Sun™ Crypto Accelerator 4000 介面卡 1.1 版安裝與使用者指南

Sun Microsystems, Inc.
www.sun.com

文件號碼 817-5928-10
2004 年 1 月，修訂版 A

請在 http://www.sun.com/hwdocs/feedback 上提交有關此文件的意見

請回收

Adobe PostScript

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。

目錄

表

前言

*Sun Crypto Accelerator 4000 介面卡 1.1 版安裝與使用者指南*列出了 Sun Crypto Accelerator 4000 介面卡的功能、通訊協定及介面，並說明如何在系統中安裝、設定及管理介面卡。

本書假設您是網路管理員，熟悉如何設定下列一個或多個項目：Solaris 作業環境、裝有 PCI I/O 卡的 Sun 平台、Sun ONE 與 Apache 網站伺服器、IPsec、SunVTS™ 軟體，並熟悉如何取得授權機構的憑證。

本書的組織結構

本書的組織結構如下：

- 第 1 章列出 Sun Crypto Accelerator 4000 介面卡的產品功能、通訊協定及介面，並說明硬體與軟體需求。
- 第 2 章說明如何安裝與移除 Sun Crypto Accelerator 4000 的硬體與軟體。
- 第 3 章定義 Sun Crypto Accelerator 4000 的可調整驅動程式參數，並說明如何使用 `ndd` 公用程式與 `vca.conf` 檔案設定這些參數。本章還說明如何在 OpenBoot™ PROM 介面上啓用連結參數的自動協商與強制模式，以及如何設定網路 `hosts` 檔案。
- 第 4 章說明如何使用 `vcaadm` 與 `vcadiag` 公用程式，來設定 Sun Crypto Accelerator 4000 介面卡並管理金鑰庫。
- 第 5 章說明如何設定 Sun Crypto Accelerator 4000 介面卡以與 Sun ONE 網站伺服器配合使用。
- 第 6 章說明如何設定 Sun Crypto Accelerator 4000 介面卡以與 Apache 網站伺服器配合使用。
- 第 7 章說明如何使用 SunVTS 診斷應用程式與內建 FCode 自我測試來測試 Sun Crypto Accelerator 4000 介面卡。本章還提供使用 OpenBoot PROM 指令進行疑難排解的方法。

- 第 8 章說明不同組態的介面卡如何與 PKCS#11 介面配合工作。
- 附錄 A 列出了 Sun Crypto Accelerator 4000 介面卡的規格。
- 附錄 B 說明如何在不使用安裝指令碼的情況下手動安裝 Sun Crypto Accelerator 4000 軟體。
- 附錄 C 列出了使用 Sun Crypto Accelerator 4000 軟體設定 Apache 網站伺服器 SSL 支援的指令。
- 附錄 D 說明了 Sun Crypto Accelerator 4000 介面卡隨附的軟體，以及如何建立 OpenSSL 相容應用程式以利用介面卡的編碼加速功能。
- 附錄 E 提供其他軟體組織的軟體注意事項與授權。與 Sun Crypto Accelerator 4000 介面卡配合使用的協力廠商軟體在使用時受相應軟體組織的管轄。
- 附錄 F 將說明 Sun Crypto Accelerator 4000 指令，並列出每個指令的線上說明頁。
- 附錄 G 說明如何將 Sun Crypto Accelerator 4000 介面卡化零爲原廠狀態，即介面卡的 failsafe 模式。

使用 UNIX 指令

本文件不包含基本 UNIX® 指令與程序 (例如：關閉系統、啓動系統及設定裝置) 的資訊。

請參閱下列一個或多個文件以取得此資訊：

- *Solaris 硬體平台指南*
- Solaris 作業環境的線上文件，可在 `http://docs.sun.com` 取得
- 系統隨附的其他軟體文件

Shell 提示

Shell	提示
C Shell	*machine-name*%
C Shell 超級使用者	*machine-name*#
Bourne Shell 與 Korn Shell	$
Bourne Shell 與 Korn Shell 超級使用者	#

排版慣例

字型	意義	範例
AaBbCc123	指令、檔案及目錄的名稱；電腦的螢幕輸出	請編輯您的 .login 檔案。 請使用 ls -a 列出所有檔案。 % You have mail.
AaBbCc123	您所鍵入的內容 (相對於電腦的螢幕輸出)	% **su** Password:
AaBbCc123	書名、新的字彙或術語、要強調的字彙	請參閱*使用者指南*第 6 章。 這些被稱爲*類別*選項。 您*必須*是超級使用者才能執行此操作。
	指令行變數；用實際的名稱或值取代	要刪除檔案，請鍵入 rm *檔案名稱*。

線上存取 Sun 文件

您可以在下列網站檢視、列印或購買各種 Sun 文件 (包括本土化版本)：

http://www.sun.com/documentation

與 Sun 技術支援聯絡

如果您在本文件中找不到本產品技術問題的解答，請到：

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

Sun 歡迎您提出寶貴意見

Sun 非常樂於提高文件品質，誠心歡迎您提出寶貴意見與建議。您可以將您的意見傳送到：

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

請隨函附上文件書名與文件號碼：

Sun Crypto Accelerator 4000 介面卡 1.1 版安裝與使用者指南，文件號碼 817-5928-10

第 1 章

產品概述

本章提供 Sun Crypto Accelerator 4000 介面卡的概述，章節如下：

產品功能

Sun Crypto Accelerator 4000 介面卡是一個十億位元乙太網路介面卡，可在 Sun 伺服器上支援 IPsec 與 SSL (對稱式與非對稱式) 編碼硬體加速。除了可作爲標準十億位元乙太網路介面卡用於未加密的網路流量傳輸外，該介面卡還包含編碼硬體，比標準軟體解決方案支援更高的傳送量，以用於加密 IPsec 流量傳輸。

該介面卡在安裝後即可使用 `vcaadm` 公用程式進行初始化與設定，該公用程式可管理金鑰庫與使用者資訊，並可決定介面卡的安全操作等級。設定金鑰庫與安全管理員帳號後，可使用 `iplsslcfg` 與 `apsslcfg` 指令碼來設定 Sun ONE 網站與應用程式伺服器，或 Apache 網站伺服器，以使用該介面卡進行 SSL 加速。您還可以使用 Sun ONE 管理主控台與 `modutil` 和 `certutil` 公用程式，來設定 Sun ONE 目錄、訊息及入口網站伺服器，以使用該介面卡進行 SSL 加速。此外，需要 PKCS#11 介面以取得金鑰庫與編碼服務的大多數應用程式均可使用該介面卡。

主要通訊協定與介面

Sun Crypto Accelerator 4000 介面卡可以在現有乙太網路設備上運作，條件如下：乙太網路框架大小位於標準之內 (64 到 1518 位元組)、框架格式符合標準，並符合下列標準與通訊協定：

- 全尺寸 PCI 33/66 Mhz，32/64 位元
- IEEE 802.3 CSMA/CD (乙太網路)

- IEEE 802.2 邏輯連結控制
- SNMP (有限的 MIB)
- 全雙工與半雙工十億位元介面 (IEEE 802.z)
- 通用雙電壓訊號 (3.3V 與 5V)

主要功能

- 採用銅或光纖介面的十億位元乙太網路
- 加速 IPsec 與 SSL 編碼功能
- 工作階段建立速率：高達每秒 4300 次作業
- 大量加密速率：高達 800 Mbps
- 提供高達 2048 位元的 RSA 加密
- 最高可提供快 10 倍的 3DES 大量資料加密
- 爲 Sun ONE 網站伺服器提供了防篡改、集中式安全金鑰與憑證管理，可提高安全性並簡化金鑰管理
- 專爲 FIPS 140-2 第 3 級憑證設計
- 低 CPU 使用率 — 有效釋放伺服器系統資源與頻寬
- 安全私人金鑰儲存與管理
- 在 Sun 中階與高階伺服器上提供動態重新組態 (DR) 與備援/當機接手支援
- 在多個 CPU 之間平衡 RX 封包負載
- 完整的流量控制支援 (IEEE 802.3x)

Sun Crypto Accelerator 4000 介面卡在設計上符合聯邦資訊處理標準 (FIPS) 140-2 第 3 級中規定的編碼模組安全要求。

支援的應用程式

- Solaris 8 與 9 作業環境 (IPsec VPN)
- Sun ONE Web Server 4.1 與 6.0
- Sun ONE Application Server 7.0
- Sun ONE Directory Server 5.2
- Sun ONE Messaging Server 5.2
- Sun ONE Portal Server 6.2
- Apache Web Server 1.3.x 與 2.x

支援的編碼通訊協定

本介面卡支援下列通訊協定：

- 用於 IPv4 與 IPv6 的 IPsec，包含 IKE
- SSLv2、SSLv3、TLSv1 (傳輸層安全性)

本介面卡可加速下列 IPsec 功能：

- ESP (DES、3DES) 加密
- ESP (SHA1、MD5) 驗證 *
- AH (SHA1、MD5) 驗證 *

* 設定用於線上 IPsec 加速時 (請參閱第 5 頁的「線上 IPsec 硬體加速」)

本介面卡可加速下列 SSL 功能：

- 保全用戶端與伺服器間建立的一組編碼參數與私密金鑰
- 保全介面卡上儲存的金鑰 — 金鑰經過加密後才從介面卡送出

診斷支援

- 使用者可透過 OpenBoot PROM 執行的自我測試
- SunVTS 診斷測試

編碼演算法加速

本介面卡可以加速在硬體與軟體上的編碼演算法。這個問題複雜的原因在於，加速編碼演算法的成本並非所有演算法都一致。有些編碼演算法是特別設計在硬體上執行，而有些則是使用軟體來執行。若使用硬體加速，必須將資料從使用者應用程式傳送到硬體加速裝置，然後再將結果傳回使用者應用程式，因而增加了額外成本。請注意，部分編碼演算法可以經由高度微調的軟體執行，速度和在專用硬體中執行一樣快。

支援的編碼演算法

Sun Crypto Accelerator 4000 驅動程式 (`vca`) 會檢查所有編碼要求，然後決定最佳加速位置 (主機處理器或 Sun Crypto Accelerator 4000)，以達成最大傳送量。負載分佈是根據編碼演算法、目前工作負載、以及資料大小來決定的。

本介面卡可加速下列 IPsec 演算法：

表 1-1 IPsec 編碼演算法

類型	演算法
對稱式	DES、3DES
雜湊*	MD5、SHA1

* 設定用於線上 IPsec 硬體加速時。

本介面卡可以加速下列 SSL 演算法。

表 1-2 SSL 編碼演算法

類型	演算法
對稱式	DES、3DES、ARCFOUR
非對稱式	Diffie-Hellman (限 Apache) 與 RSA (高達 2048 位元金鑰)、DSA
雜湊	MD5、SHA1

IPsec 加速

本介面卡支援兩種形式的 IPsec 加速：頻帶外與線上。這兩種組態均會將 SPARC® 處理器需要執行的高常耗性編碼操作卸載到介面卡。請參閱第 49 頁的「設定 IPsec 硬體加速」。

表 1-3 加速 IPsec 演算法

演算法	頻帶外	線上
DES	X	X
3DES	X	X
MD5		X
SHA1		X

頻帶外 IPsec 硬體加速

將介面卡設定用於頻帶外 IPsec 加速時，可以加速安裝於 Solaris 9 (或更新版本) 系統中硬體上所執行的受支援加密與解密操作。所有 IPsec 特定封包處理程序均由主機 Solaris IPsec 軟體來執行。請參閱第 50 頁的「啓用頻帶外 IPsec 加速」。

注意 – 無需組態或微調 IPsec 即可在 Solaris 9 中將介面卡用於頻帶外 IPsec 加速。您只需安裝 Sun Crypto Accelerator 4000 套件並重新啓動。

線上 IPsec 硬體加速

將介面卡設定用於線上 IPsec 加速時，可以加速安裝於 Solaris 9 12/03 (或更新版本) 系統中硬體上所執行的受支援加密、解密及驗證操作。部分 IPsec 特定封包處理程序將由介面卡直接執行。請參閱第 50 頁的「啓用線上 IPsec 加速」以取得有關如何設定介面卡以進行線上 IPsec 加速的說明。

SSL 加速

表 1-4 顯示了哪些 SSL 加速演算法可以卸載到硬體，以及哪些軟體演算法可以提供給 Sun ONE 與 Apache 網站伺服器使用。

表 1-4 支援的 SSL 演算法

	Sun ONE 網站伺服器		**Apache 網站伺服器**	
演算法	**硬體**	**軟體**	**硬體**	**軟體**
RSA	X	X	X	X
DSA	X	X	X	X
ARCFOUR		X		X
Diffie-Hellman			X	X
DES	X	X	X	X
3DES	X	X	X	X
MD5	X	X		
SHA1	X	X		

大量加密

根據預設值，供 Sun ONE 伺服器軟體使用的 Sun Crypto Accelerator 4000 大量加密功能已停用。您必須建立一個檔案並重新啓動 Sun ONE 伺服器軟體，以手動啓用此功能。

要使 Sun ONE 伺服器軟體能夠使用介面卡的大量加密功能，只需在 `/etc/opt/SUNWconn/cryptov2/` 目錄下建立一個名爲 `sslreg` 的空檔案，然後重新啓動伺服器軟體。

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

要停用大量加密功能，則必須刪除 `sslreg` 檔案，然後重新啓動伺服器軟體。

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

根據預設值，供 Apache 網站伺服器軟體使用的大量加密功能已啓用，您無法停用此功能。

硬體概述

Sun Crypto Accelerator 4000 硬體是一個全尺寸 (4.2 英吋 × 12.283 英吋) 的編碼加速器 PCI 十億位元乙太網路介面卡，可在 Sun 伺服器上增強 IPsec 與 SSL 的效能。

Sun Crypto Accelerator 4000 MMF 介面卡

Sun Crypto Accelerator 4000 MMF 介面卡是一個單埠十億位元乙太網路光纖 PCI 匯流排介面卡，僅適用於 1000 Mbps 乙太網路。

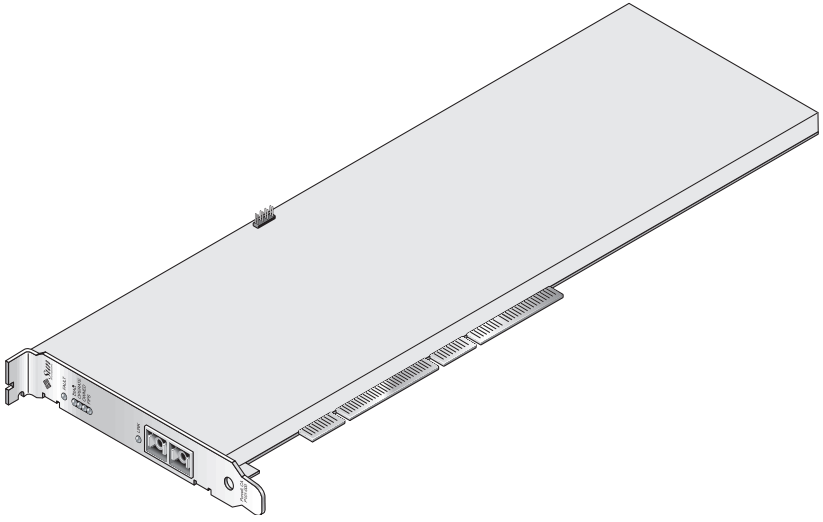

圖 1-1 Sun Crypto Accelerator 4000 MMF 介面卡

LED 顯示

表 1-5 MMF 介面卡的前面板顯示 LED

標記	亮燈意義	顏色
FAULT	在介面卡處於 HALTED (嚴重錯誤) 狀態或低階硬體初始化失敗時亮起。 如果啓動時發生錯誤，則會閃爍。	紅色
DIAG	在 POST、DIAGNOSTICS 及 FAILSAFE (韌體未升級) 狀態下亮起。 在執行 DIAGNOSTICS 時閃爍。	綠色
OPERATE	在 POST、DIAGNOSTICS 及 DISABLED (驅動程式未安裝) 狀態下亮起。 在 IDLE、OPERATIONAL 及 FAILSAFE 狀態下閃爍。	綠色
INIT	如果安全管理員已使用 `vcaadm` 初始化介面卡，則會亮起。請參閱第 62 頁的「使用 `vcaadm` 初始化介面卡」。 如果具有 ZEROIZE 跳線，則會閃爍。	綠色
FIPS	在 FIPS 140-2 第 3 級認證模式下運作時亮起。 在非 FIPS 模式下運作時熄滅。	綠色
LINK	在連結啓用時亮起。	綠色

Sun Crypto Accelerator 4000 UTP 介面卡

Sun Crypto Accelerator 4000 UTP 介面卡是一個單埠十億位元乙太網路銅線 PCI 匯流排介面卡，可以設定在 10、100 或 1000 Mbps 乙太網路中運作。

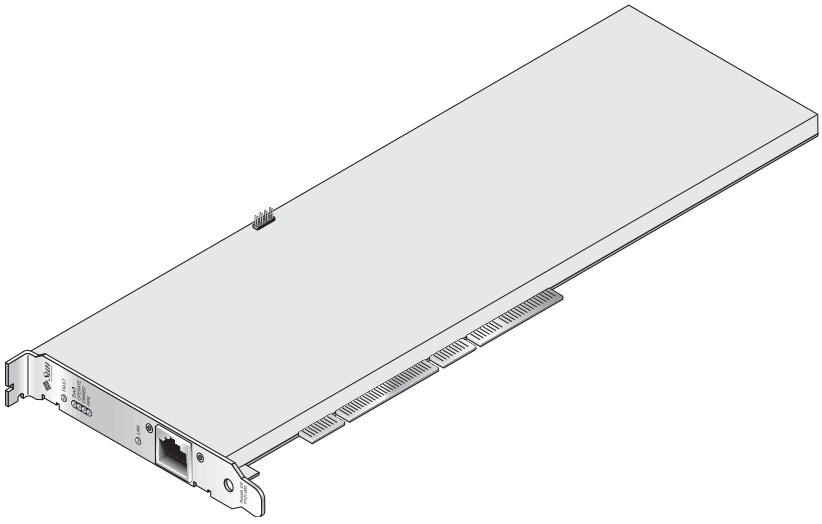

圖 1-2 Sun Crypto Accelerator 4000 UTP 介面卡

LED 顯示

表 1-6 UTP 介面卡的前面板顯示 LED

標記	亮燈意義	顏色
FAULT	在介面卡處於 HALTED (嚴重錯誤) 狀態或低階硬體初始化失敗時亮起。 如果啓動時發生錯誤，則會閃爍。	紅色
DIAG	在 POST、DIAGNOSTICS 及 FAILSAFE (韌體未升級) 狀態下亮起。 在執行 DIAGNOSTICS 時閃爍。	綠色
OPERATE	在 POST、DIAGNOSTICS 及 DISABLED (驅動程式未安裝) 狀態下亮起。 在 IDLE、OPERATIONAL 及 FAILSAFE 狀態下閃爍。	綠色
INIT	如果安全管理員已使用 `vcaadm` 初始化介面卡，則會亮起。請參閱第 62 頁的「使用 `vcaadm` 初始化介面卡」。 如果具有 ZEROIZE 跳線，則會閃爍。	綠色
FIPS	在 FIPS 140-2 第 3 級認證模式下運作時亮起。 在非 FIPS 模式下運作時熄滅。	綠色
1000	在使用十億位元乙太網路時亮起。	綠色
ACTIVITY (無標記)	在連結正在進行傳輸或接收操作時亮起。	黃色
LINK (無標記)	在連結啓用時亮起。	綠色

注意 – 在本書中提到 Sun ONE Web Server 4.1 或 6.0 時，將以服務套件編號 (SP9 或 SP1) 來表示。

動態重新組態與高可用性

Sun Crypto Accelerator 4000 硬體及相關軟體可以讓支援動態重新組態 (DR) 與熱插拔的 Sun 平台運作更有效率。在 DR 或熱插拔作業期間，Sun Crypto Accelerator 4000 軟體層會自動偵測新增或移除的介面卡，並調整排程演算法以配合硬體資源的變動。

爲達成高可用性 (HA) 組態，數個 Sun Crypto Accelerator 4000 介面卡可以同時安裝在一個系統或網域內，以確保硬體加速持續可用。Sun Crypto Accelerator 4000 幾乎不會發生硬體故障，但如果出現這種狀況，軟體層會偵測出故障，並將有故障的介面卡從可用硬體編碼加速器清單中移除。Sun Crypto Accelerator 4000 軟體會調整排程演算法以配合硬體資源的縮減。後續編碼要求會排程到其餘的介面卡上。

請注意，Sun Crypto Accelerator 4000 硬體提供了高品質的熵 (entropy) 以產生長期金鑰。如果移除網域或系統中所有的 Sun Crypto Accelerator 4000 介面卡，將會以低品質的熵產生長期金鑰。

負載分擔

Sun Crypto Accelerator 4000 軟體會在 Solaris 網域或系統上所有安裝的介面卡之間分配負載。收到的編碼要求會依據固定長度工作佇列，在介面卡間進行分配。編碼要求會送到第一個介面卡，而後續要求仍會送到第一個介面卡，直到滿載爲止。一旦第一個介面卡滿載了，隨後的要求會依佇列送到下一個可以接受此類要求的可用介面卡上。佇列機制的設計可促進結合介面卡上的要求，以發揮傳送量的最大效果。

硬體與軟體需求

表 1-7 提供了介面卡硬體與軟體 Sun Crypto Accelerator 4000 需求的摘要。

表 1-7 硬體與軟體需求

硬體與軟體	要求
硬體	Sun Fire™ V120、V210、V240、280R、V480、V880、4800、4810、6800、12K、15K；Netra™ 20 (lw4)；Sun Blade™ 100、150、1000、2000
作業環境	Solaris 8 2/02 與未來相容版本 (需要使用 Solaris 9 才能加速 IPsec)

所需修正程式

請參閱 *Sun Crypto Accelerator 4000 介面卡 1.1 版版本說明*，取得所需修正程式的詳細資訊。

在系統上執行 Sun Crypto Accelerator 4000 介面卡時需要下列修正程式。Solaris 更新版包含早期版本的修正程式。使用 `showrev -p` 指令可判斷所列的修正程式是否已安裝。

您可以從下列網站下載修正程式：`http://sunsolve.sun.com`

請安裝最新版本的修正程式。修正程式每推出一個新的版本，編號尾數 (例如：-01) 也會跟著增加。如果網站上的版本比下表中更新，則屬較新版本。

如果在 SunSolve℠ 網站上找不到所需的修正程式，請與當地的業務代表聯絡。

Apache 網站伺服器修正程式

如果您計劃將 Apache 網站伺服器與 Solaris 8 配合使用，您必須在安裝 Sun Crypto Accelerator 4000 軟體之前先安裝修正程式 109234-09。新增 `SUNWkcl2a` 套件後，系統會設定爲 Apache Web Server mod_ssl 1.3.26。

Solaris 8 修正程式

表 1-8 列出了 Sun Crypto Accelerator 4000 軟體所需的 Solaris 8 修正程式。

表 1-8 所需的 Solaris 8 修正程式

修正程式 ID	說明
110383-01	`libnvpair`
108528-23	`KU-05` (`nvpair` 支援)
112438-01	`/dev/random`
110900-10	`pcifg`、SunFire 15K 支援及 DR
110824-04	DR
110842-11	匯流排速度與 DR
110839-04	次要節點與 DLPI 供應器名稱
109234-09	Apache 支援

Solaris 9 修正程式

表 1-9 列出了 Sun Crypto Accelerator 4000 軟體所需的 Solaris 9 修正程式。

表 1-9 所需的 Solaris 9 修正程式

修正程式 ID	說明
113068-04	匯流排速度、Sun Fire 15K 支援及 DR
112838-08	`pcicfg`、DR 及 Sun Fire 15K 支援
113218-08	十億位元效能 `vca` 記憶體流失
112904-08	十億位元效能
114758-01	次要節點與 DLPI 供應器名稱
112233-08	(只有 Solaris 9 9/04 之前的 Solaris 版本才需要)

第 2 章

安裝 Sun Crypto Accelerator 4000 介面卡

本章說明如何安裝 Sun Crypto Accelerator 4000 硬體以及如何使用自動指令碼安裝與移除軟體。本章包含下列章節：

安裝介面卡的硬體與軟體後，您需要使用組態與金鑰庫資訊初始化介面卡。請參閱第 62 頁的「使用 vcaadm 初始化介面卡」以取得有關如何初始化介面卡的資訊。

處理介面卡

所有介面卡都包裝在特別的防靜電袋中，以在運送與存放的過程中保護介面卡。爲了避免介面卡上對靜電極爲敏感的元件受損，在您的身體接觸介面卡前，請使用下列其中一種方法減少身上的靜電：

- 觸碰電腦的金屬邊緣。
- 在手腕繫上防靜電腕帶，並接地至金屬表面。

警告 – 爲了避免損壞介面卡上敏感的元件，握持介面卡時請穿戴防靜電腕帶，拿取介面卡時請握住邊緣，並將介面卡放置在防靜電表面上 (如隨卡附帶的塑膠袋)。

安裝介面卡

安裝 Sun Crypto Accelerator 4000 介面卡程序包含將介面卡插入系統，並載入軟體工具。硬體安裝說明只包含安裝介面卡的一般步驟。請參閱系統隨附的文件，以取得特定的安裝說明。

▼ 安裝硬體

1. **請以超級使用者身份登入，並按照系統隨附的說明關閉電腦、切斷電源、拔下電源線，然後卸下電腦護蓋。**
2. **找出未使用的 PCI 插槽 (最好是 64 位元、66 MHz 插槽)。**
3. **將防靜電腕帶繫在手腕上，並將另一頭接地至金屬表面。**
4. **使用十字型螺絲起子，將螺絲從 PCI 插槽蓋卸下。**

   將螺絲保存好以在步驟 5 中固定托架。
5. **握住 Sun Crypto Accelerator 4000 介面卡的邊緣，從塑膠袋中取出後插入 PCI 插槽，然後固定後托架上的螺絲。**
6. **裝回電腦護蓋，重新連接電源線，然後開啟系統電源。**
7. **在 OpenBoot PROM** `ok` **提示下執行** `show-devs` **指令，以檢查介面卡是否已正確安裝：**

```
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
.
```

在上述範例中，`/pci@8,600000/network@1` 代表 Sun Crypto Accelerator 4000 介面卡的裝置路徑。系統中的每個介面卡都會有這一行。

要判斷 Sun Crypto Accelerator 4000 裝置屬性是否正確列出，請在 ok 提示下，瀏覽至裝置路徑，然後鍵入 .properties 以顯示屬性清單。

```
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         00 03 ba 0e 99 ca
version                   Sun PCI Crypto Accelerator 4000 1000Base-T FCode
FCode 2.11.13 03/03/04
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
max-latency               00000040
cache-line-size           00000010
max-latency               00000040
min-grant                 00000040
subsystem-vendor-id       0000108e
subsystem-id              00003de8
revision-id               00000002
device-id                 0000b555
vendor-id                 00008086
```

安裝 Sun Crypto Accelerator 4000 軟體

Sun Crypto Accelerator 4000 軟體包含在 Sun Crypto Accelerator 4000 CD 中。您可能需要從 SunSolve 網站下載修正程式。請參閱第 10 頁的「所需修正程式」以取得更多資訊。

有兩種方法可以安裝軟體：手動安裝或使用 `install` 指令碼安裝。本章節說明如何使用 `install` 指令碼安裝軟體。要手動安裝軟體，請參閱附錄 B。

▼ 安裝軟體

1. **將 Sun Crypto Accelerator 4000 CD 放入連接到系統的 CD-ROM 光碟機。**
   - 如果系統執行的是 Sun Enterprise Volume Manager™，應會自動將 CD-ROM 掛載到 `/cdrom/cdrom0` 目錄。
   - 如果系統未執行 Sun Enterprise Volume Manager，請如下所述掛載 CD-ROM：

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

您可在 /cdrom/cdrom0 目錄中看到下列檔案與目錄。

表 2-1 /cdrom/cdrom0 目錄中的檔案

檔案或目錄	內容	
Copyright	美國著作權聲明檔案	
FR_Copyright	法文著作權聲明檔案	
install	安裝 Sun Crypto Accelerator 4000 軟體的指令碼	
remove	移除 Sun Crypto Accelerator 4000 軟體的指令碼	
Docs	*Sun Crypto Accelerator 4000 介面卡 1.1 版安裝與使用者指南* *Sun Crypto Accelerator 4000 介面卡版本注意事項*	
Packages	包含 Sun Crypto Accelerator 4000 軟體套件：	
	SUNWkcl2r	編碼核心元件
	SUNWkcl2u	編碼管理公用程式與程式庫
	SUNWkcl2a	Apache SSL 支援 *(選用)*
	SUNWkcl2m	編碼管理說明頁 (*選用*)
	SUNWvcar	VCA 編碼加速器 (root)
	SUNWvcau	VCA 編碼加速器 (usr)
	SUNWvcaa	VCA 管理
	SUNWvcafw	VCA 韌體
	SUNWvcamn	VCA 編碼加速器說明頁 (*選用*)
	SUNWvcav	VCA 編碼加速器的 SunVTS 測試 *(選用)*
	SUNWkcl2o	SSL 開發工具與程式庫 *(選用)*
	SUNWkcl2i.u	具有 KCLv2 編碼的 IPsec 加速 *(選用)*

此安裝指令碼會按特定順序安裝所需套件，這些套件必須在安裝任何選用套件之前安裝。安裝所需套件後，您可以按任何順序安裝與移除選用套件。

只有在計劃使用 Apache 作爲網站伺服器時，才安裝選用的 SUNWkcl2a 套件。

只有在計劃重新連結到其他版本的 Apache 網站伺服器時，才安裝選用的 SUNWkcl2o 套件。

只有在計劃執行 SunVTS 測試時，才安裝選用的 SUNWvcav 套件。您必須先安裝 SunVTS 4.4 或更新版本 (可高達 5.x)，才能安裝 SUNWvcav 套件。

注意 – Sun Crypto Accelerator 4000 CD 上的選用 SUNWkcl2i.u 套件僅具有 .u 副檔名。安裝此套件後，名稱會變更爲 SUNWkcl2i。CD 上此套件的 .u 副檔名會將該套件定義爲 sun4u architecture-specific。

2. **鍵入下列指令以安裝所需的軟體：**

```
# cd /cdrom/cdrom0
# ./install
```

安裝指令碼會分析系統以決定需要安裝何種修正程式，然後安裝此類修正程式、安裝主要軟體並會選擇性安裝選用軟體。例如：

注意 – 下列範例中已省略著作權與授權資訊。請參閱附錄 E 以瞭解著作權與軟體授權。

```
# ./install
This program installs the software for the Sun Crypto Accelerator
4000, Version 1.1.

*** Checking if Sun Crypto Accelerator support is already installed...
*** Checking for required OS patch(es):
 113146-01 112838-07 113068-04 113449-02 113453-04 114758-01
*** Checking for incompatible OS patch(es) ...
*** Checking for optional package dependencies...

Do you wish to install the optional Crypto IPsec Acceleration software
(SUNWkcl2i.u)?  [y,n,?,q]

Do you wish to install the optional Crypto Apache Support (SSL) (SUNWkcl2a
SUNWkcl2o)?  [y,n,?,q] y

Do you wish to install the optional Crypto QA Tools (SUNWkcl2q SUNWvcaq)?
[y,n,?,q] n

Do you wish to install the optional VCA Crypto Accelerator/Gigabit Ethernet
SunVTS Diagnostics (SUNWvcav)?  [y,n,?,q] n

This script is about to take the following actions:
- Install Sun Crypto Accelerator 4000 support for Solaris 9
- Install Optional Crypto IPsec Acceleration software
- Install Optional Crypto Apache Support (SSL) software

To cancel installation of this software, press 'q' followed by a Return.
 **OR**
Press Return key to begin installation:

*** Installing Sun Crypto Accelerator 4000 software for Solaris 9...
Installing required packages:
```

```
 SUNWkcl2r SUNWkcl2u SUNWkcl2m SUNWvcar SUNWvcau SUNWvcaa SUNWvcamn SUNWvcafw

Installation of <SUNWkcl2u> was successful.
Installation of <SUNWkcl2m> was successful.
Installation of <SUNWvcar> was successful.
Installation of <SUNWvcau> was successful.
Installation of <SUNWvcaa> was successful.
Installation of <SUNWvcamn> was successful.
Installation of <SUNWvcafw> was successful.
*** Installing selected optional software for Solaris 9...
Installing optional package(s):
 SUNWkcl2i.u SUNWkcl2a SUNWkcl2o
Installation of <SUNWkcl2i> was successful.

Checking operating environment requirements...
Determining package requirements...
Verifying required packages are installed...
All required packages installed.
Determining patch requirements...
Verifying required patches are installed...
Requirement for 113146-01 met by 113146-01.
All required patches installed.

Installation of <SUNWkcl2a> was successful.

Installation of <SUNWkcl2o> was successful.
*** Installation complete.
```

選擇要安裝的選用套件

要僅安裝爲 Apache 網站伺服器及 Sun Crypto Accelerator 4000 線上說明頁提供 SSL 支援的選用套件，請選擇 `SUNWkcl2a` 與 `SUNWkcl2m`。

要安裝全部選用軟體套件，請選擇下列項目：`SUNWkcl2a`、`SUNWkcl2m`、`SUNWvcamn`、`SUNWvcav`、`SUNWkcl2o` 及 `SUNWkcl2i.u`。

請參閱表 2-1 以取得上述範例中選用套件的套件內容說明。

目錄與檔案

表 2-2 顯示預設安裝 Sun Crypto Accelerator 4000 軟體時所建立的目錄。

表 2-2 Sun Crypto Accelerator 4000 目錄

目錄	內容
`/etc/opt/SUNWconn/vca/keydata`	金鑰庫資料 (已加密)
`/opt/SUNWconn/cryptov2/bin`	公用程式
`/opt/SUNWconn/cryptov2/lib`	支援程式庫
`/opt/SUNWconn/cryptov2/sbin`	管理指令

圖 2-1 顯示這些目錄與檔案的結構。

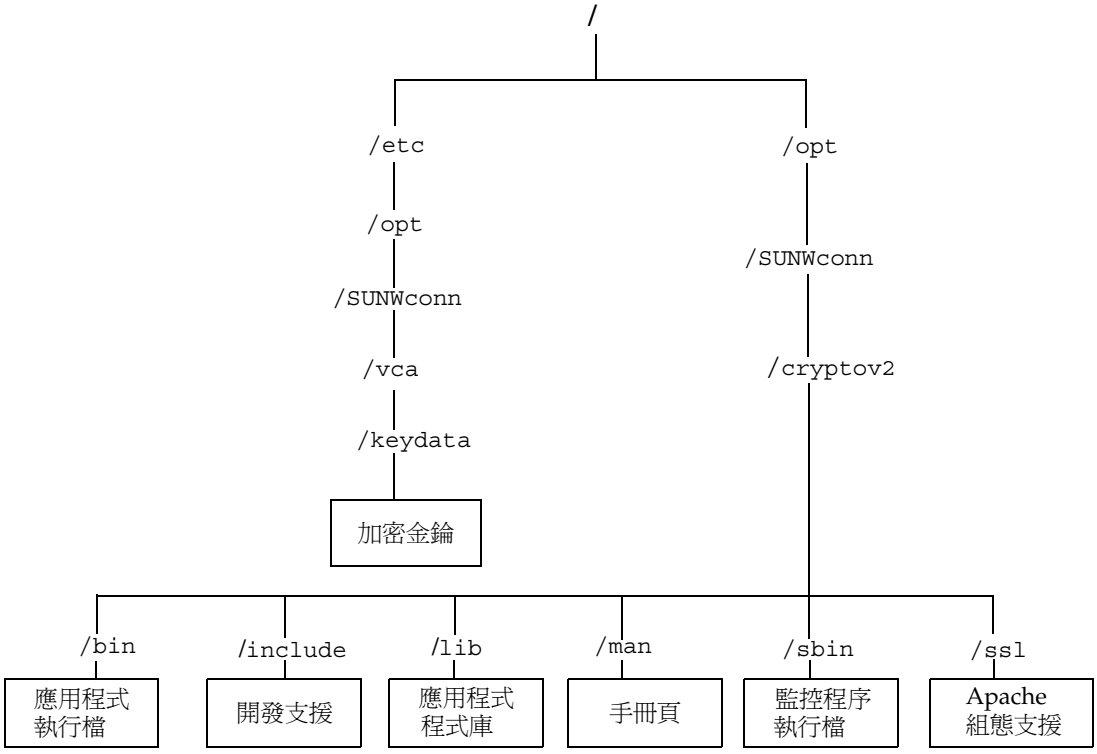

圖 2-1 Sun Crypto Accelerator 4000 目錄與檔案

注意 – 安裝 Sun Crypto Accelerator 4000 硬體與軟體後，您需要使用組態與金鑰庫資訊初始化介面卡。請參閱第 62 頁的「使用 `vcaadm` 初始化介面卡」以取得有關如何初始化介面卡的資訊。

移除 Sun Crypto Accelerator 4000 軟體

可以使用三種方法來移除軟體：CD-ROM 上的 `remove` 指令碼、伺服器上的 `/var/tmp/crypto_acc.remove` 指令碼或 `pkgrm` 指令。本章節說明如何使用兩種移除指令碼移除軟體。要取得有關使用 `pkgrm` 指令移除軟體的說明，請參閱附錄 B。

如果您 `install` 指令碼安裝軟體，請使用 `remove` 指令碼移除軟體。如果手動安裝軟體，請使用 `/var/tmp/crypto_acc.remove` 指令碼 (附錄 B)。

▼ 使用 `remove` 指令碼移除軟體

- **插入 Sun Crypto Accelerator 4000 CD-ROM 後，鍵入下列內容：**

```
# cd /cdrom/cdrom0
# ./remove
```

▼ 使用 `/var/tmp/crypto_acc.remove` 指令碼移除軟體

此安裝記錄可在下列路徑中找到：

```
/var/tmp/crypto_acc.install.2003.10.13
```

- **鍵入下列內容：**

```
# /var/tmp/crypto_acc.remove
```

第 3 章

設定驅動程式參數

本章說明如何設定 Sun Crypto Accelerator 4000 UTP 與 MMF 乙太網路介面卡使用的 vca 裝置驅動程式參數。本章包含下列章節：

乙太網路裝置驅動程式 (vca) 參數

vca 裝置驅動程式控制 Sun Crypto Accelerator 4000 UTP 與 MMF 乙太網路裝置。vca 驅動程式安裝於 Sun Crypto Accelerator 4000 (108e 是廠商 ID，3de8 是 PCI 裝置 ID) 的 UNIX pci 名稱屬性 pci108e,3de8。

您可以手動設定 vca 裝置驅動程式參數以自訂系統中的每個 Sun Crypto Accelerator 4000 裝置。本章節概述在介面卡中使用的 Sun Crypto Accelerator 4000 乙太網路裝置功能，列出可用的 vca 裝置驅動程式參數，並說明如何設定這些參數。

Sun Crypto Accelerator 4000 乙太網路 UTP 與 MMF PCI 介面卡可以操作第 37 頁的「使用 OpenBoot PROM 啓用連結參數的自動協商或強制模式」列出的速度與模式。根據預設值，vca 裝置在自動協商模式中使用連結 (連結夥伴) 遠端操作，以選擇 speed、duplex 及 link-clock 參數操作的常見模式。link-clock 參數僅適用於介面卡以 1000 Mbps 操作的情況。vca 裝置也可以爲這些參數中的每一個設定，以便以強制模式操作。

警告 – 要建立適當的連結，兩個連結夥伴必須以自動協商或強制模式爲每個 `speed`、`duplex` 及 `link-clock` (僅適用於 1000 Mbps) 參數操作。如果兩個連結夥伴不以相同的模式爲這些參數的每一個操作，將發生網路錯誤。請參閱第 37 頁的「使用 OpenBoot PROM 啓用連結參數的自動協商或強制模式」。

驅動程式參數值與定義

表 3-1 說明 `vca` 裝置驅動程式的參數與設定。

表 3-1 `vca` 驅動程式參數、狀態及說明

參數	狀態	說明
`instance`	讀取與寫入	裝置例項
`adv-autoneg-cap`	讀取與寫入	操作模式參數
`adv-1000fdx-cap`	讀取與寫入	操作模式參數 (限 MMF 介面卡)
`adv-1000hdx-cap`	讀取與寫入	操作模式參數
`adv-100fdx-cap`	讀取與寫入	操作模式參數 (限 UTP 介面卡)
`adv-100hdx-cap`	讀取與寫入	操作模式參數 (限 UTP 介面卡)
`adv-10fdx-cap`	讀取與寫入	操作模式參數 (限 UTP 介面卡)
`adv-10hdx-cap`	讀取與寫入	操作模式參數 (限 UTP 介面卡)
`adv-asmpause-cap`	讀取與寫入	流量控制參數
`adv-pause-cap`	讀取與寫入	流量控制參數
`pause-on-threshold`	讀取與寫入	流量控制參數
`pause-off-threshold`	讀取與寫入	流量控制參數
`link-master`	讀取與寫入	1 Gbps 速度的強制模式參數
`enable-ipg0`	讀取與寫入	在傳送封包之前啓用額外延遲時間
`ipg0`	讀取與寫入	在傳送封包之前的額外延遲時間
`ipg1`	讀取與寫入	封包間隙參數
`ipg2`	讀取與寫入	封包間隙參數
`rx-intr-pkts`	讀取與寫入	接收中斷遮沒值
`rx-intr-time`	讀取與寫入	接收中斷遮沒值

表 3-1 vca 驅動程式參數、狀態及說明 *(續)*

參數	狀態	說明
red-dv4to6k	讀取與寫入	隨機早期偵測與封包丟棄向量
red-dv6to8k	讀取與寫入	隨機早期偵測與封包丟棄向量
red-dv8to10k	讀取與寫入	隨機早期偵測與封包丟棄向量
red-dv10to12k	讀取與寫入	隨機早期偵測與封包丟棄向量
tx-dma-weight	讀取與寫入	PCI 介面參數
rx-dma-weight	讀取與寫入	PCI 介面參數
infinit-burst	讀取與寫入	PCI 介面參數
disable-64bit	讀取與寫入	PCI 介面參數

通知連結參數

下列參數將確定傳送與接收，由 vca 驅動程式通知給其連結夥伴的 speed 與 duplex 連結參數。表 3-2 說明操作模式參數及其預設值。

注意 – 如果參數的初始設定爲 0，將無法變更。如果您嘗試變更爲 0 的初始設定，它將重新恢復爲 0。根據預設值，這些參數將設定爲 vca 裝置的功能。

Sun Crypto Accelerator 4000 UTP 介面卡通知連結參數與那些在表 3-2 中顯示的 Sun Crypto Accelerator 4000 MMF 參數不同。

表 3-2 操作模式參數

參數	說明	UTP 介面卡	MMF 介面卡
adv-autoneg-cap	由硬體通知的本地介面功能 0 = 強制模式 1 = 自動協商 (預設)	X	X
adv-1000fdx-cap	由硬體通知的本地介面功能 0 = 非 1000 Mbps 全雙工功能 1 = 1000 Mbps 全雙工功能 (預設)		X
adv-1000hdx-cap	由硬體通知的本地介面功能 0 = 非 1000 Mbps 半雙工功能 1 = 1000 Mbps 半雙工功能 (預設)	X	X

表 3-2 操作模式參數 *(續)*

參數	說明	UTP 介面卡	MMF 介面卡
adv-100fdx-cap	由硬體通知的本地介面功能 0 = 非 100 Mbps 全雙工功能 1 = 100 Mbps 全雙工功能 (預設)	X	
adv-100hdx-cap	由硬體通知的本地介面功能 0 = 非 100 Mbps 半雙工功能 1 = 100 Mbps 半雙工功能 (預設)	X	
adv-10fdx-cap	由硬體通知的本地介面功能 0 = 非 10 Mbps 全雙工功能 1 = 10 Mbps 全雙工功能 (預設)	X	
adv-10hdx-cap	由硬體通知的本地介面功能 0 = 非 10 Mbps 半雙工功能 1 = 10 Mbps 半雙工功能 (預設)	X	

如果表 3-2 中所有之前的參數設定爲 1，自動協商將使用最高的可能速度。如果所有參數設定爲 0，您將會收到下列錯誤訊息：

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

注意 – 在之前的範例中，vca0 是字串 vca 用於每個 Sun Crypto Accelerator 4000 介面卡的 Sun Crypto Accelerator 4000 裝置名稱。此字串後面始終會緊跟著介面卡的裝置例項號碼。因此，vca0 介面卡的裝置例項號碼是 0。

流量控制參數

vca 裝置可以發出 (傳送) 與終止 (接收) 符合 IEEE 802.3x 框架基礎連結等級流量控制通訊協定的暫停框架。在回應接收的流量控制框架時，vca 裝置可以降低傳輸速率。此外，vca 裝置可以發出流量控制框架，要求連結夥伴降低傳輸速度 (如果連結夥伴支援此功能)。根據預設值，驅動程式將在自動協商時通知傳送與接收暫停功能。

表 3-3 提供流量控制關鍵字，並說明其功能。

表 3-3 讀寫流量控制關鍵字說明

關鍵字	說明		
adv-asmpause-cap	MMF 與 UTP 介面卡支援非對稱暫停；因此，vca 裝置僅可以在一個方向上暫停。 0=關閉 (預設) 1=開啓		
adv-pause-cap	此參數具有兩個意義，視 adv-asmpause-cap 的值而定。(預設值=0)		
	參數值 +	**參數值 =**	**說明**
	adv-asmpause-cap=	adv-pause-cap=	
	1	1 或 0	adv-pause-cap 可以決定執行暫停的方向。
	1	1	暫停可以接收，但無法傳送。
	1	0	暫停可以傳送，但無法接收。
	0	1	暫停可以傳送與接收。
	0	1 或 0	adv-pause-cap 決定暫停功能的開啓或關閉。
pause-on-threshold	定義在導致介面卡產生 XON-PAUSE 框架的接收 (RX) FIFO 中之 64 位元組區塊數目。		
pause-off-threshold	定義在導致介面卡產生 XOFF-PAUSE 框架的 RX FIFO 中之 64 位元組區塊數目。		

十億位元強制模式參數

對於十億位元連結，此參數可決定 link-master。通常，會將交換器啓用作爲 link master；在此情況下，此參數可以保持不變。如果不是這種情況，則 link-master 參數可用來將 vca 裝置作爲 link master 啓用。

表 3-4 十億位元強制模式參數

參數	說明
link-master	設定爲 1 時，此參數將啓用主要操作，假設連結夥伴爲從屬操作。 設定爲 0 時，此參數將啓用從屬操作，假設連結夥伴爲主要操作 (預設)。

封包間隙參數

vca 裝置支援 enable-ipg0 的可程式化模式。

在傳送具有啓用 enable-ipg0 的封包 (預設) 時，vca 裝置會增加額外的延遲時間。此時間延遲由 ipg0 參數設定，還有由 ipg1 與 ipg2 參數設定的時間延遲。額外的 ipg0 時間延遲會減少衝突。

如果禁用 enable-ipg0，則會忽略 ipg0 的值，且不會設定任何額外時間延遲。僅使用由 ipg1 與 ipg2 設定的時間延遲。如果其他系統繼續傳送大量的連續封包，停用 enable-ipg0。已啓用 enable-ipg0 的系統在網路上可能沒有足夠的時間。您可以將 ipg0 參數設定爲從 0 至 255 的值以增加額外的延遲時間，此爲媒體位元組延遲時間。表 3-5 定義 enable-ipg0 與 ipg0 參數。

