



# Solaris™ Security Toolkit 4.1.1

## 发行说明

---

Sun Microsystems, Inc.  
www.sun.com

文件号码 819-3288-10  
2005 年 8 月, 修订版 A

请将有关本文档的意见和建议提交至: <http://www.sun.com/hwdocs/feedback>

Copyright 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. 版权所有。

对于本文中介绍的产品，Sun Microsystems, Inc. 对其所涉及的技术拥有相关的知识产权。需特别指出的是（但不局限于此），这些知识产权可能包含在 <http://www.sun.com/patents> 中列出的一项或多项美国专利，以及在美国和其他国家/地区申请的一项或多项其他专利或待批专利。

本文档及其相关产品的使用、复制、分发和反编译均受许可证限制。未经 Sun 及其许可方（如果有）的事先书面许可，不得以任何形式、任何手段复制本产品或本文档的任何部分。

第三方软件，包括字体技术，均已从 Sun 供应商处获得版权和使用许可。

本产品的某些部分可能是从 Berkeley BSD 系统衍生出来的，并获得了加利福尼亚大学的许可。UNIX 是 X/Open Company, Ltd. 在美国和其他国家/地区独家许可的注册商标。

Sun、Sun Microsystems、Sun 徽标、docs.sun.com 和 Solaris 是 Sun Microsystems, Inc. 在美国和其他国家/地区的商标或注册标记。

所有 SPARC 商标的使用均已获得许可，它们是 SPARC International, Inc. 在美国和其他国家/地区的商标或注册商标。带有 SPARC 商标的产品均基于由 Sun Microsystems, Inc. 开发的体系结构。

OPEN LOOK 和 Sun™ 图形用户界面是 Sun Microsystems, Inc. 为其用户和许可证持有者开发的。Sun 感谢 Xerox 在研究和开发可视或图形用户界面的概念方面为计算机行业所做的开拓性贡献。Sun 已从 Xerox 获得了对 Xerox 图形用户界面的非独占性许可证，该许可证还适用于实现 OPEN LOOK GUI 和在其他方面遵守 Sun 书面许可协议的 Sun 许可证持有者。

美国政府权利 — 商业用途。政府用户应遵循 Sun Microsystems, Inc. 的标准许可协议，以及 FAR（Federal Acquisition Regulations，即“联邦政府采购法规”）的适用条款及其补充条款。

本文档按“原样”提供，对于所有明示或默示的条件、陈述和担保，包括对适销性、适用性或非侵权性的默示保证，均不承担任何责任，除非此免责声明的适用范围在法律上无效。



请回收



Adobe PostScript

# 目录

---

前言 v

**Solaris Security Toolkit 4.1.1 发行说明 1**

Solaris Security Toolkit 4.1.1 软件中的更改 1

所需的操作系统 2

支持 SMS 1.5 软件 2

Solaris Security Toolkit 文档 2

Solaris Security Toolkit 软件已知的局限性 3

常见注意事项和问题 3

    SMS 软件与 Solaris Security Toolkit 3

    Solaris Security Toolkit 与 CTRL-C 3

    fix-modes 显示警告 3

    Solaris Security Toolkit 问卷 4

Solaris Security Toolkit 软件中的错误 4

    undo 报告 logadm.conf 已更改（错误 ID 5067303） 4

Solaris Security Toolkit 文档勘误表 5

    “参考手册”中未列出 banner.msg（错误 ID 6177578） 5

    过时的 env var（错误 ID 6177598） 5



# 前言

---

本文档介绍针对 Solaris™ Security Toolkit 4.1.1 软件的发行说明。该软件随 Service Management System (SMS) 1.5 软件附带，其中包含了默认的安全保护特性。

---

## 阅读本文档之前

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。

由于本文档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文档。

---

## 使用 UNIX 命令

本文档不会介绍基本的 UNIX 命令和操作过程，如关闭系统、启动系统和配置设备等。欲获知此类信息，请参阅以下文档：

- 系统附带的软件文档
- 有关 Solaris OS 的文档，其网址为：

<http://docs.sun.com>

---

## Shell 提示符

Shell	提示符
C shell	<i>machine-name%</i>
C shell 超级用户	<i>machine-name#</i>
Bourne shell 和 Korn shell	\$
Bourne shell 和 Korn shell 超级用户	#

---

## 印刷约定

字体*	含义	示例
AaBbCc123	命令、文件和目录的名称；计算机屏幕输出	编辑 <code>.login</code> 文件。 使用 <code>ls -a</code> 列出所有文件。 % You have mail.
<b>AaBbCc123</b>	用户键入的内容，与计算机屏幕输出的显示不同	% <b>su</b> Password:
<i>AaBbCc123</i>	保留未译的新词或术语以及要强调的词。要使用实名或值替换的命令行变量。	这些称为 <i>class</i> 选项。 要删除文件，请键入 <b>rm filename</b> 。
<b>新词术语强调</b>	新词或术语以及要强调的词。	您 <b>必须</b> 成为超级用户才能执行此操作。
《书名》	书名	阅读《用户指南》的第 6 章。

