Sun™ Crypto 加速器 4000 板安装和用户指南

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

部件号 817-2339-10
2003 年 5 月，修订版 A

请将有关本文档的意见发送至：docfeedback@sun.com

请回收

Declaration of Conformity (Fiber MMF)

Compliance Model Number: Venus-FI
Product Family Name: Sun Crypto Accelerator 4000 - Fiber (X4012A)

EMC

USA - FCC Class B

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

1) This equipment may not cause harmful interference.

2) This equipment must accept any interference that may cause undesired operation.

European Union

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

As Telecommunication Network Equipment (TNE) in both Telecom Centers and Other Than Telecom Centers per (as applicable):

EN300-386 V.1.3.1 (09-2001) Required Limits:

EN55022/CISPR22	Class B
EN61000-3-2	Pass
EN61000-3-3	Pass
EN61000-4-2	6 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m 80-1000MHz, 10 V/m 800-960 MHz and 1400-2000 MHz
EN61000-4-4	1 kV AC and DC Power Lines, 0.5 kV Signal Lines,
EN61000-4-5	2 kV AC Line-Gnd, 1 kV AC Line-Line and Outdoor Signal Lines, 0.5 kV Indoor Signal Lines > 10m.
EN61000-4-6	3 V
EN61000-4-11	Pass

As information Technology Equipment (ITE) Class B per (as applicable):

EN55022:1998/CISPR22:1997 Class B

EN55024:1998 Required Limits:

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 60950:2000, 3rd Edition
Evaluated to all CB Countries
UL 60950, 3rd Edition, CSA C22.2 No. 60950-00

Supplementary Information

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

/S/

Dennis P. Symanski
Manager, Compliance Engineering
Sun Microsystems, Inc.
4150 Network Circle, MPK15-102
Santa Clara, CA 95054, USA
Tel: 650-786-3255
Fax: 650-786-3723

/S/

Pamela J Dullaghan
Quality Program Manager
Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom
Tel: +44 1 506 672 395
Fax: +44 1 506 672 855

Declaration of Conformity (Copper UTP)

Compliance Model Number:	Venus-CU
Product Family Name:	Sun Crypto Accelerator 4000 - Copper (X4011A)

EMC

USA - FCC Class B

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

1) This equipment may not cause harmful interference.

2) This equipment must accept any interference that may cause undesired operation.

European Union

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

As Telecommunication Network Equipment (TNE) in both Telecom Centers and Other Than Telecom Centers per (as applicable):

EN300-386 V.1.3.1 (09-2001) Required Limits:

EN55022/CISPR22	Class B
EN61000-3-2	Pass
EN61000-3-3	Pass

EN61000-4-2	6 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m 80-1000MHz, 10 V/m 800-960 MHz and 1400-2000 MHz
EN61000-4-4	1 kV AC and DC Power Lines, 0.5 kV Signal Lines,
EN61000-4-5	2 kV AC Line-Gnd, 1 kV AC Line-Line and Outdoor Signal Lines, 0.5 kV Indoor Signal Lines > 10m.
EN61000-4-6	3 V
EN61000-4-11	Pass

As information Technology Equipment (ITE) Class B per (as applicable):

EN55022:1998/CISPR22:1997	Class B
EN55024:1998 Required Limits:	
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 60950:2000, 3rd Edition

Evaluated to all CB Countries

UL 60950, 3rd Edition, CSA C22.2 No. 60950-00

Supplementary Information

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

/S/

Dennis P. Symanski
Manager, Compliance Engineering
Sun Microsystems, Inc.
4150 Network Circle, MPK15-102
Santa Clara, CA 95054, USA
Tel: 650-786-3255
Fax: 650-786-3723

/S/

Pamela J Dullaghan
Quality Program Manager
Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom
Tel: +44 1 506 672 395
Fax: +44 1 506 672 855

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.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

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

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

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

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

表

序言

本 《*Sun Crypto 加速器 4000 板安装和用户指南*》介绍 Sun™ Crypto 加速器 4000 板的功能、协议和接口，并说明如何在系统中安装、配置和管理 Sun Crypto 加速器 4000 板。

本书假定您是一位对下列一项或多项具有丰富配置经验的网络管理员：Solaris™ 操作环境、配设 PCI I/O 卡的 Sun 平台、 Sun™ ONE 和 Apache Web 服务器、 IPsec、SunVTS™ 软件以及获取认证中心授权。

本书的内容编排

本书包括以下内容：

- 第 1 章介绍 Sun Crypto 加速器 4000 板的产品功能、协议和接口，并说明了板的硬件和软件要求。
- 第 2 章说明如何安装和删除 Sun Crypto 加速器 4000 的硬件及软件。
- 第 3 章定义 Sun Crypto 加速器 4000 的可调驱动程序参数，并说明如何使用 `ndd` 实用程序和 `vca.conf` 文件配置这些参数。另外，本章还说明了如何通过 OpenBoot™ PROM 界面为链接参数启用自动协商模式或强制模式，以及如何配置网络 `hosts` 文件。
- 第 4 章介绍如何配置 Sun Crypto 加速器 4000 板以及使用 `vcaadm` 和 `vcadiag` 实用程序管理密钥库。
- 第 5 章说明如何配置 Sun Crypto 加速器 4000 板以便与 Sun ONE Web 服务器配合使用。
- 第 6 章介绍如何配置 Sun Crypto 加速器 4000 板以便与 Apache Web 服务器配合使用。
- 第 7 章说明如何使用 SunVTS 诊断应用程序和板载 FCode 自测程序来测试 Sun Crypto 加速器 4000 板。另外，本章还提供了使用 OpenBoot 命令进行排除故障的技巧。

- 附录 A 列出了 Sun Crypto 加速器 4000 板的规格。
- 附录 B 列出了使用 Sun Crypto 加速器 4000 软件为 Apache Web 服务器配置 SSL 支持的指令。
- 附录 C 介绍 Sun Crypto 加速器 4000 板随附的软件，并说明了如何构建 OpenSSL 兼容应用程序以便充分利用板的加密加速功能。
- 附录 D 提供了一些来自其它软件组织的软件声明和许可，用于管理与 Sun Crypto 加速器 4000 板一起使用的第三方软件。
- 附录 E 说明 Sun Crypto 加速器 4000 的命令并列出了每个命令的联机资料。
- 附录 F 介绍如何恢复 Sun Crypto 加速器 4000 板的出厂状态，即板的 `failsafe` 模式。
- 附录 G 提供了一些常见问题的解答。

使用 UNIX 命令

本文档没有介绍基本 UNIX® 命令和操作过程的有关信息，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，请参阅下列文档：

- *Solaris 硬件平台指南*
- `http://docs.sun.com` 网站上面向 Solaris 操作环境的联机文档
- 系统随附的其它软件文档

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；需用真名或实际值替换	若要删除文件，请键入 rm *文件名*。

Shell 提示

Shell	提示
C shell	*计算机名* %
C shell 超级用户	*计算机名* #
Bourne shell 和 Korn shell	$
Bourne shell 和 Korn shell 超级用户	#

在线访问 Sun 文档

用户可从以下网站查看、打印或订购 Sun 提供的各类文档，包括本地化版本：

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

Sun 欢迎您提出意见

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内注明本文档的部件号 (817-2339-10)。

第 1 章

产品概述

本章简要介绍 Sun Crypto 加速器 4000 板的有关信息，包括以下几节：

产品功能

Sun Crypto 加速器 4000 板是一种基于千兆位以太网的网络接口卡，可为 Sun 服务器上运行的 IPsec 和 SSL （对称和非对称均可）提供加密硬件加速功能。除作为标准千兆位以太网接口卡进行非加密型网络通信之外，该板附带的加密硬件还可以为加密型 IPsec 通信提供高于标准软件方案的吞吐量。

主要协议和接口

Sun Crypto 加速器 4000 板可与现有的以太网设备相互配合操作，前提是这些设备采用标准以太网最小和最大帧大小 （64 至 1518 字节）和帧格式，且与以下标准和协议兼容：

- Full-size PCI 33/66 Mhz， 32/64 位
- IEEE 802.3 CSMA/CD （以太网）
- IEEE 802.2 逻辑链路控制
- SNMP (limited MIB)
- 全双工和半双工千兆位以太网接口 (IEEE 802.z)
- 通用双压信号 （3.3V 和 5V）

主要功能

- 带铜或光纤接口的千兆位以太网
- 加速 IPsec 和 SSL 加密功能
- 会话建立速率：高达 4300 次/秒
- 批量加密速率：高达 800 Mbps
- 提供多达 2048 位的 RSA 加密方法
- 提供快达 10 倍的 3DES 批量数据加密
- 可为 Sun ONE Web 服务器提供能防篡改的集中化安全密钥和证书管理策略，从而实现更高的安全性能和简化的密钥管理
- 符合 FIPS 140-2 Level 3 认证
- 较低的 CPU 利用率 — 释放服务器系统资源和带宽
- 安全可靠的私钥存储和管理
- 在中型和高端服务器上支持动态重配置 (DR) 和冗余/故障接管
- 在多个 CPU 之间实现 RX 数据包负载均衡
- 支持全流量控制 (IEEE 802.3x)

Sun Crypto 加速器 4000 板符合 Federal Information Processing Standard (FIPS) 140-2，Level 3 中有关加密模块的安全性能要求。

支持的应用程序

- Solaris 8 和 9 操作环境 (IPsec VPN)
- Sun ONE Web 服务器
- Apache Web 服务器

支持的加密协议

Sun Crypto 加速器 4000 板支持以下协议：

- IPsec for IPv4 和 IPsec for IPv6，包括 IKE
- SSLv2、SSLv3 和 TLSv1

Sun Crypto 加速器 4000 板可以加速以下 IPsec 功能：

- ESP（DES 和 3DES）加密

Sun Crypto 加速器 4000 板可以增强以下 SSL 功能：

- 在客户机和服务器之间安全建立一套加密参数和密钥
- 板上配有安全可靠的密钥库 — 密钥一旦离开板便会加密

诊断支持

- 用户可通过 OpenBoot™ PROM 执行自测程序
- SunVTS™ 诊断测试程序

加密算法加速

Sun Crypto 加速器 4000 板既可加速硬件中的加密算法，也可加速软件中的加密算法。其复杂性的原因在于加速加密算法的开销对于各种算法并非完全一样。有些加密算法只能通过硬件来实现，而其它一些加密算法则只能通过软件来实现。对于硬件加速而言，数据从用户应用程序移到硬件加速设备中以及将结果移回用户应用程序中均会增加开销。注意：一些加密算法可以由精心调试的软件执行，其速度与在专用硬件中一样。

支持的加密算法

Sun Crypto 加速器 4000 驱动程序 (`vca`) 检查每一个加密请求并确定最佳的加密位置（主机处理器或 Sun Crypto 加速器 4000），从而获得最大的吞吐量。负载分布取决于加密算法、当前作业量和数据大小。

Sun Crypto 加速器 4000 板可以加速下列 IPsec 算法。

表 1-1 IPsec 加密算法

类型	算法
对称	DES， 3DES

Sun Crypto 加速器 4000 板可以加速下列 SSL 算法。

表 1-2 SSL 加密算法

类型	算法
对称	DES， 3DES， ARCFOUR
非对称	Diffie-Hellman （只适用于 Apache）和 RSA （多达 2048 位密钥），DSA
Hash	MD5， SHA1

SSL 加速

表 1-3 列出了可以向硬件分配负载的 SSL 加速算法以及为 Sun ONE 和 Apache 网络服务器提供的软件算法。

表 1-3 支持的 SSL 算法

	Sun ONE 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
ARCFOUR		X		
Diffie-Hellman			X	X
DES	X	X	X	X
3DES	X	X	X	X
MD5	X	X		
SHA1	X	X		

批量加密

默认情况下，系统已禁用了 Sun Crypto 加速器 4000 板为 Sun ONE 服务器软件提供的批量加密功能。您必须手动启用此功能，方法是：创建相关文件，然后重新启动 Sun ONE 服务器软件。

要使 Sun ONE 服务器软件可以使用 Sun Crypto 加速器 4000 板上的批量加密功能，您只需在 `/etc/opt/SUNWconn/cryptov2/` 目录中创建一个名为 `sslreg` 的空文件，然后重新启动服务器软件。

```
# touch /etc/opt/SUNWconn/cryptov2/sslreg
```

要禁用批量加密功能，您必须删除 `sslreg` 文件，然后重新启动服务器软件。

```
# rm /etc/opt/SUNWconn/cryptov2/sslreg
```

默认情况下，系统已为 Apache Web 服务器软件启用了批量加密功能，且不能禁用。

硬件概述

Sun Crypto 加速器 4000 硬件是一个全长 （4.2 英寸 × 12.283 英寸）的加密加速器 PCI 千兆位以太网适配器，用于提高 Sun 服务器上 IPsec 和 SSL 的性能。

IPsec 硬件加速

Sun Crypto 加速器 4000 板可在硬件中加密和解密 IPsec 数据包，从而降低 SPARC™ 处理器的此类高开销操作。另外，加密硬件还支持在其它应用程序中使用一般的非对称和对称加密操作，并包含一个随机编号的硬件源。

注意 – 使用 Sun Crypto 加速器 4000 板进行 IPsec 加速时，不需要配置或调整 IPsec。您只需安装 Sun Crypto 加速器 4000 软件包然后重新引导。

安装 Sun Crypto 加速器 4000 板和软件包之后，任何现有的 IPsec 配置和将来的 IPsec 配置均将使用 Sun Crypto 加速器 4000 板 （而非核心 Solaris 软件）。板将处理表 1-1 中列出的任何支持的 IPsec 算法。Sun Crypto 加速器 4000 板不支持的 IPsec 算法仍由核心 Solaris 加密软件进行处理。有关 IPsec 的配置，请参阅 `http://docs.sun.com` 网站上 Solaris System Administrator Collection （Solaris 系统管理员系列）中的 《*System Administration Guide*》。

Sun Crypto 加速器 4000 MMF 适配器

Sun Crypto 加速器 4000 MMF 适配器是一种单端口的基于光纤的千兆位以太网 PCI 总线卡。它只能在 1000 Mbps 以太网中使用。

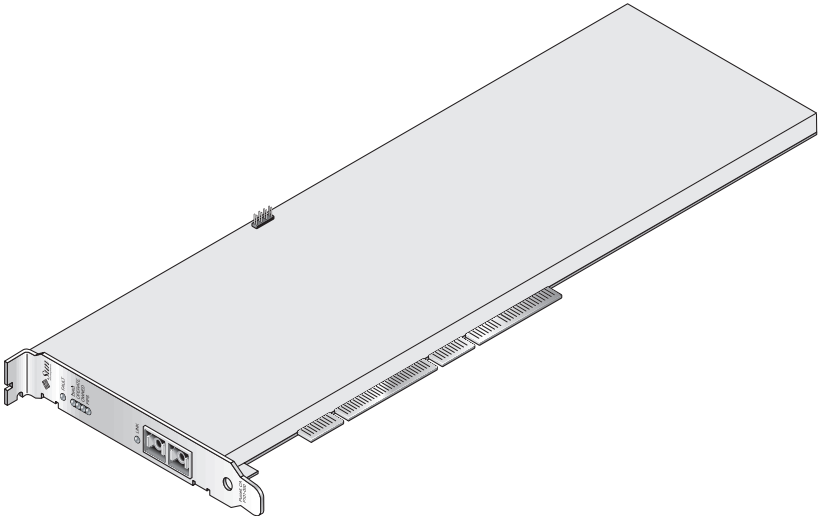

图 1-1 Sun Crypto 加速器 4000 MMF 适配器

LED 显示

参见表 1-4。

表 1-4 MMF 适配器的前面板显示 LED

标签	亮起时的含义	颜色
Fault （故障）	当板处于 HALTED （致命错误）状态或低级硬件初始化失败时亮起。 引导过程中出现错误时闪烁。	红色
Diag （诊断）	处于 POST、 DIAGNOSTICS 和 FAILSAFE （固件未升级）状态时亮起。 运行 DIAGNOSTICS 时闪烁。	绿色
Operate （操作）	处于 POST、 DIAGNOSTICS 和 DISABLED （未附带驱动程序）状态时亮起。 处于 IDLE、 OPERATIONAL 和 FAILSAFE 状态时闪烁。	绿色

表 1-4 MMF 适配器的前面板显示 LED *（续）*

标签	亮起时的含义	颜色
Owned （已拥有）	安全主管已使用 `vcaadm` 初始化板时亮起。 参阅第 56 页 “通过 `vcaadm` 初始化 Sun Crypto 加速器 4000 板”。 存在 ZEROIZE 跳线时闪烁。	绿色
FIPS Mode （FIPS 模式）	在 FIPS 140-2 level 3 认证模式下运行时亮起。在非 FIPS 模式下运行时熄灭。	绿色
Link （链接）	链连就绪。	绿色

Sun Crypto 加速器 4000UTP 适配器

Sun Crypto 加速器 4000 UTP 适配器是一种单端口的基于铜线的千兆位以太网 PCI 总线卡。经过配置，它可以在 10、 100 或 1000 Mbps 以太网中使用。

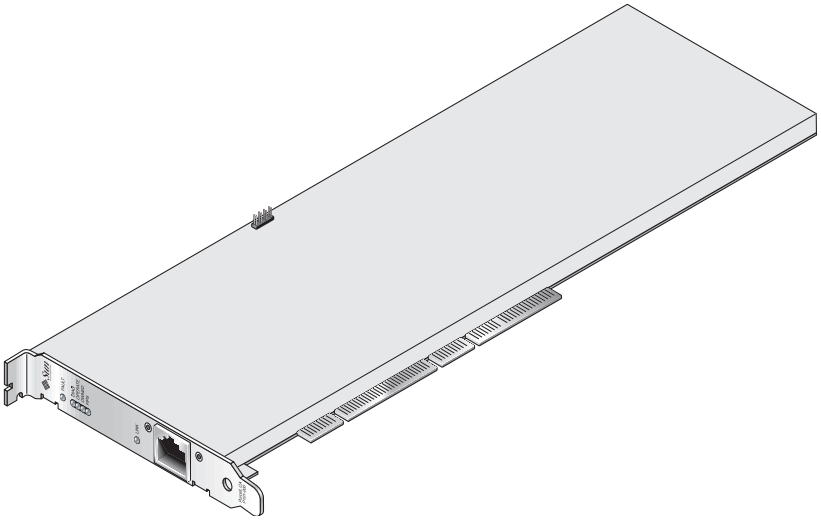

图 1-2 Sun Crypto 加速器 4000UTP 适配器

LED 显示

参见表 1-5。

表 1-5 UTP 适配器的前面板显示 LED

标签	亮起时的含义	颜色
Fault （故障）	当板处于 HALTED （致命错误）状态或低级硬件初始化失败时亮起。 引导过程中出现错误时闪烁。	红色
Diag （诊断）	处于 POST、 DIAGNOSTICS 和 FAILSAFE （固件未升级）状态时亮起。 运行 DIAGNOSTICS 时闪烁。	绿色
Operate （操作）	处于 POST、 DIAGNOSTICS 和 DISABLED （未附带驱动程序）状态时亮起。 处于 IDLE、 OPERATIONAL 和 FAILSAFE 状态时闪烁。	绿色
Owned （已拥有）	安全主管已使用 `vcaadm` 初始化板时亮起。 参阅第 56 页 “通过 `vcaadm` 初始化 Sun Crypto 加速器 4000 板”。 存在 ZEROIZE 跳线时闪烁。	绿色
FIPS Mode （FIPS 模式）	在 FIPS 140-2 level 3 认证模式下运行时亮起。在非 FIPS 模式下运行时熄灭。	绿色
1000 （无标签）	表示千兆位以太网。	绿色
活动 （无标签）	链路正在发送或接收数据。	琥珀色
链接	链连就绪。	绿色

注意 – 每次述及 iPlanet Web 服务器 4.1 或 6.0 时，均意指服务包号 （SP9 或 SP1）。

动态重配置和高可用性

Sun Crypto 加速器 4000 硬件和相关软件能够高效地在支持动态重配置 (DR) 和热插拔的 Sun 平台上工作。在 DR 或热插拔操作中， Sun Crypto 加速器 4000 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，可以在系统或域中安装多块 Sun Crypto 加速器 4000 板，以确保硬件加速功能连续可用。当 Sun Crypto 加速器 4000 硬件出现故障时 （机率很小），软件层会检测到此故障并从可用的硬件加密加速器列表中删除出现故障的板。Sun Crypto 加速器 4000 将会调整计划算法，从而适应硬件资源减少的情况。后续的加密请求将会安排给剩余的板。

注意：Sun Crypto 加速器 4000 硬件为生成长期密钥提供了高质量信息熵 (Entropy) 的来源。如果拆卸某域或系统中的所有 Sun Crypto 加速器 4000 板，则会生成信息熵质量较低的长期密钥。

负载共享

Sun Crypto 加速器 4000 软件在 Solaris 域或系统中安装的各个板上分配负载。收到的加密请求依据固定长度的作业队列分配给各个不同的板。也就是说，加密请求首先分配给第一块板，后续请求仍然分配给第一块板，直到该板满荷运行为止。一旦第一块板满荷运行，后续请求会分配给下一块可以接受此类请求的板。排队机制的作用在于疏导那些汇集在板上的请求，从而达到优化吞吐量的目的。

硬件和软件要求

表 1-6 简要列出了 Sun Crypto 加速器 4000 适配器的硬件及软件要求。

表 1-6 硬件和软件要求

硬件和软件	要求
硬件	Sun Fire™ V120, V210, V240, 280R, V480, V880, 4800, 4810, 6800, 12K, 15K; Netra™ 20 (lw4); Sun Blade™ 100, 150, 1000, 2000
操作环境	Solaris 8 2/02 和以后的兼容版本 （对于 IPsec 加速，需要使用 Solaris 9 版本。）

必需的修补程序

有关其它必需的修补程序信息，请参阅 《*Sun Crypto 加速器 4000 板版本说明*》。

要在系统上运行 Sun Crypto 加速器 4000 板，可能需要以下修补程序。Solaris 更新版本包含以前版本的修补程序。您可运行 `showrev -p` 命令来确定系统中是否已安装了所列的修补程序。

您可从以下 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列出的版本，请使用最新的版本。

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

Apache Web 服务器修补程序

如果您准备使用 Apache Web 服务器，则还必须安装修补程序 109234-09。添加 `SUNWkcl2a` 软件包后，系统将会配有 Apache Web 服务器 mod_ssl 1.3.26。

Solaris 8 修补程序

下面几张表列出了使用本产品时必需和推荐安装的 Solaris 8 修补程序。表 1-7 列出并说明了必需的修补程序。

表 1-7 Sun Crypto 加速器 4000 软件必需的 Solaris 8 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`

Solaris 9 修补程序

当前没有必需的 Solaris 9 修补程序。

第 2 章

安装 Sun Crypto 加速器 4000 板

本章介绍如何安装 Sun Crypto 加速器 4000 硬件和软件，包括以下几节：

板的处理

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，使用以下其中一种方法消除身上的静电：

- 触摸计算机的金属机箱。
- 戴上防静电腕带，并将其连接到接地的金属表面。

警示 – 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上 （如板的包装塑料袋）。

板的安装

Sun Crypto 加速器 4000 板的安装涉及两个方面，其一是将板插入系统，其二是加载软件工具。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，按照系统随附的文档关闭系统，关闭计算机，拔掉电源线并卸下计算机外壳。**
2. **找到一个未用的 PCI 插槽 （最好是 64 位 66 MHz 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. **使用十字头螺丝刀拧下 PCI 插槽盖板上的螺丝。**

   收好螺丝，以备在步骤 5 中固定支架时使用。
5. **只抓住 Sun Crypto 加速器 4000 板的边缘，将其从塑料袋中取出，插入 PCI 插槽，然后拧入螺丝以固定后支架。**
6. **装回计算机外壳，接回电源线，然后打开系统电源。**
7. **在 OpenBoot™ PROM (OBP)** `ok` **提示符下，输入** `show-devs` **命令以检查是否正确安装了板：**

```
ok show-devs
.
/chosen
/packages
/upa@8,480000/SUNW,ffb@0,0
/pci@8,600000/network@1
/pci@8,600000/SUNW,qlc@4
/pci@8,600000/SUNW,qlc@4/fp@0,0
.
```

上面的示例中，`/pci@8,600000/network@1` 表示 Sun Crypto 加速器 4000 板的设备路径。系统中的每块板均应有各自的设备路径行。

要确定是否正确列出了 Sun Crypto 加速器 4000 的设备属性，请按以下进行操作：在 ok 提示符下，浏览至所需的设备路径，然后输入 .properties 命令以显示属性列表。

```
ok cd /pci@8,600000/network@1
ok .properties
assigned-addresses       82000810 00000000 00102000 00000000 00002000
                          81000814 00000000 00000400 00000000 00000100
                          82000818 00000000 00200000 00000000 00200000
                          82000830 00000000 00400000 00000000 00100000
d-fru-len                00 00 00 00
d-fru-off                00 00 e8 00
d-fru-dev                eeprom
s-fru-len                00 00 08 00
s-fru-off                00 00 e0 00
s-fru-dev                eeprom
compatible               70 63 69 38 30 38 36 2c 62 35 35 35 2e 31 30 38
reg                      00000800 00000000 00000000 00000000 00000000
                          02000810 00000000 00000000 00000000 00002000
                          02000814 00000000 00000000 00000000 00000100
                          02000818 00000000 00000000 00000000 00200000
                          02000830 00000000 00000000 00000000 00100000
address-bits             00 00 00 30
max-frame-size           00 00 40 00
network-interface-type   ethernet
device_type              network
name                     network
local-mac-address        08 00 20 aa bb cc
version                  Sun PCI Crypto Accelerator 4000 1000Base-T FCode
12.11.13 02/10/31
phy-type                 mif
board-model              501-6039
model                    SUNW,pci-vca
fcode-rom-offset         00000000
66mhz-capable
fast-back-to-back
devsel-speed             00000001
class-code               00100000
interrupts               00000001
latency-timer            00000040
cache-line-size          00000010
max-latency              00000040
min-grant                00000040
subsystem-id             00003de8
subsystem-vendor-id      0000108e
revision-id              00000002
device-id                0000b555
vendor-id                00008086
```

安装 Sun Crypto 加速器 4000 软件

Sun Crypto 加速器 4000 CD 中附带了 Sun Crypto 加速器 4000 软件 。您需要从 SunSolve Web 站点下载修补程序。有关详细信息，请参阅第 10 页 “必需的修补程序”。

▼ 安装软件

1. **将 Sun Crypto 加速器 4000 CD 插入与系统相连的 CD-ROM 驱动器。**
   - 如果系统正在运行 Sun Enterprise Volume Manager™，则它应自动将 CD-ROM 挂装到 `/cdrom/cdrom0` 目录。
   - 如果系统未运行 Sun Enterprise Volume Manager，请按以下方法挂装 CD-ROM：