表 3-5 定義 enable-ipg0 與 ipg0 的參數

參數	值	說明
enable-ipg0	0 1	enable-ipg0 啓用 enable-ipg0 停用 (預設值=1)
ipg0	0 至 255	傳送封包 (在接收封包後) 之前的額外延遲時間 (間隙) (預設值=8)

vca 裝置支援可程式化的封包間隙 (IPG) 參數 ipg1 與 ipg2。總 IPG 爲 ipg1 與 ipg2 的和。總 IPG 是 0.096 微秒 (連結速度爲 1000 Mbps)。

表 3-6 列出 IPG 參數的預設值與允許值。

表 3-6 讀寫封包間隙參數值與說明

參數	值(位元組-時間)	說明
ipg1	0 至 255	封包間隙 1 (預設值=8)
ipg2	0 至 255	封包間隙 2 (預設值=4)

根據預設值，驅動程式將 ipg1 設定爲 8 位元組時間，將 ipg2 設定爲 4 位元組時間，均爲標準值。(位元組時間是在連結速度爲 1000 Mbps 時，在連結上傳送一個位元組所用的時間。)

如果網路具有使用較長 IPG (ipg1 與 ipg2 的和) 的系統，且如果那些機器存取網路時好像較慢，請增加 ipg1 與 ipg2 的值，以符合其他機器較長的 IPG。

中斷參數

表 3-7 說明接收中斷遮沒值

表 3-7 別名讀取的 RX 遮沒註冊

欄位名稱	值	說明
rx-intr-pkts	0 至 511	從服務上一封包開始，此數目的封包到達後將中斷。零值表示沒有封包遮沒 (預設值=3)。
rx-intr-time	0 至 524287	從服務上一封包開始，在過去 4.5 微秒 (Usec) 後將中斷。零值表示沒有時間遮沒 (預設值=3)。

隨機早期丟棄參數

這些參數提供基於接收 FIFO 的完整性丟棄封包的功能。根據預設值，會停用此功能。在 FIFO 佔有量達到特定範圍時，將根據預設的可能性丟棄封包。在 FIFO 等級增加時，這種可能性也應該增加。控制封包不會受到丟棄，並不會在統計中計數。

表 3-8 RX 隨機早期偵測 8 位元向量

欄位名稱	值	說明
red-dv4to6k	0 至 255	隨機早期偵測與封包丟棄，適用於 FIFO 門檻值大於 4096 位元組、小於 6,144 位元組的情況。丟棄的可能性可以根據 12.5% 的間隔來進行。例如，如果設定位元 0，則每八個封包中的第一個將在此區域受到丟棄 (預設值=0)。
red-dv6to8k	0 至 255	隨機早期偵測與封包丟棄向量，適用於 FIFO 門檻值大於 6,144 位元組、小於 8,192 位元組的情況。丟棄的可能性可以根據 12.5% 的間隔來進行。例如，如果設定位元 8，則每八個封包中的第一個將在此區域受到丟棄 (預設值=0)。
red-dv8to10k	0 至 255	隨機早期偵測與封包丟棄，適用於 FIFO 門檻值大於 8,192 位元組、小於 10,240 位元組的情況。丟棄的可能性可以根據 12.5% 的間隔來進行。例如，如果設定位元 16，則每八個封包中的第一個將在此區域受到丟棄 (預設值=0)。
red-dv10to12k	0 至 255	隨機早期偵測與封包丟棄，適用於 FIFO 門檻值大於 10,240 位元組、小於 12,288 位元組的情況。丟棄的可能性可以根據 12.5% 的間隔來進行。例如，如果設定位元 24，則每八個封包中的第一個將在此區域受到丟棄 (預設值 =0)。

PCI 匯流排介面參數

這些參數可讓您修改 PCI 介面功能，以便爲指定的應用程式取得更好的 PCI 相互效能。

表 3-9 PCI 匯流排介面參數

參數	說明
`tx-dma-weight`	決定大量循環配置資源仲裁時授權傳送 (TX) 邊的乘數；其值爲 0 至 3 (預設值=0)。零表示沒有額外的加權。其他值使用大量流量的 2 次方。例如：如果 `tx-dma-weight` = 0 且 `rx-dma-weight` = 3，則只要 RX 流量持續到達，RX 流量的優先權比存取 PCI 的 TX 流量大 8 倍。
`rx-dma-weight`	決定大量循環配置資源仲裁時授權 RX 邊的乘數。其值爲 0 至 3 (預設值=0)。
`infinite-burst`	如果啓用此參數且使用了系統支援無限激增，可允許使用無限激增功能。所有封包都通過匯流排後，介面卡才會釋放匯流排。其值爲 0 或 1 (預設值=0)。
`disable-64bit`	關閉介面卡的 64 位元功能。 注意：對於 UltraSPARC® III 的平台，此參數可以預設爲 1。對於 UltraSPARC II 的平台，預設值爲 0。其值爲 0 或 1 (預設值=0，支援 64 位元功能)。

設定 vca 驅動程式參數

您可以使用兩種方式來設定 `vca` 裝置驅動程式參數：

- 使用 `ndd` 公用程式
- 使用 `vca.conf` 檔案

如果您使用 `ndd` 公用程式，只有先重新啓動系統，參數方能生效。此方法適用於測試參數設定。

要設定參數使其在重新啓動系統後依然有效，請在需要爲系統中裝置設定特定參數時，建立 `/kernel/drv/vca.conf` 檔案，然後將參數值新增至此檔案。請參閱第 35 頁的「使用 `vca.conf` 檔案設定驅動程式參數」以取得詳細資料。

使用 ndd 公用程式設定參數

使用 `ndd` 公用程式，以設定重新啓動系統後才有效的參數。

下列幾個部份說明如何使用 `vca` 驅動程式與 `ndd` 公用程式，以便爲每個 `vca` 裝置修改 (使用 `-set` 選項) 或顯示 (不使用 `-set` 選項) 參數。

▼ 爲 ndd 公用程式指定裝置例項

在使用 ndd 公用程式爲 vca 裝置取得或設定參數之前，您必須爲公用程式指定裝置例項。

1. **檢查** /etc/path_to_inst **檔案以識別特定裝置的例項號碼。請參閱** path_to_inst**(4) 線上說明頁。**

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

在上述範例中，三個 Sun Crypto Accelerator 4000 乙太網路例項都來自安裝的介面卡。例項號碼是 0 與 1。

2. **使用例項號碼選擇裝置。**

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

注意 – 在此使用者指南的範例中，*N* 代表裝置的例項號碼。

在您變更選擇前，裝置將保持選定。

非*互*動與*互*動模式

您可以使用 ndd 公用程式的兩個模式：

- 非*互*動
- *互*動

在非*互*動模式中，您可以啓動公用程式以執行特定的指令。執行指令後，您將結束此公用程式。在*互*動模式中，您可以使用公用程式取得或設定多個參數值。請參閱 ndd(1M) 線上說明頁以取得更多資訊。

在非互動模式中使用 ndd *公用程式*

本章節說明如何修改與顯示參數值。

- **要修改參數值，請使用 `-set` 選項。**

  如果您使用 `-set` 選項啓動 ndd 公用程式，公用程式將傳送 *value*，必須指定給已命名的 `/dev/vca` 的驅動程式例項，並將其指定給參數：

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

  變更任何 `adv` 參數後，將出現類似於以下所顯示的訊息：

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

- **要顯示參數值，請指定參數名稱，並省略其值。**

  省略 `-set` 選項後，將假定查詢操作且公用程式將查詢已命名的驅動程式例項，擷取與指定參數相關的值，然後在螢幕上顯示：

```
# ndd /dev/vcaN parameter
```

注意 – 上述範例中，*N* 指的是 `vca` 裝置的例項號碼。此號碼應該反映在其中執行 `kstat` 指令之介面卡的例項號碼。

在互動模式中使用 ndd *公用程式*

- **要在互動模式中修改參數值，請指定 `ndd /dev/vca`*N*，如下所示。**

  然後，ndd 公用程式會提示參數名稱：

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

注意 – 上述範例中，*N* 指的是 `vca` 裝置的例項號碼。此號碼應該反映在其中執行 `kstat` 指令之介面卡的例項號碼。

鍵入參數名稱後，ndd 公用程式會提示參數值 (請參閱表 3-1 至表 3-9)。

- **要列出** vca **驅動程式支援的所有參數，請鍵入** ndd /dev/vca*N*
  (請參閱表 3-1 至表 3-9 中的參數說明)。

```
# ndd /dev/vcaN
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 ?
#
```

注意 – 上述範例中，*N* 指的是 vca 裝置的例項號碼。此號碼應該反映在其中執行 kstat 指令之介面卡的例項號碼。

設定自動協商或強制模式

可以設定下列連結參數以便在自動協商或強制模式中操作：

- speed
- duplex
- link-clock

根據預設值，將爲這些連結參數啓用自動協商模式。在這些參數中的一個處於自動協商模式時，vca 裝置將與連結夥伴通訊，以協商確定相容的值與流量控制功能。將這些參數中的一個設定爲 auto 以外的值時，將不會發生協商，且連結參數設定爲強制模式。在強制模式中，speed 參數值必須在連結夥伴之間相符。請參閱第 37 頁的「使用 OpenBoot PROM 啓用連結參數的自動協商或強制模式」。

▼ 停用自動協商模式

如果網路設備不支援自動協商，或如果您要強制執行網路 speed、duplex 或 link-clock 參數，您可以在 vca 裝置上停用自動協商模式。

1. **將下列驅動程式參數設定為連結夥伴裝置 (例如：交換器) 隨附文件中所說明的值：**
   - adv-1000fdx-cap
   - adv-1000hdx-cap
   - adv-100fdx-cap
   - adv-100hdx-cap
   - adv-10fdx-cap
   - adv-10hdx-cap
   - adv-asmpause-cap
   - adv-pause-cap

   請參閱表 3-2 以獲得這些參數的說明與可能的值。

2. **將** adv-autoneg-cap **參數設定為** 0 **。**

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

變更任何 ndd 連結參數後，將出現類似於以下所顯示的訊息：

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

注意 – 如果您停用自動協商模式，您必須啓用 speed、duplex 及 link-clock (限 1000 Mbps) 參數以便在強制模式中操作。相關說明，請參閱第 37 頁的「使用 OpenBoot PROM 啓用連結參數的自動協商或強制模式」。

使用 vca.conf 檔案設定參數

您也可以將項目新增至 /kernel/drv 目錄中的 vca.conf 檔案，以指定驅動程式參數的屬性。參數名稱與在第 24 頁的「驅動程式參數值與定義」中列出的名稱相同。

警告 – 請勿移除 /kernel/drv/vca.conf 檔案中的任何預設項目。

prtconf(1) 與 driver.conf(4) 的線上說明頁包括其他詳細資料。下一個程序顯示在 vca.conf 檔案中設定參數的範例。

在之前章節定義的變數適用於系統中的已知裝置。使用 vca.conf 檔案設定 Sun Crypto Accelerator 4000 介面卡的變數，您必須知道裝置的下列三種資訊：裝置名稱、裝置父項及裝置位址。

▼ 使用 vca.conf 檔案設定驅動程式參數

1. **在裝置樹中取得 vca 裝置的硬體路徑名稱。**

   a. **檢查 /etc/driver_aliases 檔案以識別與特定裝置相關的名稱。**

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

   在之前的範例中，與 Sun Crypto Accelerator 4000 軟體驅動程式 (vca) 相關的名稱是「pci108e,3de8」。

   b. **在 /etc/path_to_inst 檔案中找出裝置父項名稱與裝置位址。**

   請參閱 path_to_inst(4) 線上說明頁。

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

在之前的範例中，有三個輸出欄：裝置路徑名稱、例項號碼及軟體驅動程式名稱。

之前範例首行中的裝置路徑名稱是 「/pci@8,600000/network@1」。裝置路徑名稱由三部分組成：裝置父項名稱、裝置節點名稱及裝置位址。請參閱表 3-10。

表 3-10 裝置路徑名稱

完整的裝置路徑名稱	父項名稱部分	節點名稱部分	裝置位址部分
"/pci@8,600000/network@1"	/pci@8,600000	network	1
"/pci@8,700000/network@1"	/pci@8,700000	network	1

要清楚識別 vca.conf 檔案中的 PCI 裝置，請使用裝置的完整裝置路徑名稱 (父項名稱、節點名稱及裝置位址)。請參閱 pci(4) 線上說明頁，以取得有關 PCI 裝置規格的更多資訊。

2. **在** /kernel/drv/vca.conf **檔案中設定** vca **裝置的參數。**

   在下列項目中，將停用特定 Sun Crypto Accelerator 4000 乙太網路裝置的 adv-autoneg-cap 參數。

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

3. **儲存** vca.conf **檔案。**
4. **儲存與關閉所有的檔案與程式，然後結束視窗系統。**
5. **關閉並重新啟動系統。**

使用 vca.conf 檔案設定所有 Sun Crypto Accelerator 4000 vca 裝置的參數

如果您省略裝置路徑名稱 (父項名稱、節點名稱及裝置位址)，則將設定所有 Sun Crypto Accelerator 4000 乙太網路裝置所有例項的變數。

▼ 使用 vca.conf 檔案設定所有 Sun Crypto Accelerator 4000 vca 裝置的參數

1. **輸入** *parameter=value;* **，即可在** vca.conf **檔案中新增一行以變更所有例項的參數值。**

   下列範例可將所有 Sun Crypto Accelerator 4000 乙太網路裝置所有例項的 adv-autoneg-cap 參數設定爲 1：

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

範例 vca.conf 檔案

下列是範例 vca.conf 檔案：

```
#
# Copyright 2003 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
#ident  "@(#)vca.conf   1.3     03/10/13 SMI"

#
# Use the new Solaris 9 ddi-no-autodetach property to prevent the
# driver from being unloaded by the cleanup modunload -i 0.
#
ddi-no-autodetach=1;
```

使用 OpenBoot PROM 啓用連結參數的自動協商或強制模式

可以設定下列參數，以便在 OpenBoot PROM 介面中以自動協商或強制模式操作。

表 3-11 本地連結網路裝置參數

參數	說明
speed	此參數可設定爲 auto、1000、100 或 10；語法如下所示： • speed=auto (預設) • speed=1000 • speed=100 • speed=10
duplex	此參數可設定爲 auto、full 或 half；語法如下所示： • duplex=auto (預設) • duplex=full • duplex=half
link-clock	此參數僅適用於將 speed 參數設定爲 1000 或您在使用 1000 Mbps MMF Sun Crypto Accelerator 4000 介面卡的情況。此參數的值必須符合連結夥伴上的值 — 例如，如果本地連結具有一個 master 的值，則連結夥伴必須有一個 slave 值。此參數可設定爲 master、slave 或 auto；語法如下所示： • link-clock=auto (預設) • link-clock=master • link-clock=slave

要建立適當的連結，必須在本地連結與連結夥伴之間正確設定 speed、duplex 及 link-clock (限 1000 Mbps) 參數。兩個連結夥伴必須以自動協商或強制模式爲每個 speed、duplex 及 link-clock (限 1000 Mbps) 參數操作。這些參數的任何一個 auto 值將設定連結，以便爲該參數在自動協商模式中操作。如果在 OpenBoot PROM ok 提示中缺少參數，則系統將爲該參數設定一個預設值 auto。一個非 auto 的參數將設定本地連結，以便爲該參數在強制模式中操作。

本地連結以 100 Mbps 或更低及全雙式與半雙工，爲 speed 與 duplex 參數在自動協商模式中操作時，連結夥伴將使用具有一個雙工的 100 Mbps 或 10 Mbps 速度。

speed 參數在強制模式中操作時，其值必須與連結夥伴的 speed 值相符。如果 duplex 參數在本地連結與連結夥伴之間不相符，則可能會出現連結；但是，將發生流量衝突。

在本地連結 speed 參數設定爲自動協商，且連結夥伴 speed 參數設定爲強制時，可能會出現連結，視 speed 值是否可以在本地連結與連結夥伴之間協商而定。根據預設值，自動協商模式中的介面會一直嘗試以半雙工建立連結 (如果速度相符)。因爲這兩個介面中的一個不是自動協商模式，自動協商模式中的介面僅偵測到 speed 參數；沒有偵測到雙工參數。此方法稱爲並列偵測。

警告 – 使用雙工衝突建立連結經常導致流量衝突。

對於在強制模式中操作的本地連結參數，參數必須具有一個 auto 以外的值。例如：要使用半雙工以 100 Mbps 建立強制模式連結，請在 OpenBoot PROM ok 提示中鍵入下列指令：

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

注意 – 在本章節的範例中，net 是預設整合網路介面裝置路徑的別名。您可以指定裝置路徑而不是使用 net，以設定其他網路裝置。

要使用屬於主時脈的半雙工以 1000 Mbps 建立強制模式連結，請在 OpenBoot PROM ok 提示中鍵入下列指令：

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

注意 – link-clock 參數必須具有符合連結夥伴 link-clock 值的值。例如：如果將本地連結上的 link-clock 值設定爲 master，則必須將連結夥伴上的 link-clock 值設定爲 slave。

如果要爲 10 Mbps 的速度建立強制模式，爲雙工建立自動協商模式，請在 OpenBoot PROM ok 提示中鍵入下列指令：

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

您也可以像前一個範例一樣，在 OpenBoot PROM ok 提示中鍵入下列指令以建立相同的本地連結參數：

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

請參閱 IEEE 802.3 文件以取得詳細資料。

編碼與乙太網路驅動程式操作統計

本章節說明 kstat(1M) 指令顯示的統計。

編碼驅動程式統計

表 3-12 說明編碼驅動程式統計。

表 3-12 編碼驅動程式統計

參數	說明	穩定或不穩定
vs-mode	其值爲 FIPS、standard 或 unitialized。FIPS 表示介面卡處於 FIPS 模式。standard 表示介面卡不處於 FIPS 模式。unitialized 表示介面卡沒有初始化。	穩定
vs-status	其值爲 ready、faulted 或 failsafe。ready 表示介面卡在進行一般操作。faulted 表示介面卡不在進行操作。failsafe 表示 failsafe 模式，這是介面卡的原廠狀態。	穩定

乙太網路驅動程式統計

表 3-13 說明乙太網路驅動程式統計。

表 3-13 乙太網路驅動程式統計

參數	說明	穩定或不穩定
ipackets	輸入封包的數目。	穩定
ipackets64	ipackets 的 64 位元版本。	穩定
ierrors	接收到因爲含有太多錯誤而無法處理的所有封包 (長)。	穩定
opackets	要求在介面上傳送的所有封包。	穩定
opackets64	要求在介面上傳送的所有封包 (64 位元)。	穩定
oerrors	因爲錯誤沒有成功傳送的所有封包 (長)。	穩定
rbytes	在介面上成功接收的總位元組。	穩定
rbytes64	在介面上成功接收的所有位元組 (64 位元)。	穩定
obytes	要求在介面上傳送的所有位元組。	穩定
obytes64	要求在介面上傳送的所有位元組 (64 位元)。	穩定
multircv	成功接收多點傳送封包，包括群組與功能位址 (長)。	穩定
multixmt	要求傳送的多點傳送封包，包括群組與功能位址 (長)。	穩定
brdcstrcv	成功接收的多點傳送封包 (長)。	穩定
brdcstxmt	要求傳送的多點傳送封包 (長)。	穩定
norcvbuf	因未配置緩衝接收封包而丟棄有效傳入封包的已知次數 (長)。	穩定
noxmtbuf	封包在輸出時被丟棄，因爲傳送緩衝忙碌，或沒有緩衝可配置來傳送 (長)。	穩定

表 3-14 說明傳送與接收 MAC 計數器。

表 3-14 TX 與 RX MAC 計數器

參數	說明	穩定或不穩定
`tx-collisions`	導致衝突的每個框架傳送嘗試之 16 位元可載入的計數器增加。	穩定
`tx-first-collisions`	第一次嘗試時遇到衝突，但第二次嘗試時成功傳送的每個框架傳送之 16 位元可載入的計數器增加。	不穩定
`tx-excessive-collisions`	已超過嘗試限制的每個框架傳送之 16 位元可載入的計數器增加。	不穩定
`tx-late-collisions`	遇到衝突的每個框架傳送之 16 位元可載入的計數器增加。此參數表示因爲在傳送至少最小框架大小位元組數後發生衝突，造成 TxMAC 丟棄的框架數。通常，這表示在網路上至少有一個位置違反了網路所允許的最大值。	不穩定
`tx-defer-timer`	嘗試傳送框架時，TxMAC 依從網路流量時的 16 位元可載入計時器增加。計時器的時基是按 256 分開的媒體位元組區塊。	不穩定
`tx-peak-attempts`	8 位元註冊表示每個成功傳送框架連續衝突的最高數目，因爲此註冊最後讀取而發生。此註冊可達到的最大值爲 255。如果每個成功傳送框架的連續衝突數目超過 255，則軟體將產生一個可遮罩的中斷。此註冊受到讀取後，將自動在 0 時清除。	不穩定
`tx-underrun`	從網路上接收到有效的框架後之 16 位元可載入的計數器增加。	不穩定
`rx-length-err`	已從網路中接收到框架後的 16 位元可載入的計數器增加，此框架的長度大於在「最大框架大小註冊」中編排的值。	不穩定
`rx-alignment-err`	在接收框架中偵測到對齊錯誤的 16 位元可載入的計數器增加。在接收框架放棄循環重覆檢查和 (CRC) 檢查演算法後報告的對齊錯誤，*並且*框架包含一個非整數位元組 (即以位元爲單位的框架大小不等於零)。	不穩定
`rx-crc-err`	在接收框架未通過 CRC 檢查演算法後 16 位元可載入的計數器增加，*並且*框架包含一個整數位元組 (即以位元爲單位的框架大小等於零)。	不穩定

表 3-14 TX 與 RX MAC 計數器 *(續)*

參數	說明	穩定或不穩定
rx-code-violations	XCVR 透過 MII 產生 Rx_Err 提示時的 16 位元可載入的計數器增加，此時正在接收框架。在接收到的資料流中偵測到無效代碼時，此指示由收發器產生。接收代碼違反不會視爲 FCS 或對齊錯誤。	不穩定
rx-overflows	乙太網路框架的數目因缺少資源而遭丟棄。	不穩定
rx-no-buf	因爲沒有更多的接收緩衝空間，硬體無法接收資料的次數。	不穩定
rx-no-comp-wb	硬體無法爲接收的資料發佈完整項目的次數。	不穩定
rx-len-mismatch	在註明的長度與實際框架長度不相符時所接收的框架數。	不穩定

下列乙太網路屬性 (表 3-15) 衍生自裝置功能與連結夥伴功能的交集。

表 3-15 目前乙太網路連結屬性

參數	說明	穩定或不穩定
ifspeed	1000、100 或 10 Mbps	穩定
link-duplex	0 = half、1 = full	穩定
link-pause	連結的目前暫停設定，請參閱第 26 頁的「流量控制參數」	穩定
link-asmpause	連結的目前暫停設定，請參閱第 26 頁的「流量控制參數」	穩定
link-up	1 = up、0 = down	穩定
link-status	1 =u p、0 = down	穩定
xcvr-inuse	使用中收發器的類型：1 = 內部 MII、2 = 外部 MII、3 = 外部 PCS	穩定

表 3-16 說明唯讀媒體獨立介面 (MII) 功能。這些參數可以定義硬體的功能。十億位元媒體獨立介面 (GMII) 支援所有下列功能。

表 3-16 唯讀 vca 裝置功能

參數	說明	穩定或不穩定
cap-autoneg	0 = 不適用於自動協商 1 = 自動協商功能	穩定
cap-1000fdx	本地介面全雙工功能 0 = 非 1000 Mbps 全雙工功能 1 = 1000 Mbps 全雙工功能	穩定
cap-1000hdx	本地介面半雙工功能 0 = 非 1000 Mbps 半雙工功能 1 = 1000 Mbps 半雙工功能	穩定
cap-100fdx	本地介面全雙工功能 0 = 非 100 Mbps 全雙工功能 1 = 100 Mbps 全雙工功能	穩定
cap-100hdx	本地介面半雙工功能 0 = 非 100 Mbps 半雙工功能 1 = 100 Mbps 半雙工功能	穩定
cap-10fdx	本地介面全雙工功能 0 = 非 10 Mbps 全雙工功能 1 = 10 Mbps 全雙工功能	穩定
cap-10hdx	本地介面半雙工功能 0 = 非 10 Mbps 半雙工功能 1 = 10 Mbps 半雙工功能	穩定
cap-asm-pause	本地介面流量控制功能 0 = 不適用於非對稱暫停 1 = 適用於非對稱暫停 (從本地裝置) (請參閱第 26 頁的「流量控制參數」)	穩定
cap-pause	本地介面流量控制功能 0 = 不適用於對稱暫停 1 = 適用於對稱暫停 (請參閱第 26 頁的「流量控制參數」)	穩定

報告連結夥伴功能

表 3-17 說明唯讀連結夥伴功能。

表 3-17 唯讀連結夥伴功能

參數	說明	穩定或不穩定
`lp-cap-autoneg`	0 = 非自動協商 1 = 自動協商	穩定
`lp-cap-1000fdx`	0 = 非 1000 Mbps 全雙工傳送 1 = 1000 Mbps 全雙工	穩定
`lp-cap-1000hdx`	0 = 非 1000 Mbps 半雙工傳送 1 = 100 Mbps 半雙工	穩定
`lp-cap-100fdx`	0 = 非 100 Mbps 全雙工傳送 1 = 100 Mbps 全雙工	穩定
`lp-cap-100hdx`	0 = 非 100 Mbps 半雙工傳送 1 = 100 Mbps 半雙工	穩定
`lp-cap-10fdx`	0 = 非 10 Mbps 全雙工傳送 1 = 10 Mbps 全雙工	穩定
`lp-cap-10hdx`	0 = 非 10 Mbps 半雙工傳送 1 = 10 Mbps 半雙工	穩定
`lp-cap-asm-pause`	0 = 不適用於非對稱暫停 1 = 連結夥伴功能的非對稱暫停 (請參閱第 26 頁的「流量控制參數」)	穩定
`lp-cap-pause`	0 = 不適用於對稱暫停 1 = 適用於對稱暫停 (請參閱第 26 頁的「流量控制參數」)	穩定

如果連結夥伴*不*適用於自動協商 (`lp-cap-autoneg` 爲 0 時)，在表 3-17 中說明的其餘資訊不相關，且參數值爲 0。

如果連結夥伴*不*適用於自動協商 (`lp-cap-autoneg` 爲 1 時)，則在您使用自動協商與連結夥伴功能時將顯示速度與模式資訊。

表 3-18 說明驅動程式特定的參數。

表 3-18 驅動程式特定的參數

參數	說明	穩定或不穩定
lb-mode	裝置所在的迴路模式副本 (如果有的話) 。	不穩定
promisc	啓用時，裝置處於混雜模式。停用時，裝置不處於混雜模式。	不穩定
乙太網路傳送計數器		
tx-wsrv	傳送環已滿時的次數計數。	不穩定
tx-msgdup-fail	嘗試複製封包失敗。	不穩定
tx-allocb-fail	嘗試配置記憶體失敗。	不穩定
tx-queue0	在第一個硬體傳送佇列上傳送佇列的封包數。	不穩定
tx-queue1	在第二個硬體傳送佇列上傳送佇列的封包數。	不穩定
tx-queue2	在第三個硬體傳送佇列上傳送佇列的封包數。	不穩定
tx-queue3	在第四個硬體傳送佇列上傳送佇列的封包數。	不穩定
乙太網路接收計數器		
rx-hdr-pkts	接收到小於 256 位元組的封包數。	不穩定
rx-mtu-pkts	接收到大於 256 位元組而小於 1514 位元組的封包數。	不穩定
rx-split-pkts	分割跨兩頁的封包數。	不穩定
rx-nocanput	因爲無法傳送至 IP 堆疊而丟棄的封包數。	不穩定
rx-msgdup-fail	無法複製的封包數。	不穩定
rx-allocb-fail	配置失敗的區塊數。	不穩定
rx-new-pages	在接收時取代的頁數。	不穩定
rx-new-hdr-pages	裝滿在接收時被取代且小於 256 位元組封包的頁數。	不穩定
rx-new-mtu-pages	裝滿在接收時被取代且大於 256 位元組而小於 1514 位元組封包的頁數。	不穩定
rx-new-nxt-pages	包含在接收時被取代且分割於多頁之封包的頁數。	不穩定
rx-page-alloc-fail	配置失敗的頁數。	不穩定
rx-mtu-drops	因爲驅動程式無法對應至新頁面以取代此頁面，而將整頁大於 256 位元組且小於 1514 位元組的封包丟棄的次數。	不穩定

表 3-18 驅動程式特定的參數 *(續)*

參數	說明	穩定或不穩定
rx-hdr-drops	因爲驅動程式無法對應至新頁面以取代此頁面，而將整頁小於 256 位元組的封包丟棄的次數。	不穩定
rx-nxt-drops	因爲驅動程式無法對應至新頁面以取代此頁面，而將含分割封包的頁面丟棄的次數。	不穩定
rx-rel-flow	驅動程式被告知釋放流量的次數。	不穩定
乙太網路 PCI 屬性		
rev-id	有助於識別現場所用裝置的 Sun Crypto Accelerator 4000 乙太網路裝置之修正 ID。	不穩定
pci-err	所有 PCI 錯誤總和。	不穩定
pci-rta-err	接收到的目標中止數。	不穩定
pci-rma-err	接收到的主要中止數。	不穩定
pci-parity-err	偵測到的 PCI 同位檢查錯誤數。	不穩定
pci-drto-err	達到延遲交易重試逾時的次數。	不穩定
dma-mode	由 Sun Crypto Accelerator 4000 驅動程式 (vca) 使用。	不穩定

▼ 檢查連結夥伴設定

- **以超級使用者身份鍵入** `kstat vca:`*N* **指令：**

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

其中 *N* 指的是 vca 裝置的例項號碼。此號碼應該反映在其中執行 kstat 指令之介面卡的例項號碼。

IPsec 線上加速統計

表 3-19 說明介面卡設定用於線上 IPsec 硬體加速時遞增的核心統計。請參閱第 50 頁的「啓用線上 IPsec 加速」以取得有關如何設定介面卡以使用線上 IPsec 配置的說明。

表 3-19 線上 IPsec 加速的編碼驅動程式統計

參數	說明	穩定或不穩定
ipsec_ierrrors	接收到因爲含有太多錯誤而無法處理的所有 IPsec 封包 (長)	穩定
ipsec_ipackets	輸入 IPsec 封包的數目。	穩定
ipsec_ipackets64	輸入 IPsec 封包的數目 (64 位元)。	穩定
ipsec_obytes	要求在介面上傳送的所有 IPsec 位元組。	穩定
ipsec_obytes64	要求在介面上傳送的所有 IPsec 位元組 (64 位元)。	穩定
ipsec_oerrors	因爲錯誤沒有成功傳送的所有 IPsec 封包 (長)。	穩定
ipsec_opackets	要求在介面上傳送的所有 IPsec 封包。	穩定
ipsec_opackets64	要求在介面上傳送的所有 IPsec 封包 (64 位元)。	穩定
ipsec_rbytes	在介面上成功接收的總 IPsec 位元組	穩定
ipsec_rbytes64	在介面上成功接收的總 IPsec 位元組 (64 位元)	穩定
sadb_cache_misses	遺失的韌體快取數量	穩定
sadb_cache_overflows	溢出的韌體快取數量	穩定
sadb_entries	SADB 驅動程式中的項目數量	穩定
sadb_operations	從 Solaris IPsec 傳送到驅動程式中的 SADB 操作次數	穩定

注意 – 表 3-19 中列出的 IPsec 核心統計僅遞增列出硬體實際在線上處理的 IPsec 封包。收到小於 256 位元組的封包不會在線上處理，IPsec 核心統計也不會按照這些封包遞增。這些核心統計也不會套用於頻帶外 IPsec 流量 (請參閱第 49 頁的「設定 IPsec 硬體加速」)。如果啓用了 snoop，計數器不會遞增。頻帶外封包將會遞增定期網路核心統計與任何適用的編碼統計，即 3desbytes 與 3desjobs。

網路組態

本章節說明如何在系統安裝介面卡後編輯網路主機檔案。

設定網路主機檔案

安裝驅動程式軟體後，您必須爲介面卡的乙太網路介面建立 hostname.vca*N* 檔案。請注意，在檔案名稱 hostname.vca*N* 中，*N* 與您計劃使用的 vca 介面之例項號碼相對應。您還必須在 /etc/hosts 檔案中爲其乙太網路介面建立 IP 位址與主機名稱。

1. **在 /etc/path_to_inst 檔案中找到正確的 vca 介面與例項號碼。**

   請參閱 path_to_inst(4) 線上說明頁。

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

   上述範例中的例項號碼爲 0。

2. **使用 ifconfig(1M) 指令以設定介面卡的 vca 介面。**

   使用 ifconfig 指令將 IP 位址指派給網路介面。在指令行中鍵入下列指令，使用介面卡的 IP 位址取代 *ip-address*：

```
# ifconfig vcaN plumb ip-address up
```

   請參閱 ifconfig(1M) 說明頁與 Solaris 文件以取得更多資訊。

   - 如果您需要在重新啓動後保持相同設定，請建立 /etc/*hostname*.vca*N* 檔案，其中 *N* 與您計劃使用的 vca 介面之例項號碼相對應。

     要使用步驟 1 所示範例的 vca 介面，請建立 /etc/*hostname*.vca*N* 檔案，其中 *N* 與裝置的例項號碼 (在此範例中爲 0) 相對應。如果例項號碼是 1，則檔案名稱將是 /etc/*hostname*.vca1。

   - 請勿爲不計劃使用的 Sun Crypto Accelerator 4000 介面建立 /etc/*hostname*.vca*N* 檔案。
   - /etc/*hostname*.vca*N* 檔案必須包含適當 vca 介面的主機名稱。
   - 主機名稱必須具有 IP 位址，且必須在 /etc/hosts 檔案中列出。

- 主機名稱必須與任何其他介面的任何其他主機名稱不同，例如：
  /etc/*hostname*.vca0 與 /etc/*hostname*.vca1 無法共用相同的主機名稱。

下列範例顯示 /etc/*hostname*.vca*N* 檔案，此檔案爲名稱是 zardoz 且具有 Sun Crypto Accelerator 4000 介面卡 (zardoz-11) 的系統所需。

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

3. **為每個使用中的 vca 介面在 /etc/hosts 檔案中建立適當的項目。**

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
```

設定 IPsec 硬體加速

介面卡具有線上與頻帶外兩種 IPsec 硬體加速組態。兩種組態均會加速 IPsec 編碼操作。但兩種方法各有所長，應考慮系統的整體要求，然後再決定使用哪種組態。

注意 – Solaris 9 之後的版本支援 IPsec 加速，Solaris 8 則不支援。僅 Solaris 9 12/03 之後的版本支援線上 IPsec 加速 (請參閱表 3-20)。

表 3-20 IPsec 加速的 Solaris 版本要求

Solaris 版本	頻帶外加速	線上加速
所有 Solaris 8 版本	不支援	不支援
Solaris 9 至 Solaris 9 8/03	支援	不支援
Solaris 9 12/03 之後的版本	支援	支援

頻帶外爲預設組態，最佳適用於多處理器系統操作。此組態會卸載介面卡的 DES 與 3DES 編碼功能，它適用於無需考慮主機處理能力的多處理器系統。

線上 IPsec 組態使用驗證支援 (MD5 與 SHA1) 可增強頻帶外功能，並會卸載部分傳送至介面卡的主機封包。透過處理額外封包，介面卡可顯著減少主機 CPU 的使用。

注意 – 在僅要求 DES 或 3DES 加密演算法的多處理器系統上，使用頻帶外組態比線上組態能提供更大 IPsec 傳送量。

啓用頻帶外 IPsec 加速

要求 Solaris 9 或更新版本。介面卡預設組態爲頻帶外。無需組態或微調 IPsec 即可在 Solaris 9 中將介面卡用於頻帶外 IPsec 加速。您只需安裝 Sun Crypto Accelerator 4000 套件並重新啓動。

啓用線上 IPsec 加速

要求 Solaris 9 12/03 或更新版本。要設定線上加速，您必須同時變更 Solaris 軟體與 `vca` 驅動程式中的組態檔案。

▼ 啓用線上 IPsec 硬體加速

1. **透過在 `/etc/system` 組態檔案中新增下列項目可在 Solaris 軟體中啟用線上加速：**

```
set ip:ip_use_dl_cap=1
```

要讓 `/etc/system` 檔案中的變更生效，必須重新啓動系統。

2. **透過在 `/kernel/drv/vca.conf` 組態檔案中新增下列項目可在 `vca` 驅動程式中啟用線上加速：**

```
inline-ipsec=1;
```

要讓 `/kernel/drv/vca.conf` 檔案中的變更生效，您必須重新啓動系統，或卸載然後重新裝上 `vca` 驅動程式。

注意 – 如果 Solaris 軟體中沒有啓用線上加速，則不應在驅動程式中啓用線上加速，否則可能會導致非 IPsec 效能下降。

一旦啓用了線上加速，您可以使用標準 IPsec 組態程序將 Solaris 軟體 IPsec 政策設定用於介面。要取得關在 Solaris 中設定 IPsec 政策的資訊，請在下列網站參閱 *IPsec and IKE Administration Guide*：`http://docs.sun.com`

線上加速可用於加速 AH 與 ESP 演算法，但無法在介面卡執行多重巢狀傳輸 (包括 AH+ESP)。如果使用多重傳輸，在線上只能執行最外層傳輸。剩餘傳輸由 Solaris IPsec 組態來執行。如果 Solaris 9 系統中已安裝了 KCL IPsec 加速 (`SUNWkcl2i.u`) 套件，這些傳輸也可以在硬體中完成 (頻帶外)。

將介面卡設定用於 IPsec 線上加速後，`kstat`(1M) 指令顯示的其他統計資料將會遞增。請參閱表 3-19 以取得有關 IPsec 線上加速 `kstat` 統計的說明。

第 4 章

管理 Sun Crypto Accelerator 4000 介面卡

本章概述使用 vcaadm、vcad、vcadiag、pk11export 公用程式管理介面卡。包含下列章節：

使用 vcaadm 公用程式

vcaadm 公用程式爲 Sun Crypto Accelerator 4000 介面卡提供了指令行介面。只有指定爲安全管理員的使用者才能使用 vcaadm 公用程式。使用 vcaadm 第一次連接到 Sun Crypto Accelerator 4000 介面卡時，系統會提示您建立初始安全管理員與密碼。

要輕鬆存取 vcaadm 公用程式，請將 Sun Crypto Accelerator 4000 工具目錄放在搜尋路徑中，例如：

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

vcaadm 指令行語法爲：

- vcaadm [-H]
- vcaadm [-y] [-h *hostname*] [-p *port*] [-d vca*N*] [-f *filename*]
- vcaadm [-y] [-h *hostname*] [-p *port*] [-d vca*N*] [-s *sec-officer*] *command*

注意 – 使用 -d 屬性時，vca*N* 是介面卡的裝置名稱，其中 *N* 與 Sun Crypto Accelerator 4000 裝置例項號碼相對應。

表 4-1 顯示了 vcaadm 公用程式的選項。

表 4-1 vcaadm 選項

選項	意義
-H	顯示 vcaadm 指令的說明檔案並結束。
-d vca*N*	連接到將 *N* 作爲驅動程式例項號碼的 Sun Crypto Accelerator 4000 介面卡。例如：將 -d vca1 連接到裝置 vca1，其中 vca 是介面卡裝置名稱中的字串，1 是裝置的例項號碼。此預設值是 vca0，且必須是 vca*N* 的格式，其中 *N* 與裝置例項號碼相對應。
-f *filename*	從 *filename* 中斷一個或多個指令並結束。
-h *hostname*	連接到 *hostname* 上的 Sun Crypto Accelerator 4000 介面卡。 *host* 的值可以是主機名稱或 IP 位址，預設值是迴路位址。
-p *port*	連接到 *port* 上的 Sun Crypto Accelerator 4000 介面卡。*port* 的預設值是 6870。
-s *sec-officer*	以稱爲 *sec-officer* 的安全管理員身份登入。
-y	對於所有一般會提示要求確認的指令，強迫回答「yes」。

注意 – 本使用者指南中，使用名稱 *sec-officer* 作爲安全管理員名稱範例。

作業模式

vcaadm 可以在三種模式之一執行。這些模式的主要差異，在於指令如何傳送到 vcaadm。這三種模式是單一指令模式、檔案模式及互動模式。

注意 – 要使用 vcaadm，您必須以安全管理員的身份進行驗證。需要以安全管理員的身份進行驗證的頻率由使用的作業模式決定。

單一指令模式

在單一指令模式下，您必須以安全管理員的身份爲每個指令進行驗證。執行指令後，您會登出 vcaadm。

在單一指令模式下輸入指令時，您可在指定所有指令行參數後指定要執行的指令。例如：在單一指令模式下，下列指令將會顯示指定金鑰庫中的所有使用者，並將使用者恢復爲指令 shell 提示。

```
$ vcaadm show user
Security Officer Name: sec-officer
Security Officer Password:
```

下列指令會以安全管理員 (*sec-officer*) 的身份進入登入，然後在金鑰庫中建立使用者 *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 – 第一個密碼是安全管理員密碼，接著是新使用者 *web-admin* 的密碼及其確認密碼。

所有單一指令模式的輸出，都會送往標準輸出串流。此輸出可以使用標準 UNIX shell 方法加以重新導向。

檔案模式

在檔案模式下，您必須以安全管理員的身份爲每個要執行的檔案進行驗證。執行指令檔案中的指令後，您會登出 vcaadm。

要在檔案模式下輸入指令，您必須指定一個檔案以供 vcaadm 讀取一個或多個指令。檔案必須是 ASCII 文字，每行包含一個指令。每個註解以井字號 (#) 字元開頭。如果已設定檔案模式選項，vcaadm 會忽略最後一個選項後的所有指令行引數。下列範例會執行 deluser.scr 檔案中的指令，並對所有提示進行確認回答：

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

互動模式

在互動模式下，每次連接到介面卡時，您必須以安全管理員的身份進行驗證。這是 vcaadm 的預設作業模式。要在互動模式下登出 vcaadm，請使用 logout 指令。請參閱第 56 頁的「使用 vcaadm 登入與登出」。

互動模式提供使用者與 ftp(1) 類似的介面，您可以一次輸入一個指令。互動模式不支援 -y 選項。

使用 vcaadm 登入與登出

使用指令行中的 vcaadm 並分別使用 -h、-p 及 -d 屬性指定 *host*、*port* 及 *device* 時，如果已成功建立網路連線，系統會立即提示您以安全管理員身份登入。

vcaadm 公用程式會在 vcaadm 應用程式與特定介面卡上執行的 Sun Crypto Accelerator 4000 韌體之間建立加密網路連線 (通道)。

在設定加密通道期間，介面卡會透過其硬體乙太網路位址與 RSA 公開金鑰來進行自我辨識。vcaadm 第一次連接到介面卡時，即會建立信任資料庫 ($HOME/.vcaadm/trustdb)。此檔案包含安全管理員目前信任的所有介面卡。

使用 vcaadm 登入介面卡

如果安全管理員連接到新介面卡，vcaadm 會通知安全管理員並提示下列選項：

```
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)
```

如果安全管理員連接到已變更遠端存取金鑰的介面卡，vcaadm 會通知安全管理員並提示下列三個選項：

```
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
```

登入新介面卡

注意 – 本章中的其餘範例使用 vcaadm 的互動模式建立。

連接到新介面卡時，vcaadm 必須在信任資料庫中建立新項目。以下是登入新介面卡的範例。

```
# 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 -->
```

登入已變更遠端存取金鑰的介面卡

連接到已變更遠端存取金鑰的介面卡時，vcaadm 必須變更與信任資料庫中介面卡對應的項目。以下是登入已變更遠端存取金鑰的介面卡範例。

```
# 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*

互動模式下的 vcaadm 提示顯示如下：

```
vcaadm{vcaN@hostname, sec-officer}> command
```

下表說明 vcaadm 提示變數：

表 4-2 vcaadm 提示變數定義

提示變數	定義
vca*N*	vca 是代表 Sun Crypto Accelerator 4000 介面卡的字串。*N* 是介面卡裝置路徑名稱中的裝置例項號碼 (裝置位址)。請參閱第 35 頁的「使用 vca.conf 檔案設定驅動程式參數」以取得有關擷取此裝置號碼的詳細資料。
hostname	實體連接 Sun Crypto Accelerator 4000 介面卡的主機名稱。*hostname* 可以由實體主機的 IP 位址取代。
sec-officer	目前已登入介面卡的安全管理員名稱。

使用 vcaadm 登出介面卡

如果在互動模式下工作，您可能要中斷一個介面卡的連接，並在沒有完全結束 vcaadm 的情況下連接至另一個介面卡。要中斷介面卡的連接並登出，但仍然保留在互動模式，請使用 logout 指令：

```
vcaadm{vcaN@hostname, sec-officer}> logout
vcaadm>
```

在上述範例中，請注意，vcaadm> 提示不會再顯示裝置例項號碼、主機名稱或安全管理員名稱。要登入另一個裝置，請使用下列選用參數鍵入 connect 指令。

表 4-3 connect 指令選用參數

參數	意義
dev vcaN	連接到驅動程式實例號碼爲 *N* 的 Sun Crypto Accelerator 4000 介面卡。例如：-d vca1 連接到裝置 vca1；此裝置預設值爲 vca0。
host *hostname*	連接到 *hostname* 上的 Sun Crypto Accelerator 4000 介面卡 (迴路位址的預設值)。*hostname* 可以由實體主機的 IP 位址取代。
port *port*	連接到連接埠 *port* 上的 Sun Crypto Accelerator 4000 介面卡 (預設值爲 6870)。

範例：

```
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}>
```

如果您已連接到 Sun Crypto Accelerator 4000 介面卡，vcaadm 不會讓您發出 connect 指令。您必須先登出，然後發出 connect 指令。

每個新連線會導致 vcaadm 與目標 Sun Crypto Accelerator 4000 韌體重新交涉新工作階段金鑰，以保護傳送的管理資料。

使用 vcaadm 輸入指令

vcaadm 公用程式具有指令語言，您必須加以使用才能與 Sun Crypto Accelerator 4000 介面卡互動。您可以使用指令的全部或部分 (足以從任何其他指令中唯一地識別該指令) 進行輸入指令。輸入「sh」而不是「show 」應能正常工作，但「re」可能會產生混淆，因爲這可能是「reset」或「rekey」。

下列範例顯示了如何使用完整字彙輸入指令：

```
vcaadm{vcaN@hostname, sec-officer}> show user
User                                        Status
-----------------------------------------------------
web-admin                                  enabled
Tom                                         enabled
-----------------------------------------------------
```

您也可以在上述範例中使用部分字彙作爲指令取得相同的資訊，例如：sh us。

模糊的指令會導致解說性回應：

```
vcaadm{vcaN@hostname, sec-officer}> re
Ambiguous command: re
```

取得指令說明

vcaadm 具有內建說明功能。要取得說明，您必須輸入問號「?」字元，後面跟著要取得更多說明的指令。如果輸入整個指令且指令行中包含「?」，則系統會顯示該指令的語法，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
```

您也可以在 vcaadm 提示時輸入問號，以查看所有 vcaadm 指令及其說明的清單，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
```

不處於 vcaadm 互動模式下時，「?」字元可能會由使用的 shell 解讀。在此情況下，請確定在問號前使用指令 shell 逸出字元。

在互動模式下結束 vcaadm 公用程式

下列兩個指令可讓您結束 vcaadm：quit 與 exit。Ctrl-D 按鍵組合也可以結束 vcaadm。

使用 vcaadm 初始化介面卡

設定 Sun Crypto Accelerator 4000 介面卡的第一步是加以初始化。初始化介面卡時需要建立金鑰庫。(請參閱第 96 頁的 「概念與術語」。) 使用 vcaadm 第一次連接到 Sun Crypto Accelerator 4000 介面卡時，系統會提示您使用新的金鑰庫初始化介面卡或使用備份檔案中儲存的現有金鑰庫初始化介面卡。vcaadm 會提示您提供任一類型介面卡初始化所需的所有資訊。

