Solaris™ Security Toolkit 4.1
管理指南

Sun Microsystems, Inc.
www.sun.com

文件号码 817-7655-10
2004 年 10 月，修订版 A

请将有关本文档的意见或建议提交至：http://www.sun.com/hwdocs/feedback

目录

前言　xvii

1.　简介　1

使用 Solaris Security Toolkit 软件保护系统安全　1

了解软件组件　2

目录　3

`Audit` 目录　4

`Documentation` 目录　4

`man` 目录　4

`Drivers` 目录　5

`Files` 目录　7

`Finish` 目录　8

`OS` 目录　8

`Packages` 目录　9

`Patches` 目录　9

`Profiles` 目录　10

`Sysidcfg` 目录　10

数据信息库　10

维护版本控制　10

运行受支持的 Solaris OS 版本　11

运行受支持的 SMS 版本　11
配置和定制 Solaris Security Toolkit 软件　11
策略和要求　12
准则　12

2.　保护系统安全：方法论　15
规划和准备　15
考虑风险和收益　15
查看安全策略、标准和相关文档　17
实例 1　17
实例 2　17
确定应用程序和服务要求　18
确定应用程序和可用服务清单　18
确定服务要求　18
开发和执行 Solaris Security Toolkit 配置文件　25
安装软件　25
执行安装前任务　26
备份数据　26
验证系统稳定性　26
执行安装后的任务　26
验证应用程序和服务功能　27
验证安全性配置文件安装　27
验证应用程序和服务功能　27
维护系统安全　27

3.　安装和运行安全性软件　29
执行规划及安装前任务　29
从属性　30
硬件从属性　30

软件从属性 30
确定使用的模式 30
独立模式 31
JumpStart 模式 31
下载安全性软件 31
下载 Solaris Security Toolkit 软件 32
▼ 下载 tar 版本 32
▼ 下载 pkg 版本 33
下载推荐的修补程序群集软件 33
▼ 下载推荐的修补程序群集软件 34
下载 FixModes 软件 35
▼ 下载 FixModes 软件 35
下载 OpenSSH 软件 36
▼ 下载 OpenSSH 软件 36
下载 MD5 软件 37
▼ 下载 MD5 软件 37
定制安全性配置文件 38
安装和执行软件 38
在独立模式下执行软件 39
▼ 在独立模式下执行软件 41
审计选项 42
显示帮助选项 42
驱动程序选项 43
电子邮件通知选项 44
执行历史记录选项 45
最新执行选项 45
输出文件选项 45
静止输出选项 46

根目录选项　46
撤消选项　47
在 JumpStart 模式下执行软件　47
▼ 在 JumpStart 模式下执行软件　47
验证系统修改　48
对服务执行 QA 检查　48
对配置进行安全性评估　48
验证安全性配置文件　49
执行安装后的任务　49

4. 取消系统更改　51
了解如何记录并取消更改　51
撤消系统更改的要求　52
定制脚本以撤消更改　52
检查手动更改的文件　53
使用带有撤消功能的选项　54
备份选项　55
强制选项　55
保留选项　56
输出文件选项　56
静止输出选项　56
电子邮件通知选项　56
撤消系统更改　57
▼ 撤消 Solaris Security Toolkit 运行操作　57

5. 配置和管理 JumpStart 服务器　63
配置 JumpStart 服务器和环境　63
▼ 配置 JumpStart 模式　64
使用 JumpStart 配置文件模板　65

32-bit-minimal.profile 66
core.profile 66
end-user.profile 66
developer.profile 66
entire-distribution.profile 66
oem.profile 67
minimal-Sun_ONE-WS-Solaris*.profile 67
minimal-SunFire_Domain*.profile 67
添加和删除客户机 67
add-client 脚本 68
rm-client 脚本 69

6. 审计系统安全性 71

维护安全性 71
执行加强操作之前检查安全性 72
定制安全性审计 72
审计安全性的准备工作 73
使用选项和控制审计输出 73
命令行选项 74
显示帮助选项 74
电子邮件通知选项 75
输出文件选项 76
静止选项 76
冗长选项 76
标题与消息输出 77
主机名称、脚本名称和时间戳输出 79
进行安全性审计 80
▼ 进行安全性审计 80

7. 保护系统安全 83

规划与准备 83

假设与限制 84

系统环境 84

安全性要求 85

创建安全性配置文件 85

安装软件 85

下载和安装安全性软件 86

▼ 下载和安装安全性软件 86

安装修补程序 86

▼ 安装修补程序 86

指定和安装 OS 群集 87

▼ 指定和安装 OS 群集 87

配置 JumpStart 服务器和客户机 88

准备基础结构 89

▼ 准备基础结构 89

验证和检查 rules 文件 91

定制加强安全性配置 93

启用 FTP 服务 94

▼ 启用 FTP 服务 94

安装 Secure Shell 软件 94

▼ 安装 Secure Shell 94

启用 RPC 服务 95

▼ 启用 RPC 95

定制 `syslog.conf` 文件 96

▼ 定制 `syslog.conf` 文件 96

安装客户机 97

▼ 安装客户机 97

质量保证测试　98

- 验证配置文件安装　98
- 验证应用程序和服务的功能　99

术语表　101

索引　107

图

图 1-1 软件组件结构 3

图 1-2 驱动程序控制流程 6

表

表 1-1 定制文件的命名标准 13

表 2-1 列出最近使用的服务 23

表 3-1 将命令行选项与 `jass-execute` 结合使用 40

表 4-1 将命令行选项与撤消命令结合使用 55

表 5-1 JumpStart `add-client` 命令 68

表 5-2 JumpStart `rm-client` 命令 69

表 6-1 将命令行选项与审计命令结合使用 74

表 6-2 审计冗长级别 77

表 6-3 在审计输出中显示标题和消息 77

表 6-4 显示主机名称、脚本名称和时间戳审计输出 79

代码实例

代码实例 1-1 驱动程序控制流程 6

代码实例 2-1 获得有关文件系统对象的信息 19

代码实例 2-2 从正在运行的进程中收集信息 19

代码实例 2-3 确定动态加载的应用程序 19

代码实例 2-4 确定是否正在使用配置文件 20

代码实例 2-5 确定哪些应用程序使用 RPC 21

代码实例 2-6 验证 `rusers` 服务 22

代码实例 2-7 确定使用 RPC 的应用程序的备选方法 23

代码实例 2-8 确定哪些服务或应用程序拥有哪些端口 24

代码实例 2-9 确定哪些进程正在使用文件和端口 24

代码实例 3-1 将一个修补程序文件移动到`/opt/SUNWjass/Patches` 目录 34

代码实例 3-2 独立模式下命令行使用的样例 39

代码实例 3-3 在独立模式下执行软件 41

代码实例 3-4 `-h` 选项输出样例 42

代码实例 3-5 `-d` *driver* 选项输出样例 44

代码实例 3-6 `-H` 选项输出样例 45

代码实例 3-7 `-l` 选项输出样例 45

代码实例 3-8 `-o` 选项输出样例 46

代码实例 3-9 `-q` 选项输出样例 46

代码实例 4-1 手动更改的文件输出样例 54

代码实例 4-2 可撤消的运行操作的输出样例 58
代码实例 4-3 撤消运行操作处理多个清单文件条目的输出样例 58
代码实例 4-4 撤消异常的输出样例 60
代码实例 4-5 在撤消过程中选择备份选项的输出样例 60
代码实例 6-1 -h 选项输出样例 75
代码实例 6-2 -o 选项输出样例 76
代码实例 6-3 -q 选项输出样例 76
代码实例 6-4 仅报告审计失败的输出样例 78
代码实例 6-5 审计日志条目的输出样例 79
代码实例 6-6 审计运行操作的输出样例 81
代码实例 7-1 在 JumpStart 服务器上添加一台客户机 89
代码实例 7-2 创建一个配置文件 90
代码实例 7-3 修改的脚本的输出样例 90
代码实例 7-4 检查 rules 文件以纠正错误 91
代码实例 7-5 rules 文件的输出样例 92
代码实例 7-6 错误脚本样例 92
代码实例 7-7 正确脚本样例 93
代码实例 7-8 修改的 xsp-firewall-hardening.driver 输出样例 97
代码实例 7-9 评估安全性配置 99

前言

本手册包含的参考信息有助于您了解和使用 Solaris Security Toolkit 软件。它主要针对使用 Solaris Security Toolkit 软件来提高 Solaris™ 操作系统 (OS) 版本 8 至 9 安全性的读者，例如部署新的 Sun 系统或保护已部署系统安全的管理员、安全顾问以及其他人员。本书中的指导适用于以 JumpStart™ 模式或独立模式来使用该软件。

阅读本书之前

您应当是经过 Sun 认证的 Solaris™ 操作系统的系统管理员或网络管理员。同时还应该对标准网络协议和拓扑知识有一定的了解。

由于本书所针对的读者在安全性方面的经验或知识千差万别，因此您的经验和知识决定了您应如何使用本书。

本书的结构

您可以将本手册作为用户指南来使用。其中的章节包含使用该软件保护系统安全的信息、指导和准则。本书的结构如下所示：

第 1 章介绍 Solaris Security Toolkit 软件的设计和用途。其中涉及关键组件、功能、优点和所支持平台方面的信息。

第 2 章提供保护系统安全的方法论。其中介绍了在使用 Solaris Security Toolkit 软件保护系统安全之前可以应用的过程。

第 3 章提供有关下载、安装和运行 Solaris Security Toolkit 软件以及其他与安全性相关的软件的指导信息。

第 4 章提供有关在加强安全性过程中撤销由 Solaris Security Toolkit 软件所做更改的信息和过程。

第 5 章提供有关配置和管理 JumpStart 服务器以使用 Solaris Security Toolkit 软件的信息。

第 6 章介绍如何使用 Solaris Security Toolkit 软件来审计 （验证）系统安全性。可在加强安全性后使用本章的信息和过程维护已建立的安全性配置文件。

第 7 章介绍如何将前面章节中提供的信息和技巧，应用到安装并保护新系统安全的实际情况中。

使用 UNIX® 命令

本文档没有介绍基本的 UNIX® 命令和过程，如关闭系统、引导系统和配置设备等。有关此类信息，请参阅以下文档：

- 系统附带的软件文档
- Solaris 操作系统文档，位于：

  `http://docs.sun.com`

Shell 提示符

Shell	提示符
C shell	*machine-name*%
C shell 超级用户	*machine-name*#
Bourne shell 和 Korn shell	$
Bourne shell 和 Korn shell 超级用户	#

印刷约定

字体*	含义	实例
AaBbCc123	命令、文件和目录的名称；计算机屏幕输出	编辑 .login 文件。 使用 ls -a 命令列出所有文件。 % You have mail.
AaBbCc123	键入的内容，与计算机屏幕输出相区别	% **su** Password:
AaBbCc123	书名、新词或术语以及要强调的词。将用实际名称或值来替代命令行变量。	请阅读 *"用户指南"* 中的第 6 章。 这些称为*类*选项。 要执行该操作，您*必须*是超级用户。 要删除文件，请键入 rm *filename*。

* 您所使用的浏览器的设置可能与这里的设置不同。

访问 Sun 文档

您可以查看、打印或购买种类繁多的 Sun 文档，包括本地化版本，其网址如下：

http://www.sun.com/documentation

第三方 Web 站点

Sun 对本文档中提到的第三方 Web 站点的可用性不承担任何责任。对于此类站点或资源中的（或通过它们获得的）任何内容、广告、产品或其他材料， Sun 并不表示认可，也不承担任何责任。对于因使用或信任此类站点或资源中的（或通过它们获得的）任何内容、产品或服务而造成的或连带产生的实际或声称的损坏或损失， Sun 概不负责，也不承担任何责任。

相关资源

下面列出了相关的出版物及 Web 站点。

出版物

- Andert Donna、 Wakefield Robin 和 Weise Joel。“Trust Modeling for Security Architecture Development”， Sun BluePrints™ OnLine， 2002 年 12 月，`http://www.sun.com/blueprints/1202/817-0775.pdf`。
- Dasan Vasanthan、 Noordergraaf Alex 和 Ordica Lou。“The Solaris Fingerprint Database - A Security Tool for Solaris Software and Files”， Sun BluePrints OnLine， 2001 年 5 月，`http://www.sun.com/blueprints/0501/Fingerprint.pdf`。
- Englund Martin，“Securing Systems with Host-Based Firewalls - Implemented With SunScreen Lite 3.1 Software”， Sun BluePrints OnLine， 2001 年 9 月，`http://sun.com/blueprints/0901/sunscreenlite.pdf`。
- Garfinkel Simon 和 Spafford Gene。*《Practical UNIX and Internet Security》*，第二版， O'Reilly & Associates， 1996 年 4 月。
- Howard John S. 和 Noordergraaf Alex。*《JumpStart Technology: Effective Use in the Solaris Operating Environment》*，Sun Microsystems 官方资源系列，Prentice Hall，2001 年 10 月。
- Moffat Darren J.， FOCUS on SUN: *《Solaris BSM Auditing》*，`http://www.securityfocus.com/infocus/1362`
- Noordergraaf Alex。“Solaris™ Operating Environment Minimization for Security: A Simple, Reproducible and Secure Application Installation Methodology Updated for Solaris 8 Operating Environment”， Sun BluePrints OnLine， 2000 年 11 月， `http://sun.com/blueprints/1100/minimize-updt1.pdf`。

- Noordergraaf Alex。“Minimizing the Solaris Operating Environment for Security: Updated for Solaris 9 Operating Environment”， Sun BluePrints OnLine， 2002 年 11 月， http://sun.com/blueprints/1102/816-5241.pdf。
- Noordergraaf Alex。“Securing the Sun Cluster 3.x Software”， Sun BluePrints OnLine article， 2003 年 2 月， http://www.sun.com/solutions/blueprints/0203/817-1079.pdf。
- Noordergraaf Alex，“Securing the Sun Enterprise 10000 System Service Processors”， Sun BluePrints OnLine 文章， 2002 年 3 月， http://www.sun.com/blueprints/0302/securingenter.pdf
- Noordergraaf Alex 等。*《Enterprise Security: Solaris Operating Environment Security Journal, Solaris Operating Environment Versions 2.5.1, 2.6, 7, and 8》*， Sun Microsystems™， Prentice Hall Press， ISBN 0-13-100092-6， 2002 年 6 月。
- Noordergraaf Alex 和 Nimeh Dina。“Securing the Sun Fire 12K and 15K Domains”， Sun BluePrints OnLine 文章， 2003 年 2 月， http://www.sun.com/blueprints/0203/817-1357.pdf。
- Noordergraaf Alex 和 Nimeh Dina。“Securing the Sun Fire 12K and 15K System Controllers”， Sun BluePrints OnLine 文章， 2003 年 2 月， http://www.sun.com/blueprints/0203/817-1358.pdf。
- Noordergraaf Alex 和 Watson Keith。“Solaris Operating Environment Security: Updated for the Solaris 9 Operating Environment”， Sun BluePrints OnLine， 2002 年 12 月， http://www.sun.com/blueprints/1202/816-5242.pdf。
- O'Donnell Nicholas 和 Noordergraaf Alex。“Minimizing Domains for Sun Fire V1280, 6800, 12K, and 15K Systems”， Sun BluePrints OnLine 文章， 2003 年 9 月， http://www.sun.com/blueprints/0903/817-3340.pdf [Part I] 和 http://www.sun.com/blueprints/0903/817-3628.pdf [Part II]
- Osser William 和 Noordergraaf Alex。“Auditing in the Solaris 8 Operating Environment”， Sun BluePrints OnLine， 2001 年 2 月 http://www.sun.com/blueprints/0201/audit_config.pdf。
- Reid Jason M. 和 Watson Keith。“Building and Deploying OpenSSH in the Solaris Operating Environment”， Sun BluePrints OnLine， 2001 年 7 月， http://sun.com/blueprints/0701/openSSH.pdf。
- Reid Jason M.，“Configuring OpenSSH for the Solaris Operating Environment”， Sun BluePrints OnLine 文章， 2002 年 1 月， http://www.sun.com/blueprints/0102/configssh.pdf。
- Reid Jason。*《Secure Shell in the Enterprise》*， Sun Microsystems 官方资源系列， Prentice Hall， 2003 年 6 月
- *《Solaris Advanced Installation Guide》*, Sun Microsystems, http://docs.sun.com。
- *《SunSHIELD Basic Security Module Guide》*, Sun Microsystems, Inc., http://docs.sun.com。

- Watson Keith 和 Noordergraaf Alex。“Solaris Operating Environment Network Settings for Security: Updated for Solaris 9 Operating Environment”， Sun BluePrints OnLine， 2003 年 6 月，
  `http://www.sun.com/solutions/blueprints/0603/816-5240.pdf`。
- Weise Joel 和 Martin Charles R.“Developing a Security Policy”，Sun BluePrints OnLine 文章， 2001 年 12 月，
  `http://www.sun.com/solutions/blueprints/1201/secpolicy.pdf`。

Web 站点

- AUSCERT，*《UNIX Security Checklist》*，
  http://www.auscert.org.au/render.html?it=1935&cid=1920
- CERT/CC （网址为 `http://www.cert.org`）是联邦政府投资的研究和开发中心，致力于研究计算机安全性问题。
- Chkrootkit， `http://www.chkrootkit.org`
- Galvin Peter Baer，*《The Solaris Security FAQ》*，
  `http://www.itworld.com/Comp/2377/security-faq/`
- HoneyNet Project, “Know Your Enemy: Motives”
  `http://project.honeynet.org/papers/motives/`
- 列出开放式文件软件，
  `ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/`
- Nmap Port Scanner, `http://www.insecure.org`
- OpenSSH 工具， `http://www.openssh.com/`
- Pomeranz Hal，*《Solaris Security Step by Step》*， `http://www.sans.org/`
- Rhoads Jason，*《Solaris Security Guide》*，
  `http://www.sabernet.net/papers/Solaris.html`
- “Security Focus”（网址为 `http://www.securityfocus.org`）是一个专门讨论与安全性相关主题的网站。
- Sendmail Consortium， `sendmail` 配置信息，
  `http://www.sendmail.org/`
- Spitzner Lance，*《Armoring Solaris》*，
  `http://secinf.net/unix_security/Armoring_Solaris.html`
- SSH 通信安全性，安全 Shell (SSH) 工具， `http://www.ssh.com/`
- Sun BluePrints OnLine， `http://sun.com/blueprints`
- Sun BluePrints OnLine Tools for FixModes 软件和 MD5 脚本，
  `http://jsecom15k.sun.com/ECom/EComActionServlet?StoreId=8&PartDetailId=817-0074-10&TransactionId=try&LMLoadBalanced=`
- Sun Enterprise Authentication Mechanism™ 信息，
  `http://www.sun.com/software/solaris/ds/ds-seam`

- SunSolve℠ — `http://sunsolve.sun.com`

联系 Sun 技术支持

如果您遇到本文档无法解决的技术问题，请访问以下网址：

`http://www.sun.com/service/contacting`

Sun 欢迎您提出意见和建议

Sun 乐于对其文档进行改进，欢迎您提出意见和建议。您可以访问以下网址提交您的意见：

`http://www.sun.com/hwdocs/feedback`

请在您的反馈信息中包含文档的书名和文件号码：

《Solaris Security Toolkit 4.1 管理指南》，文件号码 817-7655-10

第 1 章

简介

本章介绍 Solaris Security Toolkit 软件的设计和用途。其中涉及关键组件、功能、优点和所支持平台方面的信息。本章还提供有关对修改和部署进行版本控制的准则，并提出有关定制 Solaris Security Toolkit 软件的重要准则。

本章包含以下主题：

- 第 1 页 “使用 Solaris Security Toolkit 软件保护系统安全”
- 第 2 页 “了解软件组件”
- 第 10 页 “维护版本控制”
- 第 11 页 “运行受支持的 Solaris OS 版本”
- 第 11 页 “运行受支持的 SMS 版本”
- 第 11 页 “配置和定制 Solaris Security Toolkit 软件”

使用 Solaris Security Toolkit 软件保护系统安全

Solaris Security Toolkit 软件的非正式名称为 JASS （JumpStart 体系结构和安全脚本）工具包，可提供自动化、可扩展、可伸缩的机制来构建和维护 Solaris OS 系统的安全。使用 Solaris Security Toolkit 软件可以加强、最小化和审计系统的安全性。

- **加强系统安全性** — 修改 Solaris OS 配置以提高系统的安全性。
- **最小化系统安全性** — 删除特定系统不需要的 Solaris OS 软件包。（因为每个系统的要求都不尽相同，所以不需要的内容也会不同，从而必须进行评估。）这种删除会减少要进行修补和加强安全性的组件数量，从而减少可供入侵者使用的入口点。
- **审计系统安全性** — 确定系统配置是否与预定义的安全性配置文件相符合的过程。
- **安全性计分** — 得分是与审计运行过程中暴露出来的故障数量相关联的值。因此，如果未发现 （任何种类的）故障，那么最后得分应为 0。检测到一个故障， Solaris Security Toolkit 便将得分 （也称为安全漏洞值）增加 1 分。

系统安装和配置应该尽可能实现自动化 （理想状态为 100%）。本准则包括 OS 安装和配置、网络配置、用户帐户、应用程序和安全性修改方面的信息。安全性修改包括加强系统安全性和/或最小化系统安全性，具体取决于系统的用途。 JumpStart 软件是一种可用于实现 Solaris OS 安装自动化的技术。JumpStart 软件提供一种通过网络安装系统的机制，很少需要或不需要人为干预。 Solaris Security Toolkit 软件提供了一个框架和多个脚本，可在基于 JumpStart 软件的安装中实现并使大部分与加强和最小化 Solaris OS 系统安全性相关的任务自动化。

此外， Solaris Security Toolkit 软件还具有独立模式。该模式能够执行与 JumpStart 模式中相同的所有安全性加强功能，但是只能在经过部署的系统上使用。在上述两种模式中，安全性修改的定制可以并且应该与系统的安全性要求相匹配。

无论采取哪种方式安装系统，您都可以在初始阶段使用 Solaris Security Toolkit 软件来加强和最小化系统的安全性。然后，定期使用 Solaris Security Toolkit 软件来审计安全系统的安全性配置文件是否被意外或恶意地进行了修改。

注 – 术语 *审计* 指的是 Solaris Security Toolkit 软件对安全性状态的自动化验证过程，方法是与预先定义的安全性配置文件相比较。本出版物中使用此术语，并不表示在使用审计选项后便可保证系统的绝对安全。

了解软件组件

本节概述了 Solaris Security Toolkit 软件的组件结构。 Solaris Security Toolkit 软件是多个文件和目录的集合。图 1-1 为该软件的结构示意图。

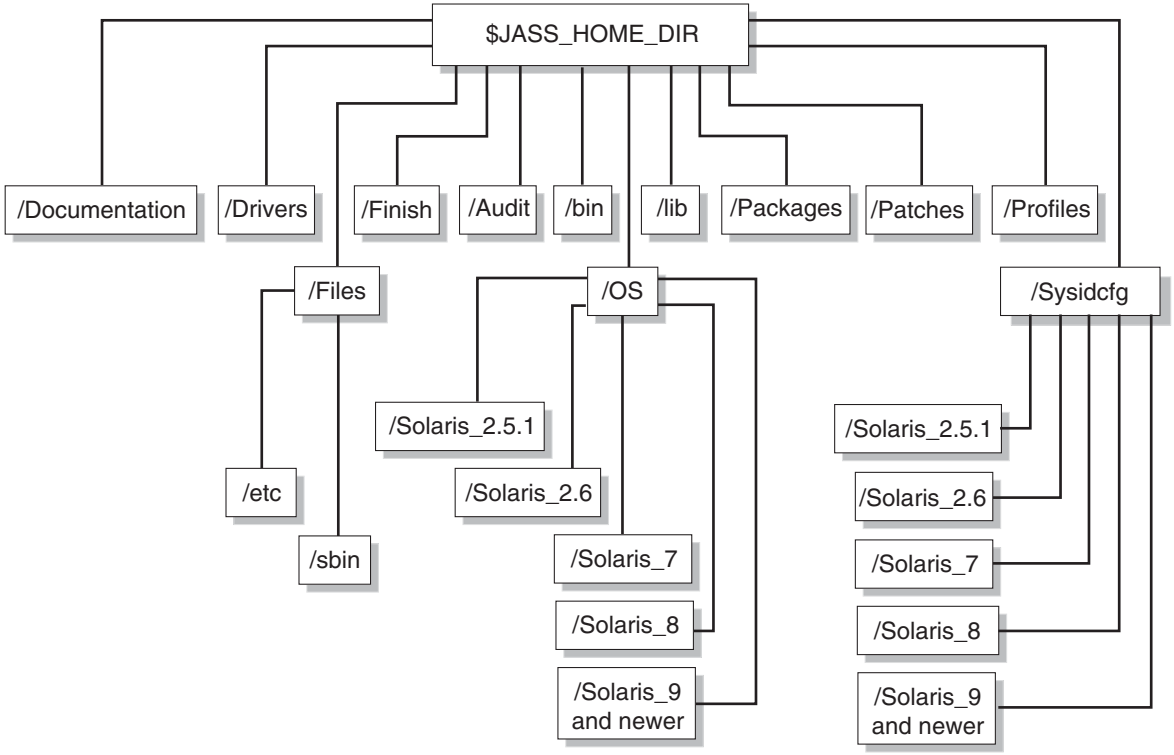

图 1-1 软件组件结构

除这些目录和子目录外，以下文件位于 Solaris Security Toolkit 软件结构的顶层，在 `/bin` 中：

- `add-client` — 一个 JumpStart 帮助程序，用于将客户机添加到 JumpStart 环境中。
- `rm-client` — 一个 JumpStart 帮助程序，用于将客户机从 JumpStart 环境中删除。
- `make-jass-pkg` — 该命令能够从 Solaris Security Toolkit 目录内容中创建 Solaris OS 软件包，以简化已定制的 Solaris Security Toolkit 配置在内部的分发。
- `jass-check-sum` — 该命令能够确定曾经由 Solaris Security Toolkit 软件修改过的文件是否已被更改（基于每次 Solaris Security Toolkit 运行过程中所创建的校验和）。
- `jass-execute` — 配置 Solaris Security Toolkit 应用程序的命令。

目录

Solaris Security Toolkit 体系结构的组件按以下目录进行组织：

- /Audit
- /bin
- /Documentation
- /man
- /Drivers
- /Files
- /Finish
- /lib
- /OS
- /Packages
- /Patches
- /Profiles
- /Sysidcfg

本节中逐一介绍了每个目录，并在适当的位置列出了每个脚本、配置文件或子目录，同时还将提供其他章节作为参考以便您获得详细信息。

Solaris Security Toolkit 目录结构是基于 Sun BluePrints 书籍 *《JumpStart Technology: Effective Use in the Solaris Operating Environment》*中所述的结构。

