Notes de version 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° 816-4571-10
juillet 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 licencié par des fournisseurs de Sun.

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

Sun, Sun Microsystems, le logo Sun, SunVTS, AnswerBook2, docs.sun.com, iPlanet, Sun Enterprise, Sun Enterprise Volume Manager et Solaris sont des marques de fabrique, 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 le Project OpenSSL pour l'utilisation 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> pour l'utilisation dans le 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.

Produit
recyclable

Adobe PostScript

Notes de version de la carte Crypto Accelerator 1000 Version 1.1 de Sun

Ces notes de version apportent des informations supplémentaires non disponibles à la date de parution du *Guide de l'utilisateur et d'installation de la carte Crypto Accelerator 1000 Version 1.1 de Sun*.

Problèmes possibles avec les serveurs Web iPlanet

1. Si vous exécutez le serveur d'administration iPlanet 4.x ou 6.x et que le serveur Web pris en charge ne fonctionne pas, il existe plusieurs situations où des boîtes de dialogues d'authentification forte apparaissent. Si vous utilisez une très grande police ou s'il existe de nombreuses authentifications fortes (et par conséquent de nombreux champs de saisie de mots de passe), les boutons sur la partie inférieure du panneau ne seront pas affichés car la boîte de dialogue a une taille fixe qui n'est pas suffisante. Il est alors impossible de cliquer sur le bouton « Accept » (Accepter) de la partie inférieure du panneau et de soumettre la modification car il est impossible de redimensionner la boîte de dialogue.

   Il existe deux solutions à ce problème.

   - Démarrez tout d'abord le serveur Web à partir de la ligne de commandes ou du serveur d'administration avec la préférence d'interface utilisateur graphique définie sur « On / Off » (Activé / Désactivé).
   - Appliquez la configuration sans démarrer le serveur : « Apply-> Load Configuration Files » (Appliquer-> Charger les fichiers de configuration).

     Bogue n° : 4532645

2. Les serveurs Web iPlanet ne peuvent pas fonctionner si des configurations comportent plusieurs domaine(s), ou si différents utilisateurs sont présents sur différents serveurs Web.

   Il existe deux solutions à ce problème.

   - Configurez au maximum un domaine et un utilisateur par serveur Web.
   - Vous pouvez exécuter différentes instances du serveur Web iPlanet sous différents utilisateurs UNIX et configurer `$HOME/.SUNWconn_crypto_slots` comme vous le souhaitez, pour chaque utilisateur. Veuillez consulter le *Guide de l'utilisateur et d'installation de la carte Crypto Accelerator 1000 Version 1.1 de Sun* pour plus d'informations sur les fichiers de jetons.

     Bogue n° : 4532941 et 4593111

3. L'utilitaire iPlanet fourni, `pk12util`, exporte des certificats et des clés à partir de bases de données internes (logicielles) et les importe vers des bases de données externes (matérielles). Il ne permet pas d'exporter des certificats ou des clés à partir d'une base de données externe :

```
% cd /usr/iplanet/servers/alias
% pk12util -o temp.p12 -n "Our Token:Server-Cert" -d .
Enter Password or Pin for "Our Token":
Enter password for PKCS12 file:
Re-enter password:
pk12util: add cert and key failed: Unable to export. Private Key
could not be located and exported.
```

   Bogue n° : 4620283

4. Lors de la configuration du serveur Web iPlanet 6.0, après la sélection des paramètres de chiffrement par défaut, la sélection du certificat, la pression sur le bouton OK et la sélection du lien « Apply » (Appliquer), dans le coin supérieur droit, en vue d'appliquer les chiffres, il se peut que l'entrée *utilisateur@nom-domaine* soit supprimée si les étapes ne sont pas suivies dans l'ordre précis indiqué dans le *Guide de l'utilisateur et d'installation de la carte Crypto Accelerator 1000 Version 1.1 de Sun*.

   Cette entrée est obligatoire pour que le serveur Web démarre correctement avec la carte Crypto Accelerator 1000 de Sun. Vous le constaterez si vous suivez les étapes dans l'ordre indiqué ci-dessous :

   - Sélectionnez « Cipher Default » (Chiffre par défaut), chiffre SSL2 ou SSL3.
   - Cliquez sur OK.
   - Cliquez sur « Apply ».
   - Cliquez sur « Load Configuration » (Chargement de la configuration).