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

您可在 `/cdrom/cdrom0` 目录中找到以下文件和目录。

表 2-1 `/cdrom/cdrom0` 目录中的文件

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 4000 板安装和用户指南* *Sun Crypto 加速器 4000 板版本说明*	
`Packages`	包含以下 Sun Crypto 加速器 4000 软件包：	
	`SUNWkcl2r`	加密核心组件
	`SUNWkcl2u`	加密管理实用程序和程序库
	`SUNWkcl2a`	Apache 的 SSL 支持 *（可选）*
	`SUNWkcl2m`	加密管理手册页 *（可选）*
	`SUNWvcar`	VCA Crypto 加速器 (Root)
	`SUNWvcau`	VCA Crypto 加速器 (Usr)
	`SUNWvcaa`	VCA 管理
	`SUNWvcafw`	VCA 固件

表 2-1 /cdrom/cdrom0 目录中的文件 *（续）*

文件或目录	内容	
	SUNWvcamn	VCA Crypto 加速器手册页 *（可选）*
	SUNWvcav	VCA Crypto 加速器的 SunVTS 测试程序 *（可选）*
	SUNWkcl2o	SSL 开发工具和程序库 *（可选）*
	SUNWkcl2i.u	采用 KCLv2 Crypto 的 IPSec 加速 *（可选）*

必需的软件包必须按特定的顺序安装，并且必须在安装任何可选软件包之前安装。安装必需的软件包之后，您可以按任意顺序安装和删除可选软件包。

仅在计划将 Apache 用作 Web 服务器时，才有必要安装可选的 SUNWkcl2a 软件包。

仅在计划重新链接到另一（不支持）版本的 Apache Web 服务器时，才有必要安装可选的 SUNWkcl2o 软件包。

仅在计划执行 SunVTS 测试时，才有必要安装可选的 SUNWvcav 软件包。您必须在安装 SunVTS 4.4 或最新 5.x 版本之后才能安装 SUNWvcav 软件包。

注意 – Sun Crypto 加速器 4000 CD 中的可选 SUNWkcl2i.u 软件包只有 .u 扩展名。安装该软件包之后，其名称会更改为 SUNWkcl2i。该软件包在 CD 上的 .u 扩展名表示此软件包专用于 sun4u 体系结构。

---

2. 通过输入以下命令安装必需的软件包：

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2r SUNWkcl2u SUNWvcar SUNWvcau SUNWvcaa SUNWvcafw
```

3.（可选）若要检查是否正确安装了软件，请运行 pkginfo 命令。

```
# pkginfo SUNWkcl2r SUNWkcl2u SUNWvcar SUNWvcau SUNWvcaa SUNWvcafw
system  SUNWkcl2r   Cryptography Kernel Components
system  SUNWkcl2u   Cryptographic Administration Utility and Libraries
system  SUNWvcar    VCA Crypto Accelerator (Root)
system  SUNWvcau    Crypto Accelerator/Gigabit Ethernet (Usr)
system  SUNWvcaa    VCA Administration
system  SUNWvcafw   VCA Firmware
```

4.（可选）若要检查是否已附带了驱动程序，请运行 prtdiag 命令。参阅 prtdiag(1m) 联机手册页。

```
# prtdiag -v
```

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

```
# modinfo | grep Crypto
62   1317f62  20b1f 198   1  vca (VCA Crypto/Ethernet v1.102)
63   13360e9  12510 200   1  kcl2 (Kernel Crypto Library v1.148)
197  136d5d6   19b0 199   1  vcactl (VCA Crypto Control v1.19)
```

安装可选软件包

如果只想安装为 Apache Web 服务器以及加密管理实用程序和程序库提供 SSL 支持的可选软件包，请输入以下命令：

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2a SUNWkcl2u
```

若要安装所有的可选软件包，请输入以下命令：

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2a SUNWkcl2m SUNWvcamn SUNWvcav SUNWkcl2o SUNWkcl2i.u
```

有关上述示例中可选软件包的内容说明，请参见表 2-1。

目录和文件

表 2-2 列出了 Sun Crypto 加速器 4000 软件在采用默认方式安装时所创建的目录。

表 2-2 Sun Crypto 加速器 4000 目录

目录	内容
/etc/opt/SUNWconn/vca/keydata	密钥库数据 （已加密）
/opt/SUNWconn/cryptov2/bin	实用程序
/opt/SUNWconn/cryptov2/lib	支持程序库
/opt/SUNWconn/cryptov2/sbin	管理命令

图 2-1 显示了这些目录和文件的层次结构。

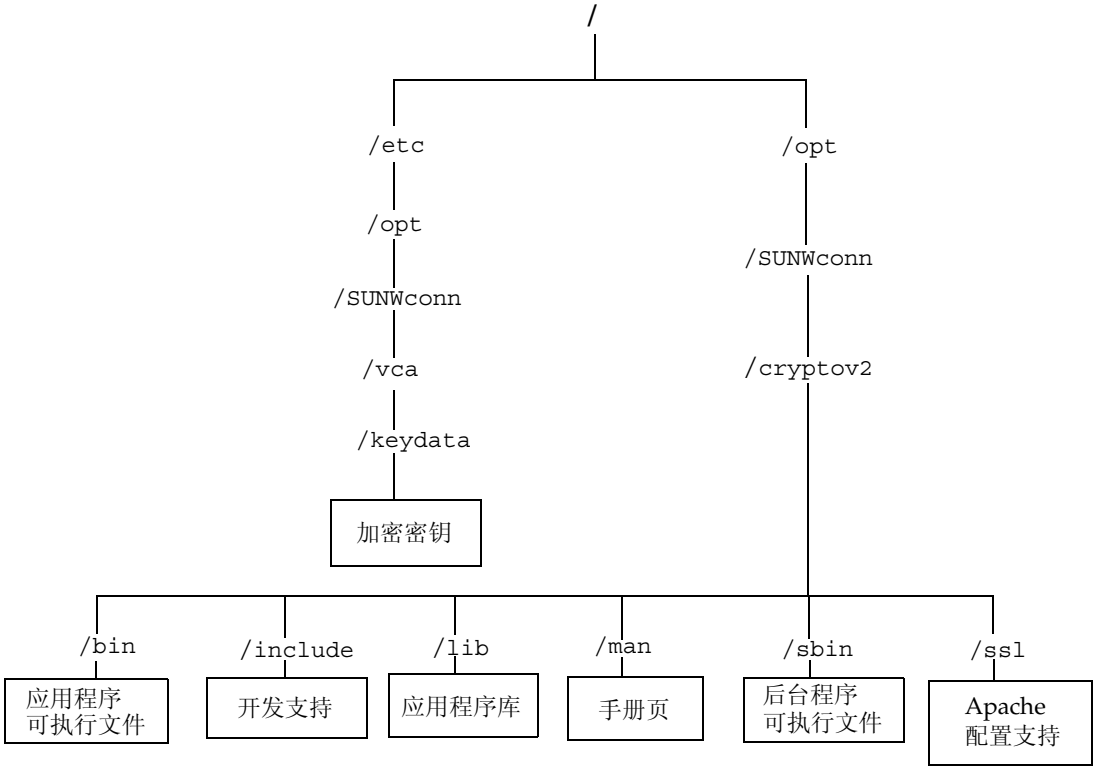

图 2-1 Sun Crypto 加速器 4000 目录和文件

注意 – 安装板的硬件和软件之后，您需使用配置和密钥库信息来初始化板。有关如何初始化板的信息，请参阅第 56 页 “通过 vcaadm 初始化 Sun Crypto 加速器 4000 板”。

删除软件

如果您已创建了密钥库 （参阅第 59 页 “通过 vcaadm 管理密钥库”），则在删除软件之前必须删除 Sun Crypto 加速器 4000 板配置的密钥库信息。 zeroize 命令可删除所有密钥资料，但不能删除密钥库文件 （该文件位于安装 Sun Crypto 加速器 4000 板的物理主机的文件系统中）。有关 zeroize 命令的详细说明，请参阅第 69 页 “零置 Sun Crypto 加速器 4000 板”。要删除保存在系统中的密钥库文件，请先成为超级用户，然后删除密钥库文件。如果尚未创建任何密钥库文件，则可以跳过该步骤。

警示 – 如果某个密钥库正在使用中，或者由其他用户和密钥库共用，则不可删除该密钥库。要释放对密钥库的引用，必须关闭 Web 服务器和/或管理服务器。

警示 – 删除 Sun Crypto 加速器 4000 软件之前，必须禁用任何与 Sun Crypto 加速器 4000 板配合使用的 Web 服务器。否则，这些 Web 服务器都将无法工作。

▼ 删除软件

- **成为超级用户，使用 pkgrm 命令只删除您所安装的软件包。**

警示 – 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时会显示相关性警告，并且会使核心模块仍处于加载状态。

如果您安装了所有软件包，则应按如下所示顺序进行删除：

```
# pkgrm SUNWkcl2o SUNWvcav SUNWvcar SUNWkcl2a SUNWkcl2u SUNWkcl2r
SUNWvcamn SUNWkcl2m SUNWkcl2i SUNWvcaa SUNWvcafw SUNWvcau
```

注意 – 安装或删除 Sun Crypto 加速器 4000 板的 SunVTS 测试程序 (SUNWvcav) 时，如果 SunVTS 正在运行，则在安装或删除之后必须重新检测系统，以更新可用的测试程序。有关详细信息，请参见您的 SunVTS 文档。

第 3 章

配置驱动程序参数

本章介绍如何配置 Sun Crypto 加速器 4000 UTP 和 MMF 以太网适配器所用的 vca 设备驱动程序参数。本章包括以下几节：

Sun Crypto 加速器 4000 以太网设备驱动程序 (vca) 参数

vca 设备驱动程序用于控制 Sun Crypto 加速器 4000 UTP 和 MMF 以太网设备的操作。vca 驱动程序与 Sun Crypto 加速器 4000 的 UNIX pci 名称属性 pci108e， 3de8（其中 108e 是厂商 ID， 3de8 是 PCI 设备 ID）相连。

您可以手动配置 vca 设备驱动程序参数，从而自定义系统中的每一个 Sun Crypto 加速器 4000 设备。本节简要介绍了板中所用的 Sun Crypto 加速器 4000 以太网设备的性能，并说明了可用的 vca 设备驱动程序参数及其配置方法。

Sun Crypto 加速器 4000 以太网 UTP 和 MMF PCI 适配器可以按第 30 页 “设置自动协商或强制模式”中列出的速率和模式进行操作。默认情况下， vca 设备以自动协商模式与链接的远端 （链接伙伴）一起操作，以使两者的 speed、 duplex 和 link-clock 参数使用共同的操作模式。只有板的操作速率为 1000 Mbps 时， link-clock 参数才适用。 vca 设备也可以配置为在这些参数的强制模式下操作。

警示 – 要建立正确链接，链接伙伴双方的每一个 `speed`、 `duplex` 和 `link-clock`（只适用于 1000 Mbps）参数必须同时在自动协商模式或强制模式下进行操作。如果链接伙伴双方的任何一个参数未在相同的模式下进行操作，将会出现网络错误。有关说明，请参阅第 35 页 “使用 OpenBoot PROM 为链接参数启用自动协商或强制模式”。

驱动程序参数值和定义

表 3-1 列出了 `vca` 设备驱动程序的参数和设置。

表 3-1 `vca` 驱动程序参数、状态和说明

参数	状态	说明
`instance`	读和写	设备例程
`adv-autoneg-cap`	读和写	操作模式参数
`adv-1000fdx-cap`	读和写	操作模式参数 （只适用于 MMF 适配器）
`adv-1000hdx-cap`	读和写	操作模式参数
`adv-100fdx-cap`	读和写	操作模式参数 （只适用于 UTP 适配器）
`adv-100hdx-cap`	读和写	操作模式参数 （只适用于 UTP 适配器）
`adv-10fdx-cap`	读和写	操作模式参数 （只适用于 UTP 适配器）
`adv-10hdx-cap`	读和写	操作模式参数 （只适用于 UTP 适配器）
`adv-asmpause-cap`	读和写	流控制参数
`adv-pause-cap`	读和写	流控制参数
`pause-on-threshold`	读和写	流控制参数
`pause-off-threshold`	读和写	流控制参数
`link-master`	读和写	1 Gbps 速率强制模式参数
`enable-ipg0`	读和写	允许在发送数据包之前使用额外的延迟
`ipg0`	读和写	发送数据包之前的额外延迟
`ipg1`	读和写	数据包收发间隔参数
`ipg2`	读和写	数据包收发间隔参数
`rx-intr-pkts`	读和写	接收中断消隐值
`rx-intr-time`	读和写	接收中断消隐值
`red-dv4to6k`	读和写	随机提前检测和数据包丢弃矢量

表 3-1 vca 驱动程序参数、状态和说明 *（续）*

参数	状态	说明
red-dv6to8k	读和写	随机提前检测和数据包丢弃矢量
red-dv8to10k	读和写	随机提前检测和数据包丢弃矢量
red-dv10to12k	读和写	随机提前检测和数据包丢弃矢量
tx-dma-weight	读和写	PCI 接口参数
rx-dma-weight	读和写	PCI 接口参数
infinit-burst	读和写	PCI 接口参数
disable-64bit	读和写	PCI 接口参数

声明的链接参数

以下参数确定由 vca 驱动程序向其链接伙伴声明的发送及接收 speed 和 duplex 链接参数。表 3-2 介绍了操作模式参数及其默认值。

注意 – 如果参数的初始设置是 0，请不要更改该参数。如果您尝试更改了初始设置为 0 的参数，它仍恢复至 0。默认情况下，这些参数根据 vca 设备的性能进行设置。

Sun Crypto 加速器 4000 UTP 适配器的声明链接参数不同于表 3-2 中所示的 Sun Crypto 加速器 4000 MMF 适配器链接参数。

表 3-2 操作模式参数

参数	说明
以下参数适用于 Sun Crypto 加速器 4000 UTP 和 MMF 适配器。	
adv-autoneg-cap	由硬件声明的本地接口性能 0 = 强制模式 1 = 自动协商模式 （默认）
以下参数只适用于 Sun Crypto 加速器 4000 MMF 适配器。	
adv-1000fdx-cap	由硬件声明的本地接口性能 0 = 不能进行 1000 Mbps 全双工 1 = 能够进行 1000 Mbps 全双工 （默认）

表 3-2 操作模式参数 *（续）*

参数	说明
以下参数适用于 Sun Crypto 加速器 4000 UTP 和 MMF 适配器。	
`adv-1000hdx-cap`	由硬件声明的本地接口性能 0 = 不能进行 1000 Mbps 半双工 1 = 能够进行 1000 Mbps 半双工 （默认）
以下参数只适用于 Sun Crypto 加速器 4000 UTP 适配器。	
`adv-100fdx-cap`	由硬件声明的本地接口性能 0 = 不能进行 100 Mbps 全双工 1 = 能够进行 100 Mbps 全双工 （默认）
`adv-100hdx-cap`	由硬件声明的本地接口性能 0 = 不能进行 100 Mbps 半双工 1 = 能够进行 100 Mbps 半双工 （默认）
`adv-10fdx-cap`	由硬件声明的本地接口性能 0 = 不能进行 10 Mbps 全双工 1 = 能够进行 10 Mbps 全双工 （默认）
`adv-10hdx-cap`	由硬件声明的本地接口性能 0 = 不能进行 10 Mbps 半双工 1 = 能够进行 10 Mbps 半双工 （默认）

如果您将上述所有参数均设为 1，自动协商模式将尽量采用最高的速度。如果您将上述所有参数均设为 0，则会收到以下错误消息：

```
NOTICE: Last setting will leave vca0 with no link capabilities.
WARNING: vca0: Restoring previous setting.
```

注意 – 在上面的示例中，`vca0` 是 Sun Crypto 加速器 4000 板的设备名称，其中字符串 `vca` 表示每一个 Sun Crypto 加速器 4000 板。此字符串后面始终紧跟板的设备例程号。因此， `vca0` 板的设备例程号为 `0`。

流控制参数

vca 设备能够产生 （发送）和终止 （接收）符合 EEE 802.3x Frame Based Link Level Flow Control Protocol 要求的暂停帧。回应收到的流控制帧时， vca 设备可以降低其发送速率。此外， vca 设备还可以产生流控制帧以及请求链接伙伴降低其发送速率（如果链接伙伴支持此项功能）。默认情况下，驱动程序会在自动协商期间声明发送和接收暂停性能。

表 3-3 列出了流控制关键字并说明了它们的作用。

表 3-3 读-写流控制关键字说明

关键字	说明		
adv-asmpause-cap	MMF 适配器和 UTP 适配器均支持非对称暂停；因此， vca 设备只能单向暂停。 0 = 关闭 （默认） 1 = 打开		
adv-pause-cap	此参数有两种含义，具体取决于 adv-asmpause-cap 参数的值。（默认值 = 0）		
	参数值 +	**参数值 =**	**说明**
	adv-asmpause-cap=	adv-pause-cap=	
	1	1 或 0	adv-pause-cap 确定暂停操作的方向。
	1	1	接收暂停但不发送。
	1	0	发送暂停但不接收。
	0	1	发送和接收暂停。
	0	1 或 0	adv-pause-cap 参数确定是打开还是关闭暂停功能。
pause-on-threshold	定义接收 (RX) FIFO 中的 64 字节块的数量，这可以使板生成 XON-PAUSE 帧。		
pause-off-threshold	定义 RX FIFO 中的 64 字节块的数量，这可以使板生成 XOFF-PAUSE 帧。		

千兆位强制模式参数

对于千兆位链接，此参数用于确定 link-master。通常，交换机用作链接主控设备；在这种情况下，此参数可以保持不变。如果交换机没有用作链接主控设备，则可用 link-master 参数指定 vca 设备作为链接主控设备。

表 3-4 千兆位强制模式参数

参数	说明
link-master	设为 1 时，该参数启用主控操作 （假定链接伙伴为从属设备）。 设为 0 时，该参数启用从属操作 （假定链接伙伴为主控设备）。（默认）

数据包收发间隔参数

vca 设备支持一种名为 enable-ipg0 的可编程模式。

当启用 enable-ipg0 （默认）时， vca 设备会在发送数据包之前增加额外的延迟时间。这一延迟 （由 ipg0 参数设定）是对 ipg1 和 ipg2 参数所设定延迟的补充。增加额外的 ipg0 延迟可以降低冲突机会。

当禁用 enable-ipg0 时， ipg0 参数值会被忽略，且不会设定额外的延迟。此时，只使用由 ipg1 和 ipg2 参数设定的延迟。如果其它系统持续发送大量的连续数据包，请禁用 enable-ipg0。已启用 enable-ipg0 的系统在网络上可能没有充足的时间。您可以通过设定 ipg0 参数 （范围是 0 至 255，这是介质字节延迟时间）来增加额外的延迟时间。表 3-5 定义了 enable-ipg0 和 ipg0 参数。

表 3-5 定义 enable-ipg0 和 ipg0 参数

参数	值	说明
enable-ipg0	0 1	启用 enable-ipg0 禁用 enable-ipg0 （默认值 = 1）
ipg0	0 至 255	收到发数据包与发送数据包之间的额外延迟时间 （或间隔）（默认值 = 8）

vca 设备支持可编程的数据包收发间隔参数 (IPG, interpacket gap parameter) ipg1 和 ipg2。总 IPG 是 ipg1 与 ipg2 之和。链接速率为 1000 Mbps 时，总 IPG 为 0.096 微秒。

表 3-6 列出了 IPG 参数的默认值和允许值。

表 3-6 读-写数据包收发间隔参数值和说明

参数	值 （字节时间）	说明
ipg1	0 至 255	数据包收发间隔 1 （默认值 = 8）
ipg2	0 至 255	数据包收发间隔 2 （默认值 = 4）

默认情况下，驱动程序将 ipg1 设为 8 字节时间， ipg2 设为 4 字节时间，这些都是标准值。（字节时间是指通过速率为 1000 Mbps 的链接发送一个字节所用的时间。）

如果在您的网络中，某些系统使用较长的 IPG 时间 （ipg1 与 ipg2 之和），并且它们访问网络的速度似乎较慢，请适当增加 ipg1 和 ipg2 的值，以便与其它系统的较长 IPG 时间一致。

中断参数

表 3-7 介绍了接收中断消隐值。

表 3-7 用于读取别名的 RX 消隐寄存器

字段名称	值	说明
rx-intr-pkts	0 至 511	自处理上一个数据包后，收到此数量的数据包之后即会中断。零值表示无数据包消隐。（默认值 = 3）
rx-intr-time	0 至 524287	自处理上一个数据包后，等待 4.5 微秒 (usecs)，然后中断。零值表示无时间消隐。（默认值 = 3）

随机提前丢弃参数

这些参数用于依据接收 FIFO 的充满程度来丢弃数据包。默认情况下，此功能禁用。当 FIFO 占用率达到某一范围时，将会根据预定的概率丢弃数据包。当 FIFO 等级增加时，概率也会随之增加。控制数据包永远不会丢弃，且不计入统计数据。

表 3-8 RX 随机提前检测 8 位矢量

字段名称	值	说明
red-dv4to6k	0 至 255	当 FIFO 阈值大于 4096 字节且小于 6,144 字节时，适用的随机提前检测和数据包丢弃矢量。丢弃概率可以按 12.5 百分比的增量进行设定。例如，如果设为位 0，则会丢弃此范围内的每八个数据包中的第一个数据包。（默认值 = 0）
red-dv6to8k	0 至 255	当 FIFO 阈值大于 6,144 字节且小于 8,192 字节时，适用的随机提前检测和数据包丢弃矢量。丢弃概率可以按 12.5 百分比的增量进行设定。例如，如果设为位 8，则会丢弃此范围内的每八个数据包中的第一个数据包。（默认值 = 0）
red-dv8to10k	0 至 255	当 FIFO 阈值大于 8,192 字节且小于 10,240 字节时，适用的随机提前检测和数据包丢弃矢量。丢弃概率可以按 12.5 百分比的增量进行设定。例如，如果设为位 16，则会丢弃此范围内的每八个数据包中的第一个数据包。（默认值 = 0）
red-dv10to12k	0 至 255	当 FIFO 阈值大于 10,240 字节且小于 12,288 字节时，适用的随机提前检测和数据包丢弃矢量。丢弃概率可以按 12.5 百分比的增量进行设定。例如，如果设为位 24，则会丢弃此范围内的每八个数据包中的第一个数据包。（默认值 = 0）

PCI 总线接口参数

您可使用这些参数来修改 PCI 接口功能，从而使给定的应用程序获得更好的 PCI 互连性能。

表 3-9 PCI 总线接口参数

参数	说明
`tx-dma-weight`	确定在繁重的循环仲裁过程中为发送 (TX) 端赋予的倍增因数；其值为 0 至 3 （默认值 = 0）。零值表示没有额外的加权。其它值表示为繁重的通信赋予以 2 为底数的幂的额外加权。例如，如果 `tx-dma-weight` = 0 且 `rx-dma-weight` = 3, 则只要 RX 通信持续进行， RX 通信访问 PCI 的优先级是 TX 通信访问 PCI 优先级的 8 倍（即 2 的 3 次幂）。
`rx-dma-weight`	确定在加权循环仲裁过程中为接收 (RX) 端赋予的倍增因数。其值为 0 至 3 （默认值 = 0）。
`infinite-burst`	当启用此参数且系统支持 infinite burst （无限提速）功能时，允许使用无限提速功能。适配器不会释放总线，直到数据包通过总线传输完毕为止。其值为 0 或 1 （默认值 = 0）。
`disable-64bit`	关闭适配器的 64 位功能。 注意：对于基于 UltraSPARC® 的平台，此参数的默认值可能为 1。对于基于 UltraSPARC II 的平台，默认值为 0。其值为 0 或 1 （默认值 =0，即启用 64 位功能）。

设置 vca 驱动程序参数

您可采用两种方法设置 `vca` 设备驱动程序的参数：

- 使用 `ndd` 实用程序
- 使用 `vca.conf` 文件

如果使用 `ndd` 实用程序，则所设的参数将在重新启动系统后失效。此方法适于测试参数设置。

要使您设置的参数在重新启动系统后仍保持有效，请创建 `/kernel/drv/vca.conf` 文件，并在需要为系统中的设备设置特殊参数时，向其中添加必要的参数值。有关详情，请参阅第 32 页 “使用 `vca.conf` 文件设置驱动程序参数”。

使用 ndd 实用程序设置参数

使用 ndd 实用程序配置参数时，所设的参数将在重新启动系统后失效。

以下几节介绍如何使用 vca 驱动程序和 ndd 实用程序修改 （使用 -set 选项）或显示（不用 -set 选项）每一个 vca 设备的参数。

▼ 指定 ndd 实用程序的设备例程

使用 ndd 实用程序获取或设置 vca 设备的参数之前，必须指定此实用程序的设备例程。

1. **检查 /etc/path_to_inst 文件，确定与特定设备相关的例程号。有关说明，请参阅 path_to_inst(4) 的联机手册页。**

```
# grep vca /etc/path_to_inst
"/pci@8,600000/network@1" 0 "vca"
"/pci@8,700000/network@1" 1 "vca"
```

上述示例中，有二个 Sun Crypto 加速器 4000 以太网例程来自已安装的适配器。例程号是 0 和 1。

2. **使用例程号选择设备。**

```
# ndd -set /dev/vcaN
```

注意 – 在本用户指南介绍的示例中， *N* 表示设备的例程号。

此设备会一直保持选定状态，直到您更改选择为止。

非交互和交互模式

您可在两种模式下使用 ndd 实用程序：

- 非交互模式
- 交互模式

在非交互模式下，您可以运行实用程序以执行某个特殊命令。执行该命令之后，您将退出实用程序。在交互模式下，您可以使用实用程序来获得或设置多个参数值。有关详细信息，请参阅 ndd(1M) 联机手册页。

在非交互模式下使用 ndd *实用程序*

本节介绍如何修改和显示参数值。

- **要修改参数值，请使用** -set **选项。**

  如果您运行 ndd 实用程序及其 -set 选项，实用程序将传递*值*（该值必须分配给指定的 /dev/vca 驱动程序例程），并将其分配给参数：

```
# ndd -set /dev/vcaN parameter value
```

  更改任意 adv 参数时，屏幕上会显示一则类似于以下的消息：

```
- link up 1000 Mbps half duplex
```

- **要显示参数的值，请指定参数名并忽略其值。**

  当忽略 -set 选项时，会出现查询操作，实用程序询问指定的驱动程序例程，检索与指定参数相关的值，然后打印该值：

```
# ndd /dev/vcaN 参数
```

在交互模式下使用 ndd *实用程序*

- **要在交互模式下修改参数值，请指定** ndd /dev/vca**，如下所示。**

  ndd 实用程序随后会提示您输入参数名称：