Audit 目录

该目录包含的脚本，可评估系统是否符合预定义的安全性配置文件或审计脚本集。该目录中的脚本分为以下类别：

- 禁用
- 启用
- 安装
- 最小化
- 打印
- 删除
- 设定
- 更新

有关每个类别中脚本的详细列表和每个脚本的说明，请参阅 *《Solaris Security Toolkit 4.1 Reference Manual》*。

Documentation 目录

本目录包含针对用户使用信息的文本文件，如自述文件。

man 目录

本目录包含命令、功能和驱动程序手册页部分的子目录。此外，本目录还包含 `windex` 文件，该文件是命令的索引，且免费提供。

有关上述手册页的详细信息，请参见手册页本身或 *《Solaris Security Toolkit 4.1 Man Page Guide》*。

Drivers 目录

该目录包含配置信息文件，这些配置信息指定了运行 Solaris Security Toolkit 软件时需要执行和安装的文件。该目录还包含驱动程序、脚本和配置文件。

以下是 Drivers 目录中的驱动程序和脚本的实例：

- common_{log|misc}.funcs
- config.driver
- desktop-{config|hardening|secure}.driver
- driver.{funcs|init|run}
- hardening.driver
- finish.init
- install-Sun_ONE-WS.driver
- jumpstart-{config|hardening|secure}.driver
- secure.driver
- starfire-{config|hardening|secure}.driver
- suncluster3x-{config|hardening|secure}.driver
- sunfire_15k_domain-{config|hardening|secure}.driver
- sunfire_15k_sc-{config|hardening|secure}.driver
- sunfire_mf_msp-{config|hardening|secure}.driver
- undo.{funcs|init|run}
- hardening.driver
- user.init.SAMPLE
- user.run.SAMPLE
- audit_{private|public}.funcs

所有特定产品的驱动程序以及某些其他驱动程序均包括三个文件：

- *name*-secure.driver
- *name*-config.driver
- *name*-hardening.driver

在以上列表中，这三个文件是在括号中列出的，例如 sunfire_15k_sc-{config|hardening|secure}.driver。列出这些文件是为了突出完整性。执行某个驱动程序时，仅使用 *name*-secure.driver 即可。该驱动程序会自动调用相关的驱动程序。

Solaris Security Toolkit 体系结构包括可以使驱动程序、 finish 和 audit 脚本不经修改（不修改实际的脚本本身）便可用于不同环境的配置信息。在 finish 和 audit 脚本中的所有变量都在一个配置文件集中进行维护 — 这些配置文件是由驱动程序导入的，当驱动程序调用脚本时 finish 和 audit 脚本就可以使用变量。

Solaris Security Toolkit 软件具有三个主要配置文件，它们都存储在 Drivers 目录中：

- driver.init

- finish.init
- user.init

由驱动程序调用的 finish 脚本位于 Finish 目录中。由驱动程序调用的 audit 脚本位于 Audit 目录中。由驱动程序安装的文件从 Files 目录中读取。有关 finish 脚本和 audit 脚本的详细信息，请参阅本书中相应的章节。

图 1-2 显示了驱动程序控制流程的流程图。

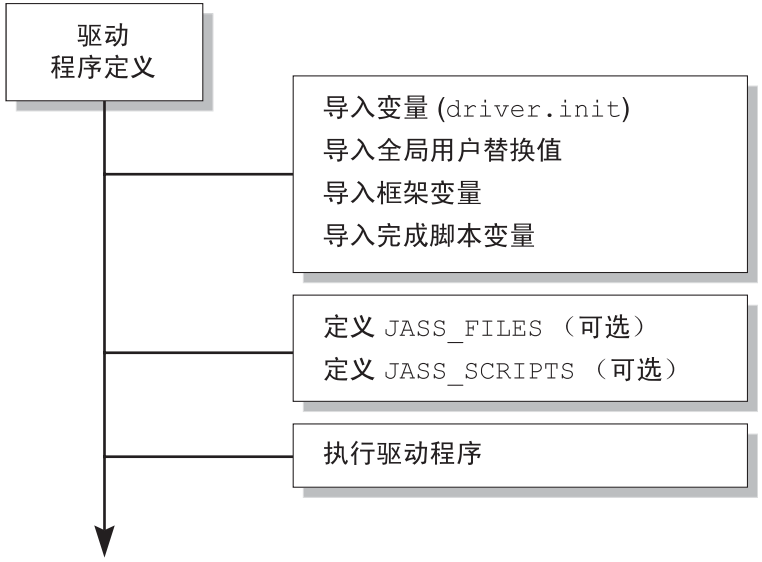

图 1-2 驱动程序控制流程

首先从 .init 文件导入所有环境变量。完成后，驱动程序继续进行到第二部分：定义 JASS_FILES 和 JASS_SCRIPTS。这两个定义是可选的；可以定义任意一个单独的环境、也可以定义两个或者不定义任何环境。驱动程序的第三部分调用 driver.run 来执行由 JASS_FILE 和 JASS_SCRIPTS 环境变量所定义的任务。

代码实例 1-1显示了驱动程序控制流程。

代码实例 1-1 驱动程序控制流程

```
DIR="`/bin/dirname $0`"

export DIR
. ${DIR}/driver.init

JASS_FILES="
                            /etc/cron.d/cron.allow
                            /etc/default/ftpd
```

代码实例 1-1 驱动程序控制流程 *（接上页）*

```
                            /etc/default/telnetd
"

JASS_SCRIPTS="
                            install-at-allow.fin
                            remove-unneeded-accounts.fin
"
. ${DIR}/driver.run
```

该代码实例设置 DIR 环境变量并将其导出，以使驱动程序识别启动目录。接下来，将 JASS_FILES 环境变量定义为包含从 JASS_HOME_DIR/Files 目录复制到客户机上的那些文件。然后，将 JASS_SCRIPTS 环境变量定义为包含由 Solaris Security Toolkit 软件运行的 finish 脚本。最后，通过调用 driver.run 驱动程序执行运行加强系统安全性的操作。一旦调用， driver.run 将复制 JASS_FILES 中指定的文件，并运行 JASS_SCRIPTS 中指定的脚本。

Files 目录

该目录用于 JASS_FILES 环境变量和 driver.run 脚本。该目录存储着复制到 JumpStart 客户机的文件。

该目录中包含以下文件：

- /.cshrc
- /.profile
- /etc/default/sendmail
- /etc/dt/config/Xaccess
- /etc/hosts.{allow|deny}
- /etc/init.d/nddconfig
- /etc/init.d/set-tmp-permissions
- /etc/init.d/sms_arpconfig
- /etc/init.d/swapadd
- /etc/issue
- /etc/motd
- /etc/notrouter
- /etc/rc2.d/S00set-tmp-permissions
- /etc/rc2.d/S07set-tmp-permissions
- /etc/rc2.d/S70nddconfig
- /etc/rc2.d/S73sms_arpconfig
- /etc/rc2.d/S73swapadd
- /etc/security/audit_class
- /etc/security/audit_control
- /etc/security/audit_event
- /etc/sms_domain_arp
- /etc/sms_sc_arp

- /etc/syslog.conf

Finish 目录

该目录包含 finish 脚本，该脚本在安装过程中执行系统修改和更新。该目录中的脚本分为以下类别：

- 禁用
- 启用
- 安装
- 最小化
- 打印
- 删除
- 设定
- 更新

有关每个类别中脚本的详细列表和每个脚本的说明，请参阅 *《Solaris Security Toolkit 4.1 Reference Manual》*。

OS 目录

该目录仅包含 Solaris OS 映像。这些映像将作为客户机的安装源在 JumpStart 软件安装过程中加以使用，同时这些映像还将提供 `add_install_client` 和 `rm_install_client` 脚本。 `add_client` 脚本接受这些附加目录名称。

有关加载和修改 Solaris OS 映像的详细信息，请参阅 Sun BluePrints 书籍 *《JumpStart Technology: Effective Use in the Solaris Operating Environment》*。

标准安装命名惯例如下。

Solaris OS

对于 Solaris OS，请使用以下的命名标准：

`Solaris_`*OS 版本*`_`*CD 版本的 4 位数年份*`_`*2 位数月份*

例如，日期为 2001 年 4 月的 Solaris 8 Operating Environment CD 的目录名称应为 `Solaris_8_2001-04`。通过将 Solaris OS 的更新和版本分开，可以对测试和开发目的维护进行非常精细的控制。

Trusted Solaris OS

对于 Trusted Solaris，请使用以下目录命名标准：

`Trusted_Solaris_`*OS 版本*`_`*CD 版本的 4 位数年份*`_`*2 位数月份*

例如，如果 Trusted Solaris 软件版本日期为 2000 年 2 月，则该目录名称应为：`Trusted_Solaris_8_2000-02`。

Solaris OS Intel Platform Edition

对于 Solaris OS Intel Platform Edition，请使用以下目录命名标准：

`Solaris_`*OS 版本*`_CD `*版本的 4 位数年份*`_2 `*位数月份*`_ia`

例如，如果 Solaris OS Intel Platform Edition 发布日期为 2001 年 4 月，则该目录名称应为：`Solaris_8_2001-04_ia`。

`Packages` 目录

该目录包含可以使用 finish 脚本进行安装的软件包。例如， Sun Java™ System Web Server （之前称为 Sun™ ONE Web Server，在其之前又称为 iPlanet™ Web Server）软件包存储在 `Packages` 目录中，以便在需要时由相应的 finish 脚本安装该软件。

Solaris Security Toolkit 软件包含的几个 finish 脚本可以执行软件安装和基本的配置功能。从 `Packages` 目录中安装软件的脚本包括：

- `install-fix-modes.fin`
- `install-Sun_ONE-WS.fin`
- `install-jass.fin`
- `install-md5.fin`
- `install-openssh.fin`

`Patches` 目录

本目录用于存储 Solaris OS 的 Recommended and Security Patch Clusters。下载必需的修补程序并将其提取到本目录中。

通过将修补程序放置在该目录中并在其中提取，可以简化安装操作。当修补程序提取到该目录中时， Solaris Security Toolkit 软件修补程序安装脚本会使安装自动化，因此无须手动为每个系统安装提取修补程序群集。

为所使用的每个 Solaris OS 版本创建子目录。例如， `Patches` 目录中可能已经存在 `2.5.1_Recommended` 和 `2.6_Recommended` 目录。

Solaris Security Toolkit 软件支持 Solaris OS Intel Platform Edition 修补程序群集。这些修补程序群集所支持的命名惯例与通过 SunSolve OnLine℠ 服务获得的命名惯例相同。

格式为 `Solaris_<release>_x86_Recommended`。用于 Solaris 8 OS 的 Solaris OS Intel Platform Edition 修补程序群集将位于一个名称为 `Solaris_8_x86_Recommended` 的目录中。

Profiles 目录

该目录包含所有 JumpStart 配置文件。JumpStart 软件使用这些配置文件中包含的配置信息以确定安装的 Solaris OS 群集 （例如，核心、最终用户、开发人员或完整分发）、磁盘布局以及要执行的安装类型 （例如，独立安装）。

rules 文件列出了它使用的 JumpStart 配置文件，以定义如何构建特定的系统或系统组。

Sysidcfg 目录

与 Profiles 目录类似， Sysidcfg 目录包含仅在 JumpStart 模式安装过程中使用的文件。通过提供必需的安装信息，这些文件可使 Solaris OS 安装自动化。特定操作系统的信息存储在单独的目录树中。

每个 Solaris OS 都具有一个单独的目录。每个版本都有一个名为 Solaris_*OS 版本* 的目录。Solaris Security Toolkit 软件提供了用于 Solaris OS 版本 2.5.1 至 9 的样例 sysidcfg 文件。

sysidcfg 文件样例可以扩展为其他类型，例如每个网络、主机等等。Solaris Security Toolkit 软件支持任意 sysidcfg 文件。

有关 sysidcfg 文件的其他信息，请参见 Sun BluePrints 书籍 *《JumpStart Technology: Effective Use in the Solaris Operating Environment》*。

数据信息库

数据信息库是 JASS_REPOSITORY 目录中的一个环境变量，它支持 Solaris Security Toolkit 将运行操作撤消，根据每个运行操作的执行方式来保存数据，维护由软件修改的文件清单以及保存执行日志的数据。撤消功能依赖于存储在数据信息库中的信息。

维护版本控制

维护由 Solaris Security Toolkit 软件使用的所有文件和脚本的版本控制非常关键，有以下两个原因。第一，该环境的其中一个目标就是能够重新创建系统安装。如果没有安装过程中所用到所有文件版本的快照，那么该目标是不可能实现的。第二，因为这些脚本执行安全性功能 （这对很多组织来说都是关键的过程），所以必须给予严格的警告以确保仅适当并经过测试的更改加以了实施。

在 Solaris OS SUNWsprot 软件包中提供了源代码控制系统 (SCCS) 的版本控制软件包。用户可以使用来自免费软件和商业供应商的其他版本控制软件来管理版本信息。无论您使用哪种版本控制产品，都要使用一个过程，从而为将来系统的重新创建管理更新信息并获取版本信息。

除版本控制外，还要使用完整性管理解决方案以确定文件的内容是否已经被修改。尽管系统的特权用户可能能够绕过版本控制系统，但他们无法轻易地绕过完整性管理系统，该系统在远程系统上维护其完整性数据库。进行集中管理时，完整性管理解决方案会充分发挥其作用，因为本地存储的数据库可能会被恶意修改。

运行受支持的 Solaris OS 版本

对于 Solaris Security Toolkit 软件的 Sun 支持，仅限于在 Solaris 8 和 Solaris 9 操作系统中使用该软件。虽然该软件能够在 Solaris 2.5.1、Solaris 2.6 和 Solaris 7 操作系统中使用，但 Sun 支持并不适用于在这些操作系统中使用该软件。

Solaris Security Toolkit 软件可自动检测已安装的 Solaris OS 软件的版本，然后运行适合该操作系统版本的任务。

运行受支持的 SMS 版本

如果您使用 System Management Service (SMS) 来管理系统控制器 (SC)，且所使用的 SMS 版本在 1.3 至 1.4.1 之间，则 Sun 支持可用于 Solaris Security Toolkit 4.1 软件。

配置和定制 Solaris Security Toolkit 软件

Solaris Security Toolkit 软件包含用于脚本、框架功能和变量的缺省值，这些缺省值可实现 Sun BluePrints 书籍 *《Enterprise Security: Solaris Operating Environment Security Journal, Solaris Operating Environment Versions 2.5.1, 2.6, 7, and 8》* 以及关于安全性的 Sun BluePrints OnLine 文章中的所有安全准则。这些设置并不适用于所有系统，因此必须定制 Solaris Security Toolkit 软件来满足系统的安全性要求。

Solaris Security Toolkit 软件的一个最重要特征就是可以轻松地定制，使它符合您的环境、系统和要求。要定制 Solaris Security Toolkit 软件，请通过驱动程序、 finish 脚本、 audit 脚本、框架功能、环境变量以及文件模板来对其进行调整。

大多数用户不需要修改 Solaris Security Toolkit 代码。任何更改都可能对支持性和升级产生负面影响。如果在用户环境中使用 Solaris Security Toolkit 软件必须修改代码，那么请将该代码复制到一个唯一的文件或功能名称中，以便轻松地跟踪更改，如第 12 页“准则”中所述。

在整个指南中，每章的适当位置提供了用于定制 Solaris Security Toolkit 软件的准则和指导。请参见 *《Solaris Security Toolkit 4.1 Reference Manual》* 以查找关于定制驱动程序的帮助信息。定制包括修改和创建文件或变量。

以下章节提供了用于定制 Solaris Security Toolkit 软件的实例。实例重点介绍了定制 Solaris Security Toolkit 软件的某些方法；然而，还存在许多其他方法。

在尝试定制 Solaris Security Toolkit 软件之前，必须准确理解以下各节所给出的信息。这些信息基于从很多部署方案收集的共享经验，因此可以避免通常所犯的错误。

策略和要求

定制和部署 Solaris Security Toolkit 软件时，适当的规划可以确保正确配置结果平台配置，并且与组织的期望相一致。

在规划阶段中，请务必从各种来源中获取输入，这些来源包括安全性策略和标准、工业规程和准则以及供应商提供的首选做法。

除此之外非常重要的一点是，应该考虑应用程序和操作要求以确保配置结果不会影响平台为其预期的业务功能提供服务。

准则

定制 Solaris Security Toolkit 软件时，请考虑以下准则。了解并遵守这些准则有助于使维持部署的过程更加简单、有效。

- 作为一般规则，请不要更改由 Solaris Security Toolkit 软件提供的任何*原始* 文件（驱动程序、脚本、文件等等）。更改原始文件将阻止并限制您的组织升级到 Solaris Security Toolkit 软件最新版本的能力，因为对原始文件的任何更改都可能会被该文件的新版本所覆盖。（定制的所有更改都将丢失，而系统配置的更改方式可能不合适。）要定制其中任何文件，请首先制作一个副本，然后修改该副本，保留原始文件不变。本准则只有三个例外，`sysidcfg` 文件、 Files 目录中的模板以及 Sun BluePrints OnLine 文章中指导的操作。

■ 请对驱动程序或脚本的副本进行适当地命名，以便区别于其原始版本。使用可表明脚本用途的前缀或关键字。例如，包含公司的名称或股票标记、部门标识符或平台、应用程序类型的前缀都是不错的命名标准。表 1-1 列出了几个命名标准的实例。

表 1-1 定制文件的命名标准

定制文件	命名标准
`abccorp-secure.driver`	公司前缀
`abcc-nj-secure.driver`	公司股票代码、位置
`abbcorp-nj-webserver.driver`	公司、位置、应用程序类型
`abc-nj-trading-webserver.driver`	公司、位置、组织、应用程序类型

■ 查看以下 Solaris Security Toolkit 文件是否适合您的系统。要定制这些文件，请复制原始文件、将副本重命名为 `user.init` 和 `user.run`，然后对副本的内容进行修改或添加。

`Drivers/user.init.SAMPLE`	用于定制全局参数。
`Drivers/user.run.SAMPLE`	用于定制全局功能。

■ 如要必要，可修改以下原始文件。*只有* 这些文件是允许您直接修改的 Solaris Security Toolkit 原始文件。

`Sysidcfg/*/sysidcfg`	用于 JumpStart 自动配置。
`Files/*`	用作文件模板并复制到系统。

注 – 请注意，如果您使用 `pkgrm` 命令删除了 `SUNWjass`，由其创建的 `user.init` 和 `user.run` 文件不会被删除。这种情况同样会发生在其他不包含在分发版中的、后来添加到 Solaris Security Toolkit 目录结构中的用户文件。同理，存在于 Solaris Security Toolkit 分发版本 Files 目录中的文件和 `sysidcfg` 文件将删除。

第 2 章

保护系统安全：方法论

本章提供保护系统安全的方法论。它提供了一个在使用 Solaris Security Toolkit 软件保护系统安全之前可以采用的过程。

本章包含以下主题：

- 第 15 页 “规划和准备”
- 第 25 页 “开发和执行 Solaris Security Toolkit 配置文件”
- 第 25 页 “安装软件”
- 第 27 页 “验证应用程序和服务功能”
- 第 27 页 “维护系统安全”

规划和准备

适当的规划是成功使用 Solaris Security Toolkit 软件来保护系统安全的关键。规划阶段将根据组织的安全策略和标准以及系统的应用程序和操作要求，为系统构建一个 Solaris Security Toolkit 配置文件。该阶段分为以下任务：

- 第 15 页 “考虑风险和收益”
- 第 17 页 “查看安全策略、标准和相关文档”
- 第 18 页 “确定应用程序和服务要求”

尽管未在本书中说明，该阶段的其他注意事项可能包括了解风险和收益，了解基础结构及其安全要求，考虑责任，日志以及对使用的审计。

考虑风险和收益

本节给出了在尝试保护系统安全之前必须准确理解的注意事项。仔细权衡风险与收益以确定适合您的组织的操作。

加强系统的安全性时，必须采取特殊的预防措施以确保在使用 Solaris Security Toolkit 软件之后，系统可以正常运行。此外，优化该过程来确保尽可能短的停机时间也非常重要。

注 – 在保护经过部署的系统的安全时，在某些情况下，重新构建系统是更加有效的方法，这样可在安装时加强系统的安全性，然后重新加载操作所需的全部软件。

---

1. 了解系统上的服务和应用程序的要求。

   在运行 Solaris Security Toolkit 软件之前，必须识别运行在系统上的服务和应用程序。必须列举出所有与服务和应用程序相关的从属性，以便 Solaris Security Toolkit 软件可以有效地进行调整。无法执行此操作可能会禁用或阻止必需的服务启动。因为由 Solaris Security Toolkit 软件所做的更改在大多数情况下都可以撤消，在安装之前开发正确的配置文件可以限制与 Solaris Security Toolkit 软件实现相关的潜在的停机时间。

2. 要考虑到系统必须脱机和重新引导的情况。

   要使由 Solaris Security Toolkit 软件所做的更改生效，必须重新引导系统。根据系统的重要程度、系统所提供的服务、维护窗口的可用性，组织可能在执行该软件时遇到不同的困难。在仔细权衡停机时间的花费与不增强安全性的风险之后，必须做出一个决定。

3. 系统可能要求多次重新引导以验证其功能性。

   在将更改应用到影响关键任务的实际环境之前，首先应在非生产系统中进行试验。但有时无法满足这样的要求，例如，没有足够的硬件和软件对目标环境进行有效的镜像。在 Solaris Security Toolkit 软件安装前后都必须进行测试。在系统加强安全性后，可能仍然存在未识别的、需要进行错误诊断的从属性。在大多数情况下，可以使用本章中介绍的技术非常快速地解决这些问题。如果在 Solaris Security Toolkit 软件安装后发现了功能问题，可能需要额外的平台重新引导来撤消 Solaris Security Toolkit 软件的影响或者对系统的配置做进一步的更改以支持并启用缺失的功能。

4. 平台安全性需要的不仅仅是加强和最小化。

   当考虑改进系统配置以增强其安全状态时，必须了解的是，平台加强和最小化只代表了可以用于和应该用于保护系统、服务和数据的一小部分措施。其他措施和控制不在本文的范围之内，但希望您考虑到与帐户管理、权限管理、文件系统和数据完整性、基于主机的访问控制、入侵检测、安全漏洞扫描和分析以及应用程序安全相关的问题。

5. 系统可能已经被利用或者具有可被利用的安全漏洞。

   正在加强安全性的平台可能已经被攻击者利用。Solaris Security Toolkit 软件的执行可能已经太晚而无法为已被利用的安全漏洞提供保护。在这种情况下，请重新安装系统，然后安装并使用 Solaris Security Toolkit 软件来增强安全性。

查看安全策略、标准和相关文档

保护系统安全的首要任务就是了解组织的相关安全策略、标准以及关于平台安全性的准则。使用这些文档来构成您的 Solaris Security Toolkit 配置文件的基础，因为这些文档提供了对于组织内的所有系统要遵循的要求和实践。如果您的组织没有这些文档，则开发它可以提高定制 Solaris Security Toolkit 软件的能力。

注 – 当查找这些文档时，请记住某些材料可能列于最佳做法或其他文档中。

有关安全策略的详细信息，请参阅 Sun BluePrints OnLine 文章 “Developing a Security Policy”。该文档可以使您对安全策略在组织安全性计划中发挥的作用有更进一步的了解。

以下两个实例说明了策略声明是如何直接影响 Solaris Security Toolkit 配置文件的配置方式的。

实例 1

- **策略** — 组织必须使用支持强用户身份验证和传输数据的加密的管理协议。
- **配置文件影响** — 不应该使用纯文本协议，例如 Telnet、 FTP、 SNMPv1 和其他协议。缺省情况下， Solaris Security Toolkit 禁用这些服务，因此不需要额外的配置。

注 – 可以使用扩展 （例如 Kerberos）将 Telnet 和 FTP 服务配置为支持更强的身份验证和加密。这些服务作为实例列出，虽然它们的缺省配置并不支持这些已添加的安全级别。

实例 2

策略 — 强制所有用户每 30 天更改一次他们的口令。

配置文件影响 — 可以将 Solaris Security Toolkit 软件配置为启用口令过期。缺省情况下，Solaris Security Toolkit 软件设定口令最长的过期时间为 8 周（56 天）。要符合该策略，必须更改 Solaris Security Toolkit 软件的配置文件。请参阅 *《Solaris Security Toolkit 4.1 Reference Manual》*。

尽管 Solaris Security Toolkit 软件在系统上运行时缺省情况下启用了口令过期，但这种更改并不会影响现有用户。要为现有用户启用口令过期，请在每个用户帐户上调用 `passwd`(1) 命令。

确定应用程序和服务要求

该任务确保在系统加强安全性后服务仍然保持正常工作。该任务包括以下步骤：

- 第 18 页 “确定应用程序和可用服务清单”
- 第 18 页 “确定服务要求”

确定应用程序和可用服务清单

清点应用程序、服务和可用功能或管理功能。该清单对于确定实际在系统上使用的软件是必需的。在很多情况下，系统会配置比使用的软件更多的软件，甚至配置有不支持业务功能的软件。

应该构建尽可能小的系统。也就是说，不应该安装不是支持业务功能所必需的软件。系统上不必要的软件应用程序会增加攻击者可以用于利用系统的机会的数量。此外，系统上安装更多的软件通常就等于必须要应用更多的修补程序。有关最小化 Solaris 操作系统的信息，请参阅 Sun BluePrints OnLine 文章 “Minimizing the Solaris Operating Environment for Security”。

当构建软件的清单时，请确保除包括位于系统上的应用程序之外，还要包括基础结构组件 （例如管理、监视以及备份软件）。

确定服务要求

在完成应用程序和服务清单后，确定加强安全性的过程是否会影响到组件的从属性。很多第三方应用程序不直接使用由 Solaris OS 提供的服务。对于直接使用 Solaris OS 提供的服务的应用程序，以下各节提供了有用的信息。

- 第 18 页 “共享库”
- 第 20 页 “配置文件”
- 第 21 页 “服务框架”

共享库

了解支持应用程序需要的库是非常重要的。在调试环境时这种知识最为有用，在准备要进行安全性加强的系统时也很有用。当系统状态未知时，收集尽可能多的信息以便准确地理解问题 （例如，软件相关性）。

有三种方法可以确定应用程序所使用的库，这取决于所安装的 Solaris OS 版本：

- 第一种方法用于文件系统对象 （例如，应用程序二进制）。
- 第二种方法用于分析正在运行的应用程序。
- 第三种方法用于在程序启动时对其进行跟踪。

实例：确定支持 DNS 服务器软件所需要的库。

要收集有关文件系统对象的信息，请使用 /usr/bin/ldd 命令。

代码实例 2-1 获得有关文件系统对象的信息

```
# ldd /usr/sbin/in.named
libresolv.so.2 => /usr/lib/libresolv.so.2
libsocket.so.1 => /usr/lib/libsocket.so.1
libnsl.so.1 =>    /usr/lib/libnsl.so.1
libc.so.1 =>      /usr/lib/libc.so.1
libdl.so.1 =>    /usr/lib/libdl.so.1
libmp.so.2 =>    /usr/lib/libmp.so.2
/usr/platform/SUNW,Ultra-5_10/lib/libc_psr.so.1
```

