Version 2.8.1/3.8.1/4.3.1

Instructions d'installation du CD de mise à niveau

À lire attentivement

Important

Veuillez lire ce manuel dans son intégralité. Si ce manuel présente des instructions relatives à l'installation ou au fonctionnement du produit, prêtez une attention particulière à toutes les consignes de sécurité.

Avis

Marques

- Cisco, Cisco Systems, le logo Cisco, le logo Cisco Systems, Explorer, PowerKEY et PowerTV sont des marques déposées ou des marques commerciales de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans certains autres pays.
- DOCSIS est une marque déposée de Cable Television Laboratories, Inc.
- CableCARD, M-Card et OCAP sont des marques de Cable Television Laboratories, Inc.
- *Toutes les autres marques commerciales mentionnées dans ce document sont la propriété de leurs détenteurs respectifs.*

Déclaration de non-responsabilité

Cisco Systems, Inc. décline toute responsabilité en cas d'erreurs ou d'omissions dans le présent document. Nous nous réservons le droit de modifier ce document à tout moment et sans avis préalable. Ce document ne doit pas être interprété comme concédant, par implication, préclusion ou autrement, une licence ou un droit lié à un droit d'auteur ou à un brevet, que l'utilisation d'informations présentées dans ce document emploie ou non une invention revendiquée dans un brevet existant ou enregistré ultérieurement.

Copyright

Table des matières

À propos de ce guide

Objectif

Ce guide fournit des instructions détaillées sur la mise à niveau d'un système Digital Broadband Delivery System (DBDS) vers la version 2.8.1/3.8.1/4.3.1. Les sites qui utilisent ce guide pour une mise à niveau doivent actuellement prendre en charge la version 2.8/3.8/4.3.

CD des fonctionnalités de la version 2.8.1/3.8.1/4.3.1

Cette mise à niveau vers la version 2.8.1/3.8.1/4.3.1 s'effectue avec la série de CD suivante :

- DNCS 4.3.1.6
- DNCS 4.3.1.6 p2
- DNCS WUI/GUI 4.3.1.6
- DNCS Online Help 4.3.1.0
- Report Writer 1.0.0.3

Combien de temps dure la mise à niveau ?

La mise à niveau vers la version 2.8.1/3.8.1/4.3.1 doit être effectuée selon une période d'entretien qui démarre habituellement à minuit. Les ingénieurs de mise à niveau ont déterminé qu'un site classique peut être mis à niveau dans une seule période d'entretien. La période d'entretien doit débuter lorsque vous arrêtez les composants système au chapitre 2.

Impact sur les performances du système

Les services interactifs ne sont pas disponibles pendant la période d'entretien.

Public visé

Ce guide a été rédigé pour les ingénieurs de terrain et les opérateurs système en charge de la mise à niveau d'un système DBDS existant vers la version 2.8.1/3.8.1/4.3.1.

Veillez à lire ce manuel dans son intégralité

N'oubliez pas de lire ce manuel dans son intégralité avant de commencer l'installation. Si une procédure vous semble difficile, n'hésitez pas à contacter les services Cisco au 1-866-787-3866.

Important : Effectuez toutes les procédures indiquées dans ce guide dans l'ordre auquel elles sont présentées. Si vous ne suivez pas toutes les instructions, vous risquez de ne pas obtenir des résultats escomptés.

Compétences et savoir-faire requis

Les ingénieurs ou opérateurs système qui mettent à niveau le logiciel ISDS doivent posséder les compétences suivantes :

- Être familier avec UNIX
  - Savoir utiliser l'éditeur UNIX vi. La procédure de mise à niveau du système nécessite plusieurs modifications des fichiers système avec l'éditeur UNIX vi. L'éditeur UNIX vi n'est pas intuitif. Les instructions fournies dans ce guide ne dispensent pas de posséder des connaissances avancées sur l'utilisation de vi.
  - Savoir revoir et modifier des fichiers cron
- Expertise étendue sur le système DBDS
  - L'aptitude à identifier les fichiers de clés spécifiques du site à mettre à niveau
  - L'aptitude à ajouter et supprimer des comptes utilisateur

Éléments prérequis

Avant de commencer la mise à niveau vers la version 2.8.1/3.8.1/4.3.1, assurez -vous que le site que vous mettez à niveau remplit les conditions suivantes :

- La version 2.8/3.8/4.3 ou une version ultérieure est actuellement installée sur votre système.
- Vous disposez du CD intitulé DBDS Maintenance CD 3.3.x qui permet d'effectuer les sauvegardes nécessaires de la base de données et du système de fichiers.
- Les sites qui utilisent le composant RNCS ont besoin du DVD dont l'intitulé est similaire au DVD d'installation de RNCS.

  Remarque : Notez qu'il s'agit d'un DVD et non d'un CD. Ce DVD sera uniquement fourni aux clients qui ont un système RNCS actif.
- Les sites qui utilisent le composant OCAP ont besoin du DVD dont l'intitulé est similaire au DVD d'installation d'OCAP.

  Remarque : Notez qu'il s'agit d'un DVD et non d'un CD. Ce DVD sera uniquement fourni aux clients qui ont un système OCAP actif.

- Le système doit prendre en charge une des combinaisons suivantes du code SARA (application résidente SA) et de celui du système d'exploitation PowerTV® ou d'une version ultérieure :
  - SARA 1.54 et OS 3.10
  - SARA 1.43.5a3 et OS 3.3.4.1008
- La dernière version de DBDS Utilities est installée sur votre système.

Serveur d'applications non SA et/ou application tierce

Si le site que vous mettez à niveau prend en charge un serveur d'applications non SA, contactez le fournisseur de ce serveur d'applications pour obtenir Les éléments prérequis pour la mise à niveau, ainsi que les procédures de mise à niveau et de restauration.

Si le site que vous mettez à niveau exécute une application logicielle tierce, contactez le fournisseur de cette application afin d'obtenir tous les éléments prérequis pour la mise à niveau.

Important : Vérifiez que tous les fournisseurs tiers savent que la mise à niveau vers la version 2.8.1/3.8.1/4.3.1 repose sur une plate-forme Solaris 10.

Publications connexes

Visitez notre site Web (https://www.sciatl.com/subscriberextranet/techpubs) pour afficher des publications supplémentaires sur nos produits.

Vous avez besoin d'un nom d'utilisateur et d'un mot de passe pour accéder à ce site Web. Si vous n'avez pas de nom d'utilisateur ni de mot de passe, accédez à https://www.scientificatlanta.com/dsnexplorer/register.htm pour remplir et envoyer un formulaire d'inscription.

Remarque : vous devrez peut-être installer un lecteur de documents PDF, par exemple Adobe Acrobat Reader, sur votre système pour afficher ces publications.

Plates-formes serveur prises en charge

Le serveur DNCS et les plates-formes matérielles indiqués ci-après sont pris en charge par la version 2.8.1/3.8.1/4.3.1 :

Serveur DNCS

Plate-forme	Disques durs	Mémoire
Sun Fire V890	■ 6 x 146 Go ■ 12 x 146 Go	■ 8 Go au minimum ■ 16 Go au minimum
Sun Fire V880	■ 6 x 73 Go ■ 12 x 73 Go	■ 4 Go au minimum ■ 8 Go au minimum
Sun Fire V445	2 x 73 Go	512 Mo au minimum

Serveur d'applications

Plate-forme	Disques durs	Mémoire
Sun Fire V240	2 x 36 Go	512 Mo au minimum
Sun Blade 150	■ 1 x 40 Go ■ 1 x 80 Go	512 Mo au minimum

Dépendances des versions des plates-formes d'applications

Le tableau suivant indique les dépendances des versions des plates-formes de terminal et du module Multi-Stream CableCARD™ (M-Card™) pour cette version logicielle.

Important : Si une version appropriée de la plate-forme d'applications *ou une version ultérieure* n'est pas installée sur votre système *avant* l'installation du logiciel, un figeage des vidéos ou des écrans noirs peuvent se produire lors de l'utilisation des applications de vidéo à la demande (VOD) ou des applications xOD.

Plate-forme de terminal ou M-Card	Système d'exploitation (OS)	SARA	Version d'accès conditionnel à PowerKEY®
Explorer® 8300 DVR version 1.4.3a10 ou ultérieure v. 1.5.2	OS 6.14.74.1 OS 6.14.79.1	1.88.22.1 1.89.16.2	3.9 3.9
Explorer 8000/8010 DVR version 1.4.3a10 ou ultérieure v. 1.5.2	OS 6.12.74.1 OS 6.12.79.1	1.88.21.1 1.89.16.2	3.7.5 3.7.5
Explorer 3250HD MR4 P1 ou une version ultérieure	OS 3.24.5.2	1.59.18.1	3.9

Plate-forme de terminal ou M-Card	Système d'exploitation (OS)	SARA	Version d'accès conditionnel à PowerKEY®
Explorer 2xxx, 31xx, 3200, 3100HD	OS 3.13.6.1	1.60.6.2	1.0.6.20 (Explorer 2000s) 1.0.7 (toutes les autres versions)
Explorer 4250HDC Exp. 2.0.0 (0701) ou une version ultérieure	OS 6.20.28.1	1.61.5.a100	4.0.1.1
Explorer 8300HDC DVR 1.5.3 (0801) ou une version ultérieure	OS 6.20.28.1	1.90.5a101	3.9.7.13
M-Card OS 1.1.10p5 ou une version ultérieure	OS 1.1.10p5	Non applicable	Non applicable
Explorer 8550HDC Explorer 8540HDC RNG200 DVR1.5.5	OS 8.0.42.1	1.90.19.1	Non applicable

Important : Si vous n'utilisez pas SARA, contactez votre fournisseur d'applications résidentes pour vérifier que vous avez la version la plus récente.

Version du document

La présente version est la version initiale du document.

1

Procédures de pré-mise à niveau vers la version 2.8.1/3.8.1/4.3.1

Introduction

Ce chapitre contient les procédures à suivre avant de commencer la mise à niveau réelle vers la version 2.8.1/3.8.1/4.3.1. Les procédures de pré-mise à niveau comportent essentiellement des contrôles système, des sauvegardes et diverses opérations à réaliser sur les métapériphériques du DNCS.

La mise à niveau réelle vers la version 2.8.1/3.8.1/4.3.1, notamment quelques-unes des procédures présentées dans ce chapitre, doit être effectuée dans une période d'entretien. Toutefois, quelques-unes des procédures présentées dans ce chapitre peuvent être suivies avant le démarrage de la période d'entretien . Voir ***Quand effectuer ces procédures ?*** (à la page 3), pour consulter la liste des procédures qui peuvent être réalisées avant le démarrage de la période d'entretien.

Important : Ne supprimez aucun fichier des applications tierces du DNCS et ne modifiez aucun de leurs paramètres avant de réaliser la mise à niveau vers la version 2.8.1/3.8.1/4.3.1.

Avant de commencer

Avant de commencer la mise à niveau, effectuez les deux opérations suivantes :

- Contactez les services Cisco et ouvrez un dossier de suivi de mise à niveau.
- Vérifiez que vous avez facilement accès au CD-ROM qui contient votre version actuelle du serveur d'applications. Vous pouvez avoir besoin de ce CD pour restaurer la version précédente du système.

Dans ce chapitre

Quand effectuer ces procédures ?

Processus de mise à niveau

Lorsque vous planifiez la mise à niveau, veillez à contacter votre fournisseur de facturation pour interrompre l'interface de facturation pendant la nuit de la mise à jour. Cette étape est importante. Votre système ne doit pas tenter d'accéder à la base de données lors de la mise à niveau. Par ailleurs, contactez les fournisseurs de toutes les applications tierces que votre système prend en charge. Suivez leurs instructions pour déterminer si les interfaces tierces doivent être arrêtées et si l'application nécessite une mise à jour pendant la mise à niveau.

Toutes les procédures présentées dans ce chapitre doivent être suivies avant d'entrer dans la période d'entretien. Les CD d'installation doivent être vérifiés dès que possible après leur réception. Cela donne le temps d'identifier les CD de remplacement et de les expédier s'il y a lieu. Des sauvegardes des systèmes de fichiers doivent être démarrées au matin de la mise à niveau pour qu'elles soient terminées avant le démarrage de la période d'entretien.

Exécution des procédures

Période d'entretien préalable

Pour gagner du temps précieux, exécutez les procédures indiquées dans ce chapitre avant le démarrage de la période d'entretien. Selon la taille du système que vous mettez à niveau, l'exécution de ces procédures prend 3 ou 4 heures.

Prévoir les fonctionnalités facultatives qui seront prises en charge

Fonctionnalités facultatives

Ce logiciel comprend plusieurs fonctionnalités facultatives que les opérateurs système peuvent choisir d'activer sur leurs systèmes. Certaines de ces fonctionnalités nécessitent que l'opérateur système obtienne une licence pour les activer ; d'autres ne nécessitent aucune licence et sont simplement activées par les ingénieurs des services Cisco.

Important : Toutes les fonctionnalités qui sont actuellement activées ou sous licence n'ont pas besoin d'être réactivées.

Déterminez quelles fonctionnalités facultatives (sous licence ou non) doivent être activées suite à cette mise à niveau. Vous activerez ces fonctions facultatives lorsque les processus système seront arrêtés.

Si les fonctionnalités sous licence doivent être activées suite à cette mise à niveau, contactez votre représentant local pour acheter la licence requise.

Fonctionnalités sous licence

La liste suivante répertorie brièvement les fonctionnalités sous licence disponibles avec la version 2.8.1/3.8.1/4.3.1

- EAS FIPS Code Filtering - Prise en charge des codes FIPS (Federal Information Processing Standards) pour filtrer le trafic de messages EAS
- DOCSIS DHCT Support - Prise en charge des DHCT (DOCSIS® Digital Home Communication Terminals)
- Enhanced VOD Session Throughput - Prise en charge des performances de session supérieures à deux sessions par seconde
- VOD Session Encryption - Prise en charge du cryptage de type session pour les sessions de vidéo à la demande (VOD)
- Distributed DNCS - Prise en charge de l'exécution du DNCS via un système RCS (Regional Control System)
- OpenCable Application Platform (OCAP™) - Prise en charge d'Open Cable Access Platform

La liste suivante contient certaines des fonctionnalités facultatives qui peuvent être activées par les ingénieurs des services Cisco sans licence spéciale. Toutes ces fonctionnalités ne concernent pas le logiciel que vous installez en utilisant ce guide. Consultez votre point de vente en Amérique du nord ou les services Cisco pour vérifier les fonctionnalités facultatives prises en charge par ce logiciel.

- Conditional Access Mode - Indique si le DNCS fournit un accès conditionnel PowerKEY ou non conditionnel non SA, tel qu'un NDS.
- DBDS Network Overlay - Autorise la prise en charge d'un DNCS pour assurer la transparence d'un système tiers dans un système SA
- SI Type to Use - Spécifie le type de système/d'informations de service (SI) que le système donné utilisera
- PID Mapping Mode - indique si l'ID de flux de transport (TSID) que le système utilisera est « Dynamic Unique » ou « Static non-Unique »
- PreAllocated Session Management - Prise en charge de la pré-allocation des sessions par le processus SRM (Shared Resource Manager) du DNCS
- Direct ASI - Permet au système de ne plus recourir au BIG (Broadband Integrated Gateway) pour transmettre des données BFS (Broadcast File System) aux modulateurs
- Third-Party Source - Prise en charge des sources SI tierces

  Remarque : Pour Plus d'informations, voir le bulletin technique *Program and System Information Protocol Configuration for System Releases 2.5, 2.7, 3.5, 3.7, 4.0, 4.2, and CV 3.4* (référence 4011319).
- Split Channels - Prise en charge des canaux split dans les mappages de canaux définis
- Multiflow Multicast - Prise en charge de la fonctionnalité Multiflow Multicast pour utiliser la fonctionnalité DSG (DOCSIS Settop Gateway) dans le DBDS
- SSP 2.4 Compliant - Prise en charge d'une demande de session interactive de serveur et d'une version de session interactive de serveur
- OOB Staging Bridge - Prise en charge de l'utilisation, dans le DBDS, d'un sous-ensemble de ponts hors bande dédiés à la préparation des DHCT
- Switched Digital Video - Prise en charge de la fonctionnalité SDV (Switched Digital Video)
- Trusted Domain - Prise en charge de la fonctionnalité MSO Trusted Domain, qui comprend la prise en charge du compte personnel (home account)
- Fixed Key Encryption - Prise en charge de l'utilisation de l'algorithme avec clé fixe à utiliser dans les tâches de cryptage
- DNO Encrypted VOD - Prise en charge de la VOD cryptée dans un environnement transparent
- OpenCAS PowerKEY Interface - Prise en charge d'une interface OpenCAS pour appliquer un cryptage PowerKEY à une session « en clair »

- Overlay Netcrypt Bulk Encryptor - Prise en charge de la fonctionnalité Netcrypt Bulk Encryptor
- Content Delivery Mode - Prise en charge de la fonctionnalité ISDS (IPTV Service Delivery System)
- Generic QAM Support - Prise en charge des QAM tiers pour permettre au DNCS/ISDS de gérer des sessions de diffusion et des sessions SVD et VOD
- Downloadable CAS - Prise en charge du sous-système d'accès conditionnel téléchargeable
- Open Cable MP3 Audio Support - Prise en charge du codage des messages audio EAS au format MP3 pour leur distribution sur le réseau TS
- SRM CAS PowerKEY Interface - Prise en charge d'une OCAI (Open Conditional Access Interface) de type RPC, par exemple URSM ou GSRM, ou d'une session externe et d'un gestionnaire de ressources compatible RPC OCAI.
- iGuide IPG Support - Active le proxy DREDD sur le DNCS/ISDS pour assurer la prise en charge des données IPG Macrovision iGuide

Vérifier l'intégrité des CD

Effectuez les opérations suivantes pour chaque CD figurant dans le classeur du logiciel.

Remarque : Vous vérifierez le CD de maintenance de DBDS dans une procédure distincte.

1. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le DNCS.
2. Effectuez les opérations suivantes pour vous connecter à la fenêtre d'émulation de terminal en tant qu'utilisateur **racine**.
   a. Saisissez **su -** et appuyez sur **Entrée**. Un message vous invitant à saisir un mot de passe s'affiche.
   b. Saisissez le mot de passe de l'utilisateur racine et appuyez sur **Entrée**.
3. Insérez un CD dans le lecteur de CD sur le DNCS.

   Remarque : Après avoir inséré le CD, si une fenêtre de gestionnaire de fichiers s'ouvre, fermez cette fenêtre.
4. Saisissez la commande suivante et appuyez sur **Entrée**. Le répertoire /cdrom/cdrom0 devient le répertoire de travail.

   ```
   cd /cdrom/cdrom0
   ```
5. Saisissez la commande suivante et appuyez sur **Entrée**. Le système répertorie le contenu du CD.

   ```
   ls -la
   ```
6. Le système a -t-il répertorié le contenu du CD comme prévu ?
   - Si **c'est le cas**, passez à l'étape 7.
   - Si **ce n'est pas le cas**, le CD est peut-être défectueux. Appelez les services Cisco pour obtenir de l'aide.
7. Saisissez la commande suivante et appuyez sur **Entrée**. Le système répertorie le contenu du CD.

   ```
   pkgchk -d . SAI*
   ```

   Important : N'oubliez pas de saisir le point entre **-d** et **SAI***.

   Résultats :
   - Le système vérifie sur le CD chaque progiciel qui commence par SAI.
   - Le système effectue un total de contrôle sur chaque progiciel et vérifie que le total de contrôle correspond au contenu de la liste des progiciels.
   - Le système répertorie les résultats de la vérification des progiciels.

   Remarque : Le système peut énumérer certains avertissements. Ils sont normaux, n'en tenez donc pas compte. Le système répertorie clairement les erreurs trouvées dans la vérification des progiciels.

8 La vérification des progiciels a-t-elle révélé des erreurs ?
   - Si **c'est le cas**, contactez les services Cisco.
     Important : *N'effectuez pas*la mise à niveau si le CD contient des erreurs.
   - Si **ce n'est pas le cas**, procédez comme suit :
     a Saisissez **cd /** puis appuyez sur **Entrée**.
     b Saisissez **eject cdrom** puis appuyez sur **Entrée**.

9 Répétez les étapes 3 à 8 pour chaque CD contenu dans le classeur du logiciel.

Vérifier l'intégrité du CD de maintenance de DBDS

Effectuez les opérations suivantes pour vérifier l'intégrité du CD de maintenance de DBDS.

1 sérez le CD de maintenance de DBDS dans le lecteur CD du DNCS.

Remarque : Après avoir inséré le CD, si une fenêtre de gestionnaire de fichiers s'ouvre, fermez cette fenêtre.

2 Saisissez la commande suivante et appuyez sur **Entrée**. Le répertoire /cdrom/cdrom0 devient le répertoire de travail.

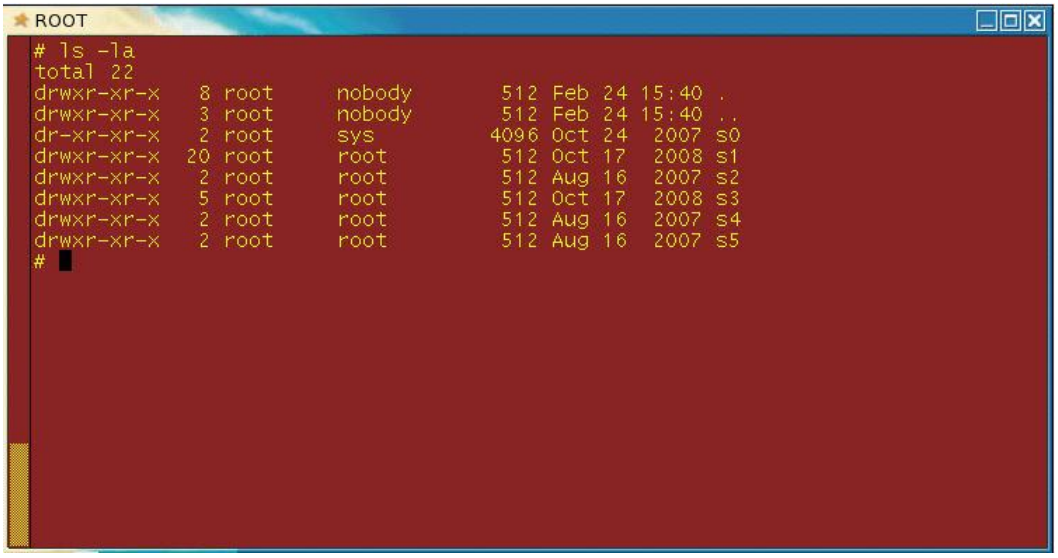
```
cd /cdrom/cdrom0
```

3 Saisissez la commande suivante et appuyez sur **Entrée**.

```
ls -la
```

Résultat : Le système affiche le contenu du CD, qui doit être similaire à l'exemple qui suit.