\* 浏览器的设置可能会与这些设置有所不同。

---

## 相关文档

Solaris Security Toolkit 的联机文档可通过访问下列网址获得：

[http://www.sun.com/products-n-solutions/hardware/docs/Software/enterprise\\_computing/systems\\_management/sst/index.html](http://www.sun.com/products-n-solutions/hardware/docs/Software/enterprise_computing/systems_management/sst/index.html)

System Management Services 1.5 的联机文档可通过访问下列网址获得：

[http://www.sun.com/products-n-solutions/hardware/docs/Servers/High-End\\_Servers/Sun\\_Fire\\_e25K-e20K/SW\\_FW\\_Documentation/SMS/index.html](http://www.sun.com/products-n-solutions/hardware/docs/Servers/High-End_Servers/Sun_Fire_e25K-e20K/SW_FW_Documentation/SMS/index.html)

应用	书名	文件号码	格式	位置
管理	《Solaris Security Toolkit 4.1 管理指南》	817-7655-10	PDF HTML	联机
参考	《Solaris Security Toolkit 4.1 Reference Manual》	817-7750-10	PDF HTML	联机
手册页	《Solaris Security Toolkit 4.1 Man Page Guide》	819-0111-10	PDF	联机
SMS 1.5 安全性 管理	《System Management Services (SMS) 1.5 Administrator Guide》，第 2 章	817-7295-10	PDF HTML	联机
最新消息、错误， 以及可用的解决 方法	《System Management Services (SMS) 1.5 发行说明》	819-3301-10	PDF HTML	联机

---

## 文档、技术支持和培训

Sun 功能	URL	说明
文档	<a href="http://www.sun.com/documentation/">http://www.sun.com/documentation/</a>	下载 PDF 和 HTML 文档，订购印刷文档
技术支持	<a href="http://www.sun.com/support/">http://www.sun.com/support/</a>	获取技术支持和下载修补程序
培训	<a href="http://www.sun.com/training/">http://www.sun.com/training/</a>	学习 Sun 课程

---

## 第三方 Web 站点

Sun 对本文中提到的第三方 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、产品或其他资料，Sun 并不表示认可，也不承担任何责任。对于因使用或依靠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名义损坏或损失，Sun 概不负责，也不承担任何责任。

---

## Sun 欢迎您提出意见和建议

Sun 致力于提高文档资料的质量，并十分乐意收到您的意见和建议。请将有关本文档的意见和建议提交至：

<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 4.1.1 发行说明》，文件号码 819-3288-10



# Solaris Security Toolkit 4.1.1 发行说明

---

这些针对 Solaris Security Toolkit 4.1.1 软件的发行说明包含以下主题：

- 第 1 页 “Solaris Security Toolkit 4.1.1 软件中的更改”
- 第 2 页 “支持 SMS 1.5 软件”
- 第 2 页 “所需的操作系统”
- 第 2 页 “Solaris Security Toolkit 文档”
- 第 3 页 “Solaris Security Toolkit 软件已知的局限性”
- 第 3 页 “常见注意事项和问题”
- 第 4 页 “Solaris Security Toolkit 软件中的错误”
- 第 5 页 “Solaris Security Toolkit 文档勘误表”

---

## Solaris Security Toolkit 4.1.1 软件中的更改

本节汇总了 Solaris Security Toolkit 4.1.1 软件版本相对于 Solaris Security Toolkit 4.1 软件所作的有关更改。

---

**注** – Solaris Security Toolkit 4.1.1 软件版本不是 Solaris Security Toolkit 4.1 软件版本的错误修正版本。

---

- 添加了 SMS 1.5 支持。
- SMS 1.5 用户必须按特定的顺序执行 `undo`（取消加强安全性）操作并重新加强安全性，以确保故障转移功能对那些版本号低于 1.5 的 SMS 也有效。要使低于 1.5 版的 SMS 能正常运行，必须启用某些特定的服务：`login`、`shell` 和 `exec`。有关详细信息，请参阅《System Management Services (SMS) 1.5 Administrator Guide》中的第 2 章或《System Management Services (SMS) 1.5 发行说明》。
- 无需配置 Secure Shell (`ssh`) 和非安全的服务，即可使故障转移功能生效。

- 无需再对 SC 设置静态地址解析协议 (ARP)。
- 必须手动进行域排除。有关说明，请参阅《System Management Services (SMS) 1.5 Administrator Guide》。

---

## 所需的操作系统

Solaris Security Toolkit 4.1.1 软件只能在 Solaris 8 或 9 操作系统上使用。本 Solaris Security Toolkit 4.1.1 版本既不支持 Solaris 10 操作系统，也无法在该系统上使用。

