Sun™ Crypto 加速器 1000 板安装和用户指南

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054 U.S.A.
650-960-1300

部件编号 816-4569-10
2002 年 3 月，修订版 A

有关此文档的建议可发送到：docfeedback@sun.com

请回收
利用

Declaration of Conformity

EMC

Compliance Model Number: DEIMOS
Product Family Name: Sun Crypto Accelerator 1000 (X6762A)

European Union

This equipment complies with the following requirements of the EMC Directive 89/336/EEC:

EN55022:1998/CISPR22:1997		Class A
EN55024:1998	Required Limits (as applicable):	
	EN61000-4-2	4 kV (Direct), 8 kV (Air)
	EN61000-4-3	3 V/m
	EN61000-4-4	1 kV AC Power Lines, 0.5 kV Signal and DC Power Lines
	EN61000-4-5	1 kV AC Line-Line and Outdoor Signal Lines
		2 kV AC Line-Gnd, 0.5 kV DC Power Lines
	EN61000-4-6	3 V
	EN61000-4-8	1 A/m
	EN61000-4-11	Pass
EN61000-3-2:1995 + A1, A2, A14		Pass
EN61000-3-3:1995		Pass

Safety

This equipment complies with the following requirements of the Low Voltage Directive 73/23/EEC:

EC Type Examination Certificates:

EN 60950:2000, 3rd Edition
IEC 60950:1999, 3rd Edition

Supplementary Information

This product was tested and complies with all the requirements for the CE Mark.

/S/

Dennis P. Symanski DATE
Manager, Compliance Engineering
Sun Microsystems, Inc.
901 San Antonio Road, MPK15-102
Palo Alto, CA 94303-4900 U.S.A.
Tel: 650-786-3255
Fax: 650-786-3723

/S/

Peter Arkless DATE
Quality Manager
Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom
Tel: 0506-670000 Fax: 0506-760011

Regulatory Compliance Statements

Your Sun product is marked to indicate its compliance class:

- Federal Communications Commission (FCC) — USA
- Industry Canada Equipment Standard for Digital Equipment (ICES-003) — Canada
- Voluntary Control Council for Interference (VCCI) — Japan
- Bureau of Standards Metrology and Inspection (BSMI) — Taiwan

Please read the appropriate section that corresponds to the marking on your Sun product before attempting to install the product.

FCC Class A Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Shielded Cables: Connections between the workstation and peripherals must be made using shielded cables to comply with FCC radio frequency emission limits. Networking connections can be made using unshielded twisted-pair (UTP) cables.

Modifications: Any modifications made to this device that are not approved by Sun Microsystems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

FCC Class B Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

Shielded Cables: Connections between the workstation and peripherals must be made using shielded cables in order to maintain compliance with FCC radio frequency emission limits. Networking connections can be made using unshielded twisted pair (UTP) cables.

Modifications: Any modifications made to this device that are not approved by Sun Microsystems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

ICES-003 Class A Notice - Avis NMB-003, Classe A

This Class A digital apparatus complies with Canadian ICES-003.

ICES-003 Class B Notice - Avis NMB-003, Classe B

This Class B digital apparatus complies with Canadian ICES-003.

VCCI 基準について

クラス A VCCI 基準について

クラス A VCCI の表示があるワークステーションおよびオプション製品は、クラス A 情報技術装置です。これらの製品には、下記の項目が該当します。

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

クラス B VCCI 基準について

クラス B VCCI の表示  があるワークステーションおよびオプション製品は、クラス B 情報技術装置です。これらの製品には、下記の項目が該当します。

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

BSMI Class A Notice

The following statement is applicable to products shipped to Taiwan and marked as Class A on the product compliance label.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用
時，可能會造成射頻 干擾，在這種情況下，
使用者 會被要求採取某些適當的對策。

目录

1. 产品概述 1

硬件概述 1

产品功能 2

动态重配置和高可用性因素 3

负载共享 3

硬件和软件要求 4

必需的修补程序 4

2. 安装和拆卸 Sun Crypto 加速器 1000 板 7

板的操作 7

板的安装 8

▼ 安装硬件 8

Sun Crypto 加速器 1000 安装软件 9

▼ 安装软件 9

目录和文件 11

删除软件 13

▼ 删除领域 13

▼ 删除软件 14

3. 为 iPlanet Web 服务器启用板 15

密码 15

创建并填充领域 16

▼ 创建并填充领域 16

启用 iPlanet Web 服务器概述 18

4. 安装和配置 iPlanet Web Server 4.1 19

安装 iPlanet Web Server 4.1 19

▼ 安装 iPlanet Web Server 4.1 19

▼ 创建可信数据库 20

▼ 生成服务器证书 22

▼ 安装服务器证书 25

配置 iPlanet Web Server 4.1 26

▼ 配置 iPlanet Web Server 4.1 26

5. 安装和配置 iPlanet Web Server 6.0 29

安装 iPlanet Web Server 6.0 29

▼ 安装 iPlanet Web Server 6.0 29

▼ 创建可信数据库 30

▼ 生成服务器证书 33

▼ 安装服务器证书 35

配置 iPlanet Web Server 6.0 36

▼ 配置 iPlanet Web Server 6.0 36

6. 启用 Apache Web 服务器 39

启用 Apache Web 服务器 39

▼ 启用 Apache Web 服务器 39

创建证书 42

▼ 创建证书 42

7. 故障诊断和排除 47

SunVTS 诊断软件 47

▼ 运行 dcatest 48

dcatest 的测试参数选项 49

dcatest 命令行语法 50

Sun Crypto 加速器 1000 故障排除 51

A. 用 iPlanet Web 服务器管理 Sun Crypto 加速器 1000 板 53

概念和术语 53

领域、用户和 iPlanet Web 服务器 54

标记和插槽文件 54

插槽文件 55

使用 secadm 56

操作模式 57

用 secadm 输入命令 58

使用 secadm 进行验证 59

获得命令帮助 60

退出 secadm 程序 61

设置和管理领域 61

创建领域 62

设置当前工作领域 63

列出领域 64

列出领域类 64

删除领域 64

设置并管理用户帐户 65

创建用户 65

列出用户 65

更改用户密码 66

启用或禁用用户　66

删除用户　67

B.　Manual 页　69

C.　Apache Web 服务器的 SSL 配置指令　71

D.　构建同 Sun Crypto 加速器 1000 板使用的应用程序　79

E.　规格 Sun Crypto 加速器 1000 板　81

物理尺寸　81

接口规格　82

电源要求　82

环境规范　83

F.　Third-Party Licenses（第三方许可）　85

表

表 1-1 支持的 SSL 算法 3

表 1-2 硬件和软件要求 4

表 1-3 必需的 Sun Crypto 加速器 1000 软件修补程序 5

表 1-4 推荐的 Sun Crypto 加速器 1000 软件修补程序 5

表 2-1 Sun Crypto 加速器 1000 目录 11

表 3-1 Planet Web 服务器要求的密码 15

表 7-1 `dcatest` 的测试参数选项 49

表 7-2 `dcatest` 子测试 49

表 7-3 `dcatest` 命令行语法 50

表 A-1 `secadm` 选项 56

表 A-2 命令表 59

表 B-1 Sun Crypto 加速器 1000 `man` 页 69

表 C-1 SSL 协议 72

表 C-2 可用的 SSL 密码 73

表 C-3 SSL 别名 74

表 C-4 配置密码首选项的特殊字符 75

表 C-5 SSL 验证客户机级别 76

表 C-6 SSL 日志级别值 77

表 C-7 可用的 SSL 选项 78

表 E-1 物理尺寸 81

表 E-2 接口规格 82
表 E-3 电源要求 82
表 E-4 环境规范 83

序言

*Sun Crypto 加速器 1000 板安装和用户指南*介绍了 Sun™ Crypto 加速器 1000 板的功能以及该板在系统中的安装和使用方法。

本书假定您是一位熟悉 Solaris 操作环境的系统管理员。

使用 UNIX 命令

本文档不包含有关基本 UNIX® 命令和操作过程方面的信息，如关闭系统、启动系统和配置设备等。

有关此类信息的详细情况，请参阅以下文档：

- *Solaris 硬件平台指南*
- 面向 Solaris™ 操作环境的 AnswerBook2™ 联机文档
- 系统随带的其它软件文档

印刷约定

字样	含义	示例
AaBbCc123	命令、文件和目录的名称；计算机的屏幕输出	编辑 .login 文件。 使用 ls -a 列出所有文件。 % You have mail.
AaBbCc123	键入的内容（相对于计算机的屏幕输出）	% **su** Password:
AaBbCc123	书的标题、新词或术语、需要强调的词	阅读*用户指南*的第 6 章。 这些称为 *class* 选项。 执行该操作时，您*必须*为超级用户。
	命令行变量；应替换为真正的名称或值	若要删除文件，请键入 rm *文件名*。

Shell 提示

Shell	提示
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	#

联机访问 Sun 文档

如需更多 Sun 系统文档，请访问：

`http://www.sun.com/products-n-solutions/hardware/docs`

有关全套 Solaris 文档和众多其他主题的文档，可以访问：

`http://docs.sun.com`

Sun 欢迎您发表意见

Sun 十分注重改进自身文档的质量，并欢迎您提出宝贵的意见和建议。您可以通过电子邮件将意见发送至：

`docfeedback@sun.com`

请在电子邮件的主题行中注明文档的部件编号 (816-4569-10)。

第 1 章

产品概述

本章介绍 Sun Crypto 加速器 1000 板。

本章包含以下几节：

- 第 1 页 “硬件概述”
- 第 4 页 “硬件和软件要求”

硬件概述

Sun Crypto 加速器 1000 板是一块 PCI 短板，充当加密的协处理器，用来加速公共密钥和对称加密。本产品没有外部接口。本板通过内置 PCI 总线接口与主机通信。本板用于加速电子商务应用程序中各种要求计算资源较多的安全性协议的加密算法。

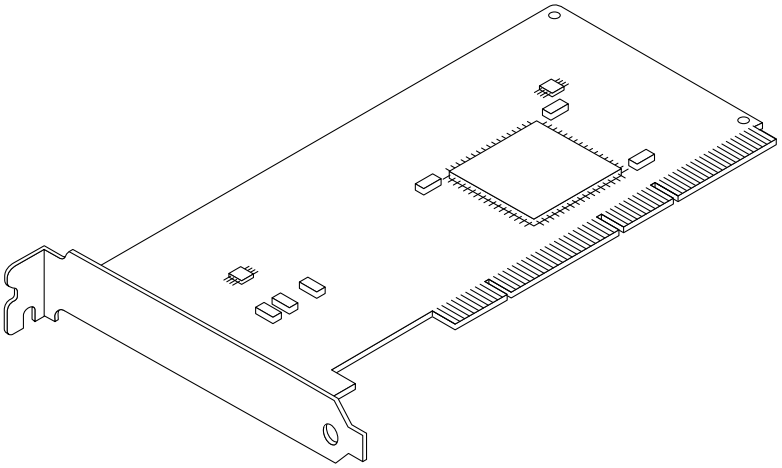


图 1-1 Sun Crypto 加速器 1000 板

产品功能

Sun Crypto 加速器 1000 是一块用于提高 Sun 平台上 SSL 性能的加密加速器板。Sun Crypto 加速器 1000 用于加速软硬件中的加密算法。其复杂性的原因在于加速加密算法的成本对于各种算法并非完全一样。有些加密算法专门利用硬件来实现，而其它加密算法则专门利用软件来实现。另外，对于硬件加速而言，将数据从用户应用程序空间移到硬件加速设备中以及将结果移回到用户应用程序中的成本较高。

注意：一些加密算法（例如 ARCFOUR）可以由精心调试的软件执行，其速度与在专用硬件中一样。Sun Crypto 加速器 1000 产品检查每个加密请求并确定最佳的加密位置（主处理器或 Sun Crypto 加速器 1000）以获得最大吞吐量。负载分配依据加密算法、当前作业负载和数据大小来进行。

表 1-1 显示了哪些加速算法可以向硬件分配负载以及 iPlanet 和 Apache Web 服务器可以使用哪些软件算法。

表 1-1 支持的 SSL 算法

	iPlanet Web 服务器		Apache Web 服务器	
算法	**硬件**	**软件**	**硬件**	**软件**
RSA	X	X	X	X
DSA	X	X	X	X
Diffie-Hellman			X	X
DES	X	X	X	X
3DES	X	X	X	X
ARCFOUR		X		X

动态重配置和高可用性因素

Sun Crypto 加速器 1000 硬件和相关软件可以有效地在支持动态重配置 (DR) 和热插拔的 Sun 平台上工作。如果发生 DR 或热插拔操作，则 Sun Crypto 加速器 1000 软件层会自动检测板的插拔情况并调节计划算法，以适应硬件资源的变化。

对于高可用性 (HA) 配置，可以在一个系统或域内安装多块 Sun Crypto 加速器 1000 板，以确保硬件加速连续可用。万一 Sun Crypto 加速器 1000 硬件出现故障，软件层会检测到故障并从可用的硬件加密加速器列表中删除故障卡。Sun Crypto 加速器 1000 会调整计划算法，以适应硬件资源减少的情况。后续的加密请求将调整由余下的卡来实现。

另外，Sun Crypto 加速器 1000 软件库具备以软件方式实现所有加密操作的功能。它支持系统域内所有 Sun Crypto 加速器 1000 板的 DR 或热插拔拆卸，而没有任何负面的功能影响。恢复 Sun Crypto 加速器 1000 硬件的配置之前，性能会显著下降。

注意：Sun Crypto 加速器 1000 硬件为长期密钥的生成提供了高质量熵的来源。如果拆卸某域或系统中的所有 Sun Crypto 加速器 1000 板，则会生成长期密钥，熵质量较低。

负载共享

Sun Crypto 加速器 1000 软件在 Solaris 域或系统内安装的板上分配负载。引入的加密请求根据固定长度作业队列在板之间进行分配。请求被加入可以接受此类请求的第一个可用板的排队之中。排队机制的作用在于通过疏导汇集在板上的请求来优化吞吐量。

硬件和软件要求

表 1-2 概要介绍了 Sun Crypto 加速器 1000 板的软硬件要求。

表 1-2 硬件和软件要求

硬件和软件	要求
硬件	Sun Blade™ 1000 Sun Enterprise™ 220R、 250、 420R、 450 Sun Fire™ 280R、 V480、 V880、 4800、 4810、 6800 Sun Netra™ T1 AC200/DC200、 Netra 20、 Netra t 1400/1405 Sun Ultra™ 60、 80
操作环境	Solaris 8 7/01 或后续兼容发行版
PCI 插槽	32 位或 64 位 33 MHz 或 66 MHz
软件	iPlanet™ Web Server 4.1 SP9、6.0 SP1 或 Apache Web Server 1.3.12 运行 iPlanet 或 Apache Web 服务器必需的各种修补程序