```
# ndd /dev/vcaN
name to get/set? (Enter the parameter name or ? to view all
parameters)
```

  输入参数名称后， ndd 实用程序会提示您输入参数值 （参见表 3-1 至表 3-9）。

- **要列出** vca **驱动程序支持的所有参数，请输入** ndd /dev/vca。
  （有关参数说明，请参见表 3-1 至表 3-9）。

```
# ndd /dev/vca
name to get/set ? ?
?                               (read only)
instance                        (read and write)
adv-autoneg-cap                 (read and write)
adv-1000fdx-cap                 (read and write)
adv-1000hdx-cap                 (read and write)
adv-100fdx-cap                  (read and write)
adv-100hdx-cap                  (read and write)
adv-10fdx-cap                   (read and write)
adv-10hdx-cap                   (read and write)
adv-asmpause-cap                (read and write)
adv-pause-cap                   (read and write)
pause-on-threshold              (read and write)
pause-off-threshold             (read and write)
link-master                     (read and write)
enable-ipg0                     (read and write)
ipg0                            (read and write)
ipg1                            (read and write)
ipg2                            (read and write)
rx-intr-pkts                    (read and write)
rx-intr-time                    (read and write)
red-p4k-to-6k                   (read and write)
red-p6k-to-8k                   (read and write)
red-p8k-to-10k                  (read and write)
red-p10k-to-12k                 (read and write)
tx-dma-weight                   (read and write)
rx-dma-weight                   (read and write)
infinite-burst                  (read and write)
disable-64bit                   (read and write)
name to get/set ?
#
```

设置自动协商或强制模式

下列链接参数可以设为在自动协商或强制模式下进行操作：

- speed
- duplex
- link-clock

默认情况下，系统会为这些链接参数启用自动协商模式。当这些参数均处于自动协商模式下时， vca 设备将与链接伙伴通信，以协商相互兼容的值和流控制性能。当为这些参数设置 auto 之外的值时，不会进行协商，并在强制模式下配置链接参数。在强制模式下，链接伙伴双方的 speed 参数值必须一致。有关说明，请参阅第 35 页 “使用 OpenBoot PROM 为链接参数启用自动协商或强制模式”。

▼ 禁用自动协商模式

如果您的网络设备不支持自动协商模式，或者您想在强制模式下使用网络 speed、duplex 或 link-clock 参数，则可以在 vca 设备上禁用自动协商模式。

1. **将以下驱动程序参数的值设为链接伙伴设备 （例如，交换机）附带文档中所述的值：**
   - adv-1000fdx-cap
   - adv-1000hdx-cap
   - adv-100fdx-cap
   - adv-100hdx-cap
   - adv-10fdx-cap
   - adv-10hdx-cap
   - adv-asmpause-cap
   - adv-pause-cap

   有关这些参数的说明和可能值，请参见表 3-2。

2. **将** adv-autoneg-cap **参数设为** 0。

```
# ndd -set /dev/vcaN adv-autoneg-cap 0
```

更改任意 ndd 参数时，屏幕上均会显示一则类似于以下的消息：

```
link up 1000 Mbps half duplex
```

注意 – 如果禁用自动协商模式，则必须使 speed、 duplex 和 link-clock （只适用于 1000 Mbps）参数以在强制模式下操作。有关说明，请参阅第 35 页 “使用 OpenBoot PROM 为链接参数启用自动协商或强制模式”。

使用 vca.conf 文件设置参数

您也可以通过向 /kernel/drv 目录下的 vca.conf 文件中添加条目来指定驱动程序参数属性。参数名称与第 20 页 “驱动程序参数值和定义”中列出的名称相同。

警示 – 请勿删除 /kernel/drv/vca.conf 文件中的任何默认条目。

有关其它详细资料，请参阅 prtconf(1) 和 driver.conf(4) 联机手册页。下面的过程介绍了在 vca.conf 文件中设置参数的示例。

上一节中定义的变量适用于系统中的已知设备。要通过 vca.conf 文件为 Sun Crypto 加速器 4000 板设置变量，必须知道以下三条设备信息：设备名称、父设备、设备单元地址。

▼ 使用 vca.conf 文件设置驱动程序参数

1. **获取设备树中 vca 设备的硬件路径名称。**

   a. **检查 /etc/driver_aliases 文件，确定与特定设备相关的名称。**

```
# grep vca /etc/driver_aliases
vca "pci108e,3de8"
```

   在上面的示例中，与 Sun Crypto 加速器 4000 软件驱动程序 (vca) 相关的设备名称是 "pci108e,3de8"。

   b. **在 /etc/path_to_inst 文件中找到父设备名称和设备单元地址。**

   有关说明，请参阅 path_to_inst(4) 的联机手册页。

```
# grep vca /etc/path_to_inst
"/pci@8,600000/network@1" 0 "vca"
"/pci@8,700000/network@1" 1 "vca"
```

在上面的示例中，共有三栏输出值：设备路径名称、例程号和软件驱动程序名称。

上述示例中第一行内的设备路径名称是 “/pci@8,600000/network@1”。设备路径名称由三部分组成：父设备名称、设备节点名称和设备单元地址。有关说明，请参见表 3-10。

表 3-10 设备路径名称

完整设备路径名称	父设备名称部分	节点名称部分	单元地址部分
"/pci@8,600000/network@1"	/pci@8,600000	network	1
"/pci@8,700000/network@1"	/pci@8,700000	network	1

要在 vca.conf 文件中明确标识 PCI 设备，请使用设备的完整设备路径名称 （父设备名称、节点名称和单元地址）。有关 PCI 设备规格的详细信息，请参阅 pci(4) 联机手册页。

2. **在** /kernel/drv/vca.conf **文件中为上述设备设置参数。**

   在下面的条目中，系统为某个特定 Sun Crypto 加速器 4000 以太网设备禁用了 adv-autoneg-cap 参数。

```
name="pci108e,3de8" parent="/pci@8,700000" unit-address="1" adv-autoneg-cap=0;
```

3. **保存** vca.conf **文件。**
4. **保存和关闭所有文件及程序，然后退出窗口系统。**
5. **关闭然后重新启动系统。**

使用 vca.conf 文件为所有 Sun Crypto 加速器 4000 vca 设备设置参数

如果忽略设备路径名称 （父设备名称和单元地址），则系统会为所有 Sun Crypto 加速器 4000 以太网设备的每一个例程设置参数。

▼ 使用 vca.conf 文件为所有 Sun Crypto 加速器 4000 vca 设备设置参数

1. **在** vca.conf **文件中，通过输入***参数* = *值*;**添加一行，更改所有例程的参数值。**

   下面的示例将所有 Sun Crypto 加速器 4000 以太网设备的每一个例程的 adv-autoneg-cap 参数值设为 1：

```
adv-autoneg-cap=1;
```

vca.conf 文件示例

下面是 vca.conf 文件的示例：

```
#
# Copyright 2002 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
#ident  "@(#)vca.conf   1.2     02/06/26 SMI"

#
# Use the new Solaris 9 properties to ensure that the driver is attached
# on boot, to get us to register with KCL2.  This also prevents us from
# being unloaded by the cleanup modunload -i 0.
#
ddi-forceattach=1 ddi-no-autodetach=1;
name="pci108e,3de8" parent="/pci@8,700000" unit-address="1" adv-autoneg-cap=0;
adv-autoneg-cap=1;
```

使用 OpenBoot PROM 为链接参数启用自动协商或强制模式

通过 OpenBoot PROM (OBP) 界面，您可将以下参数设为在自动协商或强制模式下操作：

表 3-11 本地链接网络设备参数

参数	说明
speed	此参数可以设为 auto、 1000、 100 或 10 ；语法如下： • speed=auto（默认值） • speed=1000 • speed=100 • speed=10
duplex	此参数可以设为 auto、 full 或 half ；语法如下： • duplex=auto（默认值） • duplex=full • duplex=half
link-clock	只有 speed 参数设为 1000 或使用 1000 Mbps MMF Sun Crypto 加速器 4000 板时，此参数才适用。此参数的值必须与为链接伙伴设置的值相对应。例如，当本地链接的值为 master 时，则链接伙伴的值必须为 slave。此参数可以设为 master、 slave 或 auto ；语法如下： • link-clock=auto（默认值） • link-clock=master • link-clock=slave

要建立正确的链接，必须在本地链接和链接伙伴双方正确配置 speed、 duplex 和 link-clock （只适用于 1000 Mbps）参数。本地链接和链接伙伴的每一个 speed、 duplex 和 link-clock （只适用于 1000 Mbps）参数必须在自动协商或强制模式下进行操作。当其中一个参数值设为 auto 时，会使链接在该参数的自动协商模式下进行操作。如果在 OBP 提示符下未输入参数，则系统会将参数的值默认设为 auto。当其中一个参数设为 auto 之外的其它值时，会使本地链接在该参数的强制模式下进行操作。

当本地链接在 speed 和 duplex 参数的自动协商模式下操作时，如果其速率设为 100 Mbps 或更低，并且启用了全双工和半双工模式，则链接伙伴可以采用 100 Mbps 或 10 Mbps 的速度以及任何一种双工模式进行操作。

当 speed 参数在强制模式下操作时，本地链接的 speed 值必须与链接伙伴的 speed 值相匹配。如果本地链接和链接伙伴双方的 duplex 参数不匹配，则可以进行链接；但会出现通信冲突。

当本地链接的 speed 参数设为自动协商模式，链接伙伴的 speed 参数设为强制模式时，您也许可以建立链接，具体取决于 speed 值是否可在本地链接和链接伙伴双方进行协商。默认情况下，自动协商模式下的接口会始终尝试采用半双工模式建立链接（如果速度匹配的话）。由于这两个接口中的其中一个不处于自动协商模式，自动协商模式下的接口将只检测 speed 参数；而不检测双工参数。这种方法称为“并行检测”。

警示 – 在双工不一致时建立的链接总会导致通信冲突。

对于要在强制模式下操作的本地链接参数，其值必须是 auto 之外的值。例如，要建立速度为 100 Mbps 且半双工的强制模式链接，请在 OBP 提示符下输入以下命令：

```
ok boot net:speed=100,duplex=half
```

注意 – 在本节的示例中， net 是默认的集成网络接口设备路径的别名。您也可以通过指定某个设备路径（而非使用 net）来配置其它网络设备。

要建立具有主控时钟的、速度为 1000 Mbps 且半双工的强制模式链接，请在 OBP 提示符下输入以下命令：

```
ok boot net:speed=1000,duplex=half,link-clock=master
```

注意 – 本地链接的 link-clock 参数值必须与链接伙伴的 link-clock 值相对应。例如，当本地链接的 link-clock 值设为 master 时，链接伙伴的 link-clock 值必须设为 slave。

要建立速度为 10 Mbps 的强制模式和双工的自动协商模式，请在 OBP 提示符下输入以下命令：

```
ok boot net:speed=10,duplex=auto
```

您也可以在 OBP 提示符下输入以下命令，以建立与上一示例相同的本地链接参数：

```
ok boot net:speed=10
```

有关详细信息，请参阅 IEEE 802.3 文档。

Sun Crypto 加速器 4000 加密和以太网驱动程序操作统计

本节介绍由 kstat(1M) 命令提供的统计信息。

加密驱动程序统计

表 3-12 介绍了加密驱动程序的统计信息。

表 3-12 加密驱动程序统计

参数	说明	稳定或不稳定
vs-mode	其值可为 FIPS、 standard 或 unitialized。 FIPS 表示板处于 FIPS 模式。 standard 表示板不处于 FIPS 模式。 unitialized 表示板未初始化。	稳定
vs-status	其值可为 ready、 faulted 或 failsafe。 ready 表示板操作正常。 faulted 表示板未进行操作。 failsafe 表示 failsafe 模式，是板的原始出厂状态。	稳定

以太网驱动程序统计

表 3-13 介绍了以太网驱动程序的统计信息。

表 3-13 以太网驱动程序统计

参数	说明	稳定或不稳定
ipackets	调入数据包的数量。	稳定
ipackets64	64 位版本的 ipackets。	稳定
ierrors	已收到的因包含错误而无法处理的总数据包数（长）。	稳定
opackets	请求通过接口发送的总数据包数。	稳定
opackets64	请求通过接口发送的总数据包数 （64 位）。	稳定
oerrors	因错误而未成功发送的总数据包数 （长）。	稳定

表 3-13 以太网驱动程序统计 *（续）*

参数	说明	稳定或不稳定
rbytes	通过接口成功接收的总字节数。	稳定
rbytes64	通过接口成功接收的总字节数 （64 位）。	稳定
obytes	请求通过接口发送的总字节数。	稳定
obytes64	请求通过接口发送的总字节数 （64 位）。	稳定
multircv	成功接收的多播数据包数，包括组和功能地址（长）。	稳定
multixmt	请求发送的多播数据包数，包括组和功能地址（长）。	稳定
brdcstrcv	成功接收的广播数据包数 （长）。	稳定
brdcstxmt	请求发送的广播数据包数 （长）。	稳定
norcvbuf	由于无法为收到的数据包分配缓冲器，有效进入的数据包被丢弃的已知次数 （长）。	稳定
noxmtbuf	由于发送缓冲器繁忙，或者没有可分配用于发送的缓冲器，而在输出时被丢弃的数据包数 （长）。	稳定

表 3-14 介绍了发送和接收 MAC 计数器。

表 3-14 TX 和 RX MAC 计数器

参数	说明	稳定或不稳定
tx-collisions	对于导致冲突的每一次帧发送尝试， 16 位可加载计数器的增量。	稳定
tx-first-collisions	对于符合以下条件的每一次帧发送：第一次尝试时遇到故障，但第二次尝试获得成功， 16 位可加载计数器的增量。	不稳定
tx-excessive-collisions	对于已超出发送限制次数的每一次帧发送， 16 位可加载计数器的增量。	不稳定
tx-late-collisions	对于发生冲突的每一次帧发送， 16 位可加载计数器的增量。它表示 TxMAC 在发送至少 Minimum Frame Size （最小帧大小）字节数之后因出现的故障而丢弃的帧数。通常，它表示网络上至少有一个站点违背了所允许的最大网络范围。	不稳定
tx-defer-timer	TxMAC 在尝试发送帧期间推迟网络上的通信时， 16 位可加载计时器的增量。计时器的计时单位是介质字节时钟除以 256。	不稳定

表 3-14 TX 和 RX MAC 计数器 *（续）*

参数	说明	稳定或不稳定
tx-peak-attempts	8 位寄存器，表示自上次读取寄存器之后每一次成功发送帧的最大连续冲突数。此寄存器的最大值是 255。如果每次成功发送帧的连续冲突数超过 255，则该软件会发生可屏蔽中断。该寄存器会在读取之后自动归零。	不稳定
tx-underrun	通过网络收到有效帧之后， 16 位可加载计数器的增量。	不稳定
rx-length-err	通过网络收到长度大于 Maximum Frame Size Register （最大帧大小寄存器）中设定值的帧之后， 16 位可加载计数器的增量。	不稳定
rx-alignment-err	在接收帧中检测到校准错误时， 16 位可加载计数器的增量。当接收帧未能通过 CRC 检查算法，且帧包含非整数的字节数 （即以位表示的帧大小不能被 8 除尽）时，系统即会报告校准错误。	不稳定
rx-crc-err	当接收帧未能通过 CRC 检测算法，但帧包含整数的字节数 （即以位表示的帧大小可被 8 除尽）时， 16 位可加载计数器的增量。	不稳定
rx-code-violations	在接收帧期间， XCVR 通过 MII 生成 Rx_Err 指示时， 16 位可加载计数器的增量。当收发器在收到的数据流中检测到无效代码时，即会生成此指示。接收代码违例不被计为 FCS 或校准错误。	不稳定
rx-overflows	由于缺乏资源而被丢弃的以太网帧数。	不稳定
rx-no-buf	硬件因没有更多的接收缓冲器空间而无法接收数据的次数。	不稳定
rx-no-comp-wb	硬件无法为收到的数据传送完成条目的次数。	不稳定
rx-len-mismatch	已收到的且帧声明长度与实际帧长度不匹配的帧数量。	不稳定

以下以太网属性 （表 3-15）是设备性能和链接伙伴性能的共同部分：

表 3-15 列出了当前的以太网链接属性。

表 3-15 当前以太网链接属性

参数	说明	稳定或不稳定
ifspeed	1000、 100 或 10 Mbps	稳定
link-duplex	0 = 半双工， 1 = 全双工	稳定
link-pause	有关链接的当前暂停设置，请参阅第 23 页 “流控制参数”	稳定
link-asmpause	有关链接的当前暂停设置，请参阅第 23 页 “流控制参数”	稳定
link-up	1 = 启动， 0 = 关闭	稳定
link-status	1 = 启动， 0 = 关闭	稳定
xcvr-inuse	当前正在使用的收发器类型：1 = 内部 MII，2 = 外部 MII， 3 = 外部 PCS	稳定

表 3-16 介绍了只读介质独立接口 (MII, Media Independent Interface) 的性能。这些参数用于定义硬件的性能。千兆位介质独立接口 (GMII, Gigabit Media Independent Interface) 支持下列所有性能。

表 3-16 只读 vca 设备性能

参数	说明	稳定或不稳定
cap-autoneg	0 = 不能自动协商 1 = 能够自动协商	稳定
cap-1000fdx	本地接口全双工性能 0 = 不能进行 1000 Mbps 全双工 1 = 能够进行 1000 Mbps 全双工	稳定
cap-1000hdx	本地接口半双工性能 0 = 不能进行 1000 Mbps 半双工 1 = 能够进行 1000 Mbps 半双工	稳定
cap-100fdx	本地接口全双工性能 0 = 不能进行 100 Mbps 全双工 1 = 能够进行 100 Mbps 全双工	稳定
cap-100hdx	本地接口半双工性能 0 = 不能进行 100 Mbps 半双工 1 = 能够进行 100 Mbps 半双工	稳定

表 3-16 只读 vca 设备性能 *（续）*

参数	说明	稳定或不稳定
cap-10fdx	本地接口全双工性能 0 = 不能进行 10 Mbps 全双工 1 = 能够进行 10 Mbps 全双工	稳定
cap-10hdx	本地接口半双工性能 0 = 不能进行 10 Mbps 半双工 1 = 能够进行 10 Mbps 半双工	稳定
cap-asm-pause	本地接口流控制性能 0 = 不能执行非对称暂停 1 = 能够从本地设备执行非对称暂停 （参阅第 23 页“流控制参数”）	稳定
cap-pause	本地接口流控制性能 0 = 不能执行对称暂停 1 = 能够执行对称暂停 （参阅第 23 页 “流控制参数”）	稳定

报告链接伙伴性能

表 3-17 介绍了只读链接伙伴性能。

表 3-17 只读链接伙伴性能

参数	说明	稳定或不稳定
lp-cap-autoneg	0 = 无自动协商 1 = 自动协商	稳定
lp-cap-1000fdx	0 = 不能进行 1000 Mbps 全双工发送 1 = 1000 Mbps 全双工	稳定
lp-cap-1000hdx	0 = 不能进行 1000 Mbps 半双工发送 1 = 1000 Mbps 半双工	稳定
lp-cap-100fdx	0 = 不能进行 100 Mbps 全双工发送 1 = 100 Mbps 全双工	稳定
lp-cap-100hdx	0 = 不能进行 100 Mbps 半双工发送 1 = 100 Mbps 半双工	稳定
lp-cap-10fdx	0 = 不能进行 10 Mbps 全双工发送 1 = 10 Mbps 全双工	稳定

表 3-17 只读链接伙伴性能 *（续）*

参数	说明	稳定或不稳定
lp-cap-10hdx	0 = 不能进行 10 Mbps 半双工发送 1 = 10 Mbps 半双工	稳定
lp-cap-asm-pause	0 = 不能执行非对称暂停 1 = 用于链接伙伴性能的非对称暂停 （参阅第 23 页 “流控制参数”）	稳定
lp-cap-pause	0 = 不能执行对称暂停 1 = 能够执行对称暂停 （参阅第 23 页 “流控制参数”）	稳定

如果链接伙伴不能进行自动协商 （当 lp-cap-autoneg 为 0 时），表 3-17 中的其余信息不适用，并且参数值为 0。

如果链接伙伴能够进行自动协商 （当 lp-cap-autoneg 为 1 时），则在使用自动协商和链接伙伴性能时，屏幕上会显示速度和模式信息。

表 3-18 介绍了驱动程序专用的参数。

表 3-18 驱动程序专用参数

参数	说明	稳定或不稳定
lb-mode	设备所处的回送模式 （如果有的话）的复件。	不稳定
promisc	当启用该参数时，设备处于混合模式。当禁用该参数时，设备不处于混合模式。	不稳定
以太网发送计数器		
tx-wsrv	发送环充满的次数。	不稳定
tx-msgdup-fail	尝试复制数据包失败。	不稳定
tx-allocb-fail	尝试分配内存失败。	不稳定
tx-queue0	在第一个硬件发送队列中等待发送的数据包的数量。	不稳定
tx-queue1	在第二个硬件发送队列中等待发送的数据包的数量。	不稳定
tx-queue2	在第三个硬件发送队列中等待发送的数据包的数量。	不稳定
tx-queue3	在第四个硬件发送队列中等待发送的数据包的数量。	不稳定

表 3-18 驱动程序专用参数 *（续）*

参数	说明	稳定或不稳定
以太网接收计数器		
rx-hdr-pkts	收到的少于 256 字节的数据包数量。	不稳定
rx-mtu-pkts	收到的大于 256 字节且小于 1514 字节的数据包数量。	不稳定
rx-split-pkts	被分割为两页的数据包数量。	不稳定
rx-nocanput	由于发送至 IP 堆栈失败而丢弃的数据包数量。	不稳定
rx-msgdup-fail	不能进行复制的数据包数量。	不稳定
rx-allocb-fail	块分配失败的次数。	不稳定
rx-new-pages	在接收期间被替换的页数。	不稳定
rx-new-hdr-pages	包含小于 256 字节的数据包的页数，这些页在接收期间会被替换。	不稳定
rx-new-mtu-pages	包含大于 256 字节且小于 1514 字节的数据包的页数，这些页在接收期间会被替换。	不稳定
rx-new-nxt-pages	包含那些在多个页上分割的数据包的页数，这些页在接收期间会被替换。	不稳定
rx-page-alloc-fail	页分配失败的次数。	不稳定
rx-mtu-drops	由于驱动程序无法映射新页来替换一整页大于 256 字节且小于 1514 字节的数据包，而造成此类页被丢弃的次数。	不稳定
rx-hdr-drops	由于驱动程序无法映射新页来替换一整页小于 256 字节的数据包，而造成此类页被丢弃的次数。	不稳定
rx-nxt-drops	由于驱动程序无法映射新页来替换具有分割数据包的页，而造成此类页被丢弃的次数。	不稳定
rx-rel-flow	驱动程序被要求释放流的次数。	不稳定
以太网 PCI 属性		
rev-id	Sun Crypto 加速器 4000 以太网设备的版本 ID 对于识别字段中所用的设备非常有用。	不稳定
pci-err	所有 PCI 错误的总和。	不稳定
pci-rta-err	收到目标中断的次数。	不稳定
pci-rma-err	收到主控中断的数量。	不稳定

表 3-18 驱动程序专用参数 *（续）*

参数	说明	稳定或不稳定
pci-parity-err	检测到的 PCI 奇偶校验错误数量。	不稳定
pci-drto-err	延迟发送重试超时所达到的次数。	不稳定
dma-mode	由 Sun Crypto 加速器 4000 驱动程序 (vca) 使用。	不稳定

▼ 检查链接伙伴设置

- **成为超级用户，输入** `kstat vca:`*N* **命令：**

```
# kstat vca:N
module: vca                             instance: 0
name:   vca0                            class:    misc
```

注意 – 在上面的示例中， *N* 是 vca 设备的例程号。此号码应反映您正在为其运行 kstat 命令的板的例程号。

网络配置

本节介绍如何在系统中安装适配器之后编辑网络主机文件。

配置网络主机文件

安装驱动程序软件之后，必须为适配器的以太网接口创建一个 hostname.vca*N* 文件。注意，在文件名 hostname.vca*N* 中， *N* 表示您要使用的 vca 接口的例程号。此外，您还必须在 /etc/hosts 文件中为其以太网接口创建 IP 地址和主机名。

1. **在** /etc/path_to_inst **文件中查找正确的** vca **接口和例程号。**

   参阅 path_to_inst(4) 的联机手册页。

```
# grep vca /etc/path_to_inst
"/pci@8,600000/network@1" 0 "vca"
```

上面示例中的例程号为 0。

2. **使用 ifconfig(1M) 命令设置适配器的 vca 接口。**

使用 ifconfig 命令指定网络接口的 IP 地址。在命令行输入以下命令，并用适配器的 IP 地址替换 *ip_address*：

```
# ifconfig vcaN plumb ip_address up
```

注意 – 在本节的示例中， *N* 表示设备的例程号。

有关详情，请参阅 ifconfig(1M) 联机手册页和 Solaris 文档。

- 如果您想让设置在系统重新启动之后仍保持有效，请创建 /etc/*hostname*.vca*N* 文件，其中 *N* 表示您要使用的 vca 接口的例程号。

  要使用步骤 1 中所示的 vca 接口示例，请创建 /etc/*hostname*.vca*N* 文件，其中 *N* 表示设备的例程号，本示例为 0。如果设备例程号为 1，则文件应为 /etc/*hostname*.vca1。
- 不要为您不想使用的 Sun Crypto 加速器 4000 接口创建 /etc/*hostname*.vca*N* 文件。
- /etc/*hostname*.vca*N* 文件中必须包含相应 vca 接口的主机名。
- 主机名必须具有 IP 地址，且必须在 /etc/hosts 文件中列出。
- 此主机名必须不得与其它任何接口的主机名相同，例如， /etc/*hostname*.vca0 和 /etc/*hostname*.vca1 不能共用相同的主机名。

对于配有 Sun Crypto 加速器 4000 板（zardoz-11）的名为 zardoz 的系统而言，需要具有下面示例中的 /etc/*hostname*.vca*N* 文件。

```
# cat /etc/hostname.hme0
zardoz
# cat /etc/hostname.vca0
zardoz-11
```

3. **在 /etc/hosts 文件中为每一个活动的 vca 接口创建相应的条目。**

例如：

