

Guide de l'utilisateur et d'installation de la carte Crypto Accelerator 1000 Version 1.1 de Sun™

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

Référence n° 816-4566-11
juin 2002, révision A

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

Copyright 2002 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 Etats-Unis. Tous droits réservés.

Ce produit ou document est distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et accordé sous licence par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD accordés sous licence par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et accordée sous licence exclusive de X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, SunVTS, AnswerBook2, docs.sun.com, iPlanet, Sun Enterprise, Sun Enterprise Volume Manager, Sun Fire, SunSolve, Netra et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc. Netscape est une marque de Netscape Communications Corporation aux Etats-Unis et dans d'autres pays. Ce produit comprend le logiciel développé par OpenSSL Project conçu pour être utilisé dans le Toolkit OpenSSL (<http://www.openssl.org/>). Ce produit comprend le logiciel cryptographique écrit par Eric Young (eay@cryptsoft.com). Ce produit comprend le logiciel développé par Ralf S. Engelschall (rse@engelschall.com) conçu pour être utilisé dans le cadre du projet mod_ssl (<http://www.modssl.org/>).

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

LA DOCUMENTATION EST FOURNIE « EN L'ETAT » ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.



Declaration of Conformity

EMC

Compliance Model Number: DEIMOS

Product Family Name: Sun Crypto Accelerator 1000 (X6762A)

European Union

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

EN55022:1998/CISPR22:1997 Class A

EN55024:1998 Required Limits (as applicable):

EN61000-4-2 4 kV (Direct), 8 kV (Air)

EN61000-4-3 3 V/m

EN61000-4-4 1 kV AC Power Lines, 0.5 kV Signal and DC Power Lines

EN61000-4-5 1 kV AC Line-Line and Outdoor Signal Lines

2 kV AC Line-Gnd, 0.5 kV DC Power Lines

EN61000-4-6 3 V

EN61000-4-8 1 A/m

EN61000-4-11 Pass

EN61000-3-2:1995 + A1, A2, A14 Pass

EN61000-3-3:1995 Pass

Safety

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

EC Type Examination Certificates:

EN 60950:2000, 3rd Edition

IEC 60950:1999, 3rd Edition

Supplementary Information

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

/S/

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

DATE

/S/

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

DATE

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

1. Présentation du produit 1

Présentation du matériel 1

Caractéristiques du produit 2

Prise en compte de la fonctionnalité Dynamic Reconfiguration et de la
caractéristique High Availability 3

Partage de charge 4

Conditions logicielles et matérielles requises 5

Correctifs requis 5

Correctifs Solaris 8 6

Correctifs Solaris 9 6

2. Installation de la Carte Crypto Accelerator 1000 de Sun 7

Manipulation de la carte 7

Installation de la carte 8

▼ Pour installer le matériel 8

Installation du logiciel Crypto Accelerator 1000 de Sun 9

▼ Pour installer le logiciel 9

Répertoires et fichiers 12

Désinstallation du logiciel 13

▼ Pour désinstaller le logiciel 14

3. Activation de la carte pour les serveurs Web iPlanet	15
Mots de passe	15
Création et remplissage d'un domaine	16
▼ Pour créer et remplir un domaine	16
Aperçu de l'activation des serveurs Web iPlanet	18
4. Installation et configuration d'un serveur Web iPlanet 4.1	19
Installation d'un serveur Web iPlanet 4.1	19
▼ Pour installer un serveur Web iPlanet 4.1	19
▼ Pour créer une base de données certifiée	20
▼ Pour créer un certificat de serveur	23
▼ Pour installer le certificat de serveur	25
Configuration d'un serveur Web iPlanet 4.1	26
▼ Pour configurer le serveur Web iPlanet 4.1	26
5. Installation et configuration d'un serveur Web iPlanet 6.0	29
Installation du serveur Web iPlanet 6.0	29
▼ Pour installer le serveur Web iPlanet 6.0	29
▼ Pour créer une base de données certifiée	30
▼ Pour créer un certificat de serveur	33
▼ Pour installer le certificat de serveur	35
Configuration du serveur Web iPlanet 6.0	36
▼ Pour configurer le serveur Web iPlanet 6.0	36
6. Activation du serveur Web Apache	39
Activation du serveur Web Apache	39
▼ Pour activer le serveur Web Apache	39
Création d'un certificat	42
▼ Pour créer un certificat	42

7. Diagnostics et dépannage	47
Logiciel de diagnostics SunVTS	47
▼ Pour lancer dcatest	48
Options de paramètres de test pour dcatest	49
Syntaxe de la ligne de commande dcatest	49
Dépannage du périphérique Crypto Accelerator 1000 de Sun	51
A. Administration de la carte Crypto Accelerator 1000 de Sun avec un serveur Web iPlanet	53
Concepts et terminologie	53
Domaines, utilisateurs et serveur Web iPlanet	54
Jetons et fichiers de jetons	55
Fichiers de jetons	55
Utilisation de secadm	56
Modes de fonctionnement	57
Saisie de commandes avec secadm	59
Authentification à l'aide de secadm	59
Obtention d'aide pour les commandes	61
Fermeture du programme secadm	62
Configuration et gestion des domaines	62
Création d'un domaine	63
Configuration du domaine actuellement en fonctionnement	64
Création d'une liste des domaines	65
Création d'une liste des classes de domaines	66
Suppression d'un domaine	66
Configuration et gestion des comptes utilisateur	67
Création d'utilisateurs	67
Création d'une liste d'utilisateurs	67

Modification des mots de passe utilisateur	68
Activation ou désactivation des utilisateurs	68
Suppression des utilisateurs	69
B. Pages manuel	71
C. Directives de configuration SSL pour le serveur Web Apache	73
D. Création d'applications pour une utilisation avec la Carte Crypto Accelerator 1000 de Sun	83
E. Spécifications de la Carte Crypto Accelerator 1000 de Sun	85
Dimensions physiques	85
Spécifications de l'interface	86
Alimentation requise	86
Caractéristiques environnementales	86
F. Licences tierces	87

Tableaux

TABLEAU 1-1	Algorithmes SSL pris en charge	3
TABLEAU 1-2	Conditions logicielles et matérielles requises	5
TABLEAU 1-3	Correctifs Solaris 8 requis pour le logiciel Crypto Accelerator 1000 de Sun	6
TABLEAU 1-4	Correctifs Solaris 8 recommandés pour le logiciel Crypto Accelerator 1000 de Sun	6
TABLEAU 2-1	Fichiers du répertoire /cdrom/cdrom0	10
TABLEAU 2-2	Répertoires Crypto Accelerator 1000 de Sun	12
TABLEAU 3-1	Mots de passe requis pour les serveurs Web iPlanet	16
TABLEAU 7-1	Sous-tests dcatetest	49
TABLEAU 7-2	Syntaxe de la ligne de commande dcatetest	50
TABLEAU A-1	Options secadm	57
TABLEAU A-2	Tableau des commandes d'administration	60
TABLEAU B-1	Crypto Accelerator 1000 de Sun Pages man du logiciel	71
TABLEAU C-1	Protocoles SSL	75
TABLEAU C-2	Chiffres SSL disponibles	76
TABLEAU C-3	Alias SSL	77
TABLEAU C-4	Caractères spéciaux pour la configuration des préférences de chiffre	78
TABLEAU C-5	Niveaux de vérification SSL des clients	79
TABLEAU C-6	Valeurs de niveau du fichier journal SSL	80
TABLEAU C-7	Options SSL disponibles	81
TABLEAU E-1	Dimensions physiques	85

TABLEAU E-2	Spécifications de l'interface	86
TABLEAU E-3	Alimentation requise	86
TABLEAU E-4	Caractéristiques environnementales	86

Préface

Le Guide de l'utilisateur et d'installation de la carte Crypto Accelerator 1000 Version 1.1 de Sun décrit les caractéristiques de la carte Crypto Accelerator 1000 de Sun™ ainsi que son installation et utilisation 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 iPlanet et Apache, du logiciel SunVTS™ et dans l'acquisition d'autorités de certification.

Présentation du manuel

Le manuel est composé des chapitres suivants :

- Le chapitre 1 - présentation de la carte Crypto Accelerator 1000 de Sun et aperçu des exigences matérielles et logicielles.
- Le chapitre 2 - description des procédures d'installation logicielle et matérielle de Crypto Accelerator 1000 de Sun.
- Le chapitre 3 - explication du mode d'activation de la carte Crypto Accelerator 1000 de Sun pour l'utiliser avec les serveurs Web iPlanet.
- Le chapitre 4 - explication du mode d'activation de la carte Crypto Accelerator 1000 de Sun pour l'utiliser avec les serveurs Web iPlanet 4.1.
- Le chapitre 5 - explication du mode d'activation de la carte Crypto Accelerator 1000 de Sun pour l'utiliser avec les serveurs Web iPlanet 6.0.
- Le chapitre 6 - explication du mode d'activation de la carte Crypto Accelerator 1000 de Sun pour l'utiliser avec les serveurs Web Apache.
- Le chapitre 7 - description des tests de diagnostic et du dépannage pour le logiciel Crypto Accelerator 1000 de Sun.

- L'annexe A - présentation des fonctionnalités de la carte Crypto Accelerator 1000 de Sun administrée avec un serveur Web iPlanet.
- L'annexe B - descriptions des pages man comprises avec le logiciel Crypto Accelerator 1000 de Sun.
- L'annexe C - directives de configuration de la prise en charge SSL des serveurs Web Apache dotés du logiciel Crypto Accelerator 1000 de Sun.
- L'annexe D - présentation du logiciel accompagnant la carte Crypto Accelerator 1000 de Sun version 1.1, qui peut être utilisé pour construire des applications compatibles avec OpenSSL afin de bénéficier des fonctions d'accélération cryptographique de la carte Crypto Accelerator 1000 de Sun.
- L'annexe E - description des diverses spécifications de la carte Crypto Accelerator 1000 de Sun.
- L'annexe F - énonciation de consignes et de licences relatives à certaines portions du logiciel et émanant d'autres parties qui régissent l'utilisation de ces portions.

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, à l'adresse `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 <code>.login</code> . Utilisez <code>ls -a</code> 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 Password:
<i>AaBbCc123</i>	Titres de guide, nouveaux mots ou termes, mots à mettre en valeur.	Consultez le chapitre 6 du <i>Guide de l'utilisateur</i> . Il s'agit d'options de <i>catégorie</i> . Vous <i>devez</i> 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 <code>rm nomfichier</code> .

Invites Shell

Shell	Invite
C shell	<i>nom_machine%</i>
C shell superutilisateur	<i>nom_machine#</i>
Bourne shell et Korn shell	\$
Bourne shell et Korn shell superutilisateur	#

Accès à la documentation de Sun en ligne

Vous trouverez un grand choix de documentation sur les systèmes Sun à l'adresse suivante :

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

Vous trouverez une documentation exhaustive sur Solaris, ainsi que d'autres ouvrages, à l'adresse :

<http://docs.sun.com>

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 (816-4566-11) de votre documentation dans l'objet de votre message électronique.

Présentation du produit

Ce chapitre décrit la carte Crypto Accelerator 1000 de Sun et est composé des sections suivantes :

- « Présentation du matériel », page 1
- « Conditions logicielles et matérielles requises », page 5

Présentation du matériel

La carte Crypto Accelerator 1000 de Sun est une petite carte PCI qui fonctionne de la même manière qu'un co-processeur cryptographique ; elle vise à accélérer la cryptographie symétrique et la cryptographie de clés publiques. Ce produit ne comporte aucune interface externe. En effet, la carte communique avec l'hôte par l'interface du bus PCI interne. Elle a été conçue dans le but d'accélérer tout un ensemble d'algorithmes cryptographiques sollicitant des calculs à très hautes vitesses, pour des protocoles de sécurité utilisés dans le cadre d'applications de commerce électronique.

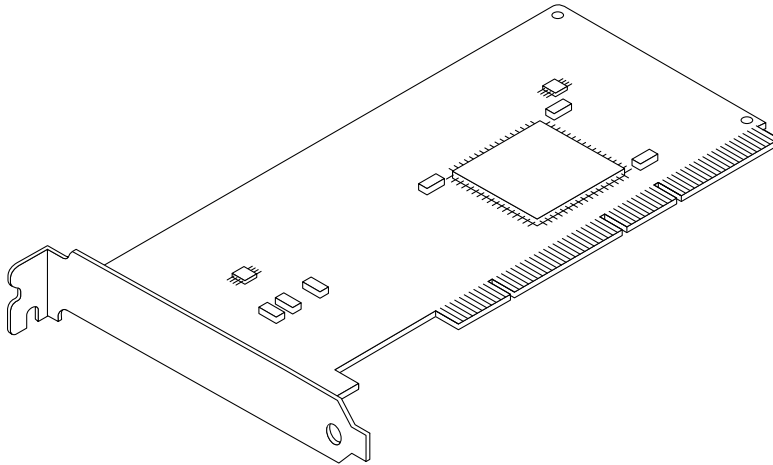


FIGURE 1-1 Carte Crypto Accelerator 1000 de Sun

Caractéristiques du produit

La carte Crypto Accelerator 1000 de Sun est une carte d'accélération cryptographique permettant d'optimiser les performances de SSL sur les plates-formes Sun. La carte Crypto Accelerator 1000 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 (par exemple, ARCFOUR) peuvent être traités par un logiciel hautement optimisé aussi rapidement que par du matériel dédié.

