Guide de l'utilisateur et d'installation de la carte Crypto Accelerator 4000 de Sun™

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054 Etats-Unis
650-960-1300

Référence n° 817-2326-10
mai 2003, révision A

Envoyez vos commentaires concernant ce document à l'adresse : docfeedback@sun.com

Produit
Recyclable

Declaration of Conformity (Fiber MMF)

Compliance Model Number: Venus-FI
Product Family Name: Crypto Accelerator 4000 de Sun - 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: Crypto Accelerator 4000 de Sun - 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。

Table des matières

Tableaux

Préface

Le *Guide de l'utilisateur et d'installation de la carte Crypto Accelerator 4000 de Sun* répertorie les fonctions, protocoles et interfaces de la carte Sun™ Crypto Accelerator 4000 et décrit les procédures d'installation, de configuration et de gestion de la carte sur votre système.

Ce guide est conçu pour les administrateurs réseau possédant une expérience dans la configuration de l'environnement d'exploitation Solaris™, des plates-formes Sun équipées de cartes d'E/S PCI, des serveurs Web ONE et Apache de Sun™, du protocole IPsec ou du logiciel SunVTS™, ainsi que dans l'acquisition d'autorités de certification.

Présentation du manuel

Le manuel est composé des chapitres suivants :

- Le chapitre 1 répertorie les fonctions, protocoles et interfaces de la carte Crypto Accelerator 4000 de Sun et décrit les conditions matérielles et logicielles requises.
- Le chapitre 2 décrit les procédures d'installation et de retrait de la carte Crypto Accelerator 4000 de Sun.
- Le chapitre 3 définit les paramètres réglables du pilote de la carte Crypto Accelerator 4000 de Sun et décrit les procédures de configuration à l'aide de l'utilitaire `ndd` et du fichier `vca.conf`. Ce chapitre décrit également comment activer l'auto-négociation ou le mode forcé pour les paramètres de liaison à l'interface OpenBoot™ PROM et comment configurer le fichier réseau `hosts`.
- Le chapitre 4 décrit les procédures de configuration de la carte Crypto Accelerator 4000 de Sun et de gestion des stockages de clés à l'aide des utilitaires `vcaadm` et `vcadiag`.

- Le chapitre 5 explique les procédures de configuration de la carte Crypto Accelerator 4000 de Sun pour une utilisation avec les serveurs Web Sun ONE.
- Le chapitre 6 explique la procédure de configuration de la carte Crypto Accelerator 4000 de Sun pour une utilisation avec les serveurs Web Apache.
- Le chapitre 7 décrit la procédure de test de la carte Crypto Accelerator 4000 de Sun à l'aide de l'application de diagnostic SunVTS et de l'autotest embarqué FCode. Ce chapitre propose également des techniques de dépannage à l'aide des commandes OpenBoot PROM.
- L'annexe A répertorie les spécifications de la carte Crypto Accelerator 4000 de Sun.
- L'annexe B répertorie les directives d'utilisation du logiciel de la Crypto Accelerator 4000 de Sun pour configurer la prise en charge SSL pour les serveurs Web Apache.
- L'annexe C traite du logiciel fourni avec la carte Crypto Accelerator 4000 de Sun et aborde les méthodes de conception d'applications compatibles avec OpenSSL afin de bénéficier des fonctions d'accélération cryptographique de la carte.
- L'annexe D traite des consignes et des licences logicielles émanant d'autres entreprises régissant l'utilisation de logiciels tiers utilisés avec la carte Crypto Accelerator 4000 de Sun.
- L'annexe E décrit les commandes de la Crypto Accelerator 4000 de Sun et répertorie les pages manuel en ligne pour chacune de ces commandes.
- L'annexe F décrit la procédure de remise à zéro de la carte Crypto Accelerator 4000 de Sun telle qu'elle l'était à sa sortie d'usine, correspondant au mode `failsafe` de la carte.
- L'annexe G fournit des réponses aux questions fréquemment posées.

Utilisation des commandes UNIX

Ce document ne contient pas d'informations sur les commandes et procédures de base UNIX®, telles que l'arrêt du système, l'amorçage du système ou la configuration des périphériques.

Pour plus d'informations, consultez la documentation suivante :

- *Guide de la plate-forme matérielle Solaris*
- Documentation en ligne relative à l'environnement d'exploitation Solaris, disponible à l'adresse `http://docs.sun.com`
- Toute autre documentation sur les logiciels livrée avec votre système

Conventions typographiques

Police	Description	Exemples
`AaBbCc123`	Noms de commandes, fichiers et répertoires. Messages apparaissant à l'écran.	Modifiez votre fichier `.login`. Utilisez `ls -a` pour afficher la liste de tous les fichiers. `% Vous avez reçu du courrier.`
`AaBbCc123`	Ce que l'utilisateur tape par opposition aux messages apparaissant à l'écran.	`% su` `Mot de passe :`
AaBbCc123	Titres de guide, nouveaux mots ou termes, mots à mettre en valeur.	Consultez le chapitre 6 du *Guide de l'utilisateur.* Il s'agit d'options de *catégorie*. Vous *devez* être superutilisateur pour effectuer cette opération.
	Variable de ligne de commande, à remplacer par une valeur ou un nom réel.	Pour supprimer un fichier, entrez `rm` *nomfichier.*

Invites Shell

Shell	Invite
C shell	*nom_machine*%
C shell superutilisateur	*nom_machine*#
Bourne shell et Korn shell	$
Bourne shell et Korn shell superutilisateur	#

Accès à la documentation de Sun en ligne

Vous pouvez visualiser, imprimer ou acheter un large choix de documentation Sun, dont des versions localisées, à l'adresse :

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

Vos commentaires sont les bienvenus chez Sun

Dans le souci d'améliorer notre documentation, tous vos commentaires et suggestions sont les bienvenus. N'hésitez pas à nous les faire parvenir à l'adresse suivante :

`docfeedback@sun.com`

Mentionnez le numéro de référence (817-2326-10) de votre documentation dans l'objet de votre message électronique.

CHAPITRE 1

Présentation du produit

Ce chapitre présente la carte Crypto Accelerator 4000 de Sun et comprend les sections suivantes :

Caractéristiques du produit

La carte Crypto Accelerator 4000 de Sun est une carte d'interface réseau Gigabit Ethernet qui prend en charge l'accélération matérielle cryptographique pour IPsec et SSL (symétrique et asymétrique) sur les serveurs Sun. Outre le fait qu'elle fonctionne comme une carte d'interface réseau Gigabit Ethernet normale pour le trafic réseau non chiffré, la carte contient un matériel cryptographique permettant de prendre en charge un débit du trafic IPsec chiffré plus élevé que la solution logicielle standard.

Protocoles et interfaces clés

La carte Crypto Accelerator 4000 de Sun est compatible avec le matériel Ethernet existant avec un format de trame et une taille de trame minimale et maximale (64 à 1 518 octets) Ethernet standard et conforme aux normes et aux protocoles standard suivants :

- PCI 33/66 Mhz, 32/64 bits, taille réelle
- CSMA/CD IEEE 802.3 (Ethernet)
- LLC IEEE 802.2
- SNMP (MIB limitée)
- Interface Gigabit Ethernet intégrale et semi-duplex (IEEE 802.z)
- Signalisation de tension universelle double (3,3 V et 5 V)

Fonctionnalités clés

- Interface Gigabit Ethernet en cuivre ou en fibre.
- Accélère les fonctions cryptographiques IPsec et SSL.
- Fréquence d'établissement de session : jusqu'à 4 300 opérations par seconde.
- Fréquence de chiffrement de masse : jusqu'à 800 Mbits/s.
- Chiffrement RSA jusqu'à 2 048 bits.
- Chiffrement de données de masse 3DES jusqu'à 10 fois plus rapide.
- Fournit une clé de sécurité et une administration de certificats centralisées et inviolables pour le serveur Web Sun ONE pour une sécurité accrue et une gestion de clé simplifiée.
- Conçue pour la certification FIPS 140-2 de niveau 3.
- Faible utilisation de l'unité centrale ; libère les ressources système et la bande passante du serveur.
- Gestion et stockage sécurisés de la clé privée.
- Prise en charge de la fonctionnalité Dynamic Reconfiguration et de la redondance/défaillance sur les serveurs de pointe et de capacité moyenne.
- Equilibrage de la charge pour les paquets RX sur plusieurs unités centrales.
- Prise en charge intégrale des commandes de flux (IEEE 802.3x).

Les cartes Crypto Accelerator 4000 de Sun sont conformes aux normes de sécurité pour les modules cryptographiques, conformément aux directives de la norme FIPS (Federal Information Processing Standard) 140-2, niveau 3.

Applications prises en charge

- Environnements d'exploitation Solaris 8 et 9 (IPsec VPN)
- Serveur Web Sun ONE
- Serveur Web Apache

Protocoles cryptographiques pris en charge

La carte prend en charge les protocoles suivants :

- IPsec pour IPv4 et IPv6, y compris IKE ;
- SSLv2, SSLv3, TLSv1.

La carte accélère les fonctions IPsec suivantes :

- Chiffrement ESP (DES, 3DES).

La carte accélère les fonctions SSL suivantes :

- Etablissement sécurisé d'un jeu de paramètres cryptographiques et de clés secrètes entre un client et un serveur.
- Stockage de la clé sécurisée sur la carte ; les clés sont chiffrées quand elles quittent la carte.

Prise en charge de diagnostic

- Test automatique exécutable par l'utilisateur à l'aide d'OpenBoot™ PROM
- Tests de diagnostic SunVTS™

Accélération de l'algorithme cryptographique

La carte Crypto Accelerator 4000 de Sun accélère les algorithmes cryptographiques à la fois logiciels et matériels. Des coûts d'accélération des algorithmes cryptographiques différents pour chaque algorithme expliquent la complexité de leurs caractéristiques. Certains algorithmes cryptographiques ont été spécialement conçus pour être implémentés sur du matériel, d'autres sur du logiciel. De plus, une accélération matérielle implique un coût supplémentaire pour le déplacement de données de l'application de l'utilisateur vers le périphérique d'accélération matérielle, puis en sens inverse pour le ré-acheminement des résultats. Notez que quelques algorithmes cryptographiques peuvent être traités par un logiciel hautement optimisé aussi rapidement que par du matériel dédié.

Algorithmes cryptographiques pris en charge

Le pilote Crypto Accelerator 4000 de Sun (`vca`) examine chaque requête cryptographique et détermine le meilleur emplacement pour l'accélération (processeur hôte ou Crypto Accelerator 4000 de Sun), afin de parvenir à un débit maximal. La distribution de la charge dépend de l'algorithme cryptographique, du chargement en cours et de la taille des données.

La carte Crypto Accelerator 4000 de Sun accélère les algorithmes IPsec suivants.

TABLEAU 1-1 Algorithmes cryptographiques IPsec

Type	Algorithme
Symétrique	DES, 3DES

La carte Crypto Accelerator 4000 de Sun accélère les algorithmes SSL suivants.

TABLEAU 1-2 Algorithmes cryptographiques SSL

Type	Algorithme
Symétrique	DES, 3DES, ARCFOUR
Asymétrique	Diffie-Hellman (Apache uniquement) et RSA (clé jusqu'à 2 048 bits), DSA
Hachage	MD5, SHA1

Accélération SSL

Le TABLEAU 1-3 indique quels algorithmes SSL accélérés peuvent être délégués au matériel et quels algorithmes logiciels sont fournis pour les serveurs Web Sun ONE et Apache.

TABLEAU 1-3 Algorithmes SSL pris en charge

	Serveurs Web Sun ONE		Serveurs Web Apache	
Algorithme	**Matériel**	**Logiciel**	**Matériel**	**Logiciel**
RSA	X	X	X	X
DSA	X	X	X	X
ARCFOUR		X		
Diffie-Hellman			X	X
DES	X	X	X	X
3DES	X	X	X	X
MD5	X	X		
SHA1	X	X		

Chiffrement de masse

La fonctionnalité de chiffrement de masse de Crypto Accelerator 4000 de Sun pour le logiciel du serveur Sun ONE est désactivée par défaut. Vous devez l'activer manuellement en créant un fichier et en redémarrant le logiciel du serveur Sun ONE.

Pour activer le logiciel du serveur Sun ONE pour qu'il utilise le chiffrement de masse sur la carte Crypto Accelerator 4000 de Sun, créez simplement un fichier vide nommé `sslreg` dans le répertoire `/etc/opt/SUNWconn/cryptov2/` et redémarrez le logiciel du serveur.

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

Pour désactiver la fonctionnalité de chiffrement de masse, supprimez le fichier `sslreg` et redémarrez le logiciel du serveur.

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

La fonctionnalité de chiffrement de masse pour le logiciel du serveur Web Apache est activée par défaut et ne peut pas être désactivée.

Présentation du matériel

Le matériel Crypto Accelerator 4000 de Sun est un adaptateur PCI Gigabit Ethernet accélérateur cryptographique de taille réelle (10,668 x 31,199 cm) qui améliore les performances IPsec et SSL sur les serveurs Sun.

Accélération matérielle IPsec

La carte Crypto Accelerator 4000 de Sun chiffre et déchiffre les paquets IPsec dans le matériel, en déchargeant cette opération de surcharge élevée du processeur SPARC™. Le matériel cryptographique prend également en charge les opérations cryptographiques asymétriques et symétriques générales pour les utiliser dans d'autres applications et comprend une source matérielle de numéros aléatoires.

Remarque – Aucune configuration ni aucun paramétrage IPsec ne sont requis pour utiliser la carte Crypto Accelerator 4000 de Sun pour l'accélération IPsec. Il vous suffit d'installer les progiciels Crypto Accelerator 4000 de Sun et de redémarrer l'ordinateur.

Une fois les progiciels et la carte Crypto Accelerator 4000 de Sun installés, les configurations IPsec existantes ou ultérieures utiliseront la carte Crypto Accelerator 4000 de Sun plutôt que le logiciel Solaris fourni. La carte gère tous les algorithmes IPsec pris en charge répertoriés dans le TABLEAU 1-1. Les algorithmes IPsec non pris en charge par la carte Crypto Accelerator 4000 de Sun seront toujours gérés par le logiciel de chiffrement Solaris fourni. La configuration d'IPsec est détaillée dans le *Guide d'administration système* de la documentation Solaris System Administrator Collection accessible à l'adresse suivante : `http://docs.sun.com`.

Adaptateur MMF Crypto Accelerator 4000 de Sun

L'adaptateur MMF Crypto Accelerator 4000 de Sun est une carte bus PCI à fibres optiques Gigabit Ethernet à port unique. Il fonctionne uniquement sur les réseaux Ethernet 1 000 Mbits/s.

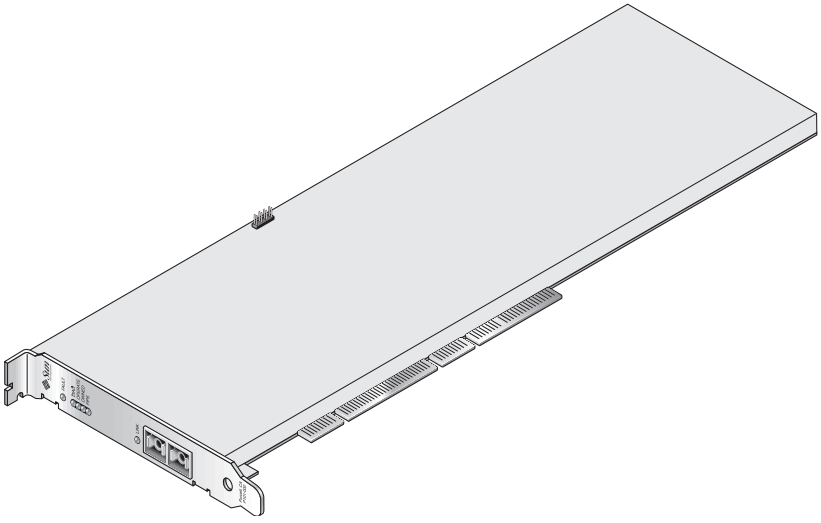

FIGURE 1-1 Adaptateur MMF Crypto Accelerator 4000 de Sun

Ecrans à cristaux liquides

Voir le TABLEAU 1-4.

TABLEAU 1-4 Ecrans à cristaux liquides du panneau avant pour l'adaptateur MMF

Nom	Signification si allumé	Couleur
Fault	Allumé si la carte est dans un état HALTED (erreur fatale) ou si l'initialisation matérielle de faible niveau a échoué. Clignotant si une erreur est survenue au cours du processus de réinitialisation.	Rouge
Diag	Allumé s'il y a un état POST, DIAGNOSTICS ou FAILSAFE (microprogramme non mis à niveau). Clignotant lorsque DIAGNOSTICS est en cours.	Vert
Operate	Allumé s'il y a un état POST, DIAGNOSTICS ou DISABLED (pilote non attaché). Clignotant s'il y a un état IDLE, OPERATIONAL ou FAILSAFE.	Vert
Owned	Allumé si le responsable de la sécurité a initialisé la carte avec `vcaadm`. Voir la section « Initialisation de la Carte Crypto Accelerator 4000 de Sun avec `vcaadm` », page 68. Clignotant si le cavalier ZEROIZE est présent.	Vert
FIPS Mode	Allumé lors d'un fonctionnement en mode certifié FIPS 140-2 niveau 3. Eteint en mode autre que FIPS.	Vert
Link	Etablissement de liaison.	Vert

Adaptateur UTP Crypto Accelerator 4000 de Sun

L'adaptateur UTP Crypto Accelerator 4000 de Sun est une carte bus PCI en alliage cuivre Gigabit Ethernet à port unique. Il peut être configuré pour fonctionner sur des réseaux Ethernet 10, 100 ou 1 000 Mbits/s.

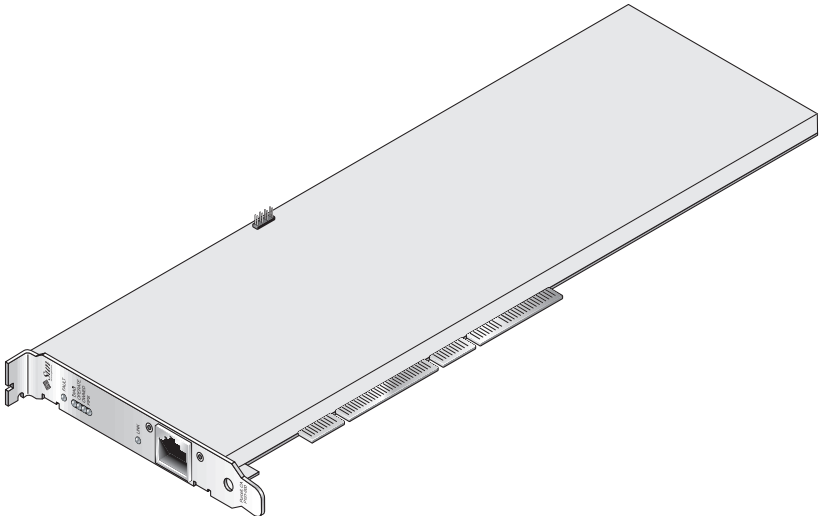

FIGURE 1-2 Adaptateur UTP Crypto Accelerator 4000 de Sun

Ecrans à cristaux liquides

Voir le TABLEAU 1-5.

TABLEAU 1-5 Ecrans à cristaux liquides du panneau avant pour l'adaptateur UTP

Nom	Signification si allumé	Couleur
Fault	Allumé si la carte est dans un état HALTED (erreur fatale) ou si l'initialisation matérielle de faible niveau a échoué. Clignotant si une erreur est survenue au cours du processus de réinitialisation.	Rouge
Diag	Allumé s'il y a un état POST, DIAGNOSTICS ou FAILSAFE (microprogramme non mis à niveau). Clignotant lorsque DIAGNOSTICS est en cours.	Vert
Operate	Allumé s'il y a un état POST, DIAGNOSTICS ou DISABLED (pilote non attaché). Clignotant s'il y a un état IDLE, OPERATIONAL ou FAILSAFE.	Vert
Owned	Allumé si le responsable de la sécurité a initialisé la carte avec `vcaadm`. Voir la section « Initialisation de la Carte Crypto Accelerator 4000 de Sun avec `vcaadm` », page 68. Clignotant si le cavalier ZEROIZE est présent.	Vert
FIPS Mode	Allumé lors d'un fonctionnement en mode certifié FIPS 140-2 niveau 3. Eteint en mode autre que FIPS.	Vert
1 000 (aucun nom)	Indique Gigabit Ethernet.	Vert
Activité (aucun nom)	La liaison est en cours de transmission ou de réception.	Orange
Liaison	Etablissement de liaison.	Vert

Remarque – Le numéro du service pack (SP9 ou SP1) est indiqué chaque fois que le serveur Web Sun ONE 4.1 ou 6.0 est mentionné.

Dynamic Reconfiguration et High Availability

Le matériel Crypto Accelerator 4000 de Sun et le logiciel associé fournissent une capacité de fonctionnement efficace sur les plates-formes Sun qui prennent en charge la fonctionnalité Dynamic Reconfiguration (DR) et les connexions à chaud. Dans le cas où une opération de DR ou de connexion à chaud est réalisée, la couche logicielle de la carte Crypto Accelerator 4000 de Sun détecte automatiquement l'ajout ou la suppression d'une carte et règle les algorithmes de programmation en fonction des ressources matérielles.

Pour les configurations High Availability (HA), plusieurs cartes Crypto Accelerator 4000 de Sun peuvent être installées dans un système ou un domaine, afin de garantir la disponibilité constante de l'accélération matérielle. Dans le cas peu probable d'une panne du matériel Crypto Accelerator 4000 de Sun, la couche logicielle détecte la panne et supprime la carte concernée de la liste des accélérateurs cryptographiques matériels disponibles. Le logiciel Crypto Accelerator 4000 de Sun paramètre les algorithmes de programmation en fonction de la réduction des ressources matérielles. Les requêtes cryptographiques suivantes seront programmées sur les cartes restantes.

Notez que le matériel Crypto Accelerator 4000 de Sun fournit une source d'entropie de haute qualité pour la création de clés de longue durée. Si toutes les cartes Crypto Accelerator 4000 de Sun au sein d'un même domaine ou système sont supprimées, les clés de longue durée sont créées avec une entropie de qualité plus faible.

Partage de charge

Le logiciel Crypto Accelerator 4000 de Sun répartit la charge sur toutes les cartes installées sur le domaine ou le système Solaris. Les requêtes cryptographiques entrantes sont réparties selon des files d'attente de longueur fixe. Elles sont dirigées vers la première carte, jusqu'à ce que cette dernière atteigne sa capacité maximale. A ce moment, les requêtes supplémentaires sont dirigées vers la prochaine carte disponible qui peut accepter ce type de requêtes. Le mécanisme de mise en attente a été conçu pour optimiser le débit en simplifiant le regroupement des requêtes sur une carte.

Conditions logicielles et matérielles requises

Le TABLEAU 1-6 résume les conditions logicielles et matérielles requises pour l'adaptateur Crypto Accelerator 4000 de Sun.

TABLEAU 1-6 Conditions logicielles et matérielles requises

Matériel et logiciel	Conditions requises
Matériel	Sun Fire™ V120, V210, V240, 280R, V480, V880, 4800, 4810, 6800, 12K, 15K ; Netra™ 20 (lw4) ; Sun Blade™ 100, 150, 1000, 2000.
Environnement d'exploitation	Solaris 8 2/02 et versions compatibles ultérieures (Solaris 9 est requis pour l'accélération IPsec).

Correctifs requis

Reportez-vous aux *Notes de version de la Carte Crypto Accelerator 4000 de Sun* pour des informations supplémentaires sur le correctif requis.

Les correctifs suivants sont requis pour exécuter la carte Crypto Accelerator 4000 de Sun sur votre système. Les mises à jour de Solaris comportent les correctifs des versions précédentes. Utilisez la commande `showrev -p` pour déterminer si les correctifs énumérés ont déjà été installés.

Vous pouvez télécharger les correctifs à partir du site Web suivant : `http://sunsolve.sun.com`.

Installez la dernière version des correctifs. Le numéro comportant un tiret (-01, par exemple) augmente à chaque nouvelle version du correctif. Si le numéro de version sur le site Web est supérieur à celui indiqué dans les tableaux suivants, il s'agit tout simplement d'une version ultérieure.

Si le correctif dont vous avez besoin n'est pas disponible sur SunSolve℠, contactez un représentant du personnel commercial ou technique.

Correctif du serveur Web Apache

Si vous prévoyez d'utiliser le serveur Web Apache, installez également le correctif 109234-09. Une fois le progiciel `SUNWkcl2a` installé, le système sera configuré avec mod_ssl 1.3.26 du serveur Web Apache.

Correctifs Solaris 8

Les tableaux suivants répertorient les correctifs Solaris 8 requis et recommandés, à utiliser avec ce produit. Le TABLEAU 1-7 répertorie et décrit les correctifs requis.

TABLEAU 1-7 Correctifs Solaris 8 requis pour le logiciel Crypto Accelerator 4000 de Sun

Numéro de correctif	Description
110383-01	`libnvpair`
108528-05	`KU-05` (prise en charge `nvpair`)
112438-01	`/dev/random`

Correctifs Solaris 9

Il n'existe actuellement aucun correctif Solaris 9 requis.

CHAPITRE **2**

Installation de la Carte Crypto Accelerator 4000 de Sun

Ce chapitre décrit les procédures d'installation logicielle et matérielle de la carte Crypto Accelerator 4000 de Sun. Il est composé des sections suivantes :

Manipulation de la carte

Chaque carte est emballée dans un sachet antistatique spécial qui la protège lors de l'expédition et du stockage. Pour éviter d'endommager les composants de la carte avec l'électricité statique présente sur votre corps, réduisez cette dernière avant de toucher la carte en utilisant l'une des méthodes suivantes :

- Touchez la partie métallique de l'ordinateur.
- Fixez un bracelet antistatique à votre poignet et à une surface métallique mise à la terre.

Attention – Pour éviter d'endommager les composants de la carte sensibles à l'électricité statique, portez un bracelet antistatique pendant la manipulation de la carte, tenez-la par les bords uniquement et placez-la toujours sur une surface antistatique (comme le sachet en plastique qui la contenait).

Installation de la carte

L'installation de la carte Crypto Accelerator 4000 de Sun consiste à l'insérer dans le système et à charger les outils logiciels. Les instructions d'installation matérielle abordent uniquement les étapes générales à suivre pour installer la carte. Reportez-vous à la documentation fournie avec votre système pour connaître les instructions d'installation spécifiques.

▼ Pour installer le matériel

1. **En tant que superutilisateur, suivez les instructions fournies avec votre système pour éteindre votre ordinateur et le mettre hors tension, déconnecter le cordon d'alimentation et retirer le couvercle de l'ordinateur.**
2. **Recherchez un emplacement PCI disponible (de préférence un emplacement de 64 bits, 66 MHz).**
3. **Fixez un bracelet antistatique à votre poignet et à une surface métallique mise à la terre.**
4. **A l'aide d'un tournevis Phillips, retirez la vis du couvercle de l'emplacement PCI.**

   Mettez-la de côté en vue de fixer le support à l'étape 5.
5. **En tenant la carte Crypto Accelerator 4000 de Sun par le bord uniquement, retirez-la de son emballage et insérez-la dans l'emplacement PCI. Fixez ensuite la vis à l'arrière du support.**
6. **Replacez le couvercle de l'ordinateur, reconnectez le cordon d'alimentation et mettez le système sous tension.**
7. **Assurez-vous que la carte est correctement installée en exécutant la commande `show-devs` à l'invite `ok` d'OpenBoot™ PROM (OBP) :**

```
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
.
```

Dans l'exemple précédent, `/pci@8,600000/network@1` identifie le chemin du périphérique vers la carte Crypto Accelerator 4000 de Sun. Chaque carte du système sera associée à une ligne de ce type.

Pour déterminer si les propriétés du périphérique Crypto Accelerator 4000 de Sun sont correctement répertoriées : dans l'invite `ok`, naviguez jusqu'au chemin du périphérique et saisissez `.properties` pour afficher la liste des propriétés.

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

```
max-latency               00000040
min-grant                 00000040
subsystem-id              00003de8
subsystem-vendor-id       0000108e
revision-id               00000002
device-id                 0000b555
vendor-id                 00008086
```

Installation du logiciel Crypto Accelerator 4000 de Sun

Le logiciel Crypto Accelerator 4000 de Sun figure sur le CD Crypto Accelerator 4000 de Sun. Vous devrez peut-être télécharger des correctifs à partir du site Web SunSolve. Voir la section « Correctifs requis », page 11 pour plus d'informations.

▼ Pour installer le logiciel

1. **Insérez le CD Crypto Accelerator 4000 de Sun dans le lecteur de CD-ROM connecté à votre système.**
   - Si votre système exécute Sun Enterprise Volume Manager™, il installera automatiquement le CD-ROM dans le répertoire `/cdrom/cdrom0`.
   - S'il ne l'exécute pas, installez le CD-ROM de cette manière :

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

Les fichiers et répertoires suivants s'affichent alors dans le répertoire `/cdrom/cdrom0`.

TABLEAU 2-1 Fichiers du répertoire `/cdrom/cdrom0`

Fichier ou répertoire	Contenu	
`Copyright`	Fichier de copyright américain	
`FR_Copyright`	Fichier de copyright français	
`Docs`	*Guide de l'utilisateur et d'installation de la carte Crypto Accelerator 4000 de Sun* *Notes de version de la carte Crypto Accelerator 4000 de Sun*	
`Packages`	Contient les progiciels Crypto Accelerator 4000 de Sun :	
	`SUNWkcl2r`	Composants du noyau de cryptographie
	`SUNWkcl2u`	Bibliothèques et utilitaire d'administration cryptographique
	`SUNWkcl2a`	Prise en charge SSL pour Apache *(en option)*
	`SUNWkcl2m`	Pages manuel d'administration cryptographique *(en option)*
	`SUNWvcar`	VCA Crypto Accelerator (Root)
	`SUNWvcau`	VCA Crypto Accelerator (Usr)
	`SUNWvcaa`	Administration VCA
	`SUNWvcafw`	Microprogramme VCA
	`SUNWvcamn`	Page manuel VCA Crypto Accelerator (*en option*)
	`SUNWvcav`	Test SunVTS de VCA Crypto Accelerator *(en option)*
	`SUNWkcl2o`	Outils et bibliothèques de développement SSL *(en option)*
	`SUNWkcl2i.u`	Accélération IPSec avec KCLv2 Crypto *(en option)*

Les progiciels requis doivent être installés dans un ordre spécifique et avant l'installation des progiciels en option. Une fois les progiciels requis installés, vous pouvez installer et retirer les progiciels en option dans n'importe quel ordre.

Installez le progiciel `SUNWkcl2a` en option uniquement si vous envisagez d'utiliser Apache comme votre serveur Web.

Installez le progiciel `SUNWkcl2o` en option uniquement si vous envisagez de vous relier à une autre version (non prise en charge) du serveur Web Apache.

Installez le progiciel `SUNWvcav` en option uniquement si vous prévoyez de réaliser des tests SunVTS. SunVTS 4.4 ou version ultérieure (jusqu'à 5.x) doit être installé pour pouvoir installer le progiciel `SUNWvcav`.

Remarque – Le progiciel `SUNWkcl2i.u` en option comporte l'extension `.u` uniquement sur le CD Crypto Accelerator 4000 de Sun. Une fois installé, le nom devient `SUNWkcl2i`. L'extension `.u` sur le CD signifie que ce progiciel utilise l'architecture spécifique `sun4u`.

---

2. **Installez les progiciels requis en saisissant :**

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

3. **(Facultatif) Pour vous assurer que le logiciel a été installé correctement, exécutez la commande** `pkginfo`**.**

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

4. **(Facultatif) Pour vous assurer que le pilote est relié, exécutez la commande** `prtdiag`**. Reportez-vous aux pages manuel en ligne** `prtdiag`**(1m).**

```
# prtdiag -v
```

5. **(Facultatif) Exécutez la commande** `modinfo` **pour vérifier que les modules sont chargés.**

```
# 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)
```

Installation des progiciels en option

Pour installer uniquement les progiciels en option qui prennent en charge SSL pour le serveur Web Apache et qui fournissent l'utilitaire et les bibliothèques d'administration cryptographique, saisissez les commandes suivantes :

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

Pour installer tous les progiciels en option, saisissez les commandes suivantes :

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

Reportez-vous au TABLEAU 2-1 pour obtenir une description du contenu des progiciels en option des exemples précédents.