```
# cat /etc/hosts
#
# Internet host table
#
127.0.0.1     localhost
129.144.10.57 zardoz    loghost
129.144.11.83 zardoz-11
```

第 4 章

使用 vcaadm 和 vcadiag 实用程序管理 Sun Crypto 加速器 4000 板

本章简要介绍了 vcaadm 和 vcadiag 实用程序，其中包括以下几节：

使用 vcaadm

vcaadm 程序提供了 Sun Crypto 加速器 4000 板的命令行界面。只有身为安全主管的用户才允许使用 vcaadm 实用程序。首次通过 vcaadm 连接至 Sun Crypto 加速器 4000 板时，系统会提示您创建初始安全主管和密码。

为了便于访问 secadm 程序，请在搜索路径中指定 Sun Crypto 加速器 4000 工具目录，例如：

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

vcaadm 命令行语法如下：

- vcaadm [-H]
- vcaadm [-y] [-h *host*] [-p *port*] [-d vca*N*] [-f *filename*]
- vcaadm [-y] [-h *host*] [-p *port*] [-d vca*N*] [-s *sec_officer*] *command*

注意 – 使用 `-d` 属性时， `vca`*N* 是指板的设备名称，其中 *N* 表示 Sun Crypto 加速器 4000 的设备例程号。

表 4-1 列出了 `vcaadm` 实用程序的选项。

表 4-1 `vcaadm` 选项

选项	含义
`-H`	显示 `vcaadm` 命令的帮助文件并退出。
`-d vca`*N*	连接至 Sun Crypto 加速器 4000 板 （其中 *N* 表示板的驱动程序例程号）。例如，键入 `-d vca1` 命令可连接至设备 `vca1`，其中 `vca` 是板设备名称中的字符串， 1 是设备的例程号。该值默认为 `vca0`，并且必须采用 `vca`*N* 格式，其中 *N* 表示设备例程号。
`-f` *filename*	解释 *filename* 中的一个或多个命令并退出。
`-h` *host*	连接到 *host* 上的 Sun Crypto 加速器 4000 板。 *host* 的值可以是主机名或 IP 地址，默认值为回送地址。
`-p` *port*	连接至 *port* 上的 Sun Crypto 加速器 4000 板。 *port* 的默认值为 6870。
`-s` *sec_officer*	以安全主管的身份登录，安全主管名为 *sec_officer*。
`-y`	对任何正常提示确认的命令强制回答 “是”。

注意 – 本用户指南中，使用 *sec_officer* 作为安全主管名称的示例。

操作模式

`vcaadm` 可按三种模式运行。这些模式的主要差异在于命令传送给 `vcaadm` 的方式不同。这三种模式分别为单命令模式、文件模式和交互模式。

注意 – 要使用 `vcaadm`，您必须进行安全主管身份验证。安全主管身份验证的频率取决于所用的操作模式。

单命令模式

在单命令模式下，对于每一个命令，您均必须进行安全主管身份验证。执行命令之后，您即会退出 vcaadm。

在单命令模式下输入命令时，您需在指定所有命令行参数之后指定要运行的命令。例如，在单命令模式下，下面的命令将显示指定密钥库中的所有用户，然后向用户返回命令 shell 提示符。

```
$ vcaadm show user
Security Officer Name: sec_officer
Security Officer Password:
```

下面的命令将作为安全主管 *sec_officer* 执行登录，并在密钥库中创建用户 *web_admin*。

```
$ vcaadm -s sec_officer create user web_admin
Security Officer Password:
Enter new user password:
Confirm password:
User web_admin created successfully.
```

注意 – 第一个密码是安全主管密码，随后是新用户 *web_admin* 的密码和确认密码。

单命令模式下的所有输出都转至标准的输出流。使用基于标准 UNIX shell 的方法可以重新指定此类输出的位置。

文件模式

在文件模式下，对于所运行的每一份文件，您均必须进行安全主管身份验证。执行命令文件中的命令之后，您即会退出 vcaadm。

要在文件模式下输入命令，您需指定 vcaadm 可以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。每条注释均以井字符 (#) 开头。如果设置了文件模式选项，则 vcaadm 会忽略最后一个选项之后的任何命令行参数。下面的示例将运行 deluser.scr 文件中的命令，并对所有提示作肯定回答：

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

交互模式

在交互模式下，您必须在每次连接至板时进行安全主管身份验证。这是 vcaadm 的默认操作模式。要在交互模式下退出 vcaadm，请使用 logout 命令。有关说明，请参阅第 50 页 “通过 vcaadm 登录和退出板”。

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

通过 vcaadm 登录和退出板

从命令行中运行 vcaadm 且使用 -h、 -p 和 -d 属性分别指定*主机*、*端口*和*设备*时，系统会立即提示您以安全主管身份登录 （如果已成功建立网络连接）。

vcaadm 程序会在 vcaadm 应用程序和特定板上运行的 Sun Crypto 加速器 4000 固件之间建立加密网络连接 （信道）。

在设置加密信道期间，板可以通过各自的硬件以太网地址和 RSA 公钥来识别自身。vcaadm 首次连接至板时，会创建一个信任数据库 ($HOME/.vcaadm/trustdb)。此文件包含安全主管当前信任的所有板。

通过 vcaadm 登录板

如果安全主管连接至一个新板， vcaadm 会通知安全主管并提示以下选项：

```
1. Abort the connection
2. Trust the connection one time only (no changes to trust
   database)
3. Trust this board forever (adds the hardware ethernet address
   and RSA public key to the trust database).
```

如果安全主管所连接的板的远程访问密钥已发生更改， vcaadm 会通知安全主管并提示以下三种选项：

```
1. Abort the connection
2. Trust the connection one time only (no changes to trust
   database)
3. Replace the old public key bound to this hardware ethernet
   address with the new public key.
```

登录新板

注意 – 本章以后的示例都是在 vcaadm 的交互模式下创建的。

当连接至新板时， vcaadm 必须在信任数据库中创建一个新条目。下面是登录新板的示例。

```
# vcaadm -h hostname
Warning: MAC ID and Public Key Not Found
-----------------------------------------------------
The MAC ID and public key presented by this board were
not found in your trust database.

MAC ID: 08:00:20:EE:EE:EE
Key Fingerprint: 29FC-7A54-4014-442F-7FD9-5FEA-8411-CFB4
-----------------------------------------------------
Please select an action:

1. Abort this connection
2. Trust the board for this session only.
3. Trust the board for all future sessions.

Your Choice -->
```

登录已更改远程访问密钥的板

当连接至已更改远程访问密钥的板时， vcaadm 必须更改信任数据库中与该板对应的条目。下面是登录已更改远程访问密钥的板的示例。

```
# vcaadm -h hostname
Warning: Public Key Conflict
-----------------------------------------------------
The public key presented by the board you are connecting
to is different than the public key that is trusted for
this MAC ID.

MAC ID: 08:00:20:EE:EE:EE
New Key Fingerprint: 29FC-7A54-4014-442F-7FD9-5FEA-8411-CFB4
Trusted Key Fingerprint: A508-38D1-FED8-8103-7ACC-0D19-C9C9-11F2
-----------------------------------------------------
Please select an action:

1. Abort this connection
2. Trust the board for this session only.
3. Replace the current trusted key with the new key.

Your Choice -->
```

vcaadm 提示符

交互模式下的 vcaadm 提示符如下所示：

```
vcaadm{vcaN@hostname, sec_officer}> command
```

下表介绍了 vcaadm 提示符变量：

表 4-2 vcaadm 提示符变量定义

提示符变量	定义
vca*N*	vca 是一个表示 Sun Crypto 加速器 4000 板的字符串。 *N* 表示设备例程号 （单元地址），位于板的设备路径名中。有关检索设备例程号的详细说明，请参阅第 32 页 “使用 vca.conf 文件设置驱动程序参数”。
hostname	Sun Crypto 加速器 4000 板物理连接的主机的名称。*hostname* 可用物理主机的 IP 地址替换。
sec_officer	当前登录板的安全主管名。

通过 vcaadm 退出板

在交互模式下工作时，您可能想断开与一个板的连接并连接到另一个板，而无需完全退出 vcaadm。如果您要断开与一个板的连接并退出，但同时想保持交互模式，请使用 logout 命令：

```
vcaadm{vcaN@hostname, sec_officer}> logout
vcaadm>
```

注意，在上面的示例中， vcaadm> 提示符不再显示设备例程号、主机名或安全主管名。要登录另一个设备，请输入带以下可选参数的 connect 命令。

表 4-3 connect 命令可选参数

参数	含义
dev vca*N*	连接至驱动程序例程号为 *N* 的 Sun Crypto 加速器 4000 板。例如，-d vca1 表示连接至设备 vca1；此参数的默认值是设备 vca0。
host *hostname*	连接至 *hostname*（默认值是回送地址）上的 Sun Crypto 加速器 4000 板。 *hostname* 可用物理主机的 IP 地址替换。
port *port*	连接至端口 *port*（默认为 6870）上的 Sun Crypto 加速器 4000 板。

示例：

```
vcaadm{vcaN@hostname, sec_officer}> logout
vcaadm> connect host hostname dev vca2
Security Officer Login: sec_officer
Security Officer Password:
vcaadm{vcaN@hostname, sec_officer}>
```

如果您已连接至某个 Sun Crypto 加速器 4000 板，则 vcaadm 不允许您输入 connect 命令。您必须首先退出该板，然后才能输入 connect 命令。

每次进行新连接时， vcaadm 和目标 Sun Crypto 加速器 4000 固件均会重新协商新的会话密钥，从而保护发送的管理数据。

通过 vcaadm 输入命令

vcaadm 程序的命令语言只能与 Sun Crypto 加速器 4000 板配合使用。您可以输入命令字符串的全部，也可以输入命令字符串的一部分（必须足以与其它任何命令字符串区分开来）。例如，可以输入 sh 来代替 show，但 re 比较含糊，因为它既可以表示 reset，也可以表示 rekey。

下面的示例显示了完整输入命令字符串的情况：

```
vcaadm{vcaN@hostname, sec_officer}> show user
User                                          Status
------------------------------------------------------
web_admin                                    enabled
Tom                                           enabled
------------------------------------------------------
```

在上面的示例中，使用命令字符串的一分部，如 sh us，也可以获得同样的信息。

含糊不清的命令会产生解释性的响应：

```
vcaadm{vcaN@hostname, sec_officer}> re
Ambiguous command: re
```

获得命令帮助

vcaadm 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问号 (?) 字符。如果已输入完整的命令，并且该命令行中的某个位置存在问号 (?)，则您会得到该命令的语法。例如：

```
vcaadm{vcaN@hostname, sec_officer}> create ?
Sub-Command                    Description
-------------------------------------------------------
so                             Create a new security officer
user                           Create a new user

vcaadm{vcaN@hostname, sec_officer}> create user ?
Usage: create user [<username>]

vcaadm{vcaN@hostname, sec_officer}> set ?
Sub-Command                    Description
-------------------------------------------------------
passreq                        Set password requirements
password                       Change an existing security officer password
timeout                        Set the auto-logout time
```

另外，您还可以在 vcaadm 提示符下输入问号，以查看所有 vcaadm 命令及其说明，例如：

```
vcaadm{vcaN@hostname, sec_officer}> ?
Sub-Command                    Description
-------------------------------------------------------
backup                         Backup master key
connect                        Begin admin session with firmware
create                         Create users and accounts
delete                         Delete users and accounts
diagnostics                    Run diagnostic tests
disable                        Disable a user
enable                         Enable a user
exit                           Exit vcaadm
loadfw                         Load new firmware
logout                         Logout current session
quit                           Exit vcaadm
rekey                          Generate new system keys
reset                          Reset the hardware
set                            Set operating parameters
show                           Show system settings
zeroize                        Delete all keys and reset board
```

不在 vcaadm 交互模式下时，问号 (?) 字符将由您当前所在的 shell 进行解译。在这种情况下，请确保在问号之前使用命令 shell 转义字符。

在交互模式下退出 vcaadm 程序

您可使用两个命令从 vcaadm 退出：quit 和 exit。此外，也可使用 Ctrl-D 组合键从 vcaadm 退出。

通过 vcaadm 初始化 Sun Crypto 加速器 4000 板

配置 Sun Crypto 加速器 4000 板的第一个步骤是对其进行初始化。初始化板时，需要创建密钥库。有关说明，请参阅第 73 页 “概念和术语”。您可以初始化 Sun Crypto 加速器 4000 板使之使用新的密钥库，也可使用备份文件初始化板，使之使用现有的密钥库。

首次通过 vcaadm 连接至 Sun Crypto 加速器 4000 板时，系统会提示您是将板初始化为使用新密钥库，还是初始化为使用备份文件中现有的密钥库。 vcaadm 提示您输入任何一种板初始化类型所需的信息。

▼ 初始化 Sun Crypto 加速器 4000 板以使用新密钥库

1. **从安装 Sun Crypto 加速器 4000 板的系统的命令提示符下输入** vcaadm **，或输入** vcaadm -h *hostname* **（如果系统为远程系统），然后选择 1 以初始化板：**

```
# vcaadm -h hostname
This board is uninitialized.
You will now initialize the board.  You may
either completely initialize the board and
start with a new keystore or restore the board
using a backup file.

1. Initialize the board with a new keystore
2. Initialize the board to use an existing keystore

Your Choice (0 to exit) --> 1
```

2. **创建初始安全主管名和密码 （参阅第 59 页 “命名要求”）：**

```
Initial Security Officer Name: sec_officer
Initial Security Officer Password:
Confirm Password:
```

3. **创建密钥库名称 （参阅第 59 页 “命名要求”）：**

```
Keystore Name: keystore_name
```

4. **选择 FIPS 140-2 模式或非 FIPS 模式。**

   当处于 FIPS 模式时， Sun Crypto 加速器 4000 板与 FIPS 140-2，级别 3 兼容。 FIPS 140-2 是一种联邦信息处理标准，用于防止篡改数据，并实现高级的数据完整性和安全性能。有关说明，请参阅以下网址提供的 FIPS 140-2 文档：
   http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

```
Run in FIPS 140-2 mode? (Y/Yes/N/No) [No]: y
```

注意 – 更改或删除基本参数之前，或在执行可导致严重后果的命令之前， vcaadm 会提示您输入 Y、 Yes、 N 或 No 进行确认。这些值不区分大小写；默认值为 No。

5. **验证配置信息：**

```
Board initialization parameters:
-----------------------------------------------------
Initial Security Officer Name: sec_officer
Keystore name: keystore_name
Run in FIPS 140-2 Mode: Yes
-----------------------------------------------------

Is this correct? (Y/Yes/N/No) [No]: y
Initializing crypto accelerator board...
```

初始化 Sun Crypto 加速器 4000 板以使用现有的密钥库

如果要将多个板添加至单个密钥库，则可能需要初始化所有板，以便使用相同的密钥库信息。另外，您也可能想将 Sun Crypto 加速器 4000 板恢复至原来的密钥库配置。本节介绍如何初始化板，以便使用保存在备份文件中的现有密钥库。

执行本过程之前，必须先创建一个包含现有板配置信息的备份文件。创建和恢复备份文件时，必须提供密码才能加密和解密备份文件中的数据。有关说明，请参阅第 64 页“备份主密钥”。

▼ 初始化 Sun Crypto 加速器 4000 板以使用现有的密钥库

1. **从安装 Sun Crypto 加速器 4000 板的系统的命令提示符下输入** `vcaadm`，**或输入** `vcaadm -h` *hostname*（**如果系统为远程系统**），**然后选择 2 以使用备份文件中的现有密钥库：**

```
# vcaadm -h hostname
This board is uninitialized.
You will now initialize the board.  You may
either completely initialize the board and
start with a new keystore or restore the board
using a backup file.

1. Initialize the board with a new keystore
2. Initialize the board to use an existing keystore

Your Choice (0 to exit) --> 2
```

2. **输入备份文件的路径和密码：**

```
Enter the path to the backup file: /tmp/board-backup
Password for restore file:
```

3. **验证配置信息：**

```
Board restore parameters:
-------------------------------------------------
Path to backup file: /tmp/board-backup
Keystore name: keystore_name
-------------------------------------------------

Is this correct? (Y/Yes/N/No) [No]: y
Restoring data to crypto accelerator board...
```

通过 vcaadm 管理密钥库

密钥库是密钥资料的储存库。与密钥库信息密切相关的是安全主管和用户。密钥库不但可以存储密钥，而且还是一种用户帐户拥有密钥对象的方式。它可以使那些未通过所有者身份验证的应用程序无法看到密钥。密钥库由三部分组成：

- **密钥对象 —** 为应用程序 （如 Sun ONE Web 服务器）保存的长期密钥。
- **用户帐户 —** 这些帐户可使应用程序验证和访问特定的密钥。
- **安全主管帐户 —** 这些帐户可通过 vcaadm 访问密钥管理功能。

注意 – 每个 Sun Crypto 加速器 4000 板只能有一个密钥库。不过，多个 Sun Crypto 加速器 4000 板可以共同使用同一个密钥库，以便提供额外的性能和容错功能。

命名要求

安全主管名、用户名和密钥库名必须符合以下要求：

表 4-4 安全主管名、用户名和密钥库名要求

名称要求	说明
最小长度	至少一个字符
最大长度	用户名 63 个字符，密钥库名 32 个字符
有效字符	字母数字、下划线 (_)、连字号 (-) 和圆点 (.)
第一个字符	必须是字母

密码要求

密码要求因当前的 `set passreq` 设置（`low`、`med` 或 `high`）而异。

设置密码要求

使用 `set passreq` 命令可设置 Sun Crypto 加速器 4000 板的密码要求。对于 `vcaadm` 要求输入的任何密码，均可使用此命令来设置这些密码的字符要求。共有三种密码要求设置：

表 4-5 密码要求设置

密码设置	要求
`low`	不需要任何密码限制。这是板处于非 FIPS 模式时的默认值。
`med`	要求最少六个字符，其中一个字符必须是非字母字符。这是板处于 FIPS 140-2 模式时的默认设置，并且也是 FIPS 140-2 模式下所允许的最低密码要求。
`high`	要求最少八个字符；其中三个字符必须是字母字符，一个字符必须是非字母字符。这不是默认设置，必须进行手动配置。

要更改密码要求，请输入 `set passreq` 命令，并在后面附上 `low`、`med` 或 `high` 选项。以下命令用于将 Sun Crypto 加速器 4000 板的密码要求设为 `high`：

```
vcaadm{vcaN@hostname, sec_officer}> set passreq high

vcaadm{vcaN@hostname, sec_officer}> set passreq
Password security level (low/med/high): high
```

向密钥库中添加安全主管

一个密钥库可能有多个安全主管。安全主管名只能在 Sun Crypto 加速器 4000 板的域中被识别，且不必与主机系统上的用户名相同。

创建安全主管时，安全主管名是命令行的可选参数。如果未输入安全主管名， `vcaadm` 会提示您输入。（参阅第 59 页 “命名要求”。）

```
vcaadm{vcaN@hostname, sec_officer}> create so Alice
Enter new security officer password:
Confirm password:
Security Officer Alice created successfully.

vcaadm{vcaN@hostname, sec_officer}> create so
New security officer name: Bob
Enter new security officer password:
Confirm password:
Security Officer Bob created successfully.
```

向密钥库中添加用户

这些用户名只能在 Sun Crypto 加速器 4000 板的域中被识别，且不必与 Web 服务器进程实际所用的 UNIX 用户名相同。

创建用户时，用户名是命令行的可选参数。如果未输入用户名， `vcaadm` 会提示您输入。（参阅第 59 页 “命名要求”。）

```
vcaadm{vcaN@hostname, sec_officer}> create user web_admin
Enter new user password:
Confirm password:
User web_admin created successfully.

vcaadm{vcaN@hostname, sec_officer}> create user
New user name: Tom
Enter new user password:
Confirm password:
User Tom created successfully.
```

在 Web 服务器启动期间进行验证时，用户必须使用此密码。

警示 – 用户必须牢记自己的密码。没有密码，就无法访问自己的密钥。丢失的密码无法找回。

注意 – 如果在五分钟之内未输入任何命令，用户帐户会被注销。这是一个可调选项；有关详细说明，请参阅第 65 页 “设置自动注销时间”。

列出用户和安全主管

要列出与密钥库相关的用户或安全主管，请输入 `show user` 或 `show so` 命令。

```
vcaadm{vcaN@hostname, sec_officer}> show user
User                                          Status
------------------------------------------------------
web_admin                                     Enabled
Tom                                           Enabled
------------------------------------------------------


vcaadm{vcaN@hostname, sec_officer}> show so
Security Officer
------------------------------------------------------
sec_officer
Alice
Bob
------------------------------------------------------
```

更改密码

只有安全主管密码才可以通过 `vcaadm` 进行更改，而且安全主管只能更改自己的密码。使用 `set password` 命令可更改安全主管密码。

```
vcaadm{vcaN@hostname, sec_officer}> set password
Enter new security officer password:
Confirm password:
Security Officer password has been set.
```

用户密码可通过 Sun ONE Web 服务器 `modutil` 实用程序的 PKCS#11 界面来进行更改。有关 `modutil` 的详细信息，请参阅 Sun ONE Web 服务器文档。

启用或禁用用户

注意 – 安全主管不能被禁用。一旦创建安全主管，它即会启用，除非将其删除。

默认情况下，创建的每个用户的状态均为 “启用”。用户可以被禁用。用户被禁用后，将不能通过 PKCS#11 界面访问其密钥资料。已禁用的用户在重新启用后可以重新访问自身的所有密钥资料。

启用或禁用用户时，用户名是命令行的可选参数。如果未输入用户名， `vcaadm` 会提示您输入。要禁用用户帐户，请输入 `disable user` 命令。

```
vcaadm{vcaN@hostname, sec_officer}> disable user Tom
User Tom disabled.
vcaadm{vcaN@hostname, sec_officer}> disable user
User name: web_admin
User web_admin disabled.
```

要启用用户帐户，请输入 `enable user` 命令。

```
vcaadm{vcaN@hostname, sec_officer}> enable user Tom
User Tom enabled.

vcaadm{vcaN@hostname, sec_officer}> enable user
User name: web_admin
User web_admin enabled.
```

删除用户

输入 `delete user` 命令并指定要删除的用户。删除用户时，用户名是命令行的可选参数。如果未输入用户名， `vcaadm` 会提示您输入。

```
vcaadm{vcaN@hostname, sec_officer}> delete user web_admin
Delete user web_admin? (Y/Yes/N/No) [No]: y
User web_admin deleted successfully.

vcaadm{vcaN@hostname, sec_officer}> delete user
User name: Tom
Delete user Tom? (Y/Yes/N/No) [No]: y
User Tom deleted successfully.
```

删除安全主管

输入 `delete so` 命令并指定要删除的安全主管。删除安全主管时，安全主管名是命令行的可选参数。如果未输入安全主管名， `vcaadm` 会提示您输入。

```
vcaadm{vcaN@hostname, sec_officer}> delete so Bob
Delete Security Officer Bob? (Y/Yes/N/No) [No]: y
Security Officer Bob deleted.

vcaadm{vcaN@hostname, sec_officer}> delete so
Security Officer name: Alice
Delete Security Officer Alice? (Y/Yes/N/No) [No]: y
Security Officer Alice deleted.
```

备份主密钥

密钥库保存在磁盘上，并已使用主密钥进行了加密。该主密钥保存在 Sun Crypto 加速器 4000 固件中，可由安全主管加以备份。

要备份主密钥，请使用 `backup` 命令。 `backup` 命令将要求您输入用于保存备份文件的路径名。该路径名可以在命令行中输入，如果未输入， `vcaadm` 会提示您输入路径名。

您必须为备份数据设置密码。该密码用于加密备份文件中的主密钥。

```
vcaadm{vcaN@hostname, sec_officer}> backup /opt/SUNWconn/vca/backups/bkup.data
Enter a password to protect the data:
Confirm password:
Backup to /opt/SUNWconn/vca/backups/bkup.data successful.
```

警示 – 制作备份文件时，您应选择难以猜测的密码，因为此密码用于保护密钥库的主密钥。同时，您必须牢记输入的密码。没有密码，就无法访问主密钥备份文件。一旦遗忘，将无法恢复由密码保护的数据。

锁定密钥库以防止备份

某些站点可能具有严格的安全措施，不允许 Sun Crypto 加速器 4000 板的主密钥离开硬件。您可以使用 `set lock` 命令来强制执行这一防范措施。

警示 – 输入此命令之后，所有备份主密钥的尝试都将失败。即使主密钥被重新设置，此锁定仍会保持不变。清除此设置的唯一方法是使用 `zeroize` 命令零置 Sun Crypto 加速器 4000 板。有关说明，请参阅第 69 页 “零置 Sun Crypto 加速器 4000 板”。

```
vcaadm{vcaN@hostname, sec_officer}> set lock
WARNING: Issuing this command will lock the
         master key.  You will be unable to back
         up your master key once this command
         is issued.  Once set, the only way to
         remove this lock is to zeroize the board.
Do you wish to lock the master key? (Y/Yes/N/No) [No]: y
The master key is now locked.
```

通过 vcaadm 管理板

本节介绍如何通过 `vcaadm` 实用程序来管理 Sun Crypto 加速器 4000 板。

设置自动注销时间

要自定义安全主管被板自动注销的时间，请使用 `set timeout` 命令。要更改自动注销时间，请输入 `set timeout` 命令，并附上板在自动注销安全主管之前所等待的分钟数。零值表示禁用自动注销功能，最大延迟时间是 1,440 分钟 （即 1 天）。新初始化的 Sun Crypto 加速器 4000 板的默认时间为 5 分钟。

下面的命令可将安全主管的自动注销时间改为 10 分钟。

```
vcaadm{vcaN@hostname, sec_officer}> set timeout 10
```

显示板状态

要获取 Sun Crypto 加速器 4000 板的当前状态，请输入 `show status` 命令。此命令可以显示板的硬件和固件版本、网络接口的 MAC 地址、网络接口状态（启动或关闭、速度、双工等）以及密钥库名称和 ID。

```
vcaadm{vcaN@hostname, sec_officer}> show status
Board Status
----------------------------------------------------------------
Hardware Version: 1.0
Firmware Version: 1.0
Bootstrap Firmware Version: VCA Crypto Accelerator 1.0  March 2003
Current Firmware Version: VCA Crypto Accelerator 1.0  March 2003
MAC Address: 00:03:ba:0e:96:aa
Interface information: Link up, 1000Mbps, Full Duplex
Keystore Name: keystore_name
Keystore ID: 832aece03e654790
Login Session Timeout (in minutes): 10
Password policy security level: HIGH
Number of master key backups: 0
* Device is in FIPS 140-2 Mode
----------------------------------------------------------------
```

确定板是否在 FIPS 140-2 模式下操作

如果 Sun Crypto 加速器 4000 板正在 FIPS 140-2 模式下操作， `show status` 命令会输出下面的信息行：

```
* Device is in FIPS 140-2 Mode
```

如果板不在 FIPS 140-2 模式下操作，则 `show status` 命令不会输出指示 FIPS 140-2 模式的信息行。

另外，您也可以使用 `kstat`(1M) 实用程序来确定板是否在 FIPS 140-2 模式下操作。如果板正在 FIPS 140-2 模式下操作， `kstat`(1M) 参数 `vs-mode` 返回的值将是 `FIPS`。有关 `kstat`(1M) 实用程序的说明，请参阅第 37 页 “Sun Crypto 加速器 4000 加密和以太网驱动程序操作统计”和联机手册页。

加载新固件

当添加新功能时，可能需要更新 Sun Crypto 加速器 4000 板的固件。要加载固件，请输入 `loadfw` 命令并提供固件文件的路径。

为了成功更新固件，必须使用 `reset` 命令对板进行手动重新设置。重新设置板时，当前登录的安全主管会被注销。

```
vcaadm{vcaN@hostname, sec_officer}> loadfw /opt/SUNWconn/cryptov2/firmware/sca4000fw
Security Officer Login: sec_officer
Security Officer Password:
WARNING: This command will load new firmware onto the
          the target device.  You must issue a reset
          command and log back into the target device in
          order to use the new firmware.