La carte Crypto Accelerator 1000 de Sun examine chaque requête cryptographique et détermine le meilleur emplacement pour l'accélération (processeur hôte ou carte Crypto Accelerator 1000 de Sun), afin de parvenir à un débit maximum. La distribution de la charge dépend de l'algorithme cryptographique, du chargement en cours et de la taille des données.

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

TABLEAU 1-1 Algorithmes SSL pris en charge

Algorithme	Serveurs Web iPlanet		Serveurs Web Apache	
	Matériel	Logiciel	Matériel	Logiciel
RSA	X	X	X	X
DSA	X	X	X	X
Diffie-Hellman			X	X
DES	X	X	X	X
3DES			X	X
ARCFOUR				X

Prise en compte de la fonctionnalité Dynamic Reconfiguration et de la caractéristique High Availability

Le matériel Crypto Accelerator 1000 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 1000 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 1000 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 1000 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 1000 de Sun règle les algorithmes de programmation en fonction de la réduction des ressources matérielles. Les requêtes cryptographiques suivantes seront programmées sur les cartes restantes.

De plus, les bibliothèques du logiciel Crypto Accelerator 1000 de Sun permettent d'effectuer toutes les opérations cryptographiques logicielles, comme la DR et la suppression à chaud de toutes les cartes Crypto Accelerator 1000 de Sun, au sein

d'un domaine de système, sans provoquer de dysfonctionnement. Cependant, il faudra prévoir une perte de performance significative, jusqu'à ce que la configuration du matériel Crypto Accelerator 1000 de Sun prise en charge soit restaurée.

Notez que le matériel Crypto Accelerator 1000 de Sun fournit une source d'entropie de haute qualité pour la création de clés de longue durée. Si toutes les cartes Crypto Accelerator 1000 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 1000 de Sun répartie 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 première 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 1-2 résume les conditions logicielles et matérielles requises pour la Carte Crypto Accelerator 1000 de Sun.

TABLEAU 1-2 Conditions logicielles et matérielles requises

Matériel et logiciel	Conditions requises
Matériel	Sun Blade™ 1000 Sun Enterprise™ 220R, 250, 420R, 450 Sun Fire™ 280R, V480, V880, 4800, 4810, 6800, Sun Netra™ T1 AC200/DC200, 20, t 100/105, t 1120/1125 t 1400/1405 Sun Ultra™ 5, 10, 30, 60, 80
Environnement d'exploitation	Solaris 8 7/01 ou version ultérieure compatible Solaris 9 ou version ultérieure compatible
Emplacements PCI	32 ou 64 bits 33 ou 66 MHz
Logiciel	Serveur Web iPlanet 4.1 SP9, 6.0 SP1, ou serveur Web Apache 1.3.12, 1.3.22 Tout correctif nécessaire pour le démarrage des serveurs Web iPlanet ou Apache

Remarque – Le numéro du service pack (SP9 ou SP1) est indiqué toutes les fois que le serveur Web iPlanet 4.1 ou 6.0 est mentionné.

Correctifs requis

Les correctifs suivants sont requis pour le démarrage de la carte Crypto Accelerator 1000 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, le cas échéant, 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 SunSolveSM, contactez un représentant du personnel commercial ou technique.

Correctifs Solaris 8

Les tableaux suivants répertorient les correctifs Solaris 8 requis et recommandés pour l'utilisation avec ce produit. Le TABLEAU 1-3 répertorie et décrit les correctifs requis.

TABLEAU 1-3 Correctifs Solaris 8 requis pour le logiciel Crypto Accelerator 1000 de Sun

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

Remarque – Si vous envisagez d'utiliser le serveur Web Apache 1.3.12, vous devez également installer le correctif 109234-02.

Le TABLEAU 1-4 répertorie et décrit les correctifs Solaris 8 recommandés.

TABLEAU 1-4 Correctifs Solaris 8 recommandés pour le logiciel Crypto Accelerator 1000 de Sun

Numéro de correctif	Description
108528-13	KU-13 (corrections relatives à la sécurité nvpair)

Correctifs Solaris 9

Aucun correctif Solaris 9 n'est requis ni recommandé pour le moment.

Installation de la Carte Crypto Accelerator 1000 de Sun

Ce chapitre décrit les procédures d'installation logicielle et matérielle de la carte Crypto Accelerator 1000 de Sun ; il est composé des sections suivantes :

- « Manipulation de la carte », page 7
- « Installation de la carte », page 8
- « Répertoires et fichiers », page 12

Manipulation de la carte

Chaque carte est emballée dans un sachet antistatique spécial par souci de protection lors de l'expédition et du stockage. Pour éviter d'endommager les composants de la carte à cause de 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 1000 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 pour tenir le support à l'étape 5.
5. En tenant la carte Crypto Accelerator 1000 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. Remplacez 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 partir de l'invite `ok` :

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

Les lignes `/pci@1f,2000/pci108e,5455@n` indiquent que la carte est installée et reconnue par le système. Chaque carte du système sera associée à une ligne de ce type.

Installation du logiciel Crypto Accelerator 1000 de Sun

Le logiciel Crypto Accelerator 1000 de Sun est compris dans le CD-ROM Crypto Accelerator 1000 de Sun. Vous devrez peut-être télécharger des correctifs à partir du site Web SunSolve. Voir la section « Correctifs requis », page 5 pour plus d'informations.

▼ Pour installer le logiciel

1. Désinstallez la totalité du logiciel Crypto Accelerator 1000 de Sun version 1.0 avant d'installer la version 1.1. Pour cela, utilisez la commande suivante :

```
# pkgrm SUNwcrysl SUNWdcav SUNWdcar SUNwcrysu SUNwcrypu SUNwcrypr  
SUNWdcamn SUNwcrypm
```

2. Insérez le CD-ROM Crypto Accelerator 1000 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 1000 Version 1.1 de Sun
Packages	Contient les progiciels Crypto Accelerator 1000 de Sun :
	SUNWcrypr composants du noyau de cryptographie
	SUNWcrypu bibliothèques et utilitaire d'administration cryptographique
	SUNWcrysu prise en charge SSL pour Apache (<i>facultatif</i>)
	SUNWcrypm pages manuel d'administration cryptographique
	SUNWdcar accélérateur cryptographique DCA (racine)
	SUNWdcamn page manuel de l'accélérateur cryptographique DCA
	SUNWdcav test SunVTS de l'accélérateur cryptographique DCA (<i>facultatif</i>)
	SUNWcrys1 outils et bibliothèques de développement SSL (<i>facultatif</i>)

Installez le progiciel SUNWcrys1 uniquement si vous envisagez d'utiliser Apache comme votre serveur Web.

Installez le progiciel SUNWcrys1 uniquement si vous envisagez de vous relier à une autre version (non prise en charge) du serveur Web Apache.

Installez le progiciel SUNWdcav uniquement si vous envisagez d'effectuer les tests SunVTS™. Pour installer le progiciel SUNWdcav, vous devez d'abord installer SunVTS 4.4, 4.5, 4.6 ou 5.0.

3. Installez les progiciels en saisissant :

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

4. Pour vous assurer que le logiciel a été installé correctement, exécutez la commande `pkginfo`.

```
# pkginfo SUNWcrypr SUNWcrypu SUNWcrys1 SUNWcrys2 SUNWcryptm SUNWdcar SUNWdcamn
SUNWdcav
system SUNWcrypr   Cryptography Kernel Components
system SUNWcrypu   Cryptographic Administration Utility and Libraries
system SUNWcrys1   SSL Development Tools and Libraries
system SUNWcrys2   SSL Support for Apache
system SUNWcryptm   Cryptographic Administration Manual Pages
system SUNWdcar     DCA Crypto Accelerator (Root)
system SUNWdcamn    DCA Crypto Accelerator Manual Page
system SUNWdcav     SunVTS Test of DCA Crypto Accelerator
```

5. (Facultatif) Pour vous assurer que le pilote est relié, exécutez la commande `prtconf`. Si plusieurs cartes Crypto Accelerator 1000 de Sun sont installées, plusieurs lignes apparaissent, comme dans l'exemple suivant.

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

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

Toutefois, tant que vous n'avez pas utilisé la carte Crypto Accelerator 1000 de Sun pour effectuer des cryptographies, il se peut que `kcl` et `cryptio` ne soient pas chargés ou n'apparaissent pas.

```
# modinfo | grep Crypto
130 1033e946 6df0 79 1 cryptio (Cryptographic IOCTL v1.58)
131 1030240c 2d93 - 1 kcl (Cryptographic Library v1.64)
132 10313ac8 131e - 1 kcp1 (Crypto Provider Interface v1.27)
135 103178be 8684 82 1 dca (PCI Crypto Accelerator v1.156)
```

Répertoires et fichiers

Le TABLEAU 2-2 indique les répertoires créés après l'installation par défaut du logiciel Crypto Accelerator 1000 de Sun.

TABLEAU 2-2 Répertoires Crypto Accelerator 1000 de Sun

Répertoire	Contenu
/etc/opt/SUNWconn/crypto/realms	Domaine et données de l'utilisateur
/opt/SUNWconn/crypto/bin	Exécutables d'application
/opt/SUNWconn/crypto/lib	Bibliothèques d'application
/opt/SUNWconn/crypto/sbin	Exécutables liés statiquement

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

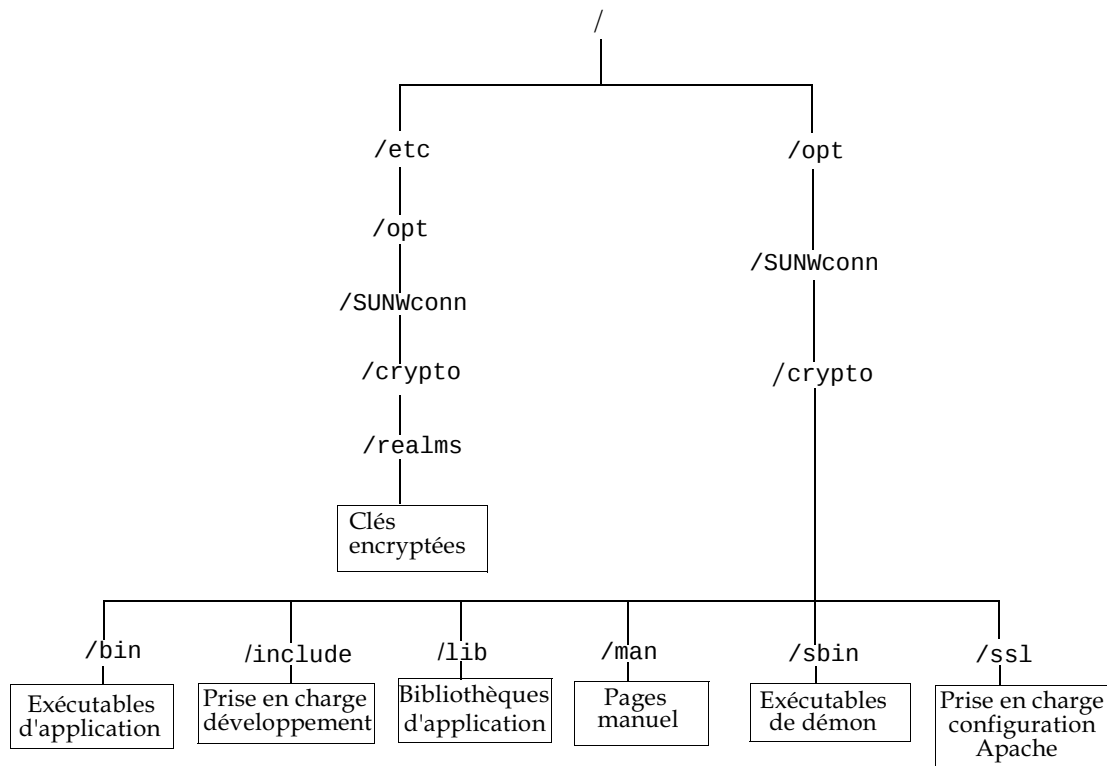


FIGURE 2-1 Crypto Accelerator 1000 de Sun - Répertoires et fichiers

Désinstallation du logiciel

Si vous avez créé des domaines, vous devez les supprimer avant de désinstaller le logiciel. Veuillez vous reporter à la section « Pour supprimer les domaines », page 66. Si vous n'avez créé aucun domaine, vous pouvez ignorer cette procédure. Vous ne pouvez pas supprimer un domaine qui est en cours d'utilisation. Pour supprimer des références dans les domaines, il se peut que vous deviez fermer le serveur Web et/ou le serveur d'administration.