Exemple :



4 Les résultats de l'étape 3 sont-ils similaires à l'exemple ?

- Si **c'est le cas**, effectuez les opérations suivantes :
  - **a** Saisissez **cd /** puis appuyez sur **Entrée**.
  - **b** Saisissez **eject cdrom** puis appuyez sur **Entrée**.
- Si **ce n'est pas le cas**, contactez les services Cisco.

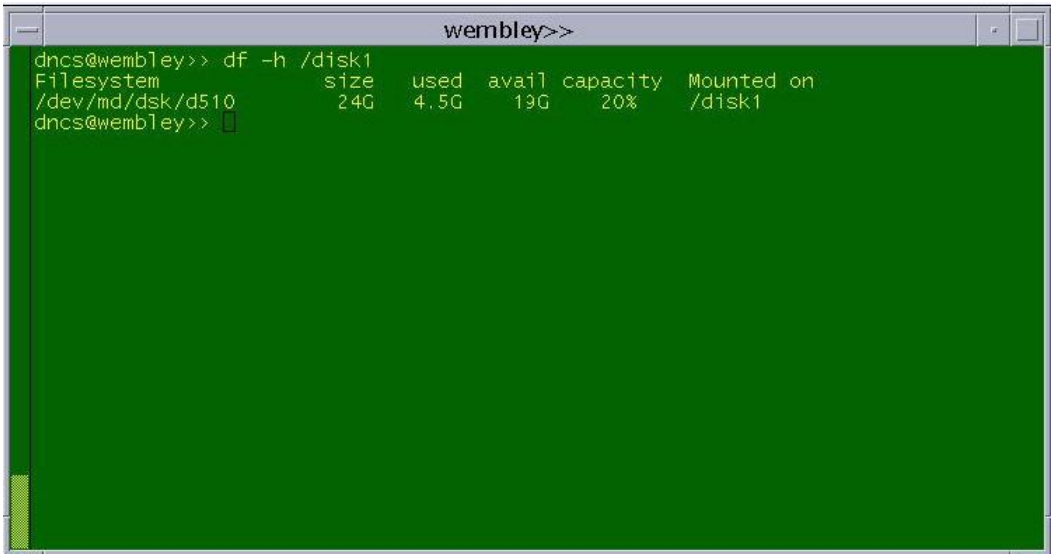
Vérifier l'espace disque libre

Nous vous recommandons de disposer d'un espace libre d'au moins 700 Mo sur le système de fichiers /disk1 pour installer la mise à niveau. Cette procédure comporte les instructions de vérification de l'espace disque libre sur le DNCS.

Vérification de l'espace disque libre

1 Dans une fenêtre d'émulation de terminal du DNCS, saisissez la commande suivante et appuyez sur **Entrée**. Le système affiche la quantité d'espace utilisé et d'espace libre sur le système de fichiers /disk1.

```
df -h  /disk1
```



2 La colonne **avail** affiche-t-elle au moins 700 Mo d'espace disque libre ?
   - Si **c'est le cas**, allez à ***Exécuter Doctor Report*** (à la page 12). Vous avez suffisamment d'espace pour effectuer la mise à niveau.
   - Si **ce n'est pas le cas**, appelez les services Cisco. Les ingénieurs des services Cisco peuvent vous conseiller sur les procédures à suivre pour nettoyer le disque.

Exécuter Doctor Report

Avant de mettre à niveau le DNCS vers la version 2.8.1/3.8.1/4.3.1, exécutez Doctor Report en tant qu'utilisateur **dncs**. Utilisez les instructions fournies dans *DBDS Utilities Version 6.3 Installation Instructions and User Guide* (référence 4031374). Doctor Report fournit des données de base de configuration système qui sont très utiles avant de commencer la mise à niveau.

Remarque : Sur un système traditionnel, l'exécution de Doctor Report prend 10 minutes.

Analyser le rapport de Doctor Report

Lorsque vous analysez le rapport de Doctor Report, assurez-vous qu'aucune partition de disque ne dépasse 85 % de sa capacité. Contactez les services Cisco si ce rapport révèle qu'une partition de disque dépasse 85 % de sa capacité.

Analysez également la sortie du rapport de Doctor Report pour vérifier que la valeur de la variable SI_INSERT_RATE d'intra-bande *n'est pas* supérieure à zéro (0). Si l'intra-bande SI_INSERT_RATE est supérieure à zéro (0), consultez *Recommendation for Setting System Information to Out-of-Band* (référence 738143), puis suivez les procédures proposées pour désactiver l'intra-bande SI.

Remarque : Si l'intra-bande SI est désactivée, la valeur du SI_INSERT_RATE est égale à 0.

Important : *Ne passez pas* à la procédure suivante avant d'avoir terminé d'exécuter et d'analyser le rapport de Doctor Report et d'avoir résolu les problèmes qu'il a signalés.

Examiner les périphériques mis en miroir

Avant de désactiver les fonctions de mise en miroir des disques lors de la préparation d4une mise à niveau, vous devez examiner l'état des disques mis en miroir présents sur le système. Toutes les fonctions de mise en miroir des disques doivent fonctionner normalement avant de procéder à la mise à niveau.

ATTENTION :
Si les fonctions de mise en miroir des disques du DNCS ne fonctionnent pas correctement avant la mise à niveau, vous ne pourrez peut-être pas procéder facilement à une récupération en cas d'échec de la mise à niveau.

Examen des périphériques mis en miroir

Effectuez les opérations suivantes pour examiner l'état des disques mis en miroir sur le DNCS.

1. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le DNCS.
2. Saisissez la commande suivante et appuyez sur **Entrée**. Le système affiche l'état de tous les métapériphériques présents sur le DNCS.

   ```
   metastat -c
   ```

   Remarque : Appuyez si nécessaire sur la **barre d'espacement** pour faire défiler toute la sortie.
3. Vérifiez tous les périphériques pour lesquels le système signale un besoin de maintenance.
4. Des périphériques ont-ils besoin d'une maintenance ?
   - Si **c'est le cas**, appelez les services Cisco pour qu'ils vous aident à résoudre vos problèmes de métapériphériques.
   - Si **ce n'est pas le cas**, passez à la procédure suivante indiquée dans ce chapitre.

Vérifier la stabilité de DBDS

1. Effectuez les opérations suivantes pour exécuter un démarrage lent et un démarrage rapide sur un DHCT avec un chemin de retour en fonctionnement (mode bidirectionnel).
   - **a** Démarrez un DHCT.

     Remarque : *N'appuyez pas* sur le bouton d'alimentation.
   - **b** Accédez à l'écran de diagnostic d'état de l'auto-test de mise sous tension et du démarrage sur le DHCT et vérifiez que tous les paramètres, sauf UNcfg, affichent **Ready**. UNcfg affiche **Broadcast**

     Remarque : Le renseignement des champs de cet écran peut prendre jusqu'à 2 minutes.
   - **c** Appuyez sur le bouton d'**alimentation** du DHCT pour le mettre sous tension et établissez une connexion réseau bidirectionnelle.
   - **d** Accédez à l'écran de diagnostic d'état de l'auto-test de mise sous tension et du démarrage sur le DHCT et vérifiez que tous les paramètres, notamment UNcfg, affichent **Ready**.
2. Vérifiez que vous pouvez exécuter un ping à destination du DHCT test.
3. Préparez au moins un nouveau DHCT. Après avoir préparé le DHCT, vérifiez les éléments suivants :
   - Le DHCT a chargé la version du logiciel client actuelle.
   - Le DHCT a reçu au moins 33 EMM (Entitlement Management Messages).
   - Le DHCT a reçu correctement son Entitlement Agent.
4. Vérifiez que le Guide interactif des programmes (IPG, Interactive Program Guide) affiche 7 jours de données valides et exactes.
5. Vérifiez que les chaînes invitation avec paiement à la séance s'affichent correctement sur les chaînes PPV (Partner Program View).
6. Vérifiez que toutes les applications tierces sont chargées et qu'elles fonctionnent correctement.
7. Vérifiez que vous pouvez acheter un programme VOD et/ou xOD.
8. Vérifiez que les chaînes SDV sont disponibles.

Obtenir la configuration système

Effectuez les opérations suivantes pour obtenir les données de configuration système de base pour *à la fois* le DNCS et le serveur d'applications. Vous pouvez avoir besoin d'une part de ces informations dans une phase ultérieure de la mise à niveau.

1. Dans une fenêtre d'émulation de terminal du DNCS, saisissez la commande suivante et appuyez sur **Entrée**. Une liste d'adresses IP (Internet Protocol) et de noms d'hôte s'affiche.

   ```
   more /etc/hosts
   ```

2. Prenez une feuille de papier et notez les adresses IP des hôtes figurant dans le fichier /etc/hosts.

   Important : Notez au moins les adresses IP des hôtes suivants :

   - appservatm _____
   - dncsatm _____
   - dncseth _____
   - dncsted _____

3. Saisissez la commande suivante et appuyez sur **Entrée**. Le nom d'hôte du DNCS s'affiche.

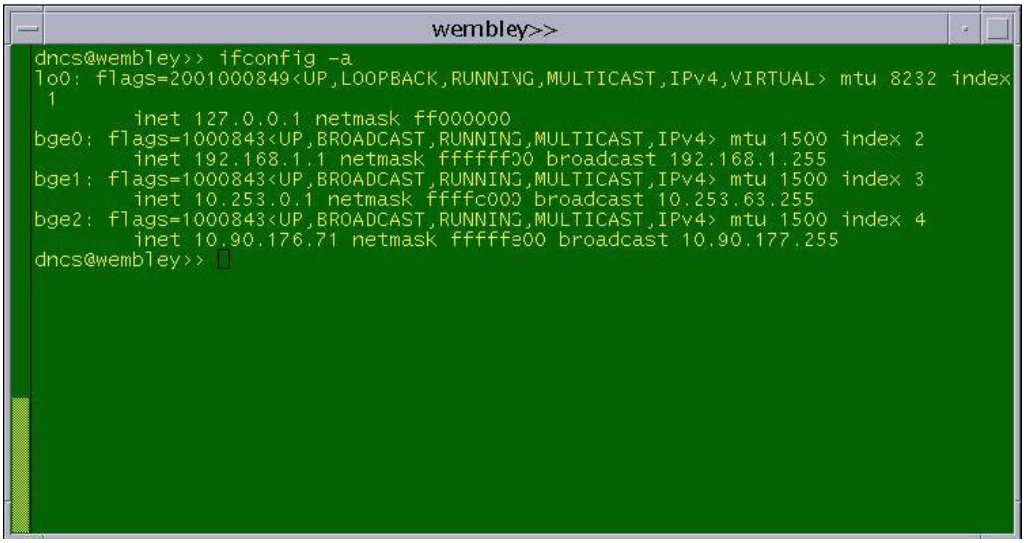
   ```
   uname  -n
   ```

   Important : Appelez les services Cisco si le nom d'hôte contient un point (.). Les ingénieurs des Services Cisco vous aideront à le remplacer par un nom d'hôte valide.

4. Notez le nom d'hôte du DNCS tel qu'il est affiché à l'étape 3 : _____

5. Saisissez la commande suivante et appuyez sur **Entrée** pour vérifier que les interfaces réseau ont été raccordées et configurées correctement. La sortie doit être similaire à l'exemple suivante :

   ```
   ifconfig -a
   ```



6 Dans une fenêtre d'émulation de terminal du serveur d'applications, saisissez la commande suivante et appuyez sur **Entrée**. Une liste d'adresses IP et de noms d'hôte s'affiche.

```
more  /etc/hosts
```

7 Notez les adresses IP et les noms d'hôtes des hôtes suivants :

- dncsatm _____
- appservatm (si appservatm ne correspond pas à 10.253.0.10) _____

8 Saisissez la commande suivante sur le serveur d'applications et appuyez sur **Entrée**. Le nom d'hôte du serveur d'applications s'affiche.

```
uname  -n
```

9 Notez le nom d'hôte du serveur d'applications tel qu'il est affiché à l'étape 8 :

_____

Collecter les informations réseau

Dans cette section, vous collectez les informations réseau requises pour reconstruire le système si la mise à niveau échoue.

1. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le DNCS.
2. Effectuez les opérations suivantes pour vous connecter à la fenêtre d'émulation de terminal en tant qu'utilisateur **racine**.
   - **a** Saisissez **su -** et appuyez sur **Entrée**. Un message vous invitant à saisir un mot de passe s'affiche.
   - **b** Saisissez le mot de passe de l'utilisateur racine et appuyez sur **Entrée**.
3. Saisissez **cd /export/home/dncs** puis appuyez sur **Entrée**. Le répertoire /export/home/dncs devient le répertoire de travail.
4. Saisissez **mkdir network.pre431** puis appuyez sur **Entrée**. Le système crée un répertoire appelé network.pre431.
5. Saisissez **cd network.pre431** puis appuyez sur **Entrée**. Le répertoire /export/home/dncs/network.pre431 devient le répertoire de travail.
6. Saisissez les commandes suivantes pour copier les fichiers nécessaires dans ce répertoire nouvellement créé.

   Important :
   - Appuyez sur **Entrée** après la saisie d'une commande.
   - Notez que certaines de ces commandes nécessitent un espace, suivi d'un point, après le corps de la commande.

   - **a** **cp -p /etc/hosts .**
   - **b** **cp -p /etc/hostname.* .**
   - **c** **cp -p /etc/inet/hosts inet.hosts**
   - **d** **cp -p /etc/netmasks .**
   - **e** **cp -p /etc/defaultrouter .**

     Remarque : Si ce fichier n'est pas présent, vous recevrez le message **cp : cannot access /etc/defaultrouter**. Dans ce cas, poursuivez avec la commande suivante.
   - **f** **cp -p /etc/defaultdomain .**

     Remarque : Si ce fichier n'est pas présent, vous recevrez le message **cp : cannot access /etc/defaultrouter**. Dans ce cas, poursuivez avec la commande suivante.
   - **g** **cp -p /etc/vfstab .**
   - **h** **cp -p /etc/nsswitch.conf .**
   - **i** **cp -p /etc/rc2.d/S82atminit .**
   - **j** **cp -p /etc/rc2.d/S85SAspecial .**
   - **k** **cp -p /etc/inet/ipnodes .**

l netstat -nrv > netstat.out

m ifconfig -a > ifconfig.out

n df -k > df.out

o eeprom nvramrc > nvramrc.out

7 Saisissez **cd /var/spool/cron** puis appuyez sur **Entrée**.

8 Saisissez **tar cvf crontabs.< date >.tar crontabs** puis appuyez sur **Entrée**.

Remarque : Remplacez < date > par la date actuelle.

Exemple : tar cvf crontabs.020107.tar crontabs

9 Saisissez **mv crontabs.< date >.tar /export/home/dncs/network.pre431** puis appuyez sur **Entrée**.

10 Saisissez **exit** puis appuyez sur **Entrée** pour vous déconnecter en tant qu'utilisateur racine.

11 Saisissez **cd /export/home/dncs/network.pre431** puis appuyez sur **Entrée**.

12 Saisissez **ls -ltr** puis appuyez sur **Entrée** pour vérifier que chaque fichier a été copié correctement dans le répertoire /export/home/dncs/network.pre431 et qu'aucun fichier n'a une taille égale à 0 (zéro).

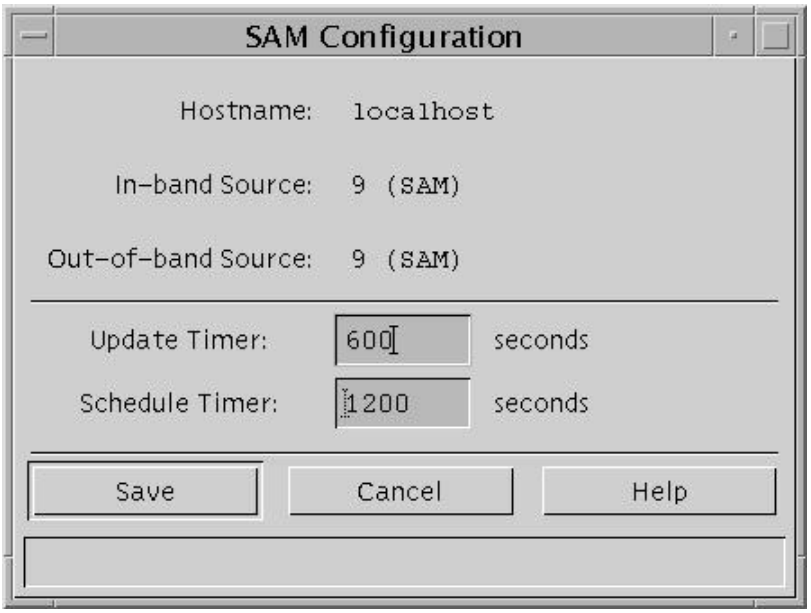
Remarque : Le "l" dans **ls** et **-ltr** correspond à la lettre L minuscule.

Vérifier les alarmes SAM

Suivez les instructions indiquées ci-après pour vérifier les champs **Update Timer** et **Schedule Timer** de la fenêtre de configuration SAM.

Important : La valeur conseillée par Cisco pour le champ **Update Timer** est 600. Celle conseillée pour **Schedule Timer** est 1200. Les valeurs actuellement définies sur le DNCS peuvent être différentes. N'effectuez aucune modification sans commencer par vérifier avec l'opérateur système.

1 Dans la console d'administration DNCS, sélectionnez l'onglet **Application Interface Modules** puis cliquez sur **SAM Config**. La fenêtre SAM Configuration s'ouvre.



2 Enregistrez ici la valeur actuelle du champ **Update Timer** : _____.
Remarque : Si vous modifiez cette valeur, enregistrez la nouvelle valeur ici : _____.

3 Enregistrez la valeur actuelle de **Schedule Timer** ici : _____.
Remarque : Si vous modifiez cette valeur, enregistrez la nouvelle valeur ici : _____.

4 Enregistrez les modifications que vous avez effectuées.

Vérifier le serveur CableCARD

Effectuez les opérations suivantes pour enregistrer les valeurs minimales des champs **Authorization Time-out Period** et **DeAuthorization Time-out Period** dans la fenêtre CableCARD Server.

1. Dans la console d'administration DNCS, sélectionnez l'onglet **DNCS**.
2. Sélectionnez l'onglet **Home Element Provisioning** puis cliquez sur **CableCARD**. L'écran CableCARD Data Summary s'ouvre.
3. Cliquez sur **Server Configuration**. L'écran CableCARD Data Summary se met à jour et affiche la partie Server Configuration de l'écran.
4. Suivez ces instructions pour enregistrer les paramètres spécifiques CableCARD.
   a. Dans l'espace ci-dessous, enregistrez la valeur du champ **Authorization Time-out Period**. _____
   b. Dans l'espace ci-dessous, enregistrez la valeur du champ **Authorization Time-out Period**. _____

   Remarque : Dans une procédure ultérieure, ***Configurer le serveur CableCARD*** (à la page 70), vous vérifierez que ces valeurs subsistent après la mise à niveau.
5. Cliquez sur **Exit** pour fermer la fenêtre active.
6. Cliquez sur **Exit all CableCARD Screens**.

Vérifier la configuration EAS - Pré-mise à niveau

Avant d'installer la version 2.8.1/3.8.1/4.3.1 du logiciel, vérifiez que votre équipement EAS fonctionne correctement en testant la capacité du système à transmettre des messages EAS. Suivez toutes les procédures indiquées au chapitre 5, **Testing the EAS** du guide *Configuring and Troubleshooting the Digital Emergency Alert System* (référence 4004455).

Lorsque vous avez terminé les procédures du chapitre 5, **Testing the EAS**, vérifiez que vous pouvez générer un message EAS pour l'EAC (Emergency Alert Controller) lui-même.

Vérifier les entrées profile

Vérifier la variable EAS

Effectuez les opérations suivantes pour ajouter la variable LOCAL_EAS_IP au fichier .profile.

1. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le DNCS.
2. Saisissez la commande suivante et appuyez sur **Entrée**. Le système recherche LOCAL_EAS_IP dans le fichier /export/home/dncs/.profile.

   ```
   grep -i LOCAL_EAS_IP /export/home/dncs/.profile
   ```

   Remarque : N'oubliez pas de saisir un espace entre grep –i LOCAL_EAS_IP et /export/home/dncs/.profile.
3. Les résultats de l'étape 2 indiquent-ils qu'il existe déjà une entrée pour LOCAL_EAS_IP dans /export/home/dncs/.profile ?
   - Si **c'est le cas**, passez à la procédure suivante indiquée dans ce chapitre.
   - Si **ce n'est pas le cas**, passez à l'étape 4.
4. Saisissez la commande suivante et appuyez sur **Entrée**. Le système affiche la valeur de la variable dncseth figurant dans le fichier /etc/hosts.

   ```
   cat /etc/hosts | grep dncseth
   ```
5. Saisissez la commande suivante et appuyez sur **Entrée**. Le système affiche la valeur de la variable eac figurant dans le fichier /etc/hosts.

   ```
   cat /etc/hosts | grep eac
   ```
6. Évaluez les résultats des étapes 4 et 5 pour déterminer si l'EAC se trouve sur le même réseau que le DNCS ou s'il se trouve sur un réseau différent. Pour cela, reportez-vous à l'exemple suivant :

Même réseau	**Réseau différent**
dncseth=192.168.2.1	dncseth=192.168.2.1
eac=192.168.1.5	eac=192.168.4.5

   Remarque : Lorsque le DNCS et l'EAC sont situés sur le même réseau, les trois premiers octets de l'adresse IP sont identiques. Ils sont situés sur des réseaux différents lorsque les trois premiers octets de l'adresse IP sont différents.
7. Le DNCS et l'EAC se trouvent-ils sur le même réseau ?
   - Si **c'est le cas**, passez à l'étape 11.
   - Si **ce n'est pas le cas** (ils sont situés sur des réseaux différents), passez à l'étape 8.
8. Utilisez un éditeur de texte pour ajouter la ligne suivante au fichier .profile :

   ```
   export LOCAL_EAS_IP=[Ethernet address of the DNCS]
   ```

   Remarque : Remplacez l'adresse Ethernet du DNCS dans [Ethernet address of the DNCS], qui est affichée à l'étape 4.

   Exemple : `LOCAL_EAS_IP=192.168.2.1`
9. Enregistrez et fermez le fichier.
10. Passez à la procédure suivante indiquée dans ce chapitre.
11. Saisissez **ifconfig -a** puis appuyez sur **Entrée**. Examinez la sortie et recherchez l'adresse IP du DNCS qui se trouve sur le même réseau que l'EAC.