Répertoires et fichiers

Le TABLEAU 2-2 indique les répertoires créés après l'installation par défaut du logiciel Crypto Accelerator 4000 de Sun.

TABLEAU 2-2 Répertoires Crypto Accelerator 4000 de Sun

Répertoire	Contenu
`/etc/opt/SUNWconn/vca/keydata`	Données de stockage de clés (chiffrées)
`/opt/SUNWconn/cryptov2/bin`	Utilitaires
`/opt/SUNWconn/cryptov2/lib`	Bibliothèques de prise en charge
`/opt/SUNWconn/cryptov2/sbin`	Commandes administratives

La FIGURE 2-1 indique l'ordre hiérarchique des répertoires et des fichiers.

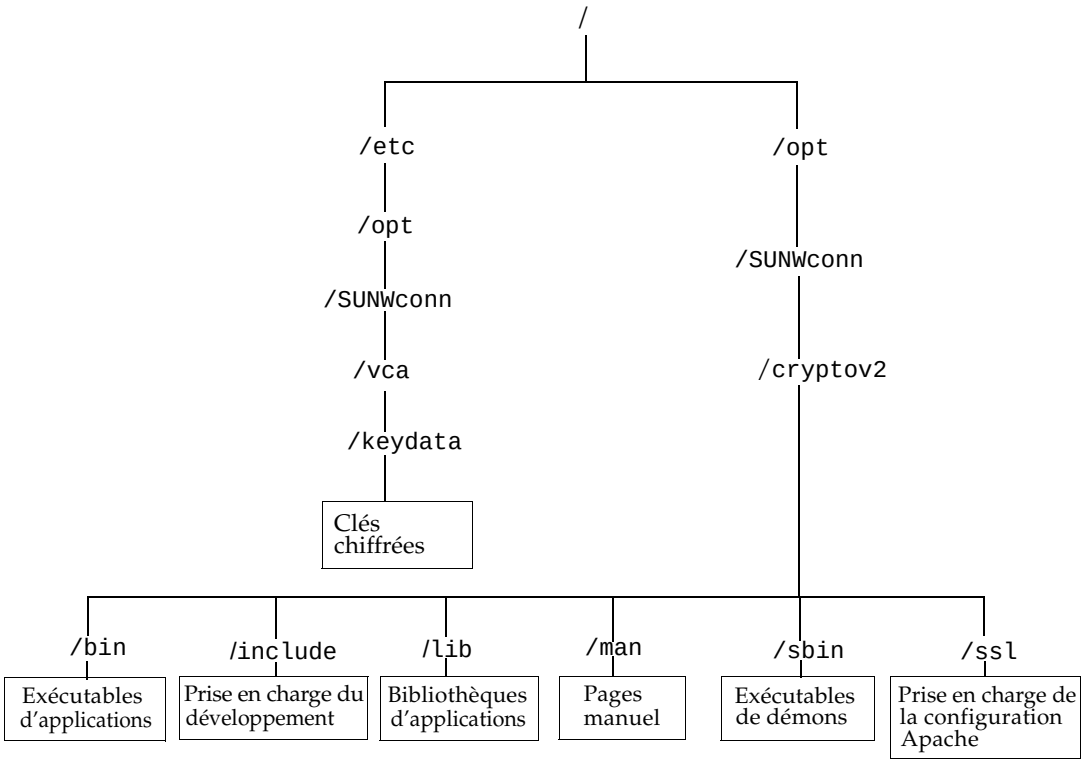

FIGURE 2-1 Répertoires et fichiers Crypto Accelerator 4000 de Sun

---

Remarque – Une fois le matériel et le logiciel de la carte installés, vous devez initialiser la carte avec les informations de configuration et de stockage de clés. Reportez-vous à la section « Initialisation de la Carte Crypto Accelerator 4000 de Sun avec `vcaadm` », page 68 pour obtenir des informations sur l'initialisation de la carte.

Désinstallation du logiciel

Si vous avez créé des stockages de clés (voir la section « Gestion des stockages de clés avec `vcaadm` », page 72), vous devez supprimer les informations de stockage de clés avec lesquelles la carte Crypto Accelerator 4000 de Sun est configurée avant de désinstaller le logiciel. La commande `zeroize` supprime toutes les clés matérielles, mais elle ne supprime pas les fichiers de stockage de clés stockés dans le système de fichiers de l'hôte physique sur lequel la carte Crypto Accelerator 4000 de Sun est installée. Reportez-vous à la section « Remise à zéro d'une Carte Crypto Accelerator 4000 de Sun », page 84 pour plus de détails sur la commande `zeroize`. Pour supprimer les fichiers de stockage de clés stockés sur le système, vous devez être un superutilisateur. Si vous n'avez pas encore créé de stockages de clés, vous pouvez ignorer cette procédure.

Attention – Ne supprimez pas un stockage de clés qui est déjà en cours d'utilisation ou qui est partagé par d'autres utilisateurs et stockages de clés. Pour supprimer des références aux stockages de clés, il se peut que vous deviez fermer le serveur Web et/ou le serveur d'administration.

Attention – Avant de désinstaller le logiciel Crypto Accelerator 4000 de Sun, vous devez désactiver tous les serveurs Web activés pour l'utilisation de la carte Crypto Accelerator 4000 de Sun. Si vous ne prenez pas cette précaution, les serveurs Web concernés ne fonctionneront plus.

▼ Pour désinstaller le logiciel

- **En tant que superutilisateur, utilisez la commande `pkgrm` pour désinstaller uniquement les progiciels que vous avez installés.**

Attention – Les progiciels installés doivent être désinstallés dans l'ordre indiqué ci-dessous. Si vous omettez de les désinstaller dans cet ordre, il se peut que vous fassiez l'objet de mises en garde relatives à l'interdépendance des éléments et que les modules du noyau soient toujours chargés.

Si vous avez installé tous les progiciels, désinstallez-les comme suit :

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

Remarque – Après l'installation ou la désinstallation du test SunVTS (`SUNWvcav`) pour la carte Crypto Accelerator 4000 de Sun, si SunVTS est déjà en cours d'exécution, il se peut que vous deviez re-tester le système pour mettre à jour les tests disponibles. Pour plus d'informations, consultez votre documentation SunVTS.

CHAPITRE 3

Configuration des paramètres du pilote

Ce chapitre décrit les procédures de configuration des paramètres du pilote de périphérique `vca` utilisés par les deux adaptateurs UTP et MMF Ethernet Crypto Accelerator 4000 de Sun. Il est composé des sections suivantes :

Paramètres du pilote de périphérique Ethernet Crypto Accelerator 4000 de Sun (`vca`)

Le pilote de périphérique `vca` contrôle les périphériques UTP et MMF Ethernet Crypto Accelerator 4000 de Sun. Le pilote `vca` est lié à la propriété du nom `pci` UNIX `pci108e,3de8` de la carte Crypto Accelerator 4000 de Sun (`108e` correspond au numéro de constructeur et `3de8` au numéro du périphérique PCI).

Vous pouvez configurer manuellement les paramètres du pilote de périphérique `vca` afin de personnaliser chaque périphérique Crypto Accelerator 4000 de Sun de votre système. Cette section donne un aperçu des capacités du périphérique Ethernet

Crypto Accelerator 4000 de Sun utilisé sur la carte. Elle répertorie également les paramètres du pilote de périphérique `vca` disponibles. Enfin, elle décrit la procédure de configuration des paramètres.

Les adaptateurs PCI UTP et MMF Ethernet Crypto Accelerator 4000 de Sun prennent en charge les vitesses et modes de fonctionnement répertoriés à la section « Définition de l'auto-négociation ou du mode forcé », page 36. Par défaut, le périphérique `vca` fonctionne en mode auto-négociation avec l'extrémité de la liaison (partenaire de liaison) pour sélectionner un mode de fonctionnement commun aux paramètres `speed`, `duplex` et `link-clock`. Le paramètre `link-clock` n'est applicable que si la carte fonctionne à une vitesse de 1 000 Mbits/s. Le périphérique `vca` peut également être configuré pour que chaque paramètre fonctionne en mode forcé.

Attention – Pour établir une liaison correcte, les partenaires de liaison doivent utiliser le même mode (auto-négociation ou mode forcé) pour chaque paramètre `speed`, `duplex` et `link-clock` (1 000 Mbits/s uniquement). S'ils ne fonctionnent pas sur le même mode pour chaque paramètre, des erreurs réseau risquent de se produire. Voir « Activation de l'auto-négociation ou du mode forcé pour les paramètres de liaison à l'aide de l'invite OpenBoot PROM », page 42.

Valeurs et définitions des paramètres du pilote

Le TABLEAU 3-1 décrit les paramètres et les réglages du pilote de périphérique `vca`.

TABLEAU 3-1 Paramètres, statuts et descriptions du pilote `vca`

Paramètre	Statut	Description
`instance`	Lecture et écriture	Instance du périphérique
`adv-autoneg-cap`	Lecture et écriture	Paramètre du mode de fonctionnement
`adv-1000fdx-cap`	Lecture et écriture	Paramètre du mode de fonctionnement (adaptateur MMF uniquement)
`adv-1000hdx-cap`	Lecture et écriture	Paramètre du mode de fonctionnement
`adv-100fdx-cap`	Lecture et écriture	Paramètre du mode de fonctionnement (adaptateur UTP uniquement)
`adv-100hdx-cap`	Lecture et écriture	Paramètre du mode de fonctionnement (adaptateur UTP uniquement)
`adv-10fdx-cap`	Lecture et écriture	Paramètre du mode de fonctionnement (adaptateur UTP uniquement)
`adv-10hdx-cap`	Lecture et écriture	Paramètre du mode de fonctionnement (adaptateur UTP uniquement)

TABLEAU 3-1 Paramètres, statuts et descriptions du pilote `vca` *(suite)*

Paramètre	Statut	Description
`adv-asmpause-cap`	Lecture et écriture	Paramètre de contrôle de flux
`adv-pause-cap`	Lecture et écriture	Paramètre de contrôle de flux
`pause-on-threshold`	Lecture et écriture	Paramètre de contrôle de flux
`pause-off-threshold`	Lecture et écriture	Paramètre de contrôle de flux
`link-master`	Lecture et écriture	Paramètre du mode forcé, vitesse 1 Gbps
`enable-ipg0`	Lecture et écriture	Active un délai supplémentaire avant transmission d'un paquet
`ipg0`	Lecture et écriture	Délai supplémentaire avant transmission d'un paquet
`ipg1`	Lecture et écriture	Paramètre d'intervalle entre paquets
`ipg2`	Lecture et écriture	Paramètre d'intervalle entre paquets
`rx-intr-pkts`	Lecture et écriture	Valeurs de suppression de trame d'interruption de réception
`rx-intr-time`	Lecture et écriture	Valeurs de suppression de trame d'interruption de réception
`red-dv4to6k`	Lecture et écriture	Détection précoce aléatoire et vecteurs de perte de paquets
`red-dv6to8k`	Lecture et écriture	Détection précoce aléatoire et vecteurs de perte de paquets
`red-dv8to10k`	Lecture et écriture	Détection précoce aléatoire et vecteurs de perte de paquets
`red-dv10to12k`	Lecture et écriture	Détection précoce aléatoire et vecteurs de perte de paquets
`tx-dma-weight`	Lecture et écriture	Paramètre de l'interface PCI
`rx-dma-weight`	Lecture et écriture	Paramètre de l'interface PCI
`infinit-burst`	Lecture et écriture	Paramètre de l'interface PCI
`disable-64bit`	Lecture et écriture	Paramètre de l'interface PCI

Communication des paramètres de liaison

Ci-dessous figurent les paramètres de liaison `speed` et `duplex` de transmission et de réception communiqués par le pilote `vca` à son partenaire de liaison. Le TABLEAU 3-2 décrit les paramètres des modes de fonctionnement et leur valeur par défaut.

Remarque – Si le réglage initial d'un paramètre est 0, il ne peut être modifié. Si vous tentez de le modifier, celui-ci reviendra systématiquement sur 0. Par défaut, ces paramètres sont définis en fonction des capacités du périphérique `vca`.

Les paramètres de liaison communiqués de l'adaptateur UTP Crypto Accelerator 4000 de Sun diffèrent de ceux de l'adaptateur MMF Crypto Accelerator 4000 de Sun comme indiqué dans le TABLEAU 3-2.

TABLEAU 3-2 Paramètres des modes de fonctionnement

Paramètre	Description
Le paramètre suivant concerne les adaptateurs UTP et MMF Crypto Accelerator 4000 de Sun.	
`adv-autoneg-cap`	Capacité d'interface locale communiquée par le matériel 0 = Mode forcé 1 = Auto-négociation (par défaut)
Le paramètre suivant concerne uniquement l'adaptateur MMF Crypto Accelerator 4000 de Sun.	
`adv-1000fdx-cap`	Capacité d'interface locale communiquée par le matériel 0 = duplex intégral 1 000 Mbits/s impossible 1 = duplex intégral 1 000 Mbits/s possible (par défaut)
Le paramètre suivant concerne les adaptateurs UTP et MMF Crypto Accelerator 4000 de Sun.	
`adv-1000hdx-cap`	Capacité d'interface locale communiquée par le matériel 0 = semi-duplex 1 000 Mbits/s impossible 1 = semi-duplex 1 000 Mbits/s possible (par défaut)
Les paramètres suivants concernent uniquement l'adaptateur UTP Crypto Accelerator 4000 de Sun.	
`adv-100fdx-cap`	Capacité d'interface locale communiquée par le matériel 0 = duplex intégral 100 Mbits/s impossible 1 = duplex intégral 100 Mbits/s possible (par défaut)

TABLEAU 3-2 Paramètres des modes de fonctionnement *(suite)*

Paramètre	Description
`adv-100hdx-cap`	Capacité d'interface locale communiquée par le matériel 0 = semi-duplex 100 Mbits/s impossible 1 = semi-duplex 100 Mbits/s possible (par défaut)
`adv-10fdx-cap`	Capacité d'interface locale communiquée par le matériel 0 = duplex intégral 10 Mbits/s impossible 1 = duplex intégral 10 Mbits/s possible (par défaut)
`adv-10hdx-cap`	Capacité d'interface locale communiquée par le matériel 0 = semi-duplex 10 Mbits/s impossible 1 = semi-duplex 10 Mbits/s possible (par défaut)

Si tous les paramètres ci-dessus sont définis sur 1, l'auto-négociation utilise la vitesse la plus élevée possible. En revanche, s'ils sont définis sur 0, vous recevrez le message d'erreur suivant :

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

Remarque – Dans l'exemple précédent, `vca0` est le nom du périphérique de la carte Crypto Accelerator 4000 de Sun où la chaîne `vca` est utilisée pour chaque carte Crypto Accelerator 4000 de Sun. Cette chaîne est toujours suivie du numéro d'instance de périphérique de la carte. Par conséquent, le numéro d'instance de périphérique de la carte `vca0` est `0`.

Paramètres de contrôle de flux

Le périphérique `vca` prend en charge la transmission et la réception de trames de pause conformément à la norme IEEE 802.3x relative au protocole de contrôle de flux au niveau de la liaison des trames. En réponse aux trames de contrôle de flux reçues, le périphérique `vca` est capable de réduire sa vitesse de transmission. Alternativement, le périphérique `vca` est capable d'émettre des trames de contrôle de flux, en demandant au partenaire de liaison de réduire sa vitesse de transmission si cette fonction est prise en charge. Par défaut, le pilote communique les capacités de pause de transmission et de réception lors de l'auto-négociation.

Le TABLEAU 3-3 fournit les mots-clé du contrôle de flux et une description de leurs fonctions.

TABLEAU 3-3 Descriptions des mots-clé de contrôle de flux en lecture-écriture

Mot-clé	Description		
`adv-asmpause-cap`	Les adaptateurs UTP et MMF prennent en charge la pause asymétrique ; par conséquent, le périphérique `vca` ne peut faire une pause que dans une direction. 0 = Off (par défaut) 1 = On		
`adv-pause-cap`	Ce paramètre a deux significations selon la valeur de `adv-asmpause-cap`. (par défaut = 0)		
	Valeur du paramètre + `adv-asmpause-cap=`	**Valeur du paramètre =** `adv-pause-cap=`	**Description**
	1	1 ou 0	`adv-pause-cap` détermine la direction de fonctionnement des pauses.
	1	1	Les pauses sont reçues, mais ne sont pas transmises.
	1	0	Les pauses sont transmises, mais ne sont pas reçues.
	0	1	Les pauses sont envoyées et reçues.
	0	1 ou 0	`adv-pause-cap` détermine si la fonction de pause est activée ou désactivée.
`pause-on-threshold`	Définit le nombre de blocs de 64 octets dans la file d'attente de réception (RX) de type FIFO, provoquant la génération par la carte d'une trame XON-PAUSE.		
`pause-off-threshold`	Définit le nombre de blocs de 64 octets dans la file d'attente de réception FIFO, provoquant la génération par la carte d'une trame XOFF-PAUSE.		

Paramètre du mode forcé en gigabit

Pour les liaisons en gigabit, ce paramètre détermine le `link-master`. En général, les commutateurs sont activés en tant que maître de liaison. Dans ce cas, il n'est pas nécessaire de modifier le paramètre. Dans le cas contraire, il est possible d'utiliser le paramètre `link-master` pour activer le périphérique `vca` en tant que maître de liaison.

TABLEAU 3-4 Paramètre du mode forcé en gigabit

Paramètre	Description
`link-master`	Lorsqu'il est sur 1, ce paramètre active le fonctionnement maître, considérant que le partenaire de liaison est un esclave. Lorsqu'il est sur 0, ce paramètre active le fonctionnement esclave, considérant que le partenaire de liaison est un maître. (par défaut)

Paramètres d'intervalles entre paquets

Le périphérique `vca` prend en charge un mode programmable appelé `enable-ipg0`.

Avant de transmettre un paquet lorsque `enable-ipg0` est activé (par défaut), le périphérique `vca` ajoute un délai supplémentaire. Ce délai, défini par le paramètre `ipg0`, vient s'ajouter à celui défini par les paramètres `ipg1` et `ipg2`. Ce délai `ipg0` supplémentaire permet de réduire les collisions.

Si `enable-ipg0` est désactivé, la valeur de `ipg0` est ignorée et aucun délai supplémentaire n'est défini. Seuls les délais définis par `ipg1` et `ipg2` seront utilisés. Désactivez `enable-ipg0` si d'autres systèmes continuent à envoyer une quantité importante de paquets continus. Les systèmes pour lesquels `enable-ipg0` est activé risquent de manquer de temps sur le réseau. Vous pouvez ajouter un délai supplémentaire en définissant le paramètre `ipg0` sur une valeur comprise entre 0 et 255, correspondant au délai en octet du support. Le TABLEAU 3-5 définit les paramètres `enable-ipg0` et `ipg0`.

TABLEAU 3-5 Définition des paramètres `enable-ipg0` et `ipg0`

Paramètre	Valeurs	Description
`enable-ipg0`	0 1	`enable-ipg0` activé `enable-ipg0` désactivé (par défaut = 1)
`ipg0`	0 à 255	Délai supplémentaire (ou intervalle) avant transmission d'un paquet (après réception du paquet) (par défaut = 8)

Le périphérique `vca` prend en charge les paramètres programmables d'intervalles entre paquets (IPG) `ipg1` et `ipg2`. L'IPG total est la somme de `ipg1` et `ipg2`. L'IPG total est 0,096 microsecondes pour une vitesse de liaison de 1 000 Mbits/s.

Le TABLEAU 3-6 répertorie les valeurs par défaut et les valeurs possibles pour les paramètres IPG.

TABLEAU 3-6 Valeurs et descriptions des paramètres d'intervalles entre paquets en lecture-écriture

Paramètre	Valeurs (Octet/temps)	Description
`ipg1`	0 à 255	Intervalle entre paquets 1 (par défaut = 8)
`ipg2`	0 à 255	Intervalle entre paquets 2 (par défaut = 4)

Par défaut, le pilote définit `ipg1` à 8 octets/temps et `ipg2` à 4 octets/temps, correspondant aux valeurs standard. (Octet/temps est le temps nécessaire pour transmettre un octet sur la liaison, avec une vitesse de liaison de 1 000 Mbits/s.

Si certains systèmes de votre réseau utilisent un IPG plus long (somme de `ipg1` et `ipg2`) et s'ils accèdent lentement au réseau, augmentez les valeurs de `ipg1` et `ipg2` pour les aligner sur les IPG plus longs des autres systèmes.

Paramètres d'interruption

Le TABLEAU 3-7 décrit les valeurs de suppression de trame d'interruption de réception.

TABLEAU 3-7 Registre de suppression de trame à la réception pour lecture de raccourcis

Nom du champ	Valeurs	Description
`rx-intr-pkts`	0 à 511	S'interrompt à l'arrivée du groupe de paquets après le traitement du dernier paquet. La valeur 0 indique qu'aucun paquet n'est supprimé. (par défaut = 3)
`rx-intr-time`	0 à 524287	S'interrompt 4,5 microsecondes après le traitement du dernier paquet. La valeur 0 indique aucune suppression de temps. (par défaut = 3)

Paramètres de perte précoce aléatoire

Ces paramètres offrent la possibilité de perdre des paquets en fonction du remplissage de la file d'attente de réception FIFO. Par défaut, cette option est activée. Lorsque l'occupation de la file d'attente FIFO atteint un certain niveau, les paquets sont perdus selon la probabilité prédéfinie. La probabilité augmente lorsque le niveau de la file d'attente FIFO augmente. Les paquets de contrôle ne sont jamais perdus et ne sont pas comptés dans les statistiques.

TABLEAU 3-8 Vecteurs 8 bits de détection précoce aléatoire à la réception

Nom du champ	Valeurs	Description
`red-dv4to6k`	0 à 255	Détection précoce aléatoire et vecteurs de perte de paquets lorsque le seuil de la file d'attente FIFO se situe entre 4 096 octets et 6 144 octets. La probabilité de perte peut être programmée sur une granularité de 12,5 %. Par exemple, si le bit 0 est défini, le premier paquet sur une série de huit sera perdu autour de ce pourcentage. (par défaut = 0)
`red-dv6to8k`	0 à 255	Détection précoce aléatoire et vecteurs de perte de paquets lorsque le seuil de la file d'attente FIFO se situe entre 6 144 octets et 8 192 octets. La probabilité de perte peut être programmée sur une granularité de 12,5 %. Par exemple, si le bit 8 est défini, le premier paquet sur une série de huit sera perdu de ce pourcentage. (par défaut = 0)
`red-dv8to10k`	0 à 255	Détection précoce aléatoire et vecteurs de perte de paquets lorsque le seuil de la file d'attente FIFO se situe entre 8 192 octets et 10 240 octets. La probabilité de perte peut être programmée sur une granularité de 12,5 %. Par exemple, si le bit 16 est défini, le premier paquet sur une série de huit sera perdu de ce pourcentage. (par défaut = 0)
`red-dv10to12k`	0 à 255	Détection précoce aléatoire et vecteurs de perte de paquets lorsque le seuil de la file d'attente FIFO se situe entre 10 240 octets et 12 288 octets. La probabilité de perte peut être programmée sur une granularité de 12,5 %. Par exemple, si le bit 24 est défini, le premier paquet sur une série de huit sera perdu de ce pourcentage. (par défaut = 0)

Paramètres de l'interface bus PCI

Ces paramètres vous permettent de modifier les caractéristiques de l'interface PCI afin d'augmenter les performances entre PCI pour une application spécifique.

TABLEAU 3-9 Paramètres de l'interface bus PCI

Paramètre	Description
`tx-dma-weight`	Détermine le coefficient multiplicateur pour attribuer un crédit de transmission (TX) lors d'un arbitrage important de type circulaire ; les valeurs sont comprises entre 0 et 3 (par défaut = 0). Zéro signifie pas de trafic supplémentaire. Les autres valeurs utilisent une puissance de 2 pour un trafic dense. Par exemple, si `tx-dma-weight` = 0 et `rx-dma-weight` = 3, tant que le trafic de réception (RX) ne cesse d'arriver, la priorité accordée à ce dernier sera huit fois supérieure à celle du trafic de transmission (TX) pour accéder au PCI.
`rx-dma-weight`	Détermine le coefficient multiplicateur pour attribuer un crédit de réception lors d'un arbitrage important de type circulaire. Les valeurs sont comprises entre 0 et 3 (par défaut = 0).
`infinite-burst`	S'il est activé, ce paramètre permet d'utiliser la fonction de rafale infinie si celle-ci est prise en charge par le système. L'adaptateur ne libère pas le bus tant que des paquets entiers sont acheminés sur le bus. Les valeurs sont comprises entre 0 et 1 (par défaut = 0).
`disable-64bit`	Arrête la capacité 64 bits de l'adaptateur. Remarque : pour les plates-formes utilisant UltraSPARC® III, il est possible de définir ce paramètre par défaut sur 1. Pour les plates-formes utilisant UltraSPARC II, la valeur par défaut du paramètre est 0. Les valeurs sont comprises entre 0 et 1 (par défaut = 0, ce qui active la capacité 64 bits).

Définition des paramètres du pilote vca

Vous pouvez définir les paramètres du pilote de périphérique vca de deux façons :
- à l'aide de l'utilitaire nnd ;
- à l'aide du fichier vca.conf.

Si vous utilisez l'utilitaire nnd, les paramètres sont conservés jusqu'au prochain redémarrage du système uniquement. Cette méthode est utile pour tester la définition des paramètres.

Pour que le réglage des paramètres soit conservé après le redémarrage du système, créez un fichier /kernel/drv/vca.conf et ajoutez-y les valeurs des paramètres lorsque vous devez définir un paramètre spécifique pour un périphérique du système. Pour plus d'informations, consultez la section « Pour définir les paramètres du pilote à l'aide du fichier vca.conf », page 38.

Définition des paramètres à l'aide de l'utilitaire ndd

Utilisez l'utilitaire ndd pour configurer des paramètres valides jusqu'au redémarrage du système.

Les sections suivantes expliquent comment utiliser le pilote vca et l'utilitaire ndd pour modifier (à l'aide de l'option -set) ou afficher (sans l'option -set) les paramètres de chaque périphérique vca.

▼ Pour spécifier des instances de périphérique pour l'utilitaire ndd

Avant d'utiliser l'utilitaire nnd pour obtenir ou définir un paramètre d'un périphérique vca, vous devez spécifier l'instance de périphérique pour l'utilitaire.

1. **Vérifiez le fichier `/etc/path_to_inst` pour identifier le numéro d'instance correspondant à un périphérique spécifique. Reportez-vous aux pages manuel en ligne pour `path_to_inst`(4).**

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

Dans l'exemple précédent, les trois instances Ethernet Crypto Accelerator 4000 de Sun proviennent des adaptateurs installés. Les numéros d'instance sont 0 et 1.

2. **Utilisez le numéro d'instance pour sélectionner le périphérique.**

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

Remarque – Dans les exemples illustrés dans ce guide de l'utilisateur, *N* représente le numéro d'instance du périphérique.

Le périphérique reste sélectionné jusqu'à ce que vous modifiiez la sélection.

Modes non-interactif et interactif

Vous pouvez utiliser l'utilitaire `nnd` dans deux modes différents :

- Non-interactif
- Interactif

En mode non-interactif, vous appelez l'utilitaire pour exécuter une commande spécifique. Une fois la commande exécutée, vous quittez l'utilitaire. En mode interactif, vous pouvez utiliser l'utilitaire pour obtenir ou définir plusieurs valeurs de paramètres. Pour plus d'informations, reportez-vous à la page manuel en ligne de l'utilitaire `ndd`(1M).

Utilisation de l'utilitaire ndd *en mode non-interactif*

Cette section explique comment modifier et afficher les valeurs des paramètres.

- **Pour modifier la valeur d'un paramètre, utilisez l'option `-set`.**

  Si vous appelez l'utilitaire `nnd` avec l'option `-set`, l'utilitaire rencontre la *valeur*, que vous devez spécifier à l'instance de périphérique `/dev/vca` nommé, et lui attribue le paramètre suivant :

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

  Lorsque vous modifiez n'importe quel paramètre `adv`, un message semblable au suivant apparaît :

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

- **Pour afficher la valeur d'un paramètre, spécifiez le nom du paramètre sans la valeur.**

  Lorsque vous omettez l'option `-set`, une opération de recherche est lancée et l'utilitaire cherche l'instance du pilote nommé, extrait la valeur correspondant au paramètre spécifié et l'imprime :

```
# ndd /dev/vcaN paramètre
```

Utilisation de l'utilitaire ndd *en mode interactif*

- **Pour modifier la valeur d'un paramètre en mode interactif, spécifiez `ndd /dev/vca`, comme indiqué ci-dessous.**

  L'utilitaire `ndd` vous demande alors le nom du paramètre :

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

  Une fois le nom du paramètre indiqué, l'utilitaire `ndd` vous demande la valeur du paramètre (voir TABLEAU 3-1 à TABLEAU 3-9).

- **Pour répertorier tous les paramètres pris en charge par le pilote** vca**, saisissez** ndd /dev/vca. **(Voir** TABLEAU 3-1 **à** TABLEAU 3-9 **pour connaître la description des paramètres.)**

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

Définition de l'auto-négociation ou du mode forcé

Les paramètres de liaison suivants peuvent être définis pour fonctionner en mode auto-négociation ou en mode forcé :

- speed
- duplex
- link-clock

Par défaut, le mode auto-négociation est activé pour ces paramètres de liaison. Quand l'un de ces paramètres est en mode auto-négociation, le périphérique `vca` communique avec le partenaire de liaison pour négocier une valeur compatible et une capacité de contrôle de flux. Lorsqu'une valeur autre que `auto` est définie pour l'un de ces paramètres, aucune négociation ne se produit et le paramètre de liaison est configuré en mode forcé. En mode forcé, la valeur du paramètre `speed` doit être identique à celle de tous les partenaires de liaison. Voir « Activation de l'auto-négociation ou du mode forcé pour les paramètres de liaison à l'aide de l'invite OpenBoot PROM », page 42.

▼ Pour désactiver le mode auto-négociation

Si votre équipement réseau ne prend pas en charge l'auto-négociation ou si vous souhaitez forcer les paramètres réseau `speed`, `duplex` ou `link-clock`, vous pouvez désactiver le mode auto-négociation sur le périphérique `vca`.

1. **Définissez les paramètres du pilote suivant sur les valeurs indiquées dans la documentation livrée avec votre périphérique de partenaire de liaison (par exemple, un commutateur) :**
   - `adv-1000fdx-cap`
   - `adv-1000hdx-cap`
   - `adv-100fdx-cap`
   - `adv-100hdx-cap`
   - `adv-10fdx-cap`
   - `adv-10hdx-cap`
   - `adv-asmpause-cap`
   - `adv-pause-cap`

   Reportez-vous au TABLEAU 3-2 pour les descriptions et valeurs possibles de ces paramètres.

2. **Définissez le paramètre `adv-autoneg-cap` sur `0`.**

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

Lorsque vous modifiez un paramètre de liaison `ndd`, un message semblable au suivant apparaît :

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

Remarque – Si vous désactivez l'auto-négociation, vous devez activer les paramètres `speed`, `duplex` et `link-clock` (1 000 Mbits/s uniquement) pour qu'ils fonctionnent en mode forcé. Pour obtenir des instructions, reportez-vous à la section « Activation de l'auto-négociation ou du mode forcé pour les paramètres de liaison à l'aide de l'invite OpenBoot PROM », page 42.

Définition des paramètres à l'aide du fichier `vca.conf`

Vous pouvez également spécifier les propriétés des paramètres du pilote en ajoutant des entrées au fichier `vca.conf` dans le répertoire `/kernel/drv`. Les noms des paramètres sont les mêmes que ceux indiqués à la section « Valeurs et définitions des paramètres du pilote », page 24.