Attention – Avant de désinstaller le logiciel Crypto Accelerator 1000 de Sun, vous devez désactiver tous les serveurs Web activés pour l'utilisation de la carte Crypto Accelerator 1000 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 SUNwcrysl SUNwdcav SUNwdcar SUNwcrysu SUNwcrypu SUNwcrypr  
SUNwdcamn SUNwcrypm
```

Remarque – Après l'installation ou la désinstallation du test SunVTS (SUNwdcav) pour la carte Crypto Accelerator 1000 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.

Activation de la carte pour les serveurs Web iPlanet

Ce chapitre indique comment activer la carte Crypto Accelerator 1000 de Sun pour l'utiliser avec les serveurs Web iPlanet. Il est composé des sections suivantes :

- « Mots de passe », page 15
- « Création et remplissage d'un domaine », page 16
- « Aperçu de l'activation des serveurs Web iPlanet », page 18

Mots de passe

Vous devez saisir plusieurs mots de passe au cours de l'activation d'un serveur Web iPlanet (iWS). Le TABLEAU 3-1 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 3-1.

TABLEAU 3-1 Mots de passe requis pour les serveurs Web iPlanet

Type de mot de passe	Description
Serveur d'administration iWS	Requis pour démarrer le serveur d'administration iPlanet. Ce mot de passe a été affecté lors de la configuration de iPlanet.
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 affecté lors de la création d'une base de données certifiée à partir du serveur d'administration du serveur Web iPlanet. Il est également requis lorsque vous effectuez une demande de certificats et que vous les installez dans le module cryptographique interne.
Administrateur système	Requis lors de l'exécution d'opérations privilégiées <code>secadm</code> . Il s'agit du mot de passe hôte UNIX pour le superutilisateur (ou tout autre compte UID 0 sur l'hôte Solaris).
<i>utilisateur@nom-domaine</i>	Requis pour démarrer le module Crypto Accelerator 1000 de Sun lors de l'exécution en mode sécurisé. Ce mot de passe a été affecté lors de la création d'un utilisateur pour un domaine à l'aide de <code>secadm</code> . Il est également requis lorsque vous effectuez une demande de certificats et que vous les installez dans le module cryptographique <i>utilisateur@nom-domaine</i> .

Création et remplissage d'un domaine

Avant de pouvoir activer la carte pour une utilisation avec les serveurs Web iPlanet, vous devez tout d'abord configurer et remplir les domaines. Si ce n'est déjà fait, vous devez configurer au minimum un domaine et un utilisateur. Voir l'annexe A pour plus d'informations sur les domaines.

▼ Pour créer et remplir un domaine

1. Placez le répertoire des outils Crypto Accelerator 1000 de Sun dans votre chemin de recherche, si vous ne l'avez déjà fait. Par exemple :

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

2. Accédez à l'utilitaire secadm :

```
$ secadm
```

3. A l'aide de l'utilitaire secadm, créez un nouveau domaine :

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

4. Remplissez les domaines avec les utilisateurs.

Ces noms d'utilisateur sont uniquement connus avec la carte Crypto Accelerator 1000 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 la création de l'utilisateur, rappelez-vous que vous devez tout d'abord configurer le domaine actuellement en cours d'utilisation et vous connecter en tant qu'administrateur système.

Avant de créer les utilisateurs, vous devez configurer le domaine qui les accueillera.

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

5. S'il vous faut un seul utilisateur de domaine, vous pouvez éviter de configurer un fichier de jetons en utilisant le nom d'utilisateur « nobody ». Voir la section « Fichiers de jetons », page 55 pour plus d'informations.

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

Vous devez utiliser ce mot de passe lors de l'authentification effectuée au cours du démarrage d'un serveur Web. Il s'agit du mot de passe *utilisateur@nom-domaine*.



Attention – Vous devez vous souvenir du mot de passe que vous saisissez. Sans ce mot de passe, vous ne pourrez pas accéder à vos clés. Il est impossible de récupérer un mot de passe oublié.

6. Quittez secadm.

```
secadm{root@nom-domaine}# exit
```

Aperçu de l'activation des serveurs Web iPlanet

Pour activer les serveurs Web iPlanet vous devez suivre les étapes suivantes, qui sont expliquées en détail dans les deux chapitres suivants.

1. Installez le serveur Web iPlanet.
2. Créez une base de données certifiée.
3. Demandez un certificat.
4. Installez le certificat.
5. Configurez le serveur Web iPlanet.



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

- Si vous utilisez le serveur Web iPlanet 4.1, reportez-vous au chapitre 4.
- Si vous utilisez le serveur Web iPlanet 6.0, reportez-vous au chapitre 5.

Installation et configuration d'un serveur Web iPlanet 4.1

Ce chapitre décrit l'installation et la configuration d'un serveur Web iPlanet 4.1. Il est composé des sections suivantes :

- « Installation d'un serveur Web iPlanet 4.1 », page 19
- « Configuration d'un serveur Web iPlanet 4.1 », page 26

Installation d'un serveur Web iPlanet 4.1

Vous devez respecter l'ordre des étapes. Pour de plus amples informations sur l'utilisation d'un serveur Web iPlanet, veuillez consulter la documentation qui s'y rapporte.

▼ Pour installer un serveur Web iPlanet 4.1

1. Téléchargez le logiciel du serveur Web iPlanet 4.1.

Ce logiciel est disponible à l'adresse URL suivante :

<http://www.iplanet.com>

2. Installez le serveur Web.

Vous trouverez ici un exemple d'instructions, mais vous pouvez choisir de configurer votre serveur Web différemment. Par défaut, le nom de chemin du serveur est : `/usr/netscape/server4`

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

3. Lancez le programme de configuration 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. Saisissez deux fois le mot de passe du serveur d'administration iWS.

d. A l'invite, appuyez sur Entrée.

▼ Pour créer une base de données certifiée

1. Démarrez le serveur d'administration.

Pour démarrer un serveur Web iPlanet 4.1, utilisez la commande suivante (au lieu d'exécuter startconsole comme l'exige le programme setup) :

```
# /usr/netscape/server4/https-admserv/start
iPlanet-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 le serveur d'administration iPlanet en ouvrant un navigateur Web et en saisissant :

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

Dans la fenêtre indépendante, saisissez le nom d'utilisateur et le mot de passe du serveur d'administration iWS que vous avez sélectionnés au cours du programme setup.

Remarque – Si vous avez configuré le serveur Web iPlanet avec les paramètres par défaut, saisissez le mot `admin` pour l'identificateur d'utilisateur ou le nom d'utilisateur du serveur d'administration iWS.

3. Cliquez sur OK.

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

Il est recommandé d'activer la sécurité sur plus d'une instance du serveur Web. Pour cela, répétez les étapes 1 à 4 pour chaque instance du serveur Web.

Remarque – Si vous voulez également exécuter SSL sur le serveur d'administration, la configuration d'une base de données certifiée est identique. Reportez-vous à la documentation iPlanet pour plus d'informations.

- a. Cliquez sur l'onglet « Servers » (Serveurs) du serveur d'administration.
- b. Sélectionnez un serveur et cliquez sur le bouton « Manage » (Gestion).
- c. Cliquez sur l'onglet « Security » (Sécurité) sur 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) dans les deux boîtes de dialogue et cliquez sur OK.

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

5. Exécutez le script suivant pour activer la carte Crypto Accelerator 1000 de Sun :

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

Ce script vous invite à choisir le serveur Web. Il installe les modules cryptographiques Crypto Accelerator 1000 de Sun pour le serveur Web iPlanet ou Apache. Puis, il met à jour les fichiers de configuration pour activer la carte Crypto Accelerator 1000 de Sun.

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

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

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

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

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

<Press ENTER to continue>
```

9. Saisissez **0** pour quitter.

▼ Pour créer un certificat de serveur

1. Redémarrez le serveur d'administration en saisissant les commandes suivantes :

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

2. Pour effectuer une demande de certificat de serveur, cliquez sur l'onglet « Security » sur la partie supérieure de la page.

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

3. Sélectionnez le lien « Request a Certificate » (Demander un certificat) sur la partie gauche.

The screenshot shows the Netscape Web Server Administration interface. The top navigation bar includes tabs for Preferences, Programs, Servlets, Security, Status, Styles, Content Mgmt, Web Publishing, and Search. The 'Security' tab is selected. On the left sidebar, there are links for 'Create Database', 'Request a Certificate', 'Install Certificate', 'Change Password', 'Manage Certificates', and 'Migrate Certificate'. The 'Request a Certificate' link is highlighted. The main content area is titled 'Request a Server Certificate' and contains the following fields and options:

- ☒ New certificate.
- ☐ Certificate renewal.
- A link: [You can also see a list of available certificate authorities.](#)
- Submit to Certificate Authority via:
 - ☒ CA Email Address: [text input]
 - ☐ CA URL: [text input]
- Select the module to use with this certificate.
 - Cryptographic Module: [dropdown menu showing 'nobody@engineering']
 - Key Pair File Password: [text input]
- A warning box: 'Before requesting a certificate, you should read the [overview](#) of the certificate process, and then go through the [detailed steps](#) on creating a correct distinguished name which you should enter below. You will also generate the proper authorization letter that you will use to obtain your certificate from a certification authority.'
- Requestor name: [text input]
- Telephone number: [text input]
- Common name: [text input]
- Email address: [text input]

4. 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 domaine dispose de sa propre entrée dans ce menu déroulant. Assurez-vous de sélectionner le domaine correct. Pour utiliser la carte Crypto Accelerator 1000 de Sun, vous devez sélectionner un module sous la forme de *utilisateur@nom-domaine*.

c. Dans la boîte de dialogue « Key Pair File Password » (Mot de passe de fichier de paire de clés), saisissez le mot de passe pour le module *utilisateur@nom-domaine* qui sera en possession de la clé.

d. Indiquez les informations appropriées pour les champs suivants :

- « Requestor Name » (Nom du demandeur) : coordonnées du demandeur.
- « Telephone Number » (Numéro de téléphone) : 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 sur le certificat, le cas échéant.
- « State » (Département) : (facultatif) nom complet du département.
- « Country » (Pays) : code ISO de deux lettres désignant le pays (par exemple, US pour les Etats-Unis).

e. Cliquez sur le bouton OK pour envoyer les informations.

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

- Si vous choisissez d'envoyer votre demande de certificat à une URL d'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.

6. Une fois le certificat créé, copiez-le avec les en-têtes sur le presse-papier.

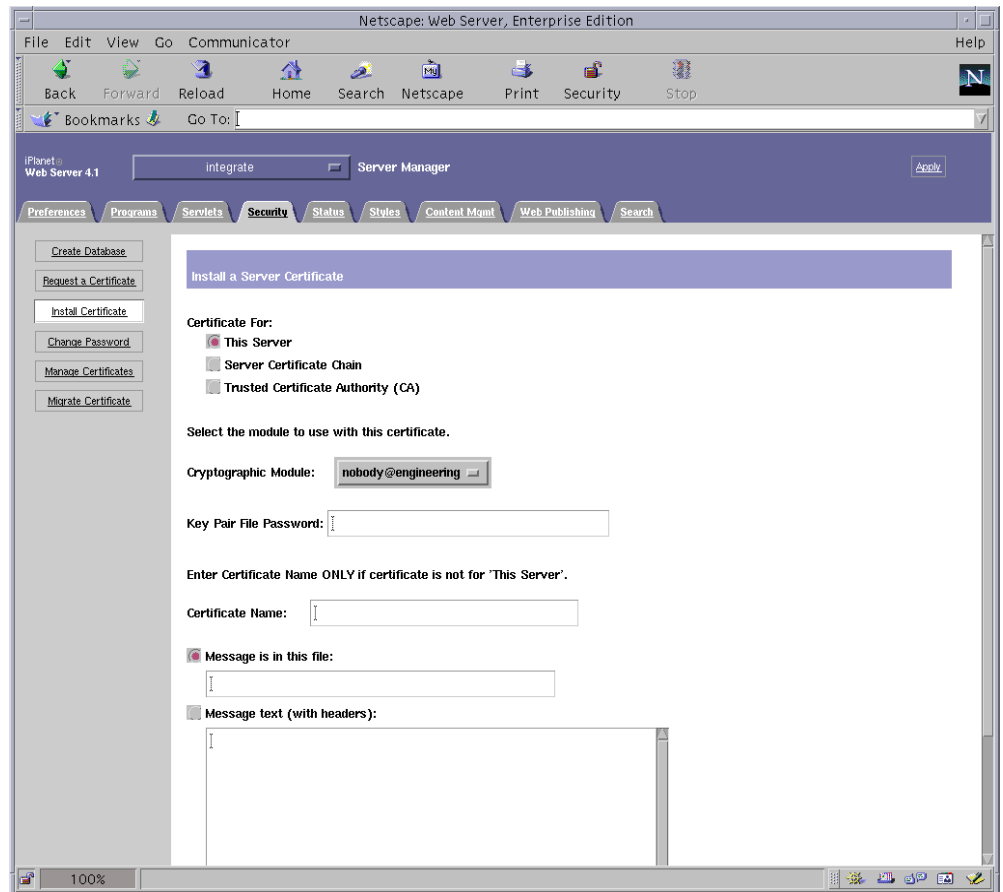
Notez que le certificat est différent de la demande de certificat et qu'il vous est généralement présenté sous forme de texte.

▼ Pour installer le certificat de serveur

1. Sélectionnez le lien « Install Certificate » (Installer le certificat) sur la partie gauche de la page.

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

2. Sélectionnez l'onglet « Security ».
3. Sur la partie gauche, sélectionnez le lien « Install Certificate ».



4. Remplissez le formulaire pour installer votre certificat :

- « Certificate For » (Certificat pour) : ce serveur.
- « Cryptographic Module » (Module cryptographique) : sélectionnez le nom *utilisateur@nom-domaine* approprié.

- « Key Pair File Password » : saisissez le mot de passe pour le module *utilisateur@nom-domaine* qui possède la clé créée précédemment.
 - « 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 la prise en charge SSL.
5. Dans le champ « Message text (with headers) » [Texte du message (avec en-têtes)] collez le certificat copié précédemment.
 6. Cliquez sur le bouton OK sur la partie inférieure de la page.
 7. Copiez le certificat copié à partir de l'autorité de certification dans la boîte de message.
Des informations de base sur le certificat s'affichent alors.
 8. Si tout vous semble correct, cliquez sur le bouton « Add Server Certificate » (Ajouter le certificat de serveur).
Des messages à l'écran vous indiquent de redémarrer le serveur. Cela n'est pas nécessaire car l'instance du serveur Web a été arrêtée pendant toute la durée des opérations. Vous êtes également notifié 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 iPlanet 4.1

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 iPlanet 4.1

1. A partir de la page principale d'administration, choisissez l'instance du serveur Web avec laquelle vous désirez travailler et cliquez sur le bouton « Manage » (Gestion).
2. Si l'onglet « Preferences » (Préférences) n'est pas sélectionné sur la partie supérieure de la page, cliquez dessus.
3. Cliquez sur le lien « Encryption On/Off » (Chiffrement activé/désactivé) sur 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. Cliquez sur le bouton OK.

6. Appliquez ces modifications en cliquant sur 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` en ajoutant la ligne suivante.

`CERTDefaultNickname utilisateur@nom-domaine:Server-Cert`

où *nomhôte* est le nom du serveur Web.

Par défaut, le certificat créé à l'étape 2 et l'étape 4 est nommé `Server-Cert`. Si votre certificat a un nom différent, remplacez-le par `Server-Cert`.

8. Sélectionnez le serveur que vous voulez gérer et cliquez sur le bouton « Apply » (Appliquer) dans le coin supérieur droit de la page.

Cette action applique les modifications dans le serveur d'administration.

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

Si vous cliquez sur le bouton « Apply Changes » (Appliquer les modifications) alors que le serveur est arrêté, une fenêtre indépendante vous invite à saisir un mot de passe. 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.

- Cliquez plutôt sur le bouton « Load Configuration Files ».
- Démarrez d'abord le serveur Web, puis cliquez sur le bouton « Apply Changes ».

10. Sur la page du serveur Web, cliquez sur le lien « On/Off » (Activé/Désactivé) sur la partie gauche de la page.

11. Saisissez les mots de passe des serveurs et cliquez sur 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 du module *utilisateur@nom-domaine*, saisissez le mot de passe que vous avez défini lorsque vous avez créé l'*utilisateur* dans *nom-domaine* à l'aide de *secadm*.

- 12. Vérifiez que SSL est activé sur le nouveau serveur Web à l'adresse URL suivante :**
`https://nomhôte.domaine:port_serveur/`
Notez que le *port_serveur* par défaut est 443.

Installation et configuration d'un serveur Web iPlanet 6.0

Ce chapitre décrit l'activation de la carte Crypto Accelerator 1000 de Sun pour l'utilisation avec le serveur Web iPlanet 6.0. Il est composé des sections suivantes :

- « Installation du serveur Web iPlanet 6.0 », page 29
- « Configuration du serveur Web iPlanet 6.0 », page 36

Installation du serveur Web iPlanet 6.0

Vous devez respecter l'ordre des étapes. Pour de plus amples informations sur l'utilisation d'un serveur Web iPlanet, veuillez consulter la documentation qui s'y rapporte.

▼ Pour installer le serveur Web iPlanet 6.0

1. Téléchargez le logiciel du serveur Web iPlanet 6.0.

Ce logiciel est disponible à l'adresse URL suivante :

<http://www.iplanet.com>

2. Installez le serveur Web.

Vous trouverez ici un exemple d'instructions, mais vous pouvez choisir de configurer votre serveur Web différemment. Par défaut, le nom de chemin du serveur est : `/usr/ipplanet/servers`

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

3. Lancez le programme de configuration 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. Saisissez deux fois le mot de passe du serveur d'administration iWS.

d. A l'invite, appuyez sur Entrée.

▼ Pour créer une base de données certifiée

1. Démarrez le serveur d'administration.

Pour démarrer un serveur Web iPlanet, utilisez la commande suivante (au lieu d'exécuter startconsole comme l'exige le programme setup) :