    Remarque : Dans cet exemple, l'adresse IP de l'EAC (à partir de l'étape 6) est

192.168.4.5 ; l'adresse IP du DNCS qui se trouve sur le même réseau que l'EAC est 192.168.4.1.

Exemple :

```
hme0: flags=1000843< UP,BROADCAST,RUNNING,MULTICAST,IPv4 > mtu
1500 index 2
   inet 192.168.2.1 netmask ffffff00 broadcast 192.168.2.255
ci0: flags=1000842< BROADCAST,RUNNING,MULTICAST,IPv4 > mtu
9180 index 5
   inet 192.168.4.1 netmask ffffff00 broadcast
192.168.40.255
```

12 Utilisez un éditeur de texte pour ajouter la ligne suivante au fichier /export/home/dncs/.profile

```
export LOCAL_EAS_IP=[Ethernet address of the DNCS]
```

Remarque : Remplacez l'adresse Ethernet du DNCS dans [Ethernet address of the DNCS], qui est affichée à l'étape 11.

Exemple : `LOCAL_EAS_IP=192.168.4.1`

13 Enregistrez et fermez le fichier.

Vérifier les variables PSIP et SI_REGENERATION_TIME

La procédure suivante vérifie les variables PSIP_INSERT_RATE et SI_REGENERATION_TIME par rapport à leurs valeurs recommandées. Une brève explication de la raison pour laquelle vous vérifiez ces variables suit.

PSIP_INSERT_RATE

Si le site que vous mettez à niveau *n'utilise pas* le DNCS pour SIP et les messages EAS d'intra-bande qui sont destinés aux hôtes, tels que les TV tuner QAM, vous pouvez désactiver la distribution de ces messages par le DNCS en affectant 0 à la variable **PSIP_INSERT_RATE** dans le fichier .profile. Si vous n'utilisez pas le DNCS pour fournir ces messages, vous devez prendre des dispositions pour que ces signaux soient fournis par un autre équipement d'agrégation PSIP ou EAS présents dans votre système.

Important :

- Sachez qu'il existe des réglementations FCC concernant la fourniture de PSIP et EAS à ces périphériques.
- Si le DNCS est utilisé pour les messages PSIP et EAS d'intra-bande destinés aux hôtes, tels que les TV tuner QAM, la variable **PSIP_INSERT_RATE** ne doit pas figurer dans le fichier .profile. Si elle figure dans le fichier .profile, elle ne doit pas avoir la valeur 0.

SI_REGENERATION_TIME

La variable **SI_REGENERATION_TIME** figurant dans le fichier .profile doit avoir la valeur **1200** (20 minutes) pour que les mises à jour soient effectuées au plus une fois toutes les 20 minutes.

Effectuez les opérations suivantes pour vérifier les variables **PSIP_INSERT_RATE** et **SI_REGENERATION_TIME** du fichier.profile.

1. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le DNCS.
2. Saisissez la commande suivante et appuyez sur **Entrée** :
   ```
   grep PSIP_INSERT_RATE  /export/home/dncs/.profile
   ```
3. Les résultats de l'étape 2 indiquent-ils que la variable PSIP existe déjà dans le fichier .profile ?
   - Si **c'est le cas** et que le DNCS N'EST PAS utilisé pour le PSIP et l'EAS d'intra-bande destinés aux hôtes, passez à l'étape 4.
   - Si **ce n'est pas le cas** et que le DNCS N'EST PAS utilisé pour le PSIP et l'EAS d'intra-bande destinés aux hôtes, passez à l'étape 5.
   - Si **ce n'est pas le cas** et que le DNCS est utilisé pour le PSIP et l'EAS d'intra-bande destinés aux hôtes, passez à l'étape 8 ; aucune modification du fichier relative à la variable PSIP_INSERT_RATE n'est requise.
4. La variable **PSIP_INSERT_RATE** a-t-elle déjà la valeur **0** ?
   - Si **c'est le cas**, passez à l'étape 8 ; aucune modification du fichier .profile relative à la variable PSIP_INSERT_RATE n'est requise.
   - Si **ce n'est pas le cas**, passez à l'étape 5.
5. Ouvrez le fichier .profile avec un éditeur de texte.
6. La variable **PSIP_INSERT_RATE** figure-t-elle déjà dans le fichier ?
   - Si **c'est le cas**, affectez la valeur **0** à cette variable.
   - Si **ce n'est pas le cas**, ajoutez les entrées suivantes au bas du fichier :
     ```
     PSIP_INSERT_RATE=0
     export PSIP_INSERT_RATE
     ```
7. Enregistrez et fermez le fichier.
8. Dans la fenêtre d'émulation de terminal du DNCS, saisissez la commande suivante et appuyez sur **Entrée** :
   ```
   grep SI_REGENERATION_TIME  /export/home/dncs/.profile
   ```
9. Les résultats de l'étape 8 indiquent-ils que la variable **SI_REGENERATION_TIME** existe *et* qu'elle a la valeur **1200** ?
   - Si **c'est le cas** (dans les deux configurations), passez à la procédure suivante indiquée dans ce chapitre.
   - Si **ce n'est pas le cas**, passez à l'étape 10.
10. Ouvrez le fichier .profile avec un éditeur de texte.

11 Choisissez l'une des options suivantes :
   - Si la variable **SI_REGENERATION_TIME** ne figure pas encore dans le fichier .profile, ajoutez-la au fichier et affectez-lui la valeur **1200**.
   - Si la variable **SI_REGENERATION_TIME** figure dans le fichier .profile mais qu'elle est définie incorrectement, remplacez sa valeur par **1200**.

     Exemple : Lorsque vous avez terminé, votre entrée doit être :
     `SI_REGENERATION_TIME=1200`
12 Enregistrez et fermez le fichier.

Redémarrer le processus siManager

Si vous avez modifié les variables **PSIP_INSERT_RATE** ou **SI_REGENERATION_TIME** dans le fichier .profile, vous devez redémarrer le processus siManager du DNCS pour permettre au système de reconnaître ces modifications.

1 Lorsque vous avez suivi la procédure ***Vérifier les variables PSIP et SI_REGENERATION_TIME*** (à la page 23), avez -vous modifié le fichier .profile ?
   - Si **c'est le cas**, passez à l'étape 2.
   - Si **ce n'est pas le cas**, passez à la procédure suivante indiquée dans ce chapitre. Vous n'avez pas besoin de redémarrer le processus siManager.
2 Déconnectez-vous du DNCS.
3 Reconnectez-vous au DNCS en tant qu'utilisateur dncs. Les modifications que vous avez effectuées dans le fichier .profile sont désormais accessibles par le processus siManager.
4 Suivez les instructions ci-après pour arrêter le processus siManager.
   - **a** Sélectionnez **siManager** dans la fenêtre DNCS Control.
   - **b** Cliquez sur **Process**.
   - **c** Sélectionnez **Stop Process**.
   - **d** Attendez que le voyant du processus siManager devienne rouge.
5 Suivez les instructions ci-après pour redémarrer le processus siManager.
   - **a** Sélectionnez **siManager** dans la fenêtre DNCS Control.
   - **b** Cliquez sur **Process**.
   - **c** Sélectionnez **Start Process**.
   - **d** Attendez que le voyant du processus siManager devienne vert.

Vérifier les sessions et les enregistrer

Vérifier les sessions BFS sur le BFS QAM ou GQAM

Effectuez les opérations suivantes pour vérifier le nombre de sessions BFS de pré-mise à niveau.

1. Suivez les instructions ci-après pour vérifier le nombre de sessions actives sur le BFS QAM et/ou GQAM.
   a. Appuyez sur le bouton **Options** sur la façade avant du modulateur jusqu'à ce que la valeur totale **Session Count** s'affiche. Enregistrez ici la valeur de **Session Count**. _____
   b. Appuyez à nouveau sur le bouton **Options** et enregistrez ici la valeur de **Program Count**. _____
2. Dans une fenêtre d'émulation de terminal du DNCS, saisissez la commande suivante et appuyez sur **Entrée** :
   `auditQam -query [IP address] [output port number]`
3. Enregistrez ici les résultats de l'étape 2 : _____
4. Saisissez la commande suivante et appuyez sur **Entrée**.
   `/opt/solHmux64/vpStatus -d /dev/Hmux0 -P 0`
5. Enregistrez ici la valeur de **Active Streams Count**. _____
6. Les résultats des étapes 1 à 5 indiquent-ils tous le même nombre de sessions ?
   - Si **c'est le cas**, passez à la procédure suivante indiquée dans ce chapitre.
   - Si **ce n'est pas le cas**, contactez les services Cisco pour obtenir de l'aide pour résoudre ce problème.

Sauvegarder les systèmes de fichiers DNCS et ceux du serveur d'applications

Effectuez maintenant une sauvegarde complète du système de fichiers. Les procédures de sauvegarde du système de fichiers sont présentées dans *DBDS Backup and Restore Procedures For SR 2.2 Through 4.3 User Guide* (référence 4013779). Les procédures de sauvegarde ont été modifiées. Ainsi, il n'est plus nécessaire d'arrêter le DNCS ou le serveur d'applications pour effectuer la sauvegarde. Si nécessaire, appelez les services Cisco pour obtenir un exemplaire des procédures de sauvegarde et de restauration indiquées ci-après.

Arrêter les processus dhctStatus, signonCount et cmd2000

Lors de la mise à niveau des sites, les DHCT peuvent parfois être en cours d'interrogation par l'utilitaire dhctStatus. En outre, l'utilitaire signonCount peut être actif dans la mémoire système. Nos ingénieurs ont détecté que les mises à niveau se déroulent mieux lorsque l'utilitaire dhctStatus n'interroge pas activement les DHCT et que les processus cmd2000 ne sont pas actifs dans la mémoire système. Les instructions indiquées dans ce chapitre contiennent les opérations à effectuer pour arrêter ces processus.

Arrêt de la tâche d'interrogation de l'utilitaire dhctStatus

Effectuez les opérations suivantes pour déterminer si l'utilitaire dhctStatus interroge actuellement activement les DHCT, puis arrêter cette tâche d'interrogation s'il y a lieu.

1. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le DNCS.
2. Saisissez **ps -ef | grep dhctStatus** puis appuyez sur **Entrée** pour déterminer si l'utilitaire dhctStatus est en cours de exécution.

   Exemple : (s'il est en cours d'exécution)

   ```
   dncs 12514 12449 0 13:50:27 pts/3 0:00 /bin/ksh
   /dvs/dncs/bin/dhctStatus
   dncs 12556 12514 0 13:50:28 pts/3 0:01 /usr/local/bin/perl
   /dvs/dncs/bin/DhctStatus/dhctStatus.pl
   dncs 12681 12632 0 13:50:54 pts/10 0:00 grep dhct
   ```

3. Les résultats de l'étape 2 indiquent-ils que l'utilitaire dhctStatus est en cours d'exécution ?
   - Si **c'est le cas**, saisissez **dhctStatus** et appuyez sur **Entrée** pour afficher le menu de dhctStatus.
   - Si **ce n'est pas le cas**, passez la suite de cette procédure.
4. Pour arrêter la tâche d'interrogation, procédez comme suit :
   - **a** Tapez **p** puis appuyez sur **Entrée**. Le système affiche un menu d'interrogation.
   - **b** Tapez **t** puis appuyez sur **Entrée**. Le système arrête l'opération d'interrogation.
   - **c** Pour retourner au menu principal, appuyez sur **Entrée**.
   - **d** Pour quitter le menu, appuyez sur **q** puis sur **Entrée**.

5 Saisissez **ps -ef | grep dhctStatus** puis appuyez sur **Entrée** pour déterminer si tous les processus sont arrêtés.

Exemple :

```
dncs 12514 12449 0 13:50:27 pts/3 0:00 /bin/ksh
/dvs/dncs/bin/dhctStatus
dncs 12556 12514 0 13:50:28 pts/3 0:01 /usr/local/bin/perl
/dvs/dncs/bin/DhctStatus/dhctStatus.pl
dncs 12681 12632 0 13:50:54 pts/10 0:00 grep dhct
```

6 Saisissez **kill -9 <ID_processus>** puis appuyez sur **Entrée** pour tous les ID de processus affichés à l'étape 5.

Exemple : kill -9 12449

Suppression de l'utilitaire signonCount de la mémoire système

1 Saisissez **ps -ef | grep signonCount** puis appuyez sur **Entrée**. La liste des processus DNCS et leurs ID de processus s'affichent à l'écran.

2 Les résultats de l'étape 1 indiquent-ils que l'utilitaire signonCount est en cours d'exécution ?

- Si **c'est le cas**, passez à l'étape 3.
- Si **ce n'est pas le cas**, ignorez la suite de la procédure.

3 Dans une fenêtre d'émulation de terminal, saisissez **signonCount uninstall** et appuyez sur **Entrée**.

Remarque : L'utilitaire n'est pas définitivement désinstallé ; il retournera dans la mémoire système la prochaine fois que vous l'exécuterez.

4 Saisissez **ps -ef | grep signonCount** puis appuyez sur **Entrée**. La liste des processus DNCS et leurs ID de processus s'affichent à l'écran.

5 Saisissez **kill -9 [ID_processus]>** puis appuyez sur **Entrée** pour tous les ID de processus affichés à l'étape 4.

Remarque : Les ID de processus à supprimer sont localisés en commençant par la deuxième colonne de la sortie de l'étape 4.

6 Saisissez **ps -ef | grep signonCount** puis appuyez sur **Entrée** pour vérifier que tous les processus sont arrêtés.

7 Répétez les étapes 5 et 6 pour tous les processus qui continuent à s'afficher comme actifs. Le système doit uniquement afficher le processus grep.

Arrêt des processus cmd2000

1. Saisissez **ps -ef | grep cmd2000** puis appuyez sur **Entrée**. Le système affiche la liste des processus cmd2000 et leurs ID de processus.
2. Des processus cmd2000 fonctionnent-ils ?
   - Si **c'est le cas**, saisissez **kill -9 < ID_processus >** puis appuyez sur **Entrée** pour tous les processus cmd2000 en cours d'exécution ; passez ensuite à l'étape 3.
   - Si **ce n'est pas le cas**, passez à la procédure suivante indiquée dans ce chapitre.
3. Saisissez **ps -ef | grep cmd2000** puis appuyez sur **Entrée** pour vérifier que tous les processus cmd2000 ont été arrêtés.

   Remarque : Répétez les étapes 2 et 3 pour tous les processus cmd2000 restés actifs.

Sauvegarder les différents fichiers de données

Nos ingénieurs vous recommandent de sauvegarder sur bande les données des fichiers signonCount.out et signonCount.fixrpt, ainsi que celles du répertoire dhctStatus2. Vous pouvez ensuite vous référer à ces données et vous en servir pour le dépannage si des problèmes surviennent avec le système après la mise à niveau. Les instructions fournies dans cette section vous guident dans les opérations de sauvegarde de ces fichiers.

Sauvegarde de différents répertoires de données

Suivez les instructions de sauvegarde des fichiers signonCount.out et signonCount.fixrpt, et des données du répertoire dhctStatus2.

1. Marquez une bande en indiquant la date et le nom suivant :
   signonCount / dhctStatus2 Backups
2. Insérez la bande dans le lecteur de bande du DNCS.
3. Dans une fenêtre d'émulation de terminal, saisissez **tar cvf [nom du périphérique] /dvs/dncs/tmp/signonCount.out /dvs/dncs/tmp/signonCount.fixrpt /dvs/dncs/tmp/dhctStatus2** puis appuyez sur **Entrée**. Le système sauvegarde les fichiers spécifiés.

   Remarque : Remplacez le nom de périphérique du lecteur de bande du DNCS par [nom du périphérique].

   Exemple : tar cvf /dev/rmt/0h /dvs/dncs/tmp/signonCount.out /dvs/dncs/tmp/signonCount.fixrpt /dvs/dncs/tmp/dhctStatus2
4. Lorsque la sauvegarde est terminée, éjectez la bande et stockez-la dans un endroit sûr.

Sauvegarder le fichier copyControlParams et le supprimer

Effectuez les opérations suivantes pour sauvegarder le fichier copyControlParams.inf et le supprimer du DNCS. Pendant la mise à niveau, le système recrée le fichier copyControlParams.inf avec les valeurs par défaut appropriées. Vous pouvez ajouter à nouveau des entrées personnalisées au fichier après la mise à niveau.

1. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le DNCS.
2. Saisissez **cd /export/home/dncs** puis appuyez sur **Entrée**. Le répertoire /export/home/dncs devient le répertoire de travail.
3. Le fichier copyControlParams.inf a-t-il des entrées personnalisées ?
   - Si **c'est le cas**, saisissez **cp copyControlParams.inf copyControlParams.inf.bak** puis appuyez sur **Entrée**. Le système réalise une copie de sauvegarde du fichier copyControlParams.inf.
   - Si **ce n'est pas le cas**, passez à l'étape 4.
4. Saisissez **rm copyControlParams.inf** puis appuyez sur **Entrée**. Le système supprime le fichier copyControlParams.inf.

   Remarque : Lorsque vous redémarrez le DNCS après la mise à niveau, le système note l'absence du fichier copyControlParams.inf et en crée un nouveau.

   Important : Après la mise à niveau, utilisez la copie de sauvegarde du fichier copyControlParams.inf comme référence pour ajouter toutes les entrées personnalisées au nouveau fichier.

2

Procédures de mise à niveau de la version 2.8.1/3.8.1/4.3.1

Introduction

Dans ce chapitre, vous allez installer la version 2.8.1/3.8.1/4.3.1. La version 2.8.1/3.8.1/4.3.1 comprend un nouveau logiciel pour le DNCS, ainsi que pour les interfaces utilisateur graphiques Web (GUI et WUI) du DNCS.

Important : Ne tentez pas d'effectuer plusieurs fois les procédures présentées dans ce chapitre. Si vous rencontrez des problèmes lors de la mise à niveau du DNCS ou du serveur d'applications vers la version 2.8.1/3.8.1/4.3.1, contactez les services Cisco au 1-866-787-3866.

Dans ce chapitre

Interrompre les interfaces de facturation et les interfaces tierces

Remarque importante concernant la période d'entretien

ATTENTION :

Assurez -vous que vous êtes dans une période d'entretien lorsque vous commencez cette procédure. Vous resterez dans la période d'entretien tant que vous effectuerez l'installation. Les procédures postérieures à la mise à niveau peuvent être réalisées le jour suivant la fin de l'installation.

Interruption des interfaces de facturation et des interfaces tierces

Avant d'installer ce logiciel, contactez votre fournisseur de facturation pour interrompre l'interface de facturation. En outre, suivez les instructions du fournisseur d'application tierce que vous avez reçues avant que la période d'entretien ne commence à arrêter les applications pendant le processus d'installation, ce qui concerne aussi les outils de surveillance en temps réel.

Arrêt du processus ippvReceiver

Suivez les instructions ci-après pour arrêter le processus ippvReceiver.

1. Dans la fenêtre DNCS Control, sélectionnez **ippvReceiver**.
2. Cliquez sur **Process**.
3. Cliquez sur **Stop Processes**. Le voyant des processus ippvReceiver passe du vert au rouge.

Arrêter les tâches cron

Arrêtez toutes les tâches cron qui s'exécutent actuellement sur le DNCS et le serveur d'applications. Cela garantit qu'aucune application ou aucun programme ne s'initialise au cours du processus d'installation. Suivez les instructions indiquées dans cette section pour arrêter toutes les tâches cron.

Remarque : Notez l'heure à laquelle vous arrêtez les tâches cron. Vous pouvez être amené à exécuter manuellement ces applications ou ces programmes une fois l'installation terminée.

Arrêt des tâches cron sur le DNCS

Effectuez les opérations suivantes pour arrêter les tâches cron sur le DNCS.

Remarque : Vous devez être connecté en tant qu'utilisateur racine à une fenêtre d'émulation de terminal sur le DNCS.

1. Saisissez **ps -ef | grep cron** puis appuyez sur **Entrée**. Le système répertorie les processus en cours d'exécution qui comprennent le mot cron.
2. Les résultats de l'étape 1 comprennent-ils **/usr/sbin/cron** ?
   - Si **c'est le cas**, saisissez **svcadm -v disable -s cron** puis appuyez sur **Entrée**.
   - Si **ce n'est pas le cas**, allez à **Arrêt des tâches cron sur le serveur d'applications** ; les tâches cron sont déjà arrêtées sur le DNCS.
3. Vérifiez que les tâches cron sont arrêtées en saisissant à nouveau **ps -ef | grep cron** puis en appuyant sur **Entrée**. Le système ne doit répertorier que le processus grep.

Arrêt des tâches cron sur le serveur d'applications

Effectuez les opérations suivantes pour arrêter les tâches cron sur le serveur d'applications.

Remarque : Vous devez être connecté en tant qu'utilisateur racine à une fenêtre d'émulation de terminal du serveur d'applications.

1. Saisissez **ps -ef | grep cron** puis appuyez sur **Entrée**. Le système répertorie les processus en cours d'exécution qui comprennent le mot "cron".
2. Les résultats de l'étape 1 comprennent-ils **/usr/sbin/cron** ?
   - Si **c'est le cas**, saisissez **svcadm -v disable -s cron** puis appuyez sur **Entrée**.
   - Si **ce n'est pas le cas**, les tâches cron sont déjà arrêtées sur le serveur d'applications ; allez à la procédure suivante indiquée dans ce chapitre.

Sauvegarder la base de données Informix

Sauvegarde de la base de données Informix

Cette procédure doit être exécutée aussi près que possible du démarrage de la période d'entretien, ce qui permet ainsi d'effectuer la sauvegarde avant d'entrer dans la période d'entretien. Suivez les procédures ci-après pour sauvegarder les bases de données du DNCS et du serveur d'applications.

Remarques :

- Les composants système peuvent fonctionner pendant la sauvegarde de la base de données Informix.
- La sauvegarde d'une base de données traditionnelle contenant à peu près 100 000 DHCT peut prendre jusqu'à 30 minutes.
- Si vous utilisez un lecteur DVD externe, remplacez *cdrom1* par *cdrom0*.

1. Dans une fenêtre d'émulation de terminal, saisissez **df -n** puis appuyez sur **Entrée**. La liste des systèmes de fichiers montés s'affiche.

   Remarque : La présence de /cdrom dans la sortie confirme que le système a correctement monté le DVD.

2. Marquez votre bande de sauvegarde en indiquant les informations suivantes :

   [DNCS ou serveur d'applications] Sauvegarde de la base de données [jour de la semaine]

   [Nom du site]

   [Version logicielle]

   DVD SR 2.8.1/3.8.1/4.3.1] [version]

   [Bande n°]

   Remarques :

   - Personnalisez l'étiquette en y indiquant le jour de la semaine, le nom du site et la version logicielle du site que vous sauvegardez.
   - Si votre sauvegarde de base de données nécessite plusieurs bandes, n'oubliez pas de noter le numéro de la bande sur l'étiquette.