▼ 使用新的金鑰庫初始化介面卡

1. **在已安裝介面卡的系統之指令提示下輸入** vcaadm**，或輸入** vcaadm -h *hostname* **(如果系統位於遠端)，然後選擇 1 以初始化介面卡：**

```
# vcaadm -h hostname
Please select an action:

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

Your Choice --> 2
This board is uninitialized.
You will now initialize the board. You may either
completely initialize the board and start with a new
keystore or initialize the board to use an existing
keystore, providing a backup file in the process.

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

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

2. **建立金鑰庫名稱 (請參閱第 65 頁的 「命名要求」。)：**

```
Keystore Name: keystore-name
```

3. **選擇 FIPS 140-2 模式或非 FIPS 模式。**

處於 FIPS 模式時，介面卡與 FIPS 140-2 第 3 級相容。FIPS 140-2 是一種聯邦資訊處理標準，可提供抗侵入及資料高度完整性與安全性功能。請參閱下列位置的 FIPS 140-2 文件：`http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf`

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

4. **建立初始安全管理員名稱與密碼 (請參閱第 65 頁的 「命名要求」。)：**

```
Initial Security Officer Name: sec-officer
Initial Security Officer Password:
Confirm Password:
```

注意 – 重要參數變更或刪除之前，或在執行可能會導致嚴重結果的指令之前，`vcaadm` 會提示您輸入 `Y`、`Yes`、`N` 或 `No` 來加以確認。這些值不區分大小寫；預設值爲 `No`。

---

5. **檢查組態資訊：**

```
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... This may take a few
minutes...Done.
```

使用現有金鑰庫初始化介面卡

如果要將多個介面卡新增到單一金鑰庫，您可能要使用相同的金鑰庫資訊初始化所有介面卡。此外，您可能要將 Sun Crypto Accelerator 4000 介面卡回復爲原始金鑰庫組態。本章節說明如何使用備份檔案中儲存的現有金鑰庫初始化介面卡。

執行此程序之前，您必須先建立現有介面卡組態的備份檔案。建立與回復備份檔案需要密碼才能對備份檔案中的資料進行加密與解密。(請參閱第 70 頁的「備份主要金鑰」)。

▼ 使用現有金鑰庫初始化介面卡

1. **在已安裝 Sun Crypto Accelerator 4000 介面卡的系統的指令提示下輸入** `vcaadm`**，或輸入** `vcaadm -h` *hostname* **(如果系統位於遠端)，然後選擇 2 以透過備份初始化介面卡：**

```
# 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. **輸入備份檔案的路徑與密碼：**

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

3. **檢查組態資訊：**

```
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...
```

使用 vcaadm 管理金鑰庫

金鑰庫是金鑰資料的儲存庫。安全管理員及使用者與金鑰庫相關聯。金鑰庫不僅提供了儲存空間，還提供了使用者帳號擁有金鑰物件的方法。這可讓未以擁有者身份驗證的應用程式看不到金鑰。金鑰庫具有下列三種元件：

- **金鑰物件 –** 儲存用於 Sun ONE 網站伺服器等應用程式的長期金鑰。
- **使用者帳號 –** 這些帳號爲應用程式提供驗證與存取特定金鑰的方法。
- **安全管理員帳號 –** 這些帳號透過 vcaadm 存取金鑰管理功能。

注意 – 單一 Sun Crypto Accelerator 4000 介面卡只能有一個金鑰庫。您可以將多個介面卡設定爲與相同的金鑰庫共同配合運作，以提供額外效能與容錯功能。

命名要求

安全管理員名稱、使用者名稱及金鑰庫名稱必須符合下列要求：

表 4-4 安全管理員名稱、使用者名稱及金鑰庫名稱要求

名稱要求	說明
最小長度	至少一個字元
最大長度	使用者名稱爲 63 個字元，金鑰庫名稱爲 32 個字元
有效字元	文數字、底線 (_)、破折號 (-) 及點 (.)
第一個字元	必須是文數字

密碼要求

密碼要求視目前的 set passreq 設定 (low、med 或 high) 而異。

設定密碼要求

請使用 `set passreq` 指令設定 Sun Crypto Accelerator 4000 介面卡的密碼要求。此指令可爲 `vcaadm` 提示的任何密碼設定密碼字元要求。密碼要求有三個設定，如下表所示：

表 4-5 密碼要求設定

密碼設定	要求
`low`	沒有任何密碼限制。這是介面卡處於非 FIPS 模式時的預設值。
`med`	要求最少六個字元，其中三個字元必須是文數字，且其中一個字元必須是非文數字。這是介面卡處於 FIPS 140-2 模式時的預設值，且在 FIPS 140-2 模式下允許的最少密碼要求。
`high`	要求最少八個字元：其中三個字元必須是文數字，且其中一個字元必須是非文數字。這不是預設值，且必須手動設定。

要變更密碼要求，請輸入 `set passreq` 指令，接著輸入 `low`、`med` 或 `high`。下列指令會將 Sun Crypto Accelerator 4000 介面卡的密碼要求設定爲 `high`：

```
vcaadm{vcaN@hostname, sec-officer}> set passreq high

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

在金鑰庫中建立安全管理員

金鑰庫可以有多個安全管理員。安全管理員名稱只能使用在 Sun Crypto Accelerator 4000 介面卡的網域中，且無需與主機系統上的任何使用者名稱一樣。

建立安全管理員時，名稱是指令行中的選用參數。如果省略安全管理員名稱，`vcaadm` 會提示您提供名稱。(請參閱第 65 頁的「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.
```

在金鑰庫中建立使用者

這些使用者名稱只能使用在 Sun Crypto Accelerator 4000 介面卡的網域中，且無需與網站伺服器程序的 UNIX 使用者名稱一樣。

建立使用者時，使用者名稱是指令行中的選用參數。如果省略使用者名稱，vcaadm 會提示您提供使用者名稱。(請參閱第 65 頁的「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.
```

網站伺服器啓動時，使用者必須使用此密碼進行驗證。

警告 – 使用者必須記住他們的密碼以便存取其金鑰。沒有任何方法可以擷取遺失的密碼。

注意 – 如果超過五分鐘未輸入指令，使用者帳號會登出。這是可調整的選項。請參閱第 71 頁的「設定自動登出時間」以取得詳細資料。

列出使用者與安全管理員

要列出與金鑰庫相關的使用者或安全管理員，請輸入 `show user` 或 `show so` 指令。

```
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
-----------------------------------------------------
```

變更密碼

僅有安全管理員密碼可以使用 `vcaadm` 變更。安全管理員可以變更他們自己的密碼。請使用 `set password` 指令來變更安全管理員密碼。

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

您可以使用 Sun ONE 網站伺服器 `modutil` 公用程式透過 PKCS#11 介面變更使用者密碼。請參閱 Sun ONE 網站伺服器文件以取得詳細資料。

啓用或停用使用者

注意 – 無法停用安全管理員。建立安全管理員後，即會啓用直到受刪除。

根據預設值，每個使用者建立時均處於啓用狀態。使用者可以停用。停用的使用者無法使用 PKCS#11 介面存取金鑰資料。啓用停用的使用者可回復存取所有該使用者的金鑰資料。

啓用或停用使用者時，使用者名稱是指令行中的選用參數。如果省略使用者名稱，vcaadm 會提示您提供使用者名稱。要停用使用者帳號，請輸入 disable user 指令。

```
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.
```

要啓用帳號，請輸入 enable user 指令。

```
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.
```

刪除使用者

發出 delete user 指令並指定要刪除的使用者。刪除使用者時，使用者名稱是指令行中的選用參數。如果省略使用者名稱，vcaadm 會提示您提供使用者名稱。

```
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.
```

刪除安全管理員

發出 `delete so` 指令並指定要刪除的安全管理員。刪除安全管理員時，安全管理員名稱是指令行中的選用參數。如果省略安全管理員名稱，`vcaadm` 會提示您提供安全管理員名稱。

```
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.
```

備份主要金鑰

金鑰庫儲存在磁碟上，並以主要金鑰加密。此主要金鑰儲存在 Sun Crypto Accelerator 4000 韌體中，且可以由安全管理員備份。

要備份主要金鑰，請使用 `backup` 指令。`backup` 指令需要儲存備份的備份檔案路徑名稱。此路徑名稱可以放在指令行上，如果省略，`vcaadm` 會提示您提供路徑名稱。

備份資料必須設定密碼。此密碼用於對備份檔案中的主要金鑰進行加密。

```
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.
```

警告 – 備份檔案時，請選擇很難猜出的密碼，因爲此密碼可保護金鑰庫的主要金鑰。您還必須記住輸入的密碼。如果沒有密碼，您無法存取主要金鑰備份檔案。如果遺失密碼，沒有任何方法可以擷取該密碼保護的資料。

鎖定金鑰庫以防止備份

網站可能有嚴格的安全性原則，不允許使用 Sun Crypto Accelerator 4000 介面卡的主要金鑰來結束硬體。這可以使用 `set lock` 指令來強制執行。

警告 – 發出此指令後，所有備份主要金鑰的嘗試將失敗。即使重新鎖定主要金鑰，此鎖定仍然存在。清除此設定的唯一方法是使用 `zeroize` 指令將 Sun Crypto Accelerator 4000 介面卡化零。(請參閱第 74 頁的「對介面卡執行軟體化零」)。

```
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.
```

使用 vcaadm 管理介面卡

本章節說明如何使用 `vcaadm` 公用程式管理 Sun Crypto Accelerator 4000 介面卡。

設定自動登出時間

要自訂安全管理員自動登出介面卡之前的時間，請使用 `set timeout` 指令。要變更自動登出時間，請輸入 `set timeout` 指令，接著輸入安全管理員自動登出之前的分鐘數。0 值會禁用自動登出功能。最大延遲時間爲 1,440 分鐘 (1 天)。新初始化的介面卡預設值爲 5 分鐘。

下列指令會將安全管理員的自動登出時間變更爲 10 分鐘：

```
vcaadm{vcaN@hostname, sec-officer}> set timeout 10
```

顯示介面卡狀態

要取得目前 Sun Crypto Accelerator 4000 介面卡的狀態，請發出 `show status` 指令。此指令會顯示該介面卡的硬體與韌體版本、網路介面的 MAC 位址、網路介面的狀態 (開啓與關閉、速度、雙工等等) 及金鑰庫名稱與 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
----------------------------------------------------------------
```

判斷介面卡是否在 FIPS 140-2 模式下操作

如果 Sun Crypto Accelerator 4000 介面卡在 FIPS 140-2 模式下操作，`show status` 指令會顯示下列指令行：

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

如果介面卡不是在 FIPS 140-2 模式下操作，`show status` 指令不會顯示指定 FIPS 140-2 模式的指令行。

您也可以使用 `kstat`(1M) 公用程式判斷介面卡是否在 FIPS 140-2 模式下操作。如果介面卡在 FIPS 140-2 模式下操作，`kstat`(1M) 參數 `vs-mode` 會傳回 `FIPS` 值。請參閱第 39 頁的「編碼與乙太網路驅動程式操作統計」與 `kstat`(1M) 的線上說明頁。

載入新韌體

新增了新功能時，您可以更新 Sun Crypto Accelerator 4000 介面卡的韌體。要載入韌體，請發出 `loadfw` 指令並提供韌體檔案的路徑。

您需要手動使用 `reset` 指令重設介面卡，才能成功更新韌體。重設介面卡時，目前登入的安全管理員會登出。

```
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
```

重設介面卡

在某些情況下，可能需要重設介面卡。要執行此操作，您必須發出 `reset` 指令。系統會詢問您這是否是您要執行的操作。重設 Sun Crypto Accelerator 4000 介面卡可能會暫時停止系統上的編碼加速，除非有其他可以控制載入的活動中 Sun Crypto Accelerator 4000 介面卡。此外，此指令會自動讓您登出 `vcaadm`，因此，如果要繼續管理此裝置，您必須重新登入 `vcaadm` 來重新連接到該裝置。

```
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.
```

重新鎖定介面卡

如果安全性原則變更，您可以要使用新金鑰作爲主要金鑰或遠端存取金鑰。`rekey` 指令可讓您重新產生這些金鑰。

重新鎖定主要金鑰也會導致金鑰庫根據新金鑰重新加密，並會在具有新金鑰庫檔案的情況下使較舊的備份主要金鑰檔案無效。在重新鎖定時備份主要金鑰。如果多個 Sun Crypto Accelerator 4000 介面卡使用相同的金鑰庫，您需要備份此新的主要金鑰，並將其回復到其他其他介面卡。

重新鎖定遠端存取金鑰會讓安全管理員登出，並強制新連線使用新的遠端存取金鑰。

發出 rekey 指令時，您可以指定下列其中一種金鑰類型：

表 4-6 金鑰類型

金鑰類型	動作
master	重新鎖定主要金鑰。
remote	重新鎖定遠端存取金鑰。讓安全管理員登出。
all	重新鎖定主要與遠端存取金鑰。

以下是使用 rekey 指令輸入 all 的金鑰類型的範例：

```
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.
```

對介面卡執行軟體化零

有兩種方式可清除所有金鑰資料上的介面卡。第一種方法是使用硬體跳線 (跳線帽)；此化零形式會將介面卡恢復爲原廠狀態 (Failsafe 模式)。(請參閱第 231 頁的「將 Sun Crypto Accelerator 4000 硬體化零爲原廠狀態」) 第二種方法是使用 zeroize 指令。

注意 – zeroize 指令會移除金鑰資料，而將任何更新的韌體保持不變。此指令也會在成功清除金鑰資料後讓安全管理員登出。

使用 zeroize 指令對介面卡執行軟體化零，請輸入此指令並確認：

```
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 指令

可從 vcaadm 公用程式與 SunVTS 軟體執行診斷。vcaadm 中的 diagnostics 指令在 Sun Crypto Accelerator 4000 硬體中包含三個主要類別：一般硬體、編碼子系統及網路子系統。一般硬體的測試包含 DRAM、快閃記憶體、PCI 匯流排、DMA 控制器及其他硬體內部。編碼子系統的測試包含隨機號碼產生器與編碼加速器。網路子系統上的測試包含 vca 裝置。

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

使用 vcad 指令

vcad 指令可設定與啓動 vcad 監控程序，該監控程序可 vcaadm(1M) 及其他編碼應用程式提供編碼金鑰庫。vcad 監控程序程序也爲驅動程式與硬體處理金鑰庫資料的讀取與寫入。

要輕鬆存取 vcad 指令，請將 Sun Crypto Accelerator 4000 工具目錄放在搜尋路徑中，例如：

```
$ PATH=$PATH:/opt/SUNWconn/cryptov2/sbin/
$ export PATH
```

vcad 指令的指令行語法爲：

```
/opt/SUNWconn/cryptov2/sbin/vcad [-dFlV] [-f config-file]
[-h host-address] [-k keystore-dir] [-L logfile] [-p port] [-s max-size]
[-t seconds][-u username]
```

表 4-7 說明 vcad 指令的支援選項。

表 4-7 vcad 指令選項

選項	說明
-d	開啓除錯功能。除實際訊息本身外，每則訊息包含 vcad 的程序 ID、目前的執行緒 ID 及訊息類別。多個 -d 選項會增加詳細度 (最大爲 2)。使用多個 -d 選項時，一個 -d 相當於將組態檔案中的 DebugLevel 參數設定爲 INFO，-dd 相當於設定爲 DEBUG。
-f *config-file*	指定組態檔案的位置。此組態檔案的預設位置爲 /etc/opt/SUNWconn/vca/vcad.conf。如果使用此選項且無法開啓檔案，vcad 將不會啓動。
-F	在前景中執行 vcad，並將記錄輸出傳送至 stderr。此行爲將取代使用 -L 旗標選擇的 *logfile*。
-h *host-address*	爲 vcad 指定要連結的主機 IPv4 或 IPv6 位址，並接聽收到的連接。使用額外的 -h 選項可指定多個主機或 IP 位址。如果沒有使用此選項，vcad 的預設行爲將在所有可用介面上接聽收到的連接。當特定主機或 IP 位址指定爲連結時，連接僅可建立在回答那些位址與 localhost 的介面上。使用 -h 旗標指定的任何位址或主機會由 -l 選項取代。
-k *keystore-dir*	使用 *keystore-dir* 作爲所有金鑰庫資料的目錄。如果監控程序作爲非超級使用者執行，此目錄必須由該使用者可讀取與可寫入，金鑰庫資料檔案本身也應如此。金鑰庫資料的預設目錄爲：/etc/opt/SUNWconn/vca/keydata。
-l	僅接受來自於本地主機產生的管理用戶端所收到的連接。此選項會取代任何讓監控程序在任何其他介面接聽的指令行或 .conf 檔案指令。
-L *logfile*	將記錄輸出傳送至 *logfile* 而不是系統記錄的標準位置。
-p *port*	使用 *port* 進行所收到連接的連結。用於 6870 的預設連接埠。
-s *max-size*	可讓資料長度達到 *max-size* 位元組的指令傳送至 Sun Crypto Accelerator。管理員可使用此功能，以防止較大的資料磁碟區以單一指令傳送至核心元件。單一指令的預設最大大小爲 4 MB (4194304 位元組)。

表 4-7 vcad 指令選項 *(續)*

選項	說明
`-t` *seconds*	在 vcad 停止等待來自用戶端的資料時，請將秒設定爲 *seconds* 的數目。如果此計時器過期，則 vcad 與用戶端之間的連線將關閉。
`-u` *username*	作爲 *username* 執行 vcad。如果指定使用者名稱，vcad 將嘗試作爲啓動 vcad 的使用者執行。如果指定使用者名稱且無法在系統中找到此使用者名稱，vcad 將無法啓動。如果 vcad 作爲超級使用者或任何具有使用者 ID 0 的其他帳號執行，vcad 將發出警告。請參閱第 78 頁的「vcad 監控程序安全」以取得作爲超級使用者執行 vcad 的建議。
`-V`	顯示 vcad 的版本資訊。

vcad 組態檔案

vcad 監控程序可從組態檔案取得操作參數。根據預設值，監控程序將在 `/etc/opt/SUNWconn/vca/vcad.conf` 中尋找組態檔案，雖然在執行 vcad 監控程序時其他檔案可使用 vcad 指令的 `-f` 旗標指定。如果沒有使用 `-f` 旗標且無法找到或讀取預設的組態檔案，vcad 監控程序將嘗試使用所有預設值啓動。在此情況下，警告訊息將傳送至標準錯誤輸出。

組態檔案每行包含一個指令。每個指令必須具有一個與其關聯的值。可以使用註解，但必須以井字號 (#) 字元開頭。指令名稱不區分大小寫，但它們的值可能區分大小寫。請參閱表 4-8 中的每個指令說明以取得更多詳細資料。

組態檔案指令可透過使用相同操作參數的指令行選項取代。例如：您可以使用 `-p` 選項取代「Port」組態檔案指令。沒有使用指令行選項或組態檔案指令指定的操作參數將使用內建的預設值。表 4-8 說明 vcad 指令的支援指令行指令。

表 4-8 vcad 指令的指令行指令

指令	說明
`DebugLevel` *level*	可讓使用者設定組態檔案中的三個錯誤層級之一。這三人上層級 (從最少的 verbose 到最多) 爲 Notice (注意事項)、Info (資訊) 及 Debug (錯誤)。Notice 層級爲預設值。
`HostBind` *host*/*IP*	告訴 vcad 連結並接聽指定的 IPv4 或 IPv6 位址，或主機解析的 IP 位址。多個 `HostBind` 指令可讓 vcad 接聽多個位址。如果組態檔案中沒有 `HostBind` 項目，則預設行爲將接聽連接的所有介面。請注意：`-l` 指令行旗標將取代所有 `HostBind` 項目。
`KeyStoreDir` *directory*	可讓管理員爲金鑰庫檔案的儲存選擇備用目錄。該目錄必須爲執行 vcad 的使用者讀取與寫入權限 (請參閱 [illegible]/指令)。金鑰庫目錄的預設位置爲：`/etc/opt/SUNWconn/vca/keydata`。

表 4-8 vcad 指令的指令行指令 *(續)*

指令	說明
`LogFile` *logfile*	使用 *logfile* 作爲寫入所有記錄資料的位置。根據預設值，記錄資料將寫入系統記錄。如果使用 `-F` (在前景中執行) 指令行旗標，該指令將被忽略，且 `vcad` 記錄資料將被傳送至標準的錯誤裝置。
`MaxData` *size*	設定單一指令傳送的最大允許資料的位元組大小。根據預設值，該值爲 4 MB (4194304 位元組)。如果傳送的資料超過此值，`vcad` 會將錯誤返回至用戶端並關閉連接。
`Port` *port*	設定接聽連接埠。`vcad` 接聽的預設連接埠爲 6870。如果管理員需要讓 `vcad` 接聽特定連接埠 (通常小於 1024 的連接埠)，`vcad` 必須以具有超級使用者權限的使用者身份執行。請參閱第 78 頁的「`vcad` 監控程序安全」與安全相關的注意事項。
`Timeout` *seconds*	在接收到該資料的第一個位元組後，可讓管理員設定指令資料的逾時值。此逾時值可延遲的讀取對特定卡的鎖定存取。當其等待傳送新指令的連接用戶端時，此逾時不適用於 `vcad`。韌體逾時值會涉及此問題。(請參閱第 71 頁的「設定自動登出時間」。) 預設逾時爲 300 秒 (五分鐘)。
`User` *username*	設定 vcad 以 username 身份執行。監控程序嘗試將其真實使用者 ID 設定爲與 username 關聯的 UID。該指令的預設值爲啓動 vcad 程序的使用者。

vcad 監控程序安全

因爲 `vcad` 監控程序會使用 TCP 連接埠接聽，所以應該考量某些安全建議。

在執行 `vcad` 時，程序應該以使用者 ID 身份執行，該使用者 ID 不具有超級使用者權限，即不是 `UID0` 帳號。您不得直接從網路登入此使用者帳號。該帳號應該沒有密碼或有鎖定的密碼及沒有登入 shell。`/etc/shadow` 檔案中用於此帳號的項目應該具有 `NP` 或 `*LK*`。

根據預設值，`vcad` 監控程序將嘗試以監控程序使用者帳號啓動。即使此帳號已停用，`vcad` 監控程序將正確啓動，但是此帳號應該在系統中存在。執行下列步驟，以便手動設定 `vcad` 以不同的使用者名稱執行。

▼ 設定 vcad 監控程序以不同的使用者名稱執行

1. 設定對 /dev/vcactl 的讀/寫存取。

vcad 監控程序會直接與 /dev/vcactl 通訊，以傳送指令資料，並從 Sun Crypto Accelerator 4000 韌體獲得金鑰庫 I/O 指令。應該設定權限與所有權，以便僅由執行 vcad 的使用者帳號可以讀取並寫入 /dev/vcactl。根據預設值，將新增 vcactl 模組，以便僅由具有所有者讀取與寫入權限的監控程序可以擁有次要節點。變更這些權限最安全的方式是，使用 rem_drv(1m) 與 add_drv(1m) 重新註冊 vcactl 模組。

```
rem_drvvcactl
add_drv-m '* MODE USERGROUP' vcactl
```

USER 與 GROUP 資料位置應該包含裝置次要節點所需的使用者與群組所有權。MODE 是裝置次要節點的檔案模式。0600 是 vcactl 模組的建議模式。請參閱 add_drv(1m) man 說明頁以取得更多詳細資料。

2. 設定對金鑰庫的讀/寫存取。

對於執行金鑰庫 I/O 操作的 vcad 監控程序，它必須能夠存取在其組態中指定的金鑰庫目錄。金鑰庫目錄必須具有僅對執行 vcad 的使用者帳號適用的讀取、寫入及執行權限。此目錄中的金鑰庫檔案應該僅允許該使用者的讀取與寫入權限。

3. 執行非特定 TCP 連接埠上的 vcad 監控程序。

如果不具有超級使用者權限而執行 vcad 監控程序，它無法連結至特定連接埠。通常，非特定連接埠爲 1024 或更高。如果特定系統上 tcp_smallest_nonpriv_port 參數的值不是 1024，請使用 ndd 確定該值。根據預設值，vcad 監控程序使用連接埠 6870。

範例

範例 1：啓動 vcad 監控程序以接聽連接埠 5525。

```
# /opt/SUNWconn/cryptov2/sbin/vcad -p 5525
```

範例 2：啓動具有額外除錯資訊的 vcad 監控程序，並將資訊傳送至螢幕。

```
# /opt/SUNWconn/cryptov2/sbin/vcad -Fdd
```

該啓動方法會在啓動時產生下列執行結果：

```
vcad[1679/1]: [debug] got exclusive lock
vcad[1679/1]: [info] Security daemon starting up
vcad[1679/1]: [debug] Starting file handling thread
vcad[1679/1]: [debug] Starting TCPserver
vcad[1679/1]: [debug] TCP socket bound on port 6870
vcad[1679/1]: [debug] fd is 6
```

執行兩個層級的執行結果時新連接將會開啓與關閉，此時 vcad 監控程序也會提供注意事項。

範例 3：啓動 vcad 監控程序，並使用備用組態檔案。

```
# /opt/SUNWconn/cryptov2/sbin/vcad -f /etc/opt/SUNWconn/vca/alt-vcad.conf
```

使用 vcadiag 公用程式

vcadiag 公用程式提供了 Sun Crypto Accelerator 4000 介面卡的指令行介面，可讓超級使用者在未以安全管理員的身份進行驗證的情況下執行管理工作。指令行選項可判斷 vcadiag 執行的動作。

要輕鬆存取 vcadiag 公用程式，請將 Sun Crypto Accelerator 4000 工具目錄放在搜尋路徑中，例如：

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

vcadiag 指令行語法爲：

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

注意 – 使用 [-DFKRZ] 選項時，vca*N* 是介面卡的裝置名稱，其中 *N* 與 Sun Crypto Accelerator 4000 裝置例項號碼相對應。

表 4-9 說明 vcadiag 公用程式的支援選項。

表 4-9 vcadiag 選項

選項	意義
-D vca*N*	在 Sun Crypto Accelerator 4000 介面卡上執行診斷。
-F vca*N*	顯示 Sun Crypto Accelerator 4000 介面卡使用的可保護管理工作階段的公開金鑰指紋。
-K vca*N*	顯示 Sun Crypto Accelerator 4000 介面卡使用的可保護管理工作階段的公開金鑰與公開金鑰指紋。
-Q	提供有關 Sun Crypto Accelerator 4000 裝置與軟體元件的資訊。執行結果爲下列以冒號分隔的資訊清單： • 裝置 • 內部功能 • 金鑰庫名稱 • 金鑰庫序號 • 金鑰庫參考計數。 您可以使用此選項來判斷裝置與金鑰庫之間的關聯。
-R vca*N*	重設介面卡。
-Z vca*N*	將介面卡化零。

以下是 -D 選項的範例：

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

以下是 -F 選項的範例：

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

以下是 -K 選項的範例：

```
# 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
```

以下是 -Q 選項的範例：

```
# 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
```

以下是 -R 選項的範例：

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

以下是 -Z 選項的範例：

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

使用 pk11export 公用程式

pk11export 公用程式從金鑰資料庫擷取金鑰與憑證，並將其轉換爲 PKCS#12 可匯入格式。該公用程式要求 PKCS#11 介面擷取物件，並將金鑰與憑證置於 PKCS#12 檔案中。每次僅能擷取一個金鑰與憑證組。

如果動態程式庫中包含介面，則此公用程式將用於不同的 PKCS#11 供應器。在滿足下列要求時，pk11export 公用程式將透過 PKCS#11 供應器匯出金鑰：

- PKCS#11 介面必須執行 C_WrapKey PKCS#11 功能。
- PKCS#11 介面必須執行 CKM_DES3_CBC_PAD 與 CKM_SHA_1 PKCS#11 機制。
- 要匯出的金鑰必須設定 CKA_EXTRACTABLE 屬性。

pk11export 的指令行語法如下所示：

- /opt/SUNWconn/cryptov2/bin/pk11export -V
- /opt/SUNWconn/cryptov2/bin/pk11export -l [-p *pkcs11-lib*]
- /opt/SUNWconn/cryptov2/bin/pk11export [-n *friendly-name*] [-o *filename*] [-p *pkcs11-lib*] *token-name*

表 4-10 說明 pk11export 公用程式的支援選項。

表 4-10 pk11export 選項

選項	說明
-l	列出了由指定 PKCS#11 程式庫辨識的所有可用標記。
-n *friendly-name*	指定要匯出的金鑰與憑證對。*friendly-name* 爲字串值。
-o *filename*	將結果 PKCS#12 檔案置於 *filename* 檔案中。如果沒有指定執行結果 *filename*，PKCS#12 檔案將以檔案名稱 pkcs12file 置於目前目錄中。
-p *pkcs11-lib*	指定從其中擷取金鑰與憑證的 PKCS#11 程式庫。該選項要求至動態程式庫的完整路徑，在 *pkcs11-lib* 變數中有提供。根據預設值，pk11export 使用 Sun Crypto Accelerator 1000 PKCS#11 程式庫 (/opt/SUNWconn/crypto/lib/libpkcs11.so)，但是，任何 PKCS#11 程式庫可使用該選項中的 *pkcs11-lib* 變數指定。
-V	顯示 pk11export 的版本資訊。

範例

範例 1：列出 PKCS#11 實作的標記。

```
# pk11export -l -p /opt/SUNWconn/cryptov2/bin/libvpkcs11.so
0. SUNW acceleration only
1. arf
```

範例 2：從 PKCS#11 標記 nobody@webserv 匯出 Server-Cert 憑證，並置於 /tmp/webserv-export.p12 檔案中。

```
example% pk11export -o /tmp/webserv-export.p12 nobody@webserv
Enter password for nobody@webserv:
Enter password for pkcs12 file:
Re-enter password for pkcs12 file:
/tmp/webserv-export.p12 was created successfully
```

使用 iplssl cfg 指令碼

iplssl cfg 指令碼的選項 1 與 2 會安裝模組以使用 Sun ONE 網站與應用程式伺服器設定與註冊介面卡。指令碼的選項 3 與 4 會將 Sun ONE 網站伺服器金鑰匯入 PKCS#12 格式，或從中匯出。

▼ 在 Sun ONE Web Server 4.1 中使用 iplssl cfg 指令碼的選項 1

- **請參閱第 104 頁的 「設定 Sun ONE Web Server 4.1」。**

▼ 在 Sun ONE Web Server 6.0 中使用 iplssl cfg 指令碼的選項 1

- **請參閱第 113 頁的 「設定 Sun ONE Web Server 6.0」。**

▼ 使用 iplsslcfg 指令碼的選項 2

1. **鍵入下列指令以執行** iplsslcfg **指令碼：**

```
# /opt/SUNWconn/cryptov2/bin/iplsslcfg
```

2. **為 Sun ONE Application Server 鍵入** 2**，然後輸入二進位程式碼與網域路徑。**

```
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): 2

You will now be prompted for four pieces of information:
 1. The location of the Sun ONE Application Server binaries
 2. The location where Sun ONE Server domains are stored
 3. The Application Server domain (e.g. domain1)
 4. The Application Server server name (e.g. server1)

Full path to Application Server binaries: [/opt/SUNWappserver7]:
/opt/SUNWappserver7
Full path to Application Server domains: [/var/opt/SUNWappserver7]:
/var/opt/SUNWappserver7
Application Server domain: domain1
Application Server server name: server1
This script will update your Sun ONE Application Server installation
in /opt/SUNWappserver7 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
/var/opt/SUNWappserver7/domains/domain1/server1/config...
Module "Sun Crypto Accelerator 4000" added to database.
/opt/SUNWappserver7 has been configured to use
the Sun Crypto Accelerator.

<Press ENTER to continue>
```

3. **鍵入 `0` 以結束。**

▼ 使用 `iplsslcfg` 指令碼的選項 3

此選項會從 Sun ONE 網站伺服器內部資料庫中以 PKCS#12 格式匯出 SSL 憑證與金鑰。然後，這些憑證可以被重新匯入 Sun Crypto Accelerator 4000 模組。

1. **鍵入下列指令以執行 `iplsslcfg` 指令碼：**

```
# /opt/SUNWconn/cryptov2/bin/iplsslcfg
```

2. **鍵入 `3` 以將 Sun ONE 網站伺服器金鑰匯出為 PKCS#12 格式，然後按下 Return。**

```
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): 3
```

3. **鍵入 Sun ONE 伺服器目錄的路徑。**

`iplsslcfg` 公用程式會搜尋您可以匯出金鑰的任何潛在憑證與金鑰資料庫。

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

4. **從提供的清單中鍵入名稱。**

```
The following certificate databases were found:
https-machine.domain.com-webserv1-
https-machine.domain.com-webserv2-
Which certificate database do you wish to export from?
https-machine.domain.com-webserv1-
```

5. **提供您要匯出的伺服器憑證友好名稱。**

   根據預設值，該名稱爲 erver-Cert。

```
Please provide the name for the certificate you wish to export.
If you wish to export from a hardware device, you will need to
provide the token name followed by a ":" and the certificate name.
Not all external tokens will allow keys to be exported.
Certificate Name [Server-Cert]: Server-Cert
```

6. **指定 CS#12 檔案的路徑與檔案名稱。**

```
Please specify the path where the PKCS#12 file will be stored:
/tmp/export.p12
```

7. **輸入密碼**

   在成功驗證時，系統會提示您設定 PKCS#12 檔案的密碼。建立密碼後，PKCS#12 檔案將被寫入您在步驟 6 中選擇的檔案名稱。

```
Enter Password or Pin for "NSS Certificate DB":
Enter password for PKCS12 file:
Re-enter password:
pk12util: PKCS12 EXPORT SUCCESSFUL
Successfully created the PKCS#12 file.
<Press ENTER to continue>
```

8. **鍵入 0 以結束。**

▼ 使用 iplsslcfg 指令碼的選項 4

該選項會將金鑰與憑證從 PKCS#12 格式匯入介面卡。

1. **鍵入下列指令以執行 iplsslcfg 指令碼：**

```
# /opt/SUNWconn/cryptov2/bin/iplsslcfg
```

2. **鍵入 4 以便為 Sun ONE 網站伺服器從 PKCS#12 格式匯入金鑰，然後按下 Return。**

```
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): 4
```

3. **鍵入 Sun ONE 伺服器目錄的路徑。**

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

4. **鍵入您要匯入的 PKCS#12 檔案之路徑。**

```
Enter the path to the PKCS#12 file: /tmp/export.p12
```

5. **對下面的問題回答是。**

```
Will you be importing to a hardware device? [Y/N]: Y
```

6. **鍵入您設定在初始化時使用的介面卡之金鑰庫名稱。**

```
Enter the token name: vca0
```

7. **鍵入 *username:password* 字串以成功驗證。請參閱**表 5-1**。**

```
Enter Password or Pin for "vca0":
```

8. **鍵入用於保護 PKCS#12 檔案的密碼。**

```
Enter password for PKCS12 file:
Import successful.

<Press ENTER to continue>
```

使用 apsslcfg 指令碼

apsslcfg 指令碼的選項 1 會設定 SSL 的 Apache 網站伺服器。選項 2 會設定 Apache 網站伺服器的金鑰。

注意 – apsslcfg 指令碼僅支援 Apache Web Server 1.3.26。

▼ 使用 apsslcfg 指令碼的選項 1

- **請參閱第 162 頁的 「設定 Apache Web Server 1.3x」。**

使用 apsslcfg 指令碼的選項 2

選項 2 有 3 個後續選項，如下所示：

1. 產生金鑰組並 Apache 的憑證
2. 將 Apache (PEM 編碼 X.509) 金鑰匯出爲 PKCS#12 格式
3. 將金鑰從 PKCS#12 格式匯入 Apache (PEM 編碼 X.509)

▼ 產生金鑰組並 Apache 的憑證

該選項會產生可提交至授權單位的 RSA 金鑰與憑證要求。

1. **鍵入 `1` 以選擇此選項。**
2. **鍵入二進位程式碼與 Apache 模組的路徑，及組態檔案的路徑。**

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

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

3. **鍵入金鑰的路徑。**

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

4. **鍵入金鑰與憑證要求檔案的基礎名稱。**

   該名稱爲預先準備的檔案名稱。例如：如果您選擇 `cert1`，金鑰檔案名稱將爲 `cert1-key.pem` 且憑證要求檔案名稱爲 `cert1-certreq.pem`。

```
Please choose a base name for the key and request file: cert1
```

5. **選擇要產生的 RSA 金鑰的大小。**

   選擇位元組大小後，即可產生 RSA 金鑰。

```
What size would you like the RSA key to be [1024]? 1024
```

6. **鍵入加密金鑰檔案的密碼。**

   使用強固式密碼，不要忘記。

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

7. **鍵入要求的憑證名稱元件。**

憑證要求將被寫入可提交至授權單位的檔案。

```
-----
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]: California
Locality Name (eg, city) []: San Diego
Organization Name (eg, company) []: Company
Organizational Unit Name (eg, section) []: Department
SSL Server Name (eg, www.company.com) []: www.company.com
Email Address []: admin@domain.com

The keyfile is stored in /etc/apache/keys/cert1-key.pem.
The certificate request is in /etc/apache/keys/cert1-certreq.pem.

<Press ENTER to continue>
```

▼ 將 Apache (PEM 編碼 X.509) 金鑰匯出爲 PKCS#12 格式

該選項可讓您將 Apache 網站伺服器金鑰與憑證置於 PKCS#12 檔案中。

1. **鍵入 2 以選擇此選項。**
2. **鍵入金鑰與憑證檔案的路徑。**

   如果金鑰與憑證檔案是同一檔案，請將相同的路徑鍵入兩次。

注意 – 金鑰與憑證資料可以儲存在相同檔案或單獨的檔案中。但是，在儲存不同檔案時，檔案名稱必須相同。

```
Enter the path to the key file:
Enter the path to the certificate file:
```

3. **鍵入輸出 PKCS#12 檔案的路徑。**

```
Please specify the path where the PKCS#12
file will be stored:
```

4. **鍵入憑證的友好名稱。**

   該名稱可唯一識別憑證與金鑰組。

```
Please provide a friendly name for the PKCS#12 being
built.  This friendly name is necessary when
importing your PKCS#12 file for use by other web servers.
Friendly Name [Server-Cert]:
```

5. **鍵入可保護將金鑰置於 PCKS#12 檔案中的密碼。**

```
Enter pass phrase for /etc/apache/keys/ap1-key.pem:
```

6. **鍵入保護 PKCS#12 檔案中金鑰資料的密碼。**

   PKCS#12 檔案將被寫入上面指定的檔案。

```
Enter Export Password:
Verifying - Enter Export Password:
Your PKCS#12 file has been created successfully and is in
/tmp/exp.p12

<Press ENTER to continue>
```

▼ 將金鑰從 PKCS#12 格式匯入 Apache (PEM 編碼 X.509)

該選項可讓您從 PKCS#12 檔案擷取金鑰與憑證，並在 Apache 網站伺服器中使用。

1. **鍵入 `3` 以選擇此選項。**
2. **鍵入 PKCS#12 檔案的路徑與檔案名稱。**

```
Enter the path to the PKCS#12 file:
```

3. **鍵入所擷取金鑰與憑證的路徑。**

```
Enter the directory where keys and certificates
will be stored:
```

4. **鍵入金鑰與憑證檔案的檔案名稱。**

   兩個加密的金鑰與憑證都將包含在同一檔案中。

```
Please choose a name for the key and
Certificate file. This file will contain
both the encrypted key and the certificate:
```

5. **鍵入用於保護 PKCS#12 檔案的密碼。**

```
Enter Import Password:
MAC verified OK
```

6. **鍵入新密碼以保護 Apache 可讀格式的加密金鑰檔案。**

   金鑰與憑證資料將被寫入在步驟 4 中指定的檔案。

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

The keys have been successfully extracted to the file
/etc/apache/key2/yakstuff.pem.

<Press ENTER to continue>
```

將不同的 MAC 位址指派給安裝在相同伺服器中的多個介面卡

有兩種方法可以將不同的 MAC 位址指派給一個伺服器中的多個介面卡。第一種方法是針對作業系統階層，第二種方法是針對 OpenBoot PROM 階層。

▼ 從終端視窗指派不同的 MAC 位址

1. **請輸入下列指令：**

```
# eeprom "local-mac-address?"=true
```

注意 – 將「local-mac-address?」參數設定爲 true 時，所有非整合網路介面裝置將使用指派給生產設備產品的本地 MAC 位址。

---

2. **重新啟動系統。**

▼ 從 OpenBoot PROM 階層指派不同的 MAC 位址

1. **請在 OpenBoot PROM** ok **提示下輸入下列指令：**

```
ok setenv local-mac-address? true
```

注意 – 將「local-mac-address?」參數設定爲 true 時，所有非整合網路介面裝置將使用指派給生產設備產品的本地 MAC 位址。

---

2. **啟動作業系統。**

第 5 章

安裝與設定 Sun ONE 伺服器軟體

本章說明如何設定 Sun Crypto Accelerator 4000 介面卡以與 Sun ONE 伺服器配合使用。本章包含下列章節：

注意 – 本手冊所述的 Sun ONE 伺服器之前稱爲 iPlanet™ 伺服器。

管理 Sun ONE 網站伺服器的安全

本章節概述使用 Sun ONE 網站伺服器管理 Sun Crypto Accelerator 4000 介面卡的安全功能。

注意 – 要管理金鑰庫，您必須存取系統的系統管理員帳號。

概念與術語

對於透過 PKCS#11 介面與 Sun Crypto Accelerator 4000 介面卡通訊的應用程式 (例如：Sun ONE 網站伺服器)，必須建立金鑰庫與使用者。

注意 – Apache 網站伺服器 (第 6 章) 無法使用本章中所述的金鑰庫或使用者帳號功能。

Sun Crypto Accelerator 4000 介面卡內的使用者是編碼金鑰資料的擁有者。每個金鑰由單一使用者擁有。每個使用者可以擁有多重金鑰。使用者可能會希望擁有多重金鑰以支援不同的組態，例如：`production` 金鑰與 `development` 金鑰 (以反映使用者支援的組織)。

注意 – *使用者*或*使用者帳號*指的是以 `vcaadm` 建立的 Sun Crypto Accelerator 4000 使用者，而非傳統的 UNIX 使用者帳號。UNIX 使用者名稱與 Sun Crypto Accelerator 4000 使用者名稱之間，並沒有固定對應。

金鑰庫是金鑰資料的儲存庫。安全管理員及使用者與金鑰庫相關聯。金鑰庫不僅提供了儲存空間，還提供了使用者帳號擁有金鑰物件的方法。這可讓未以擁有者身份驗證的應用程式看不到金鑰。金鑰庫具有下列三種元件：

- **金鑰物件 –** 儲存用於 Sun ONE 網站伺服器等應用程式的長期金鑰。
- **使用者帳號 –** 這些帳號爲應用程式提供驗證與存取特定金鑰的方法。
- **安全管理員帳號 –** 這些帳號透過 `vcaadm` 存取金鑰管理功能。

注意 – 單一 Sun Crypto Accelerator 4000 介面卡只能有一個金鑰庫。您可以將多個 Sun Crypto Accelerator 4000 介面卡設定爲與相同的金鑰庫共同配合運作，以提供額外效能與容錯功能。

一般安裝包含單一金鑰庫與三個使用者。例如，此類組態可能包含單一金鑰庫 *sca4000-ks-1* 與該金鑰庫中的三個使用者 *webserv*、*dirserv* 及 *mailserv*。這可以讓三個使用者擁有並維護該單一金鑰庫中的伺服器金鑰的存取控制權。圖 5-1 一般安裝概述的圖解。

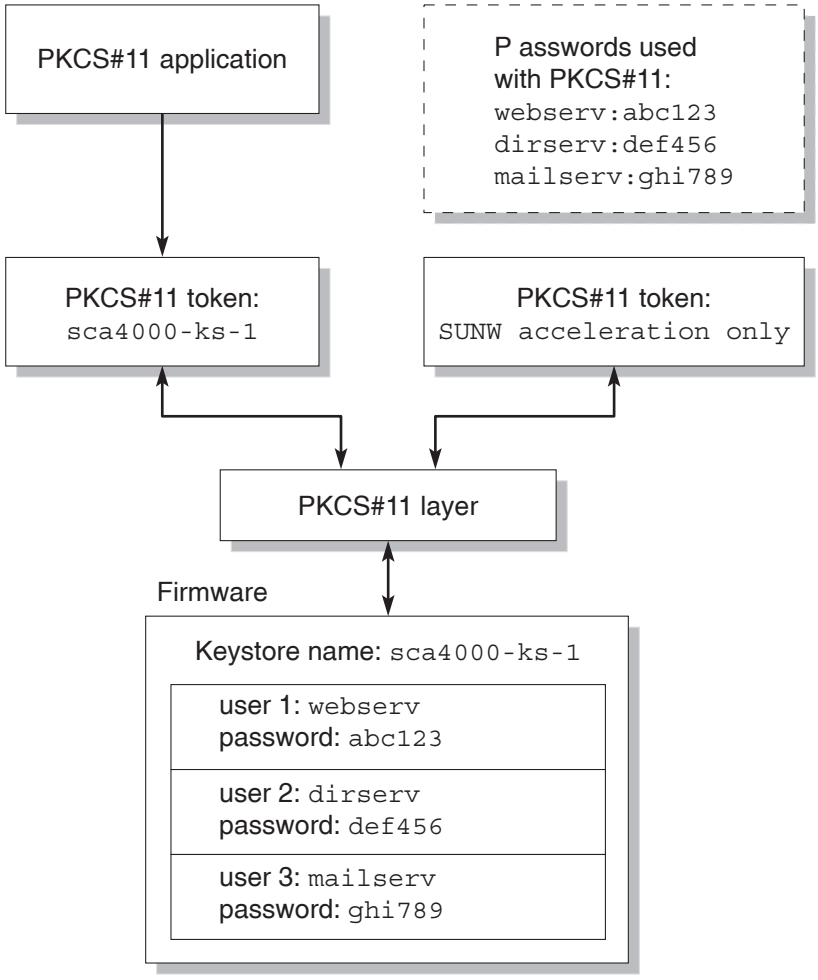

圖 5-1 金鑰庫與使用者概述

您可以使用 `vcaadm` 管理工具來管理 Sun Crypto Accelerator 4000 金鑰庫與使用者。請參閱第 65 頁的「使用 `vcaadm` 管理金鑰庫」。

標記與標記檔案

Keystores 在 Sun ONE 網站伺服器中顯示爲 *tokens*。標記檔案可讓 Sun Crypto Accelerator 4000 管理員對特定應用程式選擇性僅呈現指定標記。

範例

如果根據預設值建立了三個金鑰庫 *engineering*、*finance* 與 *legal*，三個標記將呈現給 Sun ONE 網站伺服器：

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

標記檔案

要取代預設設定，系統上必須有標記檔案。某些應用程式無法處理多個標記。標記檔案是包含一個或多個標記名稱的文字檔案，每行一個標記名稱。

注意 – 標記名稱與金鑰庫名稱是相同的。

Sun ONE 網站伺服器僅會呈現列在標記檔案中的標記。指定標記檔案的方法如下 (依序介紹)：

1. 由環境變數 `SUNW_PKCS11_TOKEN_FILE` 命名的檔案

   某些應用程式軟體會隱藏環境變數，在此情況下則不能使用此方式。

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

   此檔案必須存在於執行 Sun ONE 網站伺服器的 UNIX 使用者的根目錄。Sun ONE 網站伺服器可能會以沒有根目錄的 UNIX 使用者的身份執行，在此情況下則不能使用此方式。

