性进行配置，用以在指定条件下自动锁定用户帐户（防止进一步登录）。

一旦系统锁定了用户帐户，必须由系统管理员在 **/etc/security/lastlog** 文件中将用户的 **unsuccessful_login_count** 属性重设为低于登录重试的值，用户才能登录。可以通过以下 **chsec** 命令来实现:

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

可以使用 **chsec** 命令编辑相应安全性文件，如 **/etc/security/user** 或 **/etc/security/limits** 文件中的 *default* 节来更改缺省值。系统将许多缺省值定义为标准行为。要明确指定每次创建新用户都要设定的属性，可以对 **/usr/lib/security/mkuser.default** 中的 *user* 条目进行更改。

要了解用户密码属性的详细信息，请参阅第 37 页的『密码』。

登录用户标识

操作系统通过登录用户标识来识别用户。登录用户标识让系统可以追踪所有的用户操作到它们的源头。用户登录系统之后，运行初始用户程序之前，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。在登录会话中随后的所有进程都用这个标识做标记。这些标记使登录用户标识进行的所有活动都留下痕迹。用户可以在登录过程中重新设置有效用户标识、真正的用户标识、有效组标识、真正的组标识和补充组标识，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

要在系统上取得相应的安全水平，要有一个一贯的安全策略来管理用户帐户。最常用的安全机制是访问控制表（ACL）。有关访问控制表和编制安全策略的详细信息，请参阅本书的『访问控制表』章节。

PATH 环境变量

PATH 环境变量是一个重要的安全控制。它指定要查找某一命令所需搜索的目录。系统范围 **PATH** 值的缺省值是在 **/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** 值既可以将系统范围 **PATH** 值覆盖，也可以在它里面添加另外的目录。

对 **PATH** 环境变量的非法更改可能让某系统用户对其他用户（包括 root 用户）进行“欺骗”。欺骗程序（也称为″特洛伊木马″程序）替换系统命令，然后将预定给该命令的信息，例如用户密码，捕获。

例如，假定某用户更改 **PATH** 值使系统运行命令时首先查找 **/tmp** 目录。然后该用户在 **/tmp** 目录中放进一个称为 **su** 的程序，该程序就象 **su** 命令一样要求根密码。接着，该 **/tmp/su** 程序将 root 密码邮寄给用户，并在退出前调用 **su** 命令。在这种情况下，使用 **su** 命令的任何用户将暴露 root 密码，而自己还不知道。这只是通过改变 **PATH** 值取得机密信息的许多种情况中的一种。

然而，只要遵循一些简单的步骤，系统管理员和用户就可以防止 **PATH** 环境变量问题:

- 当有怀疑时，请指定全路径名。如果指定了全路径名，系统将忽略 **PATH** 环境变量。
- 切勿将当前目录（由 **.**（句点）指定）写入为 root 用户指定的 **PATH** 值。切勿在 **/etc/profile** 中指定当前目录。
- root 用户应在自己专用的 **.profile** 中有自己的 **PATH** 规范，通常 **/etc/profile** 中的该规范列出所有用户的最低标准，而 root 用户可能需要比缺省值要多一些目录。
- 警告其他用户在没有征询系统管理员同意的情况下，不要更改他们的 **.profile** 文件。否则，受信任用户做出的更改可能让人有机可乘。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。用户可以根据个人的喜好设定 **.profile** 文件。系统管理员应用自己的标识，使用下列命令以 root 用户或更高的身份登录用户机:

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

  这样，确保在会话期间使用 root 环境。如果系统管理员在另一个用户会话中确实以 root 用户进行操作，则系统管理员应在整个会话过程指定全路径名。
- 防止输入字段分隔符（**IFS**）环境变量在 **/etc/profile** 文件中被更改。并留意任何用户对 **.profile** 文件中的 **IFS** 变量做更改。它也可以用来改变 **PATH** 值。

用安全的用户帐户设置匿名 FTP

该场景用安全用户帐户设置匿名 **ftp**，采用命令行界面和脚本。

注: 该场景不能用在带有 受控的访问保护概要文件（CAPP）和 评定级别 4+(EAL4+）功能的系统中。

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

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

   如果您没有接收到输出，则不安装文件集。关于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. 验证系统 **/home** 目录下中至少有 8MB 的可用空间，通过输入以下命令:

   ```
   df -k /home
   ```

   步骤 4 中的脚本要求 **/home** 目录下至少有 8MB 的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，切换到 **/usr/samples/tcpip** 目录。例如:

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

   ```
   ./anon.ftp
   ```
5. 当提示Are you sure you want to modify /home/ftp? 时，输入 **yes**。输出类似于下面的显示:

```
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. 切换到 **/home/ftp** 目录。例如:

   ```
   cd /home/ftp
   ```

7. 创建 **home** 子目录，通过输入:

   ```
   mkdir home
   ```

8. 将 **/home/ftp/home** 目录的许可权更改为 drwxr-xr-x，通过输入:

   ```
   chmod 755 home
   ```

9. 切换到 **/home/ftp/etc** 目录，通过输入:

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

10. 创建 **objrepos** 子目录，通过输入:

    ```
    mkdir objrepos
    ```

11. 将 **/home/ftp/etc/objrepos** 目录的许可权更改为 drwxrwxr-x，通过输入:

    ```
    chmod 775 objrepos
    ```

12. 将 **/home/ftp/etc/objrepos** 目录的所有者和组更改为 root 用户和 system 组，通过输入:

    ```
    chown root:system objrepos
    ```

13. 创建 **security** 子目录，通过输入:

    ```
    mkdir security
    ```

14. 将 **/home/ftp/etc/security** 目录的许可权更改为 drwxr-x---，通过输入:

    ```
    chmod 750 security
    ```

15. 将 **/home/ftp/etc/security** 目录的所有者和组更改为 root 用户和 security 组，通过输入:

    ```
    chown root:security security
    ```

16. 更改 **/home/ftp/etc/security** 目录，通过输入:

    ```
    cd security
    ```

17. 通过输入以下 SMIT 快速路径来添加用户:

    ```
    smit mkuser
    ```

    本场景中，我们要添加一个名为 test 的用户。

18. 在 SMIT 字段中，输入以下值:

    ```
    User NAME                                       [test]
    ADMINISTRATIVE USER?                             true
    Primary GROUP                                   [staff]
    Group SET                                       [staff]
    Another user can SU TO USER?                     true
    HOME directory                                  [/home/test]
    ```

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

19. 用下列命令为该用户创建密码:

    ```
    passwd test
    ```

    提示时，输入想要用的密码。您必须再输一次新密码来确认。

20. 切换到 **/home/ftp/etc** 目录，通过输入:

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

21. 复制 **/etc/passwd** 文件到 **/home/ftp/etc/passwd** 文件，使用使用命令:

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

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

```
vi passwd
```

23. 从复制的内容中删去除 root、ftp 和测试用户以外的所有行。编辑之后，内容看起来应该类似于以下的形式:

```
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，退出编辑器。
25. 将 **/home/ftp/etc/passwd** 文件的许可权更改为 `-rw-r--r--`，通过输入:

```
chmod 644 passwd
```

26. 将 **/home/ftp/etc/passwd** 目录的所有者和组更改为 root 用户和 security 组，通过输入:

```
chown root:security passwd
```

27. 复制 **/etc/security/passwd** 文件内容到 **/home/ftp/etc/security/passwd** 文件，使用下列命令:

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

28. 使用您最喜欢的编辑器，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 用户节中删除 `flags = ADMCHG` 的行。编辑之后，内容看起来应该类似于以下的形式:

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

31. 保存更改，退出编辑器。
32. 将 **/home/ftp/etc/security/passwd** 文件的许可权更改为 `-rw-------`，通过输入:

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

33. 将 **/home/ftp/etc/security/passwd** 目录的所有者和组更改为 root 用户和 security 组，通过输入:

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

34. 使用您最喜欢的编辑器，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，退出编辑器。
37. 使用下列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. 切换到 **/home/ftp/home** 目录，通过输入:

```
cd ../home
```

39. 为您的用户新建一个主目录，通过输入:

```
mkdir test
```

这将是新的 ftp 用户的主目录。

40. 将 **/home/ftp/home/test** 目录的所有者和组更改为 test 用户和 staff 组，通过输入:

```
chown test:staff test
```

41. 将 **/home/ftp/home/test** 文件的许可权更改为 -rwx------，通过输入:

```
chmod 700 test
```

这时，您可以在您的机器上设置 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. 作为 anonymous 登录。当提示输入密码时，按下回车键。
3. 切换至新近创建的 test 用户，使用以下命令:

```
user test
```

当提示输入密码时，使用您在步骤第 29 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否存在。例如:

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

输出将 **/home/test** 显示为 **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 提供了一组缺省的系统特殊用户帐户，它使 root 和系统不能拥有所有操作系统文件和文件系统。

警告: 除去系统特殊用户帐户时要谨慎使用。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。不过，小心不要禁用 **root** 用户帐户。如果您除去了系统特殊用户帐户或禁用 **root** 帐户，那么操作系统就不起作用了。

下列的帐户是在操作系统中预定义的:

root root 用户帐户，即 UID 0，有时也称为超级用户帐户，通过该帐户您可执行系统维护任务以及对系统问题进行故障诊断。

daemon
守护程序用户帐户只是为了拥有和执行系统服务器进程及其相关文件而存在。这个帐户保证进程使用适当的文件访问许可权来执行。

bin bin 用户帐户通常拥有大多数用户命令的可执行文件。这个帐户的主要用途是帮助分布重要系统目录和文件的所有权，因此不是任何东西都是由 root 和 sys 用户帐户独占的。

sys sys 用户拥有缺省的分布式文件服务高速缓存的安装点，这必须在客户机上安装或配置 DFS 之前存在。**/usr/sys** 目录也能够储存安装映象。

adm adm 用户帐户拥有两个基本的系统功能:

1. 诊断，相应的工具储存在 **/usr/sbin/perf/diag_tool** 目录中。
2. 记帐，相应的工具储存在下列目录中:
   - **/usr/sbin/acct**
   - **/usr/lib/acct**

- **/var/adm**
- **/var/adm/acct/fiscal**
- **/var/adm/acct/nite**
- **/var/adm/acct/sum**

nobody

nobody 用户帐户由网络文件系统（NFS）产品用于启用远程打印。由于有这个帐户，程序就会允许 root 用户对 root 的临时访问。例如，在打开安全 RPC 或安全 NFS 之前，检查主 NFS 服务器 **/etc/public** 上的密钥以找到被指定了公用密钥和秘密密钥的用户。作为 root 用户，您可以为每个未指定的用户在数据库中创建一个条目，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条目，然后任何用户都可以不作为 root 用户登录，而是运行 **chkey** 程序就可在数据库中创建它们自己的条目。

除去不必要的缺省用户帐户

在操作系统安装过程中，会创建许多缺省的用户和组标识。根据您在系统上运行的应用程序和您的系统在网络中所处的位置，其中某些用户和组标识会成为安全弱点，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达到最小。

下列的表列出了大多数您能够除去的公共的缺省用户标识:

表 6. 您能够除去的公共的缺省用户标识。

用户标识	描述
uucp，nuucp	uucp 协议所用的隐藏文件的所有者。uucp 用户帐户用于 UNIX-TO-UNIX 复制程序，该程序是一组大多数 UNIX 系统上都有的命令、程序以及文件，它允许用户与专线或电话线上的另一个 UNIX 系统通信。
lpd	打印子系统所用文件的所有者
imnadm	（文档库搜索）所用的 IMN 搜索引擎。
guest	允许那些不能访问帐户的用户访问

下列的表列出了可能不需要的公共组标识:

表 7. 可能不需要的公共组标识。

组标识	描述
uucp	uucpand 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是真的不需要的。也许另外会有您不需要的用户和组标识。在您的系统生产之前，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，其指定授权谁访问这些资源。操作系统考虑到了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到那些资源的读或写访问权。赋予对象访问权的用户可以创建额外的对象副本并给第三方到新建对象的访问权。然而，只有此对象的所有者才可以授权第三方到原对象的访问权。只有对象的所有者和 root 用户可以更改对象的访问权。

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）通过添加修改对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访问文件而无需更改基本许可权。

访问控制也涉及使用 **setuid** 和 **setgid** 程序和硬拷贝标签来管理保护资源。操作系统支持多种类型的信息资源或对象。这些对象允许用户处理存储或通信信息。

最重要的对象类型是:

- 文件和目录（用来存储信息）
- 命名管道、消息队列、共享内存段和信号（用来在进程间传送信息）

每个对象有相应的所有者、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 特权的情况下不能更改。

对 System V 进程间通信（SVIPC）对象，创建者和所有者都可以更改所有者。SVIPC 对象有相关的含有所有者的所有权限的创建者（包括访问授权）。然而，即使有 root 特权也不能更改创建者。

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

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。（如上所述，SVIPC 对象有不得更改并共享对象组访问授权的相关创建组。）

注: 文件的访问控制列表不能超出一个内存页（大约 4096 字节）的大小。

维护访问控制列表，使用 **aclget**、**acledit** 和 **aclput** 命令。

数字方式（用八进制记号）的 **chmod** 命令可以设置基本许可权和属性。**chmod** 子例程（本命令调用的那个）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。要得到关于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

在多数情况下许可位机制允许对资源的有效访问控制。但是对于更严格的访问控制，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** 程序执行其所有者的访问权，而 **setgid** 程序有其组的访问权并且两个位都可以依照许可机制来设置。

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。这样，**setuid** 和 **setgid** 程序允许间接授权访问权的用户编程的访问控制。程序作为可信子系统，控制用户的访问权。

虽然可以更有效地使用这些程序，如果不小心设计将有安全性危险。特别地，程序必须在它仍有其所有者的访问权时必须从不返回控制给用户，因为这样将允许用户无限制地使用用户的权限。

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。带有有效用户和组标识 0 的用户为特权用户。

带有效用户标志 0 的进程为 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** 命令允许调用的所有程序和 root 用户进程有相同的功能，而且 **su** 是管理系统的灵活的方法，但是不是非常的安全。

使一个程序成为 **setuid-root** 程序意味着此程序是设置了 setuid 位的 root 用户所有的程序。**setuid-root** 程序提供对普通用户不需要安全性许可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设置到文件所有者、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）。

在访问控制列表中，基本许可权为下列格式，并带有表示为 rwx（在每个没有指定许可权的地方用连字符（-）代替）的 *Mode* 参数:

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

属性

可以添加三个属性到访问控制列表:

setuid (SUID)
设置用户标识（Set-user-ID）方式位。本属性将进程实际的和保存的用户标识设置为所执行程序的所有者标识。

setgid (SGID)
设置组标识（Set-group-ID）方式位。本属性将进程实际的和保存的用户标识设置为所执行文件的组标识。

savetext (SVTX)
对目录使用，表示只有文件所有者能链接到指定目录中的文件或取消链接。

这些属性以如下格式添加:

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

扩展许可权

扩展许可权允许文件的所有者更严格地定义到那个文件的访问。扩展许可权通过为指定的个人、组或组和用户的结合体指定允许、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	授权用户或组到文件的指定访问权
deny	限制用户或组使用到文件的指定访权
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那个访问拒绝。

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，扩展许可权有如下格式:

```
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**（在每个没有指定许可权的地方用连字符（-）代替）。*UserInfo* 参数表示成 `u:UserName` 或 `g:GroupName` 或逗号隔开的 `u:UserName` 和 `g:GroupName` 的联合体。

> **注**: 如果在一个项中指定多于一个的用户名，那个项不能用来访问控制判定，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 的各部分和它们的含义如下:

- 第一行表示打开了 **setuid** 位。
- 下一行引入了基本许可权，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和文件组。只有 **chown** 命令和 **chgrp** 命令可以更改这些文件属性。
- 下一行表示扩展许可权，这是可选的。
- 下一行表示启用下列扩展许可权。
- 最后四行是扩展项。第一个扩展项授权用户 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 为 gateway 组和 mail 组的成员，就有读（r）访问权限。如果用户 john 不是这两个组的成员，本扩展许可权不适用。
- 最后一个扩展项授权在 account 和 finance *两*个组中的任何用户读（r）和写（w）权限。

注: 对请求访问受控对象的进程可适用多个扩展项，限制项优于许多方式。

请参阅 《*AIX 5L V5.2 命令参考大全*》中的 **acledit** 命令来得到完整的语法。

访问授权

信息资源的所有者对管理访问权负责。资源由许可权位保护，这包含在对象方式中。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。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，关联此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:

- 对在访问控制列表（ACL）中的每个访问控制项（ACE），比较标识列表和进程的标识。如果匹配，进程接受此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）并且不是限制（包含在限制并集中），则授权访问。否则，拒绝访问。

具有用户标志 0 的进程为 *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的相应的有效标识，则 ACL 的标识列表匹配进程。用户类型的标识匹配等同于进程的有效用户标识，且如果组标识等同于进程的有效组标识或副组标识的一个则组类型的标识匹配。例如，ACE 带有如下的标识列表:

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

将匹配带有有效用户标识为 fred 和组设置为:

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

但是不匹配带有有效用户标识 fred 和组设置为:

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

注意，带有如下标识列表的 ACE 将匹配上两个进程:

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

也就是说，ACE 标识列表的功能是设置必须包含指定的授权访问的条件。

当对象第一次访问时，在系统调用级上做这些对象的所有访问许可检查。因为 System V 进程间通信（SVIPC）对象为无状态访问，对每一个访问做检查。对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（相对与进程工作目录），也可以是绝对的（相对进程根目录）。所有名称解析通过搜索其中一个开始。

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只对生成它们的用户有效。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

猜测密码是系统经历的最通常的攻击方法之一。因此，控制和监视您的密码限制策略是及其重要的。AIX 提供机制以帮助您执行更强大的密码策略，例如建立以下项目的值:

- 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，可使用的字母的最小数目

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

- 『什么是一个好密码？』
- 第 38 页的『/etc/passwd 文件』
- 第 39 页的『/etc/passwd 文件和网络环境』
- 第 39 页的『隐藏用户名和密码』
- 第 39 页的『设置推荐的密码选项』
- 第 41 页的『扩展密码限制』

什么是一个好密码?

如果密码符合下列要求，则它们就是抵御未授权进入系统的第一道有效防线:

- 大小写字母的混合
- 字母、数字或标点符号的结合。它们也可以包含特殊字符，比如 `~!@#$%^&*()-_=+[]{}|\;:'",.<>?/<space>`
- 未在任何地方写下来
- 如果使用 **/etc/security/passwd** 文件，长度为至少七个字符到最大八个字符（使用注册表—如 LDAP—的认证实现，可拥有超出这个最大长度的密码）
- 不是在字典中可查到的真实单词
- 不是键盘上字母的模式，比如 *qwerty*
- 不是真实单词或已知模式的反向拼写
- 不包含任何与您自己、您家庭或朋友有关的信息
- 不与从前一个密码的模式相同
- 可以被较快输入，以至旁边人不能确定您的密码

除了这些机制，您可以通过限制密码不可以包含可猜测的标准 UNIX 单词，从而进一步执行更严厉的规则。该功能使用 **dictionlist**，它要求您首先安装 **bos.data** 和 **bos.txt** 文件集。

要实现先前定义的 **dictionlist**，请编辑 **/etc/security/users** 文件中的下列行:

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

/usr/share/dict/words 文件使用 **dictionlist** 来预防使用标准 UNIX 单词作为密码。

/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** 文件是以冒号分隔的，它包含下列信息:

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

这里是一个 **/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
```

AIX 不像 UNIX 系统那样，将加密的密码存储在 **/etc/password** 文件中，而是存储在缺省情况下的 **/etc/security/password** 文件中，该文件唯有超级用户可读。AIX 使用 **/etc/passwd** 中归档的密码来表示是否有一个密码或帐户是否被封锁。

/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--`。如果用户标识有密码，则密码字段会有 `!`（感叹号）。如果用户标识没有密码，则密码字段会有一个 `*`（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** 文件中最后四个条目，它们是基于以上显示的 **/etc/passwd** 文件中的条目。

```
guest:
        password = *

nobody:
        password = *

lpd:
        password = *

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

请注意，用户标识 jdoe 在 **/etc/security/passwd** 文件中没有条目，这是由于它在 **/etc/passwd** 文件中没有设置的密码。

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。

/etc/passwd 文件和网络环境

传统上，在网络环境中，用户必须在每个系统上有一个帐户从而获得对那个系统的访问权。这通常意味着用户要在每个系统上的每个 **/etc/passwd** 文件中有一个条目。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。为了解决这个问题，人们开发了一些方法使 **/etc/passwd** 文件中的信息在整个网络中可用，包括以下方法:

- 网络信息系统（Network Information System，NIS）
- NIS+

这两个主题都在 NIS 一章中讨论。

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，这样它的内容像明文一样清楚显示。要查找这些文件，运行下列命令:

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

您找到这些文件后，请删除它们。保存密码的一个更有效的方法是设置 Kerberos。

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。但为了提供一些额外的安全性，操作系统提供可配置的密码限制。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。密码选项和扩展的用户属性位于 **/etc/security/user** 文件中。这是一个包含用户属性节的 ASCII 文件。每当为用户定义新密码时，就执行这些限制。所有密码限制都是针对每个用户来定义的。通过在 **/etc/security/user** 文件的缺省节中保存限制，对所有用户实行相同限制。为了维护密码安全性，所有密码必须受到类似的保护。

操作系统也为管理员提供扩展密码限制的方法。使用 **/etc/security/user** 文件的 **pwdchecks** 属性，管理员可以将新建子例程（称为方法）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，并由操作系统实行该策略。要了解更多信息，请参阅第 41 页的『扩展密码限制』。

请明智地应用密码限制。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（用户可能会写下密码），都会危及密码安全性。最终地，密码安全性要依靠用户。简单的密码限制，加上明智的指导和偶尔的审计以检查当前密码是否是唯一的，是最好的策略。

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

表 8. 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**	NA[注 1]	NA
histexpire	密码可重用前的星期数。	26	0	260[注 2]
histsize	可允许的密码重复次数。	20	0	50

表 8. 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
maxage	必须更改密码前的最大星期数。	8	0	52
maxexpired	超过 *maxage*、用户要更改失效密码可允许的最大星期数。（root 用户免于此规定。）	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。该值不可设置为非零值，除非管理员总是很容易联系到，来重置一个最近更改过、却被意外危及的密码。	0	0	52
minalpha	密码必须包含的字母字符的最小数目。	2	0	8
mindiff	密码必须包含的唯一字符的最小数目。	4	0	8
minlen	密码长度的最小值。	6（对 root 用户是 8）	0	8
minother	密码必须包含的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	NA	NA
pwdchecks	该条目通过使用一个检查密码质量的定制代码，可用来增强 **passwd** 命令。	要了解更多信息，请参阅第 41 页的『扩展密码限制』。	NA	NA

注:

1. NA 意味着*不适用*。
2. 最多保留 50 个密码。

对于受控访问保护概要文件和评估保证级别 4+（Controlled Access Protection Profile and Evaluation Assurance Level 4+, CAPP/EAL4+）系统，请使用第 11 页的『用户与端口配置』中推荐的值。

如果文本处理安装在系统上，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。由于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** 属性的值加上 **minother** 属性的值，这两个值中较大的一个来设置。密码的最大长度为八个字符。**minalpha** 属性的值加上 **minother** 属性的值永远不可以大于八。如果 **minalpha** 的值加上 **minother** 属性的值大于八，则 **minother** 属性的值减为八，减去 **minalpha** 属性的值。

如果 **histexpire** 属性和 **histsize** 属性的值都设置好了，系统保留满足两个条件所要求的密码数目，但不超过系统限制的每个用户 50 个密码的数目。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，您可以使用 **chuser** 命令来更改属性的值。

可以与该文件一起使用的另一些命令有：**mkuser**、**lsuser** 和 **rmuser**。**mkuser** 命令为 **/etc/security/user** 文件中的每个新建用户创建一个条目，并用 **/usr/lib/security/mkuser.default** 文件中定义的属性初始化该条目的属性。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（密码组合限制）可由系统管理员进行扩展，以提供对特定站点的限制。扩展限制通过添加称为 *methods* 的子例程进行，该子例程在密码更改过程被调用。**/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确认的子例程接口。要正确地扩展密码组合限制，系统管理员必须在写密码限制方法时，编制这个接口的程序。请谨慎对待扩展密码组合限制。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。请只使用您信任的代码。

用户认证

识别和认证建立用户身份。要求每一个用户登录系统中。如果帐户有名称的话（安全系统中，所有帐户必须密码或无效），用户提供一帐户和密码的用户名称。如果密码正确，用户登录到该帐户，用户获得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** 属性把认证的另一种方法集成在系统中。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使得这些密码生效。

其它 **SYSTEM** 属性值是 **compat**、**files** 和 **NONE**。当名称解析（和以后的认证）符合本地数据库时，使用 **compat** 标记，而且如果找不到解析，就会尝试网络信息服务（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。

在 **/usr/lib/security/methods.cfg** 中定义了 **SYSTEM** 属性可接受的其它标记。

注：root 用户总是采用本地系统安全文件得到认证。root 用户的 **SYSTEM** 属性记录在 **/etc/security/user** 中特别设置为 **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用这个标识做标记，并且当您生成审计记录时也可以检查所有的审计事件。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》*。

磁盘限额系统概述

磁盘限额系统允许系统管理员控制可能分配给用户或组的文件和数据块的数量。下面节提供了有关磁盘限额、运行以及使用的信息:

- 『理解磁盘限额系统』
- 『从超限额条件中恢复』
- 『设置启动磁盘限额系统』

理解磁盘限额系统

磁盘限额系统，它基于 Berkeley 磁盘限额系统，提供了控制使用磁盘空间的有效方式。为个人用户或组定义限额系统，并且为每一类文件系统维护限额系统。

磁盘限额系统基于下列参数建立限额，可以使用 **edquota** 命令更改这些参数:

- 用户或组的软限额
- 用户或组的硬限额
- 限额宽延时间

*软限额*定义了 1 KB 的磁盘块数或文件数，用户必须保留。*硬限额*定义了在已创建的磁盘限额下用户可以累积的最大磁盘块或文件。*限额宽延时间*允许用户在短期内（缺省值是一周）超过软限额。如果在特定的时间内用户不能把使用空间减小到软限额以下，系统会会把软限额解释为最大允许的分配，不再给用户分配更多存储空间。通过移除足够的文件把使用空间减小到软限额以下用户可以重新设置该条件。

磁盘限额系统在 **quota.user** 和 **quota.group** 文件中跟踪用户和组的限额，这两个文件在已启用限额的文件系统的根目录下。用 **quotacheck** 和 **edquota** 命令创建这些文件而且用限额命令可读取这些文件。

从超限额条件中恢复

在超过限额时为了减小文件系统使用，可以使用下列方法:

- 杀死致使文件系统达到限额的当前进程，移除过剩的文件使限制低于限额，并且重试失败的程序。
- 如果正在运行诸如 vi 的编辑器，使用 shell 转义序列检测文件空间，移除多余文件并在没有丢失编辑的文件下返回。或者，如果正在使用 C 或者 Korn shell，可以用 Ctrl-Z 键序列暂挂编辑器，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限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。

设置启动磁盘限额系统

通常，只有包含用户主目录和文件的文件系统才需要磁盘限额。考虑在下列条件下执行磁盘限额系统:

- 系统已限制了磁盘空间。
- 需要更多文件系统安全性。
- 磁盘使用程度很大，例如在许多大学。

如果这些条件不使用于您的环境，那么可以执行磁盘限额系统不去创建磁盘使用限制。

磁盘限额系统只使用于日志文件系统。

注: 不必为 **/tmp** 文件系统创建磁盘限额。

使用下列步骤设置磁盘限额系统:

1. 用 root 权限登录。
2. 确定哪些文件系统需要限额。

   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，因此必须没有限额。
3. 使用 **chfs** 命令包含 **/etc/filesystems** 文件中的 **userquota** 和 **groupquota** 限额配置属性。下列示例使用 **chfs** 命令启用 **/home** 文件系统中用户限额:

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

   启用 **/home** 文件系统的用户和组限定额，键入:

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

   /etc/filesystems 文件中的相应记录显示如下:

   ```
   /home:
   dev         = /dev/hd1
   vfs         = jfs
   log         = /dev/hd8
   mount       = true
   check       = true
   quota       = userquota,groupquota
   options     = rw
   ```
4. 选择地指定备用磁盘限额文件名称。**quota.user** 和 **quota.group** 文件名称是缺省名称，在已应用限额的文件系统的根目录下。可以用 **/etc/filesystems** 文件中的 **userquota** 和 **groupquota** 属性为这些限额文件指定备用名称或目录。

   下列示例使用 **chfs** 命令为 **/home** 文件创建用户和组限额，并且给 **myquota.user** and **myquota.group** 限额文件命名:

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

   /etc/filesystems 中相应的记录显示如下:

   ```
   /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. 如果以前没有计算它们，那么计算指定文件系统。
6. 为每一个用户或组设置需要的限额限制。使用 **edquota** 命令创建每一个用户或组的软和硬限制为了得到允许的磁盘空间和最大文件数量。

   下列示例记录为 *davec* 用户显示限额限制:

   ```
   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 的最大磁盘空间的 30 KB。在最多创建 200 个文件中，*davec* 已经创建了 73 个。该用户有 50 KB 磁盘空间和 50 个文件缓冲分配给临时存储。

   当为多用户建立磁盘限额时，使用带 **edquota** 命令的 **-p** 标志为另一用户复制用户的限额。

为用户 nanc 复制已为用户 davec 建立的限额，键入:

```
edquota -p davec nanc
```

7. 用 **quotaon** 命令启用限额系统。**quotaon** 命令启用指定文件系统的限额，或使用 **-a** 标志为带有限额（如 **/etc/filesystems** 文件指定的）的所有文件启用限额。
8. 使用 **quotacheck** 命令检测限额文件和实际磁盘使用率的一致性。

   注: 建议您每当第一次启用文件系统限额以及重新启动系统之后，检测它们的一致性。

   在系统启动过程中，启用检测和打开限额，在 **/etc/rc** 文件的结尾添加下列行:

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

第 3 章 审计过程

审计过程子系统让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反。

本节包含如下主题的信息:

- 『审计过程子系统』
- 第 46 页的『事件选择』
- 第 47 页的『审计过程子系统配置』
- 第 48 页的『审计日志程序配置』
- 第 51 页的『设置启动审计过程』

审计过程子系统

审计过程子系统有如下功能:

- 『检测事件』
- 『收集事件信息』
- 第 46 页的『处理审计跟踪信息』

系统管理员可以配置每一项功能。

检测事件

事件检测在整个可信计算基（TCB）、在内核（管理状态码）和可信程序（用户状态码）中都是分布式的。在系统中发生的任何安全性相关的事件为可查的事件。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负有责任的安全策略的试图或实际的违例、或者两者都是。检测可查的事件的程序和内核模块报告这些事件到系统审计日志程序，这作为内核的一部分运行并可由子例程（对可信程序审计过程）或在内核过程调用中（对主管审计过程）访问。报告的信息包含可查的事件的名称、此事件的成功与否以及任何附加的跟安全性审计过程有关的指定事件的信息。

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事件展开。本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查的事件的内部内核过程调用界面。

审计日志程序用来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）和审计跟踪，其包含特定事件的信息。审计日志程序将每个后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
: 跟踪写到备用文件，用来作安全的和长期的存储。

STREAM 方式
: 跟踪写到循环缓冲区，缓冲区通过审计伪设备读取。STREAM 方式提供快速的响应。

可在前端（事件记录）和后端（跟踪处理）配置信息收集。事件记录以每个用户为基础选择的。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，逐个地配置本方式，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 方式审计过程配置为在跟踪的可用的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、或格式化输出、或任何这些的适当的联合（如果有的话）。通过霍夫曼编码压缩。通过类标准查询语言（SQL）选择审计记录来过滤（使用 **auditselect** 命令），这提供了选择查看和选择保留审计跟踪。格式化审计跟踪记录可以用来检查审计跟踪、生成周期的安全性报告以及打印审计跟踪到纸上。

可实时监视 STREAM 方式审计跟踪，从而能够快速监视威胁。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的程序处理，虽然某些过滤程序更适合于某种方式或另一种。

事件选择

系统上的可查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，可查的事件必须包含系统上的安全性相关事件。用来定义可查的时间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。为说明本讨论，*检测事件*是任何单个的可查事件的实例；例如，可在不同的地方检测到某事件。基本原则为：选定有类似安全性属性的检测事件为相同的可查事件。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
- 负责任的事件
  - 添加用户、在密码数据库中更改用户属性
  - 添加组、在组数据库中更改组属性
  - 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
  - 审计过程管理：选择事件和审计跟踪、转换打开或关闭、定义用户审计过程类
- 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 和关机
  - RAS 配置
  - 其它系统配置
- 安全性违例（潜在的）
  - 访问许可拒绝
  - 特权失败
  - 诊断检测故障和系统错误
  - 尝试更改 TCB

审计过程子系统配置

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本进程的信息的本地状态变量。这两种变量决定了是否用可信计算基（TCB）和程序来检测事件。关闭指定进程的 TCB 审计过程允许此进程做它自己的审计过程并且不忽略系统负责任的策略。允许可信程序自身审计给更有效率和有效的信息收集提供方便。

收集审计过程子系统信息

信息收集有**事件选择**和**内核审计跟踪**两种方式。提供登录信息给界面（检测可查的事件的 TCB 组成部分使用的）和界面配置（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

可查的事件有下列界面记录: 用户状态和监督状态。TCB 的用户状态部分使用 **auditlog** 或 **auditwrite** 子例程，而 TCB 的监督状态部分使用一系列内核过程调用。

对每个记录，审计事件日志程序附加审计标题为指定事件信息的前缀。此标题标识审计本事件针对的用户和进程以及事件发生的时间。检测事件的代码支持事件类型并返回代码或状态以及可选的、额外的特定事件的信息（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。

符号地定义事件而不是数字地定义。在不使用事件注册计划时，这减少了名称冲突的可能。由于子例程是可查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内核界面扩展或重定义。

审计记录格式

审计记录由公共标题、跟有指定记录的审计时间的审计跟踪组成。在 **/usr/include/sys/audit.h** 文件中定义标题的结构。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。

通常收集在审计标题中的信息由登录例程来确保它的准确性，而在审计跟踪中的信息是由检测时间的代码提供的。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** 子例程写记录到审计跟踪。审计日志程序内核组成部分记录指定主题信息（用户标识、进程标识、时间）到标题并附加此到另外的信息。调用程序仅支持事件名称和在标题中的结果字段。

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

审计事件选择有如下类型:

每个进程审计过程

为了有效选择进程事件，操作系统允许系统管理员定义审计类。审计类是系统中的基本审计事件的子集。审计过程类提供方便的基本审计过程事件的合理的分组。

对系统中的每个用户，系统管理员定义确定可为用户记录的基本事件的审计类的集合。用户运行的每个进程标记有其审计类。

每对象审计过程

操作系统提供通过名称访问对象的审计过程；即指定对象（通常是文件）的审计过程。按名称的对象审计过程防止必须涵盖所有对象访问，以此来审计几个相关的对象。另外，可以指定审计过程方式，以便只记录指定的方式（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之处。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。请参阅下图来了解审计 BIN 方式:

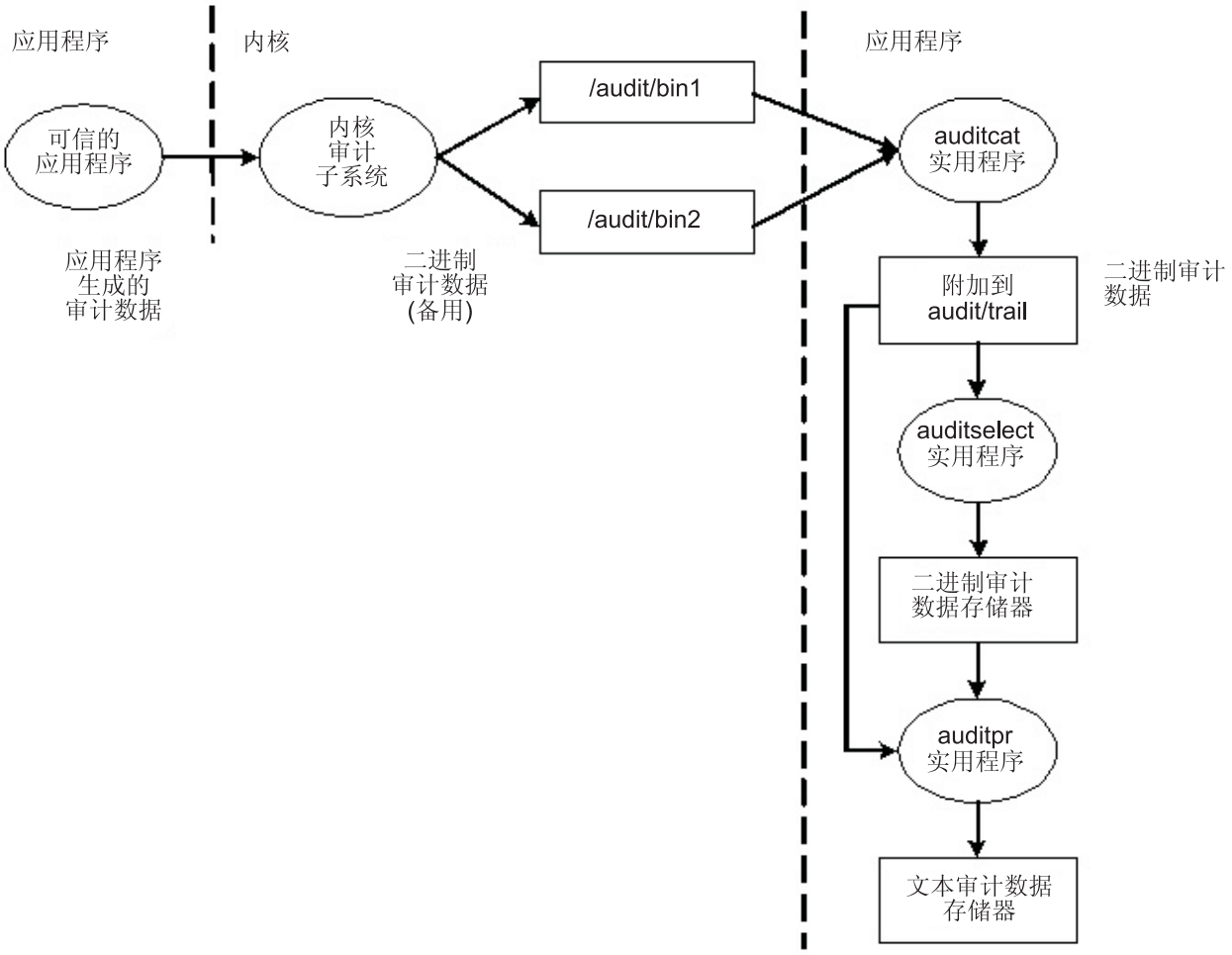


图 1. 审计 BIN 方式的过程。. 本说明显示了审计 BIN 方式的过程。

交替使用 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，转移内容到**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。如果系统没有此处指定的 512 位的块数总数，它生成 **syslog** 消息。

如果启用审计过程，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，它只是返回开头。进程从名为 **/dev/audit** 的伪设备读取信息。当进程打开此设备时，为此进程创建一个新的通道。可选择地，可将在通道上读取的事件指定为审计类的列表。请参阅下图来了解审计 STREAM 方式:

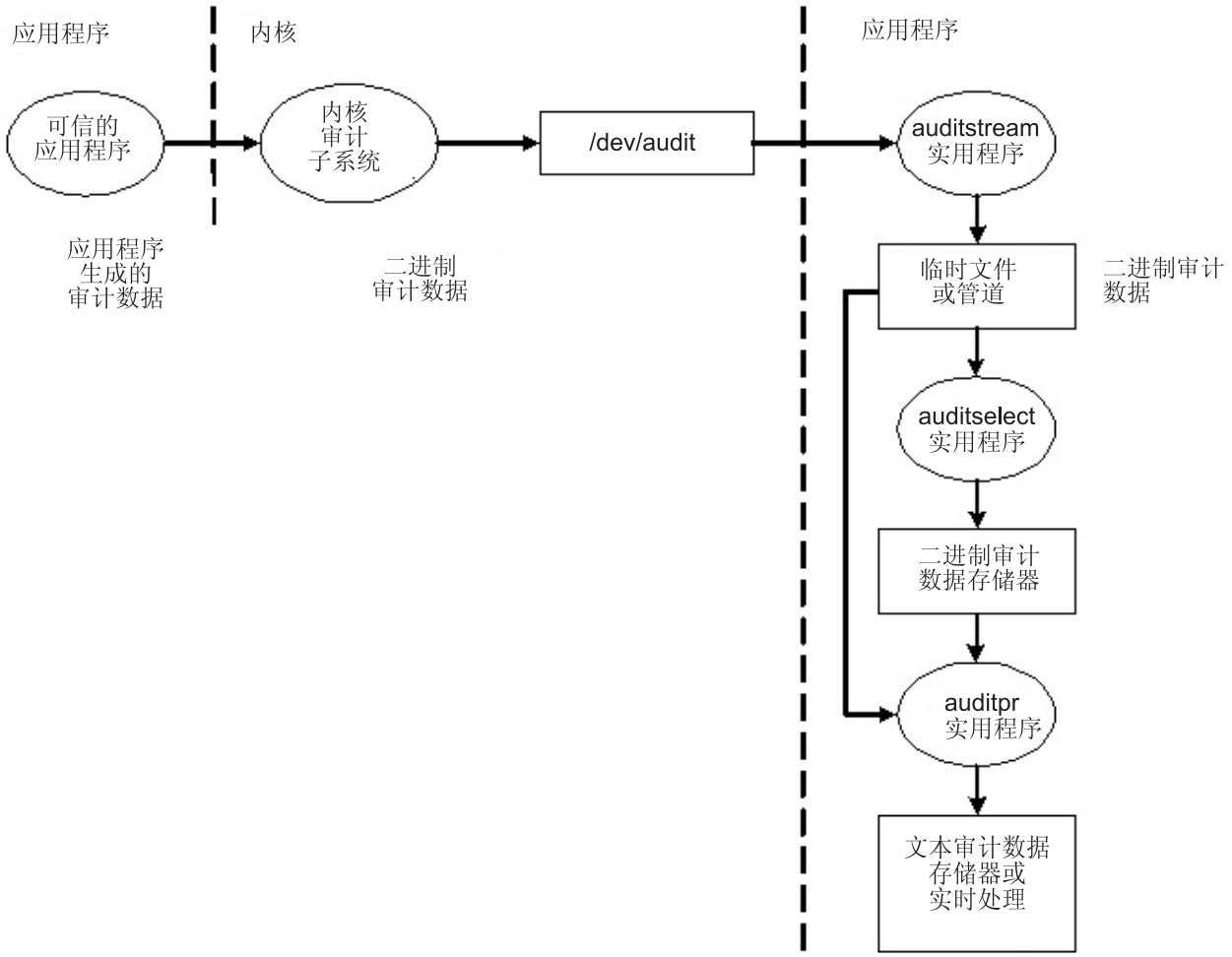


图 2. 审计 STREAM 方式的过程。. 本插图显示了审计 STREAM 方式的过程。

STREAM 方式的主要用途是允许及时地读取审计跟踪，这可用来监视实时威胁。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，这允许近时处理，而且同时防止审计信息在源主机受到篡改。

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更易使用，这特别适用于 STREAM 方式的审计过程。

auditselect

可用来用类似 SQL 语句仅选出特定的审计记录。例如，仅选择由用户 **afx** 生成的 **exec()** 事件，输入如下:

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

auditpr

用来将 bin 审计记录转换为人类可读表单。所显示的信息量取决于在命令行中指定的标志。要得到所有可用信息，应该如下运行 **auditpr**:

```
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 bin 审计跟踪。这在需要联接几个系统的审计跟踪时非常有用。**auditmerge** 命令获取在命令行中的跟踪的名称并发送合并的 bin 跟踪到标准输出，所以仍需要使用 **auditpr** 来使它成为可读的。例如，可运行 **auditmerge** 和 **auditptr** 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受怀疑的程序，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，输入如下:

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

文件 **/tmp/vi.watch** 将显示编辑器会话的所有 FILE_Open 事件。

设置启动审计过程

下列是启动审计过程子系统必须采取的步骤的概述。关于更多特定信息，请参考这些步骤里注释的配置文件。

1. 从 **/etc/security/audit/events** 文件里的列表选择系统活动（事件）审计。如果添加新建的审计事件到应用程序或内核扩展，必须编辑文件添加新事件。
   - 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，必须添加事件到文件。
   - 确保任意新建审计事件的格式指示信息包含在 **/etc/security/audit/events** 文件里。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** 文件的类节里的审计类。
3. 如下指定单独用户的审计类和指定审计到需要审计的文件:
   - 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，为文件添加节到 **/etc/security/audit/objects** 文件。
   - 也可以通过编辑 **/usr/lib/security/mkuser.default** 为新用户指定缺省审计类。当生成新建用户 ID 时，文件保留要使用的用户属性。例如，如下为所有新建用户 ID 使用 **general** 审计类:

     ```
     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 systrem 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** 文件里，配置要使用的 BIN 收集、STREAM 收集或两种方式都用。通过为审计数据使用分开的文件系统确信审计数据不能和文件空间的其它数据竞争。确保审计数据有足够的空间。如下配置数据收集类型:
   - 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 bins 和 trail，并且指定包含 binmode 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**。

c. 确信审计 bins 足够大能满足需要并且如果正在填充文件系统设置 **freespace** 参数从而获取警告。

d. 包含在 **/etc/security/audit/bincmds** 文件中审计管道里处理审计 audit 的 shell。

- 配置 STREAM 收集

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

b. 编辑 streammode 节指定包含 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**。

c. 包含在 **/etc/security/audit/streamcmds** 文件中审计管道里处理审计 stream 的 shell 命令。

5. 当完成任意必须的更改配置文件时，准备使用 **audit start** 命令启用审计子系统。
6. 使用 **audit query** 命令查看在审计哪一个事件和对象。
7. 使用 **audit shutdown** 命令再次取消激活审计子系统。

选择审计事件

审计的用途是检测可能有损系统安全性的活动。当未授权用户执行时，下列活动违反系统安全性并且是审计的对象:

- 在可信计算基里从事活动
- 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
- 把信息传入到传出系统

审计系统没有审计事件的缺省设置。不得不根据需要选择事件或事件类。

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** 文件里。那么必须添加事件到 **/etc/security/audit/config** 文件里的相应类或到 **/etc/security/audit/objects** 文件里的对象节。请参阅系统上 **/etc/security/audit/events** 文件里的审计事件和跟踪格式化说明列表。关于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。然后审计类分配给用户。

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。

下列是一些典型的审计类:

general 改变系统状态和更改用户认证的事件。审计试图取得系统访问控制。
objects 安全性配置文件的写入权限。
kernel 通过内核的进程管理功能生成内核类里的事件。

如下是 **/etc/security/audit/config** 里节的示例:

```
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。审计记录写进临时的 bin 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

下列示例用于监控关键文件的实时文件存取:

1. 设置监控关键文件改变的列表，例如 **/etc** 里的全部文件，并且在 **objects** 文件里配置它们以获得 **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全部文件写操作，但在生产环境下可以有一个后端，它发送事件到入侵检测系统。) **/etc/security/audit/streamcmds** 文件与下列相似:

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

3. 在 **/etc/security/audit/config** 里设置 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。

一般审计日志情景说明的示例

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在可管理的大小内。

以下是审计检测中审计事件:

FILE_Write	要知道对配置文件的文件写操作，因此此事件用于 **/etc** 树里的全部文件。
PROC_SetUserIDs	用户 id 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	通知丢失记录
CRON_JobAdd	新建 **cron** 作业
AT_JobAdd	新建 **at** 作业
USER_Login	所有登陆
PORT_Locked	因为太多无效的尝试，锁定终端

以下是如何生成一般审计日志的示例:

1. 设置受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，如下所示:

   ```
   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** 文件与下列相似:

   ```
   /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. 添加 **custom** 审计类到 **/usr/lib/security/mkuser.default** 文件，因此新建 ID 将自动拥有权限审计相关调用:

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

5. 使用 SMIT 或 **crfs** 命令创建名为 **/audit** 的新文件系统。应该相当大足以容纳两个 bin 和一个大的审计跟踪。

6. 现在运行 **audit start** 并查看 **/audit**: 应该观察到两个 bin 文件和一个初始为空的 **trail** 文件。在使用系统一定时间后，您应该在 **trail** 文件里有了审计记录，它们可以用以下命令阅读:

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

此例仅使用一些事件。要看到全部事件，您可以为所有用户指定类名 **ALL**。这将生成大量的数据。可以添加与用户更改和权限更改有关的全部事件到 **custom** 类。

第 4 章 安全子系统的 LDAP 利用

轻型目录访问协议（LDAP）定义了一种在客户机／服务器模型的目录（数据库）中本地或远程访问和更新信息的标准方法。群集的主机可以使用 LDAP 方法以允许集中安全认证以及访问用户和组信息。这个功能可期望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 利用可实现为 LDAP 认证装入模块。就概念而言，它与其它装入模块（如 NIS、DCE 以及 Kerberos 5）相似。该装入模块在 **/usr/lib/security/methods.cfg** 文件中有所定义。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后，大多数高级的 API、命令以及系统管理工具还是以通常的方式运作。引进 **-R** 标志以使大多数高级的命令在不同的装入模块下运作。例如，要从客户机创建 LDAP 用户名 joe，使用下列的命令:

```
mkuser -R LDAP joe
```

客户机系统通过在 **/etc/security/user** 文件中的用户 SYSTEM 属性来检查用户是否是 LDAP 用户。如果将用户的 SYSTEM 属性设置为 LDAP，那么用户只能通过 LDAP 来认证。如果将 default 节的 SYSTEM 属性设置为 LDAP，那么就会将所有不具有 SYSTEM 属性设置的用户视为 LDAP 用户。LDAP 关键字可以和其它在第 41 页的『用户认证』中描述的 SYSTEM 属性值一起使用。客户机端通过 **secldapclntd** 守护程序与服务器进行通信。**secldapclntd** 守护程序也负责存储。

安装 LDAP 安全信息服务器

要将系统安装成 LDAP 安全信息服务器，让它能通过 LDAP 提供认证、用户和组信息，必须安装 LDAP 服务器和客户机软件包。必须将 LDAP 服务器配置成为客户机和服务器。LDAP 服务器也要求有 DB2 数据库。如果要求安全套接字层（SSL），那么必须安装 GSKit。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 命令可用于安装 LDAP 安全信息服务器。其建立称为 **ldapdb2** 的数据库，用来自本地主机的用户和组信息植入数据库，设置 LDAP 服务器管理员 DN（区别名）和密码。它可选择性地安装用于客户机／服务器通信的 SSL。然后 **mksecldap** 装入服务器插件（**libsecldap.a**）并启动 LDAP 服务器进程（**slapd**）。**mksecldap** 命令将一个条目加进 **/etc/inittab** 文件以在每次重新引导时启动 LDAP 服务器。整个 LDAP 服务器安装是通过 **mksecldap** 命令而完成的，该命令更新 **slapd.conf** 文件（SecureWay® Directory V 3.1） 或 **slapd32.conf** 文件（SecureWay Directory V 3.2）。没有必要配置 LDAP Web 管理接口。

在 LDAP 服务器设置过程中将所有本地系统的用户和组迁移到 LDAP 服务器。这个步骤可以选择下列的 LDAP 模式的其中之一:

AIX 特定模式
: 包含 aixAccount 和 aixAccessGroup 对象类。这个模式提供 AIX 用户和组的全套属性。

NIS 模式（RFC 2307）
: 包含 posixAccount 和 posixGroup 帐户，并由几个供应商的目录产品使用。NIS 模式只定义 AIX 使用的一个小子集属性。

具有完全 AIX 支持的 NIS 模式
: 包含 posixAccount 和 posixGroup 对象类以及 aixAusAccount 和 aixAusGroup 对象类。aixAusAccount 和 aixAuxGroup 对象类提供了 AIX 使用的属性，但 NIS 模式没有定义这个属性。推荐使用具有完全 AIX 支持的 NIS 模式来安装 LDAP 服务器，除非有必要安装特定于 AIX 模式 LDAP 服务器以与现有的 LDAP 服务器兼容。

所有的用户和组信息储存在公共的 AIX 树（后缀）。缺省的后缀是 "cn=aixsecdb"。**mksecldap** 命令通过 **-d** 标志来接受用户提供的后缀。如果用户提供的前缀的第一相对区别名（RDN）不叫 "cn=aixsecdb"，那么 **mksecldap** 命令使用 "cn=aixsecdb" 作为用户提供后缀的前缀。这个 AIX 树是受 ACL（访问控制列表）保护的。A 客户机必须绑定为 LDAP 服务器管理员以便能够访问 AIX 树。

即使 LDAP 服务器是为了其它用途（如蓝页信息）而安装的，**mksecldap** 命令也会运作。在本例中，**mksecldap** 添加了 AIX 树，并将现有数据库的 AIX 安全信息植入其中。这个树是受保护的访问控制列表，并独立于其它树。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: 推荐在运行 **mdsecldap** 命令来安装安全服务器以便共享同一数据库之前备份现有的数据库。

在成功安装 LDAP 安全信息之后，必须将同一主机设置为客户机，以便完成用户和组管理，并且 LDAP 用户能够登录这个服务器。

如果安装 LDAP 安全信息服务器没有成功，您可以运行带有 **-U** 标志的 **mksecldap** 命令来撤销安装。这会使 **slapd.conf**（或 **slapd32.conf**）文件恢复到原来的状态。在试图安装失败后，尝试再次运行 **mksecldap** 命令前，运行具有 **-U** 标志的 **mksecldap** 命令。否则，残余的安装信息会保留在配置文件里，这会引起后继的安装失败。作为安全预防，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，那就确定采取什么步骤以便从失败的安装试图中的恢复过来。

从 AIX 5.2 开始，**mknisldap** 命令也可用来安装 LDAP 安全信息服务器。**mknisldap** 命令用与 **mksecldap** 命令同样的方式安装服务器，并且将其它 NIS 数据以及用户和组迁移到 LDAP 服务器。

关于更多安装 LDAP 安全信息服务器的信息，请参阅 **mksecldap** 命令。

安装 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，必须创建密钥，同时必须将 LDAP 服务器 SSL 密钥证书添加到这个密钥。

可以使用 **mksecldap** 命令来安装客户机。要客户机与 LDAP 安全信息服务器联系，就必须在安装过程中提供服务器名称。也需要服务器管理员域名和密码以使客户机能够访问服务器上的 AIX 树。**mksecldap** 命令将服务器管理员域名、密码、服务器名称、服务器上的 AIX 树域名以及 SSL 密钥路径和密码保存到 **/etc/security/ldap/ldap.cfg** 文件。

在客户机安装过程中可以向 **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到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重要的。

通过客户机端守护程序（**secldapclntd**），客户机可与 LDAP 安全信息服务器联系。如果在客户机启用了装入模块，那么高级命令通过库 API 最终会找到守护程序。守护程序查询服务器，并将信息返回给调用者。

在客户机安装过程中，可以向 **mksecldap** 命令提供其它微调选项，如设置守护程序所用的线程数、高速缓存条目大小以及高速缓存到期超时。只有有经验的用户才可以使用这些选项。对于大多数环境而言，缺省值是足够的。

在客户机安装过程中，可以向 **mksecldap** 命令提供逗号分隔的用户列表。将这些用户 SYSTEM 属性设置为 LDAP。一旦完成设置后，这些用户只能通过 LDAP 装入模块认证。注意，为了避免在 LDAP 数据库中复制用户标识，**mksecldap** 命令不会将这些用户添加到 LDAP 安全信息服务器。推荐使用具有 **-R LDAP** 标志的 **mkuser** 命令在服务器上创建这些用户。

在客户机安装的最后步骤，**mksecldap** 命令启动客户机端守护程序，并在 **/etc/inittab** 文件中添加一个条目，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** 进程来检查安装是否成功。假定安装和运行 LDAP 安全信息服务器，如果安装成功，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 主机上管理 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（如 DCE、DCE 以及 Kerberos）来管理用户和组。更多关于 **-R** 标志的信息，请参考每个用户或组管理命令。

要使用户通过 LDAP 来认证，运行 **chuser** 命令将用户的 SYSTEM 属性值改变为 LDAP。根据定义的语法来设置 SYSTEM 属性值，能够通过一个以上的装入模块（如 compat 和 LDAP）来认证用户。更多关于设置用户认证方法的信息，请参阅第 41 页的『用户认证』和在 **/etc/security/user** 文件中定义的系统属性语法。

以下列任何一种格式运行带 **-u** 标志运行 **mksecldap** 命令，用户能够在客户机安装时变成 LDAP 用户:

1. 运行 `mksecldap -c -u user1,user2,...`，其中 **user1,user2,...** 是用户列表。在该列表中的用户既可以是本地定义的也可以是远程 LDAP 定义的用户。将上述每个用户节中的 SYSTEM 属性设置为 LDAP，这些节在 **/etc/security/user** 文件中。这些用户只能通过 LDAP 来认证。列表中的用户必须在 LDAP 安全信息服务器上存在；否则，它们不能从主机登录。运行 **chuser** 命令来修改 SYSTEM 属性，并允许通过多种方法（如，本地和 LDAP）认证。
2. 运行 "mksecldap -c -u ALL"。对于所有本地定义的用户，在 **/etc/security/user** 文件中的每个用户的节中将 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；否则它们不能从主机上登录。在 LDAP 服务器上定义而不是本地定义的用户不能从主机上登录。要允许远程 LDAP 定义的用户从主机上登录，运行 **chuser** 命令将用户的 SYSTEM 属性设置为 LDAP。

作为选择，您也可以将 **/etc/security/user** 文件中的缺省节的值修改为 LDAP，从而使所有的 LDAP 用户（不管它们是否是本地定义的）通过本地主机上的 LDAP 来认证。所有其 SYSTEM 属性未定义值的用户必须跟随在缺省节中定义的值。例如，如果缺省 stanza 具有 "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″" 使这些用户专门通过 LDAP 来认证。缺省节不会影响那些定义了系统属性值的用户。

LDAP 主机访问控制

AIX 提供系统的用户级别主机访问（登录）控制。管理员能够通过将用户的 SYSTEM 属性值设置为 LDAP 来配置 LDAP 用户，以使其登录到 AIX 系统。SYSTEM 属性在 **/etc/security/user** 文件中。**chuser** 命令可用于设置它的值，与下列的内容相似:

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

注: 不要使用这种控制将缺省的 SYSTEM 属性设置为 LDAP，LDAP 允许所有的 LDAP 用户登录到该系统。这会将 LDAP 属性设置成允许用户 `foo` 登录到系统。它也将注册表设置为 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，以便使某些用户登录。

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。这个功能允许集中的主机访问控制管理。管理员能够对一个用户帐户指定两个主机访问控制列表: 允许列表和拒绝列表。这两个用户属性储存在具有用户帐户的 LDAP 服务器中。用户可以对在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系统，那么

用户不能对系统进行访问。有两种方法指定用户的访问列表: 当用户创建的时候可以使用 **mkuser** 命令，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。要利用这个主机访问控制功能，强烈推荐将所有的 LDAP 客户机系统升级到 AIX 5.2 或以后的版本，从而同时定义了允许列表和拒绝列表的用户不能登录到特定的系统。

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 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，除了在地址 192.9.200.1 客户机系统。

更多信息，请参阅 **chuser** 命令。

LDAP 安全信息服务器审计

SecureWay 目录版本 3.2 提供了缺省的服务器审计记录功能。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。更多关于缺省审计插件的信息，请参阅 *Packaging Guide for LPP Installation* 中的 LDAP 文档。

在 AIX 5.1 和以后的版本中已经实现了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 目录缺省审计服务，因此可以启用这两个审计子系统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，在 **/etc/security/audit/event** 文件中需包含下列的审计事件:

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

ldapserver 审计类定义也在 **/etc/security/audit/config** 文件中创建了，它包含所有上述的事件。

要审计 LDAP 安全信息服务器，将下列的行添加到 **/etc/security/audit/config** 文件中每个用户的节。

```
ldap = ldapserver
```

因为 LDAP 信息服务器审计插件在 AIX 系统审计的框架内实现，所以它是 AIX 系统审计子系统的一部分。使用系统审计命令，如 **audit start** 或 **audit shutdown**可以启用或禁用 LDAP 安全信息服务器审计。将所有的记录添加到系统审计跟踪中，它能够使用 **auditpr** 命令来检查。更多信息，请参阅第 45 页的第 3 章，『审计过程』。

LDAP 命令

mksecldap 命令

mksecldap 命令可以用来构建 IBM SecureWay 目录安全认证和数据管理的服务器和客户机。该命令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。当构建服务器时，**mksecldap** 命令在该机器上运行两次。第一次运行来构建服务器，第二次运行构建客户机。
2. AIX 3.2 或后来的 AIX 5.2 的 SecureWay Directory 服务器配置文件 **/etc/slapd32.conf** 仅支持 SecureWay 目录 3.2 或后续版本。

要构建服务器，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** 文件集和后端的 DB2 软件。构建 LDAP 服务器时不要求运行任何的 DB2 预配置。当您运行 **mksecldap** 命令构建服务器时，命令将是:

1. 用 **ldapdb2** 创建一个使用缺省名称的 DB2 实例。
2. 用 **ldapdb2** 创建一个使用缺省名称的 DB2 数据库。如果数据库已经存在，**mksecldap** 将跳过以上两步。（这是构建 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／组数据放置在 **cn=aixsecdb,cn=aixdata** DN。这是建议的方案。否则，**mksecldap** 命令提取用户提供的 DN 并置 **cn=aixdata** 前缀，并使新建的 DN 成为后缀。下表显示了这种行为。括号里的值代表了可选的由用户从命令行提供的 DN。

CMD-line DN:	[o=ibm]
suffix:	cn=aixdata[,o=ibm]
sucurrity DN:	cn=aixsecdb,cn=aixdata[,o=ibm]
user DN:	ou=aixuser,cn=aixsecdb,cn=aixdata[,o=ibm]
group DN:	ou=aixgroup,cn=aixsecdb,cn=aixdata[,o=ibm]

如果本地系统已构建 LDAP 服务器，**mksecldap** 命令从 **slapd32.conf** 配置文件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 LDAP 组件共享的普通基本 DN。如果 **mksecldap** 命令找到了关键字，它把关键字和用户提供的 DN 进行对照。如果有相同的，将会把用户／组放在 **cn=aixsecdb**，**cn=aixdata**，**[userDN]**下边。如果他们不相同，**mksecldap** 命令打印一个错误消息警告存在 **cn=aixdata,...** DN，而不把用户／组移到用户提供的 DN 下边。通过再次运行 **mksecldap** 命令您可以选择使用和该现有的 DN 一起的现有的 **cn=aixdata**，**...**。

4. 把数据从本地主机的安全数据库文件里移到 LDAP 数据库。取决于 **-S** 选项，**mksecldap** 命令移动用户／组时使用三个 LDAP 方案之一:
   - **AIX** — AIX 方案（**aixaccount** 和 **aixaccessgroup** 对象类）

- **RFC2307** — RFC 2307 方案（**posixaccount**、**shadowaccount** 和 **posixgroup** 对象类）
- **RFC2307AIX** — RFC 2307 方案和全部 AIX 支持（**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 的配置成 LDAP 客户机的系统只能用于 AIX 类型方案的服务器。他们不和 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／密码对也用于访问控制 AIX 树。
6. 设置在该服务器和客户机间传送的安全数据的 SSL（安全套接字层）。该设置要求安装了 **GSKIT**。

   注: 如果使用了该选项，在运行 **mksecldap** 命令之前必须创建 SSL 密钥。否则，服务器可能不能启动。
7. 安装 **/usr/ccs/lib/libsecldapaudit.a**，一个 LDAP 服务器的插件。该插件支持 LDAP 服务器 AIX 的审计。
8. 在完成了上述步骤后，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，撤销以前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**。每个后继运行 **mksecldap**，**当前 slapd32.conf** 仅保存到 **/etc/security/ldap/slapd32.conf.save** 文件。撤销选项把 **/etc/slapd32.conf** 服务器配置文件恢复为 **/etc/security/ ldap/slapd32.conf.save** 副本。

    注: 撤销选项仅用于服务器配置文件。它不影响数据库。

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

对客户机设置，确保构建了 LDAP 服务器并且它正在运行。**mksecldap** 命令在客户机设置期间做以下的事情:

1. 保存 LDAP 服务器主机名称。
2. 保存服务器的用户基本 DN 和组基本 DN。如果命令行没有提供 **-d** 选项，**mksecldap** 命令在 LDAP 服务器上搜索 **aixaccount**、**aixaccessgroup**、**posixaccount**、**posixgroup** 和 **aixauxaccount** 对象类，并构建相应的基本 DN。如果服务器有多个用户／组基，您必须提供有 RDN 的 **-d** 选项，使 **mksecldap** 命令可以构建该 RDN 里的选项的基本 DN。

   如果在客户机构建期间没有找到**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，并保存所有找到的实体。
3. 确定 LDAP 服务器 — **AIX** 特定方案、**RFC 2307** 方案或有 AIX 支持的 **RFC 2307** 方案（请参阅第2步列出的对象类）使用的方案类型。它在相应的 **/etc/security/ldap/ ldap.cfg** 文件设置了对象类和属性映射。**mksecldap** 命令不识别其它的方案类型，所以必须手工设置客户机。
4. 为在该主机和 LDAP 服务器之间传送的安全数据设置 SSL。该设置要求预先创建客户机的 SSL 密钥和密钥密码，而且必须设置服务器使用 SSL 以使客户机 SSL 起作用。
5. 保存 LDAP 服务器管理员 DN 和密码。DN／密码对必须和服务器设置期间指定的对相同。
6. 根据客户机端守护程序使用的条目数目来设置缓存大小。对用户有效值范围是 100 – 10,000，对组为 10 – 1,000。对用户缺省的值是 1,000，对组为100。
7. 设置客户端守护程序的超时缓存。有效值范围为 60 – 3600 秒。缺省值为 300 秒。把值设为 0 来禁用缓存。
8. 设置客户端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。有效值范围为 60 – 3600 秒。缺省值为 300。
10. 在 **/etc/security/user** 文件里修改 SYSTEM 行来选择性地设置使用 LDAP 的用户或全部用户的列表。关于实现 ldap 登录的更多信息，请参阅下列注释。

11. 启动客户机守护程序（**secldapclntd**）。
12. 把客户端守护程序添加到 **/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** 文件的以前步骤。

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

示例

1. 要设置指定了用户和组的 AIX LDAP 服务器，请输入:

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

   这设置了 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移到缺省的 **cn=aixdata** 后缀。
2. 要设置一个有基本 DN 非缺省的有 SSL 安全通信的 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
   ```