Proceed with firmware update? (Y/Yes/N/No) [No]: y
```

重新设置 Sun Crypto 加速器 4000 板

某些情况下，可能需要重新设置板。要重新设置板，您必须运行 `reset` 命令。系统会询问您是否确实要重新设置板。重新设置 Sun Crypto 加速器 4000 板会暂时停止系统上的加密加速过程，除非该板的任务由其它活动的 Sun Crypto 加速器 4000 板接管。同时，该命令也会使您自动退出 `vcaadm`。因此，如果您要继续管理板，则必须重新登录 `vcaadm` 以重新连接至设备。

```
vcaadm{vcaN@hostname, sec_officer}> reset
WARNING: Issuing this command will reset the
         the board and close this connection.

Proceed with reset? (Y/Yes/N/No) [No]: y
Reset successful.
```

重新设置 Sun Crypto 加速器 4000 板的密钥

出于安全策略考虑，您可能每隔一段时间便要设置新的密钥来取代旧的主密钥或远程访问密钥。 `rekey` 命令用于重新生成其中任何一个密钥，或者重新生成这两个密钥。

重新设置主密钥还会导致在新密钥下重新加密密钥库，且会使旧的备份主密钥文件失效而启用新的密钥库文件。建议用户在重新设置主密钥时制作主密钥的备份。如果多个 Sun Crypto 加速器 4000 板使用相同的密钥库，则需备份新的主密钥，然后将其恢复至其它板。

重新设置远程访问密钥会注销安全主管，并强制使用新远程访问密钥进行新的连接。

运行 `rekey` 命令时，您可以指定以下三种密钥类型之一：

表 4-6 密钥类型

密钥类型	操作
`master`	重新设置主密钥。
`remote`	重新设置远程访问密钥。注销安全主管。
`all`	重新设置主密钥和远程访问密钥。

以下是通过 `rekey` 命令输入 `all` 密钥类型的示例：

```
vcaadm{vcaN@hostname, sec_officer}> rekey

Key type (master/remote/all): all
WARNING: Rekeying the master key will render all old board backups
         useless with the new keystore file. If other boards use this
         keystore, they will need to have this new key backed up and
         restored to those boards. Rekeying the remote access key will
         terminate this session and force you to log in again.

Rekey board? (Y/Yes/N/No) [No]: y
Rekey of master key successful.
Rekey of remote access key successful.  Logging out.
```

零置 Sun Crypto 加速器 4000 板

某些情况下，可能需要清除板的所有密钥资料。这可以通过两种方法完成。第一种方法是使用硬件跳线；这种零置方法可使 Sun Crypto 加速器 4000 板恢复至其原始出厂状态（failsafe 模式）。有关说明，请参阅第 149 页 “将 Sun Crypto 加速器 4000 硬件零置为原始出厂状态”。第二种方法是使用 zeroize 命令。

注意 – zeroize 命令只能删除密钥资料，并保持所有更新的固件完好无损。此命令在成功完成时还会注销安全主管。

要使用 zeroize 命令恢复板的出厂设置，请输入以下内容：

```
vcaadm{vcaN@hostname, sec_officer}> zeroize
WARNING: Issuing this command will zeroize all keys
         on the board.  Once zeroized, these keys
         cannot be recovered unless you have
         previously backed up your master key.

Proceed with zeroize? (Y/Yes/N/No) [No]: y
All keys zeroized successfully.
```

使用 vcaadm diagnostics 命令

除 SunVTS 之外，还可以从 vcaadm 实用程序运行诊断程序。 vcaadm 中的 diagnostics 命令涉及 Sun Crypto 加速器 4000 硬件中的三个主要类别：一般硬件、加密子系统和网络子系统。一般硬件的测试包括 DRAM、闪存、 PCI 总线、 DMA 控制器和其它内部硬件。加密子系统的测试包括随机号码发生器和加密加速器。网络子系统的测试包括 vca 设备。

```
vcaadm{vcaN@hostname, sec_officer}> diagnostics
Performing diagnostic tests...Done.
Diagnostic Results
-----------------------------------------------------
General Hardware:                PASS
Cryptographic Subsystem:         PASS
Network Subsystem:               PASS
-----------------------------------------------------
```

使用 vcadiag

vcadiag 程序提供了 Sun Crypto 加速器 4000 板的命令行界面。通过此界面， root 用户无需进行安全主管身份验证即可执行管理任务。命令行选项决定 vcadiag 所执行的操作。

为了便于访问 vcadiag 程序，请在搜索路径中包含 Sun Crypto 加速器 4000 工具目录，例如：

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

vcadiag 命令行语法如下：

- vcadiag [-D] vca*N*
- vcadiag [-F] vca*N*
- vcadiag [-K] vca*N*
- vcadiag [-Q]
- vcadiag [-R] vca*N*
- vcadiag [-Z] vca*N*

注意 – 当使用 [-DFKRZ] 属性时，vca*N* 表示板的设备名称，其中 *N* 表示 Sun Crypto 加速器 4000 的设备例程号。

表 4-7 显示了 vcadiag 实用程序的选项。

表 4-7 vcadiag 选项

选项	含义
-D vca*N*	在 Sun Crypto 加速器 4000 板上运行诊断程序。
-F vca*N*	显示 Sun Crypto 加速器 4000 板为保证管理会话的安全而采用的公钥指纹。
-K vca*N*	显示 Sun Crypto 加速器 4000 板为保证管理会话的安全而采用的公钥和公钥指纹。
-Q	提供 Sun Crypto 加速器 4000 设备和软件组件的有关信息。输出是由冒号隔开的一组信息片段：设备、内部功能、密钥库名、密钥库序列号以及密钥库参考计数。您可以使用此命令确定设备和密钥库之间的关联。
-R vca*N*	重新设置 Sun Crypto 加速器 4000 板。
-Z vca*N*	零置 Sun Crypto 加速器 4000 板。

下面是使用 -D 选项的示例：

```
# vcadiag -D vca0
Running vca0 on-board diagnostics.
Diagnostics on vca0 PASSED.
```

下面是使用 -F 选项的示例：

```
# vcadiag -F vca0
5f26-b516-83b4-d254-a75f-c70d-0544-4de6
```

下面是使用 -K 选项的示例：

```
# vcadiag -K vca0
Device: vca0
Key Length: 1024 bits
Key Fingerprint: 5f26-b516-83b4-d254-a75f-c70d-0544-4de6
Modulus:
        b7215a99 8bb0dfe9 389363a0 44dac2b0 7c884161
        20ee8c8b d751437d 4e6a5cdb 76fdcb2a ad353c0b
        248edc1d 3c76591d dbca5997 f6ee8022 e8bb5a6d
        465a4f8c 601d46be 573e8681 506e5d8d f240a0db
        11d5c095 2d237061 df27b2de c353900f f531092b
        7d9a755b c5d79782 95a1180b e17303bb aca939ef
        006c73f7 74469031
Public Exponent:
        00010001
```

下面是使用 -Q 选项的示例：

```
# vcadiag -Q
vca0:cb
vca0:cb:keystore_name:83097c2b3e35ef5b:1
vca0:ca
vca0:ca:keystore_name:83097c2b3e35ef5b:1
kcl2pseudo
vca0:om
vca0:om:keystore_name:83097c2b3e35ef5b:1
libkcl
```

下面是使用 -R 选项的示例：

```
# vcadiag -R vca0
Resetting device vca0, this may take a minute.
Please be patient.
Device vca0 reset ok.
```

下面是使用 -Z 选项的示例：

```
# vcadiag -Z vca0
Zeroizing device vca0, this may take a few minutes.
Please be patient.
Device vca0 zeroized.
```

第 5 章

配置 Sun ONE 服务器软件以便与 Sun Crypto 加速器 4000 板配合使用

本章说明如何配置 Sun Crypto 加速器 4000 板以便与 Sun ONE Web 服务器配合使用。本章包括以下几节：

注意 – 本手册中所述的 Sun ONE Web 服务器此前称为 iPlanet™ Web 服务器。

Sun ONE Web 服务器的安全管理性能

本节概述了 Sun Crypto 加速器 4000 板由 Sun ONE 服务器管理时的安全性能。

注意 – 要管理密钥库，您必须对系统拥有系统管理员帐户的访问权限。

概念和术语

您必须为通过 PKCS#11 界面 （如 Sun ONE Web 服务器）与 Sun Crypto 加速器 4000 板通信的应用程序创建密钥库和用户。

在与 Sun Crypto 加速器 4000 相关的环境中，用户是指加密密钥资料的所有者。一个密钥只能由单个用户拥有，但每个用户可以拥有多个密钥。用户可能需要使用多个密钥来支持不同的配置，如生产密钥和开发密钥 （用以反映用户所支持的组织）。

注意 – 术语*用户*或*用户帐户*是指在 vcaadm 中创建的 Sun Crypto 加速器 4000 用户，而非传统的 UNIX 用户帐户。UNIX 用户名与 Sun Crypto 加速器 4000 用户名之间没有固定的一一对应关系。

密钥库是密钥资料的储存库。与密钥库信息密切相关的是安全主管和用户。密钥库不但可以存储密钥，而且还是一种用户帐户拥有密钥对象的方式。它可以使那些未通过所有者身份验证的应用程序无法看到密钥。密钥库由三部分组成：

- **密钥对象 —** 为应用程序 （如 Sun ONE Web 服务器）保存的长期密钥。
- **用户帐户 —** 这些帐户可使应用程序验证和访问特定的密钥。
- **安全主管帐户 —** 这些帐户可通过 vcaadm 访问密钥管理功能。

注意 – 每个 Sun Crypto 加速器 4000 板只能有一个密钥库。不过，多个 Sun Crypto 加速器 4000 板可以共同使用同一个密钥库，以便提供额外的性能和容错功能。

在典型安装中，将会创建一个密钥库，并且该库只有一位用户。例如，此类配置可以由单个密钥库 *web_server* 和该密钥库中的单个用户 *web_admin* 组成。用户 *web_admin* 对该密钥库中的服务器密钥拥有访问控制权限，并可对这些权限进行维护。

管理工具 vcaadm 用于管理 Sun Crypto 加速器 4000 的密钥库和用户。有关说明，请参阅第 59 页 “通过 vcaadm 管理密钥库”。

令牌和令牌文件

*密钥库*以*令牌*的形式呈现给 Sun ONE Web 服务器。令牌文件是 Sun Crypto 加速器 4000 管理员选择性地向给定应用程序提供特定令牌的技术。

示例

现有三个密钥库，分别为 *engineering （工程）*、*finance （金融）*和 *legal （法律）*密钥库。此时，需要向 Sun ONE Web 服务器提供以下令牌：

- `engineering`
- `finance`
- `legal`

令牌文件

要改写默认情况，必须要有令牌文件。某些应用程序无法处理多个令牌。令牌文件是包含一个或多个令牌名 （每行一个）的文本文件。

注意 – 令牌名与密钥库名相同。

Sun ONE Web 服务器仅提供令牌文件中列出的令牌。指定令牌文件的方法如下 （按优先顺序排列）：

1. 由环境变量 `SUNW_PKCS11_TOKEN_FILE` 命名的文件

   某些应用程序软件禁止使用环境变量。此情况下，不能采用这种方法。

2. 文件 `$HOME/.SUNWconn_cryptov2/tokens`

   此文件必须位于运行 Sun ONE Web 服务器时所用的 UNIX 用户的主目录下。当 Sun ONE Web 服务器运行时所用的 UNIX 用户没有主目录时，不能使用这种方法。

3. 文件 `/etc/opt/SUNWconn/cryptov2/tokens`

如果不存在任何令牌文件 , Sun Crypto 加速器 4000 软件将会向 Sun ONE Web 服务器提供所有令牌。

下面是令牌文件内容的示例：

```
==============================
# This is an example token file

engineering # Comments are acceptable on the same line

legal

# Because the finance keystore is not listed, the Sun Crypto
# Accelerator will not present it to the Sun ONE Web Server.

...
==============================
```

注意 – 文件中的注释内容以井字符 (#) 开头，且允许存在空行。

如果找不到本节介绍的任何文件，则采用第 74 页 “令牌和令牌文件”中所述的默认方法。

启动和禁用批量加密

默认情况下，系统已禁用了 SunONE 服务器软件的批量加密功能。有时，您可能需要启用此功能以便安全传送较大的文件。

要使 Sun ONE 服务器软件可以使用 Sun Crypto 加速器 4000 板上的批量加密功能，您只需在 `/etc/opt/SUNWconn/cryptov2/` 目录中创建一个名为 `sslreg` 的空文件，然后重新启动服务器软件。

```
# touch /etc/opt/SUNWconn/cryptov2/sslreg
```

要禁用批量加密功能，您必须删除 `sslreg` 文件，然后重新启动服务器软件。

```
# rm /etc/opt/SUNWconn/cryptov2/sslreg
```

配置 Sun ONE Web 服务器

本节介绍以下内容：

密码

在启用 Sun ONE Web 服务器 的过程中，系统会要求您提供几个密码。表 5-1 对每个密码进行了说明。本章介绍的各个过程会用到这些密码。如果不清楚应该使用哪个密码，请参见表 5-1。

表 5-1 Sun ONE Web 服务器所需的密码

密码类型	说明
Sun ONE Web 服务器管理服务器	启动 Sun ONE Web 服务器管理服务器时需要提供此密码。此密码在设置 Sun ONE Web 服务器期间指定。
Web 服务器信任数据库	在安全模式下启动内部加密模块时需要提供此密码。此密码是在通过 Sun ONE Web 服务器管理服务器创建信任数据库时指定的。此外，在申请证书并将其安装到内部加密模块时也要求提供该密码。
安全主管	执行 `vcaadm` 权限操作时需要提供此密码。
username:password	在安全模式下启动 Sun Crypto 加速器 4000 模块时需要提供此密码。此外，在申请证书并将其安装到内部加 密模块 (*keystore_name*) 时也需提供此密码。此密码包括在 `vcaadm` 中创建的密钥库用户的 *username*（*用户名*）和 *password*（*密码*）。密钥库 *username*（*用户名*）和 *password*（*密码*）以冒号 (:) 隔开。

填充密钥库

启用与 Sun ONE Web 服务器配合使用的板之前，您必须先将此板初始化，然后向此板的密钥库中添加至少一位用户。板的密钥库是在初始化过程中创建的。另外，您也可以对 Sun Crypto 加速器 4000 板进行初始化，使之使用现有的密钥库。有关说明，请参阅第 56 页 “通过 `vcaadm` 初始化 Sun Crypto 加速器 4000 板”。

注意 – 每个 Sun Crypto 加速器 4000 板仅能配置一个密钥库，您必须为每个板配置一个密钥库。不过，多个 Sun Crypto 加速器 4000 板可以配置为共同使用同一个密钥库，以便提供其它性能和容错功能。

▼ 填充密钥库

1. **将 Sun Crypto 加速器 4000 工具目录放入您的搜索路径（如果尚未这样做），例如：**

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

2. **使用** `vcaadm` **命令访问** `vcaadm` **实用程序，或输入** `vcaadm -h` *hostname* **将** `vcaadm` **连接至远程主机上的板。**

   参阅第 47 页 “使用 vcaadm”。

```
$ vcaadm -h hostname
```

3. **向板的密钥库中添加用户。**

   这些用户名仅在 Sun Crypto 加速器 4000 板的域中被识别，而且不必与 Web 服务器进程所用的 UNIX 用户名相同。请注意，在尝试创建用户之前，必须先以 `vcaadm` 安全主管的身份登录。

4. **运行** `create user` **命令创建用户。**

```
vcaadm{vcaN@hostname, sec_officer}> create user username
Initial password:
Confirm password:
User username created successfully.
```

   此处创建的 *username （用户名）*和 *password （密码）*共同组成了 *username:password*（参见表 5-1）。在 Web 服务器启动期间进行验证时，必须使用此密码。这是单个用户的密钥库密码。

警示 – 用户必须记住此 *username:password*。没有密码，用户将无法访问自己的密钥。丢失的密码无法找回。

5. **退出** `vcaadm`。

```
vcaadm{vcaN@hostname, sec_officer}> exit
```

启用 Sun ONE Web 服务器概述

要启用 Sun ONE Web 服务器，必须完成以下步骤。接下来的两节将对这些步骤进行详细说明。

- 安装 Sun ONE Web 服务器。
- 创建信任数据库。
- 申请证书。
- 安装证书。
- 配置 Sun ONE Web 服务器。

警示 – 这些步骤必须按指定的顺序进行。否则，则可能导致配置错误。

- 如果您使用 Sun ONE Web 服务器 4.1，请转至第 79 页“安装和配置 Sun ONE Web 服务器 4.1”。
- 如果您使用 Sun ONE Web 服务器 6.0，请转至第 88 页“安装和配置 Sun ONE Web 服务器 6.0”。

安装和配置 Sun ONE Web 服务器 4.1

本部分介绍如何安装和配置 Sun ONE Web 服务器 4.1，包括以下几节：

安装 Sun ONE Web 服务器 4.1

您必须按顺序执行这些步骤。有关使用 Sun ONE Web 服务器的详细信息，请参阅 Sun ONE Web 服务器文档。

▼ 安装 Sun ONE Web 服务器 4.1

1. **下载 Sun ONE Web 服务器 4.1 软件。**

   您可从以下 URL 找到该 Web 服务器软件：`http://www.sun.com/`

2. **安装 Web 服务器。**

   本节采用一个示例加以说明，您可根据需要对 Sun ONE Web 服务器进行不同的配置。服务器的默认路径名为：`/usr/netscape/server4`

   请在 Sun ONE Web 服务器安装期间接受默认路径。本文档中使用此默认路径。如果您想将 Web 服务器软件安装在不同的位置，请记住其安装位置。

3. **运行 `setup` 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. **输入完整的 *hostname.domain*。**

   c. **输入两次 Sun ONE Web 服务器 4.1 管理服务器的密码。**

   d. **提示时，按回车键。**

▼ 创建信任数据库

1. **启动 Sun ONE Web 服务器 4.1 管理服务器。**

   使用以下命令来启动 Sun ONE Web 服务器 4.1 管理服务器（而不要将 `startconsole` 作为 `setup` 请求运行）：

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

   此响应提供了用于连接到管理服务器的 URL。

2. **通过打开 Web 浏览器并输入以下内容来启动管理图形用户界面 (GUI)：**

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

   在验证对话框中，输入您在运行 `setup` 时选择的 Sun ONE Web 服务器 4.1 管理服务器用户名及密码。

注意 – 如果您在设置 Sun ONE Web 服务器期间使用的是默认设置，则在用户 ID 或 Sun ONE Web 服务器 4.1 管理服务器用户名字段中键入 `admin`。

---

3. **选择 OK（确定）。**

   屏幕上会显示 Sun ONE Web 服务器 4.1 管理服务器窗口。

4. **创建 Web 服务器例程的信任数据库。**

   a. **在 Sun ONE Web 服务器 4.1 管理服务器窗口中选择 Servers（服务器）选项卡。**

   b. **选择所需的服务器，然后选择 Manage（管理）按钮。**

   c. **选择靠近页首的 Security（安全）选项卡，然后选择 Create Database（创建数据库）链接。**

   d. **在两个对话框中输入密码（Web 服务器信任数据库；参见**表 5-1**），然后选择 OK（确定）。**

      选择一个至少包含 8 个字符的密码。 Sun ONE Web 服务器在安全模式下运行时，将使用此密码来启动内部加密模块。

      您可能想对多个 Web 服务器例程启用安全保护功能。如果是这样，请对每一个 Web 服务器例程重复步骤 1 至 步骤 4。

注意 – 如果您还想在 Sun ONE Web 服务器 4.1 管理服务器上运行安全套接层 (SSL) 功能，则此过程与设置信任数据库的过程类似。有关详情，请参阅 `http://docs.sun.com` 网站上的 《*iPlanet Web Server, Enterprise Edition Administrator's Guide*》。

5. **执行以下脚本启用 Sun Crypto 加速器 4000 板：**

```
# /opt/SUNWconn/bin/iplssslcfg
```

此脚本会提示您选择 Web 服务器。它将为 Sun ONE Web 服务器安装 Sun Crypto 加速器 4000 加密模块。然后，脚本会更新配置文件以启用 Sun Crypto 加速器 4000 板。

6. **键入 `1`，配置 Sun ONE Web 服务器以使用 SSL，然后按回车键。**

```
Sun Crypto Accelerator Sun ONE Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for Sun ONE Products.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Sun ONE Web Server for SSL
2. Configure Sun ONE Application Server for SSL
3. Export Sun ONE Web Server keys to PKCS#12 format
4. Import keys from PKCS#12 format for Sun ONE Web Server

Your selection (0 to quit): 1
```

7. **提示时，输入 Web 服务器根目录的路径，然后按回车键。**

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

8. **如果要继续操作，请在提示时键入** `y` **并按回车键。**

```
This script will update your Sun ONE 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/N]: y

Using database directory /usr/netscape/server4/alias...
Module "Sun Crypto Accelerator 4000" 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. **键入以下命令，重新启动 Sun ONE Web 服务器 4.1 管理服务器：**

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

此响应提供了用于连接到管理服务器的 URL。

2. **通过打开 Web 浏览器并输入以下地址来启动管理 GUI：**

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

在验证对话框中，输入您在运行 `setup` 命令时选择的 Sun ONE Web 服务器 4.1 管理服务器用户名及密码。

注意 – 如果您在设置 Sun ONE Web 服务器期间使用的是默认设置，则在用户 ID 或 Sun ONE Web 服务器 4.1 管理服务器用户名字段中键入 `admin`。

---

3. **选择 OK（确定）。**

屏幕上会显示 Sun ONE Web 服务器 4.1 管理服务器窗口。

4. **要申请服务器证书，请选择 Sun ONE Web 服务器 4.1 管理服务器窗口顶部附近的 Security （安全）选项卡** （图 5-1）。

   屏幕上会显示 Create Trust Database （创建信任数据库）页面。

5. **选择左窗格中的 Request a Certificate （申请证书）链接** （图 5-1）。

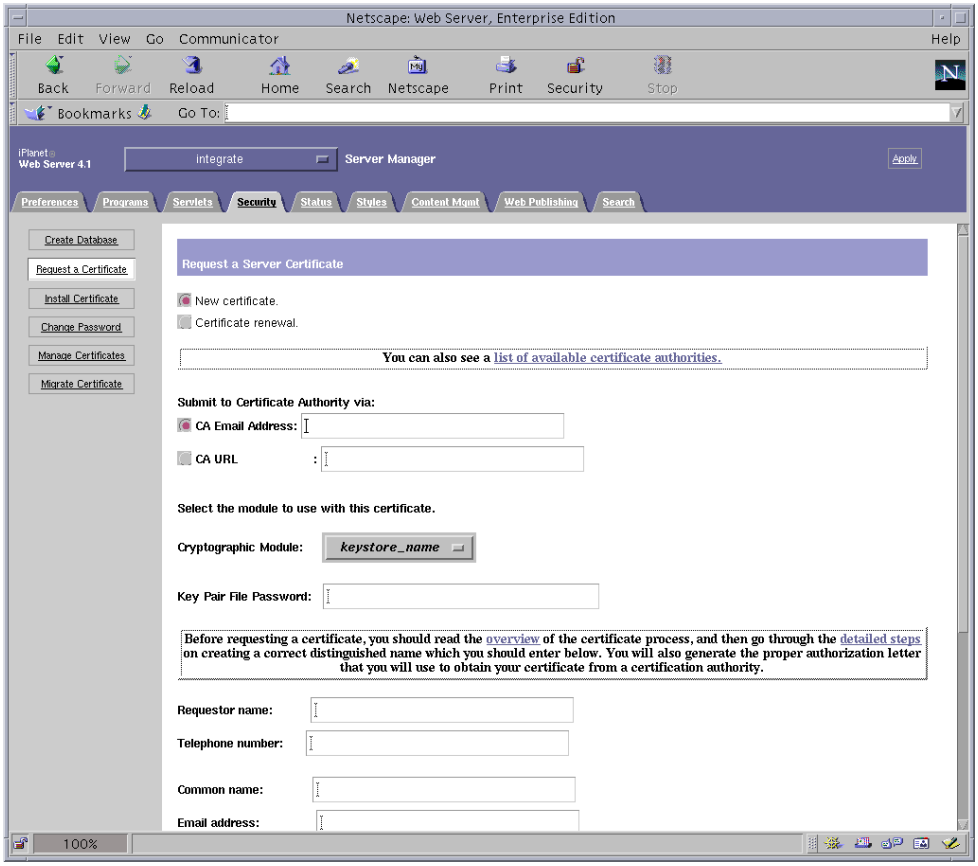

图 5-1 Sun ONE Web 服务器 4.1 管理服务器的申请服务器证书页面

6. **使用以下信息填写表单以生成证书申请：**

   a. **选择 New Certificate （新证书）。**

      如果您可以直接将证书申请发送到可通过 Web 访问的证书机构或注册机构，请选择“CA URL”链接。否则，请选择 CA Email Address （CA 电子邮件地址），然后输入您要将证书申请发送至的电子邮件地址。

   b. **选择您要使用的加密模块。**

      此下拉菜单中包含每一个密钥库的条目。务必选择正确的密钥库。请不要只选择 SUNW 加速。

c. 在 Key Pair File Password （密钥对文件密码）对话框中，为将要拥有密钥的用户输入密码。

此密码为 *username:password* （表 5-1）。

d. 在以下申请人字段中输入正确的信息：

表 5-2 申请人信息字段

字段	说明
Requestor Name （申请人姓名）	申请人的联系信息
Telephone Number （电话号码）	申请人的联系信息
Common Name （通用名称）	在来访者的浏览器 *hostname.domain* 中键入的 Web 站点域
Email Address （邮件地址）	申请人的联系信息
Organization （组织）	将在证书上声明的组织
Organizational Unit （组织单位）	（可选）将在证书上声明的组织单位
Locality （地区）	（可选）城市、郡县、公国或国家/地区，如果提供也会在证书上予以声明
State （省/州）	（可选）省/州的全称
Country （国家/地区）	由两个字母组成的国家/地区 ISO 代码 （例如，中国为 CN）

e. 选择 OK （确定）按钮提交信息。

7. 利用证书机构生成证书。

- 如果选择将证书申请发送给 CA URL，则证书申请会自动发送到该处。
- 如果选择 CA Email Address （CA 电子邮件地址），请复制通过电子邮件发给您的证书申请及标题，然后将其交给证书机构。