Attention – Ne supprimez aucune des entrées par défaut contenues dans le fichier `/kernel/drv/vca.conf`.

Pour plus d'informations, consultez les pages manuel en ligne pour `prtconf`(1) et `driver.conf`(4). La procédure suivante donne un exemple de définition des paramètres dans un fichier `vca.conf`.

Les variables définies dans la section précédente s'appliquent à des périphériques connus dans le système. Pour définir une variable d'une carte Crypto Accelerator 4000 de Sun à l'aide du fichier `vca.conf`, vous devez connaître les trois informations suivantes : le nom, le parent et l'adresse du périphérique.

▼ Pour définir les paramètres du pilote à l'aide du fichier `vca.conf`

1. **Obtenez les noms des chemins du matériel pour les périphériques `vca` dans l'arborescence du périphérique.**

a. Vérifiez le fichier `/etc/driver_aliases` pour identifier le nom correspondant à un périphérique spécifique.

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

Dans l'exemple précédent, le nom du périphérique correspondant au pilote (`vca`) du logiciel Crypto Accelerator 4000 de Sun est « `pci108e,3de8` ».

b. Repérez le nom du parent du périphérique et l'adresse de l'unité du périphérique dans le fichier `/etc/path_to_inst`.

Reportez-vous aux pages manuel en ligne pour `path_to_inst`(4).

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

Dans l'exemple précédent, trois colonnes apparaissent : nom du chemin vers le périphérique, numéro d'instance et nom du pilote du logiciel.

Le nom du chemin vers le périphérique à la première ligne dans l'exemple précédent est « `/pci@8,600000/network@1` ». Les noms des chemins du périphérique sont constitués de trois parties : le nom du parent du périphérique, le nom du nœud du périphérique et l'adresse de l'unité du périphérique. Voir TABLEAU 3-10.

TABLEAU 3-10 Nom du chemin vers le périphérique

Nom complet du chemin du périphérique	Portion du nom du parent	Portion du nom du nœud	Portion de l'adresse de l'unité
"/pci@8,600000/network@1"	/pci@8,600000	network	1
"/pci@8,700000/network@1"	/pci@8,700000	network	1

Pour identifier un périphérique PCI sans ambiguïté dans le fichier `vca.conf`, utilisez le nom complet du chemin du périphérique (nom du parent, nom du nœud et adresse de l'unité) pour le périphérique. Pour obtenir plus d'informations sur la spécification du périphérique PCI, reportez-vous à la page manuel en ligne `pci`(4).

2. **Définissez les paramètres pour les périphériques ci-dessus dans le fichier** `/kernel/drv/vca.conf`.

   Dans l'entrée suivante, le paramètre `adv-autoneg-cap` est désactivé pour un périphérique Ethernet Crypto Accelerator 4000 de Sun spécifique.

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

3. **Enregistrez le fichier** `vca.conf`.
4. **Enregistrez et fermez tous les fichiers et programmes, puis quittez le système de fenêtrage.**
5. **Arrêtez et redémarrez le système.**

Définition des paramètres pour tous les périphériques Crypto Accelerator 4000 de Sun `vca` à l'aide du fichier `vca.conf`

Si vous omettez le nom du chemin du périphérique (nom du parent, nom du nœud et adresse de l'unité), la variable est définie pour toutes les instances de tous les périphériques Ethernet Crypto Accelerator 4000 de Sun.

▼ Pour définir les paramètres pour tous les périphériques Crypto Accelerator 4000 de Sun `vca` à l'aide du fichier `vca.conf`

1. **Ajoutez une ligne dans le fichier** `vca.conf` **pour modifier la valeur d'un paramètre pour toutes les instances en entrant** *paramètre=valeur;*.

   L'exemple suivant définit le paramètre `adv-autoneg-cap` sur `1` pour toutes les instances de tous les périphériques Ethernet Crypto Accelerator 4000 de Sun :

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

Exemple de fichier `vca.conf`

Voici un exemple de fichier `vca.conf` :

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

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

Activation de l'auto-négociation ou du mode forcé pour les paramètres de liaison à l'aide de l'invite OpenBoot PROM

Les paramètres suivants peuvent être configurés pour fonctionner en auto-négociation ou en mode forcé à l'interface de l'invite OpenBoot PROM (OBP) :

TABLEAU 3-11 Paramètres du périphérique de réseau de liaison locale

Paramètre	Description
`speed`	Ce paramètre peut être défini sur `auto`, `1000`, `100` ou `10` ; la syntaxe est la suivante : • `speed=auto` (par défaut) • `speed=1000` • `speed=100` • `speed=10`
`duplex`	Ce paramètre peut être défini sur `auto`, `full` ou `half` ; la syntaxe est la suivante : • `duplex=auto` (par défaut) • `duplex=full` • `duplex=half`
`link-clock`	Ce paramètre n'est applicable que si le paramètre `speed` est défini sur `1000` ou si vous utilisez une carte Crypto Accelerator 4000 de Sun MMF de 1 000 Mbits/s. La valeur de ce paramètre doit correspondre à la valeur du partenaire de liaison. Par exemple, si la valeur de la liaison locale est `master`, le partenaire de liaison doit avoir une valeur `slave`. Ce paramètre peut être défini sur `master`, `slave` ou `auto` ; la syntaxe est la suivante : • `link-clock=auto` (par défaut) • `link-clock=master` • `link-clock=slave`

Pour établir une liaison correcte, les paramètres `speed`, `duplex` et `link-clock` (1 000 Mbits/s uniquement) doivent être configurés de façon appropriée entre la liaison locale et le partenaire de liaison. Les deux partenaires de liaison doivent fonctionner soit en auto-négociation soit en mode forcé pour chaque paramètre `speed`, `duplex` et `link-clock` (1 000 Mbits/s uniquement). Si l'un de ces paramètres est défini sur `auto`, alors la liaison fonctionne en mode auto-négociation pour ce paramètre. L'absence d'un paramètre à l'invite OBP configure ce paramètre pour qu'il ait une valeur `auto` par défaut. Une valeur autre que `auto` configure la liaison locale pour fonctionner en mode forcé pour ce paramètre.

Lorsque la liaison locale fonctionne en mode auto-négociation pour les paramètres `speed` et `duplex` à 100 Mbits/s au plus, en duplex intégral et semi-duplex, alors le partenaire de liaison utilise des vitesses de 100 Mbits/s ou de 10 Mbits/s avec les deux duplex.

Lorsque le paramètre `speed` fonctionne en mode forcé, la valeur doit correspondre à la valeur `speed` du partenaire de liaison. Si le paramètre `duplex` ne correspond pas à la liaison locale et au partenaire de liaison, la liaison peut s'établir. Toutefois, des collisions se produiront dans le trafic.

Lorsque le paramètre `speed` de la liaison locale est défini sur auto-négociation et celui du partenaire de liaison est en mode forcé, la liaison peut s'établir à condition que la valeur `speed` puisse être négociée entre la liaison locale et le partenaire de liaison. L'interface en mode auto-négociation essaiera toujours d'établir une liaison (si la vitesse correspond) en semi-duplex par défaut. L'une des deux interfaces n'étant pas en mode auto-négociation, l'interface en mode auto-négociation ne détecte que le paramètre `speed` ; le paramètre duplex n'est pas détecté. Cette méthode est appelée détection parallèle.

Attention – La mise en place d'une liaison présentant un conflit duplex conduit systématiquement à des collisions dans le trafic.

Pour qu'un paramètre de liaison locale fonctionne en mode forcé, il doit avoir une valeur autre que `auto`. Par exemple, pour établir une liaison en mode forcé à 100 Mbits/s avec semi-duplex, tapez la commande suivante à l'invite OBP :

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

Remarque – Dans les exemples de cette section, `net` est un raccourci pour le chemin par défaut du périphérique de l'interface réseau intégré. Vous pouvez configurer d'autres périphériques réseau en spécifiant un chemin de périphérique plutôt que d'utiliser `net`.

Pour établir une liaison en mode forcé à 1 000 Mbits/s en semi-duplex comme maître horloge, tapez la commande suivante à l'invite OBP :

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

Remarque – La valeur du paramètre `link-clock` doit correspondre à la valeur `link-clock` du partenaire de liaison. Par exemple, si la valeur `link-clock` sur la liaison locale est définie sur `master`, la valeur `link-clock` sur le partenaire de liaison doit être définie sur `slave`.

Pour établir un mode forcé pour une vitesse de 10 Mbits/s et un mode auto-négociation pour duplex, tapez la commande suivante à l'invite OBP :

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

Vous pouvez également tapez la commande suivante à l'invite OBP pour établir les mêmes paramètres de liaison locale comme dans l'exemple précédent :

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

Pour plus d'informations, consultez la documentation relative à la norme IEEE 802.3.

Statistiques cryptographiques et de fonctionnement du pilote Ethernet Crypto Accelerator 4000 de Sun

Cette section décrit les statistiques présentées par la commande `kstat`(1M).

Statistiques cryptographiques du pilote

Le TABLEAU 3-12 décrit les statistiques cryptographiques du pilote.

TABLEAU 3-12 Statistiques cryptographiques du pilote

Paramètre	Description	Stable ou instable
`vs-mode`	Les valeurs sont `FIPS`, `standard` ou `unitialized`. `FIPS` indique que la carte est en mode FIPS. `standard` indique que la carte n'est pas en mode FIPS. `unitialized` indique que la carte n'est pas initialisée.	Stable
`vs-status`	Les valeurs sont `ready`, `faulted` ou `failsafe`. `ready` indique que la carte fonctionne normalement. `faulted` indique que la carte ne fonctionne pas. `failsafe` indique le mode `failsafe` (sans échec), c'est-à-dire l'état initial de la carte à sa sortie d'usine.	Stable

Statistiques du pilote Ethernet

Le TABLEAU 3-13 décrit les statistiques du pilote Ethernet.

TABLEAU 3-13 Statistiques du pilote Ethernet

Paramètre	Description	Stable ou instable
`ipackets`	Nombre de paquets entrant.	Stable
`ipackets64`	Version 64 bits de `ipackets`.	Stable
`ierrors`	Ensemble des paquets reçus n'ayant pu être traités en raison des erreurs qu'ils contenaient (long).	Stable

TABLEAU 3-13 Statistiques du pilote Ethernet *(suite)*

Paramètre	Description	Stable ou instable
`opackets`	Ensemble des paquets devant être transmis sur l'interface.	Stable
`opackets64`	Ensemble des paquets devant être transmis sur l'interface (64 bits).	Stable
`oerrors`	Ensemble des paquets dont la transmission a échoué en raison d'erreurs (long).	Stable
`rbytes`	Ensemble d'octets reçus sur l'interface.	Stable
`rbytes64`	Ensemble d'octets reçus sur l'interface (64 bits).	Stable
`obytes`	Ensemble d'octets devant être transmis sur l'interface.	Stable
`obytes64`	Ensemble d'octets devant être transmis sur l'interface (64 bits).	Stable
`multircv`	Paquets multidiffusés reçus, adresses de groupe et fonctionnelles comprises (long).	Stable
`multixmt`	Paquets multidiffusés devant être transmis, adresses de groupe et fonctionnelles comprises (long).	Stable
`brdcstrcv`	Paquets diffusés reçus (long).	Stable
`brdcstxmt`	Paquets diffusés devant être transmis (long).	Stable
`norcvbuf`	Nombre de fois qu'un paquet entrant valide a été rejeté car aucune mémoire tampon n'a pu être allouée à sa réception (long).	Stable
`noxmtbuf`	Paquets rejetés à la sortie car la mémoire tampon pour la transmission était occupée ou aucune mémoire n'a pu être allouée à la transmission (long).	Stable

Le TABLEAU 3-14 décrit les compteurs MAC de transmission et de réception.

TABLEAU 3-14 Compteurs MAC de transmission (TX) et de réception (RX)

Paramètre	Description	Stable ou instable
`tx-collisions`	Incréments du compteur chargeable 16 bits pour chaque tentative de transmission de trame se soldant par une collision.	Stable
`tx-first-collisions`	Incréments du compteur chargeable 16 bits pour chaque transmission de trame ayant fait l'objet d'une collision au premier essai, mais ayant été transmise lors de la deuxième tentative.	Instable
`tx-excessive-collisions`	Incréments du compteur chargeable 16 bits pour chaque transmission de trame ayant dépassé le délai de tentative.	Instable
`tx-late-collisions`	Incréments du compteur chargeable 16 bits pour chaque transmission de trame ayant rencontré une collision. Cela indique le nombre de trames perdues par le TxMAC en raison de collisions survenues après avoir transmis au moins le nombre d'octets de taille de trame minimale. En général, cela indique qu'il existe au moins une station sur le réseau qui viole l'étendue maximale autorisée du réseau.	Instable
`tx-defer-timer`	Incréments de l'horloge chargeable 16 bits lorsque le TxMAC retarde le trafic sur le réseau lors d'une tentative de transmission d'une trame. La base temps de l'horloge est l'horloge media byte divisée par 256.	Instable
`tx-peak-attempts`	Le registre 8 bits indique le nombre le plus élevé de collisions consécutives par trame correctement transmise, survenues depuis la dernière lecture du registre. La valeur maximale que peut atteindre le registre est 255. Une interruption masquable survient dans le logiciel si le nombre de collisions consécutives par trame correctement transmise dépasse 255. Une fois lu, ce registre sera automatiquement remis à 0.	Instable
`tx-underrun`	Incréments du compteur chargeable 16 bits après réception d'une trame valide depuis le réseau.	Instable

TABLEAU 3-14 Compteurs MAC de transmission (TX) et de réception (RX) *(suite)*

Paramètre	Description	Stable ou instable
`rx-length-err`	Incrément du compteur chargeable 16 bits après réception d'une trame (en provenance du réseau), dont la longueur est supérieure à la valeur programmée dans le registre de taille maximale de trame.	Instable
`rx-alignment-err`	Incréments du compteur chargeable 16 bits lorsqu'une erreur d'alignement est détectée dans une trame de réception. Une erreur d'alignement est rapportée lorsqu'une trame de réception n'achève pas l'algorithme CRC (code de redondance cyclique) et que la trame contient un nombre non entier d'octets (autrement dit, la taille de la trame en bits est différente de 0).	Instable
`rx-crc-err`	Incréments du compteur chargeable 16 bits lorsqu'une trame de réception n'achève pas l'algorithme CRC (code de redondance cyclique) et que la trame contient un nombre entier d'octets (autrement dit, la taille de la trame en bits est égale à 0).	Instable
`rx-code-violations`	Incréments du compteur chargeable 16 bits lorsqu'une indication Rx_Err est générée par le XCVR couvrant le MII, pendant la réception d'une trame. Cette indication est générée par l'émetteur-récepteur lorsqu'il détecte un code non valide dans la transmission de données reçues. Une violation du code de réception n'est pas comptée comme une séquence de contrôle de trame (FCS) ni comme une erreur d'alignement.	Instable
`rx-overflows`	Nombre de trames Ethernet perdues en raison du manque de ressources.	Instable

TABLEAU 3-14 Compteurs MAC de transmission (TX) et de réception (RX) *(suite)*

Paramètre	Description	Stable ou instable
`rx-no-buf`	Nombre de fois où il est matériellement impossible de recevoir des données en raison du manque d'espace dans la mémoire tampon de réception.	Instable
`rx-no-comp-wb`	Nombre de fois où il est matériellement impossible de poursuivre les entrées pour les données reçues.	Instable
`rx-len-mismatch`	Nombre de trames reçues pour lesquelles la longueur théorique ne correspond pas à la longueur véritable.	Instable

Les propriétés Ethernet suivantes (TABLEAU 3-15) sont dérivées de l'intersection entre les capacités du périphérique et celles du partenaire de liaison.

Le TABLEAU 3-15 décrit les propriétés courantes de la liaison Ethernet.

TABLEAU 3-15 Propriétés courantes de la liaison Ethernet

Paramètre	Description	Stable ou instable
`ifspeed`	1 000, 100 ou 10 Mbits/s	Stable
`link-duplex`	0 = half, 1 = full	Stable
`link-pause`	Paramètres actifs de la pause pour la liaison, voir « Paramètres de contrôle de flux », page 27	Stable
`link-asmpause`	Paramètres actifs de la pause pour la liaison, voir « Paramètres de contrôle de flux », page 27	Stable
`link-up`	1 = haut, 0 = bas	Stable
`link-status`	1 = haut, 0 = bas	Stable
`xcvr-inuse`	Type d'émetteur-récepteur utilisé : 1 = MII interne, 2 = MII externe, 3 = PCS externe	Stable

Le TABLEAU 3-16 décrit les capacités de l'interface MII (Media Independent Interface) en lecture seule. Ces paramètres définissent les capacités du matériel. L'interface MII Gigabit (GMII) prend en charge toutes les capacités suivantes :

TABLEAU 3-16 Capacités du périphérique `vca` en lecture seule

Paramètre	Description	Stable ou instable
`cap-autoneg`	0 = Auto-négociation impossible 1 = Auto-négociation possible	Stable
`cap-1000fdx`	Capacité duplex intégral de l'interface locale 0 = duplex intégral 1 000 Mbits/s impossible 1 = duplex intégral 1 000 Mbits/s possible	Stable
`cap-1000hdx`	Capacité semi-duplex de l'interface locale 0 = semi-duplex 1 000 Mbits/s impossible 1 = semi-duplex 1 000 Mbits/s possible	Stable
`cap-100fdx`	Capacité duplex intégral de l'interface locale 0 = duplex intégral 100 Mbits/s impossible 1 = duplex intégral 100 Mbits/s possible	Stable
`cap-100hdx`	Capacité semi-duplex de l'interface locale 0 = semi-duplex 100 Mbits/s impossible 1 = semi-duplex 100 Mbits/s possible	Stable
`cap-10fdx`	Capacité duplex intégral de l'interface locale 0 = duplex intégral 10 Mbits/s impossible 1 = duplex intégral 10 Mbits/s possible	Stable
`cap-10hdx`	Capacité semi-duplex de l'interface locale 0 = semi-duplex 10 Mbits/s impossible 1 = semi-duplex 10 Mbits/s possible	Stable
`cap-asm-pause`	Capacité de contrôle de flux de l'interface locale 0 = Pause asymétrique impossible 1 = Pause asymétrique possible (à partir du périphérique local) (Voir « Paramètres de contrôle de flux », page 27)	Stable
`cap-pause`	Capacité de contrôle de flux de l'interface locale 0 = Pause symétrique impossible 1 = Pause symétrique possible (Voir « Paramètres de contrôle de flux », page 27)	Stable

Rapport des capacités du partenaire de liaison

Le TABLEAU 3-17 décrit les capacités du partenaire de liaison en lecture seule.

TABLEAU 3-17 Capacités du partenaire de liaison en lecture seule

Paramètre	Description	Stable ou instable
`lp-cap-autoneg`	0 = Aucune auto-négociation 1 = Auto-négociation	Stable
`lp-cap-1000fdx`	0 = Aucune transmission duplex intégral 1 000 Mbits/s 1 = duplex intégral 1 000 Mbits/s	Stable
`lp-cap-1000hdx`	0 = Aucune transmission semi-duplex 1 000 Mbits/s 1 = semi-duplex 1 000 Mbits/s	Stable
`lp-cap-100fdx`	0 = Aucune transmission duplex intégral 100 Mbits/s 1 = duplex intégral 100 Mbits/s	Stable
`lp-cap-100hdx`	0 = Aucune transmission semi-duplex 100 Mbits/s 1 = semi-duplex 100 Mbits/s	Stable
`lp-cap-10fdx`	0 = Aucune transmission duplex intégral 10 Mbits/s 1 = duplex intégral 10 Mbits/s	Stable
`lp-cap-10hdx`	0 = Aucune transmission semi-duplex 10 Mbits/s 1 = semi-duplex 10 Mbits/s	Stable
`lp-cap-asm-pause`	0 = Pause asymétrique impossible 1 = Pause symétrique vers la capacité du partenaire de liaison (Voir « Paramètres de contrôle de flux », page 27)	Stable
`lp-cap-pause`	0 = Pause symétrique impossible 1 = Pause symétrique possible (Voir « Paramètres de contrôle de flux », page 27)	Stable

Si le partenaire de liaison ne prend pas en charge l'auto-négociation (quand `lp-cap-autoneg` est égal à 0), les informations restantes décrites dans le TABLEAU 3-17 ne sont pas pertinentes et la valeur du paramètre est 0.

Si le partenaire de liaison prend en charge l'auto-négociation (quand `lp-cap-autoneg` est égal à 1), alors les informations relatives à la vitesse et au mode s'affichent lorsque vous utilisez l'auto-négociation et les capacités du partenaire de liaison.

Le TABLEAU 3-18 décrit les paramètres spécifiques au pilote.

TABLEAU 3-18 Paramètres spécifiques au pilote

Paramètre	Description	Stable ou instable
`lb-mode`	Copie du mode de bouclage dans lequel se trouve le périphérique, le cas échéant.	Instable
`promisc`	Lorsqu'il est activé, le périphérique est en mode espion. Lorsqu'il est désactivé, le périphérique n'est pas en mode espion.	Instable
Compteurs de transmission Ethernet		
`tx-wsrv`	Compte le nombre de fois où l'anneau de transmission est plein.	Instable
`tx-msgdup-fail`	Echec lors de la tentative de duplication d'un paquet.	Instable
`tx-allocb-fail`	Echec lors de la tentative d'attribution de la mémoire.	Instable
`tx-queue0`	Nombre de paquets en attente de transmission dans la première file d'attente de transmission du matériel.	Instable
`tx-queue1`	Nombre de paquets en attente de transmission dans la deuxième file d'attente de transmission du matériel.	Instable
`tx-queue2`	Nombre de paquets en attente de transmission dans la troisième file d'attente du matériel.	Instable
`tx-queue3`	Nombre de paquets en attente de transmission dans la quatrième file d'attente de transmission du matériel.	Instable
Compteurs de réception Ethernet		
`rx-hdr-pkts`	Nombre de paquets reçus dont la taille était inférieure à 256 octets.	Instable
`rx-mtu-pkts`	Nombre de paquets reçus dont la taille était supérieure à 256 octets, mais inférieure à 1 514 octets.	Instable
`rx-split-pkts`	Nombre de paquets répartis sur deux pages.	Instable
`rx-nocanput`	Nombre de paquets perdus en raison d'échecs lors de la livraison à la pile IP.	Instable

TABLEAU 3-18 Paramètres spécifiques au pilote *(suite)*

Paramètre	Description	Stable ou instable
`rx-msgdup-fail`	Nombre de paquets ne pouvant être dupliqués.	Instable
`rx-allocb-fail`	Nombre d'échecs à l'attribution des paquets.	Instable
`rx-new-pages`	Nombre de pages remplacées pendant la réception.	Instable
`rx-new-hdr-pages`	Nombre de pages remplies de paquets dont la taille est inférieure à 256 octets, remplacées pendant la réception.	Instable
`rx-new-mtu-pages`	Nombre de pages remplies de paquets dont la taille est comprise entre 256 octets et 1 514 octets, remplacées pendant la réception.	Instable
`rx-new-nxt-pages`	Nombre de pages contenant des paquets répartis sur plusieurs pages, remplacées pendant la réception.	Instable
`rx-page-alloc-fail`	Nombre d'échecs à l'attribution des pages.	Instable
`rx-mtu-drops`	Nombre de fois où une page entière de paquets dont la taille est comprise entre 256 octets et 1 514 octets a été perdue, le pilote étant incapable d'en trouver une autre pour la remplacer.	Instable
`rx-hdr-drops`	Nombre de fois où une page entière de paquets dont la taille est inférieure à 256 octets a été perdue, le pilote étant incapable d'en trouver une autre pour la remplacer.	Instable
`rx-nxt-drops`	Nombre de fois où une page avec un paquet réparti a été perdue, le pilote étant incapable d'en trouver une autre pour la remplacer.	Instable
`rx-rel-flow`	Nombre de fois où le pilote a reçu l'instruction de libérer un flux.	Instable
Propriétés PCI Ethernet		
`rev-id`	ID de révision du périphérique Ethernet Crypto Accelerator 4000 de Sun utile pour la reconnaissance du périphérique utilisé sur site.	Instable
`pci-err`	Somme de toutes les erreurs PCI.	Instable
`pci-rta-err`	Nombre d'abandons cible reçus.	Instable
`pci-rma-err`	Nombre d'abandons maître reçus.	Instable

TABLEAU 3-18 Paramètres spécifiques au pilote *(suite)*

Paramètre	Description	Stable ou instable
`pci-parity-err`	Nombre d'erreurs de parité PCI détectées.	Instable
`pci-drto-err`	Nombre de fois où le délai pour une nouvelle tentative de transaction retardée a été dépassé.	Instable
`dma-mode`	Utilisé par le pilote Crypto Accelerator 4000 de Sun (`vca`).	Instable

▼ Pour vérifier les paramètres du partenaire de liaison

- **En tant que superutilisateur, tapez la commande** `kstat vca:`*N*`:`

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

Remarque – Dans l'exemple précédent, *N* est le numéro d'instance du périphérique `vca`. Ce chiffre devrait correspondre au numéro d'instance de la carte pour laquelle vous exécutez la commande `kstat`.

Configuration du réseau

Cette section explique comment modifier les fichiers hôte du réseau après installation de l'adaptateur sur votre système.

Configuration des fichiers hôte du réseau

Après installation du logiciel du pilote, vous devez créer un fichier `hostname.vca`*N* pour l'interface Ethernet de l'adaptateur. Notez que dans le nom du fichier `hostname.vca`*N*, *N* correspond au numéro d'instance de l'interface `vca` que vous envisagez d'utiliser. Vous devez également créer une adresse IP et un nom d'hôte pour son interface Ethernet dans le fichier `/etc/hosts`.

1. **Repérez les interfaces `vca` et les numéros d'instance appropriés dans le fichier `/etc/path_to_inst`.**

   Reportez-vous aux pages manuel en ligne pour `path_to_inst`(4).

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

   Le numéro d'instance dans l'exemple précédent est `0`.

2. **Utilisez la commande `ifconfig`(1M) pour paramétrer l'interface `vca` de l'adaptateur.**

   Utilisez la commande `ifconfig` pour attribuer une adresse IP à l'interface réseau. Tapez la ligne de commande suivante, en remplaçant *adresse_ip* par l'adresse IP de l'adaptateur :

```
# ifconfig vcaN plumb adresse_ip up
```

Remarque – Dans les exemples de cette section, *N* représente le numéro d'instance du périphérique.

Pour plus d'informations, consultez la page manuel en ligne `ifconfig`(1M) et la documentation Solaris.

- Si vous souhaitez conserver la configuration après le redémarrage, créez un fichier `/etc/`*nom d'hôte*`.vca`*N*, où *N* correspond au numéro d'instance de l'interface `vca` que vous envisagez d'utiliser.

  Pour utiliser l'interface `vca` de l'exemple illustré à l'étape 1, créez un fichier `/etc/`*nom d'hôte*`.vca`*N*, où *N* correspond au numéro d'instance du périphérique désigné par 0 dans cet exemple. Si le numéro d'instance était 1, le nom du fichier aurait été `/etc/`*nom d'hôte*`.vca1`.

- Ne créez pas de fichier `/etc/`*nom d'hôte*`.vca`*N* pour une interface Crypto Accelerator 4000 de Sun que vous n'allez pas utiliser.
- Le fichier `/etc/`*nom d'hôte*`.vca`*N* doit contenir le nom d'hôte de l'interface `vca` appropriée.
- Le nom d'hôte doit contenir une adresse IP et être répertorié dans le fichier `/etc/hosts`.

- Le nom d'hôte doit être différent des autres noms d'hôte quelle que soit l'interface, par exemple : `/etc/`*nom d'hôte*`.vca0` et `/etc/`*nom d'hôte*`.vca1` ne peuvent pas avoir un nom d'hôte identique.

L'exemple suivant indique le fichier `/etc/`*nom d'hôte*`.vca`*N* nécessaire pour un système appelé `zardoz` doté d'une carte Crypto Accelerator 4000 de Sun (`zardoz-11`).

```
# cat /etc/nom d'hôte.hme0
zardoz
# cat /etc/nom d'hôte.vca0
zardoz-11
```

3. **Créez une entrée appropriée dans le fichier `/etc/hosts` pour chaque interface active `vca`.**

   Par exemple :

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

CHAPITRE 4

Administration de la carte Sun Crypto Accelerator 4000 avec les utilitaires vcaadm et vcadiag

Ce chapitre présente les utilitaires vcaadm et vcadiag. Il comprend les sections suivantes :

Utilisation de vcaadm

Le programme vcaadm fournit une interface de ligne de commande à la carte Crypto Accelerator 4000 de Sun. Seuls les utilisateurs désignés comme responsables de la sécurité sont autorisés à utiliser l'utilitaire vcaadm. Lors de la première connexion à une carte Crypto Accelerator 4000 de Sun avec vcaadm, vous êtes invité à créer un responsable de la sécurité et un mot de passe d'origine.

Pour accéder facilement au programme vcaadm, placez le répertoire d'outils Crypto Accelerator 4000 de Sun dans votre chemin de recherche. Par exemple :

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

La syntaxe de la ligne de commande `vcaadm` est la suivante :

- `vcaadm [-H]`
- `vcaadm [-y] [-h` *hôte*`] [-p` *port*`] [-d vca`*N*`] [-f` *nom fichier*`]`
- `vcaadm [-y] [-h` *hôte*`] [-p` *port*`] [-d vca`*N*`] [-s` *resp_sécurité*`]` *command*

Remarque – Lorsque vous utilisez l'attribut `-d`, `vca`*N* est le nom de périphérique de la carte, où *N* correspond au numéro d'instance du périphérique Crypto Accelerator 4000 de Sun.

Le TABLEAU 4-1 présente les options de l'utilitaire `cvcaadm`.

TABLEAU 4-1 Options `vcaadm`

Option	Description
`-H`	Affiche les fichiers d'aide pour les commandes `vcaadm` et quitte.
`-d vca`*N*	Etablit la connexion à la carte Crypto Accelerator 4000 de Sun dont le numéro d'instance de pilote est *N*. Par exemple, `-d vca1` établit la connexion au périphérique `vca1`, où `vca` est une chaîne du nom de périphérique de la carte et 1 le numéro d'instance du périphérique. Cette valeur est définie par défaut sur `vca0` et doit avoir la forme `vca`*N*, où *N* correspond au numéro d'instance du périphérique.
`-f` *nomfichier*	Interprète une ou plusieurs commandes à partir de *nomfichier* et quitte.
`-h` *hôte*	Etablit la connexion à la carte Crypto Accelerator 4000 de Sun sur l'*hôte*. La valeur pour l'*hôte* peut être un nom d'hôte ou une adresse IP, et est définie par défaut sur l'adresse de bouclage.
`-p` *port*	Etablit la connexion à la carte Crypto Accelerator 4000 de Sun sur le *port*. La valeur de *port* est 6870 par défaut.
`-s` *resp_sécurité*	Ouvre la session pour le responsable de la sécurité nommé *resp_sécurité.*
`-y`	Force une réponse oui à toute commande qui devrait normalement demander une confirmation.

Remarque – Le nom *resp_sécurité* est utilisé dans le présent guide de l'utilisateur comme un exemple de nom de responsable de la sécurité.

Modes de fonctionnement

`vcaadm` peut fonctionner dans l'un des trois modes suivants, dont la principale différence réside dans la manière dont les commandes sont communiquées à `vcaadm`. Les trois modes sont : mode commande simple, mode fichier, mode interactif.

Remarque – Pour utiliser `vcaadm`, authentifiez-vous comme responsable de la sécurité. Le mode de fonctionnement utilisé détermine le nombre de fois où vous devrez vous authentifier en tant que responsable de la sécurité.

Mode commande simple

En mode commande simple, vous devez vous authentifier comme responsable de la sécurité pour chaque commande. Une fois la commande exécutée, vous êtes déconnecté de `vcaadm`.