```
# /usr/iplanet/servers/https-admserv/start
iPlanet-WebServer-Enterprise/6.0SP1 B08/20/2001 00:58
warning: daemon is running as super-user
[LS ls1] http://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 le serveur d'administration iPlanet en ouvrant un navigateur Web et en saisissant :

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

Dans la fenêtre indépendante, saisissez le nom d'utilisateur et le mot de passe du serveur d'administration iWS que vous avez sélectionnés au cours du programme setup.

Remarque – Si vous avez configuré le serveur Web iPlanet avec les paramètres par défaut, saisissez le mot `admin` pour l'identificateur d'utilisateur ou le nom d'utilisateur du serveur d'administration iWS.

3. Cliquez sur OK.

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

Il est recommandé d'activer la sécurité sur plus d'une instance du serveur Web. Pour cela, répétez cette opération pour chaque instance du serveur Web.

Remarque – Si vous voulez également exécuter SSL sur le serveur d'administration, la configuration d'une base de données certifiée est identique. Reportez-vous à la documentation iPlanet pour plus d'informations.

- a. Cliquez sur l'onglet « Servers » (Serveurs) du serveur d'administration.
- b. Sélectionnez un serveur et cliquez sur le bouton « Manage » (Gestion).
- c. Cliquez sur l'onglet « Security » (Sécurité) sur 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) dans les deux boîtes de dialogue et cliquez sur 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 iPlanet est exécuté en mode sécurisé.

5. Exécutez le script suivant pour activer la carte Crypto Accelerator 1000 de Sun :

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

Ce script vous invite à choisir le serveur Web. Il installe les modules cryptographiques Crypto Accelerator 1000 de Sun pour le serveur Web iPlanet ou Apache. Puis, il met à jour les fichiers de configuration pour activer la carte Crypto Accelerator 1000 de Sun.

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

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

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

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

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

<Press ENTER to continue>
```

9. Saisissez 0 pour quitter.

▼ Pour créer un certificat de serveur

1. Redémarrez le serveur d'administration en saisissant les commandes suivantes :

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

2. Pour effectuer une demande de certificat de serveur, cliquez sur l'onglet « Security » sur la partie supérieure de la page.

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

3. Sélectionnez le lien « Request a Certificate » (Demander un certificat) sur la partie gauche.

The screenshot shows the Netscape Web Server, Enterprise Edition interface. The browser window title is "Netscape: Web Server, Enterprise Edition". The address bar shows "Go To:". The main content area displays the "Request a Server Certificate" page. On the left sidebar, there are links: "Create Database", "Request a Certificate", "Install Certificate", "Change Password", "Manage Certificates", "Request VeriSign Certificate", "Install VeriSign Certificate", "Install CRL/CKL's", "Manage CRL/CKL's", and "Migrate Certificate". The "Request a Certificate" page has a title bar "Request a Server Certificate". It contains two radio buttons: "New certificate." (selected) and "Certificate renewal.". Below this is a link: "You can also see a [list of available certificate authorities.](#)". Under the heading "Submit to Certificate Authority via:", there are two radio buttons: "CA Email Address:" (selected) and "CA URL:". The "CA Email Address:" field has a text input box containing "nobody@engineering". The "CA URL:" field has a text input box. Below this is the text "Select the module to use with this certificate." followed by "Cryptographic Module:" and a text input box containing "nobody@engineering". The "Key Pair File Password:" field has a text input box. At the bottom, there is a text box with the following text: "Before requesting a certificate, you should read the [overview](#) of the certificate process, and then go through the [detailed steps](#) on creating a correct distinguished name which you should enter below. You will also generate the proper authorization letter that you will use to obtain your".

4. 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 domaine dispose de sa propre entrée dans ce menu déroulant. Assurez-vous de sélectionner le domaine correct. Pour utiliser la carte Crypto Accelerator 1000 de Sun, vous devez sélectionner un module sous la forme de *utilisateur@nom-domaine*.

c. Dans la boîte de dialogue « Key Pair File Password » (Mot de passe de fichier de paire de clés), saisissez le mot de passe pour le module *utilisateur@nom-domaine* qui sera en possession de la clé.

d. Indiquez les informations appropriées pour les champs suivants :

- « Requestor Name » (Nom du demandeur) : coordonnées du demandeur.
- « Telephone Number » (Numéro de téléphone) : 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 sur le certificat, le cas échéant.
- « State » (Département) : (facultatif) nom complet du département.
- « Country » (Pays) : code ISO de deux lettres désignant le pays (par exemple, US pour les Etats-Unis).

e. Cliquez sur le bouton OK pour envoyer les informations.

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

- Si vous choisissez d'envoyer votre demande de certificat à une URL d'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.

6. Une fois le certificat créé, copiez-le avec les en-têtes sur le presse-papier.

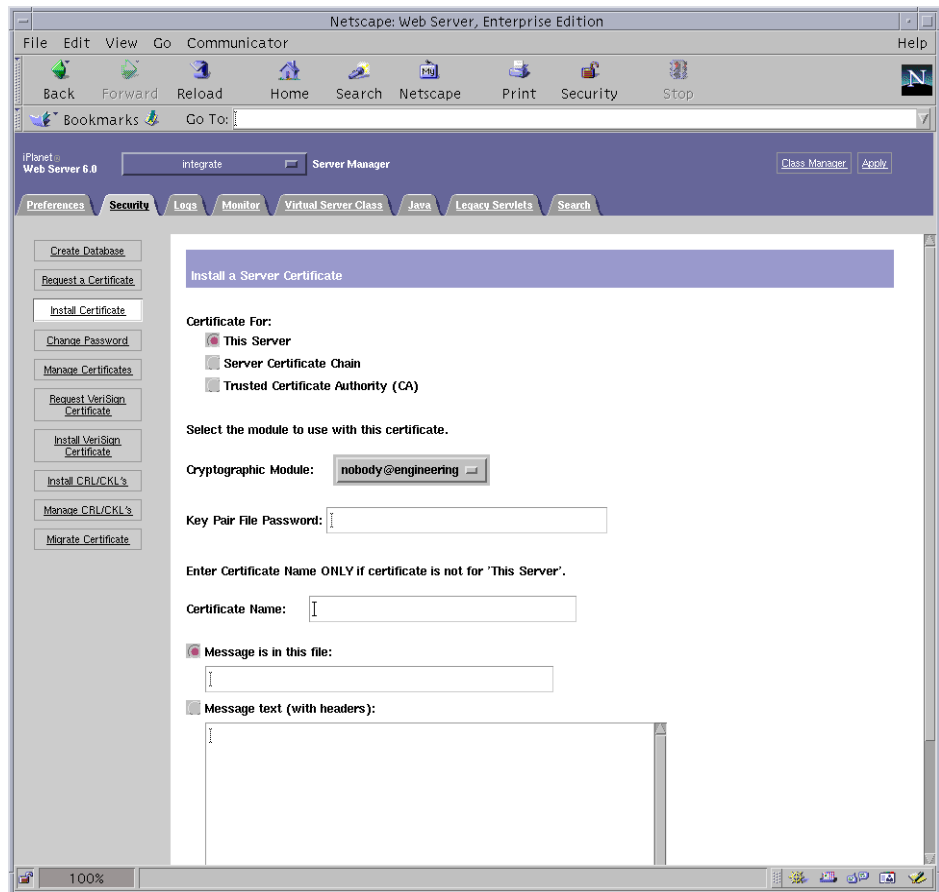
Notez que le certificat est différent de la demande de certificat et qu'il vous est généralement présenté sous forme de texte.

▼ Pour installer le certificat de serveur

1. Sélectionnez le lien « Install Certificate » (Installer le certificat) sur la partie gauche de la page.

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

2. Sélectionnez l'onglet « Security ».
3. Sur la partie gauche, sélectionnez le lien « Install Certificate ».



4. Remplissez le formulaire pour installer votre certificat :

- « Certificate For » (Certificat pour) : ce serveur.
- « Cryptographic Module » (Module cryptographique) : sélectionnez le nom *utilisateur@nom-domaine* approprié.

- « Key Pair File Password » : saisissez le mot de passe pour le module *utilisateur@nom-domaine* qui possède la clé créée précédemment.
 - « Certificate Name » (Nom du certificat) : dans la plupart des cas, vous pouvez laisser ce champ vierge. Si vous choisissez de saisir 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 la prise en charge SSL.
5. Dans le champ « Message text (with headers) » [Texte du message (avec en-têtes)], collez le certificat copié précédemment.
 6. Cliquez sur le bouton OK sur la partie inférieure de la page.
 7. Copiez le certificat copié à partir de l'autorité de certification dans la boîte de message.
Des informations de base sur le certificat s'affichent alors.
 8. Si tout vous semble correct, cliquez sur le bouton « Add Server Certificate » (Ajouter le certificat de serveur).
Des messages à l'écran vous indiquent de redémarrer le serveur. Cela n'est pas nécessaire car l'instance du serveur Web a été arrêtée pendant toute la durée des opérations. Vous êtes également notifié que le serveur Web doit être configuré de manière à pouvoir utiliser SSL. Suivez la procédure suivante pour configurer le serveur Web.

Configuration du serveur Web iPlanet 6.0

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 iPlanet 6.0

1. Cliquez sur l'onglet « Preferences » (Préférences) sur la partie supérieure de la page.
2. Cliquez sur le lien « Edit Listen Sockets » (Modifier les prises de réception) dans le cadre situé sur la partie gauche.
Le cadre 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 » : défini sur On (activé).

b. Cliquez sur le bouton OK pour appliquer ces changements.

Dans le champ « Security » de la page « Edit Listen Sockets », le lien « Attributes » (Attributs) devrait maintenant apparaître.

3. Cliquez sur le lien « Attributes ».

4. Entrez le mot de passe *utilisateur@nom-domaine* pour authentifier votre identité auprès du module *utilisateur@nom-domaine* du système.

5. Sélectionnez les paramètres SSL à partir de la fenêtre indépendante.

Vous pouvez choisir les paramètres de chiffrement par défaut, SSL2 ou SSL3/TLS. L'option par défaut n'affiche pas les paramètres par défaut. Les deux autres options nécessitent la sélection des algorithmes que vous voulez activer.

6. Sélectionnez le certificat pour le module *utilisateur@nom-domaine* suivi de : Server-Cert (ou le nom que vous avez choisi s'il est différent).

Seules les clés appartenant au module *utilisateur@nom-domaine* approprié sont affichées dans le champ « Certificate Name » (Nom du certificat).

7. Une fois le certificat choisi et tous les paramètres de sécurité confirmés, cliquez sur le bouton OK.

8. Cliquez sur le lien « Apply » (Appliquer) dans le coin supérieur droit pour appliquer ces changements avant de démarrer le serveur.

9. Cliquez sur le lien « Load Configuration Files » pour appliquer ces modifications.

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

Si vous cliquez sur le bouton « Apply Changes » (Appliquer les modifications) alors que le serveur est arrêté, une fenêtre indépendante vous invite à saisir un mot de passe. 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 :

- Cliquez plutôt sur le bouton « Load Configuration Files ».
- Démarrez d'abord le serveur Web, puis cliquez sur le bouton « Apply Changes ».

10. Entrez les mots de passe requis dans les boîtes de dialogue pour démarrer le serveur.

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.

- 11. A l'invite du module *utilisateur@nom-domaine*, saisissez le mot de passe que vous avez défini lorsque vous avez créé l'utilisateur dans *nom-domaine* à l'aide de *secadm*.**
- 12. Vérifiez que SSL est activé sur le nouveau serveur Web à l'adresse URL suivante :**
`https://nomhôte.domaine:port_serveur/`
Notez que le *port_serveur* par défaut est 443.

Activation du serveur Web Apache

Ce chapitre décrit l'activation de la carte Crypto Accelerator 1000 de Sun pour une utilisation avec un serveur Web Apache. Il est composé des sections suivantes :

- « Activation du serveur Web Apache », page 39
 - « Création d'un certificat », page 42
-

Activation du serveur Web Apache

Le serveur Web Apache 1.3.12 est fourni avec l'environnement d'exploitation Solaris 8 7/01. Le serveur Web Apache 1.3.22 est fourni avec l'environnement d'exploitation Solaris 9. Les instructions suivantes sont spécifiquement applicables à ces versions 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 `http.conf`.

3. Démarrez sslconfig.

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

4. Sélectionnez 2 pour configurer votre serveur Web Apache pour l'utilisation de SSL :

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

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

Your selection (0 to quit): 2
```