8. 一旦生成证书，请将证书及标题一起复制到剪贴板上。

注意 – 证书通常以文本格式向您提供，这与证书申请不同。请将此数据保留在剪贴板上，以便在下一节的步骤 5 中使用。

▼ 安装服务器证书

1. **选择 Sun ONE Web 服务器 4.1 管理服务器窗口左侧的 Install Certificate （安装证书）链接。**

   一旦证书机构批准您的申请并签发证书，您必须将证书安装在 Sun ONE Web 服务器中。

2. **选择 Security （安全）选项卡。**

3. **在左窗格中，选择 Install Certificate （安装证书）链接。**

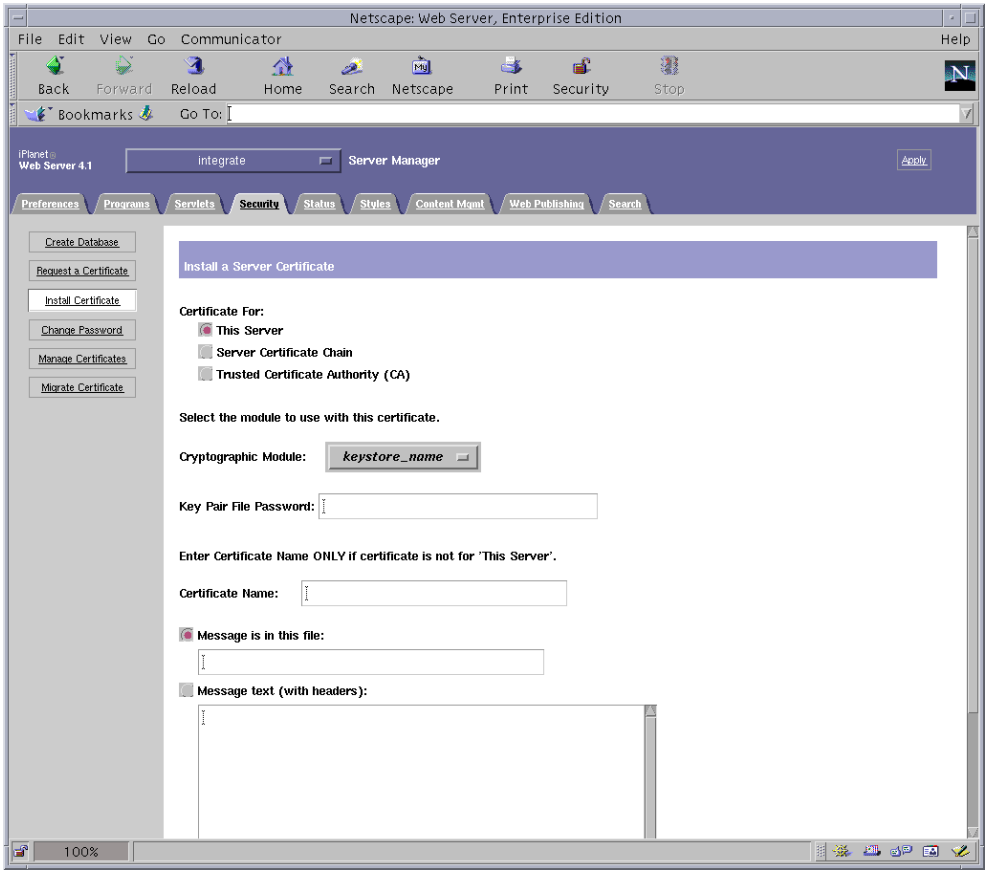

图 5-2 Sun ONE Web 服务器 4.1 管理服务器的安装服务器证书页面

4. **填写表单，安装证书：**

表 5-3 要安装证书的字段

字段	说明
Certificate For（证书适用对象）	本服务器。
Cryptographic Module （加密模块）	此下拉菜单中包含每一个密钥库的条目。请务必选择正确的密钥库名称。要使用 Sun Crypto 加速器 4000，必须选择与密钥库名称相同的模块。
Key Pair File Password （密钥对文件密码）	此密码为 *username:password* （表 5-1）。
Certificate Name（证书名称）	多数情况下，您可以将此字段留空。如果提供一个名称，该名称将会改变 Web 服务器在 SSL 模式下运行时用来访问证书和密钥的名称。此字段的默认值为 `Server-Cert`。

5. **将从证书机构复制的证书 （第 82 页 “生成服务器证书” 的步骤 8）粘贴到 Message （消息）框内。**

   屏幕上会显示证书的一些基本信息。

6. **选择该页底部的 OK （确定）按钮。**

7. **如果输入的内容正确无误，请选择 Add Server Certificate （添加服务器证书）按钮。**

   屏幕上会显示一则消息，通知您重新启动服务器。由于 Web 服务器例程一直处于关闭状态，因此不必重新启动服务器。

   另外，系统还会通知您，为使 Web 服务器使用 SSL，必须对 Web 服务器进行相应配置。请执行下面的步骤来配置 Web 服务器。

配置 Sun ONE Web 服务器 4.1 以使用 SSL

现在，您已安装了 Web 服务器和服务器证书，不过，您必须对 Web 服务器进行配置才能使用 SSL。

▼ 配置 Sun ONE Web 服务器 4.1

1. **从 Sun ONE Web 服务器 4.1 管理服务器主页上，选择您要与 SSL 一起使用的 Web 服务器例程，然后选择 Manage （管理）。**

2. **选择该页顶部的 Preferences （首选项）选项卡 （如果尚未选定）。**

3. **选择该页左侧的 Encryption On/Off （加密开启/关闭）链接。**

4. **将加密设为 On （开启）。**

   对话框中的 Port （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。

5. **选择 OK （确定）按钮。**

6. **选择 Save （保存）按钮，应用这些更改。**

   现在， Web 服务器即可在安全模式下运行。

7. **打开** `/usr/netscape/server4/https-`*hostname*`/config/magnus.conf` **文件（***hostname* **是 Web 服务器的名称），在其中添加下面的行：**

   ```
   CERTDefaultNickname keystore_name:Server-Cert
   ```

   默认情况下，您生成的证书名为 `Server-Cert`。如果您的证书采用其它名称，请务必用您选择的名称代替 `Server-Cert`。

8. **选择您要管理的服务器，然后选择该页右上角的 Apply （应用）按钮。**

   此选项会将更改应用于整个 Sun ONE Web 服务器 4.1 管理服务器。

9. **选择 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。**

   屏幕上会显示一个允许您启动 Web 服务器例程的页面。

   如果您在服务器关闭时选择 Apply Changes （应用更改）按钮，则会出现一个验证对话框，提示您输入 *username:password*。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。

   该问题有两种解决办法：

   - 改选 Load Configuration Files （加载配置文件）。
   - 先启动 Web 服务器，然后选择 Apply Changes （应用更改）按钮。

10. **在 Sun ONE Web 服务器 4.1 管理服务器窗口中，选择窗口左侧的 On/Off 链接。**

11. **输入服务器密码，然后选择 OK （确定）按钮。**

    系统会提示您输入一个或多个密码。出现 Module Internal （内部模块）提示时，请输入 Web 服务器信任数据库的密码。

    出现模块 *keystore_name* 提示时，请输入该密钥库的 *username:password*。

    出现其它密钥库的提示时，请输入相应的 *username:password*。

12. **在下面的 URL 上验证已启用 SSL 的新 Web 服务器：**

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

注意 – 默认 *server_port* 为 443。

安装和配置 Sun ONE Web 服务器 6.0

本部分介绍如何启用 Sun Crypto 加速器 4000 板以便与 Sun ONE 6.0 Web 服务器配合使用。本部分包括以下内容：

- 第 88 页 “安装 Sun ONE Web 服务器 6.0”
- 第 95 页 “配置 Sun ONE Web 服务器 6.0 以使用 SSL”

安装 Sun ONE Web 服务器 6.0

您必须按顺序执行这些步骤。有关使用 Sun ONE Web 服务器的详细信息，请参阅 Sun ONE Web 服务器文档。

▼ 安装 Sun ONE Web 服务器 6.0

1. **下载 Sun ONE Web 服务器 6.0 软件。**

   您可从以下 URL 找到该 Web 服务器软件：`http://www.sun.com/`

2. **安装 Web 服务器。**

   本节采用一个示例加以说明，您可根据需要对 Sun ONE Web 服务器进行不同的配置。服务器的默认路径名为：`/usr/iplanet/servers`

   请在 Sun ONE 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。如果您想将软件安装在不同的位置，请记住其安装位置。

3. **运行 `setup` 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. **输入全整的 *hostname.domain*。**

   c. **输入两次 Sun ONE Web 服务器 6.0 管理服务器的密码。**

   d. **提示时，按回车键。**

▼ 创建信任数据库

1. **启动 Sun ONE Web 服务器 6.0 管理服务器。**

   要启动 Sun ONE Web 服务器 6.0 管理服务器，请使用以下命令 （而不要将 `startconsole` 作为 `setup` 请求运行）：

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

   此响应提供了用于连接到管理服务器的 URL。

2. **通过打开 Web 浏览器并输入以下地址来启动管理 GUI:**

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

   在验证对话框中，输入您在运行 `setup` 时选择的 Sun ONE Web 服务器 6.0 管理服务器用户名及密码。

注意 – 如果您在设置 Sun ONE Web 服务器期间使用的是默认设置，则在用户 ID 或 Sun ONE Web 服务器 6.0 管理服务器用户名字段中键入 `admin`。

---

3. **选择 OK （确定）。**

   屏幕上会显示 Sun ONE Web 服务器 6.0 管理服务器窗口。

4. **创建 Web 服务器例程的信任数据库。**

   您可能想对多个 Web 服务器例程启用安全保护功能。如果是这样，请对每一个 Web 服务器例程重复步骤 1 至 步骤 4。

注意 – 如果您还想在 Sun ONE Web 服务器 6.0 管理服务器上运行 SSL 功能，则此过程与设置信任数据库的过程类似。有关详情，请参阅 `http://docs.sun.com` 网站上的《*iPlanet Web Server, Enterprise Edition Administrator's Guide*》。

---

   a. **在 Sun ONE Web 服务器 6.0 管理服务器窗口中选择 Servers （服务器）选项卡。**

   b. **选择所需的服务器，然后选择 Manage （管理）按钮。**

   c. **选择靠近页首的 Security （安全）选项卡，然后选择 Create Database （创建数据库）链接。**

d. 在两个对话框中输入密码 （Web 服务器信任数据库 [表 5-1]），然后选择 OK （确定）。

选择一个至少包含 8 个字符的密码。 Sun ONE Web 服务器在安全模式下运行时，将使用此密码来启动内部加密模块。

5. 执行以下脚本启用 Sun Crypto 加速器 4000 板：

```
# /opt/SUNWconn/crypto/bin/iplsslcfg
```

此脚本会提示您选择 Web 服务器。它将为 Sun ONE Web 服务器安装 Sun Crypto 加速器 4000 加密模块。然后，脚本会更新配置文件以启用 Sun Crypto 加速器 4000 板。

6. 键入 1，配置 Sun ONE Web 服务器以使用 SSL，然后按回车键。

```
Sun Crypto Accelerator Sun ONE Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for Sun ONE Products.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Sun ONE Web Server for SSL
2. Configure Sun ONE Application Server for SSL
3. Export Sun ONE Web Server keys to PKCS#12 format
4. Import keys from PKCS#12 format for Sun ONE Web Server

Your selection (0 to quit): 1
```

7. 提示时，输入 Web 服务器根目录的路径，然后按回车键。

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

8. **如果要继续操作，请在提示时键入** `y` **并按回车键。**

```
This script will update your Sun ONE 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/N]: y

Using database directory /usr/iplanet/servers/alias...
Module "Sun Crypto Accelerator 4000" 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. **键入以下命令，重新启动 Sun ONE Web 服务器 6.0 管理服务器：**

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

此响应提供了用于连接到管理服务器的 URL。

2. **通过打开 Web 浏览器并输入以下地址来启动管理 GUI：**

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

在验证对话框中，输入您在运行 `setup` 时选择的 Sun ONE Web 服务器 6.0 管理服务器用户名及密码。

注意 – 如果您在设置 Sun ONE Web 服务器期间使用的是默认设置，则在用户 ID 或 Sun ONE Web 服务器 6.0 管理服务器用户名字段中键入 `admin`。

---

3. **选择 OK（确定）。**

屏幕上会显示 Sun ONE Web 服务器 6.0 管理服务器窗口。

4. **要申请服务器证书，请选择 Sun ONE Web 服务器 6.0 管理服务器窗口顶部附近的 Security（安全）选项卡。**

屏幕上会显示 Create Trust Database （创建信任数据库）窗口。

5. **选择 Sun ONE Web 服务器 6.0 管理服务器窗口左侧的 Request a Certificate （申请证书）链接。**

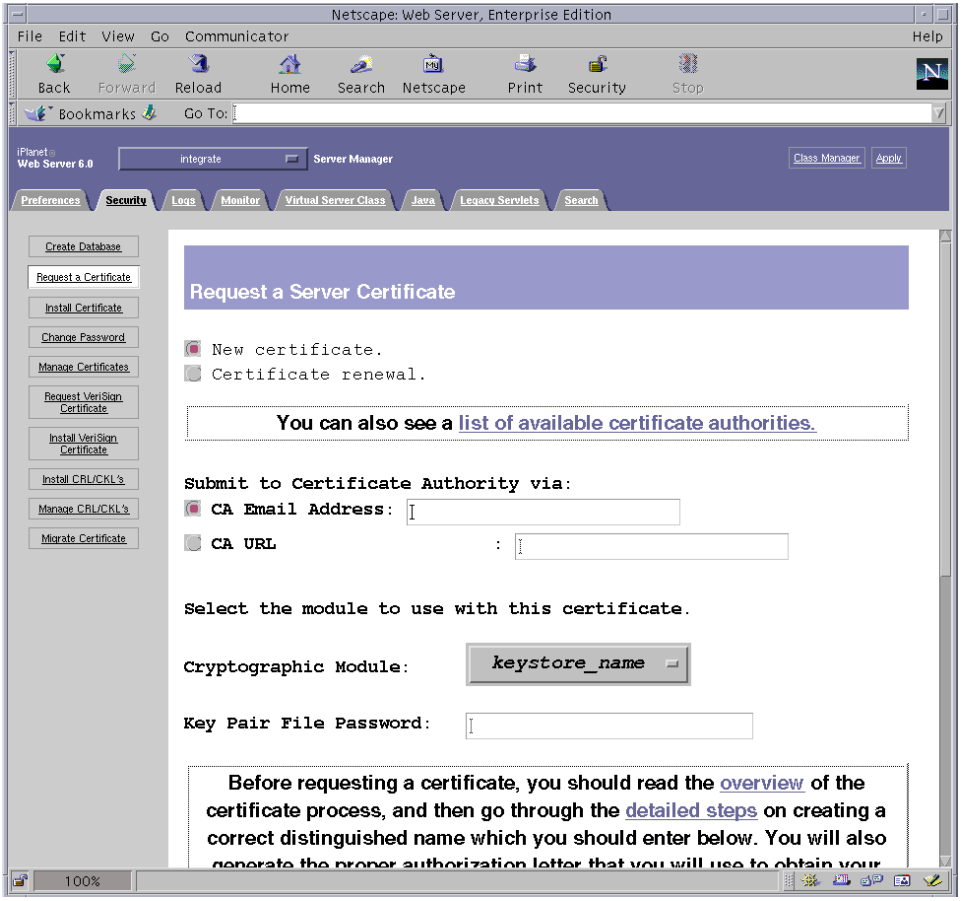

图 5-3 Sun ONE Web 服务器 6.0 管理服务器的申请服务器证书页面

6. **使用以下信息填写表单以生成证书申请：**

   a. **选择 New Certificate （新证书）。**

   如果您可以直接将证书申请发送到可通过 Web 访问的证书机构或注册机构，请选择“CA URL”链接。否则，请选择 CA Email Address （CA 电子邮件地址），然后输入您要将证书申请发送至的电子邮件地址。

   b. **选择您要使用的加密模块。**

   此下拉菜单中包含每一个密钥库的条目。务必选择正确的密钥库。请不要只选择 SUNW 加速。

c. 在 Key Pair File Password （密钥对文件密码）对话框中，为将要拥有密钥的用户输入密码。

此密码为 *username:password* （表 5-1）。

d. 在以下申请人字段中输入正确的信息：

表 5-4 申请人信息字段

字段	说明
Requestor Name （申请人姓名）	申请人的联系信息
Telephone Number （电话号码）	申请人的联系信息
Common Name （通用名称）	在来访者的浏览器 *hostname.domain* 中键入的 Web 站点域
Email Address （邮件地址）	申请人的联系信息
Organization （组织）	将在证书上声明的组织
Organizational Unit （组织单位）	（可选）将在证书上声明的组织单位
Locality （地区）	（可选）城市、郡县、公国或国家/地区，如果提供也会在证书上予以声明
State （省/州）	（可选）省/州的全称
Country （国家/地区）	由两个字母组成的国家/地区 ISO 代码 （例如，中国为 CN）

e. 选择 OK （确定）按钮提交信息。

7. 利用证书机构生成证书。

- 如果选择将证书申请发送给 CA URL，则证书申请会自动发送到该处。
- 如果选择 CA Email Address （CA 电子邮件地址），请复制通过电子邮件发给您的证书申请及标题，然后将其交给证书机构。

8. 一旦生成证书，请将证书及标题一起复制到剪贴板上。

注意 – 证书通常以文本格式向您提供，这与证书申请不同。请将此数据保留在剪贴板上，以便在第 94 页 “安装服务器证书”的步骤 5 中使用。

▼ 安装服务器证书

1. **选择 Sun ONE Web 服务器 6.0 管理服务器窗口左侧的 Install Certificate （安装证书）链接。**

   一旦证书机构批准您的申请并签发证书，您必须将证书安装在 Sun ONE Web 服务器中。

2. **选择 Security （安全）选项卡。**

3. **在左窗格中，选择 Install Certificate （安装证书）链接。**

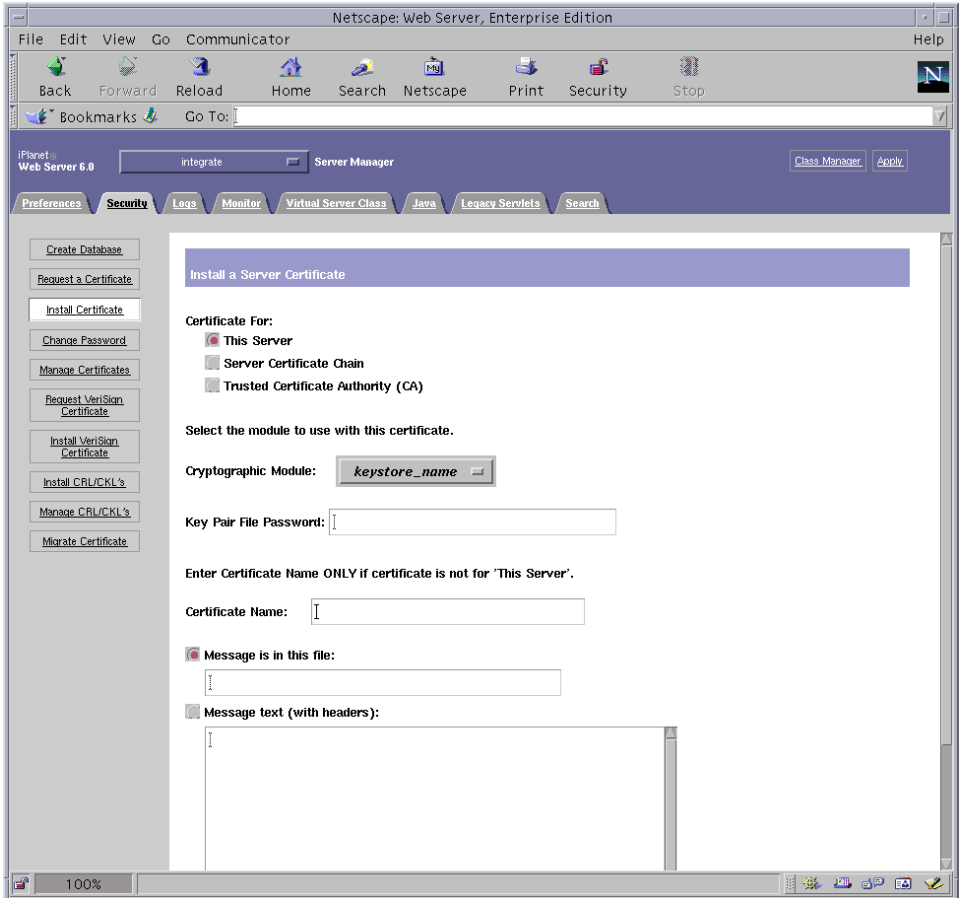

图 5-4 Sun ONE Web 服务器 6.0 管理服务器的安装服务器证书页面

4. **填写表单，安装证书：**

表 5-5 要安装证书的字段

字段	说明
Certificate For（证书适用对象）	本服务器。
Cryptographic Module（加密模块）	此下拉菜单中包含每一个密钥库的条目。务必选择正确的密钥库名称。要使用 Sun Crypto 加速器 4000，必须选择一个格式为 *keystore_name* 的模块。
Key Pair File Password（密钥对文件密码）	此密码为 *username:password*（表 5-1）。
Certificate Name（证书名称）	多数情况下，您可以将此字段留空。如果提供一个名称，该名称将会改变 Web 服务器在 SSL 模式下运行时用来访问证书和密钥的名称。此字段的默认值为 `Server-Cert`。

5. **将从证书机构复制的证书（第 91 页 “生成服务器证书” 的步骤 8）粘贴到 Message（消息）文本框内。**

   屏幕上会显示证书的一些基本信息。

6. **选择该页底部的 OK（确定）按钮。**

7. **如果输入的内容正确无误，请选择 Add Server Certificate（添加服务器证书）按钮。**

   屏幕上会显示一则消息，通知您重新启动服务器。由于 Web 服务器例程一直处于关闭状态，因此不必重新启动服务器。

   另外，系统还会通知您，为使 Web 服务器使用 SSL，必须对 Web 服务器进行相应配置。请执行下面的步骤来配置 Web 服务器。

配置 Sun ONE Web 服务器 6.0 以使用 SSL

现在，您已安装了 Web 服务器和服务器证书，不过，您必须对 Web 服务器进行配置才能使用 SSL。

▼ 配置 Sun ONE Web 服务器 6.0

1. **选择页首附近的 Preferences（首选项）选项卡。**

2. **在左窗格中选择 Edit Listen Sockets（编辑监听套接口）链接。**

   主窗格中将会列出 Web 服务器例程的所有监听套接口。

a. 更改以下字段：

- **Port （端口）：** 设置为您要运行已启用 SSL 的 Web 服务器的端口 （通常为端口 443）。
- **Security （安全）：** 设置为 On。

b. 选择 OK （确定）按钮应用这些更改。

现在， Edit Listen Sockets （编辑监听套接口）页面的安全字段中应显示了一个 Attributes （属性）链接。

3. **选择 Attributes （属性）链接。**
4. **输入 *username:password*，在系统上验证密钥库。**
5. **如果您想更改一组默认密码，请在 Ciphers （密码）标题下面选择所需的密码组。**

屏幕上会显示用于更改密码设置的对话框。您可以选择 Cipher Default （默认密码）设置、 SSL2 或 SSL3/TLS （传输层安全）。如果您选择 Cipher Default （默认密码），则不会显示默认设置。其它两个选项需要您在弹出式对话框中选择要启用的算法。有关密码选项，请参阅 Sun ONE 文档。

6. **为密钥库选择后跟：`Server-Cert` 的证书 （如果不同，则使用您选择的名称）。**

Certificate Name （证书名）字段中仅显示相应密钥库用户所拥有的密钥。此密钥库用户是指使用 *username:password* 验证的用户。

7. **选择证书并确认所有安全设置均正确无误后，选择 OK （确定）按钮。**
8. **选择右上角的 Apply （应用）链接，以便在启动服务器之前应用这些更改。**
9. **选择 Load Configuration Files （加载配置文件）链接应用更改。**

屏幕上会显示一个允许您启动 Web 服务器例程的页面。

如果您在服务器关闭时选择 Apply Changes （应用更改）按钮，则会出现一个验证对话框，提示您输入 *username:password*。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。

该问题有两种解决办法：

- 改选 Load Configuration Files （加载配置文件）。
- 先启动 Web 服务器，然后选择 Apply Changes （应用更改）按钮。

10. **在 Sun ONE Web 服务器 6.0 管理服务器窗口中，选择窗口左侧的 On/Off 链接。**
11. **输入服务器密码，然后选择 OK （确定）按钮。**

系统会提示您输入一个或多个密码。出现 Module Internal （内部模块）提示时，请输入 Web 服务器信任数据库的密码。

出现模块 *keystore_name* 提示时，请输入 *username:password*。

出现其它密钥库的提示时，请输入相应的 *username:password*。

12. **在下面的 URL 上验证已启用 SSL 的新 Web 服务器：**
    `https://hostname.domain:server_port/`

注意 – 默认 *server_port* 为 443。

第 6 章

配置 Apache Web 服务器以便与 Sun Crypto 加速器 4000 板配合使用

本章介绍如何配置与 Sun Crypto 加速器 4000 板配合使用的 Apache Web 服务器，包括以下几节：

警示 – 配置 Apache Web 服务器时，不要让它与 Sun Crypto 加速器 1000 板和 Sun Crypto 加速器 4000 同时配合使用。如果让这两个板同时使用 Apache Web 服务器，Apache 将无法正常工作。

如果您要使用 Apache Web 服务器，则还必须安装修补程序 109234-09。添加 `SUNWkcl2a` 软件包后，系统将会配有 Apache Web 服务器 mod_ssl 1.3.26。

注意 – 默认情况下，系统已为 Apache Web 服务器软件启用了批量加密功能，且不能禁用。

为 Apache Web 服务器启用板

本节简要介绍如何启用 Apache Web 服务器以便与 Sun Crypto 加速器 4000 板配合使用。

启用 Apache Web 服务器

要使用 Sun Crypto 加速器 4000 板时，必须安装 Apache Web 服务器 1.3.26 或更新版本。以下说明适用于 Apache Web 服务器 1.3.26 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` 文件通常位于 `/etc/apache` 目录下。您可以将此文件用作模板并进行如下复制：

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

2. **在** `httpd.conf` **文件中将** `ServerName` **替换为您的服务器名**。

3. **启动** `apsslcfg`。

```
# /opt/SUNWconn/cryptov2/bin/apsslcfg
```

4. **选择** `1`，**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 Apache.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Apache for SSL
2. Work with Apache keys

Your selection (0 to quit): 1
```