Lorsque vous saisissez des commandes en mode commande simple, vous spécifiez la commande à exécuter une fois toutes les options de ligne de commande spécifiées. Par exemple, en mode commande simple, la commande suivante afficherait tous les utilisateurs dans un stockage de clés donné et renverrait l'utilisateur à l'invite de commande shell.

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

La commande suivante ouvre une session pour le responsable de la sécurité, *resp_sécurité*, puis crée l'utilisateur *web_admin* dans le stockage de clés.

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

Remarque – Le premier mot de passe concerne le responsable de la sécurité et est suivi du mot de passe et de la confirmation pour le nouvel utilisateur *web_admin*.

Toutes les sorties du mode commande simple sont dirigées vers le flux de sortie standard. Cette sortie peut être redirigée à l'aide de méthodes UNIX standard basées sur le shell.

Mode fichier

En mode fichier, vous devez vous authentifier en tant que responsable de la sécurité pour chaque fichier que vous exécutez. Vous êtes déconnecté de `vcaadm` une fois les commandes du fichier de commandes exécutées.

Pour saisir les commandes en mode fichier, spécifiez un fichier à partir duquel `vcaadm` lira une ou plusieurs commandes. Le fichier doit être du texte ASCII comportant une commande par ligne. Chaque commentaire doit être précédé du caractère dièse (#). Si l'option en mode fichier est définie, `vcaadm` ignore tous les arguments de la ligne de commande après la dernière option. L'exemple suivant lance les commandes dans le fichier `deluser.scr` et répond à toutes les invites par l'affirmative.

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

Mode interactif

En mode interactif, vous devez vous authentifier comme responsable de la sécurité chaque fois que vous vous connectez à une carte. Il s'agit du mode de fonctionnement par défaut pour `vcaadm`. Pour vous déconnecter de `vcaadm` en mode interactif, utilisez la commande `logout`. Reportez-vous à la section « Connexion et déconnexion avec `vcaadm` », page 60.

Le mode interactif fournit à l'utilisateur une interface similaire à `ftp`(1), où les commandes peuvent être saisies l'une après l'autre. L'option `-y` n'est pas prise en charge en mode interactif.

Connexion et déconnexion avec `vcaadm`

Lorsque vous utilisez `vcaadm` depuis la ligne de commande et que vous spécifiez *hôte*, *port* et *périphérique* à l'aide des attributs `-h`, `-p` et `-d`, respectivement, vous êtes immédiatement invité à vous connecter en tant que responsable de la sécurité si une connexion réseau a été établie.

Le programme vcaadm établit une connexion réseau chiffrée (canal) entre l'application vcaadm et le microprogramme Crypto Accelerator 4000 de Sun exécuté sur la carte spécifiée.

Au cours de la configuration du canal chiffré, les cartes s'identifient elles-mêmes par leur adresse Ethernet et par une clé publique RSA. Une base de données certifiée (`$HOME/.vcaadm/trustdb`) est créée lors de la première connexion de vcaadm à une carte. Ce fichier contient toutes les cartes actuellement certifiées par le responsable de la sécurité.

Connexion à une carte avec vcaadm

Si le responsable de la sécurité se connecte à une nouvelle carte, vcaadm l'en avertit et l'invite à choisir l'une des options suivantes :

```
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).
```

Si le responsable de la sécurité se connecte à une carte dont la clé d'accès à distance a changé, vcaadm l'en avertit et l'invite à choisir l'une des options suivantes :

```
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.
```

Connexion à une nouvelle carte

Remarque – Les exemples restants de ce chapitre ont été créés avec le mode interactif de vcaadm.

Lors de la connexion à une nouvelle carte, `vcaadm` doit créer une nouvelle entrée dans la base de données certifiée. L'exemple suivant illustre la connexion à une nouvelle carte.

```
# vcaadm -h nomhôte
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 -->
```

Connexion à une carte avec une clé d'accès à distance modifiée

Lors de la connexion à une carte dont la clé d'accès à distance a été modifiée, `vcaadm` doit modifier l'entrée correspondante à la carte dans la base de données certifiée. L'exemple suivant illustre la connexion à une carte dont la clé d'accès à distance a été modifiée.

```
# vcaadm -h nomhôte
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 -->
```

Invite `vcaadm`

L'invite `vcaadm` en mode interactif est affichée comme suit :

```
vcaadm{vcaN@nomhôte, resp_sécurité}> command
```

Le tableau suivant décrit les variables de l'invite `vcaadm` :

TABLEAU 4-2 Définitions des variables de l'invite `vcaadm`

Variable d'invite	Définition
`vca`*N*	`vca` est la chaîne représentant la carte Crypto Accelerator 4000 de Sun. *N* est le numéro d'instance de périphérique (adresse de l'unité) figurant dans le nom du chemin du périphérique de la carte. Reportez-vous à la section « Pour définir les paramètres du pilote à l'aide du fichier `vca.conf` », page 38 pour plus de détails sur la récupération de ce numéro pour un périphérique.
nomhôte	Nom de l'hôte auquel la carte Crypto Accelerator 4000 de Sun est physiquement connectée. *nomhôte* peut être remplacé par l'adresse IP de l'hôte physique.
resp_sécurité	Nom du responsable de la sécurité actuellement connecté à la carte.

Déconnexion de la carte avec `vcaadm`

Si vous travaillez en mode interactif, vous aurez peut-être à vous déconnecter d'une carte et à vous connecter à une autre sans complètement quitter `vcaadm`. Pour cela, utilisez la commande `logout` :

```
vcaadm{vcaN@nomhôte, resp_sécurité}> logout
vcaadm>
```

Dans l'exemple précédent, notez que l'invite `vcaadm>` n'affiche plus le numéro d'instance du périphérique, le nom d'hôte ni le nom du responsable de la sécurité. Pour vous connecter à un autre périphérique, saisissez la commande `connect` avec les paramètres facultatifs suivants.

TABLEAU 4-3 Paramètres facultatifs de la commande `connect`

Paramètre	Description
`dev vca`*N*	Connectez-vous à la carte Crypto Accelerator 4000 de Sun avec le numéro d'instance de périphérique de *N*. Par exemple, `-d vca1` se connecte au périphérique `vca1` ; le périphérique par défaut est `vca0`.
`host` *nomhôte*	Se connecte à la carte Crypto Accelerator 4000 de Sun sur *nomhôte* (par défaut, l'adresse du bouclage). *nomhôte* peut être remplacé par l'adresse IP de l'hôte physique.
`port` *port*	Se connecte par défaut à la carte Crypto Accelerator 4000 de Sun sur le port *port* (par défaut, 6870).

Exemple :

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

`vcaadm` ne vous permettra pas d'émettre la commande `connect` si vous êtes déjà connecté à la carte Crypto Accelerator 4000 de Sun. Vous devez d'abord vous déconnecter, puis émettre la commande `connect`.

Chaque nouvelle connexion va provoquer la renégociation par `vcaadm` et le microprogramme Crypto Accelerator 4000 de Sun cible des nouvelles clés de session pour protéger les données administratives envoyées.

Saisie de commandes avec vcaadm

Le programme vcaadm dispose d'un langage de commande qui doit être utilisé pour interagir avec la carte Crypto Accelerator 4000 de Sun. Les commandes sont saisies en utilisant tout ou partie d'un mot (partie suffisamment longue pour pouvoir identifier le mot de manière unique). L'utilisation de sh au lieu de show conviendrait, mais l'utilisation de re est ambiguë car cela peut signifier reset ou rekey.

L'exemple suivant indique la saisie de commandes à l'aide de mots entiers :

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

Les mêmes informations peuvent être obtenues dans l'exemple précédent en utilisant des parties de mots comme commandes, telles que sh us.

Une commande ambiguë produit une demande d'explication :

```
vcaadm{vcaN@nomhôte, resp_sécurité}> re
Ambiguous command: re
```

Obtention d'aide pour les commandes

`vcaadm` comporte des fonctions d'aide intégrées. Pour obtenir de l'aide, vous devez saisir le caractère « ? » suivi de la commande pour laquelle vous souhaitez obtenir de l'aide. Si une commande est saisie dans son ensemble et qu'un « ? » existe quelque part sur une ligne, vous obtiendrez la syntaxe de la commande. Par exemple :

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

vcaadm{vcaN@nomhôte, resp_sécurité}> create user ?
Usage: create user [<nomutilisateur>]

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

Vous pouvez également entrer un point d'interrogation à l'invite `vcaadm` pour afficher la liste de toutes les commandes `vcaadm` et leur description, par exemple :

```
vcaadm{vcaN@nomhôte, resp_sécurité}> ?
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
```

Lorsque vous n'êtes pas en mode interactif `vcaadm`, le caractère « ? » peut être interprété par le shell dans lequel vous travaillez. Dans ce cas, veillez à utiliser le caractère d'échappement du shell de commande avant le point d'interrogation.

Fermeture du programme `vcaadm` en mode interactif

Deux commandes vous permettent de quitter `vcaadm` : `quit` et `exit`. La séquence de clés Ctrl-D existe également à partir de `vcaadm`.

Initialisation de la Carte Crypto Accelerator 4000 de Sun avec `vcaadm`

La première étape pour la configuration d'une carte Crypto Accelerator 4000 de Sun consiste à l'initialiser. Lorsque vous initialisez une carte, vous devez créer un stockage de clés ; reportez-vous à la section « Concepts et terminologie », page 90. Vous pouvez initialiser la carte Crypto Accelerator 4000 de Sun avec un nouveau stockage de clés ou utiliser un fichier de sauvegarde pour utiliser un stockage de clés existant.

Lors de la première connexion d'une carte Crypto Accelerator 4000 de Sun avec `vcaadm`, vous êtes invité à initialiser la carte avec un nouveau stockage de clés ou à l'initialiser pour utiliser un stockage de clés existant stocké dans un fichier de sauvegarde. `vcaadm` vous demande toutes les informations requises pour l'initialisation de la carte.

▼ Pour initialiser la Carte Crypto Accelerator 4000 de Sun avec un nouveau stockage de clés

1. **Saisissez `vcaadm` à l'invite de commande du système avec la carte Crypto Accelerator 4000 de Sun installée ou saisissez `vcaadm -h` *nomhôte* si le système est distant, et sélectionnez 1 pour initialiser la carte :**

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

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

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

2. **Créez un nom de responsable de la sécurité et un mot de passe d'origine (reportez-vous à la section « Conditions de dénomination », page 72) :**

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

3. **Créez un nom de stockage de clés (reportez-vous à la section « Conditions de dénomination », page 72) :**

```
Keystore Name: nom_stockageclés
```

4. **Sélectionnez le mode FIPS 140-2 ou non-FIPS.**

   En mode FIPS, la carte Crypto Accelerator 4000 de Sun est conforme à la norme FIPS 140-2, niveau 3 ; il s'agit d'une norme de traitement d'informations fédérale relative à l'inviolabilité et à un haut niveau d'intégrité et de sécurité des données. Reportez-vous au document FIPS 140-2 figurant à l'adresse : `http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf`

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

Remarque – Avant de modifier ou de supprimer un paramètre essentiel ou avant d'exécuter une commande dont les conséquences sont considérables, `vcaadm` vous invite à entrer `Y`, `Yes`, `N` ou `No` pour confirmer. Ces valeurs ne sont pas sensibles à la casse ; la valeur par défaut est `No`.

5. **Vérifiez les informations de configuration :**

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

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

Initialisation de la Carte Crypto Accelerator 4000 de Sun pour utiliser un stockage de clés existant

Si vous ajoutez plusieurs cartes à un seul stockage de clés, vous pouvez initialiser toutes les cartes afin d'utiliser les mêmes informations de stockage de clés. En outre, vous pouvez restaurer la configuration d'un stockage de clés d'origine d'une carte Crypto Accelerator 4000 de Sun. Cette section décrit comment initialiser une carte pour utiliser un stockage de clés existant stocké dans un fichier de sauvegarde.

Vous devez au préalable créer un fichier de sauvegarde à partir d'une configuration de carte existante avant d'exécuter cette procédure. Lors de la création et de la restauration d'un fichier de sauvegarde, un mot de passe est requis pour coder et décoder les données du fichier. Reportez-vous à la section « Sauvegarde de la clé principale », page 78.

▼ Pour initialiser la Carte Crypto Accelerator 4000 de Sun en vue d'utiliser un stockage de clés existant

1. **Saisissez** `vcaadm` **à l'invite de commande du système avec la carte Crypto Accelerator 4000 de Sun installée ou saisissez** `vcaadm -h` *nomhôte* **si le système est distant, et sélectionnez 2 pour initialiser la carte depuis une sauvegarde :**

```
# vcaadm -h nomhôte
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. **Saisissez le chemin et le mot de passe pour le fichier de sauvegarde :**

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

3. **Vérifiez les informations de configuration :**

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

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

Gestion des stockages de clés avec `vcaadm`

Un stockage de clés est un référentiel pour clé matérielle. Des responsables de la sécurité et des utilisateurs sont associés à un stockage de clés. Les stockages de clés fournissent non seulement un espace de stockage, mais permettent également aux objets clés d'être détenus par les comptes utilisateur. Cela permet de dissimuler les clés aux applications qui ne sont pas authentifiées comme les détentrices. Les stockages de clés disposent de trois composants :

- **Objets clés** : clés de longue durée stockées pour les applications telles que le serveur Web Sun ONE.
- **Comptes utilisateur** : ces comptes permettent aux applications d'authentifier des clés spécifiques et d'y accéder.
- **Comptes de responsables de la sécurité** : ces comptes donnent accès aux fonctions de gestion de clé via `vcaadm`.

Remarque – Une carte Crypto Accelerator 4000 de Sun unique doit avoir exactement un stockage de clés. Plusieurs cartes Crypto Accelerator 4000 de Sun peuvent être configurées pour fonctionner de manière collective avec le même stockage de clés, afin de fournir des performances supplémentaires et une tolérance aux pannes.

Conditions de dénomination

Les noms de responsables de la sécurité, les noms d'utilisateur et les noms de stockage de clés doivent respecter les conditions suivantes :

TABLEAU 4-4 Conditions pour l'attribution des noms de responsables de la sécurité, d'utilisateur et de stockage de clés

Condition de dénomination	Description
Longueur minimale	Au moins un caractère
Longueur maximale	63 caractères pour les noms d'utilisateur et 32 caractères pour les noms de stockage de clés
Caractères valides	Alphanumérique, trait de soulignement (_), tiret (-) et point (.)
Premier caractère	Doit être alphabétique

Conditions pour le mot de passe

Les conditions pour l'attribution du mot de passe varient selon le paramètre `set passreq` défini (`low`, `med` ou `high`).

Définition des conditions pour le mot de passe

Utilisez la commande `set passreq` pour définir les conditions du mot de passe pour la carte Crypto Accelerator 4000 de Sun. Cette commande définit les conditions relatives aux caractères du mot de passe pour les mots de passe demandés par `vcaadm`. Il existe trois paramètres pour les conditions du mot de passe :

TABLEAU 4-5 Paramètres conditionnels du mot de passe

Définition du mot de passe	Conditions requises
`low`	Ne nécessite aucune restriction pour le mot de passe. Il s'agit du paramètre par défaut lorsque la carte n'est pas en mode FIPS.
`med`	Nécessite au moins six caractères, un caractère ne devant pas être alphabétique. Il s'agit du paramètre par défaut lorsque la carte est en mode FIPS 140-2 et cela correspond aux conditions de mot de passe minimales requises autorisées en mode FIPS 140-2.
`high`	Nécessite au moins huit caractères, trois caractères devant être alphabétiques et un caractère ne devant pas être alphabétique. Ce paramètre n'est pas une valeur par défaut et doit être configuré manuellement.

Pour modifier les conditions du mot de passe, saisissez la commande `set passreq`, suivie de `low`, `med` ou `high`. Les commandes suivantes définissent les conditions du mot de passe pour une carte Crypto Accelerator 4000 de Sun sur `high` :

```
vcaadm{vcaN@nomhôte, resp_sécurité}> set passreq high

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

Remplissage d'un stockage de clés avec des responsables de la sécurité

Il peut y avoir plusieurs responsables de la sécurité pour un stockage de clés. Les noms des responsables de la sécurité sont connus uniquement au sein du domaine de la carte Crypto Accelerator 4000 de Sun et il n'est pas nécessaire qu'ils soient identiques à des noms d'utilisateur sur le système hôte.

Lors de la création d'un responsable de la sécurité, le nom est un paramètre facultatif sur la ligne de commandes. Si le nom du responsable de la sécurité est omis, `vcaadm` vous invite à l'entrer (reportez-vous à la section « Conditions de dénomination », page 72).

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

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

Remplissage d'un stockage de clés avec des utilisateurs

Ces noms d'utilisateur sont connus uniquement au sein du domaine de la carte Crypto Accelerator 4000 de Sun et il n'est pas nécessaire qu'ils soient identiques au nom d'utilisateur UNIX sous lequel le serveur Web s'exécute.

Lors de la création d'un utilisateur, le nom est un paramètre facultatif sur la ligne de commande. Si le nom de l'utilisateur est omis, `vcaadm` vous invite à l'entrer (reportez-vous à la section « Conditions de dénomination », page 72).

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

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

Les utilisateurs doivent utiliser ce mot de passe lors de l'authentification effectuée au cours du démarrage d'un serveur Web.

Attention – Les utilisateurs doivent mémoriser leur mot de passe ; sans mot de passe, ils ne pourront pas accéder à leurs clés. Il est impossible de récupérer un mot de passe oublié.

Remarque – Le compte utilisateur est fermé si aucune commande n'est entrée pendant plus de cinq minutes. Cette option peut être modifiée ; consultez la section « Définition du délai de déconnexion automatique », page 80 pour plus de détails.

Liste des utilisateurs et des responsables de la sécurité

Pour répertorier les utilisateurs et les responsables de la sécurité associés à un stockage de clés, saisissez la commande `show user` ou `show so`.

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


vcaadm{vcaN@nomhôte, resp_sécurité}> show so
Security Officer
-------------------------------------------------------
resp_sécurité
Alice
Bob
-------------------------------------------------------
```

Modification des mots de passe

Seuls les mots de passe des responsables de la sécurité peuvent être modifiés avec `vcaadm` et les responsables de la sécurité peuvent modifier uniquement leur mot de passe. Utilisez la commande `set password` pour modifier les mots de passe des responsables de la sécurité.

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

Les mots de passe utilisateur peuvent être modifiés via l'interface PKCS#11 avec l'utilitaire `modutil` du serveur Web Sun ONE. Reportez-vous à la documentation du serveur Web Sun ONE pour `modutil` pour plus de détails.

Activation ou désactivation des utilisateurs

Remarque – Les responsables de la sécurité ne peuvent pas être désactivés : une fois créés, ils restent activés jusqu'à ce qu'ils soient supprimés.

Par défaut, chaque utilisateur est créé avec le statut activé. Les utilisateurs peuvent être désactivés. Les utilisateurs désactivés ne peuvent pas accéder à leur clé matérielle via l'interface PKCS#11. L'activation d'un utilisateur désactivé restaurera l'accès à l'ensemble de ses clés matérielles.

Lors de l'activation ou de la désactivation d'un utilisateur, le nom est un paramètre facultatif sur la ligne de commandes. Si le nom de l'utilisateur est omis, `vcaadm` vous invite à l'entrer. Pour désactiver un compte utilisateur, saisissez la commande `disable user`.

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

Pour activer un compte, saisissez la commande `enable user`.

```
vcaadm{vcaN@nomhôte, resp_sécurité}> enable user Tom
User Tom enabled.

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

Suppression des utilisateurs

Exécutez la commande `delete user` en spécifiant l'utilisateur à supprimer. Lors de la suppression d'un utilisateur, le nom est un paramètre facultatif sur la ligne de commande. Si le nom de l'utilisateur est omis, `vcaadm` vous invite à l'entrer.

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

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

Suppression des responsables de la sécurité

Exécutez la commande `delete so` en spécifiant le responsable de la sécurité à supprimer. Lors de la suppression d'un responsable de la sécurité, le nom est un paramètre facultatif sur la ligne de commande. Si le nom est omis, `vcaadm` vous invite à l'entrer.

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

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

Sauvegarde de la clé principale

Les stockages de clés sont stockés sur le disque et chiffrés dans une clé principale, qui est alors stockée dans le microprogramme Crypto Accelerator 4000 de Sun et peut être sauvegardée par un responsable de la sécurité.

Pour sauvegarder la clé principale, utilisez la commande `backup`. Cette commande nécessite un nom de chemin vers un fichier où sera stockée la sauvegarde. Ce nom de chemin peut être placé sur la ligne de commande ou, s'il est omis, `vcaadm` vous invitera à l'indiquer.

Un mot de passe doit être défini pour les données de sauvegarde. Il est utilisé pour chiffrer la clé principale figurant dans le fichier de sauvegarde.

```
vcaadm{vcaN@nomhôte, resp_sécurité}> 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.
```

Attention – Choisissez un mot de passe difficile à deviner lors de la création de fichiers de sauvegarde, car il protège la clé principale de votre stockage de clés. Vous devez également vous souvenir du mot de passe que vous avez saisi. Sans mot de passe, vous ne pourrez pas accéder au fichier de sauvegarde de la clé principale. Il n'existe aucun moyen de récupérer les données protégées par un mot de passe perdu.

Verrouillage du stockage de clés pour empêcher les sauvegardes

Un site peut disposer d'une politique de sécurité stricte qui interdit à la clé principale d'une carte Crypto Accelerator 4000 de Sun de quitter le matériel. Pour cela, vous pouvez utiliser la commande `set lock`.

Attention – Une fois cette commande exécutée, tous les essais de sauvegarde de la clé principale échoueront. Ce verrouillage perdure même si la clé principale est recomposée. Le seul moyen d'effacer ce paramètre consiste à remettre à zéro la carte Crypto Accelerator 4000 de Sun à l'aide de la commande `zeroize`. Reportez-vous à la section « Remise à zéro d'une Carte Crypto Accelerator 4000 de Sun », page 84.

```
vcaadm{vcaN@nomhôte, resp_sécurité}> 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.
```

Gestion des cartes avec `vcaadm`

Cette section explique comment gérer les cartes Crypto Accelerator 4000 de Sun avec l'utilitaire `vcaadm`.

Définition du délai de déconnexion automatique

Pour personnaliser la durée après laquelle un responsable de la sécurité est automatiquement déconnecté de la carte, utilisez la commande `set timeout`. Pour modifier la durée de déconnexion automatique, entrez la commande `set timeout` suivie d'un chiffre unique désignant le nombre de minutes après lequel un responsable de la sécurité sera automatiquement déconnecté. Une valeur nulle (0) désactive la fonction de déconnexion automatique ; la durée maximale est de 1 440 minutes (soit 24 heures). La valeur par défaut pour une carte Crypto Accelerator 4000 de Sun nouvellement initialisée est de 5 minutes.

La commande suivante redéfinit sur 10 minutes le délai de déconnexion automatique pour un responsable de la sécurité :

```
vcaadm{vcaN@nomhôte, resp_sécurité}> set timeout 10
```

Affichage de l'état de la carte

Pour connaître l'état actuel d'une carte Crypto Accelerator 4000 de Sun, exécutez la commande `show status`. Cette commande affiche les versions du matériel et du microprogramme de la carte, l'adresse MAC et l'état (ascendant/descendant, vitesse, duplex, etc.) de l'interface réseau, ainsi que le nom et l'ID du stockage de clés.

```
vcaadm{vcaN@nomhôte, resp_sécurité}> 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: nom_stockageclés
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
----------------------------------------------------------------
```

Détermination du mode de fonctionnement de la carte

Si la carte Crypto Accelerator 4000 de Sun fonctionne en mode FIPS 140-2, la commande `show status` imprime la ligne suivante :

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

Si la carte ne fonctionne pas en mode FIPS 140-2, la commande `show status` n'imprime aucune ligne spécifiant le mode FIPS 140-2.

Vous pouvez également utiliser l'utilitaire `kstat`(1M) pour déterminer si la carte fonctionne en mode FIPS 140-2. Le paramètre `kstat`(1M), `vs-mode`, renvoie une valeur de `FIPS` si la carte fonctionne en mode FIPS 140-2. Reportez-vous à la section « Statistiques cryptographiques et de fonctionnement du pilote Ethernet Crypto Accelerator 4000 de Sun », page 45 et à la page manuel en ligne pour plus d'informations sur `kstat`(1M).

Chargement d'un nouveau microprogramme

Il est possible de mettre à jour le microprogramme de la carte Crypto Accelerator 4000 de Sun quand de nouvelles fonctions sont ajoutées. Pour charger le microprogramme, exécutez la commande `loadfw` et fournissez un chemin vers le fichier du microprogramme.

Pour que la mise à jour soit réussie, vous devez réinitialiser manuellement la carte à l'aide de la commande `reset` ; le responsable de la sécurité actuellement connecté est alors déconnecté.

```
vcaadm{vcaN@nomhôte, resp_sécurité}> loadfw /opt/SUNWconn/cryptov2/firmware/sca4000fw
Security Officer Login: resp_sécurité
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
```

Réinitialisation d'une Carte Crypto Accelerator 4000 de Sun

Dans certaines circonstances, il peut être nécessaire de réinitialiser la carte. Pour ce faire, exécutez la commande `reset`. Un message de confirmation s'affichera. La réinitialisation d'une carte Crypto Accelerator 4000 de Sun peut interrompre temporairement l'accélération de la cryptographie sur le système, à moins que d'autres cartes Crypto Accelerator 4000 de Sun actives puissent prendre le relais. En outre, cette commande vous déconnecte automatiquement de `vcaadm` ; vous devrez alors vous reconnecter au périphérique en vous reconnectant à `vcaadm` si vous désirez en poursuivre l'administration.

```
vcaadm{vcaN@nomhôte, resp_sécurité}> 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.
```

Recomposition d'une Carte Crypto Accelerator 4000 de Sun

Au fil du temps, du fait de votre politique de sécurité, il peut s'avérer nécessaire d'utiliser de nouvelles clés comme clé principale ou comme clé d'accès à distance. La commande `rekey` vous permet de régénérer l'une de ces clés ou les deux.

La recomposition d'une clé principale provoque également le rechiffrement du stockage de clés sous la nouvelle clé, et invalide les fichiers de clé principale sauvegardés avec le nouveau fichier de stockage de clés. Il est conseillé de sauvegarder la clé principale avant de la recomposer. Si vous disposez de plusieurs cartes Crypto Accelerator 4000 de Sun utilisant le même stockage de clés, vous devez sauvegarder cette nouvelle clé principale et la restaurer pour les autres cartes.

La recomposition d'une clé d'accès à distance déconnecte le responsable de la sécurité, en forçant une nouvelle connexion qui utilise la nouvelle clé d'accès à distance.

Vous pouvez spécifier l'un des trois types de clé lors de l'exécution de la commande `rekey` :

TABLEAU 4-6 Types de clé

Type de clé	Action
`master`	Recompose la clé principale.
`remote`	Recompose la clé d'accès à distance. Déconnecte le responsable de la sécurité.
`all`	Recompose les clés principale et d'accès à distance.

L'exemple suivant illustre la saisie d'un type de clé `all` avec la commande `rekey` :

```
vcaadm{vcaN@nomhôte, resp_sécurité}> 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.
```

Remise à zéro d'une Carte Crypto Accelerator 4000 de Sun

Dans certains cas, il peut s'avérer nécessaire d'effacer toutes les clés matérielles d'une carte. Il existe deux méthodes pour y parvenir. La première méthode consiste à utiliser un cavalier matériel ; cette forme de remise à zéro restaure l'état d'origine (mode `failsafe`) de la carte Crypto Accelerator 4000 de Sun. Reportez-vous à la section « Restauration de l'état par défaut du matériel Crypto Accelerator 4000 de Sun », page 175. La seconde méthode consiste à utiliser la commande `zeroize`.

Remarque – La commande `zeroize` supprime uniquement la clé matérielle, sans affecter le microprogramme mis à jour (le cas échéant). Cette commande déconnecte également le responsable de la sécurité si elle se termine normalement.

Pour remettre à zéro une carte à l'aide de la commande `zeroize`, entrez la commande suivante :

```
vcaadm{vcaN@nomhôte, resp_sécurité}> 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.
```

Utilisation de la commande `vcaadm diagnostics`

Outre SunVTS, les diagnostics peuvent être exécutés depuis l'utilitaire `vcaadm`. La commande `diagnostics` dans `vcaadm` couvre trois catégories principales du matériel Crypto Accelerator 4000 de Sun : matériel général, sous-système cryptographique et sous-système de réseau. Les tests pour le matériel général couvrent la mémoire vive dynamique, la mémoire flash, le bus PCI, le contrôleur DMA et d'autres matériels internes. Les tests pour le sous-système cryptographique couvrent les générateurs de nombres aléatoires et les accélérateurs cryptographiques. Les tests du sous-système de réseau couvrent le périphérique `vca`.

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

Utilisation de vcadiag

Le programme vcadiag fournit une interface de ligne de commande à la carte Crypto Accelerator 4000 de Sun qui autorise les utilisateurs racines à exécuter des tâches administratives sans qu'ils aient à s'authentifier comme responsables de la sécurité. Les options de la ligne de commande déterminent les actions exécutées par vcadiag.

Pour accéder facilement au programme vcadiag, placez le répertoire d'outils Crypto Accelerator 4000 de Sun dans votre chemin de recherche. Par exemple :

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

La syntaxe de la ligne de commande vcadiag est la suivante :

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

Remarque – Lorsque vous utilisez les attributs [-DFKRZ], vca*N* est le nom de périphérique de la carte, où *N* correspond au numéro d'instance du périphérique Crypto Accelerator 4000 de Sun.

Le TABLEAU 4-7 présente les options de l'utilitaire `vcadiag`.

TABLEAU 4-7 Options `vcadiag`

Option	Description
`-D vca`*N*	Exécute les diagnostics sur la carte Crypto Accelerator 4000 de Sun.
`-F vca`*N*	Affiche l'empreinte de la clé publique utilisée par la carte Crypto Accelerator 4000 de Sun pour la sécurisation des sessions d'administration.
`-K vca`*N*	Affiche la clé publique et son empreinte utilisées par la carte Crypto Accelerator 4000 de Sun pour la sécurisation des sessions d'administration.
`-Q`	Fournit des informations sur les périphériques et les composants logiciels Crypto Accelerator 4000 de Sun. La sortie est une liste des informations suivantes séparées par des deux-points : périphérique, fonction interne, nom du stockage de clés, numéro de série du stockage de clés et numéro de référence du stockage de clés. Vous pouvez utiliser cette commande pour déterminer l'association entre les périphériques et les stockages de clés.
`-R vca`*N*	Réinitialise la carte Crypto Accelerator 4000 de Sun.
`-Z vca`*N*	Remet la carte Crypto Accelerator 4000 de Sun à zéro.

L'exemple suivant illustre l'option `-D` :

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

L'exemple suivant illustre l'option `-F` :

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

L'exemple suivant illustre l'option `-K` :

```
# 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
```

L'exemple suivant illustre l'option `-Q` :

```
# 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
```

L'exemple suivant illustre l'option `-R` :

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

L'exemple suivant illustre l'option `-Z` :

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

CHAPITRE 5

Configuration du logiciel du serveur Sun ONE pour une utilisation avec la Carte Crypto Accelerator 4000 de Sun

Ce chapitre explique comment configurer la carte Crypto Accelerator 4000 de Sun pour une utilisation avec un serveur Web Sun ONE. Il est composé des sections suivantes :

Remarque – Les serveurs Web Sun ONE décrits dans ce manuel étaient précédemment nommés serveurs Web iPlanet™.

Administration de la sécurité pour les serveurs Web Sun ONE

Cette section présente les fonctions de sécurité de la carte Crypto Accelerator 4000 de Sun administrée avec un serveur Sun ONE.

Remarque – Pour pouvoir gérer des stockages de clés, votre système doit avoir accès au compte de l'administrateur système.

Concepts et terminologie

Des stockages de clés et des utilisateurs doivent être créés pour les applications communiquant avec la carte Crypto Accelerator 4000 de Sun par une interface PKCS#11, telles que le serveur Sun ONE.