注意 – 每当提及 iPlanet Web Server 4.1 或 6.0 时，隐含 SP 号 （SP9 或 SP1）。

必需的修补程序

在您的系统上运行 Sun Crypto 加速器 1000 时可能需要以下修补程序。 Solaris 更新版本包含以前发行版的修补程序。使用 `showrev -p` 命令，确定是否已经安装了所列的修补程序。

如果需要，可从以下 Web 站点下载修补程序：`http://sunsolve.sun.com`。

安装最新版本的修补程序。每发布一个新版本的修补程序，破折号后的数字 （例如 -01）就会增加。如果 Web 站点上的版本高于下面几张表中所给出的版本，请使用更新的版本。

如果 SunSolve℠ 不提供所需的修补程序，请与当地的销售或服务代表联系。

下面几张表列出了使用本产品必需和推荐使用的修补程序。表 1-3 列出并说明了必需的修补程序。

表 1-3 必需的 Sun Crypto 加速器 1000 软件修补程序

修补程序 ID	说明
110383-01	`libnvpair`
108528-05	`KU-05 （nvpair 支持）`
112438-01	`/dev/random`

注意 – 如果您打算使用 Apache 1.3.12 Web 服务器，您还必须安装编号为 109234-02 的修补程序。

表 1-4 列出并说明了推荐的修补程序。

表 1-4 推荐的 Sun Crypto 加速器 1000 软件修补程序

修补程序 ID	说明
108528-13	`KU-13 （nvpair 安全修补程序）`

第 2 章

安装和拆卸 Sun Crypto 加速器 1000 板

本章介绍如何安装 Sun Crypto 加速器 1000 硬件和软件。

本章包括以下几节

- 第 7 页 “板的操作”
- 第 8 页 “板的安装”
- 第 11 页 “目录和文件”

板的操作

每块板都采用特制的防静电包进行包装，以确保安全运输和存储。为避免损坏板上的静电敏感组件，请在接触板之前，使用以下方法之一减少身上的静电：

- 触摸计算机的金属机箱。
- 将防静电腕带连接到手腕和接地的金属表面。

警告 – 为避免损坏板上的静电敏感组件，请在装卸板时戴上防静电腕带，只抓住板的边缘，始终将板放在防静电的表面 （如装板的塑料袋）。

板的安装

安装 Sun Crypto 加速器 1000 板需要将板插入系统中并加载软件工具。硬件安装说明仅包括板的一般安装步骤。有关具体安装说明，请参阅您的系统随附的文档。

▼ 安装硬件

1. **作为超级用户，按系统随附说明关闭计算机，断开电源，拔掉电源线并打开计算机机壳。**
2. **找到一个未用的 PCI 插槽（最好是 64 位 66 MHz 的插槽）。**
3. **将防静电腕带的一端连接到手腕，另一端连接到接地的金属表面。**
4. **使用 Phillips 螺丝刀卸下 PCI 插槽盖板上的螺丝。**
   保存好螺丝以备在步骤 5 中固定支架时使用。
5. **只能抓住 Sun Crypto 加速器 1000 板的边缘，将其从塑料袋中取出，插入 PCI 插槽，然后固定后支架上的螺丝。**
6. **重新装上计算机机壳，重新连接电源线并打开系统电源。**
7. **在 `ok` 提示符处输入 `show-devs` 命令，检查板的安装是否正确：**

```
ok show-devs
. . .
/pci@1f,2000/pci108e,5455@1
/pci@1f,4000/pci108e,5455@5
. . .
```

`/pci@1f,2000/pci108e,5455@`*n* 行表明板已安装而已被系统识别。

Sun Crypto 加速器 1000 安装软件

Sun Crypto 加速器 1000 软件随 *Sun Crypto 加速器 1000* CD 提供。您需要从 SunSolve Web 站点下载修补程序：有关详细信息，请参见第 4 页 “必需的修补程序”。

▼ 安装软件

1. **将 *Sun Crypto 加速器 1000* CD 插入与系统连接相连的 CD-ROM 驱动器。**
   - 如果系统正在运行 Sun Enterprise Volume Manager™，它应自动将 CD-ROM 安装到 `/cdrom/cdrom0` 目录。
   - 如果系统未运行 Volume Manager，请按以下方法装入 CD-ROM：

```
# mkdir /cdrom
# mount -F hsfs -o ro /dev/dsk/c0t6d0s2 /cdrom
```

您将会在 /cdrom/cdrom0 目录中看到以下文件和目录。

文件或目录	内容	
Copyright	美国版权文件	
FR_Copyright	法国版权文件	
Docs	Sun Crypto 加速器 1000 板安装和用户指南	
Packages	包含 Sun Crypto 加速器 1000 软件包：	
	SUNWcrypr	Cryptography Kernel Components
	SUNWcrypu	Cryptographic Administration Utility and Libraries
	SUNWcrysu	SSL Support for Apache (optional)
	SUNWcrypm	Cryptographic Administration Manual Pages
	SUNWdcar	DCA Crypto Accelerator (Root)
	SUNWdcamn	DCA Crypto Accelerator Manual Page
	SUNWdcav	SunVTS Test of DCA Crypto Accelerator (optional)
	SUNWcrysl	SSL Development Tools and Libraries for Apache (optional)

仅在计划将 Apache 用作 Web 服务器时安装 SUNWcrysu 软件包。

仅在计划重新链接到 Apache Web 服务器的另一（不支持）版本时安装 SUNWcrysl 软件包。

仅在计划进行 SunVTS™ 测试时安装 SUNWdcav 软件包。要安装 SUNWdcav 软件包，必须装有 SunVTS 4.4、 4.5 或 4.6。

2. **通过键入以下内容安装软件包：**

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d .
```

3. **要检查软件是否正确安装，请运行** pkginfo **命令。**

```
# pkginfo SUNWcrypr SUNWcrypu SUNWcrysl SUNWcrysu SUNWcrypm SUNWdcar SUNWdcamn
SUNWdcav
system  SUNWcrypr   Cryptography Kernel Components
system  SUNWcrypu   Cryptographic Administration Utility and Libraries
system  SUNWcrysl   SSL Development Tools and Libraries
system  SUNWcrysu   SSL Support for Apache
system  SUNWcrypm   Cryptographic Administration Manual Pages
system  SUNWdcar    DCA Crypto Accelerator (Root)
system  SUNWdcamn   DCA Crypto Accelerator Manual Page
system  SUNWdcav    SunVTS Test of DCA Crypto Accelerator
```

4. **（可选）要检查是否已附加驱动程序，您可以运行** prtconf **命令。**

```
# prtconf
pci108e,5455, instance #0
pci108e,5455, instance #1
```

5. **（可选）运行** modinfo **命令，查看是否加载模块。**

```
# modinfo | grep Crypto
130 1033e946   6df0  79   1  cryptio (Cryptographic IOCTL v1.58)
131 1030240c   2d93   -   1  kcl (Cryptographic Library v1.64)
132 10313ac8   131e   -   1  kcpi (Crypto Provider Interface v1.27)
135 103178be   8684  82   1  dca (PCI Crypto Accelerator v1.156)
```

但是，只有真正使用 Sun Crypto 加速器 1000 执行加密操作之后，才会加载或显示 kcl 和 cryptio。

目录和文件

表 2-1 列出了 Sun Crypto 加速器 1000 软件的默认安装所创建的目录。

表 2-1 Sun Crypto 加速器 1000 目录

目录	内容
/etc/opt/SUNWconn/crypto/realms	领域和用户数据
/opt/SUNWconn/crypto/bin	应用程序可执行文件
/opt/SUNWconn/crypto/lib	应用程序库
/opt/SUNWconn/crypto/sbin	静态链接的可执行文件

图 2-1 显示的是这些目录和文件的层次结构。

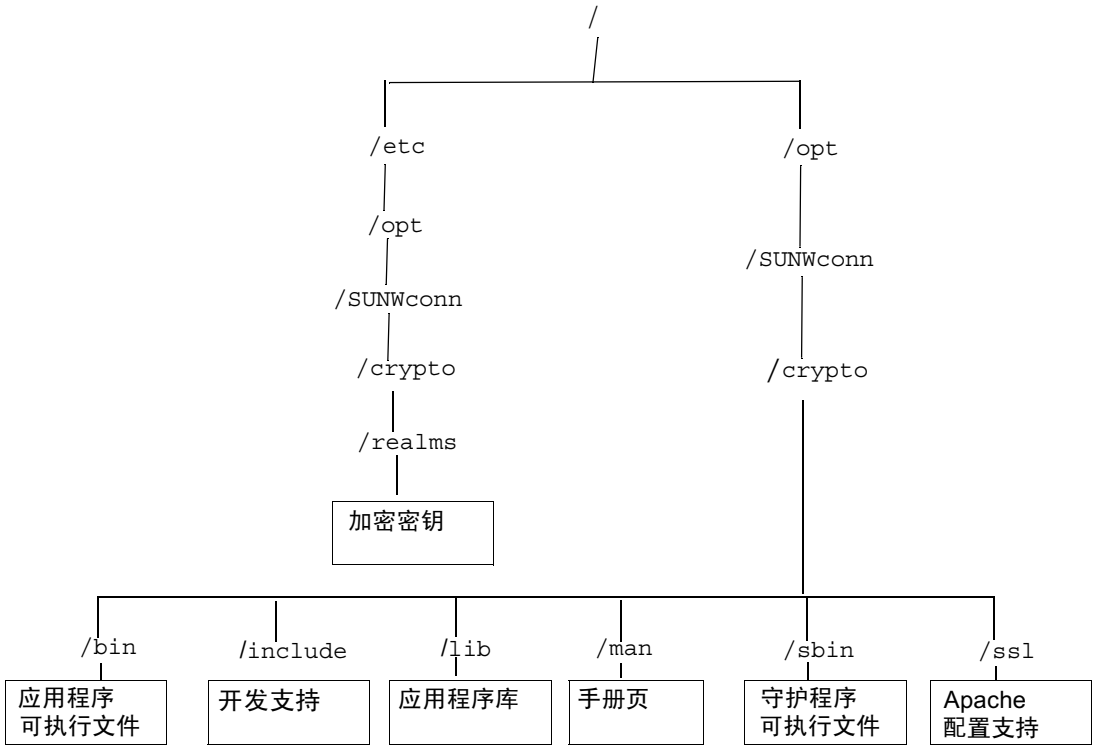


图 2-1 Sun Crypto 加速器 1000 目录和文件

删除软件

如果已创建领域，则必须在删除软件之前先删除领域。如果未创建领域，则可以忽略以下步骤。您无法删除当前正在使用的领域。要取消领域引用，您必须关掉 Web 服务器和/或管理服务器。

警告 – 删除 Sun Crypto 加速器 1000 软件之前，您必须禁用任何已启用与 Sun Crypto 加速器 1000 板一起使用的 Web 服务器。否则，这些 Web 服务器都将无法工作。

▼ 删除领域

1. **作为超级用户，访问** `secadm` **实用程序：**

```
# /opt/SUNWconn/crypto/bin/secadm
secadm>
```

2. **使用** `secadm` **实用程序删除每个领域。**

```
secadm> delete realm=realm-name
Delete realm realm-name? [Y/N]: Y
System Administrator Login Required
Login: root
Password:
Realm realm-name deleted successfully.
```

它会删除所有与站点相关的领域数据，包括密码资料。

▼ 删除软件

- **作为超级用户，使用 `pkgrm` 命令只删除您所安装的软件包。**

  安装的软件包必须按所示顺序删除。不按此顺序删除软件包，则会显示相关性警告，核心模块仍处于加载状态。

  如果安装了所有软件包，则应按如下所示进行删除：

```
# pkgrm SUNWcrysl SUNWdcav SUNWdcar SUNWcrysu SUNWcrypu SUNWcrypr
SUNWdcamn SUNWcrypm
```

注意 – 安装或删除 Sun Crypto 加速器 1000 的 SunVTS 测试 (`SUNWdcav`) 后，如果 SunVTS 已在运行，则必须让 SunVTS 重新浏览系统，以更新可用的测试。有关详细信息，请参见您的 SunVTS 文档。

第 3 章

为 iPlanet Web 服务器启用板

本章介绍如何启用 Sun Crypto 加速器 1000 板与 iPlanet Web 服务器一同使用。

本章包括以下几节

- 第 15 页 “密码”
- 第 18 页 “启用 iPlanet Web 服务器概述”
- 第 16 页 “创建并填充领域”

密码

在启用 iPlanet Web 服务器 (iWS) 的过程中，会要求您提供几个密码。表 3-1 对每个密码进行了说明。本章通篇都将要到这些密码。如果不清楚应该使用哪个密码，请参阅表 3-1。

表 3-1 Planet Web 服务器要求的密码

密码类型	说明
iWS 管理服务器	启动 iPlanet 管理服务器时需要。该密码在设置 iPlanet 时分配。
Web 服务器可信数据库	在安全模式下运行时、在请求证书时以及在安装证书时启动内部加密模块需要。在 iPlanet Web 服务器中，该密码又称为密钥对文件密码和模块内部密码。
系统管理员	执行 `secadm` 权限操作时需要。这是 UNIX 主机密码。
user@realm-name	在安全模式下启动 Sun Crypto 加速器 1000 模块时需要。使用 `secadm` 创建领域用户时分配该密码。

创建并填充领域

要启用板与 iPlanet Web 服务器一起使用，您必须先设置并填充领域。如果您尚未这样做，则必须设置至少一个领域和一个用户。有关领域的详细信息，请参阅附录 A。

▼ 创建并填充领域

1. **如果您尚未这样做，请将 Sun Crypto 加速器 1000 工具目录放入您的搜索路径，例如：**

```
$ PATH=$PATH:/opt/SUNWconn/crypto/bin
$ export PATH
```

2. **访问** `secadm` **实用程序：**

```
$ secadm
```

3. **使用** `secadm` **实用程序创建新领域：**

```
secadm> create realm=realm-name
System Administrator Login Required
Login: root
Password:
Realm realm-name created successfully.
```

4. **用用户填充领域。**

   这些用户名仅在 Sun Crypto 加速器 1000 的域中被识别，而且不必与 Web 服务器进程实际运行的 UNIX 用户名相同。尝试创建用户之前，请记住必须先设置当前的工作领域并以系统管理员身份登录。

   创建用户之前，您必须先设置要创建用户的领域。