3. Insérez la bande dans le lecteur de bande du DNCS et attendez que le voyant vert cesse de clignoter.

   Important : Veillez à utiliser des bandes différentes pour chaque jour de la semaine.

4. Saisissez **. /dvs/dncs/bin/dncsSetup** puis appuyez sur **Entrée**. Le système établit l'environnement de l'utilisateur racine.

   Important : N'oubliez pas de saisir le point, suivi d'un espace, avant de saisir /dvs.

5 Choisissez l'une des options suivantes :
   - Si vous utilisez la configuration de lecteur de bande standard, procédez comme suit :
     a Saisissez **/cdrom/cdrom0/s3/backup_restore/backupDatabase -v** puis appuyez sur **Entrée**.

       Résultat : Le système affiche le message suivant :
       Please mount tape 1 on /dev/rmt/0h and then press Return to continue.

     b Passez à l'étape 6.
   - Si vous utilisez une configuration personnalisée de lecteur de bande, passez à l'étape 6.

6 Si vous utilisez une configuration personnalisée de lecteur de bande, saisissez **/cdrom/cdrom0/s3/backup_restore/backupDatabase -v -b [taille de bloc] -s [taille de bande]** puis appuyez sur **Entrée**.

   Remarque : Remplacez la taille de bloc et la taille de bande relatives à votre système par [taille de bloc] et [taille de bande].

   Exemple :
   /cdrom/cdrom0/s3/backup_restore/backupDatabase - v - b - 128 s 13212058

   Résultat : Le système affiche le message suivant :
   Please mount tape 1 on /dev/rmt/0h and then press Return to continue.

7 Appuyez sur **Entrée**. Le système sauvegarde votre base de données Informix.

   Remarques :
   - Le système vous invitera à insérer d'autres bandes si votre sauvegarde a besoin de plusieurs bandes.
   - Le message **Successfully completed the database backup** s'affiche la sauvegarde s'est terminée correctement.
   - Si la sauvegarde de la base de données n'a pas réussi, le système affiche un message d'erreur. Contactez les services Cisco au 1-866-787-3866 pour obtenir de l'aide pour résoudre le message d'erreur.

8 Retirez les bandes et stockez-les dans un endroit sûr.

Arrêter les serveurs de sauvegarde de base ou de sauvegarde automatique

i le site que vous mettez à niveau utilise le serveur de sauvegarde de base ou de sauvegarde automatique et que ce serveur est configuré pour démarrer une sauvegarde pendant la période d'entretien, désactivez cette sauvegarde ou reprogrammez-la après la période d'entretien.

Arrêter les composants système

Avant de poursuivre l'installation de la version 2.8.1/3.8.1/4.3.1, suivez les instructions indiquées dans cette section pour arrêter le serveur d'applications et le DNCS.

Important : Vous devez être dans une période d'entretien lorsque vous effectuez cette procédure et les autres procédures indiquées dans ce chapitre.

ATTENTION :
Ne continuez pas si vous N'ÊTES PAS dans la période d'entretien. Les procédures qui arrêtent les composants système interrompent les services.

Arrêter les serveurs tiers

Certains sites utilisent des périphériques qui montent des disques sur le DNCS ou le serveur d'applications. Ces périphériques sont généralement utilisés pour enregistrer des fichiers sur le BFS ou pour envoyer des transactions BOSS. Veillez à arrêter ces périphériques. De même, veillez à arrêter toutes les applications tierces.

Arrêt du serveur d'applications

Cette section présente les procédures à suivre pour arrêter un serveur SARA ou un serveur tiers. Choisissez la procédure qui concerne votre système.

Arrêt du serveur d'applications sur les sites SARA

1. Amenez le curseur sur le serveur d'applications, appuyez sur le bouton du milieu de la souris et sélectionnez **App Serv Stop**.
2. Dans une fenêtre d'émulation de terminal du serveur d'applications, saisissez **appControl** puis appuyez sur **Entrée**. La fenêtre Applications Control s'affiche.
3. Saisissez **2** (pour démarrer/arrêter un seul groupe d'éléments), puis appuyez sur **Entrée**. Le système affiche tous les processus du serveur d'applications.

   Remarque : Le système met à jour l'écran régulièrement, mais vous pouvez aussi appuyer sur **Entrée** pour forcer une mise à jour.
4. Lorsque le champ **Curr Stt** (État actuel) de la fenêtre Applications Control indique que tous les processus du serveur d'applications sont arrêtés, suivez les instructions affichées à l'écran pour fermer la fenêtre Applications Control.
5. Saisissez **appKill** puis appuyez sur Entrée.

Préparation du serveur d'applications Rovi

Consultez **Aptiv Technical Note Number 41**. Suivez les étapes 1 à 3 pour préparer le serveur d'applications Rovi à la mise à niveau du service pack.

Remarque : Contactez Rovi Corporation pour obtenir la dernière copie de la note technique.

Arrêt du DNCS

1. Amenez le curseur sur le DNCS, appuyez sur le bouton du milieu de la souris et sélectionnez **DNCS Stop**. Un message de confirmation s'affiche.
2. Cliquez sur **Yes**.
3. Dans une fenêtre d'émulation de terminal du DNCS, saisissez **dncsControl** puis appuyez sur **Entrée**. La fenêtre de l'utilitaire Dncs Control s'ouvre.
4. Saisissez **2** (pour démarrer/arrêter un seul groupe d'éléments), puis appuyez sur **Entrée**. Le système affiche tous les processus DNCS.

   Remarque : Le système met à jour l'écran régulièrement, mais vous pouvez aussi appuyer sur **Entrée** pour forcer une mise à jour.
5. Lorsque le champ **Curr Stt** (État actuel) de la fenêtre de l'utilitaire indique que tous les processus DCNS sont arrêtés, suivez les instructions affichées à l'écran pour fermer la fenêtre Dncs Control.

S'assurer qu'aucune session de base de données n'est active sur le DNCS

Suivez les instructions ci-après pour vous assurer qu'aucune session de base de données active n'est en cours d'exécution sur le DNCS.

Remarques :

- Vous devez être l'utilisateur racine pour exécuter certaines commandes indiquées dans cette procédure.
- Si vous avez suivi jusqu'ici les instructions, vous devez encore avoir une fenêtre d'émulation de terminal ouverte et y être connectée en tant qu'utilisateur **racine**.

1. Êtes -vous déjà connecté à une fenêtre d'émulation de terminal en tant qu'utilisateur **racine** ?
   - Si **c'est le cas**, passez à l'étape 2.
   - Si**ce n'est pas le cas**, connectez-vous à la fenêtre d'émulation de terminal en tant qu'utilisateur racine.
2. Saisissez **/dvs/dncs/bin/dncsSetup** puis appuyez sur **Entrée**. Le système établit l'environnement de l'utilisateur racine.

   Important : N'oubliez pas de saisir le point, suivi d'un espace, avant de saisir /dvs.
3. Saisissez **showActiveSessions** puis appuyez sur **Entrée**. L'un des messages suivants s'affiche :
   - Un message indiquant que l'INFORMIXSERVER est inactif
   - Un message répertoriant les sessions actives
4. Le message à l'étape 3 indique-t-il qu'il y a des sessions actives ?
   - Si **c'est le cas**, passez à l'étape 5.
   - Si **ce n'est pas le cas**, passez à l'étape 6.

5 Suivez les instructions ci-après pour supprimer les sessions actives.
   a Saisissez **killActiveSessions** puis appuyez sur **Entrée**. Le système supprime toutes les sessions actives de la base de données.
   b Saisissez à nouveau **showActiveSessions** puis appuyez sur **Entrée**.
   c Un message s'est-il affiché en indiquant qu'il existe des sessions actives ?
      – Si **c'est le cas**, contactez les services Cisco.
      – Si **ce n'est pas le cas**, passez à l'étape 6.
6 Saisissez **dncsKill/** puis appuyez sur **Entrée**. Le système arrête le processus dncsInitd s'il fonctionne toujours.
7 Attendez quelques instants puis saisissez **ps -ef | grep dncsInitd** et appuyez sur **Entrée**. Le système signale si le processus dncsInitd fonctionne toujours.
8 Le processus dncsInitd fonctionne-t-il toujours ?
   - Si **c'est le cas**, répétez les étapes 6 à 8.
   - Si **ce n'est pas le cas**, passez à l'étape 9.
9 Saisissez **clearDbSessions** et appuyez sur **Entrée**.

Déconnecter des disques en miroir sur le DNCS

Dans ***Examiner les périphériques en miroir*** (à la page 13), les sites vérifient que la fonction de mise en miroir des disques fonctionne correctement avant le début du processus de mise à niveau. Au cours de cette procédure vous désactivez désormais les fonctions de mise en miroir sur le DNCS pour assurer que le contenu du disque mis en miroir reflète les données et la configuration du DNCS avant d'effectuer une mise à niveau. Si la mise à niveau échoue pour une raison quelconque, vous pouvez alors permuter les emplacements des disques mis en miroir pour restaurer l'état de votre système tel qu'il était avant la tentative de mise à niveau.

Remarque : La désactivation de la mise en miroir des disques est généralement appelée déconnexion de la mise en miroir des disques.

Déconnexion des miroirs de disques sur le DNCS

Suivez les instructions ci-après pour déconnecter la fonction de mise en miroir des disques du DNCS Entreprise 450 ou Sun Fire V445, V880 ou V890.

Remarque : Vous devez encore être connecté en tant qu'utilisateur racine à une fenêtre d'émulation de terminal du DNCS.

1. Insérez le CD intitulé **DBDS Maintenance CD** dans le lecteur de CD-ROM du DNCS.
2. Saisissez **df -n/** puis appuyez sur **Entrée**. La liste des systèmes de fichiers montés s'affiche.

   Remarque : La présence de /cdrom dans la sortie confirme que le système a correctement monté le CD.
3. Saisissez **/cdrom/cdrom0/s3/backup_restore/mirrState -d** puis appuyez sur **Entrée**. Le système affiche le message suivant :

   WARNING!!
   Proceeding beyond this point will DETACH all d7xx submirrors.
   Are you certain you want to proceed?
4. Tapez **y** puis appuyez sur **Entrée**. Le système désactive les fonctions de mise en miroir sur le DNCS.
5. Saisissez **eject cdrom** puis appuyez sur **Entrée**. Le système éjecte le CD.

Installer le logiciel DNCS

Effectuez les opérations suivantes pour installer la version 2.8.1/3.8.1/4.3.1 du logiciel DNCS.

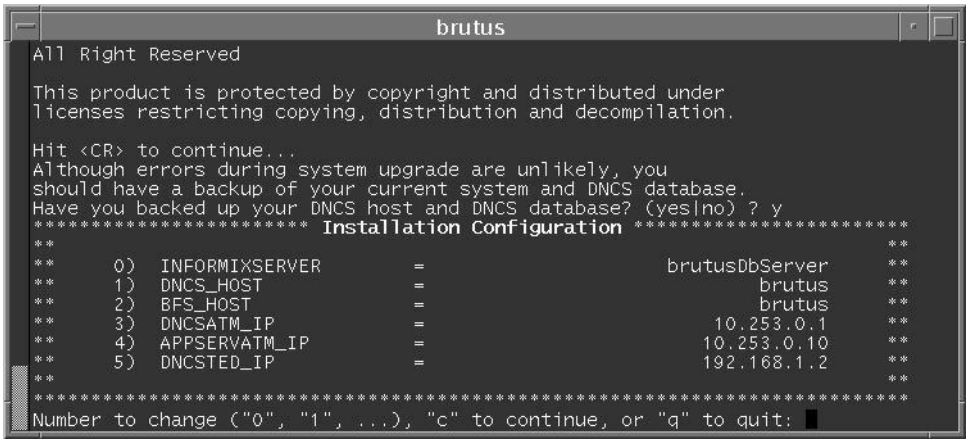
Remarques :

- Vous devez encore être connecté en tant qu'utilisateur racine à la fenêtre d'émulation de terminal du DNCS.
- L'installation du logiciel DNCS peut prendre 1 heure.

1. Insérez le CD portant un intitulé similaire à **DNCS Application x.x.x.x** dans le lecteur CD du DNCS. Le système monte automatiquement le CD dans /cdrom dans un délai de 30 secondes.
2. Saisissez **df -n/** puis appuyez sur **Entrée**. La liste des systèmes de fichiers montés s'affiche.

   Remarque : La présence de /cdrom dans la sortie confirme que le système a correctement monté le CD.
3. Saisissez **cd /cdrom/cdrom0** puis appuyez sur **Entrée**. Le répertoire /cdrom/cdrom0 devient le répertoire de travail.
4. Saisissez **install_pkg** puis appuyez sur **Entrée**. Un message de confirmation s'affiche.
5. Tapez **y** puis appuyez sur **Entrée**. Le système affiche un message **Press Enter to continue**.
6. Appuyez sur **Entrée**. Le système affiche un message qui demande si vous avez sauvegardé la base de données
7. Tapez **y** puis appuyez sur **Entrée**. Le système affiche un message qui vous demande de définir le nombre de jours jusqu'à la suppression des EMM du système.

   Remarque : Pour afficher la valeur actuelle utilisée par le système, saisissez **less /dvs/dncs/bin/CED.in** et appuyez sur **Entrée**.
8. Tapez **d** (pour la valeur par défaut), ou entrez un nombre entier valide représentant le nombre de jours, puis appuyez sur **Entrée**. Un message de confirmation s'affiche.
9. Tapez **y** puis appuyez sur **Entrée**. Le système répertorie certains paramètres de configuration des composants système et demande que vous confirmiez leur exactitude.



10 Reportez-vous aux notes que vous avez prises dans la section ***Obtenir la configuration système*** (à la page 15) du chapitre 1 et vérifiez que les paramètres de configuration sont répertoriés correctement ; appuyez ensuite sur **c** pour continuer. Le logiciel DNCS s'installe sur le DNCS.

Remarque : Si vous avez besoin de modifier un paramètre, suivez les instructions affichées à l'écran pour le faire. Vous aurez à modifier un paramètre seulement dans de rares cas.

11 Une fois la mise à niveau terminée, suivez les instructions ci-dessous pour éjecter le CD.

Saisissez **cd /** puis appuyez sur **Entrée**.

Saisissez **eject cdrom** puis appuyez sur **Entrée**.

12 Consultez les erreurs dans le fichier. Passez à la procédure suivante indiquée dans ce chapitre si le fichier journal indique que le logiciel DNCS s'est installé sans erreur.

Remarques :

- Le fichier journal d'installation se trouve dans le répertoire /var/sadm/system/logs du DNCS.
- Le fichier journal correspondant au logiciel DNCS s'appelle **SAIdncs_[n° de version]_install.log**.
- Contactez les services Cisco pour obtenir de l'aide si le fichier journal révèle des erreurs.

Installer les interfaces utilisateur graphique et Web

Effectuez les opérations suivantes pour installer les logiciels de l'interface utilisateur graphique et de l'interface Web DNCS version 2.8.1/3.8.1/4.3.1.

Remarque : L'installation des logiciels d'interface utilisateur graphique et d'interface Web DNCS ne prend pas plus de 15 minutes.

1. Insérez le CD portant un intitulé similaire à **DNCS GUI / WUI x.x.x.x** dans le lecteur de CD du DNCS. Le système monte automatiquement le CD dans /cdrom dans un délai de 30 secondes.
2. Saisissez **df -n/** puis appuyez sur **Entrée**. La liste des systèmes de fichiers montés s'affiche.

   Remarque : La présence de /cdrom dans la sortie confirme que le système a correctement monté le CD.
3. Saisissez **cd /cdrom/cdrom0** puis appuyez sur **Entrée**. Le répertoire /cdrom/cdrom0 devient le répertoire de travail.
4. Saisissez **install_pkg** puis appuyez sur **Entrée**. Un message de confirmation s'affiche.
5. Tapez **y** puis appuyez sur **Entrée**. Le logiciel s'installe sur le DNCS.
6. Une fois la mise à niveau terminée, suivez les instructions ci-dessous pour éjecter le CD.
   - **a** Saisissez **cd /** puis appuyez sur **Entrée**.
   - **b** Saisissez **eject cdrom** puis appuyez sur **Entrée**.
7. Consultez les erreurs dans le fichier. Allez à ***Installer d'autres logiciels*** (à la page 47) si le fichier journal indique que les logiciels d'interface utilisateur graphique et d'interface Web se sont installés sans erreur.

   Remarques :
   - Le fichier journal d'installation se trouve dans le répertoire /var/sadm/system/logs du DNCS.
   - Le fichier journal de l'interface utilisateur graphique DNCS s'appelle **SAIgui_[version #]_install.log**.
   - Le fichier journal de l'interface utilisateur Web DNCS s'appelle **SAIwebui_[version #]_install**.log.
   - Contactez les services Cisco pour obtenir de l'aide si le fichier journal révèle des erreurs.

Installer d'autres logiciels

Installez le logiciel version 4.3.1 suivant maintenant :

- DNCS Online Help 4.3.1.0
- Report Writer r1.0.0.3

Effectuez les opérations ci-après pour chaque CD de logiciel.

1. Insérez le CD dans le lecteur CD du DNCS. Le système monte automatiquement le CD dans /cdrom dans un délai de 30 secondes.
2. Saisissez **df -n/** puis appuyez sur **Entrée**. La liste des systèmes de fichiers montés s'affiche.

   Remarque : La présence de /cdrom dans la sortie confirme que le système a correctement monté le CD.
3. Saisissez **cd /cdrom/cdrom0** puis appuyez sur **Entrée**. Le répertoire /cdrom/cdrom0 devient le répertoire de travail.

   Remarque : La plupart des CD sont accompagnés d'un fichier readme (lisez-moi) que vous pouvez lire à ce stade.
4. Saisissez **install_pkg** puis appuyez sur **Entrée**. Un message de confirmation s'affiche.
5. Tapez **y** puis appuyez sur **Entrée**. Le logiciel s'installe sur le DNCS.
6. Une fois la mise à niveau terminée, suivez les instructions ci-dessous pour éjecter le CD.
   - **a** Saisissez **cd /** puis appuyez sur **Entrée**.
   - **b** Saisissez **eject cdrom** puis appuyez sur **Entrée**.
7. Consultez les erreurs dans le fichier journal approprié.

   Remarques :
   - Les fichiers journaux se trouvent dans le répertoire /var/sadm/system/logs du DNCS.
   - Contactez les services Cisco pour obtenir de l'aide si le fichier journal révèle des erreurs.

Logiciel patch

Installez le logiciel patch DNCS 4.3.1.6 p2 maintenant. Le CD de correctifs doit être accompagné d'un fichier readme (lisez -moi). Suivez les instructions indiquées dans le fichier README pour installer le logiciel patch.

Vérifier les composants installés de la version 2.8.1/3.8.1/4.3.1

Utilisez *pkginfo*, un outil de gestion des logiciels Solaris, pour vérifier les versions logicielles installées sur le DNCS et le serveur d'applications. Utilisez le champ **Version** et le champ **Status** de la sortie générée par *pkginfo* pour obtenir les informations dont vous avez besoin. Si le champ Status indique que le logiciel n'est pas complètement installé, contactez les services Cisco au 1-866-787-3866 pour obtenir de l'aide.

Remarque : L'exécution de Doctor Report avec l'option *–g* affiche aussi les versions logicielles installées. Si vous préférez, n'hésitez pas à obtenir ces informations dans Doctor Report.

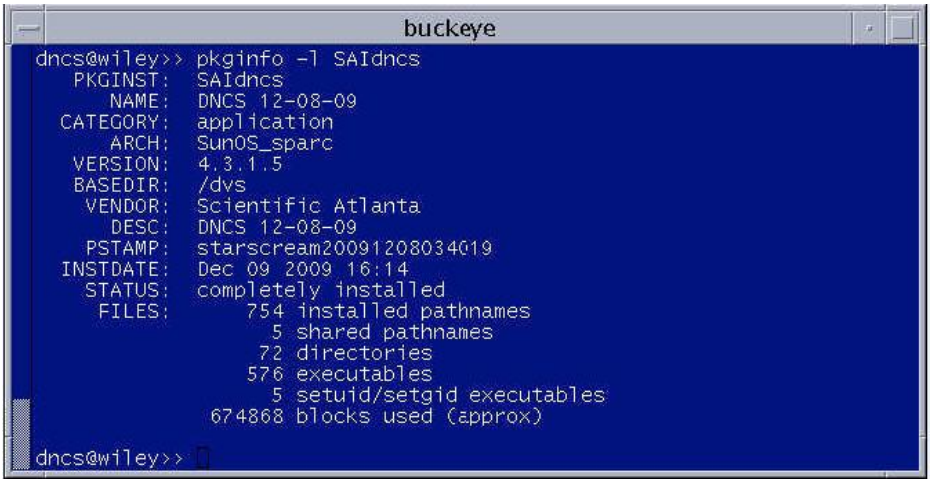
Vérification des versions du DNCS

Suivez les instructions ci-après pour vérifier les versions logicielles installées sur le DNCS.

1 Dans une fenêtre d'émulation de terminal, saisissez **pkginfo -l [nom du progiciel]** puis appuyez sur **Entrée**.

Remarques :

- -l correspond à la lettre L minuscule.
- Remplacez le composant logiciel que vous vérifiez par [nom du progiciel].
- Utilisez **SAIdncs** comme nom de progiciel lorsque vous exécutez cette procédure pour la première fois.



Exemple : Notez que le champ Version indique que DNCS version 4.3.1.x est installé sur le DNCS et que le champ Status indique que le logiciel est complètement installé.

2 Enregistrez le numéro de version figurant dans la colonne Actual Results du tableau fourni pour chaque progiciel que vous vérifiez.

Composant	Nom du progiciel	Résultats attendus	Résultats réels
Application DNCS	SAIdncs	4.3.1.6p2	
Interface utilisateur DNCS	SAIgui	4.3.1.6	
Interface Web DNCS	SAIwebui	4.3.1.6p2	
DNCS Online Help	SAIhelp	4.3.1.0	
DNCS Report Writer	SAIrptwrt	r1.0.0.3	

3 Répétez les étapes 1 et 2 pour chaque nom de progiciel figurant dans le tableau à l'étape 2.

4 Les trois premiers chiffres figurant dans le champ **Actual Results** correspondent-ils aux trois premiers chiffres figurant dans le champ **Expected Results** pour chaque composant contenu dans le tableau à l'étape 2 ?

- Si **c'est le cas**, passez à la procédure suivante indiquée dans ce chapitre.
- Si **ce n'est pas le cas**, appelez les services Cisco et informez-les de la différence.

Remarque : Le numéro de build (le quatrième chiffre du numéro de version) peut varier.

