Notes de version de la carte Crypto Accelerator 4000 de Sun™

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

Référence n° 817-2347-10
mai 2003, révision A

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

Produit recyclable

Notes de version de la carte Crypto Accelerator 4000 de Sun™

Ces notes de version décrivent les problèmes possibles de la carte Crypto Accelerator 4000 de Sun.

Le correctif 114795-01 s'installe automatiquement lors de l'installation du logiciel Crypto Accelerator 4000 de Sun. Utilisez la commande `showrev -p` pour vérifier la version de ce correctif en vue des futures mises à jour.

Problèmes possibles avec le logiciel Crypto Accelerator 4000 de Sun

Plates-formes prises en charge

La plate-forme Sun Fire™ 15K n'est pas actuellement prise en charge par la carte Crypto Accelerator 4000 de Sun.

Version FCODE

La version FCODE pour la carte Crypto Accelerator 4000 de Sun est 12.11.13. La version FCODE adéquate n'apparaît pas dans la liste des sorties `.properties` qui se trouve à la page 15 du *Guide de l'utilisateur et d'installation de la carte Crypto Accelerator 4000 de Sun*.

Bogue 4757594 : variable `vca.conf`

La solution à ce bogue consiste en une variable `vca.conf` à utiliser manuellement, en attendant sa résolution définitive dans le logiciel Solaris. Ajoutez l'entrée suivante au fichier `kernel/drv/vca.conf` :

```
dma-mode=1;
```

Cette solution ne devrait être requise que pour les plates-formes d'entrée de gamme comme Sun Blade™ 100 et 150, par exemple.

Bogue 4470196 : correctifs requis pour Solaris 8

Dans les environnements d'exploitation Solaris 8, vous devez installer les correctifs 112438-01 et 109234-09 avant d'installer le logiciel Crypto Accelerator 4000 de Sun. Vous pouvez trouver ces correctifs dans le sous-répertoire `patches` du CD-ROM du produit ou les télécharger en vous rendant à l'adresse suivante : `http://sunsolve.sun.com`.

Remarque – Après avoir appliqué ces correctifs, vous devez redémarrer le système ***avant*** d'installer le logiciel Crypto Accelerator 4000 de Sun.

Bogue 4621453 : extraction des clés

Le serveur Web Sun™ ONE version 4.x ne fournit pas les outils logiciels pour l'extraction des clés car ils sont fournis par le serveur Web Sun ONE version 6.x.

Remarque – Auparavant, les serveurs Web Sun ONE étaient appelés les serveurs Web iPlanet™.

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.mozilla.org`

  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).

Bogue 4630250 : clés et certificats

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 4000 de Sun. Veuillez consulter le site Web suivant pour vous assurer qu'un correctif existe pour résoudre ce problème : `http://sunsolve.sun.com`.

Bogue 4796664 : test de bouclage interne

Les cartes MMF Crypto Accelerator 4000 de Sun peuvent échouer au test de bouclage interne du test de SunVTS™ ou de `netlbtest`. Les messages d'erreurs suivants peuvent s'afficher :

```
"
19/12/02 17:20:03 nomutilisateur SunVTS4.5: VTSID 8003 netlbtest.
 FATAL vca1:    "Failed to get the link up.
 Probable_Cause(s):
    (1)Loopback cable not connected.
    (2)Faulty loopback cable.
 Recommended_Action(s):
    (1)Check and replace, if necessary, the loopback cable.
    (2)If problem persists, call your authorized Sun service
provider.
```

Bogue 4826508 : connexion en mode de commande simple

Si vous utilisez `vcaadm` en mode de commande simple et que la connexion échoue, le programme affiche les messages suivants :

```
Security Officer Login: so
Security Officer Password:
Login failed.

Error writing data: Bad file number
```

Bogue 4816009 : activation du mode FIPS

Si une carte inconnue est utilisée pour des opérations cryptographiques au moment où le responsable de la sécurité en devient le propriétaire et qu'il active le mode FIPS, elle peut se bloquer.