```
secadm> set realm=realm-name
secadm{realm-name}> su
System Administrator Login Required
Login: root
Password:
secadm{root@realm-name}#
```

   a. **如果仅需要一个领域用户，您可以通过使用用户名 “nobody” 来避免设置插槽文件。（详细信息，请参见第 55 页 “插槽文件”。）**

```
secadm{root@realm-name}# create user=nobody
Initial password:
Confirm password:
User nobody created successfully.
```

   在 Web 服务器启动期间进行验证时，必须使用此密码。这是 *user@realm-name* 密码。

警告 – 必须记住输入的密码。没有密码，就无法访问您的密钥。丢失的密码无法重新找到。

5. **退出 secadm。**

```
secadm> exit
```

启用 iPlanet Web 服务器概述

要启用 iPlanet Web 服务器，您必须完成以下步骤。下面两章会进行详细说明。

1. 安装 iPlanet Web 服务器
2. 创建可信数据库。
3. 请求证书。
4. 安装证书。
5. 配置 iPlanet Web 服务器。

警告 – 以下步骤必须按指定顺序进行。否则，则可能导致错误配置。

- 如果您使用 iPlanet Web Server 4.1，请转至第 4 章。
- 如果您使用 iPlanet Web Server 6.0，请转至第 5 章。

第 4 章

安装和配置 iPlanet Web Server 4.1

本章介绍如何安装和配置 iPlanet Web Servers 4.1

本章包括以下几节

- 第 19 页 “安装 iPlanet Web Server 4.1”
- 第 26 页 “配置 iPlanet Web Server 4.1”

安装 iPlanet Web Server 4.1

以下几节介绍如何安装 iPlanet Web Server 4.1。这些步骤必须按指定顺序执行。有关使用 iPlanet Web 服务器的详细信息，请参阅 iPlanet Web 服务器文档。

▼ 安装 iPlanet Web Server 4.1

1. **安装 iPlanet Web Server 4.1 软件**。

   您可从以下的 URL 找到该 Web 服务器软件：

   `http://www.iplanet.com`

2. **安装 Web 服务器**。

   此处提供了一个例子的说明，您可以决定对 Web 服务器进行不同的配置。服务器的默认路径名为：`/usr/netscape/server4`

   在 iPlanet Web 服务器安装期间接受默认路径。本书中使用这些默认路径。如果您决定将其安装在不同的位置，务必记住它的安装位置。

3. **运行安装程序。**

4. **回答安装脚本中的提示。**

   除以下提示外，为方便起见，您可以接受默认值。

   a. 通过键入 `yes` **同意接受许可条款。**

   b. 输入全限定的 *hostname.domain*。

   c. 输入 iWS 管理服务器密码两次。

   d. 提示时，按回车键。

▼ 创建可信数据库

1. **启动管理服务器。**

   - 要启动 iPlanet Web Server 4.1，请使用以下命令 （而不是将 `startconsole` 作为 setup 请求来运行）：

```
# /usr/netscape/server4/https-admserv/start
iPlanet-WebServer-Enterprise/4.1SP9 BB1-08/23/2001 05:50
startup: listening to http://hostname.domain, port 8888 as root
```

   响应消息提供要连接到的 URL 以管理您的服务器。

2. **通过打开 Web 浏览器并输入以下内容来启动 iPlanet 管理服务器：**

```
http://hostname.domain:admin_port
```

   随即弹出一个窗口，要求输入用户 ID 和密码。请输入在运行安装程序期间选择的 iWS 管理服务器用户名和密码。

注意 – 如果在 iPlanet Web 服务器安装期间使用了默认值，则请为用户 ID 或 iWS 管理服务器用户名输入 `admin`。

---

3. **单击 “OK （确定）”。**

4. **创建 Web 服务器的可信数据库。**

   最好对多个 Web 服务器实例启用安全性。对每个 Web 服务器实例重复此过程。

注意 – 如果您也想在管理服务器上运行 SSL，则设置可信数据库的过程类似。有关详细信息，请参阅 iPlanet 文档。

---

   a. **单击管理服务器中的 “Servers （服务器）” 选项卡。**

   b. **选择服务器，然后单击 “Manage （管理）” 按钮。**

   c. **在靠近页首的地方单击 “Security （安全）” 选项卡，然后选择 “Create Database （创建数据库）” 选项。**

   d. **在两个对话框中输入密码 （Web 服务器可信数据库），然后单击 “OK （确定）”。**

      选择一个至少有 8 个字符的密码。iPlanet Web 服务器以安全模式运行时，此密码将用来启动内部加密模块的密码。

5. **执行以下脚本启用 Sun Crypto 加速器 1000 板：**

```
# /opt/SUNWconn/crypto/bin/sslconfig
```

   此脚本提示您选择 Web 服务器。它为 iPlanet Web 服务器或 Apache Web 服务器安装 Sun Crypto 加速器 1000 加密模块。脚本然后会更新配置文件以启用 Sun Crypto 加速器 1000 板。

6. **键入 `1` 来配置 iPlanet Web 服务器以使用 SSL，然后按 “Enter”。**

```
Sun Crypto Accelerator Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for iPlanet Web Server
or Apache.

Please select the type of web server you wish to configure
to use the Sun Crypto Accelerator:
------------------------------------------------------------
1. Configure iPlanet Web Server for SSL
2. Configure Apache for SSL
3. Work with iPlanet and Apache keys
Your selection (0 to quit):  1
```

7. **提示时输入 Web 服务器根目录的路径，然后按 “Enter”。**

```
Please enter the full path of the web server
root directory [/usr/netscape/server4]: /usr/netscape/server4
```

8. **如果要继续，请在提示时键入** y **并按 “Enter”。**

```
This script will update your iPlanet Web Server installation
in /usr/netscape/server4 to use the Sun Crypto Accelerator
You will need to restart your admin server after this has
completed.
Ok to proceed? y

Using database directory /usr/netscape/server4/alias...
Module "Sun Crypto Accelerator" added to database.
/usr/netscape/server4 has been configured to use
the Sun Crypto Accelerator.


<Press ENTER to continue>
```

9. **键入** 0 **退出。**

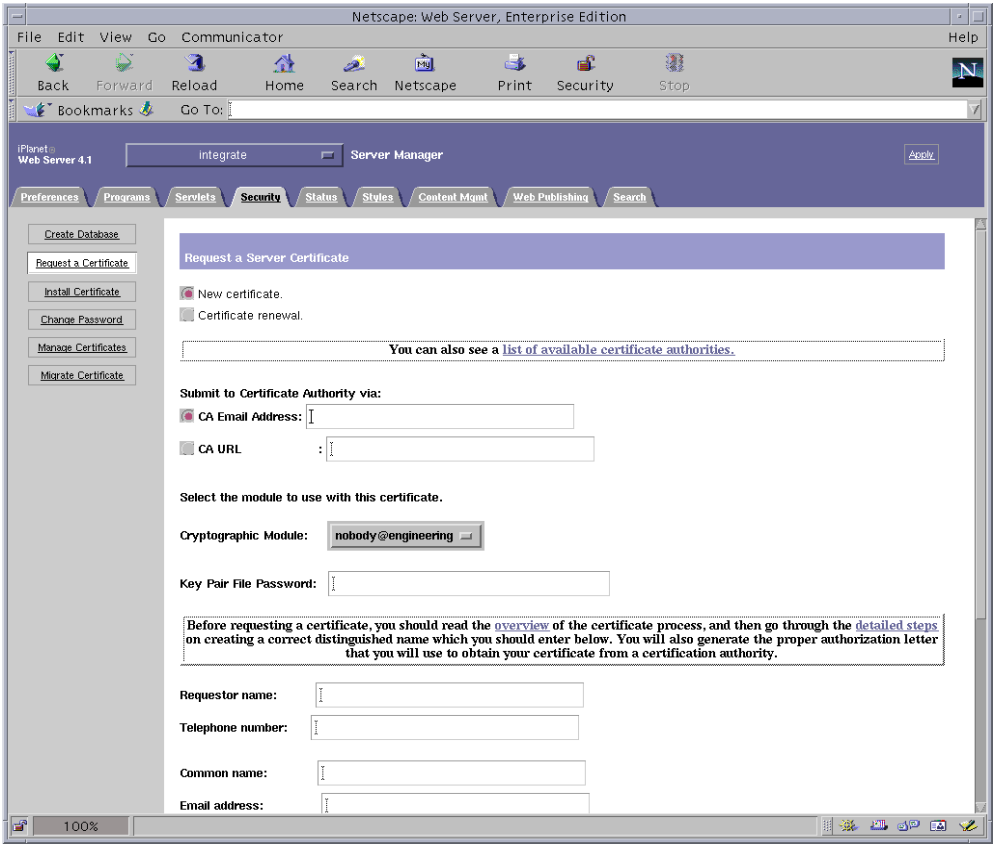
▼ 生成服务器证书

1. **通过键入以下命令重新启动管理服务器：**

```
# /usr/netscape/server4/https-admserv/stop
# /usr/netscape/server4/https-admserv/start
```

2. **要请求服务器证书，请单击靠近页首的 “Security （安全）” 选项卡。**
   随即会显示 “Create Trust Database （创建可信数据库）” 窗口。

3. **在该页的左侧选择 “Request Certificate （请求证书）”链接。**



4. **使用以下信息填写表单以生成证书请求：**

   a. **选择 “New Certificate （新建证书）”**

   如果可以直接将证书请求发送到可通过 Web 访问的证书机构或注册机构，请选择 “CA URL”选项。否则，请选择 “CA Email Address （CA 电子邮件地址）”，选择希望通过电子邮件发送证书请求的电子邮件收件人地址。

   b. **选择您要使用的加密模块。**

   在此下拉菜单中，每个领域都有自己的条目。务必选择正确的领域。要使用 Sun Crypto 加速器 1000，必须选择一个格式为 *user@realm-name* 的模块。

   c. **在 “Key Pair File Password （密钥对文件密码）”对话框中，为将拥有密钥的 *user@realm-name* 提供密码。**

d. 为以下字段提供正确信息：

- Requestor Name：请求者的联系信息
- Telephone Number：请求者的联系信息
- Common Name：在来访者的浏览器 *hostname.domain* 中键入的 Web 站点域
- Email Address：请求者的联系信息
- Organization：证书上声明的 Organization 的值
- Organizational Unit：（可选）将在证书上声明的 Organizational Unit 的值
- Locality：（可选）城市、郡县、公国或国家/地区，如果提供也在证书上予以声明
- State：（可选）本字段中州省的全称
- Country：由两个字母组成的国家/地区 ISO 代码，在证书上予以声明，为必填字段

e. 一旦输入所有信息，单击 “OK” 按钮提交。

5. 利用证书机构生成证书。

- 如果选择将证书请求发送给 CA URL，则证书请求会自动发送到此处。
- 如果选择 “CA Email Address （CA 电子邮件地址）”，请带标题复制通过电子邮件发给您的证书请求，然后将其交给证书机构。

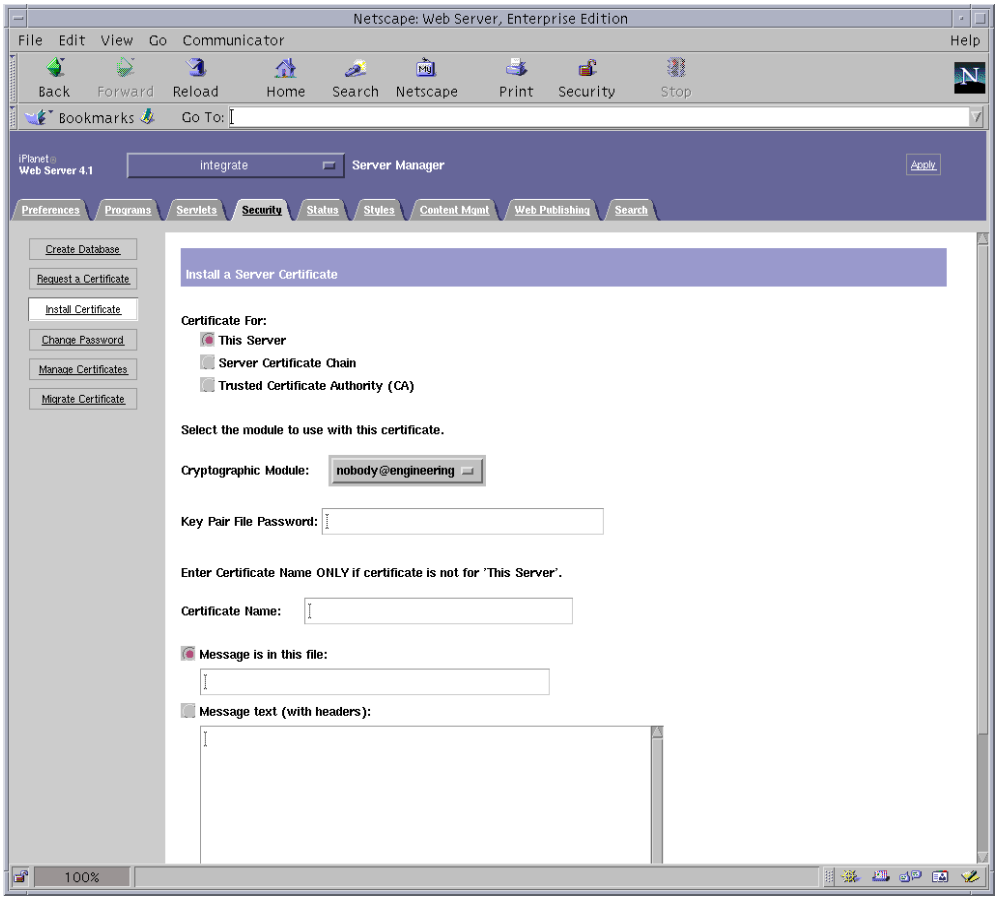
6. 一旦生成证书，请将其连标题一起复制到剪贴板上。

注意：证书与证书请求不同，常常以文本格式向您提供。

▼ 安装服务器证书

1. **在该页的左侧选择 “Install Certificate （安装证书）” 链接。**
   一旦证书机构批准您的请求并签发证书，您必须将其安装在 iPlanet Web 服务器中。

2. **选择 “Security （安全）” 选项卡，然后在左框上选择 “Install Certificate （安装证书）” 选项。**



3. **填写表单，安装证书：**
   - Certificate For：This Server
   - Cryptographic Module：选择正确的 *user@realm-name* 名称。
   - Key Pair File Password：为拥有以前生成的密钥的 *user@realm-name* 提供密码。
   - Certificate Name：在大多数情况下，您可以空着不填。如果选择提供名称，该名称将改变 Web 服务器在使用 SSL 支持运行时用来访问证书和密钥的名称。

4. **选择 “Message text (with headers) （带标题的消息文本）”，粘贴前面复制的证书。**

5. **单击该页底部的 “OK （确定）”按钮，将您从证书机构复制的证书粘贴到 “Message （消息）”框中。**

   随即会显示证书的一些基本信息。

6. **如果输入的内容正确，请单击 “Add Server Certificate （添加服务器证书）”按钮。**

   随即会显示屏幕消息，通知您重新启动服务器。 Web 服务器实例一直处于关闭状态时不必重新启动服务器。同时还会通知您，为使 Web 服务器使用 SSL，必须对 Web 服务器进行相应配置。使用以下步骤配置 Web 服务器。

配置 iPlanet Web Server 4.1

既然已安装 Web 服务器和服务器证书，必须对 Web 服务器进行配置以使用 SSL。

▼ 配置 iPlanet Web Server 4.1

1. **在主管理页上选择要使用的 Web 服务器实例然后单击 “Manage （管理）”。**

   默认情况下，您应该处于页首的 “Preferences （参数选择）”选项卡上。如果没有，请单击该选项卡。

2. **在靠近页首的地方单击 “Preferences （参数选择）”选项卡。在该页左侧选择 “Encryption On/Off （加码开/关）”链接。将加密设置为 “On （开）”。**

   对话框中的端口字段应更新为默认的 SSL 端口号 443。如果需要，请更改端口号。

3. **单击 “OK （确定）”按钮。**

4. **通过单击 “Save （保存）”按钮应用这些更改。**

   现在已对 Web 服务器进行配置，它可以在安全模式下运行。

5. **通过添加下行编辑**
   `/usr/netscape/server4/https-`*h*`ostname/config/magnus.conf` **文件：**

   ```
   CERTDefaultNickname user@realm-name:Server-Cert
   ```

   其中 *hostname* 为 Web 服务器名称。

   默认情况下，您在步骤 2 和步骤 3 中生成的证书命名为 `Server-Cert`。如果您的证书有另一名称，请将证书名替换为 `Server-Cert`。

6. **选择您要管理的服务器，然后单击该页右上角的 “Apply （应用）”按钮。**

   此操作通过管理服务器应用这些更改。

7. **单击 “Load Configuration Files （加载配置文件）”按钮应用您刚对** `magnus.conf` **文件所做的更改。**

   如果在服务器关闭时单击 “Apply Changes”按钮，则会弹出一个窗口，提示输入密码。此窗口不可以调整大小，因此在提交更改时可能会遇到问题。该问题有两个临时解决办法：

   - 改为单击 “Load Configuration Files （加载配置文件）”。
   - 先启动 Web 服务器，然后单击 “Apply Changes （应用更改）”按钮。

8. **在 Web 服务器页上，选择该页左侧上的 “On/Off （开/关）”链接。输入服务器密码，单击 “OK （确定）”按钮。**

   将会提示您提供一个或多个密码。出现 “Module Internal”提示时，为 Web 服务器可信数据库提供密码。

   出现 “Module *user@realm-name*”提示时，输入您使用 `secadm` 在 *realm-name* 中创建*用户*时设置的密码。

9. **通过转至下面的 URL 在浏览器中检查启用 SSL 的新 Web 服务器：**

   `https://`*hostname.domain*`:`*server_port*`/`

   注意：默认 *server_port* 为 443。

第 5 章

安装和配置 iPlanet Web Server 6.0

本章介绍如何启用 Sun Crypto 加速器 1000 板与 iPlanet 6.0 Web 服务器一同使用。

本章包括以下几节

- 第 29 页 “安装 iPlanet Web Server 6.0”
- 第 36 页 “配置 iPlanet Web Server 6.0”

安装 iPlanet Web Server 6.0

以下几节介绍如何安装和配置 iPlanet Web 服务器。这些步骤必须按指定顺序执行。有关使用 iPlanet Web 服务器的详细信息，请参阅 iPlanet Web 服务器文档。

▼ 安装 iPlanet Web Server 6.0

1. **安装 iPlanet Web Server 6.0 软件**。

   您可从以下 URL 找到该 Web 服务器软件：

   `http://www.iplanet.com`

2. **安装 Web 服务器**。

   此处提供了一个例子的说明，您可以决定对 Web 服务器进行不同的配置。服务器的默认路径名为：`/usr/iplanet/servers`

   在 iPlanet Web 服务器安装期间接受默认路径。本书中使用这些默认路径。如果您决定将其安装在不同的位置，务必记住它的安装位置。

3. **运行安装程序。**

4. **回答安装脚本中的提示。**

   除以下提示外，为方便起见，您可以接受默认值。

   a. 通过键入 `yes` **同意接受许可条款。**

   b. 输入全限定的 *hostname.domain*。

   c. 输入 iWS 管理服务器密码两次。

   d. 提示时，按回车键。

▼ 创建可信数据库

1. **启动管理服务器。**

   要启动 iPlanet Web 服务器，请使用以下命令（而不是将 `startconsole` 作为 `setup` 请求来运行）：