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 en créer une, vous devrez le faire ultérieurement et utiliser `sslconfig` 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 42.

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:
```

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 1024 bits est suffisamment solide ; vous pouvez toutefois opter pour des clés plus solides si vous le désirez.

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

11. Créez votre phrase-clé PEM.

Cette phrase-clé protège la clé matérielle. Assurez-vous de choisir une phrase-clé solide dont vous pourrez vous souvenir. Si vous oubliez le mot de passe, 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 1000 de Sun.

▼ Pour créer un certificat

1. Créez une demande de certificat en utilisant les clés que vous venez de créer.

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 « . » et appuyez sur Entrée).
- « Locality » (Localité) : (facultatif) ville, département, principauté ou pays, également déclaré 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 1000 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/crypto/bin/sslpasword
```

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 39, 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 iPlanet and Apache keys" from the **sslconfig** main menu.

4. Sélectionnez 0 pour quitter, une fois les opérations terminées avec l'utilitaire `sslconfig`.
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 39) 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.

Il est entendu 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.

Diagnostics et dépannage

Ce chapitre décrit les tests de diagnostics et le dépannage pour le logiciel Crypto Accelerator 1000 de Sun. Il est composé des sections suivantes :

- « Logiciel de diagnostics SunVTS », page 47
- « Dépannage du périphérique Crypto Accelerator 1000 de Sun », page 51

Logiciel de diagnostics SunVTS

Le test SunVTS `dcatest`, fourni dans le progiciel `SUNWdcav`, sur le CD-ROM Crypto Accelerator 1000 de Sun, fonctionne avec l'interface d'utilisation et de contrôle de tests SunVTS fournie dans les progiciels `SUNWvts` et `SUNWvtsx`, sur le CD-ROM Supplement de Solaris. Ce test effectue des diagnostics pour la carte Crypto Accelerator 1000 de Sun.

Reportez-vous à la documentation SunVTS pour obtenir des instructions de démarrage et de contrôle de ces tests de diagnostics. Ces documents sont disponibles dans le manuel « Solaris on Sun Hardware AnswerBook », fourni avec le CD-ROM Supplement de Solaris pour la version Solaris de votre système.

Remarque – SunVTS ne peut être utilisé que si vous avez installé les progiciels SunVTS à partir du CD-ROM Supplement de Solaris.

▼ Pour lancer dctest

1. Lancez SunVTS en tant que superutilisateur.

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

Reportez-vous au manuel *SunVTS User's Guide* 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 pour afficher tous les tests du groupe « Cryptography ».
5. Désélectionnez les cases du groupe « Cryptography » qui ne sont pas nommées dctest.

- Si un dctest est affiché, rendez-vous à l'étape 6.
- Si un dctest n'est pas affiché, cherchez-le en sondant le système et en sélectionnant « Reprobe system » (Re-tester le système) dans le menu déroulant « Commands » (Commandes).

Reportez-vous à la documentation SunVTS pour connaître la procédure exacte. Une fois la recherche terminée et un dctest affiché, poursuivez à l'étape 6.

6. Sélectionnez l'une des instances de dctest, puis cliquez dessus avec le bouton droit de la souris et déplacez-la pour afficher les options de paramètres de test. Ces options, qui se rapportent uniquement à dctest, sont décrites dans la section « Options de paramètres de test pour dctest », page 49.
7. Après avoir effectué toutes les sélections, cliquez sur « Apply » (Appliquer), dans le menu déroulant « Within Instance » (Dans l'instance), pour modifier l'instance sélectionnée de dctest, ou cliquez sur « Apply », dans le menu déroulant « Across All Instances » (Dans toutes les instances), pour modifier toutes les instances sélectionnées de dctest.

Cette action supprime la fenêtre indépendante et vous renvoie à la fenêtre principale de diagnostics Sun.

8. Sélectionnez l'une des instances de `dcatest`, puis cliquez dessus avec le bouton droit de la souris et déplacez-la pour afficher les options d'exécution de tests.
Une autre méthode d'affichage des options d'exécution de tests consiste à cliquer sur le menu principal déroulant « Options » puis sur « Test Executions » (Exécution de tests). Ces options sont des commandes générales de SunVTS qui concernent tous les tests. Reportez-vous à la documentation SunVTS pour obtenir des informations détaillées.
9. Une fois toutes les sélections effectuées, cliquez sur « Apply » (Appliquer) pour supprimer la fenêtre indépendante et retourner à la fenêtre principale de diagnostics Sun.
10. Cliquez sur le bouton « Start » (Lancer) pour exécuter les tests sélectionnés.
11. Cliquez sur « Stop » pour arrêter tous les tests.

Options de paramètres de test pour `dcatest`

Le TABLEAU 7-1 décrit les sous-tests `dcatest`.

TABLEAU 7-1 Sous-tests `dcatest`

Test	Description
3DES	Teste le chiffrement de masse 3DES.
RSA	Teste les clés publiques et privées RSA.
DSA	Teste la vérification de la signature DSA.
RNG	Teste la génération de nombres aléatoires.

Syntaxe de la ligne de commande `dcatest`

Si vous choisissez de lancer `dcatest` à partir de la ligne de commande au lieu de l'environnement CDE, vous devez alors spécifier tous les arguments dans la chaîne de la ligne de commande.

En mode 32 bits, le chemin vers `dcatest` est `/opt/SUNWvts/bin/`. En mode 64 bits, le chemin vers `dcatest` est `/opt/SUNWvts/bin/sparcv9/`.

Toutes les options SunVTS standard sont prises en charge à partir de l'interface de ligne de commande de `dcatest`. Les options se rapportant aux tests sont signalées par l'argument `-o`.

Reportez-vous au manuel *SunVTS Test Reference Manual* pour obtenir une définition des arguments de ligne de commande standard. Comme `dcatest` 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 démontre l'invocation de `dcatest` en mode 32 bits en tant que programme autonome. La commande suivante effectue tous les sous-tests sur `dca0` :

```
# /opt/SUNWvts/bin/dcatest -f -o dev=dca0,t1=3DES+RSA+DSA+RNG
```

L'exemple suivant démontre l'invocation de `dcatest` en mode 64 bits à partir de l'infrastructure SunVTS. La commande suivante teste RCA sur `dca2` :

```
# /opt/SUNWvts/bin/sparcv9/dcatest -f -o dev=dca2,t1=RSA
```

Lors de l'exécution de `dcatest` 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 7-2.

TABLEAU 7-2 Syntaxe de la ligne de commande `dcatest`

Option	Description
<code>dev=dcan</code>	Spécifie l'instance du périphérique à tester, telle que <code>dca0</code> ou <code>dca2</code> . Indique la valeur <code>dca0</code> par défaut si aucune valeur n'est incluse.
<code>t1=listetests</code>	Indique la liste de sous-tests à exécuter. Les sous-tests pour <code>t1</code> sont séparés par les caractères <code>+</code> (plus). Les seuls sous-tests pris en charge sont 3DES, RSA, DSA et RNG ; par conséquent, <code>t1=3DES+RSA+DSA+RNG</code> active tous les sous-tests. Vous pouvez également insérer <code>t1=all</code> pour exécuter tous les tests. Indique la valeur <code>all</code> par défaut si aucun sous-test n'est spécifié.

Dépannage du périphérique Crypto Accelerator 1000 de Sun

Pour déterminer si le périphérique Crypto Accelerator 1000 de Sun est répertorié dans le système, à partir de l'invite OpenBoot PROM (OBP) saisissez `show-devs` pour afficher la liste des périphériques. Des lignes semblables aux exemples ci-dessous, spécifiques à la carte Crypto Accelerator 1000 de Sun, s'affichent alors :

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

Dans l'exemple ci-dessus, `pci108e,5455` identifie le chemin de périphérique de la carte Crypto Accelerator 1000 de Sun. Il n'y a aucun microprogramme sur cette carte. C'est pourquoi les diagnostics de niveau OBP ne sont pas disponibles.

La carte Crypto Accelerator 1000 de Sun ne comporte aucun voyant ou 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 -m dca -i 0 -n dca0

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

L'affichage des informations `kstat` indique si les requêtes cryptographiques, ou « jobs », sont envoyées à la carte Crypto Accelerator 1000 de Sun. Une modification de la valeur « jobs » au cours du temps indique que la carte Crypto Accelerator 1000 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/dca.conf`, la capture et l'affichage des statistiques seront activés. Cette propriété peut contribuer à empêcher l'analyse du trafic.

Administration de la carte Crypto Accelerator 1000 de Sun avec un serveur Web iPlanet

Cette annexe présente les fonctions de sécurité de la carte Crypto Accelerator 1000 de Sun administrée avec un serveur Web iPlanet.

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

Cette annexe comprend les sections suivantes :

- « Concepts et terminologie », page 53
- « Configuration et gestion des domaines », page 62
- « Configuration et gestion des comptes utilisateur », page 67

Concepts et terminologie

Des domaines et des utilisateurs doivent être créés pour les applications communiquant avec la carte Crypto Accelerator 1000 de Sun par une interface PKCS#11, telles que le serveur Web iPlanet.

Les utilisateurs de la carte Crypto Accelerator 1000 de Sun sont les uniques propriétaires des clés matérielles cryptographiques. Chaque utilisateur peut détenir plusieurs clés. Un utilisateur peut décider de détenir plusieurs clés afin de prendre en charge différentes configurations ; par exemple, une clé de « production » et une clé de « développement » (marquant les différents organismes de l'utilisateur). Il peut également avoir besoin de plusieurs clés pour faciliter une configuration High Availability (HA). Notez que les termes « utilisateur » ou « compte utilisateur »

se rapportent aux utilisateurs de la carte Crypto Accelerator 1000 de Sun, non pas aux comptes utilisateur UNIX traditionnels. Il n'y a pas de mappage fixe entre les noms d'utilisateur UNIX et ceux de la carte Crypto Accelerator 1000 de Sun.