要从正在运行的进程中收集信息，请使用 /usr/proc/bin/pldd 命令 （在 Solaris OS 版本 8 和 9 中可用）。

代码实例 2-2 从正在运行的进程中收集信息

```
# pldd 20307
20307:  /usr/sbin/in.named
/usr/lib/libresolv.so.2
/usr/lib/libsocket.so.1
/usr/lib/libdhcpagent.so.1
/usr/lib/libdhcpagent.so.1
/usr/lib/libdhcpagent.so.1
/usr/lib/libmp.so.2
/usr/platform/sun4u/lib/libc_psr.so.1
/usr/lib/dns/dnssafe.so.1
/usr/lib/dns/cylink.so.1
```

除应用程序所链接的库之外， pldd 命令还显示由应用程序动态加载的共享库。也可以使用以下 truss 命令来收集该信息。

注 – 为简洁起见，将输出内容做了删节。

代码实例 2-3 确定动态加载的应用程序

```
# truss -f -topen,open64 /usr/sbin/in.named
20357:  open("/usr/lib/libresolv.so.2", O_RDONLY)       = 3
20357:  open("/usr/lib/libsocket.so.1", O_RDONLY)       = 3
20357:  open("/usr/lib/libnsl.so.1", O_RDONLY)          = 3
20357:  open("/usr/lib/libc.so.1", O_RDONLY)            = 3
20357:  open("/usr/lib/libdl.so.1", O_RDONLY)           = 3
20357:  open("/usr/lib/libmp.so.2", O_RDONLY)           = 3
20357:  open("/usr/lib/nss_files.so.1", O_RDONLY)       = 4
20357:  open("/usr/lib/nss_files.so.1", O_RDONLY)       = 4
```

代码实例 2-3 确定动态加载的应用程序 *（接上页）*

```
# truss -f -topen,open64 /usr/sbin/in.named
20357:  open("/usr/lib/dns/dnssafe.so.1", O_RDONLY)      = 4
20357:  open("/usr/lib/dns/cylink.so.1", O_RDONLY)       = 4
20357:  open("/usr/lib/dns/sparcv9/cylink.so.1", O_RDONLY) = 4
```

此输出的版本包含进程标识符、系统调用 （在本例中为 open）及其变量以及系统调用的返回值。使用返回值，可清晰地看到系统调用成功找到和打开共享库。

了解清楚共享库列表后，请使用以下命令来确定它们属于哪个 Solaris OS 软件包。

```
# grep '/usr/lib/dns/cylink.so.1' /var/sadm/install/contents
/usr/lib/dns/cylink.so.1 f none 0755 root bin 63532 24346 \
  1018126408 SUNWcsl
```

结果输出表示该共享库属于 SUNWcsl （核心，共享库）软件包。当执行平台最小化时该进程尤其有用，因为它有助于确定支持应用程序或服务所必需的软件包。

配置文件

另一种收集要求的方法就是通过配置文件。因为可以重命名或删除配置文件以禁用服务，该过程更直接地影响系统的安全性加强方式。有关详细信息，请参阅 *《Solaris Security Toolkit 4.1 Reference Manual》*。

要确定是否正在使用配置文件，请使用 truss 命令。

注 – 为简洁起见，将输出内容做了删节。

代码实例 2-4 确定是否正在使用配置文件

```
# truss -f -topen,open64 /usr/sbin/in.named 2>&1 | \
grep -v "/usr/lib/.*.so.*"
20384:  open("/etc/resolv.conf", O_RDONLY)               = 3
20384:  open("/dev/conslog", O_WRONLY)                   = 3
20384:  open("/usr/share/lib/zoneinfo/US/Eastern", O_RDONLY) = 4
20384:  open("/var/run/syslog_door", O_RDONLY)           = 4
20384:  open("/etc/nsswitch.conf", O_RDONLY)             = 4
20384:  open("/etc/services", O_RDONLY)                  = 4
20384:  open("/etc/protocols", O_RDONLY)                 = 4
20384:  open("/etc/named.conf", O_RDONLY)                = 4
20384:  open("named.ca", O_RDONLY)                       = 5
20384:  open("named.local", O_RDONLY)                    = 5
20384:  open("db.192.168.1", O_RDONLY)                   = 5
20384:  open("db.internal.net", O_RDONLY)                = 5
```

在本例中， DNS 服务使用了配置文件 （例如 /etc/named.conf）。正如前面的实例中介绍的，如果服务的返回值表明一个错误，则可能存在问题。仔细记录加强安全性前后的结果有助于加速整个验证过程。

服务框架

该类别包括框架或元服务，基于这些来构建更大、更复杂的应用程序。通常可以在该类别中找到的框架类型是命名服务 （例如， NIS、 NIS+ 和 LDAP）、身份验证服务 （例如， Kerberos 和 LDAP）以及由 RPC 工具所使用的服务 （例如端口映射器）。

并不能总是清楚地了解应用程序何时依赖于这些类型的服务。当需要特殊的调整来配置应用程序时 （例如将其添加到 Kerberos 领域），相关性是已知的。在某些情况下，应用程序相关性不需要添加任何任务，而且供应商可能不会记录实际的相关性。

这样的一个实例是 RPC 端口映射器。缺省情况下， Solaris Security Toolkit 软件禁用 RPC 端口映射器。该操作可能会引起依赖于该服务的其他服务中的异常行为。基于过去的经验，服务退出、挂起或者失败取决于处理异常情况的应用程序代码编写的好坏程度。要确定应用程序是否正在使用 RPC 端口映射器，请使用 rpcinfo 命令。例如：

代码实例 2-5 确定哪些应用程序使用 RPC

```
# rpcinfo -p
100000    3   tcp    111  rpcbind
100000    4   udp    111  rpcbind
100000    2   udp    111  rpcbind
100024    1   udp  32777  status
100024    1   tcp  32772  status
100133    1   udp  32777
100133    1   tcp  32772
100021    1   udp   4045  nlockmgr
100021    2   udp   4045  nlockmgr
100021    3   udp   4045  nlockmgr
100021    4   udp   4045  nlockmgr
100021    1   tcp   4045  nlockmgr
```

服务列中填充了来自 /etc/rpc 文件和/或已配置的命名服务（例如 LDAP）的信息。

如果该文件没有用于某个服务 （通常是第三方产品）的条目，该服务字段可能为空。这就使确定由其他应用程序注册的应用程序变得更加困难。

例如，考虑 rusers 命令。该命令依赖于 RPC 端口映射服务。如果 RPC 端口映射器没有运行， rusers 命令显示为挂起。程序最终会超时，并显示以下错误消息：

```
# rusers -a localhost

localhost: RPC: Rpcbind failure
```

出现此问题是因为该程序无法与服务进行通信。在从 /etc/init.d/rpc 启动 RPC 端口映射服务之后，该程序立即产生其结果。

作为另一个实例，请考虑 RPC 端口映射服务正在运行，而 rusers 服务没有配置为运行的情况。在这种情况下，就会产生完全不同的响应，并且可以相对简单地进行验证。

代码实例 2-6 验证 rusers 服务

```
# rusers -a localhost

localhost: RPC: Program not registered

# grep rusers /etc/rpc

rusersd         100002  rusers

# rpcinfo -p | grep rusers

<No output generated>
```

假设 rpcinfo 命令没有用于 rusers 服务的注册表，可以肯定的认为该服务没有配置为运行。这种假设是通过查看 /etc/inet/inetd.conf 中的服务条目进行验证的。

```
# grep rusers /etc/inet/inetd.conf

# rusersd/2-3    tli      rpc/datagram_v,circuit_v     wait root
/usr/lib/netsvc/rusers/rpc.rusersd     rpc.rusersd
```

该服务行开头的注释标记 (#) 表明已禁用 rusers 服务。要启用该服务，请取消注释行并将 SIGHUP 信号发送到 /usr/sbin/inetd 进程，如下所示。

```
# pkill -HUP inetd
```

注 – 仅 Solaris OS 版本 7 至 9 中有 pkill 命令。对于其他版本，请分别使用 ps 和 kill 命令来查找并通知该进程。

另一种确定应用程序是否使用 RPC 工具的方法是使用前面介绍的 ldd 命令。

代码实例 2-7 确定使用 RPC 的应用程序的备选方法

```
# ldd /usr/lib/netsvc/rusers/rpc.rusersd
libnsl.so.1 =>   /usr/lib/libnsl.so.1
librpcsvc.so.1 =>        /usr/lib/librpcsvc.so.1
libc.so.1 =>     /usr/lib/libc.so.1
libdl.so.1 =>    /usr/lib/libdl.so.1
libmp.so.2 =>    /usr/lib/libmp.so.2
/usr/platform/SUNW,Ultra-250/lib/libc_psr.so.1
```

librpcsvc.so.1 条目与文件名指明该服务依赖于 RPC 端口映射服务。

除 RPC 端口映射器外，应用程序可能依赖于其他常用的 OS 服务，例如 FTP、SNMP 或 NFS。可以使用类似的技术来调试这些服务并确定它们是否确实是支持业务功能所必需的。一种方法涉及使用 netstat 命令，如下所示。

```
# netstat -a | egrep "ESTABLISHED|TIME_WAIT"
```

该命令返回一个最近使用的服务列表，例如：

表 2-1 列出最近使用的服务

```
localhost.32827      localhost.32828      49152      0 49152      0
ESTABLISHED

localhost.35044      localhost.32784      49152      0 49152      0
ESTABLISHED

localhost.32784      localhost.35044      49152      0 49152      0
ESTABLISHED

localhost.35047      localhost.35046      49152      0 49152      0
ESTABLISHED

localhost.35046      localhost.35047      49152      0 49152      0
ESTABLISHED

filefly.ssh 192.168.0.3.2969    17615     1 50320     0 ESTABLISHED
```

在此实例中，正在使用多种服务，但是不清楚哪些服务或应用程序拥有哪些端口。可以通过使用 pfiles 命令 （在 Solaris OS 版本 8 和 9 上可用）对进程进行检查以收集该信息。

代码实例 2-8 确定哪些服务或应用程序拥有哪些端口

```
# for pid in `ps -aeo pid | grep -v PID`; do

> pfiles ${pid} | egrep "^${pid}:|sockname:"

> done
```

一个更显著、有效的确定这些从属性的方法就是使用 lsof （列出打开的文件）命令。该命令确定哪些进程正在使用哪些文件和端口。例如，要确定前面实例中的哪些进程使用端口 35047，请使用以下命令。

代码实例 2-9 确定哪些进程正在使用文件和端口

```
# ./lsof -i | grep 35047

ttsession   600 root 9u  IPv4 0x3000b4d47e8      0t1  TCP
localhost:35047->localhost:35046 (ESTABLISHED)

dtexec     5614 root 9u  IPv4 0x3000b4d59e8      0t0  TCP
localhost:35046->localhost:35047 (ESTABLISHED)
```

lsof 的输出表明端口 35047 正在用于 dtexec 和 ttsession 进程之间的通信。

使用 lsof 程序，您可能能够更迅速地确定系统之间或应用程序之间的需要使用文件系统或网络的从属性。在本节中阐述的几乎所有内容都可以使用 lsof 程序来获取。

要获得 lsof 程序，请从以下位置下载：

ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/

注 – 此处介绍的确定从属性的方法可能无法找出那些极少使用的从属性。除使用这些方法外，还请查看此文档和供应商提供的文档。

开发和执行 Solaris Security Toolkit 配置文件

在完成规划和准备阶段后，即可开发和执行安全性配置文件。安全性配置文件包括安全性加强驱动程序（例如 *name*-hardening.driver）、所有相关的驱动程序、脚本以及与执行现场相关的安全策略的文件。

定制 Solaris Security Toolkit 软件附带的一个安全性配置文件，或者自己进行开发。每个组织的策略、标准和应用程序都不会相同，即使只有细微的差别。

要定制一个安全性配置文件，请通过 finish 脚本、audit 脚本、环境变量、框架功能以及文件模板来调整该文件的操作。

有关详细信息，请参阅以下各章节：

- 有关定制软件的重要准则，请参阅第 1 章，第 11 页 “配置和定制 Solaris Security Toolkit 软件”。
- 有关其中创建安全性配置文件的方案的实例，请参阅第 7 章，第 85 页 “创建安全性配置文件”。
- 有关定制驱动程序的信息，请参阅 *《Solaris Security Toolkit 4.1 Reference Manual》*。

  根据需要，请参阅 *《Solaris Security Toolkit 4.1 Reference Manual》* 的其他相应章节以获得有关脚本、框架功能、环境变量和文件的信息。您可能要定制的两个关键环境变量是 JASS_FILES 和 JASS_SCRIPTS。

要跨越大多数平台强制执行标准，同时保证特定平台之间的差异，请使用嵌套或分层安全性配置文件技术。有关详细信息，请参阅 *《Solaris Security Toolkit 4.1 Reference Manual》*。比较结果配置文件与您组织的策略、标准和要求以确保不存在粗心大意或错误的更改。

安装软件

Solaris Security Toolkit 软件的安装对于经过部署的或正在安装的新系统来说是相同的。有关详细指导，请参阅第 3 章。

对于经过部署的系统，一些特定的例子可以使该过程更简单、迅速。这些例子的重点不在于加强安全性过程，而是在于安装前和安装后的任务。

执行安装前任务

在加强经过部署的系统的安全性之前，请考虑并计划两个主要任务 — 备份和验证。这两个任务有助于确定已部署系统的状态，并且有助于在加强系统安全性之前解决所有潜在的配置问题。

备份数据

该任务重点在于意外事故的规划。发生问题时，必须确保系统的配置和数据以某种形式进行了归档。必须备份系统，确保可以读取备份媒体并验证其内容可以进行恢复。在对系统配置进行任何重要更改之前，请采用此步骤。

验证系统稳定性

验证任务几乎与备份任务同等重要。在实现任何配置更改（例如，由加强安全性过程所做的更改）之前，验证过程可确保系统处于稳定工作状态。此验证过程涉及到在成功测试任何应用程序或服务之后的重新引导。尽管已经选择了定义好的测试和验收计划，文档也可能无法始终可用。如果情况确实如此，请根据系统的使用方式以合理的方式测试该系统。其目的在于确保实际运行的配置与所保存的配置相匹配。

当系统引导或应用程序启动时，查看所显示的任何错误消息或警告。如果无法纠正错误，请记录它们，以便在加强安全性过程中不会将其当作问题的潜在原因。当查看日志文件时，确保将系统、服务以及应用程序日志包括在内，例如：

- `/var/adm/messages`
- `/var/adm/sulog`
- `/var/log/syslog`
- `/var/cron/log`

重新启动系统时如果没有遇到错误或警告消息，或者没有遇到任何未知的错误或警告（所有已知的都已记录），则该任务完成。系统应该重新启动到一个已知并稳定的状态。如果在验证过程中发现系统正在运行的配置和存储的配置有所不同，请重新评估您组织的更改控制策略和过程以确定导致该情况的原因。

执行安装后的任务

安装后的任务是安装前的任务的延伸。目的在于确保安全性加强过程没有对系统或应用程序造成任何新的问题。该任务主要是通过查看系统和应用程序日志文件来完成的。在加强安全性以及随后的重新引导之后创建的日志文件应该与那些在对系统进行定型之前收集的日志文件相似。在某些情况下，由于只启动了较少的服务，因此消息可能会少一些。最重要的一点是，不应该出现新的错误或警告消息。

除查看日志文件外，还要测试功能，因为某些应用程序可能会发生故障但不生成日志条目。请参阅下节以获得详细的验证信息。

验证应用程序和服务功能

保护系统安全过程的最后任务会涉及到验证由系统提供的应用程序和服务是否能够正确地运行。该任务还验证安全性配置文件是否成功地满足了安全策略的要求。在加强安全性的平台启动之后彻底地执行该任务，以确保可检测到任何异常或问题并立即得到纠正。该任务分为两个子任务：验证安全性配置文件安装和验证应用程序和服务功能。

验证安全性配置文件安装

要验证 Solaris Security Toolkit 软件正确无误地安装了安全性配置文件，请查看安装日志文件。该文件安装在 `JASS_REPOSITORY/jass-install-log.txt` 中。

注 – 请参考该日志文件以了解 Solaris Security Toolkit 软件对系统所完成的操作。对于系统上的每个运行操作，都会有一个新的日志文件存储在一个基于运行操作起始时间的目录中。

除了要验证所安装的配置文件外，还要评估系统的安全配置。执行手动检查或使用工具使该过程自动化。

验证应用程序和服务功能

要对过程应用程序和服务进行验证，请执行已定义好的测试和验收计划。该计划将运行系统或应用程序的各个组件以确定它们处于可用和正常工作状态。如果没有这样的计划，则根据系统的使用方式以合理的方式测试该系统。其目的在于确保安全性加强安全性过程绝对不会影响应用程序或服务执行其功能的能力。

如果发现在加强系统安全性后，应用程序或服务出现故障，请查看应用程序日志文件来确定该问题。在很多情况下，可以使用 `truss` 命令来确定应用程序遇到的问题。在知道问题所在后，可以针对该问题并跟踪返回到 Solaris Security Toolkit 软件所做的更改。

维护系统安全

很多组织通常会犯的一个错误就是仅在安装过程中强调安全，然后就很少或不再重新考虑它。维护安全是一个实时进行的过程。必须定期查看和重新考虑系统安全。

维护一个安全的系统要求提高警惕，因为任何系统的缺省安全配置随着时间的推移都会逐渐地公开。例如，系统漏洞就会暴露出来。以下基本准则提供了一个概述：

- Solaris OS 修补程序可能在安装过程中安装其他软件包，并且会覆盖系统配置文件。确保在安装任何修补程序前后都要查看系统的安全状态。同样，保持系统具有最新的修补程序非常重要。

  Solaris Security Toolkit 软件可以协助您应用修补程序，因为它支持在系统上的重复运行操作，所以可以在安装修补程序后保护系统的安全。在安装任何修补程序后，以适当的驱动程序运行该软件以确保您的配置与已定义的安全策略保持一致。此外，请手动查看系统，因为正在使用的 Solaris Security Toolkit 软件的版本可能不支持由已安装的修补程序添加的新功能。

- 对系统进行实时监视以确保不会发生未经授权的行为。查看系统帐户、密码和访问模式，它们可以提供大量有关系统当前状态的信息。
- 部署和维护中央的 `syslog` 信息库以收集和解析 `syslog` 消息。可以通过收集和查看这些日志来获得有价值的信息。
- 制定一个全面的安全漏洞和审计策略来监视和维护系统配置。当在一段时间内维护系统处于安全的配置时，该要求尤为重要。
- 定期使用 Solaris Security Toolkit 软件的最新版本更新您的系统。

Solaris Security Toolkit 软件包括用作起点的缺省安全性配置文件。

第 3 章

安装和运行安全性软件

本章提供下载、安装、运行 Solaris Security Toolkit 软件及其他与安全相关的软件的指导。其中包含将环境配置为独立或 JumpStart 模式以及获得支持的指导。

请按照本节提供的指导和过程以安装、配置和执行软件。这些指导包括下载附加的安全性软件、帮助实例和准则。

虽然 Solaris Security Toolkit 软件是独立产品，然而当与下载的附加的安全性软件同时使用时最有效。该软件包括来自 SunSolve Online 的最新推荐的修补程序群集和安全性修补程序群集、Solaris OS 版本中未包含的 Secure Shell 软件、用于限制 Solaris OS 和第三方软件权限的权限和所有权修改软件，以及用于验证 Sun 文件和可执行文件完整性的完整性验证二进制文件。

本节包含以下任务：

- 第 29 页 “执行规划及安装前任务”
- 第 30 页 “从属性”
- 第 30 页 “确定使用的模式”
- 第 31 页 “下载安全性软件”
- 第 38 页 “定制安全性配置文件”
- 第 38 页 “安装和执行软件”
- 第 48 页 “验证系统修改”

执行规划及安装前任务

正确的规划是成功使用 Solaris Security Toolkit 软件以保护系统安全的关键。有关安装本软件前规划的详细信息，请参阅第 2 章。

如果要在已部署的系统上安装本软件，请参阅第 26 页 “执行安装前任务”，以了解有关在已部署的系统上执行安装前任务的信息。

从属性

Solaris Security Toolkit 4.1 软件具有以下从属性。

硬件从属性

有关所支持的 Solaris 操作系统版本，请参见第 11 页 “运行受支持的 Solaris OS 版本”。

软件从属性

Solaris Security Toolkit 4.1 软件从属于 SUNWloc 软件包。该软件包的缺失将导致 Solaris Security Toolkit 发生故障。

有关所支持的 System Managements Services (SMS) 软件版本的信息，请参见第 11 页 “运行受支持的 SMS 版本”。

确定使用的模式

在安装过程中或者在安装结束后马上加强系统安全性，可以减少系统在不安全状态下可能遭受攻击的时间。在使用 Solaris Security Toolkit 软件保护系统安全之前，请配置 Solaris Security Toolkit 软件，使其能在您的环境中正常运行。

Solaris Security Toolkit 软件具有模块化的框架。如果当前没有使用 JumpStart 产品，则 Solaris Security Toolkit 软件框架的灵活性使您能够有效地为以后使用 JumpStart 版本做准备。如果正在使用 JumpStart，则由于 Solaris Security Toolkit 软件能够集成到现有的 JumpStart 体系结构中，因此您可从中受益。

以下几节介绍了独立和 JumpStart 模式。

独立模式

在独立模式下，Solaris Security Toolkit 软件可直接从 Solaris OS shell 提示符下运行。这种模式使您可以在那些需要安全性修改或更新但还不能中断服务以完全重新安装 OS 的系统上使用 Solaris Security Toolkit 软件。然而如果可能的话，应完全重新安装系统以保护其安全。

在安装完修补程序后加强系统安全性时，独立模式更加有用。可以在系统上多次运行 Solaris Security Toolkit 软件而没有不良后果。修补程序会覆盖或修改 Solaris Security Toolkit 软件已经修改的文件；再次运行 Solaris Security Toolkit 软件，会重新执行由修补程序安装所撤消的任何安全性修改。

注 – 在生产环境中，将修补程序安装到现实环境之前，请在测试和开发环境中对其进行测试。

独立模式是尽可能快地加强已部署系统安全性的最佳选择之一。除了第 31 页 “下载安全性软件”提供的下载和安装指导中的步骤之外，不需要任何专门的步骤即可将 Solaris Security Toolkit 软件集成到不带 JumpStart 的体系结构中。

JumpStart 模式

JumpStart 技术是 Sun 的基于网络的 Solaris OS 安装机制，能够在安装过程中运行 Solaris Security Toolkit 脚本。本书假设读者熟悉 JumpStart 技术并具有可用的 JumpStart 环境。有关 JumpStart 技术的更多信息，请参阅 Sun BluePrints 书籍 *《JumpStart Technology: Effective Use in the Solaris Operating Environment》*。

在 JumpStart 环境中，将 `JASS_HOME_DIR`（用于 `tar` 文件下载）或 `/opt/SUNWjass`（用于 `pkg` 文件下载）中的 Solaris Security Toolkit 源代码复制到 JumpStart 服务器的主目录下。缺省路径是 JumpStart 服务器上的`/jumpstart`。`JASS_HOME_DIR` 将成为 Jumpstart 服务器上的主目录。

将 Solaris Security Toolkit 软件集成到 JumpStart 体系结构中只需要几个步骤。有关如何配置 JumpStart 服务器的指导，请参阅第 5 章。

下载安全性软件

加强系统安全性的第一步是将附加的安全性软件包下载到要保护的系统上。本节涵盖以下主题：

- 第 32 页 “下载 Solaris Security Toolkit 软件”
- 第 33 页 “下载推荐的修补程序群集软件”

- 第 35 页 “下载 FixModes 软件”
- 第 36 页 “下载 OpenSSH 软件”
- 第 37 页 “下载 MD5 软件”

注 – 本节讲到的软件中，Solaris Security Toolkit 软件、推荐的修补程序群集和安全性修补程序群集、FixModes 和 MD5 软件是必需的。可以用 Secure Shell（可从许多供应商获得）的商业版本来替代 OpenSSH。在所有系统上安装并使用 Secure Shell 产品。如果使用 Solaris 9 OS，请使用其附带的 Secure Shell 版本。

下载 Solaris Security Toolkit 软件

首先下载 Solaris Security Toolkit 软件，然后以独立模式将其安装在要使用 Solaris Security Toolkit 软件的服务器上，或者以JumpStart 模式安装在 JumpStart 服务器上。

注 – 以下指导中使用的文件名未涉及版本号。请始终从网站下载所提供的最新版本。

在本指南的剩余部分中，`JASS_HOME_DIR` 环境变量是指 Solaris Security Toolkit 软件的根目录。当从 `tar` 归档文件安装 Solaris Security Toolkit 软件时，将`JASS_HOME_DIR` 定义为路径，并包括 `jass-`*n.n* 如果在`/opt` 目录下安装`tar` 分发版本，则将 `JASS_HOME_DIR` 环境变量定义为 `/opt/jass-`*n.n*。

除了传统的压缩的 `tar` 归档格式外，Solaris Security Toolkit 软件还以 Solaris OS 软件包格式进行分发。相同的 软件包含在两种归档格式中。

选择最适合您的环境的格式。`pkg` 格式最适用于客户机，而`tar` 最适用于 JumpStart 系统和开发定制软件包。

以下几节提供下载和安装这两种不同归档类型的步骤。

▼ 下载 `tar` 版本

1. **下载软件分发文件 (**`jass-`*n.n*`.tar.Z`**)**。

   源文件位于以下网站：

   `http://www.sun.com/security/jass`

2. **使用** `zcat` **和** `tar` **命令将软件分发文件解压缩到服务器上的一个目录中，如下所示：**

```
# zcat jass-n.n.tar.Z | tar xvf -
```

   其中， *n.n* 是下载的最新版本。

执行该命令，在当前工作目录下创建 jass-*n.n* 子目录。该子目录包含所有 Solaris Security Toolkit 目录和相关文件。

▼ 下载 pkg 版本

1. **下载软件分发文件 (**SUNWjass-*n.n*.pkg.Z**)**。

   源文件位于：

   http://www.sun.com/security/jass

注 – 如果您在下载软件过程中遇到困难，请使用浏览器中集成的 “Save As” 选项。

---

2. **使用 uncompress 命令将软件分发文件解压缩到服务器的一个目录中：**

```
# uncompress SUNWjass-n.n.pkg.Z
```

3. **使用 pkgadd 命令将软件分发文件安装到服务器的一个目录中。**

```
# pkgadd -d SUNWjass-n.n.pkg SUNWjass
```