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

如果沒有標記檔案，Sun Crypto Accelerator 4000 軟體會將所有標記呈現給 Sun ONE 網站伺服器。

下列是標記檔案的範例：

```
================================
# 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 – 每個註解以井字號 (#) 開頭，並可接受空行。

如果找不到本小節所述的檔案，則請使用第 98 頁的「標記與標記檔案」中所述的預設方法。

啓用與停用大量加密

根據預設值，Sun ONE 伺服器軟體使用的大量加密功能已停用。您可能要啓用此功能以主要安全地傳輸大檔案。

要使 Sun ONE 伺服器軟體能夠使用 Sun Crypto Accelerator 4000 介面卡的大量加密功能，只要在 `/etc/opt/SUNWconn/cryptov2/` 目錄下建立一個名爲 `sslreg` 的空檔案，然後重新啓動伺服器軟體。

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

要停用大量加密功能，則必須刪除 `sslreg` 檔案，然後重新啓動伺服器軟體。

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

設定 Sun ONE 網站伺服器

本章節說明下列主題：

密碼

啓用 Sun ONE 網站伺服器的過程中，系統會要求您輸入幾個密碼。表 5-1 提供了每一個步驟的說明。這些密碼會在本章中說明。

表 5-1 Sun ONE 網站伺服器所需的密碼

密碼類型	說明
Sun ONE 網站伺服器管理伺服器	啓動 Sun ONE 網站伺服器管理伺服器所需的密碼。此密碼是在安裝 Sun ONE 網站伺服器時指派。
網站伺服器信任資料庫	在安全模式下啓動內部編碼模組時所需的密碼。此密碼是在透過 Sun ONE 網站伺服器管理伺服器建立信任資料庫時指派的。要求與安裝憑證到內部編碼模組時也需要此密碼。
安全管理員	執行 `vcaadm` 特權作業時所需的密碼。
使用者名稱:*密碼*	在安全模式下啓動 Sun Crypto Accelerator 4000 模組時所需的密碼。要求與安裝憑證到內部編碼模組 (*keystore_name*) 時也需要此密碼。此密碼包含以 `vcaadm` 建立的金鑰庫使用者的*使用者名稱*與*密碼*。金鑰庫*使用者名稱*與*密碼*以冒號 (:) 分隔。

建立金鑰庫

您必須先初始化介面卡並在介面卡的金鑰庫中至少建立一個使用者，才能啓用介面卡以用於 Sun ONE 網站伺服器。在初始化過程中爲介面卡建立金鑰庫。您也可以使用現有金鑰庫初始化 Sun Crypto Accelerator 4000 介面卡。請參閱第 62 頁的「使用 `vcaadm` 初始化介面卡」。

注意 – 每個 Sun Crypto Accelerator 4000 介面卡只能設定一個金鑰庫，且每個介面卡必須設定一個金鑰庫。您可以將多個 Sun Crypto Accelerator 4000 介面卡設定爲與相同的金鑰庫共同配合運作，以提供額外效能與容錯功能。

▼ 建立金鑰庫

1. **如果您尚未完成此操作，請將 Sun Crypto Accelerator 4000 工具目錄放在搜尋路徑中，例如：**

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

2. **使用** `vcaadm` **指令存取** `vcaadm` **公用程式，或輸入** `vcaadm -h` *hostname* **以將** `vcaadm` **連接到遠端主機上的介面卡。**

請參閱第 53 頁的「使用 vcaadm 公用程式」。

```
$ vcaadm -h hostname
```

3. **在介面卡的金鑰庫中建立使用者。**

這些使用者名稱只能使用在 Sun Crypto Accelerator 4000 介面卡的網域中，且無需與網站伺服器程序使用的 UNIX 使用者名稱一樣。嘗試建立使用者之前，請記住您必須先以 vcaadm 安全管理員的身份登入。

4. **使用** `create user` **指令建立使用者。**

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

此處建立的*使用者名稱*與*密碼*可同時產生*使用者名稱:密碼* (請參閱表 5-1)。網站伺服器啓動時，您必須使用此密碼進行驗證。這是單一使用者的金鑰庫密碼。

警告 – 使用者必須記住此*使用者名稱:密碼*。如果沒有密碼，使用者無法存取金鑰。沒有任何方法可以擷取遺失的密碼。

5. **結束** `vcaadm`。

```
vcaadm{vcaN@hostname, sec-officer}> exit
```

啓用 Sun ONE 網站伺服器概述

要啓用 Sun ONE 網站伺服器，您必須完成下列程序，下兩個章節會有更詳盡的說明。

1. 安裝 Sun ONE 網站伺服器。
2. 建立信任資料庫。
3. 要求憑證。
4. 安裝憑證。
5. 設定 Sun ONE 網站伺服器。

警告 – 這些程序必須按指定的順序執行，否則會導致不正確的組態設定。

- 如果使用的是 Sun ONE Web Server 4.1，請參閱第 103 頁的「安裝與設定 Sun ONE Web Server 4.1」。
- 如果使用的是 Sun ONE Web Server 6.0，請參閱第 112 頁的「安裝與設定 Sun ONE Web Server 6.0」。

設定 Sun ONE 網站伺服器以在重新啓動時無需使用者互動進行啓動

您可以啓用 Sun ONE 網站伺服器，以在重新啓動時使用加密金鑰執行無人看管啓動。

▼ 建立 Sun ONE 網站伺服器重新啓動時的自動啓動加密金鑰

1. **導覽至** `config` **子目錄以取得 Sun ONE 網站伺服器例項 — 例如：**
   `/usr/iplanet/servers/https-`*webserver-instance-name*`/config`。

2. **建立只有下列幾行的** `password.conf` **檔案 (請參閱**表 5-1 **以瞭解密碼定義)：**

```
internal:trust-db-password
keystore-name:username:password
```

3. **將密碼檔案的檔案所有權設定為網站伺服器用以執行的 UNIX 使用者 ID，並將檔案權限設定為僅檔案所有者可以讀取：**

```
# chown web-server-UNIX-user-ID password.conf
# chmod 400 password.conf
```

安裝與設定 Sun ONE Web Server 4.1

本章節說明如何安裝與設定 Sun ONE Web Server 4.1 以使用介面卡。您必須依序執行這些程序。請參閱 Sun ONE 網站伺服器文件，以取得更多有關安裝與使用 Sun ONE 網站伺服器的資訊。本章節包含下列程序：

▼ 安裝 Sun ONE Web Server 4.1

1. **下載 Sun ONE Web Server 4.1 軟體。**

   您可以在下列 URL 中找到網站伺服器軟體：`http://www.sun.com/`

2. **變更至安裝目錄並擷取網站伺服器軟體。**

3. **透過在指令行中使用 `setup` 指令碼來安裝網站伺服器。**

   伺服器的預設路徑名稱爲 `/usr/netscape/server4`。

   本章參照預設路徑。如果您決定將網站伺服器軟體安裝在不同的位置，請務必記下安裝的位置。

   ```
   # ./setup
   ```

4. **回答安裝指令碼的提示。**

   除下列提示外，您可以接受預設值。

   a. **鍵入 `yes` （是）以同意接受授權條款。**

   b. **輸入完整的網域名稱。**

   c. **輸入兩次 Sun ONE Web Server 4.1 管理伺服器密碼。**

   d. **出現提示時按下 Return。**

設定 Sun ONE Web Server 4.1

這些程序將爲網站伺服器例項建立信任資料庫、使用網站伺服器註冊介面卡、產生並安裝伺服器憑證、啓用 SSL 的網站伺服器。

Sun ONE 網站伺服器管理伺服器必須在設定時啓動並執行。

▼ 建立信任資料庫

1. **啟動 Sun ONE Web Server 4.1 管理伺服器。**

   請透過鍵入下列指令 (而不是執行 `setup` 要求的 `startconsole`) 來啓動 Sun ONE Web Server 4.1 管理伺服器：

   ```
   # /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
   ```

   回應提供了連接伺服器的 URL。

2. **開啟網頁瀏覽器並鍵入下列指令以啟動管理圖形使用者介面：**

   ```
   http://hostname.domain:admin-port
   ```

   在驗證對話方塊中，輸入執行 `setup` 時選擇的 Sun ONE Web Server 4.1 管理伺服器的使用者名稱與密碼。

   注意 – 如果在安裝 Sun ONE 網站伺服器時已使用預設值，請在使用者 ID 或 Sun ONE Web Server 4.1 管理伺服器的使用者名稱中鍵入 **`admin`**。

   ---

3. **選擇 OK (確定)。**

   Sun ONE Web Server 4.1 管理伺服器視窗將會顯示。

4. **為網站伺服器例項建立信任資料庫。**

   a. **在 Sun ONE Web Server 4.1 管理伺服器視窗中按一下 Servers (伺服器) 標籤。**

   b. **選擇伺服器並按一下 Manage (管理) 按鈕。**

   c. **按一下頁面頂部的 Security (安全性) 標籤，然後按一下 「Create Database (建立資料庫)」連結。**

d. 在兩個對話方塊中輸入密碼 (網站伺服器信任資料庫；請參閱表 5-1**)，然後選擇 OK (確定)。**

選擇至少八個字元的密碼。Sun ONE 網站伺服器在安全模式下執行時，您可使用此密碼來啓動內部編碼模組。

您可能要在多個網站伺服器例項中啓用安全功能。如果是這樣，請對每個網站伺服器例項重複步驟 1 到步驟 4。

注意 – 如果要在 Sun ONE Web Server 4.1 管理伺服器上執行 Secure Socket Layer (SSL)，設定信任資料庫的程序是類似的。請參閱 `http://docs.sun.com` 的 *iPlanet Web Server, Enterprise Edition Administrator's Guide*，以取得更多資訊。

▼ 使用網站伺服器註冊介面卡

1. 執行下列指令碼以使用網站伺服器註冊介面卡：

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

此指令碼會提示您選擇伺服器，並爲所選擇的 Sun ONE 伺服器安裝 Sun Crypto Accelerator 4000 編碼模組。然後，此指令碼會更新組態檔以啓用介面卡。

2. 鍵入 `1` **以將 Sun ONE 網站伺服器設定為使用 SSL，然後按下 Return。**

注意 – 此程序假定您在該提示下選擇選項 `1`。如果您要選擇選項 `2`、`3` 或 `4`，請參閱第 84 頁的「使用 `iplsslcfg` 指令碼」。

```
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
```

3. **出現提示時輸入網站伺服器根目錄的路徑，然後按下 Return。**

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

4. **在出現提示時鍵入 y 並按下 Return。**

```
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>
```

5. **鍵入 0 以結束。**

▼ 產生伺服器憑證

1. **鍵入下列指令以重新啟動 Sun ONE Web Server 4.1 管理伺服器：**

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

回應提供了連接伺服器的 URL。

2. **開啟網頁瀏覽器並鍵入下列指令以啟動管理 GUI：**

```
http://hostname.domain:admin-port
```

在驗證對話方塊中，輸入執行 setup 時選擇的 Sun ONE Web Server 4.1 管理伺服器的使用者名稱與密碼。

注意 – 如果在安裝 Sun ONE 網站伺服器時已使用預設值，請在使用者 ID 或 Sun ONE Web Server 4.1 管理伺服器的使用者名稱中鍵入 admin。

---

3. **選擇 OK。**

   Sun ONE Web Server 4.1 管理伺服器視窗將會顯示。

4. **要求伺服器憑證，請選擇 Sun ONE Web Server 4.1 管理伺服器視窗上方附近的 Security (安全性) 標籤** (圖 5-2)**。**

   Create Trust Database (建立信任資料庫) 頁將會顯示。

5. **選擇左窗格上的「Request a Certificate (要求憑證)」連結** (圖 5-2)**。**

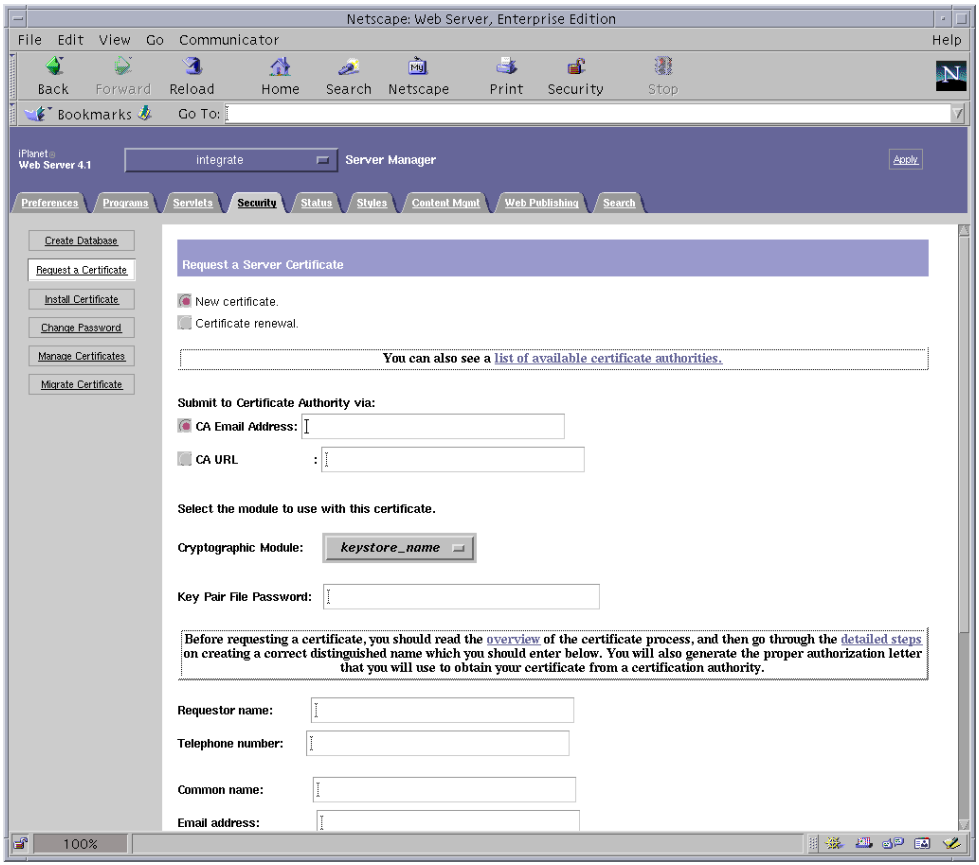

圖 5-2 Sun ONE Web Server 4.1 管理伺服器的 Request a Server Certificate (要求憑證) 對話方塊

6. 使用下列資訊填妥表單，以產生憑證要求：

a. 選擇 New Certificate (新增憑證)。

如果您可以將憑證要求直接發佈到可由網路連線的憑證授權機構或註冊機構，請選擇「CA URL (憑證授權 URL)」連結。否則，請選擇「CA Email Address (憑證授權電子郵件地址)」，然後輸入希望接收憑證要求的電子郵件地址。

b. 選擇要使用的「Cryptographic Module (編碼模組)」。

在此下拉式功能表中，每個金鑰庫都有自己的項目。請確定已選擇正確的金鑰庫。請勿選擇「SUNW acceleration only (僅 SUNW 加速)」。

c. 在「Key Pair File Password (金鑰組檔案密碼)」對話方塊中，為將擁有金鑰的使用者提供密碼。

此密碼是*使用者名稱:密碼* (表 5-1)。

d. 在表 5-2 **的要求者資訊欄位中鍵入適當資訊。**

表 5-2 要求者資訊欄位

欄位	說明
Requestor Name (要求者名稱)	要求者的聯絡資訊
Telephone Number (電話號碼)	要求者的聯絡資訊
Common Name (一般名稱)	造訪者瀏覽器中輸入的網站網域
Email Address (電子郵件地址)	要求者的聯絡資訊
Organization (組織)	公司名稱
Organizational Unit (組織單位)	(選填) 公司部門
Locality (地區)	(選填) 城市、郡、所在地或國家
State (州)	(選填) 完整州名
Country (國家)	代表國家的兩個字母的 ISO 代碼 (例如：美國的代碼爲 US)

e. 按一下 OK (確定) 以提交資訊。

7. 透過憑證授權機構產生憑證。

- 如果選擇將憑證要求發佈到 CA URL，則憑證要求會在此處自動發佈。
- 如果選擇「CA Email Address (憑證授權電子郵件地址)」，請複製以電子郵件傳送給您的憑證要求及標題，並將其送交憑證授權機構。

8. **憑證產生後，請連同標題一起複製到剪貼簿。**

注意 – 憑證不同於憑證要求，且通常以文字格式顯示。請將此資料保留在剪貼簿上，以供下一程序的步驟 5 使用。

▼ 安裝伺服器憑證

1. **選擇 Sun ONE Web Server 4.1 管理伺服器視窗左側的 「Install Certificate (安裝憑證)」連結。**

   憑證授權機構核准憑證要求並核發憑證後，您必須將此憑證安裝在 Sun ONE 網站伺服器中。

2. **按一下 Security (安全性) 標籤。**

3. **在左窗格中，選擇 「Install Certificate (安裝憑證)」連結。**

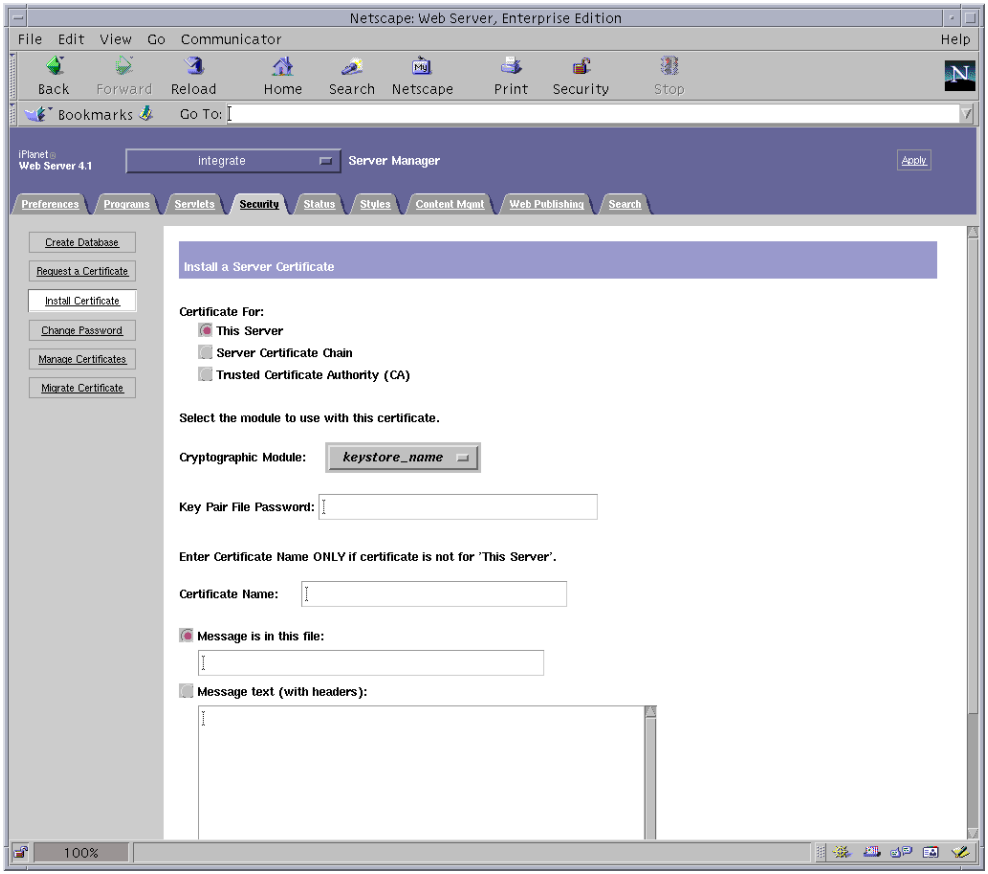

圖 5-3 Sun ONE Web Server 4.1 管理伺服器的 Install a Server Certificate (安裝伺服器憑證) 對話方塊

4. **填妥表單以安裝憑證：**

表 5-3 安全憑證的欄位

欄位	說明
Certificate For (安裝憑證對象)	本伺服器
Cryptographic Module (編碼模組)	在此下拉式功能表中，每個金鑰庫都有自己的項目。請務必選擇正確的金鑰庫名稱。要使用介面卡，您選擇的模組必須與指派給金鑰庫的名稱相同。
Key Pair File Password (金鑰組檔案密碼)	此密碼是*使用者名稱*:*密碼* (表 5-1)。
Certificate Name (憑證名稱)	在大多數情況下，您可以將此欄位留白。如果您提供名稱，在 SSL 支援下執行時，它會變更網站伺服器用來存取憑證與金鑰的名稱。此欄位的預設值爲 `Server-Cert`。

5. **將您從憑證授權機構中複製的憑證 (第 106 頁的 「產生伺服器憑證」的步驟 8 中) 貼到 Message (訊息) 方塊中。**

   系統會顯示一些有關憑證的基本資訊。

6. **按一下 OK (確定)。**

7. **如果所有資料都正確，請選擇 「Add Server Certificate (新增伺服器憑證)」按鈕。**

   螢幕上的訊息會要求您重新啓動伺服器。這不是必要的，因爲網站伺服器例項已完全關閉。

   系統也會通知您，爲使網站伺服器使用 SSL，必須這樣設定網站伺服器。請使用下列程序設定網站伺服器。

注意 – 請參閱 mod_SSL 與 OpenSSL 文件，以取得有關如何自簽憑證以進行測試的資訊。

安裝網站伺服器與伺服器憑證後，您必須啓用 SSL 的網站伺服器。

▼ 啓用 SSL 的網站伺服器

1. **在主 Sun ONE Web Server 4.1 管理伺服器頁中，選擇要執行的網站伺服器例項，然後選擇 Manage (管理)。**

2. **如果未在頁面上方選擇 Preferences (喜好設定) 標籤，請按一下 Preferences (喜好設定) 標籤。**

3. **選擇頁面左側的 Encryption On/Off (加密開啟/關閉) 連結。**

4. **將加密設定為 On (開啟)。**

   對話方塊中的 Port (連接埠) 欄位應該更新爲預設 SSL 連接埠號碼 443。如有必要，請變更連接埠號碼。

5. **按一下 OK (確定) 按鈕。**

6. **按一下 Save (儲存) 按鈕以套用這些變更。**

   網站伺服器目前設定爲在安全模式下執行。

7. **新增下列指令行以編輯** `/usr/netscape/server4/https-`*hostname*`/config/magnus.conf` **檔案 (***hostname* **是網站伺服器的名稱)：**

   ```
   CERTDefaultNickname keystore-name:Server-Cert
   ```

   根據預設值，您所產生的憑證命名爲 `Server-Cert`。如果憑證有不同的名稱，請務必使用您選擇的名稱，而不是 `Server-Cert`。

8. **請選擇您想要管理的伺服器，然後按一下本頁右上角的 Apply (套用) 按鈕。**

   此選項會透過 Sun ONE Web Server 4.1 管理伺服器套用變更。

9. **請按一下「Load Configuration Files (載入組態檔案)」按鈕來套用您稍早在** `magnus.conf` **檔案裡所作的變更。**

   系統會重新導向到可讓您啓動網站伺服器例項的頁面。

   如果在伺服器關閉時選擇 Apply Changes (套用變更) 按鈕，驗證對話方塊會提示您提供*使用者名稱:密碼*。此視窗無法重新調整大小，且您可能會在送出變更時遇到問題。

   此問題有兩種解決方法：

   - 選擇 Load Configuration Files (載入組態檔案)。
   - 先啓動網站伺服器，然後按一下 Apply Changes (套用變更) 按鈕。

10. **在 Sun ONE Web Server 4.1 管理伺服器視窗中，選擇視窗左側的 On/Off 連結。**

11. **輸入伺服器的密碼，然後選擇 OK 按鈕。**

    系統會提示您輸入一個或多個密碼。在內部模組提示下，提供網站伺服器信任資料庫的密碼。

    在模組 *keystore-name* 提示下，輸入該金鑰庫的*使用者名稱:密碼*。

    出現提示時，輸入其他金鑰庫的*使用者名稱:密碼*。

12. **請到下列 URL 檢查具有 SSL 功能的新網站伺服器：**

    `https://`*hostname.domain*`:`*server-port*`/`

注意 – *server-port* 的預設值是 443。

安裝與設定 Sun ONE Web Server 6.0

本章節說明如何安裝與設定 Sun ONE Web Server 6.0 以使用介面卡。您必須依序執行這些程序。請參閱 Sun ONE 網站伺服器文件，以取得更多有關安裝與使用 Sun ONE 網站伺服器的資訊。本章節包含下列程序：

▼ 安裝 Sun ONE Web Server 6.0

1. **下載 Sun ONE Web Server 6.0 軟體。**

   您可以在下列 URL 中找到網站伺服器軟體：`http://www.sun.com/`

2. **變更至安裝目錄並擷取網站伺服器軟體。**

3. **透過在指令行中使用 setup 指令碼來安裝網站伺服器。**

   伺服器的預設路徑名稱爲：`/usr/iplanet/servers`。

   本章參照預設路徑。如果您決定將該軟體安裝在不同的位置，請務必記下安裝的位置。

   ```
   # ./setup
   ```

4. **回答安裝指令碼的提示。**

   除下列提示外，您可以接受預設值：

   a. **鍵入** `yes` （是）**以同意接受授權條款。**

   b. **輸入完整的網域名稱。**

   c. **輸入兩次 Sun ONE Web Server 6.0 管理伺服器密碼。**

   d. **出現提示時按下 Return。**

設定 Sun ONE Web Server 6.0

這些程序將爲網站伺服器例項建立信任資料庫、使用網站伺服器註冊介面卡、產生並安裝伺服器憑證、啓用 SSL 的網站伺服器。

Sun ONE 網站伺服器管理伺服器必須在設定時啓動並執行。

▼ 建立信任資料庫

1. **啟動 Sun ONE Web Server 6.0 管理伺服器。**

   要啓動 Sun ONE Web Server 6.0 管理伺服器，請使用下列指令 (而不是執行 `setup` 要求的 `startconsole`)：

```
# /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
```

   回應提供了連接伺服器的 URL。

2. **開啟網頁瀏覽器並鍵入下列指令以啟動管理 GUI：**

```
http://hostname.domain:admin-port
```

   在驗證對話方塊中，輸入執行 `setup` 時選擇的 Sun ONE Web Server 6.0 管理伺服器的使用者名稱與密碼。

注意 – 如果在安裝 Sun ONE 網站伺服器時已使用預設值，請在使用者 ID 或 Sun ONE Web Server 6.0 管理伺服器的使用者名稱中輸入 `admin`。

---

3. **按一下 OK (確定)。**

   Sun ONE Web Server 6.0 管理伺服器視窗將會顯示。

4. **為網站伺服器例項建立信任資料庫。**

   您可能要在多個網站伺服器例項中啓用安全功能。如果是這樣，請對每個網站伺服器例項重複步驟 1 到步驟 4。

注意 – 如果要在 Sun ONE Web Server 6.0 管理伺服器上執行 SSL，設定信任資料庫的程序是類似的。請參閱 `http://docs.sun.com` 的 *iPlanet Web Server, Enterprise Edition Administrator's Guide*，以取得更多資訊。

---

a. 在「Sun ONE Web Server 6.0 管理伺服器」對話方塊中選擇 Servers (伺服器) 標籤。

b. 選擇伺服器並按一下 Manage (管理) 按鈕。

c. 按一下頁面頂部的 Security (安全性) 標籤，然後按一下「Create Database (建立資料庫)」連結。

d. 在兩個對話方塊中輸入密碼 (網站伺服器信任資料庫；請參閱表 5-1**)，然後按一下 OK (確定)。**

選擇至少八個字元的密碼。Sun ONE 網站伺服器在安全模式下執行時，此密碼將用於啓動內部編號模組。

▼ 使用網站伺服器註冊介面卡

1. 執行下列指令碼以使用網站伺服器註冊介面卡：

```
# /opt/SUNWconn/cryptov2/bin/iplsslcfg
```

此指令碼會提示您選擇伺服器，並爲所選擇的 Sun ONE 伺服器安裝 Sun Crypto Accelerator 4000 編碼模組。然後，此指令碼會更新組態檔以啓用介面卡。

2. 鍵入 `1` 以將 Sun ONE 網站伺服器設定為使用 SSL，然後按下 Return。

注意 – 此程序假定您在該提示下選擇選項 `1`。如果您要選擇選項 `2`、`3` 或 `4`，請參閱第 84 頁的「使用 `iplsslcfg` 指令碼」。

```
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
```

3. 出現提示時輸入網站伺服器根目錄的路徑，然後按下 Return。

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

4. **如果要繼續進行，請在出現提示時鍵入 y，然後按下 Return。**

```
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>
```

5. **鍵入 0 以結束。**

▼ 產生伺服器憑證

1. **鍵入下列指令以重新啟動 Sun ONE Web Server 6.0 管理伺服器：**

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

回應提供了連接伺服器的 URL。

2. **開啟網頁瀏覽器並鍵入下列指令以啟動管理 GUI：**

```
http://hostname.domain:admin-port
```

在驗證對話方塊中，輸入執行 setup 時選擇的 Sun ONE Web Server 6.0 管理伺服器的使用者名稱與密碼。

注意 – 如果在安裝 Sun ONE 網站伺服器時已使用預設值，請在使用者 ID 或 Sun ONE Web Server 6.0 管理伺服器的使用者名稱中輸入 **admin**。

---

3. **按一下 OK (確定)。**

Sun ONE Web Server 6.0 管理伺服器視窗將會顯示。

4. **要求伺服器憑證，請選擇 Sun ONE Web Server 6.0 管理伺服器視窗上方附近的 Security (安全性) 標籤。**

Create Trust Database (建立信任資料庫) 視窗將會顯示。

5. **按一下 Sun ONE Web Server 6.0 管理伺服器視窗左窗格上的 「Request a Certificate (要求憑證)」連結。**

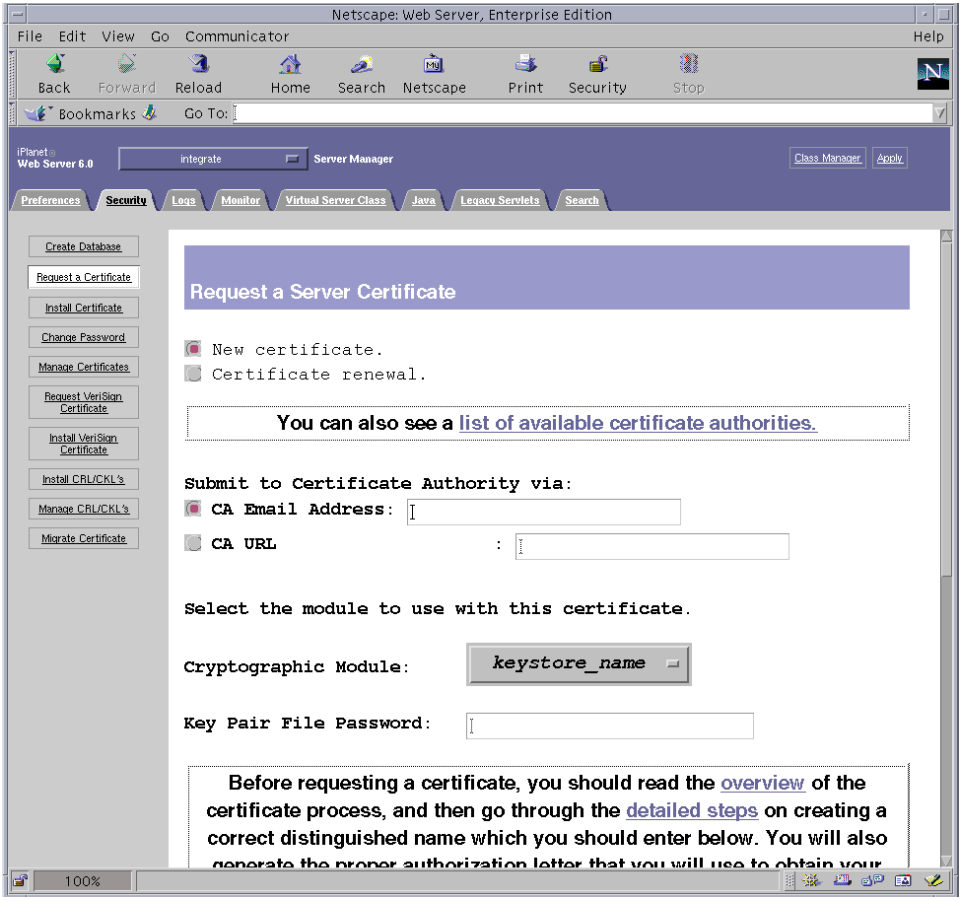

圖 5-4 Sun ONE Web Server 6.0 管理伺服器的 Request a Server Certificate (要求憑證) 對話方塊

6. **使用下列資訊填妥表單，以產生憑證要求：**

   a. **選擇 New Certificate (新增憑證)。**

   如果您可以將憑證要求直接發佈到可由網路連線的憑證授權機構或註冊機構，請選擇 CA URL 連結。否則，請選擇 CA Email Address，然後輸入希望接收憑證要求的電子郵件地址。

   b. **選擇要使用的 「Cryptographic Module (編碼模組)」。**

   在此下拉式功能表中，每個金鑰庫都有自己的項目。請確定已選擇正確的金鑰庫。請勿選擇 「SUNW acceleration only (僅 SUNW 加速)」。

c. 在「Key Pair File Password (金鑰組檔案密碼)」對話方塊中，為將擁有金鑰的使用者提供密碼。

此密碼是*使用者名稱:密碼* (表 5-1)。

d. 在表 5-4 **的要求者資訊欄位中鍵入適當資訊。**

表 5-4 要求者資訊欄位

欄位	說明
Requestor Name (要求者名稱)	要求者的聯絡資訊
Telephone Number (電話號碼)	要求者的聯絡資訊
Common Name (一般名稱)	造訪者瀏覽器中輸入的網站網域
Email Address (電子郵件地址)	要求者的聯絡資訊
Organization (組織)	公司名稱
Organizational Unit (組織單位)	(選填) 公司部門
Locality (地區)	(選填) 城市、郡、所在地或國家
State (州)	(選填) 完整州名
Country (國家)	代表國家的兩個字母的 ISO 代碼 (例如：美國的代碼爲 US)

e. 按一下 OK (確定) 以提交資訊。

7. 透過憑證授權機構產生憑證。

- 如果選擇將憑證要求發佈到 CA URL，則憑證要求會在此處自動發佈。
- 如果選擇 CA Email Address (憑證授權電子郵件地址)，請複製以電子郵件傳送給您的憑證要求及標題，並將其送交憑證授權機構。

8. 憑證產生後，請連同標題一起複製到剪貼簿。

注意 – 憑證不同於憑證要求，且通常以文字格式顯示。請將此資料保留在剪貼簿上，以供第 118 頁的「安裝伺服器憑證」的步驟 5 使用。

▼ 安裝伺服器憑證

1. **選擇 Sun ONE Web Server 6.0 管理伺服器視窗左側的 「Install Certificate (安裝憑證)」連結。**

   憑證授權機構核准憑證要求並核發憑證後，您必須將此憑證安裝在 Sun ONE 網站伺服器中。

2. **按一下 Security (安全性) 標籤。**

3. **在左窗格中，按一下 「Install Certificate (安裝憑證)」連結。**

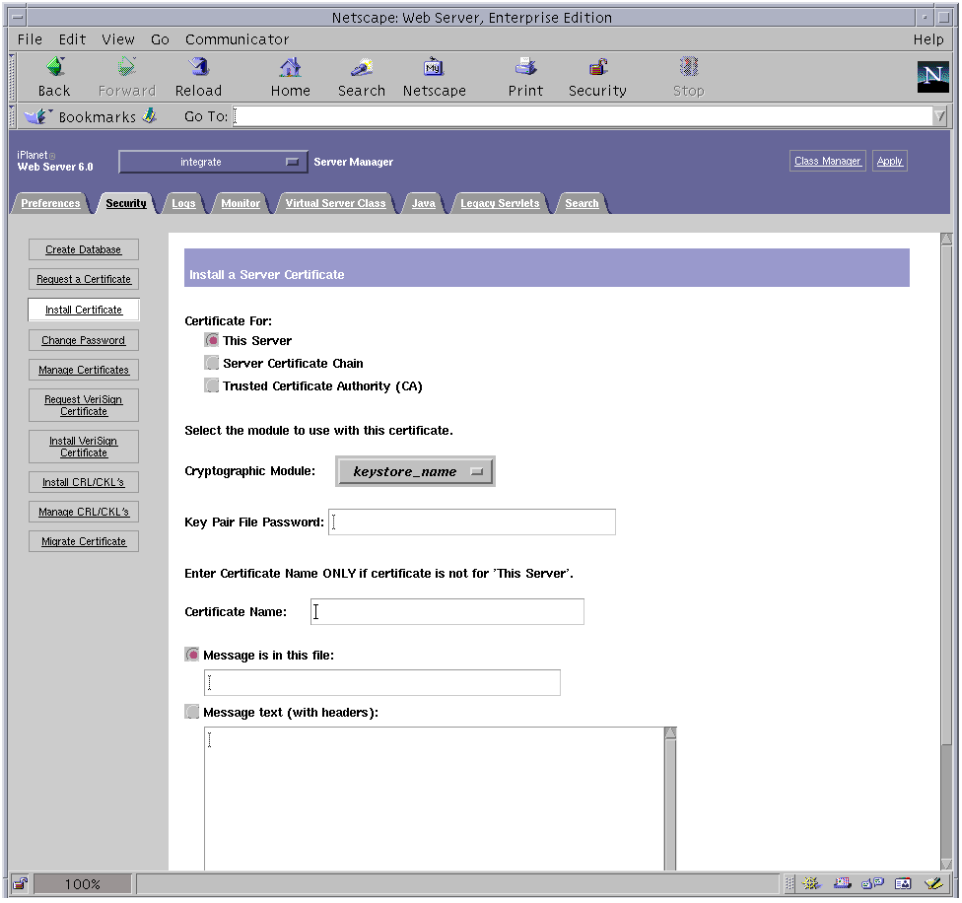

圖 5-5 Sun ONE Web Server 6.0 管理伺服器的 Install a Server Certificate (安裝伺服器憑證) 對話方塊

4. **填妥表單以安裝憑證：**

表 5-5 安裝憑證的欄位

欄位	說明
Certificate For (安裝憑證對象)	本伺服器
Cryptographic Module (編碼模組)	在此下拉式功能表中，每個金鑰庫都有自己的項目。請確定已選擇正確的金鑰庫名稱。要使用介面卡，您必須在 *keystore-name* 表單中選擇模組。
Key Pair File Password (金鑰組檔案密碼)	此密碼是*使用者名稱:密碼* (表 5-1)。
Certificate Name (憑證名稱)	在大多數情況下，您可以將此欄位留白。如果您提供名稱，在 SSL 支援下執行時，它會變更網站伺服器用來存取憑證與金鑰的名稱。此欄位的預設值爲 `Server-Cert`。

5. **將您從憑證授權機構中複製的憑證 (第 115 頁的 「產生伺服器憑證」的步驟 8 中) 貼到 Message (訊息) 文字方塊中。**

   系統會顯示一些有關憑證的基本資訊。

6. **按一下 OK (確定)。**

7. **如果所有資料都正確，請按一下 「Add Server Certificate (新增伺服器憑證)」按鈕。**

   螢幕上的訊息會要求您重新啓動伺服器。這不是必要的，因爲網站伺服器例項已完全關閉。

   系統也會通知您，爲使網站伺服器使用 SSL，必須這樣設定網站伺服器。請使用下列程序設定網站伺服器。

注意 – 請參閱 mod_SSL 與 OpenSSL 文件，以取得有關如何自簽憑證以進行測試的資訊。

安裝網站伺服器與伺服器憑證後，您必須啓用 SSL 的網站伺服器。

▼ 啓用 SSL 的網站伺服器

1. **選擇頁面上方附近的 Preferences 標籤。**

2. **選擇左窗格上的 「Edit Listen Sockets (編輯接聽通訊端)」連結。**

   主窗格會列出該網站伺服器例項的所有接聽通訊端設定。

a. 變更下列欄位：

- **Port (連接埠)：**設定爲將執行具有 SSL 功能的網站伺服器的連接埠 (通常是連接埠 443)。
- **Security (安全性)：**設定爲 On (開啓)。

b. 按一下 OK (確定) 以套用這些變更。

在 Edit Listen Sockets (編輯接聽通訊端) 頁的安全欄位中，現在應該有一個 Attributes (屬性) 連結。

3. **選擇 Attributes (屬性) 連結。**
4. **輸入*使用者名稱*:*密碼*以驗證系統上的金鑰庫。**
5. **如果要變更編碼器的預設值，請選擇編碼器標題下的編碼器套件。**

一個對話方塊將會顯示以變更編碼器設定。您可以選擇「Cipher Default (編碼器預設值)」設定、SSL2、或 SSL3/TLS。如果選擇 Cipher Default (編碼器預設值)，將不會顯示預設值。另外兩個選項需要您選擇要在快顯對話方塊中啓用的演算法。有關編碼器選擇，請參閱 Sun ONE 文件。

6. **選擇金鑰庫的憑證，後接：`Server-Cert` (或您所選擇的名稱)。**

只有適當的金鑰庫使用者所擁有的金鑰會顯示在 Certificate Name (憑證名稱) 欄位中。此金鑰庫使用者是經*使用者名稱*:*密碼*驗證的使用者。

7. **當您已選擇了認證，並確認所有的安全性設定，請按一下 OK (確定) 按鈕。**
8. **選擇右上角的 Apply (套用) 連結，以在啟動伺服器前套用這些變更。**
9. **選擇「Load Configuration Files (載入組態檔案)」連結以套用這些變更。**

系統會重新導向到可讓您啓動網站伺服器例項的頁面。

如果在伺服器關閉時按一下「Apply Changes (套用變更)」按鈕，驗證對話方塊會提示您提供*使用者名稱*:*密碼*。此視窗無法重新調整大小，且您可能會在送出變更時遇到問題。

此問題有兩種解決方法：

- 選擇「Load Configuration Files (載入組態檔案)」。
- 首先啓動網站伺服器，然後按一下「Apply Changes (套用變更)」。

10. **在 Sun ONE Web Server 6.0 管理伺服器視窗中，選擇視窗左側的 On/Off (開啟/關閉) 連結。**
11. **輸入伺服器密碼並按一下 OK (確定) 按鈕。**

系統會提示您輸入一個或多個密碼。在內部模組提示下，提供網站伺服器信任資料庫的密碼。

在模組 *keystore-name* 提示下，輸入*使用者名稱*:*密碼*。

出現提示時，輸入其他金鑰庫的*使用者名稱*:*密碼*。

12. **請到下列 URL 檢查具有 SSL 功能的新網站伺服器：**
    `https://`*hostname.domain:server-port*`/`

注意 – *server-port* 的預設值是 443。

安裝與設定 Sun ONE Application Server 7

本章節說明如何安裝與設定 Sun ONE Application Server 7 以使用介面卡。除應用程式伺服器軟體外，還必須安裝應用程式伺服器附加軟體。您必須依序執行這些程序。請參閱 Sun ONE Application Server 文件，以取得更多有關安裝與使用 Sun ONE Application Server 的資訊。本章節包含下列程序：

▼ 安裝 Sun ONE Application Server 7

1. **下載 Sun ONE Application Server 7 軟體。**
   您可以在下列 URL 中找到應用程式伺服器軟體：`http://www.sun.com/`
   提供幾種不同的 Sun ONE Application Server 7 分佈方式，每種具有獨特的功能。
2. **變更至安裝目錄並擷取應用程式伺服器軟體。**
   安裝目錄的預設路徑與 Sun ONE Application Server 7 軟體的每個分佈不同。
3. **執行 `setup` 程式以啟動基於 GUI 的安裝。**

注意 – 您也可以在終端視窗中執行 `setup -console` 程式以啓動基於指令行的安裝。此程序中的範例假定您使用的是基於 GUI 的安裝。

```
# ./setup
```

4. **回答安裝指令碼中的提示。**

   除下列提示外，您可以接受預設值：

   a. **鍵入 yes (是) 以同意接受授權條款。**

   b. **在系統提示您輸入 JDK (Java™ Development Kit) 位置時，您可以選擇：Use Existing Installation (使用現有安裝程式) (若支援的話)，或 Install From the Appserver Build (從 Appserver 版本安裝)。**

   c. **輸入 Sun ONE Application Server 管理伺服器使用者名稱 (您可以選擇任何名稱)。**

   d. **輸入 Sun ONE Application Server 管理伺服器密碼兩次。**

注意 – 僅在您使用 Solaris 8 OE 時，方可執行下列步驟。

---

5. **如果您使用的是 Solaris 8，請安裝 Solaris 8 Sun ONE Application Server 修正程式 (109326-08)。**

   Solaris 9 無需此修正程式。請從 SunSolve 網站下載 Solaris 8 Sun ONE Application Server 修正程式：`http://sunsolve.sun.com`

   按如下方式新增修正程式：

```
# cd patch-location/SUNWappserver7/patches
# cd patches/109326-08
# ./patchadd .
```

6. **重新啟動系統。**

▼ 安裝 Sun ONE Application Server 附加軟體

1. **下載 Sun ONE Application Server 7 附加軟體。**

   您可以在下列 URL 中找到應用程式伺服器軟體：`http://www.sun.com/`

2. **擷取應用程式伺服器附加軟體。**

3. **變更至** `./AddOns/SSLUtils` **目錄**

4. **建立** `iplsslcfg` **指令碼可在其中調用** `modutil` **安全工具的目錄。**

```
# mkdir /usr/bin/mps
```

   `iplsslcfg` 指令碼可透過此路徑找到 `modutil` 安全工具。

5. **將** `modutil`、`certutil` **及** `pk12util` **二進位程式碼複製到** `/usr/bin/mps/` **路徑。**

```
# cp modutil /usr/bin/mps/
# cp certutil /usr/bin/mps/
# cp pk12util /usr/bin/mps/
```

6. **啟用** `/usr/bin/mps/` **目錄中二進位程式碼的擷取權限。**

```
# chmod 544 /usr/bin/mps/*
```

設定 Sun ONE Application Server 7

這些程序可爲應用程式伺服器例項建立信任資料庫、使用應用程式伺服器註冊介面卡、產生並安裝伺服器認證、啓用 SSL 與 TLS 應用程式伺服器。

Sun ONE Application Server 管理伺服器必須在設定時啓動並執行。

▼ 建立信任資料庫

1. **啟動 Sun ONE Application Server 與 Sun ONE Application Server 管理伺服器。**

```
# installation-directory/bin/asadmin start-appserv
```

注意 – 出現一則訊息，表示應用程式伺服器正在執行。

2. **開啟網頁瀏覽器並輸入下列 URL 以啟動管理 GUI。**

```
http://hostname:4848
```

在驗證對話方塊中，輸入您在執行 `setup` 程式期間建立的 Sun ONE Application Server 使用者名稱與密碼。

注意 – 如果在安裝 Sun ONE Application Server 時已使用預設值，請在使用者 ID 或 Sun ONE Application Server 管理伺服器的使用者名稱中輸入 `admin`。

3. **按一下 OK (確定)。**

4. **為應用程式伺服器例項建立信任資料庫。**

   您可能要在多個應用程式伺服器例項中啓用安全功能。如果是這樣，請對每個應用程式伺服器例項重複步驟 1 到步驟 4。

注意 – 如果要在 Sun ONE Application Server 管理伺服器上執行 SSL，設定信任資料庫的程序是類似的。請參閱 `http://docs.sun.com/source/816-7158-10/` 的 *Sun ONE Application Server 7 Administrator's Guide* 以取得更多資訊。

---

   a. **導覽至管理 GUI 的「Manage Database (管理資料庫)」部分。**

      在左窗格中選擇 Security (安全性) 連結，然後在右窗格中按一下 Manage Database (管理資料庫) 標籤。

   b. **在兩個文字方塊中鍵入至少八個字元的密碼，然後按一下 OK (確定)。**

      此密碼是 Sun ONE Application Server 的信任資料庫密碼。此密碼用於應用程式伺服器在安全模式下執行時，啓動內部編碼模組。

▼ 使用應用程式伺服器註冊介面卡

1. **執行 `iplsslcfg` 指令碼以使用應用程式伺服器註冊介面卡。**

```
# /opt/SUNWconn/cryptov2/bin/iplsslcfg
```

   此指令碼會提示您選擇伺服器，並爲所選擇的 Sun ONE 伺服器安裝 Sun Crypto Accelerator 4000 編碼模組。然後，此指令碼會更新組態檔以啓用介面卡。

2. **為 Sun ONE Application Server 鍵入 `2`，然後輸入二進位程式碼與網域路徑。**

注意 – 此章節中的程序假定您在此提示下選擇選項 1。如果您要選擇選項 3 或 4，請參閱第 84 頁的「使用 iplsslcfg 指令碼」。

```
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): 2
```

3. 鍵入二進位程式碼與網域的位置，以及網域與伺服器名稱。

```
You will now be prompted for four pieces of information:
 1. The location of the Sun ONE Application Server binaries
 2. The location where Sun ONE Server domains are stored
 3. The Application Server domain (e.g. domain1)
 4. The Application Server server name (e.g. server1)

Full path to Application Server binaries: [/opt/SUNWappserver7]:
/opt/SUNWappserver7
Full path to Application Server domains:
[/var/opt/SUNWappserver7]: /var/opt/SUNWappserver7
Application Server domain: domain1
Application Server server name: server1
This script will update your Sun ONE Application Server
installation in /opt/SUNWappserver7 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
/var/opt/SUNWappserver7/domains/domain1/server1/config...
Module "Sun Crypto Accelerator 4000" added to database.
/opt/SUNWappserver7 has been configured to use
the Sun Crypto Accelerator.