5. **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
```

6. **提供 Apache 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
```

7. **为系统创建 RSA 密钥对。**

   如果您现在不创建密钥对，则以后必须返回并使用 apsslcfg 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 102 页 “创建证书”。

8. **提供用于存储密钥的目录。**

   如果提供的目录不存在，则系统会创建该目录。

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

9. **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、证书申请文件和稍后的证书文件。

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

10. **提供长度介于 512 和 2048 位之间的密钥。**

    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，如果您愿意，也可选择更安全的密钥。

```
What size would you like the RSA key to be [1024]? 1024
Using configuration from /opt/SUNWconn/cryptov2/ssl/openssl.cnf
Generating a 1024 bit RSA private key
........++++++
.....................................................++++++
writing new private key to /etc/apache/keys/base_name
```

11. **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，将无法访问您的密钥。

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

警示 – 必须记住输入的密码。没有密码，就无法访问您的密钥。丢失的密码无法找回。

创建证书

以下步骤介绍如何为使用 Sun Crypto 加速器 4000 板的 Apache Web 服务器创建必要的证书。

▼ 创建证书

1. **使用您在第 100 页 “启用 Apache Web 服务器”中创建的密钥来创建证书申请。**

   您必须先输入密码才能访问密钥，然后为以下字段提供正确信息：

   - Country Name （国家/地区名称）：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 （例如，中国是 CN）
   - State or Province Name （州或省名称）：（可选）在本字段中填写州/省的全称 （或键入圆点(.) 然后按回车键）
   - Locality （地点）：（可选）城市、郡县、公国或国家/地区，如果提供，也会在证书上予以声明
   - Organization Name （组织名称）：将在证书上声明的组织名称
   - Organizational Unit Name （组织单位名称）：（可选）将在证书上声明的组织单位名称

- SSL Server Name（SSL 服务器名称）：在来访者的浏览器中键入的 Web 站点域
- Email Address（电子邮件地址）：申请人的联系信息

下面是如何输入证书字段的示例：

```
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. **按照说明修改** `/etc/apache/httpd.conf` **文件**。

   屏幕上会显示有关您的密钥和证书文件的信息。另外，还会指导您如何修改 `/etc/apache/httpd.conf` 文件以便与 Sun Crypto 加速器 4000 软件配合使用。

```
The keyfile is stored in /etc/apache/keys/base_name-key.pem.
The certificate request is in /etc/apache/keys/base_name-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.version-number

In the AddModule section, add the following:

AddModule mod_ssl.c
```

注意 – 屏幕上将显示您的配置对应的 *version-number*。

3. **如果选择不设置** `VirtualHost`，**则必须在** `httpd.conf` **文件中添加** `SSLEngine`、`SSLCertificateFile` **和** `SSLCertificateKeyFile` **指令，这些指令必须刚好位于** `SSLPassPhraseDialog` **指令前面**。

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

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

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

SSLPassPhraseDialog exec:/opt/SUNWconn/cryptov2/bin/apgetpass

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>
```

如果对第 100 页 “启用 Apache Web 服务器”步骤 7 中的问题回答 “No”，则系统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 Sun ONE and Apache keys" from the
apsslcfg main menu.
```

4. **在** `apsslcfg` **运行完毕后，选择** `0` **退出**。

5. **从** `/etc/apache/keys/`*base_name*`-certreq.pem` **（其中** *base_name* **已在第 100 页“启用 Apache Web 服务器”中的步骤 9 设置）中复制证书申请及标题，然后将其提交给认证机构。**

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. **在浏览器中输入下面的 URL，检查已启用 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 4000 软件的诊断测试和故障排除方法，包括以下几节：

SunVTS 诊断软件

核心 SunVTS 程序包提供了用于执行一系列测试的测试控件和用户界面。其中一些测试程序随 SUNWvts 和 SUNWvtsx 软件包一起提供，它们与核心 SunVTS 程序包一起组成 Solaris 8/9 Software Supplement CD 上的工具套件。其它使用核心 SunVTS 程序包的零散测试程序则随所测试设备的驱动程序软件一起提供。

Sun Crypto 加速器 4000 板可通过三个 SunVTS 测试程序进行测试。其中两个测试程序， nettest 和 netlbtest，与 SunVTS 5.1 Patch Set (PS) 2 版本以后的核心 SunVTS 软件捆绑在一起。这些测试程序用于对板的以太网电路进行测试。

第三个 SunVTS 测试程序 vcatest 位于 Sun Crypto 加速器 4000 CD 上的 SUNWvcav 软件包中，它与核心 SunVTS 程序包一起用于诊断板的加密电路。

为 vca 驱动程序安装 SunVTS netlbtest 和 nettest 支持

表 7-1 说明了如何更新已安装的 SunVTS 软件以便为 vca 驱动程序提供 SunVTS netlbtest 和 nettest 支持。

表 7-1 vca 驱动程序必需的 SunVTS netlbtest 和 nettest 软件

基本 Solaris 软件	基本 SunVTS 软件	必需的替换软件包	必需的更新修补程序
Solaris 8 7/01	SunVTS4.4		111854-04
Solaris 8 10/01	SunVTS4.5		112250-04
Solaris 8 2/02	SunVTS4.6	SunVTS5.1ps2	
Solaris 9 5/02	SunVTS5.0	SunVTS5.1ps2	
Solaris 9 9/02	SunVTS5.1		113614-11
Solaris 8 HW 12/02	SunVTS5.1ps1		113614-11
Solaris 9 12/02	SunVTS5.1ps1		113614-11
Solaris 8 HW 5/03	SunVTS5.1ps2		
Solaris 9 4/03	SunVTS5.1ps2		

SunVTS 软件位于每个 Solaris 版本附带的 Solaris Software Supplement CD 上。表 7-1 “基本 SunVTS 软件”栏中列出的 SunVTS 软件版本位于同一行内 Solaris 版本附带的 Solaris Software Supplement CD 上。

表 7-1 中以 “SunVTS”开头的条目表示一套 SunVTS 软件包的版本。每套 SunVTS 软件包中必须安装 SUNWvts 和 SUNWvtsx 软件包。

表 7-1 “必需的替换软件包”栏中列出的 SunVTS 软件包必须替换以前安装的 SunVTS 软件包。添加 SunVTS 替换软件包之前，必须删除以前安装的 SunVTS 软件包。删除以前安装的 SunVTS 软件包的方法必须与以前安装它们的方法相同。例如，如果以前安装软件包时所用的命令是 pkgadd，则应使用 pkgrm 命令删除软件包。

如果表 7-1 “必需的更新修补程序”栏中列有条目，则必须使用 patchadd 命令安装该修补程序以更新 “基本 SunVTS 软件”栏中列出的 SunVTS 软件包。添加必需的修补程序之前，不要删除以前安装的 SunVTS 软件包。

使用 patchadd 命令安装修补程序 113614-11 相当于用 SunVTS5.1ps2 软件包替换以前安装的 SunVTS 软件包。

您可从以下网址获得替换软件包：http://www.sun.com/oem/products/vts/

您可从以下网址获得更新修补程序：http://sunsolve.sun.com/

注意 – 安装 SUNWvcav 软件包之前，必须先安装必需的 SunVTS 软件包和修补程序。SUNWvcav 软件包中包括 SunVTS 测试程序 vcatest。

使用 SunVTS 软件执行 vcatest、nettest 和 netlbtest

有关如何执行和监控这些诊断测试程序的说明，请参阅 SunVTS 测试程序参考手册、用户指南和快速参考卡。这些文档位于 http://docs.sun.com 网站上的“Solaris on Sun Hardware Documentation Set”中。此外，您的系统 Solaris 版本附带的 Solaris Software Supplement CD 中也提供了这些文档。

注意 – 只有在安装了必需的 SunVTS 软件包和 SunVTS 修补程序之后才能使用 SunVTS。

▼ 执行 vcatest

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 用户指南。

以下说明假定您已使用 CDE 用户界面启动了 SunVTS。

2. **在 “SunVTS Diagnostic” 主窗口中，将 “System Map” 设为 “Logical” 模式。**

注意 – 系统也支持 “Physical”模式；不过，本过程假定使用 “Logical”模式。

3. **清除所有测试程序的复选框，将它们禁用。**
4. **选择 “Cryptography” 的复选框，然后再选择 “Cryptography” 的加号框，显示 Cryptography 组中的所有测试程序。**

5. **清除 Cryptography 组中除 `vcatest` 以外的复选框。**
   - 如果显示了 `vcatest`，则转至步骤 6。
   - 如果未显示 `vcatest`，则可以通过检测系统以找到它，方法是：选择“Commands”下拉菜单中的“Reprobe System”。

   有关确切步骤，请参阅 SunVTS 用户指南。检测过程完成并显示 `vcatest` 后，继续执行步骤 6。

6. **选择其中一个 `vcatest` 例程，然后单击右键并拖动鼠标以显示“Test Parameter Options”对话框。**

   第 110 页“`vcatest` 的测试参数选项”介绍了这些只属于 `vcatest` 的选项。

7. **选择所有必要的选项后，从“Within Instance”下拉菜单中选择“Apply”以更改所选的 `vcatest` 例程；或者从“Across All Instances”下拉菜单中选择“Apply”以更改选定的所有 `vcatest` 例程。**

   进行该操作后，对话框消失，并且返回“Sun Diagnostic”主窗口。

8. **选择其中一个 `vcatest` 例程，然后单击右键并拖动鼠标以显示“Test Execution Options”对话框。**

   显示“Test Execution Options”对话框的另一种方法是选择“Options”下拉主菜单，然后再选择“Test Executions”。这些选项是通用 SunVTS 控件，将会影响所有测试程序。有关详细信息，请参阅 SunVTS 用户指南。

9. **选择所有必要的选项后，单击“Apply”以清除对话框并返回“SunVTS Diagnostic”主窗口。**

10. **选择“Start”执行选定的测试程序。**

11. **选择“Stop”停止所有测试程序。**

`vcatest` 的测试参数选项

表 7-2 说明了 `vcatest` 子测试程序。

表 7-2 `vcatest` 子测试程序

测试程序名称	说明
`CDMF`	测试 CDMF 批量加密。
`DES`	测试 DES 批量加密。
`3DES`	测试 3DES 批量加密。
`RSA`	测试 RSA 公钥和私钥。
`DSA`	测试 DSA 签名验证。

表 7-2 vcatest 子测试程序 *（续）*

测试程序名称	说明
MD5	测试 MD5 消息摘要/数字签名。
SHA1	测试 SHA1 摘要密钥创建。
RNG	测试随机号码生成性能。

vcatest 命令行语法

如果您从命令行 （而不是 CDE 界面）选择运行 vcatest，则所有参数必须在命令行字符串中指定。

在 32 位模式下， vcatest 的路径是 /opt/SUNWvts/bin/。在 64 位模式下，vcatest 的路径是 /opt/SUNWvts/bin/sparcv9/。

vcatest 的命令行界面能够支持所有 SunVTS 标准选项。测试程序专用的选项通过 -o 参数指定。

有关标准命令行参数的定义，请参阅 SunVTS 测试程序参考手册。 vcatest 是一个功能模式的测试程序，因此必须包括 -f 参数。使用 -u 参数可以显示用法消息，或者使用 -v 参数显示 VERBOSE （详细）消息。方括号中包含的项目表示可选条目。

下面是一个在 32 位模式下将 vcatest 作为独立程序调用的示例。以下命令用于在 vca0 上执行所有子测试程序：

```
# /opt/SUNWvts/bin/vcatest -f -o dev=vca0,tl=all
```

下面是一个在 64 位模式下从 SunVTS 体系中调用 vcatest 的示例。以下命令用于在 vca2 上执行 RSA、 DSA 和 MD5 测试程序：

```
# /opt/SUNWvts/bin/sparcv9/vcatest -f -o dev=vca2,tl=RSA+DSA+MD5
```

从命令行中运行 vcatest 时，如果忽略某个选项，则会使用该选项的默认操作，如表 7-3 中所示。

表 7-3 vcatest 命令行语法

选项	说明
dev=vca*N*	指定要测试的设备的例程，如 vca0 或 vca2。如果不指定，则默认为 vca0。请注意 *N* 表示要测试的设备的例程号。
tl=*testlist*	指定要执行的子测试程序的列表。 tl 的子测试程序由 + （加号）隔开。支持的子测试程序为 CDMF、 DES、 3DES、 DSA、 RSA、 MD5、 SHA1 和 RNG，因此 tl=CDMF+DES+3DES+DSA+RSA+MD5+SHA1+RNG 将启用所有子测试程序。您也可以插入 tl=all，以便执行所有测试程序。如果未指定任何子测试程序，则默认为 all。

▼ 执行 netlbtest

1. **以超级用户身份启动 SunVTS。**

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

有关启动的详细信息，请参阅 SunVTS 用户指南。

以下说明假定您已使用 CDE 用户界面启动了 SunVTS。

2. **在 “SunVTS Diagnostic” 主窗口中，将 “System Map” 设为 “Logical” 模式。**

注意 – 系统也支持 “Physical” 模式；不过，本过程假定使用 “Logical” 模式。

3. **清除所有测试程序的复选框，将它们禁用。**

4. **选择 “Network” 的复选框，然后再选择 “Network” 的加号框，显示 Network 组中的所有测试程序。**

5. **清除 Network 组中除 vca*N*(netlbtest) 以外的复选框。请注意 *N* 表示要测试的设备的例程号。**
   - 如果显示了 vca*N*(netlbtest)，则转至步骤 6。
   - 如果未显示 vca*N*(netlbtest)，则可以通过检测系统以找到它，方法是：选择 “Commands” 下拉菜单中的 “Reprobe System”。

   有关确切步骤，请参阅 SunVTS 用户指南。检测过程完成并显示 vca*N*(netlbtest) 后，继续执行步骤 6。

6. **选择 “Intervention Mode”按钮。选择其中一个** `vca`*N*`(netlbtest)` **例程，然后单击右键并拖动鼠标以显示 “Test Parameter Options”对话框。**

   SunVTS 测试程序参考手册中介绍了只属于 `netlbtest` 的选项。

7. **选择所有必要的选项后，从 “Within Instance”下拉菜单中选择 “Apply”以更改所选的** `vca`*N*`(netlbtest)` **例程；或者从 “Across All Instances”下拉菜单中选择 “Apply”以更改所有选定的** `vca`*N*`(netlbtest)` **例程。**

   进行该操作后，对话框消失，并且返回 “Sun Diagnostic”主窗口。

8. **选择其中一个** `vca`*N*`(netlbtest)` **例程，然后单击右键并拖动鼠标以显示 “Test Execution Options”对话框。**

   显示 “Test Execution Options”对话框的另一种方法是选择 “Options”下拉主菜单，然后再选择 “Test Executions”。这些选项是通用 SunVTS 控件，将会影响所有测试程序。有关详细信息，请参阅 SunVTS 用户指南。

9. **选择所有必要的选项后，选择 “Apply”以清除对话框并返回 “SunVTS Diagnostic”主窗口。**

10. **选择 “Start”执行选定的测试程序。**

11. **选择 “Stop”停止所有测试程序。**

▼ 执行 `nettest`

1. **以超级用户身份启动 SunVTS。**

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

   有关启动的详细说明，请参阅 SunVTS 用户指南。

   以下说明假定您已使用 CDE 用户界面启动了 SunVTS。

2. **在 “SunVTS Diagnostic”主窗口中，将 “System Map”设为 “Logical”模式。**

注意 – 系统也支持 “Physical”模式；不过，本过程假定使用 “Logical”模式。

---

3. **清除所有测试程序的复选框，将它们禁用。**

4. **选择 “Network”的复选框，然后再选择 “Network”的加号框，显示 Network 组中的所有测试程序。**

5. **清除 Network 组中除 vca*N*(nettest) 以外的复选框。请注意 *N* 表示要测试的设备的例程号。**
   - 如果显示了 vca*N*(nettest)，则转至步骤 6。
   - 如果未显示 vca*N*(nettest)，则在安装 vca*N* 板的服务器上的另一个窗口中输入 ifconfig -a。此时会列出以下条目：

```
vcaN up inet ip-address plumb
```

   如果未列出前面的 ifconfig 条目， nettest 检测程序则会认为此设备不可测试，您需根据 ifconfig 联机手册页的说明使接口联机。

   如果 ifconfig -a 列出了前面的条目，请返回 “SunVTS Diagnostic”主窗口，然后通过在 “Commands”下拉菜单中选择 “Reprobe System”来检测系统，从而找到 vca。

   有关确切步骤，请参阅 SunVTS 用户指南。检测过程完成并显示 vca0(nettest) 后，继续执行步骤 6。

6. **选择其中一个 vca*N*(nettest) 例程，然后单击右键并拖动鼠标以显示 “Test Parameter Options”对话框。**

   SunVTS 测试程序参考手册中介绍了只属于 nettest 的选项。

7. **选择所有必要的选项后，从 “Within Instance”下拉菜单中选择 “Apply”以更改所选的 vca*N*(nettest) 例程；或者从 “Across All Instances”下拉菜单中选择 “Apply”以更改所有选定的 vca*N*(nettest) 例程。**

   进行该操作后，对话框消失，并且返回 “Sun Diagnostic”主窗口。

8. **选择其中一个 vca*N*(nettest) 例程，然后单击右键并拖动鼠标以显示 “Test Execution Options”对话框。**

   显示 “Test Execution Options”对话框的另一种方法是选择 “Options”下拉主菜单，然后再选择 “Test Executions”。这些选项是通用 SunVTS 控件，将会影响所有测试程序。有关详细信息，请参阅 SunVTS 用户指南。

9. **选择所有必要的选项后，选择 “Apply”以清除对话框并返回 “SunVTS Diagnostic”主窗口。**

10. **选择 “Start”执行选定的测试程序。**

11. **选择 “Stop”停止所有测试程序。**

注意 – 不要同时执行 nettest 和 netlbtest。

使用 kstat 确定加密活动

Sun Crypto 加速器 4000 板没有配备用于反映板上加密活动的指示灯或其它指示器。要确定加密作业请求是否已在板上执行，请使用 kstat(1M) 命令显示设备的用法：

```
# kstat vca:0
module: vca                     instance: 0
name:   vca0                    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
```

注意 – 在上面的示例中， 0 是 vca 设备的例程号。此号码应反映您正在为其执行 kstat 命令的板的例程号。

显示的 kstat 信息指明了加密请求或“作业”是否正发送给 Sun Crypto 加速器 4000 板。*作业*值随时间变化，表明板正在加速那些发送给 Sun Crypto 加速器 4000 板的加密作业请求。如果无加密作业请求发送给板，请根据 Web 服务器的特定配置来验证您的 Web 服务器配置。

不要试图解释 kstat(1M) 返回的内核/驱动程序统计值。这些值保存在驱动程序内，用于进行现场支持服务。其含义和实际名称可能会随时间而变化。

注意 – 如果 nostats 属性已在 /kernel/drv/vca.conf 文件中定义，则不会捕获和显示统计数字。此属性可以用来防止进行通信量分析。

使用 OpenBoot PROM FCode 自测程序

以下测试程序有助于在系统无法引导时识别适配器的故障。

您可以使用 OpenBoot PROM (OBP) `test` 或 `test-all` 命令来调用 FCode 自测诊断程序。如果在执行诊断程序时发生故障，则会显示相应的消息。有关 `test` 和 `test-all` 命令的详细信息，请参阅 《*OpenBoot Command Reference Manual*》。

FCode 自测程序按子组件运行大多数功能子组件，并确保：

- 在适配器板安装期间的连通性
- 验证系统引导过程所需的所有组件是否正常

▼ 执行以太网 FCode 自测诊断程序

要执行以太网诊断程序，您必须先执行重置命令，并使系统停止在 OBP 提示符下。如果不重置系统，诊断测试程序可能会导致系统挂起。

有关本节中 OpenBoot 命令的详细信息，请参阅 《*OpenBoot Command Reference Manual*》。

1. **关闭系统。**

   使用 《*Solaris Handbook for Sun Peripherals*》中所述的标准关机过程。

2. **在 OBP 提示符下，将 `auto-boot?` 配置变量设为 `false`。**

```
ok setenv auto-boot? false
```

3. **重置系统。**

```
ok reset-all
```

4. **键入** `show-nets` **以显示设备列表，并选择所需的选项：**

   您会看到类似于下面示例的设备列表，这些设备因适配器的不同而变化。

```
ok show-nets
a) /pci@8,600000/network@1
b) /pci@8,700000/network@5,1
q) NO SELECTION
Enter Selection, q to quit: a
/pci@8,600000/network@1 has been selected.
Type ^Y ( Control-Y ) to insert it in the command line.
e.g. ok nvalias mydev ^Y for creating devalias mydev for
/pci@8,600000/network@1
```

注意 – 要使用 `test` 命令执行以下自测程序，必须将以太网端口连接至网络。

5. **使用** `test` **命令执行自测程序：**

   运行 `test` 命令时，将会执行以下测试程序：

   - `vca` 寄存器测试程序 （仅在 `diag-switch?` 设为 true 时发生）
   - 内部回送测试程序
   - 链路连接/断开测试程序

注意 – 对于使用外部回送缆线的 1000 Mbps 连接，由于链路时钟无法调整，因此无法执行 Sun Crypto 加速器 4000 UTP 适配器自测程序。对于此类测试，本地端口和远程端口必须调整为主控时钟与从属时钟。使用外部回送缆线时，本地端口和远程端口相同。因此，单个端口不能既是主控时钟又是从属时钟，否则会始终导致 PHY 链路连接失败。要使 Sun Crypto 加速器 4000 UTP 适配器自测程序可以正确测试 1000 Mbps 连接，必须连接远程 1000Base-T 端口。

键入以下命令：

```
ok test device_path
```

如果通过 test 测试，则会看到以下消息：

```
ok test /pci@8,600000/network@1
Testing /pci@8,600000/network@1
Register tests: passed
Internal loopback test: passed
/pci@8,600000/network@1: 100 Mbps half duplex link up
```

如果板未连接至网络，则会看到以下消息：

```
ok test /pci@8,600000/network@1
Testing /pci@8,600000/network@1
Register tests: passed
Internal loopback test: passed
/pci@8,600000/network@1: link down
```

6. **测试适配器之后，请键入以下命令，以将 OBP 界面恢复至标准操作模式：**

```
ok setenv diag-switch? false
```

7. **将** auto-boot? **配置参数设为** true。

```
ok setenv auto-boot? true
```

8. **重置并重新引导系统。**

排除 Sun Crypto 加速器 4000 板的故障

本节介绍用于排除板故障的 OBP 级命令。有关以下小节所述命令的详细说明，请参阅《*OpenBoot Command Reference Manual*》。

show-devs 命令

要确定 Sun Crypto 加速器 4000 设备是否在系统中列出，请执行以下步骤：在 OBP 提示符下，键入 show-devs 命令以显示设备列表。您应该在设备列表中看到类似于下面示例的几行。这些行的内容可能会有所不同，具体取决于所用的 Sun Crypto 加速器 4000 板。

```
ok show-devs
.
.
/chosen
/packages
/upa@8,480000/SUNW,ffb@0,0
/pci@8,600000/network@1
/pci@8,600000/SUNW,qlc@4
/pci@8,600000/SUNW,qlc@4/fp@0,0
.
.
```

在上面的示例中，/pci@8,600000/network@1 条目表示 Sun Crypto 加速器 4000 板的设备路径。系统中的每块板均应有各自的设备路径行。

.properties 命令

要确定是否正确列出了 Sun Crypto 加速器 4000 的设备属性，请执行以下步骤：
在 OBP 提示符下，键入 .properties 命令以显示属性列表。

```
ok .properties
assigned-addresses        82000810 00000000 00102000 00000000 00002000
                           81000814 00000000 00000400 00000000 00000100
                           82000818 00000000 00200000 00000000 00200000
                           82000830 00000000 00400000 00000000 00100000
d-fru-len                 00 00 00 00
d-fru-off                 00 00 e8 00
d-fru-dev                 eeprom
s-fru-len                 00 00 08 00
s-fru-off                 00 00 e0 00
s-fru-dev                 eeprom
compatible                70 63 69 38 30 38 36 2c 62 35 35 35 2e 31 30 38
reg                       00000800 00000000 00000000 00000000 00000000
                           02000810 00000000 00000000 00000000 00002000
                           02000814 00000000 00000000 00000000 00000100
                           02000818 00000000 00000000 00000000 00200000
                           02000830 00000000 00000000 00000000 00100000
address-bits              00 00 00 30
max-frame-size            00 00 40 00
network-interface-type    ethernet
device_type               network
name                      network
local-mac-address         08 00 20 aa bb cc
version                   Sun PCI Crypto Accelerator 4000 1000Base-T Code
2.11 02/10/31
phy-type                  mif
board-model               501-6039
model                     SUNW,pci-vca
fcode-rom-offset          00000000
66mhz-capable
fast-back-to-back
devsel-speed              00000001
class-code                00100000
interrupts                00000001
latency-timer             00000040
cache-line-size           00000010
max-latency               00000040
min-grant                 00000040
subsystem-id              00003de8
subsystem-vendor-id       0000108e
revision-id               00000002
device-id                 0000b555
vendor-id                 00008086
```

watch-net 命令

要监控网络连接，请执行以下步骤：在 OBP 提示符下，键入 `apply watch-net` 命令和设备路径：