其中， *n.n* 是下载的最新版本。

执行此命令在 /opt 中创建 SUNWjass 目录。该子目录包含所有 Solaris Security Toolkit 目录和相关文件。

下载推荐的修补程序群集软件

修补程序由 Sun 发布，为 Solaris OS 提供对性能、稳定性、功能和安全性的修正。对于系统安全性最重要的是安装最新的修补程序群集。为确保系统上安装了 Solaris OS 推荐的修补程序群集和安全性修补程序群集，本节讲述了如何下载最新的修补程序群集。

注 – 在安装任何修补程序之前，请在非生产系统中或在预定的维护窗口中对其进行测试和评估。

▼ 下载推荐的修补程序群集软件

在安装修补程序群集之前，请查看每个修补程序的 README 文件和其他所提供的信息。信息通常包括安装修补程序群集之前需要知道的建议及帮助信息。

1. **从联机的 SunSolve 网站上下载最新的修补程序群集。**

   `http://sunsolve.sun.com`

2. **在左侧导航栏的顶部单击 “Patches”链接。**

3. **单击 “Recommended Patch Clusters”链接。**

   将显示许可证协议。

4. **在 “Recommended Solaris Patch Cluster”框中选择适当的 Solaris OS 版本。**

   在此实例中，选择 Solaris 8 OS。

5. **用相关的单选按钮选择最佳的下载选项 （HTTP 或 FTP），然后单击 “Go”。**

   在浏览器窗口中会显示一个 “Save As”对话框。

6. **将文件保存到本地。**

7. **将文件安全地移动到要加强安全性的系统中。**

   使用 `scp` （`scp(1)`– 安全复制 （远程复制程序））命令，或其他提供安全文件传输的方法。

   按如下所示使用 `scp` 命令：

```
# scp 8_Recommended.zip target01:
```

8. **将文件移动到`/opt/SUNWjass/Patches`目录下并解压缩。**

   例如：

代码实例 3-1 将一个修补程序文件移动到`/opt/SUNWjass/Patches` 目录

```
# cd /opt/SUNWjass/Patches
# mv /directory in which file was saved/8_Recommended.zip .
# unzip 8_Recommended.zip
Archive:     8_Recommended.zip
   creating: 8_Recommended/
  inflating: 8_Recommended/CLUSTER_README
  inflating: 8_Recommended/copyright
  inflating: 8_Recommended/install_cluster
[. . .]
```

在下载了附加安全性软件包并执行了 Solaris Security Toolkit 软件后，会自动安装修补程序群集软件。

注 – 如果没有将推荐的修补程序群集和安全性修补程序群集软件放到 /opt/SUNWjass/Patches目录下，则当执行 Solaris Security Toolkit 软件时会显示一条警告消息。在没有修补程序群集应用时可以安全地忽略这条消息，因为这种情形通常出现在新的操作系统版本中。

下载 FixModes 软件

FixModes 是一个限制缺省的 Solaris OS 目录和文件权限的软件包。限制这些权限能够有效地提高整体安全性。更多的限制性权限可以使恶意用户更难在系统中获得权限。

注 – 在 Solaris 9 OS 版本中，进行的更改主要是为了提高以前由 FixModes 软件修改的缺省的对象权限。然而， FixModes 软件仍然是必要的，因为第三方和另售的软件需要限制文件和目录权限。

▼ 下载 FixModes 软件

1. **从以下网址下载 FixModes 预编译的二进制文件：**

   http://www.sun.com/security/jass

   FixModes 软件是作为预编译和压缩的软件包版本文件分发的，其格式适用于 Solaris OS 系统。文件名是 SUNBEfixm.pkg.Z。

2. **使用 scp 命令或者其他提供安全文件传输的方法，将文件安全地移动到要加强安全性的系统中。**

   按如下所示使用 scp 命令：

```
# scp SUNBEfixm.pkg.Z target01:
```

3. **用以下命令将文件SUNBEfixm.pkg.Z 解压缩并保存在 /opt/SUNWjass/Packages 下的 Solaris Security Toolkit Packages 目录中。**

```
# uncompress SUNBEmd5.pkg.Z
# mv SUNBEmd5.pkg /opt/SUNWjass/Packages/
```

在下载了所有附加安全性软件包并执行了 Solaris Security Toolkit 软件后，会自动安装 FixModes 软件。

下载 OpenSSH 软件

在任何安全的环境下，需要将加密与强身份验证结合使用以保护用户交互式会话。最低限度,访问网络必须进行加密。

最常用于实行加密的工具是Secure Shell 软件 （Solaris OS 附带的版本、第三方商业版本或免费版本）。要实现 Solaris Security Toolkit 软件所进行的所有安全性修改，必须具有一个 Secure Shell 软件产品。

注 – 如果使用 Solaris 9 OS，请使用软件附带的 Secure Shell 版本。Secure Shell 的该版本集成了其他 Solaris OS 安全功能 （例如，基本安全模块 (BSM)）以及 Sun 的支持机构对该版本的支持。

第 xx 页 “相关资源”提供了有关从何处获得 Secure Shell 商业版本的信息。

Solaris Security Toolkit 软件禁用了系统中所有未加密的用户交互式服务和守护进程，特别是守护进程 （例如， `in.telnetd`、 `in.ftpd`、 `in.rshd` 和 `in.rlogind`）。

Secure Shell 使您可以使用 Telnet 和 FTP 访问系统。

▼ 下载 OpenSSH 软件

注 – 如果服务器当前运行 Solaris 9 OS，则可以使用附带的 Secure Shell 软件并跳过本节中的 OpenSSH 安装步骤。

● **获取以下 Sun BluePrints OnLine 文章，并使用文章中的指导来下载软件。**

Sun BluePrints OnLine 上的一篇有关如何编译与部署 OpenSSH 的名为 “Building and Deploying OpenSSH on the Solaris Operating Environment”的文章可以在下列网址获得：

`http://www.sun.com/blueprints`

或者从书店购买 Sun BluePrints 出版物 *《Secure Shell in the Enterprise》*。

在下载了所有附加安全性软件包并执行了 Solaris Security Toolkit 软件后，会自动安装 OpenSSH 软件。

注意 – 请不要在需要加强安全性的系统上编译 OpenSSH，也不要在需要加强安全性的系统上安装编译器。使用单独的 Solaris OS 系统 — 运行相同的 Solaris OS 版本、体系结构和模式 （例如， Solaris 8 OS、 Sun4U (sun4u) 和 64位） — 编译 OpenSSH。如果要使用 SSH 的商业版本，则不需要任何编译程序。目的是限制潜在入侵者对编译器的使用。然而，对于本地系统编译器安装的限制并不能对抗蓄意攻击者，因为他们仍然可以安装预编译的工具。

下载 MD5 软件

MD5 软件在要加强安全性的系统上生成 MD5 数字指纹。生成数字指纹后，将其与 Sun 公司发布的正确数字指纹相对比，以检测被未授权用户更改或*特洛伊式更改*（隐藏在看起来安全的事物中）的系统二进制文件。通过修改系统二进制文件，攻击者可利用后门访问系统；他们隐藏了自己的存在并使系统在不稳定的状态下运行。

▼ 下载 MD5 软件

1. **从以下网址下载 MD5 二进制文件：**

   `http://www.sun.com/security/jass`

   MD5 程序以压缩的软件包版本文件形式分发。

2. **使用 `scp` 命令或其他提供安全文件传输的方法，将文件 `SUNBEmd5.pkg.Z` 安全地移动到要加强安全性的系统中。**

   按如下所示使用 `scp` 命令：

```
# scp SUNBEmd5.pkg.Z target01:
```

3. **使用与以下相似的命令，将文件解压缩并移动到 `/opt/SUNWjass/Packages`下的 Solaris Security Toolkit `Packages` 目录中。**

```
# uncompress SUNBEmd5.pkg.Z
# mv SUNBEmd5.pkg /opt/SUNWjass/Packages/
```

将 MD5 软件保存到`/opt/SUNWjass/Packages` 目录中后，执行 Solaris Security Toolkit 软件以安装 MD5 软件。

在 MD5 二进制文件安装完毕后，通过 Solaris 指纹数据库可以使用它们验证系统上可执行文件的完整性。有关 Solaris 指纹数据库的更多信息，可以从 Sun BluePrints OnLine 上名为 “The Solaris Fingerprint Database — A Security Tool for Solaris Software and Files”的文章中获得。

4. **（可选）从位于以下位置的 Sun BluePrint 网站下载并安装 Solaris Fingerprint Database Companion 和 Solaris Fingerprint Database Sidekick 软件：**

   `http://www.sun.com/blueprints/tools`

   安装这些可选工具并与 MD5 软件一起使用。这些工具简化了通过 MD5 校验和数据库验证系统二进制文件的过程。需要经常使用这些工具来验证安全的系统上 Solaris OS 二进制和文件的完整性。

   这些工具及相关下载指导在 Sun BluePrints OnLine 上名为 “The Solaris Fingerprint Database — A Security Tool for Solaris Software and Files”的文章中可以找到。

   需要验证下载的安全性工具的完整性。在安装和运行 Solaris Security Toolkit 软件及附加安全性软件前，请使用 MD5 校验和验证其完整性。在 Solaris Security Toolkit 下载页面上，可以获得用于该用途的 MD5 校验和。

定制安全性配置文件

很多安全性配置文件模板是作为驱动程序包含在 Solaris Security Toolkit 软件分发版本中的。正如前面章节所述，缺省的安全性配置文件和由这些驱动程序进行的更改很可能并不适用于您的系统。由驱动程序实现的安全性配置文件禁用了那些不需要的服务，并启用了缺省情况下禁用的可选的安全功能。

在运行 Solaris Security Toolkit 软件之前，请查看并定制环境的缺省安全性配置文件，或者开发新的文件。Sun BluePrints 书籍 *《Securing Systems with the Sun Security Toolkit》*提供了定制安全性配置文件的技巧和准则。

安装和执行软件

在执行 Solaris Security Toolkit 软件前完成以下预备任务是很重要的。运行 Solaris Security Toolkit 软件时，会自动完成大部分加强安全性工作。

- 在要加强安全性的系统上或在 JumpStart 服务器上下载附加安全性软件和 Solaris Security Toolkit 软件。请参阅第 31 页 “下载安全性软件”。
- 将系统配置为独立或 JumpStart 模式。请参阅第 30 页 “确定使用的模式”。
- 如果可行，请为系统定制 Solaris Security Toolkit 软件。
- 在安装和运行 Solaris Security Toolkit 软件及附加安全性软件前，需要使用 MD5 校验和验证其完整性。

可以直接从命令行或 JumpStart 服务器上执行 Solaris Security Toolkit 软件。

有关命令行选项及其他关于执行软件的信息，请参阅以下之一：

■ 第 39 页 “在独立模式下执行软件”
■ 第 47 页 “在 JumpStart 模式下执行软件”

在独立模式下执行软件

代码实例 3-2 显示独立模式下命令行使用的样例。

代码实例 3-2 独立模式下命令行使用的样例

```
# ./jass-execute -h

usage:

To apply this Toolkit to a system, using the syntax:
   jass-execute [-r root_directory -p os_version ]
      [ -q | -o output_file ] [ -m e-mail_address ]
      [ -V [3|4] ] [ -d ] driver

To undo a previous application of the Toolkit from a system:
   jass-execute -u [ -b | -f | -k ] [ -q | -o output_file ]
      [ -m e-mail_address ] [ -V [3|4] ]

To audit a system against a pre-defined profile:
   jass-execute -a driver [ -V [0-4] ] [ -q | -o output_file ]
      [ -m e-mail_address ]

To display the history of Toolkit applications on a system:
   jass-execute -H

To display the last application of the Toolkit on a system:
   jass-execute -l

To display this help message:
   jass-execute -h
   jass-execute -?

To display version information for this program:
   jass-execute -v

#
```

表 3-1 列出了可用的命令行选项并逐个进行说明。

表 3-1 将命令行选项与 jass-execute 结合使用

选项	说明
-a	确定系统与其安全性配置文件是否兼容。
-b	与 -u 选项结合使用。备份自最后一次加强安全性运行操作以来手动更改的所有文件，然后将系统恢复至其原始状态。
-d	指定在独立模式下运行的驱动程序。
-f	与 -u 选项结合使用。在不询问是否有例外的情况下，取消加强安全性运行操作所作的更改，在执行加强安全性操作后进行手动更改的文件也不例外。
-h	显示 jass-execute 帮助消息，提供了可用选项的概述。
-H	提供一种确定 Solaris Security Toolkit 软件在系统中已运行多少次的简单机制。
-k	与 -u 选项结合使用。保持自最后一次执行加强安全性运行操作以来所作的手动更改。
-l	显示系统上 Solaris Security Toolkit 的最新应用程序。
-m	将输出发送到一个电子邮件地址。
-o	将输出定向到一个文件。
-p	与 -r *root_directory* 选项结合使用。 指定 Solaris 操作系统的 OS 版本。格式与 uname -r 相同。
-q	防止将输出显示到屏幕上。又称为静止选项。
-r	必须与 -p *os_version*结合使用。 指定在 jass-execute 运行时使用的根目录。缺省情况下， root 文件系统为 /。此根目录由 Solaris Security Toolkit (JASS) 环境变量 JASS_ROOT_DIR 定义。可通过 /保护 Solaris OS 的安全。例如，如果您希望保护一个单独 OS 目录 （临时安装在 r /mnt 中）的安全，那么可以使用 -r 选项来指定 /mnt。
-u	发生异常时，运行带有交互式提示 （询问要采取何种措施）的撤销选项。不可与 -d、 -a、 -h、 -l 或 -H 选项结合使用。
-v	显示本程序的版本信息。
-V	指定消息输出的详细级别。
-?	显示 jass-execute 帮助消息，其中概述了可用的选项。

有关在独立模式下可与 jass-execute 命令一同使用的选项的详细信息，请参阅以下几节：

- 第 42 页 “审计选项”
- 第 42 页 “显示帮助选项”

- 第 43 页 “驱动程序选项”
- 第 44 页 “电子邮件通知选项”
- 第 45 页 “执行历史记录选项”
- 第 45 页 “最新执行选项”
- 第 45 页 “输出文件选项”
- 第 46 页 “静止输出选项”
- 第 46 页 “根目录选项”
- 第 47 页 “撤消选项”

有关可用的驱动程序的完整列表，请参见 Drivers 目录。新的软件版本可能包含额外的驱动程序。

▼ 在独立模式下执行软件

1. **执行**secure.driver **（或产品的专用脚本，例如** sunfire_15k_sc-secure.driver**），如下所示。**

代码实例 3-3 在独立模式下执行软件

```
# cd /opt/SUNWjass
# ./jass-execute -d secure.driver

[NOTE] The following prompt can be disabled by setting
JASS_NOVICE_USER to 0.
[WARN] Depending on how the Solaris Security Toolkit is configured,
it is both possible and likely that by default all remote shell
and file transfer access to this system will be disabled upon
reboot effectively locking out any user without console access to
the system.

Are you sure that you want to continue? (YES/NO) [NO]
y

[NOTE] Executing driver, secure.driver

================================================================
secure.driver: Driver started.
================================================================

================================================================
Solaris Security Toolkit Version: 4.1.0
Node name:                        ufudu
Host ID:                          8085816e
Host address:                     10.8.31.115
MAC address:                      8:0:20:85:81:6e
OS version:                       5.9
```

代码实例 3-3 在独立模式下执行软件 *（接上页）*

```
Date:                                  Tue May 4 16:28:24 EST 2004
================================================================
[...]
```

有关可用的驱动程序的完整列表，请参见 Drivers 目录。新的软件版本可能包含额外的驱动程序。

2. **在系统上运行 Solaris Security Toolkit 软件后，请重新引导系统以执行更改。**

   在加强安全性过程中，需要对客户机的配置做大量修改。这些更改可能包括禁用服务启动脚本，禁用服务选项和通过修补程序安装新的二进制文件或库。只有客户机重新启动后，这些更改才可能生效。

3. **重新引导系统后，请检查更改的正确性和完整性。**

   请参阅第 48 页 “验证系统修改”。

4. **如果出现任何错误，请进行修正并再次在独立模式下运行 Solaris Security Toolkit 软件。**

审计选项

通过 `-a` 选项， Solaris Security Toolkit 软件能够进行审计运行，以确定系统是否与其安全性配置文件相兼容。此运行不仅验证系统文件修改是否仍然起作用，还验证之前禁用的过程是否在运行或者删除的软件包是否已重新安装。有关此功能的更多信息，请参阅第 6 章。

审计系统与安全性配置文件的用法实例：

```
# jass-execute -a driver [ -V [0-4] ] [ -q | -o output-file ]
[ -m email-address ]
```

显示帮助选项

`-h` 选项显示 `jass-execute` 帮助信息，提供了可用选项的概述。

`-h` 选项产生的输出与以下内容相似：

代码实例 3-4 `-h` 选项输出样例

```
# ./jass-execute -h
To apply this Toolkit to a system, using the syntax:
   jass-execute [-r root_directory -p os_version ]
      [ -q | -o output_file ] [ -m e-mail_address ]
      [ -V [3|4] ] [ -d ] driver
```

代码实例 3-4 -h 选项输出样例 *（接上页）*

```
To undo a previous application of the Toolkit from a system:
   jass-execute -u [ -b | -f | -k ] [ -q | -o output_file ]
      [ -m e-mail_address ] [ -V [3|4] ]

To audit a system against a pre-defined profile:
   jass-execute -a driver [ -V [0-4] ] [ -q | -o output_file ]
      [ -m e-mail_address ]

To display the history of Toolkit applications on a system:
   jass-execute -H

To display the last application of the Toolkit on a system:
   jass-execute -l

To display this help message:
   jass-execute -h
   jass-execute -?

To display version information for this program:
   jass-execute -v

Note that just the driver name should be specified when using the
'-d' or '-a' options. A path need not be specified as the script
is assumed to exist in the Drivers directory.

The '-u' undo option is mutually exclusive with the '-d' and '-a'
options. The default undo behavior is to ask the user what to do if
a file to be restored has been modified as the checksum is
incorrect.

The -u option can be combined with the '-k', '-b', or '-f' to
override the default interactive behavior. The use of one of these
options is required when run in quiet mode ('-q').

The '-k' option can be used to always keep the current file and
backup if checksum is incorrect. The 'b' can be used to backup the
current file and restore original if the checksum is incorrect.
The 'f' option will always overwrite the original if the checksum
is incorrect, without saving the modified original.
```

驱动程序选项

-d *driver* 选项指定在独立模式下运行的驱动程序。

必须用 -d 选项指定驱动程序。Solaris Security Toolkit 软件将 Drivers/ 附加在所添加脚本的名称之前。因此只需在命令行中输入脚本名称。

注 – 不能将 -d 选项与 -u、 -H、 -h 或 -a 选项一同使用。

使用了 -d *driver* 选项的 jass-execute 加强安全性运行操作产生的输出类似于以下内容：

代码实例 3-5 -d *driver* 选项输出样例

```
# ./jass-execute -d secure.driver
[...]
[NOTE] Executing driver, secure.driver

============================================================
secure.driver: Driver started.
============================================================

============================================================
Solaris Security Toolkit Version: 4.1.0
Node name:                        ufudu
Host ID:                          8085816e
Host address:                     10.8.31.115
MAC address:                      8:0:20:85:81:6e
OS version:                       5.9
Date:                             Tue Oct 4 16:28:24 EST 2004
============================================================
[...]
```

电子邮件通知选项

-m *email-address* 选项提供了一种机制，通过该机制， Solaris Security Toolkit 软件可在运行完成后将独立加强安全性运行操作和撤消运行操作的输出用电子邮件发送出去。使用其他选项除了可在系统上生成日志外，还可生成电子邮件报告。

使用电子邮件选项调用 sunfire_15k_sc-config.driver 的 Solaris Security Toolkit 运行类似于以下内容：

```
# ./jass-execute -m root -d sunfire_15k_sc-config.driver
[...]
```

执行历史记录选项

-H 选项提供一种确定 Solaris Security Toolkit 软件在系统中已运行多少次的简单机制。该选项将列出所有的运行，无论其撤消与否。

-H 选项产生的输出类似于以下内容：

代码实例 3-6 -H 选项输出样例

```
# ./jass-execute -H
Note: This information is only applicable for applications of
      the Solaris Security Toolkit starting with version 0.3.

The following is a listing of the applications of the Solaris
Security Toolkit on this system. This list is provided in
reverse chronological order:

1.   June 31, 2004 at 12:20:19 (20040631122019) (UNDONE)
2.   June 31, 2004 at 12:10:29 (20040631121029)
3.   June 31, 2004 at 12:04:15 (20040631120415)
```

此输出表明， Solaris Security Toolkit 软件已在系统上运行了三次，且最后一次运行被撤消。

最新执行选项

-l 选项提供了确定最近一次运行的机制。这通常是-H 选项列出的最后一次运行。

-l 选项产生的输出类似于以下内容：

代码实例 3-7 -l 选项输出样例

```
# ./jass-execute -l

Note: This information is only applicable for applications of
      the Solaris Security Toolkit starting with version 4.1.0.

The last application of the Solaris Security Toolkit was:

1.   June 31, 2004 at 12:20:19 (20040631122019) (UNDONE)
```

输出文件选项

-o *output-file* 选项将 jass-execute 的控制台输出重定向到一个单独的文件 (*output-file*)。

此选项不影响 JASS_REPOSITORY 目录内的日志。此选项对于在较慢的终端连接上运行特别有帮助，因为 Solaris Security Toolkit 运行会产生大量输出。

此选项可与 -d、 -u 或 -a 选项一起使用。

-o 选项产生的输出类似于以下内容：

代码实例 3-8 -o 选项输出样例

```
# ./jass-execute -o jass-output.txt -d secure.driver
[NOTE] Executing driver, secure.driver
[NOTE] Recording output to jass-output.txt
```

静止输出选项

在加强安全性运行操作中， -q 选项可禁止 Solaris Security Toolkit 输出到标准输入输出 (stdio) 流。

此选项不影响 JASS_REPOSITORY 目录内的日志。与 -o 选项类似，此选项特别有助于通过 cron （时钟守护进程）作业或较慢的网络连接来运行 Solaris Security Toolkit 软件。

此选项可与 -d、 -u 或 -a 选项一起使用。

-q 选项产生的输出类似于以下内容：

代码实例 3-9 -q 选项输出样例

```
# ./jass-execute -q -d secure.driver
[NOTE] Executing driver, secure.driver
```

根目录选项

-r *root-directory* 选项用于在运行 jass-execute 时指定根目录。使用 -r 选项还需要使用 -p 选项指定平台 (OS) 版本。-p 选项的格式与 uname -r 产生的格式相同。

缺省情况下，文件系统根目录是 /。此根目录由 Solaris Security Toolkit 环境变量 JASS_ROOT_DIR 进行定义。可通过/ 访问要保护的 Solaris OS。例如，如果要保护一个独立的 OS 目录，请临时在 /mnt下装入，然后使用 -r 选项指定 /mnt。则会将所有脚本应用到该 OS 映像。

撤消选项

通过 -u 选项， Solaris Security Toolkit 软件可以在加强安全性过程中撤消系统修改。每个 finish 脚本都可以通过 -u 选项来撤消。此外， Solaris Security Toolkit 的撤消功能与每次运行时所产生的校验和紧密相关。有关此功能的更多信息，请参阅第 4 章。

撤消命令的命令行使用实例：

```
# jass-execute -u [ -b | -f | -k ] [ -q | -o output_file ]
        [ -m e-mail_address ] [ -V [3|4] ]
```

在 JumpStart 模式下执行软件

JumpStart 模式由插入到 JumpStart 服务器上 rules 文件中的 Solaris Security Toolkit 驱动程序控制。

如果未将环境配置为使用 JumpStart 模式，请参阅第 5 章。

有关 JumpStart 技术的更多信息，请参阅 Sun BluePrints 书籍 《*JumpStart Technology: Effective Use in the Solaris Operating Environment*》。

▼ 在 JumpStart 模式下执行软件

要在 JumpStart 模式下执行 Solaris Security Toolkit 软件，必须将其集成到 JumpStart 环境中并作为和 JumpStart 安装相关的 finish 脚本的一部分进行调用。有关如何将 Solaris Security Toolkit 软件集成到系统中的信息，请参阅第 5 章。

1. **完成对驱动程序的所有必要修改后，请使用 JumpStart 基础结构安装客户机。**

   在客户机的 ok 提示符中使用以下命令完成该任务。

   ```
   ok> boot net - install
   ```

   一旦安装完成， JumpStart 软件就会重新引导系统。

   系统的配置应该正确。在加强安全性过程中，需要对客户机的配置做大量修改。这些修改可能包括禁用服务启动脚本，禁用服务选项和通过修补程序安装新的二进制文件或库。只有客户机重新启动后，这些更改才可能生效。

2. **重新引导系统后，检查更改的正确性和完整性。**

   请参阅第 48 页 “验证系统修改”。

3. **如果出现错误，修正它们并重新安装客户机的 OS。**

验证系统修改

重新引导系统后，按照以下几节所述对修改的正确性和完整性进行验证。

对服务执行 QA 检查

保证系统安全的重大挑战之一是，确定必须使哪些 OS 服务处于启用状态以使系统正常运行。由于要直接使用 Solaris OS 服务 （例如，用于登录系统的 Secure Shell），因此可能需要它们。或者间接使用它们，例如使用第三方软件管理工具的图形用户界面的远程过程调用 (RPC) 守护进程。

在运行 Solaris Security Toolkit 软件之前，应该确定这些要求中的大部分。（请参阅第 18 页 “确定应用程序和服务要求”）。然而，唯一确定的机制是安装并保护系统安全，然后通过质量保证 (QA) 测试对其所要求的功能进行完全测试。在加强系统安全性后，要对所有新系统正确地执行 QA 计划。类似的，对于要加强安全性的经过部署的系统，需要进行完全的测试以确保其具备了所有要求的和所期望的功能。

如果 QA 过程发现了任何差异，请执行以下步骤：

1. 根据第 2 章中的准则，确定问题出现区域。
2. 验证应用程序在已修改的配置中运行。
3. 撤消 Solaris Security Toolkit 运行。
4. 根据问题的解决方案，修改安全性配置文件 （驱动程序）。
5. 再次运行 Solaris Security Toolkit 软件。

最终结果应为一个安全性配置文件，它可在系统上运行而不对任何所需的功能产生负面影响。

对配置进行安全性评估

在验证系统可执行所有需要的功能时，还要对安全性配置做出评估，以确定系统是否达到需要的安全级别。根据在系统上执行的加强安全性及最小化系统操作，这种评估可能涉及不同的方面。

至少应该从以下几方面检查系统的配置：

- 确保安装了所有适当的安全性修补程序和推荐的修补程序。
- 确定当前仅运行适当并且必需的进程，并且以适当的参数运行。
- 确定当前仅运行必需的守护进程，并且以适当的参数运行。