<Press ENTER to continue>
```

注意 – 視 Sun ONE Application Server 7 分佈而定，預設安裝目錄可能有所不同。

4. **鍵入** 0 **以結束。**

▼ 產生伺服器憑證

1. **導覽至管理 GUI 的「Certificate Management (憑證管理)」部分。**

   在左窗格中選擇 Security (安全性) 連結，然後在右窗格中選擇「Certificate Management (憑證管理)」標籤。您現在位於管理 GUI「Certificate Management (憑證管理)」部分的 Request (要求) 子功能表視窗中。

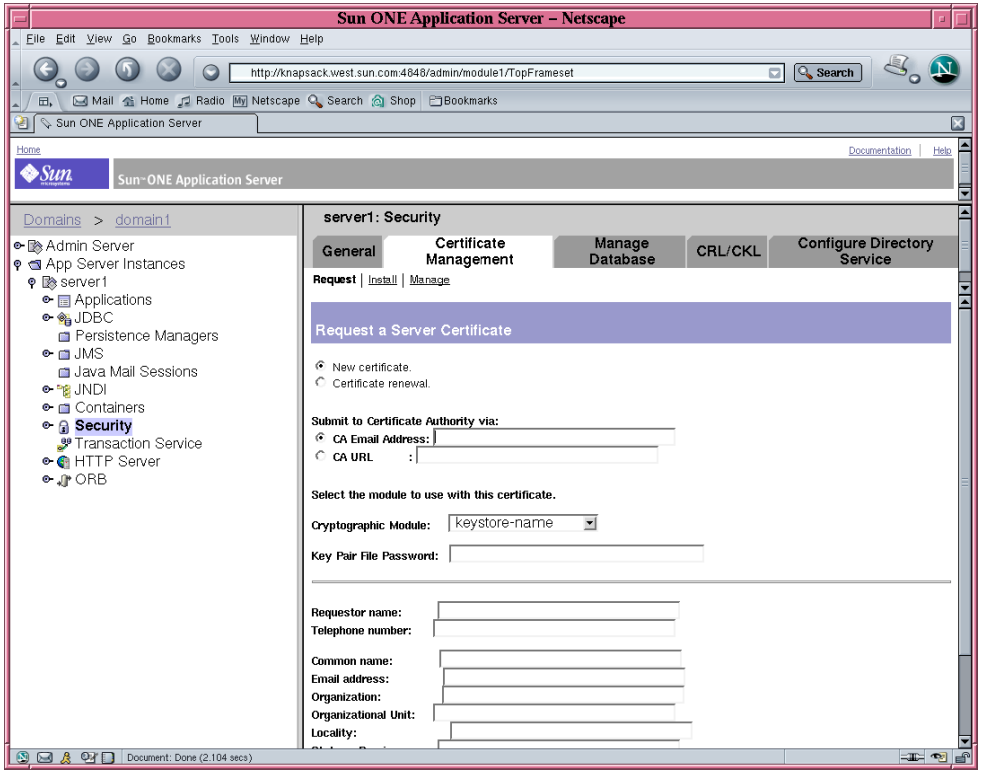

圖 5-6 Sun ONE Application Server 管理伺服器的 Request a Server Certificate (要求伺服器憑證) 對話方塊

2. 使用下列資訊填妥表單，以產生憑證要求：

a. 選擇 New Certificate (新增憑證)。

如果您可以將憑證要求直接發佈到可由網路連線的憑證授權機構或註冊機構，請選擇 CA URL 連結。否則，請選擇 CA Email Address (憑證授權電子郵件地址)，然後輸入希望接收憑證要求的電子郵件地址。

b. 選擇要使用的 「Cryptographic Module (編碼模組)」。

在此下拉式功能表中，每個金鑰庫都有自己的項目。請確定已選擇正確的金鑰庫。請勿選擇 「SUNW acceleration only (僅 SUNW 加速)」。

c. 在 「Key Pair File Password (金鑰組檔案密碼)」對話方塊中，為將擁有金鑰的使用者提供密碼。

此密碼爲 *username:password* (請參閱表 5-1)。

d. 在表 5-6 的要求者資訊欄位中鍵入適當資訊。

表 5-6 要求者資訊欄位

欄位	說明
Requestor Name (要求者名稱)	要求者的聯絡資訊
Telephone Number (電話號碼)	要求者的聯絡資訊
Common Name (一般名稱)	造訪者瀏覽器中輸入的網站網域
Email Address (電子郵件地址)	要求者的聯絡資訊
Organization (組織)	公司名稱
Organizational Unit (組織單位)	(選填) 公司部門
Locality (地區)	(選填) 城市、郡、所在地或國家
State (州)	(選填) 完整州名
Country (國家)	代表國家的兩個字母的 ISO 代碼 (例如：美國的代碼爲 US)

e. 按一下 OK (確定) 以提交資訊。

3. 透過憑證授權機構產生憑證。

- 如果選擇將憑證要求發佈到 CA URL，則憑證要求會在此處自動發佈。
- 如果選擇 CA Email Address (憑證授權電子郵件地址)，請複製以電子郵件傳送給您的憑證要求及標題，並將其送交憑證授權機構。

4. **憑證產生後，請連同標題一起複製到剪貼簿。**

注意 – 憑證不同於憑證要求，且通常以文字格式顯示。請將此資料保留在剪貼簿上，以供第 128 頁的「安裝伺服器憑證」的步驟 4 使用。

▼ 安裝伺服器憑證

1. **在管理 GUI「Certificate Management (憑證管理)」的右窗格中選擇 Install (安裝) 連結。**

   您現在位於管理 GUI「Certificate Management (憑證管理)」部分的 Install (安裝) 子功能表視窗中。

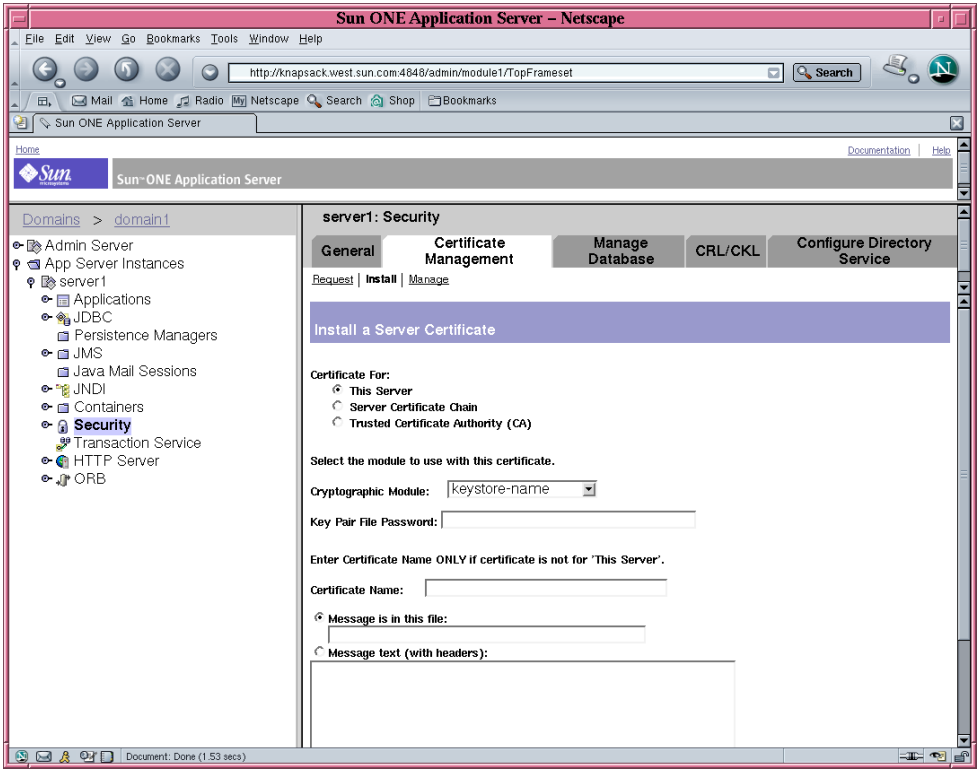

圖 5-7 Sun ONE Application Server 管理伺服器的 Install a Server Certificate (安裝伺服器憑證) 對話方塊

2. **填妥表單以安裝憑證：**

表 5-7 安全憑證的欄位

欄位	說明
Certificate For (安裝憑證對象)	本伺服器
Cryptographic Module (編碼模組)	在此下拉式功能表中，每個金鑰庫都有自己的項目。請確定已選擇正確的金鑰庫名稱。要使用 Sun Crypto Accelerator 4000 介面卡，您必須選擇具有與您在要求憑證時選定名稱相同的模組。
Key Pair File Password (金鑰組檔案密碼)	此密碼是*使用者名稱:密碼*。
Certificate Name (憑證名稱)	在大多數情況下，您可以將此欄位留白。如果您提供名稱，在 SSL 支援下執行時，它會變更應用程式伺服器用來存取憑證與金鑰的名稱。此欄位的預設值爲 `Server-Cert`。

3. **選擇 Message (訊息) 文字 (含標頭) 圓形按鈕。**

4. **按一下「Message (訊息) 文字 (含標頭)：」圓形按鈕，然後將您在憑證授權複製的憑證 (步驟 4 中的第 126 頁的「產生伺服器憑證」) 貼到圓形按鈕正文的文字方塊中。**

5. **按一下 OK (確定)。**

   系統會顯示一些有關憑證的基本資訊。

6. **如果所有資料都正確，請按一下「Add Server Certificate (新增伺服器憑證)」。**

   系統將提示您重新啓動應用程式伺服器。請勿重新啓動應用程式伺服器，它會在 SSL 組態完成後重新啓動。系統也會通知您，爲使應用程式伺服器使用 SSL，必須這樣設定應用程式伺服器。

▼ 啓用 SSL 的應用程式伺服器

1. **在終端視窗中鍵入下列指令。**

   您也必須在執行此指令後鍵入 Sun ONE Application Server 管理伺服器密碼。

注意 – 如果您在本地主機上執行指令且 Sun ONE Application Server 管理伺服器設定爲使用預設的 4848 連接埠，則您可省略 `--host` *hostname* `--port` *administration-server-port* 引數。

```
# installation-directory/bin/asadmin create-ssl --user app-admin --host
hostname --port administration-server-port --type http-listener --certname
keystore-name:server-certificate-name --instance server-name http-listener
password>
```

2. **在管理 GUI 的左窗格中，選擇 HTTP Server (HTTP 伺服器) 連結左邊的擴展器圖示。**
   HTTP Server (HTTP 伺服器) 子功能表項目將會出現。

3. **選擇「HTTP Server (HTTP 伺服器)」連結下面的「HTTP Listeners (HTTP 監聽器)」子功能表項目。**

4. **在右窗格中，選擇您要設定用於 SSL/TLS 的 HTTP 監聽器，並選擇 HTTP 監聽器的相關連結。**
   將會出現一個視窗，您可在其中編輯 HTTP 監聽器的內容。

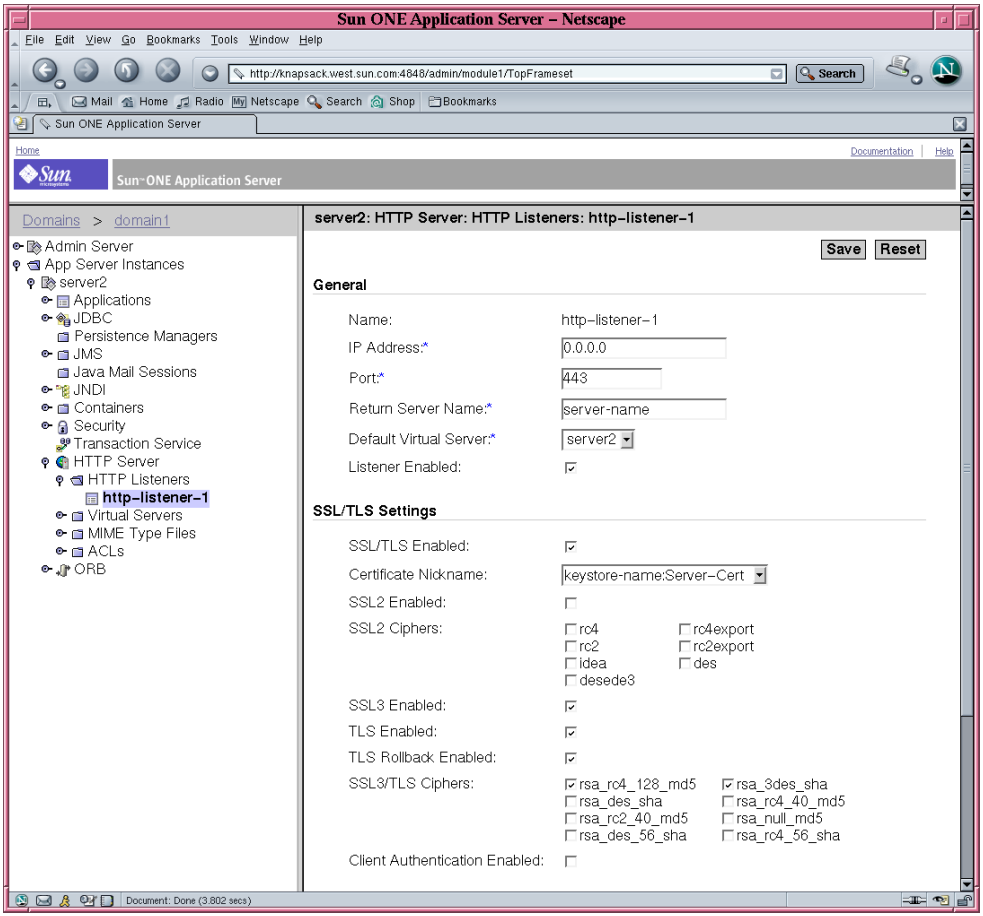

圖 5-8 Sun ONE Application Server 管理伺服器的 HTTP Listener Properties (HTTP 監聽器內容) 對話方塊

5. **對於 SSL/TLS 設定，請檢查 Certificate Nickname (憑證名稱) 與您使用指令的 `--certname` 選項 (第 129 頁的「啟用 SSL 的應用程式伺服器」中的步驟 1) 選擇的憑證名稱是否相符。**

6. **檢查至少下列方塊：**
   - SSL/TLS Enabled (SSL/TLS 啓用)
   - SSL3 Enabled (SSL3 啓用)
   - TLS Enabled (TLS 啓用)
   - TLS Rollback Enabled (TLS 反轉啓用)
   - SSL3/TLS 編碼器：`rsa_rc4_128_md5` 和 `rsa_3des_sha`
7. **設定連接埠 — 通常為 443。**
8. **對於反轉，TLS 必須在瀏覽器中啟用以存取您的伺服器。**
   - 對於 Netscape Navigator 6.0，請檢查 TLS 和 SSL3。
   - 對付 Microsoft Internet Explorer 5.0 和 5.5，請使用 TLS Rollback (TLS 反轉選項)。
   - 對於 TLS Rollback，請檢查 TLS 並確保 SSL3 與 SSL2 停用。
9. **按一下 Save (儲存)。**
10. **在左窗格中選擇「App Server Instances (應用程式伺服器例項)」，在右窗格中選擇「Apply Changes (套用變更)」。**
11. **停止並啟動伺服器以使變更生效。**

    `init.conf` 檔案將自動修改爲顯示安全性，所有虛擬伺服器將自動指派給預設的安全參數。

    在伺服器上啓用 SSL 後，其 URL 將使用 `https` 而不是 `http`。在啓用 SSL 的伺服器上指向文件的 URL 具有下列格式：

    ```
    https://server-name.domain.dom:port-number
    ```

    例如：

    ```
    https://admin.sun.com:443
    ```

注意 – 如果您使用預設的安全 HTTP 連接埠編號 (443)，則無法在 URL 中輸入連接埠編號。

請參閱 *Sun ONE Application Server 7 Administrator's Guide to Security* 的 Enabling SSL/TLS (啓用 SSL/TLS) 部分，位於：
`http://docs.sun.com/source/816-7158-10/sgencryp.html#14403`

安裝與設定 Sun ONE Directory Server 5.2

本章節說明如何安裝與設定 Sun ONE Directory Server 5.2 以使用介面卡。您必須依序執行這些程序。請參閱 Sun ONE Directory Server 文件，以取得更多有關安裝與使用 Sun ONE Directory Server 的資訊。本章節包含下列程序：

安裝 Sun ONE Directory Server 5.2

此程序將從指令行安裝目錄伺服器軟體。

▼ 安裝 Sun ONE Directory Server 5.2

1. **下載 Sun ONE Directory Server 5.2 軟體。**
   您可以在下列 URL 中找到目錄伺服器軟體：`http://www.sun.com/`
2. **變更至安裝目錄。**
3. **執行 `./idsktune` 指令以確定已安裝建議使用的修正程式。**
4. **擷取目錄伺服器軟體。**
5. **執行 `setup` 指令碼以安裝軟體。**

注意 – 您無需個別安裝套件，因爲 `setup` 指令碼將安裝所有套件。

安裝完成後，Sun ONE Directory Server 與管理伺服器將自動啓動。

手動啓動目錄伺服器

1. **變更至啟動目錄。**

```
# cd /var/Sun/mps
```

2. **執行** `start-admin` **指令。**

```
# ./start-admin
```

3. **變更至** `slapd-`*servername* **目錄。**

```
# cd slapd-servername
```

其中的 *servername* 是例項名稱。

4. **鍵入** `start-slapd` **指令。**

```
# ./start-slapd
```

設定 Sun ONE Directory Server 5.2

這些程序將爲目錄伺服器例項建立信任資料庫、使用目錄伺服器註冊介面卡、產生並安裝伺服器憑證、檢視並安裝 root CA 憑證、啓用 SSL 目錄伺服器。

組態目錄與 Sun ONE Directory Server 管理伺服器必須在組態時啓動並執行。

▼ 建立信任資料庫

此程序將新增 Sun Crypto Accelerator 4000 模組，適用於 32 位元與 64 位元安裝。

1. **啟動目錄伺服器中主控台。**
2. **選擇您要設定的目錄伺服器例項，然後在主控台主視窗中選擇 Open (開啟)。**

3. **在出現的新視窗中，選擇 Console (主控台)→Security (安全性)→Manage Certificates (管理憑證)。**

   此步驟將爲目錄伺服器例項建立信任資料庫。

   a. **選擇密碼並輸入兩個方塊，然後按一下 OK (確定) (請參閱**圖 5-9**)。**

   b. **關閉隨後出現的 「Manage Certificates (管理憑證)」。**

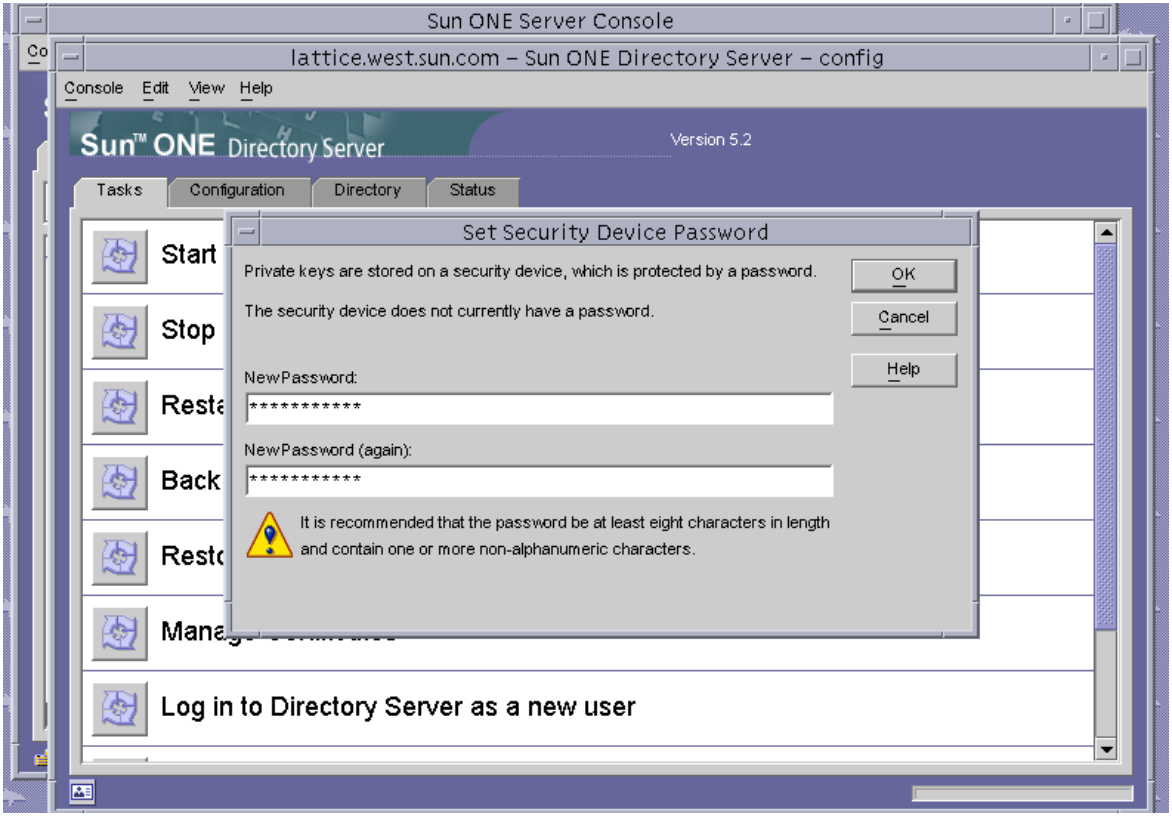

圖 5-9 Sun ONE Directory Server 的 Set Security Device Password (設定安全裝置密碼) 對話方塊

4. **在出現的新視窗中，選擇 Console (主控台)→Security (安全性)→Configure Security Modules (設定安全性模組)。**

   a. **按一下 Install (安裝)。**

   b. **在 *Enter the PKCS#11 module driver filename* 項目中輸入下列路徑：**

```
/opt/SUNWconn/cryptov2/lib/libvpkcs11.so
```

5. **在 *Enter an identifying name for this module* 項目中輸入名稱，例如：**

```
Sun Crypto Accelerator 4000
```

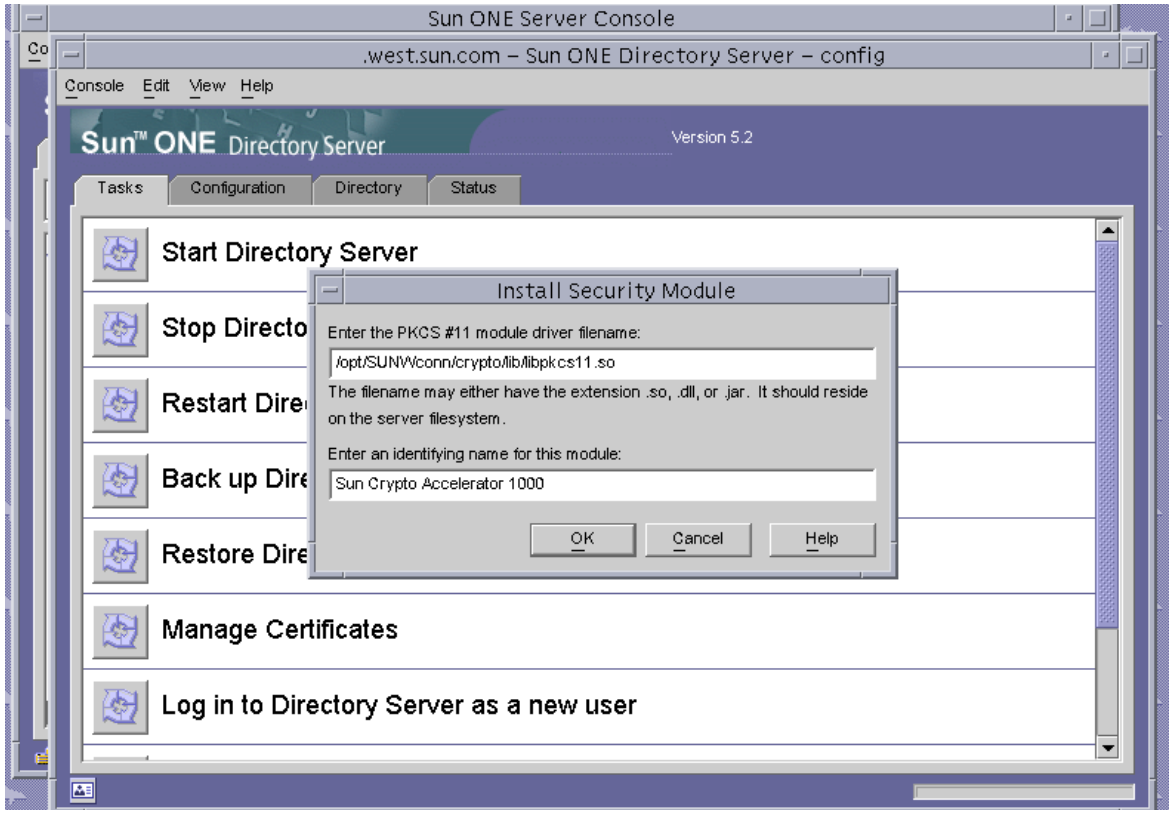

圖 5-10 Sun ONE Directory Server 的 Install Security Module (安裝安全模組) 對話方塊

6. **按一下 OK (確定)。**

▼ 使用目錄伺服器 (32 位元) 註冊介面卡

此程序將從指令行新增 32 位元介面卡模組。

1. **鍵入下列指令以設定適當的路徑。**

```
# setenv LD_LIBRARY_PATH server-inst/lib:${LD_LIBRARY_PATH}
```

2. **將介面卡新增至** secmod.db **資料庫。**

   a. **變更至下列目錄：**

```
# cd server-inst/alias
```

   b. **使用** modutil **公用程式新增程序庫。**

```
# server-inst/shared/bin/modutil -dbdir . -nocertdb -add "Sun Crypto Acclerator
4000" -libfile /opt/SUNWconn/cryptov2/lib/libvpkcs11.so
```

▼ 使用目錄伺服器 (64 位元) 註冊介面卡

此程序將從指令行新增 64 位元介面卡模組。

1. **從** http://www.mozilla.org **獲取 64 位元版 Netscape Security Services (NSS) 公用程式。**

```
ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_3_2_RTM/SunO
S5.8_64_OPT.OBJ/
```

   儲存 nss-3.3.2.tar.gz tar 檔案。

2. **鍵入下列指令以設定適當的路徑。**

注意 – 在本章節中，*server-inst* 指產品的 root 安裝目錄，*nss64-inst* 指您安裝 64 位元版 NSS 工具的位置。

```
# setenv LD_LIBRARY_PATH server-inst/lib/64:${LD_LIBRARY_PATH}
```

3. **將介面卡新增至** secmod.db **資料庫。**

   a. **變更至** alias **目錄：**

```
# cd server-inst/alias
```

   b. **新增程式庫。**

```
# nss64-inst/bin/modutil -dbdir . -nocertdb -add "Sun Crypto Acclerator 4000"
-libfile /opt/SUNWconn/cryptov2/lib/64/libvpkcs11.so
```

產生並安裝伺服器憑證

除表 5-8 中說明的不同路徑變數外，此程序適合安裝的 32 位元與 64 位元版 PKCS#11 程式庫。

表 5-8 32 位元與 64 位元路徑變數差別

變數定義	32 位元	64 位元
LD_LIBRARY_PATH	*server-inst*/lib	*server-inst*/lib/64
NSS 工具的位置	*server-inst*/shared/bin	*nss64-inst* (無論您是否安裝了 NSS 工具)

表 5-9 說明在本章節中用於 certutil 指令的變數。

表 5-9 certutil 變數說明

變數	說明
token-name	PKCS#11 標記的名稱；這是您在初始化介面卡時選擇的金鑰庫名稱。
subject-name	註明在數位憑證上的名稱，通常格式爲： CN=*Fully-Qualified-Domain-Name*,OU=*Organization-Unit*,O=*Organization.* 名稱可能與組織不同。
output-file	憑證要求的位置。
certfile	ASCII 編碼的憑證位置。
instname	目錄伺服器例項名稱。
nickname	使用者選擇的伺服器憑證友好名稱。

▼ 產生伺服器憑證

1. **變更至下列目錄。**

```
# cd server-inst/alias
```

2. **要求憑證。**

```
# certutil -R -d . -h token-name -s "subject-name" -a -o output-file [-g key-size] -P
slapd-instname-
```

3. **將 *output-file* 中的憑證要求提交給您選擇的 Certificate Authority (憑證授權)。**

   將 base64-encoded 憑證放入名稱爲 *certfile* 的文字檔案中。

▼ 安裝伺服器憑證

1. **安裝伺服器憑證。**

```
# certutil -A -d . -h token-name -t "Pu,Pu,Pu" -P slapd-instname- -a -i certfile -n
nickname
```

檢視並安裝 Root CA 憑證

Sun ONE Directory Server 包括幾個公開的目前信任的 Root Certificate Authority (Root 憑證授權) 憑證。如果伺服器憑證由其中一個已知的 Root CA 發出，請略過此程序。

▼ 檢視目錄伺服器已知的 Root CA 憑證

1. **在目錄伺服器主控台視窗中，開啟用於介面卡的目錄伺服器例項。**
2. **在主控台視窗頂部的功能表中，選擇 Console (主控台)→Security (安全性)→Manage Certificates (管理憑證)**
3. **在 「Manage Certificates (管理憑證)」視窗的頂部選擇 CA Certs (CA 憑證) 標籤。**

   將會顯示 Sun ONE Directory Server 例項已知的 CA 憑證。您可以透過反白顯示項目並按一下 Detail (詳細資料) 按鈕，以檢視更多有關指定 CA 憑證的詳細資訊。

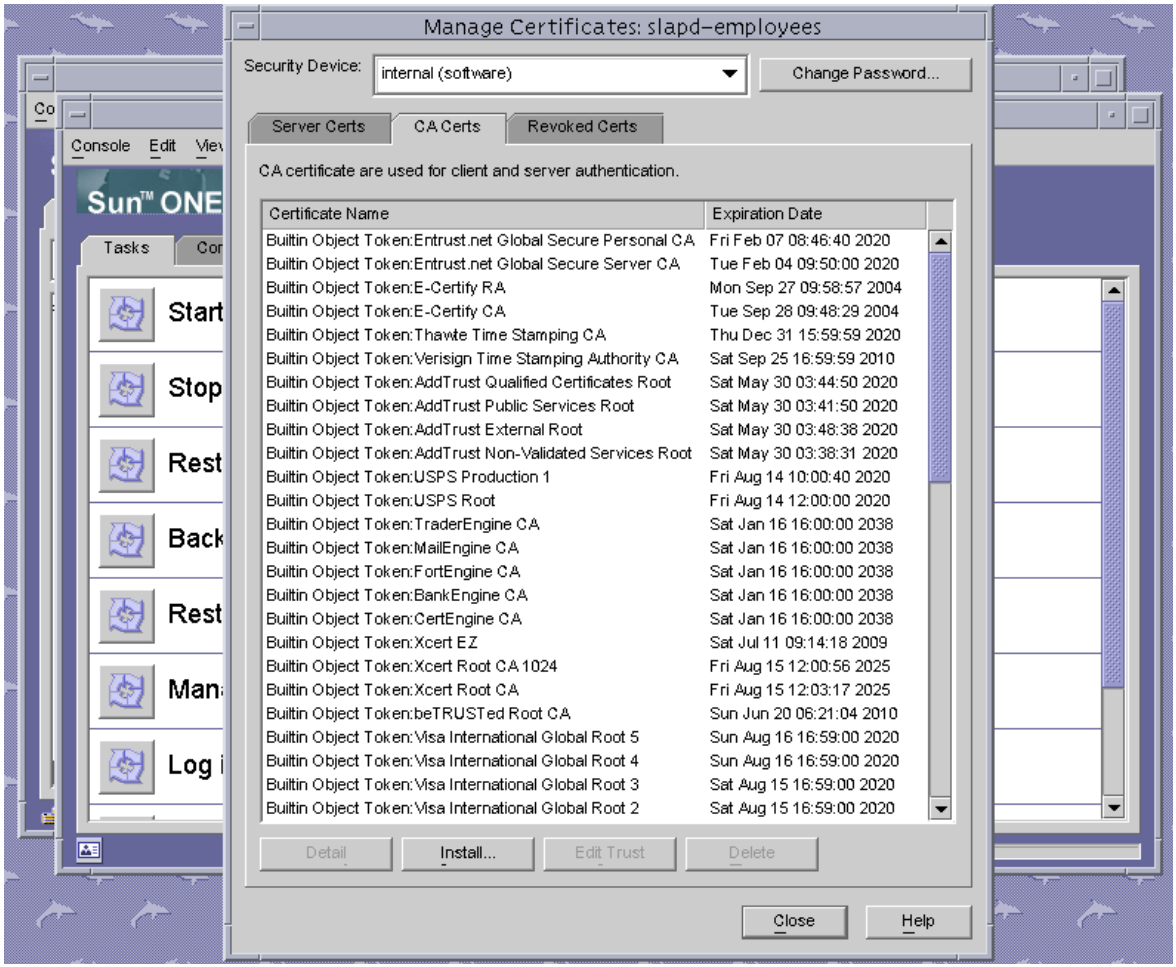

圖 5-11 Sun ONE Directory Server 的 Managing Certificates (管理憑證) 對話方塊

▼ 安裝 Root CA 憑證

僅在您從專屬 PKI 擷取憑證時，才可執行下列程序。也就是說，如果您使用 VeriSign、Thawte 或 GTE，請勿執行此程序。此程序適用於由具有中間 CA (尚未安裝在 Sun ONE 預設信任 CA 清單中) 的主要廠商發出憑證的情況。

1. **變更至** `alias` **目錄。**

```
# cd server-inst/alias
```

2. **安裝 root CA 憑證。**

注意 – 如果您安裝多個 CA 憑證，請使用不同的 `-n` 值。如果您使用相同的 `-n` 值，憑證將相互取代。使用 CA 憑證主旨名稱的 CommonName 元件取代 `CA-Cert` (在 SubjectName 中尋找 CN=)。

```
# certutil -A -d . -P slapd-instname- -n "CA-Cert" -t "CT,CT,CT" -a -i path-to-ca-cert
```

▼ 啓用 SSL 的目錄伺服器

1. **啟動目錄伺服器主控台 (如果未啟動的話)。**

```
# ./cd server-root
# ./startconsole
```

2. **在主控台主視窗左窗格中連按兩下介面卡的目錄伺服器例項，以開啟目錄伺服器例項。**
3. **在主控台主視窗中按一下 Directory (目錄) 標籤。**
4. **開啟 Directory (目錄) 標籤左窗格中的 `cn=config` 項目，然後修改下列參數 (請參閱**圖 5-12**)：**

   a. **將 `nsslapd-security` 設定為開啟。**

   b. **將 `nsslapd-secureport` 設定為所需的連接埠 (預設值為 636)。**

c. **按一下 OK (確定)。**

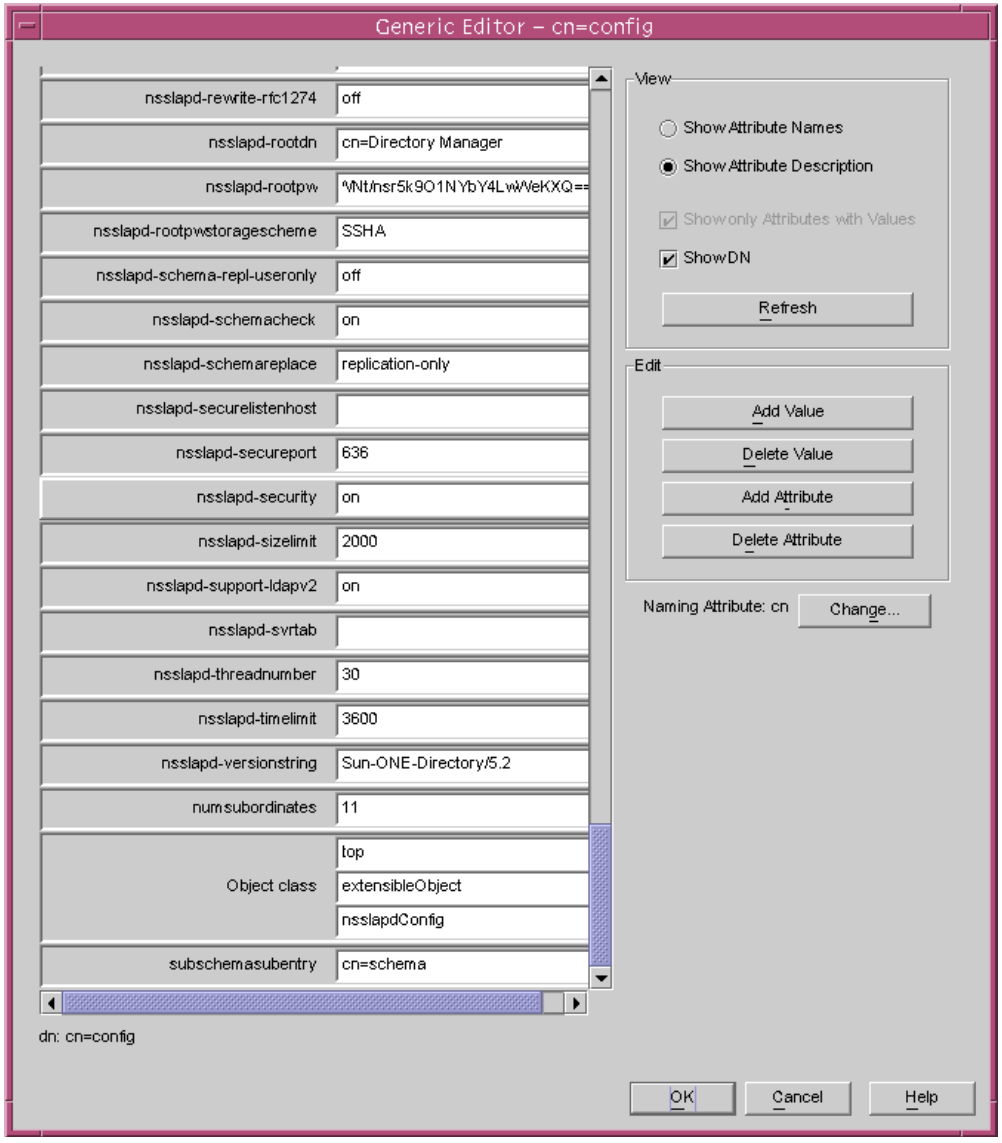

圖 5-12 Sun ONE Directory Server `cn=config` 的 Editor (編輯器) 對話方塊

5. **開啟主控台主視窗左窗格中的 `cn=encryption,cn=config` 項目，然後修改下列參數 (請參閱**圖 5-13**)：**

   a. **將 `nsssl3` 設定為開啟。**

b. **使用「Add Attribute (新增屬性)」按鈕以新增具有值** `alias/slapd-instname-cert8.db` **的** `nsCertFile`

c. **使用「Add Attribute (新增屬性)」按鈕以新增具有值** `alias/slapd-`*instname*`-key3.db` **的** `nsKeyFile`

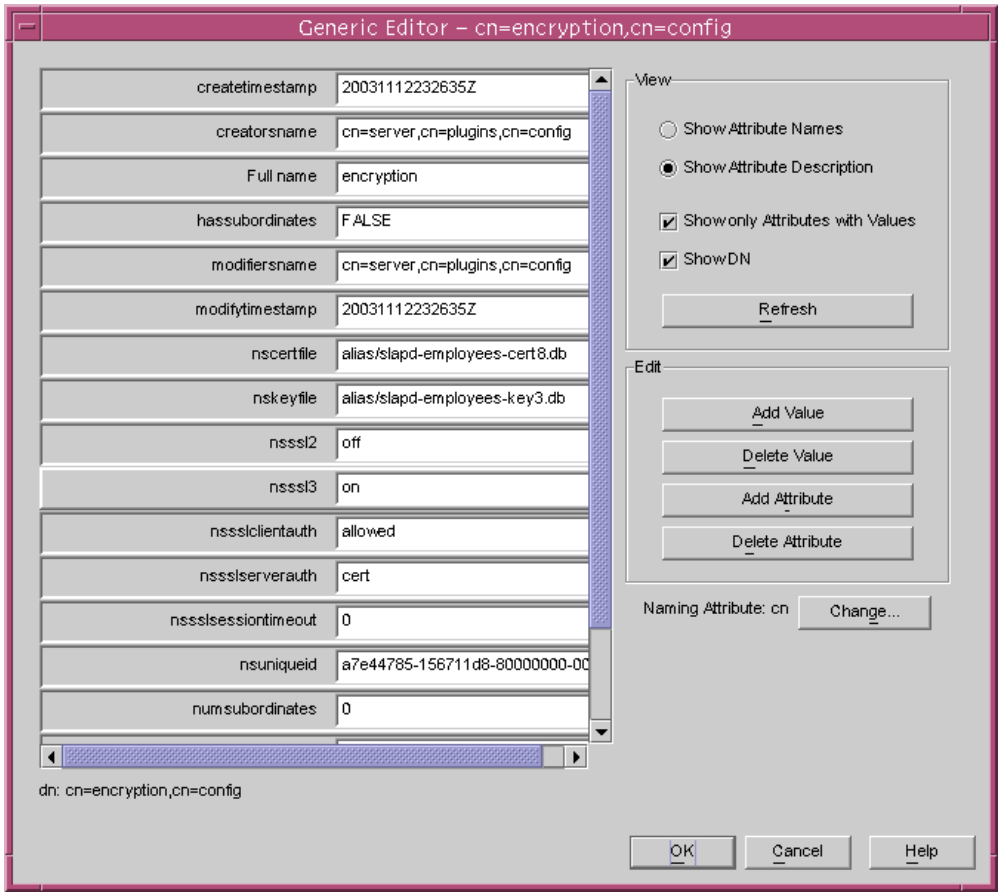

圖 5-13 Sun ONE Directory Server `cn=encryption,cn=config` 對話方塊

d. **按一下 OK (確定)。**

6. **在資料庫中的** `cn=encryption,cn=config` **下建立新項目**

a. **在主視窗中的加密圖示上按一下滑鼠右鍵，然後在功能表中選擇 New (新增)→Other (其他)。**

b. **選擇** `nsEncryptionModule`**。**

c. 將「Full Name (全名)」屬性的值從「New (新增)」變更為「RSA」(遠端安全存取) (請參閱圖 5-14**)。**

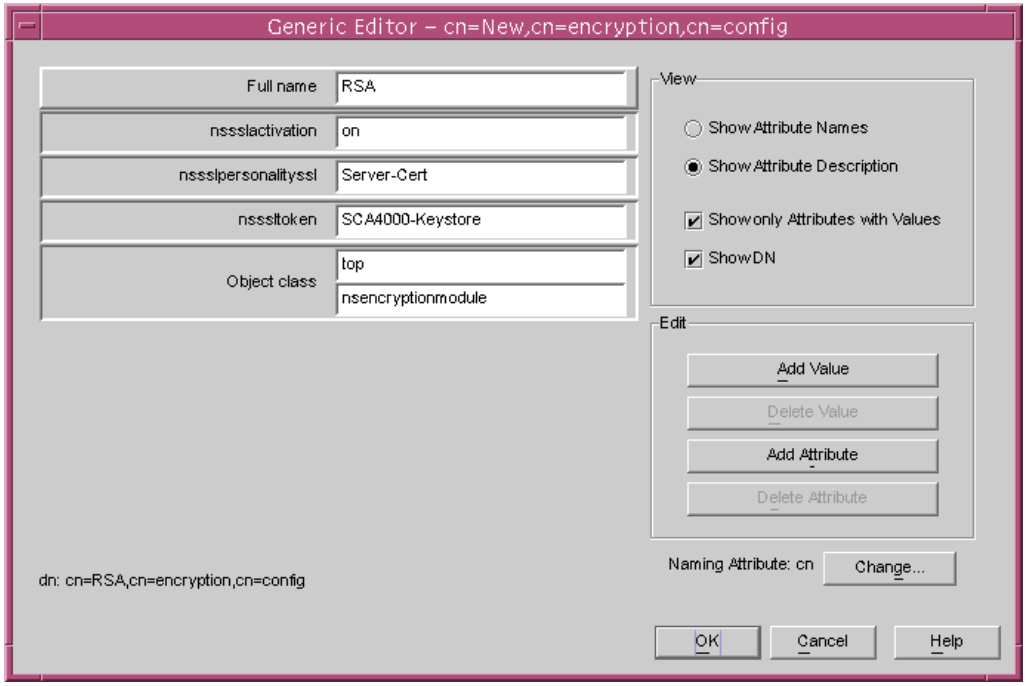

圖 5-14 Sun ONE Directory Server 的 `nsEncryption` Module (模組) 對話方塊

d. 使用「Add Attribute (新增屬性)」按鈕以新增下列屬性與值：

`nsssltoken`	*token-name*
`nsslpersonalityssl`	*nickname*
`nssslactivation`	`on`

e. 按一下 OK (確定)。

安裝與設定 Sun ONE Messaging Server 5.2

本章節說明如何安裝與設定 Sun ONE Messaging Server 5.2 以使用介面卡。您必須依序執行這些程序。請參閱 Sun ONE Messaging Server 文件，以取得更多有關安裝與使用 Sun ONE Messaging Server 的資訊。本章節說明下列主題：

安裝 Sun ONE Messaging Server 5.2

此程序將從指令行安裝 Sun ONE Messaging Server 5.2。

▼ 安裝 Sun ONE Messaging Server 5.2

1. **下載 Sun ONE Messaging Server 5.2 軟體。**
   您可以在下列 URL 中找到訊息伺服器軟體：`http://www.sun.com/`
2. **變更至安裝目錄並擷取訊息伺服器軟體。**
3. **使用** `setup` **指令碼安裝訊息伺服器。**
   a. **在系統提示時鍵入安裝路徑。**
   b. **在系統提示時鍵入您要安裝的元件。**
   c. **執行** `./setup` **指令以安裝元件。**

設定 Sun ONE Messaging Server 5.2

這些程序將爲訊息伺服器例項建立信任資料庫、使用訊息伺服器註冊介面卡、產生並安裝伺服器憑證、啓用 SSL 的訊息伺服器。

組態目錄與 Sun ONE Messaging Server 管理伺服器必須在組態時啓動並執行。

▼ 建立信任資料庫

1. **啟動訊息伺服器主控台。**
2. **開啟 Sun ONE Messaging server 例項。**
   將會出現圖 5-15 中的功能表：

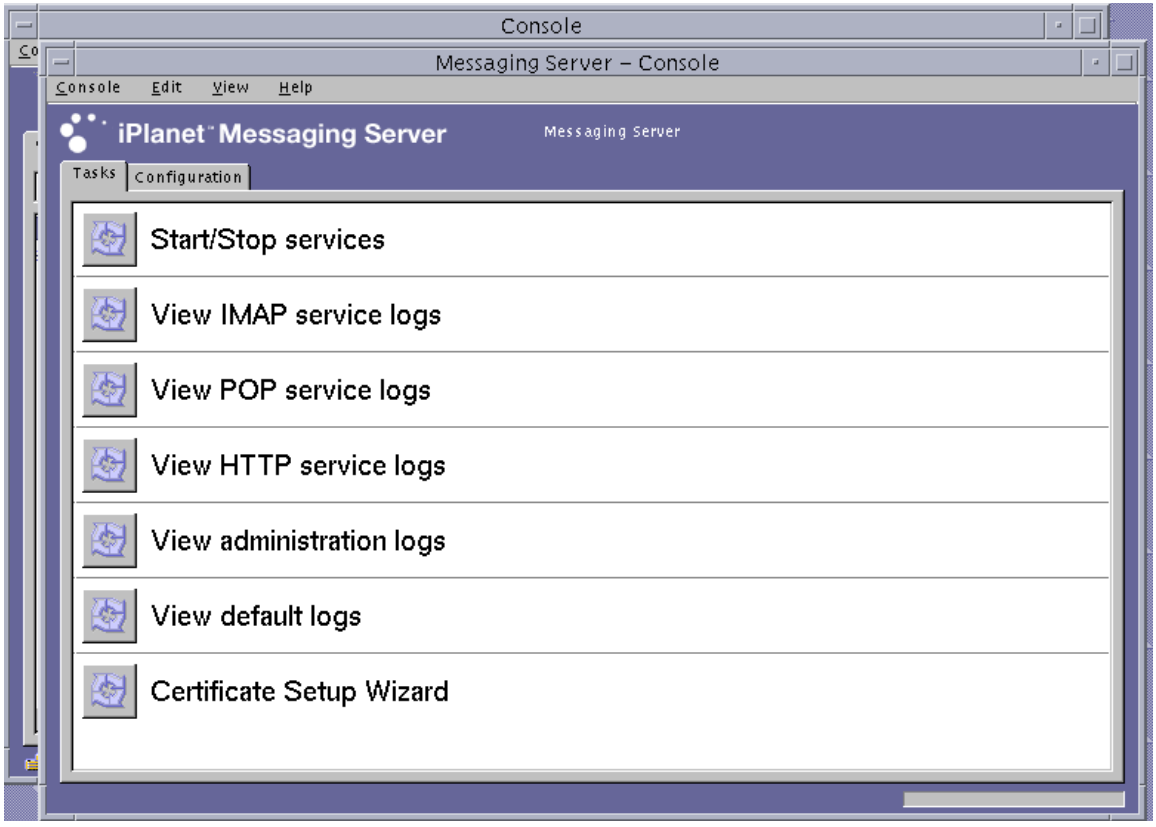

圖 5-15 Sun ONE Messaging Server 主控台主視窗

3. **選擇 Console (主控台)→Certificate Setup Wizard (憑證設定精靈)**
   Certificate Setup Wizard (憑證設定精靈) 將會出現。
   a. **按一下 Next (下一步)。**
   b. **選擇「internal (software) (內部 [軟體])」標記。**
   c. **選擇「Do not install a certificate (請勿安裝憑證)」，然後按一下 Next (下一步)。**
   d. **按一下 Next (下一步)。**

e. 為內部資料庫設定密碼，然後按一下 Next (下一步)。

f. 按一下 Done (完成)。

▼ 使用訊息伺服器註冊介面卡

1. 變更至下列目錄。