Activer les fonctionnalités facultatives et sous licence

Si vous avez bien suivi jusqu'ici toutes les instructions, les composants système doivent être arrêtés. Le moment est venu d'activer toutes les fonctionnalités facultatives ou sous licence qui concernent cette installation. Contactez les services Cisco pour activer toutes les fonctions facultatives ou sous licence.

Vérifier les entrées .profile

Vérifier la variable EAS

Effectuez les opérations suivantes pour ajouter la variable LOCAL_EAS_IP au fichier .profile.

1. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le DNCS.
2. Saisissez la commande suivante et appuyez sur **Entrée**. Le système recherche LOCAL_EAS_IP dans le fichier /export/home/dncs/.profile.

   ```
   grep -i LOCAL_EAS_IP /export/home/dncs/.profile
   ```

   Remarque : N'oubliez pas de saisir un espace entre grep –i LOCAL_EAS_IP et /export/home/dncs/.profile.
3. Les résultats de l'étape 2 indiquent-ils qu'il existe déjà une entrée pour LOCAL_EAS_IP dans /export/home/dncs/.profile ?
   - Si **c'est le cas**, passez à la procédure suivante indiquée dans ce chapitre.
   - Si **ce n'est pas le cas**, passez à l'étape 4.
4. Saisissez la commande suivante et appuyez sur **Entrée**. Le système affiche la valeur de la variable dncseth figurant dans le fichier /etc/hosts.

   ```
   cat /etc/hosts | grep dncseth
   ```
5. Saisissez la commande suivante et appuyez sur **Entrée**. Le système affiche la valeur de la variable eac figurant dans le fichier /etc/hosts.

   ```
   cat /etc/hosts | grep eac
   ```
6. Évaluez les résultats des étapes 4 et 5 pour déterminer si l'EAC se trouve sur le même réseau que le DNCS ou s'il se trouve sur un réseau différent. Pour cela, reportez-vous à l'exemple suivant :

Même réseau	**Réseau différent**
dncseth=192.168.2.1	dncseth=192.168.2.1
eac=192.168.1.5	eac=192.168.4.5

   Remarque : Lorsque le DNCS et l'EAC sont situés sur le même réseau, les trois premiers octets de l'adresse IP sont identiques. Ils sont situés sur des réseaux différents lorsque les trois premiers octets de l'adresse IP sont différents.
7. Le DNCS et l'EAC se trouvent-ils sur le même réseau ?
   - Si **c'est le cas**, passez à l'étape 11.
   - Si **ce n'est pas le cas** (ils sont situés sur des réseaux différents), passez à l'étape 8.
8. Utilisez un éditeur de texte pour ajouter la ligne suivante au fichier .profile :

   ```
   export LOCAL_EAS_IP=[Ethernet address of the DNCS]
   ```

   Remarque : Remplacez l'adresse Ethernet du DNCS dans [Ethernet address of the DNCS], qui est affichée à l'étape 4.

   Exemple : `LOCAL_EAS_IP=192.168.2.1`

9 Enregistrez et fermez le fichier.

10 Passez à la procédure suivante indiquée dans ce chapitre.

11 Saisissez **ifconfig -a** puis appuyez sur **Entrée**. Examinez la sortie et recherchez l'adresse IP du DNCS qui se trouve sur le même réseau que l'EAC.

Remarque : Dans cet exemple, l'adresse IP de l'EAC (à partir de l'étape 6) est 192.168.4.5 ; l'adresse IP du DNCS qui se trouve sur le même réseau que l'EAC est 192.168.4.1.

Exemple :

```
hme0: flags=1000843< UP,BROADCAST,RUNNING,MULTICAST,IPv4 > mtu
1500 index 2
   inet 192.168.2.1 netmask ffffff00 broadcast 192.168.2.255
ci0: flags=1000842< BROADCAST,RUNNING,MULTICAST,IPv4 > mtu
9180 index 5
   inet 192.168.4.1 netmask ffffff00 broadcast 192.168.40.255
```

12 Utilisez un éditeur de texte pour ajouter la ligne suivante au fichier /export/home/dncs/.profile

```
export LOCAL_EAS_IP=[Ethernet address of the DNCS]
```

Remarque : Remplacez l'adresse Ethernet du DNCS dans [Ethernet address of the DNCS], qui est affichée à l'étape 11.

Exemple : `LOCAL_EAS_IP=192.168.4.1`

13 Enregistrez et fermez le fichier.

Vérifier les variables PSIP et SI_REGENERATION_TIME

La procédure suivante vérifie les variables PSIP_INSERT_RATE et SI_REGENERATION_TIME par rapport à leurs valeurs recommandées. Une brève explication de la raison pour laquelle vous vérifiez ces variables suit.

PSIP_INSERT_RATE

Si le site que vous mettez à niveau *n'utilise pas* le DNCS pour SIP et les messages EAS d'intra-bande qui sont destinés aux hôtes, tels que les TV tuner QAM, vous pouvez désactiver la distribution de ces messages par le DNCS en affectant 0 à la variable **PSIP_INSERT_RATE** dans le fichier .profile. Si vous n'utilisez pas le DNCS pour fournir ces messages, vous devez prendre des dispositions pour que ces signaux soient fournis par un autre équipement d'agrégation PSIP ou EAS présents dans votre système.

Important :

- Sachez qu'il existe des réglementations FCC concernant la fourniture de PSIP et EAS à ces périphériques.
- Si le DNCS est utilisé pour les messages PSIP et EAS d'intra-bande destinés aux hôtes, tels que les TV tuner QAM, la variable **PSIP_INSERT_RATE** ne doit pas figurer dans le fichier .profile. Si elle figure dans le fichier .profile, elle ne doit pas avoir la valeur 0.

SI_REGENERATION_TIME

La variable **SI_REGENERATION_TIME** figurant dans le fichier .profile doit avoir la valeur **1200** (20 minutes) pour que les mises à jour soient effectuées au plus une fois toutes les 20 minutes.

Effectuez les opérations suivantes pour vérifier les variables **PSIP_INSERT_RATE** et **SI_REGENERATION_TIME** du fichier.profile.

1. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le DNCS.
2. Saisissez la commande suivante et appuyez sur **Entrée** :
   ```
   grep PSIP_INSERT_RATE  /export/home/dncs/.profile
   ```
3. Les résultats de l'étape 2 indiquent-ils que la variable PSIP existe déjà dans le fichier .profile ?
   - Si **c'est le cas** et que le DNCS N'EST PAS utilisé pour le PSIP et l'EAS d'intra-bande destinés aux hôtes, passez à l'étape 4.
   - Si **ce n'est pas le cas** et que le DNCS N'EST PAS utilisé pour le PSIP et l'EAS d'intra-bande destinés aux hôtes, passez à l'étape 5.
   - Si **ce n'est pas le cas** et que le DNCS est utilisé pour le PSIP et l'EAS d'intra-bande destinés aux hôtes, passez à l'étape 8 ; aucune modification du fichier relative à la variable PSIP_INSERT_RATE n'est requise.
4. La variable **PSIP_INSERT_RATE** a-t-elle déjà la valeur **0** ?
   - Si **c'est le cas**, passez à l'étape 8 ; aucune modification du fichier .profile relative à la variable PSIP_INSERT_RATE n'est requise.
   - Si **ce n'est pas le cas**, passez à l'étape 5.
5. Ouvrez le fichier .profile avec un éditeur de texte.
6. La variable **PSIP_INSERT_RATE** figure-t-elle déjà dans le fichier ?
   - Si **c'est le cas**, affectez la valeur **0** à cette variable.
   - Si **ce n'est pas le cas**, ajoutez les entrées suivantes au bas du fichier :
     ```
     PSIP_INSERT_RATE=0
     export PSIP_INSERT_RATE
     ```
7. Enregistrez et fermez le fichier.
8. Dans la fenêtre d'émulation de terminal du DNCS, saisissez la commande suivante et appuyez sur **Entrée** :
   ```
   grep SI_REGENERATION_TIME  /export/home/dncs/.profile
   ```
9. Les résultats de l'étape 8 indiquent-ils que la variable **SI_REGENERATION_TIME** existe *et* qu'elle a la valeur **1200** ?
   - Si **c'est le cas** (dans les deux configurations), passez à la procédure suivante indiquée dans ce chapitre.
   - Si **ce n'est pas le cas**, passez à l'étape 10.

10 Ouvrez le fichier .profile avec un éditeur de texte.

11 Choisissez l'une des options suivantes :

- Si la variable **SI_REGENERATION_TIME** ne figure pas encore dans le fichier .profile, ajoutez-la au fichier et affectez-lui la valeur **1200**.
- Si la variable **SI_REGENERATION_TIME** figure dans le fichier .profile mais qu'elle est définie incorrectement, remplacez sa valeur par **1200**.

  Exemple : Lorsque vous avez terminé, votre entrée doit être :
  `SI_REGENERATION_TIME=1200`

12 Enregistrez et fermez le fichier.

Redémarrer le processus siManager

Si vous avez modifié les variables **PSIP_INSERT_RATE** ou **SI_REGENERATION_TIME** dans le fichier .profile, vous devez redémarrer le processus siManager du DNCS pour permettre au système de reconnaître ces modifications.

1 Lorsque vous avez suivi la procédure ***Vérifier les variables PSIP et SI_REGENERATION_TIME*** (à la page 52), avez-vous modifié le fichier .profile ?

- Si **c'est le cas**, passez à l'étape 2.
- Si **ce n'est pas le cas**, passez à la procédure suivante indiquée dans ce chapitre. Vous n'avez pas besoin de redémarrer le processus siManager.

2 Déconnectez-vous du DNCS.

3 Reconnectez-vous au DNCS en tant qu'utilisateur dncs. Les modifications que vous avez effectuées dans le fichier .profile sont désormais accessibles par le processus siManager.

4 Suivez les instructions ci-après pour arrêter le processus siManager.

   a Sélectionnez **siManager** dans la fenêtre DNCS Control.

   b Cliquez sur **Process**.

   c Sélectionnez **Stop Process**.

   d Attendez que le voyant du processus siManager devienne rouge.

5 Suivez les instructions ci-après pour redémarrer le processus siManager.

   a Sélectionnez **siManager** dans la fenêtre DNCS Control.

   b Cliquez sur **Process**.

   c Sélectionnez **Start Process**.

   d Attendez que le voyant du processus siManager devienne vert.

Supprimer les scripts qui redémarrent le processus de transfert

Afin de résoudre certains problèmes liés au processus de transfert sur le DNCS, certains sites ont régulièrement redémarré ce processus via des scripts résidant dans le fichier crontab. La version 2.8.1/3.8.1/4.3.1 contient le logiciel qui vous permet de résoudre les problèmes liés au processus de transfert. Par conséquent, après la mise à niveau, vous devez supprimer toutes les entrées du fichier crontab qui font référence à des scripts qui redémarrent le processus de transfert. Les instructions fournies dans cette section vous guident tout au long du processus de suppression de ces références.

Remarques :

- Le processus de redémarrage d'un processus consiste à arrêter et redémarrer ce processus.
- Les scripts que Cisco a écrits pour redémarrer le processus de transfert s'appellent **elop.sh** et **bouncePassThru**.

Suppression des scripts qui redémarrent le processus de transfert

1. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le DNCS.
2. Suivez les instructions ci-après pour vérifier la présence de scripts dans le fichier crontab qui redémarrent le processus de transfert.
   a. Saisissez **crontab -l | grep -i elop.sh** puis appuyez sur **Entrée**. Le système répertorie les lignes contenues dans le fichier crontab qui contiennent elop.ksh.
   b. Saisissez **crontab -l | grep -i bouncePassThru** puis appuyez sur **Entrée**. Le système répertorie les lignes contenues dans le fichier crontab qui contiennent bouncePassThru.
3. Le résultat de l'étape 2 contient-il des références aux scripts elop.sh ou bouncePassThru ?
   - Si **c'est le cas**, passez à l'étape 4 pour supprimer ces références.
   - Si **ce n'est pas le cas**, passez à la procédure suivante indiquée dans ce chapitre.

     Remarque : Il n'est pas nécessaire de supprimer les références aux scripts dans le fichier crontab.
4. Saisissez **crontab -l > /tmp/dncs.crontab** puis appuyez sur **Entrée**. Le système redirige le contenu du fichier crontab dans dncs.crontab.

   Remarque : Alors que vous pouvez modifier le fichier crontab directement, nous vous recommandons de commencer par rediriger le contenu de ce fichier dans dncs.crontab pour vous permettre de récupérer le fichier crontab initial en cas de besoin.
5. Saisissez **vi /tmp/dncs.crontab** puis appuyez sur **Entrée**. Le fichier dncs.crontab s'ouvre et vous pouvez le modifier avec l'éditeur de texte vi.

6. Supprimez toutes les lignes du fichier dncs.crontab qui font référence aux scripts elop.ksh ou bouncePassThru.
7. Enregistrez le fichier dncs.crontab et fermez l'éditeur de texte vi.
8. Saisissez **crontab /tmp/dncs.crontab** puis appuyez sur **Entrée**. Le fichier dncs.crontab que vous venez de modifier devient le fichier crontab.

Redémarrer le DNCS et le serveur d'applications

Après avoir installé le logiciel sur le DNCS, procédez comme suit pour redémarrer le DNCS et le serveur d'applications.

1. Choisissez l'une des options suivantes :
   - Si vous utilisez un serveur d'applications Cisco, ouvrez une fenêtre d'émulation de terminal (si nécessaire) sur le serveur d'applications.
   - Si vous utilisez un serveur d'applications Rovi Corporation, passez à l'étape 4.
2. Effectuez les opérations suivantes pour vous connecter à la fenêtre d'émulation de terminal en tant qu'utilisateur **racine**.
   - **a** Saisissez **su -** et appuyez sur **Entrée**. Un message vous invitant à saisir un mot de passe s'affiche.
   - **b** Saisissez le mot de passe de l'utilisateur racine et appuyez sur **Entrée**.
3. Dans la fenêtre d'émulation de terminal du serveur d'applications, saisissez **/usr/sbin/shutdown -g0 -y -i0** et appuyez sur **Entrée**. Le serveur d'applications s'arrête.
4. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le DNCS.
5. Effectuez les opérations suivantes pour vous connecter à la fenêtre d'émulation de terminal en tant qu'utilisateur **racine**.
   - **a** Saisissez **su -** et appuyez sur **Entrée**. Un message vous invitant à saisir un mot de passe s'affiche.
   - **b** Saisissez le mot de passe de l'utilisateur racine et appuyez sur **Entrée**.
6. Dans la fenêtre d'émulation de terminal du DNCS, saisissez **/usr/sbin/shutdown -g0 -y -i6** et appuyez sur **Entrée**. Le DNCS redémarre et la fenêtre de connexion CDE (Common Desktop Environment) s'ouvre.
7. Connectez-vous au DNCS en tant qu'utilisateur **dncs**.
8. À l'invite **ok** sur le serveur d'application Cisco, saisissez **boot** puis appuyez sur **Entrée**. Le serveur d'applications redémarre.
9. Connectez-vous au serveur d'applications en tant qu'utilisateur **dncs**.

Désactiver le processus SAM sur les systèmes Rovi et MDN/ODN

Si le site que vous mettez à niveau utilise le serveur d'applications Rovi Corporation, vous devez désactiver le processus SAM avant de redémarrer les composants système. Effectuez les opérations ci-après pour désactiver le processus SAM.

Remarques :

- Si le site que vous mettez à niveau n'utilise pas le serveur d'applications Rovi Corporation, ignorez cette procédure et passez à la procédure suivante indiquée dans ce chapitre.
- Vous devez être connecté au DNCS en tant qu'utilisateur **dncs**.

1. Dans la section DNCS de la fenêtre DNCS Administrative Console Status, cliquez sur **Control**. La fenêtre DNCS Monitor s'ouvre.
2. Dans une fenêtre d'émulation de terminal du DNCS, saisissez **dncsControl** puis appuyez sur **Entrée**. La fenêtre DNCS Control s'ouvre.
3. Saisissez **4** (pour Define/Update Grouped Elements) puis appuyez sur **Entrée**. La fenêtre se met à jour et répertorie une série de groupes d'éléments.
4. Saisissez **14** (pour saManager) puis appuyez sur **Entrée** La fenêtre se met à jour et répertorie les éléments du groupe.
5. Saisissez **1** (pour /dvs/dncs/bin/saManager) puis appuyez sur **Entrée**. Le premier d'une série de messages de confirmation s'affiche.
6. Appuyez sur **Entrée** à chaque message de confirmation pour accepter le paramètre par défaut jusqu'à ce qu'un message sur **cpElmtExecCtrlStatus** s'affiche. Au total, vous devez voir environ six messages de confirmation.
7. Au niveau du message cpElmtExecCtrlStatus, tapez **2** (pour Désactivé) et appuyez sur **Entrée**. Un message de confirmation s'affiche.
8. Tapez **y** (pour yes) puis appuyez sur **Entrée**. Le message **Element Definition was Modified** s'affiche.
9. Suivez les instructions affichées à l'écran pour quitter la fenêtre DNCS Control.

Redémarrer les composants système

Après avoir installé la version 2.8.1/3.8.1/4.3.1, suivez les instructions ci-après pour redémarrer les composants système.

Redémarrage du DNCS

1. Amenez le curseur sur le DCNS, appuyez sur le bouton du milieu de la souris et sélectionnez **DNCS Start**. Les processus DNCS démarrent.
2. Amenez le curseur sur le DNCS, appuyez sur le bouton du milieu de la souris et sélectionnez **Administrative Console**. La console d'administration DNCS s'ouvre.
3. Dans la fenêtre DNCS Administrative Console Status, cliquez sur **DNCS Control**.

   Résultats :
   - La fenêtre DNCS Control s'ouvre.
   - Les voyants verts commencent à remplacer les voyants rouges dans la fenêtre DNCS Control.
4. Dans une fenêtre d'émulation de terminal du DNCS, saisissez **dncsControl** puis appuyez sur **Entrée**. La fenêtre de l'utilitaire Dncs Control s'ouvre.
5. Saisissez **2** (pour démarrer/arrêter un seul groupe d'éléments), puis appuyez sur **Entrée**. La fenêtre Dncs Control se met à jour et répertorie l'état de tous les processus et serveurs exécutés sur le DNCS.
6. Attendez que la fenêtre Dncs Control répertorie l'état actuel (Curr STT) de tous les processus et serveurs comme étant **actif**.

   Remarques :
   - La fenêtre Dncs Control se met à jour automatiquement toutes les quelques secondes ; vous pouvez aussi appuyer sur **Entrée** pour forcer une mise à jour.
   - Tous les voyants de la fenêtre DNCS Control deviennent verts lorsque les processus et les serveurs ont redémarré.

Redémarrage du serveur d'applications SARA

Important : Si le site que vous mettez à niveau utilise le serveur d'applications Rovi Corporation, passez cette procédure et allez à ***Redémarrer le serveur d'applications sur les sites Rovi*** (à la page 61).

Remarque : Le serveur d'applications doit être à une invite **OK**.

1. Saisissez **boot** et appuyez sur **Entrée**. Le serveur redémarre.
2. Connectez-vous en tant qu'utilisateur **dncs**.
3. Ouvrez une fenêtre d'émulation de terminal sur le serveur d'applications.

4 Saisissez **appControl** puis appuyez sur **Entrée**. La fenêtre Applications Control s'ouvre.

5 Sélectionnez l'option **2** dans la fenêtre Applications Control. Le système affiche la liste des processus du serveur d'applications et leur état actuel.

6 Le mot **running** est -il affiché en regard du champ d'état actuel (Curr STT) de chaque processus ?

- Si **c'est le cas**, ignorez le reste de cette procédure et passez à la procédure suivante indiquée dans ce chapitre.
- Si **ce n'est pas le cas**, passez à l'étape 7.

7 Appuyez sur le bouton du milieu de la souris, puis sélectionnez **App Serv Start**.

8 Lorsque la fenêtre Application Control indique que l'état actuel (Curr STT) de chaque processus est **actif**, passez à l'étape 9.

Remarque : Sur certains systèmes, le processus distant BFS peut conserver la valeur **Stopped** ; c'est normal.

9 Suivez les instructions affichées à l'écran pour fermer la fenêtre Applications Control.

Redémarrer le serveur d'applications sur les sites Rovi

Suivez cette procédure *uniquement* si le site que vous mettez à niveau prend en charge le serveur d'applications Rovi Corporation. Si le site que vous mettez à niveau prend en charge le serveur SARA, ignorez cette section et passez à la procédure suivante indiquée dans ce chapitre.

Redémarrage du serveur d'applications sur un site Rovi

Effectuez les opérations suivantes pour vérifier si l'application Rovi a démarré sur le serveur d'applications puis pour le redémarrer en cas de besoin.

1. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le serveur d'applications.
2. Saisissez **CheckServices** puis appuyez sur **Entrée**. Une liste de pilotes s'affiche.

   Remarque : Chaque pilote est associé à un processus de serveur d'applications.
3. Le mot **Yes** est-il affiché en regard de chaque pilote ?
   - Si **c'est le cas**, ignorez le reste de cette procédure et passez à la procédure suivante indiquée dans ce chapitre.
   - Si **ce n'est pas le cas**, passez à l'étape 4.

   Remarque : Le mot **Yes** en regard d'un pilote indique que le processus a commencé.
4. Appuyez sur le bouton du milieu de la souris, puis sélectionnez **Passport Start**.
5. Lorsque le mot **Yes** est affiché en regard de chaque pilote, passez à l'étape 6.
6. Suivez les instructions affichées à l'écran pour fermer la fenêtre qui contient la liste des pilotes Rovi.

   Remarque : La fenêtre AppServer Control dans la fenêtre DNCS Administrative Console Status peut s'afficher à l'état inactif. C'est normal pour un site Rovi.

Redémarrer les interfaces de facturation et les interfaces tierces

Redémarrer les interfaces de facturation et les interfaces tierces

Contactez votre fournisseur de facturation pour redémarrer l'interface de facturation. Si vous avez arrêté des interfaces tierces avant d'installer la version 2.8.1/3.8.1/4.3.1, redémarrez aussi ces interfaces.

Redémarrage du serveur d'applications Time Warner Mystro

Si nécessaire, reportez -vous aux documents fournis par Mystro pour redémarrer le MDN.