- 进行本地检查（例如，`netstat -a`）和使用扫描器（例如 Nmap，它可以确定网络接口上可用的端口）进行远程检查，以确定系统中仅开放了必需的端口。
- 如果系统是最小化的，请确保只安装了必需的 Solaris OS 软件包。

对于新构建的并已保护安全的系统，至少应该考虑到这种检查。在加强传统系统的安全性时，需要检查底层的 OS 以确定是否执行了未授权的修改。对于这种完整性检查，最好在只读模式下装入系统的文件系统，然后从一个已知 OS 实例上运行完整性检查软件。在 Sun BluePrints OnLine 上名为 “The Solaris Fingerprint Database — A Security Tool for Solaris Software and Files”的文章所介绍的工具在这些情况下非常有用。

验证安全性配置文件

在保护系统安全并且已经验证了所需的服务和功能后，请使用审计功能以确保正确且完全地应用了安全性配置文件。此任务非常关键，原因有两个。第一，要确保按照要求加强了系统的安全性。第二，要确保为系统定义的安全性配置文件正确地反映在了 Solaris Security Toolkit 配置中。由于配置信息用于在系统的整个部署生命周期中维护系统的安全性配置文件，因此这种检查十分重要。

有关审计功能的更多信息，请参阅第 6 章。

执行安装后的任务

如果在一台经过部署的系统上安装软件，请参阅第 26 页 “执行安装后的任务”，以了解有关在经过部署的系统上执行安装后任务的信息。

第 4 章

取消系统更改

本章提供的信息和步骤可用于取消 （撤消） Solaris Security Toolkit 软件在加强安全性运行过程中所做的更改。此选项提供一种自动机制，通过该机制可使系统返回到 Solaris Security Toolkit 加强安全性操作或一系列操作之前的状态。

本章包含以下主题：

- 第 51 页 “了解如何记录并取消更改”
- 第 52 页 “撤消系统更改的要求”
- 第 52 页 “定制脚本以撤消更改”
- 第 53 页 “检查手动更改的文件”
- 第 54 页 “使用带有撤消功能的选项”
- 第 57 页 “撤消系统更改”

了解如何记录并取消更改

每次 Solaris Security Toolkit 加强安全性操作都在 `JASS_REPOSITORY` 下创建一个运行目录。这些目录的名称基于运行的日期和时间。除了在屏幕上显示输出之外，Solaris Security Toolkit 软件还会在目录下创建一系列文件以跟踪更改并记录其操作。

存储在目录中的文件跟踪对系统进行的修改，并使撤消功能生效。

注意 – 管理员不应更改 `JASS_REPOSITORY` 中的文件内容。

当在 JumpStart 或者独立模式下使用 Solaris Security Toolkit 软件加强系统的安全性时，软件将系统更改记录在 `JASS_REPOSITORY/jass-manifest.txt` 文件中。此文件列出了撤消功能用于取消更改的操作。该文件包含有关通过 Solaris Security Toolkit 软件加强安全性操作的信息，包括创建、复制、移动或删除的文件。另外，此文件还可包含取消更复杂的更改 （例如软件包安装）时所需的条目 （标准条目和定制条目）。每次加强安全性操作都会创建一个单独的 `jass-manifest.txt` 文件。

注 – Solaris Security Toolkit 软件的撤消功能仅能取消那些在清单文件中具有相应条目的更改。

撤消操作会仔细检查那些在 Solaris Security Toolkit 运行过程中生成并保存在JASS_REPOSITORY 中的清单文件。并将备份文件恢复到它们原来的位置。如果文件没有备份，则无法使用撤消功能。

撤消 Solaris Security Toolkit 操作并不会删除相关的目录。而是在 JASS_REPOSITORY 目录下创建两个文件：jass-undo-log.txt 和 reverse-jass-manifest.txt。随后再次执行 jass-execute -u 时，不会列出已撤消的操作。加强安全性操作只能撤消一次。

撤消系统更改的要求

在使用 Solaris Security Toolkit 软件的撤消功能时，请注意以下限制和要求。

- 在 Solaris Security Toolkit 版本 0.3 至 4.1 中，可以在独立模式或者 JumpStart 模式下对已开始进行的运行操作使用撤消功能。然而，仅可以在独立模式下撤消更改。在 JumpStart 安装过程中不能使用撤消功能。
- 如果选择了 Solaris Security Toolkit 选项，不创建备份文件；则无论在 JumpStart 模式还是在独立模式下，撤消功能均不可用。将 JASS_SAVE_BACKUP 参数设为 0，可禁止创建备份文件副本。
- 运行操作只能撤消一次。
- 如果开发了一个新的没有使用 Solaris Security Toolkit 框架功能的 finish 脚本，则必须创建一个与之匹配的 audit 脚本并使用 add_to_manifest 功能向清单文件中添加条目。否则， Solaris Security Toolkit 无法了解您定制的开发。
- 在任何情况下都不要修改 JASS_REPOSITORY 目录的内容。修改文件会破坏文件内容，且当使用撤消功能时，会引起不可预知的错误或系统崩溃。

定制脚本以撤消更改

Solaris Security Toolkit 框架为设计和构建 finish 脚本提供了灵活性。该框架允许扩展 Solaris Security Toolkit 软件的功能以更好地满足组织的要求，同时也能帮助您在配置的生命周期内改善对系统配置的管理。

当定制脚本时，了解所采取的操作如何影响撤消功能是非常重要的。为了简化定制脚本，助手功能可对清单文件做适当的更改。（撤消功能根据清单文件的内容取消加强系统安全性运行操作。）在多数情况下，这些助手功能提供了为您机构定制脚本所需的操作。

有关助手功能的列表和使用它们的信息，请参阅 *《Solaris Security Toolkit 4.1 Reference Manual》*。使用这些助手功能代替它们对应的系统命令，从而使撤消运行操作能够参考清单文件中的相关条目。

在某些情况下，要执行的功能可能不具有助手功能。在这些情况下，请使用名为 `add_to_manifest` 的特殊功能。使用此功能可将条目手动插入到清单文件中，而不必调用助手功能。请慎重使用此特殊功能，以保护系统和 Solaris Security Toolkit 信息库的完整性。例如，可使用此特殊功能添加非 Sun 的 `pkg` 格式的软件包。在此实例中，需要通知撤消功能如何删除在加强安全性运行操作过程中以其他格式添加的软件包。

利用助手功能和特殊的 `add_to_manifest` 功能，Solaris Security Toolkit 软件提供了一种简单灵活的方法，可定制脚本，并可撤消运行操作对系统进行的更改。

如果更改 finish 脚本时，没有使用这些功能，则 Solaris Security Toolkit 无法了解已经发生的更改。因此，必须手动撤消清单文件没有相关记录的任何更改。

在另一个实例中，在更改系统中的文件之前，应首先保存文件的原始版本。在 Solaris Security Toolkit 软件环境外，用户通常执行 `/usr/bin/cp` 命令以完成该任务。然而，在 Solaris Security Toolkit 软件环境下，如果直接使用此命令， Solaris Security Toolkit 软件无从了解需要创建一个清单条目。因此，请使用 `backup_file` 助手功能，而不要使用 `cp` 命令。该功能以 `JASS_SUFFIX` 为后缀保存了原始文件的副本，并添加了一个清单条目以通知 Solaris Security Toolkit 软件已复制了文件的副本。同时此功能还使文件校验和开始计算。文件校验和由撤消功能以及 `jass-check-sum` 命令使用。

检查手动更改的文件

虽然使用 `jass-execute -u` 命令可以自动检查在加强安全性运行操作后手动更改的文件，但有时使用 `jass-check-sum` 命令列出并检查已经更改的文件也很有帮助。

此命令可检查 `JASS_REPOSITORY` 的内容并对清单文件中列出的所有文件执行校验和，以确定自加强安全性运行操作（执行并保存校验和）以来，哪些文件进行了更改。在强制运行撤消操作之前进行检查，该操作可提供有价值的信息，从而节省数小时没必要的错误诊断时间。

以下为一个输出样例。

代码实例 4-1 手动更改的文件输出样例

```
# ./jass-check-sum
File Name              Saved CkSum              Current CkSum
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
/etc/inet/inetd.con    1643619259:6883          2801102257:6879
/etc/logadm.conf       2362963540:1042          640364414:1071
/etc/default/inetd     3677377803:719           2078997873:720
```

该输出表明加强安全性运行操作结束后更改了三个文件。

使用带有撤消功能的选项

本节介绍了 `jass-execute -u` 命令和在执行撤消操作时可使用的选项。

注 – 不能在撤消功能中使用 `-d`、`-a`、`-h`、`-l` 或 `-H` 选项。在静止模式下运行撤销功能时，您必须提供 `-b`、`-k` 或 `-f` 选项。

`jass-execute -u`命令是执行撤消操作的标准命令。此命令会自动发现上次执行加强安全性操作以来手动进行的任何更改。如果 Solaris Security Toolkit 软件发现了上次执行加强安全性操作以来手动更改的文件，系统会提示选择以下响应操作：

1. 在恢复原始的文件 （加强安全性运行操作前存在的文件）之前，请备份最新的文件。
2. 保留最新的文件，且不要恢复原始文件。
3. 强制覆盖手动更改的任何文件 （可能会丢失数据）并恢复原始文件。

如果要更改缺省的撤消操作，在执行撤消命令时请使用 `-b`、`-k` 和 `-f` 选项。

表 4-1 列出了可与撤消操作一起使用的命令行选项。有关每个选项的详细信息，请参阅以下几节。

表 4-1 将命令行选项与撤消命令结合使用

选项	说明
-b	备份自上次加强安全性运行操作以来手动更改的所有文件，然后将系统恢复到原始状态。
-f	取消在加强安全性运行操作时未遇到异常情况下的更改，也包括加强安全性运行操作后手动更改的文件。
-k	在加强安全性运行操作后保存对文件所做的手动更改。
-m	将输出发送到一个电子邮件地址。
-o	将输出定向到一个文件。
-q	防止将输出显示到屏幕上。又称为静止选项。输出存储在 JASS_REPOSITORY/jass-undo-log.txt 文件中。

备份选项

-b 选项自动备份自上次加强安全性运行操作以来手动更改的任何文件，然后将文件恢复到加强安全性运行操作前的原始状态。为实现手动更改，需要将恢复文件与备份文件作对比，并手工调整它们之间的不同。使用此选项备份文件的实例用法如下。

```
/etc/motd.BACKUP.JASS_SUFFIX
```

强制选项

-f 选项取消加强安全性运行操作过程中未发生异常情况的更改，也包括在加强安全性运行操作之后手动更改的文件。该撤消运行操作不会将所保存的文件校验和与现有文件版本的校验和进行比较。因此，如果在加强安全性运行操作后手动更改了文件，则在执行具有强制选项的撤消操作后，文件更改会被覆盖或者丢失。

您可能需要在撤消运行操作完成后再次进行手动更改。此外，有必要根据所做的更改类型调整文件组之间的差异。为避免发生这些问题，请使用前面提到的 jass-check-sum 命令或 -b 命令行选项。

保留选项

-k 选项自动保留加强安全性运行操作后所做的手动更改而不恢复原始文件。-k 选项可搜索文件中的任何不匹配内容，生成通知并进行记录，但不用原始文件覆盖现有文件。只有那些在文件 jass-checksums.txt中保存了有效的校验和的更改才会进行取消。

此选项并非没有缺点。例如，如果使用 finish 脚本修改了一部分文件之后又手动修改了这些文件，则该选型会导致系统不一致。

以 finish 脚本remove-unneeded-accounts.fin 为例。该脚本修改了系统中的 /etc/passwd 和 /etc/shadow 文件。如果用户在加强安全性运行操作完成后手动更改了口令，则与 /etc/shadow 文件相关的校验和将与 Solaris Security Toolkit 软件保存的值不匹配。因此，如果使用了保留选项，则只将 /etc/passwd 文件复制回原始状态， /etc/shadow 文件仍保持其当前形式，两个文件不再一致。

输出文件选项

-o *output-file* 选项将 jass-execute 运行的控制台输出重新定向到一个单独的文件 (*output-file*)。

此选项不影响 JASS_REPOSITORY 目录中的日志。终端连接缓慢时，可使用该选项，因为 Solaris Security Toolkit 撤消操作会产生大量重要的输出。

静止输出选项

-q 选项可阻止 Solaris Security Toolkit 软件将输出显示到屏幕上。此选项不影响 JASS_REPOSITORY 目录中的日志。与 -o 选项类似，此选项特别有助于通过 cron（时钟守护进程）作业或较慢的网络连接来运行 Solaris Security Toolkit 软件。

电子邮件通知选项

-m *email-address* 选项指示 Solaris Security Toolkit 软件将一个已完成运行操作的副本发送到一个电子邮件地址。使用其他选项除了可在系统上生成日志外，还可生成电子邮件报告。

撤消系统更改

有时必须取消在一个或多个 Solaris Security Toolkit 加强安全性运行操作过程中所做的更改。如果发现在加强安全性运行操作时所做的更改对系统产生了负面影响，请撤消这些更改。

例如，如果在加强安全性运行操作后发现禁用了一项所需的服务 （例如 NFS），请撤消这次加强安全性运行操作。然后，启用 NFS 并用修订的安全性配置文件重复加强安全性运行操作。

本节提供了在一个或者多个加强安全性运行操作的过程中取消更改的指导。请注意，对于有效地取消加强安全性运行操作有一些限制和要求。请参阅第 52 页 “撤消系统更改的要求”。

▼ 撤消 Solaris Security Toolkit 运行操作

1. **备份并重新引导系统。**

   在每次撤消运行前重新引导并备份系统以确保能够返回或恢复到一个已知的工作状态。

2. **确定在使用 `jass-execute -u` 命令时使用哪些选项。**

   请参阅第 54 页 “使用带有撤消功能的选项”。

   以下指导假设您正在使用 `jass-execute -u` 命令。

3. **要使用标准 `-u` 选项撤消一个或多个加强安全性运行操作，请在 `JASS_HOME_DIR` 中输入以下命令：**

```
# ./jass-execute -u
```

Solaris Security Toolkit 软件通过查找 JASS_REPOSITORY 中的所有清单文件收集有关每次加强安全性运行操作的信息。如果清单文件为空或者根本不存在，则认为没有可撤消的更改并忽略该运行操作。此外，如果一个名为 jass-undo-log.txt 的文件与清单文件存在于同一目录下，则认为已运行了取消操作，从而忽略该运行操作。收集过程完成之后，会显示结果。以下是一个输出样例。

代码实例 4-2 可撤消的运行操作的输出样例

```
# ./jass-execute -u
[NOTE] Executing driver, undo.driver
Please select a JASS run to restore through:
1. January 24, 2003 at 13:57:27
(/var/opt/SUNWjass/run/20030124135727)
2. January 24, 2003 at 13:44:18
(/var/opt/SUNWjass/run/20030124134418)
3. January 24, 2003 at 13:42:45
(/var/opt/SUNWjass/run/20030124134245)
4. January 24, 2003 at 12:57:30
(/var/opt/SUNWjass/run/20030124125730)

Choice? ('q' to exit)?
```

在本例中，存在四个独立的加强安全性运行操作。这些运行操作使系统发生更改并且尚未被撤消。加强安全性运行操作列表通常按时间从远到近列出。列表中的第一项为最近执行的加强安全性运行操作。

4. **检查输出以确定需要撤消哪些运行操作，然后输入相应的数字。**

对于所选的项， Solaris Security Toolkit 软件取消每个索引号等于或小于所选值的运行操作。即撤消运行操作将按照与原先所做更改相反的顺序来撤消这些更改，从最近的加强安全性运行操作开始一直到所选的运行操作。使用前面的实例作为指导，如果选择了运行操作 3，则撤消运行操作首先取消运行操作 1 的更改，然后取消运行操作 2 的更改，最后取消运行操作 3 的更改。

以下实例显示了撤消运行操作处理两个清单文件条目时生成的输出。

代码实例 4-3 撤消运行操作处理多个清单文件条目的输出样例

```
[...]

================================================================

undo.driver: Performing UNDO of

//var/opt/SUNWjass/run/20030124135727.

================================================================
```

代码实例 4-3 撤消运行操作处理多个清单文件条目的输出样例 *（接上页）*

```
[...]

================================================================

undo.driver: Undoing Finish Script: update-cron-allow.fin

================================================================

[NOTE] Undoing operation COPY.

cp -p /etc/cron.d/cron.allow.JASS.20030125223417

/etc/cron.d/cron.allow

rm -f /etc/cron.d/cron.allow.JASS.20030125223417

[NOTE] Removing a JASS-created file.

rm -f /etc/cron.d/cron.allow

[...]
```

在此实例中， Solaris Security Toolkit 软件撤消了一个复制操作并删除了加强安全性运行过程中所添加的一个文件。撤消运行操作的输出记录了用于恢复系统的实际命令，在需要对系统配置进行错误诊断时可以清楚地理解此过程并用作参考。

撤消运行操作会继续进行，直到处理完所有运行操作和相关的清单文件并取消了更改为止。

Solaris Security Toolkit 软件除了通过查找所有位于 `JASS_REPOSITORY` 中的清单文件以收集有关每次加强安全性运行的信息之外，它还会比较每个修改的文件的校验和。在校验和文件中的任何不匹配都会产生一个通知并进行记录。对于这些文件，撤消运行操作会询问所要采取的操作。

5. **如果撤消运行操作发现异常 （在加强安全性运行操作后手动更改了文件），请输入这些选项之中的一个。**

以下是一个显示了异常和处理异常选择的实例。

代码实例 4-4 撤消异常的输出样例

```
[...]

================================================================
undo.driver: Undoing Finish Script: install-templates.fin
================================================================

[NOTE] Undoing operation COPY.
cp -p /etc/skel/local.login.JASS.20030125223413
/etc/skel/local.login
rm -f /etc/skel/local.login.JASS.20030125223413

[NOTE] Undoing operation COPY.
[WARN] Checksum of current file does not match the saved value.
[WARN]    filename = /etc/.login
[WARN]    current = 3198795829:585, saved = 1288382808:584

Please select the course of action:

1. Backup.  Save current file before restoring original.
2. Keep.    Keep the current file, making no changes.
3. Force.   Ignore manual changes and overwrite current file.

Enter 1, 2, or 3:
```

在本实例中，如果选择条目 1，会显示以下输出。

代码实例 4-5 在撤消过程中选择备份选项的输出样例

```
Enter 1, 2, or 3: 1

[NOTE] BACKUP specified, creating backup copy of /etc/.login.
[NOTE] File to be backed up is from an undo operation.
[NOTE] Copying /etc/.login to /etc.login.BACKUP.JASS.20030125224926
cp -p /etc/.login.JASS.20030125223413 /etc/.login
rm -f /etc/.login.JASS.20030125223413

[...]
```

对于在任何加强安全性运行操作后手动更改的文件采取适当的操作。

当撤消运行操作遇到更改的文件并且选择不覆盖它们时，请在重新引导系统之前解决这些问题。

注 – 在本实例实例中，更改的文件以新的文件名保存：`/etc/.login.BACKUP.JASS.20030125224926`。在撤消运行操作完成后，将文件与 `/etc/.login` 相比较以确定是否需要进一步进行处理。

6. **在继续之前解决异常情况。**

7. **解决完异常情况后，请重新引导系统。**

   在加强安全性运行操作前重新引导系统对于停止和启动可用的服务是必要的。

第 5 章

配置和管理 JumpStart 服务器

本章提供了配置和管理 JumpStart 服务器以使用 Solaris Security Toolkit 软件的信息。JumpStart 技术是 Sun 基于网络的 Solaris OS 安装机制，能够在安装过程中运行 Solaris Security Toolkit 软件。

Solaris Security Toolkit 的 JumpStart 模式基于JumpStart 技术，且对于 Solaris OS 2.1 以后的产品都是可用的。JumpStart 技术可帮助您使 Solaris OS 和系统软件安装完全自动化，实现系统的正确性和标准化，以进行复杂的管理。它提供了一种方法，可满足快速安装和部署系统的要求。

在系统安全领域使用 JumpStart 技术的优点是很明显的。通过将 JumpStart 技术与 Solaris Security Toolkit 软件结合使用，可以在 Solaris OS 自动安装过程中保护系统安全。此做法有助于确保在系统安装时已使系统安全标准化并进行了处理。有关 JumpStart 技术的更多信息，请参阅 Sun BluePrints 书籍 *《JumpStart Technology: Effective Use in the Solaris Operating Environment》*。

本章包含以下主题：

- 第 63 页 “配置 JumpStart 服务器和环境”
- 第 65 页 “使用 JumpStart 配置文件模板”
- 第 67 页 “添加和删除客户机”

配置 JumpStart 服务器和环境

在 JumpStart 环境中，将 `JASS_HOME_DIR`（用于 `tar` 文件下载）或 `/opt/SUNWjass`（用于 `pkg`文件下载）中的 Solaris Security Toolkit 源代码复制到 JumpStart 服务器的主目录下。缺省目录是 JumpStart 服务器上的 `/jumpstart`。完成该任务后， `JASS_HOME_DIR` 成为 Jumpstart 服务器上的主目录。

本节假设读者熟悉 JumpStart 技术并已经有一个可用的 JumpStart 运行环境。

将 Solaris Security Toolkit 软件集成到JumpStart 体系结构中只需要几个步骤。

▼ 配置 JumpStart 模式

1. **将 Solaris Security Toolkit 源代码复制到 JumpStart 服务器的根目录中。**

   例如，如果将 Solaris Security Toolkit 归档文件解压缩到 JASS_REPOSITORY，而 JumpStart 服务器的根目录是 /jumpstart，请用以下命令复制 Solaris Security Toolkit 源代码：

```
# pwd
/opt/SUNWjass
# tar cf - . | (cd /jumpstart; tar xf -)
```

   Solaris Security Toolkit 软件通常安装在 JumpStart 服务器上的 SI_CONFIG_DIR 目录中，通常也会是 JASS_HOME_DIR。

2. **如果对 Solaris 2.5.1 OS sysidcfg 文件做了修改，则也要对 JASS_HOME_DIR /Sysidcfg/Solaris_2.5.1 目录中的文件做相应修改。**

   如果使用 Solaris 2.5.1 OS，则不能直接使用JASS_HOME_DIR/Sysidcfg /Solaris_2.5.1 中的sysidcfg文件，因为 Solaris 的版本仅支持 SI_CONFIG_DIR 中而不支持独立子目录中的 sysidcfg 文件。为解决 Solaris 2.5.1 OS 的这种限制，Solaris Security Toolkit 软件具有了 SI_CONFIG_DIR/sysidcfg，它链接到 JASS_HOME_DIR/Sysidcfg/Solaris_2.5.1/sysidcfg 文件。

3. **使用以下命令将 JASS_HOME_DIR/Drivers/user.init.SAMPLE 复制为 JASS_HOME_DIR/Drivers/user.init。**

```
# pwd
/jumpstart/Drivers
# cp user.init.SAMPLE user.init
```

4. **如果在使用多宿主的 JumpStart 服务器时遇到问题，请修改 JASS_PACKAGE_MOUNT 和 JASS_PATCH_MOUNT 中的两个条目，以将路径纠正为 JASS_HOME_DIR/Patches 和 JASS_HOME_DIR/Packages 目录。**

5. **如果要在 SI_CONFIG_DIR 子目录（例如，SI_CONFIG_DIR/path/to/JASS）中安装 Solaris Security Toolkit 软件，请向 user.init 文件中添加以下内容：**

```
if [ -z "${JASS_HOME_DIR}" ]; then
       if [ "${JASS_STANDALONE}" = 0 ]; then
                JASS_HOME_DIR="${SI_CONFIG_DIR}/path/to/JASS"
       fi
fi
export JASS_HOME_DIR
```

6. **选择或创建一个 Solaris Security Toolkit 驱动程序 （例如，缺省的 `secure.driver`）。**
   - 如果要使用 `hardening.driver` 和 `config.driver` 中列出的所有脚本，请向 `rules` 文件中添加`Drivers/secure.driver` 路径。
   - 如果仅使用所选脚本，请复制这些文件，然后修改其副本。
7. **完成驱动程序后，在 `rules` 文件中创建适当的条目。**

   该条目与以下内容相似：

```
hostname imbulu - Profiles/core.profile Drivers/secure.driver
```

注意 – 请勿修改 Solaris Security Toolkit 软件中附带的原始脚本。为允许 Solaris Security Toolkit 软件新版本有效的迁移，请单独保存原始文件和定制的文件。

要成功地将 Solaris Security Toolkit 软件集成到现有的 JumpStart 环境中还需要做另一项修改。

8. **如果使用 Solaris Security Toolkit 软件提供的 `sysidcfg` 文件以使 JumpStart 客户机安装自动化，请检查它们的适用性。**

   如果在解析 `sysidcfg` 文件时 JumpStart 服务器遇到问题，则会忽略整个文件的内容。

   完成本节所有的配置步骤之后，可以在客户机上使用 JumpStart 技术，并可在安装过程中成功地加强或者最小化 OS 的安全性。

使用 JumpStart 配置文件模板

JumpStart 配置文件模板是只能在 JumpStart 模式中使用的文件。在 Sun BluePrints 书籍 *《JumpStart Technology: Effective Use in the Solaris Operating Environment》* 中介绍了配置文件中必需的和可选的内容。

可使用 JumpStart 配置文件模板作为样例，在此基础上针对您的站点要求进行修改。检查配置文件以确定需要进行哪些更改 （如果有），以应用于您的环境。

复制配置文件，然后在您的环境中修改其副本。不要更改原始文件，因为更新 Solaris Security Toolkit 软件时可能会覆盖定制的内容。

以下是 Solaris Security Toolkit 软件中包含的 JumpStart 配置文件。

- `32-bit-minimal.profile`
- `core.profile`
- `end-user.profile`
- `developer.profile`

- entire-distribution.profile
- oem.profile
- minimal-Sun_ONE-WS-Solaris*.profile
- minimal-SunFire_Domain*.profile