```
# cd server-root/shared/bin
```

2. 確定 LD_LIBRARY_PATH **變數正確設定。**

```
# setenv LD_LIBRARY_PATH server-root/lib:${LD_LIBRARY_PATH}
```

3. 將介面卡模組新增至 secmod.db **資料庫。**

```
# ./modutil -dbdir ../../admin-serv/config \
-nocertdb \
-add "Sun Crypto Accelerator 4000" \
-libfile "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
```

▼ 產生伺服器憑證

1. 透過選擇 Console (主控台) -> Certificate Setup Wizard (憑證設定精靈) 開啟 Certificate Setup Wizard (憑證設定精靈)，使用訊息伺服器主控台以要求憑證。

a. 按一下 Next (下一步)

b. 選擇與您要儲存金鑰的 Sun Crypto Accelerator 4000 標記相符的標記，如圖 5-16 **中所示。**

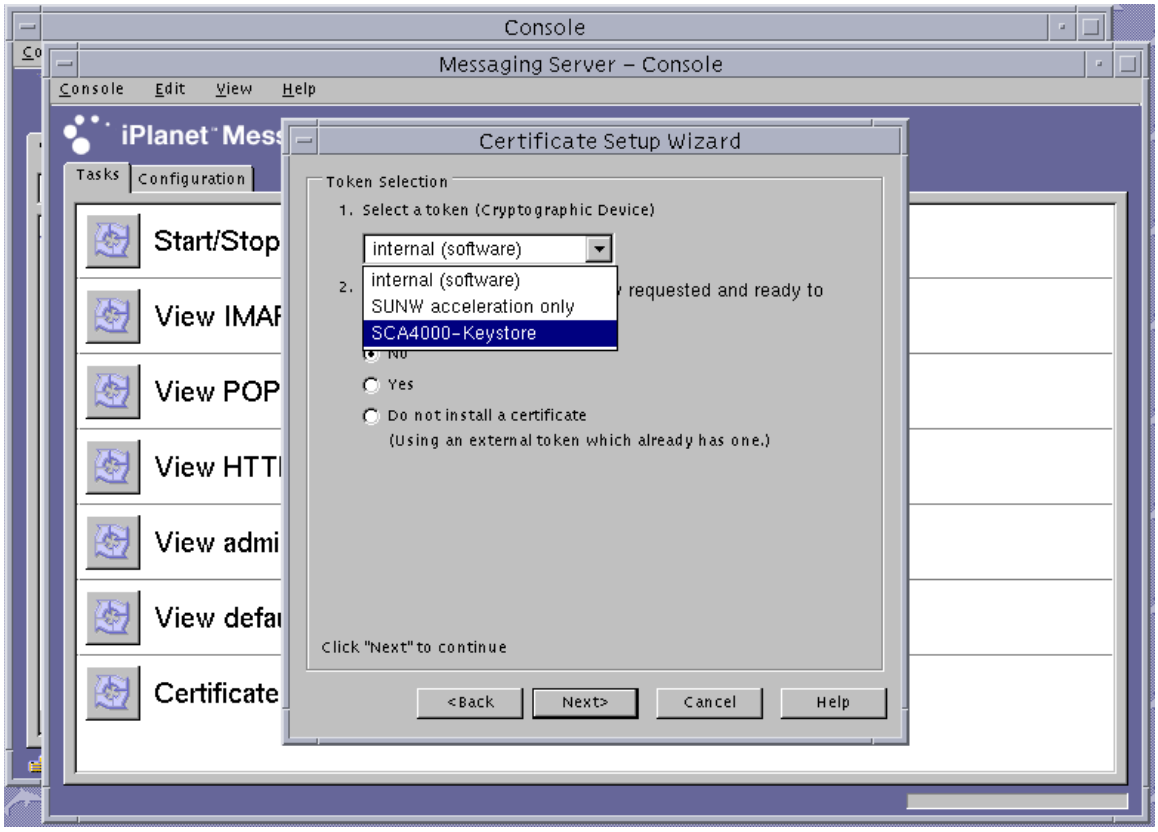

圖 5-16 Sun ONE Messaging Server 的 Certificate Setup Wizard Token Selection (憑證設定精靈標記選項) 對話方塊

c. 對「Is the certificate already requested and ready to install? (是否已經要求憑證並準備安裝？)」回答 NO (否)，然後按一下 Next (下一步)。

d. 按一下 Next (下一步)。

e. 選擇「New Certificate (新增憑證)」，然後選擇向憑證授權 (圖 5-17) 提交憑證要求的方法 (透過電子郵件或 HTTPS)，然後按一下 Next (下一步)。

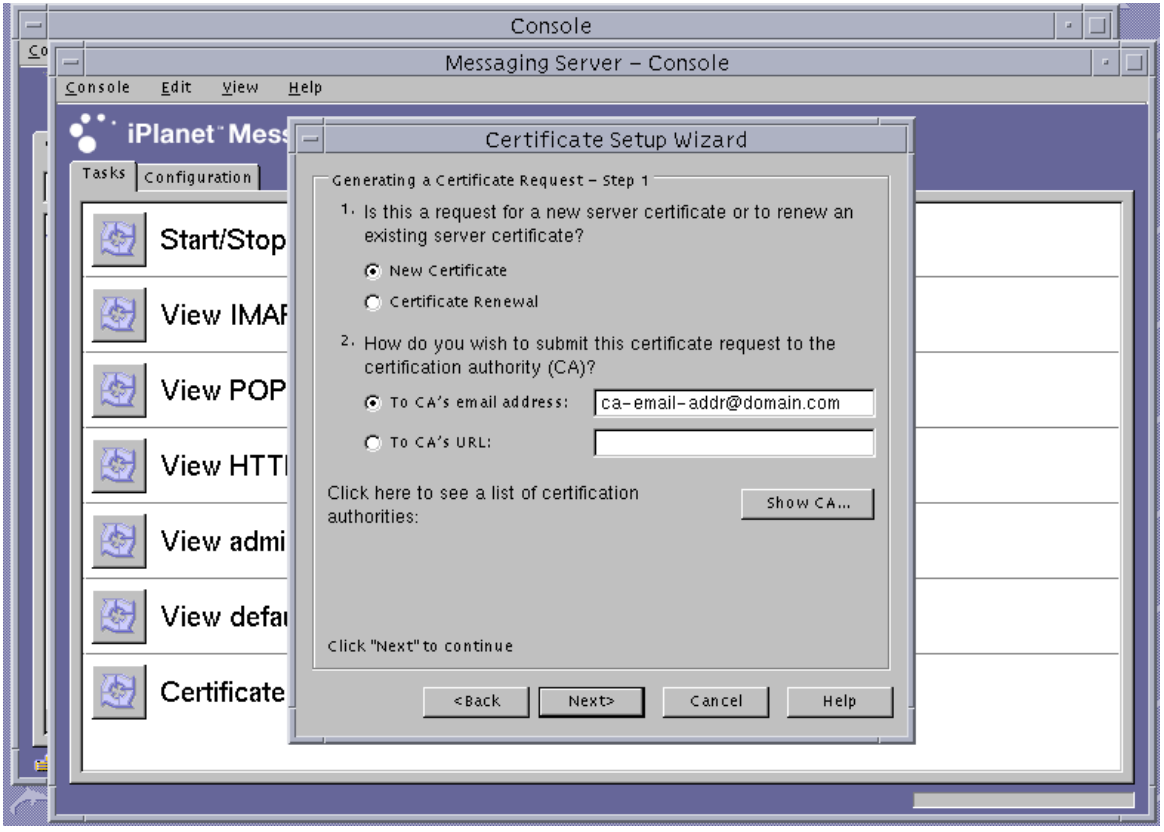

圖 5-17 Sun ONE Messaging Server 的 Certificate Setup Wizard Certificate Request (憑證設定精靈憑證要求) 對話方塊

f. 在表 5-10 的要求者資訊欄位中鍵入適當資訊，然後按一下 Next (下一步)。

表 5-10 要求者資訊欄位

欄位	說明
Requestor Name (要求者名稱)	要求者的聯絡資訊
Telephone Number (電話號碼)	要求者的聯絡資訊
Common Name (一般名稱)	造訪者瀏覽器中輸入的網站網域

表 5-10 要求者資訊欄位 *(續)*

欄位	說明
Email Address (電子郵件地址)	要求者的聯絡資訊
Organization (組織)	公司名稱
Organizational Unit (組織單位)	(選填) 公司部門
Locality (地區)	(選填) 城市、郡、所在地或國家
State (州)	(選填) 完整州名
Country (國家)	代表國家的兩個字母的 ISO 代碼 (例如：美國的代碼爲 US)

g. 此螢幕要求您輸入在建立信任資料庫時使用的密碼。為金鑰庫使用者 (*使用者名稱:密碼*) 輸入密碼，然後按一下 Next (下一步)。

請參閱表 5-1 以取得有關*使用者名稱:密碼*的詳細資料。

h. 如果您在步驟 e 中選定 HTTPS 方法，則要求應已傳送至 CA。如果您在步驟 e 中選定電子郵件方法，則請按一下「Copy to Clipboard (複製到剪貼簿)」，然後按一下 Next (下一步) (圖 5-18)。

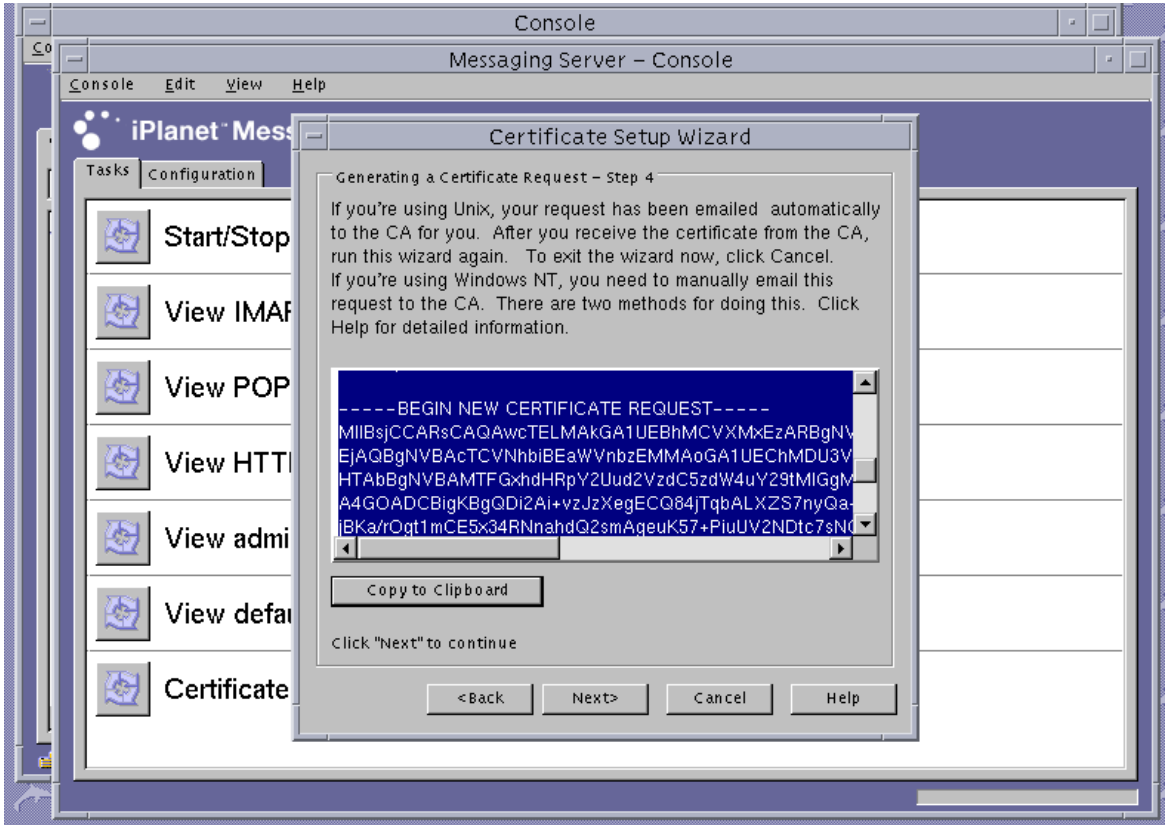

圖 5-18 Sun ONE Messaging Server 的 Certificate Setup Wizard Certificate Delivery (憑證設定精靈憑證傳送) 對話方塊

i. 按一下 Next (下一步)。

注意 – 要求憑證後，Certificate Setup Wizard (憑證設定精靈) 將繼續進行，並可讓您將發出的憑證安裝在 Sun Crypto Accelerator 4000 金鑰庫中。如果您在產生憑證後未進行安裝即退出 Certificate Setup Wizard (憑證設定精靈)，您可以重新啓動 Certificate Setup Wizard (憑證設定精靈)，然後重新回到未完成的步驟。

▼ 安裝伺服器憑證

1. **如果您在產生伺服器憑證程序中退出 Certificate Setup Wizard (憑證設定精靈)，請透過選擇 Console (主控台) -> Certificate Setup Wizard (憑證設定精靈) 重新啟動 Wizard (精靈)，然後按一下第一個螢幕中的 Next (下一步)。**
2. **選擇您要在其中安裝憑證的 Sun Crypto Accelerator 4000 標記。**

   此標記必須與您產生要求的標記相同。
3. **對於是否準備安裝伺服器憑證的詢問回答 Yes (是)，然後按一下 Next (下一步)。**
4. **按一下 Next (下一步)。**
5. **安裝 「This Server (本伺服器)」並輸入金鑰庫密碼 (*使用者名稱:密碼*) (如果 Wizard [精靈] 尚未提供的話)，然後按一下 Next (下一步) (請參閱**圖 5-19**)。**

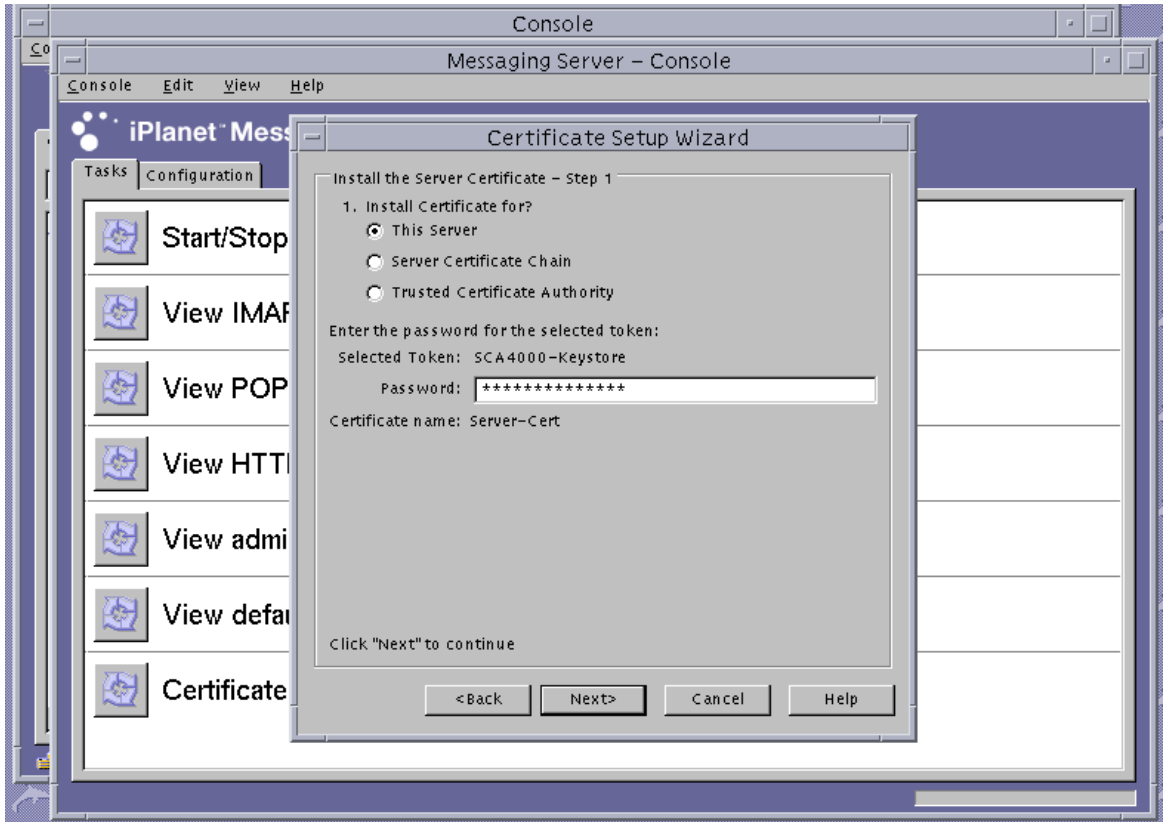

圖 5-19 Sun ONE Messaging Server 的 Certificate Setup Wizard Password (憑證設定精靈密碼) 對話方塊

注意 – 預設憑證名稱爲 `Server-Cert`。

6. **將基本 64 編碼的憑證複製到剪貼簿並貼到標記為「The certificate is located in the following text field (憑證位於下列文字欄位中)」文字方塊，然後按一下 Next (下一步) (請參閱**圖 5-20**)。**

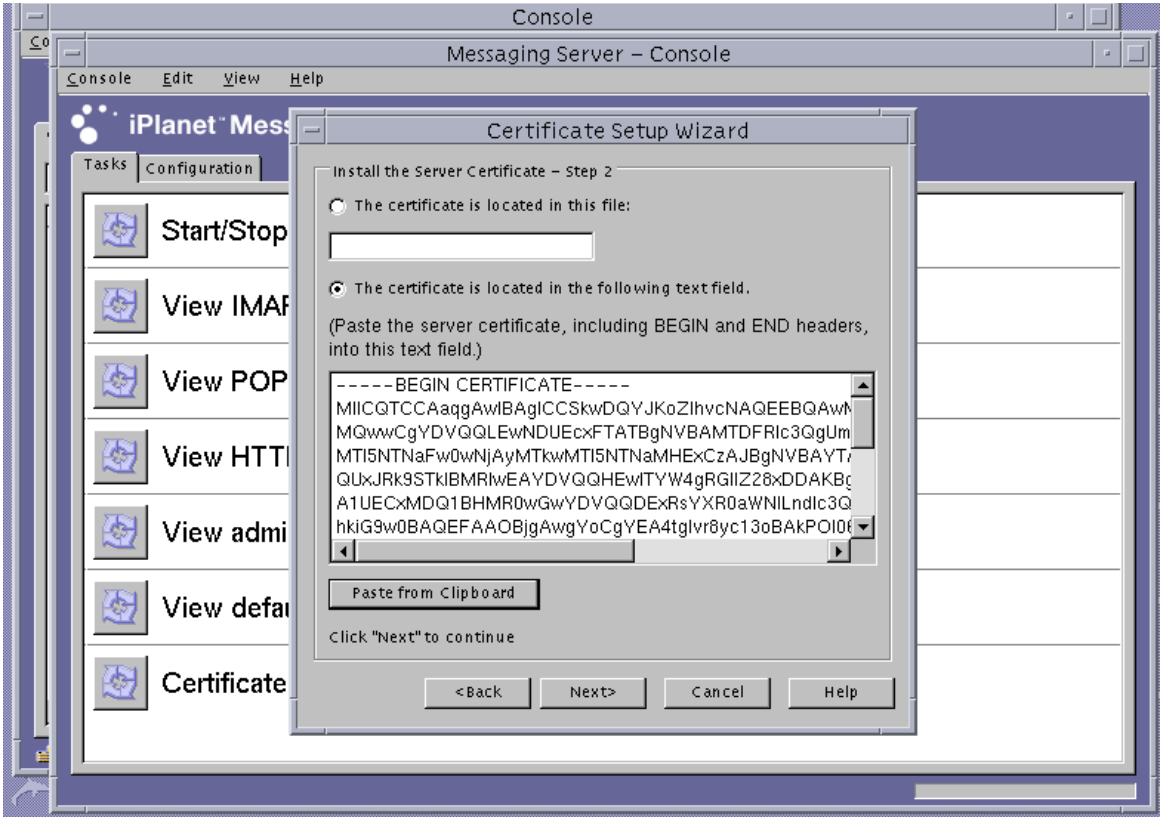

圖 5-20 Sun ONE Messaging Server 的 Certificate Setup Wizard Certificate Entry (憑證設定精靈憑證項目) 對話方塊

   a. **按一下 Add (新增) 以新增憑證。**

   b. **按一下 Done (完成)。**

7. **新增 root CA 憑證 (如果非 root 憑證授權已受訊息伺服器信任)。**

   在此步驟中使用 Certificate Setup Wizard (憑證設定精靈)。

   a. **在訊息伺服器主控台中，選擇 Console (主控台)→Certificate Setup Wizard (憑證設定精靈)。**

   b. **按一下 Next (下一步)。**

c. **選擇「internal (software) (內部 [軟體])」作為標記，然後對於「Is the certificate already requested and ready to install? (是否已經要求憑證並准備安裝？)」回答 Yes (是)，然後按一下 Next (下一步)。**

d. **按一下 Next (下一步)。**

e. **選擇「Trusted Certificate Authority (信任憑證授權)」，然後按一下 Next (下一步)。**

f. **將基本 64 編碼的 CA 憑證複製到剪貼簿並貼到標記為「The certificate is located in the following text field (憑證位於下列文字欄位中)」文字方塊，然後按一下 Next (下一步)。**

g. **按一下 Add (新增) 以新增憑證 (**圖 5-21**)。**

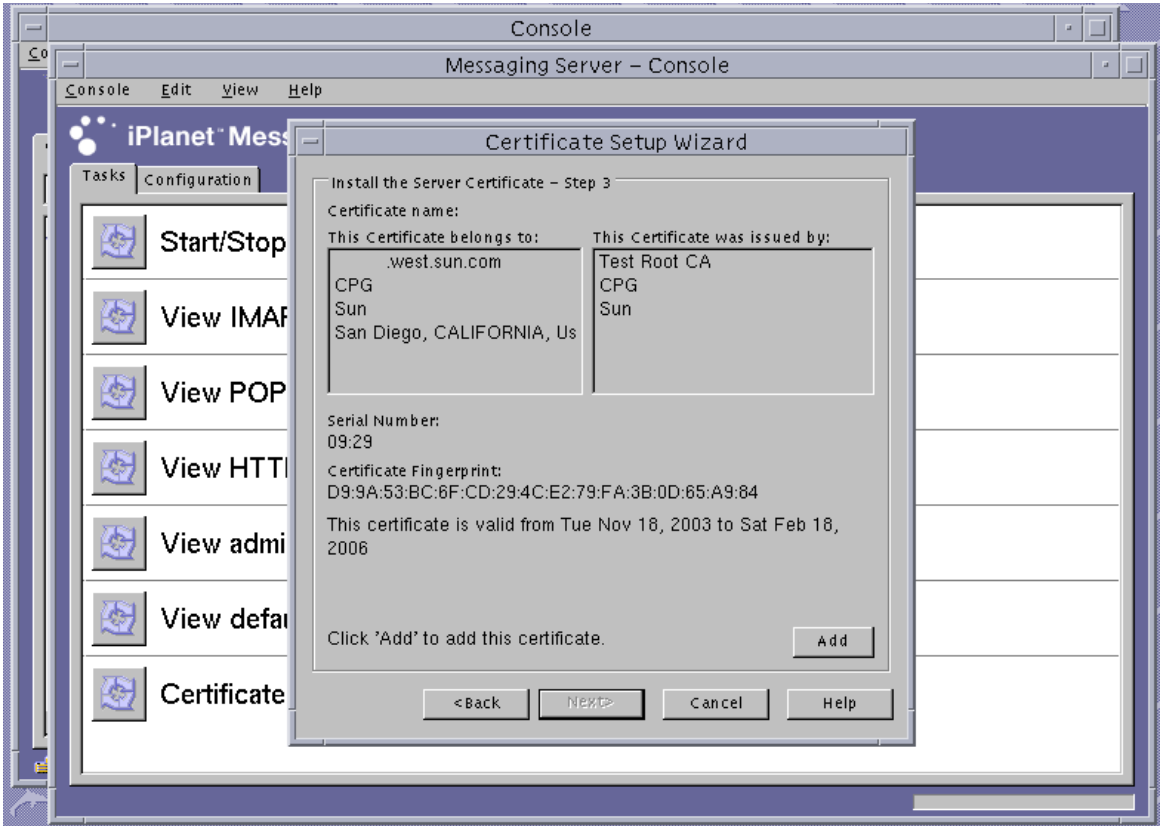

圖 5-21 Sun ONE Messaging Server 的 Certificate Setup Wizard Password (憑證設定精靈密碼) 對話方塊

h. **按一下 Done (完成)。**

▼ 啓用 SSL 訊息伺服器

1. 使用 `su` 指令以您選擇用於執行訊息伺服器的使用者身份登入。

如果您忘記此使用者名稱，是可搜尋 *server-root*`/msg-`*instname*`/config/msg.conf` 檔案的 `local.serveruid` 內容並擷取使用者名稱。

```
# cd server-root/msg-instname
# su username
```

2. 使用 `configutil` 工具以設定訊息伺服器的 SSL 參數。

表 5-11 說明使用`configutil` 工具的變數定義。

表 5-11 `configutil` 變數說明

變數	定義
keystorename	步驟 1 中使用的金鑰庫名稱。
certname	要使用的憑證友好名稱。預設值爲 `Server-Cert`。
portnumber	在 SSL 上執行 POP3 的連接埠編號，通常爲 995。

```
# ./configutil -o nsserversecurity -v on
# ./configutil -o encryption.rsa.nssslactivation -v on
# ./configutil -o encryption.rsa.nsssltoken -v keystorename
# ./configutil -o encryption.rsa.nssslpersonalityssl -v certname
# ./configutil -l -o service.pop.enablesslport -v yes
# ./configutil -l -o service.pop.sslport -v portnumber
```

3. 在訊息伺服器主控台中，按一下用於管理 Sun ONE Messaging Server 例項的主控台視窗之 Configuration (組態) 標籤。按一下 Messaging Server (訊息伺服器) -> Services (服務) -> IMAP 中的 System (系統) 標籤。

4. 在上一個視窗中，設定「Use separate port for IMAP over SSL (透過 SSL 使用用於 IMAP 的單個連接埠)」的連接埠編號。此連接埠的預設編號為 993。

5. **為訊息伺服器例項設定** `sslpassword.conf` **檔案。**

```
# cd server-root/msg-instname/config
# vi sslpassword.conf
```

使用 *tokenname:username:password* 行取代 `Internal (Software) token:netscape!` 其中 *tokenname* 爲金鑰庫名稱。此 tokenname 是您在步驟 1 中選擇用以產生金鑰的標記之名稱。*username:password* 用於驗證該標記。請參閱表 5-1 以取得有關 *username:password* 的詳細資料。

6. **變更** `sslpassword.conf` **檔案的所有權與權限。**

由於 `sslpassword.conf` 檔案包含用於驗證金鑰資料的密碼資訊，所以該檔案必須由執行監控程序的使用者擁有，且該檔案必須只能由該使用者讀取。

```
# cd server-root/msg-instname/config
# chown msg-user sslpassword.conf
# chmod 0400 sslpassword.conf
```

7. **從指令行重新安裝伺服器。**

```
# cd server-root
# msg-instname/start-msg
```

安裝與設定 Sun ONE Portal Server 6.2

本章節說明如何安裝與設定 Sun ONE Portal Server 6.2 以使用介面卡。您必須依序執行這些程序。請參閱 Sun ONE Portal Server 文件，以取得更多有關安裝與使用 Sun ONE Portal Server 的資訊。本章節包含下列程序：

本章節說明如何安裝與設定 Sun ONE Portal Server 6.2 以使用介面卡。您必須依序執行這些程序。請參閱 Sun ONE Portal Server 文件，以取得更多有關安裝與使用 Sun ONE Portal Server 的資訊。

Sun ONE Portal Server 6.2 包含 Sun ONE Web Server 6.0。您必須在安裝與設定入口伺服器之前安裝與設定 Sun ONE Web Server 軟體 (請參閱第 112 頁的「安裝與設定 Sun ONE Web Server 6.0」)。

注意 – 在安裝與設定 Sun ONE Web Server 以使用入口伺服器時，請使用下列安裝路徑：`/opt/SUNWam/servers`。

安裝 Sun ONE Portal Server 6.2

本章節說明如何從指令行安裝 Sun ONE Portal Server 6.1。

▼ 安裝 Sun ONE Portal Server 6.2

1. **下載 Sun ONE Portal Server 6.1 軟體。**
   您可以在下列 URL 中找到入口伺服器軟體：`http://www.sun.com/`
2. **變更至安裝目錄並擷取入口伺服器軟體。**
3. **使用** `setup` **指令碼安裝入口伺服器。**
   a. **在系統提示時輸入安裝路徑。**
   b. **在系統提示時輸入您要安裝的元件。**
   c. **執行** `./setup` **指令以安裝元件。**

注意 – 信任資料庫將在安裝期間自動建立。

設定 Sun ONE Portal Server 6.2

這些程序可設定入口伺服器安全性遠端存取 (SRA) 閘道、使用入口伺服器註冊介面卡、產生並安裝伺服器憑證、啓用 SSL 的入口伺服器。

開始之前，請確定已安裝 SRA 與閘道伺服器憑證 (自行簽署或由任何 CA 發出)。Sun ONE Portal Server 管理伺服器必須在設定時啓動並執行。

▼ 使用入口伺服器註冊介面卡

1. **使用 vcaadm 公用程式為介面卡建立新的使用者帳號 (請參閱第 53 頁的「使用 vcaadm 公用程式」)。**

```
vcaadm{vca0@localhost, sec-officer}> create user
New user name: username
Enter new user password:
Confirm password:
User crypta created successfully.
```

2. **載入 Sun Crypto Accelerator 4000 模組。**

   LD_LIBRARY_PATH 變數必須指向下列位置：

```
/usr/lib/mps/secv2/
```

   a. **載入模組。**

```
# /usr/bin/mps/modutil -dbdir /etc/opt/SUNWps/cert/default -add "Sun Crypto
Accelerator 4000" -libfile /opt/SUNWconn/cryptov2/lib/libvpkcs11.so
```

   b. **檢查是否已載入此模組。**

```
# /usr/bin/mps/modutil -list -dbdir /etc/opt/SUNWps/cert/default -nocertdb
```

產生並安裝伺服器憑證

在這些程序中，LD_LIBRARY_PATH 環境變數必須指向下列位置：

```
/usr/lib/mps/secv1/
```

表 5-12 說明在本章節中用於 certutil 指令的變數。

表 5-12 certutil 變數說明

變數	說明
token-name	PKCS#11 標記的名稱；這是您在初始化介面卡時選擇的金鑰庫名稱。
subject-name	註明在數位憑證上的名稱，通常格式爲： CN=*Fully-Qualified-Domain-Name*,OU=*Organization-Unit*,O=*Organization.* 名稱可能與組織不同。
output-file	憑證要求的位置。
certfile	ASCII 編碼的憑證位置。
instname	入口伺服器例項名稱。
nickname	使用者選擇的伺服器憑證友好名稱。

▼ 產生伺服器憑證

1. **變更至下列目錄。**

```
# cd /etc/opt/SUNWps/cert/default
```

2. **要求憑證。**

```
# /usr/bin/mps/bin/certutil -R -d . -h token-name -s "subject-name" -a -o output-file
[-g key-size]
```

3. **將 *output-file* 中的憑證要求提交給您選擇的 Certificate Authority (憑證授權)。**

   將 base64-encoded 憑證放入名稱爲 *certfile* 的文字檔案中。

▼ 安裝伺服器憑證

1. **安裝伺服器憑證。**

```
# /usr/bin/mps/certutil -A -d . -h token-name -t "Pu,Pu,Pu" -a -i certfile -n nickname
```

檢視並安裝 Root CA 憑證

Sun ONE Portal Server 包括幾個公開的目前信任的 Root Certificate Authority (Root 憑證授權) 憑證。如果伺服器憑證由其中一個已知的 Root CA 發出，請略過此程序。

▼ 檢視入口伺服器已知的 Root CA 憑證

- **鍵入下列指令：**

```
# /usr/bin/mps/certutil -L -d /etc/opt/SUNWps/cert/default
```

▼ 安裝 Root CA 憑證

僅在您從專屬 PKI 擷取憑證時，才可執行下列程序。也就是說，如果您使用 VeriSign、Thawte 或 GTE，請勿執行此程序。此程序適用於由具有中間 CA (尚未安裝在 Sun ONE 預設信任 CA 清單中) 的主要廠商發出憑證的情況。

1. **變更為 certificate database 目錄。**

```
# cd /etc/opt/SUNWps/cert/default
```

2. **安裝 root CA 憑證。**

注意 – 如果您安裝多個 CA 憑證，請使用不同的 `-n` 值。如果您使用相同的 `-n` 值，憑證將相互取代。使用 CA 憑證主旨名稱的 CommonName 元件取代 `CA-Cert` (在 SubjectName 中尋找 CN=)。

```
# /usr/bin/mps/certutil -A -d . -n "CA-Cert" -t "CT,CT,CT" -a -i path-to-ca-cert
```

▼ 啓用 SSL 入口伺服器

1. **建立** `/etc/opt/SUNWps/cert/default/.nickname` **檔案。**

```
# vi /etc/opt/SUNWps/cert/default/.nickname
```

檔案必須僅包含下列行，且不帶空格：

```
keystore-name:server-cert
```

2. **選擇加速編碼器。**

注意 – 必須爲在 Sun Crypto Accelerator 4000 硬體中加速的 DES 與 3DES 演算法提供 `/etc/opt/SUNWconn/cryptov2/sslreg` 檔案。請參閱第 99 頁的「啓用與停用大量加密」。

介面卡將加速 RSA 功能，但僅支援 DES 與 3DES 編碼器加速。執行下列步驟以啓用其中一個編碼器：

```
Gateway（閘道） >> Security（安全性） >> Enable SSL Cipher Selection:
（啟用 SSL 編碼器選項：） >> SSL3 Ciphers: (SSL3 編碼器：) >>
SSL3_RSA_WITH_3DES_EDE_CBC_SHA 或
SSL3_RSA_WITH_DES_CBC_SHA
```

3. **修改** `/etc/opt/SUNWps/platform.conf.`*gateway-profile-name* **以啟用介面卡。**

```
gateway.enable.accelerator=true
```

4. **在終端視窗中，重新啟動閘道。**

```
# InstallDir/SUNWps/bin/gateway -n gateway-profile-name start
```

閘道將提示您輸入金鑰庫密碼。輸入 *sra-keystore*:*username*:*password* 的密碼或個人識別碼。

第 6 章

安裝與設定 Apache 網站伺服器軟體

本章說明如何安裝與設定 Apache 網站伺服器以使用介面卡，包含下列章節：

- 第 162 頁的「設定 Apache Web Server 1.3x」
- 第 167 頁的「建立與設定 Apache Web Server 2.x」
- 第 171 頁的「設定 Apache 網站伺服器以在重新啓動時無需使用者互動進行啓動」
- 第 172 頁的「設定 Sun Crypto Accelerator 1000 以在安裝 Sun Crypto Accelerator 4000 軟體後 使用 Apache」

以上是設定 Apache 網站伺服器以使用介面卡的軟體需求：

- Apache Web Server 1.3.26 或更新版本 — Sun Crypto Accelerator 4000 軟體隨附了 1.3.26 版
- 用於 Solaris 8 的修正程式 109234-09，可從 `http://sunsolve.sun.com` 取得
- 用於 Solaris 9 的修正程式 113146-02，可從 `http://sunsolve.sun.com` 取得
- Sun Crypto Accelerator 4000 軟體隨附的 `SUNWkcl2a` 套件

新增 `SUNWkcl2a` 套件後，系統會使用 Apache 網站伺服器與 mod_ssl 1.3.26 進行設定。

注意 – Apache 網站伺服器不會使用第 5 章第 96 頁的「概念與術語」中所述的金鑰庫或使用者帳號功能。

警告 – 請勿將 Apache 網站伺服器設定爲同時與 Sun Crypto Accelerator 1000 介面卡及 Sun Crypto Accelerator 4000 介面卡配合使用。否則，Apache 將無法正常工作。

注意 – 根據預設值，供 Apache 軟體使用的 大量加密功能已啓用，您無法停用此功能。

設定 Apache Web Server 1.3x

本章節說明如何使用 apsslcfg 指令碼設定網站伺服器以使用介面卡。本章節還說明如何建立與安裝伺服器憑證。

▼ 設定 Apache 網站伺服器

1. **如果尚未建立 httpd 組態檔案，請建立。**

   對於 Solaris 系統，httpd.conf-example 檔案通常位於 /etc/apache 目錄。您可以使用本檔案做爲範本，依照下列方式加以複製：

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

2. **在 httpd.conf 檔案中，將 ServerName 改成您的伺服器名稱。**

3. **啟動 apsslcfg。**

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

4. **選擇 1，將 Apache 網站伺服器設定為使用 SSL。**

注意 – 此程序假定您在此提示下選擇選項 1。如果您要選擇選項 2，請參閱第 89 頁的「使用 apsslcfg 指令碼」。

```
Sun Crypto Accelerator Apache 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. **鍵入 Apache 二進位程式碼的路徑。**

   在 Solaris 系統上，該路徑通常是 /usr/apache。

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

6. **鍵入 Apache 組態檔案的路徑。**

   在 Solaris 系統上，該路徑通常是 /etc/apache。

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

7. **為系統建立遠端安全存在 (RSA) 金鑰組。**

   如果您選擇不建立金鑰組，您必須稍後使用 apsslcfg 產生金鑰組。

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

   如果您回答 no，請跳到第 164 頁的「產生伺服器憑證」。

8. **提供儲存金鑰的目錄。**

   如果目錄不存在，則會建立該目錄。

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

9. **選擇金鑰資料的基礎名稱。**

   該名稱附有不同字尾以識別金鑰檔案、憑證要求檔案及相互之間的憑證檔案。

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

10. **提供長度介於 512 到 2048 位元之間的金鑰長度。**

    對於多數網站伺服器應用程式，1024 位元夠強了，但您可以選擇使用更強的金鑰。

```
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. 建立 PEM 通行碼。

此通行碼會保護金鑰資料。請確定選擇夠強的通行碼，但記得牢記該通行碼。如果忘記通行碼，您將無法存取金鑰。

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

警告 – 您必須記得輸入的通行碼。沒有通行碼，您將無法存取金鑰。沒有任何方法可以擷取失去的通行碼。

▼ 產生伺服器憑證

1. 使用您在第 162 頁的 「設定 Apache 網站伺服器」的步驟 7 中建立的金鑰建立憑證要求。

a. 鍵入密碼以存在金鑰。然後在要求者資訊欄位中鍵入適當資訊。

表 6-1 提供了要求者資訊欄位的說明。

```
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) []: Company
Organizational Unit Name (eg, section) []: Department
SSL Server Name (eg, www.company.com) []:www.company.com
Email Address []:admin@company.com
```

表 6-1 要求者資訊欄位

欄位	說明
Country Name (國家名稱)	代表國家的兩個字母的 ISO 代碼 (例如：美國的代碼爲 US)
State or Province Name (州或省名稱)	(選填) 完整州名，您也可以輸入點 (.)
Locality (地區)	城市、郡、所在地或國家
Organization Name (機構名稱)	公司名稱
Organizational Unit Name (機構單位名稱)	公司部門
SSL Server Name (SSL 伺服器名稱)	造訪者瀏覽器中鍵入的網站網域
Email Address (電子郵件地址)	要求者的聯絡資訊

2. **依照說明，修改** `/etc/apache/httpd.conf` **檔案。**

   有關金鑰與憑證檔案的資訊及如何修改 `/etc/apache/httpd.conf` 檔案的說明將會出現。

```
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 – 正確的*版本號碼*將會出現以供您設定組態。

3. **如果您選擇不要設立** VirtualHost**，您必須在** httpd.conf **檔案中的** SSLPassPhraseDialog **指令上加入** SSLEngine、SSLCertificateFile **及** SSLCertificateKeyFile **指令。**

```
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>
```

如果您對第 168 頁的「設定 Apache Web Server 2.x」中的步驟 7 問題回答 no，您將獲得如何產生金鑰資料的進一步資訊。

```
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. **完成** apsslcfg **的操作後，鍵入** 0 **以結束。**

▼ 安裝伺服器憑證

1. **從** `/etc/apache/keys/`*base-name*`-certreq.pem` **檔案 (其中，***base-name* **在第 162 頁的 「設定 Apache 網站伺服器」的步驟 9 中設定) 複製您的憑證要求及檔頭，並將憑證要求傳輸給憑證授權機構。**

2. **憑證產生後，請建立憑證檔案** `/etc/apache/keys/`*base-name*`-cert.pem` **並將您自己的憑證貼到檔案中。**

3. **啟動 Apache 網站伺服器。**

   下列路徑假定 Apache 二進位程式碼目錄是 `/usr/apache/bin`。如果這不是您的二進位程式碼目錄，請鍵入正確路徑。

   ```
   # /usr/apache/bin/apachectl sslstart
   ```

4. **在系統提示時輸入 PEM 通行碼。**

5. **使用瀏覽器造訪下列 URL，以檢查具有 SSL 功能的新網站伺服器：**
   `https://`*server-name*`:`*server-port*`/`

   請注意，預設的 *server-port* 是 443。

注意 – 請參閱 mod_SSL 與 OpenSSL 文件，以取得有關如何自簽憑證以進行測試的資訊。

建立與設定 Apache Web Server 2.x

Sun Crypto Accelerator 4000 軟體並不包含用於 Apache 2.x 網站伺服器的 mod_ssl 程式庫。本章節說明建立網站伺服器時需要包含的選項，及說明如何設定 Apache 2.x 以使用介面卡。

建立 Apache 2.x 網站伺服器

要啓動此程序，OpenSSL 實作必須具有所有所需的修正程式。本章節僅包含介面卡專屬選項，並不是建立整套 Apache 2.x 套件的完備指令集。要取得完整說明，請參閱 `http://www.apache.org` 提供的文件。

▼ 建立 Apache 2.x

1. **將 SH_LIBS 環境變數預設為符合 configure 指令碼要求。**

```
sh:
# SH_LIBS="-lssl -lcrypto"
# export SH_LIBS
csh/tcsh:
# setenv SH_LIBS "-lssl -lcrypto"
```

2. **變更至安裝目錄並執行 configure 指令碼。**

   此指令碼有許多指令行選項，設定網站伺服器以使用介面卡時需要下列指令：

```
# ./configure --enable-ssl --enable-mods-shared=ssl
--with-ssl=/opt/SUNWconn/cryptov2
```

3. **完成指令碼後，執行下列其中一項操作：**

   a. 如果第一次建立與安裝 Apache 2.x，請鍵入下列指令。

```
# make
# make install
```

   b. 如果要為現有 Apache 2.x 網站伺服器建立 mod_ssl 共用程式庫，請鍵入下列指令：

```
# make shared-build
# cp modules/ssl/.libs/mod_ssl.so Apache-directory/modules
```

設定 Apache Web Server 2.x

本章節說明如何透過產生與安裝伺服器憑證及啓用 SSL 的網站伺服器，來設定網站伺服器以使用介面卡。

▼ 產生伺服器憑證

1. 產生金鑰與憑證要求

```
# /opt/SUNWconn/cryptov2/bin/openssl req \
-new -newkey rsa:keysize -keyout key-output-file \
-out cert-request-output-file \
-config /opt/SUNWconn/cryptov2/ssl/openssl.cnf
Generating a 1024 bit RSA private key
.....................................................................
..........++++++
.......++++++
writing new private key to '/tmp/key1.pem'
```

2. 鍵入保護金鑰檔案的密碼。

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

3. 鍵入「Distinguished Name (辨別名稱)」值 (請參閱表 6-2**)。**