```
# /usr/iplanet/servers/https-admserv/start
iPlanet-WebServer-Enterprise/6.0SP1 B08/20/2001 00:58
warning: daemon is running as super-user
[LS ls1] http://hostname.domain/port 8888 ready to accept requests
startup: server started successfully
```

   响应消息提供要连接到的 URL 以管理您的服务器。

2. **通过打开 Web 浏览器并输入以下内容来启动 iPlanet 管理服务器：**

```
http://hostname.domain:admin_port
```

   随即弹出一个窗口，要求输入用户 ID 和密码。请输入在运行安装程序期间选择的 iWS 管理服务器用户名和密码。

注意 – 如果在 iPlanet Web 服务器安装期间使用了默认值，则请为用户 ID 或 iWS 管理服务器用户名输入 `admin`。

---

3. **单击 “OK （确定）”。**

4. **创建 Web 服务器实例的可信数据库。**

   最好对多个 Web 服务器实例启用安全性。对每个 Web 服务器实例重复此过程。

注意 – 如果您也想在管理服务器上运行 SSL，则设置可信数据库的过程类似。有关详细信息，请参阅 iPlanet 文档。

a. 单击管理服务器中的 “Servers （服务器）” 选项卡。

b. 选择服务器，然后单击 “Manage （管理）” 按钮。

c. 在靠近页首的地方单击 “Security （安全）” 选项卡，然后选择 “Create Database （创建数据库）” 选项。

d. 在两个对话框中输入密码 （Web 服务器可信数据库），然后单击 “OK （确定）”。

选择一个至少有 8 个字符的密码。iPlanet Web 服务器以安全模式运行时，此密码将用来启动内部加密模块的密码。

5. 执行以下脚本启用 Sun Crypto 加速器 1000 板：

```
# /opt/SUNWconn/crypto/bin/sslconfig
```

此脚本提示您选择 Web 服务器。它为 iPlanet Web 服务器或 Apache Web 服务器安装 Sun Crypto 加速器 1000 加密模块。脚本然后会更新配置文件以启用 Sun Crypto 加速器 1000 板。

6. 键入 `1` 来配置 iPlanet Web 服务器以使用 SSL，然后按 “Enter”。

```
Sun Crypto Accelerator Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for iPlanet Web Server
or Apache.

Please select the type of web server you wish to configure
to use the Sun Crypto Accelerator:
------------------------------------------------------------
1. Configure iPlanet Web Server for SSL
2. Configure Apache for SSL
3. Work with iPlanet and Apache keys
Your selection (0 to quit):  1
```

7. **提示时输入 Web 服务器根目录的路径，然后按 “Enter”。**

```
Please enter the full path of the web server
root directory [/usr/iplanet/servers]: /usr/iplanet/servers
```

8. **如果要继续，请在提示时键入** y **并按 “Enter”。**

```
This script will update your iPlanet Web Server installation
in /usr/iplanet/servers to use the Sun Crypto Accelerator
You will need to restart your admin server after this has
completed.
Ok to proceed? y

Using database directory /usr/iplanet/servers/alias...
Module "Sun Crypto Accelerator" added to database.
/usr/iplanet/servers has been configured to use
the Sun Crypto Accelerator.


<Press ENTER to continue>
```

9. **键入** 0 **退出。**

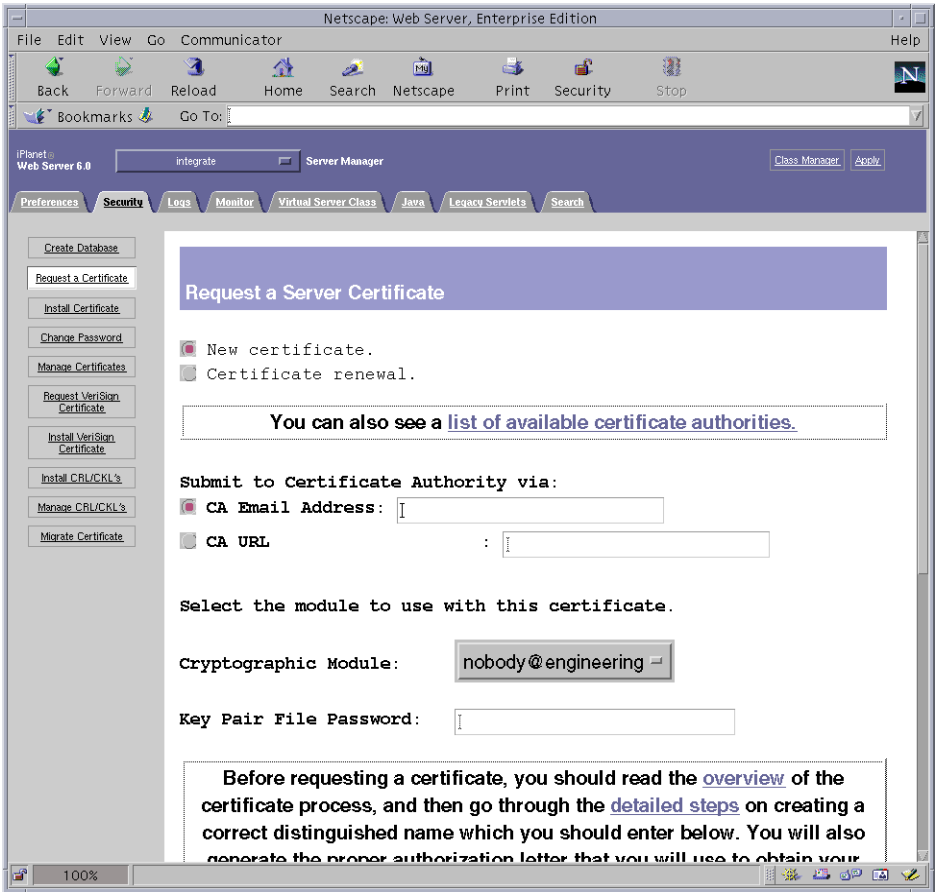
▼ 生成服务器证书

1. **通过键入以下命令重新启动管理服务器：**