以下几小节介绍这些配置文件。

32-bit-minimal.profile

该 JumpStart 配置文件是相对通用的 JumpStart 配置文件，可用于 32 位的最小化安全性的系统。它是最小化安全性的系统的合理开发起点，并且可用作 minimal-Sun_ONE-WS-Solaris*.profile 最小化安全性脚本的起点。

core.profile

该 JumpStart 配置文件安装最小的Solaris OS 群集 (SUNWCreq)。除了指定包含根分区与交换分区的磁盘分区外，没有做任何其他的配置修改。

end-user.profile

该 JumpStart 配置文件安装 End User Solaris OS 群集 (SUNWCuser) 和使进程统计正常运行所需的两个 Solaris OS 软件包。另外，将磁盘分区定义为仅包含根分区和交换分区。

developer.profile

该 JumpStart 配置文件安装 Developer Solaris OS 群集 (SUNWCprog) 和使进程统计正常运行所需的两个 Solaris OS 软件包。与在 core.profile 中定义的一样，除了 Solaris OS 群集之外唯一需要定义的配置是为了使磁盘分区包含根分区和交换分区。

entire-distribution.profile

该 JumpStart 配置文件安装 Entire Distribution Solaris OS 群集 (SUNWCall)。和其他配置文件一样，将磁盘分区定义为包含根分区和交换分区。

oem.profile

该 JumpStart 配置文件安装 OEM Solaris OS 群集 (SUNWCXall)。本群集是 Entire Distribution 群集的父群集，它安装 OEM 提供的软件。

minimal-Sun_ONE-WS-Solaris*.profile

以下所有配置文件均基于 Sun BluePrints OnLine 中标题为 *"Minimizing the Solaris Operating Environment for Security"* 的文章。该文章中提到的所有 Solaris OS 版本均具有特定的配置文件。以下 JumpStart 配置文件与该文章所引用的那些配置文件相同。

- minimal-Sun_ONE-WS-Solaris.26.profile
- minimal-Sun_ONE-WS-Solaris7-32bit.profile
- minimal-Sun_ONE-WS-Solaris7-64bit.profile
- minimal-Sun_ONE-WS-Solaris8-32bit.profile
- minimal-Sun_ONE-WS-Solaris8-64bit.profile
- minimal-Sun_ONE-WS-Solaris9-64bit.profile

minimal-SunFire_Domain*.profile

以下所有配置文件均基于 Sun BluePrints OnLine 中标题为 *"Minimizing Domains for Sun Fire V1280, 12K, and 15K Systems"* 的文章。以下 JumpStart 配置文件与该文章所引用的那些配置文件相同。

- minimal-SunFire_Domain-Apps-Solaris8.profile
- minimal-SunFire_Domain-Apps-Solaris9.profile
- minimal-SunFire_Domain-NoX-Solaris8.profile
- minimal-SunFire_Domain-NoX-Solaris9.profile
- minimal-SunFire_Domain-X-Solaris8.profile
- minimal-SunFire_Domain-X-Solaris9.profile

添加和删除客户机

以下信息描述了在 JumpStart 模式下可用的脚本。该模式由插入到 JumpStart 服务器上 rules 文件中的 Solaris Security Toolkit 驱动程序控制。

如果没有配置环境以使用 JumpStart 模式，请参阅第 63 页 "配置 JumpStart 服务器和环境"。

add-client 脚本

为简化从 JumpStart 服务器添加客户机的过程，请使用包含在 Solaris Security Toolkit 软件中的该脚本。以下段落介绍了命令和选项，然而没有介绍底层的 JumpStart 技术。有关 JumpStart 技术的信息，请参阅 Sun BluePrints 书籍 *《JumpStart Technology: Effective Use in the Solaris Operating Environment》*。

add-client 脚本是 add_install_client 命令的外壳，它接受以下参数。

用法实例：

```
# add-client -c client -i server -m client-class -o client-OS -s sysidcfg
```

表 5-1 介绍了 add-client 命令的有效输入。

表 5-1 JumpStart add-client 命令

值	说明
-c *client*	JumpStart 客户机的可解析的主机名。
-h	显示使用信息。使用时不能带有任何其他选项。任何其他选项都将被忽略。
-i *server*	JumpStart 服务器接口的 IP 地址或可解析的主机名，该地址或主机名用于 JumpStart 客户机。如果没有指定值，则会显示本地主机上可用接口的列表。
-m *client-class*	JumpStart 客户机的计算机类型。该值与 uname -m 命令的输出格式相同。
-o *client-OS*	Solaris OS 的修订版。可以在安装在客户机上的 JASS_HOME_DIR/OS 目录下获得该值 。如果没有指定值，则会显示 JASS_HOME_DIR/OS 目录中可用的 Solaris OS 版本的列表。
-s *sysidcfg*	备用目录的可选路径名，此目录包含一个用于系统识别和配置的 sysidcfg 文件。缺省情况下，该值被设定为 JASS_HOME_DIR/Sysidcfg /Solaris_version/ 目录，其中version是从指定给该客户机的 OS 中抽取的。如果已指定，则必须使用和 JASS_HOME_DIR 目录相关的路径名。仅指定 sysidcfg 文件的路径。
-v	本程序的版本信息。
-?	显示使用信息。使用时不能带有任何其他选项。任何其他选项都将被忽略。

要将一台 JumpStart 客户机 （名为 jordan）添加到某个接口 （名为nomex-jumpstart）上的 JumpStart 服务器 （名为 nomex，使用 Solaris 8 OS (4/01)），请使用以下 add-client 命令：

```
#./add-client -c jordan -o Solaris_8_2001-04 -m sun4u -i nomex-jumpstart
updating /etc/bootparams
```

要使用 sysidcfg 选项添加同一 JumpStart 客户机 (jordan)，请使用以下命令：

```
#./add-client -c jordan -o Solaris_8_2001-04 -m sun4u -i nomex-jumpstart -s
Hosts/jordan
updating /etc/bootparams
```

rm-client 脚本

该脚本包含在 Solaris Security Toolkit 软件中，可简化从 JumpStart 服务器中删除客户机的操作。请使用包含在 Solaris Security Toolkit 软件中的该脚本。以下段落介绍了这些命令和选项，但没有介绍底层的 JumpStart 技术。有关 JumpStart 技术的信息，请参阅 *《JumpStart Technology: Effective Use in the Solaris Operating Environment》*。

与 add-client相似， rm-client 脚本是 rm_install_client 命令的外壳：

用法实例：**rm-client** [-c] *client*

其中， *client* 是 JumpStart 客户机的可解析的主机名。

表 5-2 介绍了 rm-client 命令的有效输入。

表 5-2 JumpStart rm-client 命令

Value	Description
-c *client*	JumpStart 客户机的可解析的主机名。
-h	显示使用信息。不使用任何其他选项。任何其他选项都将忽略。
-v	本程序的版本信息。
-?	显示使用信息。不使用任何其他选项。任何其他选项都将忽略。

要删除一台名为 jordan 的 JumpStart 客户机，请使用以下 rm-client 命令：

```
# ./rm-client -c jordan
removing jordan from bootparams
```

第 6 章

审计系统安全性

本章介绍如何使用 Solaris Security Toolkit 软件审计（验证）系统的安全性。使用本章中的信息和过程在加强安全性运行操作之后维护已创建的安全性配置文件。对于经过部署的系统，在加强安全性之前需要使用本章中的信息对安全性进行评估。

注 – 本章和本书中使用的术语 *审计* 是 Solaris Security Toolkit 软件对安全性状态的自动化验证过程，方法是与预先定义的安全性配置文件相比较。本出版物中使用此术语，并不表示在使用审计选项后便可保证系统的绝对安全。

本章包含以下主题：

- 第 71 页 “维护安全性”
- 第 72 页 “执行加强操作之前检查安全性”
- 第 72 页 “定制安全性审计”
- 第 73 页 “审计安全性的准备工作”
- 第 73 页 “使用选项和控制审计输出”
- 第 80 页 “进行安全性审计”

维护安全性

维护安全性是一个进行中的过程，必须定期检查及访问。维护系统安全性需要警惕性，因为任何系统缺省的安全性配置会随着时间的逝去而愈加趋向公开。（有关维护安全性的更多信息，请参阅第 27 页 “维护系统安全”。）

基于用户的经验和要求，我们为 Solaris Security Toolkit 软件开发了一种自动方法，通过确定与指定的安全性配置文件的兼容水平来审计系统安全性状态。

注 – 本方法仅能用于使用 `jass-execute -a` 命令的独立模式下，而不能在 JumpStart 安装过程中使用。

定期审计系统的安全性状态，既可以通过手工方式也可以通过自动方式 （例如，通过 cron （时钟守护进程）作业或 rc 脚本）。例如，在加强一个全新安装系统的安全性之后，请在五天后执行 Solaris Security Toolkit 软件审计命令 (jass-execute -a *driver-name*) 以确定系统安全性是否已更改 （与安全性配置文件所定义的状态不同）。

审计安全性的频繁程度取决于环境的紧急程度与安全策略。有些用户每小时、每天或者每月进行一次审计运行操作。而有些用户每小时运行一次最小扫描 （仅检查有限数量），每天运行一次完整扫描 （进行全部检查）。

审计重要组件以维护已部署系统的安全性状态。如果不定期审计安全性状态，则由于平均信息量或者修改会不知不觉或恶意地更改所需的安全性状态，导致配置随之变化。如果不进行定期检查，则不会发现这些更改并采取相应的纠正措施。这将导致系统的安全性降低，更容易受攻击。

除了定期审计之外，在升级、安装修补程序与其他的重要系统配置发生更改后也需要进行审计。

执行加强操作之前检查安全性

在某些情况下，会发现在加强已部署系统的安全性*之前* 检查其安全性状态是有用的。例如，如果接管之前由他人管理的已部署系统，则应检测系统以了解其状态，如果必要的话可以使它们与其他系统所使用的相同安全性配置文件相兼容。

定制安全性审计

审计选项为评估系统状态提供了一种高度灵活与可扩展的机制。像加强安全性脚本一样，也可以定制 audit 脚本的操作。例如，可以定制环境变量、定制框架与助手功能、添加新的检查和为审计框架添加功能。

大部分用户会发现标准的或产品专用的 audit 脚本可以作为自己定制 audit 脚本的模板。对于这种情形，可以通过驱动程序、finish 脚本、环境变量与文件模板定制 audit 脚本。只需很少的工作即可完成这些定制更改，且无需修改代码。进行审计时，Solaris Security Toolkit 软件可自动了解加强安全性运行操作中所做的任何更改。

有时候，需要添加 Solaris Security Toolkit 软件未提供的检查或功能。对于这种情形，请向 audit 脚本中添加检查或者新的功能。（您或许会在相应的 finish 脚本中做相关更改。）在某些情况下，可能需要修改代码。在添加和修改代码时需要格外慎重以避免引入错误及故障。

有些用户需要创建全新所有权的或站点专用的驱动程序和脚本。使用模板和样例作为编写新驱动程序和脚本代码的准则。请注意，使用审计选项时 Solaris Security Toolkit 软件*无法* 自动了解站点专用的驱动程序、finish 脚本、变量与功能。例如，如果添加了一个名为 `abcc-nj-secure.driver` 的站点专用驱动程序，且该驱动程序包含站点专用的 finish 脚本 `abcc-nj-install-foo.fin`，则需要创建一个站点专用的 audit 脚本 `abcc-nj-install-foo.aud`。同样地，如果仅启动 audit 脚本，则应当创建与之匹配的 finish 脚本。

要定制或创建新的驱动程序、脚本、变量和功能，请参阅 *《Solaris Security Toolkit 4.1 Reference Manual》*。

例如，若要添加一个 Solaris Security Toolkit 软件没有安装的修补程序。则既可以扩展标准的或者产品专用的模板，也可以创建自己的模板。创建自己的模板时，请创建用来添加修补程序的 finish 脚本，然后创建相应的 audit 脚本以检查修补程序的安装。

审计安全性的准备工作

为使用本章的指导和准则，您需要一个安全性配置文件。有关开发与实现安全性配置文件的信息，请参阅第 2 章。

许多安全性配置文件模板包含在 Solaris Security Toolkit 附带的驱动程序内。正如本书前面所述，缺省的安全性配置文件和由驱动程序提供的更改很可能并不适用于您的系统。通常情况下，这些驱动程序实现的安全性配置文件是安全性的“水印上限”标记。意思是，它们能够禁用不需要的服务并启用缺省情况下禁用的可选安全性功能。

许多 Solaris Security Toolkit 软件用户发现标准的和产品专用的安全性配置文件模板适用于他们的环境。如果您遇到这种情形，请确定与安全性状态最接近的安全性配置文件，并将其用于评估和加强系统的安全性。

为您的环境检查并定制安全性配置文件或者开发新的文件。定制安全性配置文件的技巧和指导在 *《Solaris Security Toolkit 4.1 Reference Manual》* 中进行了介绍。此方法提供了为您的组织定制的安全性状态，并且可以将安全性评估过程中返回的故障错误减至最少。例如，如果需要启用 Telnet，则可以定制安全性配置文件，使其在安全性评估过程中不会将 Telnet 视为攻击。例如，一个使用 Telnet 和 Kerbero （用于验证和加密）的站点不会将使用 Telnet 视为攻击。

使用选项和控制审计输出

本节介绍了执行审计运行操作的可用选项和控制输出的选项。本节包含以下主题：

■ 第 74 页 “命令行选项”

■ 第 77 页 “标题与消息输出”
■ 第 79 页 “主机名称、脚本名称和时间戳输出”

命令行选项

根据安全性配置文件审计系统的用法实例：

```
# jass-execute -a driver [ -V [0-4] ] [ -q | -o output-file ]
[ -m email-address ]
```

当执行 Solaris Security Toolkit 软件审计命令时，可以使用表 6-1 中所列的以下选项。

表 6-1 将命令行选项与审计命令结合使用

选项	说明
-a	确定系统与其安全性配置文件是否相符。
-h	显示 jass-execute 帮助消息，提供了可用选项的概述。
-m	将输出发送到一个电子邮件地址。
-o	定向输出到一个文件。
-q	禁止将输出显示到屏幕上。又称为静止选项。
-V	指定审计运行操作的冗长级别。

有关 jass-execute -a 命令可用选项的详细信息，请参阅以下几节：

■ 第 74 页 “显示帮助选项”
■ 第 75 页 “电子邮件通知选项”
■ 第 76 页 “输出文件选项”
■ 第 76 页 “静止选项”
■ 第 76 页 “冗长选项”

显示帮助选项

-h 选项显示 jass-execute 帮助消息，提供了可用选项的概述。

-h 选项产生的输出与以下内容相似：

代码实例 6-1 -h 选项输出样例

```
# ./jass-execute -h

To apply this Toolkit to a system, using the syntax:
  jass-execute [-r root_directory -p os_version ]
  [ -q | -o output_file ] [ -m e-mail_address ]
  [ -V [3|4] ] [ -d ] driver

To undo a previous application of the Toolkit from a system:
  jass-execute -u [ -b | -f | -k ] [ -q | -o output_file ]
     [ -m e-mail_address ] [ -V [3|4] ]

To audit a system against a pre-defined profile:
  jass-execute -a driver [ -V [0-4] ] [ -q | -o output_file ]
     [ -m e-mail_address ]

To display the history of Toolkit applications on a system:
  jass-execute -H

To display the last application of the Toolkit on a system:
  jass-execute -l

To display this help message:
  jass-execute -h
  jass-execute -?

To display version information for this program:
  jass-execute -v
```

电子邮件通知选项

-m *email-address* 选项提供了一种机制，通过该机制， Solaris Security Toolkit 软件的审计运行操作完成后可使用电子邮件将输出自动发送出去。使用其他选项除了可在系统上生成日志外，还可生成电子邮件报告。

使用电子邮件选项调用 sunfire_15k_sc-config.driver 的 Solaris Security Toolkit 运行操作类似于以下内容：

```
# ./jass-execute -m root -a sunfire_15k_sc-config.driver
[...]
```

输出文件选项

-o *output-file* 选项将 jass-execute 运行操作的控制台输出重新定向到一个单独的文件 (*output-file*)。

此选项对于JASS_REPOSITORY 目录内的日志无效。此选项可用于连接缓慢的终端，因为 Solaris Security Toolkit 运行操作会产生大量的输出。

此选项可与 -d、 -u 或 -a 选项一起使用。

-o 选项产生的输出与以下内容相似：

代码实例 6-2 -o 选项输出样例

```
# ./jass-execute -o jass-output.txt -a secure.driver
[NOTE] Executing driver, secure.driver
[NOTE] Recording output to jass-output.txt
#
```

静止选项

-q 选项禁止 Solaris Security Toolkit软件在执行加强安全性运行操作时输出到标准输入输出 (stdio) 流。

此选项不影响 JASS_REPOSITORY 目录中的日志。与 -o 选项相似，此选项特别有助于通过 cron（时钟守护进程）作业或在较慢的网络连接上运行 Solaris Security Toolkit 软件。

此选项可与 -d、 -u 或 -a 选项一起使用。

-q 选项产生的输出与以下内容相似：

代码实例 6-3 -q 选项输出样例

```
# ./jass-execute -q -a secure.driver
[NOTE] Executing driver, secure.driver
```

冗长选项

-v 选项指定了审计运行操作的冗长级别。此选项仅可用于审计。冗长级别为显示审计运行操作结果提供了高度灵活的方式。例如，如果要审计 100 台计算机，您需要将每台计算机的输出限制到单独一行，以便容易确定哪些计算机通过审计而哪些计算机没有通过审计。然后对于没有通过审计的计算机，可能需要进行一个能够提供扩展输出的审计以将注意力集中到有问题的区域。

-V 选项控制五个冗长级别 （0 到 4）。每个递增的级别都提供了附加细节，可用它来更加完整地了解哪些检查通过而哪些检查没有通过。表 6-2 介绍了冗长级别。

表 6-2 审计冗长级别

级别	输出
0	单独行，表明通过或者没有通过审计。
1	对于每个脚本，单独一行表明通过或者没有通过审计。在所有脚本行下面有一个重要的总分数行。
2	对于每个脚本，提供了所有检查的结果。
3	提供完整输出的多行，包括标题与标题消息。
4	多行 （所有级别 3 中提供的数据）加上 logDebug 日志功能产生的所有项。本级别用于调试。

注 – jass-execute -V 命令缺省的冗长级别为 3。

有关冗长级别的完整说明，请参阅 *《Solaris Security Toolkit 4.1 Reference Manual》*。

标题与消息输出

可以配置 Solaris Security Toolkit 审计选项以报告或者忽略标题和消息。JASS_LOG_BANNER 变量不能用于冗长级别 0-2。这些输出选项适用于冗长级别 3 和 4。例如，您可能要从输出中忽略掉通过的消息 （JASS_LOG_SUCCESS 变量）以便报告并且仅将注意力集中到没有通过的消息上 （JASS_LOG_FAILURE 变量）。

表 6-3 列出了能够通过日志变量控制的标题和消息。（有关日志变量的详细信息，请参阅 *《Solaris Security Toolkit 4.1 Reference Manual》*。）如果日志变量设置为 0，则不会产生这种类型消息的任何输出。相反，如果日志变量设置为 1，那么会显示出消息。每个变量缺省的操作是显示输出。表 6-3 介绍了日志变量。

表 6-3 在审计输出中显示标题和消息

日志变量	日志前缀	说明
JASS_LOG_BANNER	所有标题输出	此参数控制标题消息的显示。这些消息周围通常都是由等号 ("=") 或者破折号 ('-') 组成的分隔符。
JASS_LOG_ERROR	[ERR]	此参数控制错误消息的显示。如果设置为 0，则不会产生任何错误消息。
JASS_LOG_FAILURE	[FAIL]	此参数控制失败消息的显示。如果设置为 0，则不会产生任何失败消息。

表 6-3　在审计输出中显示标题和消息 *（接上页）*

日志变量	日志前缀	说明
JASS_LOG_NOTICE	[NOTE]	此参数控制通知消息的显示。如果设置为 0，则不会产生任何通知消息。
JASS_LOG_SUCCESS	[PASS]	此参数控制成功或者通过状态消息的显示。如果设置为 0，则不会产生任何成功消息。
JASS_LOG_WARNING	[WARN]	此参数控制警告消息的显示。如果设置为 0，则不会产生任何警告消息。

仅当需要查看特定消息时使用这些选项是非常有用的。通过设置这些选项，能够最小化输出，并仍然将注意力集中到您认为重要的地方。例如，除了 JASS_LOG_FAILURE（保留其缺省值 1）将所有登录变量设置为 0，运行 logFailure 功能只会产生有关失败的审计报告。

代码实例 6-4　仅报告审计失败的输出样例

```
# JASS_LOG_FAILURE=1
# export JASS_LOG_FAILURE
[setting of other parameters to 0 omitted]
# ./jass-execute -a secure.driver -V 2
update-at-deny        [FAIL] User test is not listed in
   /etc/cron.d/at.deny.
update-at-deny        [FAIL] Audit Check Total : 1 Error(s)
update-inetd-conf     [FAIL] Service ftp is enabled in
   /etc/inet/inetd.conf.
update-inetd-conf     [FAIL] Service telnet is enabled in
   /etc/inet/inetd.conf.
update-inetd-conf     [FAIL] Service rstatd is enabled in
   /etc/inet/inetd.conf.
update-inetd-conf     [FAIL] Audit Check Total : 3 Error(s)
```

主机名称、脚本名称和时间戳输出

可以配置 Solaris Security Toolkit 审计选项以包含主机名称、脚本名称和冗长级别为 0 – 2 的时间戳信息。例如，如果有许多待审计的计算机，可能希望能够通过主机名称、脚本名称或者时间戳对输出进行排序。表 6-4 列出了变量。

表 6-4 显示主机名称、脚本名称和时间戳审计输出

变量名称	变量说明
JASS_DISPLAY_HOSTNAME	将此参数设置为 1 会使 Solaris Security Toolkit 软件将每个日志条目附加在系统的主机名称之前。此信息基于 JASS_HOSTNAME 参数。缺省情况下，该参数为空，因此 Toolkit 不会显示此信息。
JASS_DISPLAY_SCRIPTNAME	缺省情况下，此参数值设置为 1，因此 Solaris Security Toolkit 软件会将每个日志附加在 audit 脚本名称之前。将该参数设定为其他任何值都会使 Toolkit 不显示此信息。
JASS_DISPLAY_TIMESTAMP	将该参数设置为 1 使 Solaris Security Toolkit 软件将每个日志附加在与审计运行操作相关的时间戳之前。此信息基于 JASS_TIMESTAMP 参数。缺省情况下，该参数为空，因此软件不会显示此信息。

通过配置 Solaris Security Toolkit 软件来附加主机、脚本和时间戳信息，可以将单个系统或者一组系统中的许多运行操作结合起来并按照关键数据对它们进行排序。可以使用此信息查找跨越几个系统的或者是在配置过程中有症状的问题。例如，以这种方式使用信息，管理员会能够辨别使用了给定进程的每个系统版本是否总是具有同样的故障检查。

例如，通过将 JASS_DISPLAY_TIMESTAMP 参数设置为 1 并将 JASS_DISPLAY_SCRIPTNAME 值设置为 0，会产生与以下相似的输出。

代码实例 6-5 审计日志条目的输出样例

```
# JASS_DISPLAY_SCRIPTNAME=0
# JASS_DISPLAY_TIMESTAMP=1
# export JASS_DISPLAY_SCRIPTNAME JASS_DISPLAY_TIMESTAMP
# ./jass-execute -a secure.driver -V 2
20030101233525 [FAIL] User test is not listed in
   /etc/cron.d/at.deny.
20030101233525 [FAIL] Audit Check Total : 1 Error(s)
20030101233525 [FAIL] Service ftp is enabled in
   /etc/inet/inetd.conf.
20030101233525 [FAIL] Service telnet is enabled in
   /etc/inet/inetd.conf.
20030101233525 [FAIL] Service rstatd is enabled in
   /etc/inet/inetd.conf.
20030101233525 [FAIL] Audit Check Total : 3 Error(s)
```

进行安全性审计

在系统上定期进行安全性评估可提供一个基准，以判断安全性与所执行的安全性配置文件的匹配接近程度。安全性评估最通常的情形是在加强一个新安装的系统的安全性之后，作为一项安全性维护任务进行。安全评估选项可使您简化操作 （对驱动程序使用和系统一致的安全性加强操作）。而现在可使用 -a 选项与加强安全性过程中执行的安全性配置文件相比较以检查当前的状态。该设计消除了复杂性并提供了灵活性。例如，当升级安全性配置文件时，后续的安全性评估会使用更新的安全性配置文件。

在另外的可能情形中，可能应该对经过部署的系统安全性负责。在加强它们的安全性之前，需要进行安全性评估。在这种情形中，需要定义自己的安全性配置文件，定制一个 Solaris Security Toolkit 安全性配置文件模板或者按原样使用其中一个安全性配置文件模板。

▼ 进行安全性审计

在进行审计之前，需要定义或者选择一个安全性配置文件。有关更多信息，请参阅第 73 页 “审计安全性的准备工作”。

注意 – 对已部署但尚未加强安全性的系统进行安全性评估时，请首先对计算机进行备份并重新引导以验证计算机处于一个已知、工作且一致的配置下。进行安全性评估之前，预备的重新引导过程中所遇的任何错误与警告都应得到更正并进行记录。

1. **选择要使用的安全性配置文件 （加强安全性驱动程序）：**
   - 如果之前加强了系统安全，请使用同样的安全性配置文件。

     例如， `secure.driver`。
   - 如果您还没有加强系统安全，请使用一个标准的安全性配置文件或者自己的文件。

     例如， `secure.driver` 或者 `abccorp-secure.driver`。

   有关可用驱动程序的完整且最新的列表，请从以下网站下载 Solaris Security Toolkit 软件的最新版本。

   http://www.sun.com/security/jass

   有关标准的和产品专用的驱动程序的信息，请参阅 *《Solaris Security Toolkit 4.1 Reference Manual》*。有关驱动程序的最新列表，请参见 Drivers 目录。

2. **确定所需的命令行选项和控制输出的方式。**

   请参阅第 73 页 “使用选项和控制审计输出”。

3. **输入 `jass-execute -a` 命令、安全性配置文件名称和所需的选项。**

以下是一个使用 sunfire_15k_sc-secure.driver 的审计运行操作样例。

代码实例 6-6 审计运行操作的输出样例

```
# ./jass-execute -a sunfire_15k_sc-secure.driver
[NOTE] Executing driver, sunfire_15k_sc-secure.driver

[...]

================================================================
sunfire_15k_sc-secure.driver: Audit script: enable-rfc1948.aud
================================================================

#----------------------------------------------------------------
# RFC 1948 Sequence Number Generation
#
# Rationale for Audit:
#
# The purpose of this script is to audit that the system is
# configured and is in fact using RFC 1948 for its TCP sequence
# number generation algorithm (unique-per-connection ID). This is
# configured by setting the 'TCP_STRONG_ISS' parameter to '2' in
# the /etc/default/inetinit file.
#
# Determination of Compliance:
#
[...]
#----------------------------------------------------------------

[PASS] TCP_STRONG_ISS is set to '2' in /etc/default/inetinit.
[PASS] System is running with tcp_strong_iss=2.

# The following is the vulnerability total for this audit script.

[PASS] Audit Check Total : 0 Error(s)

================================================================

# The following is the vulnerability total for this driver profile.

[PASS] Driver Total : 0 Error(s)

================================================================
sunfire_15k_sc-secure.driver: Driver finished.
================================================================

[PASS] Grand Total : 0 Error(s)
```