Les utilisateurs de la Crypto Accelerator 4000 de Sun sont les propriétaires des clés matérielles cryptographiques. Chaque clé est détenue par un seul utilisateur. Chaque utilisateur peut détenir plusieurs clés. Il est possible qu'un utilisateur détienne plusieurs clés pour prendre en charge différentes configurations, telles qu'une clé `production` et une clé `développement` (marquant les différents organismes de l'utilisateur).

Remarque – Les termes *utilisateur* ou *compte utilisateur* se rapportent aux utilisateurs de Crypto Accelerator 4000 de Sun créés dans `vcaadm` et non pas aux comptes utilisateur UNIX traditionnels. Il n'existe pas de mappage fixe entre les noms d'utilisateur UNIX et ceux de la carte Crypto Accelerator 4000 de Sun.

Un stockage de clés est un référentiel pour clé matérielle. Des responsables de la sécurité et des utilisateurs sont associés à un stockage de clés. Non seulement les stockages de clés fournissent un espace de stockage, mais ils permettent également aux objets clés d'être détenus par les comptes utilisateur. Cela permet de dissimuler les clés aux applications qui ne sont pas authentifiées comme les détentrices. Les stockages de clés disposent de trois composants :

- **Objets clés** : clés de longue durée stockées pour les applications telles que le serveur Web Sun ONE.
- **Comptes utilisateur** : ces comptes permettent aux applications d'authentifier des clés spécifiques et d'y accéder.
- **Comptes de responsables de la sécurité** : ces comptes donnent accès aux fonctions de gestion de clé via `vcaadm`.

Remarque – Une carte Crypto Accelerator 4000 de Sun unique doit avoir exactement un stockage de clés. Plusieurs cartes Crypto Accelerator 4000 de Sun peuvent être configurées pour fonctionner de manière collective avec le même stockage de clés afin de fournir des performances supplémentaires et une tolérance aux pannes.

Une installation type comprend un stockage de clés et un utilisateur uniques. Par exemple, une telle configuration peut être composée d'un stockage de clés unique *web_server* et d'un utilisateur unique dans ce stockage de clés, *web_admin* ; ce qui autorise l'utilisateur *web_admin* à obtenir et à maintenir le contrôle d'accès des clés du serveur au sein d'un stockage de clés unique.

Un outil d'administration, `vcaadm`, permet de gérer les domaines et les utilisateurs de la carte Crypto Accelerator 4000 de Sun. Reportez-vous à la section « Gestion des stockages de clés avec `vcaadm` », page 72.

Jetons et fichiers de jetons

Les *stockages de clés* apparaissent sur les serveurs Web Sun ONE comme des *jetons*. Les fichiers de jetons constituent pour les administrateurs de la carte Crypto Accelerator 4000 de Sun une technique de présentation de jetons spécifiques à une application donnée.

Exemple

Soit trois stockages de clés : *engineering*, *finance* et *legal*. Les jetons suivants sont présentés au serveur Web Sun ONE :

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

Fichiers de jetons

Pour ignorer la case par défaut, un fichier de jetons doit exister. Certaines applications ne peuvent pas gérer plusieurs jetons. Les fichiers de jetons sont des fichiers texte qui contiennent un ou plusieurs noms de jetons, un par ligne.

Remarque – Les noms de jetons et de stockages de clés sont identiques.

Un serveur Web Sun ONE présente uniquement les jetons répertoriés dans le fichier de jetons. Les méthodes de spécification des fichiers de jetons sont les suivantes (par ordre de priorité) :

1. Le fichier nommé par la variable d'environnement `SUNW_PKCS11_TOKEN_FILE`

   Certains logiciels suppriment les variables d'environnement, auquel cas cette approche peut être irréalisable.

2. Le fichier `$HOME/.SUNWconn_cryptov2/tokens`

   Ce fichier doit exister dans le répertoire d'accueil de l'utilisateur UNIX sous lequel s'exécute le serveur Web Sun ONE. Il se peut que le serveur Web Sun ONE s'exécute sous le nom d'un utilisateur UNIX ne disposant d'aucun répertoire d'accueil ; dans ce cas, cette approche peut être irréalisable.

3. Le fichier `/etc/opt/SUNWconn/cryptov2/tokens`

Si aucun fichier de jetons n'existe, le logiciel Crypto Accelerator 4000 de Sun présente tous les jetons aux serveurs Web Sun ONE.

L'exemple suivant illustre le contenu d'un fichier de jetons :

```
================================
# 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.

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

Remarque – Les commentaires sont précédés d'un signe dièse (#) et les lignes vierges sont acceptables.

Si aucun des fichiers ci-dessus n'est trouvé, alors la méthode par défaut décrite dans la section « Jetons et fichiers de jetons », page 91 est utilisée.

Activation et désactivation d'un chiffrement de masse

La fonction de chiffrement de masse pour le logiciel du serveur Sun ONE est désactivée par défaut. Vous pouvez activer cette fonction pour le transfert sécurisé des fichiers volumineux.

Pour activer le logiciel du serveur Sun ONE afin d'utiliser le chiffrement de masse sur la carte Crypto Accelerator 4000 de Sun, créez simplement un fichier vide nommé `sslreg` dans le répertoire `/etc/opt/SUNWconn/cryptov2/` et redémarrez le logiciel du serveur.

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

Pour désactiver la fonction de chiffrement de masse, supprimez le fichier `sslreg` et redémarrez le logiciel du serveur.

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

Configuration des serveurs Web Sun ONE

Cette section traite des points suivants :

Mots de passe

Vous devez saisir plusieurs mots de passe au cours de l'activation d'un serveur Web Sun ONE. Le TABLEAU 5-1 décrit chacun d'eux. Il sera fait référence à ces mots de passe au cours de ce chapitre. Si vous ne savez pas lequel utiliser, reportez-vous au TABLEAU 5-1.

TABLEAU 5-1 Mots de passe requis pour les serveurs Sun ONE

Type de mot de passe	Description
Serveur d'administration Sun ONE	Requis pour démarrer le serveur d'administration Sun ONE. Ce mot de passe a été attribué lors de la configuration du serveur Web Sun ONE.
Base de données certifiée du serveur Web	Requis pour démarrer le module cryptographique interne lors de l'exécution en mode sécurisé. Ce mot de passe a été attribué lors de la création d'une base de données certifiée à partir du serveur d'administration Sun ONE. Il est également requis lorsque vous effectuez une demande de certificats et que vous les installez dans le module cryptographique interne.
Responsable de la sécurité	Requis lors de l'exécution d'opérations privilégiées `vcaadm`.
nomutilisateur:motpasse	Requis pour démarrer le module Crypto Accelerator 4000 de Sun lors de l'exécution en mode sécurisé. Il est également requis lorsque vous effectuez une demande de certificats et que vous les installez dans le module cryptographique interne (*nom_stockageclés*). Ce mot de passe comprend le *nom d'utilisateur* et le *mot de passe* d'un utilisateur de stockage de clés créé dans `vcaadm`. Le *nom d'utilisateur* et le *mot de passe* du stockage de clés sont séparés par un signe deux-points (:).

Remplissage d'un stockage de clés

Avant que vous ne puissiez activer la carte pour l'utiliser avec un serveur Web Sun ONE, vous devez d'abord l'initialiser et ajouter au moins un utilisateur au stockage de clés correspondant. Le stockage de clés de la carte est créé au cours de l'initialisation. Vous pouvez initialiser les cartes Crypto Accelerator 4000 de Sun pour utiliser un stockage de clés existant. Reportez-vous à la section « Initialisation de la Carte Crypto Accelerator 4000 de Sun avec `vcaadm` », page 68.

Remarque – Un seul stockage de clés peut et doit être configuré par carte Crypto Accelerator 4000 de Sun. Plusieurs cartes Crypto Accelerator 4000 de Sun peuvent être configurées pour fonctionner de manière collective avec le même stockage de clés afin de fournir des performances supplémentaires et une tolérance aux pannes.

▼ Pour remplir un stockage de clés

1. **Placez le répertoire des outils Crypto Accelerator 4000 de Sun dans votre chemin de recherche, si vous ne l'avez déjà fait. Par exemple :**

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

2. **Accédez à l'utilitaire** `vcaadm` **à l'aide de la commande** `vcaadm` **ou entrez** `vcaadm -h` ***nomhôte*** **pour connecter** `vcaadm` **à une carte sur un hôte distant.**

   Reportez-vous à la section « Utilisation de `vcaadm` », page 57.

```
$ vcaadm -h nomhôte
```

3. **Remplissez le stockage de clés de la carte avec des utilisateurs.**

   Ces noms d'utilisateur sont connus uniquement au sein du domaine de la carte Crypto Accelerator 4000 de Sun et il n'est pas nécessaire qu'ils soient identiques au nom d'utilisateur UNIX sous lequel le serveur Web s'exécute. Avant de créer l'utilisateur, pensez au préalable à vous connecter en tant que responsable de la sécurité `vcaadm`.

4. **Créez un utilisateur à l'aide de la commande** `create user`**.**

```
vcaadm{vcaN@nomhôte, resp_sécurité}> create user username
Initial password:
Confirm password:
User nomutilisateur created successfully.
```

   Les *nom d'utilisateur* et *mot de passe* créés ici de manière collective composent le *nomutilisateur:motpasse* (voir TABLEAU 5-1). Vous devez utiliser ce mot de passe lors de l'authentification effectuée au cours du démarrage d'un serveur Web. Il s'agit d'un mot de passe de stockage de clés pour un utilisateur unique.

Attention – Les utilisateurs doivent mémoriser ce *nomutilisateur:motpasse* ; sinon, ils ne pourront pas accéder à leurs clés. Il est impossible de récupérer un mot de passe oublié.

5. **Quittez** `vcaadm`**.**

```
vcaadm{vcaN@nomhôte, resp_sécurité}> exit
```

Présentation de l'activation des serveurs Web Sun ONE

Pour activer les serveurs Web Sun ONE vous devez suivre les étapes suivantes, qui sont expliquées en détail dans les deux sections suivantes.

- Installez le serveur Web Sun ONE.
- Créez une base de données certifiée.
- Demandez un certificat.
- Installez le certificat.
- Configurez le serveur Web Sun ONE.

Attention – Vous devez exécuter cette procédure dans l'ordre indiqué, sinon vous risquez d'obtenir une configuration incorrecte.

- Si vous utilisez le serveur Web Sun ONE 4.1, reportez-vous à la section « Installation et configuration d'un serveur Web Sun ONE 4.1 », page 96.
- Si vous utilisez le serveur Web Sun ONE 6.0, reportez-vous à la section « Installation et configuration d'un serveur Web Sun ONE 6.0 », page 107.

Installation et configuration d'un serveur Web Sun ONE 4.1

Cette section décrit l'installation et la configuration d'un serveur Web Sun ONE 4.1. Il est composé des sections suivantes :

- « Installation d'un serveur Web Sun ONE 4.1 », page 97
- « Configuration d'un serveur Web Sun ONE 4.1 pour SSL », page 105

Installation d'un serveur Web Sun ONE 4.1

Vous devez respecter l'ordre des étapes. Reportez-vous à la documentation du serveur Web Sun ONE pour plus d'informations sur l'utilisation des serveurs Web Sun ONE.

▼ Pour installer le serveur Web Sun ONE 4.1

1. **Téléchargez le logiciel du serveur Web Sun ONE 4.1.**

   Ce logiciel est disponible à l'URL suivante :
   `http://www.sun.com/`

2. **Installez le serveur Web.**

   Cette section comprend des instructions s'appuyant sur un exemple donné ; vous pouvez configurer votre serveur Web Sun ONE différemment. Par défaut, le nom de chemin du serveur est : `/usr/netscape/server4`

   Acceptez le chemin par défaut pendant l'installation du serveur Web Sun ONE. Ce document fait référence aux chemins par défaut. Si vous décidez d'installer le logiciel du serveur Web à un emplacement différent, assurez-vous de noter ce dernier.

3. **Lancez le programme `setup`.**

4. **Répondez aux invites du script d'installation.**

   Pour simplifier l'utilisation vous pouvez accepter les paramètres par défaut, excepté pour les invites suivantes :

   a. **Acceptez les termes de la licence en saisissant `yes`.**

   b. **Saisissez un *nomhôte.domaine* entièrement valide.**

   c. **Entrez deux fois le mot de passe du serveur d'administration Sun ONE 4.1.**

   d. **A l'invite du système, appuyez sur Entrée.**

▼ Pour créer une base de données certifiée

1. **Démarrez le serveur d'administration Sun ONE 4.1.**

   Au lieu d'exécuter `startconsole` comme requête `setup`, démarrez le serveur d'administration Sun ONE 4.1 à l'aide de la commande suivante :

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

   La réponse indique l'URL avec laquelle vous devez vous connecter à vos serveurs.

2. **Démarrez l'interface utilisateur graphique Administration en ouvrant un navigateur Web et en saisissant :**

   ```
   http://nomhôte.domaine:port_admin
   ```

   Dans la boîte de dialogue d'authentification, saisissez le nom d'utilisateur et le mot de passe du serveur d'administration Sun ONE 4.1 que vous avez sélectionnés lors de l'exécution du programme `setup`.

   Remarque – Si vous avez utilisé les paramètres par défaut lors de la configuration du serveur Web Sun ONE, saisissez comme nom d'utilisateur `admin` ou le nom d'utilisateur du serveur d'administration Sun ONE 4.1.

   ---

3. **Sélectionnez OK.**

   La fenêtre du serveur d'administration Sun ONE 4.1 s'affiche.

4. **Créez la base de données certifiée pour l'instance du serveur Web.**

   a. **Sélectionnez l'onglet « Servers » (Serveurs) dans la fenêtre du serveur d'administration Sun ONE 4.1.**

   b. **Sélectionnez un serveur et cliquez sur le bouton « Manage » (Gestion).**

   c. **Sélectionnez l'onglet « Security » (Sécurité) dans la partie supérieure de la page et sélectionnez le lien « Create Database » (Créer une base de données).**

d. Saisissez un mot de passe (base de données certifiée du serveur Web ; voir TABLEAU 5-1**) dans les deux boîtes de dialogue et sélectionnez OK.**

Choisissez un mot de passe de huit caractères minimum. Il vous servira à démarrer les modules cryptographiques internes quand le serveur Web Sun ONE sera exécuté en mode sécurisé.

Il est recommandé d'activer la sécurité sur plusieurs instances du serveur Web. Pour cela, répétez cette opération de l'étape 1 à l'étape 4 pour chaque instance du serveur Web.

Remarque – Si vous voulez également exécuter SSL (Secure Socket Layer) sur le serveur d'administration Sun ONE 4.1, la procédure de configuration d'une base de données certifiée est similaire. Reportez-vous au guide *iPlanet Web Server, Enterprise Edition Administrator's Guide* à l'adresse suivante : `http://docs.sun.com` pour plus d'informations.

---

5. Exécutez le script suivant pour activer la carte Crypto Accelerator 4000 de Sun :

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

Ce script vous invite à choisir le serveur Web. Il installe les modules cryptographiques Crypto Accelerator 4000 de Sun pour le serveur Web Sun ONE. Puis il met à jour les fichiers de configuration pour activer la carte Crypto Accelerator 4000 de Sun.

6. Saisissez `1` pour configurer votre serveur Web Sun ONE afin d'utiliser SSL, puis appuyez sur Entrée.

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

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

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

7. **A l'invite, saisissez le chemin du répertoire racine du serveur Web, puis appuyez sur Entrée.**

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

8. **A l'invite, saisissez** `y` **et appuyez sur Entrée si vous désirez poursuivre.**

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

Using database directory /usr/netscape/server4/alias...
Module "Sun Crypto Accelerator 4000" added to database.
/usr/netscape/server4 has been configured to use
the Sun Crypto Accelerator.


<Press ENTER to continue>
```

9. **Saisissez** `0` **pour quitter.**

▼ Pour créer un certificat de serveur

1. **Redémarrez le serveur d'administration Sun ONE 4.1 en saisissant les commandes suivantes :**

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

La réponse indique l'URL avec laquelle vous devez vous connecter à vos serveurs.

2. **Démarrez l'interface utilisateur graphique Administration en ouvrant un navigateur Web et en saisissant :**

```
http://nomhôte.domaine:port_admin
```

Dans la boîte de dialogue d'authentification, saisissez le nom d'utilisateur et le mot de passe du serveur d'administration Sun ONE 4.1 que vous avez sélectionnés lors de l'exécution du programme `setup`.

Remarque – Si vous avez utilisé les paramètres par défaut lors de la configuration du serveur Web Sun ONE, saisissez comme nom d'utilisateur `admin` ou le nom d'utilisateur du serveur d'administration Sun ONE 4.1.

---

3. **Sélectionnez OK.**

   La fenêtre du serveur d'administration Sun ONE 4.1 s'affiche.

4. **Pour demander le certificat du serveur, sélectionnez l'onglet « Security » (Sécurité) dans la partie supérieure de la fenêtre du serveur d'administration Sun ONE 4.1 (**FIGURE 5-1**).**

   La page « Create Trust Database » (Création d'une base de données certifiée) s'affiche.

5. **Sélectionnez le lien « Request a Certificate » (Demander un certificat) dans le volet de gauche (**FIGURE 5-1**).**

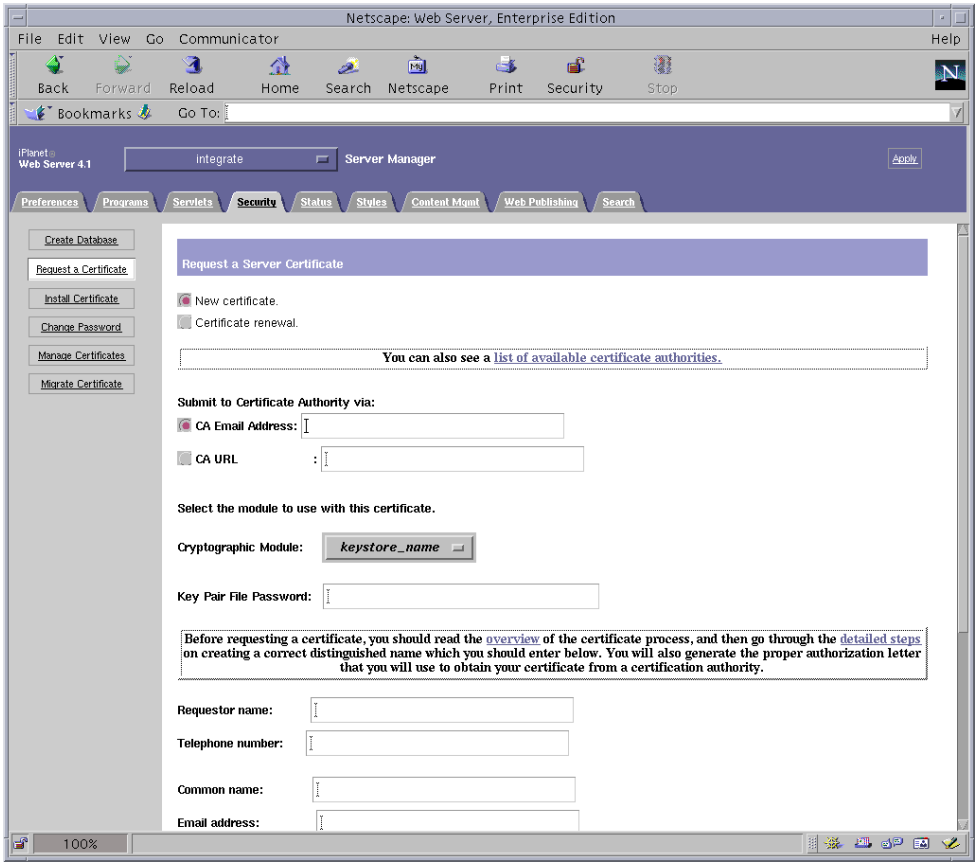

FIGURE 5-1 Page « Request a Server Certificate » (Demande d'un certificat de serveur) du serveur d'administration Sun ONE 4.1

6. **Remplissez le formulaire pour créer une demande de certificat, à l'aide des informations suivantes :**

   a. **Sélectionnez un nouveau certificat.**

      Si vous pouvez envoyer directement votre demande de certificat à une autorité de certification ou d'enregistrement sur le Web, sélectionnez le lien URL de l'autorité de certification. Sinon, dans le champ « CA Email Address » (Adresse électronique de l'autorité de certification), saisissez une adresse électronique à laquelle vous voulez envoyer votre demande de certificat.

b. Sélectionnez le module cryptographique à utiliser.

Chaque stockage de clés dispose de sa propre entrée dans ce menu déroulant. Assurez-vous de sélectionner le stockage de clés adéquat. Ne sélectionnez pas uniquement l'accélération SUNW.

c. Dans la boîte de dialogue « Key Pair File Password » (Mot de passe de fichier de paire de clés), saisissez le mot de passe de l'utilisateur qui détiendra la clé.

Ce mot de passe est *nomutilisateur:motpasse* (TABLEAU 5-1).

d. Indiquez les informations appropriées pour les champs d'informations sur le demandeur suivants :

TABLEAU 5-2 Champs d'informations sur le demandeur

Champ	Description
Requestor Name	(Nom du demandeur) Coordonnées du demandeur.
Telephone Number	(Téléphone du demandeur) Coordonnées du demandeur.
Common Name	(Nom commun) Domaine du site Web saisi dans le navigateur d'un visiteur *nomhôte.domaine.*
Email Address	(Adresse électronique) Coordonnées du demandeur.
Organization	(Organisme) Organisme à déclarer sur le certificat.
Organizational Unit	(Unité de l'organisme - facultatif) Unité de l'organisme qui sera déclarée sur le certificat.
Locality	(Localité - facultatif) Ville, département, principauté ou pays, également déclaré(e) sur le certificat, le cas échéant.
State	(Etat - facultatif) Le nom complet de l'état.
Country	(Pays) Code ISO de deux lettres désignant le pays (par exemple, US pour les Etats-Unis).

e. Sélectionnez le bouton OK pour envoyer les informations.

7. Faites appel à une autorité de certification pour créer le certificat.

- Si vous choisissez d'envoyer votre demande de certificat à l'URL d'une autorité de certification, elle sera automatiquement envoyée à cette adresse.
- Si vous choisissez une adresse électronique d'autorité de certification, copiez la demande de certificat qui vous a été envoyée avec les en-têtes et remettez-la à l'autorité de certification.

8. Une fois le certificat créé, copiez-le avec les en-têtes dans le presse-papiers.

Remarque – Le certificat est différent de la demande de certificat et il vous est généralement présenté sous forme de texte. Conservez ces données dans le presse-papiers pour l'étape 5 de la section suivante.

▼ Pour installer le certificat de serveur

1. **Sélectionnez le lien « Install Certificate » (Installer le Certificat) dans la partie gauche de la fenêtre du serveur d'administration Sun ONE 4.1.**

   Une fois votre demande approuvée par une autorité de certification et votre certificat délivré, vous devez installer ce dernier sur le serveur Sun ONE.

2. **Sélectionnez l'onglet « Security » (Sécurité).**

3. **Dans le volet de gauche, sélectionnez le lien « Install Certificate » (Installer le certificat).**

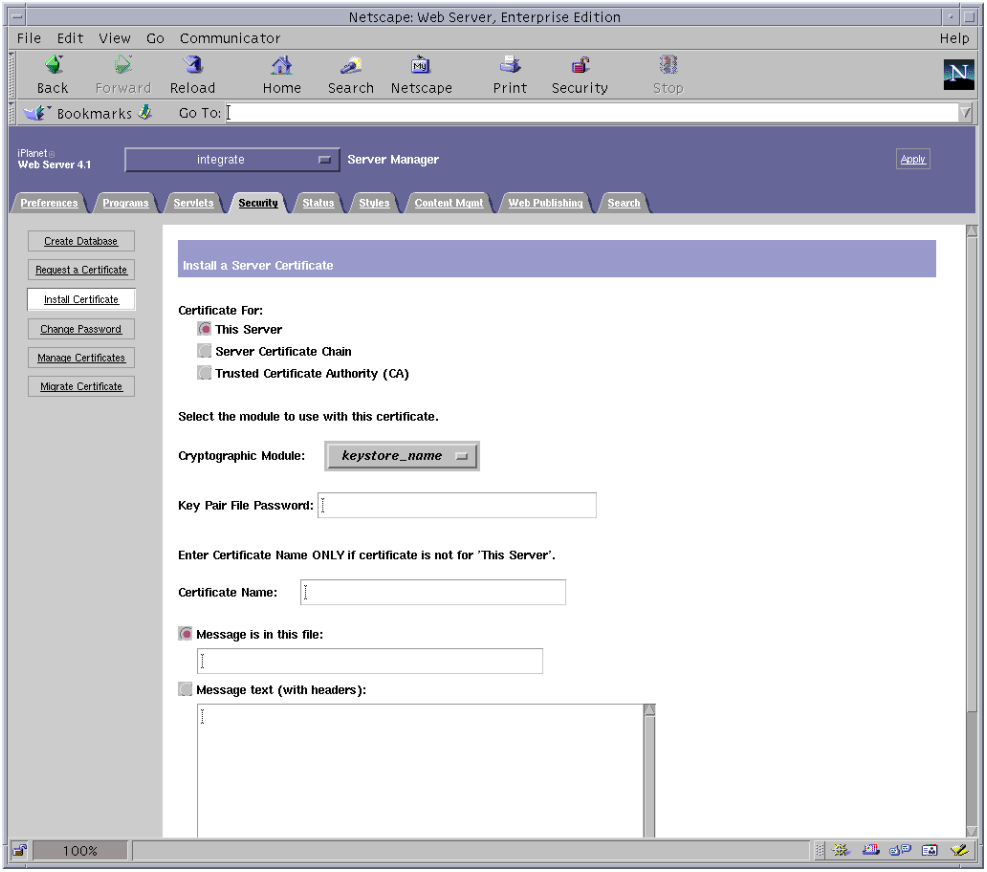

FIGURE 5-2 Page « Install a Server Certificate » (Installation d'un certificat de serveur) du serveur d'administration Sun ONE 4.1

4. **Remplissez le formulaire pour installer votre certificat :**

TABLEAU 5-3 Champs du certificat à installer

Champs	Description
Certificate For	(Certificat pour) Ce serveur
Cryptographic Module	(Module cryptographique) Chaque stockage de clés dispose de sa propre entrée dans ce menu déroulant. Veillez à sélectionner le nom de stockage de clés correct. Pour utiliser Crypto Accelerator 4000 de Sun, vous devez sélectionner un module avec le même nom que celui attribué au stockage de clés.
Key Pair File Password	(Mot de passe du fichier de paire de clés) Ce mot de passe est *nomutilisateur:motpasse* (TABLEAU 5-1).
Certificate Name	(Nom du certificat) Dans la plupart des cas, vous pouvez laisser ce champ vierge. Si vous saisissez un nom, celui-ci modifiera le nom utilisé par le serveur Web pour accéder au certificat et à la clé lors de l'exécution avec prise en charge SSL. La valeur par défaut de ce champ est `Server-Cert`.

5. **Collez le certificat copié dans l'autorité de certificat (à l'étape 8 de la section « Pour créer un certificat de serveur », page 100) dans la zone de texte « Message ».**

   Des informations de base sur le certificat s'affichent alors.

6. **Sélectionnez le bouton « OK » dans la partie inférieure de la page.**

7. **Si tout vous semble correct, sélectionnez le bouton « Add Server Certificate » (Ajouter le certificat de serveur).**

   Des messages vous invitent à redémarrer le serveur, ce qui n'est pas nécessaire car l'instance du serveur Web a été arrêtée pendant toute la durée des opérations.

   Vous êtes également averti que le serveur Web doit être configuré de manière à pouvoir utiliser SSL. Suivez la procédure suivante pour configurer le serveur Web.

Configuration d'un serveur Web Sun ONE 4.1 pour SSL

Maintenant que le serveur Web et le certificat du serveur sont installés, vous devez configurer le serveur Web pour SSL.

▼ Pour configurer le serveur Web Sun ONE 4.1

1. **Dans la page principale du serveur d'administration Sun ONE 4.1, sélectionnez l'instance du serveur Web dans laquelle vous désirez travailler et sélectionnez « Manage » (Gestion).**

2. **Si l'onglet « Preferences » (Préférences) n'est pas sélectionné dans la partie supérieure de la page, sélectionnez-le.**

3. **Cliquez sur le lien « Encryption On/Off » (Chiffrement activé/désactivé) dans la partie gauche de la page.**

4. **Activez le chiffrement (On).**

   Le champ « Port » de la boîte de dialogue doit faire apparaître le numéro de port SSL par défaut : 443. Modifiez le numéro de port si nécessaire.

5. **Sélectionnez le bouton OK.**

6. **Appliquez ces modifications en sélectionnant le bouton « Save » (Enregistrer).**

   Le serveur Web est maintenant configuré pour une exécution en mode sécurisé.

7. **Modifiez le fichier** `/usr/netscape/server4/https-`*nomhôte*`/config/magnus.conf` **(***nomhôte* **est le nom du serveur Web) en ajoutant la ligne suivante :**

   ```
   CERTDefaultNickname nom_stockageclés:Server-Cert
   ```

   Par défaut, le certificat créé est nommé `Server-Cert`. Si le nom de votre certificat est différent, veillez à utiliser le nom choisi plutôt que `Server-Cert`.

8. **Choisissez le serveur que vous voulez administrer et sélectionnez le bouton « Apply » (Appliquer) dans l'angle supérieur droit de la page.**

   Les modifications apportées au serveur d'administration Sun ONE 4.1 sont ainsi appliquées.

9. **Sélectionnez le bouton « Load Configuration Files » (Charger les fichiers de configuration) pour appliquer au fichier** `magnus.conf` **les modifications que vous venez d'effectuer.**

   Ce lien vous dirige vers une page vous permettant de démarrer l'instance du serveur Web.

   Si vous avez sélectionné le bouton « Apply Changes » (Appliquer les modifications) lorsque le serveur est désactivé, une boîte de dialogue d'authentification vous invite à préciser le *nomutilisateur:motpasse*. Il est impossible de redimensionner la fenêtre et il se peut que vous ne puissiez pas envoyer les modifications.

Il existe deux solutions à ce problème.

- Sélectionnez plutôt le bouton « Load Configuration Files » (Charger les fichiers de configuration).
- Démarrez d'abord le serveur Web, puis sélectionnez le bouton « Apply Changes » (Appliquer les modifications).

10. **Dans la partie gauche de la fenêtre du serveur d'administration Sun ONE 4.1, sélectionnez le lien On/Off (Activé/Désactivé).**

11. **Saisissez les mots de passe des serveurs et sélectionnez le bouton « OK ».**

    Vous êtes invité à saisir un ou plusieurs mots de passe. A l'invite du module interne, saisissez le mot de passe pour la base de données certifiée du serveur Web.

    A l'invite *nom_stockageclés* du module, entrez le *nomutilisateur:motpasse* de ce stockage de clés.

    Entrez le *nomutilisateur:motpasse* des autres stockages de clés lorsque vous y êtes invité.

12. **Vérifiez que SSL est activé sur le nouveau serveur Web à l'adresse URL suivante :**

    `https://`*nomhôte.domaine*`:`*port_serveur*`/`

Remarque – Le *port_serveur* par défaut est 443.

Installation et configuration d'un serveur Web Sun ONE 6.0

Cette section décrit l'activation de la carte Crypto Accelerator 4000 de Sun pour une utilisation avec le serveur Web Sun ONE 6.0. Cette section traite des points suivants :

- « Installation d'un serveur Web Sun ONE 6.0 », page 107
- « Configuration d'un serveur Web Sun ONE 6.0 pour SSL », page 116

Installation d'un serveur Web Sun ONE 6.0

Vous devez respecter l'ordre des étapes. Reportez-vous à la documentation du serveur Web Sun ONE pour plus d'informations sur l'utilisation des serveurs Web Sun ONE.