Les domaines représentent des divisions logiques d'utilisateurs et de leurs clés matérielles. Ils permettent de réunir plusieurs utilisateurs dans un même ensemble. Le maintien d'un espace de nom unique pour chaque domaine constitue l'un des avantages de la répartition des utilisateurs par domaine. Le contenu des domaines peut ainsi être géré séparément.

Une installation type comprend un domaine unique et un utilisateur unique. Par exemple, une telle configuration peut être composée d'un domaine unique `webserver` et d'un utilisateur dans ce domaine, `nobody`. Ce qui autorise l'utilisateur `nobody` à obtenir et maintenir le contrôle d'accès des clés du serveur au sein d'un domaine unique.

Il est possible de créer des domaines supplémentaires pour répartir les utilisateurs et les clés matérielles. Une configuration plus complexe consisterait en plusieurs domaines, par exemple, `finance`, `legal` et `engineering`. Chaque domaine conserve un nom d'espace unique. Par exemple, l'utilisateur `webserv` dans le domaine « `finance` » représente un compte utilisateur différent de `webserv` dans le domaine « `engineering` ».

Un outil d'administration, `secadm`, permet de gérer les domaines et les utilisateurs de la carte Crypto Accelerator 1000 de Sun.

Domaines, utilisateurs et serveur Web iPlanet

Lorsqu'un serveur Web iPlanet doit référencer une clé gérée par la carte Crypto Accelerator 1000 de Sun, il utilise un « nom de jeton » pour indiquer que la clé est gérée par le matériel et non par sa base de données logicielle interne.

La carte Crypto Accelerator 1000 de Sun crée ses noms de jeton en associant un compte utilisateur à un nom de domaine avec le symbole « @ ». Dans une installation type, un domaine unique, `webserver`, a été créé avec un utilisateur unique, `nobody`. Le nom de jeton que le serveur Web iPlanet utiliserait pour référencer les clés détenues par l'utilisateur `nobody` dans le domaine `webserver` serait `nobody@webserver`. Le mot de passe pour l'utilisateur « `nobody` » (défini lorsque l'utilisateur est créé à l'aide de `secadm`) doit être utilisé lors d'une demande de certificat, de l'installation de ce dernier ou d'une authentification pour démarrer le serveur Web iPlanet.

Jetons et fichiers de jetons

Le serveur Web iPlanet accède à la clé matérielle à l'aide des jetons. Les fichiers de jetons constituent, pour les administrateurs de la carte Crypto Accelerator 1000 de Sun, une technique de présentation, selon leurs choix, de jetons spécifiques à une application donnée.

Si aucun fichier de jetons n'existe, le logiciel Crypto Accelerator 1000 de Sun présente un ensemble de jetons par défaut au serveur Web iPlanet. Dans ce cas, un jeton est présenté par domaine, avec le nom *nobody@nom-domaine*.

Exemple

Soient trois domaines : *engineering*, *finance* et *legal*. Les jetons suivants sont présentés au serveur Web iPlanet :

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

Cependant, pour que ces noms puissent être utilisables, un utilisateur *nobody* doit exister dans chacun de ces domaines.

Fichiers de jetons

Pour ignorer la case par défaut, un fichier de jetons doit exister. Les fichiers de jetons sont des fichiers texte qui contiennent un ou plusieurs noms de jetons, un par ligne. Un serveur Web iPlanet présente uniquement les jetons répertoriés dans ce fichier. Les méthodes de spécification des fichiers de jetons sont les suivantes (par ordre de priorité) :

1. Fichier `$HOME/.SUNWconn_crypto_slots`

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

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

Le fichier `/etc/opt/SUNWconn/crypto/slots` est un fichier général par défaut, utilisé dans le cas où un fichier `.SUNWconn_crypto_slots` n'existe pas dans le répertoire d'accueil de l'utilisateur.

Voici un exemple du contenu d'un fichier de jetons :

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

Si aucun des fichiers ci-dessus n'est trouvé, alors la méthode par défaut décrite dans la section « Jetons et fichiers de jetons », page 55 est utilisée.

Voir le chapitre 3 pour plus d'informations sur les noms de jetons se rapportant à la configuration du serveur Web iPlanet.

Utilisation de secadm

Le programme `secadm` fournit une interface de ligne de commande à la carte Crypto Accelerator 1000 de Sun.

Pour accéder facilement au programme `secadm`, placez le répertoire d'outils Crypto Accelerator 1000 de Sun dans votre chemin de recherche. Par exemple :

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

La syntaxe de la commande `secadm` est :

`secadm [-h]`

`secadm [-y] [-f nomfichier]`

`secadm [-y] [-r nom-domaine] [-u nomutilisateur | -s nom-admin] commande`

La commande est placée dans le répertoire `/opt/SUNWconn/crypto/bin/`.

Le TABLEAU A-1 indique les options de l'outil `secadm`.

TABLEAU A-1 Options `secadm`

Option	Description
-h	Afficher l'aide relative à la commande <code>secadm</code> et quitter.
-f <i>nomfichier</i>	Lire une ou plusieurs commandes à partir de <i>nomfichier</i> et quitter.
-r <i>nom-domaine</i>	Utilisée uniquement en mode commande simple. L'option -r indique à <code>secadm</code> d'exécuter la commande communiquée dans le domaine <i>nom-domaine</i> .
-s <i>nom-admin</i>	Utilisé uniquement en mode commande simple. L'option -s indique à <code>secadm</code> de se connecter en tant que System Administrator (administrateur système) en utilisant <i>nom-admin</i> comme nom d'utilisateur.
-u <i>nomutilisateur</i>	Utilisée uniquement en mode commande simple. L'option -u indique à <code>secadm</code> de se connecter en tant que <i>nomutilisateur</i> . La connexion aura lieu avant que la commande communiquée soit exécutée.
-y	Impose la réponse « oui » à toutes les commandes qui invitent généralement à une confirmation.

Modes de fonctionnement

`secadm` peut fonctionner dans l'un des trois modes suivants, qui diffèrent principalement selon la manière dont les commandes sont communiquées à `secadm`. Les trois modes sont : mode commande simple, mode fichier, mode interactif. Chacun requiert un mot de passe différent.

Mode commande simple

En mode commande simple, l'utilisateur précise la commande à exécuter par `secadm` après avoir spécifié toutes les options de ligne de commandes. Par exemple, la commande suivante indiquerait tous les domaines existants et renverrait l'utilisateur à l'invite du shell de commande.

```
$ secadm show realm
```

La commande suivante effectue une connexion en tant que System Administrator et crée l'utilisateur webserv dans le domaine engineering.

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

Notez que le mot de passe saisi à l'invite **Password:** correspond au mot de passe du System Administrator tandis que le mot de passe saisi aux invites **Initial password:** et **Confirm password:** correspond au mot de passe de l'utilisateur récemment créé.

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, l'utilisateur spécifie un fichier à partir duquel **secadm** lit une ou plusieurs commande. Le fichier doit être du texte ASCII comportant une commande par ligne. Chaque commentaire doit être précédé du caractère « # ». Si l'option en mode fichier est définie, **secadm** ignore tous les arguments de la ligne de commandes après la dernière option. L'exemple suivant lance les commandes dans **deluser.scr** et répond à toutes les invites par l'affirmative.

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

Mode interactif

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.

Saisie de commandes avec secadm

Le programme `secadm` dispose d'un langage de commande qui doit être utilisé pour interagir avec la carte Crypto Accelerator 1000 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). Utiliser `sh` au lieu de `show` conviendrait parfaitement, mais utiliser `lo` est ambigu car cela peut signifier `login` ou `logout`.

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

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

Les mêmes informations peuvent être obtenues en utilisant des parties de mots comme commandes, telles que `sh us`.

Une commande ambiguë produit une demande d'explication :

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

Authentification à l'aide de secadm

De nombreuses commandes, particulièrement celles liées aux comptes utilisateur et aux clés, exigent une authentification de votre part en tant que System Administrator ou utilisateur. Les comptes System Administrator doivent effectuer une authentification auprès de la carte Crypto Accelerator 1000 de Sun pour la création de domaines, de comptes utilisateur, l'activation et la désactivation de comptes utilisateur et la suppression de domaines et de comptes utilisateur, entre autres opérations. L'authentification en tant qu'utilisateur est nécessaire afin de

modifier le mot de passe d'un utilisateur ou de répertorier les objets clés détenus par l'utilisateur. Le TABLEAU A-2 indique les commandes pouvant être utilisées par le System Administrator et celles pouvant être utilisées par l'utilisateur.

TABLEAU A-2 Tableau des commandes d'administration

Commande	Authentifier	Informations d'authentification maintenues	Utilisateur authentifié
<code>create user=nomutilisateur</code>	Non	Oui	Administrateur système
<code>create realm=nom-domaine</code>	Oui	Non	Administrateur système
<code>delete user=nomutilisateur</code>	Non	Oui	Administrateur système
<code>delete realm=nom-domaine</code>	Oui	Non	Administrateur système
<code>disable user=nomutilisateur</code>	Non	Oui	Administrateur système
<code>enable user=nomutilisateur</code>	Non	Oui	Administrateur système
<code>exit</code>	Non	Non	Tous
<code>login</code>	Oui	Non	Utilisateur
<code>logout</code>	Non	Non	Tous
<code>passwd</code>	Oui	Oui	Utilisateur
<code>set realm=nom-domaine</code>	Non	Non	Tous
<code>show class</code>	Non	Non	Tous
<code>show key</code>	Non	Oui	Utilisateur
<code>show realm</code>	Non	Non	Tous
<code>show user</code>	Non	Oui	Administrateur système
<code>su</code>	Oui	Non	Administrateur système
<code>quit</code>	Non	Non	Tous
<code>unset realm</code>	Non	Non	Tous

Pour vous identifier en tant que System Administrator, vous devez fournir, à l'invite, un nom d'utilisateur UNIX UID 0 (par exemple superutilisateur) ainsi que le mot de passe. Les utilisateurs ont besoin du mot de passe créé à leur intention lorsque l'utilisateur a été créé. Lorsque vous vous connectez en tant que System Administrator ou utilisateur, vous devez tout d'abord sélectionner un domaine.

Pour vous connecter en tant qu'utilisateur, saisissez :

```
secadm{nom-domaine}> login user=nomutilisateur
```

Pour vous connecter en tant que System Administrator, saisissez :

```
secadm{nom-domaine}> su
```

Lorsque vous vous connectez en tant qu'utilisateur ou System Administrator, l'invite `secadm` vous indique l'utilisateur actuellement connecté. Une connexion utilisateur se différencie d'une connexion System Administrator par le dernier caractère de l'invite. Les utilisateurs sont définis par un crochet pointu (>) tandis que les comptes System Administrator le sont par un dièse (#). Si vous êtes actuellement connecté en tant qu'utilisateur ou System Administrator et que vous essayez de vous connecter en tant qu'un autre utilisateur ou System Administrator, les informations d'authentification vous concernant seront perdues lors de l'établissement de la nouvelle connexion. Par exemple :

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

Obtention d'aide pour les commandes

`secadm` 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 :

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

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

En saisissant un « ? », vous obtiendrez la liste des mots des commandes valides, par exemple :

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

Si vous souhaitez obtenir de l'aide en mode ligne de commande, rappelez-vous que dans certains cas, le caractère « ? » est interprété par le shell dans lequel vous travaillez. Assurez-vous d'utiliser le caractère d'échappement du shell de commande avant le point d'interrogation.

Fermeture du programme secadm

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

Configuration et gestion des domaines

Un domaine est un référentiel pour clé matérielle. Les administrateurs et utilisateurs sont également associés au domaine. Les domaines 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 détenteurs. Les domaines sont composés de deux éléments :

- Objets clés : il s'agit de clés de longue durée stockées pour des applications telles que le serveur Web iPlanet.

- Comptes utilisateur : ces comptes permettent aux applications d'authentifier des clés spécifiques et d'y accéder.

Il peut arriver que plusieurs domaines soient présents et que chaque domaine possède ses propres comptes utilisateur, bien qu'un seul domaine soit nécessaire. Par exemple, si une application est authentifiée en tant qu'utilisateur `webserve` et qu'elle a besoin d'accéder à des clés dans un domaine, alors le compte utilisateur `webserve` doit exister dans ce domaine.

Création d'un domaine

La création d'un domaine entraîne la création des répertoires, des fichiers et d'autres ressources nécessaires au stockage des objets clés de longue durée. Pour créer un domaine, l'administrateur doit utiliser la commande `create realm` et saisir le nom du domaine à créer. Quelles que soient les informations d'authentification maintenues, le System Administrator doit être authentifié pour que cette commande s'exécute. A l'invite, saisissez le mot de passe UNIX de l'administrateur système. Par exemple :

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

Vous pouvez nommer les domaines selon vos besoins. Par exemple, vous choisirez peut-être de configurer des domaines pour différents départements, tels que « finance » et « engineering ». Dans ce cas, vous nommerez les domaines `finance` et `engineering`. Par exemple :

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

Configuration du domaine actuellement en fonctionnement

secadm peut uniquement gérer les clés et les comptes utilisateur d'un domaine à la fois. La majorité des commandes relatives aux domaines et aux comptes utilisateur exigent que vous sélectionniez d'abord un domaine. Pour sélectionner un domaine, exécutez la commande `set realm`, comme indiqué dans l'exemple suivant :

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

Une fois le domaine sélectionné, l'invite `secadm` indique son nom entre accolades.