   这设置了 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** 也必须得提供。用户和组用 RFC 2307 方案迁移。
3. 要撤销以前的服务器设置:

   ```
   mksecldap -s -U
   ```

   这撤销了 **/etc/slapd32.conf** 服务器配置文件以前的设置。由于安全原因，它不移动任何数据库条目或以前的设置创建的数据库。如果不再需要数据库条目或数据库，则手工除去他们。
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
   ```

   必须给该客户机提供 LDAP 服务器管理员 DN 和密码使服务器进行认证。**mksecldap** 命令联系 LDAP 服务器以求所用的方案类型，并相应地设置客户机。如果命令行没有 **-d** 选项，则要要搜索整个服务器 DIT，寻找用户基本 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** 命令为获得用户基本 DN 和组基本 DN 搜索 **o=mycompany, c=us** RDN。通过 LDAP 配置用户 1 帐户和用户 2 帐户进行认证。

   注: **-u ALL** 选项使得所有 LDAP 用户登录到该客户机。
6. 要撤销以前的客户机设置，请输入:

   ```
   mksecldap -c -U
   ```

   这便撤销了 **/etc/security/ldap/ldap.cfg** 文件以前的设置。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》* 里的 **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 **/etc/security/ldap/ldap.cfg** 文件定义的配置信息，并使用服务器管理员的区别名和密码到 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** 文件里指定了多个服务器，**secldapclntd** 守护程序就连接到所有的服务器上。然而在特定时间，它只和它们其中之一会话。**secldapclntd** 守护程序可以检测到和它会话的服务器什么时候关闭，并自动和另外的可用服务器会话。它也能检测到什么时候服务器再次可用，并新重和该服务器建立连接（但它继续和它正在会话的服务器会话）。这种自动检测特性通过 **secldapclntd** 守护程序来完成，它周期性的检查每一个服务器。后继检查之间的时间间隔的缺省值是 300 秒，可以在守护程序启动时通过命令行或修改 **/etc/ security/ldap/ldap.cfg** 文件相应的项来进行更改。

在启动时，**secldapclntd** 守护程序尝试和 LDAP 服务器建立连接。如果它不能与任何一个服务器连接，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** 守护程序进程退出。

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调整系统性能。

secldapclntd 守护程序在高速缓存里存放从 LDAP 安全信息服务器上检索到的调整性能用途的信息。如果在高速缓存里能找到所要求的数据并且高速缓存条目没有过期，该数据就被送回到请求者。否则，**secldapclntd** 守护程序发出一个请求到 LDAP 安全信息服务器来获取信息。

用户的高速缓存条目的有效数目范围是 100-10,000，对组为 10-1,000。对用户条目数的缺省值是 1000，对组为 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，高速缓存的条目在 300 秒后过期。如果高速缓存的超时设为 0，高速缓存功能将被禁止。

示例

1. 要启动 **secldapclntd** 守护程序，请输入:
   ```
   /usr/sbin/secldapclntd
   ```
2. 要启动 **secldapclntd** 并使用 20 个线程并且高速缓存的超时值为 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。也建议您在 **/etc/security/ldap/ldap.cfg** 文件指定这些值，使得每次您启动 **secldapclntd** 进程时这些值可以被使用。

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》* 里的 **secldapclntd**。

LDAP 管理命令

start-secldapclntd 命令

如果 **secldapclntd** 守护程序没有运行，**start-secldapclntd** 命令启动它。如果 **secldapclntd** 守护程序运行了，它将不做任何事。在脚本启动 **secldapclntd** 守护程序之前，它也从 **secldapclntd** 守护程序进程里清除端口映射程序的注册（如果有的话）。这阻止了因新的守护程序进程的启动失败而导致端口映射程序注册失败。

示例:

1. 要启动 **secldapclntd** 守护程序，请输入:

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

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

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

   建议您在 **/etc/security/ldap/ldap.cfg** 文件指定这些值，使得每次您启动 **secldapclntd** 进程时这些值可以被使用。

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

stop-secldapclntd 命令

stop-secldapclntd 命令终止运行的 **secldapclntd** 守护程序进程。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** 守护程序进程，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》* 里的 **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，它只是启动它。

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** 并使用 30 个线程并且高速缓存的超时值为 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》* 里的 **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:

- 和 **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（id）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 服务器的波动信号间隔

- **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》* 里的 **ls-secldapclntd**。

flush-secldapclntd 命令

flush-secldapclntd 命令清除 **secldapclntd** 守护程序进程的高速缓存。

示例:

1. 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》* 里的 **flush-secldapclntd**。

sectoldif 命令

sectoldif 命令读取本地定义的用户和组，并使用**标准输出**以 ldif 格式把结果打印出来。如果重定向到一个文件，可以用 **ldapadd** 命令或 **db2ldif** 命令把结果添加到 LDAP 服务器。

-S 选项指定了 ldif 输出所使用的方案类型。**sectoldif** 命令接受三种方案类型:

- **AIX** — AIX 方案（**aixaccount** 和 **aixaccessgroup** 对象类）
- **RFC2307** — RFC 2307 方案（**posixaccount**、**shadowaccount** 和 **posixgroup** 对象类）
- 有全部 AIX 支持的 **RFC2307AIX**— RFC 2307 方案（**posixaccount**、**shadowaccount** 和 **posixgroup** 对象类以及**aixauxaccount** 和 **aixauxgroup** 对象类）。

mksecldap 命令调用 **sectoldif** 命令在 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 服务器时要注意。**ldapadd** 和 **db2ldif** 命令仅用于条目名（用户名或组名称而不用于在添加条目时的数字 id,使用 **sectoldif** 输出从多个系统迁移用户和组可能会导致多个帐户共享一个数字 id，这违背了安全原则。

示例:

1. 要打印本地定义的所有用户和组，请输入下列命令:

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

   它用**标准输出**以 ldif 格式打印本地定义的所有用户和组。使用 rfc2307aix 方案类型表示用户条目和组条目。基本 DN 设置为 `cn=aixsecdb, cn=aixdata`。
2. 仅打印本地定义的用户占位符，请输入下列命令:

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

   它用**标准输出**以 ldif 格式打印本地定义的用户占位符。如果没有 **-S** 选项，则使用缺省的 AIX 方案类型表示占位符的 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》* 里的 **sectoldif**。

ldap.cfg 文件格式

/etc/security/ldap/ldap.cfg 文件包含正确启动和运行了 **secldapclntd** 守护程序的信息，也包含了调整守护程序性能的信息。**/etc/security/ldap/ldap.cfg** 文件通过客户机配置的 **mksecldap** 命令来更新。

/etc/security/ldap/ldap.cfg 文件可能包含下列字段:

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／或主服务器的复本。
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。有效信息是 ON 和 OFF。缺省值为 OFF。 **注**: 您将需要 neSSL 密钥和对密钥的密码来启用该功能。
ldapsslkeyf	指定到 SSL 密钥的全路径。
ldapsslkeypwd	指定到 SSL 密钥的密码。 **注**: 注释掉该行使用存储的密码。密码的存储文件必须和 SSL 密钥本身驻留在同一个目录，并和密钥文件具有相同的名称，但用扩展名 **.sth** 替代了**.kdb**。
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 ID 指定到 AIX-LDAP 属性映射的全路径。当创建 LDAP 用户时用 **mkuser** 命令使用这些 ID。
userbasedn	指定用户基本 DN。
groupbasedn	指定组基本 DN。
idbasedn	指定 ID 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	指定网组基本本 DN。
rpcbasedn	指定 RPC 基本 DN。
userclasses	指定用户使用的对象类条目。
groupclasses	指定组使用的对象类条目。
ldapversion	指定 LDAP 服务器版本。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	指定是否使用别名。有效值是 NEVER、SEARCHING、FINDING 和 ALWAYS。缺省值是 NEVER。
usercachesize	指定用户stash高速缓存大小。有效值是 100 – 1,000 个条目。缺省值是 1,000。
groupcachesize	指定组高速缓存大小。有效值是 10 – 1,000 个条目。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* 里的 **/etc/security/ldap/ldap.cfg**。

LDAP 属性映射文件格式

/usr/lib/security/LDAP 模块和 **secldapclntd** 守护程序使用这些映射文件来在把 AIX 属性名称转换为 LDAP 属性名称。映射文件的每个条目代表一个属性的转换。一个条目有四个空格间隔的字段:

```
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。值为 **s** 表示单一值，**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* 里的 **LDAP 属性映射文件格式**。

相关信息

mksecldap、**start-secldapclntd**、**stop-secldapclntd**、**restart-secldapclntd**、**ls-secldapclntd**、**sectoldif** 以及 **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 子系统以设备无关方式为应用程序提供访问硬件设备的方法。本章内容符合 PKCS #11 标准的版本 2.01。

使用下列组件实现该子系统:

- 槽管理器守护进程（**pkcsslotd**），它为子系统提供关于可用的硬件设备状态信息。在安装过程中以及当系统重新启动时，自动启动守护进程。
- 为已经实现 PKCS #11 的适配器提供 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，为适配器提供 PKCS #11 支持。在不用重编译应用程序就能得到 PKCS #11 设备时，该分层设计允许用户使用新的 PKCS #11 设备。

本章包含下列信息:

- 『IBM 4758 模型 2 密码协处理器』
- 『PKCS #11 子系统配置』
- 第 71 页的『PKCS #11 使用』

IBM 4758 模型 2 密码协处理器

IBM 4758 模型 2 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可支持的微码进行适当地配置过。

用 PKCS #11 子系统验证使用的 IBM 4758 模型 2 密码协处理器。

PKCS #11 子系统旨在自动检测适配器在安装和重新启动过程中是否支持 PKCS #11 调用。因此，任何没有适当配置的 IBM 4758 模型 2 密码协处理器都不能从 PKCS #11 接口中得到，并且发送到适配器的调用失败。完成如下任务来验证适配器是否正确安装:

1. 使用下列命令确保适配器的软件正确安装:

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

   如果在结果列表中没有显示 IBM 4758 模型 2 密码协处理器，那么检测卡是否恰当放置，支持软件是否正确安装。

2. 使用 **csufclu** 实用程序确定是否把合适的固件加载到卡上:

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

   验证 Segment 3 Image 是否加载 PKCS #11 应用程序。如果没有加载，参照适配器的具体文档获得最新的微码和安装说明。

   注: 如果找不到该实用程序，就不能安装支持软件。

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。这些任务包含:

- 第 70 页的『初始化标记』
- 第 70 页的『设置 Security Officer PIN』

- 『初始化用户 PIN』

通过 API （通过写 PKCS #11 应用程序）或使用 SMIT 接口，执行这些任务。通过主 SMIT 菜单的 **Manage the PKCS11 subsystem** 或通过使用 **smit pkcs11** 快速路径访问 PKCS #11 选项。

初始化标记

在成功使用每一个适配器或 PKCS #11 标记之前，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标记。因此，标签不能重复。然而，API 不能验证标签是否重新使用过。通过 PKCS #11 应用程序或通过使用 SMIT 的系统管理员执行初始化。如果标记是 Security Officer PIN，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。

初始化标记:

1. 通过键入 `smit pkcs11` 进入标记管理屏幕。
2. 选择 **Initialize a Token**.
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: 这样会擦除标记上的所有信息。
5. 输入 Security Officer PIN（SO PIN）和唯一的标记标签。

如果输入的 PIN 正确，命令运行完以后会初始化或重新初始化适配器。

设置 Security Officer PIN

如果标记是一个 SO PIN，可以从它的缺省值更改 PIN，如下:

1. 键入 `smit pkcs11`.
2. 选择 **Set the Security Officer PIN**.
3. 选择您想设置 SO PIN 的初始化适配器。
4. 输入当前的 SO PIN 和新的 PIN。
5. 验证新的 PIN。

初始化用户 PIN

标记初始化以后，有必要设置用户 PIN 以允许应用程序访问标记对象。参考设备的特定文档确定在访问对象之前是否需要用户登录。

初始化用户 PIN:

1. 通过键入 `smit pkcs11` 进入标记管理屏幕。
2. 选择 **Initialize the User 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. 验证后，必须更改用户 PIN。

重新设置用户 PIN

为重新设置用户 PIN，可以使用 SO PIN 重新初始化 PIN 或使用现存的用户 PIN 设置用户 PIN。这样做:

1. 通过键入 `smit pkcs11` 进入标记管理屏幕。

2. 选择 **Set the User PIN**。
3. 选择您想设置用户 PIN 的初始化适配器。
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

没有加载函数控制向量，标记可能不支持强加密操作。参考设备的特定文档确定标记是否需要函数控制向量并在何处加载。

如果需要函数控制向量，应该有一个密钥文件。为了加载函数控制向量:

1. 通过键入 `smit pkcs11` 进入标记管理屏幕。
2. 选择 **Set the function control vector**。
3. 从标记中选择 PKCS #11 插槽。
4. 输入函数控制向量文件的路径。

PKCS #11 使用

应用程序要使用 PKCS #11 子系统，子系统的槽管理器守护程序必须在运行，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，从而启动槽管理器。该脚本在启动槽管理器前，验证系统中的适配器。因此，在用户登录系统前，槽管理器守护程序是不可用的。守护程序启动后，子系统将对数字的任何更改以及支持适配器的类型的更改进行合并，而没有来自系统管理员的干涉。

可以通过运行时链接入对象或使用延迟的符号解决方案，将 API 装入。例如，应用程序可以用下列方式获取 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和进程关联作为用户身份的证明的能力。通过可装载的认证模块结构（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该能力。

本节讨论下列主题:

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。登录过程中使用与密码连接的证书认证用户。PKI 证书基于公用密钥／私人密钥技术。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。用户保存一个叫作专用密钥，存储在专用的密钥存储器中，而发布其它的叫作公用密钥且以证书为形式的密钥。证书一般维护在轻量级目录访问协议（LDAP）服务器上，或者在组织中为公司内使用，或者在因特网上为世界范围使用。

用户 John 为了发送数据给用户 Kathy，此数据仅仅她能解密，John 必须从 Kathy 的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的她的专用密钥解密来自 John 的数据。

该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。许多类型的专用的密钥存储器包括智能卡和文件，但是所有存储器类型都通过密码或个人识别码（PIN）的使用保护专用密钥。通常，为多个专用密钥，连同证书和其它 PKI 对象一起提供存储器。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。证书认证服务定位用户的证书和基于用户帐户名称的密钥存储器，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，用来自证书的用户的公用密钥来检查签名。用户认证后，通过将证书与用户创建的每个进程关联，系统在受保护的内存中存储用户的证书。对用户和操作系统内核拥有的任意进程，该内存中关联能够加快对用户证书的访问。

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有基本的理解。证书是遵循 X.509 标准化的对象，版本 3（X.509v3）是其中的最新版。认证中心（CA）创建、标识和发出证书，它是接受和处理证书申请的最一般的软件应用程序。证书由几个认证属性组成。一些属性是必需的，但许多是可选的。在该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－一个证书序列号，它使该证书和所有其它由相同 CA 签发的证书唯一地区别开来。

- 签发者名称 – 指定证书的签发 CA 的名称。
- 有效期 – 证书的激活和过期日期。
- 公用密钥 – 公共的密钥。
- 主题区别名称 – 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。

每个证书有一个表示遵循 X.509 中哪个版本标准的唯一的版本号。每个证书有一个从同一 CA 发布的所有其它证书中将它唯一区别的序列号。序列号仅对发出的 CA 是唯一的。证书的签发者名称标识签发 CA。

证书只有在两个指定的日期之间是有效的: “不是之后”日期和“不是以前”日期。因此，可能在有效日期之前创建证书，将来某个日期失效。证书有 3 个月到 5 年的生命是普遍的。

主题区别名称通过使用名为“区别名称”（DN）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、市 / 县 / 区、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 顾及所有者的 Web 站点 URI / URL 的规范。

认证中心和证书

认证中心发布、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 允许对面向团体的数据方便的访问。

CA 还处理证书的撤消和证书撤销列表（CRL）的管理。撤消证书是发布由于某些原因（除证书有效期失效之外）指定证书不再有效的事实行为。因为在发出的 CA 的控制外能维护和使用证书的副本，CA 在 CRL 中发布已撤消的证书的列表使得外面的实体能查询列表。利用已复制的证书将职责任命给实体来比较已复制的证书和发出的 CA 的 CRL。CA 可能仅仅撤消它创建或发出的证书。不能由其它 CA 发出的证书。

撤消证书管理的原因包含:

- 证书的专用密钥的损害。
- 证书所有者离开公司。
- CA 的损害。

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

许多 CA 为了查询和撤消证书支持证书管理协议（CMP）。协议支持多个方法在一台客户机（也称为端实体）和 CA 来建立安全连接，虽然不是全部客户机和 CA 支持所有方法。一个公共的方法要求每个正式创建和撤消使用引用号和 CA 识别的密码。可能也要求象 CA 识别的专用证书这种的其它数据。撤消请求可能要求撤消证书的匹配专用密钥。

虽然 CMP 为证书创建和撤消请求作准备，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，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 CA 支持 OCSP。

CA 通常由政府组织或可信专用组织拥有和操作，它们试图提供保证，使之发出的证书符合所申请的人。短语签*发证书*意味着创建证书，与请求已发布的证书的副本不同。

证书存储格式

存储个别证书的最通用的格式是使用专有编码规则（DER）的抽象语法符号表示法 V1（ASN.1）格式。称该格式为 *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的专用密钥。为了方便地识别，通常由用户将一个唯一的密钥标号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建密钥之前要求输入密码。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形式，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

证书认证服务功能为客户机／服务器模式。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。）客户机端包含每个加入 PKI 认证的系统必需的软件（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

为创建 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，但是必需其它步骤。）管理员将密钥存储器密码提供给新建用户，于是新建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、匹配密钥标号和其它相关数据。用户名和标记的组合允许证书认证服务将证书定位于 LDAP 服务器。PKI LDAP 层的更多信息，请参阅第 77 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号。检查在证书中发现的有效期值来确定证书是已经失效还是没有达到激活日期。接着系统根据密钥存储器、密钥标号和已提供的密码来检索用户的专用密钥。检索专用密钥后，系统验证通过内部签署进程来匹配专用密钥和证书。如果二者匹配，用户通过登录过程的 PKI 认证步骤。（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 执行许多其它帐户检查。）

为了当作认证证书使用证书，必须使用可信签字密钥标识该证书。为了以后的引用将签名和证书一起存储在 LDAP 中。实现要求在将标记指定给 **auth_cert** 前证书有签名。

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，使得证书撤消成为禁用用户帐号的可怜的替代品，CA 在发布撤消证书前可能延迟一个小时或更多时间）。

认证不需要 CA 也值得注意。证书认证服务本地执行主要的工作，除检索 LDAP 中存储的数据外。

服务器实现

证书认证服务的服务器端实现 Java 编写的 CA，包含连同自审查属性的注册中心（RA）。它发布证书和为 LDAP 服务器而创建的 CRL。通过一系列的配置文件（Java 属性文件），CA 是可配置的。它包含名为 **runpki** 的管

理的应用程序，该应用程序在其它函数中提供子命令来启动和停止服务器，且为创建和撤消证书支持 CMP。CA 需要 Java 1.3.1、IBM DB2 7.1 数据库和 IBM Directory 4.1。因为 DB2 的要求，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** 组成部分，服务器包含下列命令:

mksecpki

安装中使用该命令来配置 AIX PKI 服务器组成部分。作为任务的部分，为证书认证，命令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。如果不要在交互式方式中启动守护程序，管理员可以编辑 **runpki** 命令，使用 **l** 标志代替 **lb** 标志。

对于证书认证运行的所有用户帐户， **runpki** 命令必须在执行 **su -** 操作后运行。命令的位置在认证中心用户帐户的主目录下的 **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，输入如下:

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

客户机实现

证书认证服务客户机端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 可装载的认证模块结构（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，即使在使用基于文件的数据机制时。关于使用基于文件的数据库时限制的信息，请参阅第 84 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面向最多用户的软件。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 认证中必需的数据。

常规客户机功能

下列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**）
- 在用户创建时间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。

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，并划分为下列组成部分:

- 『Java 守护程序』
- 『服务管理层』
- 『PKI LDAP 层（证书存储器）』
- 第 78 页的『libpki.a 库』
- 第 78 页的『可装载的认证模块结构层』
- 第 78 页的『客户机命令』
- 第 79 页的『处理认证组命令』
- 第 79 页的『用户管理命令』
- 第 80 页的『配置文件』

Java 守护程序: 客户机端的基础是使用 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，提供全部散列和加密函数。因为 PKI 服务供应商软件包的 API 对与 C 应用程序是不标准的，叫作服务管理层（SML）的包装层 API 向应用程序和守护程序提供规格化的 API。

服务管理层: 对于 Java 守护程序的 SML 服务名为 **/usr/lib/security/pki/JSML.sml**。SML 创建证书，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 专用密钥存储: 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** 目录中的证书认证服务。

密钥存储器在大小上受限，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基于文件的密钥存储器。不支持智能卡或 LDAP 密钥存储器。通过将文件密钥存储器放置在在所有系统同一安装点下共享文件系统中能支持漫游用户。

PKI LDAP 层（证书存储器）: 证书认证服务存储证书和通过 PKI LDAP 层与 LDAP 上每个用户要素的信息关联的其它证书。证书认证服务维护 LDAP 服务器上每个用户要素上的证书关联。用户帐户可以有与它关联的多个证书。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标记的组合在 LDAP 中定位用户的证书关联。

为了性能和磁盘空间对比平衡，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，证书认证服务为获得实际的证书查询引用。在连接 LDAP 服务器上发布证书的 CA 中最常使用引用。证书认证服务支持的 URI 引用类型是 LDAP 引用。证书认证服务以 DER 格式存储证书，期望 URI 引用请参阅已格式化的 DER 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号的类型和位置。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，所有系统上用户的密钥存储器必须驻留在同一位置。

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 **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** 库收藏许多子例程。库包含执行以下操作的 API:

- 管理新建配置文件
- 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。

可装载的认证模块结构层: SML API 和 PKI LDAP API 之上驻留可装载的认证模块结构（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，当为这些技术添加新建装入模块到系统中时，这些命令自动支持新建认证和数据库技术。

证书认证服务添加新建 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 95 页的『methods.cfg 文件』中查找。

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 认证新建节值。

客户机命令: 在全部 API 层（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，还存在许多证书认证服务特定命令。这些命令帮助用户帮助证书和密钥存储器。下面是连同简短描述的命令列表。

certadd
如果已撤消证书，在 LDAP 中将证书添加到用户帐户并检查无误。

certcreate
创建证书。

certdelete
从用户帐户删除证书（也就是，从 LDAP）。

certget
从用户帐户检索证书（也就是，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，检查是否已撤消证书。

certlist
列出与包含于 LDAP 的用户帐户关联的证书。

certrevoke
撤消证书。

certverify
验证匹配证书的专用密钥，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
更改密钥存储器的密码。

获取有关这些命令的信息。请参阅 *《AIX 5L V5.2 命令参考大全》*。

处理认证组命令: 处理认证组（PAG）命令对于 AIX 是新建的。PAG 是将用户认证数据与进程关联的数据项。为了证书认证服务，如果 PAG 是启用的，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 **/usr/sbin/certdaemon** 守护程序是启用的用来提供该功能。缺省情况下，机制是非启用的。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。

为了启用 **certdaemon** 守护程序，将下列行添加到 **/etc/inittab** 文件:

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

连同简短描述的 PAG 命令列表如下:

paginit
认证用户和创建 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。

更多关于这些命令的信息，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，当将为这些技术新建的装入模块添加到系统时，这些命令自动地支持新建认证和数据库技术。

下面子节提供在 PKI 认证怎样影响用户管理命令方面更深入的考虑。

PKI 认证进程影响的命令如下:

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标识。（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，也在下面列出证书属性。**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
用户对象区别名称。

subject-alt-name
用户对象备用名称电子邮件。

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 发行商的区别名称。

mkuser

该命令为管理员提供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时，管理员能使用 **mkuser** 命令来生成证书。任选的，如果用户有认证证书，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
- 专用密钥标号
- 对象备用名称电子邮件区域名

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

该命令在 PKI 用户帐户上使用时修改用户密码。它执行在 **/etc/security/user** 文件中找出的密码限制规则，在 **/etc/security/passwd** 文件中找出的标志属性，和 PKI 服务供应商需要的任意规则。

因为基于密钥存储器用用户密码加密它们的专用密钥，**root** 用户不知道的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。如果用户忘记密钥存储器的密码，除非 root 知道密钥存储器的密码，root 用户不能重新设置密码。如果不知道密码，可能必须给用户发布新建密钥存储器和新建证书。

配置文件: 证书认证服务为配置客户机端使用配置文件: **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 节组成。CA 节包含不适合公用可读的 **ca.cfg** 文件的专用的 CA 信息，例如 CMP 引用数字和密码。LDAP 节包含不适合公共访问的专用的 LDAP，例如 PKI LDAP 管理名称和密码。

对 **ca.cfg** 文件中的每个 CA 节，**acct.cfg** 文件应该包含相同名称的 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，也必须存在至少一个命名为 **local** 的 CA 节。

CA 节包含下列属性:

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标识证书申请的专用密钥的标号。

keypasswd
指定可信密钥存储器密码。

rvpasswd
指定用于 CMP 的撤消密码。密码的长度由 CA 指定。

rvrefnum
指定用于 CMP 的撤消引用号。

LDAP 节包含下列属性:

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

ldappkiadmpwd
指定 LDAP 服务器的帐户密码。

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。

示例 **acct.cfg** 文件如下:

```
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"
```

获取更多信息，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请求，证书认证使用的公共 CA 信息。

对于 **ca.cfg** 文件中的每个 CA 节，**acct.cfg** 文件必要包含一个相同名称的 CA 节。**ca.cfg** 文件中的每个 CA 节名称必须是唯一的。必须存在至少一个命名的为 **local** 的节。节不能命名为 **ldap** 或 **default**。

CA 节包含下列属性:

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的 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
指定用于标记证书的散列算法（例如，MD5）。

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

url 为对象备用名称 URI 指定缺省值。

缺省 CA 节命名为 local。示例 **ca.cfg** 文件如下:

```
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
```

获取更多信息，请参阅 *AIX 5L Version 5.2 Files Reference*。

policy.cfg 文件: **policy.cfg** 文件由四个节组成: **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 节包含下列属性:

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** 命令使用的证书的对象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号。

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** 命令使用的证书的对象备用名称 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 节包含下列属性:

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** 命令应该检查 CRL（**yes**），还是不检查（**no**）。

comm 节包含 **timeout** 属性，该属性很短时间内指定当要求证书信息使用 HTTP 时 **certadd** 和 **certlink** 使用的超时周期（例如，正在检索 CRL）。

示例 **policy.cfg** 文件如下:

```
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
```

获取更多信息，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下列审计日志事件:

- 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生成在 3B7 和 3B8 范围内的几个新建跟踪事件。

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要求是一台 DB2 服务器，一台 IBM 目录服务器和一台证书认证服务服务器。全部能安装在系统或系统组合上。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 85 页的『配置注意事项』
- 第 85 页的『安全性注意事项』
- 第 85 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。获取支持的证书属性的清单，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 密钥存储器和其它密钥存储器类型。

缺省情况下，将用户密钥存储器保存在本地文件系统的 **/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。考虑漫游用户，或者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没有改变。（在 AIX 中，LDAP 中的每个证书包含对包含证书专用的密钥的专用密钥的路径名称。为了用于认证，密钥存储器必须定位于 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 也是受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一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，所有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（请参阅对于 **acct.cfg** 的 **carefnum**、**capasswd**、**rvrefnum** 和 **rvpasswd** 属性描述）。当创建证书和撤消证书时为了 CMP 与 CA 通信，分别单独使用这些值。如果遭受破坏，入侵者可能能随意创建证书，随意撤消任何人的证书。

为了限制危害，考虑对少数系统限制证书创建或撤消。只有在创建证书的系统上必需 **carefnum** 和 **capasswd** 属性（通过 **certcreate** 或 **mkuser** 命令）。这可能意味着限制对同一系统集的用户帐户创建。

注: 用户创建过程中为自动地创建证书配置 **mkuser** 命令，或它能没有证书创建帐户，由此管理员必须随后创建和添加证书。

同样地，只有在要撤消证书（通过 **certrevoke** 命令）的系统上，**rvrefnum** 和 **rvpasswd** 属性值是必需的。

acct.cfg 文件也包含敏感可信签字密钥信息（请参阅对于 **acct.cfg** 文件的 **keylabel** 和 **keypasswd** 属性描述）。为专门的证书验证操作单独使用这些值。如果遭受破坏，入侵者可能能伪造已验证的证书。

为了限制危害，考虑对少数系统限制证书验证。只有在需要证书验证的系统，**acct.cfg** 文件的 **keylabel** 和 **keypasswd** 属性，和 **ca.cfg** 文件上的 **trustedkey** 属性是必需的。特定地，在要求 **mkuser**（具有自动创建证书的能力）和 **certverify** 命令的系统上。

激活的新帐户

创建 PKI 用户帐户时，如果将 **policy.cfg** 文件中的 **newuser** 节的 **cert** 属性设置为 **new**，**mkuser** 命令创建活动的 PKI 帐户连同运作着的证书和密码。**newuser** 节中的 **passwd** 属性指定帐户上的密码。因为密钥存储器为了存储专用密钥要求密码。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** 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，不知道密码不能解密密钥存储器。当用户忘记密码时，必须发出新建证书，创建新建密钥存储器。

其它证书认证服务注意事项

规划证书认证服务时其它注意事项包含如下:

- 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。
- 证书认证服务要求所有命令、库和守护程序运行在 Unicode 环境中。

证书认证服务的封装

表 9. 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（装载 AIX 基介质） • Java131 安全性扩展（装载扩展压缩） • 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（装上 AIX 基介质） • Java131 安全性扩展（装上扩展压缩） • 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	n/a	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，缺省的安装 **Java131.rte 软件包**，但是手工安装其它软件包。

为了 **db2_07_01.client** 软件包运作，**db2_07_01.server** 软件包必须安装在网络的系统上。

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下列过程构成:

- 『安装和配置 LDAP 服务器』
- 第 89 页的『安装和配置证书认证服务服务器』
- 第 90 页的『为证书认证服务服务器配置』
- 第 92 页的『配置证书认证服务客户机』
- 第 95 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 时可能发生的情况如下:

1. 如果没有安装 LDAP 服务器软件，执行下列过程:
   a. 第 87 页的『LDAP 服务器安装』
   b. 第 87 页的『LDAP 服务器配置』

c. 第 88 页的『为 PKI 配置 LDAP 服务器』

2. 如果已安装和配置 LDAP 服务器软件，但没有为 PKI 配置，执行第 88 页的『为 PKI 配置 LDAP 服务器』。

LDAP 服务器安装

关于安装 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，使用下列 URL 上的 web 浏览器能查看文档: **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** 且按下 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**，且按下 Enter 键。必须安装 LDAP 服务器和客户机文件集和 DB2 后端数据库文件集。

   安装的文件集包含下列文件:

   - **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**（目录服务器结构）
   - **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**，位于扩展压缩 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。该工具要求 Web 服务器。

Apache Web 服务器应用程序位于 LINUX 应用程序 CD 的 AIX 工具箱上。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，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。以下是配置步骤的简明描述:

1. 使用 **ldapcfg** 来设置管理对于 LDAP 数据库的 DN 和密码。管理员是 LDAP 数据库的 **root** 用户。为了用密码 **secret** 配置 **cn = admin** 的管理员 DN，输入如下:

   ```
   # 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 和密码作为 **acct.cfg** 文件中 **ldap** 节的 **ldappkiadmin** 和 **ldappkiadmpwd** 属性使用。

2. 使用 Web 服务器配置文件的位置配置 web 管理员工具，如下所示:

   ```
   # 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** 访问 web 管理员。然后在步骤 2 中配置的管理员 DN 和密码登录。
5. 使用 web 管理员工具，遵循配置后端 DB2 数据库的指导，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开的 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 PKI 数据。下列步骤配置用于存储和检索每个 PKI 数据的 LDAP 目录信息树。

1. **添加 LDAP 配置后缀项**。对于 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。对于 PKI 数据的缺省数据 root 是 **ou=pkidata**，**cn=aixdata**。所有数据放置在该位置。

   PKI 数据后缀

   cn=aixdata

   对于所有 AIX 数据的公共后缀可能已经存在，如果对 AIX 数据已经使用 LDAP 服务器。

   通过 web 管理员工具，或直接通过编辑 LDAP 服务器配置文件能添加后缀配置项。

   使用 web 管理员添加后缀配置项，执行如下:

   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，执行如下:

   a. 在 **/usr/ldap/etc/slapd32.conf** 文件中，定位的行包含

      ```
      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，能添加与下列相似的后缀项:

      ```
      ibm-slapdSuffix: cn=aixdata
      ```

   c. 保存配置文件的更改。
   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，所有的 PKI 数据驻留在它之下。对于数据 Root，ACL 是为所有 PKI 数据设置访问规则的访问控制列表。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`）和对于 *password* 的值作为 **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和对 PKI 数据添加 ACL，如下所示:

```
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: 不要对 ACL 设置做任何更改。这样做可能危害 PKI 实现的完整性。
使用后缀而不是缺省值来编辑 **pkiconfig.ldif** 文件，然而只有对有经验的 LDAP 管理员推荐使用。然后使用下面的 **ldapadd** 命令能使数据库适用于 **ldif** 文件。用您本地 LDAP 管理员 DN 和密码对 **-D** 和 **-w** 选项的值替换，如下所示:

```
# 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. 从扩展包 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** 文件移动到其它目录中。该文件与 Java 安全性文件集冲突，为了证书认证服务的正确机能必须移动该文件。
3. 从扩展压缩 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

通过执行下列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，如下所示:

   ```
   # 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. 将下列后缀添加到 **slapd.conf** 文件中，如下所示:

   ```
   ibm-slapdSuffix: o=aix,c=us
   ```

   能指定不同的区别名称代替 o=aix,c=us。
4. 运行 **slapd** 命令，如下所示:

   ```
   # /usr/bin/slapd -f /etc/slapd32.conf
   ```
5. 添加对象类，如下所示:

   ```
   # ldapmodify -D cn=admin -w secret -f setup.ldif
   ```

   setup.ldif 包含的位置如下:

   ```
   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
   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 包含的位置如下:

   ```
   dn: o=aix,c=us
   changetype: add
   objectclass: organization
   objectclass: top
   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. 停止和启动 **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创建引用号和密码对。证书创建中证书认证服务客户机试图对服务器认证时，一个密码对代表证书认证服务服务器接受的认证信息。文件的格式是密码前的引用号，都在独立的行上。例如:

   ```
   12345678
   password1234
   87654321
   password4321
   ```

   此处 12345678 和 87654321 是引用号，password1234 和 password4321 是它们各自的密码。允许空格行。空格字符不能在引用号或密码之前或之后。文件中至少存在一个引用号。在 **/usr/cas/server/iafile** 中能查找到示例文件。每次启动客户机要引用这些值。

2. 使用 **mksecpki** 命令配置 CA，如下所示:

   ```
   # 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 指定对于 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位置的 LDAP 分支。

   mksecpki 命令自动生成连同 **TrustedKey** 密钥标号的可信签字密钥和 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。执行『创建可信签字密钥』中的步骤不是必需的，除非需要生成多个密钥或希望连同不同密钥标号和/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** 密钥标号的可信签字密钥和 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。如果需要生成新建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的步骤。

所有允许的证书创建和撤消所在的证书认证服务客户机为了签署用户的认证证书要求可信签字密钥。在独立的密钥存储器中保存密钥，对于能创建证书的所有系统是可用的。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，如下所示:

```
keytool -genkey -dname `cn=trusted key' -alias `TrustedKey' -keyalg RSA \
        -keystore filename.pkcs12 -storetype pkcs12ks
```

在该示例中，可信密钥标号是 **TrustedKey**，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。配置证书认证服务客户机时，需要分别对可信密钥标号和可信密钥存储器密码设置 **acct.cfg** 文件中的 **keylabel** 和 **keypasswd** 属性。

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 用户应该能访问该文件。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。关于创建可信签字密钥的信息，请参阅第 91 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 用户应该能访问该文件。

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** 文件的所有 **ldap** 节。

配置认证中心

最低限度的，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自始至终存在的单一系统，证书认证服务支持多个 CA 的使用。用户或软件指定 CA 时，使用 **local** 的缺省值。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**。

通过 SMIT 配置屏幕，以下节引导您配置本地 CA。

更改／显示认证中心:

1. 运行 PKI SMIT，如下所示:

   ```
   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. 按照 **/usr/lib/security/pki/JSML.sml** 设置**服务模块名称**字段。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. 按照本地系统上可信密钥存储器的位置的 URI 设置 **CA 的可信密钥路径名**字段。仅支持基于文件的密钥存储器。对于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. 按照 CA 的位置的 URI（**cmp://myserver:1077**）设置**认证中心服务器的 URI** 字段。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。该字段指定对该 CA 应该按照证书撤消列表的位置设置的 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. **缺省证书区别名称**字段指定创建证书时所用的基本 DN（例如 o=*XYZ*，c=*us*）。该字段不是必需的。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。该字段不是必需的。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，为支持下一步可行的字节大小，下面的公用密钥机制可能四舍五入该值。（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，系统缺省值为 1024 位。该字段映射到 **/usr/lib/security/pki/ca.cfg** 文件中的 **keysize** 属性。
14. **至多通信重试**字段指定系统放弃前试图联系 CA（当创建或撤消证书时）的次数。系统缺省值为 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**。系统缺省值为 **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，如下所示:

   ```
   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**字段指定创建证书所用的 CA 引用号。创建引用号由所有数字组成，长度上至少 7 个数字。CA 定义引用号。（请参阅第 91 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，该密码对于上面创建引用号必须是匹配密码。（请参阅第 91 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. **证书撤消引用号**字段指定撤消证书时使用的引用号。撤消引用号必须由所有数字组成，长度上至少 7 个数字。每个证书创建过程中将撤消引用号发送给 CA，通过 CA 与证书关联。为了撤消证书，撤消过程中必须发送和创建证书时发送的相同的撤消引用号（和撤消密码）。该字段映射到 **/usr/lib/security/pki/acct.cfg** 文件中的 **rvrefnum** 属性。
7. **证书撤消密码**字段指定撤消证书时使用的引用密码。撤消密码必须由 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撤消密码发送给 CA，通过 CA 与证书关联。为了撤消证书，撤消过程中必须发送和创建证书时发送的相同的撤消密码（和撤消引用号）。该字段映射到 **/usr/lib/security/pki/acct.cfg** 文件中的 **rvpasswd** 属性。
8. **可信密钥标号**字段指定定位于可信密钥存储器的可信签字密钥的标号（有时命名为 *alias*）。可信密钥标号是来自第 91 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 91 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，如下所示:

```
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。对于 CA LDAP 帐户的管理用户名是和第 87 页的『LDAP 服务器配置』和第 90 页的『为证书认证服务服务器配置』中同样的名字。值应该是 cn=admin。访问 CA LDAP 数据时为了与 LDAP 服务器通信客户机端使用它。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。管理密码是与第 87 页的『LDAP 服务器配置』和第 90 页的『为证书认证服务服务器配置』所用相同的密码。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，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**字段指定数据驻留的目录信息树的 DN 后缀。该后缀是用于第 90 页的『为证书认证服务服务器配置』的 **ibm-slapdSuffix** 属性的值。该值必须在每个 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 93 页的『添加 CA LDAP 帐户』中同样的步骤，除使用第 88 页的『为 PKI 配置 LDAP 服务器』中的**添加 PKI 后缀**和 **ACL 数据库项**步骤中所用的值之外。使用下列值:

- 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，如下所示:

   ```
   smitty pki
   ```

2. 选择**更改／显示策略**。

- **为新建用户创建证书**字段指定 **mkuser** 命令是为新建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（**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 格式中的密钥存储器目录。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** 命令使用的证书所需的有效期。所需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。如果数字后直接是字母 d，则解释为天。如果数字后直接是字母 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**），还是只是对证书的链接（**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**字段指定要求用 HTTP 的证书信息时 **certadd** 和 **certlink** 命令使用的以秒为单位的超时周期（例如，检索 CRL）。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** 属性使用的认证文法的定义。特定地，此处对于 **PKILDAP**（即使用 LDAP 的 PKI）和 **FPKI**（*文件* PKI）的认证文法必须由系统管理员定义和添加。

下面是典型的 **methods.cfg** 定义。节名称 **PKI**、**LDAP** 和 **PKILDAP** 为任意的名称，能由管理员更改。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始终使用相同的 **methods.cfg** 节名称和属性值。

管理配置示例

创建新建 PKI 用户帐户

为创建新建 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。第二种方法在用户和系统管理员之间要求界面，这可能花更多的时间设置。

两个示例都使用下列假设:

- 已经安装、配置和运行 **cas.server** 和 **cas.client**。
- 在 **methods.cfg** 中将 **PKILDAP** 定义为第 95 页的『methods.cfg 文件』中显示的那样。

示例 1:

用超级权限，系统管理员对于用户帐户 bob 执行下列命令:

```
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 用户要求创建认证证书，用户能创建新建证书，且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.
```

更改缺省新建密钥存储器密码

为修改新建 PKI 用户的密钥存储器所用的密码，编辑 **/usr/lib/security/pki/policy.cfg** 文件中的 **newuser** 节的 **passwd** 属性值。

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，用户或管理员应该撤消使用适当的原因码的证书，应该将损坏通知使用公用密钥的其它用户，同时取决于专用／公用密钥的目的，应该发布新建证书。如果作为用户的认证证书使用证书，那么应该作为新建认证证书添加另一个证书（属于用户的新建证书或现有的未损坏的证书）。

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。撤消所有用户的证书。为用户创建包含新建认证证书的新建证书。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可用的。

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，用户或管理员应该撤消使用适当的原因码的证书，应该将损坏通知使用公用密钥的其它用户，同时取决于专用／公用密钥的目的，应该发布新建证书。如果作为用户的认证证书使用证书，那么应该作为新建认证证书添加另一个证书（属于用户的新建证书或现有的未损坏的证书）。

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的专用密钥的密钥存储器位置。为了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，要求更改的与用户的证书关联的 LDAP 密钥存储器位置和名称。如果用户使用多个密钥存储器，那么必须特别注意只对密钥存储器更改影响的证书的 LDAP 信息更改。

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）结构使系统管理员具有一种能力，即通过可插入模块将多个认证机制并入现有的系统。用于使用 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:

- 在系统上选择应用程序的任何认证服务
- 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建的认证服务模块
- 使用先前输入密码来作多个模块的认证

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），用来管理 PAM 事务，并调用在可插入模块中定义的 PAM 服务编程接口。可插入模块根据调用服务及其在配置文件中的条目而由库动态装入。成功不但取决于可插入模块，也取决于定义的服务行为。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。

下列的说明显示了应用程序、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条目确定欲装入的适当的模块，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。

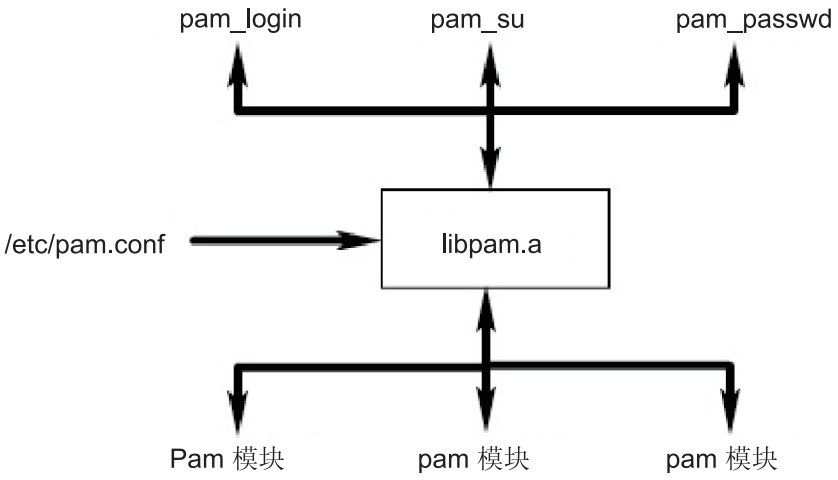


图 3. PAM 结构和实体. 这个说明显示了假定的应用程序命令如何使用 PAM 库来访问适当的 PAM 模块。

PAM 库

PAM 库，即 **/usr/lib/libpam.a**，包含用作所有 PAM 应用程序的公共接口并控制模块装入的 PAM-API。PAM 库根据在 **/etc/pam.conf** 文件中定义的堆栈行为装入模块。

下列的 PAM API 功能调用由 PAM 模块提供的相应的 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 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。下列的 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	检索模块特定数据
pam_set_data	设置模块特定数据
pam_get_item	检索公共 PAM 信息
pam_set_item	设置公共的 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 模块允许在系统上共同或单独使用多个认证机制。给定的 PAM 模块必须至少采用四种模块类型的其中一种。如下描述的是模块类型以及要求与模块类型一致的相应的 PAM SPI。

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

确定用户帐户的正确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 模块类型的服务条目组成，并通过定义的模块路径发送服务。在这个文件中的条目包含下列的空白区域划定的字段:

服务名称 模块类型 控制标志 模块路径 模块选项

其中:

service_name	指定服务的名称。关键字其它用于定义条目中没有指定的应用程序所用的缺省模块。
module_type	指定服务的模块类型。有效模块类型是认证、帐户、会话以及密码。
control_flag	指定模块的堆栈行为。支持的控制标志是必要的、充分的或可选的。
module_path	指定实现服务功能的库对象的路径名。*模块路径*的条目应该以根（**/**）目录开始。如果条目不以 **/** 开始，那么会将 **/usr/lib/security** 预设为文件名。
module_options	指定能够发送到服务模块的选项列表。该字段的值取决于模块支持的选项，该模块在*模块路径*字段中定义。

除了*模块选项*字段是可选的之外，每个条目都要求所有以上定义的字段。PAM 库会忽略变形的条目以及*模块*或*控制标志*字段具有无效值的条目。也会忽略行开头为镑符 （#）的条目，因为这表示注释。

通过使用相同的*模块类型*字段创建多个条目实现在配置文件中的堆栈。以文件中列出的顺序调用模块，并由每个条目指定的*控制标志*字段确定最终结果。*控制标志*字段的有效值和在堆栈中的相应的行为如下:

required	所有堆栈中必要的模块必须通过成功的结果。如果一个或多个必要的模块失败了，那么会尝试堆栈中所有必要的模块，但返回第一个失败的必要模块的错误。
sufficient	如果模块标志为充分的成功，没有先前的必要的或充分的模块失败，那就会忽略堆栈中所有保留的模块，并返回成功。
optional	如果堆栈中没有模块是必要的，并且没有充分的模块成功，那么至少有一个服务的可选的模块必须成功。如果在堆栈中的另一个模块成功了，那么就会忽略在可选的模块中的失败。

下列是示例的 **/etc/pam.conf** 文件，它能够在安装了额外的 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
```

示例的配置文件包含登录服务的三个条目。将 **pam_aix** 和 **pam_verify** 指定为 required 之后，用户输入两个密码认证，用户认证要求两个密码必须都成功。**pam_test** 模块的第三个条目是可选的，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 选项允许使用先前输入的密码，而不是提示输入一个新的密码。

su 命令的这种运作使得如果 **pam_aix** 成功了，那么认证也成功了。如果 **pam_aix** 失败了，那么 **pam_verify** 必须通过以便得到成功的认证。

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设置了缺省值。设置缺省值确保给定的模块类型的所有情况都至少由一个模块覆盖。

添加 PAM 模块

要添加 PAM 模块，使用下列的过程:

1. 将模块安装在 **/usr/lib/security** 目录中。
2. 将所有权设置为 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，使其包含期望的服务名称中的条目中的模块。
4. 测试受影响的服务以便确保它们的功能。不要退出系统，直到已经执行登录测试。

更改 /etc/pam.conf

更改 **/etc/pam.conf** 配置文件时，考虑下列的内容:

- AIX 不提供缺省的 **/etc/pam.conf** 文件，因此必须在使用 PAM 之前创建这个文件。创建这个文件时，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，以便得到期望的更改。
- 确定每个模块类型的缺省模块，然后使用 **OTHER** 关键字来阻止指定每个服务的模块。
- 读取提供给选定的模块的任何文档，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，牢记堆栈中 **required**、**sufficient** 以及 **optional** 控制标志的行为。

注: 配置文件的不正确配置会导致系统不能登录。更改文件后，总是要在退出系统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模式重新引导系统并更正 **/etc/pam.conf** 配置文件而恢复。

启用 PAM 调试

PAM 库在执行过程中提供调试信息。启用系统收集调试输出后，聚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，可以通过这些步骤:

1. 在 **/etc/pam_debug** 创建一个空的文件。PAM 库检查 **/etc/pam_debug** 文件的存在，如果找到这个文件，就启用 syslog 输出。
2. 编辑 **/etc/syslog.conf** 文件，使其包含期望级别信息的条目。
3. 重新启动 **syslogd** 守护程序以便识别配置更改。
4. 重新启动 PAM 应用程序时，调试信息会收集在 **/etc/syslog.conf** 配置文件定义的输出文件中。

在 AIX 中的集成 PAM

AIX 中的 PAM 集成是通过使用 AIX 可装入认证模式、PAM 以及 **pam_aix** 模块而完成的。这些模块提供 PAM 集成的下列独立的路径:

- 通过 PAM 模块提供从 AIX 安全服务到 PAM 的访问
- 通过 PAM 模块提供从 PAM 应用程序到 AIX 安全服务的访问（**pam_aix**）

PAM 模块

可将 AIX 安全性服务配置成通过使用现有的 AIX 认证模块结构调用 PAM 模块。正确设置了 **/usr/lib/security/methods.cfg** 文件时，简单的装入模块 PAM 会将 AIX 安全信息（**passwd**、**login** 等等）发送到 PAM 库。PAM 库会检查 **/etc/pam.conf** 文件以确定使用哪个模块，然后作相应的 PAM SPI 调用。从 PAM 返回的值被映射为 AIX 错误代码，并返回到调用的程序。

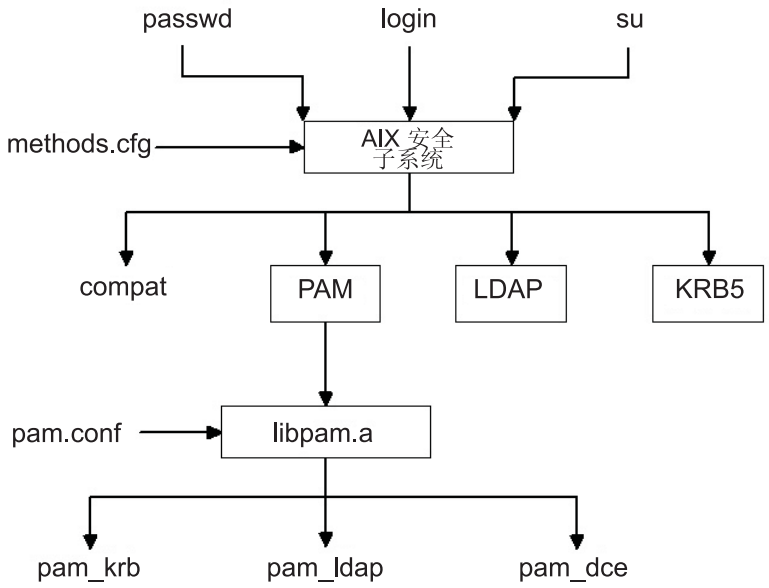


*图 4. PAM 模块路径的 AIX 安全服务. 这个说明显示了当正确配置 PAM 时 AIX 安全服务调用所采取的路径。所显示的 PAM 模块（**pam_krb**、**pam_ldap** 以及 **pam_dce**）作为第三方解决方案的示例列出。*

PAM 是安装在 **/usr/lib/security** 目录中的简单装入模块，并且是认证唯一的模块。PAM 模块必须与数据库结合以形成复合的装入模块。下列的示例显示了一些节，这些节添加到 **methods.cfg** 文件中以形成具有数据库 **files** 的复合 PAM 模块。**db** 属性的 **BUILTIN** 关键字会将数据库指派为 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** 属性而创建和修改用户。

```
mkuser -R PAMfiles SYSTEM=PAMfiles registry=PAMfiles pamuser
```

这项操作会指示 AIX 安全服务进一步调用（**login**、**passwd** 等），以便使用 PAM 装入模块认证。虽然在这个示例中 **files** 数据库用于复合模块，但是也可以使用其它数据库，如 LDAP（如果安装了的话）。如先前描述那样创建用户会导致如下那样将 AIX 安全映射到 PAM API 调用:

```
 AIX                    PAM API
=====                   =========
认证              -->   pam_authenticate
更改密码          -->   pam_chauthtok
密码到期          -->   pam_acct_mgmt
密码限制          -->   No comparable mapping exists, success returned
```

定制 **/etc/pam.conf** 文件允许将 PAM API 调用引导到期望的 PAM 模块以便认证。为了进一步优化认证机制，可以实行堆栈。

通过 **pam_set_item** 功能将 AIX 安全服务的数据传递到 PAM，因为不可能容纳来自 PAM 的用户对话。为与该 PAM 模块整合而写入的 PAM 模块应该使用 **pam_get_item** 调用检索所有的数据，而不提示用户输入数据，因为这是由安全服务来处理的。

提供循环检测以捕获可能的错误配置，其中将 AIX 安全服务发送到 PAM，然后 PAM 模块试图调用 AIX 安全服务来执行操作。循环事件的检测会导致期望操作的即刻失败。

注: 使用从 AIX 安全服务到 PAM 模块的 PAM 整合时，不应写入 **/etc/pam.conf** 文件来使用 **pam_aix** 模块，因为这会导致循环情况。

pam_aix 模块

pam_aix 模块是提供对 AIX 安全服务的 PAM 启用的应用程序访问，这是通过提供接口而达到的，这种接口在存在等同的 AIX 的位置将其调用。根据用户定义和在 **methods.cfg** 中的相应设置，这些服务依次由可装入认证模块或 AIX **builtin** 功能来执行。在执行 AIX 过程中生成的任何错误代码映射为相应的错误代码。

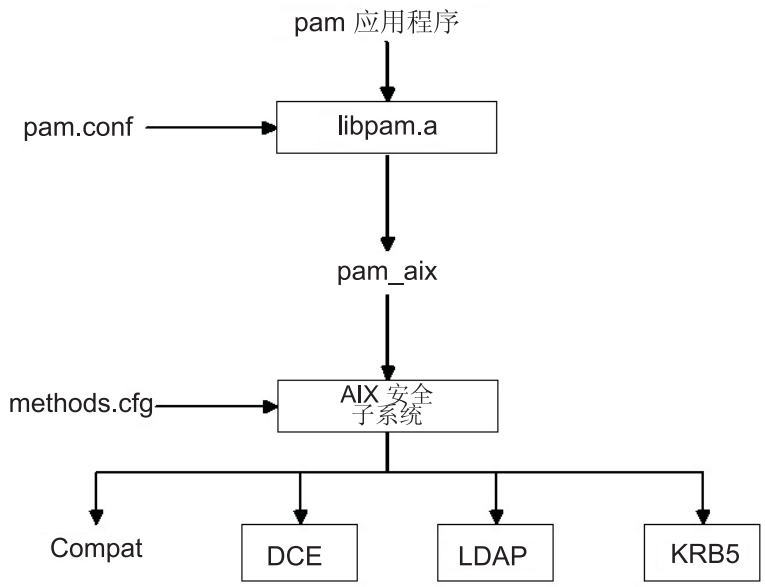


*图 5. AIX 安全子系统路径的 PAM 应用程序. 这个说明显示了将 **/etc/pam.conf** 文件配置为使用 **pam_aix** 模块时，PAM 应用程序 API 调用会跟随的路径。如图所示，整合允许任何可装入认证模块（DCE、LDAP 或 KRB5）或 在 UNIX 文件中（compat）认证用户。*

pam_aix 模块安装在 **/usr/lib/security** 目录中。**pam_aix** 模块要求将 **/etc/pam.conf** 文件配置为可以使用该模块。注意堆栈仍然可用，但是选择在 **/etc/pam.conf** 文件的下列的简单示例中不显示堆栈。

```
#
# 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** 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，但这些 SPI 只返回 PAM 成功的调用。

以下是粗略地将 PAM SPI 调用映射到 AIX 安全子系统:

```
 PAM SPI                    AIX
=========                  =====
pam_sm_authenticate   -->  认证
                           pam_sm_chauthtok      -->  密码到期，更改密码
                           注: 只有在
PAM_CHANGE_EXPIRED_AUTHTOK 标志通过时才检查密码到期。         pam_sm_acct_mgmt      -->  登录限制，密码到期
pam_sm_setcred        -->  不存在可比映射，PAM_SUCCESS 返回
pam_sm_open_session   -->  不存在可比映射，PAM_SUCCESS 返回
pam_sm_close_session  -->  不存在可比映射，PAM_SUCCESS 返回
```

将期望传递到 AIX 安全子系统的数据设置为在模块使用之前使用 **pam_set_item** 功能或如果数据还不存在，那么 **pam_aix** 模块会提示输入数据。

第 8 章 OpenSSH 软件工具

OpenSSH 软件工具支持 SSH1 和 SSH2 协议。该工具提供加密和认证的 shell 函数。OpenSSH 是基于客户机和服务器体系结构。OpenSSH 在 AIX 主机上运行 **sshd** 守护进程并等待客户连接。它为通道认证和加密支持公共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 的更多信息，请参阅下列网站:

```
http://www.openssh.org
```

以上的 Web 站点提供 OpenSSH 命令的手册页信息。

关于 AIX 的 OpenSSH 信息，请参阅下列 Web 站点，它是 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 上安装并注册 OpenSSH。OpenSSH 软件随 AIX 5.2 Bonus Pack 一起提供。使用 **openssh-3.4p1** 级的源代码编译该 OpenSSH 版本并把它打包为 **installp** 软件包。Bonus Pack CD-ROM 介质中包含的 OpenSSH 程序是根据 IBM 国际程序许可证协议（IPLA）为非授权的程序的条款而授权的。几个 RPM 格式软件包中的 AIX 4.3.3 也可以使用 OpenSSH，这些软件包是由 AIX 工具箱提供给 Linux 实用程序的。

在安装 OpenSSH **installp** 格式软件包之前，必须安装打开的安全套接字层（OpenSSL）软件。OpenSSL 软件包包含加密库。AIX 工具箱中的 RPM 软件包为 Linux 应用程序提供了 OpenSSL。该安装软件包包含了手册页和翻译的消息文件集。

1. 使用如下的 **geninstall** 命令安装 OpenSSL RPM 软件包:

   ```
   # geninstall -d/dev/cd0 R:openssl-0.9.6e
   ```

   显示与下列相似的输出:

   ```
   SUCCESSES
   ---------
   openssl-0.9.6e-1
   ```

2. 接着，使用如下的 **geninstall** 命令安装 OpenSSH **installp** 软件包:

   ```
   # geninstall -I"Y" -d/dev/cd0 I:openssh.base
   ```

   使用 **Y** 标志接受 OpenSSH 许可证协议。

   显示与下列相似的输出:

   ```
   Installation Summary
   --------------------
   Name                        Level           Part        Event       Result
   -------------------------------------------------------------------------------
   openssh.base.client         3.4.0.5200      USR         APPLY       SUCCESS
   openssh.base.server         3.4.0.5200      USR         APPLY       SUCCESS
   openssh.base.client         3.4.0.5200      ROOT        APPLY       SUCCESS
   openssh.base.server         3.4.0.5200      ROOT        APPLY       SUCCESS
   ```

也可以使用 SMIT **install_software** 快速路径安装 OpenSSL 和 OpenSSH。

由于以前的安装步骤结束后，以下的 OpenSSH 二进制文件也都安装了:

ssh	与 **rlogin** 和 **rsh** 客户机程序相似
ssh-agent	可以存储专用密钥的代理
ssh-add	把密钥添加到 **ssh-agent** 的工具

sftp	与检查 SSH1 和 SSH2 协议相似的 **FTP** 程序
scp	文件复制与 **rcp** 相似的程序
ssh-keygen	密钥生成工具
ssh-keyscan	从多数主机中集聚公共主机密钥的实用程序
ssh-keysign	基于主机认证的实用程序
sshd	允许登录的守护进程
sftp-server	SFTP 服务器子系统（**sshd** 守护进程自动启动）

下列的一般信息包含 OpenSSH:

- **/etc/ssh/ssh_config** 目录包含 **sshd** 守护进程和 **ssh** 命令的注册文件。
- **/usr/openssh** 目录包含自述文件和原始的 OpenSSH open-source 许可证文本文件。
- AIX SRC 控制 **sshd** 守护进程。可以发出下列命令启动、停止以及查看守护进程的状态:

  ```
  startsrc -s sshd   或 startsrc -g ssh  (group ) stopsrc -s sshd    或 stopsrc -g ssh
  lssrc -s sshd      或 lssrc -s ssh
  ```

  也可以发出下列命令启动并停止守护进程:

  ```
  /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 OpenSSH 服务器文件集时，一条记录添加到目录 **/etc/rc.d/rc2.d** 中。记录在 inittab 中执行运行级别 2 处理程序（`l2:2:wait:/etc/rc.d/rc 2`），那么 **sshd** 守护进程能在引导时自动启动。为了防止守护进程在引导时启动，移除 **/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*，提供在 AIX 中注册 OpenSSH 的信息，并且在下列 Web 站点中可以得到该信息:

  ```
  http://www.redbooks.ibm.com
  ```

用 PAM 使用 OpenSSH

从 AIX 5.2 开始，使用可插入认证模块（PAM）支持编译 OpenSSH。PAM 是认证用户的备用方式。通过允许一个可写用户模块添加到登录进程中，它为认证 AIX 用户提供可修改的机制。用户可以写自己的模块或使用 AIX 提供的 **pam_aix** 模块。该 **pam_aix** 模块为 AIX 安全服务提供接口。

下列是使用 **pam_aix** PAM 模块的 **/etc/pam.conf** 注册文件的示例，但是也可以使用安装在本系统上的其它模块。用该文件中的下列信息创建 **/etc/pam.conf** 文件:

```
sshd   auth            required        /usr/lib/security/pam_aix
OTHER   auth            required        /usr/lib/security/pam_aix
sshd    account         required        /usr/lib/security/pam_aix
OTHER   account         required        /usr/lib/security/pam_aix
sshd    password        required        /usr/lib/security/pam_aix
```

```
OTHER   password        required        /usr/lib/security/pam_aix
sshd    session         required        /usr/lib/security/pam_aix
OTHER   session         required        /usr/lib/security/pam_aix
```

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的安全性措施的信息。这些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；以及审计和监视网络安全性等内容。

第 9 章 TCP/IP 安全性

如果您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，您可对您的系统进行配置，使之通过网络通信。本指南不对 TCP/IP 的基本概念进行描述，而描述 TCP/IP 的相关安全注意事项。关于 TCP/IP 安装及 TCP/IP 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『传输控制协议/网际协议』章节。

不管怎样，系统管理员都必然会遇到一定级别的安全问题。例如，安全级别可能是公司决策方面的事。或系统需要访问政府系统，因而要求以一定的安全级别进行通信。这些安全标准可应用于网络、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。

您安装了 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** 快速路径来配置您的系统。

本章讨论下列主题:

操作系统特殊的安全性

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

对于联网的安全策略是对于操作系统的安全策略的扩展，它包括以下主要组成部分:

- 与用户登录本地系统的方式相同，通过用户名和密码在远程主机上提供**用户认证**。可信 TCP/IP 命令，如 **ftp**、**rexec** 和 **telnet** 有相同的要求，并象操作系统中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**。这防止远程主机假装成另一个远程主机。
- **数据导入与导出安全**允许数据以指定的安全级别流入网络接口适配器，并以同样的安全和权限级别从网络接口适配器流出。例如，绝密数据只能在设置为绝密安全级的适配器之间流动。

网络审核

TCP/IP 提供网络审计，使用审计子系统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的操作及应对这些操作负责的用户。

审计以下类型的事件:

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。当需要系统的安全通信路径，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 支持这些特性及*安全注意键*（SAK），SAK 建立您与系统之间安全通信的必要环境。每当您使用 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。但是，在 **telnet** 程序内您可用 **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。您也可定义一个单独键，用 **telnet set sak** 命令启动 SAK 请求。

关于可信计算基的更多信息，请参阅第 3 页的『可信计算基』。

TCP/IP 命令安全

TCP/IP 中的一些命令提供操作期间的安全环境。这些命令是 **ftp**、**rexec** 和 **telnet**。**ftp** 函数提供文件传送期间的安全性。**rexec** 命令提供在外部主机上运行命令的安全环境。**telnet** 函数提供登录外部主机的安全性。

ftp、**rexec** 和 **telnet** 命令只提供它们操作期间的安全性。即，它们并未建立与其它命令一起使用的安全环境。为了保护您的系统进行其它操作，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，使您能保护系统的安全。

ftp、**rexec**、**securetcpip** 和 **telnet** 命令提供以下形式的系统及数据安全:

ftp

ftp 命令提供传送文件的安全环境。当用户向外部主机调用 **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 **$HOME/.netrc** 文件以获取用于外部主机的用户标识及密码。为了安全，**$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: 因为使用 **.netrc** 文件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就不可用。将 **ftp** 命令从 **/etc/security/config** 文件的 tcpip 节中除去即可重新启用此功能。

为了使用文件传送功能， **ftp** 命令需要两个 TCP/IP 连接，一个用于文件传输协议（FTP），另一个用于数据传送。协议连接是首位的，因为它建立在可靠的通信端口上因而是安全的。第二连接是实际的数据传送所必需的，本地及远程主机都验证了此连接的另一端与首位连接的相同主机建立。如果首位连接和第二连接不是与相同主机建立，**ftp** 命令首先显示错误消息，指出数据连接未认证，然后就退出。此第二连接的验证防止第三个主机拦截准备送至另一个主机的数据。

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 **$HOME/.netrc** 文件以获取在外部主机上的用户标识及密码。为了安全，**$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: 因为使用 **.netrc** 文件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。将 **rexec** 条目从 **/etc/security/config** 文件中的 tcpip 节中除去即可重新启用此功能。

securetcpip

securetcpip 命令启用 TCP/IP 安全特性。发出此命令时，从系统中除去对非可信命令的访问。运行 **securetcpip** 命令除去下列中的每个命令:

- **rlogin** 和 **rlogind**
- **rcp**、 **rsh** 和 **rshd**
- **tftp** 和 **tftpd**
- **trpt**

使用 **securetcpip** 命令将系统从标准安全级转换为较高安全级。系统转换后，除非您重装了 TCP/IP，否则不必再次发出 **securetcpip** 命令。

telnet or **tn**

telnet（TELNET）命令提供登录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。此键标顺序不同于调用本地可信路径的顺序，并可在 **telnet** 命令中定义。

远程命令执行访问（/etc/hosts.equiv）

列在 **/etc/hosts.equiv** 文件上的主机用户，无需提供密码就可在系统上运行一定的命令。下列表中提供有关如何用基于 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。

远程命令执行访问任务

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
列出具有命令执行访问的远程主机	**s m i t lshostsequiv**	查 看 **/etc/hosts.equiv** 文件	软件 —> 网络 —> **TCPIP**（**IPv4** 和 **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。
添加命令执行访问的远程主机	**s m i t mkhostsequiv**	编 辑 **/etc/hosts.equiv** 文件 注 1	软件—> 网络 —> **TCPIP**（**IPv4** 和 **IPv6**） —> **TCPIP** 协议配置 —> **TCP/IP** —> 配置 **TCP/IP** —> 高级方法 —> 主机文件。在**添加/更改主机条目** 中，完成下列字段: **IP** 地址、主机名 、别名和**注释**。单击**添加/更改条目**，再单击 **OK**。
除去命令执行访问的远程主机	**s m i t rmhostsequiv**	编 辑 **/etc/hosts.equiv** 文件 注 1	软件—> 网络 —> **TCPIP**（**IPv4** 和 **IPv6**） —> **TCPIP** 协议配置 —> **TCP/IP** —> 配置 **TCP/IP** —> 高级方法 —> 主机文件。在 **/etc/host** 文件的内容中选择主机。单击**删除条目** —> **OK**。

注:

1. 关于这些文件过程的更多信息，请参阅 *AIX 5L Version 5.2 Files Reference*中 “TCP/IP hosts.equiv 文件格式”。

限制文件传送程序用户（/etc/ftpusers）

列在 **/etc/ftpusers** 文件中的用户受远程 FTP 访问的保护。例如，假设用户 A 登录到远程系统，那么他就知道您系统上用户 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 也不能从用户 B 的帐户或向用户 B 的帐户 FTP 文件。

下列表提供有关如何用基于 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 —> 全部用户。
添加受限用户	**smit mkftpusers**	编辑**/etc/ftpusers** 文件注 1	软件 —> 用户 —> 全部用户 —> 选定的 —> 向组添加此用户。选择组，并单击 **OK**。
除去受限用户	**smit rmftpusers**	编辑 **/etc/ftpusers** 文件注 1	软件 —> 用户 —> 全部用户 —> 选定的 —> 删除。

注:

1. 关于这些文件过程的更多信息，请参阅 *AIX 5L Version 5.2 Files Reference* 中 “TCP/IP ftpusers 文件格式”。

可信进程

可信程序或可信进程是 shell 脚本、守护程序或满足特别安全标准的程序。这些安全标准由美国国防部设置维护，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 级提供最高安全级。每个安全级别必须满足一定的要求。例如，C2 安全级可具体说明下列标准:

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由其它模块访问的模块。

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一定文件，那么用户也就无权改变此文件。
对象重用的局限性	例如，防止用户偶然找出已标出要覆盖，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，必须用可信计算基操作，即，对于单独主机，必须保护机器。对于网络，必须保护全部文件服务器、网关和其它主机。

网络可信计算基

网络可信计算基（NTCB）包含确保网络安全的硬件和软件。本节定义 NTCB 涉及 TCP/IP 时的组成部分。

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指定给本地系统的数据来控制导入数据，并通过所有系统广播可接收数据。

NTCB 的软件组成部分只包含那些看作可信程序。此程序及相关文件（安全系统的一部分）按照 directory-by-directory 列在下列表中。

/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 directory

名称	所有者	组	方式	许可权
rwho（目录）	root	system	0755	drwxr-xr-x

数据安全及信息保护

TCP/IP 的安全特性对通过网络传输的用户数据不加密。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危险，并采用相应对策。

使用国防部（DOD）环境中的 TCP/IP 安全特性可能需要遵守关于通信安全的 DOD 5200.5 和 NCSD-11。

为网际端口所设的基于用户的 TCP 端口访问控制以及自主访问控制

网际端口（DACinet）的自主访问控制，反映了基于用户的访问控制（为 AIX 5.2 主机之间通信的 TCP 端口而设）的特色。AIX 5.2 可用另外的 TCP 头传送系统之间的用户及组信息。DACinet 特性允许目标系统管理员控制基于目标端口、始发用户标识及主机的访问。

此外，DACinet 特性允许管理员限制只能 root 用户使用的本地端口。类似于 AIX，UNIX 系统将 1024 以下的端口当作只能由 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，因此防止用户在熟悉的端口运行服务器。

取决于设置非-DACinet 系统能否与 DACinet 系统连接。DACinet 特性的初始状态拒绝访问。一旦启用 DACinet，就无法禁用 DACinet。

dacinet 命令接受指定为主机名、点线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。

下列示例指定一个单一主机，它为全限定主机名 *host.domain.org* 所知:

```
host.domain.org
```

下列示例指定一个单一主机，它为 IP 地址 10.0.0.1 所知:

```
10.0.0.1
```

下列示例指定具有 10.0.0.0 值的前 24 位（网络前缀的长度）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 服务的访问控制

DACinet 使用 **/etc/rc.dacinet** 启动文件，它使用的配置文件是 **/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**，然后删除所有应当应用 ACL 的端口。ACL 存储在两个地方。当前活动的 ACL 存储在内核，可通过运行 **dacinet aclls** 来读取。将在下一个系统引导通过 **/etc/rc.tcpip** 重新激活的 ACL 存储在 **/etc/security/acl**。使用以下格式:

```
service host/prefix-length [user|group]
```

这里可用数字指定服务也可根据 **/etc/services** 中所列方式指定服务，可用主机名或具有子网掩码规范的网络地址给出主机，用 **u:** 或 **g:** 前缀指定用户或组。无用户或组指定时，ACL 只考虑发送主机。给服务加上前缀 **-** 将明确禁用访问。根据第一个匹配评估 ACL。因而您能为一组用户指定访问，但也可将组中某用户的规则置于组规则前来明确拒绝此用户，。

/etc/services 文件包括两个条目，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** 命令前除去文件中这两行。除去 **/etc/services** 文件中下列行:

```
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 只限制具有 DACinet 特性的 root 用户进入端口 TCP/25 访问，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 X11 条目从 **/etc/security/services** 除去，使 ACL 应用于此服务。

假定一个全部连接系统的 10.1.1.0/24 子网，限制访问 root 用户（仅为 **/etc/security/acl** 中的 X（TCP/6000））的 ACL 条目如下:

```
      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 条目后，使用下列 ACL 条目:

```
telnet    0.0.0.0/0   g:friends
```

禁止用户目录维护程序访问 Web 服务器，但允许其它每个人访问:

```
-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，或在 1080 置一 SOCKS 服务器。为了防止常规用户在指定端口运行服务器，可将这些端口指定成具有特权。可用 **dacinet setpriv** 命令向运行系统添加特权端口。系统启动时，设计成具有特权的端口必须列在 **/etc/security/priv** 中。

用 **/etc/services** 中定义的符号名或指定端口号将端口列在此文件中。下列条目将禁止非 root 用户在通常的端口运行 SOCKS 服务器或 Lotus Notes 系统。

```
1080
lotusnote
```

注: 此功能不能防止**用户**运行程序。它只能防止用户在已知的端口运行服务，而这些端口通常正需要这些服务。

关于 **dacinet** 命令的更多信息，请参考 *《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的请求。因为打开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不需要打开的端口。这种习惯是有用的，因为它使您知道什么系统对从因特网上访问的人是可用的。

要确定那个端口打开了，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侦听状态。

活动的 Internet 连接（包括服务器）

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	(state)
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	*.*	
udp4	0	0	*.time	*.*	

活动的 **Internet** 连接（包括服务器）

Proto	**Recv-Q**	**Send-Q**	**Local Address**	**Foreign Address**	**(state)**
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** 文件检查因特网号码认证中心（IANA）服务，在操作系统里把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-fileserver                 7000/udp             # File Server Itself
af3-callback                    7001/tcp             # Callbacks to Cache Managers
```

```
af3-callback                    7001/udp            # Callbacks to Cache Managers
```

3. 除去运行的服务来关闭不必要的端口。

识别 TCP 和 UDP 套接字

识别处在侦听状态的 TCP 套接字和处在空闲状态等待数据到达的 UDP 套接字。使用 **lsof** 命令，**netstat -af** 命令的变体。在 AIX 5.1开头，**lsof** 命令包含在 Linux 版的 *AIX 工具箱应用程序* CD 上。

例如，要显示处在侦听状态的 TCP 套接字和处在空闲状态等待数据到达的 UDP 套接字，使用如下的 **lsof** 命令。

```
# lsof -i | egrep "COMMAND|LISTEN|UDP"
```

输出结果与下面类似:

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 ID 后，您可以运行下列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密通信，而不必修改应用程序。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公司数据。

本章讨论以下主题:

IP 安全性概述

本节讨论下列主题:

- IP 安全性和操作系统
- IP 安全性特征
- 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 安全性和操作系统

操作系统使用 IP 安全性（IPsec）技术，它是一开放的、标准的安全技术，是由 Internet Engineering Task Force（IETF）开发的。IPsec 对全部在通信堆栈的 IP 层所有数据提供密码术为基础的保护。对现有的应用程序不需要更改。IPsec 是 IETF 为第 4 版和第 6 版 IP 的环境选择工业标准网络安全框架。

IPsec 使用下列的加密技术保护您的数据通信:

认证 验证主机的身份或端点的程序来处理认证

完整性检查
进行在网络上传输时没有修改数据确保的处理。

加密 对在网络上传输的隐藏数据的保密性和专用 IP 地址进行确保处理。

认证算法证实发送方的身份和数据完整性，通过使用密码术散列函数处理数据信息包（包含固定的 IP 报头字段），使用密钥产生唯一的摘要。在接收方，通过使用名称函数和密钥处理数据。如果更改了数据，或者发送方密钥无效，则废弃数据报。

加密使用一加密术算法修改和随机化数据使用某些算法和密钥产生 *cyphertext* 加密的数据。加密使数据在传输时不能读取。在接收之后，数据的恢复使用相同算法和密钥（对称的加密算法）。加密必需同认证同时发生来验证数据完整性和加密的数据。

这些基本服务的实现在 IPsec 通过使用封装安全性有效负载（ESP）和认证报头（AH）。ESP 提供保密，通过加密原始的 IP 信息包，构建 ESP 报头，在 ESP 有效负载设置机密性。

如果机密性没有发出，可以单独使用 AH 来进行认证和一致性检查。使用 AH，IP 报头的静态字段和散列算法用于计算密钥摘要。接收方使用它的密钥计算和比较摘要来确保信息包没有改变以及发送方的身份是认证了的。

IP 安全性特征

此操作系统的 IP 安全性特征提供下列功能:

- 硬件加速器用 10/100 Mbps 以太网 PCI 适配器 II。
- AH 支持使用 RFC 2402，和 ESP 支持使用 RFC 2406。
- 证书撤销列表支持检索使用 HTTP 或者 LDAP 服务器。
- 自动隧道密钥刷新使用 IETF 网际网密钥交换（IKE）协议。
- X.509 数字证书和预共享密钥支持，在密钥协商时使用 IKE 协议。
- 手工隧道可以配置为提供同其它系统的互操作，不支持自动 IKE 密钥刷新方法，使用 IP 版本 6 隧道。
- 主机或网关隧道封装的隧道方式和传送方式。
- 认证算法 HMAC（散列消息认证代码）MD5（消息摘要 5）和 HMAC SHA（安全散列算法）。
- 加密算法包含 56 位数据加密标准 （DES）代码块链接（CBC）、带有64 位初始向量（VI）、Triple DES、DES CBC 4 （32 位 IV）。
- 双 IP 堆栈支持（IP 版本 4 和 IP 版本 6）。
- 可以封装和过滤 IP 版本 4 和 IP 版本 6 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 和更新的）来创建。
- 使用各种 IP 特征，例如源和目的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的目的地址使用主机名称。主机名称自动地转换到 IP 地址（只要 DNS 可用）。
- IP 安全性事件记录到 **syslog**。
- 问题确定使用系统跟踪和统计学。
- 用户定义的缺省操作允许用户指定是否允许不匹配定义隧道的流量。

网际网密钥交换（IKE）特征

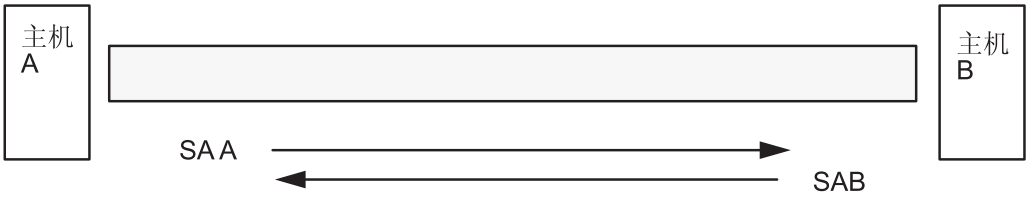
网际密钥交换（开始于 AIX 4.3.2）有下列特征:

- 有预先共享的密钥认证和 X.509 数字签名。
- 使用的主要方式（身份保护模式）和进攻模式。
- 支持 Diffie Hellman 1、2 和 5 组。

- ESP 加密支持数据加密标准（DES）、三重 DES、空加密；ESP 认证支持 HMAC MD5 和 HMAC SHA1。
- AH 支持 HMAC MD5 和 HMAC SHA1。
- IP 版本 4 和 版本 6 支持。

安全性关联

安全通信构建所在的构建模块的概念就是所知的*安全性关联*。安全性关联关联一流量类型安全参数的特定设置。使用 IP 安全保护的数据、每个方向、每个报头类型、AH 或者 ESP 都存在分离的安全性关联。包含在安全关联的信息包括通信各方的 IP 地址、唯一标识符称作安全性参数索引（SPI）、认证和加密选定的算法、认证和加密的密钥和密钥生命周期。下列数字显示了在主机 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
密锁
加密器算法和格式
认证算法
密锁生命期

图 6. 在主机 A 和 B 之间建立安全隧道。. 本说明显示运行在主机 A 和主机 B 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。一个安全性关联包括目标地址、SPI、密钥、加密器算法和格式、认证算法及密钥生命期。

密钥管理的目标是协商和计算保护 IP 流量安全性关联。

隧道和密钥管理

要在两个主机间设置安全通信，使用隧道期间必须协商和管理安全关联。下列的隧道类型是支持的，每个使用不同的密钥管理管理技术。

- 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 ISAKMP/Oakley （网际网安全性关联和密钥管理协议）标准，由 IETF 开发。使用此协议，协商和刷新安全性参数，安全的交换密钥。下列认证类型支持: 预共享密钥和 X.509v3 数字证书签名。

协商使用两阶段方法。第一阶段认证通信的各部分，并为第二阶段的安全通信指定使用的算法。在第二阶段，协商数据传输过程使用 IP 安全性参数，并创建和交换安全关联和密钥。

下列表显示的认证算法可以用于 AH 和 ESP 安全协议作为 IKE 隧道支持。

算法	AH IP 版本 4 & 6	ESP IP 版本 4 & 6
HMAC MD5	X	X
HMAC SHA1	X	X
DES CBC 8		X
Triple 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声明周期是相同的，必需手工更新的。

下列表显示的认证算法可以用于 AH 和 ESP 安全协议作为手工隧道支持。

算法	AH IP 版本 4	AH IP 版本 6	ESP IP 版本 4	ESP IP 版本 6
HMAC MD5	X	X	X	X
HMAC SHA1	X	X	X	X
Triple 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传出可以接受或否定的信息包。这允许用户或系统管理员配置主机来控制主机和其他主机之间得流量。过滤信息包的各种属性，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、（磁盘）碎片、界面和隧道定义。

称为*过滤规则*的规则用于关联某种具有特种隧道的流量。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，过滤器规则自动生成指导主机通过安全通道的所有流量。如果需要更多特定类型流量（例如子网到子网），可以编辑或替换过滤器规则来允许使用特殊的隧道进行精确的控制。

对于 IKE 隧道，一旦激活隧道，过滤器规则也将自动生成并插入到过滤器表。

相似地，如果修改或删除了隧道，则自动删除该隧道的规则，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，在机器和防火墙间继承和共享，这对于大量的机器管理是有帮助的。

过滤器规则关联隧道的特别类型的流量，但过滤的数据未必需要在隧道中传送。过滤器规则让操作系统提供基本的防火墙功能给用户，他们想限制从没有实际防火墙保护的内部网和外部网络上进入和流出他们机器的流量。在此情况，过滤器规则在一组机器间提供第二层保护屏障。

在过滤器规则生成后，他们存储在表中，并装入内核。当信息包准备从网络发送或接收，在列表中从头到尾检查过滤器规则确定信息包是否许可，是否拒绝或是否通过隧道发送。规则标准同信息包特征比较，直到找到匹配或达到缺省规则。

IP 安全性函数同样实现不安全信息包，基于分散的、用户定义标准的过滤器，这将允许对网络和机器间控制流量，不需要认证或者 IP 安全性的加密属性。

数字证书支持

IP 安全性支持使用 X.509 版本 3 数字证书。密钥管理器工具管理证书申请，维护密钥数据库，并进行其他的管理功能。

数字证书的描述在数字证书配置中。密钥管理员和它的功能的描述在使用 IBM 密钥管理员工具

虚拟专用网和 IP 安全性

一个虚拟专用网（VPN），通过如网际网一样的公共网络，安全地扩展一专用内部网。VPN 传送信息通过必须是专用的隧道，是从远程用户、分支营业处和商业伙伴/供应商通过因特网发送或接受报文的专用的隧道。VPN 通过本质上是因特网的专用通道与远程用户、分支机构和商务伙伴／供应商相互传递信息。公司可以选择因特网存取因特网服务供应商 （ISP），使用直接的线路或本地电话号码，排除更贵的专用线路，长距离的调用和无声电话号码。一 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 版本 4 和 6 的环境，现有的应用程序不需要改变。

对在 AIX 中规划和实现 VPN 的推荐资源是第 9 章*虚拟专用网的易理解指南，卷 III: 交叉平台密钥和策略管理*，ISBN SG24-5309-00。此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。需要安装的文件集合如下:

- **bos.net.ipsec.rte**（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* 是想要用的语言，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 文件集合位于扩展压缩包中。对于 IKE 数字签名支持，您必须也安装 **gskit.rte** 文件集（AIX V4）或者扩展压缩包中的 **gskkm.rte**（AIX 5.1）。

安装后，对于 IP 版本 4和 IP 版本 6，可以独立装入 IP 安全性，使用『装入 IP 安全性』中提供的推进过程或者使用 **mkdev** 命令。

装入 IP 安全性

注意: 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 安全性设备为可用。

```
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，隧道和过滤准备配置。

规划 IP 安全性配置

为了配置 IP 安全性，必须配置隧道和过滤。当为全部流量使用定义简单隧道，过滤规则可以自动地生成。如果描述更多复杂过滤，过滤规则可以分开配置。

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、或系统管理界面程序（SMIT）。如果使用 SMIT，以下可用下列快路径:

smit ips4_basic
IP 版本 4 基本配置

smit ips6_basic
IP 版本 6 基本配置

在配置站点 IP 安全性之前，必须决定用什么方法；比如，是否使用隧道或过滤器（或两个都使用），需要哪一种类型的隧道等等。以下部分提供了在做出决定之前必须理解的信息:

- 硬件加速
- 隧道与过滤器
- 隧道和安全性的关联
- 选择隧道类型
- 使用 IKE 和 DHCP 或动态的指定地址

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，以及从 AIX 操作系统中设计成卸载 IP 安全性功能。当 10/100 Mbps 以太网 PCI 适配器 II 出现在 AIX 系统中，IP 安全性堆栈使用以下适配器权能:

- 加密和解密使用 DES 或三重 DES 算法
- 认证使用 MD5 或 SHA-1 算法
- 安全性联系信息的存储。

适配器的功能用来代替软件算法。10/100 Mbps 以太网 PCI 适配器 II 对于手工和 IKE 隧道是可用的。

IP 安全性硬件加速功能在 **5.1.0.25** 或稍后级别的 **bos.net.ipsec.rte** 和 **devices.pci.1410ff01.rte** 文件集是有用的。

对于安全性联系的数量有一个限制，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:

- 通过 ESP 加密 DES，3DES 或 NULL
- HMAC-MD5 或 HMAC-SHA-1 认证，通过 ESP 或 AH，但不能同时。（如果 ESP 和 AH 同时使用，ESP 必须首先执行。对于 IKE 隧道总是真，但用户可以选择给手工隧道的订单。）
- 传送和隧道方式
- 卸载 IPV4 信息包

注: 10/100 Mbps 以太网 PCI 适配器 II 用 IP 选项处理信息包。

为使 10/100 Mbps 为了使用 IP 安全性的以太网 PCI 适配器，必须拆离网络接口，然后使 IPsec 有卸载功能。

为了拆离网络接口，使用 SMIT 接口请执行以下操作:

1. 作为 **root** 用户登陆。
2. 在命令行输入 `smitty inet` 按下 Enter 键。
3. 选择**除去网络接口**选项并按下 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下 Enter 键。

为了能使用 IPsec 卸载功能，用 SMIT 接口请执行以下操作:

1. 作为 **root** 用户登陆。
2. 在命令行输入 `smitty eadap`，并按下 Enter 键。
3. 选择**更改/显示以太网适配器的特征**选项，并按下 Enter 键。
4. 选择 10/100 Mbps 以太网 PCI 适配器 II，并按下 Enter 键。
5. 更改 **IPsec 卸载**字段成为**是**，并按下 Enter 键。

为了拆离网络接口，从命令行，输入以下:

```
# ifconfig enX detach
```

为了使用 IPsec 卸载特征，从命令行，输入以下:

```
# chdev -l entX -a ipsec_offload=yes
```

为了验证 IPsec 卸载特征可用，从命令行，输入以下:

```
# lsattr -El entX detach
```

为了禁用 IPsec 的卸载特征，输入以下:

```
# chdev -l entX -a ipsec_offload=no
```

使用 **enstat** 命令来确保隧道配置在利用 IPsec 和卸载属性。**enstat** 命令显示了发送和接收的 IPsec 信息包的全部的统计信息，当 IPsec 卸载特征启用时。例如，如果以太网接口是 *ent1*，输入以下:

```
# entstat -d ent1
```

输出与下列的信息相似:

```
.
.
.
10/100 Mbps Ethernet PCI Adapter II (1410ff01) Specific Statistics:
---------------------------------------------
.
.
.
Transmit IPsec packets: 3
Transmit IPsec packets dropped: 0
Receive IPsec packets: 2
Receive IPsec packets dropped: 0
```

隧道与过滤器

IP 安全性的两个不同部分是*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出入的信息包。这个功能允许系统管理员配置主机来控制主机之间的流量。过滤基于信息包属性来做的，比如源位置和目标位置，IP 版本（4 或 6），子网掩码协议，端口，路由特征，磁盘碎片，接口和隧道定义。过滤是在 IP 层进行的，所以应用程序无须更改。

- *隧道*定义了两个主机间的安全联系。该安全联系包括特定的安全参数，它们由隧道的端点共享。

以下的说明表示了信息包是怎样从网络适配器中到 IP 堆栈中的。从那里，如果允许或否认信息包，调用过滤器模块。如果隧道标识指定，信息包会检查现有的隧道定义。如果从隧道中成功解封，信息包传递到高层协议。该功能在流出信息包的逆向发生。隧道依赖于过滤规则来关联信息包和特定的信息包，但是过滤功能不用在发送信息包到隧道的情况下就可以发生。

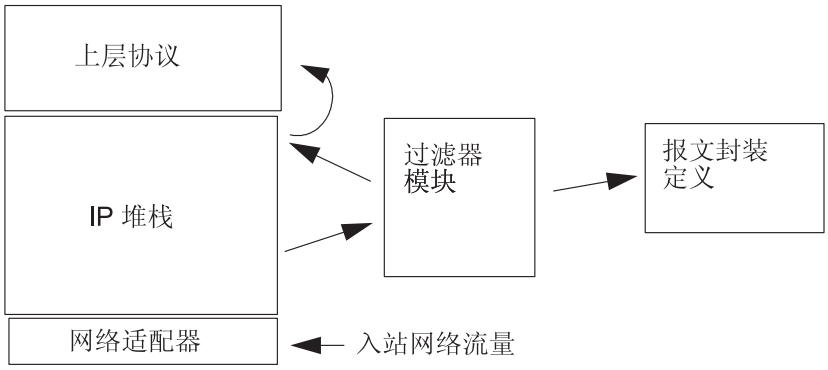
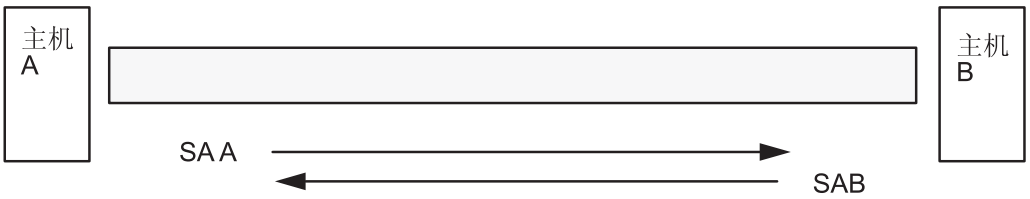


图 7. 网络信息包路由. 这个说明显示了网络信息包采用的路由。从网络入站，信息包输入网络适配器。从那里它到达 IP 堆栈，再发送到过滤器模块。从过滤模块，或者发送信息包到隧道定义，或者将其返回 IP 堆栈，从那里将其转发到上层协议。

隧道和安全性的关联

隧道不管在什么时候使用，都必须有认证的数据或认证和编码。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隧道的加密、认证算法和特征的参数。以下说明显示了主机 A 和主机 B 之间的虚拟文件分配器的隧道。



SA = 安全性关联，由下列项组成：

目标地址
SPI
密锁
加密器算法和格式
认证算法
密锁生命期

图 8. 主机 A 和主机 B 之间的安全隧道的建立. 这说明显示了虚拟文件分配器隧道，它们在主机 A 和主机 B 之间运行。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）和目的地址识别唯一的安全性关联。为了唯一指定隧道，这个参数是需要的。其它参数，比如密码算法，认证算法，密钥和生命期，都要指定或承认缺省值可用。

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与定义隧道端点不同的过程。在 IKE 中，有两步协商过程。每一步的协商过程叫做一个*阶段*，每一阶段有不同的安全性策略。

当因特网的密钥协商启动，它必须为协商建立一个安全信道。这称做*密钥管理*阶段或*阶段 1*。在这个阶段，每个当事人使用前共享密钥或数字证书来认证对方并传递 ID 信息。这个阶段安装了安全性关联，在两个当事人确定它们怎样安全的计划通信以及在第二阶段，用什么样的保护来进行通信。该阶段的结果是 *IKE* 或*阶段 1* 隧道。

第二阶段是*数据管理*阶段或*阶段 2*，它使用 IKE 隧道来创建安全性关联，为了实际保护流量 AH 和 ESP。第二阶段也要确定将要使用 IP 安全性隧道的数据。例如，它可以指定下列:

- 子网掩码
- 地址范围
- 协议和端口号合并

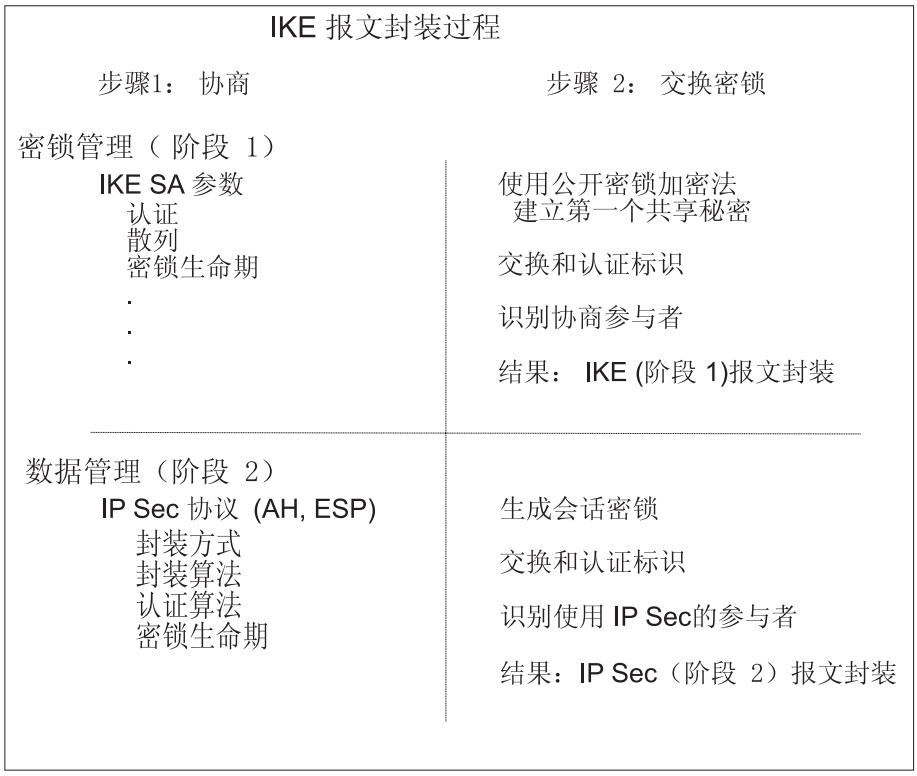


图 9. IKE 隧道安装过程. 这个说明为了安装 IKE 隧道显示两步，两阶段过程。

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标识。IKE 遂道端点是执行协议的机器的标识。IP 安全性隧道端点描述了流量的类型，它们将要使用 IP 安全性隧道。对于简单的主机对主机的隧道，在其中两隧道之间全部的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和子网（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）用下面参数来配置 IKE 隧道。

密钥管理（阶段 1）隧道	IKE 隧道的名称。对于每个隧道，协商的端点必须指定。有两个机器来发送和验证 IKE 信息。隧道的名称描述了隧道端点，比如 VPN Boston 或 VPN Acme。
主机识别类型	使用于 IKE 交换的 ID 类型。为了预共享密钥来确保合适的密钥查询的执行，ID 类型和值必须匹配。如果单一的主机有超过一个的预共享密钥值，KEY_ID 类型很有用。
主机标识	主机标识的值表示为一个 IP 地址，全限定域名（FQDN），或在全限定域名（*用户 @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 或不管什么时候主机标识类型不能由IP 地址解析时，这个值是需要的。例如，示例用户不能用本地名称服务器来解析，那么要输入远程方的 IP 地址。

不能通过指定那些在 IKE 协商中使用过的参数制定密钥管理策略。例如，有为预共享密钥或签名方式认证的密钥管理。对于阶段 1，用户必须确定某个密钥管理安全性属性，用它来执行交换。

数据管理参数和策略

数据管理协议参数在 IKE 隧道配置的阶段 2 设置。在手工隧道中使用时，它们是相同的 IP 安全参数，同时描述了用做在隧道中保护数据通信量保护类型。启动阶段可以在相同的阶段 1 隧道下启动超过一个阶段 2 隧道。

以下的端点标识类型描述了那些用 IP 安全性数据隧道的数据类型:

主机、子网或范围	描述是否在隧道中流通的数据通信量将是为了一个特定的主机、子网或地址范围。
主机/子网 ID	包含本地和远程系统主机或子网的识别，系统在隧道中传递流量。确定标识在阶段 2 协商发送，如果协商成功，将构建过滤规则。
子网掩码	描述子网内全部的 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	为地址范围提供启动的 IP 地址，它们将用隧道（例如，9.53.250.96 的 9.53.250.96 到 9.53.250.93）
结束 IP 地址范围	为地址范围的结束提供 IP 地址，它们将使用隧道（例如，9.53.250.93 的 9.53.250.96 到 9.53.250.93）
端口	描述数据，使用特定端口号（例如，21 或 23）
协议	描述正用特定协议传送的数据（例如，TCP 或 UDP）。确定协议在阶段 2 协商发送，如果协商成功，将构建过滤规则。本地端点的协议必须和远程端点协议匹配。

选择隧道类型

使用手工隧道或 IKE 隧道的描述取决于远程终端的隧道支持和需要的密钥管理的类型。推荐 IKE 隧道（当可用的时），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 头类型并支持反重演保护。有选择的配置签名方式来允许数字证书。

如果远程端使用需要手工隧道的其中一个算法，要使用手工隧道。手工隧道确保了大量主机的互操作性。因为密钥是静态的，很难改变的，可能更新很麻烦，所以它们不安全。手工隧道在运行这种操作系统的主机和其它运行 IP 安全并且有公共加密和认证设置的机器中使用。大多数供应商提供密钥 MD5 和 DES、或 HMAC MD5 和 DES。这个子集与几乎全部 IP 安全性实现一起工作。

在安装手工隧道的过程取决于是否安装隧道的第一个主机或第二个主机，第二个主机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，算法是默认的。当安装第二主机，如果可能，从远程终端导入隧道信息。

另一个重要的注意事项是确定是否远程系统在防火墙之后。如果是的，安装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

常见情况下，它用操作系统来使用 IP 安全性，是当远程系统在用服务器启动 IKE 部分时，它的识别不能连接到特定的 IP 地址。该情况在本地局域网（LAN）环境发生，比如使用 IP 安全性把一个服务器连接到 LAN 上，并加密数据。其它公共使用包括远程客户机向服务器拨号，或者使用全限定域名（FQDN）或 e-mail 地址（*user@FQDN*）来标识远程 ID。

为了制定策略判定，基于清楚的关于远程识别的信息，必须使用主动方式。这时，识别在第一协商信息中发送，并且可以在安全性策略数据库中用来作为策略查询。这将确保仅仅指定命名的远程识别将可能协商使用 IKE 协议。

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，一般数据管理器隧道可以配置。因此，如果 IP 地址在数据库中没有清楚的配置，阶段 1 期间任何认证了的请求将使用一般隧道来定义“数据管理”阶段。它允许任何地址匹配一般的隧道，只要严格公共的基于密钥的安全性确认在阶段 1 是成功的，那么就可以使用。

使用 XML 来定义一般数据管理隧道

定义一般数据管理隧道，使用 **ikedb** 可以理解的 XML 格式。一般数据管理与 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*。*一般数据管理隧道*不是真正的隧道，而是一个 **IPSecProtection**，它在进入的“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。它仅仅在 AIX 系统是响应程序的情况下使用。指定一般的数据管理隧道 **IPSecProtection** 是可选的。

一般数据管理隧道定义在 **IKEProtection** 元素里。有两个 XML 属性，叫作 **IKE_IPSecDefaultProtectionRef** 和 **IKE_IPSecDefaultAllowedTypes**，可以在这里使用。

首先，需要定义一个 **IPSecProtection**，它可以用作缺省值，如果没有 **IPSecTunnels**（数据管理隧道）。用作缺省值的 **IPSecProtection** 必须有 **IPSec_ProtectionName**，它以 `_defIPSprot_`开始。

现在执行 **IKEProtection**，它要使用 **IPSecProtection**这个默认值。指定 **IKE_IPSecDefaultProtectionRef** 属性，它包含缺省值 **IPSec_Protection** 的名称。

必须在 **IKEProtection** 里为 **IKE_IPSecDefaultAllowedTypes** 属性指定一个值。它可以有一个或更多的以下值（如果有多个值，它们需用空格分开。）