---

## 支持 SMS 1.5 软件

Solaris Security Toolkit 4.1.1 软件支持 System Management Services (SMS) 1.5 软件，其中包含了默认的安全保护特性。要使用这些特性，您必须在系统控制器 (SC) 上使用 Solaris Security Toolkit 4.1.1 软件。有关 Sun Fire 高端系统安全保护的详细信息，请参阅《System Management Services (SMS) 1.5 Administrator Guide》中的第 2 章。

---

## Solaris Security Toolkit 文档

有关适用于所有 Solaris Security Toolkit 软件的通用信息，请参阅 Solaris Security Toolkit 4.1 文档，其网址如下：

[http://www.sun.com/products-n-solutions/hardware/docs/Software/enterprise\\_computing/systems\\_management/sst/index.html](http://www.sun.com/products-n-solutions/hardware/docs/Software/enterprise_computing/systems_management/sst/index.html)

---

# Solaris Security Toolkit 软件已知的局限性

本节包含 Solaris Security Toolkit 4.1 和 4.1.1 软件已知的局限性：

- 虽然 Solaris Security Toolkit 4.1.1 软件保留了用于禁用系统帐户的功能（请参阅 `finish` 脚本 `disable-system-accounts.fin`），但是它将不再通过修改系统来记录那些已禁用的帐户的登录尝试。

---

## 常见注意事项和问题

本节包含 Solaris Security Toolkit 4.1 和 4.1.1 软件所涉及的常规注意事项和问题。

### SMS 软件与 Solaris Security Toolkit

有关受支持的 SMS 升级和降级操作，可参考 SMS 高端系统产品的文档。在由 Solaris Security Toolkit 加强安全性的系统控制器上执行 SMS 升级/降级操作时，请在升级/降级操作完成后运行审计模式。运行审计模式可检验系统控制器的配置是否正确。如果经检验发现系统配置存在漏洞，那么请重新运行加强安全性的操作。

### Solaris Security Toolkit 与 CTRL-C

在 Solaris Security Toolkit 运行加强安全性和 `undo` 操作过程中执行 CTRL-C 将导致系统状况产生不一致。正确的操作方法应该是：在加强安全性操作完成后，再执行 `undo` 操作，而不是在运行加强安全性操作的过程中将其中断。请勿将 CTRL-C 用于出错处理，或者用于中断 Solaris Security Toolkit 的运行。应等待操作完成，然后重新执行加强安全性操作，或执行 `undo` 操作。

### `fix-modes` 显示警告

如果在软件包的安装过程中执行 `fix-modes`，屏幕上将显示安全模式警告。这些警告源自 Solaris 软件中文件格式化的问题，可以放心地忽略。

# Solaris Security Toolkit 问卷

为更好地理解 Solaris Security Toolkit 用户的需求与要求，我们在 Documentation 目录（<JASS\_HOME 目录>/Documentation/QUESTIONNAIRE）中放置了一份问卷。设计该问卷的目的是为了在未来开发工作中更好地把握客户的需求。非常感谢您的积极参与。

请将填完的问卷提交至：[sst-questionnaire@sun.com](mailto:sst-questionnaire@sun.com)

---

## Solaris Security Toolkit 软件中的错误

本节简要介绍 Solaris Security Toolkit 4.1 和 4.1.1 软件中最值得注意的错误和 RFE。

### undo 报告 logadm.conf 已更改 (错误 ID 5067303)

在使用 `update-cron-log-size.fin` 和 `enable-process-accounting.fin` 脚本加强系统安全性后，如果重新引导系统并运行 `undo` 以取消加强安全性的操作，`undo` 将报告 `/etc/logadm.conf` 已更改，并提示您选择“备份”、“强制”或“保留”等常用的选项。

由于用户并未手动编辑过 `/etc/logadm.conf` 文件，因此 `undo` 本应可以继续执行而不需要用户干预。

**解决方法：**在这种情况下，请选择“强制”选项。

如果您确实编辑过 `/etc/logadm.conf` 文件，请选择“备份”或“保留”选项。

---

# Solaris Security Toolkit 文档勘误表

本节介绍 Solaris Security Toolkit 4.1 文档中的勘误表。

## “参考手册”中未列出 banner.msg (错误 ID 6177578)

《Solaris Security Toolkit 4.1 Reference Manual》第 4 章 set-banner-ftpd.fin 小节的文件列表中缺少 /etc/ftpd/banner.msg 文件。

**解决方法：**无。此错误仅出现在文档中。该文件已经包含在软件中。

## 过时的 env var (错误 ID 6177598)

Solaris Security Toolkit 4.1.1 软件不再使用 JASS\_SHELL\_DISABLE 环境变量，并已将其删除了。《Solaris Security Toolkit 4.1 Reference Manual》中提及了需要使用环境变量 JASS\_SHELL\_DISABLE，但事实上应该将之忽略。

**解决方法：**请勿尝试使用该变量。它已不再起作用了。