Si vous ne souhaitez plus travailler dans le domaine en cours d'opération, vous pouvez soit configurer ce domaine sur une nouvelle valeur soit annuler la configuration. La modification ou l'annulation de la configuration du domaine en cours d'opération déconnecte automatiquement tout utilisateur ou System Administrator actuellement authentifié dans ce domaine. Par exemple :

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

Remplissage du domaine avec les utilisateurs

Ces noms d'utilisateur sont uniquement connus avec la carte Crypto Accelerator 1000 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 d'essayer de créer l'utilisateur, n'oubliez pas de sélectionner le domaine correct et de vous connecter en tant que System Administrator. Par exemple :

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

S'il vous faut un seul utilisateur de domaine, vous pouvez éviter de configurer un fichier de jetons en utilisant le nom de domaine *nobody*. L'exemple suivant crée l'utilisateur *nobody* dans le domaine *engineering* et configure le mot de passe pour *nobody@engineering*, défini comme *utilisateur@nom-domaine* dans le TABLEAU 3-1.

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

Vous devez utiliser ce mot de passe lors de l'authentification effectuée au cours du démarrage d'un serveur Web.



Attention – Vous devez vous souvenir du mot de passe que vous avez saisi. Sans ce mot de passe, vous ne pourrez pas accéder à vos clés. Il est impossible de récupérer un mot de passe oublié.

Création d'une liste des domaines

Vous pouvez créer une liste des informations relatives à un domaine en exécutant la commande `show realm=nom-domaine`.

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

Création d'une liste des classes de domaines

Les classes de domaines sont des modules de gestion de clés contrôlant la gestion des objets clés, des comptes utilisateur et des données d'authentification par les domaines. La seule classe de domaines actuellement prise en charge par la carte Crypto Accelerator 1000 de Sun est `SUNW_filesys`. Pour créer une liste de toutes les classes de domaines actuellement prises en charge, utilisez la commande `show class`.

```
secadm> show class
```

```
Realm Class
```

```
-----
```

```
SUNW_filesys
```

```
-----
```

Suppression d'un domaine

Vous pouvez supprimer un domaine en exécutant la commande `delete realm` et en fournissant le nom du domaine à supprimer. Lorsque vous exécutez la commande, `secadm` vous invite à confirmer ou infirmer la suppression du domaine. De même que pour la création d'un domaine, le compte System Administrator doit être authentifié avant que la commande ne soit exécutée. De plus, vous ne pouvez pas supprimer un domaine en cours d'utilisation. Pour supprimer des références dans les domaines, il se peut que vous deviez fermer le serveur Web et/ou le serveur d'administration.

▼ Pour supprimer les domaines

1. A l'aide de l'utilitaire `secadm`, supprimez chaque domaine.

```
secadm> delete realm=nom-domaine
```

```
Delete realm nom-domaine? [Y/N]: Y
```

```
System Administrator Login Required
```

```
Login: root
```

```
Password:
```

```
Realm nom-domaine deleted successfully.
```

Toutes les données de domaine spécifiques à tous les sites sont alors supprimées, y compris les clés matérielles.

Configuration et gestion des comptes utilisateur

Les comptes utilisateur permettent aux applications d'être authentifiées sur la carte Crypto Accelerator 1000 de Sun et aux clés d'être séparées au sein d'un domaine. Les clés détenues par un compte utilisateur ne sont pas accessibles aux applications qui ne sont pas authentifiées, ou qui sont authentifiées sur ce domaine comme un autre utilisateur. Pour toutes ces commandes, vous devez sélectionner un domaine et le System Administrator doit être connecté à ce domaine à l'aide de la commande `secadm su`.

Création d'utilisateurs

- Exécutez la commande `create user` pour créer un utilisateur.

Cette commande exige un nom d'utilisateur sous la forme `create user=nomutilisateur`.

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



Attention – Vous devez vous souvenir du mot de passe que vous avez saisi. Sans ce mot de passe, vous ne pourrez pas accéder à vos clés. Il est impossible de récupérer un mot de passe oublié.

Création d'une liste d'utilisateurs

Seul le System Administrator peut créer une liste des utilisateurs dans un domaine. Le System Administrator doit exécuter la commande `show user`. Cette commande crée uniquement une liste des utilisateurs dans le domaine que vous avez sélectionné.

- Exécutez la commande `show user`.

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

Modification des mots de passe utilisateur

Seul l'utilisateur connecté individuellement et utilisant la commande `secadm login` peut modifier le mot de passe utilisateur. Vous devez connaître votre mot de passe actuel avant de pouvoir en définir un nouveau.

- Exécutez la commande `passwd`.

```
secadm{nomutilisateur@nom-domaine}> passwd
Enter current password:
Enter Password:
Confirm Password:
Password successfully changed for user nomutilisateur.
```



Attention – Vous devez vous souvenir du mot de passe que vous avez saisi. Sans ce mot de passe, vous ne pourrez pas accéder à vos clés. Il est impossible de récupérer un mot de passe oublié.

Activation ou désactivation des utilisateurs

Seuls les comptes `System Administrator` peuvent activer ou désactiver des utilisateurs. Par défaut, chaque utilisateur est créé avec le statut activé.

- **Pour désactiver un compte utilisateur saisissez la commande** `disable user=nomutilisateur`.

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

Toutes les tentatives d'authentification d'un utilisateur désactivé échoueront. Toutefois, aucune clé n'est modifiée de quelque façon que ce soit. Lorsqu'un compte est ré-activé, toutes les clés détenues par cet utilisateur sont une fois de plus accessibles par l'application authentifiée.

- **Pour activer un compte, saisissez la commande** `enable user=nomutilisateur`.

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

Suppression des utilisateurs

- **Exécutez la commande** `delete user` **en spécifiant l'utilisateur à supprimer.**

Le System Administrator doit fournir le nom du compte utilisateur à supprimer.

Les clés associées aux utilisateurs sont supprimées lors de l'exécution de la commande. secadm invite le System Administrator à confirmer ou infirmer la suppression de l'utilisateur.

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


Pages manuel

Cette annexe décrit les pages man comprises dans le logiciel Crypto Accelerator 1000 de Sun.

Vous pouvez consulter les pages man à l'aide de la commande :

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

Le TABLEAU B-1 répertorie et décrit les pages man.

TABLEAU B-1 Crypto Accelerator 1000 de Sun Pages **man** du logiciel

page man	Description
cryptio(7d)	Le pilote de périphérique <code>cryptio</code> offre un contrôle d'accès à l'accélérateur cryptographique matériel sous-jacent. Le pilote <code>cryptio</code> nécessite un logiciel en couches pour que les applications et les clients du noyau puissent accéder aux services fournis.
dca(7d)	Le pilote de périphérique <code>dca</code> est un pilote feuille qui offre un contrôle d'accès à l'accélérateur cryptographique matériel sous-jacent. Le pilote <code>dca</code> nécessite un logiciel en couches pour que les applications et les clients du noyau puissent accéder aux services fournis.
kc1(7d)	Le pilote de périphérique <code>kc1</code> est un module de noyau chargeable multithread offrant une prise en charge des pilotes de fournisseurs cryptographiques de Sun. Le pilote <code>kc1</code> nécessite un logiciel en couches pour que les applications et les clients du noyau puissent accéder aux services fournis.

TABLEAU B-1 Crypto Accelerator 1000 de Sun Pages **man** du logiciel (*suite*)

page man	Description
kcpi(7d)	Le pilote de périphérique kcpi est un module de noyau chargeable multithread offrant une prise en charge des pilotes de fournisseurs cryptographiques de Sun. Le pilote kcpi nécessite un logiciel en couches pour que les applications et les clients du noyau puissent accéder aux services fournis.
secadm(1m)	secadm est l'utilitaire d'administration du logiciel Crypto Accelerator 1000 de Sun. La commande secadm est utilisée pour la manipulation de la configuration, du compte et des bases de données de clés liés au logiciel Crypto Accelerator 1000 de Sun. secadm traite des informations importantes relatives aux clés cryptographiques.
secd(1m)	Le démon secd offre des services d'accès administratifs à l'application secadm.
sslconfig(1m)	sslconfig est l'utilitaire de configuration du logiciel Crypto Accelerator 1000 de Sun.

Directives de configuration SSL pour le serveur Web Apache

Cette annexe répertorie les directives d'utilisation du logiciel Crypto Accelerator 1000 de Sun pour configurer la prise en charge SSL pour le 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/crypto/bin/sslpasword` 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 `sslpasword` 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 mots de passe ne contiennent que le mot de passe non codé sur une ligne.