▼ Pour installer le serveur Web Sun ONE 6.0

1. **Téléchargez le logiciel du serveur Web Sun ONE 6.0.**

   Ce logiciel est disponible à l'adresse URL suivante :

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

2. **Installez le serveur Web.**

   Cette section comprend des instructions s'appuyant sur un exemple donné ; vous pouvez configurer votre serveur Web Sun ONE différemment. Par défaut, le nom de chemin du serveur est : `/usr/iplanet/servers`

   Acceptez le chemin par défaut pendant l'installation du serveur Web Sun ONE. Ce guide fait référence aux chemins par défaut. Si vous décidez d'installer le logiciel à un emplacement différent, assurez-vous de noter ce dernier.

3. **Lancez le programme** `setup`**.**

4. **Répondez aux invites du script d'installation.**

   Pour simplifier l'utilisation, vous pouvez accepter les paramètres par défaut, excepté pour les invites suivantes :

   a. **Acceptez les termes de la licence en saisissant** `yes`**.**

   b. **Saisissez un** *nomhôte.domaine* **complet.**

   c. **Entrez deux fois le mot de passe du serveur d'administration Sun ONE 6.0.**

   d. **A l'invite, appuyez sur Entrée.**

▼ Pour créer une base de données certifiée

1. **Démarrez le serveur d'administration Sun ONE 6.0.**

   Pour démarrer un serveur d'administration Sun ONE 6.0, utilisez la commande suivante (plutôt que d'exécuter `startconsole` comme requête `setup`) :

```
# /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://nomhôte.domaine/port 8888 ready to accept requests
startup: server started successfully
```

   La réponse indique l'URL avec laquelle vous devez vous connecter à vos serveurs.

2. **Démarrez l'interface utilisateur graphique Administration en ouvrant un navigateur Web et en saisissant :**

```
http://nomhôte.domaine:admin_port
```

Dans la boîte de dialogue d'authentification, saisissez le nom d'utilisateur et le mot de passe du serveur d'administration Sun ONE 6.0 que vous avez sélectionnés lors de l'exécution du programme `setup`.

Remarque – Si vous avez utilisé les paramètres par défaut lors de la configuration du serveur Web Sun ONE, saisissez comme nom d'utilisateur `admin` ou le nom d'utilisateur du serveur d'administration Sun ONE 6.0.

---

3. **Sélectionnez OK.**

La fenêtre du serveur d'administration Sun ONE 6.0 s'affiche.

4. **Créez la base de données certifiée pour l'instance du serveur Web.**

Il est recommandé d'activer la sécurité sur plusieurs instances du serveur Web. Pour cela, répétez cette opération de l'étape 1 à l'étape 4 pour chaque instance du serveur Web.

Remarque – Si vous voulez également exécuter SSL sur le serveur d'administration Sun ONE 6.0, la procédure de configuration d'une base de données certifiée est similaire. Reportez-vous au guide *iPlanet Web Server, Enterprise Edition Administrator's Guide* à l'adresse suivante : `http://docs.sun.com` pour plus d'informations.

---

a. **Sélectionnez l'onglet « Servers » (Serveurs) dans la fenêtre du serveur d'administration Sun ONE 6.0.**

b. **Sélectionnez un serveur et cliquez sur le bouton « Manage » (Gestion).**

c. **Sélectionnez l'onglet « Security » (Sécurité) dans la partie supérieure de la page et sélectionnez le lien « Create Database » (Créer une base de données).**

d. **Saisissez un mot de passe (base de données certifiée du serveur Web ; voir le** TABLEAU 5-1**) dans les deux boîtes de dialogue et sélectionnez OK.**

Choisissez un mot de passe de huit caractères minimum. Il s'agit du mot de passe utilisé pour lancer les modules cryptographiques internes lorsque le serveur Web Sun ONE est exécuté en mode sécurisé.

5. **Exécutez le script suivant pour activer la carte Crypto Accelerator 4000 de Sun :**

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

Ce script vous invite à choisir le serveur Web. Il installe les modules cryptographiques Crypto Accelerator 4000 de Sun pour le serveur Web Sun ONE. Puis il met à jour les fichiers de configuration pour activer la carte Crypto Accelerator 4000 de Sun.

6. **Saisissez `1` pour configurer votre serveur Web Sun ONE afin d'utiliser SSL, puis appuyez sur Entrée.**

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

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

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

7. **A l'invite, saisissez le chemin du répertoire racine du serveur Web, puis appuyez sur Entrée.**

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

8. **A l'invite, saisissez `y` et appuyez sur Entrée si vous désirez poursuivre.**

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

Using database directory /usr/iplanet/servers/alias...
Module "Sun Crypto Accelerator 4000" added to database.
/usr/iplanet/servers has been configured to use
the Sun Crypto Accelerator.


<Press ENTER to continue>
```

9. **Saisissez `0` pour quitter.**

▼ Pour créer un certificat de serveur

1. **Redémarrez le serveur d'administration Sun ONE 6.0 en saisissant les commandes suivantes :**

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

La réponse indique l'URL avec laquelle vous devez vous connecter à vos serveurs.

2. **Démarrez l'interface utilisateur graphique Administration en ouvrant un navigateur Web et en saisissant :**

```
http://nomhôte.domaine:port_admin
```

Dans la boîte de dialogue d'authentification, saisissez le nom d'utilisateur et le mot de passe du serveur d'administration Sun ONE 6.0 que vous avez sélectionnés lors de l'exécution du programme `setup`.

Remarque – Si vous avez utilisé les paramètres par défaut lors de la configuration du serveur Web Sun ONE, saisissez comme nom d'utilisateur `admin` ou le nom d'utilisateur du serveur d'administration Sun ONE 6.0.

---

3. **Sélectionnez OK.**

   La fenêtre du serveur d'administration Sun ONE 6.0 s'affiche.

4. **Pour demander le certificat du serveur, sélectionnez l'onglet « Security » (Sécurité) en haut de la fenêtre du serveur d'administration Sun ONE 6.0.**

   La fenêtre « Create Trust Database » (Création d'une base de données certifiée) s'affiche.

5. **Sélectionnez le lien « Request a Certificate » (Demander un certificat) dans le volet de gauche de la fenêtre du serveur d'administration Sun ONE 6.0.**

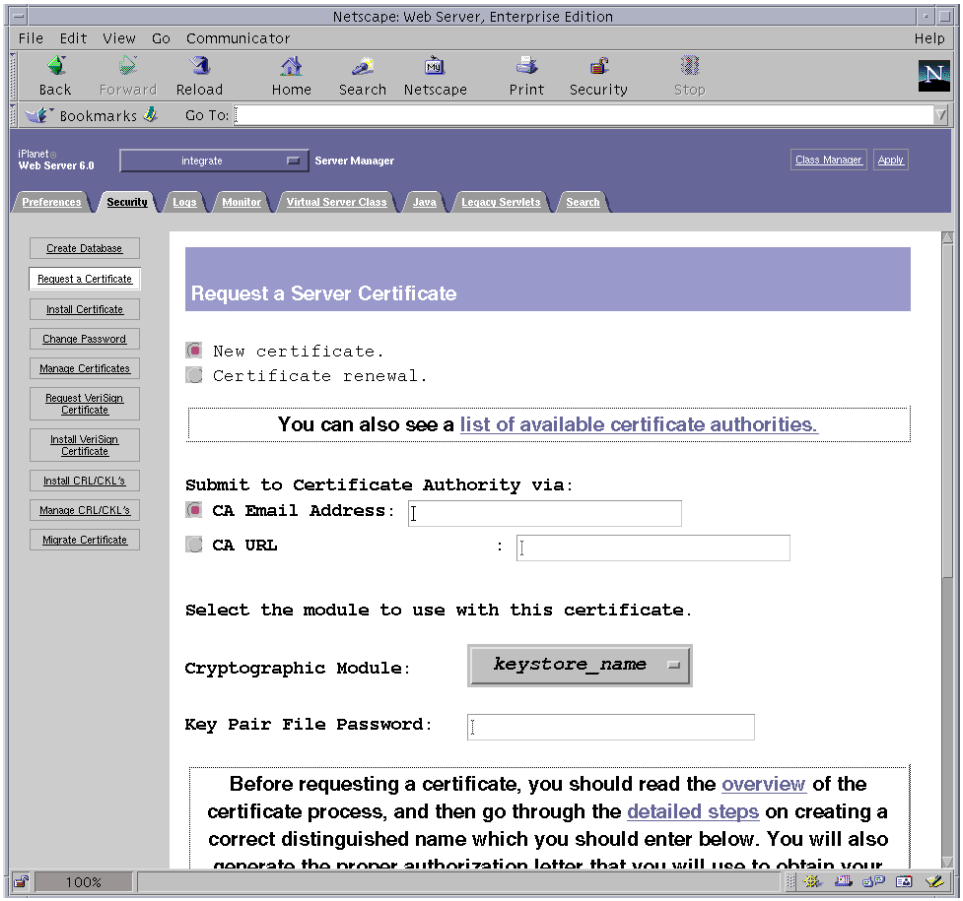

FIGURE 5-3 Page « Request a Server Certificate » (Demande d'un certificat de serveur) du serveur d'administration Sun ONE 6.0

6. **Remplissez le formulaire pour créer une demande de certificat, à l'aide des informations suivantes :**

   a. **Sélectionnez un nouveau certificat.**

      Si vous pouvez envoyer directement votre demande de certificat à une autorité de certification ou d'enregistrement sur le Web, sélectionnez le lien URL de l'autorité de certification. Sinon, dans le champ « CA Email Address » (Adresse électronique de l'autorité de certification), saisissez une adresse électronique à laquelle vous voulez envoyer votre demande de certificat.

   b. **Sélectionnez le module cryptographique que vous voulez utiliser.**

      Chaque stockage de clés dispose de sa propre entrée dans ce menu déroulant. Assurez-vous de sélectionner le stockage de clés adéquat. Ne sélectionnez pas uniquement l'accélération SUNW.

   c. **Dans la boîte de dialogue « Key Pair File Password » (Mot de passe de fichier de paire de clés), saisissez le mot de passe de l'utilisateur qui détiendra la clé.**

      Ce mot de passe est *nomutilisateur:motpasse* (TABLEAU 5-1).

   d. **Indiquez les informations appropriées pour les champs d'informations sur le demandeur suivants :**

TABLEAU 5-4 Champs d'informations sur le demandeur

Champ	Description
Requestor Name	(Nom du demandeur) Coordonnées du demandeur
Telephone Number	(Nom du demandeur) Coordonnées du demandeur
Common Name	(Nom commun) Domaine du site Web saisi dans le navigateur d'un visiteur *nomhôte.domaine*.
Email Address	(Adresse électronique) Coordonnées du demandeur
Organization	(Organisme) Organisme à déclarer sur le certificat.
Organizational Unit	(Unité de l'organisme - facultatif) Unité de l'organisme qui sera déclarée sur le certificat.
Locality	(Localité - facultatif) Ville, département, principauté ou pays, également déclaré(e) sur le certificat, le cas échéant.
State	(Etat - facultatif) Le nom complet de l'état
Country	(Pays) Code ISO de deux lettres désignant le pays (par exemple, US pour les Etats-Unis).

   e. **Sélectionnez le bouton OK pour envoyer les informations.**

7. **Faites appel à une autorité de certification pour créer le certificat.**
   - Si vous choisissez d'envoyer votre demande de certificat à l'URL d'une autorité de certification, elle sera automatiquement envoyée à cette adresse.
   - Si vous choisissez une adresse électronique d'autorité de certification, copiez la demande de certificat qui vous a été envoyée avec les en-têtes et remettez-la à l'autorité de certification.
8. **Une fois le certificat créé, copiez-le avec les en-têtes dans le presse-papiers.**

Remarque – Le certificat est différent de la demande de certificat et il vous est généralement présenté sous forme de texte. Conservez ces données dans le presse-papiers pour l'étape 5 de la section « Pour installer le certificat de serveur », page 114.

▼ Pour installer le certificat de serveur

1. **Sélectionnez le lien « Install Certificate » (Installer le Certificat) dans la partie gauche de la fenêtre du serveur d'administration Sun ONE 6.0.**

   Une fois votre demande approuvée par une autorité de certification et votre certificat délivré, vous devez installer ce dernier sur le serveur Sun ONE.
2. **Sélectionnez l'onglet « Security » (Sécurité).**

3. **Dans le volet de gauche, sélectionnez le lien « Install Certificate » (Installer le certificat).**

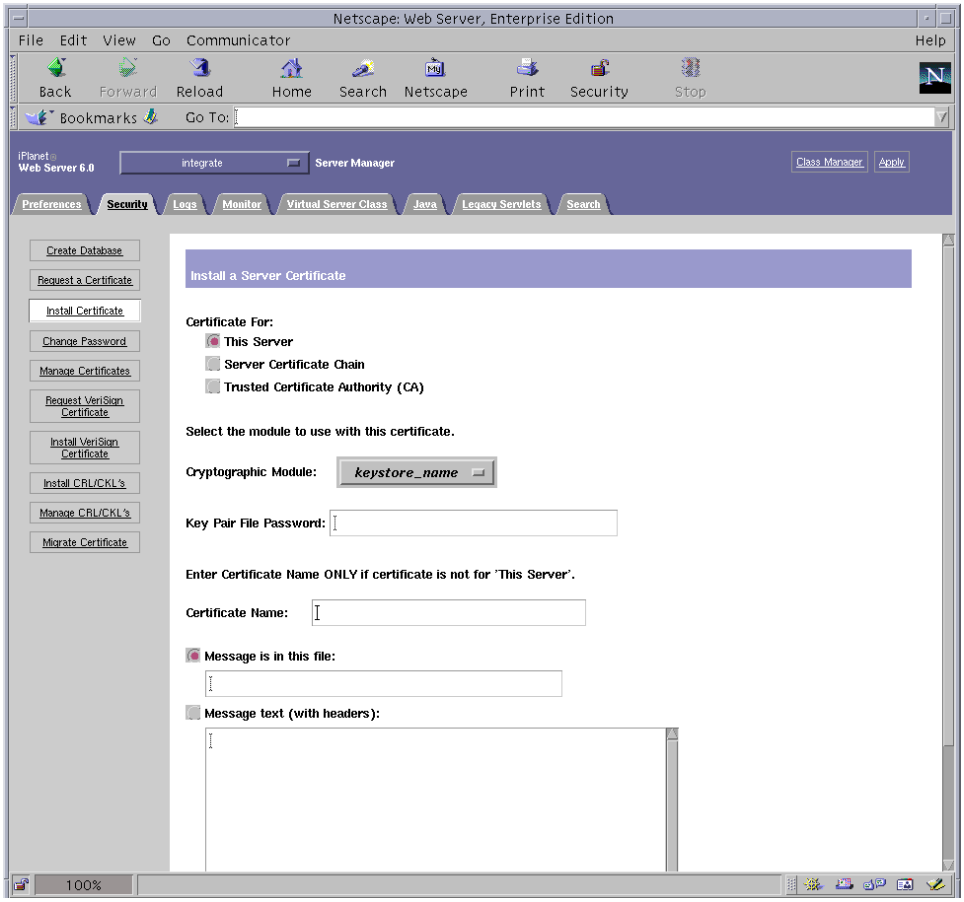

FIGURE 5-4 Page Install a Server Certificate du serveur d'administration Sun ONE 6.0

4. **Remplissez le formulaire pour installer votre certificat :**

TABLEAU 5-5 Champs du certificat à installer

Champs	Description
Certificate For	(Certificat pour) Ce serveur
Cryptographic Module	Chaque stockage de clés dispose de sa propre entrée dans ce menu déroulant. Assurez-vous de sélectionner le nom de stockage de clés correct. Pour utiliser Crypto Accelerator 4000 de Sun, vous devez sélectionner un module sous la forme de *nom_stockageclés.*
Key Pair File Password	(Mot de passe du fichier de paire de clés) Ce mot de passe est *nomutilisateur:motpasse* (TABLEAU 5-1).
Certificate Name	(Nom du certificat) Dans la plupart des cas, vous pouvez laisser ce champ vierge. Si vous saisissez un nom, celui-ci modifiera le nom utilisé par le serveur Web pour accéder au certificat et à la clé lors de l'exécution avec prise en charge SSL. La valeur par défaut de ce champ est `Server-Cert`.

5. **Collez le certificat copié dans l'autorité de certificat (à l'étape 8 de la section « Pour créer un certificat de serveur », page 111) dans la zone de texte « Message ».**

   Des informations de base sur le certificat s'affichent alors.

6. **Sélectionnez le bouton « OK » dans la partie inférieure de la page.**

7. **Si tout vous semble correct, sélectionnez le bouton « Add Server Certificate » (Ajouter le certificat de serveur).**

   Des messages vous invitent à redémarrer le serveur, ce qui n'est pas nécessaire car l'instance du serveur Web a été arrêtée pendant toute la durée des opérations.

   Vous êtes également averti que le serveur Web doit être configuré de manière à pouvoir utiliser SSL. Suivez la procédure suivante pour configurer le serveur Web.

Configuration d'un serveur Web Sun ONE 6.0 pour SSL

Maintenant que le serveur Web et le certificat du serveur sont installés, vous devez configurer le serveur Web pour SSL.

▼ Pour configurer le serveur Web Sun ONE 6.0

1. **Sélectionnez l'onglet « Preferences » (Préférences) dans la partie supérieure de la page.**
2. **Cliquez sur le lien « Edit Listen Sockets » (Modifier les prises de réception) dans le volet de gauche.**

   Le volet principal répertorie toutes les prises de réception définies pour l'instance du serveur Web.

   a. **Modifiez les champs suivants :**

      - « **Port** » : défini sur le port sur lequel vous allez exécuter votre serveur Web avec SSL activé (il s'agit généralement du port 443).
      - « **Security** » (Sécurité) : défini sur On (activé).

   b. **Sélectionnez le bouton OK pour appliquer ces changements.**

      Dans le champ « Security » (Sécurité) de la page « Edit Listen Sockets » (Modifier les prises de réception), le lien « Attributes » (Attributs) apparaît.
3. **Sélectionnez ce lien.**
4. **Entrez le** *nomutilisateur:motpasse* **pour vous authentifier auprès du stockage de clés sur le système.**
5. **Si vous voulez changer la valeur de chiffrement par défaut, sélectionnez les suites de chiffrement sous l'en-tête Ciphers (Chiffrements).**

   Une boîte de dialogue s'affiche, vous permettant de modifier les paramètres de chiffrement. Vous pouvez sélectionner les paramètres de chiffrement par défaut, SSL2 ou SSL3/TLS (Transmission Layer Security). Si vous avez sélectionné le chiffrement par défaut, les paramètres par défaut ne sont pas visibles. Pour les deux autres options, vous devez sélectionner les algorithmes à activer dans une boîte de dialogue contextuelle. Reportez-vous à votre documentation de Sun ONE pour plus de détails sur la sélection de chiffrement.
6. **Sélectionnez le certificat pour le stockage de clés, suivi de** : `Server-Cert` **(ou le nom que vous avez choisi s'il est différent).**

   Seules les clés appartenant au stockage de clés approprié sont affichées dans le champ « Certificate Name » (Nom du certificat). Cet utilisateur de stockage de clés est l'utilisateur qui est authentifié avec le *nomutilisateur:motpasse*.
7. **Une fois le certificat choisi et tous les paramètres de sécurité confirmés, sélectionnez le bouton OK.**
8. **Sélectionnez le lien « Apply » (Appliquer) dans l'angle supérieur droit pour appliquer ces changements avant de démarrer le serveur.**

9. **Sélectionnez le lien « Load Configuration Files » (Charger les fichiers de configuration) pour appliquer ces modifications.**

   Ce lien vous dirige vers une page vous permettant de démarrer l'instance du serveur Web.

   Si vous avez sélectionné le bouton « Apply Changes » (Appliquer les modifications) lorsque le serveur est désactivé, une boîte de dialogue d'authentification vous invite à préciser le *nomutilisateur:motpasse*. Il est impossible de redimensionner la fenêtre et il se peut que vous ne puissiez pas envoyer les modifications.

   Il existe deux solutions à ce problème.

   - Sélectionnez plutôt le bouton « Load Configuration Files » (Charger les fichiers de configuration).
   - Démarrez d'abord le serveur Web, puis sélectionnez le bouton « Apply Changes » (Appliquer les modifications).

10. **Dans la partie gauche de la fenêtre du serveur d'administration Sun ONE 6.0, sélectionnez le lien On/Off (Activé/Désactivé).**

11. **Saisissez les mots de passe des serveurs et sélectionnez le bouton « OK ».**

    Vous êtes invité à saisir un ou plusieurs mots de passe. A l'invite du module interne, saisissez le mot de passe de la base de données certifiée du serveur Web.

    A l'invite *nom_stockageclés* du module, entrez le *nomutilisateur:motpasse*.

    Entrez le *nomutilisateur:motpasse* des autres stockages de clés lorsque vous y êtes invité.

12. **Vérifiez que SSL est activé sur le nouveau serveur Web à l'adresse URL suivante :**

    `https://`*nomhôte.domaine:port_serveur*`/`

Remarque – Le *port_serveur* par défaut est 443.

CHAPITRE 6

Configuration des serveurs Web Apache pour une utilisation avec la Carte Crypto Accelerator 4000 de Sun

Ce chapitre explique comment configurer la carte Crypto Accelerator 4000 de Sun pour une utilisation avec un serveur Web Apache. Il est composé des sections suivantes :

Attention – Ne configurez pas le serveur Web Apache pour une utilisation simultanée avec les cartes Sun Crypto Accelerator 1000 et Sun Crypto Accelerator 4000. Sinon, Apache ne fonctionnera pas correctement.

Si vous prévoyez d'utiliser le serveur Web Apache, vous devez également installer le correctif 109234-09. Une fois le progiciel `SUNWkcl2a` ajouté, le système sera configuré avec le serveur Web Apache mod_ssl 1.3.26.

Remarque – La fonction de chiffrement de masse du logiciel du serveur Web Apache est activée par défaut et ne peut pas être désactivée.

Activation de la carte pour les serveurs Web Apache

Cette section explique comment activer la carte Crypto Accelerator 4000 de Sun pour une utilisation avec les serveurs Web Apache.

Activation du serveur Web Apache

Le serveur Web Apache 1.3.26 ou ultérieur est requis pour l'utilisation avec la carte Crypto Accelerator 4000 de Sun. Les instructions suivantes s'appliquent à la version 1.3.26 du serveur Web Apache. Pour de plus amples informations sur l'utilisation d'un serveur Web Apache, veuillez consulter la documentation qui s'y rapporte.

▼ Pour activer le serveur Web Apache

1. **Créez un fichier de configuration `httpd`.**

   Pour les systèmes Solaris, le fichier `httpd.conf-example` se trouve généralement dans `/etc/apache`. Vous pouvez utiliser ce fichier comme modèle et le copier comme suit :

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

2. **Remplacez `ServerName` par le nom de votre serveur dans le fichier `httpd.conf`.**

3. **Démarrez `apsslcfg`.**

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

4. **Sélectionnez `1` pour configurer votre serveur Web Apache pour l'utilisation de SSL :**

```
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. **Indiquez le répertoire où se trouvent les binaires Apache.**

   Sur les systèmes Solaris, il s'agit généralement de `/usr/apache`.

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

6. **Indiquez l'emplacement des fichiers de configuration Apache.**

   Sur les systèmes Solaris, il s'agit généralement de `/etc/apache`.

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

7. **Créez une paire de clés RSA pour votre système.**

   Si vous décidez de ne pas créer de paire de clés, vous devrez le faire ultérieurement et utiliser `apsslcfg` pour créer les clés.

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

   Si vous répondez non, rendez-vous directement à la section « Pour créer un certificat », page 123.

8. **Indiquez le répertoire de stockage des clés.**

   Si ce répertoire n'existe pas, il sera créé.

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

9. **Choisissez un nom de base pour la clé matérielle.**

   Ce nom comporte plusieurs suffixes pour vous permettre de distinguer les fichiers de clé, les fichiers de demande de certificat et, ultérieurement, les fichiers de certificat.

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

10. **Fournissez une clé dont la longueur se situe entre 512 et 2048 bits.**

    Pour la plupart des applications de serveur Web, une longueur de 1 024 bits est suffisamment efficace ; vous pouvez toutefois opter pour des clés plus efficaces si vous le désirez.

```
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. **Créez votre phrase-clé PEM.**

    Cette phrase-clé protège la clé matérielle. Assurez-vous de choisir une phrase-clé efficace dont vous pourrez vous souvenir. Si vous oubliez la phrase-clé, vous ne pourrez pas accéder à vos clés.

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

Attention – Vous devez vous souvenir de la phrase-clé que vous avez saisie. Sans elle, vous ne pourrez pas accéder à vos clés. Il est impossible de récupérer une phrase-clé oubliée.

Création d'un certificat

La procédure suivante décrit la création du certificat requis pour permettre à un serveur Web Apache d'utiliser la carte Crypto Accelerator 4000 de Sun.

▼ Pour créer un certificat

1. **Créez une demande de certificat en utilisant les clés que vous venez de créer à l'aide des instructions de la section « Pour activer le serveur Web Apache », page 120.**

   Vous devez d'abord entrer le mot de passe pour accéder à vos clés. Indiquez ensuite les informations correspondant aux champs suivants :

   - « Country Name » (Pays) : code ISO de deux lettres désignant le pays qui est déclaré sur le certificat. Ce champ est obligatoire (par exemple, US pour Etats-Unis).
   - « State or Province Name » (Département - facultatif) : nom complet du département (ou saisissez un point (`.`) et appuyez sur Entrée).
   - « Locality » (Localité - facultatif) : ville, département, principauté ou pays, également déclaré(e) sur le certificat, le cas échéant.
   - « Organization Name » (Organisme) : organisme à déclarer sur le certificat.
   - « Organizational Unit Name » (Unité de l'organisme - facultatif) : unité de l'organisme qui sera déclarée sur le certificat
   - « SSL Server Name » (Nom du serveur SSL) : domaine du site Web qui est saisi dans le navigateur d'un visiteur.
   - « Email Address » (Adresse électronique) : coordonnées du demandeur.

   L'exemple suivant indique comment remplir les champs du certificat :

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

2. **Modifiez le fichier** `/etc/apache/httpd.conf` **comme indiqué.**

   Des informations concernant vos fichiers de clé et de certificat s'affichent. Vous verrez également des instructions pour la modification du fichier `/etc/apache/httpd.conf` pour l'utiliser avec le logiciel Crypto Accelerator 4000 de Sun.

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

In the AddModule section, add the following:

AddModule mod_ssl.c
```

Remarque – Le *numéro-version* approprié apparaîtra lors de la configuration.

3. **Si vous choisissez de ne pas configurer un** `VirtualHost`**, les directives** `SSLEngine`**,** `SSLCertificateFile` **et** `SSLCertificateKeyFile` **doivent être placées dans le fichier** `httpd.conf`**, juste au-dessus de la directive** `SSLPassPhraseDialog`**.**