```
# /usr/iplanet/servers/https-admserv/stop
# /usr/iplanet/servers/https-admserv/start
```

2. **要请求服务器证书，请单击靠近页首的 “Security （安全）” 选项卡。**
   随即会显示 “Create Trust Database （新建可用数据库）” 窗口。

3. **在该页的左侧选择 “Request Certificate （请求证书）” 链接。**



4. **使用以下信息填写表单以生成证书请求：**

   a. **选择 “New Certificate （新建证书）”**

      如果可以直接将证书请求发送到可通过 Web 访问的证书机构或注册机构，请选择“CA URL”选项。否则，请选择 “CA Email Address （CA 电子邮件地址）”，选择希望通过电子邮件发送证书请求的电子邮件收件人地址。

   b. **选择您要使用的加密模块。**

      在此下拉菜单中，每个领域都有自己的条目。务必选择正确的领域。要使用 Sun Crypto 加速器 1000，必须选择一个格式为 *user@realm-name* 的模块。

   c. **在 “Key Pair File Password （密钥对文件密码）”对话框中，为将拥有密钥的 *user@realm-name* 提供密码。**

   d. **为以下字段提供正确信息：**

      - Requestor Name：请求者的联系信息
      - Telephone Number：请求者的联系信息
      - Common Name：在来访者的浏览器 *hostname.domain* 中键入的 Web 站点域
      - Email Address：请求者的联系信息
      - Organization：证书上声明的 Organization 的值
      - Organizational Unit：（可选）将在证书上声明的 Organizational Unit 的值
      - Locality：（可选）城市、郡县、公国或国家/地区，如果提供也在证书上予以声明
      - State：（可选）本字段中州省的全称
      - Country：由两个字母组成的国家/地区 ISO 代码，在证书上予以声明，为必填字段

   e. **一旦输入所有信息，单击 “OK （确定）”按钮提交。**

5. **利用证书机构生成证书。**

   - 如果选择将证书请求发送给 CA URL，则证书请求会自动发送到此处。
   - 如果选择 “CA Email Address （CA 电子邮件地址）”，请带标题复制通过电子邮件发给您的证书请求，然后将其交给证书机构。

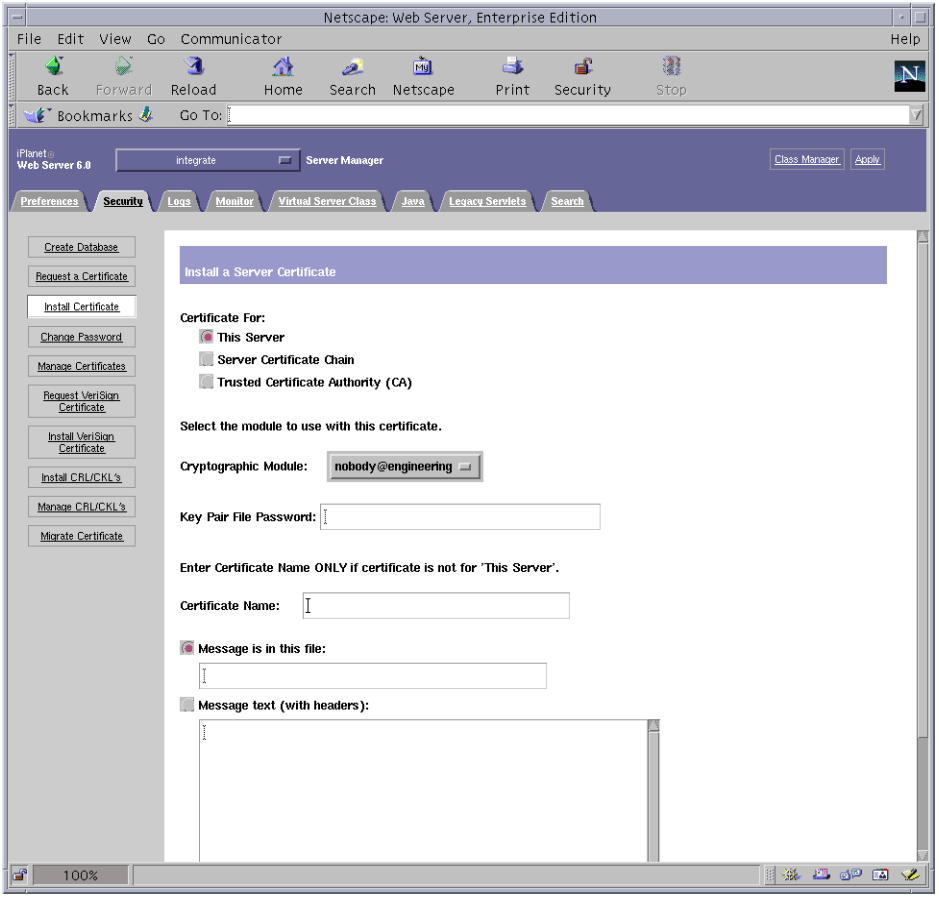
6. **一旦生成证书，请将其连标题一起复制到剪贴板上。**

   注意：证书与证书请求不同，常常以文本格式向您提供。

▼ 安装服务器证书

1. **在该页的左侧选择 “Install Certificate （安装证书）” 链接。**
   一旦证书机构批准您的请求并签发证书，您必须将其安装在 iPlanet Web 服务器中。

2. **选择 “Security （安全）” 选项卡，然后在左框上选择 “Install Certificate （安装证书）” 选项。**



3. **填写表单，安装证书：**
   - Certificate For：This Server
   - Cryptographic Module：选择正确的 *user@realm-name*。
   - Key Pair File Password：为拥有以前生成的密钥的 *user@realm-name* 提供密码。
   - Certificate Name：在大多数情况下，您可以空着不填。如果选择提供名称，该名称将改变 Web 服务器在使用 SSL 支持运行时用来访问证书和密钥的名称。

4. **选择 “Message text (with headers) （带标题的消息文本）”，粘贴前面复制的证书。**

5. **单击该页底部的 “OK （确定）”按钮，将您从证书机构复制的证书粘贴到 “Message （消息）”框中。**

   随即会显示证书的一些基本信息。

6. **如果输入的内容正确，请单击 “Add Server Certificate （添加服务器证书）”按钮。**

   随即会显示屏幕消息，通知您重新启动服务器。 Web 服务器实例一直处于关闭状态时不必重新启动服务器。同时还会通知您，为使 Web 服务器使用 SSL，必须对 Web 服务器进行相应配置。使用以下步骤配置 Web 服务器。

配置 iPlanet Web Server 6.0

既然已安装 Web 服务器和服务器证书，必须对 Web 服务器进行配置以使用 SSL。

▼ 配置 iPlanet Web Server 6.0

1. **在靠近页首的地方单击 “Preferences （参数选择）”选项卡。选择左框上的 “Edit Listen Sockets （编辑监听套接字）”选项。**

   主框列出了 Web 服务器实例的所有监听套接口。

   a. **更改以下字段：**
      - Port：设置为您要运行启用 SSL 的 Web 服务器的端口 （通常为端口 443）。
      - Security：设置为 “On （开）”。

   b. **单击 “OK （确定）”按钮应用这些更改。**

      在 “Edit Listen Sockets （编辑监听套接字）”页的安全性字段中，现在应该显示一个 “Attributes （属性）”链接。

2. **单击 “Attributes （属性）”链接。**

3. **输入 *user@realm-name* 密码对系统上的 *user@realm-name* 进行验证。**

4. **从弹出窗口中选择 SSL 设置。**

   您可以选择 “Cipher Default”设置、SSL2 或 SSL3/TLS。 Default 选择不显示默认设置。其它两个选择要求选择想启用的算法。

5. **为 *user@realm-name* 选择证书，后跟 `:Server-Cert` （如果不同，则使用您选择的名称）。**

   “Certificate Name”字段仅显示相应的 *user@realm-name* 所拥有的密钥。

6. **如果已选择证书并确认所有安全性设置，请单击 “OK （确定）”按钮。**

7. **单击右上角的 “Apply （应用）”链接，应用这些更改，然后启动服务器。**

8. **单击 “Load Configuration Files （加载配置文件）”链接应用这些更改。**

   您被重定向到允许您启动 Web 服务器实例的页上。

   如果在服务器关闭时单击 “Apply Changes （应用更改）”按钮，则会弹出一个窗口，提示输入密码。此窗口不可以调整大小，因此在提交更改时可能会遇到问题。

   上述问题有两个临时解决办法：

   - 改为单击 “Load Configuration Files （加载配置文件）”。
   - 先启动 Web 服务器，然后单击 “Apply Changes”按钮。

9. **在对话框中提供请求的密码，启动服务器。**

   将会提示您提供一个或多个密码。出现 “Module Internal”提示时，为 Web 服务器可信数据库提供密码。

   出现 “Module *user@realm-name*”提示时，输入您使用 `secadm` 在 *realm-name* 中创建*用户*时设置的密码。

10. **通过转至下面的 URL 在浏览器中检查启用 SSL 的新 Web 服务器：**

    `https://`*hostname.domain*`:`*server_port*`/`

    注意：默认 *server_port* 为 443。

第 6 章

启用 Apache Web 服务器

本章介绍如何启用 Sun Crypto 加速器 1000 板与 Apache Web 服务器一同使用。

本章包括以下几节

- 第 39 页 “启用 Apache Web 服务器”
- 第 42 页 “创建证书”

启用 Apache Web 服务器

Apache Web Server 1.3.12 随 Solaris 8 7/01 操作环境一起提供。以下说明针对特定 Apache Web 服务器版本。有关使用 Apache Web 服务器的详细信息，请参阅 Apache Web 服务器文档。

▼ 启用 Apache Web 服务器

1. **创建** `httpd` **配置文件**。

   对于 Solaris 系统， `httpd.conf-example` 文件通常都在 `/etc/apache` 中。您可以将此文件用作模板并进行如下复制：

   ```
   # cp httpd.conf-example /etc/apache/httpd.conf
   ```

   用您的服务器名替换文件中的 `ServerName`。

2. **启动** sslconfig。

```
# /opt/SUNWconn/crypto/bin/sslconfig
```

3. **选择** 2，**配置 Apache Web 服务器以使用 SSL：**

```
Sun Crypto Accelerator Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for iPlanet Web Server
or Apache.

Please select the type of web server you wish to configure
to use the Sun Crypto Accelerator:
------------------------------------------------------------
1. Configure iPlanet Web Server for SSL
2. Configure Apache for SSL
3. Work with iPlanet and Apache keys

Your selection (0 to quit):
```

4. **提供 Apache 二进制文件所在的目录。**
   在 Solaris 系统上，通常为 /usr/apache。

```
Please enter the directory where the Apache
binaries and libraries exist [/usr/apache]: /usr/apache
```

5. **提供 Apache 的配置文件所在的位置。**
   在 Solaris 系统上，通常为 /etc/apache。

```
Please enter the directory where the Apache
configuration files exist [/etc/apache]: /etc/apache
```

6. **为系统创建 RSA 密钥对。**
   如果选择不创建，您以后必须返回来使用 sslconfig 生成密钥。

```
Do you wish to create a new RSA keypair and certificate request?
[Y/N]:
```

如果您对此问题回答 “No”，则跳至第 42 页 “创建证书”。

7. **提供用于存储密钥的目录。**

   如果该目录不存在，则需创建。

```
Where would you like the keys stored? [/etc/apache/keys]:
/etc/apache/keys
```

8. **为密码资料选择一个基本名称。**

   此名称附带不同的后缀以区别密钥文件、证书请求文件和稍后的证书文件。

```
Please choose a base name for the key and request file:
```

9. **提供的密钥长度介于 512 和 2048 位之间。**

   对于大多数 Web 服务器应用程序而言， 1024 位已经足够安全，不过如果愿意，可以选择更安全的密钥。

```
What size would you like the RSA key to be [1024]? 1024
Generating RSA private key, 1024 bit long modulus
..........++++++
......++++++
e is 65537 (0x10001)
```

10. **创建您的 PEM 密码。**

    此密码用以保护密钥资料。务必选择安全且易记的密码。如果忘记密码，您将无法访问您的密钥。

```
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
```

警告 – 必须记住输入的密码。没有密码，就无法访问您的密钥。丢失的密码无法重新找到。

创建证书

以下步骤介绍如何创建 Apache Web 服务器使用 Sun Crypto 加速器 1000 板所需的证书。

▼ 创建证书

1. **用您刚刚创建的密钥来创建证书请求。**

   您必须先输入密码以访问密钥。然后为以下字段提供正确信息：

   - Country Name：由两个字母组成的国家/地区 ISO 代码，在证书上予以声明，为必填字段
   - State or Province Name：（可选）本字段中州省的全称 （或键入 . 然后按回车键）
   - Locality：（可选）城市、郡县、公国或国家/地区，如果提供也在证书上予以声明
   - Organizational Name：证书上声明的 Organization 的值
   - Organizational Unit Name：（可选）将在证书上声明的 Organizational Unit 的值
   - SSL Server Name：在来访者的浏览器中键入的 Web 站点域
   - Email Address：请求者的联系信息

```
Enter PEM pass phrase:
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:US
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) []:Fictional Company, Inc.
Organizational Unit Name (eg, section) []:Online Sales Division
SSL Server Name (eg, www.company.com) []:www.fictional-company.com
Email Address []:admin@fictional-company.com
```

2. 按说明修改 /etc/apache/httpd.conf 文件。

随即会显示有关您的密钥和证书文件的信息。还会指导您如何修改 /etc/apache/httpd.conf 文件以便与 Sun Crypto 加速器 1000 一起使用。

```
The keyfile is stored in /etc/apache/keys/ap6-key.pem.
The certificate request is in /etc/apache/keys/ap6-certreq.pem.

You will need to edit /etc/apache/httpd.conf for the following items:

You must specify the ports that Apache will listen to for
SSL connections, as well as for non-SSL connections.  One
way to accomplish this is to add the following lines in
the Listen section:

Listen 80
Listen 443

In the LoadModule section, add the following:

LoadModule ssl_module /usr/apache/libexec/mod_ssl.so.1.3.12

In the AddModule section, add the following:

AddModule mod_ssl.c
```

3. **如果选择不安装** VirtualHost，**则必须将** SSLEngine, SSLCertificateFile **和** SSLCertificateKeyFile **指令置于** httpd.conf **文件中，在** SSLPassPhraseDialog **指令之上。**

```
You may need a virtual host directive similar to
what is shown below:

<VirtualHost _default_:443>
        SSLEngine on
        SSLCertificateFile /etc/apache/keys/ap6-cert.pem
        SSLCertificateKeyFile /etc/apache/keys/ap6-key.pem
</VirtualHost>

You must add the following line after all of your VirtualHost
definitions:

SSLPassPhraseDialog exec:/opt/SUNWconn/crypto/bin/sslpassword

Other SSL-related directives and their explanations
can be found in the Sun Crypto Accelerator documentation.

Other Apache-related directives may need to be configured
in order to start your Apache web server.  Please refer
to your Apache documentation.

<Press ENTER to continue>
```

如果对步骤 6 中问题的回答为否，还会向您提供以后如何生成密码资料的其它信息：

```
Since you did not create keys, you will need to
make sure that you have a key file and a certificate
file in place before enabling SSL for Apache.

You can create a new key file and certificate request
by selecting the "Generate a keypair and request a
certificate for Apache" option after choosing
"Work with iPlanet and Apache keys" from the
sslconfig main menu.
```

4. **请在结束** sslconfig **时选择** 0 **退出。**

5. **从** /etc/apache/keys/*base_name*-certreq.pem **（其中 base_name 在步骤 8 中设置）中复制带标题的证书请求并将其交给证书机构。**

6. **一旦生成证书，请创建证书文件** `/etc/apache/keys/`*base_name*`-cert.pem` **并将您的证书粘贴到该证书文件中。**

7. **启动 Apache Web 服务器。**

   这里假定您的 Apache 二进制文件目录为 `/usr/apache/bin`。如果它不是您的二进制文件目录，请键入正确的目录。

```
# /usr/apache/bin/apachectl start
```

8. **提示时，请输入您的 PEM 密码。**

9. **通过转至下面的 URL 在浏览器中检查启用 SSL 的新 Web 服务器：**

   `https://`*server_name*`:`*server_port*`/`

   注意：默认 *server_port* 为 443。

第 7 章

故障诊断和排除

本章介绍 Sun Crypto 加速器 1000 软件的诊断测试和故障排除。其中包含以下几节：

- 第 47 页 “SunVTS 诊断软件”
- 第 51 页 “Sun Crypto 加速器 1000 故障排除”

SunVTS 诊断软件

SunVTS 测试 `dcatest` 在 *Sun Crypto 加速器 1000* CD 上的 `SUNWdcav` 包中提供。它具有核心 SunVTS 测试控件和用户界面（在 Solaris 补充 CD 上的 `SUNWvts` 和 `SUNWvtsx` 中提供），可以为 Sun Crypto 加速器 1000 板提供诊断。

有关如何运行和监控这些诊断测试的说明，请参阅 SunVTS 文档。这些文档可以在用于您的系统的 Solaris 发行版的 Solaris 补充 CD 上的 Solaris on Sun Hardware AnswerBook 中获得。

注意 – 只有遇到您从 Solaris Supplement CD 上安装了 SunVTS 的情形，才使用 SunVTS 仅在。

▼ 运行 dcatest

1. **以超级用户身份启动 SunVTS。**