Redémarrer les tâches cron

Redémarrage des tâches cron sur le DNCS

1. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le DNCS.
2. Saisissez **ps -ef | grep cron** puis appuyez sur **Entrée**. Le système doit répertorier /usr/sbin/cron. Les tâches cron ont-elles redémarré sur le DNCS ?
   - a Si **c'est le cas**, allez à ***Redémarrage des tâches cron sur le serveur d'applications*** (à la page 63).
   - b Si **ce n'est pas le cas**, passez à l'étape 3.
3. Suivez les instructions pour vous connecter à la fenêtre d'émulation de terminal en tant qu'utilisateur racine.
   - a Saisissez **su -** puis appuyez sur **Entrée**. Un message vous invitant à saisir un mot de passe s'affiche.
   - b Saisissez le mot de passe de l'utilisateur racine puis appuyez sur **Entrée**.
4. Saisissez la commande suivante et appuyez sur **Entrée** pour redémarrer toutes les tâches cron :

   ```
   svcadm -v enable -rs cron
   ```
5. Vérifiez que les tâches cron ont redémarré en saisissant **ps -ef | grep cron** puis en appuyant sur **Entrée**. Le système doit répertorier /usr/sbin/cron.
6. Allez à ***Redémarrage des tâches cron sur le serveur d'applications*** (à la page 63).

Redémarrage des tâches cron sur le serveur d'applications

Si nécessaire, suivez les instructions ci-après pour redémarrer les tâches cron sur le serveur d'applications. Les tâches cron figurant sur le serveur d'applications peuvent avoir redémarré toutes seules lorsque vous avez redémarré le serveur d'applications au début du chapitre.

Important : Cette procédure concerne uniquement le serveur SARA. Si le site que vous mettez à niveau prend en charge le serveur d'applications Rovi, vérifiez avec Rovi la procédure appropriée.

1. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le serveur d'applications.
2. Saisissez **ps -ef | grep cron** puis appuyez sur **Entrée**. Le système doit répertorier /usr/sbin/cron. Les tâches cron ont-elles redémarré sur le serveur d'applications ?
   - a Si **c'est le cas**, passez à la procédure suivante indiquée dans ce chapitre.
   - b Si **ce n'est pas le cas**, passez à l'étape 3.
3. Suivez les instructions pour vous connecter à la fenêtre d'émulation de terminal en tant qu'utilisateur racine.
   - a Saisissez **su -** puis appuyez sur **Entrée**. Un message vous invitant à saisir un mot de passe s'affiche.
   - b Saisissez le mot de passe de l'utilisateur racine puis appuyez sur **Entrée**.

4. Saisissez la commande suivante et appuyez sur **Entrée** pour redémarrer toutes les tâches cron :

   ```
   svcadm -v enable -rs cron
   ```

5. Vérifiez que les tâches cron ont redémarré en saisissant **ps -ef | grep cron** puis en appuyant sur **Entrée**. Le système doit répertorier /usr/sbin/cron.
6. Saisissez **exit** puis appuyez sur **Entrée** pour déconnecter l'utilisateur racine.

Vérifier les tâches cron

Après avoir redémarré les interfaces de facturation et les interfaces tierces, examinez les entrées racine et dncs crontab des tâches cron qui ne se sont peut-être pas exécutées, pendant la période d'entretien, telles que l'IPG Collector, alors que des tâches cron étaient arrêtées. Si nécessaire, exécutez ces tâches cron manuellement.

Suivez les instructions ci-après pour vérifier les fichiers crontab.

1. Dans une fenêtre d'émulation de terminal du DNCS, saisissez la commande suivante et appuyez sur **Entrée**.
   `cd /export/home/dncs/network`
2. Saisissez la commande suivante et appuyez sur **Entrée**.
   `tar xvf crontabs.tar`
3. Saisissez **cd crontabs** et appuyez sur **Entrée**.
4. Suivez les instructions ci-après pour comparer le fichier dncs crontab avec les entrées réelles postérieures à la mise à niveau.
   - **a** Saisissez **less dncs** et appuyez sur **Entrée**.
   - **b** Saisissez `crontab -l dncs` et appuyez sur **Entrée**.
   - **c** Comparez la sortie des étapes a et b. Vérifiez que les entrées cron propres au client de l'étape a sont incluses dans l'étape b.
   - **d** Ajoutez les entrées manquantes de l'étape a au fichier dncs crontab.
5. Répétez l'étape 4 pour le fichier crontab racine.

Redémarrer les utilitaires

Redémarrer l'utilitaire dhctStatus

L'utilitaire dhctStatus fonctionne généralement depuis cron et est lancé à l'heure programmée.

Redémarrage de l'utilitaire signonCount

Si l'utilitaire signonCount était actif avant la mise à niveau, effectuez les opérations ci-après pour le redémarrer. Si vous ne souhaitez pas démarrer l'utilitaire signonCount à ce stade, ignorez cette procédure et passez à la procédure suivante indiquée dans ce chapitre.

1. Saisissez **signonCount** et appuyez sur **Entrée**. Le processus signonCount démarre et commence par afficher l'état de connexion du terminal.
2. Appuyez simultanément sur les touches **Ctrl** et **C** pour arrêter la sortie du terminal.
3. Saisissez `tail -f /dvs/dncs/tmp/signonCount.out` et appuyez sur **Entrée** pour surveiller l'état de l'utilitaire signonCount. Le terminal affiche les 10 dernières lignes du fichier de sortie, ainsi que toutes les nouvelles entrées de ce fichier.
4. Appuyez simultanément sur les touches **Ctrl** et **C** pour arrêter le processus *tail*.

Redémarrer l'utilitaire cmd2000

1. Pour redémarrer l'utilitaire cmd2000, saisissez la commande suivante puis appuyez sur **Entrée** :

   ```
   /dvs/resapp/Tools cmd2000 -log -listen &
   ```

2. Pour vérifier que l'utilitaire cmd2000 est actif, saisissez la commande suivante et appuyez sur **Entrée** :

   ```
   ps -ef | grep cmd2000
   ```

3

Procédures après la mise à niveau de la version 2.8.1/3.8.1/4.3.1

Introduction

Après avoir installé la version 2.8.1/3.8.1/4.3.1, suivez les procédures indiquées dans ce chapitre pour exécuter le processus de mise à niveau.

Dans ce chapitre

Restaurer les fichiers de données

Dans cette procédure, vous restaurerez les fichiers de données que vous avez sauvegardés sur bande dans la section ***Sauvegarder les différents fichiers de données*** (à la page 31) du chapitre 1.

Remarque : Cette procédure fait référence au nom de périphérique du lecteur de bande DNCS. Si vous n'êtes pas sûr du nom du périphérique ou que vous voulez simplement qu'on vous le confirme, exécutez la procédure indiquée dans l'Annexe B, ***Comment déterminer le nom de périphérique du lecteur de bande*** (à la page 91).

Restauration des fichiers de données

Suivez la procédure ci-après pour restaurer les fichiers de données.

1. Insérez la bande que vous avez utilisée dans la section **Sauvegarder les différents fichiers de données** du chapitre 1 dans le lecteur de bande du DNCS.

   Remarque : Assurez -vous que la bande est protégée en écriture.
2. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le DNCS.
3. Saisissez **tar xvf [nom du périphérique]** puis appuyez sur **Entrée**. Le système restaure les fichiers spécifiés.

   Remarque : Remplacez le nom de périphérique du lecteur de bande du DNCS par [nom du périphérique].

   Exemple : tar xvf /dev/rmt/0h
4. Lorsque la restauration est terminée, éjectez la bande et stockez-la dans un endroit sûr.

Vérifier les alarmes SAM

Après avoir mis à niveau le système vers la version 2.8.1/3.8.1/4.3.1, les champs **Update Timer** et **Schedule Timer** de la fenêtre SAM Configuration doivent avoir des valeurs identiques à celles qu'elles avaient avant la mise à niveau. Ces valeurs allouent aux mappages de canaux et à la base de données suffisamment de temps pour se mettre à jour. Vous avez enregistré ces valeurs dans ***Vérifier les alarmes SAM*** (à la page 19). Suivez les instructions indiquées dans cette section pour affecter leurs valeurs appropriées aux champs **Update Timer** et **Schedule Timer**.

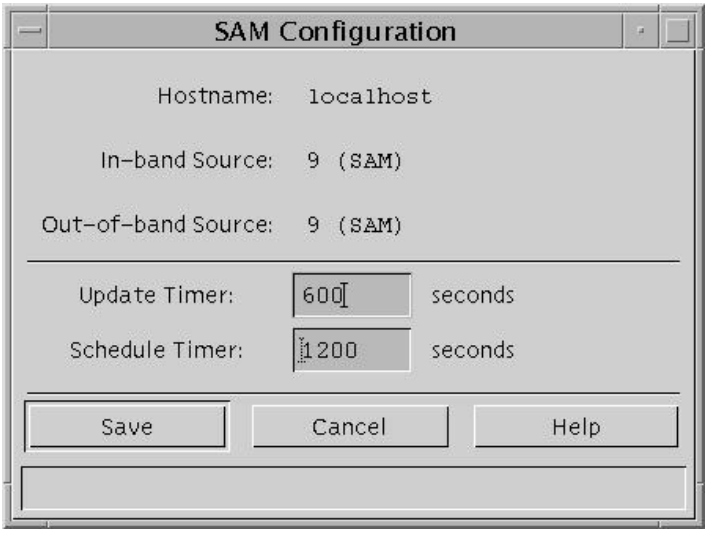
Remarque : Cette procédure concerne uniquement les sites qui prennent en charge SARA. Passez cette procédure si le site que vous avez mis à niveau ne prend pas en charge SARA.

Vérification des alarmes SAM

Suivez les instructions ci-après pour définir les champs **Update Timer** et **Schedule Timer** de la fenêtre SAM Configuration, si nécessaire.

Remarque : Ces exemples contiennent les valeurs **600** et **1200** pour les champs **Update Timer** et **Schedule Timer**, respectivement, qui sont les valeurs recommandées par Cisco. En fait, vous devez affecter à ces champs les valeurs requises par votre système.

1. Dans la console d'administration DNCS, sélectionnez l'onglet **Application Interface Modules** puis cliquez sur **SAM Config**. La fenêtre SAM Configuration s'ouvre.
2. Suivez les instructions ci-après pour paramétrer la fenêtre SAM Configuration.
   - **a** Dans le champ **Update Timer**, saisissez **600** ou la valeur requise par votre système.
   - **b** Dans le champ **Schedule Timer**, saisissez **1200** ou la valeur requise par votre système.



3. Cliquez sur **Enregistrer**.

Configurer le serveur CableCARD

Après avoir mis à niveau le système vers la version 2.8.1/3.8.1/4.3.1, les champs **Set Authorization Time-out Period** et **Set DeAuthorization Time-out Period** de la fenêtre Configure CableCARD Server doivent être définis aux valeurs spécifiques. Ces valeurs indiquent au serveur CableCARD le moment où il doit arrêter d'ajouter des enregistrement d'autorisation et d'interdiction au fichier BFS, ce qui empêche le fichier BFS de devenir trop volumineux. Les instructions contenues dans cette section vous indiquent la suite des opérations nécessaires.

Remarque : À partir de la mise à niveau vers la version 4.2, la valeur enregistrée dans le champ Max Key Session Period est multipliée par le facteur 10. Toutefois, cela ne change pas la valeur reçue par le CableCARD. Pour plus d'informations, reportez-vous à la référence CR **46084**.

Configuration du serveur CableCARD

Effectuez les opérations suivantes pour que les valeurs minimales des champs Set Authorization Time-out Period et Set DeAuthorization Time-out Period de la fenêtre Configure CableCARD Server soient définies correctement. Reportez les nombres que vous avez enregistrés dans la procédure ***Vérifier le serveur CableCARD*** (à la page 20).

1. Dans la console d'administration DNCS, sélectionnez l'onglet **DNCS**.
2. Sélectionnez l'onglet **Home Element Provisioning** puis cliquez sur **CableCARD**. L'écran CableCARD Data Summary s'ouvre.
3. Cliquez sur **Server Configuration**. L'écran CableCARD Data Summary se met à jour et affiche la partie Server Configuration de l'écran.
4. Examinez le champ **Authorization Time-out Period**. Assurez -vous que sa valeur est identique à celle que vous avez enregistrée dans ***Vérifier le serveur CableCARD*** (à la page 20).
5. Examinez le champ **DeAuthorization Time-out Period**. Assurez -vous que sa valeur est identique à celle que vous avez enregistrée dans ***Vérifier le serveur CableCARD*** (à la page 20).
6. Cliquez sur **Save CableCARD Server Config**.
7. Cliquez sur **Exit all CableCARD Screens**.

Vérifier la configuration EAS - Procédure après la mise à niveau

Vérification de la configuration EAS

Après avoir installé la version 2.8.1/3.8.1/4.3.1 du logiciel, vérifiez que votre équipement EAS fonctionne correctement en testant la capacité du système à transmettre des messages EAS. Suivez toutes les procédures indiquées au chapitre 5, **Testing the EAS** du guide *Configuring and Troubleshooting the Digital Emergency Alert System* (référence 4004455).

Après avoir suivi les procédures indiquées au chapitre 5, **Testing the EAS** du guide *Configuring and Troubleshooting the Digital Emergency Alert System, qui accompagne toutes les versions*, vérifiez que vous pouvez générer un message EAS pour l'EAC (Emergency Alert Controller) lui-même.

Vérifier les sessions BFS QAM

Le nombre de sessions BFS après la mise à niveau doit être le même que le nombre de sessions BFS avant la mise à niveau. Les procédures contenues dans cette section vous indiquent la suite des opérations nécessaires pour valider le nombre de sessions BFS.

Vérification du nombre de sessions BFS récupérées

Effectuez les opérations suivantes pour vérifier le nombre de sessions BFS après la mise à niveau.

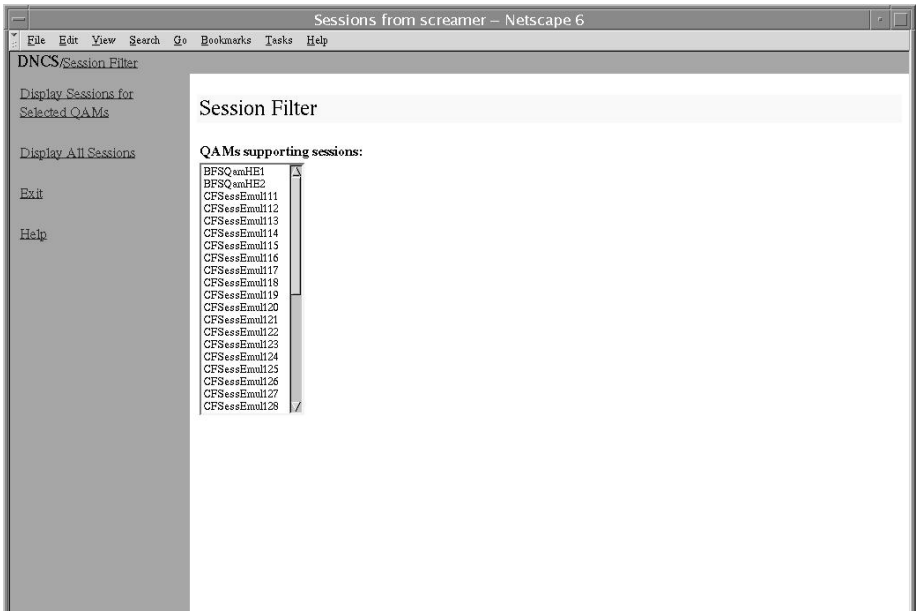
1. Choisissez l'une des options suivantes pour vérifier le nombre de sessions BFS :
   - Appuyez sur le bouton **Options** sur la façade avant du BFS QUAM jusqu'à ce que la valeur totale **Session Count** s'affiche.
   - Saisissez **/dvs/dncs/bin/auditQam -query <AdrIP> 2** et appuyez sur **Entrée**.
     Remarque : <AdrIP> est l'adresse IP du QAM de données.
2. Le nombre total de sessions indiquées dans le champ **Session Count** est-il égal au nombre de sessions que vous avez enregistrées dans la procédure ***Vérifier les sessions et les enregistrer*** (à la page 26) ?
   - Si **c'est le cas**, ignorez la suite de cette section, et passez à ***Autoriser le BRF comme serveur BFS (facultatif)*** (à la page 75). Le système a récupéré toutes les sessions BFS.
   - Si **ce n'est pas le cas**, passez à ***Arrêter les processus BFS et OSM*** (à la page 72).

Arrêter les processus BFS et OSM

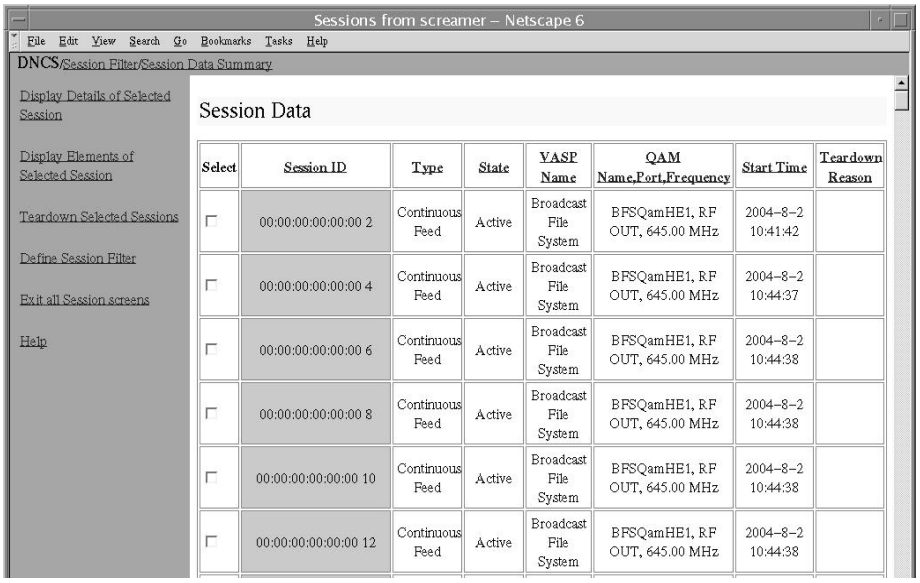
Effectuez les opérations suivantes pour arrêter les processus BFS et OSM en vue de restaurer le nombre de sessions BFS prévues.

1. Dans la fenêtre DNCS Control, mettez en surbrillance le processus **osm.**
2. Cliquez sur **Process** puis sélectionnez **Stop Process**. En quelques minutes, le voyant du processus osm passe du vert au rouge.
3. Mettez en surbrillance le processus **bfsServer**.
4. Cliquez sur **Process** puis sélectionnez **Stop Process**. En quelques minutes, le voyant du processus bfsServer passe du vert au rouge.
5. Sur la console d'administration DNCS, sélectionnez l'onglet **DNCS** et allez à **Utilities**.

6 Cliquez sur **Session List**. La fenêtre Session Filter s'ouvre.



7 Sélectionnez le BFS QAM dans la liste Session Filter puis cliquez sur **Display Sessions for Selected QAMs**. La fenêtre Session Data s'ouvre.



Select	Session ID	Type	State	VASP Name	QAM Name,Port,Frequency	Start Time	Teardown Reason
☐	00:00:00:00:00:00 2	Continuous Feed	Active	Broadcast File System	BFSQamHE1, RF OUT, 645.00 MHz	2004–8–2 10:41:42	
☐	00:00:00:00:00:00 4	Continuous Feed	Active	Broadcast File System	BFSQamHE1, RF OUT, 645.00 MHz	2004–8–2 10:44:37	
☐	00:00:00:00:00:00 6	Continuous Feed	Active	Broadcast File System	BFSQamHE1, RF OUT, 645.00 MHz	2004–8–2 10:44:38	
☐	00:00:00:00:00:00 8	Continuous Feed	Active	Broadcast File System	BFSQamHE1, RF OUT, 645.00 MHz	2004–8–2 10:44:38	
☐	00:00:00:00:00:00 10	Continuous Feed	Active	Broadcast File System	BFSQamHE1, RF OUT, 645.00 MHz	2004–8–2 10:44:38	
☐	00:00:00:00:00:00 12	Continuous Feed	Active	Broadcast File System	BFSQamHE1, RF OUT, 645.00 MHz	2004–8–2 10:44:38	

8 Dans la colonne **Select**, activez la case à cocher associée à chaque session BFS/OSM.

9 Cliquez sur **Teardown Selected Sessions**. Le système arrête les sessions BFS et OSM.

10 Dans la fenêtre DNCS Control, mettez en surbrillance le processus **bfsServer**.

11 Cliquez sur **Process** puis sélectionnez **Start Process**. En quelques minutes, le voyant du processus bfsServer passe du rouge au vert.

12 Lorsque le voyant du processus bfsServer est passé au vert, mettez en surbrillance le processus **osm**.

13 Cliquez sur **Process** puis sélectionnez **Start Process**. En quelques minutes, le voyant

du processus osm passe du rouge au vert.

14 Appuyez sur le bouton **Options** sur la façade avant du BFS QUAM jusqu'à ce que la valeur totale **Session Count** s'affiche.

15 Patientez environ 10 minutes jusqu'à ce que le système reconstitue les sessions.

16 La valeur totale contenue dans le champ **Session Count** est maintenant égale au nombre de sessions que vous avez enregistré dans ***Vérifier les sessions et les enregistrer*** (à la page 26)?

- Si **c'est le cas**, passez à la procédure suivante indiquée dans ce chapitre. Le système a récupéré toutes les sessions BFS.
- Si **ce n'est pas le cas**, appelez les services Cisco pour obtenir de l'aide.

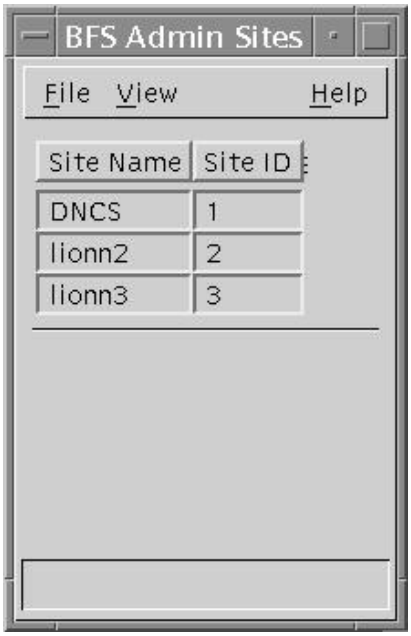
Autoriser le BRF comme serveur BFS (facultatif)

Dans les systèmes qui utilisent un chemin de retour DOCSIS pour les communications DHCT, le DCD (Downstream Channel Descriptor) n'est pas pris en charge dans le système de terminaison par modem câble (CMTS). Ces systèmes ont besoin d'un BRF (Bridge Resolution File) comme serveur BFS afin de permettre aux DHCT de reconnaître leur ID d'hub et leur adresse multicast MAC. Après une mise à niveau, le système n'autorise pas automatiquement la création du BRF comme serveur BFS ; vous devez autoriser manuellement la création du fichier. Suivez les instructions ci-après pour rechercher la présence du BRF dans les interfaces utilisateur BFS et autoriser alors le fichier s'il y a lieu.

Autoriser le BRF

Suivez les instructions ci-après pour rechercher le BRF puis autoriser ce fichier s'il y a lieu.