```
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]:California
Locality Name (eg, city) []:San Diego
Organization Name (eg, company) []: Company
Organizational Unit Name (eg, section) []: Company Division
SSL Server Name (eg, www.company.com) []:www.company.com
Email Address []: admin@domain.com
```

表 6-2 Distinguished Name (辨別名稱) 欄位

欄位	說明
Country Name (國家名稱)	代表國家的兩個字母的 ISO 代碼 (例如：美國的代碼爲 US)
State or Province Name (州或省名稱)	(選填) 完整州名，您也可以輸入點 (.)
Locality Name (地區名稱)	(選填) 城市、郡、所在地或國家
Organization Name (機構名稱)	公司名稱
Organizational Unit Name (機構單位名稱)	(選填) 公司部門
SSL Server Name (SSL 伺服器名稱)	造訪者瀏覽器中鍵入的網站網域
Email Address (電子郵件地址)	要求者的聯絡資訊

▼ 安裝伺服器憑證

- **將憑證要求與檔頭複製到在 第 169 頁的「產生伺服器憑證」的 步驟 1 中建立的金鑰檔案所在的相同目錄。**

▼ 啓用 SSL

1. **編輯 Apache 2.*x* 網站伺服器安裝目錄的 `conf` 子目錄中的 `ssl.conf` 檔案。**

   `ssl.conf` 檔案中有數個指令；網站伺服器必須設定下列指令，才能使用介面卡。

```
Listen port-number
ServerName fully-qualified-domain-name
SSLEngine on
SSLCertificateFile path-to-certificate-file
SSLCertificateKeyFile path-to-key-file
```

2. **啟動 Apache 網站伺服器。**

   這會假定 Apache 二進位程式碼目錄是 `/usr/apache/bin`。如果這不是您的二進位程式碼目錄，請鍵入正確的目錄。

```
# /usr/apache/bin/apachectl sslstart
```

3. **在系統提示時輸入 PEM 通行碼。**

4. **使用瀏覽器造訪下列 URL，以檢查具有 SSL 功能的新網站伺服器：**

   `https://`*server-name*`:`*server-port*`/`

   server-port 的預設值是 443。

注意 – 請參閱 mod_SSL 與 OpenSSL 文件，以取得有關如何自簽憑證以進行測試的資訊。

設定 Apache 網站伺服器以在重新啓動時無需使用者互動進行啓動

您可以啓用 Apache 網站伺服器，以在重新啓動時使用加密金鑰執行無人看管啓動。

▼ 建立 Apache 網站伺服器重新啓動時的自動啓動加密金鑰

1. **檢查** `httpd.conf` **檔案中是否存在下列項目：**

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

   此指令將從 `/etc/apache` 目錄中受保護的密碼檔案擷取密碼。

2. **根據下列的檔案命名常規，在** `/etc/apache` **目錄中建立僅包含密碼的密碼檔案：**

```
server-name:port.KEYTYPE.pass
```

   - *server-name* – 置於 `httpd.conf` 檔案的 ServerName 指令中的值
   - *port* – 此 SSL 伺服器將在其中執行的連接埠 (例如：443)
   - *KEYTYPE* – 可以是 `RSA` 或 `DSA`

   例如：對於具有 `RSA` 金鑰且名稱爲 `webserv101` 的伺服器 (在連接埠 443 上執行 SSL)，您可以在 `/etc/apache` 中建立下列檔案：

```
webserv101:443.RSA.pass
```

依照下列指令變更密碼檔案的權限與所有權：

```
# chmod 400 server-name:port.KEYTYPE.pass
# chown root server-name:port.KEYTYPE.pass
```

請參閱 mod_SSL 與 OpenSSL 文件以獲得更多資訊。

設定 Sun Crypto Accelerator 1000 以在安裝 Sun Crypto Accelerator 4000 軟體後使用 Apache

安裝 SUNWkcl2a 軟體套件後，系統將使用 Apache 網站伺服器 mod_ssl 1.3.26 設定。

如果要使用 Apache 設定 Sun Crypto Accelerator 1000 介面卡，則必須具有下列修正程式。

要設定 Sun Crypto Accelerator 1000 以在安裝了 SUNWkcl2a 套件的 Solaris 8 系統中使用 Apache 1.3.26，將需要下列修正程式：

- 對於 Apache 1.3.26 − Patch ID 109234-09 或更新
- 對於 Sun Crypto Accelerator 1000 1.0 版軟體 – Patch ID 112869-02
- 對於 Sun Crypto Accelerator 1000 1.1 版軟體 – Patch ID 113355-01

要設定 Sun Crypto Accelerator 1000 以在安裝了 SUNWkcl2a 套件的 Solaris 9 系統中使用 Apache 1.3.26，將需要下列修正程式：

- 對於 Apache 1.3.26 − Patch ID 113146-01 或更新
- 對於 Sun Crypto Accelerator 1000 1.1 版軟體 – Patch ID 113355-01

第 7 章

診斷與疑難排解

本章說明了 Sun Crypto Accelerator 4000 軟體的診斷測試與疑難排解。本章包含下列章節：

SunVTS 診斷軟體

核心 SunVTS 包裝函式爲一組測試提供測試控制與使用者介面。其中某些測試隨附在 SUNWvts 與 SUNWvtsx 套件中，以構成 Solaris 8/9 Software Supplement CD 中包含的套件。其他使用 SunVTS 核心的分類測試與測試裝置的驅動程式軟體組成套件。

Sun Crypto Accelerator 4000 介面卡可使用三種 SunVTS 測試來進行測試。其中兩種 nettest 與 netlbtest 測試隨附在從 SunVTS 5.1 Patch Set (PS) 2 版本開始的核心 SunVTS 軟體中。這兩種測試會對介面卡的乙太網路線路進行測試。

第三種 SunVTS 測試 vcatest 隨附在 Sun Crypto Accelerator 4000 CD 的 SUNWvcav 套件中，可與核心 SunVTS 包裝函式配合以診斷介面卡的編碼線路。

爲 vca 驅動程式安裝 SunVTS netlbtest 與 nettest 支援

表 7-1 顯示了更新安裝的 SunVTS 軟體以爲 vca 驅動程式提供 SunVTS netlbtest 及 nettest 支援的方法。

表 7-1 vca 驅動程式所需的 SunVTS netlbtest 與 nettest 軟體

基本 Solaris 軟體	基本 SunVTS 軟體	必要更換套件	必要重疊修正程式
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 軟體在各 Solaris 版本隨附的 Solaris Software Supplement CD 中提供。在表 7-1 的「基本 SunVTS 軟體」欄位中列出的 SunVTS 軟體版本，已在 Solaris 版本 (標示在同一行) 中隨附的 Solaris Software Supplement CD 中列出。

在表 7-1 中以「SunVTS」開頭的項目用以標示一組 SunVTS 套件的版本。所有的 SunVTS 套件組中，必須安裝 SUNWvts 與 SUNWvtsx 套件。

在表 7-1 的「必要更換套件」欄位中，列出了用來更換之前安裝 SunVTS 套件組的 SunVTS 套件組。新增 SunVTS 更換套件之前，請移除之前安裝的 SunVTS 套件。移除已安裝 SunVTS 套件的方法必須與安裝該套件所使用的方法相同。例如：如果使用 pkgadd 指令安裝該套件，請使用 pkgrm 指令將套件移除。

如果表 7-1 的「必要重疊修正程式」欄位中顯示了某個項目，請使用 patchadd 指令將該修正程式安裝到「基本 SunVTS 軟體」欄位中顯示的 SunVTS 套件中。新增必要修正程式之前，不需要移除之前安裝的 SunVTS 套件。

使用 patchadd 指令安裝修正程式 113614-11 與使用 SunVTS5.1ps2 套件更換之前安裝的 SunVTS 套件的結果相同。

更換套件可在下列網站取得：http://www.sun.com/oem/products/vts/

修正程式可在下列網站取得：http://sunsolve.sun.com/

注意 – 安裝 SUNWvcav 套件之前，必須先安裝所需的 SunVTS 套件與任何所需的修正程式，因爲 SUNWvcav 套件包含 SunVTS 測試 vcatest。

使用 SunVTS 軟體執行 vcatest、nettest 及 netlbtest

請參閱 SunVTS 測試參考手冊、使用者指南及快速參考卡片，以取得有關如何執行與監控這些診斷測試的說明。此類文件可在 http://docs.sun.com Sun Hardware Documentation Set 的 Solaris 中找到。此類文件也會在系統 Solaris 版本隨附的 Solaris Software Supplement CD 中提供。

注意 – 只有安裝了所需的 SunVTS 套件以及所有所需的 SunVTS 修正程式，您才能使用 SunVTS。

▼ 執行 vcatest

1. **以超級使用者身份啟動 SunVTS。**

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

請參閱 SunVTS 使用者指南以取得有關啓動 SunVTS 的詳細說明。

下列說明假定您使用 CDE 使用者介面啓動 SunVTS。

2. **在 SunVTS Diagnostic 主視窗中，將 System Map 設定為 Logical 模式。**

注意 – 雖然可支援 Physical 模式；但此程序會假定您使用的是 Logical 模式。

---

3. **清除所有核取方塊以停用所有測試。**
4. **選擇 Cryptography 核取方塊，然後選擇 Cryptography 的加號方塊，以顯示 Cryptography 群組中的所有測試。**
5. **清除 Cryptography 群組中名稱不是 vcatest 的核取方塊。**
   - 如果顯示 vcatest，請移至步驟 6。
   - 如果沒有顯示 vcatest，請在 Commands 下拉式功能表中選擇 Reprobe system，以重新偵測系統來尋找。

   請參閱 SunVTS 使用者指南以瞭解正確的程序。偵測完成、顯示 vcatest 後，請繼續進行步驟 6。
6. **選擇某個 vcatest 例項，然後按滑鼠右鍵並拖曳，以顯示 Test Parameter Options 對話方塊。**

   這些僅適用於 vcatest 的選項已在第 176 頁的「vcatest 測試參數選項」中說明。

7. **做完全部選擇後，請在 Within Instance 下拉式功能表中按一下 Apply，以變更選定的 vcatest 例項，或在 Across All Instance 下拉式功能表中選擇 Apply，以變更所有核取的 vcatest 例項。**

   此動作會移除對話方塊並返回 SunVTS Diagnostic 主視窗。

8. **選擇某個 vcatest 例項，然後按滑鼠右鍵並拖曳，以顯示 Test Execution Options 對話方塊。**

   另一種顯示 Test Execution Options 對話方塊的方法是：選擇 Options 下拉式主功能表，然後選擇 Test Executions。這些選項是通用 SunVTS 控制項，會影響所有測試。請參閱 SunVTS 使用者指南以取得詳細資訊。

9. **作完所有選擇後，選擇 Apply 以移除對話方塊，並回到 SunVTS Diagnostic 主視窗。**

10. **選擇 Start 執行所有選定的測試。**

11. **按一下「Stop」停止所有測試。**

vcatest 測試參數選項

表 7-2 說明 vcatest 子測試。

表 7-2 vcatest 子測試

測試名稱	說明
CDMF	測試 CDMP 大量加密
DES	測試 DES 大量加密
3DES	測試 3DES 大量加密。
RSA	測試 RSA 公開與私人金鑰。
DSA	測試 DSA 簽章驗證。
MD5	測試 MD5 Message Digest/Digital Signature
SHA1	測試 SHA1 Digest Key Creation
RNG	測試產生亂碼

vcatest 指令行語法

要使用指令行而不是 CDE 介面來執行 vcatest，請在指令行字串中指定所有的引數。

在 32 位元模式中，vcatest 的路徑是 /opt/SUNWvts/bin/。在 64 位元模式中，路徑是 /opt/SUNWvts/bin/sparcv9/。

所有 SunVTS 的標準選項在 vcatest 的指令行介面中亦可支援。特定的測試選項必須以 -o 引數特別指定。

請參閱 SunVTS 測試參考手冊以取得標準指令行引數的定義。由於 vcatest 是一個功能模式測試；因此您必須加上 -f。加入 -u 以顯示使用方式訊息、或加入 -v 以顯示 VERBOSE 訊息。上面以方括號括住的項目，代表選擇性項目。

下面的範例爲使用 32 位元模式、以個別程式的方式執行 vcatest。下列指令會在 vca0 上執行所有子測試：

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

下列是在 SunVTS 架構下以 64 位元模式執行 dcatest 的範例。下列指令會測試 vca2 上的 RSA、DSA 及 MD5：

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

從命令列執行 vcatest 時，如果省略某個選項，將會產生該選項的預設動作，如表 7-3 中說明。

表 7-3 vcatest 指令行語法

選項	說明
dev=vca*N*	指定要測試的裝置例項，例如 vca0 或 vca2。如果不加入此引數，預設爲 vca0。請注意 *N* 指定更換要測試裝置的例項號碼。
tl=*testlist*	指定要進行的子測試清單。tl 的子測試以 + (加號) 字元隔開。支援的子測試有 CDMF、DES、3DES、DSA、RSA、MD5、SHA1 及 RNG，這樣 tl=CDMF+DES+3DES+DSA+RSA+MD5+SHA1+RNG 會執行所有子測試。您也可以使用 tl=all 執行所有的測試。如果沒有指定子測試，會預設爲 all。

▼ 執行 netlbtest

1. **以超級使用者身份啟動 SunVTS。**

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

請參閱 SunVTS 使用者指南以取得詳細啓動說明。

下列說明假定您使用 CDE 使用者介面啓動 SunVTS。

2. **在 SunVTS Diagnostic 主視窗中，將 System Map 設定為 Logical 模式。**

注意 – 雖然可支援 Physical 模式；但此程序會假定您使用的是 Logical 模式。

---

3. **清除所有核取方塊以停用所有測試。**
4. **選擇 Network 核取方塊，然後選擇 Network 的加號方塊，以顯示 Network 群組中的所有測試。**
5. **清除 Network 群組中名稱不是 `vca`*N*`(netlbtest)` 的核取方塊。**

   請注意 *N* 指定更換正在測試裝置的例項號碼。

   - 如果顯示 `vca`*N*`(netlbtest)`，請移至步驟 6。
   - 如果沒有顯示 `vca`*N*`(netlbtest)`，請在 Commands 下拉式功能表中選擇 Reprobe system，以重新偵測系統來尋找。

   請參閱 SunVTS 使用者指南以瞭解正確的程序。偵測完成、顯示 `vca`*N*`(netlbtest)` 後，請繼續執行步驟 6。

6. **選擇 Intervention Mode 按鈕。選擇某個 `vca`*N*`(netlbtest)` 例項，然後按滑鼠右鍵並拖曳，以顯示 Test Parameter Options 對話方塊。**

   這些僅適用於 `netlbtest` 的選項已在 SunVTS 測試參考手冊中說明。

7. **做完全部選擇後，請在 Within Instance 下拉式功能表中選擇 Apply，以變更選定的 `vca`*N*`(netlbtest)` 例項，或在 Across All Instance 下拉式功能表中選擇 Apply，以變更所有核取的 `vca`*N*`(netlbtest)` 例項。**

   此動作會移除對話方塊並返回 SunVTS Diagnostic 主視窗。

8. **選擇某個 `vca`*N*`(netlbtest)` 例項，然後按滑鼠右鍵並拖曳，以顯示 Test Execution Options 對話方塊。**

   另一種顯示 Test Execution Options 對話方塊的方法是：選擇 Options 下拉式主功能表，然後選擇 Test Executions。這些選項是通用 SunVTS 控制項，會影響所有測試。請參閱 SunVTS 使用者指南以取得詳細資訊。

9. **作完所有選擇後，選擇 Apply 以移除對話方塊，並回到 SunVTS Diagnostic 主視窗。**
10. **選擇 Start 執行所有選定的測試。**
11. **按一下 「Stop」停止所有測試。**

▼ 執行 nettest

1. **以超級使用者身份啟動 SunVTS。**

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

請參閱 SunVTS 使用者指南以取得詳細啓動說明。

注意 – 下列說明假定您使用 CDE 使用者介面啓動 SunVTS。

---

2. **在 SunVTS Diagnostic 主視窗中，將 System Map 設定為 Logical 模式。**

注意 – 雖然可支援 Physical 模式；但此程序會假定您使用的是 Logical 模式。

---

3. **清除所有核取方塊以停用所有測試。**
4. **選擇 Network 核取方塊，然後選擇 Network 的加號方塊，以顯示 Network 群組中的所有測試。**
5. **清除 Network 群組中名稱不是** `vca`*N*`(nettest)` **的核取方塊。**

請注意 *N* 指定更換正在測試裝置的例項號碼。

- 如果顯示 `vca`*N*`(nettest)`，請移至步驟 6。
- 如果沒有顯示 `vca`*N*`(nettest)`，在配有 `vca`*N* 介面卡伺服器的其他視窗中輸入 `ifconfig -a`。應存在如下所示的項目：

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

如果上述 `ifconfig` 項目未列出，`nettest` 偵測會將裝置視爲無法測試。請按照 `ifconfig` 線上說明頁中的說明將介面置於線上。

一旦 `ifconfig -a` 產生上述項目，請返回 SunVTS Diagnostic 主視窗，然後在 Commands 下拉式功能表中選擇 Reprobe system，重新偵測系統以找到 `vca`。

請參閱 SunVTS 使用者指南以瞭解正確的程序。偵測完成、顯示 `vca0(nettest)` 後，請繼續執行步驟 6。

6. **選擇某個** `vca`*N*`(nettest)` **例項，然後按滑鼠右鍵並拖曳，以顯示 Test Parameter Options 對話方塊。**

這些僅適用於 `nettest` 的選項已在 SunVTS 測試參考手冊中說明。

7. **做完全部選擇後，請在 Within Instance 下拉式功能表中選擇 Apply，以變更選定的 vca*N*(nettest) 例項，或在 Across All Instance 下拉式功能表中選擇 Apply，以變更所有核取的 vca*N*(nettest) 例項。**

   此動作會移除對話方塊並返回 SunVTS Diagnostic 主視窗。

8. **選擇某個 vca*N*(nettest) 例項，然後按滑鼠右鍵並拖曳，以顯示 Test Execution Options 對話方塊。**

   另一種顯示 Test Execution Options 對話方塊的方法是：選擇 Options 下拉式主功能表，然後選擇 Test Executions。這些選項是通用 SunVTS 控制項，會影響所有測試。請參閱 SunVTS 使用者指南以取得詳細資訊。

9. **作完所有選擇後，選擇 Apply 以移除對話方塊，然後回到 SunVTS Diagnostic 主視窗。**

10. **選擇 Start 執行所有選定的測試。**

11. **按一下「Stop」停止所有測試。**

注意 – 請勿選擇同時執行 nettest 與 netlbtest。

使用 kstat 判斷編碼活動

Sun Crypto Accelerator 4000 介面卡不包含反映介面卡中編碼活動的指示燈。要判斷編碼工作要求是否是由介面卡處理，請使用 kstat(1M) 指令來顯示裝置使用情形：

```
# 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 – 上述範例中，0 指的是 vca 裝置的例項號碼。此號碼應該反映在其中執行 kstat 指令之介面卡的例項號碼。

顯示的 kstat 資訊說明編碼要求或「jobs」是否已送至 Sun Crypto Accelerator 4000 介面卡。*jobs* 數值的逐漸變更，表示介面卡正在加速傳送到 Sun Crypto Accelerator 4000 介面卡的編碼工作要求。如果編碼工作沒有傳送到介面卡上，請依照網站伺服器的特定組態，檢查網站伺服器的組態。

不要嘗試解讀 kstat(1M) 送回的核心/驅動程式統計數值。驅動程式維持這些數值的目的，是爲便利進行現地支援。其意義和實際數值可能會隨時變更。

注意 – 如果在 /kernel/drv/vca.conf 檔案中定義了 nostats 屬性，就會停用統計數字的擷取和顯示。此屬性可用來防止流量分析。

使用 OpenBoot PROM FCode 自我測試

如果系統無法啓動，可使用下列測試來協助找出介面卡的問題。

您可使用 OpenBoot PROM ok 提示中的 test 或 test-all 指令啓動 FCode 自我測試診斷。如果在執行診斷時遇到錯誤，系統會顯示適當的訊息。請參閱 *OpenBoot Command Reference Manual* 以取得更多有關 test 與 test-all 指令的資訊。

FCode 自我測試按各子章節測試功能，並確保下列內容：

- 介面卡機板安裝過程中的連線
- 驗證啓動系統所需的所有元件功能正常

▼ 執行乙太網路 FCode 自我測試診斷

要執行乙太網路診斷，您必須在發出重設指令後出現 OpenBoot PROM ok 提示時，將系統停止。如果沒有重設系統，診斷測試可能會導致系統當機。

有關本章節中 OpenBoot 指令的更多資訊，請參閱 *OpenBoot Command Reference Manual*。

1. **關閉系統。**

   請使用 *Solaris Handbook for Sun Peripherals* 中所述的標準關機程序。

2. **在 OpenBoot PROM** `ok` **提示出現時，將** `auto-boot?` **組態變數設定為** `false`**。**

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

3. **重設系統。**

```
ok reset-all
```

4. **鍵入** `show-nets` **以顯示裝置清單，並輸入選擇：**

   您會看到介面卡特定的裝置清單，如下列範例所示：

```
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` 指令執行下列自我測試，必須將乙太網路連接埠連接至網路。

---

5. **使用** `test` **指令執行自我測試：**

   發出 `test` 指令時，將會執行下列測試：

   - `vca` 註冊測試 (僅在 `diag-switch?` 爲 true 時發生)
   - 內部迴路測試
   - 連結/中斷連結測試

注意 – 用於 1000 Mbps 連線的 Sun Crypto Accelerator 4000 UTP 介面卡自我測試不支援與外部迴路纜線一同使用，因爲 link-clock 無法一致。對於此測試，本機與遠端連接埠必須配合設定爲主時脈和從屬時脈。如果使用外部迴路纜線，本機與遠端連接埠一致。因此，單個連接埠無法同時爲主時脈和從屬時脈，否則可能會導致 PHY link-up 經常出現故障。要讓用於 1000 Mbps 連線的 Sun Crypto Accelerator 4000 UTP 介面卡自我測試正常運作，必須連接遠端 1000BASE-T 連接埠。

鍵入下列內容：

```
ok test device-path
```

如果 test 通過，則會看到下列訊息：

```
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
```

如果未將介面卡連接至網路，則會看到下列訊息：

```
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. **介面卡測試完成之後，鍵入下列內容以將 OpenBoot PROM** ok **提示介面返回標準操作模式：**

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

7. **將** auto-boot? **組態參數設定為** true **。**

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

8. **重設並重新啟動系統。**

Sun Crypto Accelerator 4000 介面卡的疑難排解

本章節說明用於排解介面卡疑難之 OpenBoot PROM 等級的可用指令。請參閱 *OpenBoot Command Reference Manual* 以取得更多有關下列子章節中說明的指令資訊。

show-devs

判斷 Sun Crypto Accelerator 4000 裝置是否列在系統中：請由 OpenBoot PROM `ok` 提示，輸入 `show-devs` 以顯示裝置清單。您會看到指定至介面卡的特定裝置清單，如下列範例所示：

```
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
.
.
```

在上述範例中，`/pci@8,600000/network@1` 項目表示介面卡的裝置路徑。系統中的每個介面卡都會有這一行。

.properties

要判斷 Sun Crypto Accelerator 4000 裝置屬性是否已正確列出：請在 ok 提示出現時，鍵入 .properties 以顯示屬性清單。

```
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         00 03 ba 0e 99 ca
version                   Sun PCI Crypto Accelerator 4000 1000Base-T
FCode 2.11.13 03/03/04
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
max-latency               00000040
min-grant                 00000040
subsystem-vendor-id       0000108e
subsystem-id              00003de8
revision-id               00000002
device-id                 0000b555
vendor-id                 00008086
```

watch-net

要監控網路連線：在 ok 提示出現時，鍵入 apply watch-net 指令與裝置路徑：

```
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.....
```

系統會監控網路流量，在收到無錯封包時顯示「.」，而在收到可透過網路硬體介面偵測到的錯誤封包時顯示爲「X」。

第 8 章

PKCS#11 介面

本章說明介面卡的 PKCS#11 介面的實作，並假定 Sun Crypto Accelerator 4000 軟體安裝在預設位置。本章還假定您熟悉 PKCS#11 介面。有關 PKCS#11 標準與標頭檔案 `pkcs11.h`、`pkcs11f.h` 及 `pkcs11t.h` 的原始版本之資訊可在下列網站取得：`http://www.rsasecurity.com/rsalabs/PKCS`

本章包含下列章節：

一般問題

Sun Crypto Accelerator 4000 介面卡與相關軟體提供了 PKCS#11 介面。Sun Crypto Accelerator 4000 軟體提供了大多數應用程式所需的所有 PKCS#11 函數。

PKCS#11 專爲單一使用者系統設計。Solaris 作業系統是多使用者系統，必須處理多個同時且互不信任的使用者。爲解決此問題，介面卡新增了識別與驗證多個使用者的步驟，而無需延伸 PKCS#11。必須爲每個接受私密 PIN 的 PKCS#11 函數指派*使用者名稱:密碼*之格式的字串 (請參閱表 5-1)。雖然一些專門爲介面卡編寫的應用程式可能會個別地要求使用者名稱與密碼部分，但此 PIN 結構通常會透過應用程式傳播。

PKCS#11 可使用下列兩個函數執行有 限的管理功能：`C_InitToken` (初始化標記) 與 `C_InitPin` (設定使用者 PIN)。介面卡並不使用此功能，而是使用 `vcaadm` 公用程式。

`vcaadm` 安全管理員 (SO) 與 UNIX 超級使用者並不相關。此外，介面卡使用者的 `userid` (由 SO 使用 `vcaadm` 建立) 與任何 UNIX 使用者名稱或 ID 也不相關。

PKCS#11 的插槽與標記具有不同的概念。標記類似智慧卡，並插入*插槽*中。在 Sun Crypto Accelerator 4000 系統中，插槽與標記並沒有區別。本指南通常使用術語*標記*；但是，應用程式與其他說明文件可能使用術語*插槽*。

每個介面卡最多支援一個*金鑰庫*。SO 使用 `vcaadm` 爲每個金鑰庫提供了名稱。每個金鑰庫由介面卡顯示爲 PKCS#11 標記，且標記標籤做爲相關金鑰庫的名稱 (以空格填加至 32 個字元)。多個介面卡可以支援單一金鑰庫以取得高可用性。

此外，還具有一個含標籤 `SUNW acceleration only` 的特殊標記。此標記無法儲存任何永久性金鑰，且應用程式無法登入此標記。提交給此標記的要求將發佈給所有可用的介面卡。

許多應用程式會顯示標記的清單 — 標記通常由 PKCS#11 標記標籤識別。(標記標籤是 SO 指派的相關金鑰庫名稱，並填加了空格。)

管理使用 PKCS#11 的介面卡

使用 `vcaadm` 公用程式管理 Sun Crypto Accelerator 4000 系統 (請參閱第 4 章)。SO 會爲金鑰庫命名及建立使用者帳號，並爲每個帳號提供初始密碼。SO 還控制介面卡是否在 FIPS 模式下作業 (請參閱第 189 頁的「PKCS#11 與 FIPS 模式」)。

介面卡支援許多 PKCS#11 機制。大多數機制均可無條件地使用。但是，管理員對下列機制的表示可進行部分控制：

- `CKM_SSL3_SHA1_MAC`
- `CKM_SSL3_MD5_MAC`
- `CKM_SSL3_PRE_MASTER_KEY_GEN`
- `CKM_SSL3_MASTER_KEY_DERIVE`
- `CKM_SSL3_KEY_AND_MAC_DERIVE`
- `CKM_TLS_PRE_MASTER_KEY_GEN`
- `CKM_TLS_MASTER_KEY_DERIVE`
- `CKM_TLS_KEY_AND_MAC_DERIVE`

這些機制永遠由僅限加速標記呈現。僅在有 `/etc/opt/SUNWconn/cryptov2/sslreg` 時，它們才由具有金鑰庫的標記呈現。要建立此檔案，請以超級使用者身份鍵入下列指令：

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

重新啓動應用程式以使此變更生效。

這些機制可用時，網路安全服務 (NSS) 會加以辨識。提供這些機制後，NSS 會使用很小的緩衝區對 `C_DigestUpdate` 進行多次呼叫，從而會導致效能下降。因此，根據預設值，不會提供這些機制。

安裝與管理使用編碼服務的應用程式

PKCS#11 程式庫的預設位置爲：`/opt/SUNWconn/cryptov2/lib/libvpkcs11.so`

大多數應用程式具有包含 PKCS#11 程式庫位置的組態檔案或資料庫 (有時使用 GUI 存取)。使用編輯器或 GUI 輸入上述預設位置的值。

金鑰具有 `CKA_SENSITIVE` 屬性時，涉及該金鑰的作業會限制爲硬體。但是，並非所有作業與所有類型的金鑰都受硬體支援。如果應用程式要求無法在硬體下執行的作業，且金鑰的 `CKA_SENSITIVE` 屬性爲 true，則作業將失敗。有關金鑰、作業及機制有哪些可用組合的具體規則在第 190 頁的「硬體加速與敏感金鑰」中有詳細說明。如果應用程式由於這些規則而無法執行，您可以對其加以設定，不將其金鑰標記爲敏感。

`SSL...` 與 `TLS...` 機制是否呈現由管理員控制。如果應用程式需要這些機制，或者您要嘗試使用這些機制的效能效果，請參閱第 188 頁的「管理使用 PKCS#11 的介面卡」。

如果介面卡處於 FIPS 模式，將僅提供通過 FIPS 認證的機制 (請參閱第 189 頁的「PKCS#11 與 FIPS 模式」)。

PKCS#11 與 FIPS 模式

Sun Crypto Accelerator 4000 介面卡 由 SO (使用 `vcaadm`) 置於 FIPS 模式時，它符合聯邦資訊處理標準 FIPS 140-2 第 3 級的規定。有關 FIPS 140-2 的詳細資訊可以在下列網站找到：`http://www.nist.gov`

在 FIPS 模式下操作介面卡會導致介面卡的作業發生下列變更：

- 介面卡本身只能提供通過 FIPS 認證的機制。
- 所有金鑰與重大安全參數以加密型態通過 PCI 匯流排。
- 啓動時及在產生金鑰與隨機號碼時會進行一些附加完整性檢查。
- 隨機號碼由通過 FIPS 認證的演算法產生，該演算法使用雜湊與運算透過熱雜訊式產生器將儲存的狀態與真實的隨機資料 (熵) 相結合。熱雜訊式產生器產生的 512 位元用於每 160 位元的輸出資料。(在非 FIPS 模式下，熱雜訊式產生器產生的 512 位元以 SHA-1 雜湊爲 160 位元。)

FIPS 模式僅套用於 Sun Crypto Accelerator 4000 介面卡本身。如上所述，在介面卡處於 FIPS 模式時，介面卡僅提供通過 FIPS 認證的機制。請注意，MD5、RC2 及 RC4 並未通過 FIPS 認證。但是，由於 FIPS 規則僅適用於硬體，因此軟體將繼續提供所有軟體通常提供的機制。

在 FIPS 模式下作業時導致的主要差異在於非 FIPS 認證的作業僅在軟體下執行，這會產生兩種結果：

- 使用非 FIPS 認證的機制的編碼作業無法加速。
- 如果使用非 FIPS 認證的機制之編碼作業包含 CKA_SENSITIVE 屬性設定爲 true 的金鑰，則作業會失敗，因爲 CKA_SENSITIVE 屬性設定爲 true 的金鑰只能在硬體中使用。

硬體加速與敏感金鑰

介面卡會根據硬體功能、安全要求及效能選擇於何處執行作業。

PKCS#11 會指定許多金鑰類型與機制，但硬體並非支援所有金鑰類型與機制。當應用程式要求的作業、金鑰及機制組合，硬體並不完全支援時，可能會一部分在軟體中執行，而一部分在硬體中執行，或者完全在軟體中執行。

若金鑰的 CKA_SENSITIVE 屬性爲 true 時，必須安全地執行使用它的任何作業，也就是說，任何金鑰材料不能離開硬體。如果硬體無法安全地執行作業，則會失敗。反過來說，若金鑰的 CKA_SENSITIVE 屬性爲 false 時，介面卡會根據效能在硬體與軟體之間選擇。本章節說明在硬體、軟體及無法操作之間做選擇所使用的規則。

爲方便起見，定義了下列數組金鑰與機制：

- hardware_key_set =
  - RSA，含金鑰大小不超過 2048 位元
  - DSA，含金鑰大小不超過 1024 位元
  - DES
  - 3DES
  - CDMF
- hardware_mechanism_set =
  - CKM_CDMF_... 除 CKM_CDMF_ECB 外
  - CKM_DES_... 除 CKM_DES_ECB 外
  - CKM_DES3_... 除 CKM_DES3_ECB 外
  - CKM_DSA
  - CKM_MD5，除 FIPS 模式下外
  - CKM_RSA_...
  - CKM_SHA_1
- hardware_wrap_mechanism_set =
  - CKM_AES_CBC_PAD
  - CKM_CDMF_CBC_PAD
  - CKM_DES_CBC_PAD
  - CKM_DES3_CBC_PAD
  - CKM_RC2_CBC_PAD，除 FIPS 模式下外

爲讓所有作業在硬體中安全地執行，金鑰必須在 hardware_key_set 中，且機制必須在 hardware_mechanism_set 中。如果金鑰在 hardware_key_set 中，而機制不在 hardware_mechanism_set 中，則可能會由硬體加速作業，但加上軟體的協助。

C_DeriveKey 可能於硬體中加速，但需要軟體的協助，因此不是處於硬體等級的安全狀態。

下表說明了執行包含金鑰的作業其條件與位置：

表 8-1 大多數包含金鑰的編碼作業之處理

情況	CKA_SENSITIVE=**False**	CKA_SENSITIVE=**True**
硬體等級安全	硬體用於 RSA、DSA 及大緩衝區；其他則用軟體	硬體
在軟體的協助下可能進行硬體加速	硬體與軟體用於 RSA、DSA 及大緩衝區；其他則用軟體	失敗
僅限於軟體	軟體	失敗

C_WrapKey 與 C_UnwrapKey 涉及兩個金鑰上的兩個作業。對於 C_Wrap 金鑰，先是對已包裝的金鑰進行編碼的編碼作業，接著是使用包裝用的金鑰對編碼值進行加密的加密作業。C_UnwrapKey 則做相反的處理，先解密再解碼。

如果已包裝的金鑰是 RSA 或 DSA 金鑰，且包裝機制是 hardware_wrap_mechanism_set，則編碼與加密步驟均在硬體中執行。兩個金鑰的作業均處於硬體等級安全狀態。

如果不符合以上任一條件，編碼步驟將在軟體中進行。已包裝金鑰的作業則不是處於硬體等級安全狀態。加密步驟的作業與使用包裝用的金鑰與機制的 C_Encrypt 作業相同。請參閱表 8-1。

下表概述了各種情況：

表 8-2 C_WrapKey 與 C_UnwrapKey 的故障狀況

狀況	**已包裝的金鑰為敏感時失敗**	**包裝用的金鑰為敏感時失敗**
已包裝的金鑰是 RSA 或 DSA，且機制位於 hardware_wrap_mechanism_set	–	–
包裝用的金鑰位於 hardware_key_set 且機制位於 hardware_mechanism_set	失敗	–
所有其他情況	失敗	失敗

C_Digest 組合主機記憶體中整個緩衝區。如果緩衝區很大，但未超過 65532 位元組，C_DigestFinal 會將整個緩衝區傳送至硬體。否則，整個緩衝區會在軟體中進行。

C_DigestKey 會將金鑰材料置於主機記憶體，然後像普通資料一樣處理，再使用 C_DigestUpdate 進行處理。如果金鑰的 CKA_SENSITIVE 屬性爲 true，則會失敗。

開發使用 PKCS#11 的應用程式

所需的檔頭檔案位於 /opt/SUNWconn/cryptov2/include；請將此目錄新增至 include 路徑與 include cryptoki.h。下層等級 include 檔案 pkcs11.h、pkcs11f.h 及 pkcs11t.h 可在Sun Crypto Accelerator 4000軟體中取得。這些檔案與 PKCS#11 網站 (http://www.rsasecurity.com/rsalabs/PKCS) 提供的檔案相同。pkcs11_preamble.h 檔案可在 include 目錄中取得，必須包含在任何下層等級檔案之前。

pkcs11 程式庫爲：/opt/SUNWconn/cryptov2/lib/libvpkcs11.so。

Sun Crypto Accelerator 4000 程式庫可以作爲普通程式庫進行連結，或者可以使用 dlopen (3DL) 動態地開啓。

在作爲普通程式庫進行連結時，請使用下列指令：

```
cc [flags] files... -L /opt/SUNWconn/cryptov2/lib \
-R /opt/SUNWconn/cryptov2/lib -l vpkcs11 [other libraries...]
```

代碼應會直接調用函數，如下列範例所示：

```
rv = C_Initialize(NULL);
```

進行動態連結時，請使用下列指令 (所示爲忽略了錯誤處理)：

```
cc [flags] files... -ldl [ other libraries ... ]

#include "cryptoki.h"
#include <dlfcn.h>
#include <link.h>

void *cryptdlhandle;
CK_RV (*getfunctionlistp) (CK_FUNCTION_LIST_PTR *);
CK_FUNCTION_LIST *pk11funclist; /* may need to be globally
accessible */
CK_RV rv;
/* dlopen Sun Cryptoaccelerator 4000 library */
cryptodlhandle =
    dlopen("/opt/SUNWconn/cryptov2/lib/libvpkcs11.so",
    RTLD_NOW | RTLD_LOCAL | RTLD_GROUP);
if (cryptodlhandle == NULL) ...
/* Get pointer to C_GetFunctionList function */
getfunctionlistp = dlsym(cryptodlhandle, "C_getFunctionList");
if (getfunctionlistp == NULL) ...
/* Get libvpksc11's cryptki function list */
rv = (*getfunctionlistp) (&pk11funclist);
if (rv != CKR_OK) ...
```

代碼應會直接調用函數，如下所示：

```
rv = pk11funclist -> C_Initialize(NULL);
```

Sun Crypto Accelerator 4000 軟體強制的任何限制很少。大多數資源僅受主機記憶體限制。標記的最大數 (包括僅加速標記) 爲 1024。

爲防止有故障的或惡意程式進行本應拒絕的服務攻擊而佔用過多的核心記憶體，軟體會將任何一個 Solaris 使用者 (不是程序) 可以使用的核心記憶體量限制爲不超過 16 MB。此限制不能進行設定。

遵循下列建議可避免核心記憶體耗盡問題：

- 請勿放棄多步驟操作。呼叫適當的完成函數 (例如，`C_EncryptFinal`) 或在完成時關閉工作階段。
- 請勿放棄不需要的物件。關閉建立工作階段 (僅對變動物件有效) 或完成時呼叫 `C_DestroyObject`。
- 請勿同時提交特別大 (數 MB) 的資料量。(這不會套用於摘要作業，因爲大型摘要作業永遠在軟體中進行。)

不會執行 PKCS#11 管理函數 C_InitToken 與 C_InitPin。會拒絕具有 CKU_SO (安全管理員) 旗標的 C_Login 函數。

在 PKCS#11 中，*public token* 物件是可看見與可刪除的，而無需驗證的永久性物件。由於 Sun Crypto Accelerator 4000 軟體已知的使用者與 Solaris 使用者並不相關，且軟體在 C_Login 成功執行之前無法確定使用者身份，因此這些物件需要顯示給所有使用者，且任何使用者都能刪除。因爲無法接受此行爲，因此不允許公共標記物件。任何建立公共標記物件的嘗試將失敗。

變動 (工作階段) 物件數僅受虛擬記憶體限制。永久性物件均必須置於介面卡上的 RAM，但這並不是任何實用的限制。爲與此概念保持一致，表示最大記憶體大小的 CK_TOKEN_INFO 結構欄位 (由 C_GetTokenInfo 函數傳回) 均設定爲 CK_EFFECTIVELY_INFINITE。並不會執行 C_GetObjectSize 函數。

選用 *dual operation* 函數 (C_DigestEncryptUpdate、C_DecryptDigestUpdate、C_SignEncryptUpdate 及 C_DecryptVerifyUpdate) 不會執行，且 C_GetTokenInfo 傳回的旗標欄位中的 CKF_DUAL_OPERATIONS_FLAG 爲 false。

僅提供有限的 C_GetOperationState 實作及其附屬函數 C_SetOperationState。只有在執行 C_Digest 作業且累積的輸入資料大小未超過 65532 位元組時，C_GetOperationState 才能成功執行。

Sun Crypto Accelerator 4000 系統提供的標記被視爲無法移除。因此，CK_GetSlotInfo 傳回的 CKF_REMOVABLE_DEVICE 旗標爲 false。

並不會執行 C_WaitForSlotEvent 函數，且 Sun Crypto Accelerator 4000 系統不會呼叫作爲 C_OpenSession 的 Notify 參數傳送的 callback (回呼) 函數。軟體不會使用 C_OpenSession 的 pApplication 參數將 control back (回復控制) 交給呼叫應用程式。

Sun Crypto Accelerator 4000 介面卡 包含高品質真正隨機號碼產生器。它無需植入，而且實際上，會拒絕具有 CKR_RANDOM_SEED_NOT_SUPPORTED 的 C_SeedRandom。

如果視重要欄位是否在主機記憶體中而定的實作函數包含在 CKA_SENSITIVE 屬性設定爲 true 時建立的金鑰，這些函數將無法執行。具體的規則如下：

- 如果金鑰將 CKA_SENSITIVE 設定爲 true，C_DigestKey 將失敗。
- 如果基礎金鑰或要衍生的金鑰將 CKA_SENSITIVE 設定爲 true，所有機制的 C_DeriveKey 將失敗。
- 如果要換行或取消換行的金鑰將 CKA_SENSITIVE 設定爲 true，且如何出現下列任一狀況，C_WrapKey 與 C_UnwrapKey 將失敗：
  - 該金鑰不是 RSA 或 DSA 金鑰。
  - 機制不是 CKM_DES_CBC_PAD、CKM_DES3_CBC_PAD、CKM_RC2_CBC_PAD 或 CKM_AES_CBC_PAD。
- 如果金鑰將 CKA_SENSITIVE 設定爲 true，包含下列機制的任何作業將失敗：
  - CKM_AES...
  - CKM_CDMF_ECB
  - CKM_DES_ECB

- CKM_DES3_ECB
- CKM_DH...
- CKM_MD5_HMAC...
- CKM_RC2...
- CKM_RC4...
- CKM_SHA_1_HMAC...
- CKM_SSL3...
- CKM_TLS...