当审计运行操作启动后， Solaris Security Toolkit 软件从 JASS_HOME_DIR/Audit 目录中访问文件。虽然在 JASS_HOME_DIR/Audit 和JASS_HOME_DIR/Finish 目录下的文件具有同样的基本文件名，但它们有不同的文件名后缀。通过将后缀从 .fin 更改为 .aud， driver.run 脚本将 JASS_SCRIPTS 变量定义的 finish 脚本自动转换为 audit 脚本。

审计运行操作启动并初始化了 Solaris Security Toolkit 软件的状态。运行中所访问的每个驱动程序对所有文件模板与 audit 脚本的状态进行评估。每个检查会产生一个成功或者失败的结果，分别由攻击值 0 或者非 0 来代表。在大多数情况下，失败由数字 1 代表。每个运行脚本都根据脚本中包含的每次检查的攻击值的总和来产生总的安全性分数。此外，由每个驱动程序引起的攻击值总和会在每一个驱动程序评估完成时显示。运行结束时会显示重要的所有分数总和。

安全性评估选项提供了一个在评估运行操作启动后对系统状态的概述。Solaris Security Toolkit 软件通过检查配置文件来检查已存储的系统状态，并通过检查进程表信息、设备驱动程序信息等来检查正在运行的系统状态。Solaris Security Toolkit 软件检查每个文件及服务的存在性，并且检查与服务相关的软件是否已经安装、配置、启用和运行。此方法为系统当前状态生成了一个准确的快照。

第7章

保护系统安全

本章介绍如何将前面章节提供的信息和专门技术应用到现实的环境中，以安装新系统并保护其安全。本章举例说明如何用 Solaris 8 OS 的 Check PointFirewall-1 NG 来部署 Solaris Security Toolkit 软件。

本章的信息可用作保护新系统和应用程序安全的指南和案例。

Sun BluePrint 书籍和联机文章可为最小化系统和加强许多 Sun 系统的安全性提供指导。有关最新的产品专用的书籍和文章，请参见以下网站：

```
http://www.sun.com/blueprints
```

本章包含以下主题：

- 第 83 页 “规划与准备”
- 第 85 页 “创建安全性配置文件”
- 第 85 页 “安装软件”
- 第 88 页 “配置 JumpStart 服务器和客户机”
- 第 93 页 “定制加强安全性配置”
- 第 97 页 “安装客户机”
- 第 98 页 “质量保证测试”

规划与准备

要按照该案例研究中所述有效地部署最小化的和安全的系统，规划和准备工作是很重要的。基本的网络体系结构、策略以及过程必须适当。另外，必须对系统的支持与维护进行定义与协调。有关规划与准备的更多信息，请参阅第 2 章。本章中讲述的案例记录了系统管理员 (SA) 为防火墙系统的 Solaris OS 映像实现最小化系统和加强安全性所需执行的过程与任务。

在本案例中，系统管理员的任务是创建一种自动并可伸缩的解决方案，用于为服务提供商 (xSP) 构建和部署 Check PointFirewall-1 NG 系统，以便为其客户提供防火墙服务 。对于本案例， xSP 的要求和注意事项如下：

- 因为 xSP 计划部署许多这种系统，因而创建与部署每个系统的时间是非常关键的，而且需要改进以提高效率。
- 需要使用与每个系统内部以太网的接口相连的专用管理网络来安装系统。网络仅可以由 xSP 员工使用，订户不能使用。
- 所有其他接口都位于独立的物理网络接口上，并且会被过滤掉。
- 网络管理的安全性对于经过部署的防火墙系统的整体安全性是至关重要的。

基于这些要求，系统管理员决定使用 JumpStart 技术与 Solaris Security Toolkit 软件以使 OS 映像的安装、最小化系统与加强安全性都实现自动化。

假设与限制

本章假设 Solaris Security Toolkit 软件已经运行并使用 JumpStart 技术进行安装。本书中其他章节提供了安装软件的指导，请参阅相应章节了解有关信息。

本章假设正在为最小化和加强某个特定应用程序的安全性而开发定制的配置。Solaris Security Toolkit 软件没有任何专门用于该程序的驱动程序或 JumpStart 配置文件。因此，需要为此应用程序创建定制的驱动程序和配置文件。要完成此任务，可复制现有的驱动程序和配置文件，然后针对该应用程序对它们进行修改。

此案例中，假设系统管理员具有以下熟练级别：

- 拥有足够的知识与经验进行 OS 与应用程序的配置。
- 了解如何测试配置并进行调整以很好地使其协调。
- 了解如何从已经安装的客户机系统中构建一个 JumpStart 环境。请参阅 Sun BluePrints 书籍 *《JumpStart Technology: Effective Use in the Solaris Operating Environment》*。
- 熟悉 OS 最小化技术。请参阅 *《Enterprise Security: Solaris Operating Environment Security Journal, Solaris Operating Environment Versions 2.5.1, 2.6, 7, and 8》*。
- 熟悉 Solaris Security Toolkit 软件基础，且可随时使用最小化系统和加强安全性两种技术和准则来创建定制的配置。请参阅第 1 章。

系统环境

实例案例基于以下硬件与软件环境：

- Check PointFirewall-1 NG
- Solaris 8 OS
- JumpStart 技术
- Solaris OS 群集 (`SUNWCreq`)
- Solaris Security Toolkit 软件
- 基于 SPARC 技术的平台
- 至少两个以太网接口

安全性要求

本案例中，已确定高级别要求和软件包，但是还需要确定所有软件包的特定组件和服务。另外，需要确定管理系统所需的 Solaris OS 功能。

以下列表提供了软件组件使用方法的详细信息：

- 用于远程管理的 Secure Shell
- 用于复制文件的 FTP
- 用于镜像磁盘的 Solstice DiskSuite™ 软件
- 转发到中央信息库的 SYSLOG 消息

在此列表中，可以开发安全性配置文件。有关开发安全性配置文件和使用配置文件模板的详细信息，请参阅第 25 页 “开发和执行 Solaris Security Toolkit 配置文件”。

创建安全性配置文件

安全性配置文件定义了在加强和最小化系统安全性配置时 Solaris Security Toolkit 软件所做的安全性修改。任何包含在 Solaris Security Toolkit 软件中的标准安全性配置文件或者驱动程序都不能满足最小化 Check PointFirewall-1 NG 系统的要求。因而，必须创建一个定制的安全性配置文件以实现适当的系统修改。

对于本案例，本章中的几节介绍了适合案例的创建安全性配置文件的过程。首先，创建基于现有驱动程序的新的驱动程序文件。然后修改新的驱动程序以满足之前所述的安全性要求。最小化系统在第 85 页 “安装软件”中有讲述，而加强安全性修改在第 93 页 “定制加强安全性配置”中有讲述。

安装软件

本节演示了安装软件的过程。对于实例案例，提供了关于异常情况或者特定案例的所有指导。有关安装软件的总的指导，请参考本指南的其他部分。

注 – 可将以下指导作为模板用来处理相关情况。

本节包含以下任务：

- 第 86 页 “下载和安装安全性软件”
- 第 86 页 “安装修补程序”
- 第 87 页 “指定和安装 OS 群集”

下载和安装安全性软件

在 JumpStart 服务器上，下载并安装 Solaris Security Toolkit 及附加安全性软件 （包括修补程序），如下所示。

▼ 下载和安装安全性软件

1. **下载 Solaris Security Toolkit 软件及附加安全性软件。**

   请参阅第 31 页 “下载安全性软件”。

2. **安装已下载的 Solaris Security Toolkit 软件及附加安全性软件。**

   请参阅第 38 页 “安装和执行软件”。

注意 – 目前先不要执行 Solaris Security Toolkit 软件。首先按照以下几节所述进行附加配置和定制。

安装修补程序

OS 修补程序可以解决安全性漏洞、可用性问题、性能问题或系统其他方面的问题。安装新的 OS 时，以及在 OS 安装后的运行过程中，都要进行检查以确保安装了适当的修补程序。

Solaris Security Toolkit 软件提供了一种机制，以安装联机的 SunSolve 上可用的推荐的修补程序群集和安全性修补程序群集。此 OS 专用的修补程序群集包含通常最需要的修补程序。

▼ 安装修补程序

1. **至少，将推荐的修补程序群集和安全性修补程序群集下载到 `Patches` 目录下并解压缩。**

   如果加强安全性驱动程序中包含了 `install-recommended-patches.fin` 脚本，则会自动安装修补程序群集。

   Check PointFirewall-1 NG 还存在另外一个问题。此应用程序需要推荐的修补程序群集和安全性修补程序群集中未包含的特定修补程序。Check PointFirewall-1 NG 需要以下修补程序：

   - 108434
   - 108435

2. **要自动安装修补程序 108434 和 108435，请从联机的 SunSolve 下载最新的版本并将它们放入 `Patches` 目录。**

3. **用每个修补程序名称创建一个调用 `add_patch` 助手功能的全新 finish 脚本 （例如，`fw1-patch-install.fin`）。**

   该 finish 脚本通过两个 Check PointFirewall-1 NG 所需修补程序 ID 号调用适当的助手功能。例如：

```
# !/bin/sh

# add_patch 108434-10

# add_patch 108435-10
```

指定和安装 OS 群集

为 OS 安装定义完磁盘布局后，下一个任务是指定需要安装哪一个 Solaris OS 群集。选择 Solaris OS 可用的五个安装群集之一：`SUNWCreq`、 `SUNWCuser`、 `SUNWCprog`、`SUNWCall` 和 `SUNWCXall`。

▼ 指定和安装 OS 群集

1. **指定要安装的 OS 群集。**

   因为本案例的目标是创建一个最小且专用的防火墙设备，最小可用的 Solaris OS 群集，`SUNWCreq`，此软件包又称作 Core。

   因为本群集包含了数量相对较少的软件包，所以也可能需要其他的软件包。这些所需的其他软件包需要包含在用 Solaris OS 群集定义的配置文件中。

   基本的配置文件定义将以下内容添加到预先定义的配置文件中。

```
cluster           SUNWCreq
```

   `SUNWCreq` 安装群集包含的软件包并不都是 Sun 防火墙服务器正常运行所需要的。在具有了工作基准后，请删除这些额外的软件包。请参阅 Sun BluePrints OnLine 文章“Minimizing the Solaris Operating Environment for Security: Updated for the Solaris 9 Operating Environment”。

2. **用定义好的安全性配置文件进行安装以确定是否存在软件包从属性问题。**

   如果在安装过程中遇到一些软件包从属性问题，则认为 Check PointFirewall-1 NG 需要以下 Solaris OS 软件包：

   - `SUNWter` — 终端信息
   - `SUNWadmc` — 系统管理核心库
   - `SUNWadmfw` — 系统与网络管理框架
   - `SUNWlibC` 和 `SUNWlibCx` — Check PointNG 程序所需软件包

   配置文件中的软件包完整列表如下。

```
cluster           SUNWCreq
package           SUNWter          add
package           SUNWlibC         add
package           SUNWlibCx        add
package           SUNWadmc         add
package           SUNWadmfw        add
```

   虽然对于本案例研究而言，此列表是完整的，然而要根据部署此配置的实际环境来添加或删除附加的软件包。

   软件包的最终列表可能还需要修改，直到按第 98 页 “质量保证测试”中所述从功能及安全性两方面对系统进行了验证。若如此，请修改配置文件，重新安装系统然后重复该测试。

3. **基于之前两个步骤中的软件包从属性，创建一个** `minimize-firewall.fin` 脚本。

配置 JumpStart 服务器和客户机

本节演示了如何配置 JumpStart 服务器和客户机，以使用一个定制的安全性配置文件进行最小化。有关在 JumpStart 环境下使用 Solaris Security Toolkit 软件的详细信息，请参阅第 5 章。

本节包含以下任务：

- 第 89 页 “准备基础结构”
- 第 91 页 “验证和检查 rules 文件”

准备基础结构

执行以下任务以准备基础结构。以下任务演示了为在客户机上使用现有驱动程序、配置文件和 finish 脚本而创建基准配置的过程。确定基准后，验证其运转是否正常，然后为所选的应用程序定制基准。

▼ 准备基础结构

1. **配置 JumpStart 服务器和环境。**

   有关详细的指导，请参阅第 5 章。

2. **使用 `add-client` 命令向 JumpStart 服务器中添加客户机。**

   代码实例 7-1 在 JumpStart 服务器上添加一台客户机

```
# pwd
/jumpstart
# bin/add-client -c jordan -o Solaris_8_2002-02 -m sun4u
-s nomex-jumpstart
cleaning up preexisting install client "jordan"
removing jordan from bootparams
updating /etc/bootparams
```

3. **为客户机创建一个 `rules` 文件条目，指定适当的 JumpStart 配置文件和 finish 脚本。例如：**

```
hostname jordan - Profiles/xsp-minimal-firewall.profile \
  Drivers/xsp-firewall-secure.driver
```

4. **通过复制 Solaris Security Toolkit 软件提供的文件，创建名为 `xsp-minimal-firewall.profile` 的配置文件和名为 `xsp-firewall-secure.driver` 的驱动程序文件。**

在成功完成下一步之前必须创建这些文件。最初，这些文件可能是与 Solaris Security Toolkit 软件一起分发的文件的副本。请勿修改与 Solaris Security Toolkit 软件一起分发的原始文件。以下实例显示了如何创建文件。

代码实例 7-2 创建一个配置文件

```
# pwd
/jumpstart/Drivers
# cp install-Sun_ONE-WS.driver xsp-firewall-secure.driver
# cp hardening.driver xsp-firewall-hardening.driver
[...]
# pwd
/jumpstart/Profiles
# cp minimal-Sun_ONE-WS-Solaris8-64bit.profile \
    xsp-minimal-firewall.profile
```

本实例以一个专用的 Web 服务器配置为基础，因为它是开发专用防火墙的很好的基准。

5. **创建配置文件和驱动程序文件后，请按照以下所示修改文件：**

   a. **用** `xsp-firewall-hardening.driver` **替换与** `hardening.driver` **相关的** `xsp-firewall-secure.driver`。

   b. **替换定义在** `JASS_SCRIPTS` **中的与** `minimize-firewall.fin` **和您的 finish 脚本（例如，** `fw1-patch-install.fin`**）相关的两个 finish 脚本。**

   修改的脚本应与以下显示相似：

代码实例 7-3 修改的脚本的输出样例

```
DIR="'/bin/dirname $0'"
export DIR
. ${DIR}/driver.init
. ${DIR}/config.driver
JASS_SCRIPTS="
                minimize-firewall.fin
                fw1-patch-install.fin"
. ${DIR}/driver.run
. ${DIR}/xsp-firewall-hardening.driver
```

6. **使用以下命令检查 `rules` 文件条目以纠正错误。**

代码实例 7-4 检查 `rules` 文件以纠正错误

```
# pwd
/jumpstart
# ./check
Validating rules...
Validating profile Profiles/end-user.profile...
Validating profile Profiles/xsp-minimal-firewall.profile...
Validating profile Profiles/test.profile...
Validating profile Profiles/entire-distribution.profile...
Validating profile Profiles/oem.profile...
The custom JumpStart configuration is ok.
```

这时，应该能够在客户机（本例中为 `jordan`）上开始 JumpStart 安装。使用 JumpStart 配置和创建的 Solaris Security Toolkit 驱动程序、 finish 脚本与配置文件。

7. **如果在检查 `rules` 文件时遇到问题，请参阅第 91 页 “验证和检查 rules 文件”。**

8. **在客户机的 `ok` 提示符下，输入以下命令以使用 JumpStart 基础结构安装客户机。**

```
ok> boot net - install
```

如果不能构建客户机，请检查配置并对其进行修改直到它能正常运行。注意，本节并未提到 JumpStart 配置的所有方面。有关更多细节，请参阅 Sun BluePrints 书籍 *《JumpStart Technology: Effective Use in the Solaris Operating Environment》*。

正确运行 `rules` 文件并验证所安装的修补程序是正确的之后，可以开始进行客户机系统基础级别的安装并最小化系统和加强安全性。

验证和检查 rules 文件

当验证 `rules` 文件以纠正错误时，可能会遇到多种问题。本节提到了一些最常见的问题。

第一次运行 rules 文件会产生以下输出结果。

代码实例 7-5 rules 文件的输出样例

```
# pwd
/jumpstart
# ./check
Validating rules...
Validating profile Profiles/xsp-minimal-firewall.profile...
Error in file "rules", line 20
hostname jordan - Profiles/xsp-minimal-firewall.profile Drivers/xsp-
firewall-secure.driver
ERROR: Profile missing:
   Profiles/xsp-minimal-firewall.profile
```

在本例中，不存在 jordan 的 rules 条目中指定的配置文件。配置文件 xsp-minimal-firewall.profile 没有在配置文件目录中出现。典型地，此错误产生的原因是文件名拼写错误，忘记为配置文件指定正确的路径或者还没有创建配置文件。修正错误并再次进行检查。

第二次运行操作会暴露两个其他问题。第一个问题是在 xsp-firewall-secure.driver 中调用的驱动程序。 xsp-firewall-secure.driver 没有调用 xsp-firewall-hardening.driver，而仍然调用 hardening.driver。

第二个问题是将 JASS_SCRIPTS 变量错误地设定为 minimize-Sun_ONE-WS.fin 而不是 minimize-firewall.fin。

以下是错误的脚本。

代码实例 7-6 错误脚本样例

```
#!/bin/sh
DIR="`/bin/dirname $0`"
export DIR
. ${DIR}/driver.init
. ${DIR}/config.driver
JASS_SCRIPTS="minimize-Sun_ONE-WS.fin"
. ${DIR}/driver.run
. ${DIR}/hardening.driver
```

以下是一个正确脚本的样例。

代码实例 7-7 正确脚本样例

```
#!/bin/sh
DIR="`/bin/dirname $0`"
export DIR
. ${DIR}/driver.init
. ${DIR}/config.driver
JASS_SCRIPTS="
minimize-firewall.fin"
. ${DIR}/driver.run
. ${DIR}/xsp-firewall-hardening.driver
```

定制加强安全性配置

所建议防火墙的加强安全性配置可随时进行定制与调整。初始脚本基于 `hardening.driver`。这意味着系统进入“屏蔽墙”状态，即所有的服务程序都被禁用。

因为 Solaris 8 OS 不包含 Secure Shell 客户机，所以需要进行修改以允许对防火墙进行远程的基于网络的管理。本案例中提到的防火墙，要求 FTP 服务必须保持启用而且必须安装 Secure Shell 客户机以进行远程管理。将这两项服务限制到仅用于私用管理网络，从而不启动对任何其他网络接口的监听。有关限制这些服务的信息，请参阅 Sun BluePrints OnLine 上名为“Solaris Operating Environment Security: Updated for Solaris 9 Operating Environment”的文章。

除了保留这两项服务处于启用状态外，也保留 RPC 服务处于启用状态，以便能够使用 Solstice DiskSuite 图形用户界面 (GUI) 将 Solstice DiskSuite 配置为进行磁盘镜像配置。如果不准备使用 Solstice DiskSuite GUI，则不需要 RPC 服务。本例中，需要使用 GUI 因而要保持启用 RPC 服务。请注意，Solstice DiskSuite 的安装与配置超出了本书的范围。

本客户机所需的最终修改是使用 xSP 的中央 SYSLOG 服务器手动定制 `syslog.conf` 脚本。该定制的 `syslog.conf` 文件必须安装在防火墙系统中的每台计算机上。

这些修改需要更改许多 Solaris Security Toolkit 配置选项。在以下几节中详细介绍每个所需的修改。

- 第 94 页“启用 FTP 服务”
- 第 94 页“安装 Secure Shell 软件”
- 第 95 页“启用 RPC 服务”
- 第 96 页“定制 `syslog.conf` 文件”

启用 FTP 服务

对于本案例中的防火墙，请保留 FTP 服务处于启用状态。

▼ 启用 FTP 服务

1. **要保留 FTP 服务处于启用状态，请设定 `JASS_SVCS_DISABLE` 和 `JASS_SVCS_ENABLE` 变量以修改 `update-inetd-conf.fin` 文件的缺省操作。**

   要禁用除 FTP 之外所有标准的 Solaris OS 服务，对于本案例的最佳方法是将 `JASS_SVCS_ENABLE` 定义为 `ftp`，而确保 `JASS_SVCS_DISABLE` 保留为从 `finish.init` 脚本中获得的缺省值。请参阅 *《Solaris Security Toolkit 4.1 Reference Manual》*。

2. **要通过环境变量实现更改，请在调用 `xsp-firewall-hardening.driver` 之前，向 `xsp-firewall-secure.driver` 添加一条与以下相似的条目。**

```
JASS_SVCS_ENABLE="ftp"
```

3. **通过防火墙软件实现 FTP 服务以确保它仅在 xSP 的管理网络上可用。**

   其中的另一项要求是 FTP 应该仅在 xSP 的管理网络上可用。在 Solaris 8 OS 中，既可以通过在系统上使用 TCP 封装器，又可以通过防火墙软件本身来实现此要求。在本案例中，是通过防火墙软件实现此要求的。

安装 Secure Shell 软件

因为 Solaris 8 OS 不包含 Secure Shell 客户机，所以请安装一台 Secure Shell 客户机用于远程管理。

可以配置 Solaris Security Toolkit 软件以安装 OpenSSH 工具。请使用列在 `config.driver` 文件（由 `xsp-firewall-secure.driver` 使用）中的 `install-openssh.fin` 脚本。

▼ 安装 Secure Shell

1. **将缺省的 `config.driver` 复制到 `xsp-firewall-config.driver`。**
2. **在文件的副本中，去掉 `install-openssh.fin` 的注释条目。**
3. **修改 `xsp-firewall-secure.driver` 的条目使其原本调用 `config.driver` 转而调用 `xsp-firewall-config.driver`。**

4. **获得 OpenSSH 的最新版本。**

   与修补程序和 OS 版本一样，请使用 OpenSSH 的最新版本。有关最新版本信息，请参见 OpenSSH 网页：

   `http://www.openssh.org`

5. **编译最新的 OpenSSH 软件包，进行适当命名并将它安装到 `Packages` 目录下。**

   有关本软件包的更多信息，请参阅 Sun BluePrints OnLine 中名为 “Configuring OpenSSH for the Solaris Operating Environment”的文章。

6. **更新 `install-openssh.fin` 脚本以反映正确的 OpenSSH 软件包名称。**

   可能需要修改 `install-openssh.fin` 脚本。该脚本将 OpenSSH 软件包名称定义为与以下格式相似：

   ```
   OBSDssh-3.5p1-sparc-sun4u-5.8.pkg
   ```

   其中，软件包名称后紧跟版本号 (`3.5p1`)、体系结构 (`sparc`)、体系结构版本号 (`sun4u`)、软件包编译所针对的操作系统 (`5.8`) 和一个 `pkg` 后缀。

7. **通过防火墙软件实现 SSH 以确保它仅在 xSP 的管理网络上可用。**

   其中声明的另一项要求是 Secure Shell 仅在 xSP 的管理网络上可用。在 Solaris 8 OS 中，既可以通过系统使用 TCP 封装器，又可以通过防火墙软件本身来实现此要求。在本案例中，是通过防火墙软件实现此要求的。请注意也可以通过修改 Secure Shell 服务器的配置来实现此项要求。

启用 RPC 服务

保留 RPC 服务处于启用状态，从而可以使用 SDS 做磁盘镜像，这需要 RPC 服务。

因为在 Solaris Security Toolkit 运行过程中可使用一个特定 finish 脚本 `disable-rpc.fin` 禁用 RPC 服务，所以此修改是相对简单的。

注 – 系统的防火墙配置应该明确拒绝远程访问系统 RPC 服务。

▼ 启用 RPC

- **为 `xsp-firewall-hardening.driver` 中的 `disable-rpc.fin` 的条目加注释。**

  通过为驱动程序中的脚本加注释符而不是直接删除它们来最终禁用这些脚本。在为 `JASS_SCRIPTS` 中定义的条目添加注释符时要小心，因为只可以接受特定的注释值的组合。

以下为包含在 driver.funcs 脚本中的注释，说明了 Solaris Security Toolkit 软件可作为注释而接受的定义在 JASS_SCRIPTS 中的注释符。

```
#Very rudimentary comment handler. This code will only recognize
#comments where a single '#' is placed before the file name
#(separated by white space or not). It then will only skip the
#very next argument.
```

定制 syslog.conf 文件

本客户机所需的最终修改是使用 xSP 的中央 SYSLOG 服务器手动定制的 syslog.conf 脚本。该定义的 syslog.conf 文件必须安装在防火墙系统中的每台计算机上。

▼ 定制 syslog.conf 文件

1. **复制 xSP 的标准 syslog.conf 文件，将它重命名为 syslog.conf.jordan，再将其放到 Files/etc 目录中。**

   Solaris Security Toolkit 软件支持几种不同的复制文件模式。对于此配置最适当的选项是将系统主机名作为后缀附加到文件，以便只将 syslog.conf 文件复制到 jordan，因为它有唯一的防火墙专用修改。在本例中，客户机叫作 jordan，因而 Files/etc 中使用的实际文件名是 syslog.conf.jordan。注意，请勿为 JASS_FILES 定义添加此后缀，这点是非常重要的。有关后缀的更多信息，请参阅 *《Solaris Security Toolkit 4.1 Reference Manual》*。

2. **如果 xSP 标准的 syslog.conf 文件不可用，则按照如下所示创建一个定制文件 syslog.conf。**

   a. **复制包含在 Solaris Security Toolkit 中的 syslog.conf 文件，然后将它重新命名为 syslog.conf.jordan，再将其放到 Files/etc 目录中。**

   b. **修改 syslog.conf.jordan 以使它符合 xSP 有关 SYSLOG 的标准。**

3. **验证 /etc/syslog.conf 文件已列在 xsp-firewall-hardening.driver 的 JASS_FILES 定义中。**

   缺省情况下， xsp-firewall-hardening.driver 中的 JASS_FILE 定义会显示为如下。

代码实例 7-8 修改的 xsp-firewall-hardening.driver 输出样例

```
JASS_FILES="
                    /etc/dt/config/Xaccess
                    /etc/init.d/inetsvc
                    /etc/init.d/nddconfig
                    /etc/init.d/set-tmp-permissions
                    /etc/issue
                    /etc/motd
                    /etc/notrouter
                    /etc/rc2.d/S00set-tmp-permissions
                    /etc/rc2.d/S07set-tmp-permissions
                    /etc/rc2.d/S70nddconfig
                    /etc/syslog.conf
"
```

这时，所有需要的修改已完成。OS 的安装、最小化和加强安全性操作已为特定的应用程序进行了定制并完全自动化。唯一没有完全自动化的过程是防火墙软件和 Solstice DiskSuite 的配置及安装。虽然可以使用 JumpStart 技术进行这些配置，但已超出了本书的范围。请参阅 Sun BluePrints 书籍 *《JumpStart Technology: Effective Use in the Solaris Operating Environment》*。