```
ok apply watch-net /pci@8,600000/network@1
/pci@8,600000/network@1: 1000 Mbps full duplex link up
Watch ethernet packets
'.' is a good packet and 'X' is a bad packet
Press any key to stop
.....X...X......X.....
```

系统将会监控网络通信状态。每次收到无错误的数据包时，便会显示一个 “.” 符号；每次收到可由网络硬件接口检测到的出错数据包时，便会显示一个 “X” 符号。

附录 **A**

规格

本附录介绍 Sun Crypto 加速器 4000 MMF 和 UTP 适配器的规格，包括以下几节：

Sun Crypto 加速器 4000MMF 适配器

本节介绍 Sun Crypto 加速器 4000 MMF 适配器的规格。

连接器

图 A-1 显示了 Sun Crypto 加速器 4000 MMF 适配器的连接器。

图 A-1 Sun Crypto 加速器 4000MMF 适配器连接器

表 A-1 列出了 SC 连接器 (850 nm) 的特性。

表 A-1 SC 连接器链接特性 (IEEE P802.3z)

特性	62.5 微米 MMF	50 微米 MMF
操作范围	最长 260 米	最长 550 米

物理尺寸

表 A-2 物理尺寸

尺寸	测量	测量 （公制）
长度	12.283 英寸	312.00 毫米
宽度	4.200 英寸	106.68 毫米

性能规格

表 A-3 性能规格

功能	规格
PCI 时钟	最大 33/66 MHz
PCI 数据瞬间传输速率	最大 64 字节 （瞬间）
PCI 数据/地址宽度	32/64 位
PCI 模式	主控/从属
1 Gbps， 850 nm	1000 Mbps （全双工）

电源要求

表 A-4 电源要求

规格	测量
最大功耗	6.25 W @ 5V 12.75 W @ 3.3V
电压容差	5V +/- 5% 3.3V +/- 5%

接口规格

表 A-5 接口规格

功能	规格
PCI 时钟	33 MHz 或 66 MHz
主机接口	PCI 2.1，支持 33 MHz 或 66 MHz 时钟速率以及 3.3V 或 5V 电源。
PCI 总线宽度	32 位或 64 位

环境规格

表 A-6 环境规格

条件	工作规格	存储规格
温度	0° 至 +55°C，+32° 至 +131°F	-40° 至 +75°C，-40° 至 +167°F
相对湿度	5 至 85%（无凝结）	0 至 95%（无凝结）

Sun Crypto 加速器 4000UTP 适配器

本节介绍 Sun Crypto 加速器 4000 UTP 适配器的规格。

连接器

图 A-2 显示了 Sun Crypto 加速器 4000 UTP 适配器的连接器。

图 A-2 Sun Crypto 加速器 4000UTP 适配器连接器

表 A-7 列出了 Sun Crypto 加速器 4000 UTP 适配器所用的 5 类连接器的特性。

表 A-7 5 类连接器的链接特性

特性	说明
操作范围	最长 100 米

物理尺寸

表 A-8 物理尺寸

尺寸	测量	测量 （公制）
长度	12.283 英寸	312.00 毫米
宽度	4.200 英寸	106.68 毫米

性能规格

表 A-9 性能规格

功能	规格
PCI 时钟	最大 33/66 MHz
PCI 数据瞬间传输速率	最大 64 字节 （瞬间）
PCI 数据/地址宽度	32/64 位
PCI 模式	主控/从属
1 Gbps， 850 nm	1000 Mbps （全双工）

电源要求

表 A-10 电源要求

规格	测量
最大功耗	6.25 W @ 5V 12.75 W @ 3.3V
电压容差	5V +/- 5% 3.3V +/- 5%

接口规格

表 A-11 接口规格

功能	规格
PCI 时钟	33 MHz 或 66 MHz
主机接口	PCI 2.1，支持 33 MHz 或 66 MHz 时钟速率以及 3.3V 或 5V 电源
PCI 总线宽度	32 位或 64 位

环境规格

表 A-12 环境规格

条件	工作规格	存储规格
温度	0° 至 +55°C，+32° 至 +131°F	-40° 至 +75°C，-40° 至 +167°F
相对湿度	5 至 85%（无凝结）	0 至 95%（无凝结）

附录 **B**

Apache Web 服务器的 SSL 配置指令

本附录介绍通过 Sun Crypto 加速器 4000 软件为 Apache Web 服务器配置 SSL 支持时所用的指令。您应在 `http.conf` 文件中配置指令。有关详细信息，请参阅 Apache Web 服务器文档。

1. `SSLPassPhraseDialog exec:`*program*

   环境：全局

   该指令用于通知 Apache Web 服务器应执行指定的 *program*，以收集密钥文件的密码。 *program* 会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，并且它们使用共同的密码，则 *program* 只执行一次 （再次运行 *program* 之前，将会尝试每个收集到的密码。）

   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 – 由于该程序可以在系统启动期间运行，因此应对其进行设计，以应付控制台不是 `tty` 设备的情况 （即 `tty`(3c) 返回 false 值）。

   随附的程序 `/opt/SUNWconn/cryptov2/bin/apgetpass` 可供 *program* 的执行文件使用。该程序会自动提示您输入密码，而且在输入密码时不显示密码。

   另外，随附的 `sslpassword` 程序还可以自动搜索文件中的密码，从而避免在 Web 服务器启动期间进行用户交互操作。它将在名为 `/etc/apache/`*servername*:*port*.*keytype*`.pass` 的文件中搜索密钥文件的密码。如果该文件不存在，则使用 `/etc/apache/default.pass` 文件。这些密码文件仅包含未加密的密码，密码自成一行。

注意 – 密码文件应通过权限加以保护，从而只允许 Web 服务器以其身份运行的 UNIX 用户读取文件。该用户应该是使用标准 Apache `User` 指令配置的同一用户。

如果未指定，则默认操作会使用内部提示机制。请勿使用默认操作，而使用随附的 `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

   该指令用于启用 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>
```

此语句为监听端口 443 （标准 HTTPS 端口）的任何服务器配置 SSL。如果不存在，将禁用此协议 （默认设置）。

3. `SSLProtocol [+-]`*protocol*

   环境：全局，虚拟主机

   该指令用于配置服务器在进行 SSL 事务处理时应使用的协议。表 B-1 列出并说明了可用的协议：

表 B-1 SSL 协议

协议	说明
`SSLv2`	Netscape 提出的最初标准 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`	`SSLv3` 的更新版本，当前正由 IETF 进行规范，支持它的浏览器很少
`all`	启用所有协议

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

```
SSLProtocol all -SSLv2
```

上一语句与下一语句等效：

```
SSLProtocol +SSLv3 +TLSv1
```

4. `SSLCipherSuite` *cipher-spec*

   环境：全局，虚拟主机，目录， `.htaccess`

   SSLCipherSuite 指令用于配置可用的 SSL 密码及其首选项。在全局环境或虚拟主机环境中，该指令在初次 SSL 握手时使用。在目录环境中，它强制执行 SSL 重新协商以使用指定的密码。重新协商在读取请求之后且在发送响应之前发生。

   cipher-spec 可以是一个由冒号分隔的密码列表，表 B-2 列出了这些密码。在表 B-2 中，DH 是指 Diffie-Hellman， DSS 是指数字签名标准。

表 B-2 可用的 SSL 密码

密码标记	协议	密钥交换	验证	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
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	

表 B-2 可用的 SSL 密码 *（续）*

密码标记	协议	密钥交换	验证	加密	MAC	类型
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

表 B-3 列出并说明了可以提供类似宏分组的别名。

表 B-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
EXPORT56	所有 56 位导出密码
LOW	长度较短的密码 （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

表 B-3 SSL 别名 *（续）*

别名	说明
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

您可使用表 B-4 中列出并说明的特殊字符来配置密码的首选项。

表 B-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 — 密码无法再次添加
+	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 （以后可在列表中添加）

cipher-spec 的默认值是

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

此默认值将配置除匿名 （未验证）Diffie-Hellman 之外的所有密码，将 ARCFOUR 和 RSA 置为首选项，然后是由高至低的加密级别。

5. `SSLCertificateFile` *file*

   环境：全局，虚拟主机

   该指令用于指定此服务器的 PEM 编码 X.509 证书文件的位置。

6. `SSLCertificateKeyFile` *file*

   环境：全局，虚拟主机

   该指令用于指定此服务器的 PEM 编码私钥文件的位置，它与使用 `SSLCertificateFile` 指令配置的证书对应。

7. `SSLCertificateChainFile` *file*

   环境：全局，虚拟主机

   该指令用于指定包含 PEM 编码证书 （用于构成服务器鉴定路径）的文件的位置。当服务器证书不是由客户机认可的认证机构直接签名时，您可使用该指令来协助客户机验证服务器证书。

   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

   该指令用于指定包含认证机构 (CA) 证书级联 （用于客户机验证）的文件的位置。

9. `SSLCARevocationFile` *file*

   环境：全局，虚拟主机

   该指令用于指定包含 CA 证书调用列表级联 （用于客户机验证）的文件的位置。

10. `SSLVerifyClient` *level*

    环境：全局，虚拟主机，目录， `.htaccess`

    该指令用于配置服务器对客户机的验证。（注意：正常情况下，该指令不用于电子商务应用程序，而是用于其它应用程序。）

    表 B-5 列出并说明了 *level* 的值。

表 B-5 SSL 验证客户机级别

级别	说明
`none`	不要求客户机提供证书
`optional`	客户机可能需要提供有效证书
`require`	客户机*必须*提供有效证书
`optional_no_ca`	客户机可能需要提供证书，但证书无需有效

通常情况下使用 `none` 或 `require`。默认值为 `none`。

11. `SSLVerifyDepth` *depth*

    环境：全局，虚拟主机，目录， `.htaccess`

    该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，则表示仅自签名证书为合格证书；如果值为 1，则表示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

    该指令指定用于记录 SSL 特定信息的日志文件。如果不指定 （默认值），则不会记录 SSL 特定信息。

13. `SSLLogLevel` *level*

环境：全局，虚拟主机

该指令指定 SSL 日志文件中所记录信息的详细程度。表 B-6 列出并说明了 *level* 的值。

表 B-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`

该指令按目录来配置 SSL 运行选项。在选项前面加上加号 (+) 前缀，可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。如果多个选项应用于一个目录，则使用限制性最强的选项；选项不能合并。

表 B-7 列出并说明了这些选项。

表 B-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 — 这可能导致系统性能有所下降。
`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`	客户机证书的识别名 (DN) 被转换成一个 HTTP 基本验证用户名，且 “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，即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`	由于忽略 `SSLRequireSSL` 而强制进行非法访问，即使存在会覆盖本指令的其它指令，如 `Satisfy Any` 等，也会如此。

15. `SSLRequireSSL`

环境：目录， `.htaccess`

除非使用 HTTPS，否则该指令禁止对给定目录的访问。您可使用该指令来防止因错误配置而导致目录内容受到未验证和未加密的访问。

附录 C

构建与 Sun Crypto 加速器 4000 板配合使用的应用程序

本附录介绍 Sun Crypto 加速器 4000 随附的软件。此类软件可以用来构建与 OpenSSL 兼容的应用程序，从而使它们能够利用 Sun Crypto 加速器 4000 板的加密加速功能。相对于使用 OpenSSL 程序库 （可从 `www.openssl.org` 网站下载）进行构建而言，这种编译方式并非对所有 OpenSSL 应用程序都有益。

注意 – 本附录提供的有关构建应用程序以使用 Sun Crypto 加速器 4000 软硬件的信息完全按原样提供，并不是本产品正式发布的支持功能。提供这些信息的目的仅仅是希望对大家有所裨益，我们对此不作任何担保。如果您需要 Sun 支持的解决方案，请与 Sun 专业服务部门联系，了解适于您的方案选项。

您必须先安装包含必需头文件和程序库的 `SUNWkcl2o` 软件包。

应用程序必须经过配置，以包含 `/opt/SUNWconn/cryptov2/include` 中的 OpenSSL 头文件，如具有编译程序标志的头文件：

```
-I/opt/SUNWconn/cryptov2/include
```

另外，还必须重新定向链接程序以便引用正确的程序库。与 OpenSSL 兼容的大多数应用程序均引用 `libcrypto.a` 或 `libssl.a` 程序库，或者同时引用这两个程序库。另外，还必须包含 Sun 加密程序库。您可使用下面的链接程序属性来完成此项任务：

```
-L/opt/SUNWconn/cryptov2/lib -R/opt/SUNWconn/cryptov2/lib \
-lcrypto -lssl -lkcl
```

附录 **D**

软件许可

本附录介绍 Sun 二进制代码许可协议以及第三方软件的声明和许可。

注意 – 本附录中的第三方许可和声明完全由软件许可和声明的所有方提供。

Sun Microsystems, Inc.

二进制代码许可协议

打开软件介质包装之前，请仔细阅读本协议的条款和任何提供的补充许可条款 （统称 “协议”）。如果打开软件介质包装，即表明您接受本 “协议” 的条款。如果您以电子方式访问软件，则在本 “协议” 的末尾选择 “接受” 按钮时，即表明您接受这些条款。如果您不接受所有这些条款，请立即将尚未使用的软件退回购买处以获得退款；或者，如果以电子方式访问软件，请在本 “协议” 的末尾选择 “拒绝” 按钮。

1. **使用许可**。按照已为之支付费用的用户数目及计算机硬件类型， Sun 授予您非独占且不可转让的许可，仅允许内部使用随附的软件和文档以及 Sun 提供的任何错误更正（统称 “软件”）。

2. **限制** “软件”属于机密文件，且受版权法保护。“软件”的产权和所有相关的知识产权为 Sun 及其许可发行者所有。除非经任何补充许可条款的明确认可，否则您除制作一个 “软件”备份供存档使用外，不得对 “软件”进行其它复制。除非与相关适用法律相抵触，否则您不可以修改、反编译 “软件”，也不可以对 “软件”进行逆向工程。您承认 “软件”的设计、注册或用途并非用于设计、构造、操作或维护任何核设施。 Sun 否认任何对此类用途适用性的明示或默示保证。与 Sun 或其许可发行者的任何商标、服务商标、徽标或产品名称有关的权利、产权或利益，不在本 “协议”的许可范围之内。

3. **有限担保**。 Sun 向您保证，自购买之日起 90 天内 （以收据副本为凭证），“软件”的存储介质 （如果有的话）在正常使用的情况下不会出现材料和工艺方面的缺陷，除非这些 “软件”由第三方提供。根据此有限担保，您的所有补尝以及 Sun 承担的全部责任是更换 “软件”介质或退还您为 “软件”支付的费用 （由 Sun 决定）。

4. **担保免责声明。除非在本 “协议” 中有明确规定，否则 Sun 拒绝承担任何明示或默示的条件、表示和担保，包括任何对适销性、特定用途的适用性或非侵犯性作出的默示担保 （除非这些免责声明在法律上无效）。**

5. **责任限制。除非与法律相抵触，否则无论采用何种有关责任的理论， SUN 或其许可发行者均不会对任何因使用 “软件”或因无法使用 “软件”而导致的收入减少、利润损失或数据丢失负责，也不会对特殊、间接、必然、偶然或惩罚性的损害负责，即使 SUN 已被告知可能出现此类损失。**根据本 “协议”，在任何情况下，无论是合同、侵权行为 （包括过失）还是其它方面的责任， Sun 对您的责任均不会超过您购买 “软件”所支付的金额。即使上述担保未能达到其基本目的，上文所述的限制仍然适用。

6. **终止。**本 “协议”在终止之前有效。您可以随时终止本 “协议”，但必须销毁 “软件”的全部正本和副本。如果您未遵守本 “协议”的任何规定，则本 “协议”将不经 Sun 发出通知立即终止。终止时，您必须销毁 “软件”的全部正本和副本。

7. **出口法规。**根据本 “协议”交付的所有 “软件”和技术数据均受美国出口控制法律的约束，也可能受其他国家/地区的进出口条例的约束。您必须严格遵守所有此类法律和法规，并确认您有责任在 “软件”送达之后获得所有必要的出口、转口或进口许可。

8. **美国政府的限制权利。**如果 “软件”由美国政府或以美国政府的名义，或者由美国政府的总承包商或任何等级的分包商采购，则政府对 “软件”和随附文档的权利将仅限于本 “协议”中规定的权利；这符合 48 CFR 227.7201 至 227.7202-4 条款（适于国防部 (DOD) 采购）以及 48 CFR 2.101 和 12.212 条款 （适于非国防部门采购）。

9. **管辖法律。**与本 “协议”相关的任何诉讼均受加利福尼亚州法律及适用的美国联邦法律的管辖。任何国家和地区的选择法律的规则不予适用。

10. **可分割性。**如果本 “协议”的任何条款无法实施，则可以忽略该条款，本 “协议”的其余部分仍然有效，除非忽略该条款会损坏当事双方的意向，在这种情况下，本 “协议”立即终止。

11. **完整性。**本 “协议”是您与 Sun 就其标的达成的完整协议。它取代此前或同期的所有口头或书面往来信息、建议、陈述和担保。在本 “协议”期间，有关报价、订单、回执或各方之间就本 “协议”标的进行的其他往来通信中的任何冲突条款或附加条款，均以本 “协议”为准。对本 “协议”的任何修改均无约束力，除非通过书面进行修改并由每一方的授权代表签字。

如有疑问，请联系 : Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054

(Form ID#011801)

Sun Microsystems, Inc.

Crypto 加速器 4000 的补充条款

这些 Sun Crypto 加速器 4000 补充条款是对二进制代码许可协议 （“BCL”）的补充。此处未定义的术语 （带双引号）与 BCL 中的含义一致。这些补充条款将取代 BCL 中任何不一致或相冲突的条款。使用 “软件”意味着接受此处补充的 BCL。

1. **第三方许可条款。**“软件”的某些部分附带了第三方的声明和/或许可，用于限制对这些部分的使用。

Third Party License Terms

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

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.

Copyright (c) 1998-2000 Ralf S. Engelschall. 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 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.

附录 **E**

手册页

本附录介绍 Sun Crypto 加速器 4000 板的命令并列出了每个命令的联机手册页。 Sun Crypto 加速器 4000 软件附带了本附录介绍的命令。

您可使用以下命令来查看联机手册页：

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

表 E-1 列出并说明了可用的联机手册页。

表 E-1 Sun Crypto 加速器 4000 联机手册页

手册页	说明
vca(7d)	vca 设备驱动程序是一个叶节点驱动程序，用于控制对基本硬件加密加速器的访问。 vca 驱动程序要求具备分层软件，以使应用程序和核心客户机能够访问所提供的服务。
vcad(1m)	vcad 后台程序用于提供密钥库服务。
vcaadm(1m)	vcaadm 是 Sun Crypto 加速器 4000 的管理程序。 vcaadm 命令用于手动控制与 Sun Crypto 加速器 4000 板 有关的配置、帐户和加密数据库。 vcaadm 用于处理一些敏感的加密密钥信息。
vcadiag(1m)	vcadiag 是一种实用程序，可使 root 用户重置 Sun Crypto 加速器 4000 板和零置密钥资料。该实用程序还允许 root 用户执行基本的诊断操作。
kcl2(7d)	kcl2 是为加密硬件驱动程序提供支持的核心模块。

表 E-1 Sun Crypto 加速器 4000 联机手册页 *（续）*

手册页	说明
kcl2(7d)	kc12 设备驱动程序是一个多线程的可加载核心模块，用于为 Sun 加密提供商驱动程序提供支持。 kc12 驱动程序要求具备分层软件，以使应用程序和核心客户机能够访问所提供的服务。
apsslcfg(1m)	apsslcfg 是 Apache Web 服务器的配置实用程序。
iplsslcfg(1m)	iplsslcfg 是 Sun ONE Web 服务器的配置实用程序。

附录 F

零置硬件

本附录介绍如何将 Sun Crypto 加速器 4000 板零置为原始出厂状态，即板的 `failsafe` 模式。

警示 – 仅在绝对必要时，才可执行本附录介绍的步骤。如果您需要清除所有密钥资料，则可使用 `vcaadm` 中的 `zeroize` 命令。有关 `zeroize` 命令的详细资料，请参阅第 69 页 “零置 Sun Crypto 加速器 4000 板”。另请参阅 `vcadiag` (4) 联机手册页，了解有关清除所有密钥资料的说明。

注意 – 本附录介绍的步骤将会删除 Sun Crypto 加速器 4000 固件。您必须重新安装 Sun Crypto 加速器 4000 软件附带的固件。

将 Sun Crypto 加速器 4000 硬件零置为原始出厂状态

某些情况下，可能需要将板还原为 `failsafe` 模式，并清除板的所有密钥资料和配置信息。只有使用与板相连的硬件跳线才能完成此项操作。

注意 – 您可使用 `vcaadm` 实用程序中的 `zeroize` 命令来清除 Sun Crypto 加速器 4000 板的所有密钥资料。不过， `zeroize` 命令会保持任何更新的固件完好无损。有关说明，请参阅第 69 页 “零置 Sun Crypto 加速器 4000 板”。另请参阅 `vcadiag` 联机手册页。

▼ 使用硬件跳线零置 Sun Crypto 加速器 4000 板

1. **关闭系统电源**。

注意 – 对于某些系统，您可以根据需要在本过程中使用动态重配置功能 (DR) 来拆卸和装回板，而无需关闭系统电源。有关 DR 的正确过程，请参阅系统随附的文档。

警示 – 调节跳线时，此板不得接通任何电源。

---

2. **卸下计算机机壳，以便调节板中上部的跳线**。

3. **将跳线放在跳线块的插针 0 和 1 上**。

   插针 0 和 1 是离支架最近的插针，标有 “Z” 字样。跳线块包含四组插针，每组两个插针。跳线只能放在插针 0 和 1 上，如图 F-1 中所示。

警示 – 跳线在插针 0 和 1 上时，不能使用 Sun Crypto 加速器 4000 板。

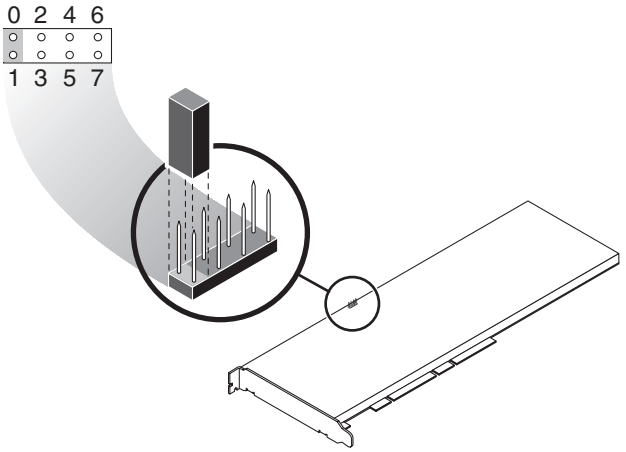

图 F-1 Sun Crypto 加速器 4000 板跳线块插针

4. **打开系统电源**。

警示 – 在调节 Sun Crypto 加速器 4000 板跳线之后打开系统电源时，所有固件、密钥资料及配置信息会被删除。本过程会将板还原为原始出厂状态，并且将它置入 `failsafe` 模式。

---

5. **关闭系统电源**。

6. **从跳线块的插针 0 和 1 上取下跳线，并放回原来的位置**。

7. **打开系统电源**。

8. **通过** `vcaadm` **连接到 Sun Crypto 加速器 4000 板**。

   `vcaadm` 会提示您输入升级固件的路径。

9. **键入** `/opt/SUNWconn/cryptov2/firmware/sca4000fw` **作为安装固件的路径**。

   固件会自动安装，且 `vcaadm` 退出。

10. **通过** `vcaadm` **重新连接到 Sun Crypto 加速器 4000 板**。

    `vcaadm` 会提示您初始化板以使用新的密钥库，或者初始化板以使用现有的密钥库。有关说明，请参阅第 56 页 “通过 vcaadm 初始化 Sun Crypto 加速器 4000 板”。

附录 G

常见问题

如何使 Web 服务器在重新引导期间启动但不进行用户交互操作？

使用加密密钥，您可以使 Sun ONE 和 Apache Web 服务器在重新引导期间自动启动。

▼ 创建加密密钥以使 Apache Web 服务器在重新引导期间自动启动

1. **验证 `httpd.conf` 文件中是否存在以下条目：**

```
SSLPassPhraseDialog exec:/opt/SUNWconn/cryptov2/bin/apgetpass
```

本指令将从 `/etc/apache` 目录下受保护的密码文件中检索密码。

2. **使用以下文件命名规则，在 `/etc/apache` 目录下创建仅包含该密码的密码文件。**

```
server_name:port.KEYTYPE.pass
```

- *server_name* — 您在 `httpd.conf` 文件的 “ServerName” 指令中指定的值
- *port* — 本 SSL 服务器的运行端口 （例如， 443）
- *KEYTYPE* — `RSA` 或 `DSA`

示例：对于使用 `RSA` 密钥在端口 443 上运行 SSL 的服务器 （名为 `webserv101`），您可以在 `/etc/apache` 目录下创建下面的文件：

```
webserv101:443.RSA.pass
```

建议您更改此密码文件的访问权限和所有权，如下所示：

```
# chmod 400 server_name:port.KEYTYPE.pass
# chown root server_name:port.KEYTYPE.pass
```

有关详细说明，请参阅 mod_SSL 和 OpenSSL 文档。

▼ 创建加密密钥以使 Sun ONE Web 服务器在重新引导期间自动启动

1. **浏览至 Sun ONE Web 服务器例程的** `config` **子目录 — 例如，** `/usr/iplanet/servers/https-`***webserver_instance_name***`/config`。
2. **创建只包含以下行的** `password.conf` **文件 （有关密码定义，请参见**表 5-1**）：**

```
internal:trust_db_password
keystore_name:username:password
```

3. **将密码文件的所有权设置为 Web 服务器以其身份运行的 UNIX 用户 ID，并将密码文件的访问权限设置为只供密码文件的所有者读取：**

```
# chown web_server_UNIX_user_ID password.conf
# chmod 400 password.conf
```

如何为安装在同一服务器中的多块板分配不同的 MAC 地址？

您可采用两种方法来为单个服务器中的多块板分配不同的 MAC 地址。第一种方法在操作环境级别下执行，第二种方法在 OpenBoot PROM (OBP) 级别下执行。

▼ 从终端窗口分配不同的 MAC 地址

1. **键入以下命令：**

```
# eeprom "local-mac-address?"=true
```

注意 – 当 “`local-mac-address?`” 参数设为 `true` 时，所有非集成网络接口设备均使用产品在工厂中制造时分配的本地 MAC 地址。

---

2. **重新引导系统。**

▼ 在 OpenBoot PROM 级别下分配不同的 MAC 地址

1. **在 OBP 提示符下键入以下命令：**

```
ok setenv local-mac-address? true
```

注意 – 当“local-mac-address?”参数设为 true 时，所有非集成网络接口设备均使用产品在工厂中制造时分配的本地 MAC 地址。

---

2. **引导操作环境。**

如何在安装 Sun Crypto 加速器 4000 软件之后配置与 Apache Web 服务器一起使用的 Sun Crypto 加速器 1000？

安装 SUNWkcl2a 软件包之后，系统将会配有 Apache Web 服务器 mod_ssl 1.3.26。

如果您想配置 Sun Crypto 加速器 1000 以便与 Apache 配合使用，则必须安装以下修补程序。

在装有 SUNWkcl2a 软件包的 Solaris 8 系统上，要配置 Sun Crypto 加速器 1000 以便与 Apache 1.3.26 配合使用，必须安装以下修补程序：

- 对于 Apache 1.3.26 — 修补程序 ID 109234-09 或更新版本
- 对于 Sun Crypto 加速器 1000 版本 1.0 软件 — 修补程序 ID 112869-02
- 对于 Sun Crypto 加速器 1000 版本 1.1 软件 — 修补程序 ID 113355-01

在装有 SUNWkcl2a 软件包的 Solaris 9 系统上，要配置 Sun Crypto 加速器 1000 以便与 Apache 1.3.26 配合使用，必须安装以下修补程序：

- 对于 Apache 1.3.26 — 修补程序 ID 113146-01 或更新版本
- 对于 Sun Crypto 加速器 1000 版本 1.1 软件 — 修补程序 ID 113355-01

如何自签用于测试的证书？

有关此过程的说明，请参阅 mod_SSL 和 OpenSSL 文档。

索引

A

B

C

R

S

T

W

X

Y

Z