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. Il est conseillé aux clients Sun d'éviter le comportement par défaut et d'utiliser le programme `sslpasword` à la place, afin d'éviter les 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>
```

Elle 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. `SSLProtocol [+ -]protocole`

Contexte : global, hôte virtuel

Cette 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 C-1 :

TABLEAU C-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 C-2. Dans le TABLEAU C-2, DH se rapporte à Diffie-Hellman et DSS à Digital Signature Standard.

TABLEAU C-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 C-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 C-3 répertorie et décrit les alias fournissant des groupements de type macro.

TABLEAU C-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 puissance faible (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 C-4.

TABLEAU C-4 Caractères spéciaux pour la configuration des préférences de chiffre

Caractère	Description
<none>	Ajouter un chiffre à la liste.
!	Supprimer définitivement un chiffre de la liste ; il est impossible de le rajouter ultérieurement.
+	Ajouter un chiffre à la liste et le situer à son emplacement actuel (ou l'abaisser).
-	Supprimer 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 degrés 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. SSLCertificateFile *fichier*

Contexte : global, hôte virtuel

Cette directive précise l'emplacement d'un fichier contenant la concaténation des certificats destinés aux autorités de certification, utilisée 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 certification, utilisée 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 C-5.

TABLEAU C-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 <i>doit</i> 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 `SSLCertificateFile`). 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 C-6.

TABLEAU C-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 C-7.

TABLEAU C-7 Options SSL disponibles

Options	Description
StdEnvVars	Un ensemble de variables standard d'environnement CGI/SSI lié à SSL est créé. Les performances en seront affectées.
ExportCertData	Provoque l'exportation des variables d'environnement <code>SSL_SERVER_CERT</code> , <code>SSL_CLIENT_CERT</code> et <code>SSL_CLIENT_CERT_CHAIN_n</code> ($n = 0, 1, \dots$). 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 <code>xxj31ZMTZzkVA</code>, qui n'est que la forme codée (<code>crypt(3c)</code>) du mot « password » (mot de passe).
StrictRequire	Oblige le refus d'un accès provoqué par le rejet de <code>SSLRequireSSL</code> , et ce, même en présence d'autres directives, telles que <code>Satisfy Any</code> , 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 qui pourraient mettre les données d'un répertoire à la disposition d'utilisateurs non authentifiés et non codés.

Création d'applications pour une utilisation avec la Carte Crypto Accelerator 1000 de Sun

Cette annexe traite du logiciel fourni avec la carte Crypto Accelerator 1000 de Sun, qui peut être utilisé pour construire des applications compatibles avec OpenSSL afin de bénéficier des fonctions d'accélération cryptographique de la carte Crypto Accelerator 1000 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 1000 de Sun sont fournies en l'état et ne constituent pas une partie officiellement prise en charge du produit. 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 `SUNWcrys1` qui contient les en-têtes de fichiers et les bibliothèques requis.

Votre application doit être configurée de manière à inclure les en-têtes OpenSSL à partir de `/opt/SUNWconn/crypto/include`, comme avec le drapeau de compilation :

-I /opt/SUNWconn/crypto/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 être également incluses. Les drapeaux d'éditeur de liens suivants effectueront ceci :

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

Spécifications de la Carte Crypto Accelerator 1000 de Sun

Cette annexe décrit les diverses spécifications de la carte Carte Crypto Accelerator 1000 de Sun. Elle comprend les sections suivantes :

- « Dimensions physiques », page 85
- « Spécifications de l'interface », page 86
- « Alimentation requise », page 86
- « Caractéristiques environnementales », page 86

Dimensions physiques

TABLEAU E-1 Dimensions physiques

Dimension	Mesures	Mesures métriques
Longueur	6,875 pouces	174,625 mm
Largeur	4,2 pouces	106,680 mm

Spécifications de l'interface

TABEAU E-2 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

Alimentation requise

TABEAU E-3 Alimentation requise

Spécification	Mesure
Consommation électrique maximale	10 W à 5 V 700 mW à 3,3 V
Tolérance	5 V +/- 5 % 3,3 V +/- 5 %
Courant	2 A à 1,8 V 150 mA à 3,3 V

Caractéristiques environnementales

TABEAU E-4 Caractéristiques environnementales

Condition	Spécification de fonctionnement	Spécification de stockage
Température	0° à 70 °C, 32° à 160 °F	-65 °C à +150 °C, -85 ° à 300 ° F
Taux d'humidité relative	5 à 85 % sans condensation	0 à 95 % sans condensation

Licences tierces

Cette annexe traite de consignes et de licences logicielles émanant des autres parties qui régissent l'utilisation de ces portions.

QUESTIONS RELATIVES A LA LICENCE OPENSSL

Le Toolkit OpenSSL est régi par une licence double ; ainsi, aussi bien les conditions de la licence OpenSSL que celles de la licence SSLeay d'origine s'appliquent au kit d'outils. Veuillez vous reporter ci-dessous au contenu réel des licences. En fait, il s'agit toutes deux de licences Open Source de type BSD. Veuillez envoyer vos questions relatives à la licence OpenSSL à l'adresse électronique suivante : openssl-core@openssl.org.

Licence OpenSSL

Copyright (c) 1998-2001 The OpenSSL Project. Tous droits réservés.

La redistribution et l'utilisation de la source ou du fichier binaire, avec ou sans modifications, sont autorisées, dans la mesure où les conditions suivantes sont remplies :

1. Les redistributions du code source doivent faire mention du copyright ci-dessus, de cette liste de conditions et du déni de responsabilité suivant.
2. Les redistributions sous forme binaire doivent reproduire le copyright ci-dessus, cette liste de conditions et le déni de responsabilité suivant dans la documentation et(ou) dans le matériel distribué.
3. Le matériel publicitaire faisant état des caractéristiques ou de l'utilisation de ce logiciel doit mentionner la déclaration suivante : « Ce produit comprend un logiciel développé par OpenSSL Project en vue d'être utilisé dans le Toolkit OpenSSL (<http://www.openssl.org/>) ».

4. Les noms « OpenSSL Toolkit » et « OpenSSL Project » ne doivent pas être utilisés pour endosser ni promouvoir les produits dérivés de ce logiciel sans autorisation préalable écrite. Veuillez faire parvenir vos demandes d'autorisation écrite à l'adresse suivante : openssl-core@openssl.org.
5. Les produits dérivés de ce logiciel ne peuvent pas être désignés sous le nom « OpenSSL » et « OpenSSL » ne peut pas apparaître dans leurs noms sans autorisation préalable écrite de OpenSSL Project.
6. Les redistributions, sous quelque forme qu'elles soient, doivent conserver la déclaration suivante : « Ce produit comprend un logiciel développé par OpenSSL Project en vue d'être utilisé dans le Toolkit OpenSSL (<http://www.openssl.org/>) ».

CE LOGICIEL EST FOURNI « EN L'ETAT » PAR OpenSSL PROJECT ET TOUTE AUTRE GARANTIE EXPRESSE OU TACITE EST FORMELLEMENT EXCLUE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE OU A L'APTITUDE A UNE UTILISATION PARTICULIERE. OpenSSL PROJECT ET SES CONTRIBUTEURS NE PEUVENT EN AUCUN CAS ETRE TENUS RESPONSABLES DE TOUT DOMMAGE DIRECT, INDIRECT, ACCIDENTEL, SPECIAL, EXEMPLAIRE OU CONSECUTIF (Y COMPRIS NOTAMMENT L'APPROVISIONNEMENT DE BIENS ET SERVICES DE REMPLACEMENT, LA PERTE D'UTILISATION, DE DONNEES OU DE PROFITS OU L'INTERRUPTION D'ACTIVITES COMMERCIALES), QUELLE QU'EN SOIT LA CAUSE ET QUELLE QUE SOIT LA RESPONSABILITE MISE EN CAUSE, QU'ELLE SOIT CONTRACTUELLE, OBJECTIVE OU DELICTUELLE (Y COMPRIS NOTAMMENT LA NEGLIGENCE), DOMMAGE CONSECUTIF A L'UTILISATION DE CE LOGICIEL, MALGRE LES AVERTISSEMENTS DE DOMMAGES EVENTUELS.

Ce produit comprend un logiciel cryptographique écrit par Eric Young (eay@cryptsoft.com). Ce produit comprend un logiciel écrit par Tim Hudson (tjh@cryptsoft.com).

Licence SSLeay d'origine

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). Tous droits réservés.

Ce progiciel est une instance SSL écrite par Eric Young (eay@cryptsoft.com), en conformité avec Netscapes SSL.

Cette bibliothèque est destinée à une utilisation commerciale et personnelle illimitée dans la mesure où les conditions ci-dessous sont respectées. Les conditions suivantes s'appliquent non seulement au code SSL, mais également à tous les codes compris dans cette distribution, qu'il s'agisse du code RC4, RSA, lhash, DES, etc. La documentation SSL comprise dans cette distribution est couverte par les mêmes conditions de copyright, à l'exception que le détenteur en est Tim Hudson (tjh@cryptsoft.com).

Le copyright demeure la propriété de Eric Young et, par conséquent, aucune clause de copyright intégrée au code ne peut être supprimée.

Si ce progiciel est intégré à un produit, les droits d'auteur des parties de la bibliothèque utilisées doivent être attribués à Eric Young. Cette reconnaissance peut se faire sous forme de message textuel apparaissant au lancement du programme ou dans la documentation (en ligne ou textuelle).

La redistribution et l'utilisation de la source ou du fichier binaire, avec ou sans modifications, sont autorisées, dans la mesure où les conditions suivantes sont remplies :

1. Les redistributions du code source doivent faire mention du copyright, de cette liste de conditions et du déni de responsabilité suivant.
2. Les redistributions sous forme binaire doivent reproduire le copyright ci-dessus, cette liste de conditions et le déni de responsabilité suivant dans la documentation et (ou) dans le matériel distribué.
3. Le matériel publicitaire faisant état des caractéristiques ou de l'utilisation de ce logiciel doit mentionner la déclaration suivante : « Ce produit comprend un logiciel cryptographique écrit par Eric Young (eay@cryptsoft.com) ». Le mot « cryptographique » peut être ignoré si les routines de la bibliothèque utilisée ne sont pas cryptographiques :-).
4. Si vous intégrez un code spécifique à Windows (ou un code qui en est dérivé) du répertoire apps (code d'applications), vous devez ajouter la déclaration : « Ce produit comprend un logiciel écrit par Tim Hudson (tjh@cryptsoft.com) ».

CE LOGICIEL EST FOURNI « EN L'ETAT » PAR ERIC YOUNG ET TOUTE AUTRE GARANTIE EXPRESSE OU TACITE EST FORMELLEMENT EXCLUE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE OU A L'APTITUDE A UNE UTILISATION PARTICULIERE. L'AUTEUR ET LES CONTRIBUTEURS NE PEUVENT EN AUCUN CAS ETRE TENUS RESPONSABLES DE TOUT DOMMAGE DIRECT, INDIRECT, ACCIDENTEL, SPECIAL, EXEMPLAIRE OU CONSECUTIF (Y COMPRIS NOTAMMENT L'APPROVISIONNEMENT DE BIENS ET SERVICES DE REMPLACEMENT, LA PERTE D'UTILISATION, DE DONNEES OU DE PROFITS OU L'INTERRUPTION D'ACTIVITES COMMERCIALES), QUELLE QU'EN SOIT LA CAUSE ET QUELLE QUE SOIT LA RESPONSABILITE MISE EN CAUSE, QU'ELLE SOIT CONTRACTUELLE, OBJECTIVE OU DELICTUELLE (Y COMPRIS NOTAMMENT LA NEGLIGENCE), DOMMAGE CONSECUTIF A L'UTILISATION DE CE LOGICIEL, MALGRE LES AVERTISSEMENTS DE DOMMAGES EVENTUELS.

Il est interdit de modifier la licence et les conditions de distribution de toute version ou tout dérivé de ce code disponible au public. Par conséquent, ce code ne peut pas être copié et transféré dans une autre licence de distribution (y compris la licence publique GNU).

« Ian Fleming était fan d'UNIX !
Comment le sais-je ? Eh bien, James Bond
avait le (permis de tuer) numéro 007,
donc il pouvait exécuter n'importe qui. »
-- Anonyme

LICENCE MOD_SSL

Le progiciel mod_ssl est rangé sous le label Logiciel Open-Source car il est distribué sous une licence de type BSD, dont les détails sont les suivants.

Copyright (c) 1998-2000 Ralf S. Engelschall. Tous droits réservés.

La redistribution et l'utilisation de la source ou du fichier binaire, avec ou sans modifications, sont autorisées, dans la mesure où les conditions suivantes sont remplies :

1. Les redistributions du code source doivent faire mention du copyright ci-dessus, de cette liste de conditions et du déni de responsabilité suivant.
2. Les redistributions sous forme binaire doivent reproduire le copyright ci-dessus, cette liste de conditions et le déni de responsabilité suivant dans la documentation et(ou) dans le matériel distribué.
3. Le matériel publicitaire faisant état des caractéristiques ou de l'utilisation de ce logiciel doit mentionner la déclaration suivante : « Ce produit comprend un logiciel développé par Ralf S. Engelschall (rse@engelschall.com) conçu pour être utilisé dans le cadre du projet mod_ssl (<http://www.modssl.org/>) ».
4. Le nom « mod_ssl » ne doit pas être utilisé pour endosser ni promouvoir les produits dérivés de ce logiciel sans autorisation préalable écrite. Veuillez faire parvenir vos demandes d'autorisation écrite à l'adresse suivante : rse@engelschall.com.
5. Les produits dérivés de ce logiciel ne peuvent pas être désignés sous le nom « mod_ssl » et « mod_ssl » ne peut pas apparaître dans leurs noms sans autorisation préalable écrite de Ralf S. Engelschall.
6. Les redistributions, qu'elle qu'en soit la forme, doivent conserver la déclaration suivante : « Ce produit comprend un logiciel développé par Ralf S. Engelschall (rse@engelschall.com) conçu pour être utilisé dans le cadre du projet mod_ssl (<http://www.modssl.org/>) ».

CE LOGICIEL EST FOURNI « EN L'ETAT » PAR RALF S. ENGELSCHALL ET
TOUTE AUTRE GARANTIE EXPRESSE OU TACITE EST FORMELLEMENT
EXCLUE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE
A LA QUALITE MARCHANDE OU A L'APTITUDE A UNE UTILISATION

PARTICULIERE. RALF S. ENGELSCHALL ET SES CONTRIBUTEURS NE PEUVENT EN AUCUN CAS ETRE TENUS RESPONSABLES DE TOUT DOMMAGE DIRECT, INDIRECT, ACCIDENTEL, SPECIAL, EXEMPLAIRE OU CONSECUTIF (Y COMPRIS NOTAMMENT L'APPROVISIONNEMENT DE BIENS ET SERVICES DE REMPLACEMENT, LA PERTE D'UTILISATION, DE DONNEES OU DE PROFITS OU L'INTERRUPTION D'ACTIVITES COMMERCIALES), QUELLE QU'EN SOIT LA CAUSE ET QUELLE QUE SOIT LA RESPONSABILITE MISE EN CAUSE, QU'ELLE SOIT CONTRACTUELLE, OBJECTIVE OU DELICTUELLE (Y COMPRIS NOTAMMENT LA NEGLIGENCE), DOMMAGE CONSECUTIF A L'UTILISATION DE CE LOGICIEL, MALGRE LES AVERTISSEMENTS DE DOMMAGES EVENTUELS.

Index

A

- activation
 - serveurs Web Apache, 39
 - serveurs Web iPlanet, 15
- administration des serveurs Web iPlanet, 53
- algorithmes, 3

B

- base de données certifiée
 - création
 - serveur Web iPlanet 4.1, 20
 - serveur Web iPlanet 6.0, 30

C

- certificat de serveur, 23, 33
- commande kstat, 51
- commandes
 - kstat, 51
- conditions
 - logicielles, 5
 - matérielles, 5
- configuration High Availability, 3
- connexion à chaud, 3
- correctifs
 - recommandés, 6
 - requis, 6
 - Solaris 8, 6
 - Solaris 9, 6

D

- dcatetest, 48
 - options de paramètres de test, 49
 - sous-tests, 49
 - syntaxe de ligne de commande, 49
- dépannage, 51
- directives SSL Apache, 73
- domaines, 53
 - configuration, 64
 - création, 63
 - création d'une liste, 65
 - suppression, 66

F

- fichiers de jetons, 55
- fichiers et répertoires
 - installation, 10
- fonctionnalité Dynamic Reconfiguration, 3

L

- licences
 - tierce partie, 87
- longueur de clé, 41

M

- mot de passe utilisateur
 - modification, 68
- mots de passe
 - administrateur système, 17
 - liste requise pour les serveurs Web iPlanet, 15
 - secadm, 17

O

- OpenBoot PROM, 51

P

- paire de clés RSA, 41
- partage de la charge, 4
- progiciels, 10

R

- répertoires
 - hiérarchique des, 12

S

- serveurs Web Apache
 - activation, 39
 - création d'un certificat, 42
- serveurs Web iPlanet
 - activation, 15
 - création et remplissage d'un domaine, 16
- serveur Web iPlanet 4.1
 - configuration, 25
 - création d'un certificat de serveur, 20
 - création d'une base de données certifiée, 20
 - installation, 19
 - installation d'un certificat de serveur, 25
- serveur Web iPlanet 6.0
 - configuration, 36
 - création d'un certificat de serveur, 33
 - création d'une base de données certifiée, 30
 - installation, 29
 - installation d'un certificat de serveur, 35
- SunVTS, 47
 - dcatest, 48

T

- tests de diagnostics, 47

U

- URL
 - pour le logiciel iPlanet, 19, 29
 - pour OpenSSL, 83
- utilisateurs, 53
 - activation ou désactivation, 68
 - création, 67
 - création d'une liste, 67
 - suppression, 69
- utilitaire secadm, 56

V

- valeurs statistiques, 52