```
# /opt/SUNWvts/bin/sunvts
```

有关启动 SunVTS 的详细说明，请参阅 *SunVTS User's Guide*。

以下说明假定您已经使用 CDE 用户界面启动了 SunVTS。

2. **在 SunVTS Diagnostic 主窗口中，将 “System Map （系统映射）”设置为 “Logical （逻辑）”模式。**
3. **清除相应复选框，禁用所有测试。**
4. **选择 “OtherDevices （其它设备）”复选框，然后再选择 “OtherDevices （其它设备）”的加号框，显示 “OtherDevices （其它设备）”组中的所有测试。**
5. **清除 “OtherDevices （其它设备）”组中除 `dcatest` 以外的复选框。**
   - 如果显示 `dcatest`，则转至步骤 6。
   - 如果不显示 `dcatest`，则在系统中浏览以找到它。可以选择 “Commands （命令）”下拉菜单中的 Reprobe 系统。

   有关确切步骤，请参阅 SunVTS 文档。探测过程完成并显示 `dcatest` 时，继续执行步骤 6。
6. **单击 `dcatest` 的一个实例，然后右键单击并拖动鼠标以显示 “Test Parameter Options （测试参数选项）”。**

   仅属于 `dcatest` 的这些选项在第 49 页 “`dcatest` 的测试参数选项”中予以说明。
7. **进行所有选择后，单击 “Within Instance Apply （在实例内应用）”以更改 `dcatest` 的所选实例。或者单击 “Across All Instances Apply （跨所有实例应用）”以更改 `dcatest` 的所有选中的实例。**

   进行该操作后，弹出框消失，返回 “Sun Diagnostic （Sun 诊断）”主窗口。
8. **单击 `dcatest` 的一个实例，然后右键单击并拖动鼠标以显示 “Test Execution Options （测试执行选项）”。**

   显示 “Test Execution Options （测试执行选项）”的另一种方法是单击 “Options （选项）”弹出框，然后再单击 “Test Executions （测试执行）”。这些选项是会影响所有测试的通用 SunVTS 控件。有关详细信息，请参阅 SunVTS 文档。
9. **进行所有选择后，单击 “Apply （应用）”，弹出窗口消失，返回 “Sun Diagnostic （Sun 诊断）”主窗口。**
10. **单击 “Start （开始）”运行所选测试。**
11. **单击 “Stop （停止）”停止所有测试。**

dcatest 的测试参数选项

表 7-1 显示了 dcatest 的测试参数选项，如第 48 页 “运行 dcatest”中步骤 6 所述。测试的板类型在弹出框的 “Configuration （配置）”区域显示。

表 7-1 dcatest 的测试参数选项

选项标签	说明
Test_Sel	指定要运行的子测试组合的十进制数值。如果值为 0，则选择所有测试。每个子测试都被分配一个以 2 为幂的数。可以输入为子测试分配的数以选择单个子测试。可以输入为若干所需子测试分配的数的和以选择多个子测试。默认设置为 0。
Info_Print	启用或禁用输出信息 （INFO 类型）消息。默认设置为 “Enable （启用）”。

表 7-2 说明了 dcatest 子测试。

表 7-2 dcatest 子测试

测试名称	号码	说明
ALL	0	执行所有测试。
SHOWINFO	1	输出 INFO 类消息，在测试信息下显示提供商和设备。
3DES	2	测试 3DES 批量加密。
RSA	4	测试 RSA 公用和私人密钥。
DSA	32	测试 DSA 签名验证。
Random	64	测试随机和伪随机号码生成。输出 INFO 类消息，显示生成的号码。

子测试生成的消息在 “SunVTS Diagnostic （Sun VTC 诊断）”主窗口的 “Test Messages （测试消息）”区域显示。子测试生成的消息按类型分组：

- INFO 类消息 （如果在 “Test Parameters （测试参数）”弹出框中启用 Info_Print 选项，则提供非重要信息）在 “Test Messages （测试消息）”区域输出并在 “Information Log （信息日志）”中记录。
- FATAL 错误类消息始终显示并在 “Error Log （错误日志）”和 “Information Log （信息日志）”中记录。
- VERBOSE 类消息 （通过子测试跟踪进度）仅在 “Test Execution （测试执行）”弹出窗口中启用 VERBOSE 选项时显示。 VERBOSE 消息不在任何日志中记录。

  显示和记录 dcatest FATAL 错误消息的静默模式可以通过禁用 VERBOSE 和 Info_Print 选项选择。

dcatest 命令行语法

如果您从命令行选择运行 dcatest，而不是 CDE 环境，则所有参数都可以在命令行字符串中指定。

在 32 位模式中， dcatest 的路径是 /opt/SUNWvts/bin/。在 64 位模式中，dcatest 的路径是 /opt/SUNWvts/bin/sparcv9/。

下例显示了 32 位模式命令的语法：

```
/opt/SUNWvts/bin/dcatest -f [Standard Command-Line Arguments]
[-o [dev=dcan][,testsel=n][,infodis]]
```

有关标准命令行参数的定义，请参阅 *SunVTS Test Reference Manual*。由于 dcatest 是一个功能模式测试，所以必须包括 -f。使用 -u 可以使用用法消息，或者使用 -v 显示 VERBOSE 消息。上面方括号中包含的项目表示可选条目。省略某选项，则使用该选项的默认行为，如表 7-3 中所述。

表 7-3 dcatest 命令行语法

参数	说明
dev=dca*n*	指定要测试的设备实例，如 dca0 或 dca2。如果不包括在内，则默认为 dca0。
testsel=*n*	指定要执行的子测试。其中， n 可以是介于 0 和 127 之间的数字。如果不包括在内，则默认为 0。
infodis	如果不禁用 INFO 类消息，则包括在内。如果不包括在内，则默认为 Info_Print Enabled。

Sun Crypto 加速器 1000 故障排除

要确定 Sun Crypto 加速器 1000 设备是否在系统中列出，请从 OpenBoot PROM (OBP) 提示符处键入 `show-devs` 以显示设备列表。您应该在设备列表中看到类似于下面几个示例中的几行。它们随所使用的特定 Sun Crypto 加速器 1000 板而异。

```
ok show-devs
. . .
/pci@1f,0/pci@1/pci108e,5455@2
. . .
```

在上例中， `pci108e,5455` 指示 Sun Crypto 加速器 1000 板的设备路径。该板上没有固件，因此 OBP 级诊断程序不可用。

Sun Crypto 加速器 1000 不包含反映板上加密活动的灯或其它指示器。为了确定加密作业请求是否实际上在板上执行，请使用 `kstat`(1M) 命令显示设备用法：

```
# kstat -m dca -i 0 -n dca0

module: dca                             instance: 0
name:   dca0                        class:    misc
    3desbytes                       3040
    3desjobs                        5
    crtime                          65.342725895
    dsasign                         0
    dsaverify                       0
    rngbytes                        10592
    rngjobs                         187
    rngsha1bytes                    16328
    rngsha1jobs                     327
    rsaprivate                      9
    rsapublic                       0
    snaptime                        106956.467004482
```

显示 kstat 信息表示加密请求或 “作业”是否正发送到 Sun Crypto 加速器 1000 板。“作业”值随时间发生变化，表示板正在加速发送到 Sun Crypto 加速器 1000 板的加密作业请求。如果未将加密作业请求发送到板，则请根据 Web 服务器特定配置验证您的 Web 服务器配置。

始终无法确定加密请求是否已经执行，类似加密请求根据提交请求时加载的子系统情况可以在不同位置执行。

不要试图解释 kstat(1M) 返回的核心/驱动程序统计值。这些值保存在驱动程序内，从而方便现场支持。含义和实际名称会随时间而变化。

附录 **A**

用 iPlanet Web 服务器管理 Sun Crypto 加速器 1000 板

本附录概述了使用 iPlanet Web 服务器管理 Sun Crypto 加速器 1000 板时该板的安全性。

注意 – 要管理领域，您的机器必须拥有对系统管理员帐户的访问权限。

本附录包括以下几节：

- 第 53 页 “概念和术语”
- 第 61 页 “设置和管理领域”
- 第 65 页 “设置并管理用户帐户”

概念和术语

必须为通过 PKCS#11 接口 （如 iPlanet Web 服务器）与 Sun Crypto 加速器 1000 通信的应用程序创建领域和用户。

Sun Crypto 加速器 1000 环境中的用户是加密密码资料的唯一所有者。每个用户可以拥有多个密钥。对于不同的配置，用户需要多个密钥，如 “生产”密钥和 “开发”密钥（反映用户的不同组织）。对于高可用性 (HA) 配置，也要求多个密钥。注意：术语 “用户”或 “用户帐户”是指 Sun Crypto 加速器 1000 用户，而非传统的 UNIX 用户帐户。UNIX 用户名和 Sun Crypto 加速器 1000 用户名之间没有固定的一一对应关系。

领域是用户及其密码资料的逻辑分类。领域可以包含多个用户。按领域对用户进行分类的优点是可以为每个领域保留唯一的名字空间。这样就可以对领域内容分别进行管理。

典型安装包含具有单个用户的单个领域。例如，这种配置可以包含单个领域“webserver”，该领域中具有单个用户 “nobody”。这样，用户 “nobody”即可在该单个领域中拥有并实施对服务器密钥的访问控制。

可以灵活构建其它领域以对用户和密码资料进行分类。较复杂的配置可以包含多个领域，如 “金融”、“法律”和 “工程”。每个领域具有唯一的名字空间。例如，金融领域中的用户 “webserv”与工程领域中的用户 “webserv”是不同的用户帐户。

管理工具 `secadm` 用于管理 Sun Crypto 加速器 1000 的领域和用户。

领域、用户和 iPlanet Web 服务器

iPlanet Web 服务器需要引用 Sun Crypto 加速器 1000 管理的密钥时，使用 “标记名”表示该密钥是由硬件而非其内部软件数据库管理的。

Sun Crypto 加速器 1000 将用户帐户和领域名以及 “@”符号合起来创建标记名。在上面的典型安装示例中，创建了单个领域 “webserver”，它具有单个用户 “nobody”。iPlanet Web 服务器用以引用领域 “webserver”用户 “nobody”的密钥的标记名为“nobody@webserver”。请求证书、安装证书或验证以启动 iPlanet Web 服务器时，必须使用用户 nobody 的密码 （即使用 `secadm` 创建用户时设置的密码）。

标记和插槽文件

iPlanet Web 服务器通过标记 （亦称为插槽）访问密码资料。插槽文件是 Sun Crypto 加速器 1000 管理员选择性地向给定应用程序提供完全特定标记的技术。

如果不存在任何插槽文件，Sun Crypto 加速器 1000 软件就会向 iPlanet Web 服务器提供一组默认标记。在这种情况下，将向每个领域提供一个标记，标记名为 `nobody@`*`realm-name`*。

示例

包含工程、金融和法律三个领域。向 iPlanet Web 服务器提供以下标记：

- nobody@engineering
- nobody@finance
- nobody@legal

但是，要使这些名称中的任何一个可用，用户 “nobody”必须在每个领域中都存在。

插槽文件

要覆盖默认情况，必须要有插槽文件。插槽文件是包含一个或多个标记名 （每行一个）的文本文件。 iPlanet Web 服务器仅提供本文件中列出的标记。指定插槽文件的方法如下 （以优先顺序排列）：

1. 文件 `$HOME/.SUNWconn_crypto_slots`

   本文件必须位于 iPlanet Web 服务器运行时使用的 UNIX 用户的主目录中。 iPlanet Web 服务器可以使用没有主目录的 UNIX 用户身份来运行，但在这种情况下这种方法并不合适。

2. 文件 `/etc/opt/SUNWconn/crypto/slots`

   `/etc/opt/SUNWconn/crypto/slots` 文件是全局默认文件，用户主目录中不存在 `.SUNWconn_crypto_slots` 文件时使用该文件。

下面是插槽文件内容的一个示例：

```
webserv@engineering
webserv@finance
```

如果找不到上面列出的任何文件，则使用第 54 页 “标记和插槽文件”中所述的默认方法。

与 iPlanet Web 服务器配置有关的标记名的详细信息，请参见第 3 章。

使用 secadm

secadm 程序提供了 Sun Crypto 加速器 1000 的命令行接口。

为了便于访问 secadm 程序，请在您的搜索路径中包含 Sun Crypto 加速器 1000 工具目录，例如：

```
$ PATH=$PATH:/opt/SUNWconn/crypto/bin
$ export PATH
```

secadm 命令语法是：

secadm [-h]

secadm [-y] [-f *filename*]

secadm [-y] [-r *realm-name*] [-u *username* | -s *admin-name*] *command*

命令位于 /opt/SUNWconn/crypto/bin/ 目录中。

表 A-1 显示了 secadm 工具的选项

表 A-1 secadm 选项

选项	含义
-h	显示 secadm 的命令帮助并退出。
-f *filename*	从 *filename* 读入一个或多个命令并退出。
-r *realm-name*	仅用于单命令模式。 -r 选项通知 secadm 在领域 *realm-name* 中执行提供的命令。
-s *admin-name*	仅用于单命令模式。 -s 选项通知 secadm 将 *admin-name* 作为登录名以系统管理员身份登录。 *admin-name* 必须是 UID 0（零） UNIX 用户（如 root）。登录在执行提供的命令之前进行。
-u *username*	仅用于单命令模式。 -u 选项通知 secadm 以 *username* 身份登录。登录在执行提供的命令之前进行。
-y	对任何通常用来提示要求确认的命令强制回答 “是”。

操作模式

secadm 可以按三种模式运行。这些模式的主要差异在于命令如何被传给 secadm。三种模式分别为单命令模式、文件模式和交互模式。每种模式都要求各自不同的密码。

单命令模式

在单命令模式中，用户在指定了所有命令行开关选项后指定 secadm 运行的命令。例如，以下命令将显示所有存在的领域并向用户返回命令 shell 提示符。

```
$ secadm show realm
```

以下命令以系统管理员身份执行登录操作并在工程领域中创建用户 webserv。

```
$ secadm -r engineering -s root create user=webserv
Password:
Initial password:
Confirm password:
User webserv created successfully.
```

注意：在 “Password:（密码）”提示处输入的密码要求系统管理员密码，而在 “Initial password:（初始密码）”和 “Confirm password:（确认密码）”处输入的密码，则要求新创建的用户的密码。

单命令模式的所有输出都进入标准的输出流。使用基于标准 UNIX shell 的方法可以对此输出进行重定向。

文件模式

在文件模式中，用户指定一个 secadm 从中读取一个或多个命令的文件。该文件必须为 ASCII 文本，每行包含一个命令。在每条注释之前加 “#”字符。如果设置了文件模式选项， secadm 则在最后选项之后忽略任何命令行参数。下例运行 deluser.scr 中的命令并对所有提示作肯定回答：

```
$ secadm -f deluser.scr -y
```

交互模式

交互模式向用户提供一个类似于 ftp(1) 的接口，一次可以输入一个命令。交互模式不支持 -y 选项。

用 secadm 输入命令

secadm 程序有一个与 Sun Crypto 加速器 1000 板进行交互必须使用的命令语言。使用一词的全部或部分来输入命令 （必须能够与任何其它可能性区分开来，唯一地识别该词）。可以使用 “sh” 代替 “show”，但 “lo” 比较含糊，因为它既可以表示 “login”，也可以表示 “logout”。

下例显示了使用整词输入命令的情况：

```
secadm{root@engineering}# show user
User                                          Status
------------------------------------------------------
webserv                                       enabled
alice                                         enabled
bob                                           enabled
------------------------------------------------------
```

使用部分词作为命令，如 sh us 可以获得相同的信息。

含糊不清的命令会产生解释性的响应：