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

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

Si vous avez répondu non à la question de l'étape 7, section « Pour activer le serveur Web Apache », page 120, vous obtiendrez également des informations supplémentaires sur la création ultérieure de clés matérielles :

```
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. **Sélectionnez** `0` **pour quitter, une fois les opérations terminées avec l'utilitaire** `apsslcfg`**.**

5. **Copiez votre demande de certificat avec les en-têtes à partir de** `/etc/apache/keys/`*nom_base*`-certreq.pem` **(où** *nom_base* **a été configuré à l'étape 9 de la section « Pour activer le serveur Web Apache », page 120) et remettez-la à votre autorité de certification.**

6. **Une fois le certificat créé, vous pouvez créer le fichier de certificat** `/etc/apache/keys/`*nom_base*`-cert.pem` **et y copier votre certificat.**

7. **Démarrez le serveur Web Apache.**

   Cela suppose que votre répertoire de binaires Apache est `/usr/apache/bin`. S'il ne s'agit pas de votre répertoire de binaires, saisissez le répertoire approprié.

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

8. **A l'invite, entrez votre phrase-clé PEM.**

9. **Vérifiez que SSL est activé sur le nouveau serveur Web, avec un navigateur, à l'adresse URL suivante :**

   `https://`*nom_serveur*`:`*port_serveur*`/`

   Notez que le *port_serveur* par défaut est 443.

CHAPITRE 7

Diagnostics et dépannage

Ce chapitre décrit les tests de diagnostics et le dépannage pour le logiciel Crypto Accelerator 4000 de Sun. Il est composé des sections suivantes :

Logiciel de diagnostics SunVTS

Le wrapper SunVTS fournit un contrôle de tests et une interface utilisateur pour un ensemble de tests. Certains de ces tests sont livrés dans les progiciels `SUNWvts` et `SUNWvtsx` et sont regroupés avec le produit principal sur le CD-ROM Supplement du logiciel Solaris 8/9. D'autres tests non groupés qui utilisent SunVTS sont contenus avec le logiciel du pilote du périphérique testé.

Trois tests SunVTS fonctionnent avec la carte Crypto Accelerator 4000 de Sun. Deux de ces tests, `nettest` et `netlbtest`, sont regroupés avec le logiciel SunVTS, à partir de la version SunVTS 5.1 Patch Set (PS) 2. Ces tests fonctionnent sur les circuits Ethernet de la carte.

Le troisième test SunVTS, `vcatest`, est livré dans le progiciel `SUNWvcav` sur le CD-ROM de Crypto Accelerator 4000 de Sun et fonctionne avec le wrapper SunVTS afin de diagnostiquer les circuits cryptographiques de la carte.

Installation de la prise en charge `netlbtest` et `nettest` de SunVTS pour le pilote `vca`

Le TABLEAU 7-1 indique, pour chaque version du logiciel SunVTS, la méthode de mise à jour à suivre afin de prendre en charge `netlbtest` et `nettest` pourle pilote `vca`.

TABLEAU 7-1 Logiciel requis par SunVTS `netlbtest` et `nettest` de SunVTS pour le pilote `vca`

Logiciel Solaris de base	Logiciel SunVTS de base	Progiciel de remplacement requis	Correctif de recouvrement requis
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		

Le logiciel SunVTS figure sur le CD-ROM Supplement du logiciel Solaris qui est inclus dans chaque version de Solaris. La version du logiciel SunVTS affichée dans la colonne « Logiciel SunVTS de base » du TABLEAU 7-1 est distribuée sur le CD-ROM Supplement du logiciel Solaris, inclus dans la version Solaris identifiée sur la même ligne.

Les entrées du TABLEAU 7-1 qui commencent par « SunVTS » identifient la version de l'ensemble des progiciels SunVTS. Dans chaque ensemble de progiciels SunVTS, les progiciels `SUNWvts` et `SUNWvtsx` doivent être installés.

La colonne « Progiciels de remplacement requis » du TABLEAU 7-1 répertorie les ensembles de progiciels SunVTS qui doivent remplacer les progiciels SunVTS précédemment installés. Vous devez retirer les progiciels SunVTS précédemment installés avant d'ajouter les progiciels de remplacement SunVTS. Les progiciels SunVTS précédemment installés doivent être supprimés selon la méthode utilisée pour les installer. Par exemple, si vous avez utilisé la commande `pkgadd` pour installer les progiciels, utilisez la commande `pkgrm` pour les supprimer.

Si la colonne « Correctif de recouvrement requis » du TABLEAU 7-1 contient une entrée, utilisez la commande `patchadd` pour installer ce correctif sur les progiciels SunVTS mentionnés dans la colonne « Logiciel SunVTS de base ». Ne supprimez pas les progiciels SunVTS précédemment installés avant d'avoir ajouté le correctif requis.

L'utilisation de la commande `patchadd` pour installer le correctif 113614-11 revient à remplacer les progiciels SunVTS précédemment installés par les progiciels SunVTS5.1ps2.

Les progiciels de remplacement sont disponibles à l'adresse suivante :
`http://www.sun.com/oem/products/vts/`

Les correctifs de recouvrement sont disponibles à l'adresse suivante :
`http://sunsolve.sun.com/`

Remarque – Les progiciels SunVTS et correctifs requis doivent être installés avant le progiciel `SUNWvcav`. Le progiciel `SUNWvcav` contient le test SunVTS `vcatest`.

Utilisation du logiciel SunVTS pour exécuter `vcatest`, `nettest` et `netlbtest`

Reportez-vous au manuel de référence des tests SunVTS, au guide d'utilisation et au guide de référence rapide pour obtenir des instructions sur l'exécution et la surveillance de ces tests de diagnostics. Ces documents sont disponibles sur le site Web de documentation matérielle de Sun pour Solaris à l'adresse suivante : `http://docs.sun.com`. Ils figurent également sur le CD Supplement du logiciel Solaris inclus dans la version Solaris de votre système.

Remarque – SunVTS peut être utilisé uniquement si vous avez installé les progiciels et correctifs SunVTS requis.

▼ Pour exécuter vcatest

1. **Lancez SunVTS en tant que superutilisateur.**

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

   Reportez-vous au guide d'utilisation de SunVTS pour obtenir des instructions détaillées sur le lancement de SunVTS.

   Les instructions suivantes supposent que vous avez lancé SunVTS à l'aide de l'interface utilisateur CDE.

2. **Dans la fenêtre principale de diagnostics SunVTS, configurez la carte du système sur le mode logique.**

   Remarque – Le mode physique est pris en charge, mais cette opération suppose que vous utilisez le mode logique.

3. **Désactivez tous les tests en désélectionnant les cases.**

4. **Sélectionnez la case « Cryptography » (Cryptographie), puis la case + (plus) « Cryptography » pour afficher tous les tests du groupe « Cryptography ».**

5. **Désélectionnez les cases du groupe « Cryptography » qui ne sont pas nommées `vcatest`.**
   - Si un `vcatest` est affiché, rendez-vous à l'étape 6.
   - Si un `vcatest` n'est pas affiché, cherchez-le sur le système en sélectionnant « Reprobe system » (Retester le système) dans le menu déroulant « Commands » (Commandes).

   Reportez-vous au guide d'utilisation de SunVTS pour connaître la procédure exacte. Une fois la recherche terminée et un `vcatest` affiché, passez à l'étape 6.

6. **Sélectionnez l'une des instances de `vcatest`, puis cliquez dessus avec le bouton droit de la souris et déplacez cette dernière pour afficher la boîte de dialogue des options de paramètres de test.**

   Ces options, qui se rapportent uniquement à `vcatest`, sont décrites dans la section « Options de paramètres de test pour `vcatest` », page 131.

7. **Après avoir effectué toutes les sélections, sélectionnez « Apply » (Appliquer) dans le menu déroulant « Within Instance » (Dans l'instance) pour modifier l'instance de `vcatest` sélectionnée ou cliquez sur « Apply » dans le menu déroulant « Across All Instances » (Dans toutes les instances) pour modifier toutes les instances sélectionnées de `vcatest`.**

   Cette action ferme la boîte de dialogue et vous renvoie à la fenêtre principale de diagnostics SunVTS.

8. **Sélectionnez l'une des instances de `vcatest`, puis cliquez dessus avec le bouton droit de la souris et déplacez cette dernière pour afficher la boîte de dialogue des options d'exécution de tests.**

   Une autre méthode permettant d'afficher les options d'exécution de tests consiste à sélectionner le menu principal déroulant « Options », puis « Test Executions » (Exécution de tests). Ces options sont des commandes générales de SunVTS qui concernent tous les tests. Reportez-vous au guide d'utilisation de SunVTS pour obtenir des informations détaillées.

9. **Une fois toutes les sélections effectuées, sélectionnez « Apply » (Appliquer) pour fermer la boîte de dialogue et pour retourner à la fenêtre principale de diagnostics SunVTS.**

10. **Sélectionnez « Start » (Démarrer) pour exécuter les tests sélectionnés.**

11. **Sélectionnez « Stop » pour arrêter tous les tests.**

Options de paramètres de test pour `vcatest`

Le TABLEAU 7-2 décrit les sous-tests `vcatest`.

TABLEAU 7-2 Sous-tests `vcatest`

Nom du test	Description
`CDMF`	Teste le chiffrement de masse CDMF.
`DES`	Teste le chiffrement de masse DES.
`3DES`	Teste le chiffrement de masse 3DES.
`RSA`	Teste les clés publiques et privées RSA.
`DSA`	Teste la vérification de la signature DSA.
`MD5`	Teste la signature Digest/numérique des messages MD5.
`SHA1`	Teste la création de clé Digest SHA1.
`RNG`	Teste la génération de nombres aléatoires.

Syntaxe de la ligne de commande vcatest

Si vous choisissez de lancer vcatest à partir de la ligne de commande et non depuis l'interface CDE, vous devez alors spécifier tous les arguments dans la chaîne de la ligne de commande.

En mode 32 bits, le chemin vers vcatest est /opt/SUNWvts/bin/. En mode 64 bits, le chemin vers vcatest est /opt/SUNWvts/bin/sparcv9/.

Toutes les options standard de SunVTS sont prises en charge depuis l'interface de la ligne de commande pour vcatest. Les options se rapportant aux tests sont signalées par l'argument -o.

Reportez-vous au manuel de référence des tests de SunVTS pour obtenir une définition des arguments de ligne de commande standard. Comme vcatest est un test en mode fonctionnel, -f doit être inclus. Incluez -u pour afficher un message d'utilisation ou -v pour des messages VERBOSE. Les éléments entre crochets indiquent les entrées facultatives.

L'exemple suivant illustre l'invocation de vcatest en mode 32 bits en tant que programme autonome. La commande suivante effectue tous les sous-tests sur vca0 :

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

L'exemple suivant illustre l'invocation de vcatest en mode 64 bits à partir de l'infrastructure SunVTS. La commande suivante teste RSA, DSA et MD5 sur vca2 :

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

Lors de l'exécution de `vcatest` à partir de la ligne de commande, l'omission d'une option entraîne le comportement par défaut de cette option, comme indiqué dans le TABLEAU 7-3.

TABLEAU 7-3 Syntaxe de la ligne de commande `vcatest`

Option	Description
`dev=vca`*N*	Spécifie l'instance du périphérique à tester, telle que `vca0` ou `vca2`. Indique la valeur `vca0` par défaut si aucune valeur n'est incluse. Notez que *N* spécifie l'emplacement du numéro d'instance du périphérique testé.
`tl`=*listetests*	Indique la liste de sous-tests à exécuter. Les sous-tests pour `tl` sont séparés par le caractère + (plus). Les sous-tests pris en charge sont : CDMF, DES, 3DES, DSA, RSA, MD5, SHA1 et RNG, alors `tl=CDMF+DES+3DES+DSA+RSA+MD5+SHA1+RNG` active tous les sous-tests. Vous pouvez également insérer `tl=all` pour exécuter tous les tests. Indique la valeur `all` par défaut si aucun sous-test n'est spécifié.

▼ Pour exécuter `netlbtest`

1. **Lancez SunVTS en tant que superutilisateur.**

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

Reportez-vous au guide d'utilisation de SunVTS pour obtenir des instructions de démarrage détaillées.

Les instructions suivantes supposent que SunVTS a été démarré à l'aide de l'interface utilisateur CDE.

2. **Dans la fenêtre principale de diagnostics SunVTS, configurez la carte du système sur le mode logique.**

Remarque – Le mode physique est également pris en charge ; cependant, cette procédure suppose que vous utilisez le mode logique.

---

3. **Désactivez tous les tests en désélectionnant les cases.**
4. **Cochez la case « Network » (Réseau), puis la case + (plus) « Network » pour afficher tous les tests du groupe « Network ».**

5. **Désélectionnez toutes les cases du groupe « Network » qui ne sont pas nommées `vca`*N*`(netlbtest)`. Notez que *N* spécifie l'emplacement du numéro d'instance du périphérique testé.**

   - Si un `vca`*N*`(netlbtest)` est affiché, rendez-vous à l'étape 6.
   - Si un `vca`*N*`(netlbtest)` n'est pas affiché, cherchez-le sur le système en sélectionnant « Reprobe system » (Retester le système) dans le menu déroulant « Commands » (Commandes).

   Reportez-vous au guide d'utilisation de SunVTS pour connaître la procédure exacte. Une fois la recherche terminée et un `vca`*N*`(netlbtest)` affiché, passez à l'étape 6.

6. **Sélectionnez le bouton « Intervention Mode » (Mode d'intervention) Sélectionnez l'une des instances de `vca`*N*`(netlbtest)`, puis cliquez dessus avec le bouton droit de la souris et déplacez cette dernière pour afficher la boîte de dialogue des options de paramètres de test.**

   Ces options, qui appartiennent uniquement à `netlbtest`, sont décrites dans le manuel de référence des tests de SunVTS.

7. **Après avoir effectué toutes les sélections, sélectionnez « Apply » (Appliquer) dans le menu déroulant « Within Instance » (Dans l'instance) pour modifier l'instance sélectionnée de `vca`*N*`(netlbtest)`, ou cliquez sur « Apply » dans le menu déroulant « Across All Instances » (Dans toutes les instances) pour modifier toutes les instances sélectionnées de `vca`*N*`(netlbtest)`.**

   Cette action ferme la boîte de dialogue et vous renvoie à la fenêtre principale de diagnostics SunVTS.

8. **Sélectionnez l'une des instances de `vca`*N*`(netlbtest)`, puis cliquez dessus avec le bouton droit de la souris et déplacez-la pour afficher la boîte de dialogue des options de paramètres de test.**

   Une autre méthode permettant d'afficher les options d'exécution de tests consiste à sélectionner le menu principal déroulant « Options », puis « Test Executions » (Exécution de tests). Ces options sont des commandes générales de SunVTS qui concernent tous les tests. Reportez-vous au guide d'utilisation de SunVTS pour obtenir des informations détaillées.

9. **Une fois toutes les sélections effectuées, sélectionnez « Apply » (Appliquer) pour supprimer la boîte de dialogue et pour retourner à la fenêtre principale de diagnostics SunVTS.**

10. **Sélectionnez « Start » (Démarrer) pour exécuter les tests sélectionnés.**

11. **Sélectionnez « Stop » pour arrêter tous les tests.**

▼ Pour exécuter `nettest`

1. **Lancez SunVTS en tant que superutilisateur.**

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

   Reportez-vous au guide d'utilisation de SunVTS pour obtenir des instructions de démarrage détaillées.

   Les instructions suivantes supposent que SunVTS a été démarré à l'aide de l'interface utilisateur CDE.

2. **Dans la fenêtre principale de diagnostics SunVTS, configurez la carte du système sur le mode logique.**

Remarque – Le mode physique est également pris en charge ; cependant, cette procédure suppose que vous utilisez le mode logique.

---

3. **Désactivez tous les tests en désélectionnant les cases.**
4. **Cochez la case « Network » (Réseau), puis la case + (plus) « Network » pour afficher tous les tests du groupe « Network ».**
5. **Désélectionnez toutes les cases du groupe « Network » qui ne sont pas nommées** `vca`*N*`(nettest)`**. Notez que** *N* **spécifie l'emplacement du numéro d'instance du périphérique testé.**
   - Si un `vca`*N*`(nettest)` est affiché, passez à l'étape 6.
   - Si un `vca`*N*`(nettest)` n'est pas affiché, saisissez `ifconfig -a` dans une autre fenêtre sur le serveur où réside la carte `vca`*N*. Il devrait y avoir une entrée répertoriée comme suit :

```
vcaN up inet adresse-ip plumb
```

   Si l'entrée `ifconfig` précédente n'est pas répertoriée, la recherche `nettest` ne prendra pas en compte le périphérique à tester ; suivez alors les instructions du manuel en ligne relatives à `ifconfig` pour afficher une interface en ligne.

   Une fois que `ifconfig -a` a produit l'entrée précédente, retournez à la fenêtre principale de diagnostics SunVTS et sondez le système pour trouver `vca` en sélectionnant « Reprobe system » (Retester le système) dans le menu déroulant « Commands » (Commandes).

   Reportez-vous au guide d'utilisation de SunVTS pour connaître la procédure exacte. Une fois la recherche terminée et un `vca0(nettest)` affiché, passez à l'étape 6.

6. **Sélectionnez l'une des instances de `vca`*N*`(nettest)`, puis cliquez dessus avec le bouton droit de la souris et déplacez cette dernière pour afficher la boîte de dialogue des options de paramètres de test.**

   Ces options, qui appartiennent uniquement à `nettest`, sont décrites dans le manuel de référence des tests de SunVTS.

7. **Après avoir effectué toutes les sélections, sélectionnez « Apply » (Appliquer) dans le menu déroulant « Within Instance » (Dans l'instance) pour modifier l'instance sélectionnée de `vca`*N*`(nettest)`, ou cliquez sur « Apply » dans le menu déroulant « Across All Instances » (Dans toutes les instances) pour modifier toutes les instances sélectionnées de `vca`*N*`(nettest)`.**

   Cette action ferme la boîte de dialogue et vous renvoie à la fenêtre principale de diagnostics SunVTS.

8. **Sélectionnez l'une des instances de `vca`*N*`(nettest)`, puis cliquez dessus avec le bouton droit de la souris et déplacez-la pour afficher la boîte de dialogue des options d'exécution de tests.**

   Une autre méthode permettant d'afficher les options d'exécution de tests consiste à sélectionner le menu principal déroulant « Options », puis « Test Executions » (Exécution de tests). Ces options sont des commandes générales de SunVTS qui concernent tous les tests. Reportez-vous au guide d'utilisation de SunVTS pour obtenir des informations détaillées.

9. **Une fois toutes les sélections effectuées, sélectionnez « Apply » (Appliquer) pour supprimer la boîte de dialogue et pour retourner à la fenêtre principale de diagnostics SunVTS.**

10. **Sélectionnez « Start » (Démarrer) pour exécuter les tests sélectionnés.**

11. **Sélectionnez « Stop » pour arrêter tous les tests.**

Remarque – `nettest` et `netlbtest` ne doivent pas être exécutées simultanément.

Utilisation de `kstat` pour déterminer l'activité cryptographique

La carte Crypto Accelerator 4000 de Sun ne comporte aucun voyant ni aucun autre indicateur reflétant son activité cryptographique. Afin de déterminer si les requêtes cryptographiques sont effectuées sur la carte, utilisez la commande `kstat`(1M) pour afficher l'utilisation du périphérique :

```
# 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
```

Remarque – Dans l'exemple précédent, `0` est le numéro d'instance du périphérique `vca`. Ce numéro doit refléter le numéro d'instance de la carte pour laquelle vous exécutez la commande `kstat`.

L'affichage des informations `kstat` indique si les requêtes cryptographiques, ou « jobs », sont envoyées à la carte Crypto Accelerator 4000 de Sun. Une modification de la valeur « *jobs* » au cours du temps indique que la carte Crypto Accelerator 4000 de Sun accélère les requêtes cryptographiques qui lui sont envoyées. Si les requêtes ne sont pas envoyées à la carte, vérifiez la configuration de votre serveur Web selon la configuration spécifique de ce dernier.

N'essayez pas d'interpréter les valeurs statistiques du noyau/pilote renvoyées par `kstat`(1M). Ces valeurs sont conservées au sein du pilote afin de faciliter la prise en charge sur site. Le sens et les noms peuvent varier au cours du temps.

Remarque – Si la propriété `nostats` est définie dans le fichier `/kernel/drv/vca.conf`, la capture et l'affichage des statistiques seront désactivés. Cette propriété peut contribuer à empêcher l'analyse du trafic.

Utilisation du test automatique OpenBoot PROM FCode

Les tests suivants sont disponibles pour vous aider à identifier les problèmes avec l'adaptateur si le système ne s'initialise pas.

Vous pouvez invoquer les diagnostics de test automatique FCode à l'aide des commandes `test` ou `test-all` d'OpenBoot PROM (OBP). Si vous rencontrez une erreur lors de l'exécution de diagnostics, les messages appropriés s'afficheront. Reportez-vous au manuel *OpenBoot Command Reference Manual* pour de plus amples informations sur les commandes `test` et `test-all`.

Le test automatique FCode exécute la plupart des fonctionnalités sous-section par sous-section et garantit les points suivants :

- connectivité au cours de l'installation de la carte ;
- vérification que tous les composants requis pour l'initialisation d'un système sont fonctionnels.

▼ Exécution du diagnostic de test automatique Ethernet FCode

Pour exécuter les diagnostics Ethernet, vous devez au préalable arrêter le système à l'invite OBP après avoir lancé une réinitialisation. Si vous ne réinitialisez pas le système, les tests de diagnostics peuvent provoquer le blocage du système.

Pour plus d'informations sur les commandes OpenBoot de cette section, reportez-vous au manuel *OpenBoot Command Reference Manual*.

1. **Eteignez le système.**

   Utilisez les procédures de fermeture standard décrites dans le manuel *Solaris Handbook for Sun Peripherals*.

2. **A l'invite OBP, définissez la variable de configuration `auto-boot?` sur `false`.**

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

3. **Réinitialisez le système.**

```
ok reset-all
```

4. **Saisissez `show-nets` pour afficher la liste des périphériques et effectuer une sélection.**

   Une liste des périphériques spécifiques à l'adaptateur devrait s'afficher, similaire à l'exemple ci-dessous :

```
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
```

Remarque – Pour exécuter le test automatique suivant avec la commande `test`, le port Ethernet doit être connecté à un réseau.

---

5. **Exécutez le test automatique à l'aide de la commande `test` :**

   Les tests suivants sont réalisés lorsque la commande `test` est exécutée :

   - Test `vca` register test (se produit uniquement si `diag-switch?` est vraie [true])
   - Test de bouclage interne
   - Test de liaison ascendante/descendante

Remarque – Le test automatique de l'adaptateur UTP Crypto Accelerator 4000 de Sun pour une connexion de 1 000 Mbits/s n'est pas pris en charge pour l'utilisation avec un câble de bouclage externe, car l'horloge de liaison ne peut pas être réorganisée. Pour ce test, le port local et le port distant doivent être réorganisés comme horloge maître et horloge esclave. Si un câble de bouclage externe est utilisé, les deux ports sont identiques. Par conséquent, le port unique ne peut pas être à la fois horloge maître et esclave, car cela entraînerait l'échec systématique de la liaison ascendante PHY. Pour qu'un test automatique de l'adaptateur UTP Crypto Accelerator 4000 de Sun pour une connexion 1 000 Mbits/s fonctionne, un port 1000Base-T distant doit être connecté.

Entrez la commande suivante :

```
ok test chemin_périphérique
```

Si le `test` réussit, les messages suivants s'affichent :

```
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
```

Si la carte n'est pas connectée à un réseau, les messages suivants s'affichent :

```
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. **Après le test de l'adaptateur, saisissez la commande suivante pour redéfinir l'interface OBP en mode de fonctionnement normal :**

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

7. **Définissez le paramètre de configuration `auto-boot?` sur `true`.**

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

8. **Réinitialisez et redémarrez le système.**

Dépannage de la Carte Crypto Accelerator 4000 de Sun

Cette section décrit les commandes disponibles au niveau OBP pour le dépannage de la carte. Reportez-vous au manuel *OpenBoot Command Reference Manual* pour de plus amples informations sur les commandes décrites dans les sous-sections suivantes :

show-devs

Pour déterminer si le périphérique Crypto Accelerator 4000 de Sun est répertorié dans le système, saisissez `show-devs` à l'invite OBP pour afficher la liste des périphériques. Des lignes semblables aux exemples ci-dessous, spécifiques à la carte Crypto Accelerator 4000 de Sun, s'affichent alors :

```
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
.
.
```

Dans l'exemple précédent, l'entrée `/pci@8,600000/network@1` identifie le chemin du périphérique vers la carte Crypto Accelerator 4000 de Sun. Chaque carte du système sera associée à une ligne de ce type.

.properties

Pour déterminer si les propriétés du périphérique Crypto Accelerator 4000 de Sun sont correctement répertoriées : dans l'invite OBP, saisissez `.properties` pourafficher la liste des propriétés.

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

watch-net

Pour surveiller une connexion réseau : dans l'invite OBP, saisissez la commande `apply watch-net` avec le chemin du périphérique :

```
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.....
```

Le système contrôle le trafic sur le réseau, affichant '.' chaque fois qu'il reçoit un paquet sans erreur et 'X' chaque fois qu'il reçoit un paquet contenant une erreur qui peut être détectée par l'interface matérielle du réseau.

ANNEXE **A**

Spécifications

Cette annexe répertorie les spécifications des adaptateurs MMF et UTP Crypto Accelerator 4000 de Sun. Il comprend les sections suivantes :

Adaptateur MMF Crypto Accelerator 4000 de Sun

Cette section présente les spécifications de l'adaptateur MMF Crypto Accelerator 4000 de Sun.

Connecteurs

La FIGURE A-1 illustre le connecteur de l'adaptateur MMF Crypto Accelerator 4000 de Sun.

FIGURE A-1 Crypto Accelerator 4000 de Sun Connecteur de l'adaptateur MMF

Le TABLEAU A-1 répertorie les caractéristiques du connecteur SC (850 nm).

TABLEAU A-1 Caractéristiques du lien du connecteur SC (IEEE P802.3z)

Caractéristique	62,5 microns MMF	50 microns MMF
Portée de fonctionnement	Jusqu'à 260 mètres	Jusqu'à 550 mètres

Dimensions physiques

TABLEAU A-2 Dimensions physiques

Dimension	Mesure	Mesures métriques
Longueur	12,283 pouces	312 mm
Largeur	4,2 pouces	106,68 mm

Spécifications de performances

TABLEAU A-3 Spécifications de performances

Fonctionnalités	Spécification
Horloge PCI	33/66 MHz max.
Taux de transfert en rafale des données PCI	Rafales jusqu'à 64 octets
Largeur adresse/données PCI	32/64 bits
Modes PCI	Maître/esclave
1 Gbit/s, 850 nm	1 000 Mbit/s (duplex intégral)

Alimentation requise

TABLEAU A-4 Alimentation requise

Spécification	Mesure
Consommation électrique maximale	6,25 W à 5 V 12,75 W à 3,3 V
Tolérance	5 V +/- 5 % 3,3 V +/- 5 %

Spécifications de l'interface

TABLEAU A-5 Spécifications de l'interface

Fonctionnalités	Spécification
Horloge PCI	33 ou 66 MHz
Interface hôte	PCI 2.1 avec prise en charge d'une fréquence d'horloge de 33 ou 66 MHz et d'une tolérance à 3,3 ou 5 V.
Largeur de bus PCI	32 ou 64 bits

Spécifications environnementales

TABLEAU A-6 Spécifications environnementales

Condition	Spécification de fonctionnement	Spécification de stockage
Température	0 ° à +55 °C, +32 ° à +131 °F	-40 ° à +75 °C, -40 ° à +167 °F
Taux d'humidité relative	5 à 85 % sans condensation	0 à 95 % sans condensation

Adaptateur UTP Crypto Accelerator 4000 de Sun

Cette section présente les spécifications de l'adaptateur UTP Crypto Accelerator 4000 de Sun.

Connecteurs

La FIGURE A-2 illustre le connecteur de l'adaptateur UTP Crypto Accelerator 4000 de Sun.

FIGURE A-2 Crypto Accelerator 4000 de Sun Connecteur de l'adaptateur UTP

Le TABLEAU A-7 répertorie les caractéristiques du connecteur Cat-5 utilisé par l'adaptateur UTP Crypto Accelerator 4000 de Sun.

TABLEAU A-7 Caractéristiques du lien du connecteur Cat-5

Caractéristique	Description
Portée de fonctionnement	Jusqu'à 100 mètres

Dimensions physiques

TABLEAU A-8 Dimensions physiques

Dimension	Mesure	Mesures métriques
Longueur	12,283 pouces	312 mm
Largeur	4,2 pouces	106,68 mm

Spécifications de performances

TABLEAU A-9 Spécifications de performances

Fonctionnalités	Spécification
Horloge PCI	33/66 MHz max.
Taux de transfert en rafale des données PCI	Rafales jusqu'à 64 octets
Largeur adresse/données PCI	32/64 bits
Modes PCI	Maître/esclave
1 Gbit/s, 850 nm	1 000 Mbit/s (duplex intégral)

Alimentation requise

TABLEAU A-10 Alimentation requise

Spécification	Mesure
Consommation électrique maximale	6,25 W à 5 V 12,75 W à 3,3 V
Tolérance	5 V +/- 5 % 3,3 V +/- 5 %

Spécifications de l'interface

TABLEAU A-11 Spécifications de l'interface

Fonctionnalités	Spécification
Horloge PCI	33 ou 66 MHz
Interface hôte	PCI 2.1 avec prise en charge d'une fréquence d'horloge de 33 ou 66 MHz et d'une tolérance à 3,3 ou 5 V
Largeur de bus PCI	32 ou 64 bits

Spécifications environnementales

TABLEAU A-12 Spécifications environnementales

Condition	Spécification de fonctionnement	Spécification de stockage
Température	0 ° à +55 °C, +32 ° à +131 °F	-40 ° à +75 °C, -40 ° à +167 °F
Taux d'humidité relative	5 à 85 % sans condensation	0 à 95 % sans condensation

ANNEXE **B**

Directives de configuration SSL pour le serveur Web Apache

Cette annexe répertorie les directives d'utilisation du logiciel Crypto Accelerator 4000 de Sun afin de configurer la prise en charge SSL du serveur Web Apache. Ces directives de configuration se trouvent dans votre fichier `http.conf`. Pour plus d'informations, reportez-vous à la documentation relative au serveur Web Apache.

1. `SSLPassPhraseDialog exec:`*programme*

   Contexte : global

   Cette directive informe le serveur Web Apache que le *programme* spécifié doit être exécuté pour obtenir le mot de passe du fichier de clés. *programme* doit imprimer le mot de passe obtenu sur la sortie standard.

   Si plusieurs fichiers de clés sont présents et qu'ils ont le même mot de passe, *programme* ne sera alors exécuté qu'une fois (chaque mot de passe obtenu est vérifié avant de relancer *programme*).

   programme est exécuté avec deux arguments. Le premier est le nom du serveur, sous la forme *nomserveur:port* ; par exemple : `www.fictional-company.com:443` (le port 443 est le port type pour les serveurs Web basés sur SSL). Le second argument est le type de clé contenu dans le fichier de clés (*typeclé*). *typeclé* peut être RSA ou DSA.

Remarque – Comme ce programme peut être exécuté lors du démarrage du système, assurez-vous qu'il est conçu de manière à s'adapter à un périphérique non `tty` (c'est-à-dire que la commande `tty`(3c) renvoie faux).

   Le programme `/opt/SUNWconn/cryptov2/bin/apgetpass` fourni peut être utilisé pour l'exécutable *programme*. Ce programme vous invite automatiquement à saisir le mot de passe en supprimant l'affichage de ce dernier à mesure qu'il est saisi.

Le programme `sslpassword` fourni recherche aussi automatiquement des mots de passe dans les fichiers. Ainsi, vous évitez l'interaction des utilisateurs au démarrage du serveur Web. Les mots de passe des fichiers de clés sont recherchés dans les fichiers nommés `/etc/apache/`*nomserveur:port.typeclé*`.pass`. Si ce fichier n'est pas présent, le fichier `/etc/apache/default.pass` sera alors utilisé. Ces fichiers de mot de passe contiennent uniquement le mot de passe non chiffré sur une ligne indépendante.

Remarque – Les fichiers de mots de passe doivent être protégés par une autorisation afin que seul l'utilisateur UNIX, sous lequel le serveur Web s'exécute, puisse lire le fichier. Cet utilisateur doit être le même que celui configuré avec la directive standard `user` Apache.

S'il n'y a aucune précision, le comportement par défaut utilise un mécanisme d'invite interne. N'utilisez pas la valeur par défaut ; utilisez plutôt le programme `sslpassword` fourni pour éviter des problèmes d'interaction au démarrage du système.

2. `SSLEngine` (`on|off`)

   Contexte : global, hôte virtuel

   Cette directive active le protocole SSL. Elle est généralement utilisée avec un hôte virtuel pour activer SSL sur un sous-système de serveurs. L'une des formes communément utilisées est :

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

Cette instruction configure l'utilisation de SSL pour tout serveur récepteur sur le port 443 (le port HTTPS standard). Si elle n'est pas présente, le protocole est désactivé par défaut.

3. `4SSLProtocol [+-]`*protocole*

   Contexte : global, hôte virtuelCette directive configure le(s) protocole(s) que le serveur doit utiliser pour les transactions SSL.

   Les protocoles disponibles sont répertoriés et décrits dans le TABLEAU B-1 :

TABLEAU B-1 Protocoles SSL

Protocole	Description
`SSLv2`	Protocole SSL standard d'origine de Netscape
`SSLv3`	Version mise à jour du protocole SSL, prise en charge par la plupart des navigateurs Web
`TLSv1`	Mise à jour de `SSLv3` en cours de normalisation IETF, avec une prise en charge de navigateur minimale
`all`	Activation de tous les protocoles

   L'utilisation des signes plus (+) ou moins (-) permet d'ajouter ou de supprimer des protocoles. Par exemple, pour désactiver la prise en charge de SSLv2, la directive suivante pourrait être utilisée :

```
SSLProtocol all -SSLv2
```

   Elle est équivalente à :

```
SSLProtocol +SSLv3 +TLSv1
```

4. `SSLCipherSuite` *spec-chiffre*

   Contexte : global, hôte virtuel, répertoire, `.htaccess`

   La directive SSLCipherSuite est utilisée pour déterminer les chiffres SSL disponibles et leur préférence. Dans un contexte global et un contexte d'hôte virtuel, elle est utilisée lors du protocole de reconnaissance SSL initial. Dans un contexte par répertoire, elle oblige une renégociation SSL à utiliser les chiffres nommés. La renégociation a lieu après la lecture de la requête, mais avant l'envoi de la réponse.

spec-chiffre est une liste délimitée par deux points des chiffres décrits dans le TABLEAU B-2. Dans le TABLEAU B-2, DH se rapporte à Diffie-Hellman et DSS à Digital Signature Standard.

TABLEAU B-2 Chiffres SSL disponibles

Label du chiffre	Protocole	Echange de clés	Authent.	Chiffrement	MAC	Type
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES (168 bits)	SHA1	
DES-CBC3-MD5	SSLv2	RSA	RSA	3DES (168 bits)	MD5	
RC4-SHA	SSLv3	RSA	RSA	ARCFOUR (128 bits)	SHA1	
RC4-MD5	SSLv3	RSA	RSA	ARCFOUR (128 bits)	MD5	
RC4-MD5	SSLv2	RSA	RSA	ARCFOUR (128 bits)	MD5	
RC2-CBC-MD5	SSLv2	RSA	RSA	ARCTWO (128 bits)		
DES-CBC-SHA	SSLv3	RSA	RSA	DES (56 bits)	SHA1	
RC4-64-MD5	SSLv2	RSA	RSA	ARCFOUR (64 bits)	MD5	
DES-CBC-MD5	SSLv2	RSA	RSA	DES (56 bits)	MD5	
EXP-DES-CBC-SHA	SSLv3	RSA (512 bits)	RSA	DES (40 bits)	SHA1	export
EXP-RC2-CBC-MD5	SSLv2	RSA (512 bits)	RSA	ARCTWO (40 bits)	SHA1	export
EXP-RC2-CBC-MD5	SSLv3	RSA (512 bits)	RSA	ARCTWO (40 bits)	SHA1	export
EXP-RC4-MD5	SSLv3	RSA (512 bits)	RSA	ARCFOUR (40 bits)	MD5	export
EXP-RC4-MD5	SSLv2	RSA (512 bits)	RSA	ARCFOUR (40 bits)	MD5	export
NULL-SHA	SSLv3	RSA	RSA	Aucun	SHA1	
NULL-MD5	SSLv3	RSA	RSA	Aucun	MD5	
ADH-DES-CBC3-SHA	SSLv3	DH	Aucun	3DES (168 bits)	SHA1	
ADH-DES-CBC-SHA	SSLv3	DH	Aucun	DES (56 bits)	SHA1	
ADH-RC4-MD5	SSLv3	DH	Aucun	ARCFOUR (128 bits)	MD5	
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES (168 bits)	SHA1	
EDH-DSS-DES-CBC3-SHA	SSLv3	DH	DSS	3DES (168 bits)	SHA1	

TABLEAU B-2 Chiffres SSL disponibles *(suite)*

Label du chiffre	Protocole	Echange de clés	Authent.	Chiffrement	MAC	Type
EDH-RSA-DES-CBC-SHA	SSLv3	DH	RSA	DES (56 bits)	SHA1	
EDH-DSS-DES-CBC-SHA	SSLv3	DH	DSS	DES (56 bits)	SHA1	
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH (512 bits)	RSA	DES (40 bits)	SHA1	export
EXP-EDH-DSS-DES-CBC-SHA	SSLv3	DH (512 bits)	DSS	DES (40 bits)	SHA1	export
EXP-ADH-DES-CBC-SHA	SSLv3	DH (512 bits)	Aucun	DES (40 bits)	SHA1	export
EXP-ADH-RC4-MD5	SSLv3	DH (512 bits)	Aucun	ARCFOUR (40 bits)	MD5	export

Le TABLEAU B-3 répertorie et décrit les alias fournissant des groupements de type macro.