Solution : ne remettez pas à zéro une carte qui est en mode FIPS et n'initialisez pas une carte en mode FIPS au moment où vous envoyez des requêtes cryptographiques à la carte.

Bogue 4825721 : test du système Sun Fire 15K

Si vous lancez des tests de Sun Fire 15K dans une configuration point à point sur des cartes MMF ou UTP, les messages d'erreurs suivants peuvent s'afficher dans la console :

```
Feb 27 11:39:04 xc15p13-b3 vca: [ID 732820 kern.warning] WARNING:
vca1: vce_link_stats_set: cant determine params
Feb 27 11:40:29 xc15p13-b3 vca: [ID 214153 kern.warning] WARNING:
vca1: Can’t determine link paramaters!
Feb 27 11:40:29 xc15p13-b3 vca: [ID 702911 kern.notice] NOTICE:
vca1: link up 0 Mbps half duplex
Feb 27 11:40:29 xc15p13-b3 vca: [ID 732820 kern.warning] WARNING:
vca1: vce_link_stats_set: cant determine params
Feb 27 11:41:08 xc15p13-b3 vca: [ID 702911 kern.notice] NOTICE:
vca0: link down
Feb 27 12:01:07 xc15p13-b3 vca: [ID 702911 kern.notice] NOTICE:
vca0: link up 1000 Mbps full duplex
```

Cela n'entraîne aucune perte de communication car la liaison est rétablie après quelques minutes.

Bogue 4753295

Le chiffrement de masse est activé par défaut pour le logiciel du serveur Web Apache et ne peut pas être désactivé. Le chiffrement de masse est désactivé par défaut pour le logiciel du serveur Sun ONE et doit être activé manuellement par la création d'un fichier vide (`/etc/opt/SUNWconn/cryptov2/sslreg`) suivie du redémarrage du logiciel du serveur Sun ONE. L'activation du chiffrement de masse pour le logiciel du serveur Sun ONE permet d'accélérer le transfert de fichiers volumineux mais peut ralentir légèrement le transfert de petits fichiers.

Solution : activez le chiffrement de masse pour le logiciel du serveur Sun ONE uniquement lors de transferts de fichiers volumineux.

Bogue 4822356 : recomposition de la clé principale avec `vcaadm`

Au cours de l'exécution de la commande `rekey master`, `vcaadm` affiche le message « Cannot get new modules from firmware » (Impossible d'obtenir de nouveaux modules à partir du microprogramme). Ce message ne signifie pas que la clé principale n'a pas été régénérée. Ce message d'erreur n'est pas valide ; en réalité, la commande s'exécute correctement.

```
vcaadm{vca0@localhost, sec_officer}> rekey master
WARNING: Rekeying the master key will render all old board backups
         useless with the new keystore file. If other boards use
this
          keystore, you will need to back up this new key and
initialize
        the other boards to use the keystore, providing the backed
up
          master key in the process.

Rekey board? (Y/Yes/N/No) [No]: y
Rekeying crypto accelerator board. This may take a few
minutes...Done.
Cannot get new modulus from firmware.
```

Bogue 4852120 : possibilité d'erreur de délai

Des messages d'erreurs similaires à ceux présentés ci-dessous peuvent s'afficher si le trafic réseau est très dense et que des opérations cryptographiques sont en cours d'exécution au même moment.

```
Apr 17 23:44:37 xc15p13-b0 vca: WARNING: stale job(s) found in ring 30000978718
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         request 0x7820aa68
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         ======================
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_key_id[0]: 0x00000000
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_key_id[1]: 0x00000000
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_cmd: 0x0013
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_key_flags[0]: 0x0
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_key_flags[1]: 0x0
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_in_len: 192
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_out_len: 192
Apr 17 23:44:37 xc15p13-b0 genunix: WARNING: vca1: fault detected in device;
service unavailable
Apr 17 23:44:37 xc15p13-b0 genunix: WARNING: vca1: crypto job timeout (device
hung?)
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE: vca1: Resetting board...
Apr 18 00:08:47 xc15p13-b0 vca: WARNING: vca1: Device is in failed state!
Apr 18 00:08:47 xc15p13-b0 last message repeated 1 time
```

Solution : réinitialisez la carte Crypto Accelerator 4000 de Sun.