```
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
```

这些值由创建人来指定，来对 ID 类型作出响应。在 IKE 协商中，忽略了实际的 ID。指定的 **IPSecProtection** 会使用，如果 **IKE_IPSecDefaultAllowedTypes** 属性包含一个以 Local_ 开始的字符串，它对创建人的本地 ID 类型作出响应，同时包含一个以 Remote_ 开始的字符串，它对创建人的远程 ID 作出响应。换句话说，至少有一个 **Local_** 值和至少一个 **Remote_** 值在任何 **IKE_IPSecDefaultAllowedTypes** 的属性里，是为了对使用的 **IPSec_Protection** 作出响应。

示例: 创建人发送下列信息到 AIX 系统，在阶段 2（数据管理）报文里:

```
local ID type:    IPV4_Address
local ID:         192.168.100.104

remote ID type:   IPV4_Subnet
remote ID:        10.10.10.2
remote netmask:   255.255.255.192
```

AIX 系统没有数据管理隧道与这些 ID 匹配。但是它有一个有下列定义属性的 **IPSecProtection**。

```
IKE_IPSecDefaultProtectionRef="_defIPSprot_protection4"
IKE_IPSecDefaultAllowedTypes="Local_IPV4_Address
                              Remote_IPV4_Address
                              Remote_IPV4_Subnet
                              Remote_IPV4_Address_Range"
```

输入报文的本地 ID 类型，**IPV4_Address**，与允许类型的 **Local_** 值的其中一个匹配，**Local_IPV4_Address**。同时，报文的远程 ID 类型，**IPV4_Subnet**，与值 **Remote_IPV4_Subnet** 匹配。因此数据管理隧道协商将作为 **IPSecProtection** 和 _defIPSprot_protection4 一起进行。

/usr/samples/ipsec/default_p2_policy.xml 文件是一个完全的 XML 文件，它定义了一个通用的 **IPSecProtection**，其可作为示例使用。

配置网际密钥交换隧道

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）隧道的信息。

使用基于 Web 的系统管理器配置 IKE 隧道

『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 隧道。更多高级选项请参阅『高级 IKE 隧道配置』.

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 的系统管理器添加一个新的密钥管理和数据管理 IKE 隧道到 IP 安全性子系统，允许您输入极小数据并选择一些选项，对于隧道生命期这样的参数，使用公共缺省值。

当使用基本配置向导时，以下的要牢记:

- 向导只可用于初始隧道配置。要修改、删除或激活隧道，使用 **IKE 隧道**插件或任务栏。
- 系统中隧道的名称是唯一的，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，隧道的名称可以是 *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 的隧道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 格式输入。
- 如果数字证书选作认证方法，则您必须使用密钥管理器来创建数字证书。
- 主机 ID 类型只能是 `IP` 地址.
- 您创建的转换和提议指定名称结束于用户定义的隧道名称。您可以在基于 Web 的系统管理器上查看转换与提议，通过 **VPN** 和 **IKE 隧道**插件。

利用向导用下列过程来配置新的隧道:

1. 打开基于 Web 的系统管理器使用命令行中的 **wsm** 命令。
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**配置基本隧道配置向导**。
6. 在步骤 1 介绍面板中单击**下一步**，然后按照步骤配置 IKE 隧道。

   如果需要的话可以使用联机帮助。

   在使用向导定义了隧道之后，隧道的定义就显示在基于 Web 的系统管理器 IKE 隧道列表中，并且可以激活或修改。

高级 IKE 隧道配置

您可以分别配置密钥管理和数据管理隧道，采用以下的过程。

配置密钥管理隧道: 采用基于 Web 的系统管理器配置 IKE 隧道。使用以下过程来添加密钥管理隧道:

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隧道。

- 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隧道的流量类型。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隧道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. 要定义密钥管理隧道端点，单击识别标签中的**网际密钥交换（IKE）隧道**。
7. 输入信息描述参与协商的系统身份。大部分情况下，采用 IP 地址，并且必须创建与远程方兼容的策略。

   在转换标签中，对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允许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**标签下输入预共享密钥。该值必须对于远程和本地机器都匹配。
9. 使用转换标签上的**添加**按钮来创建与该隧道有关的转换。

   要启用数字证书和签名方式支持，选择 **RSA 签名**或者**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 144 页的『处理数字证书和密钥管理器』。

配置数据管理隧道: 要设置数据管理隧道端点及提议并完成 IKE 隧道设置，打开基于 Web 的系统管理器，如第 138 页的『配置密钥管理隧道』所述。数据管理隧道按照以下步骤创建:

1. 选择密钥管理隧道，定义任意唯一的选项。大多数数据管理选项可以保留作缺省定义。
2. 在端点标签下指定端点类型（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，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 安全性隧道定义中的 IKE ID 分组，以使多个 ID 与单一的安全性策略相关联，而不需要创建单独的隧道定义。当设置连接到多个远程主机时，分组尤其有用，因为您可以避免设置或管理多个多个隧道定义。同样的，如果必须要更改安全性策略，您不必更改多个隧道定义。

在使用隧道定义中的那个组名称之前，必须先定义一个组。组的大小限制为 1 KB。组名在密钥管理和数据管理隧道定义中都可以用，但是它只能用作远程 ID。

组是由组名和 IKE ID 及 ID 类型列表组成的。ID 可以全都是相同的类型或者下面的组合:

- 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 ID 以获得第一个匹配。

基于 Web 的系统管理器可以用来定义一个用于密钥管理隧道的远程端点的组。关于从命令行定义组的信息，请参考第 140 页的『IKE 隧道配置的命令行界面』节。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 隧道**容器中选择密钥管理隧道。
2. 打开**属性**对话框。
3. 选择**识别**标签。

4. 对于远程主机身份类型选择**组 ID 定义**。
5. 选择**配置组定义**按钮，在窗口中输入组号。

将 SMIT 界面用于 IKE 隧道配置

您可以使用 SMIT 界面来配置 IKE 隧道并执行基本的 IKE 数据库功能。SMIT 使用基本的 XML 命令函数来执行对 IKE 隧道定义的添加、删除和修改。IKE SMIT 用在快速配置 IKE 隧道并提供了用于创建 IKE 隧道定义的 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 隧道，请使用 **smitty ike4** 快速路径。要配置 IPv6 IKE 隧道，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 数据库条目都可以通过基于 Web 的系统管理器工具查看或修改。

IKE 隧道配置的命令行界面

ikedb 命令，在 AIX 5.1 及其后版本中可用，它允许用户检索、更新、删除、导入和导出 IKE 数据库中的信息，使用 XML 界面。**ikedb** 命令允许用户从 IKE 数据库中写入（放入）或者读出（获取）。输入输出格式是一个可扩展标记语言（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 所能做的唯一的修改。任何输入 XML 文件中的外部文档类型声明都将忽略，任何内部文档类型声明可能导致出错。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，它定义了公共隧道情况。关于语法的详细信息，请参阅 **ikedb** 命令描述，在 *《AIX 5L V5.2 命令参考大全》* 中。

您可以使用 **ike** 命令来启动、停止和监视 IKE 隧道。**ike** 命令也可用于激活、除去或者列出 IKE 和 IP 安全性隧道。关于语法的详细信息，请参阅 **ike** 命令描述，在 *《AIX 5L V5.2 命令参考大全》* 中。

以下示例显示了如何使用 **ike**、**ikedb**和几个其他的命令来配置和检查您的 IKE 隧道的状态。

1. 要启动隧道协商（*激活*隧道）或者允许进入系统充当响应程序（取决于指定的角色），使用带有隧道号的 **ike** 命令，如下所示:

   ```
   # ike cmd=activate numlist=1
   ```

   您也可以使用远程标识符或者 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. 要显示隧道状态，使用 **ike** 命令，如下所示:

   ```
   # ike cmd=list
   ```

   输出类似于下面的显示:

   ```
   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 隧道。
3. 要获得隧道的详细列表，请使用 **ike** 命令，如下所示:

   ```
   # ike cmd=list verbose
   ```

   输出类似于下面的显示:

```
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最近激活的 IKE 隧道过滤器规则，使用 **lsfilt** 命令，如下所示:

```
# lsfilt -d
```

输出类似于下面的显示:

```
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 隧道无其它隧道的机器。用户可以移动动态过滤设置规则（在这个静态表格示例输出中的 #2 规则）来控制与所有其他用户定义的规则有关的设置。动态表中的规则随隧道的协商自动构造，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 #2 规则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
   ```

   关于 IKE 流量记录的更多详细信息，请参阅第 162 页的『记录设施』。

6. 要取消激活隧道，使用 **ike** 命令，如下所示:

   ```
   # ike cmd=remove numlist=1
   ```

7. 要查看隧道定义，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. 要获取名为 *tunnel_sys1_and_sys2* 的阶段 1 隧道的定义和所有带有各自提议和保护的相应的阶段 2 隧道，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 隧道分组支持的一般信息，请参阅第 139 页的『分组支持』节。您可以使用 **ikedb** 命令从命令行中定义组。

AIX IKE 与 Linux 的类似性

要配置 AIX IKE 隧道，通过 Linux 配置文件（AIX 5.1 及更新的），请使用 **ikedb** 命令，带有 **-c** 标志（转换选项），它使得您将 **/etc/ipsec.conf** 和 **/etc/ipsec.secrets** Linux 配置文件用作 IKE 定义。**ikedb** 命令分析 Linux 配置文件，创建 XML 文件，并选择性的把 XML 隧道定义添加到数据库中。然后您可以使用 **ikedb -g** 命令或基于 Web 的系统管理器来查看隧道。

IKE 隧道配置

以下场景描述了大多数客户试图设置隧道时遇到的情况的类型。这些场景可以描述分公司、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个位置的工程组。本示例中，有网关互相连接，所有通过网关的流量使用相同的隧道。隧道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，相关的 IKE 安全性在两个网关之间创建。通过 IP 安全性隧道的流量是两个子网之间的流量，子网 ID 用于阶段 2 协商。在输入隧道的安全性策略和隧道参数之后，创建了一个隧道号。使用 **ike** 命令启动隧道。

- 在业务伙伴场景中，网络是不可信的，网络管理员可能想要限制安全性网关后面少数主机的访问。在这种情况下，主机之间的隧道通过用于两台特殊主机之间的 IP 安全性来传送受保护的流量。阶段 2 隧道的协议是 AH 或 ESP。这种主机 – 主机的隧道在网关 – 网关隧道内是安全的。
- 在远程访问情况下，隧道按照要求设置，应用高级安全性。IP 地址可能没有意义，因此，全限定域名或*用户* @ 全限定域名作为首选。您可以选择性的使用密钥 ID 将密钥与主机 ID 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。以AIX 4.3.3开头，IP 安全性使用数字证书来启用*公用密钥密码术*，也是我们所熟知的*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。*密钥对*是长串数据，这些数据充任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通信的任何人。发送方数字化的签名所有带有相应的专用密钥的安全通信为其指定的密钥对。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解密了消息，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第三方，知名的*认证中心*（*CA*），来发布可信赖的数字证书。接收方指定哪个发布组织或权限是可信的。证书发布特定的时间；当超过失效日期时，必须替换它。

AIX 4.3.3 及其后的版本提供密钥管理器，它管理数字证书。以下节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段。请参阅下图获得数字证书的说明。

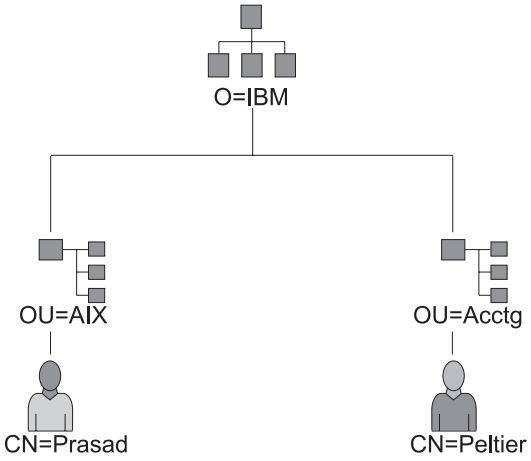
图 10. 数字证书的内容. 该插图显示了数字证书的四个实体。从上面开始是: 所有者区别名称、所有者公用密钥、发行商（CA）区别名称和发行商签名。

以下的列表进一步描述了数字证书的内容。

所有者区别名称

目录树中所有者普通名和内容（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，区别名称为:

```
/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. 目录树的派生区别名称示例. 该插图是一个目录树，顶级 0 = ABC，第二级分支到两个实体。二级包含两个单独的分支上的 OU=AIX 和 OU=Acctg；每个都有一个分支导向上一层的单独的实体。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。

发布日期
发布数字证书的日期。

失效日期
数字证书失效日期。

发行商区别名称
认证中心的区别名称。

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。数字证书只允许验证数字证书所有者的身份，通过提供所需的公用密钥来检查所有者的数字签名。您可以安全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），您的数据是无法解密的。因此，所有者必须保护专用密钥，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，发布出证书的策略应该可以理解。每个组织或用户必须确定哪个认证中心可以作为值得信任的来接受。

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。并且，简单的接收数字证书不保证它的可靠性。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。如果您还没有保留 CA 公用密钥的确定的副本，则可能需要附加的数字证书来获得 CA 的公用密钥。

证书撤销列表（CRL）

数字证书希望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失效日期之前就无效了。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。要使证书过期，您必须把详情通知相应的认证中心（CA）。当 CA 取消证书时，它添加无效的证书序列号到证书撤销列表（CRL）中。

CRL 是签署的数据结构，它周期性的发布并在一个公共资源库中可用。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。每个取消的证书用它在表中的证书序列号来识别。

配置 IKE 隧道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 签名来确认没有取消证书。如果 CRL 校验启用，在协商过程期间定位并检查列表来建立密钥管理隧道。

> **注意**：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 服务器或二者都用。如果您知道是使用 SOCK 还是 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设置选择。从数字证书菜单中选择 **CRL 配置**。

用于因特网应用程序中的数字证书

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，包括以下的:

虚拟专用网（VPN）

虚拟专用网，也称为*安全隧道*，可以在防火墙这样的系统之间设置来启动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。

用于隧道的协议遵循 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 浏览器中之间的安全连接，连同用于 LDAP 客户机和 LDAP 服务器之间安全连接的轻量级目录访问协议（LDAP）以及用于客户机和主机系统之间连接的 Host-on-Demand V.2。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区别名称、所有者公用密钥、CA 区别名称和 CA 签名等字段。自签署数字证书包含所有者区别名称、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区别名称、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，它位于扩展压缩包的 **gskkm.rte** 文件集合中。

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 隧道

要设置数字证书和签名支持，最少您必须执行任务1、2、3、4、6 和 7。然后，使用基于 Web 的系统管理器来创建 IKE 隧道并将策略和使用 RSA 签名作为认证方法的隧道相关联。

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来连接具有来自一个签发者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 148 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. 如果想要更改密码失效天数，在**设置失效时间?** 字段输入想要的天数。该字段的缺省值为 60 天。如果不想要密码失效，则清除**设置失效时间?** 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动带有 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 形式，如下所示:

```
cert.arm
```

要添加一个 CA 根数字证书到数据库中，使用下列过程:

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:

   ```
   基于64位编码的 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 证书设置缺省情况下为**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. 选择**个人证书申请**，从个人 / 自签署证书下拉菜单中（在 AIX V4 中）或者选择**创建 - > 新的证书申请**（在 AIX 5.1 中）。
6. 单击**新建**。
7. 从下面的屏幕中，输入自签署数字证书的**密钥标签**，例如:

```
keytest
```

8. 输入**普通名**（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建值。
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 地址的隧道类型，把在 IKE 隧道中配置的相同的 IP 地址输入到 IP 地址字段。对于 *user@FQDN* 的隧道 ID 类型，完成电子邮件地址字段。对于 FQDN 隧道 ID 类型，在 DNS 域名字段输入全限定域名（例如，*主机名 . 公司名 .*
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，验证您已创建了新的数字证书申请。
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 来申请一个新的数字证书。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 接收了新数字证书之后，必须把它添加到您生成申请的那个密钥数据库中。

要添加（接收）新的数字证书，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. 突出显示您从中生成证书申请的密钥数据库文件，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 / 自签署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您的数据库中）。
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**基于64位编码的 ASCII 数据**。
8. 输入新数字证书的证书文件名和位置，或者单击**浏览**来选择名称和位置。
9. 单击**确定**。
10. 输入新建的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。

    如果装入证书有出错，检查证书文件是否起始于 `---BEGIN CERTIFICATE---` 文本，结束于 `---END CERTIFICATE---` 文本。

    例如:

    ```
    -----开始证书-----
    ajdkfjaldfwwwwwwwwwwadafdw
    kajf;kdsajkflasasfkjafdaff
    akdjf;ldasjkf;safdfdasfdas
    kaj;fdljk98dafdas43adfadfa
    -----结束证书-----
    ```

    如果文本不匹配，编辑证书文件从而使它适当的开始和结束。

删除数字证书

注: 在删除数字证书之前，创建备份副本，以防止以后想要重新创建它。

要从数据库中删除数字证书，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删除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 / 自签署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，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，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**更改密码**。
3. 在**密码**字段中输入新密码，在**确认密码**字段中再次输入一遍。
4. 如果想要更改密码失效天数，在**设置失效时间?** 字段输入想要的天数。该字段的缺省值为 60 天。如果不想要密码失效，则清除**设置失效时间?** 字段。
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动带有 IP 安全性的数字证书的使用。
6. 单击**确定**。状态栏的消息表示成功完成的申请。
7. 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。

使用数字证书创建 IKE 隧道

要创建使用数字证书的 IKE 隧道，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 隧道策略时要启用数字证书的作用，必须配置使用签名方式的转换。 *签名方式*将 RSA 签名算法用于认证。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 签名认证方法。

隧道至少一个端点必须具有使用签名方式转换定义的策略。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 密钥管理隧道类型（识别标签上的**主机身份类型**字段）如下:

- IP 地址
- 全限定域名（FQDN）
- *user@FQDN*

- X.500 区别名称
- 密钥标识符

使用**基于 Web 的系统管理器**在密钥管理隧道属性 – 识别标签中选择主机 – 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**标签上从基于 Web 的系统管理器下拉列表中选择主机身份类型为 **X.500 区别名称**，并且输入**主机身份**为 **/C=US/O=ABC/OU=SERV/CN=*名称为* .austin.ibm.com**，则下面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。

- 普通名: ***名称* .austin.ibm.com**
- 组织: **ABC**
- 组织单元: **SERV**
- 国家或地区: **US**

输入的 **X.500 区别名称**是由您的系统或 LDAP 管理员设置的名称。输入单位部门值是可选的。然后，在创建数字证书时，CA 使用该信息。

另一个示例，如果您从下拉列表中选择主机身份类型为 **IP 地址**，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。

- 普通名: ***名称* .austin.ibm.com**
- 组织: **ABC**
- 组织单元: **SERV**
- 国家或地区: **US**
- 主题备用 IP 地址字段: **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 需要下面的信息:

- 您在申请 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 149 页的『申请数字证书』。

在激活 IKE 隧道之前，必须把您从 CA 接收到的个人数字证书添加到密钥管理器数据库中，**ikekey.kdb**。更多信息，请参阅第 150 页的『添加（接收）新的数字证书』。

IP 安全性支持下面的个人数字证书类型:

主题 DN

主题区别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

主题区别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

主题区别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。

主题 DN 和主题备用名称为 *user@FQDN*

主题区别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 和主题备用名称

主题区别名称可以用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。

配置人工隧道

以下过程配置 IP 安全性以使用人工隧道。

设置隧道和过滤器

要设置人工隧道，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隧道，就会自动生成必要的过滤规则。设置隧道的过程是为了在一端定义隧道，在另一端导入定义，并在两端激活隧道和过滤规则。然后隧道就准备使用。

如果没有明白的提供出来的话，则必须产生关于隧道的信息用于两端的匹配。例如，如果目标值没有指定的话，为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隧道

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 版本 4）或者 SMIT **ips6_basic** 快速路径（对于 IP 版本6）来配置隧道。您也可以使用以下过程手工创建隧道。

下面是一个用于创建人工隧道的 **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隧道的特征。输出类似于下面的显示:

```
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     : -
```

要激活隧道，输入如下:

```
mktun -v 4 -t1
```

将会自动生成与隧道有关的过滤器规则。

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，包括缺省的过滤规则，请使用 **mktun -v 4 -t 1** 命令。

要设置另一边（当它是另一台使用该操作系统的机器时），可以从 A 主机上导出隧道定义，然后将其导入到 B 主机。

下列命令将隧道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的隧道

要创建隧道的匹配端，使用如下的命令将引出的文件复制并导入远程机器:

```
imptun -v 4 -t 1 -f /tmp
```

其中

1 是要导入的隧道

/tmp 是导入文件驻留的目录

系统生成隧道号。您可以从 **gentun** 命令的输出来获得，或者使用 **lstun** 命令列出隧道并确定导入的正确的隧道数。如果在导入文件中只有一个隧道，或者所有的隧道都要导入，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隧道另一端的算法、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隧道。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 信息包的属性定义特定的过滤功能来定制过滤。通过比较源地址和 SPI 值与过滤器表中所列出源地址和 SPI 值，来完成进入信息包的匹配。因此，这种配对必须是唯一的。

过滤器表中的每个行看作是一个*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、隧道和接口类型。

过滤规则的类型如下:

- 『静态过滤器规则』创建在过滤器表中，用于流量的常规过滤或者人工隧道的关联。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 159 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*过滤规则）是为了使用 IKE 隧道而创建的特定的规则集合。静态和动态过滤规则都基于数据管理隧道信息和数据管理隧道协商来创建。
- 第 160 页的『预定义过滤器规则』是通用过滤规则，不可以修改、移动或删除，例如 `all traffic` 规则、`ah` 规则和 `esp` 规则。它们和所有流量有关。

与这些过滤规则有关的是*子网掩码*，它把与过滤规则有关的 ID 分组，以及主机 – 防火墙 – 主机配置选项。下面几节描述不同类型的过滤器规则和它们的有关特征。

静态过滤器规则

每个静态过滤器规则包含几个空格分隔字段。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 版本 4 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。

注意: 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。

注意: 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

自动生成规则的集合，它过滤通过隧道 1 的地址在 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 有一个用户定义的 *outbound traffic* 描述。

规则 6 到规则 9

用户定义的规则集合，它过滤通过隧道 2 的地址在 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，从而使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，它过滤通过隧道 3 的地址在 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，它过滤通过隧道 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

总是把自动生成规则放在表的末尾。在本示例中，它允许不匹配其它过滤器规则的所有信息包。可以设置它来拒绝所有与其它过滤器规则不匹配的流量。

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
```

下面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 接受

-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 or n.

-c 协议。值可以是 udp、icmp、tcp、tcp/ack、ospf、pip、esp、ah 及 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 二者都

-l 记录控制。

y 包含在记录日志中

n 不包含在记录日志中。

-f （磁盘）碎片。

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 隧道 ID。

-i 接口，如 tr0 或 en0。

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

某些规则自动生成用于 IP 安全性过滤器和隧道代码。自动生成规则包括:

- 更新 IKE 中 IP 版本 4 的会话密钥守护程序规则（AIX 4.3.2 及以后的）。
- 处理 AH 和 ESP 信息包的规则。

当定义隧道时，也会自动生成过滤器规则。对于人工隧道，自动生成的规则指定源地址目标地址及掩码值，以及隧道 ID。那些地址间的所有流量都将流过隧道。

对于 IKE 隧道，自动生成规则确定 IKE 协商期间的协议和端口号。IKE 过滤器规则保存在一个单独的表中，在静态过滤器规则之后和自动生成规则之前可以搜索此表。IKE 过滤器规则插入到静态过滤器表中的缺省位置，但用户不能移动它们。

自动生成规则允许通过隧道的所有流量。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。下面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
```

为简化单一隧道的配置，在定义隧道时自动生成过滤器规则。该功能可以通过在 **gentun** 中指定 **-g** 标志得以禁止。您可以用 **genfilt** 命令查找到一个为不同的 TCP/IP 服务生成过滤器规则的样本过滤器文件，该文件在 **/usr/samples/ipsec/filter.sample** 中。

预定义过滤器规则

用某些事件自动生成预定义过滤器规则。装入 ipsec_v4 或者 ipsec_v6 设备时，将预定义规则插入过滤器表，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。

> **注意**: 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，通过在激活 IP 安全性之前设置缺省操作或者配置到远程机器的隧道。

IPv4 和 IPv6 过滤器表都有一个预定义规则。可以独立的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。要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 隧道，在 IPv4 过滤器表中设置一个动态的过滤器规则。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过滤器表中向上或向下移动其位置来控制。初始化隧道管理器守护程序和 **isakmpd** 守护程序以允许 IKE 隧道协商之后，在动态过滤器表中就会自动地创建规则，以处理 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有关的 ID 集合。掩码值和过滤器规则中的 ID 进行“与”运算，并与信息包中指定的 ID 相比较。例如，源 IP 地址为 10.10.10.4 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

一个 10.10.10.x 的子网指定为 1111.1111.1111.0 或者 255.255.255.0。进入地址应该将附加子网掩码，这样可以将这个组合与过滤器规则中的 ID 比较。例如，地址 10.10.10.100 变成 10.10.10.0，在应用了子网掩码之后，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

隧道的主机 – 防火墙 – 主机配置选项允许您在主机和防火墙之间创建隧道，然后自动生成必需的过滤器规则，用于您的主机和防火墙后的主机之间的正确通信。自动生成过滤器规则允许通过指定隧道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。必须要适当的配置防火墙来完成设置。应该使用来自您所创建的隧道导出的文件来输入防火墙需要的 SPI 值和密钥。

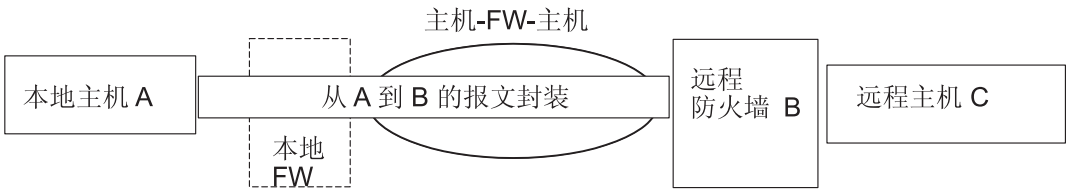


图 12. 主机 – 防火墙 – 主机. 这个插图显示了主机 – 防火墙 – 主机配置。主机 A 有一个运行的隧道，通过本地防火墙外出进入因特网。然后它转到远程防火墙 B，然后再到远程主机 C。

记录设施

本节描述与 IP 安全性有关的系统日志配置和格式。主机间通信时，传送的信息包记录在日志守护程序，**syslogd**。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协助调试选择监视记录信息。下面是设置记录设施的步骤。

1. 编辑 **/etc/syslog.conf** 文件添加下列条目:

   ```
   local4.debug var/adm/ipsec.log
   ```

   使用 local4 设施记录流量和 IP 安全性事件。标准操作系统优先级级别应用。您应该设置 debug 的优先级级别直到通过 IP 安全性隧道和过滤器显示是稳定性和正确的活动为止。

   注: 过滤器事件的日志记录能够在 IP 安全性主机创建大量的活动，并消耗大量的存储量。

2. 保存 **/etc/syslog.conf**。
3. 到您为日志文件指定的目录，并创建一个相同的名称空文件。在上面的情况，您应该换到 **/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 隧道，确保 **/etc/isakmpd.conf** 文件指定想要的 **isakmpd** 记录级别。（请参阅第 166 页的『IP 安全性问题确定』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
   ```

   通过发出下列命令停止信息包的记录:

   ```
   mkfilt -g stop
   ```

下列样本日志文件包含流量条目和其它 IP 安全日志条目:

```
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=
08. 8 月 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
    08/27/971
```

下面段落解释日志条目。

1 激活的过滤器记录守护程序。

2 过滤器信息包记录设置为打开，使用 **mkfilt -g start** 命令。

3 隧道激活，显示隧道 ID、源地址、目的地址和时间戳记。

4-9 已激活过滤器。日志记录显示全部装入的过滤规则。

10 消息显示过滤器的激活。

11-12 这些条目显示对主机的 DNS 查询。

13-15 这些条目显示一个部分 Telnet 连接（由于空间原因，已从本例中除去其他条目）。

16-19 这些条目显示两个 ping。

20 过滤器记录守护程序关闭。

下列示例从启动主机的角度显示两个主机协商阶段 1 和阶段 2 隧道。（指定 **isakmpd** 日志记录级别为 **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.
    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:
    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: (
    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: En
    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
    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
```

下列段解释日志条目。

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 守护程序。

11-12 隧道管理器从响应程序接收有效的阶段 1 安全关联。

13 为了更多工作，隧道管理器检查是否 **ike cmd=activate** 具有阶段 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 隧道。

22-29 **isakmpd** 守护程序协商阶段 2 隧道。

30-31 隧道管理器从响应程序接收有效的阶段 2 安全关联。

32 隧道管理器写动态过滤器规则。

33 **ike cmd=list** 命令查看 IKE 隧道。

字段条目的标签

缩写日志条目字段，以减少 DASD 空间要求:

引起信息包记录日志的规则号码。

R 规则类型

- **p** 允许
- **d** 否定

i/o 过滤器支持代码截获信息包时，信息包的移动方向。标识同信息包有关的适配器 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 层决定应该处理的信息包传送的适配器。

s 指定发送方信息包（从 IP 报头抽取）的 IP 地址。

d 指定接收方信息包（从 IP 报头抽取）的 IP 地址。

p 指定高级协议用于创建在信息包中数据部分的消息。或许是一数字或名称，例如: udp、icmp、tcp、tcp/ack、ospf、pip、esp、ah 或者 all。

sp/t 指定同信息包发送方（从 TCP/IP 报头抽取的）相关的协议端口号。当协议是 ICMP 或者 OSPF，此字段用 **t** 替换，这指定 IP 类型。

dp/c 指定同信息包接收方（从 TCP/IP 报头抽取的）相关的协议端口号。当协议是 ICMP 或者 OSPF，此字段用 **c** 替换，这指定 IP 代码。

- 指定没有信息可用。

r 表示信息包是否有任何本地加入。

- **f** 转发信息包
- **l** 本地信息包
- **o** 外发
- **b** 二者

l 指定特定信息包字节长度。
f 识别信息包是否是分段。
T 表示隧道 ID。
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，它们在遇到问题时提供帮助。建议在第一次配置 IPSec 时设置日志。在确定过滤器及隧道发生了什么时，日志是非常有用的。（对于详细的日志信息，请参阅第 162 页的『记录设施』。）

故障诊断手工隧道错误

错误: 发出 **mktun** 命令导致了以下错误:

```
insert_tun_man4(): write failed : The requested resource is busy.
```

问题: 需要激活的隧道已经激活，或有冲突 SPI 值。

修正: 发出 **rmtun** 命令来取消激活，然后发出 mktun 命令来激活。检查以了解发生故障的隧道的 SPI 值是否与其它任何激活的隧道匹配。每个隧道有它唯一的 SPI 值。

错误: 发出 **mktun** 命令导致了以下错误:

```
Device ipsec_v4 is in Defined status.
```

```
IP 版本的隧道激活没有进行。
```

问题: 没有使 IP 安全性设备可用。

修正: 发出下列命令:

```
mkdev -l ipsec -t 4
```

必须更改 **-t** 选项为 6，如果获取 IP 版本 6 隧道激活的相同错误。设备必须在可用的状态。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** 命令导致了以下错误:

```
Invalid Source IP address
```

问题: 没有输入源地址的有效 IP 地址。

修正: 对于 IP 版本 4 隧道，检查以确认您输入了可用的 IP 版本 4 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 版本 6 隧道，检查以确认您输入了可用的 IP 版本 6 地址。如果输入 `netstat -in` 同时没有 IP 版本 6 地址存在，运行 **/usr/sbin/autoconf6**（接口）获得链接本地自动生成地址（使用 MAC 地址）或使用 **ifconfig** 命令来手工分配地址。

错误: 发出 **gentun** 命令导致了以下错误:

```
Invalid Source IP address
```

问题: 没有输入源地址的有效 IP 地址。

修正: 对于 IP 版本 4 隧道，检查以确认您输入了本地机器的可用的 IP 版本 4 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 版本 6 隧道，检查以确认您输入了可用的 IP 版本 6 地址。如果输入 `netstat -in` 同时没有 IP 版本 6 地址存在，运行 **/usr/sbin/autoconf6**（接口）获得链接本地自动生成地址（使用 MAC 地址）或使用 **ifconfig** 命令来手工分配地址。

错误: 发出 **mktun** 命令导致了以下错误:

```
insert_tun_man4(): write failed : A system call received a parameter that is not valid.
```

问题: 隧道生成于无效的 ESP 和 AH 连接时，或在必要时不使用新的头格式。

修正: 检查以了解有问题的特定隧道使用的是什么认证算法。记住 HMAC_MD5 和 HMAC_SHA 算法需要新建的头格式。新建头格式可以使用 SMIT 快速路径 **ips4_basic** 或者用 **chtun** 命令的 **-z** 参数来更改。也要记住 DES_CBC_4 不能与头格式使用。

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报文。

问题: IP 安全性守护程序不运行。

修正: 查看哪个守护程序通过输入 `ps -ef` 命令运行。以下守护程序与 IP 安全性有关:

- **tmd**
- **isakmpd**
- **cpsd**

cpsd 守护程序是激活的，仅仅在数字证书代码被安装（文件集叫做 **gskit.rte** 或 **gskkm.rte**）同时，已经配置了密钥管理器工具来包含数字证书。

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，然后重新启动它来自动地启动相应的守护程序。

错误: 尝试使用 IP 安全性导致了以下错误:

```
The installed bos.crypto is back level and must be updated.
```

问题: **bos.net.ipsec.*** 文件已经更新为一个新版本，但是没有相应的 **bos.crypto.*** 文件。

修正: 更新 **bos.crypto.*** 文件成为对更新的 **bos.net.ipsec.*** 文件作出相应的版本。

IKE 隧道错误故障诊断

下列各节描述可发生在使用 IKE 隧道过程中的错误。

IKE 隧道进程流

IKE 隧道通过 **ike** 命令或者基于 Web 的系统管理器 VPN 面板与下列守护程序的通信而设置。

表 10. 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	认证代理守护程序

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，这个守护程序自动地启动。否则，它们必须使用基于 Web 的系统管理器启动。

隧道管理器请求 **isakmpd** 命令来启动隧道。如果隧道已经存在或者无效（例如，有无效的远程地址），它报告错误。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。如果协商成功，**ike cmd=list** 命令列出隧道的状态以确定协商是否成功。同时，隧道管理器把事件记录到 **syslog** 里，记录成 **debug**、**event** 和 **information** 级别，它们可以用作监视协商的进度。

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** 守护程序为密钥管理（阶段 1）发给 **isakmpd** 守护程序一个连接请求。
3. **isakmpd** 守护程序回应 SA created 或者报错。
4. **tmd** 守护程序为数据管理隧道（阶段 2）发给 **isakmpd** 守护程序一个连接请求。
5. **isakmpd** 守护程序回应 SA created 或者报错。
6. 隧道参数插入内核隧道高速缓存。
7. 过滤规则添加进内核动态过滤表。

当机器充当响应器时，**isakmpd** 守护程序通报“隧道协商管理器”**tmd** 守护程序，那个隧道已经成功协商，并且一个新的隧道插入了内核。在这样的情况下，此过程从步骤 3 开始，到步骤 7 结束，在此过程中没有 **tmd** 守护程序发出连接请求。

IKE 记录

isakmpd、**tmd** 和 **cpsd** 守护程序把事件记录到 **syslog** 里。对于 **isakmpd** 守护程序，可以使用 **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** 守护程序记录到一个单独的文件里，该文件也被指定在 **/etc/isakmpd.conf** 文件里。

可以为日志记录而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）。

这些选项的语法简单的来说是:

```
log_level
```

isakmpd 守护程序代码或者通过发送建议来创建，或者通过评估建议来响应。如果接受建议，创建安全性的关联并且设置隧道。如果没有接受建议或在协商完成前连接超时，**isakmpd** 守护程序显示错误。在从 **tmd** 的 **syslog** 里的项表示是否协商成功。对于 **syslog** 无效的认证记录会引起错误。为了确定协商失败的精确原因，检查指定在 **/etc/syslog.conf** 文件里的日志文件。

syslog 设施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。下列示例使用 googly 作为机器名称，使用 isakmpd 作为程序名称。

```
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
```

为了提高清晰度，**grep** 命令用来摘录所感兴趣的日志行（比如所有的 **isakmpd** 记录），同时 **cut** 命令可以用从每行中除去前缀。在本节剩余部分的 **isakmpd** 日志示例用相似方法剪切。

解析有效负载记录功能

两端点之间的安全性关联（SA）通过交换 IKE 信息建立。解析有效负载功能以人类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。在 **/etc/isakmpd.conf** 文件中的记录项与下面的相似:

```
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。示例包括“SA 有效负载”、“密钥交换有效负载”、“证书请求有效负载”、“认证有效负载”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
   Proposal Payload:
        Next Payload : 0(NONE), Payload len : 0x28(40 )         Proposal # : 0x1(1), Protocol-ID : 1(ISAKMP )         SPI
        Next Payload : 0(NONE), Payload len : 0x20(32 )         Trans # : 0x1(1), Trans.ID : 1(KEY_IKE )         Attr : 1(
        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 )
        Next Payload : 0(NONE), Payload len : 0x5(5 )         Certificate Encoding Type: 4(X.509 Certificate - Signature)
```

对于每一个有效负载，下一个有效负载字段指向跟着当前的有效负载的有效负载。如果当前的有效负载是 IKE 消息里的最后一个，那么 Next Payload 字段有个零（无）值。

示例中的每个有效负载有属于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”，它们接着显示加密算法、认证模式、散列算法、SA 生命类型和创建人建议的对响应程序的 SA 持续时间。

同时，“SA 有效负载”由一个或更多“建议有效负载”和一个或更多“转换有效负载”组成。“建议有效负载”的 Next Payload 字段，当它是唯一的协议有效负载时，是 0 值，或者有超过一个协议有效负载跟着它时，是 2 值。相似的，“转换有效负载”的 Next Payload，当它是唯一的有效负载时，是 0 值，或者当有超过一个“转换有效负载”跟着时，是 3 值，在下面的例子中显示:

```
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
   Proposal Payload:
        Next Payload : 0(NONE), Payload len : 0x48(72 )         Proposal # : 0x1(1), Protocol-ID : 1(ISAKMP )         SPI
        Next Payload : 3(Transform), Payload len : 0x20(32 )         Trans # : 0x1(1), Trans.ID : 1(KEY_IKE )         Attr
        Next Payload : 0(NONE), Payload len : 0x20(32 )         Trans # : 0x2(2), Trans.ID : 1(KEY_IKE )         Attr : 1(
```

“解析有效负载”日志的“IKE 报文消息头”显示了交换类型（“主方式”或“主动方式”），整个消息的长度，消息的标识等等。

“认证请求有效负载”从响应程序请求了证书。响应程序在不同的报文里发送证书。下列示例显示了“认证有效负载”和“签名有效负载”，它们作为 SA 协商的一部分送到了对等点。认证数据和签名数据用十六进制格式打印。

```
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 - Sign
        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。与以下项相似的项出现在日志文件里:

```
Sep 21 16:02:00 ripple CPS[19950]: Init():LoadCaCerts() failed, rc=-12
```

问题: 认证数据库还没有打开或者还没有查找到。

修正: 确保密钥管理器认证数据库在 **/etc/security** 中出现。下面的文件组成里数据库: **ikekey.crl**, **ikekey.kdb**, **ikekey.rdb**, **ikekey.sth**。

如果仅有 **ikekey.sth** 文件丢失，当密码管理器数据库创建时，没有选择 stash password 选项。必须中断密码来用 IP 安全性启用数字证书。(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认证时给出以下错误:

```
Invalid Base64-encoded data was found
```

问题: 超级数据在认证文件中找到多余数字或其它数据丢失或损坏。

修正: “DER”编码证书应该包含于下面字符串中（在下面显示）。没有其它的字符应该先于或后于 BEGIN 和 END CERTIFICATE 字符串.

```
-----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-----
```

下列选项可以帮助诊断和解决这些问题。

- 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）通过成功解析证书，来检查证书是正确的。

错误: 密钥管理器在接收到个人的证书时，给出下列错误:

```
No request key was found for the certificate
```

问题: 为正在接收的个人“个人认证请求”不存在。

修正: 重新创建“个人认证请求”和请求新的证书。

错误: 当您配置 IKE 隧道时，基于 Web 的系统管理器给出下列错误:

```
Error 171 in the Key Management (Phase 1) Tunnel operation: PUT_IRL_FAILED
```

问题: 该错误的原因是主机识别类型无效，它是在 IKE 对话框（识别表格）中配置。它发生在以下情况，当从下拉列表选择的主机识别类型不能与在 Host Identity 字段里输入的类型匹配时。例如，如果选择主机标识类型 **X500 区别名**，必须在Host Identity 字段里输入一个恰当的格式化区别名。

修正: 确保输入的区别名对于在主机标识的下拉列表里所选的类型是正确的。

错误: IKE 协商失败则在日志文件中出现与下列相似的项:

```
inet_cert_service::channelOpen():clientInitIPC():error,rc =2
(No such file or directory)
```

问题: **cpsd** 没有运行或已死亡。

修正: 用基于 Web 的系统管理器启动 IP 安全性。这个操作也启动相应的守护程序。

错误: IKE 协商失败则在日志文件中出现与下列相似的项:

```
CertRepo::GetCertObj: DN Does Not Match: ("/C=US/O=IBM/CN=ripple.austin.ibm.com")
```

问题: 当在个人证书中定义的 IKE 隧道与 X.500 DN 不能匹配时，输入 X.500 区别名（DN）。

修正: 更改在基于 Web 的系统管理器里的 IKE 隧道定义来匹配在认证中的区别名。

错误: 当定义在基于 Web 的系统管理器 IKE 中的隧道时，数字证书检查包在认证方法表中禁用。

问题: 与该隧道关联的策略没有使用 RSA 签名方式认证。

修正: 相关策略的转换来使用 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。

跟踪设施

跟踪是一种用于跟踪内核事件的调试设施。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 安全性跟踪是在高级 IP 安全性配置菜单中是有效的。通过跟踪设施交易成功的信息包括错误，过滤器，过滤器信息隧道，隧道信息，交易成功/交易不成功，交易成功信息，加密器和加密器信息。通过设计，错误跟踪 hook 提供了最严重的信息。信息跟踪 hook 可以生成严重信息，并对系统性能产生影响。该跟踪将提供线索作为问题是什么。当与服务技术人员对话时，也需要跟踪信息。为了访问跟踪设施，使用 SMIT 快路径 **smit ips4_tracing**（为 IP 版本 4）或 **smit ips6_tracing**（为 IP 版本 6）。

ipsecstat

发出 **ipsecstat** 命令来生成下面样本报告。这个样本报告显示了 IP 安全性设备在可用状态，安装了三个认证算法，以及信息包活动的当前报告。如果故障诊断 IP 安全性流量时，该信息在确定问题存在哪里时是有用的。

```
IP Security Devices:
ipsec_v4 Available
ipsec_v6 Available

Authentication Algorithm:
HMAC_MD5 -- Hashed MAC MD5 Authentication Module
HMAC_SHA -- Hashed MAC SHA Hash Authentication Module
KEYED_MD5 -- Keyed MD5 Hash Authentication Module

Encryption Algorithm:
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 Security Statistics -
Total incoming packets:  1106
Incoming AH packets:326
Incoming ESP packets:  326
Srcrte packets allowed:  0
Total outgoing packets:844
Outgoing AH packets:527
Outgoing ESP packets:  527
```

```
Total incoming packets dropped:  12
  Filter denies on input:  12
  AH did not compute: 0
  ESP did not compute:0
  AH replay violation:0
  ESP replay violation:  0
Total outgoing packets dropped:0
  Filter denies on input:0
Tunnel cache entries added: 7
Tunnel cache entries expired:  0
Tunnel cache entries deleted:  6
```

注: 开始于 AIX 4.3.3, CDMF 支持已除去，因为 DES 现在在世界范围内可用。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	开始网际密钥交换（IKE）协商（AIX 4.3.2 或更新版本）。
ike cmd=remove	取消激活 IKE 隧道（AIX 4.3.2 或更新版本）
ike cmd=list	列表 IKE 隧道（AIX 4.3.2 或更新版本）
ikedb	提供接口给 IKE 隧道数据库（AIX 5.1 或者更新版本）
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	列表隧道定义
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	移动过滤器规则
chfilt	更改过滤器定义
rmfilt	除去过滤器定义
lsfilt	列表过滤器定义
expfilt	导出过滤器定义
impfilt	导入过滤器定义
ipsec_convert	列表 IP 安全性状态
ipsecstat	列表 IP 安全性状态
ipsectrcbuf	列表 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	为 IP 版本 4 和 IP 版本 6 定义 IP 安全性实例。
cfgipsec	配置和装入 **ipsec_v4** 或者 **ipsec_v6**
ucfgipsec	不配置 **ipsec_v4** 或者 **ipsec_v6**

第 12 章 网络信息服务（NIS）和 NIS+ 安全

本章概述了 NIS+ 如何保护其名称空间。本章包含下列的节:

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*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某操作系统环境，您必须提供有效的登录标识和拨号密码。

登录门 要进入某操作系统环境，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、表条目等）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同一的。在这种情况下，您将自动通过门，而不需重新输入您的密码。（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*用来自动传递您的请求通过安全 RPC 门。生成、呈现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 兼容模式下运行的 NIS+ 环境中，安全 RPC 门提供的保护大大减弱，因为人人都有对 NIS+ 全部对象的读取权，以及对适用于它们的条目的修改权，不管他们是否拥有有效的凭证（即，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它们的条目的修改权，在兼容性模式下运行的 NIS+ 网络比在正常模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 182 页的『授权类』。）

要了解如何管理 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由适用的许可权来管辖。

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+ 对象的能力由适用的许可权管辖。该过程称为 *NIS+ 授权*。

了解 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。您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、重新指定组成员以及执行管理发展的网络所需的所有其它日常管理任务。

NIS+ 的安全性特色保护名称空间结构本身以及名称空间中的信息免受未授权的访问。没有这些安全性特色，任何 NIS+ 客户机可以获得、更改甚至销毁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，用户的身份和安全 RPC 密码要进行确认和验证。（您不必输入密码以作为认证过程的一部分。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 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，它们将被放置于四个授权类之一（owner, group, world, nobody）。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，某一类可允许修改 passwd 表中的特定列，但不能读取那一列，或另一类可允许读取一个特定表中的某些条目，但不能读取其它条目。

例如，某 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。（要了解更多关于类的信息，请参阅第 182 页的『授权类』。）

认证和授权防止拥有机器 A 超级权限的某人使用 **su** 命令来采取另一个用户的身份，（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采取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采取从*相同*机器上登录的另一个用户的身份。

下列图形详细解释了这个过程。

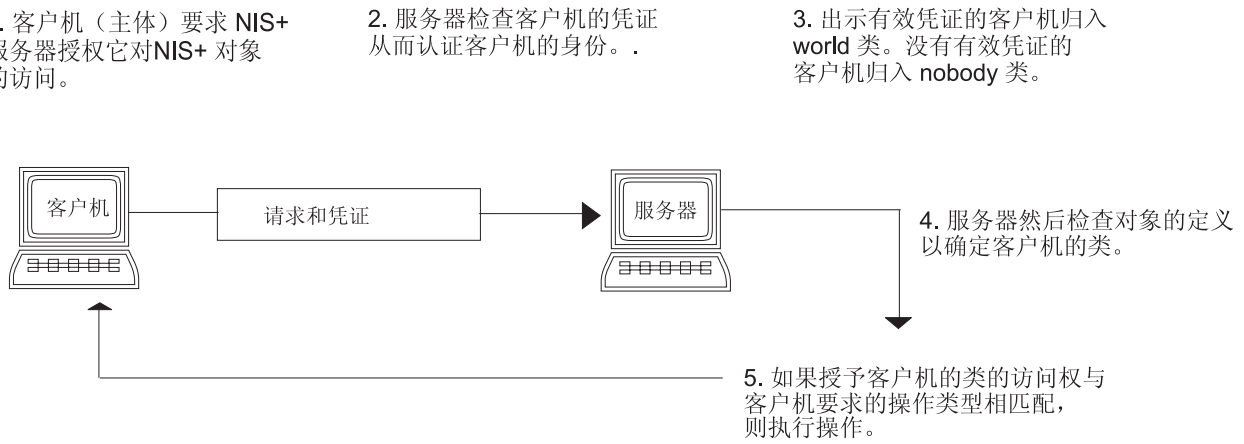


图 13. NIS+ 安全性过程的总结. 这个插图显示了 NIS+ 安全性过程的陈述。

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放置在 world 类中。*
4. *没有有效凭证的客户机被放置在 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+ 主体是那些提交请求 NIS+ 服务的实体（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+ 服务器在一个或两个安全级别上操作。这些级别决定了主体为了请求认证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。提供级别 0 只是为了测试、设置以及调试用途而提供的。下列表格总结了这些安全级别。

注: 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，不论安全级别或凭证状态。

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。在安全级别 0 上运行的 NIS+ 服务器授权任何 NIS+ 主体对域中全部 NIS+ 对象的完全访问权。级别 0 只是为了设置的用途，而管理员只能为了此用途使用该级别。常规用户不应在网络上进行正常操作时，使用级别 0。
1	安全级别 1 使用 AUTH_SYS 安全性。NIS+ 不支持该级别，不应使用该级别。

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访问权。使用无效的 DES 凭证的请求被重新尝试。在获取有效 DES 凭证的尝试接连失败后，使用无效凭证的请求以认证错误的原因失败。（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、密钥错误匹配等原因。）

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 系统的一个实现。

凭证/认证系统防止某人采取另一人的身份。即，它防止拥有一台机器超级权限的某人使用 **su** 命令来采取另一个用户的身份（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采取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采取目前登录在*相同*机器上的另一个用户的身份。

一旦服务器认证了主体，它将检查主体要访问的 NIS+ 对象，以验证有哪些操作授权给那个主体执行。（要了解关于授权的更多信息，请参阅第 182 页的『NIS+ 授权与访问』。）

用户和机器凭证

有两种基本的主体类型，*用户*和*机器*，从而也有两种不同的凭证类型:

用户凭证
当某人作为常规用户登录到 NIS+ 客户机上，对 NIS+ 服务的请求包含这人的用户凭证。

机器凭证
当用户作为 root 用户登录到 NIS+ 客户机上，要求服务的请求使用客户机工作站的凭证。

DES 凭证相对本地凭证

NIS+ 主体可以有两种凭证类型: DES 和本地凭证。

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。（请注意，使用 DES 凭证只是进行认证的方法之一。请不要将 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 部分对此进行了解释。

- 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和他们的包含其主域名的 NIS+ 主体名称之间的映射。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。

当用户登录到远程域上，那些请求使用用户的指回其主域的本地凭证。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，尽管该用户的 DES 凭证信息未存储在那个域中。下列图形说明了这个概念。

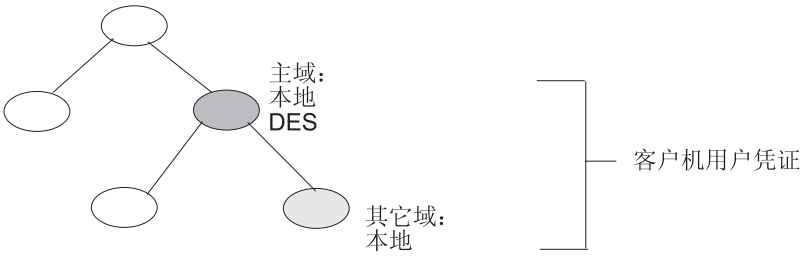


图 14. 凭证和域. 这个插图显示一个域的层次结构。用户的主域有本地和 DES 凭证。子域只有本地凭证。主域和子域标识为客户机用户凭证。

凭证和域: 本地凭证信息可存储于任何域。要登录到远程域并被认证，客户机用户*必须*在远程域的 cred 表中有一个本地凭证。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 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）尝试作为 root 访问机器 B，这将与机器 B 现有的 root 用户（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+ 主体具有的对每个 NIS+ 对象与服务的访问权。

一旦认证了提出 NIS+ 请求的主体，NIS+ 将此主体放入授权类中。在类的基础上分配访问权（许可权），这些访问权指定主体用给定的 NIS+ 对象进行哪项操作。换句话说，当不同的类有不同的权限时，一个授权类有一定的访问权。

授权类 有四个授权类: 所有者、组、世界和无人。（详细信息请参阅『授权类』 ）。

访问权 有四类访问权（许可权）: 创建、破坏、修改及读取。（详细信息请参阅第 184 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。而向四类主体授予访问权:

Owner
恰好是对象所有者的主体获取向所有者类授予的权限。

Group 每个 NIS+ 对象都有一个与其关联的组。由 NIS+ 管理器指定对象组的成员。属于对象组类的主体获取授予组类的权限。（在此上下文中，*组*指 NIS+ 组，而非操作系统或网络组。关于 NIS+ 组的描述，请参阅第 183 页的『组类』）。

World 世界类包含服务器可认证的全部 NIS+ 主体。（即，既不在所有者类又不在组类的每个认证主体。）

Nobody
所有属于无人类的主体，包括那些未认证的主体。

请看下面关于类的图解。

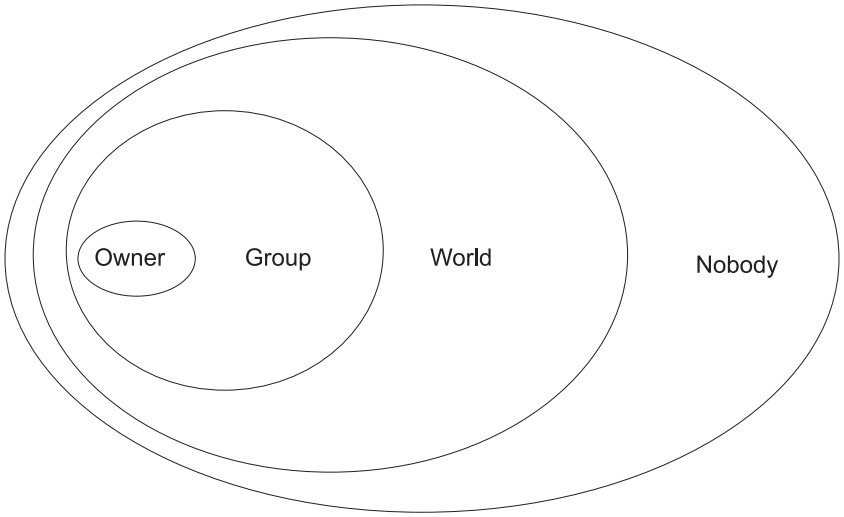


图 15. 授权类. 此图显示一系列表示授权类之间关系的椭圆。最小的椭圆是所有者，外面包围着较大的标为组的椭圆，再外面包围着标为世界的椭圆，最外面包围着标为无人的椭圆。

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什么访问权。

对象可向这些类中的每一类授予任意组合的访问权限。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，附加权限也是如此。

例如，对象向无人和世界类授予读取访问权，向组类授予读取和修改访问权，并向所有者类授予读取、修改、创建及破坏访问权。

下面详细描述这四个授权类。

所有者类

此所有者是*单一* NIS+ 主体。

向 NIS+ 对象提出访问请求的主体，必须在授于所有者访问权限前得到认证（出示 DES 有效凭证）。

缺省情况下，对象的所有者是创建此对象主体。但是，对象的所有者可通过两种不同的方法放弃对另一个主体的所有权:

- 此主体指定创建对象时的不同所有者（请参阅 *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide* 中用命令指定访问权限一节）。
- 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* 中更改对象与条目的所有权一节）。

一旦主体放弃所有权，就放弃了对对象的全部所有权的访问权，而只保留对象分配给组、世界或无人的权限。

组类

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授于组访问权限前得到认证（出示 DES 有效凭证），并属于此组。

NIS+ 组是 NIS+ 主体的集合，以便于访问名称空间。向 NIS+ 组授于的访问权用于所有主体（它们是此组中的成员）。（但是，对象的所有者不必属于此对象组。）

创建对象时，创建程序可选择缺省组。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* 中『管理 NIS+ 组』一节中。

世界类

世界类包含 NIS+ 认证的 NIS+ 全部主体（即所有者及组类的全部成员），还有出示 DES 有效凭证的所有其它主体。

授予世界类的访问权应用于所有认证主体。

无人类

无人类包含全部主体，甚至那些没有 DES 有效凭证的主体。

授权类及 NIS+ 对象分层

NIS+ 安全性将授权类单独应用于对象分层。目录对象是缺省分层的顶层，然后是组或表对象，然后是列，然后是条目。下列定义提供关于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
组包含各个条目及其它组。表包含列及各个条目。

列级 每个表有一或多列。

条目（行）级
每组或表都有一或多个条目。

四种授权类用于每一级。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。在表中，列或条目可有其自己的所有者或组，它们总体上可不同于表或目录对象的所有者和组。

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，但所有操作必为四类访问权之一：读取、修改、创建及破坏。

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 具有创建高级对象权限的主体可在此级别内创建新对象。如果您有创建 NIS+ 目录对象的权限，您可在此目录内创建新表。如果您有创建 NIS+ 表的权限，您可在此表内创建新列及新条目。

NIS+ 客户与 NIS+ 服务器的每次通信是请求在指定的 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目录的父对象的**修改**访问。

这些权限合理地向下发展，从目录到表、到表列及条目级。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，您可给您自己分配创建表的权限，此权限允许您在表中创建新条目。如果您在表中创建新条目，您就成为这些条目的缺省所有者。作为表所有者，您也可对其它类授于表级创建权。例如，您可给予表的组类表级创建权。在这种情况下，表的组中任一成员都可在此表中创建新条目。组的创建新表条目的各成员成为此条目的缺省所有者。

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。任何对对象有管理权限的人—即，创建、破坏权限以及对某些对象的修改权限—都被认为是那个对象的 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。如果创建者将管理权限限制为只有对象所有者（初始创建者）所有，则只有所有者有对那个对象的管理权。另一方面，如果创建者将管理授权授权给对象的组，则组中的每个人拥有对那个对象的管理权。

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，将严重影响 NIS+ 安全性，使该安全性无效。这样，如果您将管理权限授权给 World 类或 nobody 类，您实际上是在破坏 NIS+ 安全性的用途。

NIS+ 安全性参考大全

请使用下列命令来管理密码、凭证和密钥（要了解更多信息，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** 文件中主体的条目。

keylogin
用 **keyserv** 解密并存储主体的秘密密钥。

keylogout
从 **keyserv** 中删除存储的秘密密钥。

keyserv
使服务器能够存储专用的密钥。

newkey
在公开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开密钥。

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，网络文件系统（NFS）提供一种以 message-by-message 为基础的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:

- 保密
- 第 189 页的『NFS 认证』
- 第 191 页的『为 DES 认证命名网络实体』
- 第 191 页的『/etc/publickey 文件』
- 第 191 页的『公开密钥系统的引导注意事项』
- 第 191 页的『安全 NFS 的性能注意事项』
- 第 192 页的『管理安全 NFS 的检查表』
- 第 192 页的『配置安全 NFS』
- 第 193 页的『使用安全 NFS 导出文件系统』
- 第 194 页的『使用安全 NFS 安装文件系统』.