TABLEAU B-3 Alias SSL

Alias	Description
SSLv2	Tous les chiffres SSL version 2.0
SSLv3	Tous les chiffres SSL version 3.0
EXP	Tous les chiffres de niveau exportation
EXPORT40	Tous les chiffres d'exportation de 40 bits
EXPORT56	Tous les chiffres d'exportation de 56 bits
LOW	Chiffres de moindre puissance (DES, RC4 de 40 bits)
MEDIUM	Tous les chiffres de 128 bits
HIGH	Tous les chiffres utilisant Triple DES
RSA	Tous les chiffres utilisant l'échange de clés RSA
DH	Tous les chiffres utilisant l'échange de clés Diffie-Hellman
EDH	Tous les chiffres utilisant l'échange de clés Ephemeral Diffie-Hellman
ADH	Tous les chiffres utilisant l'échange de clés Diffie-Hellman anonyme
DSS	Tous les chiffres utilisant l'authentification DSS
NULL	Tous les chiffres n'utilisant aucun chiffrement

Les préférences des chiffres peuvent être configurées à l'aide des caractères spéciaux répertoriés et décrits dans le TABLEAU B-4.

TABLEAU B-4 Caractères spéciaux pour la configuration des préférences de chiffre

Caractère	Description
<none>	Ajoute un chiffre à la liste.
!	Supprime définitivement un chiffre de la liste ; il est impossible de le rajouter ultérieurement.
+	Ajoute un chiffre à la liste et le situe à son emplacement actuel (ou l'abaisse).
-	Supprime un chiffre de la liste (il est possible de le rajouter ultérieurement)

La valeur par défaut de *spec-chiffre* est :

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

La valeur par défaut configure tous les chiffres, à l'exception des codes Diffie-Hellman anonymes (non authentifiés), en privilégiant ARCFOUR et RSA, ainsi que les niveaux de chiffrement élevés.

5. `SSLCertificateFile` *fichier*

   Contexte : global, hôte virtuel

   Cette directive précise l'emplacement du fichier de certificats X.509 encodé au format PEM pour le serveur.

6. `SSLCertificateKeyFile` *fichier*

   Contexte : global, hôte virtuel

   Cette directive précise l'emplacement du fichier de clés privées encodé au format PEM pour le serveur, correspondant au certificat configuré avec la directive `SSLCertificateFile`.

7. `SSLCertificateChainFile` *fichier*

   Contexte : global, hôte virtuel

   Cette directive précise l'emplacement d'un fichier contenant les certificats encodés au format PEM et constituant le chemin de certification du serveur. Elle peut être utilisée pour assister des clients dans la vérification du certificat du serveur, lorsque ce dernier n'est pas directement signé par une autorité que le client reconnaît.

   Les certificats de la chaîne sont censés être valides également pour une authentification des clients, lorsque cette pratique (`SSLVerifyClient`) est utilisée.

8. `SSLCACertificateFile` *fichier*

   Contexte : global, hôte virtuel

   Cette directive précise l'emplacement d'un fichier contenant la concaténation des certificats destinés aux autorités de certification, utilisé pour l'authentification des clients.

9. `SSLCARevocationFile` *fichier*

   Contexte : global, hôte virtuel

   Cette directive précise l'emplacement d'un fichier contenant la concaténation des listes de révocation de certificat des autorités de certifications, utilisé pour l'authentification des clients.

10. `SSLVerifyClient` *niveau*

    Contexte : global, hôte virtuel, répertoire, `.htaccess`

    Cette directive configure l'authentification des clients du serveur. Notez qu'elle n'est généralement pas nécessaire pour les applications de commerce électronique, mais elle est utilisée pour d'autres applications.

    Les valeurs de *niveau* sont répertoriées et décrites dans le TABLEAU B-5.

TABLEAU B-5 Niveaux de vérification SSL des clients

Niveau	Description
`none`	Aucun certificat de client n'est requis.
`optional`	Le client peut présenter un certificat valide.
`require`	Le client *doit* présenter un certificat valide.
`optional_no_ca`	Le client peut présenter un certificat, mais celui-ci ne doit pas obligatoirement être valide.

En général, `none` ou `require` est utilisé. Le niveau par défaut est `none`.

11. `SSLVerifyDepth` *profondeur*

    Contexte : global, hôte virtuel, répertoire, `.htaccess`

    Cette directive précise la profondeur maximale de chaîne du certificat autorisée par le serveur pour les certificats de clients. Une valeur de 0 signifie que seuls les certificats auto-signés sont valides, tandis qu'une valeur de 1 signifie que les certificats de clients doivent être signés par une autorité de certification directement connue du serveur (via `SSLCACertificateFile`). Des valeurs élevées permettent une délégation de l'autorité de certification.

12. `SSLLog` *nomfichier*

    Contexte : global, hôte virtuel

    Cette directive indique le fichier journal où les informations spécifiques à SSL seront enregistrées. Si elle n'est pas précisée (valeur par défaut), aucune information spécifique à SSL ne sera enregistrée.

13. `SSLLogLevel` *niveau*

    Contexte : global, hôte virtuel

    Cette directive précise la verbosité des informations enregistrées dans le fichier journal SSL. Les valeurs de *niveau* sont répertoriées et décrites dans le TABLEAU B-6.

TABLEAU B-6 Valeurs de niveau du fichier journal SSL

Valeur	Description
`none`	Aucun enregistrement, mais les messages d'erreur sont encore envoyés au fichier journal Apache standard.
`warn`	Comporte des messages d'avertissement.
`info`	Comporte des messages d'informations.
`trace`	Comporte des messages de traçage.
`debug`	Comporte de messages de débogage.

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

    Contexte : global, hôte virtuel, répertoire, `.htaccess`

    Cette directive configure les options de temps d'exécution SSL pour chaque répertoire. Des options peuvent être ajoutées à la configuration actuelle en les faisant précéder du signe (+), ou peuvent être supprimées avec un signe moins (-). Si plusieurs options peuvent s'appliquer à un répertoire, l'option la plus restrictive est utilisée ; les options ne sont pas fusionnées.

Les options sont répertoriées et décrites dans le TABLEAU B-7.

TABLEAU B-7 Options SSL disponibles

Options	Description
`StdEnvVars`	Un ensemble standard de variables d'environnement CGI/SSI liées à SSL est créé. Les performances en seront affectées.
`ExportCertData`	Provoque l'exportation des variables d'environnement `SSL_SERVER_CERT`, `SSL_CLIENT_CERT` et `SSL_CLIENT_CERT_CHAIN`*n* (*n* = 0, 1, ...). Ces variables comportent des certificats encodés au format PEM pour le client et le serveur.
`FakeBasicAuth`	Le DN (Distinguished Name) du certificat de client est traduit en un nom d'utilisateur d'authentification basique HTTP et son authentification est simulée. Cette opération permet l'utilisation de mécanismes standard de contrôle d'accès Apache avec l'authentification de client SSL, sans inviter l'utilisateur à entrer un mot de passe. Les entrées correspondant à ces utilisateurs dans les fichiers de mots de passe Apache doivent utiliser le mot de passe codé `xxj31ZMTZzkVA`, qui n'est que la forme codée (`crypt`(3c)) du mot « password » (mot de passe).
`StrictRequire`	Force un accès interdit en raison du rejet de `SSLRequireSSL`, et ce, même en présence d'autres directives, telles que `Satisfy Any`, qui pourraient l'écraser.

15. `SSLRequireSSL`

Contexte : répertoire, `.htaccess`

Cette directive interdit l'accès à un répertoire donné, à moins d'utiliser HTTPS. Elle peut être utilisée pour prévenir les erreurs de configuration susceptibles de mettre les données d'un répertoire à la disposition d'utilisateurs non authentifiés et non codés.

ANNEXE C

Création d'applications pour une utilisation avec la Carte Crypto Accelerator 4000 de Sun

Cette annexe décrit le logiciel fourni avec la carte Crypto Accelerator 4000 de Sun, lequel peut être utilisé pour construire des applications compatibles avec OpenSSL afin de bénéficier des fonctions d'accélération cryptographique de la carte Crypto Accelerator 4000 de Sun. Certaines applications OpenSSL ne tireront aucun avantage à être compilées de la sorte (contrairement à une construction avec une bibliothèque OpenSSL, qui peut être téléchargée à partir de `www.openssl.org`).

Remarque – Ces informations sur la création d'applications pour l'utilisation du logiciel et du matériel Crypto Accelerator 4000 de Sun sont fournies en l'état et ne constituent pas un élément officiellement pris en charge. Elles sont fournies à titre indicatif, sans aucune garantie. Si vous souhaitez obtenir une solution prise en charge par Sun, veuillez contacter les services professionnels de Sun pour en savoir plus.

Vous devez d'abord installer le progiciel `SUNWkcl2o` qui contient les bibliothèques et les en-têtes de fichiers requis.

Votre application doit être configurée de manière à inclure les en-têtes OpenSSL à partir de `/opt/SUNWconn/cryptov2/include`, comme avec le drapeau de compilation :

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

De plus, l'éditeur de liens doit être dirigé de manière à inclure des références vers les bibliothèques appropriées. La plupart des applications compatibles avec OpenSSL référenceront soit l'une des bibliothèques `libcrypto.a` et `libssl.a`, soit les deux. Les bibliothèques cryptographiques de Sun doivent également être incluses. Les attributs d'éditeur de liens suivants effectueront ceci :

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

ANNEXE **D**

Licences du logiciel

Cette annexe fournit le contrat de licence relatif au code binaire de Sun, ainsi que des avertissements et des licences pour des logiciels tiers.

Remarque – Les licences et les avertissements de tiers inclus dans cette annexe sont présentés exactement sous la forme sous laquelle ils ont été fournis par leurs détenteurs.

Sun Microsystems, Inc.

Contrat de licence relatif au code binaire

LISEZ ATTENTIVEMENT LES TERMES ET CONDITIONS DE CE CONTRAT ET DE TOUT CONTRAT SUPPLEMENTAIRE FOURNI (COLLECTIVEMENT APPELES « CONTRAT ») AVANT D'OUVRIR L'EMBALLAGE DU LOGICIEL. EN OUVRANT L'EMBALLAGE DU LOGICIEL, VOUS ACCEPTEZ LES TERMES ET CONDITIONS DE CE CONTRAT. SI VOUS ACCEDEZ A CE LOGICIEL DE MANIERE ELECTRONIQUE, INDIQUEZ QUE VOUS ACCEPTEZ CES TERMES ET CONDITIONS EN SELECTIONNANT LE BOUTON « ACCEPT » SITUE A LA FIN DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAR CES TERMES ET CONDITIONS, RENVOYEZ RAPIDEMENT LE LOGICIEL INUTILISE A L'ENDROIT OU VOUS L'AVEZ ACHETE POUR OBTENIR UN REMBOURSEMENT OU, SI VOUS AVEZ ACQUIS LE LOGICIEL DE MANIERE ELECTRONIQUE, SELECTIONNEZ LE BOUTON « DECLINE » SITUE A LA FIN DE CE CONTRAT.

1. LICENCE D'UTILISATION. Sun vous octroie une licence non-exclusive et non-transférable pour l'utilisation en interne du logiciel, de la documentation et des corrections d'erreur s'y afférant fournis par Sun (collectivement nommés « Logiciel »), pour le nombre d'utilisateurs et la classe de matériel informatique pour laquelle les frais correspondants ont été payés.

2. RESTRICTIONS. Le Logiciel est confidentiel et protégé par copyright. Les droits sur le Logiciel, ainsi que tous les droits de propriétés intellectuelles associés sont la propriété de Sun et/ou de ses bailleurs de licence. Sauf mention spéciale spécifiée dans des Termes et conditions de licence supplémentaires, vous n'êtes pas autorisé à copier le Logiciel ; vous êtes cependant autorisé à en effectuer une copie unique à des fins d'archives. A moins que l'application de cette clause soit contraire à la loi en vigueur, vous ne pouvez pas modifier, ou décompiler le Logiciel, ni en inverser l'ingénierie. Vous reconnaissez que le Logiciel n'est pas conçu, fourni sous licence ni prévu pour être utilisé pour la conception, la construction, le fonctionnement ou la maintenance d'une installation nucléaire. Sun décline toute garantie explicite ou implicite d'adéquation à un usage particulier. Aucun droit, titre ou intérêt dans ou pour aucune marque, marque de service ou marque de commerce ni pour aucun logo de Sun ou de ses bailleurs de licence n'est accordé dans le cadre de ce Contrat.

3. GARANTIE LIMITEE. Sun garantit que pendant quatre-vingt-dix (90) jours à compter de la date d'achat, une copie du reçu faisant foi, le support sur lequel le Logiciel est fourni (le cas échéant) sera exempt de défauts de matériels et de façon, dans des conditions normales d'utilisation. A l'exception des mentions précédentes, le Logiciel est fourni « EN L'ETAT ». Votre seul recours et la seule responsabilité de Sun dans le cadre de cette garantie limitée consistera, à la discrétion de Sun, à remplacer le support du Logiciel ou à rembourser le prix payé pour le Logiciel.

4. EXCLUSION DE GARANTIE. SAUF MENTION CONTRAIRE SPECIFIEE DANS CE CONTRAT, TOUTES LES CONDITIONS EXPLICITES OU IMPLICITES, LES REPRESENTATIONS ET LES GARANTIES SONT FORMELLEMENT EXCLUES, NOTAMMENT LES GARANTIES IMPLICITES RELATIVES A LA QUALITE MARCHANDE, A L'ADEQUATION A UN USAGE PARTICULIER OU A LA NON-VIOLATION, DANS LA MESURE OU CES EXCLUSIONS SONT LEGALEMENT VALIDES.

5. LIMITATION DE RESPONSABILITE. DANS LES LIMITES DE LA LOI EN VIGUEUR, SUN ET SES BAILLEURS DE LICENCE NE POURRONT EN AUCUN CAS ETRE TENUS RESPONSABLES POUR LA PERTE DE CHIFFRE D'AFFAIRES, DE PROFIT OU DE DONNEES, OU POUR DES DOMMAGES SPECIAUX, INDIRECTS, DIRECTS, FORTUITS OU DISSUASIFS, QU'ILS DECOULENT DE L'UTILISATION OU DE L'INCAPACITE D'UTILISER LE LOGICIEL, QUELLE QUE SOIT LA THEORIE DE RESPONSABILITE, ET CE MEME SI SUN A ETE AVERTI DE LA POSSIBILITE DE TELS DOMMAGES. En aucun cas la responsabilité de Sun à votre égard, que ce soit par contrat, par délit (y compris la négligence) ou autre, n'excédera le montant payé par vous pour l'acquisition du Logiciel faisant l'objet de ce contrat de licence. Les limitations précédentes s'appliqueront même si la garantie mentionnée ci-dessus ne remplit pas son but.

6. RESILIATION. Ce Contrat est effectif jusqu'à sa résiliation. Vous pouvez le résilier à tout moment en détruisant toutes les copies du Logiciel. Ce Contrat sera immédiatement résilié sans préavis de Sun si vous ne vous conformez pas à l'une de ses clauses. En cas de résiliation, vous devez détruire toutes les copies du Logiciel.

7. REGLEMENTATIONS D'EXPORTATION. Le Logiciel et les données techniques faisant l'objet de ce Contrat sont soumis aux lois de contrôle à l'exportation des Etats-Unis et peuvent être régis par la réglementation pour l'exportation ou l'importation dans d'autres pays. Vous acceptez de vous conformer strictement à ces lois et ces réglementations et reconnaissez que vous assumez l'entière responsabilité pour l'obtention des licences nécessaires pour l'exportation, la réexportation ou l'importation une fois que le produit vous a été livré.

8. DROITS RESTREINTS DU GOUVERNEMENT DES ETATS-UNIS. Si le Logiciel a été acquis par ou au nom du gouvernement des Etats-Unis ou par une partie contractante ou un sous-traitant du gouvernement (à quelque niveau que ce soit), alors les droits du gouvernement relatifs au Logiciel et à la documentation s'y afférant seront restreints aux droits stipulés dans ce Contrat de licence ; ils sont conformes aux articles 48 CFR 227.7201 à 227.7202-4 (pour les acquisitions du ministère de la Défense) et aux articles 48 CFR 2.101 et 12.212 (pour les acquisitions d'autres services ou ministères).

9. LOI GOUVERNEMENTALE. Toute action relative à ce Contrat sera régie par la législation de la Californie et par les lois fédérales des Etats-Unis. Aucun choix de législation d'une juridiction donnée ne s'appliquera.

10. AUTONOMIE DES CLAUSES DU CONTRAT. Si l'une des clauses de ce Contrat s'avérait inapplicable, le Contrat restera effectif sans cette clause, à moins que cette omission ne lèse l'une des parties, auquel cas ce Contrat sera immédiatement résilié.

11. INTEGRATION. Ce Contrat représente le contrat intégral entre vous et Sun à ce sujet. Il remplace toute communication, proposition, représentation et garantie orales ou écrites, antérieures ou contemporaines, et prévaut sur tout terme conflictuel ou supplémentaire de devis, commande, reconnaissance ou autre communication entre les parties concernées par ce sujet au cours de la période de validité de ce Contrat. Aucune modification apportée à ce Contrat n'aura force de loi, à moins qu'elle ne soit écrite et signée par les représentants autorisés de chaque partie.

Si vous avez des questions, contactez : Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054, Etats-Unis

(Formulaire n° 011801)

Sun Microsystems, Inc.

Termes et conditions supplémentaires pour Sun Crypto Accelerator 4000

Ces termes et conditions supplémentaires pour Sun Crypto Accelerator 4000 complètent les termes et conditions du Contrat de licence relatif au code binaire (CLCB). Les termes commençant par une majuscule non définis ici ont la même signification que dans le CLCB. Ces termes et conditions supplémentaires remplacent tout terme incohérent ou conflictuel du CLCB. L'utilisation du logiciel signifie que vous acceptez les termes du CLCB corrigés par la présente.

1. TERMES DE LICENCE DE PARTIES TIERCES. Certaines parties du Logiciel sont fournies avec des avertissements et/ou des licences de tiers qui régissent l'utilisation de ces parties.

Third Party License Terms

OPENSSL LICENSE ISSUES

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

OpenSSL License

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

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

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

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

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

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

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

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

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

Original SSLeay License

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

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

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

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

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

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

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

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

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

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

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

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

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

MOD_SSL LICENSE

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

Copyright (c) 1998-2000 Ralf S. Engelschall. All rights reserved.

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

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

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

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

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

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

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

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

ANNEXE **E**

Pages du manuel

Cette annexe décrit les commandes de la carte Crypto Accelerator 4000 de Sun et répertorie les pages du manuel en ligne relatives à chacune d'elle. Les commandes de cette annexe sont incluses dans le logiciel Crypto Accelerator 4000 de Sun.

Les pages du manuel en ligne peuvent être affichées avec la commande suivante :

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

Le TABLEAU E-1 répertorie et décrit les pages du manuel en ligne disponibles.

TABLEAU E-1 Pages du manuel en ligne de Crypto Accelerator 4000 de Sun

Page man	Description
vca(7d)	Le pilote de périphérique vca est un pilote feuille qui offre un contrôle d'accès à l'accélérateur cryptographique matériel sous-jacent. Le pilote vca nécessite un logiciel en couches pour que les applications et les clients du noyau puissent accéder aux services fournis.
vcad(1m)	Le démon vcad fournit des services de stockage de clés.
vcaadm(1m)	vcaadm est un programme d'administration pour Crypto Accelerator 4000 de Sun. La commande vcaadm est utilisée pour la manipulation de la configuration, du compte et des bases de données de clés associés à la carte Crypto Accelerator 4000 de Sun. vcaadm traite des informations importantes relatives aux clés cryptographiques.
vcadiag(1m)	vcadiag est un utilitaire permettant aux utilisateurs racines de réinitialiser les cartes Crypto Accelerator 4000 de Sun et de remettre à zéro la clé matérielle. Cet utilitaire permet également aux utilisateurs racines d'exécuter des diagnostics de base.

TABLEAU E-1 Pages du manuel en ligne de Crypto Accelerator 4000 de Sun *(suite)*

Page `man`	Description
`kcl2`(7d)	`kcl2` est un module du noyau qui prend en charge les pilotes matériels cryptographiques.
`kcl2`(7d)	Le pilote de périphérique `kcl2` est un module de noyau chargeable multithread offrant une prise en charge des pilotes de fournisseurs cryptographiques de Sun. Le pilote `kcl2` nécessite un logiciel en couches pour que les applications et les clients du noyau puissent accéder aux services fournis.
`apsslcfg`(1m)	`apsslcfg` est l'utilitaire de configuration pour les serveurs Web Apache.
`iplsslcfg`(1m)	`iplsslcfg` est l'utilitaire de configuration pour les serveurs Web Sun ONE.

ANNEXE **F**

Remise à zéro du matériel

Cette annexe explique comment restaurer l'état par défaut de la carte Crypto Accelerator 4000 de Sun, qui correspond au mode `failsafe`.

Attention – Utilisez les procédures décrites dans cette annexe uniquement si elles s'avèrent absolument nécessaires. La commande `zeroize` dans `vcaadm` est appropriée si vous devez retirer toutes les clés matérielles. Reportez-vous à la section « Remise à zéro d'une Carte Crypto Accelerator 4000 de Sun », page 84 pour plus de détails sur la commande `zeroize`. Reportez-vous également aux pages du manuel en ligne relatives à `vcadiag`(4) pour le retrait de toutes les clés matérielles.

Remarque – Les procédures décrites dans cette annexe suppriment le microprogramme Crypto Accelerator 4000 de Sun. Vous devrez réinstaller le microprogramme fourni avec le logiciel Crypto Accelerator 4000 de Sun.

Restauration de l'état par défaut du matériel Crypto Accelerator 4000 de Sun

Dans certains cas, il peut s'avérer nécessaire de restaurer le mode `failsafe` de la carte et d'effacer toutes les clés matérielles et toutes les informations de configuration. Pour ce faire, vous devez utiliser le cavalier matériel relié à la carte.

Remarque – Vous pouvez utiliser la commande `zeroize` avec l'utilitaire `vcaadm` pour supprimer toutes les clés matérielles d'une carte Crypto Accelerator 4000 de Sun. Cependant, la commande `zeroize` n'affecte aucunement le microprogramme mis à jour. Voir la section « Remise à zéro d'une Carte Crypto Accelerator 4000 de Sun », page 84. Reportez-vous également aux pages du manuel en ligne relatives à `vcadiag`.

▼ Pour remettre à zéro la Carte Crypto Accelerator 4000 de Sun avec le cavalier matériel

1. **Mettez le système hors tension.**

Remarque – Pour certains systèmes, vous pouvez utiliser la fonction de reconfiguration dynamique pour retirer et remplacer la carte nécessaire pour cette procédure plutôt que de mettre le système hors tension. Reportez-vous à la documentation livrée avec votre système pour connaître les procédures correctes associées à cette fonction.

Attention – La carte ne doit recevoir aucune alimentation électrique pendant le réglage du cavalier.

2. **Retirez le couvercle de l'ordinateur pour avoir accès au cavalier situé au milieu de la partie supérieure de la carte.**
3. **Placez le cavalier sur les broches 0 et 1 du bloc de cavaliers.**

   Les broches 0 et 1 sont les broches les plus proches du support et portent la mention « Z ». Il existe quatre jeux de deux broches et le cavalier devrait uniquement être placé sur la broche 0 et 1, comme indiqué dans la FIGURE F-1.

Attention – Vous ne pouvez pas utiliser la carte Crypto Accelerator 4000 de Sun en disposant le cavalier sur les broches 0 et 1.

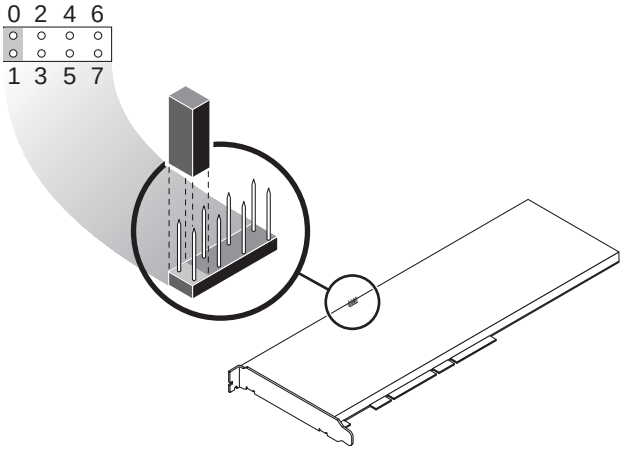

FIGURE F-1 Broches du bloc de cavaliers de la Carte Crypto Accelerator 4000 de Sun

4. **Mettez le système sous tension.**

Attention – Lorsque vous mettez le système sous tension après avoir ajusté le cavalier de la carte Crypto Accelerator 4000 de Sun, tout le microprogramme, les clés matérielles et les informations de configuration sont supprimés. Cette procédure restaure l'état par défaut de la carte et la définit en mode `failsafe`.

5. **Mettez le système hors tension.**
6. **Retirez le cavalier des broches 0 et 1 du bloc de cavaliers et placez le cavalier à son emplacement d'origine.**
7. **Mettez le système sous tension.**
8. **Etablissez la connexion à la carte Crypto Accelerator 4000 de Sun avec** `vcaadm`.

   `vcaadm` vous invite à entrer un chemin de mise à niveau du microprogramme.
9. **Saisissez** `/opt/SUNWconn/cryptov2/firmware/sca4000fw` **comme chemin pour l'installation du microprogramme.**

   Le microprogramme est automatiquement installé et vous êtes déconnecté de `vcaadm`.

10. **Rétablissez la connexion à la carte Crypto Accelerator 4000 de Sun avec `vcaadm`.**

    `vcaadm` vous invite à initialiser la carte avec un nouveau stockage de clés ou à l'initialiser pour utiliser un stockage de clés existant. Voir la section « Initialisation de la Carte Crypto Accelerator 4000 de Sun avec `vcaadm` », page 68.

ANNEXE **G**

Questions fréquentes

Comment configurer le serveur Web pour qu'il démarre sans que l'utilisateur n'ait à le redémarrer ?

Vous pouvez activer les serveurs Web Sun ONE et Apache pour qu'ils démarrent automatiquement lors du redémarrage avec une clé chiffrée.

▼ Pour créer une clé chiffrée pour un démarrage automatique des serveurs Web Apache au redémarrage

1. **Vérifiez que l'entrée suivante existe dans le fichier `httpd.conf` :**

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

Cette directive récupère un mot de passe dans un fichier de mot de passe protégé dans le répertoire `/etc/apache`.

2. **Créez un fichier de mot de passe qui contient uniquement le mot de passe dans le répertoire `/etc/apache`, en suivant la convention d'attribution de nom suivante :**

nom_serveur`:`*port*`.`*TYPECLE*`.pass`

- *nom_serveur* : la valeur que vous définissez dans la directive « ServerName » du fichier `httpd.conf`.
- *port* : le port sur lequel ce serveur SSL sera exécuté (par exemple, 443)
- *TYPECLE* : `RSA` ou `DSA`

Exemple : pour un serveur nommé `webserv101` exécutant SSL sur le port 443 avec une clé `RSA`, vous créez le fichier suivant dans `/etc/apache` :

```
webserv101:443.RSA.pass
```

Il est recommandé de changer les autorisations et la propriété du fichier de mot de passe comme suit :

```
# chmod 400 nom_serveur:port.TYPECLE.pass
# chown root nom_serveur:port.TYPECLE.pass
```

Reportez-vous à la documentation de mod_SSL et d'OpenSSL pour de plus amples informations.

▼ Pour créer une clé chiffrée pour un démarrage automatique des serveurs Web Sun ONE au redémarrage

1. **Accédez au sous-répertoire `config` pour l'instance de votre serveur Web Sun ONE, par exemple, `/usr/iplanet/servers/https-`*nom_instance_serveurweb*`/config`.**

2. **Créez un fichier `password.conf` avec uniquement les lignes suivantes (voir le** TABLEAU 5-1 **pour des définitions de mot de passe) :**

```
internal:motpasse_bd_certifiée
nom_stockageclés:nomutilisateur:motpasse
```

3. **Définissez la propriété pour le fichier de mot de passe sur l'ID de l'utilisateur UNIX avec lequel le serveur est exécuté, puis définissez les autorisations du fichier de manière à ce que ce dernier soit uniquement lisible par son propriétaire :**

```
# chown ID_utilisateur_UNIX_serveur_web password.conf
# chmod 400 password.conf
```

Comment attribuer différentes adresses MAC à plusieurs cartes installées sur le même serveur ?

Il existe deux méthodes pour affecter différentes adresses MAC à plusieurs cartes sur un même serveur. La première méthode a lieu au niveau de l'environnement d'exploitation, la seconde a lieu au niveau OpenBoot PROM (OBP).

▼ Pour attribuer différentes adresses MAC depuis une fenêtre de terminal

1. **Entrez la commande suivante :**

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

Remarque – Quand le paramètre `local-mac-address?` est défini sur `true`, tous les périphériques d'interface réseau non-intégrés utilisent l'adresse MAC affectée au produit lors de la fabrication.

---

2. **Redémarrez le système.**

▼ Pour attribuer différentes adresses MAC au niveau OpenBoot PROM

1. **Entrez la commande suivante à l'invite OBP :**

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

Remarque – Quand le paramètre `local-mac-address?` est défini sur `true`, tous les périphériques d'interface réseau non-intégrés utilisent l'adresse MAC affectée au produit lors de la fabrication.

---

2. **Démarrez l'environnement d'exploitation.**

Comment configurer Sun Crypto Accelerator 1000 pour l'utiliser avec Apache après avoir installé le logiciel Crypto Accelerator 4000 de Sun ?

Une fois le progiciel `SUNWkcl2a` installé, le système sera configuré avec mod_ssl 1.3.26 du serveur Web Apache.

Si vous voulez configurer Sun Crypto Accelerator 1000 avec Apache, vous devez disposer des correctifs mentionnés ci-après.

Pour configurer Sun Crypto Accelerator 1000 pour une utilisation avec Apache 1.3.26 sur un système Solaris 8 avec le progiciel `SUNWkcl2a` installé, vous devez disposer des correctifs suivants :

- Pour Apache 1.3.26 – Correctif 109234-09 ou ultérieur
- Pour le logiciel Sun Crypto Accelerator 1000 version 1.0 – Correctif 112869-02
- Pour le logiciel Sun Crypto Accelerator 1000 version 1.1 – Correctif 113355-01

Pour configurer Sun Crypto Accelerator 1000 pour une utilisation avec Apache 1.3.26 sur un système Solaris 9 avec le progiciel `SUNWkcl2a` installé, vous devez disposer des correctifs suivants :

- Pour Apache 1.3.26 – Correctif 113146-01 ou ultérieur
- Pour le logiciel Sun Crypto Accelerator 1000 version 1.1 – Correctif 113355-01

Comment auto-signer un certificat pour un test ?

Reportez-vous à la documentation de mod_SSL et d'OpenSSL pour de plus amples informations sur cette procédure.

Index

C

D

E

F

G

H

I

J

K

R

S

T

U

V

W

Z