Si vous pensez que vous avez suivi ces étapes et que le serveur Web ne démarre pas correctement, procédez comme suit pour résoudre le problème :

- Modifiez le fichier :

```
/usr/iplanet/servers/https-nomhôte.domaine/config/server.xml
```

- Recherchez la ligne commençant par :

```
<SSLPARAMS servercertnickname="Server-Cert". . .
```

- Insérez le texte *utilisateur@nom-domaine* : avant le texte `Serveur-Cert` dans la ligne, afin que la ligne modifiée s'apparente à la suivante :

```
<SSLPARAMS servercertnickname="utilisateur@nom-domaine:
Server-Cert". . .
```

- Redémarrez le serveur Web.

Bogue n° : 4607112

Versions des serveurs Web Apache prises en charge

Cette version du logiciel Crypto Accelerator 1000 de Sun prend en charge Apache 1.3.12 et 1.3.26 sur Solaris 8 et Apache 1.3.22 et 1.3.26 sur Solaris 9. Ces informations relatives à la prise en charge sont destinées aux versions d'Apache regroupées avec l'environnement d'exploitation ou bien fournies par des correctifs Sun officiels.

Problèmes possibles avec les serveurs Web Apache

1. Le classement des fichiers de démarrage Apache (`/etc/rc3.d/S50apache`) et `dtlogin` (`/etc/rc2.d/S99dtlogin`) provoque un problème de classement à l'initialisation de la machine. Il se peut alors que la console ne soit pas accessible pour la saisie du mot de passe Apache au démarrage. Pour résoudre le problème, connectez-vous en tant que superutilisateur et exécutez la commande suivante afin d'effectuer un reclassement pour le démarrage du serveur Web Apache :

```
# mv /etc/rc3.d/S50apache  /etc/rc2.d/S95apache
```

Problèmes possibles avec le logiciel Crypto Accelerator 1000 Version 1.1 de Sun

1. Pour les environnements d'exploitation Solaris 8, le correctif 112438-01 doit être installé avant le logiciel Crypto Accelerator 1000 Version 1.1 de Sun. Ce correctif se trouve sur le CD-ROM du produit, dans le sous-répertoire `patches`. Vous pouvez également le télécharger à partir de l'adresse `http://sunsolve.sun.com`.

   Bogue n° : 4470196

2. Contrairement à la version 6.x du serveur Web iPlanet, la version 4.x ne fournit pas les outils logiciels pour l'extraction de clés.

   Il existe deux solutions pour extraire des clés de bases de données logicielles (internes) :

   - Téléchargez NSPR 4.12 et NSS 3.3 (ou une version ultérieure) à partir du site Web suivant : `http://www.iplanet.com/downloads`

     Installez ces logiciels puis exécutez `pk12util` sur les bases de données, afin d'extraire les certificats et les clés des bases de données logicielles (internes).

   - Utilisez Netscape Communicator 4.x ou 6.x pour extraire les clés des bases de données logicielles (internes).

Il n'existe pour l'heure aucun moyen d'extraire les clés prises en charge par la carte Crypto Accelerator 1000 de Sun.

Bogue n° : 4621453

3. Il se peut que la carte Crypto Accelerator 1000 de Sun soit affichée différemment ou pas du tout, avec l'utilisation de `prtdiag`(1M), en raison des différentes instances de plates-formes de l'utilitaire `prtdiag` et de Open Boot PROM. Par exemple, sur un serveur Enterprise 450, la carte Crypto Accelerator 1000 de Sun est affichée comme suit :

```
SYS   PCI    66     4   pciclass,100000
```

Bogue n° : 4343467 et 4526901

4. A l'heure où nous imprimons ce document, il n'existe aucun mécanisme d'extraction de clés et de certificats à partir de la carte Crypto Accelerator I de Sun. Veuillez consulter le site Web suivant pour vous assurer qu'un correctif existe pour résoudre ce problème : `http://sunsolve.sun.com`.

Bogue n° : 4630250

5. La carte Crypto Accelerator 1000 de Sun ne prend pas en charge les connexions PCI à chaud, dans les emplacements de 66 MHz, sur les systèmes Sun Fire™ V880, avec l'environnement d'exploitation Solaris 9. Ce problème n'affecte pas les systèmes utilisant Solaris 8. Un correctif devrait, à l'avenir, régler ce problème.

La carte peut être installée sur un système hors tension exécutant Solaris 9, puis utilisée dans les emplacements. Elle peut être également connectée à chaud dans les emplacements de 33 MHz d'un système exécutant Solaris 9.

Bogue n° : 4698278