```
secadm{root@engineering}# lo
Ambiguous command: lo
```

使用 secadm 进行验证

许多命令，特别是处理用户帐户和密钥的命令要求您以系统管理员或用户身份来进行验证。系统管理员必须向 Sun Crypto 加速器 1000 进行验证，才能执行诸如创建领域、创建用户帐户、启用和禁用用户帐户以及删除领域和用户帐户的操作。为了更改用户密码或列出该用户的密钥对象，必须以用户身份进行验证。表 A-2 显示了系统管理员可以使用的命令与用户可以使用的命令。

表 A-2 命令表

命令	验证	持有证书	已验证用户
`create user=`*username*	无	是	系统管理员
`create realm=`*realm-name*	是	无	系统管理员
`delete user=`*username*	无	是	系统管理员
`delete realm=`*realm-name*	是	无	系统管理员
`disable user=`*username*	无	是	系统管理员
`enable user=`*username*	无	是	系统管理员
`exit`	无	无	全部
`login`	是	无	用户
`logout`	无	无	全部
`passwd`	是	是	用户
`set realm=`*realm-name*	无	无	全部
`show class`	无	无	全部
`show key`	无	是	用户
`show realm`	无	无	全部
`show user`	无	是	系统管理员
`su`	是	无	系统管理员
`quit`	无	无	全部
`unset realm`	无	无	全部

要以系统管理员身份进行验证，您必须提供 UNIX 用户名，即 UID 0 （如 root）并在提示时提供密码。创建用户时，用户需要为其设置的密码。以系统管理员身份或用户身份登录时，必须先选择领域。

以用户身份登录，请键入：

```
secadm{realm-name}> login user=username
```

以系统管理员身份登录，请键入：

```
secadm{realm-name}> su
```

以用户身份或系统管理员身份登录时， secadm 提示行会显示当前登录的用户。用户登录名与系统管理员登录名的区别在于提示行的最后一个字符。用户使用尖括号 (>)，而系统管理员使用井字符 (#)。如果您当前以用户身份或系统管理员身份登录，又想以另一用户身份或系统管理员身份登录，则您将在新登录成功时失去当前证书。例如：

```
secadm> set realm=engineering
secadm{engineering}> login user=webserv
Password:
secadm{webserv@engineering}> su
System Administration Login Required
Login: root
Password:
secadm{root@engineering}# logout
secadm{engineering}>
```

获得命令帮助

secadm 内置有帮助功能。要获得帮助，您必须在想要获得更多帮助的命令后面输入“?”字符。如果已输入整个命令，而且该行的任何位置都有 “?”，您将会得到该命令的语法。例如：

```
secadm> create ?
Usage: create {user=<username> | realm=<realm-name>}

secadm> show ?
Sub-Command                        Description
-------------------------------------------------------
class                              Show all realm classes
key                                Show all key objects in a realm
realm                              Show all realms
user                               Show all system accounts
```

输入 “?” 会向您提供有效命令词列表。例如：

```
secadm> ?
Sub-Command                         Description
-----------------------------------------------------
create                              Create users and accounts
delete                              Delete users and accounts
disable                             Disable a user
enable                              Enable a user
exit                                Exit secadm
login                               Login as a user
logout                              Logout current session
passwd                              Change password for a user
set                                 Set current working realm
show                                Show system settings
su                                  Authenticate as the System Administrator
quit                                Exit secadm
unset                               Unset secadm operating parameters
```

如果想在命令行模式中获得帮助，必须记住 “?” 字符有时是由您正在处理的 shell 来解释的。确保在问号之前使用命令 shell 转义字符。

退出 secadm 程序

可以使用两个命令从 `secadm` 退出：`quit` 和 `exit`。也可以使用 CTRL-D 组合键从 `secadm` 退出。

设置和管理领域

领域是密钥材料的储存库。管理员和用户与领域相关。领域不但提供存储，而且提供用户帐户拥有密钥对象的方式。这可以使密钥在不以所有者身份验证的应用程序中隐藏。领域有两个组成部分：

- 密钥对象：它是为应用程序 （如 iPlanet Web 服务器）存储的长期密钥。
- 用户帐户：这些帐户是应用程序验证和访问特定密钥的方式。

虽然仅需要一个领域，但却可以有多个领域，每个领域各有自己的一组用户帐户。例如，如果应用程序以用户 `webserv` 身份验证并需要访问该领域中的密钥，则用户帐户 `webserv` 必须在该领域中。

创建领域

创建领域也就创建了一个存储长期密钥对象所需的目录、文件和其它资源。要创建领域，管理员必须使用 `create realm` 命令并提供要创建的领域的名称。无论当前持有的证书，系统管理员必须进行验证以使此命令成功完成。提示密码时，请输入 UNIX 系统管理员密码。例如：

```
secadm> create realm=engineering
System Administrator Login Required
Login: root
Password:
Realm engineering successfully created.
```

您可以对领域命名，以便于使用。例如，最好为不同的部门（如金融和工程部门）设置领域。在这种情况下，常常将领域命名为 `finance` 和 `engineering`。例如：

```
secadm> create realm=finance
System Administrator Login Required
Login: root
Password:
Realm finance successfully created
```

设置当前工作领域

secadm 一次只能管理一个领域中的密钥和用户帐户。大多数有关领域和用户帐户的命令要求您先选择一个领域。要选择领域，请输入 set realm 命令，如下例所示：

```
secadm> set realm=finance
secadm{finance}>
```

选择领域后， secadm 提示行在大括号中显示领域名。

如果不想再使用当前所在的领域，您可以将当前的工作领域设置为新值或清除领域。更改或清除当前工作领域还将自动注销该领域中当前验证的任何用户和系统管理员。例如：

```
secadm{finance}> set realm=engineering
secadm{engineering}> unset realm
secadm>
```

用用户填充领域

这些用户名仅在 Sun Crypto 加速器 1000 的域中被识别，而且不必与 Web 服务器进程实际运行的 UNIX 用户名相同。尝试创建用户之前，请记住必须先选择正确的领域并以系统管理员身份登录。例如：

```
secadm> set realm=engineering
secadm{engineering}> su
System Administrator Login Required
Login: root
Password:
secadm{root@engineering}#
```

如果仅需要一个领域用户，您可以通过使用领域名 “nobody” 来避免设置插槽文件。下例在 “engineering” 领域中创建了用户 “nobody” 并为 “nobody@engineering” 设置了密码 （在表 3-1 中定义为 *user@realm-name*）。

```
secadm{root@engineering}# create user=nobody
Initial password:
Confirm password:
User nobody successfully created.
```

在 Web 服务器启动期间进行验证时，必须使用此密码。

警告 – 必须记住输入的密码。没有密码，就无法访问您的密钥。丢失的密码无法重新找到。

列出领域

您可以通过输入 `show realm=`*realm-name* 命令来列出有关领域的信息。

```
secadm> show realm
Realm Name
---------------------------------------------------
engineering
finance
---------------------------------------------------
```

列出领域类

领域类是控制领域如何管理密钥对象、用户帐户和验证数据的密钥管理模块。Sun Crypto 加速器 1000 当前支持的唯一领域类是 `SUNW_filesys` 领域类。要列出支持的所有领域类，请使用 `show class` 命令。

```
secadm> show class
Realm Class
---------------------------------------------------
SUNW_filesys
---------------------------------------------------
```

删除领域

可以通过输入 `delete realm` 命令并提供要删除的领域名来删除领域。发出命令时，`secadm` 提示您是/否确实要删除领域。与创建领域时一样，系统管理员必须在执行此命令之前进行验证。另外，您无法删除正在使用的领域。要取消领域引用，您必须关掉 Web 服务器和/或管理服务器。

设置并管理用户帐户

用户帐户提供应用程序对 Sun Crypto 加速器 1000 进行验证的方法，还提供了在领域中区分密钥的一种方式。一个用户帐户拥有的密钥无法被未进行验证的应用程序访问，也无法被以另一用户身份向同一领域进行验证的应用程序访问。对于所有这些命令，必须选择一个领域，而且系统管理员必须使用 `secadm su` 命令登录到该领域。

创建用户

- **发出** `create user` **命令创建用户**。

  此命令要求用户名采用 `create user=`*username* 格式。

```
secadm{root@engineering}# create user=username
Initial password:
Confirm password:
User username created successfully.
```

警告 – 必须记住输入的密码。没有密码，就无法访问您的密钥。丢失的密码无法重新找到。

列出用户

只有系统管理员可以列出领域中的用户。系统管理员必须发出 `show user` 命令。此命令仅列出当前选择的领域中的用户。

- **发出** `show user` **命令**。

```
secadm{root@engineering}# show user
User                                    Status
-------------------------------------------------------
webserv                                 enabled
alice                                   enabled
bob                                     enabled
-------------------------------------------------------
```

更改用户密码

只有使用 secadm login 命令登录的单个用户可以更改该用户的密码。必须先知道当前密码，然后才能设置新密码。

- **发出** passwd **命令**。

```
secadm{username@realm-name}> passwd
Enter current password:
Enter Password:
Confirm Password:
Password successfully changed for user username.
```

警告 – 必须记住输入的密码。没有密码，就无法访问您的密钥。丢失的密码无法重新找到。

启用或禁用用户

只有系统管理员可以启用或禁用用户。默认情况下，每个用户都是在已启用状态下创建的。

- **要禁用用户帐户，请输入** disable user=*username* **命令**。

```
secadm{root@engineering}# disable user=username
User is now disabled.
```

对已禁用的用户帐户进行验证的所有尝试都将失败。但是，所有密钥都不会以任何方式改变。重新启用该帐户后，该用户拥有的所有密钥可再次被已验证的应用程序访问。

- **要启用帐户，请输入** enable user=*username* **命令**。

```
secadm{root@engineering}# enable user=username
User is now enabled.
```

删除用户

- **通过指定要删除的用户发出** `delete user` **命令。**

  系统管理员必须提供要删除的用户帐户名。

  与用户相关的密钥在发出命令时被删除。 `secadm` 提示系统管理员在删除用户之前进行是/否确认。

```
secadm{root@engineering}# delete user=username
Delete user webserv? [Y/N]: y
User username deleted successfully.
```

附录 **B**

Manual 页

本附录介绍 Sun Crypto 加速器 1000 软件随附的 man 页的说明。

可以使用以下命令查看手册页：

```
man -M /opt/SUNWconn/man page
```

表 B-1 列出并介绍了可用的 man 页。

表 B-1 Sun Crypto 加速器 1000 man 页

man 页	说明
cryptio(7d)	cryptio 设备驱动程序用于提供基本的硬件加密加速器的访问控制。cryptio 驱动程序要求必须具备应用程序和核心客户程序的分层软件，才能访问所提供的服务。
dca(7d)	dca 设备驱动程序是一个 Sun 加密提供商叶节点驱动程序，用于提供基本的硬件加密加速器的访问控制。 dca 驱动程序要求必须具备应用程序和核心客户程序的分层软件，才能访问所提供的服务。
kcl(7d)	kcl 设备驱动程序是一个多线程的可加载核心模块，为 Sun 加密提供商驱动程序提供支持。 kcl 驱动程序要求必须具备应用程序和核心客户程序的分层软件，才能访问所提供的服务。
kcpi(7d)	kcpi 设备驱动程序是一个多线程的可加载核心模块，为 Sun 加密提供商驱动程序提供支持。 kcpi 驱动程序要求必须具备应用程序和核心客户程序的分层软件，才能访问所提供的服务。

表 B-1 Sun Crypto 加速器 1000 man 页

man 页	说明
secadm(1m)	secadm 是 Sun Crypto 加速器的管理实用程序。 secadm 命令用于手动控制与 Sun Crypto 加速器有关的配置、帐户和键控数据库。 secadm 用于处理敏感的加密密钥信息。
secd(1m)	secd 守护程序用于提供 secadm 应用程序的管理访问服务。
sslconfig(1m)	sslconfig 是 Sun Crypto 加速器 1000 的配置实用程序。

附录 C

Apache Web 服务器的 SSL 配置指令

本附录列出了使用 Sun Crypto 加速器 1000 软件配置 Apache Web 服务器的 SSL 支持的指令。应在 `http.conf` 文件中配置指令。有关详细信息，请参阅 Apache 文档。

1. `SSLPassPhraseDialog exec:`*program*

   环境：全局

   本指令向 Apache Web 服务器通知应该执行指定 *program*，以收集密钥文件的密码。*program* 应该将收集到的密码输出到标准输出设备上。

   如果有多个密钥文件使用共同的密码，则 *program* 只执行一次 （要先尝试收集到的每个密码，然后再重新运行 *program*。）

   program 执行时使用两个参数：第一个参数是服务器名称，采用 *servername*:*port* 格式（如 `www.fictional-company.com:443`）。（端口 443 是基于 SSL 的 Web 服务器的典型端口。）第二个参数是密钥文件中的密钥类型 (*keytype*)。 *keytype* 可以是 RSA 或 DSA。

注意 – 因为可以在系统启动时执行本程序，所以务必对其进行设计，以应付控制台不是 `tty` 设备的情况 （即 `tty`(3c) 将返回 false）。

   所提供的程序 `/opt/SUNWconn/crypto/bin/sslpassword` 可用于 *program* 的可执行文件。本程序自动提示要求输入密码，而且在输入密码时不显示密码。

同时，所提供的 sslpassword 程序会自动搜索文件中的密码，可以在 Web 服务器启动时避免用户交互。密钥文件中的密码会在 /etc/apache/*servername*:*port*.*keytype*.pass 文件中搜索。如果本文件不存在，则使用 /etc/apache/default.pass 文件。这些密码文件的内容仅仅是未加密的密码，自成一行。

注意 – 密码文件应该通过权限进行保护，只有 Web 服务器以其身份运行的 UNIX 用户可以读取本文件。该用户应该是使用标准的 Apache User 指令配置的同一用户。

如果未指定，则默认操作是使用内部提示机制。建议 Sun 客户不使用默认操作，而使用所提供的 sslpassword 程序，以避免系统启动时的交互问题。

2. SSLEngine (on|off)

   环境：全局、虚拟主机

   本指令用于启用 SSL 协议。它通常在虚拟主机中使用，以便对一小部分服务器启用 SSL。常用的一种格式是：