- 如果 CKA_SENSITIVE 設定爲 true，任何包含大於 2048 位元的 RSA 金鑰或大於 1024 位元的 DSA 金鑰之作業將失敗。

CKA_EXTRACTABLE 屬性的預設值是 true。CKA_SENSITIVE 屬性的預設值與 CKA_EXTRACTABLE 相反。使用 CKR_TEMPLATE_INCONSISTENT 將 CKA_SENSITIVE 與 CKA_EXTRACTABLE 均設定爲 false 的嘗試將失敗。

通常不會偵測不一致的屬性。例如：如果範本包含多個相同的屬性，實作只使用最後的值。只忽略與金鑰類型無關的屬性。並非所有無效的屬性都能偵測到。

並不會執行 CKA_LOCAL、CKA_ALWAYS_SENSITIVE 及 CKA_NEVER_EXTRACTABLE 屬性。

軟體傳回的錯誤代碼並不總是如預期。具體而言，傳回的 CKR_MECHANISM_INVALID 許多錯誤中，其他值可能較適當。傳回代碼 CKR_HOST_MEMORY 通常表示，對 malloc(3c) 指令的內部呼叫失敗。傳回此錯誤後，重要狀態可能未正確儲存，繼續嘗試 (除呼叫 C_Finalize 外) 可能是無效的。

爲減少額外操作，軟體的 C_EncryptInit 實作與類似函數有時會將金鑰延遲傳送至介面卡，直至存在要加密的實際資料。此延遲的結果是，某些 PKCS#11 宣告的錯誤本應由 C_EncryptInit (與類似函數) 報告，而實際上在對 C_EncryptUpdate (與類似函數) 進行第一次後續呼叫時即已報告。

下列 PKCS#11 識別代號已知的機制可在 Sun Crypto Accelerator 4000 軟體中取得。雖然 CKM_SSL3... 與 CKM_TLS... 機制會顯示在清單中，但是僅在具有檔案 /etc/opt/SUNWconn/cryptov2/sslreg 時，它們才能在具有金鑰庫的標記上使用 (請參閱第 188 頁的「管理使用 PKCS#11 的介面卡」)。

- CKM_AES_CBC
- CKM_AES_CBC_PAD
- CKM_AES_ECB
- CKM_AES_KEY_GEN
- CKM_CDMF_CBC
- CKM_CDMF_CBC_PAD
- CKM_CDMF_ECB
- CKM_CDMF_KEY_GEN
- CKM_DES2_KEY_GEN
- CKM_DES3_CBC
- CKM_DES3_CBC_PAD
- CKM_DES3_ECB
- CKM_DES3_KEY_GEN

- CKM_DES_CBC
- CKM_DES_CBC_PAD
- CKM_DES_ECB
- CKM_DES_KEY_GEN
- CKM_DH_PKCS_DERIVE
- CKM_DH_PKCS_KEY_PAIR_GEN
- CKM_DSA
- CKM_DSA_KEY_PAIR_GEN
- CKM_MD5
- CKM_MD5_HMAC
- CKM_MD5_HMAC_GENERAL
- CKM_RC2_CBC
- CKM_RC2_CBC_PAD
- CKM_RC2_ECB
- CKM_RC2_KEY_GEN
- CKM_RC4
- CKM_RC4_KEY_GEN
- CKM_RSA_PKCS
- CKM_RSA_PKCS_KEY_PAIR_GEN
- CKM_RSA_X_509
- CKM_SHA_1
- CKM_SHA_1_HMAC
- CKM_SHA_1_HMAC_GENERAL
- CKM_SSL3_KEY_AND_MAC_DERIVE
- CKM_SSL3_MASTER_KEY_DERIVE
- CKM_SSL3_MD5_MAC
- CKM_SSL3_PRE_MASTER_KEY_GEN
- CKM_SSL3_SHA1_MAC
- CKM_TLS_KEY_AND_MAC_DERIVE
- CKM_TLS_MASTER_KEY_DERIVE
- CKM_TLS_PRE_MASTER_KEY_GEN

RSA、DSA 及 Diffie-Hellman 金鑰具有下列最大金鑰大小：

表 8-3 最大金鑰大小

金鑰	非敏感最大金鑰大小	敏感最大金鑰大小
RSA	4096	2048
DSA	4096	1024
DH	2048	不適用

請勿假定物件控制元或工作階段控制元是小整數或按順序分配。這些控制元可能是任何無符號長整型 (unsigned long)。

可以傳送至 `C_Initialize` 的互斥體 (mutex) 回呼函數指標會忽略。

在許多情況下，對少量資料的作業由主機處理器而不是由介面卡處理，因爲將作業傳送至介面卡的成本超過在主機中執行的成本。但是，所有包含 CKA_SENSITIVE 屬性設定爲 true 的物件之作業均在介面卡中執行。

如果所有 C_DigestUpdate 緩衝區的累積大小超過 65532 位元組，則摘要由主機中的軟體處理。相同特性會套用於 C_Digest。因此，不管是少量資料還是大量資料均由軟體處理。

在使用者成功執行 C_Login 函數且函數保留在快取中時，在程序中會顯示有關永久性物件的資訊。可能不會顯示其他程序對永久性物件的後續建立、刪除或修改。在介面卡中執行的作業將使用目前的金鑰狀態。(如果介面卡可以執行作業且金鑰是敏感的，或介面卡可以執行作業且緩衝區足夠大能夠加以執行，則在介面卡中執行作業。) 其他所有情況以及 C_FindObjects 函數，均使用金鑰的快取狀態在軟體中處理。

警告 – 在未來版本中，以上金鑰快取行爲可能會所有變更。

按照 PKCS#11 標準的要求，使用者呼叫 C_Logout 函數或關閉最後的 PKCS#11 工作階段時，所有永久性物件控制元將無效。軟體會從軟體的快取中清除標記物件。之後成功的 C_Login 函數會產生所有最新的標記物件。請注意，此登入可能適用於不同的使用者，因此會產生不同的標記物件集。但是，即使此登入適用於相同的使用者，標記物件可能也不會取得相同的控制元，除非之前具有相同的控制元。

附錄 **A**

規格

本附錄所列爲 Sun Crypto Accelerator 4000 MMF 與 UTP 介面卡的規格，包含下列章節：

Sun Crypto Accelerator 4000 MMF 介面卡

本章節說明 Sun Crypto Accelerator 4000 MMF 介面卡的規格。

接頭

圖 A-1 顯示了 Sun Crypto Accelerator 4000 MMF 介面卡的接頭。

圖 A-1 Sun Crypto Accelerator 4000 MMF 介面卡接頭

表 A-1 列出了 SC 接頭 (850 奈米) 的特性。

表 A-1 SC 接頭連結特性 (IEEE P802.3z)

特性	62.5 微米 MMF	50 微米 MMF
操作範圍	最長 260 公尺	最長 550 公尺

實體尺寸

表 A-2 實體尺寸

尺寸	測量	公制度量
長度	12.283 英吋	312.00 公釐
寬度	4.200 英吋	106.68 公釐

效能規格

表 A-3 效能規格

功能	規格
PCI 時脈	33/66 MHz (最高)
PCI 資料激增傳輸率	激增傳輸的最高速率爲 64 位元組
PCI 資料/位址寬度	32/64 位元
PCI 模式	主要/從屬
1 Gbps，850 奈米	1000 Mbps (全雙工)

電源要求

表 A-4 電源要求

規格	測量
最大耗電量	6.25 W @ 5V 12.75 W @ 3.3V
電壓容差	5V +/- 5% 3.3V +/- 5%

介面規格

表 A-5 介面規格

功能	規格
PCI 時脈	33 MHz 或 66 MHz
主機介面	支援 33 MHz 或 66 MHz 時脈及 3.3 V 或 5 V 電源的 PCI 2.1
PCI 匯流排寬度	32 位元或 64 位元

環境規格

表 A-6 環境規格

條件	操作規格	存放規格
溫度	0° 到 +55°C，+32° 到 +131°F	-40° 到 +75°C，-40° 到 +167°F
相對濕度	5 到 85%，非冷凝	0 到 95%，非冷凝

Sun Crypto Accelerator 4000 UTP 介面卡

本章節將提供 Sun Crypto Accelerator 4000 UTP 介面卡的規格。

接頭

圖 A-1 顯示了 Sun Crypto Accelerator 4000 UTP 介面卡的接頭。

圖 A-2 Sun Crypto Accelerator 4000 UTP 介面卡接頭

表 A-7 列出了 Sun Crypto Accelerator 4000 UTP 介面卡使用的第 5 類接頭之特性。

表 A-7 第 5 類接頭連結特性

特性	說明
操作範圍	最長 100 公尺

實體尺寸

表 A-8 實體尺寸

尺寸	測量	公制度量
長度	12.283 英吋	312.00 公釐
寬度	4.200 英吋	106.68 公釐

效能規格

表 A-9 效能規格

功能	規格
PCI 時脈	33/66 MHz (最高)
PCI 資料激增傳輸率	激增傳輸的最高速率爲 64 位元組
PCI 資料/位址寬度	32/64 位元
PCI 模式	主要/從屬
1 Gbps	1000 Mbps (全雙工)
100 Mbps	100 Mbps (全雙工與半雙工)
10 Mbps	10 Mbps (全雙工與半雙工)

電源要求

表 A-10 電源要求

規格	測量
最大耗電量	6.25 W @ 5V 12.75 W @ 3.3V
電壓容差	5V +/- 5% 3.3V +/- 5%

介面規格

表 A-11 介面規格

功能	規格
PCI 時脈	33 MHz 或 66 MHz
主機介面	支援 33 MHz 或 66 MHz 時脈及 3.3 V 或 5 V 電源的 PCI 2.1
PCI 匯流排寬度	32 位元或 64 位元

環境規格

表 A-12 環境規格

條件	操作規格	存放規格
溫度	0° 到 +55°C，+32° 到 +131°F	-40° 到 +75°C，-40° 到 +167°F
相對濕度	5 到 85%，非冷凝	0 到 95%，非冷凝

附錄 **B**

不使用安裝指令碼安裝軟體

本附錄說明不使用產品 CD 中提供的安裝指令碼 (`/cdrom/cdrom0/install`) 如何手動安裝 Sun Crypto Accelerator 4000 軟體。包含下列章節：

手動安裝軟體

Sun Crypto Accelerator 4000 軟體包含在產品 CD 中。您可能需要從 SunSolve 網站 (`http://sunsolve.sun.com`) 下載修正程式。請第 10 頁的 「所需修正程式」參考以取得更多資訊。

▼ 手動安裝軟體

1. **將 Sun Crypto Accelerator 4000 CD 放入連接到系統的 CD-ROM 光碟機。**
   - 如果系統執行的是 Sun Enterprise Volume Manager，它會自動將 CD-ROM 安裝到 `/cdrom/cdrom0` 目錄中。
   - 如果系統未執行 Sun Enterprise Volume Manager，請如下所述掛載 CD-ROM：

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

您可在 /cdrom/cdrom0 目錄中看到下列檔案與目錄。

表 B-1 /cdrom/cdrom0 目錄中的檔案

檔案或目錄	內容	
Copyright	美國著作權聲明檔案	
FR_Copyright	法文著作權聲明檔案	
install	安裝 Sun Crypto Accelerator 4000 軟體的安裝指令碼	
remove	移除 Sun Crypto Accelerator 4000 軟體的移除指令碼	
Docs	*Sun Crypto Accelerator 4000 介面卡 1.1 版安裝與使用者指南* *Sun Crypto Accelerator 4000 介面卡版本注意事項*	
Packages	Sun Crypto Accelerator 4000 軟體套件：	
	SUNWkcl2r	編碼核心元件
	SUNWkcl2u	編碼管理公用程式與程式庫
	SUNWkcl2a	Apache SSL 支援 *(選用)*
	SUNWkcl2m	編碼管理說明頁 (*選用*)
	SUNWvcar	VCA 編碼加速器 (root)
	SUNWvcau	VCA 編碼加速器 (usr)
	SUNWvcaa	VCA 管理
	SUNWvcafw	VCA 韌體
	SUNWvcamn	VCA 編碼加速器說明頁 (*選用*)
	SUNWvcav	VCA 編碼加速器的 SunVTS 測試 *(選用)*
	SUNWkcl2o	SSL 開發工具與程式庫 *(選用)*
	SUNWkcl2i.u	具有 KCLv2 編碼的 IPsec 加速 *(選用)*

所需套件必須按特定順序安裝並且必須在安裝任何選用套件之前安裝。安裝所需套件後，您可以按任何順序安裝與移除選用套件。

只有在計劃使用 Apache 作爲網站伺服器時，才安裝選用的 SUNWkcl2a 套件。

只有在計劃重新連結到其他 (未支援) 版本的 Apache 網站伺服器時，才安裝選用的 SUNWkcl2o 套件。

只有在計劃執行 SunVTS 測試時，才安裝選用的 SUNWvcav 套件。您必須先安裝 SunVTS 4.4 或更新版本 (可高達 5.x)，才能安裝 SUNWvcav 套件。

注意 – Sun Crypto Accelerator 4000 CD 上的選用 SUNWkcl2i.u 套件僅具有 .u 副檔名。安裝此套件後，名稱會變更爲 SUNWkcl2i。CD 上此套件的 .u 副檔名會將該套件定義爲 sun4u architecture-specific。

1. **鍵入下列指令以安裝所需的軟體套件：**

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2r SUNWkcl2u SUNWkcl2m SUNWvcar SUNWvcau SUNWvcaa SUNWvcamn
SUNWvcafw
```

2. **(選用) 要檢查是否已正確安裝軟體，請執行** pkginfo **指令。**

```
# pkginfo SUNWkcl2r SUNWkcl2u SUNWvcar SUNWvcau SUNWvcaa SUNWvcafw
system      SUNWkcl2r      KCLv2 Crypto (Root)
system      SUNWkcl2u      KCLv2 Crypto Support Software
system      SUNWvcaa       VCA Crypto Accelerator/Gigabit Ethernet Admin
system      SUNWvcafw      VCA Crypto Accelerator/Gigabit Ethernet firmware
system      SUNWvcar       VCA Crypto Accelerator/Gigabit Ethernet Drivers
system      SUNWvcau       VCA Crypto Accelerator/Gigabit Ethernet Daemon
```

3. **(選用) 要確定是否已安裝驅動程式，請執行** prtdiag **指令。**

   請參閱 prtdiag(1m) 線上說明頁。

```
# prtdiag -v
```

4. **(選用) 執行** modinfo **指令以查看是否已載入模組。**

```
# 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)
```

安裝選用套件

要僅安裝提供 Apache 網站伺服器與 Sun Crypto Accelerator 4000 線上說明頁 SSL 支援的選用套件，請鍵入下列指令：

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2a SUNWkcl2m
```

要安裝所有選用軟體套件，請鍵入下列指令：

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

請參閱表 B-1 以取得上述範例中選用套件的套件內容說明。

目錄與檔案

表 B-2 顯示預設安裝 Sun Crypto Accelerator 4000 軟體時所建立的目錄。

表 B-2 Sun Crypto Accelerator 4000 目錄

目錄	內容
/etc/opt/SUNWconn/vca/keydata	金鑰庫資料 (已加密)
/opt/SUNWconn/cryptov2/bin	公用程式
/opt/SUNWconn/cryptov2/lib	支援程式庫
/opt/SUNWconn/cryptov2/sbin	管理指令

圖 B-1 顯示這些目錄與檔案的結構。

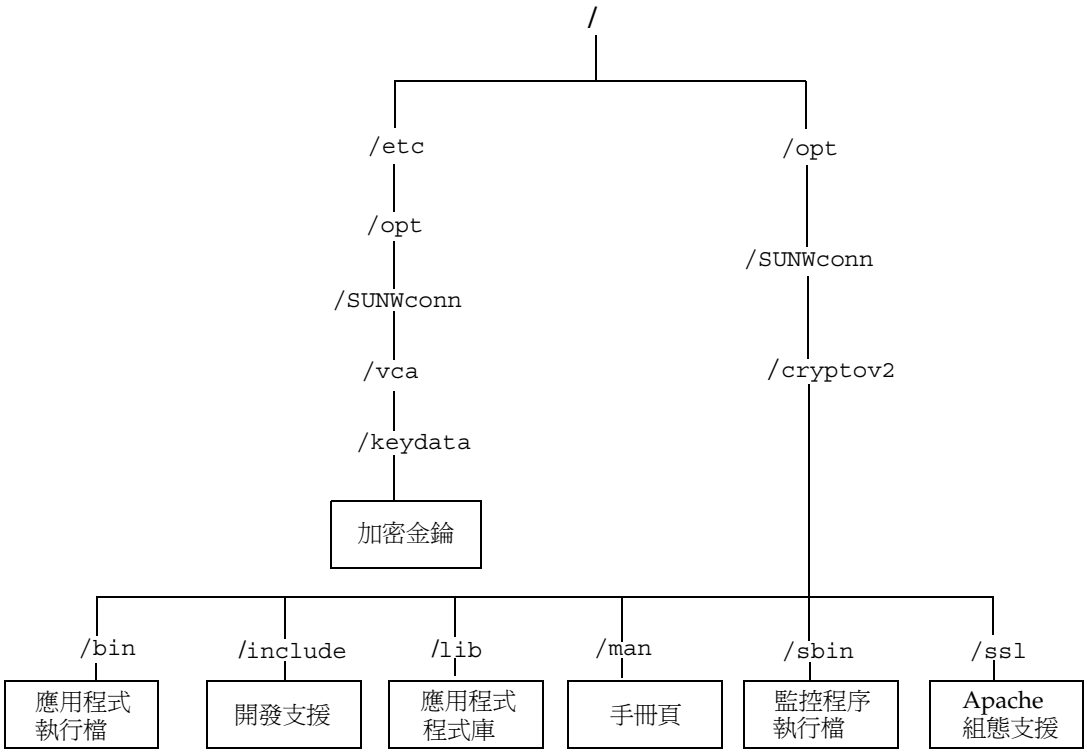

圖 B-1 Sun Crypto Accelerator 4000 目錄與檔案

注意 – 安裝介面卡的硬體與軟體後，您需要使用組態與金鑰庫資訊初始化介面卡。請參閱第 62 頁的「使用 vcaadm 初始化介面卡」以取得有關如何初始化介面卡的資訊。

手動移除軟體

如果已建立金鑰庫 (請參閱第 65 頁的「使用 vcaadm 管理金鑰庫」)，您必須先刪除設定 Sun Crypto Accelerator 4000 介面卡的金鑰庫資訊，然後再移除此軟體。zeroize 指令會移除所有金鑰資料，但不會刪除儲存在安裝了介面卡的實體主機檔案系統中的金鑰庫檔案。請參閱第 74 頁的「對介面卡執行軟體化零」以取得有關 zeroize 指令的詳細資料，要刪除系統中儲存的金鑰庫檔案，請以超級使用者身份登入，然後移除金鑰庫檔案。如果尚未建立任何金鑰庫，您可以跳過此程序。

警告 – 請勿刪除目前正在使用或其他使用者與金鑰庫共用的金鑰庫。要釋放對金鑰庫的參照，您可能要關閉網站伺服器與 (或) 管理伺服器。

警告 – 移除 Sun Crypto Accelerator 4000 軟體之前，請先停用爲了使用 Sun Crypto Accelerator 4000 介面卡而啓用的所有網站伺服器。否則，會導致這些網站伺服器無法正常運作。

▼ 手動移除軟體

- **如果只要移除已安裝的軟體套件，請以超級使用者身份登入，然後使用** `pkgrm` **指令移除。**

警告 – 已安裝的套件必須按所示順序移除。否則，可能會引起警告，因而無法卸載核心模組。

如果已安裝所有套件，則應如下所述加以移除：

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

注意 – 安裝或移除 Sun Crypto Accelerator 4000 介面卡的 SunVTS 測試 (`SUNWvcav`) 後，如果 SunVTS 已在執行，可能需要再次檢查系統以更新可用的測試。請參閱 SunVTS 文件以取得更多資訊。

附錄 C

Apache 網站伺服器的 SSL 組態指令

本附錄列出了使用 Sun Crypto Accelerator 4000 軟體設定 Apache 網站伺服器 SSL 支援的指令。請在 `http.conf` 檔案中設定指令。請參考 Apache 網站伺服器文件以獲得更多資訊。

1. `SSLPassPhraseDialog exec:`*program*

   適用範圍：全域

   本指令告知 Apache 網站伺服器應該執行指定 *program* 以蒐集金鑰檔案密碼。*program* 應該將蒐集到的密碼列印到標準輸出。

   如果存在多個金鑰檔案且有通用密碼，則只會執行 *program* 一次 (再次執行 *program* 前，會嘗試每個蒐集的密碼)。

   program 執行時有兩個引數：第一個是伺服器名稱，格式爲：*servername*:*port*，例如：`www.fictional-company.com:443`。(通訊埠 443 是以 SSL 爲基礎的網站伺服器的典型通訊埠)。第二個引數爲金鑰檔案中的金鑰類型 (*keytype*)。*keytype* 可以是 RSA 或 DSA。

注意 – 由於本程式可以在系統啓動時執行，請務必設計爲能夠應付主控台並非 `tty` 裝置的情況 (此時 `tty`(3c) 會傳回 false)。

   提供的程式 `/opt/SUNWconn/cryptov2/bin/apgetpass` 可以用於 *program* 執行檔。本程式會自動提示要求輸入密碼，且在密碼輸入時將不予顯示。

   提供的 `sslpassword` 程式也會自動在檔案中搜尋密碼 ，這可以用來在網站伺服器啓動時避免使用者互動。金鑰檔案的密碼會在名稱爲 `/etc/apache/`*servername*:*port*.*keytype*`.pass` 的檔案中進行搜尋。如果找不到該檔案，則系統會使用 `/etc/apache/default.pass` 檔案。這些密碼檔案僅包含未加密的密碼，每個密碼一行。

注意 – 密碼檔案應該使用權限加以保護，如此僅有執行網站伺服器的 UNIX 使用者可以讀取該檔案。此使用者應該與使用標準 Apache `User` 指令設定的使用者相同。

   如果沒有特別指定，預設動作是使用內部的提示機制。請勿使用預設值；請使用提供的 `sslpassword` 程式，以避免在系統啓動時進行互動的麻煩。

2. SSLEngine (on|off)

適用範圍：全域、虛擬主機

本指令會啓用 SSL 通訊協定。這一般是用來在虛擬主機上啓用伺服器子集的 SSL 功能。常用的型態之一是：

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

對於監聽連接埠 443 (標準 HTTPS 連接埠) 的所有伺服器，此陳述將設定 SSL 的使用。如果不存在，根據預設會關閉此通訊協定。

3. SSLProtocol [+-]*protocol*

適用範圍：全域、虛擬主機

本指令會設定伺服器應該用於 SSL 交易的的通訊協定。可用的通訊協定如表 C-1 中所列及說明。

表 C-1 SSL 通訊協定

通訊協定	說明
SSLv2	來自 Netscape，原始的 SSL 標準
SSLv3	更新版本的 SSL 通訊協定，爲多數受歡迎網頁瀏覽器所支援
TLSv1	SSLv3 的更新，目前正在進行 IETF 標準化，本文撰寫之時僅有極少的瀏覽器支援
all	啓用所有通訊協定

您可以使用加號 (+) 或減號 (-) 來新增或移除通訊協定。例如，要停用 SSLv2 支援，請使用下列指令：

```
SSLProtocol all -SSLv2
```

以下陳述相當於：

```
SSLProtocol +SSLv3 +TLSv1
```

4. `SSLCipherSuite` *cipher-spec*

   適用範圍：全域、虛擬主機、目錄、`.htaccess`

   SSLCipherSuite 指令用於設定可供使用的 SSL 編碼器及其偏好設定。在全域或虛擬主機的情況下，會在最初的 SSL 交握 (handshake) 中使用此指令。在單一目錄的情況下，它會強迫 SSL 協議使用指定的編碼器。協議會在讀取要求後、傳送回應前進行。

   cipher-spec 是一個用冒號分隔的編碼器清單，如表 C-2 所述。在表 C-2 中，DH 指的是 Diffie-Hellman，DSS 指的是 Digital Signature Standard (數位簽章標準)。

表 C-2 可用的 SSL 編碼器

Cipher-Tag	通訊協定	金鑰交換	驗證	加密	MAC	類型
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES (168 位元)	SHA1	
DES-CBC3-MD5	SSLv2	RSA	RSA	3DES (168 位元)	MD5	
RC4-SHA	SSLv3	RSA	RSA	ARCFOUR (128 位元)	SHA1	
RC4-MD5	SSLv3	RSA	RSA	ARCFOUR (128 位元)	MD5	
RC4-MD5	SSLv2	RSA	RSA	ARCFOUR (128 位元)	MD5	
RC2-CBC-MD5	SSLv2	RSA	RSA	ARCTWO (128 位元)		
DES-CBC-SHA	SSLv3	RSA	RSA	DES (56 位元)	SHA1	
RC4-64-MD5	SSLv2	RSA	RSA	ARCFOUR (64 位元)	MD5	
DES-CBC-MD5	SSLv2	RSA	RSA	DES (56 位元)	MD5	
EXP-DES-CBC-SHA	SSLv3	RSA (512 位元)	RSA	DES (40 位元)	SHA1	匯出
EXP-RC2-CBC-MD5	SSLv2	RSA (512 位元)	RSA	ARCTWO (40 位元)	SHA1	匯出
EXP-RC2-CBC-MD5	SSLv3	RSA (512 位元)	RSA	ARCTWO (40 位元)	SHA1	匯出
EXP-RC4-MD5	SSLv3	RSA (512 位元)	RSA	ARCFOUR (40 位元)	MD5	匯出
EXP-RC4-MD5	SSLv2	RSA (512 位元)	RSA	ARCFOUR (40 位元)	MD5	匯出
NULL-SHA	SSLv3	RSA	RSA	無	SHA1	
NULL-MD5	SSLv3	RSA	RSA	無	MD5	
ADH-DES-CBC3-SHA	SSLv3	DH	無	3DES (168 位元)	SHA1	
ADH-DES-CBC-SHA	SSLv3	DH	無	DES (56 位元)	SHA1	
ADH-RC4-MD5	SSLv3	DH	無	ARCFOUR (128 位元)	MD5	
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES (168 位元)	SHA1	
EDH-DSS-DES-CBC3-SHA	SSLv3	DH	DSS	3DES (168 位元)	SHA1	
EDH-RSA-DES-CBC-SHA	SSLv3	DH	RSA	DES (56 位元)	SHA1	
EDH-DSS-DES-CBC-SHA	SSLv3	DH	DSS	DES (56 位元)	SHA1	

表 C-2 可用的 SSL 編碼器 *(續)*

Cipher-Tag	通訊協定	金鑰交換	驗證	加密	MAC	類型
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH (512 位元)	RSA	DES (40 位元)	SHA1	匯出
EXP-EDH-DSS-DES-CBC-SHA	SSLv3	DH (512 位元)	DSS	DES (40 位元)	SHA1	匯出
EXP-ADH-DES-CBC-SHA	SSLv3	DH (512 位元)	無	DES (40 位元)	SHA1	匯出
EXP-ADH-RC4-MD5	SSLv3	DH (512 位元)	無	ARCFOUR (40 位元)	MD5	匯出

表 C-3 列出並說明了提供類似巨集分組功能的別名。

表 C-3 SSL 別名

別名	說明
SSLv2	所有 SSL 2.0 版編碼器
SSLv3	所有 SSL 3.0 版編碼器
EXP	所有匯出等級編碼器
EXPORT40	所有 40 位元匯出編碼器
EXPORT56	所有 56 位元匯出編碼器
LOW	較低強度編碼器 (DES，40 位元 RC4)
MEDIUM	全部 128 位元編碼器
HIGH	所有編碼器使用三重 DES
RSA	所有編碼器使用 RSA 金鑰交換
DH	所有編碼器使用 Diffie-Hellman 金鑰交換
EDH	所有編碼器使用 Ephemeral Diffie-Hellman 金鑰交換
ADH	所有編碼器使用匿名 Diffie-Hellman 金鑰交換
DSS	所有編碼器使用 DSS 驗證
NULL	所有編碼器都不使用加密

您可以使用表 C-4 中列出並詳細說明的特殊字元來設定編碼器偏好組態。

表 C-4 設定編碼器偏好的特殊字元

字元	說明
<無>	新增編碼器到清單
!	從清單中完全移除編碼器 — 編碼器將無法再度加入
+	新增編碼器到清單中，並放到目前位置 (可能會將它降階)
-	從清單中移除編碼器 (稍後可重新加入清單中)

cipher-spec 的預設值是

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

預設值會設定所有編碼器的組態，但匿名 (未經驗證) Diffie-Hellman 除外，ARCFOUR 與 RSA 優先使用，且高等級的加密優於低等級的加密。

5. `SSLCertificateFile` *file*

   適用範圍：全域、虛擬主機

   本指令會指定本伺服器中 PEM 編碼的 X.509 憑證檔案所在位置。

6. `SSLCertificateKeyFile` *file*

   適用範圍：全域、虛擬主機

   本指令會指定本伺服器中 PEM 編碼的私人金鑰檔案所在位置，對應於使用 `SSLCertificateFile` 指令設定組態的憑證。

7. `SSLCertificateChainFile` *file*

   適用範圍：全域、虛擬主機

   本指令會指定包含構成伺服器憑證路徑的 PEM 編碼之憑證的位置。當伺服器憑證並非由用戶端所知的授權機構直接簽署時，您可以使用指令協助用戶端檢查伺服器憑證。

   使用用戶端驗證 (`SSLVerifyClient`) 時，對於用戶端驗證，會假設鍊結中的憑證有效。

8. `SSLCACertificateFile` *file*

   適用範圍：全域、虛擬主機

   本指令會指定包含用於用戶端驗證之憑證授權機構 (CA) 的憑證連鎖檔案的所在位置。

9. `SSLCARevocationFile` *file*

   適用範圍：全域、虛擬主機

   本指令指定包含用戶端驗證所用憑證授權機構 (CA) 之憑證撤銷清單的連鎖檔案位置。

10. `SSLVerifyClient` *level*

    適用範圍：全域、虛擬主機、目錄、`.htaccess`

    本指令設定了用戶端對伺服器的驗證組態。(注意：對於電子商務應用而言一般並不需要此項設定，但在其他應用中有作用。)

level 的數值如表 C-5 所列及說明。

表 C-5 SSL 檢查用戶端階層

層級	說明
`none`	不需要用戶端憑證
`optional`	用戶端可以提出有效憑證
`require`	用戶端*必須*提出有效憑證
`optional_no_ca`	用戶端可以提出憑證，但憑證不需要一定有效

一般來說會使用 `none` 或 `require`。預設值是 `none`。

11. `SSLVerifyDepth` *depth*

適用範圍：全域、虛擬主機、目錄、`.htaccess`

本指令會指定伺服器在用戶端憑證上允許的最大憑證鍊結深度。數值 0 代表只有自行簽署的憑證有效，而數值 1 代表用戶端憑證必須由伺服器直接認可的 CA (透過 `SSLCACertificateFile`) 簽署。更大的數值允許 CA 代理

12. `SSLLog` *filename*

適用範圍：全域、虛擬主機

本指令會指定記錄 SSL 專屬資訊的記錄檔。如果未指定 (預設值)，則不會記錄任何 SSL 特定資訊。

13. `SSLLogLevel` *level*

適用範圍：全域、虛擬主機

本指令指定記錄在 SSL 記錄檔中資訊的詳細度。*level* 的數值如表 C-6 所列及說明。

表 C-6 SSL 記錄階層數值

數值	說明
`none`	不記錄，但仍會將錯誤訊息傳送到標準 Apache 錯誤記錄
`warn`	包含警告訊息
`info`	包含資訊訊息
`trace`	包含追蹤訊息
`debug`	包含除錯訊息

14. `SSLOptions [+-] option`

適用範圍：全域、虛擬主機、目錄、`.htaccess`

本指令會對每個目錄設定 SSL 執行時間選項。要將選項新增到目前組態中，請在前方加上加號 (+)；要移除，請在前方加上減號 (-)。如果同一目錄有多個選項時，將使用限制最嚴格的選項；這些選項是不會合併使用的。

選項與其描述如表 C-7 所列。

表 C-7 可用的 SSL 選項

選項	說明
`StdEnvVars`	建立標準的 SSL 相關環境變數組 — 這會導致效能衰減。
`ExportCertData`	導致匯出 `SSL_SERVER_CERT`、`SSL_CLIENT_CERT` 與 `SSL_CLIENT_CERT_CHAIN`*n* (*n* = 0, 1, ...) 環境變數。這些變數包含 PEM 編碼的用戶端與伺服器憑證。
`FakeBasicAuth`	用戶端憑證的辨別名稱 (DN) 會轉譯爲 HTTP 基本驗證使用者名稱 (Basic Authentication Username)，且會「假裝」爲有驗證。這可以在 SSL 用戶端認證上使用標準的 Apache 存取控制機制，而不提示使用者輸入密碼。 這些使用者在 Apache 密碼檔案中的項目必需使用加密密碼 `xxj31ZMTZzkVA`，這是「password」這個字的加密型態 (`crypt`(3c))。
`StrictRequire`	強制在 `SSLRequireSSL` 受拒絕時禁止存取，即使其他可能覆蓋本指令的指令如 `Satisfy Any` 存在。

15. `SSLRequireSSL`

適用範圍：目錄、`.htaccess`

本指令會禁止對特定目錄進行存取，除非使用的是 HTTPS。使用此指令可防止錯誤的組態造成未經驗證或未加密的存取權限使用目錄內容。

附錄 D

設定自訂應用程式以使用介面卡

本附錄說明介面卡隨附的軟體。此軟體可以用來建立 OpenSSL 相容應用程式，以利用介面卡的編碼加速功能。並非所有 OpenSSL 應用程式都會由這樣的編譯中獲益。某些應用程式可以使用原本的 OpenSSL 程式庫 (可以由 `http://www.openssl.org` 下載) 來建立，並可從中獲益。

設定自訂應用程式以使用介面卡

有關建立應用程式以使用 Sun Crypto Accelerator 4000 軟體與硬體的資訊，係以其「現狀」提供，並非本產品的正式支援部份。本資訊可能很有用，但不提供任何相關保固。如果您需要 Sun 支援的解決方案，請與 Sun Professional Services 聯繫，查看有哪些選擇。

▼ 設定自訂應用程式以使用介面卡

1. **安裝 `SUNWkcl2o` 套件，其中包含必要的標頭檔與程式庫。**
2. **將應用程式設定為包含 `/opt/SUNWconn/cryptov2/include` 的 OpenSSL 標題，例如包含下列編譯器旗標：**

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

3. **使連結器包含通往正確程式庫的參照。**

   多數 OpenSSL 相容應用程式會參照 `libcrypto.a` 與 `libssl.a` 程式庫之一，或兩者皆參照。請包含 Sun 編碼程式庫。下列連結器屬性可以用來達成目的：

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

附錄 **E**

軟體授權

本附錄提供 Sun 二進位代碼授權合約及協力廠商的軟體注意事項與授權。

注意 – 本附錄中提供的協力廠商授權與注意事項與軟體授權與注意事項擁有者提供的完全相同。

Sun Microsystems, Inc.

二進位代碼授權合約

在拆開軟體的媒體包裝之前，請仔細閱讀本合約條款及所有隨附的補充授權條款 (總稱為 「合約」)。拆開軟體的媒體包裝，表示您同意此合約所有條款。如果您要透過電子方式取得軟體，則可在此合約結尾處選擇 「接受」按鈕以接受這些條款。如果您不同意這所有這些條款，請立即將未用過的軟體退回至購買地點以獲得退款；如果透過電子方式取得軟體，則在此合約結尾選擇 「拒絕」。

1. 使用授權。透過支付多個使用者以及在電腦硬體等級上使用所需的相應費用，Sun 可爲您提供非專屬與非轉讓授權，僅限於內部使用隨附軟體與說明文件以及 Sun 提供的所有錯誤更正 (總稱爲 「軟體」)。

2. 限制。軟體屬於商業機密並具有著作權。軟體標題與所有相關智慧財產權爲 Sun 與/或其授權者擁有。除非任何補充授權條款中已特定授權，否則您不得複製軟體，也不得保存一份軟體副本。除非適用法律禁止執行，否則您不得修改、解編軟體或對軟體進行反向工程。您明瞭該軟體並非設計、授權或專用於設計、建造、操作或維護任何核心設備。Sun 否認對於此類用途適用性的所有明示或隱含的保固。根據本合約，Sun 或其授權者的所有商標、服務標記、標誌或商業名稱之權利或權益未獲許可。

3. 有限保固。Sun 提供自購買日起的九十 (90) 天保固 (以收據副本爲依據)，在此期限內，配備此軟體 (如果有的話) 的媒體在正常使用的情況下，將不會有材料和工藝上的缺陷。除上述條款外，軟體將以其 「現狀」提供。在此有限保固下，Sun 可以自行決定對您的專屬補償與 Sun 的全部責任，從而確定是否更換軟體媒體或退還購買軟體的費用。

4. **保固免責聲明。除非本合約特定說明，在所為免責聲明合法之限度以內，明示不為任何明示或暗示的條件、表示或保固負責，包括但不限於隱含的適銷性保固、特定用途的適用性與非侵權性。**

5. **責任限制。在法律許可範圍內，無論情況為何，SUN 或其授權者都不對任何因直接或間接使用本軟體而導致的收益、利潤或資料損失，或特殊、間接、繼發、偶發或懲罰性損害擔負任何責任，不論其起因、責任源由，即使 SUN 事前獲悉有此類損害的可能性也不例外。**根據本合約，不論在任何情況下，對於您購買軟體的超額花費，不論是否基於合約、過失 (包含怠忽) 或其他原因，Sun 均不負責。如果上述限制與上述保固條款衝突，以此限制爲准。

6. 有效期限。本合約在有效期限維持有效。您可以隨時銷毀軟體副本以終止本合約。如不遵守本合約中的任何條款，本合約將立即終止，恕 Sun 不另行通知。本合約終止時，您必須銷毀所有軟體副本。

7. 出口規定。根據本合約，所有軟體與技術資料遵守美國出口管制法，也遵守其他國家的進出口規定。您必須嚴格遵守這些法律與規定，以確保您在收到軟體後獲得出口、轉出口或進口所需的授權。

8. 美國政府有限權利。如果軟體由美國政府或其代表或美國政府主要承包商或分包商 (無論任何層級) 採購，則本合約中將事先說明軟體與隨附說明文件的政府權限；其根據係爲 48 CFR 227.7201 至 227.7202-4 (用於國防部 [DOD] 採購) 與 48 CFR 2.101 和 12.212 (用於非 DOD 採購)。

9. 準據法。與本合約相關的所有行爲均受加州法律與控制美國聯邦法律的約束。其他管轄區域的法規均不適用。

10. 其他考量事項。如果本合約中的任何條款爲不可強制執行，本合約將忽略該條款而仍然生效；如果忽略該條款會限制使用者的使用，則合約將在此情況下立即終止。

11. 總述。本合約是使用者與 Sun 所立有關其主題內容的完整合約。在本合約有效期限內，它將取代所有之前或同期的口頭或書面交流、提議、陳述及保固，如果發生條款衝突，或與任何引述、定制、承認的條款以及雙方有關其主題內容的其他交流不一致時，均以此合約爲準。除非經各方的授權代表撰寫並簽署，否則本合約中不包含任何修改內容。

如有任何疑問，請聯絡：Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054

(Form ID#011801)

Sun Microsystems, Inc.

Sun Crypto Accelerator 4000 補充條款

這些 Sun Crypto Accelerator 4000 補充條款是對二進位代碼授權合約 (「BCL」) 的補充。此處未定義的資本條款，其含義應歸類在 BCL 中。這些補充條款將取代 BCL 中所有不一致或發生衝突的條款。使用本軟體時，即表示您同意接受 BCL 的補充條款。

1. 協力廠商授權條款。本「軟體」之部份在提供時帶有管轄其使用之他方注意事項與/或授權。

協力廠商授權條款

OpenSSL 授權問題

OpenSSL 工具套件將同時受雙重授權管轄，亦即 OpenSSL 授權與原始 SSLeay 授權都適用於該工具套件。請參考下文以查閱實際的授權文字。實際上兩種授權都是 BSD 型態的「開放來源碼」授權。如果有任何與 OpenSSL 相關的授權問題，請聯絡：openssl-core@openssl.org。

OpenSSL 授權

來源程式碼或二進位程式碼的重新散佈與使用，不論是否經過修改，都在允許之列，但必須符合下列條件：

1. 來源程式碼必須保留上述著作權注意事項、本條件列表與下列免責聲明。
2. 以二進位格式進行的重新散佈必須在文件與/或其他隨散佈提供的資料中，重製上述著作權注意事項、本條件列表與下列免責聲明。
3. 所有提及本軟體之功能或使用的廣告材料，必須顯示下列聲明：「本產品包括由 OpenSSL Project 所開發的軟體，供 OpenSSL Toolkit 使用 (http://www.openssl.org/)。」
4. 未經事前書面同意，「OpenSSL Toolkit」與「OpenSSL Project」等名稱不得用於推薦或促銷本軟體之衍生產品。要取得書面同意，請聯絡 openssl-core@openssl.org。
5. 未經 OpenSSL Project 書面同意，由本軟體衍生之產品不得稱爲「OpenSSL」，「OpenSSL」字樣也不得出現在產品名稱中。
6. 任何型態的重新散佈必需包含下列聲明：「本產品包括由 OpenSSL Project 所開發的軟體，供 OpenSSL Toolkit 使用 (http://www.openssl.org/)。」

本軟體由 OpenSSL PROJECT 以其「現狀」提供，所有明示或暗示之保固，包括但不限於隱含的適銷性保固、特定用途的適用性，皆在免責聲明之列。不管在任何情況下，OpenSSL PROJECT 或其貢獻者都不對任何因使用本軟體而導致之直接、間接、偶發、特殊、典型或繼發性損害 (包括但不限於：替代性物品或服務的取得，使用時間、資料或利益的喪失，或業務的中斷) 擔負任何責任，不論其起因、責任源由，亦不論是否基於合約、嚴格責任或過失 (包含怠忽或其他原因)，即使事前獲悉該等損害的可能性也不例外。

本產品包含由 Eric Young (eay@cryptsoft.com) 所撰寫的加密軟體。本產品包含由 Tim Hudson (tjh@cryptsoft.com) 所撰寫的軟體。

原始 SSLeay 授權

著作權所有 (C) 1995-1998 年 Eric Young (eay@cryptsoft.com) 所有權利均予保留。

本套件是 Eric Young (eay@cryptsoft.com) 撰寫的 SSL 實作。本實作撰寫是以符合 Netscape SSL 的標的撰寫。

在符合下列條件的情況下，本程式庫將可以免費提供商務與非商務使用。下列條件適用於本散佈中所有的程式碼，含：RC4、RSA、lhash、DES 等程式碼，而不僅限於 SSL 程式碼。本散佈中包含的 SSL 文件受相同著作權條款的涵蓋，但著作權所有人爲 Tim Hudson (tjh@cryptsoft.com)。

著作權仍歸 Eric Young 所有，因此程式碼中之著作權注意事項不得移除。

如果將本套件應用在產品中，應公開聲明 Eric Young 爲所用程式庫部分的作者。這可以是程式啓動時的文字訊息、或套裝軟體提供的 (線上或書面) 文件。

來源程式碼或二進位程式碼的重新散佈與使用，不論是否經過修改，都在允許之列，但必須符合下列條件：

1. 來源程式碼的重新散佈必須保留著作權注意事項、本條件列表與下列免責聲明。
2. 以二進位格式進行的重新散佈必須在文件與/或其他隨散佈提供的資料中，重製上述著作權注意事項、本條件列表與下列免責聲明。
3. 所有提及本軟體之功能或使用的廣告材料，必須顯示下列聲明：「本產品包含由 Eric Young (eay@cryptsoft.com) 所撰寫的編碼軟體。」如果所使用的程式庫與編碼並無相關，則「編碼」一詞可以省略。:-)
4. 如果您由 apps 目錄加入任何 Windows 專屬程式碼 (或其衍生產品) (稱爲應用程式碼)，您必須加入下列聲明：「本產品包含由 Tim Hudson (tjh@cryptsoft.com) 所撰寫之軟體。」

此軟體由 ERIC YOUNG 以其「現狀」提供，所有明示或暗示之保固，包括但不限於隱含的適銷性保固、特定用途的適用性，皆在免責聲明之列。不管在任何情況下，作者都不對任何因使用本軟體而導致之直接、間接、偶發、特殊、典型或繼發性損害 (包含但不限於：替代性物品或服務的取得，使用時間、資料或利益的喪失，或業務的中斷) 負任何責任，不論其起因、責任源由，亦不論是否基於合約、嚴格責任或過失 (包含怠忽或其他原因)，即使被事前告知該等損害的可能性也不例外。

本程式碼任何公開或衍生版本的授權與散佈條款皆不得變更。例如，本程式碼不得複製並加入其他散佈授權之下 (含 GNU 公開授權)。

> 「Ian Fleming 是 UNIX 迷！
> 我怎麼知道？唔，詹姆士龐德
> 擁有 (殺人執照) 編號 007，
> 也就是說，他可以處決任何人。」
> -- 佚名

MOD_SSL 授權

mod_ssl 套件適用「開放來源碼軟體」標籤，因其以 BSD 型態授權散佈。詳細的授權資訊如下。

版權所有 (c) 1998-2000 年 Ralf S. Engelschall 書面同意，由本軟體衍生之產品不得稱爲「mod_ssl」，「mod_ssl」字樣也不得出現在產品名稱中。所有權利均予保留。

來源程式碼或二進位程式碼的重新散佈與使用，不論是否經過修改，都在允許之列，但必須符合下列條件：

1. 來源程式碼必須保留上述著作權注意事項、本條件列表與下列免責聲明。

2. 以二進位格式進行的重新散佈必須在文件與/或其他隨散佈提供的資料中，重製上述著作權注意事項、本條件列表與下列免責聲明。

3. 所有提及本軟體之功能或使用的廣告材料，必須顯示下列聲明：「本產品包含由 Ralf S. Engelschall <rse@engelschall.com> 所開發的軟體，供 mod_ssl 計劃使用 (http://www.modssl.org/)。」

4. 未經事前書面同意，「mod_ssl」一詞不得用於推薦或促銷本軟體之衍生產品。要取得書面同意，請聯絡 rse@engelschall.com。

5. 未經 Ralf S. Engelschall 書面同意，由本軟體衍生之產品不得稱爲「mod_ssl」，「mod_ssl」字樣也不得出現在產品名稱中。

6. 任何型態的重新散佈必須包含下列聲明：「本產品包含由 Ralf S. Engelschall <rse@engelschall.com> 所開發的軟體，供 mod_ssl 計劃使用 (http://www.modssl.org/)。」

本軟體由 RALF S. ENGELSCHALL 以其「現狀」提供，所有明示或暗示之保固，包括但不限於隱含的適銷性保固、特定用途的適用性，皆在免責聲明之列。不管在任何情況下，RALF S. ENGELSCHALL 或其貢獻者都不對任何因使用本軟體而導致之直接、間接、偶發、特殊、典型或繼發性損害 (包含但不限於：替代性物品或服務的取得，使用時間、資料或利益的喪失，或業務的中斷) 擔負任何責任，不論其起因、責任源由，亦不論是否基於合約、嚴格責任或過失 (包含怠忽或其他原因)，即使事前獲悉該等損害的可能性也不例外。

附錄 **F**

說明頁

本附錄將說明 Sun Crypto Accelerator 4000 指令與介面卡軟體中提供的公用程式，並列出其線上說明頁。

線上說明頁可以使用下列指令加以檢視：

```
man -M /opt/SUNWconn/man pagename
```

表 F-1 列出並說明了可用的線上說明頁。

表 F-1 Sun Crypto Accelerator 4000 線上說明頁

man 說明頁	說明
vca(7d)	爲下層硬體編碼加速器提供存取控制功能的 leaf 驅動程式
vcad(1m)	提供金鑰庫服務的監控程序
vcaadm(1m)	用於操控與介面卡關聯的組態、帳號及金鑰資料庫之公用程式
vcadiag(1m)	可讓超級使用者重設介面卡、將金鑰資料化零及執行基本診斷的公用程式
kcl2(7d)	kcl2 是一個核心模組，可對編碼硬體驅動程式提供支援。
apsslcfg(1m)	Apache 網站伺服器的組態公用程式
iplsslcfg(1m)	Sun ONE 網站伺服器的組態公用程式
pk11export(1m)	使用 PKCS#11 介面的金鑰匯出公用程式

附錄 G

將硬體化零

本附錄說明如何將 Sun Crypto Accelerator 4000 介面卡硬體化零。該程序會將介面卡恢復爲原廠狀態。介面卡恢復爲原廠狀態後，即處於 Failsafe 模式。

警告 – 僅在確實需要時，您才可以將硬體化零。如果您只需要移除所有金鑰資料，請在 `vcaadm` 程式中使用 `zeroize` 指令將軟體化零。請參閱第 74 頁的「對介面卡執行軟體化零」以取得有關 `zeroize` 指令的詳細資料，另請參閱線上說明頁中的 `vcadiag(4)` 以瞭解如何移除所有金鑰資料。

注意 – 對介面卡執行硬體化零程序會移除 Sun Crypto Accelerator 4000 韌體。您必須重新安裝 Sun Crypto Accelerator 4000 軟體隨附的韌體。

將 Sun Crypto Accelerator 4000 硬體化零爲原廠狀態

在某些情況下，您可能需要將介面卡恢復爲 `failsafe` 模式，並清除所有金鑰資料與組態資訊。只能使用標準 SCSI 硬體跳線 (跳線帽) 完成此操作。

注意 – 您可以使用 `zeroize` 指令與 `vcaadm` 程式從 Sun Crypto Accelerator 4000 介面卡中移除所有金鑰資料。但是，`zeroize` 指令將使任何更新的韌體保持不變。請參閱第 74 頁的「對介面卡執行軟體化零」。另請參閱 `vcadiag(4)` 線上說明頁。

▼ 使用硬體跳線將 Sun Crypto Accelerator 4000 介面卡化零

1. **關閉系統電源。**

注意 – 對於某些系統，您可以在本程序中使用動態重新組態 (DR) 以移除並裝回介面卡，而不是關閉系統電源。請參閱系統隨附文件以瞭解正確的 DR 程序。

警告 – 在調整跳線時，介面卡必須切斷所有電源。

---

2. **卸下電腦護蓋以便於操作位於介面卡中上部的跳線。**

3. **將跳線帽置於跳線針腳 1 與 2。**

針腳 1 與 2 是最靠近托架的針腳。總共有四對兩個一組的針腳。請將跳線置於 1 與 2 號針腳，如圖 G-1 所示。

警告 – 將跳線置於針腳 1 與 2 時，介面卡將無法正常運作。

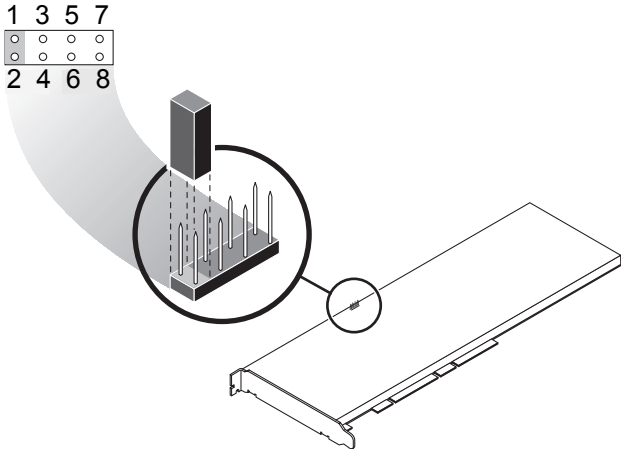

圖 G-1 硬體跳線帽針腳

4. **開啟系統電源。**

警告 – 調整硬體跳線並開啓系統電源後，將會刪除所有韌體、金鑰資料及組態資訊。此程序會將介面卡恢復爲原廠狀態，並將介面卡置於 Failsafe 模式。

---

5. **關閉系統電源。**
6. **移除跳線針腳 1 與 2 的跳線帽，使跳線回復原來位置。**
7. **開啟系統電源。**
8. **使用 `vcaadm` 連接至 Sun Crypto Accelerator 4000 介面卡。**

   `vcaadm` 將提示您升級韌體的路徑。
9. **鍵入 `/opt/SUNWconn/cryptov2/firmware/sca4000fw` 作為安裝韌體的路徑。**

   韌體會自動安裝，您將登出 `vcaadm`。
10. **使用 `vcaadm` 重新連接至 Sun Crypto Accelerator 4000 介面卡。**

    `vcaadm` 會提示您使用新金鑰庫初始化介面卡，或使用現有金鑰庫初始化介面卡。請參閱第 62 頁的「使用 `vcaadm` 初始化介面卡」。

索引

十一劃

十二劃

十三劃

十四劃

十五劃

十六劃

十七劃