保密

历史上，不同的人群都在寻找一种通信方法，使得只有发送方和接收方知道某个消息的内容。为了取得这种保密性，发送方和接收方使用一种*密码*，一种将*明文*消息转换为*密文*，然后再转换回来的方案。*加密*是将明文转换为密文的过程，而*解密*是将密文转换为明文的过程。

最早的密码之一，*Caesar 密码*，归功于 Julius Caesar。在这种密码中，由一个字母替代另一个字母。例如，‘A’ 变成 ‘C’，‘B’ 变成 ‘D’，...，‘Y’ 变成 ‘A’，而 ‘Z’ 变成 ‘B’。这样，Caesar 密码将短语 **ATTACK AT DAWN** 加密成为 **CVVCEM CV FCYP**。

如果迦太基人可以*用密码分析法破译* Caesar 密码，罗马*译解密码者*就必须发明一种全新的密码。由于密码的开发是费时费力的过程，罗马人也许可使用一种密码*密钥*来更充分地利用他们的密码。例如，罗马人可以指定一个密钥 *K*，K 表示移动一个字母的位置数，而不是指定以字母对字母的替换方法。即，如果 K = 2，则 ‘A’ 变成 ‘C’。如果 K = 4，则 ‘A’ 变成 ‘E’，以此类推。使用这种方案，如果迦太基人破解了密码，罗马人要做的只是更改密钥。当然，迦太基人也许会发现意大利人用的是何种算法，而费劲地尝试从 1 到 26 的每个 K 值。如果迦太基人有计算机，他们的任务只是一个小小的编程练习。

数据加密标准

计算机可以是闯入者试图破解密码的强大工具，现代密码的设计正是为了解决这个问题。1977 年，美国政府采用一种密码作为它的数据加密标准。这种密码在业界被广泛使用。DES 是一种高度复杂的算法。它使用一个 56 位的密钥，将 64 位的明文块转换为 64 位的密文块。由于算法的复杂和密码密钥的大小，DES 本质上是不可破解的。例如，如果闯入者有一台计算机，它可以每微秒一个密钥的速率计算 DES 的算法，则这台计算机需要超过两千年的时间来尝试每个可能的密钥。

公开密钥加密法

任何加密算法的重大弱点是它所使用的密钥。如果发送方和接收方要使用密码来进行安全通信，发送方和接收方双方都必须知道密钥。他们必须通过一个分开的通信连接（其本身必须是安全的）或亲自地来同意一个密钥。

为了解决这个问题，两位研究人员（Diffie 和 Hellman）开发了一种方法，使发送方和接收方可以公开交换密钥，而不需要威胁到他们通信的安全性。他们的方法有三个要求:

- 译码（编码（明文，E），D）= 明文

  这里，E 是密钥（公开的），D 是解密钥（只有接收方知道）。

  即，编码和译码功能是互逆的。因此，如果您取得由“编码（明文，E）”返回的加密的文本字符串，并用它和密钥 D 进行译码功能，则译码将返回原始的明文。
- 闯入者无法从“编码（）”推导出“译码（）”。
- “编码（）”是牢不可破的。

下列概要描述发送方如何发送秘密消息给接收方。

1. 发送方获得接收方公共密钥。
2. 发送方通过计算以下结果将明文消息转换为密文:

   密文 = 编码（明文，E）
3. 发送方将密文消息发送给接收方。
4. 接收方接收到密文消息，然后通过计算以下结果将它转换为明文:

   明文 = 译码（密文，D）

即使闯入者拦截了消息，他也无法译解它，因为闯入者没有解密钥。（正因如此，发送方也无法译解密文消息。）

认证

保密的一个主要应用是*认证*。认证的一个通常方法（是标准 UNIX 认证方法）使用密码。当用户要登录时，操作系统要求用户给出一个密码，这个密码只有操作系统和用户知道。如果用户给出了正确的密码，则操作系统认为该用户就是他所自称的那人。请注意，这个方法要求操作系统将用户密码以加密的形式存储在系统的一个文件中。这意味着两个不同的实体知道同一个密码。

公开密钥加密法提供了一种不同于密码认证的方法。假设发送方要发送消息，接收方想要确认消息是从发送方来的，而不是假装为发送方的闯入者。认证过程按下列方式进行:

1. 首先，发送方使用接收方的公开密钥将“请求发送”消息编码，然后发送这个请求。
2. 接收方接收到“请求发送”消息，并使用接收方的私钥译解它。
3. 接收方使用发送方的公开密钥将一个“标记”消息编码，然后发送该标记。
4. 发送方接收到标记，并使用发送方的私钥将它解译。当发送方发送消息给接收方时，发送方会以该标记为每个消息的开头，表明发送方是真正的发送方。如果闯入者试图以发送方的名义发送消息，接收方将拒绝消息，因为闯入者不知道标记是什么。

请注意，不像密码认证，接收方可以在不知道发送方的私钥情况下，认证发送方。要了解更多关于认证系统的信息，请参阅 *AIX 5L Version 5.2 Communications Programming Concepts* 中的 Understanding RPC Authentication。

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。这个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 可以认证 NFS 客户机和服务器之间交换的每个单一的 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，使用标准 UNIX 认证导出文件系统。要利用这个额外的安全级别，您可以在导出文件系统时指定 **secure** 选项。

安全 NFS 的公开密钥加密法

用户的公开密钥和秘密密钥都以其网络名称存储和索引在 **publickey.byname** 映射中。秘密密钥使用用户登录密码进行 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。用户不知道他们的公开和秘密的密钥，因为 **yppasswd** 命令除了更改登录密码，自动生成公开和秘密的密钥。

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**，请参阅 *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide*。在 NIS 中，**keyserv** 执行下列三个公开密钥子例程:

- **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；它通常是由 **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。密钥服务器查寻服务器公开密钥，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。

隐藏在这些子例程调用中的是调用程序的名称，该名称必须通过某种方法被认证。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。密钥服务器通过将秘密密钥与用户标识（UID）存储，并只同意对本地根进程的请求，来解决这个问题。客户机进程然后执行 root 用户拥有的 **setuid** 子例程，该子例程以客户机名义提出请求，告诉密钥服务器这个客户机的真正 UID。

认证要求

安全 NFS 认证是基于发送方加密当前时间的能力，接收方可以再解密这个当前时间，并与自己的时钟检查对照。这个过程有两个要求:

- 双方必须同意当前的时间。
- 发送方和接收方必须使用相同的 DES 密钥。

同意当前时间

如果网络使用时间同步，则 **timed** 守护程序保持客户机与服务器时钟同步。如果不是，则客户机根据服务器时钟计算正确的时间戳记。要做到这点，客户机在开始 RPC 会话之前确定服务器时间，再计算自己时钟与服务器时钟之间的时差。客户机然后相应调整自己的时间戳记。如果在 RPC 会话过程中，客户机与服务器的时钟不同步到一种程度，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 密钥。对于任何客户机 A 与服务器 B，有一个只有 A 和 B 可以推导出的密钥。这个密钥称为*公共密钥（common key）*。客户机通过计算下列公式得出公共密钥:

$$K_{AB} = PK_B{}^{SK}A$$

这里，*K* 代表*公共密钥*，*PK* 代表*公开密钥（Public Key）*，而 *SK* 代表*秘密密钥（Secret Key）*，每个密钥都是一个 128 位数字。服务器通过计算下列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这个公共密钥，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。

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，用作加密时间戳记。这个密钥称为*对话密钥（conversation key, CK）*。客户机使用 DES 公共密钥加密对话密钥（在认证要求中有叙述）并在第一个 RPC 事务中将它发送至服务器。下图说明了这个过程:

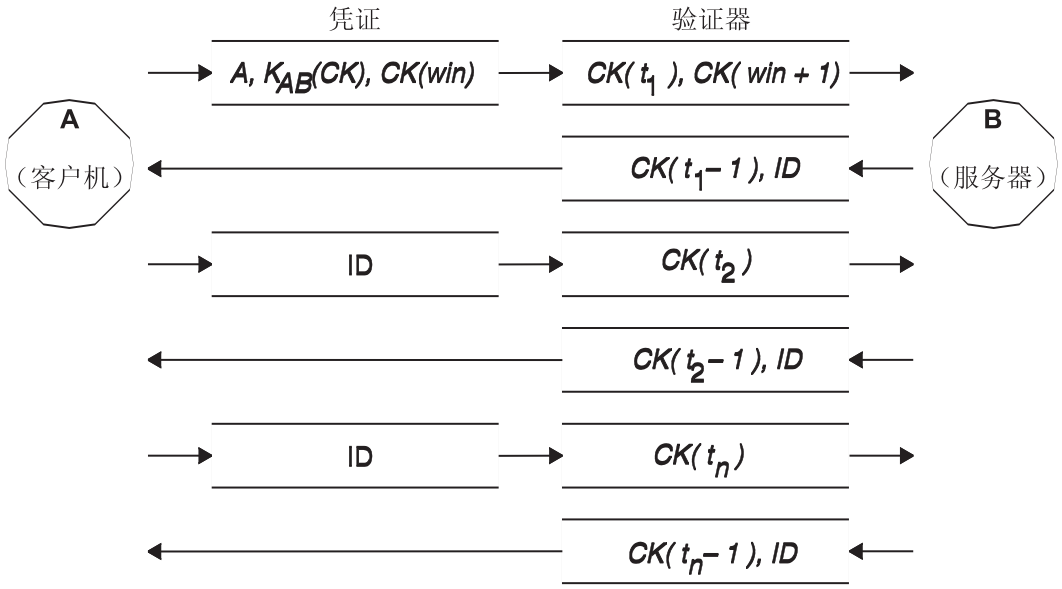


图 16. 认证过程. 这张图通过围起的文字的描述说明了认证过程。

这张图显示客户机 A 连接在服务器 B 上。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*（window，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。这个窗口验证符使猜测正确的凭证困难很多，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（按时间顺序排列）大于上次见到的时间戳记，因此任何重演的事务一定会被拒绝。服务器在验证符中返回给客户机一个凭证表中的索引标识，加上客户机时间戳记（由 *CK* 加密）减去一。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。从时间戳记中减去一是为了确保它无效，不能作为客户机验证符被重用。第一个 RPC 事务之后，客户机仅向服务器发送它的标识和一个加密的时间戳记，服务器将由 *CK* 加密的时间戳记减一发还给客户机，。

为 DES 认证命名网络实体

DES 认证使用网络名称进行命名。下列段落描述了 NIS 如何处理 DES 认证。要了解 NIS+ 如何处理 DES 认证的有关信息，请参阅 *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide*。

一个*网络名称*是要认证的一串可打印字符。公共和秘密密钥以每个网络名称（per-net-name），而不是每个用户名称（per-user-name）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。通过连接 NIS 的操作系统和用户标识以及因特网域名，指定网络名称。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。

网络名称被赋予用户，也赋予机器。机器网络名称的形成很像用户名称的形成。例如，`eng.ibm.com` 域中名称为 `hal` 的机器，它的网络名称是 `unix.hal@eng.ibm.com`。正确的机器认证对于需要对其网络上的主目录有完全访问权的无盘机器是非常重要的。

要认证任何远程域的用户，请在两个 NIS 数据库中为他们设立条目。一个是为他们的公共和秘密密钥设立的条目；另一个是为他们的本地 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系统，例如 NFS 和远程登录。

/etc/publickey 文件

/etc/publickey 文件包含名称和公开密钥，NIS 和 NIS+ 使用它们来创建 **publickey** 映射。**publickey** 映射是用来保护联网。文件中的每个条目由一个网络用户名（表示用户名或主机名）、接着是用户公开密钥（以十六进制符号表示）、冒号以及用户加密的秘密密钥（也是以十六进制符号表示）组成。缺省情况下，**/etc/publickey** 文件中的唯一用户是 nobody 用户。

请不要使用文本编辑器更改 **/etc/publickey** 文件，因为文件中包含密钥。要更改 **/etc/publickey** 文件，请使用 **chkey** 或 **newkey** 命令。

公开密钥系统的引导注意事项

当掉电故障之后重新启动机器，所有存储的秘密密钥都将丢失，也没有进程可以访问安全网络服务系统，例如安装 NFS。如果有人可以输入密码来解密 root 用户的秘密密钥，root 进程则可继续。解决方案就是将 root 用户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` 访问任何网络服务系统。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:

- 首先，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这个操作。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 事务都要求下列 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。

由于系统性能会因为安全 NFS 而减弱，请在增加安全性获得的收益以及系统性能的要求之间进行权衡。

管理安全 NFS 的检查表

请使用下列检查表以帮助确保安全 NFS 恰当运行:

- 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。如果使用名称服务器作为主机名解决方案，请确认由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，文件访问权可能会被不正确地确定。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+ 不知道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，请只在网络负载较轻时使用这些命令。
- 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。这样做使密码和私钥保持同步。
- 由于 **login** 命令不从 **keyserv** 守护程序的 **publickey** 映射中找回密钥，用户必须执行 **keylogin** 命令。您也许想将 **keylogin** 命令放在每个用户 **profile** 文件中，从而以在登录时自动执行该命令。请注意，**keylogin** 命令要求用户重新输入他们的密码。
- 当您使用 **newkey -h** 或 **chkey** 命令为每个主机的 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，它都会读取这个文件。
- 请定期验证 **yppasswdd** 和 **ypupdated** 守护程序在 NIS 主控服务器上运行。这些守护程序对维护 **publickey** 映射是很必要的。
- 请定期验证 **keyserv** 守护程序在使用安全 NFS 的所有机器上运行。

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下列步骤。要了解有关在 NIS+ 上使用 NFS，请参阅 *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide*。

1. 在 NIS 主控服务器上，使用 **newkey** 命令为 NIS **/etc/publickey** 文件中的每个用户创建一个条目。这个命令有下列选项。
   - 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，用户也可以使用 **chkey** 或 **newkey** 命令建立他们自己的公开密钥。

2. 请根据 *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** 文件中下列节的注解:

```
#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，请使用 **startsrc** 命令来启动 **keyserv** 守护程序。

使用安全 NFS 导出文件系统

您可以使用基于 Web 的系统管理器 网络应用程序来导出安全 NFS，或使用下列步骤之一。

- 要使用 SMIT 导出安全 NFS，请执行以下操作:
  1. 发出 **lssrc -g nfs** 命令以验证 NFS 已在运行。输出应表示 **nfsd** 和 **rpc.mountd** 守护程序是活动的。
  2. 验证 **publickey** 映射存在，以及 **keyserv** 守护程序正在运行。要了解更多，请参阅第 192 页的『配置安全 NFS』。
  3. 运行 **smit mknfsexp** 快速路径。
  4. 指定要导出目录的路径名的适当值、导出目录的方式、现在导出目录、系统重新启动或同时指定两个字段。Use SECURE 选项字段指定 **yes**。
  5. 指定其它可选的特征，或不指定剩下字段，从而接受它们的缺省值。
  6. 退出 SMIT。如果 **/etc/exports** 文件不存在，则创建它。
  7. 对于您想要导出的每个目录，重复步骤 3 到 6。
- 要使用文本编辑器来导出安全 NFS 文件系统，请请执行以下操作:
  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，为每个要导出的目录创建一个条目。从左页边距开始，列出要导出的每个目录。目录不可以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 **secure** 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
```

-a 选项告诉 **exportfs** 命令将 **/etc/exports** 文件中的所有信息发送到内核。

- 要将一个 NFS 文件系统临时导出（即，不更改 **/etc/exports** 文件）：

  请输入:

  ```
  exportfs -i -o secure /dirname
  ```

  这里，*dirname* 是您要导出的文件系统名称。**exportfs -i** 命令指定，对于指定的目录 **/etc/exports** 文件不被检查，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

要直接安装安全 NFS 目录，请执行以下操作:

1. 发出以下命令来验证 NFS 服务器已导出目录:

   ```
   showmount -e ServerName
   ```

   这里，*ServerName* 是 NFS 服务器名称。这个命令显示当前从 NFS 服务器中导出的目录名称。如果您要安装的目录不在列表中，请将目录从服务器中导出。
2. 使用 **mkdir** 命令建立本地安装点。要使 NFS 成功完成安装，必须存在一个作为 NFS 安装的安装点（或占位符）的目录。这个目录必须是空的。可以像创建任何其它目录一样创建这个安装点，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 192 页的『配置安全 NFS』。
4. 请输入:

   ```
   mount -o secure ServerName:/remote/directory /local/directory
   ```

   这里，*ServerName* 是 NFS 服务器名称，*/remote/directory* 是您要安装的 NFS 服务器上的目录，而 */local/directory* 是 NFS 客户机上的安装点。

   请注意: 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一组复杂的系统和应用程序组成的，因而必须管理多个用户注册表。迅速处理多个用户注册表成为一个重大的管理问题，它影响到用户、管理员和应用开发人员。企业身份映射（EIM）使得管理员和应用开发人员可以很容易的处理该问题。

本章描述了这个问题，概述了当前工业途径，并解释了 EIM 方法。

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，通过不同的用户注册表，每个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，管理员经常必须使这些身份和密码同步。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来诊断失败的登录尝试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多种多样的应用程序。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。

当前途径

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，但它们都提供了不完全的解决方案。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，管理员对于个别的资源必须管理多个安全机制，因而增加了管理开销，并潜在的增加了安全性泄漏的可能性。当多个机制支持一个单独的资源时，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，当用户适当的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及其有关的安全性语义上投入了太多资金以使用这类实际解决方案。创建另一个用户注册表及有关的安全性语义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点登录的方法。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，这种方法有几个弱点:

- 它只解决用户面临的一个问题。尽管它允许用户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。密码应该从不保存在明文文件或者容易受任何人（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，他们提供各种多层应用程序。他们必须仍然为用户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）以及企业内部代表他们的许多身份。此外，EIM 提供一套 API，允许应用程序查询关于这些关系。

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 为企业提供通用的身份映射功能。

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，管理员可以映射一个 SAP 身份（或者更好的，SAP 可以自映射）来访问 SAP 资源。

身份映射要求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 EIM 注册表定义来描述他们企业中现有的用户注册表。
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。

不需要更改现有的注册表代码。不需要映射用户注册表中所有的用户。EIM 允许一对多映射（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 也允许多对一映射（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 引入的唯一的新建数据是关系信息。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。

关于企业身份映射的更多信息，请参考以下 Web 站点:

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

第 3 部分 附录

附录 A. 安全性检查表

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的检查表。尽管这份列表不是一份完整的安全性检查表，它可作为为您的环境构建一份安全性检查表的基础。

1. 当安装新建系统时，从安全基本介质来安装 AIX。在安装时执行下列步骤:
   - 不要在服务器上安装桌面软件，比如 CDE、GNOME 或 KDE。
   - 安装要求的安全性修正和任何推荐的维护包修正。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）。
   - 在初始安装后备份系统，并将系统备份存储在安全场所。
2. 为受限制的文件和目录建立访问控制表。
3. 禁用不必要的用户帐户和系统帐户，比如 daemon、bin、sys、adm、lp、uucp。不推荐删除帐户，因为这也将删除帐户信息，比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。如果使用先前删除了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恢复了的系统的意外的访问权。
4. 定期检查 **/etc/inetd.conf**、**/etc/inittab**、**/etc/rc.nfs** 和 **/etc/rc.tcpip** 文件，并除去全部不必要的守护程序和服务。
5. 验证下列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
```

6. 使 root 帐户不能远程登录。root 帐户应只能从系统控制台登录。
7. 启用系统审计过程。要了解更多信息，请参阅第 45 页的第 3 章，『审计过程』。
8. 启用登录控制策略。要了解更多信息，请参阅第 17 页的『登录控制』。
9. 禁用运行 **xhost** 命令的用户许可权。要了解更多信息，请参阅第 20 页的『管理 X11 和 CDE 注意事项』。
10. 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 27 页的『PATH 环境变量』。
11. 禁用 telnet、rlogin 和 rsh。要了解更多信息，请参阅第 113 页的第 9 章，『TCP/IP 安全性』。
12. 建立用户帐户控制。要了解更多信息，请参阅第 26 页的『用户帐户控制』。
13. 执行严格的密码策略。要了解更多信息，请参阅第 37 页的『密码』。
14. 为用户帐户建立磁盘限额。要了解更多信息，请参阅第 42 页的『从超限额条件中恢复』。
15. 只允许管理帐户使用 **su** 命令。监视 **/var/adm/sulog** 文件中 **su** 命令的记录。
16. 使用 X 视窗时屏幕锁定。
17. 限定对 **cron** 和 **at** 命令的访问，只给那些需要访问它们的帐户访问权。
18. 给 **ls** 命令起别名，从而显示隐藏在一个文件名中的文件和字符。
19. 给 **rm** 命令起别名，以避免意外从系统中删除文件。
20. 禁用不必要的网络服务。要了解更多信息，请参阅第 121 页的第 10 章，『网络服务』。
21. 执行定期的系统备份并验证备份的完整性。
22. 订阅与安全性有关的电子邮件分发表。

附录 B. 安全性参考资料

本附录提供多方面的与安全性有关的参考资料信息。Web 站点可以在未通知情况下无效或过时。要了解更多关于 Web 站点的 IBM 策略和非 IBM 参考资料的信息，请参阅第 215 页的附录 E, 『声明』。

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, at Carnegie Mellon University): 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/

安全性邮件列表

CERT: http://www.cert.org/contact_cert/certmaillist.html

IBM Software Technical Mailings: http://techsupport.services.ibm.com/server/listserv

comp.security.unix: news:comp.security.unix

安全性网上参考资料

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/en_US/infocenter/base

附录 C. 常见 AIX 系统服务总结

下表列出在 AIX 内的较常见的系统服务。使用此表来认识保护您系统的起点。

在继续进行保护系统之前，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	已启动	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）与系统远程引导是必需的 • 与 tftp 并行工作 • 在大部分情况下禁用
inetd/chargen	inetd	/etc/inetd.conf	字符生成器（只测试）	• 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 用户运行，因此涉及安全性 • 除非用 CDE 请求此服务，否则禁用 • 后室数据库服务器上禁用
inetd/comsat	inetd	/etc/inetd.conf	通知有电子邮件进入	• 以 root 用户运行，因此涉及安全性 • 很少需要的 • 禁用的
inetd/daytime	inetd	/etc/inetd.conf	过时时间服务（只测试）	• 以 root 用户运行 • TCP 与 UDP 服务可用 • 为拒绝服务 PING 攻击提供机会 • 服务是过时的并只供测试使用 • 禁用的
inetd/discard	inetd	/etc/inetd.conf	/dev/null service（只测试）	• 可用作 TCP 与 UDP 服务 • 拒绝服务攻击使用 • 服务是过时的并只供测试使用 • 禁用
inetd/dtspc	inetd	/etc/inetd.conf	CDE 子过程控制	• 此服务通过 **inetd** 守护进程响应 CDE 客户机请求进程在守护进程的主机上启动来自动地启动。这使它易受攻击 • 在没有 CDE 的后室服务器上禁用 • 没有此服务 CDE 可能会起作用 • 除非绝对需要，否则禁用

服务	守护程序	已启动	功能	注释
inetd/echo	inetd	etc/inetd.conf	回传服务（只测试）	• 作为 TCP 与 UDP 服务可用的 • 可用于拒绝服务或 Smurf 攻击 • 用于回送信号给其他人来穿过防火墙或开始数据传输 • 禁用
inetd/exec	inetd	/etc/inetd.conf	远程执行服务	• 以 root 用户身份运行，因此是危险的 • 要求输入无保护传递的用户标识或口令 • 此服务是非常容易遭到窥探的 • 禁用
inetd/finger	inetd	/etc/inetd.conf	对用户取数的远程用户信息服务命令（程序）	• 以 root 用户身份运行，因此是危险的 • 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，因此易受窥探 • 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，因此是危险的 • 使用安全 shell 代替此服务
inetd/netstat	inetd	/etc/inetd.conf	报告当前网络状态	• 如在您的系统上运行，能潜在地把网络信息给黑客 • 禁用

服务	守护程序	已启动	功能	注释
inetd/ntalk	inetd	/etc/inetd.conf	允许用户相互交谈	• 以 root 用户身份运行，因此是危险的 • 在产品或后室服务器不是必需的 • 除非绝对需要，否则禁用
inetd/pcnfsd	inetd	/etc/inetd.conf	PC 机 NFS 文件服务	• 如果不是当前在使用，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且您有正使用只支持 POP3 的应用程序的客户机，才必需 • 如果您的客户机使用 IMAP，使用那个替代，或使用 POP3 服务 此服务有安全套接字层（SSL）通道 • 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，因此是危险的 • 用 **on** 命令窥视 • 禁用的服务 • 使用 **rsh** 与 **rshd** 代替
inetd/quotad	inetd	/etc/inetd.conf	文件限额的报告（对于 NFS 客户机）	• 如果您正运行 NFS 文件服务，才需要 • 禁用此服务，除非要求对 **quota** 命令提供回答 • 如果需要使用此服务，保存所有的补丁和最新的此服务的修正包
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 并禁用此服务 • 请求使用 **rup** 命令
inetd/rusersd	inetd	/etc/inetd.conf	用户的登录信息	• 这不是基本的服务。禁用 • 以 root 用户身份运行，因此是危险的 • 给出您的系统上当前用户的列表并用 **rusers** 窥视

服务	守护程序	已启动	功能	注释
inetd/rwalld	inetd	/etc/inetd.conf	写给所有用户	• 以 root 用户身份运行，因此是危险的 • 如果系统有交互式用户，可能需要保持此服务 • 如系统为产品或数据库服务器，这是不需要的 • 禁用
inetd/shell	inetd	/etc/inetd.conf	rsh 服务	• 如可能,禁用此服务。使用安全 shell 替代 • 如果必须使用此服务，使用 TCP Wrapper 来停止电子欺骗与限制暴露 • 对于 **xhier** 必需
inetd/sprayd	inetd	/etc/inetd.conf	RPC 喷射测试	• 以 root 用户身份运行，因此是危险的 • 可能对于 NFS 网络问题的诊断是必需的 • 如果不在运行 NFS，则禁用
inetd/systat	inetd	/etc/inted.conf	“ps -ef” 状态报告	• 允许远程站点来了解您系统上的进程状态 • 此服务缺省情况下禁用。必须周期性地检查来确保未启用此服务
inetd/talk	inetd	/etc/inetd.conf	在网上建立两个用户间的分区屏幕	• 不是必需的服务 • 用 **talk** 命令使用 • 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” 在网络上建立两个用户间的分区屏幕	• 非必需的服务 • 用 **talk** 命令使用 • 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，但未加保护地传递密码和标识 • 如果可能，禁用此服务并对远程访问使用安全 shell 替代
inetd/tftp	inetd	/etc/inetd.conf	琐碎的文件传送	• 在端口 69 提供 UDP 服务 • 以 root 用户身份运行，且可能是危及安全的 • 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	已启动	功能	注释
inetd/time	inetd	/etc/inetd.conf	废弃的时间服务	• 由 **rdate** 命令使用的 **inetd** 的内建功能。 • 作为 TCP 与 UDP 服务可用 • 有时在引导时用于同步时钟 • 此服务是过时的。使用 **ntpdate** 代替 • 只在您已用此禁用的服务测试系统（引导／重新引导）且观察无问题后，禁用此服务
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，且可能是危及安全的 • 申明为 CDE 需要的服务，但 CDE 没有它也能工作 • 不应该在后室服务器或安全性涉及的任何系统上运行
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。避免把它用于后室系统
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 • 关于 **inittab/dt** 是一样的
inittab/httpdlite	init	/etc/inittab	用于 **docsearch** 命令的 Web 服务器	• 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	• 对开发机器启用 • 对生产机器禁用 • 对有许可证要求的后室数据库机器启用 • 为编译器、数据库软件或任何其它的得到许可的产品提供支持
inittab/imnss	init	/etc/inittab	用于“docsearch”的搜索引擎	• 用于搜索引擎的缺省 Web 服务器的部分 • 除非您的机器是文档服务器，否则禁用

服务	守护程序	已启动	功能	注释
inittab/imqss	init	/etc/inittab	用于″docsearch″的搜索引擎	• 用于搜索引擎的缺省 Web 服务器的部分 • 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 • 能禁用此服务并仍发送作业到打印服务器 • 在确认打印不受影响后，禁用此服务
inittab/nfs	init	/etc/inittab	网络文件系统／网信息服务	• NFS 与 NIS 服务基于哪个建于 UDP／RPC • 认证是最小的 • 后室数据库服务器应该对此无需要 • 对后室机器禁用此项
inittab/piobe	init	/etc/inittab	打印机 I/O 后端（用于打印）	• 处理该调度、假脱机与打印由 **qdaemon** 提交的作业 • 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	队列守护程序（用于打印）	• 提交打印作业到 **piobe** 守护程序 • 如果不在从系统打印，那么禁用
inittab/uprintfd	init	/etc/inittab	内核消息	• 通常非必需 • 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、后室数据库与开发的机器禁用此服务 • 对工作站启用此服务
inittab/xdm	init	/etc/inittab	传统的 X11 显示管理	• 不要在后室生产或数据库服务器上运行 • 不要在开发系统上运行除非 X11 显示管理是必要的 • 如果图形是需要的可接受在工作站上运行
rc.nfs/automountd		/etc/rc.nfs	自动文件系统	• 如果使用 NFS，为工作站启用此服务 • 不要把自动安装器用于开发或后室服务器
rc.nfs/biod		/etc/rc.nfs	块 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** 禁用此服务

服务	守护程序	已启动	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+ 重要 • 如果您不在使用 NFS 与 NIS 与 NIS+ 禁用此服务
rc.nfs/nfsd		/etc/rc.nfs	NFS 服务（NFS 服务器所需要）	• 认证是弱的 • 能有助于堆叠崩溃帧 • 如果在 NFS 文件服务器上则启用 • 如果禁用此服务，那么一起禁用 **biod**、**nfsd** 与 **rpc.mountd**
rc.nfs/rpc.lockd		/etc/rc.nfs	NFS 文件键锁	• 如果不在使用 NFS, 禁用此服务 • 如果不在越过网络使用文件键锁禁用此服务 • 在 SANS 最高十级安全性威胁中提到 **lockd** 守护程序
rc.nfs/rpc.mountd		/etc/rc.nfs	NFS 文件安装（NFS 服务器所需要）	• 认证是微弱的 • 能有助于堆叠崩溃帧 • 应该只在 NFS 文件服务器上启用 • 如果禁用此服务，那么一起禁用 **biod** 与 **nfsd**
rc.nfs/rpc.statd		/etc/rc.nfs	NFS 文件键锁（来恢复它们）	• 通过 NFS 实现文件键锁 • 除非在使用 NFS 否则禁用此服务
rc.nfs/rpc.yppasswdd		/etc/rc.nfs	NIS 密码守护程序（用于 NIS 主控机）	• 用来处理本地密码文件 • 只当有问题的机器是 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（用于从属 NIS）	• 接收从 NIS 主控机推进的 NIS 数据库映射 • 只当有问题的机器是对于主 NIS 服务器的从属 NIS 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）	• 后室服务器不应该依赖于 DHCP。禁用此服务 • 如果主机不在使用 DHCP，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 或依赖于网络间发送的信息，则禁用

服务	守护程序	已启动	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 IP 名称、号码、网掩码、路由器与广播地址等信息 • 如果不在使用 DHCP 则禁用此项 • 在生产与后室服务器连同不在使用 DHCP的主机上禁用
rc.tcpip/dpid2		/etc/rc.tcpip	过时的 SNMP 服务	• 禁用除非需要 SNMP
rc.tcpip/gated		/etc.rc.tcpip	接口间选择的路由	• 仿真路由器功能 • 禁用此服务并使用 RIP 或路由器替代
rc.tcpip/inetd		/etc/rc.tcpip	inetd 服务	• 彻底地保护的系统应该把此服务禁用，但这通常是不实际的 • 禁用此会禁用对于一些邮件与 Web 服务器必需的远程 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	• 收集并广播数据来窥视同一网络上的服务器 • 禁用此服务

服务	守护程序	已启动	功能	注释
rc.tcpip/sendmail		/etc/rc.tcpip	邮件服务	• 以 root 用户身份运行，因此是危险的 • 有安全性违规的长历史记录 • 禁用此服务，除非该机器用作邮件服务器 • 如果禁用，那么做下列的一件事: – 在 crontab 放一条目来清除队列。使用 **/usr/lib/sendmail -q** 命令 – 配置 DNS 服务器，从而交付您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	• 禁用如果您不在通过 SNMP 工具监视该系统 • 在关键服务器上 SNMP 可能是必需的，但工作站上则可能不要
rc.tcpip/syslogd		/etc/rc.tcpip	事件的系统日志	• 决不禁用此服务 • 易于拒绝服务攻击 • 任何系统必需
rc.tcpip/timed		/etc/rc.tcpip	旧时间守护程序	• 禁用此服务并使用 xntp 代替
rc.tcpip/xntpd		/etc/rc.tcpip	新建的时间守护程序	• 用 sync 保存系统上的时钟 • 禁用此服务。 • 配置其它系统为时间服务器并用调用 ntpdate 的 cron 作业让其它系统与它们同步
dt login		/usr/dt/config/Xaccess	未限制的 CDE	• 如果不在提供 CDE 登录到 X11 站的组，可以限制 dtlogin 到控制台。
匿名 FTP 服务		用户 rmuser -p <用户名>	匿名 ftp	• 匿名 FTP 的能力使您不能对某个特定用户跟踪 FTP 的使用 • 如果用户帐户存在，除去用户 ftp，按如下操作: **rmuser -p ftp** • 通过把那些不应该 ftp 到您系统的用户的列表植入 **/etc/ftpusers** 文件，能获得更进一步的安全性

服务	守护程序	已启动	功能	注释
匿名 FTP 写			匿名 ftp 上载	• 没有文件应该属于 ftp。 • FTP 匿名上载有可能允许把行为不良的代码放到您的系统。 • 把那些您想要禁止的用户的名称放置到 **/etc/ftpusers** 文件 • 系统- 的某些示例创建那些您可能想要不允许通过 FTP 匿名地上载到您系统的用户: root, daemon, bin.sys, admin.uucp, guest, nobody, lpd, nuucp, ladp, imnadm • 按如下所示: **chown root:system /etc/ftpusers**, 更改 **ftpusers** 文件的所有者与组权限 • 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 用户登录的任何人应该先以自己的名称登录, 然后 **su** 为 root 用户; 这提供了查帐索引
snmpd.readWrite		/etc/snmpd.conf	SNMP 读写公用性	• 如果不在使用 SNMP, 禁用 SNMP 守护程序。 • 在 **/etc/snmpd.conf** 文件禁用专用的公用性与公用性系统 • 对那些正监视您系统的 IP 地址限制 'public' 公用性
syslog.conf			配置 syslogd	• 如果还未配置 **/etc/syslog.conf**, 则禁用此守护程序 • 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. 网络服务选项总结

为达到高级系统安全性，可以使用 0 禁用和 1 启用更改几个网络选项。下列表标识出可以使用 **no** 命令的参数。

参数	命令	用途
bcastping	/usr/sbin/no -o bcastping=0	允许响应广播地址中的 ICMP 回送信号包。禁用它防止 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	指定是否允许被控制的广播进入网关。设置为 0 有助于禁止被控制的包到达远程网络。
icmpaddressmask	/usr/sbin/no -o icmpaddressmask=0	指定系统是否响应 ICMP 地址掩码请求。禁用它通过源路由访问。
ipforwarding	/usr/sbin/no -o ipforwarding=0	指定内核是否应转发信息包。禁用它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	指定内核是否发送重定向的信号。禁用它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的 IPv6 信息包。禁用它通过源路由访问。
ipsrcrouteforward	/usr/sbin/no -o ipsrcrouteforward=0	指定系统是否转发源路由的信息包。禁用它通过源路由攻击访问。
ipsrcrouterecv	/usr/sbin/no -o ipsrcrouterecv=0	指定系统是否接受源路由的信息包。禁用它通过源路由攻击访问。
ipsrcroutesend	/usr/sbin/no -o ipsrcroutesend=0	指定应用程序能否发送源路由的信息包。禁用它通过源路由攻击访问。
nonlocsroute	/usr/sbin/no -o nonlocsrcroute=0	告诉网际协议严格源路由的信息包可以在本地网络以外的主机上寻址。禁用它通过源路由攻击访问。
tcp_pmtu_discover	/usr/sbin/no -o tcp_pmtu_discover=0	禁用它通过源路由攻击访问。
udp_pmtu_discover	/usr/sbin/no -o udp_pmtu_discover=0	启用或禁用路径 MTU 发现 TCP 应用程序。禁用它通过源路由攻击访问。

关于网络可调选项的更多信息，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 可能在其它国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可证。您可以用书面方式将许可证查询寄往:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

本条款不适用联合王国或任何这样的条款与当地法律不一致的国家或地区: 国际商业机器公司以“按现状”的基础提供本出版物，不附有任何形式的（无论是明示的，还是默示的）保证，包括（但不限于）对非侵权性、适销性和适用于某特定用途的默示保证。某些国家或地区在某些交易中不允许免除明示或默示的保证。因此本条款可能不适用于您。

本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它程序（包括本程序）之间进行信息交换，以及（ii）允许对已经交换的信息进行相互使用，请与下列地址联系:

IBM Corporation
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有 IBM 依据 IBM 客户协议、IBM 国际程序许可证协议或任何同等协议中的条款提供。

有关双字节（DBCS）信息的许可证查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

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、其出版说明或其它可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其它关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

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。所有这些名称都是假定的，与真实公司企业使用相似的任何名称和地址是完全保密的。

商标

下列术语是国际商业机器公司在美国和 / 或其它国家的商标:

AIX

AIX 5L

DB2

SecureWay

IBM

RS/6000

Lotus Notes 是莲花软件有限公司和 / 或 IBM 公司在美国和 / 或其它国家或地区的注册商标。

UNIX 是 The Open Group 在美国和其它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 / 或其它国家或地区的注册商标。

Microsoft 是微软公司在美国和 / 或其它国家或地区的注册商标。

其它公司、产品或服务名称可能是其它公司的商标或服务标记。

索引

L

M

N

O

P

R

S

T

V

[特别字符]

读者意见表

AIX 5L V5.2
安全指南

姓名	地址
单位及部门	
电话号码	

读者意见表

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

请沿此线
撕下或折起

中国印刷