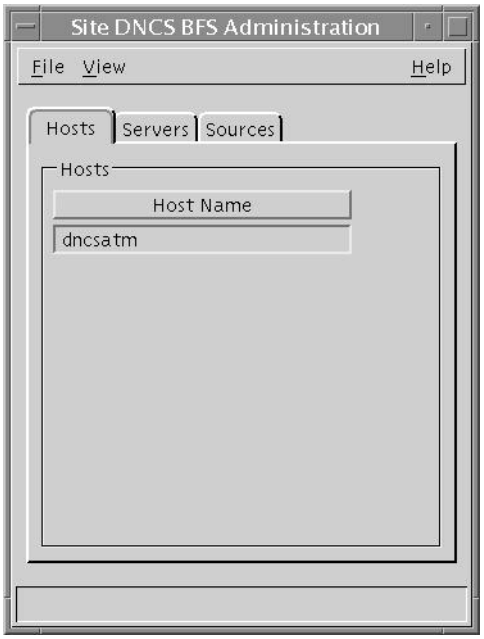
1. Dans la console d'administration DNCS, sélectionnez l'onglet **Application Interface Modules**.
2. Votre site exécute-t-il RNCS (Regional Network Control System) ?
   - **a** Si **c'est le cas**, cliquez sur **BFS Admin**. La fenêtre BFS Admin Sites s'ouvre.



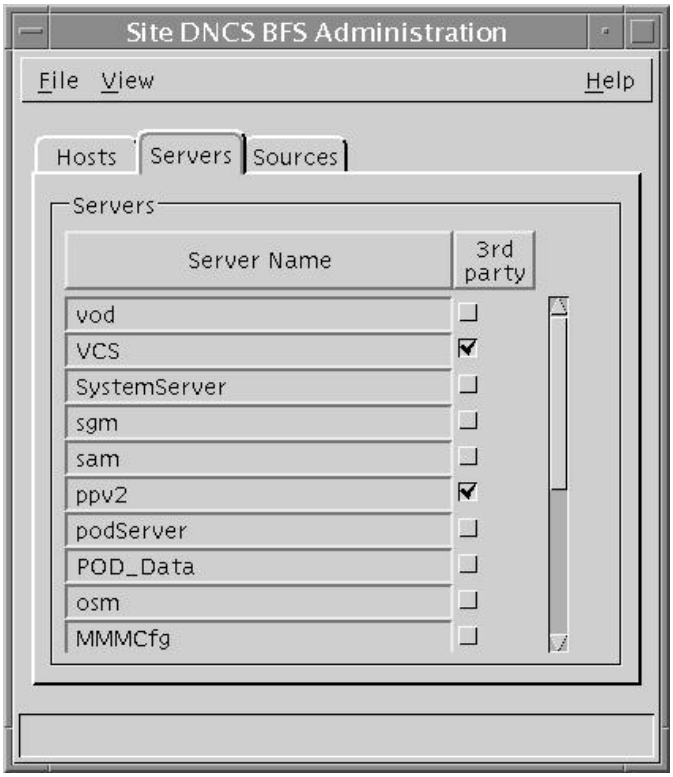
   - **b** Si **ce n'est pas le cas**, passez à l'étape 3.

3 Double-cliquez sur **DNCS**.

Remarque : Cette procédure ne s'applique pas aux sites distants. La fenêtre Site DNCS BFS Administration s'ouvre.



4 Cliquez sur l'onglet **Servers**. La liste des serveurs s'affiche.



5 **brf** figure-t-il dans la colonne **Server Name** ?

Remarque : Utilisez la barre de défilement pour afficher la liste complète.

- Si **c'est le cas**, cliquez sur **File** puis sélectionnez **Close** pour fermer la fenêtre Site DNCS BFS Administration. Vous avez terminé cette procédure ; passez à la procédure suivante indiquée dans ce chapitre.

  Remarque : Le BRF est déjà autorisé comme serveur BFS.
- Si **ce n'est pas le cas**, passez à l'étape 6.

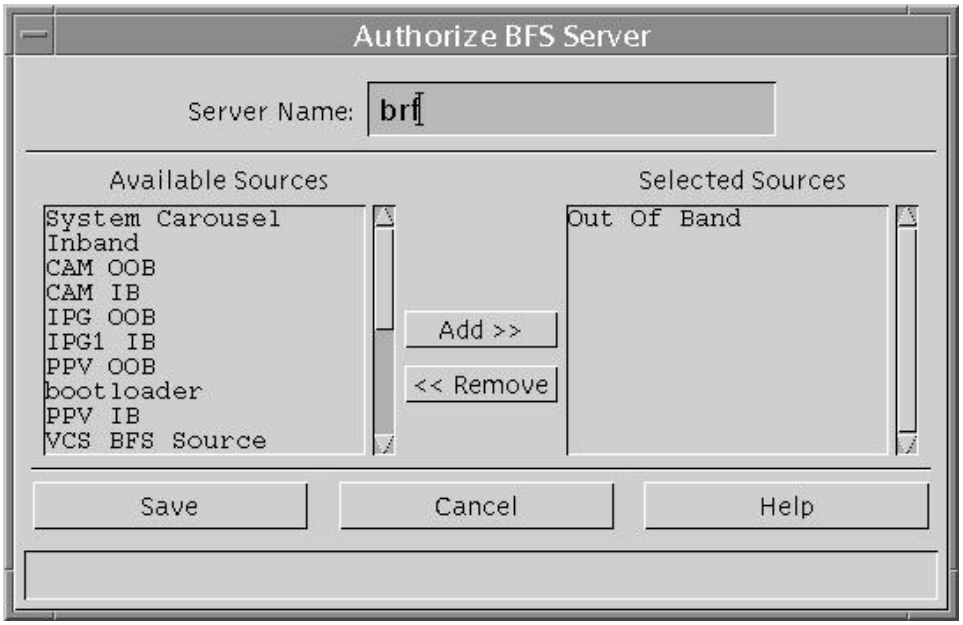
6 Cliquez sur **File** puis sélectionnez **New**. La fenêtre Authorize BFS Server s'ouvre.

7 Suivez les instructions ci-après pour configurer la fenêtre Authorize BFS Server.

a Saisissez **brf** dans la zone de texte **Server Name**.

b Dans la colonne **Available Sources**, mettez en surbrillance **Out of Band** puis cliquez sur **Add**. La source Out of Band passe dans la colonne **Selected Sources**.

Exemple : La fenêtre Authorize BFS Server doit être similaire à l'exemple qui suit lorsque vous avez terminé.



8 Cliquez sur **Enregistrer**. Le système enregistre le BRF nouvellement autorisé.

9 Cliquez sur **File** puis sélectionnez **Close** pour fermer la fenêtre Authorize BFS Server.

10 Passez à la procédure suivante indiquée dans ce chapitre.

Redémarrer les serveurs de sauvegarde de base ou de sauvegarde automatique

Si le site que vous mettez à niveau utilise le serveur de sauvegarde de base ou de sauvegarde automatique et que ces sauvegardes de serveur ont été désactivées ou reprogrammées pour la mise à niveau, réactivez les sauvegardes maintenant ou faites-les revenir à la programmation initiale.

Tests finaux de validation du système

Vérification d'une installation correcte de la version 2.8.1/3.8.1/4.3.1

Suivez les instructions ci-après pour vérifier une installation correcte de la version 2.8.1/3.8.1/4.3.1. Les DHCT que vous utilisez pour ces tests doivent répondre aux spécifications suivantes :

- Non autorisé à afficher un événement PPV sans acheter spécifiquement l'événement PPV
- Autorisé pour toutes les applications tierces

Important : Si l'un de ces tests échoue, contactez les services Cisco avant d'effectuer une restauration depuis cette mise à niveau.

1. Effectuez les opérations ci-après pour effectuer un démarrage lent et un démarrage rapide sur un DHCT avec un chemin de retour en fonctionnement (mode bidirectionnel).
   - **a** Démarrez un DHCT.
     Remarque : *N'appuyez pas* sur le bouton d'alimentation.
   - **b** Attendez 5 minutes.
   - **c** Appuyez sur le bouton d'alimentation du DHCT. Le DHCT est mis sous tension.
2. Préparez au moins un nouveau DHCT selon les spécifications de l'opérateur.
3. Après sa préparation, le DHCT a-t-il chargé correctement la version client actuelle ?
   - Si **c'est le cas**, passez à l'étape 4.
   - Si **ce n'est pas le cas**, appelez les services Cisco pour obtenir de l'aide.
4. Le DHCT a-t-il reçu au moins 32 EMM (Entitlement Management Messages)) et a-t-il reçu correctement son Entitlement Agent ?
   - Si **c'est le cas**, passez à l'étape 5.
   - Si **ce n'est pas le cas**, appelez les services Cisco pour obtenir de l'aide.
5. L'IPG affiche-t-il 7 jours de données valides et exactes ?
   - Si **c'est le cas**, passez à l'étape 6.
   - Si **ce n'est pas le cas**, appelez les services Cisco pour obtenir de l'aide.
6. Les chaînes invitation avec paiement à la séance s'affichent-elles correctement sur les canaux PPV ?
   - Si **c'est le cas**, passez à l'étape 7.
   - Si **ce n'est pas le cas**, appelez les services Cisco pour obtenir de l'aide.
7. Les applications tierces se chargent-elles et fonctionnent-elles correctement ?
   - Si **c'est le cas**, passez à l'étape 8.
   - Si **ce n'est pas le cas**, appelez les services Cisco pour obtenir de l'aide.

8 Les DHCT test peuvent-ils acheter un programme VOD et/ou xOD ?
   - Si **c'est le cas**, vous avez effectué la mise à niveau correctement.
   - Si **ce n'est pas le cas**, appelez les services Cisco pour obtenir de l'aide.
9 S'il y a lieu, les canaux SDV sont-ils disponibles ?
   - Si **c'est le cas**, le BRF est autorisé correctement.
   - Si **ce n'est pas le cas**, appelez les services Cisco pour obtenir de l'aide.

Réactiver la fonction de mise en miroir des disques

Dans ***Déconnecter les disques en miroir sur le DNCS*** (à la page 43), vous avez déconnecté la fonction de mise en miroir du DNCS. Si la mise à niveau du système semble avoir réussi, patientez une journée pour vérifier que le DNCS fonctionne correctement avec le nouveau logiciel. Réactivez ensuite la fonction de mise en miroir des disques pour permettre au DNCS de continuer à stocker des informations identiques sur plusieurs ensembles de disques durs.

Important : Si votre mise à niveau a échoué, reportez-vous à l'annexe A ***Version 2.8.1/3.8.1/4.3.1 - Procédures de restauration*** (à la page 87).

Réactivation de la fonction de mise en miroir des disques

Suivez les instructions ci-après pour réactiver la fonction de mise en miroir des disques du DNCS Entreprise 450 ou Sun Fire V880.

Important : Avant de suivre ces instructions, Patientez au moins 24 heures après la mise à niveau pour vérifier que votre DNCS fonctionne correctement avec le nouveau logiciel.

1. Dans une fenêtre d'émulation de terminal du DNCS, saisissez **su** puis appuyez sur **Entrée**. Un message vous invitant à saisir un **mot de passe** s'affiche.
2. Saisissez le mot de passe de l'utilisateur racine puis appuyez sur **Entrée**. Dans la fenêtre d'émulation de terminal, vous disposez des droits de l'utilisateur racine.
3. Insérez le CD intitulé **DBDS Maintenance CD** dans le lecteur de CD-ROM du DNCS.
4. Saisissez **/cdrom/cdrom0/s3/backup_restore/mirrState -a** puis appuyez sur **Entrée**. Le système affiche le message suivant :

   WARNING!!
   Proceeding beyond this point will ATTACH all Controller 2 submirrors.
   Are you certain you want to proceed?
5. Tapez **y** puis appuyez sur **Entrée**. Le système active les fonctions de mise en miroir sur le DNCS.

   Remarque : Selon la configuration de votre système, la mise en miroir de toutes les données sur les disques mis en miroir peut prendre 1 heure.

Surveillance du processus de mise en miroir des disques

L'utilitaire syncwait permet aux ingénieurs de surveiller l'avancement du processus de mise en miroir des disques. Suivez les instructions ci-après pour exécuter l'utilitaire syncwait.

1. Ouvrez un autre fenêtre d'émulation de terminal sur le DNCS.
2. Saisissez **syncwait.ksh** puis appuyez sur **Entrée**. Le système affiche un message indiquant le pourcentage du processus de synchronisation des miroirs qui est terminé.
3. Lorsque le système affiche le message suivant, le processus de mise en miroir de disques est terminé ; saisissez **n** (pour no) puis appuyez sur **Entrée** L'utilitaire syncwait se ferme.

   No Resync in progress …
   Continue monitoring status? (n, y ou q)
4. Saisissez **q** puis appuyez sur **Entrée** pour sortir du processus de surveillance.
5. Saisissez **metastat | more** puis appuyez sur **Entrée**. Le système affiche l'état de tous les métapériphériques présents sur le DNCS.

   Remarque : Appuyez si nécessaire sur la **barre d'espacement** pour faire défiler toute la sortie.
6. Examinez la sortie de la commande metastat concernant les deux conditions suivantes, puis passez à l'étape 7 :
   - Le mot **ok** apparaît dans la colonne **State** en regard de chaque métapériphérique.
   - *Aucun* **Hot Spare** n'indique **In Use**.
7. Ces *deux* conditions sont-elles décrites comme vraies dans l'étape 6 ?
   - Si **c'est le cas** (pour les deux conditions), passez à l'étape 8 ; la mise en miroir des disques a été activée correctement.
   - Si **ce n'est pas le cas** (pour l'une ou l'autre condition), appelez les services Cisco pour obtenir de l'aide pour résoudre les problèmes de mise en miroir des disques.
8. Dans la fenêtre d'émulation de terminal dans laquelle vous avez exécuté la commande -a, saisissez **eject cdrom** puis appuyez sur **Entrée**. Le système éjecte le CD DBDS Maintenance.
9. Saisissez **exit** puis appuyez sur **Entrée** pour fermer la fenêtre d'émulation de terminal.

4

Informations client

Introduction

Ce chapitre répertorie les coordonnées des services d'assistance pour ce produit.

Dans ce chapitre

Assistance clientèle

En cas de question

Pour toute question concernant ce produit, contactez le représentant chargé de votre compte pour obtenir des informations.

Pour toute question technique, appelez le centre d'assistance technique le plus proche à l'un des numéros ci-dessous.

Continent américain

États-Unis	Cisco® Services Atlanta, Georgia	**Assistance technique** ■ Pour les produits *Digital Broadband Delivery System* uniquement, composez le numéro suivant : – Gratuit : 1-866-787-3866 – Local : 770-236-2200 – Fax : 770-236-2488 ■ Pour tous les autres produits, composez le numéro suivant : – Gratuit : 1-800-722-2009 – Local : 678-277-1120 – Fax : 770-236-2306 **Service client** ■ Gratuit : 1-800-722-2009 ■ Local : 678-277-1120 ■ Fax : 770-236-5477

Royaume-Uni et Europe

Europe	Centre d'assistance technique européen (EuTAC), Belgique	**Informations produit** ■ Téléphone : 32-56-445-444 **Assistance technique** ■ Téléphone : 32-56-445-197 ou 32-56-445-155 ■ Fax : 32-56-445-061

Asie-Pacifique

Chine	Hong Kong	**Assistance technique** Téléphone : 011-852-2588-4745 Fax : 011-852-2588-3139

Australie

Australie	Sydney	**Assistance technique** Téléphone : 011-61-2-8446-5374 Fax : 011-61-2-8446-8015
Japon		
Japon	Tokyo	**Assistance technique** Téléphone : 011-81-3-5322-2067 Fax : 011-81-3-5322-1311

Informations supplémentaires

Accédez au site extranet de votre entreprise pour afficher ou commander des documents techniques supplémentaires. Contactez le représentant qui gère votre compte pour obtenir des instructions sur l'accès. Consultez souvent votre site extranet, car les informations sont régulièrement mises à jour.

A

Version 2.8.1/3.8.1/4.3.1 - Procédures de restauration

Introduction

Cette annexe est destinée aux ingénieurs de terrain qui rencontrent des problèmes lors de la mise à niveau d'un système numérique existant vers la version 2.8.1/3.8.1/4.3.1. Avant d'exécuter ces procédures de restauration, contactez les services Cisco au 1-866-787-3866.

Cette annexe contient les procédures de restauration de la version en place avant la mise à niveau.

Dans cette annexe

Restaurer le DNCS

Si votre mise à niveau a échoué, vous devrez peut-être utiliser les procédures décrites dans cette section pour restaurer votre système dans l'état où il se trouvait avant la mise à niveau, puis reconnecter la fonction de mise en miroir des disques du DNCS.

Important : N'oubliez pas d'informer les services Cisco avant de conclure qu'une mise à niveau a échoué et de suivre les procédures indiquées dans cette section. Dans bien des cas, les Services Cisco peuvent vous aider à résoudre facilement les problèmes liés à l'échec de la mise à niveau. De plus, les procédures décrites dans cette section sont uniquement applicables si vous n'avez pas encore suivi la procédure ***Réactivation de la fonction de mise en miroir des disques*** (à la page 81) du chapitre 3. Si vous avez déjà activé la fonction de mise en miroir des disques sur le DNCS, vous devrez restaurer votre système en utilisant les dernières bandes de sauvegarde de votre système de fichiers et de votre base de données.

Restauration du DNCS

Suivez les instructions ci-après pour restaurer le DNCS suite à l'échec d'une mise à niveau vers la version 2.8.1/3.8.1/4.3.1.

Remarque : Vous devez être dans une fenêtre de connexion CDE pour lancer cette procédure. Si vous ne pouvez pas accéder à la fenêtre de connexion CDE, contactez les services Cisco pour obtenir de l'aide.

1. Dans la section ***Arrêter les composants système*** (à la page 40) du chapitre 1, suivez, si nécessaire, les procédures ***Arrêt du serveur d'applications*** (à la page 40) et ***Arrêt du DNCS*** (à la page 41).
2. Dans une fenêtre d'émulation de terminal du serveur d'applications, saisissez **shutdown -g0 -y -i0** puis appuyez sur **Entrée**. Le système arrête tous les processus sur le serveur d'applications et une invite **ok** s'affiche.
3. Insérez le CD intitulé **DBDS Maintenance CD** dans le lecteur de CD du DNCS.
4. Connectez-vous au DNCS en tant qu'utilisateur **racine**.
5. Ouvrez une fenêtre d'émulation de terminal sur le DNCS.

   Remarque : Dans la fenêtre d'émulation de terminal, vous disposerez des droits de l'utilisateur racine.
6. Saisissez **/cdrom/cdrom0/s3/backup_restore/make_d700_bootable** puis appuyez sur **Entrée**. Un message s'affiche qui vous invite à confirmer si le périphérique de disque qui contient l'ancien logiciel doit être rendu bootable.
7. Tapez **y** puis appuyez sur **Entrée**. Un message s'affiche demandant l'autorisation de redémarrer le serveur.
8. Tapez **y** puis appuyez sur **Entrée**. La passerelle DNCS redémarre.
9. Connectez-vous au DNCS en tant qu'utilisateur **racine**.
10. Ouvrez une fenêtre d'émulation de terminal sur le DNCS.

    Remarque : Dans la fenêtre d'émulation de terminal, vous disposez des droits de l'utilisateur racine.
11. Saisissez **pkginfo -l SAIdncs** puis appuyez sur **Entrée**. Le système affiche la version du logiciel en cours d'exécution sur le DNCS.
12. La version du logiciel en cours d'exécution sur le DNCS est-elle la version 4.3.1.x ?

- Si **c'est le cas**, poursuivez la restauration en passant à l'étape 13 ; le DNCS a bien été redémarré avec l'ancien logiciel en place.
- Si **ce n'est pas le cas**, appelez les services Cisco pour obtenir de l'aide pour déterminer pourquoi le redémarrage du DNCS a échoué avec l'ancien logiciel en place.

13 Saisissez **/cdrom/cdrom0/s3/backup_restore/make_d500_bootable** puis appuyez sur **Entrée**. Un message s'affiche qui vous invite à confirmer si le périphérique de disque qui contient l'ancien logiciel doit être rendu bootable.

14 Tapez **y** puis appuyez sur **Entrée**.

Résultats :

- Le script make_d500_bootable reconfigure les disques mis en miroir sur le DNCS.
- Un message s'affiche demandant l'autorisation de redémarrer le serveur.

15 Tapez **y** puis appuyez sur **Entrée**. La passerelle DNCS redémarre.

16 Connectez-vous au DNCS en tant qu'utilisateur **racine**.

17 Saisissez **shutdown -y -g0 -i6** et appuyez sur **Entrée** pour redémarrer à nouveau le serveur.

18 Connectez-vous au DNCS en tant qu'utilisateur **racine**.

19 Ouvrez une fenêtre d'émulation de terminal sur le DNCS.

Remarque : Dans la fenêtre d'émulation de terminal, vous disposerez des droits de l'utilisateur racine.

20 Saisissez **/cdrom/cdrom0/s3/backup_restore/mirrState -a** puis appuyez sur **Entrée**. Le système affiche le message suivant :

WARNING!
Proceeding beyond this point will ATTACH all d7xx submirrors.
Are you certain you want to proceed?

21 Tapez **y** puis appuyez sur **Entrée**. Le système active les fonctions de mise en miroir sur le DNCS.

Remarque : Selon la configuration de votre système, la mise en miroir de toutes les données peut prendre 1 heure.

22 Saisissez **eject cdrom** puis appuyez sur **Entrée**. Le système éjecte le CD.

23 Saisissez **exit** puis appuyez sur **Entrée**. La fenêtre d'émulation de terminal se ferme.

24 Cliquez **EXIT** sur la barre d'outils pour vous déconnecter du DNCS.

25 Connectez-vous au DNCS en tant qu'utilisateur **dncs**.

B

Comment déterminer le nom du périphérique de lecteur de bande

Introduction

Le chapitre 2 de ce guide demande de sauvegarder le système de fichiers et la base de données DNCS avant de mettre le système à niveau. Pour sauvegarder ces fichiers, vous devez connaître le nom de périphérique du lecteur de bande du DNCS.

Si vous n'êtes pas sûr du nom de périphérique du lecteur de bande du DNCS ou que vous voulez simplement qu'on vous le confirme, exécutez la procédure indiquée dans cette Annexe pour déterminer ce nom.

Dans cette annexe

Déterminer le nom de périphérique du lecteur de bande

Utilisez cette procédure pour déterminer le nom de périphérique du lecteur de bande utilisé par votre DNCS.