Problèmes possibles avec les serveurs Web Sun ONE

Bogue 4532645 : messages du serveur d'administration

Si vous exécutez le serveur d'administration Sun ONE 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 de la fenêtre 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).

Bogues 4532941 et 4593111 : configuration avec plusieurs stockages de clés

Les serveurs Web Sun ONE peuvent ne pas fonctionner correctement avec des configurations de plusieurs stockages de clés. Ce problème est résolu dans le Service Pack 5 (SP5) du serveur Web Sun ONE 6.0.

Solution : configurez un seul stockage de clés pour toutes les instances du serveur Web. Ensuite vous pouvez configurer un autre utilisateur de stockage de clés pour chaque instance du serveur Web. Cela permet de séparer les clés de chaque instance du serveur Web les unes des autres.

Bogue 4620283 : utilitaire `pk12util`

L'utilitaire Sun ONE 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 4607112 : paramètres de chiffrement par défaut

Lors de la configuration du serveur Web Sun ONE 6.0, après la sélection des paramètres de chiffrement par défaut, la sélection du certificat, la sélection du bouton OK et la sélection du lien « Apply » (Appliquer) qui se trouve dans le coin supérieur droit et sert à appliquer les chiffres, il se peut que l'entrée *nomutilisateur:motdepasse* 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 4000 de Sun*. Ce problème est résolu dans le service Pack 3 (SP3) du serveur Web Sun ONE 6.0.

Cette entrée est obligatoire pour que le serveur Web démarre correctement avec la carte Crypto Accelerator 4000 de Sun. Vous le constaterez si vous suivez les étapes dans l'ordre indiqué ci-dessous :

1. Sélectionnez « Cipher Default » (Chiffre par défaut), chiffre SSL2 ou SSL3.
2. Sélectionnez OK.
3. Sélectionnez « Apply » (Appliquer).
4. Sélectionnez « 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 *nom_stockagedeclés*`:` avant le texte `Server-Cert` dans la ligne, afin que la ligne modifiée s'apparente à la suivante :

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

- Redémarrez le serveur Web.

Version du serveur Web Apache prise en charge

Cette version du logiciel Crypto Accelerator 4000 de Sun prend en charge Apache 1.3.26.

Problèmes possibles avec les serveurs Web Apache

Bogue 4766977 : correctifs requis pour Solaris 8

Pour configurer la carte Crypto Accelerator 4000 de Sun destinée à être utilisée avec le serveur Web Apache dans l'environnement d'exploitation Solaris 8, le correctif 109234-09 doit être installé avant d'installer le logiciel Crypto Accelerator 4000 de Sun. Vous pouvez trouver ces correctifs dans le sous-répertoire `patches` du CD-ROM du produit ou les télécharger en vous rendant à l'adresse suivante : `http://sunsolve.sun.com`.

Remarque – Après avoir installé ce correctif, vous devez redémarrer le système ***avant*** d'installer le logiciel Crypto Accelerator 4000 de Sun.

Le serveur Web Apache ne peut pas être configuré pour être utilisé simultanément avec la carte *Crypto Accelerator **1000** de Sun* et la carte *Crypto Accelerator **4000** de Sun*. Sinon, Apache ne fonctionnera pas correctement.

Installez le progiciel Crypto Accelerator 4000 de Sun `SUNWkcl2a` uniquement si vous prévoyez d'utiliser la carte avec le serveur Web Apache 1.3.26. Si vous prévoyez d'utiliser toute autre configuration ou version du serveur Web Apache, n'installez pas le progiciel `SUNWkcl2a`.

Fichiers de démarrage

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.

Solution : devenez superutilisateur et exécutez la commande suivante pour réorganiser le démarrage du serveur Web Apache :

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