安装客户机

对驱动程序做完所有修改后，请按本节所述安装客户机。

▼ 安装客户机

1. **对驱动程序进行所有要求的修改后，请使用 JumpStart 基础结构安装客户机。**

   在客户机中的 ok 提示符下使用以下命令。

```
ok> boot net - install
```

2. **如果出现错误，请修正它们并重新安装客户机的 OS。**

质量保证测试

保护系统安全过程的最终任务涉及验证系统提供的应用程序和服务是否正常运行。同时，此任务还验证安全性配置文件是否成功地实现了所需的修改。

非常重要的一点是，重新引导已加强安全性并最小化的平台后要全面完成此任务，以确保可以检测到并能够迅速纠正出现的任何异常和问题。本过程分为两个任务：验证配置文件安装和验证应用程序与服务的功能。

▼ 验证配置文件安装

要验证 Solaris Security Toolkit 软件正确地且没有任何错误地安装了安全性配置文件，请按以下进行检查与评估。

1. **检查安装日志文件。**

   此文件安装在 `JASS_REPOSITORY/jass-install-log.txt` 中。

注 – 此日志文件可以作为参考以准确理解 Solaris Security Toolkit 软件对系统所做的工作。对于系统上的每个运行操作，都会根据运行操作起始时间在目录中保存一个新的日志文件。请勿直接修改这些文件和 `JASS_REPOSITORY` 目录中的其他文件。

---

2. **使用审计选项评估系统的安全性配置。**

   有关审计选项的详细信息，请参阅第 2 章。本案例中，使用安装了 Solaris Security Toolkit 软件的客户机目录中的以下命令。

代码实例 7-9 评估安全性配置

```
# ./jass-execute -a xsp-firewall-secure.driver
[NOTE] Executing driver, xsp-firewall-secure.driver
================================================================
===
xsp-firewall-secure.driver: Driver started.
================================================================
===


================================================================
===
Solaris Security Toolkit Version:   4.1.0
[...]
```

   如果在对 Solaris Security Toolkit 运行操作验证时遇到任何不一致，请记下它们。运行操作结尾处的摘要会报告所发现的不一致总数。运行操作的全部输出位于 JASS_REPOSITORY 目录中。

▼ 验证应用程序和服务的功能

应用程序和服务的验证过程包括一个明确的测试和一个验收规划。此规划用于使用系统中各种各样的组件或者应用程序以确定它们可用且运行良好。如果这样的规划不可用，则要根据系统的运行方式以合理的方法对系统进行测试。目的是确保加强安全性过程决不会影响应用程序或服务执行其功能。

1. **如果在加强系统安全性之后，发现了应用程序或者服务的故障，请使用第 2 章中所述的技术确定问题。**

   例如，使用 truss 命令。此命令通常用于确定应用程序出现问题的故障点。一旦了解后，即可找到问题并跟踪返回到 Solaris Security Toolkit 软件所做的更改。

注 – 根据许多部署过 Solaris Security Toolkit 软件人员的共同经验，使用本书中的方法可以避免大多数问题。

---

2. **以相似的方式测试 Check PointFirewall-1 NG 软件，并将问题跟踪返回到 Solaris Security Toolkit 软件所做的更改然后纠正这些问题。**

3. **如果软件包的最终列表需要修改，则修改配置文件，重新安装系统再重复测试。**

术语表

本列表定义了 Solaris Security Toolkit 中涉及的单词缩写和首字母缩写词。

A

ab2 AnswerBook2

ABI Application Binary Interface （应用程序二进制接口）

ARP Address Resolution Protocol （地址解析协议）

ASPPP Asynchronous Point-to-Point Protocol （异步点对点协议）

B

BIND Berkeley Internet Name Domain （Berkeley Internet 名称域）

BSD Berkeley Software Distribution （Berkeley 软件分发）

BSM Basic Security Model （基本安全模型）， *Solaris*

C

CD compact disc （紧凑型光盘）

CD-ROM compact disc-read-only memory （紧凑型光盘 — 只读存储器）

CDE Common Desktop Environment （公用桌面环境）

cp(1) copy files （复制文件）

cron(1M) clock daemon （时钟守护进程）

D

DHCP Dynamic Host Configuration Protocol （动态主机配置协议）

DMI Desktop Management Interface （桌面管理界面）

DMTF Distributed Management Task Force （分布式管理任务组）

DNS Domain Name System （域名系统）

E

EEPROM electronically erasable programmable read-only memory（加电可擦写的可编程只读存储器）

F

FTP File Transfer Protocol （文件传输协议）

G

GID group identifier （组标识）

H

HTTP HyperText Transfer Protocol （超文本传输协议）

I

ID identifier （标识符）

IETF Internet Engineering Task Force （Internet 工程任务组）

INETD Internet service daemon （Internet 服务守护进程）

IP Internet Protocol （Internet 协议）

ISA instruction set architecture （指令集体系结构）

J

JASS JumpStart Architecture and Security Scripts （JumpStart 体系结构和安全脚本），*现在是* Solaris Security Toolkit

K

KDC Kerberos Key Distribution （Kerberos 密钥分发）

L

LDAP Lightweight Directory Access Protocol （轻量目录访问协议）

`lp`**(1)** line printer （行式打印机），*提交打印请求*

M

MAN management network （管理网络）， *Sun Fire High-End Systems 内部 I1 网络*

MD5 message-digest 5 algorithm （message-digest 5 算法）

MIP Mobile Internet Protocol （移动 Internet 协议）

MSP midframe service processor （中型服务处理器）

`mv`**(1)** move files （移动文件）

N

NFS Network File System （网络文件系统）

NG Next Generation （下一代）

NIS, NIS+ Network Information Services （网络信息服务）

NSCD name service cache daemon （名称服务高速缓存守护进程）

O

OE operating environment （操作环境），*以前用于 Solaris*

OEM Original Equipment Manufacturer （原始设备制造商）

OS Operating System （操作系统），*现在用于 Solaris*

P

PAM Pluggable Authentication Module （可插拔验证模块）

PDF Portable Document Format （可移植文档格式）

PICL Platform Information and Control Library （平台信息和控制库）

PPP Point-to-Point Protocol （点对点协议）

PROM programmable read-only memory （可编程只读存储器）

Q

QA quality assurance （质量保证）

R

RBAC role-based access control （基于角色的存取控制）

rc run-control （运行控制），*文件或脚本*

`rlogin`**(1)** remote login （远程登录）

RFC Remote Function Call （远程功能调用）

RPC Remote Procedure Call （远程过程调用）

`rsh`**(1)** remote shell （远程 shell）

S

SA system administrator （系统管理员）

SC system controller （系统控制器）， *Sun Fire High-End Systems 和 Sun Fire Midrange Systems*

`scp`**(1)** secure copy （安全复制），远程文件复制程序

SCCS Source Code Control System （源代码控制系统）

SLP Service Location Protocol （服务定位协议）

SMA System Management Agent （系统管理代理）

SMC Solaris Management Console

SNMP Simple Network Management Protocol （简单网络管理协议）

SP service provider （服务提供商）

SPARC Scalable Processor Architecture （可伸缩的处理器体系结构）

SPC SunSoft Print Client （SunSoft 打印客户机)

SSH Secure Shell （安全 Shell）， *Solaris*

SSP system service processor （系统服务处理器）， *Sun Enterprise 10000 服务器*

`stdio` standard input/output （标准输入/输出）

Sun ONE Sun Open Network Environment （开放式网络环境），*现在是* Sun Java System，*以前是* iPlanet

T

TCP Transmission Control Protocol （传输控制协议）

`tftp`**(1)** trivial file transfer program （琐碎文件传输程序）

`ttl` time-to-live （生存时间）

U

U.S. United States （美国）

UDP User Diagram Protocol （用户图表协议）

UID user identifier （用户标识）

UUCP UNIX-to-UNIX Copy （UNIX 对 UNIX 复制）

V

VOLD Volume Management daemon （Volume Management 守护进程）

W

WBEM Web-based Enterprise Management （基于 Web 的企业管理）

索引

符号

/opt/jass-*n.n* 目录, 32
/usr/bin/ldd 命令, 19

数字

32 位最小化系统, 66
32-bit-minimal.profile, 66

A

add_install_client 命令, 68
add_to_manifest 功能, 53
add-client 脚本, 3, 68
案例, 83
安全
  要求, 15
安全, 监视, 28
安全, 维护, 27
安全策略
  标准, 15
  查看, 17
  开发, 17
安全漏洞
  策略, 28
  分析, 16
  扫描, 16
安全配置, 评估, 27
安全性配置文件
  创建，案例, 85
  模板, 73
  嵌套或分层, 25
  缺省, 28
  验证, 49
  验证安装，案例, 98
安全性评估
  配置, 48
  执行, 80
安全性软件，下载, 31
安全性状态
  检查, 72
  审计, 72
安全性，维护, 71
安装
  安装后的任务, 26
  备份, 26
  标准化, 63
  规划, 29
  加强系统, 30
  客户机，案例, 97
  日志文件, 27
  软件, 25
  软件，案例, 85
  使 Solaris OS 自动化, 10
  新系统，案例, 83
  修补程序, 9
  验证, 26
  之后进行审计, 80

准则, 2
自动化, 2, 63
自动化修补程序, 9
安装前的任务, 26

B

-b 选项，撤消, 55, 56
backup_file 助手功能, 53
BSM, 36
-b选项，撤消, 55
版本控制, 10
报告，电子邮件通知, 56
保护经过部署的系统的安全, 16
保护系统安全, 方法论, 15
保留选项, 56
备份
撤消运行前的要求, 57
审计, 80
在安装之前, 26
备份软件, 清点, 18
备份文件
缺省操作, 52
被利用的系统, 16
编译器，安装警告, 37
编译器，限制, 37
标准, 安全策略, 17
标准, 跨平台强制执行, 25
不能构建客户机，案例, 91
部署系统, 63
部署最小化和安全的系统, 83
不一致的状态, 56

C

Check point Firewall-1 NG, 83
comment handler, 96
core.profile, 66
cp 命令, 53
测试功能, 26
测试和验收计划, 27
测试，在非生产系统上, 33
查看日志文件, 26
差异，发现, 48
超时, 程序, 22
撤消
保留选项, 56
备份选项, 55
不可用的, 52
撤消运行, 57
电子邮件选项, 56
记录并恢复更改, 51
交互式运行, 54
静止选项, 56
命令行选项, 47
强制选项, 55
使用所需信息, 51
手动撤消更改, 53
输出选项, 56
数据信息库, 10
限制, 52
选项, 55
选择运行，输出样例, 58
运行，解决文件修改, 60
运行，列表, 58
创建安全性配置文件，案例, 85
从属性
确定, 24
未识别的, 16
存储的状态, 82
错误
解析 sysidcfg 文件时， JumpStart 模式, 65
破坏内容, 52
系统崩溃, 52
消息或警告, 26
错误修正，修补程序, 33
错误诊断, 16
撤消运行, 53
系统修改, 48
重新引导, 保护系统安全, 16

D

-d 驱动程序选项限制, 44
Developer Solaris OS 群集， SUNWCprog, 66
developer.profile, 66
DNS 服务, 21
driver.init 文件
  概述, 5
dtexec 进程, 24
电子邮件通知选项, 44
调试服务, 23
定期审计, 72
定制
  安全性审计, 72
  策略和要求, 12
  Solaris Security Toolkit, 11
  syslog.conf 文件, 96
  准则, 12
定制配置，案例, 84
独立模式, 31
  使用, 40
  执行, 41
端口, 确定使用情况, 24
对审计输出进行排序, 79
对使用的审计, 15
多宿主的 JumpStart 服务器, 64

E

End User Solaris OS 群集， SUNWCuser, 66
end-user.profile, 66
Entire Distribution Solaris OS 群集，SUNWCall, 66
entire-distribution.profile, 66
二进制，验证, 38

F

files 目录, 7
Finish 脚本
  撤消功能, 52
  创建新的, 52
Finish 目录, 8
finish.init 文件
  驱动程序流程, 6
FixModes
  FixModes.tar.Z 文件, 35
  软件，下载, 35
FTP
  服务，启用，案例, 94
  缺省配置, 17
返回值, 20
方法论, 保护系统安全, 15
访问权限，保护, 35
访问网络，保护, 36
风险和益处, 考虑, 15
服务
  根据需要确定, 23
  清点, 18
  RPC, 93
  退出, 挂起, 或退出, 21
  限制, 93
  要求, 16
  识别, 16
  最近使用的, 确定, 23
服务框架, 21
服务要求, 确定, 18

G

根
  目录, 32
  选项, 46
跟踪更改, 51
更改控制策略, 26
更改原始文件, 12
更强的身份验证, 17
攻击
  值，定义的, 82
工具，可选的, 38
功能
  测试, 26
  添加, 72
  问题, 16
  修补程序, 33

共享库, 18
故障, 27
故障, 应用程序, 26
故障检查, 79
关键环境变量, 25
关键组件, 1
管理软件, 清点, 18
管理协议, 策略示例, 17
规划阶段, 15
规划与准备，案例, 83
规划，安装, 29

H

后门访问，二进制文件, 37
环境变量
  导入, 6
环境，配置, 30
恢复更改, 51

I

iPlanet Web Server
  请参见 Sun ONE Web Server

J

JASS, 1
jass 子目录, 33
JASS_DISPLAY_HOSTNAME 变量, 79
JASS_DISPLAY_SCRIPTNAME 变量, 79
JASS_DISPLAY_TIMESTAMP 变量, 79
JASS_HOME_DIR 环境变量，定义, 32
JASS_LOG_BANNER 环境变量, 77
JASS_LOG_ERROR 环境变量, 77
JASS_LOG_FAILURE 环境变量, 77
JASS_LOG_SUCCESS 环境变量, 78
JASS_LOG_WARNING 环境变量, 78
JASS_REPOSITORY
  撤消运行, 51
  检查内容, 53
  修改内容, 51
jass-check-sum 程序, 3
jass-check-sum 命令, 53
jass-execute -a 命令, 80
jass-execute -a 命令选项, 74
jass-execute 命令选项, 40
jass-execute -u 命令, 54
jass-manifest.txt 文件, 51
jass-*n.n*.tar.Z文件, 32
jass-undo-log.txt 文件, 58
基本安全模块 (BSM), 36
基础结构, 15
基础结构组件, 18
基础结构，准备，案例, 89
记录
  操作, 51
记录结果, 21
JumpStart 服务器
  多宿主的, 64
  将软件下载到, 31
  配置与管理, 63
  配置，案例, 88
JumpStart 技术, 31, 63
JumpStart 技术，受支持的 OS 版本, 63
JumpStart 客户机
  安装客户机，案例, 97
  不能构建，案例, 91
  添加，案例, 89
  文件, 存储, 7
JumpStart 模式
  安装, sysidcfg 目录, 10
  脚本, 67
  解析 sysidcfg 文件时出现错误, 65
  配置, 31, 63, 64
  使用所选脚本, 65
  使用所有脚本, 65
  修改 sysidcfg, 64
JumpStart 配置文件, 65
  模板, 65
  目录, 10

JumpStart 体系结构和安全脚本 (JASS), 1
JumpStart 体系结构，集成 Solaris Security Toolkit, 63
基于主机的访问控制, 16
集中的 syslog 信息库, 28
加密, 17
加密软件, 36
加强系统安全性, 已定义, 1
加强运行
  撤消列表, 58
  恢复更改, 57
  执行 Solaris Security Toolkit, 38
假设与限制，案例, 84
检查
  故障, 79
  添加, 72
检查安全性状态, 72
监视安全, 28
监视软件, 清点, 18
脚本
  JumpStart 模式, 67
  列表, 5
  命名, 13
  修改，警告, 65
较慢的网络连接，使用静止输出, 56
结构, 软件, 2
结果, 记录, 21
解决文件修改, 60
进程
  标识符, 20
  确定哪些正在使用文件和端口, 24
警告消息
  在系统引导或应用程序启动时显示, 26
  执行 Solaris Security Toolkit 软件, 35
经过部署的系统
  安装软件, 25
  保护, 16
静止选项, 46

K

Kerberos, 17
kill 命令, 22
可操作的或管理功能, 清点, 18
客户机
  从 JumpStart 服务器删除, 69
  从 JumpStart 服务器添加, 68
口令
  策略示例, 17
  passwd(1) 命令, 17
库, 共享, 18
快速加强系统, 31
框架, 服务, 21
框架，定制 Solaris Security Toolkit, 52
扩展, 17

L

LDAP, 21
ldd 命令, 23
librpcsvc.so.1 项, 23
lsof 程序, 24
lsof 程序, 获得, 24
历史记录选项, 45
联机的 SunSolve 网站, 34
列出打开的文件的程序, 24

M

-m 选项
  撤消, 56
  审计, 75
make-jass-pkg 程序, 3
man 目录, 4
MD5 二进制文件, 37
MD5 软件
  md5.tar.Z文件, 37
  下载, 37
minimal-Sun_ONE-WS-Solaris*.profile, 67
命令行选项
  帮助, 42
  帮助，审计, 74
  撤消, 47, 55

电子邮件通知, 44
根, 46
jass-execute 命令, 40
静止, 46
历史记录, 45
驱动程序, 43
审计, 42, 73
输出文件, 46
最近执行, 45
命名标准
安装, 8
定制文件, 13
Solaris OS, 8
命名服务, 21
命名文件, 标准, 13
模板，配置文件, 65
模式, 31
目录
/opt/jass-*n.n*, 32
finish 脚本, 8
JumpStart 配置文件, 10
结构, 3
列表, 3
man, 4
命名, 8
OS, 8
启动, 7
驱动程序, 5
软件包, 9
sysidcfg, 10
审计脚本, 4
文件, 7
修补程序, 9
运行, 51

N

netstat 命令, 23
NFS
应用程序依赖于, 23
NIS, 21

O

-o 选项，撤消, 56
-o 选项，审计, 76
OEM Solaris OS 群集， SUNWCXall, 67
oem.profile, 67
OpenSSH
编译, 37
创建及配置, 36
软件，下载, 36
OS
目录, 8
OS 群集，指定和安装，案例, 87
OS 映像, 8

P

pfiles 命令, 24
pkg 格式, 32
pkgadd 命令, 33
pkill 命令, 22
ps 命令, 22
配置
安全性评估, 48
定制，案例, 84, 93
JumpStart 服务器, 63
JumpStart 服务器，案例, 88
JumpStart 模式, 64
检查准则, 48
监视和维护, 28
脚本, 9
配置环境, 29
评估，案例, 99
审计, 72
审计报告, 79
信息, 驱动程序, 5
正在运行的和存储的之间的差异, 26
准则, 2
自动化, 2
配置文件
规划和准备, 15
JumpStart, 10, 65
JumpStart 配置文件, 10

检查, 82
目录, 10
确定是否正在使用, 20
修改, 65
主要, 5
屏蔽墙, 93
评估系统, 72
平台最小化, 20
破坏内容，文件, 52

Q

-q 选项，撤消, 56
-q 选项，审计, 76
启动目录, 7
嵌套或分层安全性配置文件, 25
强身份验证, 36
强制选项, 55
清单文件, 52
清单文件项
处理多个, 58
情形，保护系统安全, 83
驱动程序
命名, 13
目录, 5
配置信息, 5
驱动程序控制流程, 6
驱动程序目录, 5
驱动程序选项, 43
驱动程序， JumpStart 服务器, 65
权限
对象，缺省, 35
限制, 35
权限管理, 16
权限，保护, 35
确定保留为启用状态的 OS 服务, 48
确定动态加载的应用程序, 19
缺省
安全性配置文件, 28
配置, FTP 和 Telnet, 17

R

rc 脚本，审计运行, 72
Recommended and Security Patch Cluster
下载, 33
Recommended and Security Patch Clusters
存储, 9
reverse-jass-manifest.txt文件, 52
rm_install_client 命令, 69
rm-client 脚本, 3, 69
RPC
端口映射器, 21
服务, 93
rpcinfo 命令, 21, 22
rules 文件
JumpStart 服务器, 65, 67
检查，案例, 91
rusers 命令, 21
日志
考虑, 15
日志文件
安装, 27
查看, 26
冗长级别, 76
入侵检测, 16
软件安装, 脚本, 9
软件包
目录, 9
添加非 pkg 格式的软件包, 53
软件包名称，案例, 95
软件包目录, 9
软件包，添加非 pkg 格式的软件包, 53
软件组件, 2

S

SCCS, 11
scp命令, 34
Secure Shell
安装，案例, 94
产品要求, 32
创建及配置, 36
软件，获得商业版本, 36

软件，下载, 36
商业版本，编译, 37
secure.driver，执行, 41
SI_CONFIG_DIR，在子目录中安装软件, 64
SIGHUP 信号, 22
SNMP, 23
Solaris Fingerprint Database Companion, 38
Solaris Fingerprint Database Sidekick, 38
Solaris OS
服务，检查, 48
命名标准, 8
群集， SUNWCreq, 66
软件包格式, 32
修正, 33
映像, 8
Solaris Security Toolkit
软件，下载, 32
为 JumpStart 模式安装, 64
Solaris 指纹数据库, 37
Solstice DiskSuite™, 85
Sun ONE Web Server, 9
SUNWjass, 删除, 13
SUNWjass目录, 33
SUNWjass-*n.n*.pkg, 33
sysidcfg
目录, 10
文件, 65
文件, 修改, 13
文件样例, 10
文件，版本限制, 64
文件，为 JumpStart 模式做修改, 64
syslog
syslog.conf 文件，定制, 96
消息, 日志, 28
信息库, 28
删除 SUNWjass, 13
删除客户机，从 JumpStart 服务器, 69
设计, Solaris Security Toolkit 软件, 1
身份验证
服务, 21
更强, 17
强, 36
审计
案例, 99
安全性评估, 80
备份，警告, 80
标题, 77
电子邮件选项, 75
定期的, 72
定制, 72
仅报告失败, 78
进程, 82
静止选项, 76
控制输出, 73
命令, 74
排序输出, 79
配置报告, 79
日志项，示例, 79
输出选项, 76
显示结果, 76
消息, 77
选项, 73
主机名称、脚本名称和时间戳信息, 79
自动化, 71
最小扫描, 72
审计, 限制, 2
审计, 已定义, 1
审计策略, 28
审计脚本
定制, 72
目录, 4
所有权, 73
相匹配的驱动程序, 52
审计系统, 71
审计选项, 42
审计，定义的, 71
生命周期，维护安全性, 49
示例，配置文件, 65
使系统安装标准化, 63
手动查看, 安全, 28
手动更改，在撤消过程中保留, 56
守护进程作业，审计运行, 72
守护进程作业，使用静止输出选项, 56
守护进程，禁用, 36
收集信息, 正在运行的进程, 19

受支持的版本
SMS, 11
Solaris OS, 11
输出
禁用, 46
排序审计, 79
审计运行示例, 81
最小化, 78
输出选项
撤消, 56
审计, 76
文件, 46
数据完整性, 16
数据信息库, 10
数字指纹, 37
私用管理网络, 93
sun4u, 37
所有权的驱动程序和脚本, 73

T

tar命令, 32
TCP 封装器, 95
Telnet，启用, 73
truss 命令, 19, 27
ttsession 进程, 24
特洛伊，定义, 37
提取修补程序, 9
体系结构, Solaris Security Toolkit 软件, 4
添加 JumpStart 客户机，案例, 89
添加客户机，从 JumpStart 服务器, 68
停机时间, 16
通知，在撤消过程中产生, 56
脱机, 保护系统安全, 16

U

uncompress 命令, 33
undo-log.txt文件, 52
user.init 文件, 6
user.init.SAMPLE, 用途, 13
user.run.SAMPLE, 用途, 13

W

Web 站点，资源列表, xxii
完整性
二进制文件，检查, 37
可执行文件，验证, 37
软件，下载, 38
数据, 16
文件系统, 16
完整性管理解决方案, 11
维护安全, 27
维护安全性, 71
维护版本控制, 10
维护窗口, 16
文档目录, 4
稳定性, 33
文件
不一致, 56
JumpStart 客户机, 存储, 7
检查手动更改, 54
列出并检查更改, 53
命名标准, 13
目录, 7
配置文件, 65
破坏内容, 52
确定使用情况, 24
sysidcfg, 13
修改, 12
文件名, 32
文件系统
完整性, 16
文件系统对象
获得信息, 19
文件校验和, 53
文件样例, sysidcfg, 10
问题, 26

X

系统

安全漏洞, 28
崩溃, 52
调用, 20
二进制，验证, 38
配置, 监视和维护, 28
稳定性, 验证, 26
要求，案例, 84
引导, 消息, 26
状态, 18
下载安全性软件, 31
显示帮助选项, 42
显示帮助选项，审计, 74
限制编译器, 37
限制服务, 93
相关资源, xviii
消息，审计, 77
校验和, 53
性能
Solaris OS 修补程序, 33
修补程序, 33
安装, 9
安装后重新加强系统, 31
创建子目录, 9
覆盖配置文件, 28
命名目录, 9
目录, 9
README 文件, 34
提取, 9
添加未安装的修补程序, 73
移动文件, 34
修改
代码, 12
配置文件, 65
修改，跟踪, 51
修改，验证, 48
需要的软件, 32
选项
帮助, 42
帮助，审计, 74
备份，撤消, 55
撤消命令, 55
电子邮件通知, 44
电子邮件，撤消, 56
电子邮件，审计, 75
根, 46
jass-execute 命令, 40
静止, 46
静止，撤消, 56
静止，审计, 76
历史记录, 45
驱动程序, 43
审计, 42, 73
输出文件, 46
最近执行, 45

Y

压缩的tar 归档格式, 32
验证
安全性配置文件安装, 27
功能, 多次重新引导, 16
系统稳定性, 26
应用程序和服务功能, 27
验证, 在安装之前, 26
验证安全性配置文件, 49, 71
验证过程, 21
要求
安全, 17
撤消加强运行, 52
服务, 16
服务, 确定, 18
收集, 20
应用程序, 16
异常行为, 21
移动修补程序文件, 34
以太网接口，案例, 84
应用程序
清点, 18
确定动态加载的, 19
确定是否使用 RPC 端口映射器, 21
验证，案例, 98
要求, 16
识别, 16
应用程序安全性, 16

应用程序启动, 消息, 26
应用修补程序, 28
用户交互式服务，禁用, 36
用户交互式会话，保护, 36
用途, Solaris Security Toolkit 软件, 1
预防措施, 16
源代码, 31
源代码控制系统 (SCCS), 11
元服务, 21
源文件，下载, 32
运行目录, 51

Z

zcat命令, 32
在独立模式下执行软件, 41
责任, 15
站点专用的驱动程序，匹配审计脚本, 73
帐户管理, 16
指定并安装 OS 群集，案例, 87
质量保证 (QA) 测试, 48
执行 Solaris Security Toolkit, 38
注释标记 (#), 22
助手功能, 53
自动审计, 71
最近执行选项, 45
最小化, Solaris 操作系统, 18
最小化, 已定义, 1
最小化输出, 78