```
<VirtualHost _default_:443>
SSLEngine on
</VirtualHost>
```

它为监听端口 443 （标准的 HTTPS 端口）的任何服务器配置 SSL 的使用。如果不存在，则在默认情况下将禁用。

3. SSLProtocol [+-]*protocol*

   环境：全局、虚拟主机

   本指令用于配置在进行 SSL 事务处理时服务器应使用的协议。

   可用的协议在表 C-1 中列出并予以说明：

表 C-1 SSL 协议

协议	说明
SSLv2	Netscape 的最初事实标准 SSL 协议
SSLv3	SSL 协议的更新版本，是大多数流行的 Web 浏览器支持的协议
TLSv1	当前正在由 IETF 规范化的 SSLv3 的更新版本，在本文编写时支持它的浏览器很少
全部	启用所有协议

可以使用加号 (+) 或减号 (-) 添加或删除协议。例如，要禁用对 SSLv2 的支持，可以使用指令：

```
SSLProtocol all -SSLv2
```

它也与以下指令具有同等效果：

```
SSLProtocol +SSLv3 +TLSv1
```

4. `SSLCipherSuite` *cipher-spec*

   环境：全局、虚拟主机、目录、 `.htaccess`

   SSLCipherSuite 指令用于配置可以使用哪些 SSL 密码及其首选项。在全局环境或虚拟主机环境中，它在初次 SSL 握手时使用。在目录环境中，它强行让 SSL 重新协商使用指定密码。重新协商在读取请求后发送响应前发生。

   cipher-spec 是表 C-2 中的一个用冒号分隔的密码列表。

表 C-2 可用的 SSL 密码

密码标记	协议	密钥交换	鉴定	加密	MAC	类型
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES （168 位）	SHA1	
DES-CBC3-MD5	SSLv2	RSA	RSA	3DES （168 位）	MD5	
RC4-SHA	SSLv3	RSA	RSA	ARCFOUR （128 位）	SHA1	
RC4-MD5	SSLv3	RSA	RSA	ARCFOUR （128 位）	MD5	
RC4-MD5	SSLv2	RSA	RSA	ARCFOUR （128 位）	MD5	
RC2-CBC-MD5	SSLv2	RSA	RSA	ARCTWO （128 位）		
DES-CBC-SHA	SSLv3	RSA	RSA	DES （56 位）	SHA1	
RC4-64-MD5	SSLv2	RSA	RSA	ARCFOUR （64 位）	MD5	
DES-CBC-MD5	SSLv2	RSA	RSA	DES （56 位）	MD5	
EXP-DES-CBC-SHA	SSLv3	RSA （512 位）	RSA	DES （40 位）	SHA1	导出
EXP-RC2-CBC-MD5	SSLv2	RSA （512 位）	RSA	ARCTWO （40 位）	SHA1	导出

表 C-2 可用的 SSL 密码

密码标记	协议	密钥交换	鉴定	加密	MAC	类型
EXP-RC2-CBC-MD5	SSLv3	RSA（512 位）	RSA	ARCTWO （40 位）	SHA1	导出
EXP-RC4-MD5	SSLv3	RSA（512 位）	RSA	ARCFOUR（40 位）	MD5	导出
EXP-RC4-MD5	SSLv2	RSA（512 位）	RSA	ARCFOUR（40 位）	MD5	导出
NULL-SHA	SSLv3	RSA	RSA	无	SHA1	
NULL-MD5	SSLv3	RSA	RSA	无	MD5	
ADH-DES-CBC3-SHA	SSLv3	DH	无	3DES （168 位）	SHA1	
ADH-DES-CBC-SHA	SSLv3	DH	无	DES （56 位）	SHA1	
ADH-RC4-MD5	SSLv3	DH	无	ARCFOUR（128 位）	MD5	
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES （168 位）	SHA1	
EDH-DSS-DES-CBC3-SHA	SSLv3	DH	DSS	3DES （168 位）	SHA1	
EDH-RSA-DES-CBC-SHA	SSLv3	DH	RSA	DES （56 位）	SHA1	
EDH-DSS-DES-CBC-SHA	SSLv3	DH	DSS	DES （56 位）	SHA1	
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH（512 位）	RSA	DES （40 位）	SHA1	导出
EXP-EDH-DSS-DES-CBC-SHA	SSLv3	DH（512 位）	DSS	DES （40 位）	SHA1	导出
EXP-ADH-DES-CBC-SHA	SSLv3	DH（512 位）	无	DES （40 位）	SHA1	导出
EXP-ADH-RC4-MD5	SSLv3	DH（512 位）	无	ARCFOUR（40 位）	MD5	导出

在表 C-2 中， DH 指 Diffie-Hellman， DSS 指数字签名标准。

表 C-3 列出并说明了提供类似宏分组的别名。

表 C-3 SSL 别名

别名	说明
SSLv2	所有 SSL 版本 2.0 密码
SSLv3	所有 SSL 版本 3.0 密码
EXP	所有导出级别密码
EXPORT40	所有 40 位导出密码

表 C-3 SSL 别名

别名	说明
EXPORT56	所有 56 位导出密码
LOW	较低长度的密码 （DES， 40 位 RC4）
MEDIUM	所有 128 位密码
HIGH	所有使用 Triple DES 的密码
RSA	所有使用 RSA 密钥交换的密码
DH	所有使用 Diffie-Hellman 密钥交换的密码
EDH	所有使用 Ephemeral Diffie-Hellman 密钥交换的密码
ADH	所有使用匿名 Diffie-Hellman 密钥交换的密码
DSS	所有使用 DSS 鉴定的密码
NULL	所有不使用加密功能的密码

可以使用表 C-4 中列出并说明的特殊字符配置密码的首选项。

表 C-4 配置密码首选项的特殊字符

字符	说明
<none>	将密码添加到列表中
!	从列表中完全删除密码 — 密码可以再次添加
+	将密码添加到列表中并拖至当前位置 （可能要将其降级）
-	从列表中删除密码 （可以稍后在列表中添加）

cipher-spec 的默认值是

```
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
```

此默认值配置除匿名 （未验证）的 Diffie-Hellman 外的所有密码，将 ARCFOUR 和 RSA 置为首选项，然后设置更高的密级 （相对于较低的密级而言）。

5. `SSLCertificateFile` *file*

   环境：全局、虚拟主机

   本指令用于为此服务器指定 PEM 编码的 X.509 证书文件的位置。

6. `SSLCertificateKeyFile` *file*

   环境：全局、虚拟主机

   本指令用于为此服务器指定 PEM 编码的私人密钥文件的位置。它对应于用 `SSLCertificateFile` 指令配置的证书。

7. `SSLCertificateChainFile` *file*

   环境：全局、虚拟主机

   本指令用于指定包含构成服务器鉴定路径的 PEM 编码证书的文件的位置。可以使用它来协助客户机在服务器证书未由客户机认可的某权威机构直接签名时验证服务器证书。

   使用客户机验证 (`SSLVerifyClient`) 时，同时假定此链中的证书对于客户机验证有效。

8. `SSLCACertificateFile` *file*

   环境：全局、虚拟主机

   本指令用于指定包含鉴定权威机构 (CA) 证书并置、客户机验证时使用的文件的位置。

9. `SSLCARevocationFile` *file*

   环境：全局、虚拟主机

   本指令用于指定包含 CA 证书调用列表并置、客户机验证时使用的文件的位置。

10. `SSLVerifyClient` *level*

    环境：全局、虚拟主机、目录、 `.htaccess`

    本指令在服务器上配置了客户机验证。（注意：正常情况下，它不是电子商务应用程序所需的，但在其它应用程序中使用。）

    level 的值在表 C-5 中列出并说明。

表 C-5 SSL 验证客户机级别

级别	说明
`none`	不要求客户机验证
`optional`	客户机可能使用有效的证书
`require`	客户机*必须*使用有效的证书
`optional_no_ca`	客户机可能使用证书，但无需有效

一般情况下会使用 `none` 或 `require`。默认值是 `none`。

11. `SSLVerifyDepth` *depth*

    环境：全局、虚拟主机、目录、 `.htaccess`

    本指令指定服务器允许的客户机证书的最大证书链深度。如果值为 0，则说明仅自签名的证书为合格证书，而如果值为 1，则说明客户机证书必须由服务器直接识别的 CA 签名 （通过 `SSLCACertificateFile`）。值较大时允许 CA 授权。

12. `SSLLog` *filename*

环境：全局、虚拟主机

本指令用于指定记录 SSL 特定信息的日志文件。如果不指定 （默认值），则不记录 SSL 特定信息。

13. `SSLLogLevel` *level*

环境：全局、虚拟主机

本指令用于指定 SSL 日志文件中所记录的信息的详细程度。 *level* 的值在表 C-6 中列出并说明。

表 C-6 SSL 日志级别值

值	说明
`none`	不进行日志记录，但仍将错误消息发送到标准的 Apache 错误日志中
`warn`	包括警告消息
`info`	包括信息消息
`trace`	包括跟踪消息
`debug`	包括调试消息

14. `SSLOptions` [`+-`] *option*

环境：全局、虚拟主机、目录、 `.htaccess`

本指令用于配置 SSL 特定选项。可以在前面加上加号 (+) 前缀将选项添加到当前配置中，或者使用减号 (-) 删除当前配置中的选项。如果没有加号或减号，则使用一组最接近的选项。

选项在表 C-7 中列出并说明。

表 C-7 可用的 SSL 选项

选项	说明
`StdEnvVars`	创建一组标准的与 SSL 相关的 CGI/SSI 环境变量 — 它会在性能上有所下降。
`ExportCertData`	导出 `SSL_SERVER_CERT`、`SSL_CLIENT_CERT` 和 `SSL_CLIENT_CERT_CHAIN`*n* (*n* = 0, 1, ...) 环境变量。这些变量包含 PEM 编码的客户机和服务器证书。
`FakeBasicAuth`	客户机证书的判别名 (DN) 被转换为一个 HTTP 基本验证用户名，“被伪装”以进行验证。它允许在 SSL 客户机验证时使用标准的 Apache 访问控制机制，而不提示用户提供密码。 Apache 密码文件中的这些用户的条目必须使用加密密码 `xxj31ZMTZzkVA`。它只是 “密码”一词的加密形式 (`crypt`(3c))。
`StrictRequire`	由于拒绝 `SSLRequireSSL` 强制进行非法访问，即使 `Satisfy Any` 等其它指令存在，会覆盖本指令，也会如此。

15. `SSLRequireSSL`

环境：directory, `.htaccess`

除非使用 HTTPS，否则本指令禁止给定目录的访问。可以使用它来防止错误配置，避免使目录内容受到未验证和未加密的访问。

附录 **D**

构建同 Sun Crypto 加速器 1000 板使用的应用程序

本附录讨论 Sun Crypto 加速器 1000 随附的、可用来构建某些 OpenSSL 兼容应用程序、以利用 Sun Crypto 加速器的加密加速功能的软件。

注意 – 本附录提供的有关构建应用程序以使用 Sun Crypto 加速器 1000 软硬件的信息完全按原样提供，不是本产品正式发布的可支持功能。提供本信息的宗旨仅仅是希望对大家有所裨益，我们对此不提供任何担保。如果您需要 Sun 支持的解决方案，请与 Sun 专业服务部门联系，了解适合于您的方案选项。

您必须先安装包含所需头文件和程序库的 `SUNWcrysl` 软件包。

必须对您的应用程序进行配置，以采用 `/opt/SUNWconn/crypto/include` 中的头文件，如编译程序标志中包含的头文件：

```
-I /opt/SUNWconn/crypto/include
```

另外，必须对链接程序进行控制，以包含对相应程序库的引用。大多数 OpenSSL 兼容应用程序引用 `libcrypto.a` 或 `libssl.a` 程序库，或者两个程序库都引用。同时，还必须包含 Sun 加密程序库。为此可以使用下面的链接程序标志：

```
-L/opt/SUNWconn/crypto/lib -R/opt/SUNWconn/crypto/lib \
-lcrypto -lssl -lcryptography -lnvpair
```

注意：这种编译方式（相对于使用可从 `www.openssl.org` 下载的 OpenSSL 程序库构建而言）并非对所有 OpenSSL 应用程序都有益。

附录 **E**

规格 Sun Crypto 加速器 1000 板

本章概述了 Sun Crypto 加速器 1000 板的不同规格。

本附录包括以下各节：

- 第 81 页 “物理尺寸”
- 第 82 页 “接口规格”
- 第 82 页 “电源要求”
- 第 83 页 “环境规范”

物理尺寸

表 E-1 物理尺寸

尺寸	测量	测量 （公制）
长度	6.875 英寸	174.625 毫米
宽度	4.2 英寸	106.680 毫米

接口规格

表 E-2 接口规格

特性	规格
PCI 时钟	33 MHz 或 66 MHz
主机接口	支持 33 MHz 或 66 MHz 时钟速率和 3.3V 或 5V 功率的 PCI 2.1。
PCI 总线宽度	32 位或 64 位

电源要求

表 E-3 电源要求

规格	测量
最大功耗	10W @ 5V 700mW @ 3.3V
电压容差	5V +/- 5% 3.3V +/- 5%
工作电流	2A @ 1.8V 150mA @ 3.3V

环境规范

表 E-4 环境规范

条件	工作规范	存储规范
温度	0° 至 70°C， 32° 至 160°F	-65° 至 +150°C， -85° 至 300°F
相对湿度	5% 至 85% （非冷凝）	0 至 95% （非冷凝）

附录 F

Third-Party Licenses （第三方许可）

Some portions of Software are provided with notices and/or licenses from other parties which govern the use of those portions.

OPENSSL LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2001 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

``Ian Fleming was a UNIX fan!
How do I know? Well, James Bond
had the (license to kill) number 007,
i.e. he could execute anyone."
-- Unknown

MOD_SSL LICENSE

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

索引

字母

Apache SSL 指令， 71
dcatest， 48
  参数选项， 49
  命令行语法， 50
  子测试， 49
RSA 键对， 40
secadm， 56
SunVTS， 47
URL
  iPlanet 软件， 19, 29
  openssl， 79

C

插槽文件， 54

D

动态重配置， 3

F

服务器证书， 22, 33
负载共享， 3

G

高可用性， 3
管理 iPlanet Web 服务器， 53

J

键长度， 41

L

领域， 53
  创建， 62
  列出， 64
  删除， 64
  设置， 63

M

密码
  iPlanet Web 服务器要求的列表， 15
目录
  层次结构， 11

Q

启用
  Apache Web 服务器， 39
  iPlanet Web 服务器， 15

R

热插拔， 3
软件包， 10

S

算法， 3

T

统计值， 52

W

文件和目录， 10

X

修补程序
  推荐， 5
  要求， 5

Y

要求
  软件， 4
  硬件， 4
用户， 53
  创建， 65
  列出， 65
  启用或禁用， 66
  删除， 67
用户密码
  更改， 66

Z

诊断测试， 47