Remarques :

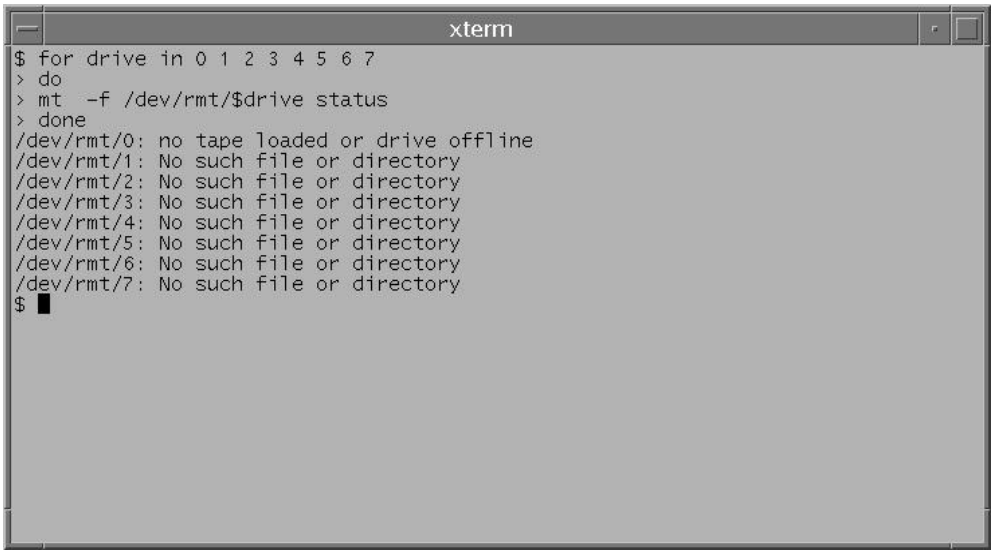
- Vous n'avez besoin d'effectuer cette procédure qu'une seule fois. Le nom du périphérique de votre lecteur de bande ne changera pas tant que vous ne modifierez pas spécifiquement la configuration du lecteur de bande.
- Veillez à ce que le lecteur de bande soit vide lorsque vous effectuez cette procédure.

1. Si nécessaire, ouvrez une fenêtre d'émulation de terminal sur le DNCS.
2. Assurez -vous qu'aucune bande ne se trouve actuellement dans le lecteur de bande.
3. Saisissez la routine UNIX ci-après. Le système vérifie l'état de huit configurations possibles de lecteur de bande et affiche les résultats.

   Important : Saisissez la routine telle qu'elle qu'elle en appuyant sur **Entrée** à la fin de chaque ligne.

   For drive in 0 1 2 3 4 5 6 7
   do
   mt -f /dev/rmt/$drive status
   done

   Remarque : Votre système affiche des résultats similaires à l'exemple qui suit.



4 Examinez vos résultats et utilisez les observations suivantes, basées sur l'exemple utilisé à l'étape 3, pour déterminer le nom du périphérique de votre lecteur de bande :

- Dans l'exemple inséré à l'étape 3, aucun lecteur de bande n'est détecté dans /dev/rmt/1 sur /dev/rmt/7 (comme indiqué par **No such file or directory**). Par conséquent, vous pouvez conclure que /dev/rmt/1 sur /dev/rmt/7 sont des noms de périphérique non valides pour les lecteurs de bande sur le système interrogé à l'étape 3.
- Dans l'exemple inséré à l'étape 3, un lecteur de bande est détecté dans /dev/rmt/0 et le système note bien qu'aucune bande n'est chargée. Par conséquent, vous pouvez conclure que le nom de périphérique du lecteur de bande présent sur le système interrogé à l'étape 3 est /dev/rmt/0.
- Si /dev/rmt/1 est le nom de périphérique de votre lecteur de bande, **no tape loaded or drive offline** s'affiche en regard de /dev/rmt/1.

5 Notez le nom de périphérique de votre lecteur de bande dans l'espace ci-dessous.

_____

C

Configuration SSL pour le service web LoadPIMS

Introduction

Le service Web LoadPIMS fournit une interface de service Web aux services d'automatisation du client pour charger par programme les fichiers PIMS sur le DNCS en vue d'activer STB. Pour sécuriser ce service sur le DNCS, les deux modifications de configuration suivantes doivent être effectuées :

- Activer SSL sur le serveur Web Apache
- Définir une configuration d'authentification de base sur loadDhctService

La configuration SSL nécessite une clé de serveur et des certificats de serveur. Le certificat peut être généré avec les utilitaires openssl ou bien le client peut choisir de fournir ces certificats pour la configuration SSL. Ces modifications de configuration s'appliquent au DNCS version 4.3.1 avec le serveur Apache version 2.0.53.

Remarque : Nous suggérons aussi d'utiliser la même paire de clés de certificat sur chaque DNCS, car cela permet au client d'accéder à plusieurs DNCS et autorise la gestion de l'utilisation des certificats.

Dans cette annexe

Installer les certificats sur le DNCS

L'accès au shell root est requis pour effectuer toutes les opérations de configuration du serveur Web Apache.

Les opérations suivantes sont effectuées pour installer le certificat SSL sur le DNCS :

- Une demande de signature de certificat (CSR) est générée sur le DNCS et envoyée à une autorité de certification (CA) de confiance.
- L'autorité de certification délivre un certificat numérique correspondant à installer sur le DNCS. (Le certificat racine de l'autorité de certification devra probablement être également installé.)
- Le certificat (accompagné de ses clés publiques et privées correspondantes) doit être copié manuellement vers un autre DNCS.

Installer le certificat numérique de l'autorité de certification

À ce stade, les fichiers de certificat et de clés suivants doivent résider sur votre système :

- server.crt : le certificat de serveur signé par l'autorité de certification

  Remarque : Reportez-vous à ***Création d'un certificat de clé de serveur auto-signé*** (à la page 113) pour créer des certificats auto-signés.
- server.key : la clé de serveur privée ; aucun mot de passe n'est nécessaire au démarrage d'Apache
- server.key.secure : La clé protégée par phrase de passe privée

Remarque : Si vous n'avez pas les fichiers de certificat numérique et la clé privée du serveur et que vous avez besoin d'en générer une, reportez-vous à ***Générer le CSR*** (à la page 116) pour créer le fichier privé server.key et pour consulter la procédure de demande de certificats numériques à l'autorité de certification.

1. Téléchargez le server.crt signé reçu de l'autorité de certification sur le serveur DNCS dans le répertoire /etc/opt/certs/.
2. Saisissez la commande ci-après puis appuyez sur **Entrée** pour copier le fichier server.crt dans cacert.crt.

   ```
   cp /etc/opt/certs/server.crt /etc/opt/certs/cacert.crt
   ```

Installer le certificat racine de l'autorité de certification de confiance

Si l'authentification du certificat du client est requise, le certificat de l'autorité racine de l'autorité de certification qui signe le certificat client doit être installé dans le fichier /etc/opt/certs/cacert.pem. Nous avons recommandé d'ajouter le certificat racine de l'autorité de certification à ce fichier, mais cela n'est pas obligatoire.

Saisissez les commandes suivantes puis appuyez sur **Entrée** pour installer le certificat racine de l'autorité racine de confiance.

```
cp /etc/opt/certs/cacert.pem /etc/opt/certs/cacert.pem.`date
+%m%d%y`
```

```
cat CA_NSO.crt.txt >> /etc/opt/certs/cacert.pem
```

Le tableau suivant répertorie les fichiers et les autorisations appropriés :

Fichier	Autorisation :		Propriétaire : Groupe	Commentaires
server.key	400	-r--------	root:root	Clé privée générée sur le DNCS (première étape de la procédure ***Générer le CSR*** (à la page 116)). Pour ne pas effectuer la procédure Générer le CSR et utiliser le même dncs_server.csr.crt reçu du NSO sur tous les DNCS, vous devez copier le fichier server.key sur tous les autres contrôleurs DNCS. Notez que ce fichier ne contient pas la phrase de passe et qu'il doit donc être conservé de manière appropriée. Pour copier ce fichier d'un contrôleur DNCS configuré vers un autre DNCS en cours de configuration, vous pouvez copier à la place le fichier server.key.secure. Toutefois, vous aurez besoin de la phrase de passe qui a été utilisée lors de l'extraction du fichier server.key (***Générer le CSR*** (à la page 116) première étape) depuis le fichier server.key.secure.
server.crt	444	-r--r--r--	root:root	Fichier dncs_server.csr.crt renommé server.crt.
server.key.secure	400	-r--------	root:root	Ce fichier est une clé de serveur protégée par phrase de passe et appropriée pour copier/sauvegarder, etc. La commande suivante extrait le fichier server.key si vous choisissez de copier le fichier server.key.secure depuis un autre DNCS (et que vous n'avez pas copié le fichier server.key) : `openssl rsa -in server.key.secure -out server.key`

Fichier	Autorisation :		Propriétaire : Groupe	Commentaires
cachain.crt	444	-r--r--r--	root:root	Ce fichier peut être identique au fichier server.crt et vous pouvez donc copier server.crt sur cachain.crt.

cacert.pem	444	-r--r--r--	root:root	Le fichier CA_NSO.crt est concaténé dans ce fichier en utilisant la commande suivante :
				`cp /etc/opt/certs/cacert.pem /etc/opt/certs/cacert.pem.`date +%m%d%y``
				`cat CA_NSO.crt.txt >> /etc/opt/certs/cacert.pem`

Configurer Apache pour autoriser la connexion des clients

Créer la directive pour le service loadPIMS

1 Utilisez un éditeur de texte pour créer le fichier /etc/apache2/conf/loadPIMS.https contenant les directives ci-après.

Remarque : Si ce fichier existe déjà, reportez-vous à ***Configurer les adresses IP client pour le service loadPIMS*** (à la page 100) pour autoriser une connexion avec le service Web loadPIMS.

Exemple : Le fichier doit être similaire à l'exemple suivant :

```
<Location /dncs/soap/loadPIMS>
   # SSLVerifyClient none
   # SSLCipherSuite +ADH-RC4-MD5
   ProxyPass
   http://localhost:18284/dncs/soap/loadPIMS
   ProxyPassReverse
   http://localhost:18284/dncs/soap/loadPIMS
   Order Deny,Allow
   Allow from localhost
   Allow from dncs
   Allow from appservatm
   #Allow from client_ip
   Deny from all
</Location>
```

Remarque : Le numéro de port 18284, utilisé dans l'exemple, doit correspondre à la valeur de la variable **SERVER_PORT** figurant dans le fichier /dvs/dncs/etc/LoadDhctServerSOAPCfg.cfg.

2 Mettez en commentaire, s'il y a lieu, les lignes suivantes du fichier rpcserver.conf :

```
#ProxyPass         /dncs/soap/loadPIMS
http://localhost:18284/dncs/soap/loadPIMS
#ProxyPassReverse  /dncs/soap/loadPIMS
http://localhost:18284/dncs/soap/loadPIMS
```

Configurer les directives WS-BOSS

Cette étape de configuration est facultative et est requise uniquement pour accéder à l'interface WS-BOSS. La configuration de WS-BOSS s'effectue via le fichier /etc/apache2/conf/boss.http. Notez que dans les versions de systèmes antérieures à la version 4.5, la configuration de WS-BOSS est conservée dans le fichier rpcserver.conf. Si votre système contient le fichier rpcserver.conf, procédez comme suit :

1. Mettez en commentaire les lignes suivantes du fichier rpcserver.conf :

```
#ProxyPass          /dncs/soap/bossreq
http://localhost:18084/dncs/soap/bossreq
#ProxyPassReverse   /dncs/soap/bossreq
http://localhost:18084/dncs/soap/bossreq
```

2. Utilisez un éditeur de texte pour créer le fichier /etc/apache2/conf/boss.http contenant les directives suivantes :

```
<Location /dncs/soap/bossreq>
   # The SSL configuration is not supported prior to 4.5
   #SSLVerifyClient      require
   #SSLVerifyDepth       5
   ProxyPass     http://localhost:18084/dncs/soap/bossreq
   ProxyPassReverse http://localhost:18084/dncs/soap/bossreq

   # The following directives will not be present after 4.5 as
client-cert
   # authentication will be used. This should be present if
client access to WS-BOSS
   # over HTTP is required.
   Order Deny,Allow
   Allow from localhost
   Allow from dncs
   Allow from appservatm
   #Allow from client_ip
   Deny from all
</Location>
```

Remarque : Les demandes envoyées à ces URL relatives seront définies si un *allow* n'est pas spécifiquement ajouté pour permettre à un client de se connecter au serveur Apache. La procédure suivante, **Configurer les adresses IP des clients pour le service loadPIMS** présente comment ajouter l'adresse IP d'un client à la liste des adresses IP autorisées à se connecter aux services web DNCS.

Configurer les adresses IP des clients pour le service loadPIMS

1. Obtenez la liste des adresses IP des clients qui se connecteront au serveur DNCS.
2. Ouvrez le fichier /etc/apache2/conf/loadPIMS.https et recherchez la section qui

contient la directive <Location /dncs/soap/loadPIMS>. Ajoutez ici ces adresses IP de clients selon l'exemple suivant :

```
<Location /dncs/soap/loadPIMS>
   #SSLVerifyClient none
   #SSLCipherSuite +ADH-RC4-MD5
            Order Deny, Allow
            Allow from localhost
            Allow from dncs
            Allow from appservatm
   #Allow from client_ip
         Allow from client_ip1
         Allow from client_ip2
         Deny from all
</Location>
```

Remarque : Cet exemple montre l'ajout de **client_ip1** et **client_ip2** à la liste des clients autorisés à accéder au serveur.

Configurer les adresses IP des clients pour WS-BOSS

Le protocole SSL n'est pas pris en charge actuellement pour l'interface WS-BOSS. Si la prise en charge de WS-BOSS n'est pas requise, passez cette section. Sinon, le fichier /etc/apache2/conf/boss.http doit être modifié en ajoutant les adresses IP des clients selon l'exemple suivant :

```
<Location /dncs/soap/bossreq>
      # The SSL configuration is currently not supported
      #SSLVerifyClient      require
      #SSLVerifyDepth       5
      ProxyPass
      http://localhost:18084/dncs/soap/bossreq
      ProxyPassReverse
      http://localhost:18084/dncs/soap/bossreq

      # The following directives will not be present after 4.5 as
client-cert
      # authentication will be used. This should be present if
client access to WS-BOSS
      # over HTTP is required.
      Order Deny,Allow
            Allow from localhost
            Allow from dncs
            Allow from appservatm
      #Allow from client_ip
            Allow from client_ip1
            Allow from client_ip2
      Deny from all
</Location>
```

Remarque : Cet exemple montre l'ajout de client_ip1 et client_ip2 à la liste des clients autorisés à accéder au service WS-BOSS.

Modifications nécessaires du fichier /etc/apache2/httpd.conf

Ajoutez une nouvelle directive Import dans la directive <VirtualHost *:80 *:8045>, juste avant la ligne </VirtualHost>. Aidez-vous de l'exemple suivant :

```
<VirtualHost *:80 *:8045>
    #
    # "/var/apache2/cgi-bin" should be changed to whatever your
ScriptAliased
    # CGI directory exists, if you have that configured.
    #
    # Allow cgi-bin access only on local box or if authenticated
      <Directory "/var/apache2/cgi-bin">
                  AllowOverride None
            Options None
                  Order Allow,Deny
                  Allow from all
      </Directory>
      <Location />
            Order Allow,Deny
            Allow from localhost
            Allow from dncs
            Allow from appservatm
            ErrorDocument 403 "<html><head><title>Error
403</title></head><body><h2>SECURITY WARNING</h2>Web connections
are only allowed from localhost.</body></html>"
      </Location>
Include /etc/apache2/conf/*.http
</VirtualHost>
```

Activer le SSL (Secure Socket Layer) avec Apache2

Modifications nécessaires du fichier /etc/apache2/ssl.conf

Le tableau suivant répertorie les propriétés de configuration SSL qui sont modifiées dans le fichier ssl.conf :

Paramètres de configuration SSL		
Variables ssl.conf		
SSLCipherSuite		Besoin d'ajouter ADH-RC4-MD5
SSLCertificateFile	/etc/opt/certs/server.crt	
SSLCertificateKeyFile	/etc/opt/certs/server.key	
SSLCertificateChainFile	/etc/opt/certs/cachain.crt	Chaîne de certificat d'autorité de certification du certificat de serveur Ce fichier doit contenir la chaîne intégrale du certificat de l'autorité de certification qui est utilisée pour signer le certificat de serveur. Le certificat de l'autorité de certification NSO doit être ajouté à ce fichier.
SSLCACertificateFile	/etc/opt/certs/cacert.pem	Les certificats de l'autorité de certification doivent être placés ici si une authentification par certificat est requise pour le client. Une authentification par certificat peut être nécessaire pour l'interface de facturation (version 4.5).

Les étapes suivantes ont trait aux modifications nécessaires pour activer SSL sur le serveur DNCS. Vérifiez que vous êtes l'utilisateur racine.

1. Suivez les instructions ci-après pour désactiver le service Apache2 sur un système Solaris 10.
   - **a** Saisissez **svcs -a | grep apache** puis appuyez sur **Entrée**.
   - **b** Les résultats de l'étape a indiquent-ils que le service Apache2 est actif (en ligne) ?
     Exemple : `online 0:45:44 svc:/network/http:apache2`
     - Si **c'est le cas**, saisissez **svcadm disable apache2** puis appuyez sur **Entrée**.
     - Si **ce n'est pas le cas**, passez à l'étape 2.

2 Saisissez les commandes suivantes puis appuyez sur **Entrée** pour activer SSL avec svccfg.

```
svccfg
svc:> select apache2
svc:/network/http:apache2> listprop httpd/ssl
httpd/ssl boolean false
svc:/network/http:apache2> setprop httpd/ssl = true
svc:/network/http:apache2> exit
```

3 Éditez le fichier /etc/apache2/ssl.conf et modifiez la propriété "SSLCipherSuite" en ajoutant "ADH-RC4-MD5". Cela active CipherSuite ADH-RC4-MD5 sur le service Apache. La ligne mise à jour doit être similaire à l'exemple suivant :

```
SSLCipherSuite ALL:!EXPORT56:-AES256-SHA:-DHE-RSA-AES256-SHA:-
DHE-DSS-AES256-SHA:RC4+RSA:+ADH-RC4-
MD5:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
```

Remarque : L'attribut par défaut de la propriété SSLCipherSuite est `'ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP''`.
Ceci est en cours de modification pour autoriser l'échange de clés Diff-Hellman anonyme, l'encodage RC4 et l'algorithme de hachage MD5 selon l'ICD de loadPIMS. L'algorithme de hachage ADH-RC4-MD5 doit être conservé pour toutes les versions futures du DNCS. La valeur par défaut '!ADH' ne permet un nouvel ajout d'ADH et doit être supprimé.

4 Suivez les instructions ci-après pour modifier le fichier ssl.conf.

Remarque : Un bug dans le code Apache 2.0.53 nécessite cette modification.

a Saisissez la commande ci-après puis appuyez sur **Entrée**.

```
cp ssl.conf  ssl.conf.`date +%m%d%y`
```

b Ouvrez le fichier ssl.conf dans un éditeur de texte.

c Recherchez l'entrée suivante :

```
VirtualHost _default_
```

d Remplacez cette entrée par `<VirtualHost *:443>`.

```
:%s/VirtualHost _default_/VirtualHost */
```

e Recherchez maintenant `ServerName acme:443 or ServerName %%%localhost%%%:443`.

f Remplacez cette entrée par `ServerName <hostname>:443`.

g Enregistrez et fermez le fichier.

5 Ajoutez une nouvelle directive Location et Import dans la directive <VirtualHost *:443>, juste avant la ligne </VirtualHost>. Les modifications doivent être similaires à l'exemple suivant :

```
<VirtualHost *:443>
   # contents omitted below
   .
   .
   <Location />
            Order Deny,Allow
            Allow from localhost
            Allow from dncs
            Deny from all
            ErrorDocument 403 "<html><head><title>Error
403</title></head><body><h2>SECURITY WARNING</h2>Web
connections are only allowed from localhost.</body></html>"
   </Location>
   Include /etc/apache2/conf/*.https
</VirtualHost>
```

6 Avant l'actualisation du service Apache, testez les modifications de configuration en saisissant la commande suivante puis en appuyant sur **Entrée**.

Important : Le message **Syntax OK** doit alors s'afficher.

```
/usr/apache2/bin/httpd -t
```

7 Suivez les instructions ci-après pour redémarrer le service Apache2.

a Saisissez `svcadm refresh apache2` puis appuyez sur **Entrée**.

b Saisissez `svcadm clear apache2` puis appuyez sur **Entrée**.

Remarque : Si le service Apache n'est pas à l'état erreur, le message suivant s'affiche :

```
svcadm: Instance "svc:/network/http:apache2" is not in a
maintenance or degraded state.
```

c Saisissez `svcadm enable apache2` puis appuyez sur **Entrée**.

8 Saisissez **cd /etc/opt/certs** puis appuyez sur **Entrée**.

9 Saisissez la commande suivante puis appuyez sur **Entrée** pour créer la liaison nécessaire.

```
ln -s /etc/opt/certs/server.crt  cachain.crt
```

10 L'authentification client est-elle nécessaire sur ce système ?

- Si **c'est le cas**, saisissez `cp server.crt cacert.pem` puis appuyez sur **Entrée**.
- Si **ce n'est pas le cas**, mettez en commentaire, dans le fichier ssl.conf, la ligne qui comprend SSL VerifyClient.

11 Saisissez `ps -ef | grep apache2` puis appuyez sur **Entrée** pour vérifier que le processus Apache2 fonctionne avec SSL.

Exemple : Un message similaire au message suivant doit s'afficher :

```
dncs 18058 18054  0 00:45:45 ?   0:00 /usr/apache2/bin/httpd -
k start -DSSL
root 18054  1   0 00:45:44 ?  0:03 /usr/apache2/bin/httpd -k
start -DSSL
```

12 Saisissez la commande suivante puis appuyez sur **Entrée** pour vérifier que le traitement SSL est actif.

```
openssl s_client -cipher ADH-RC4-MD5 -connect localhost:443 -
state -debug
```

Exemple : Une sortie similaire à la sortie suivante doit s'afficher :

```
CONNECTED(00000004)
SSL_connect:before/connect initialization
write to 0008E7D8 [0008EDE8] (46 bytes => 46 (0x2E))
0000 - 80 2c 01 03 01 00 03 00-00 00 20 00 00 18 23 98
.,........ ...#.
0010 - 3d 9f 16 9f 4c 09 90 92-fe 94 36 81 09 6d e0 b4
=...L.....6..m..
0020 - e1 92 03 52 48 df 2c 57-42 9a 48 f3 98 a1
...RH.,WB.H...
SSL_connect:SSLv2/v3 write client hello A
read from 0008E7D8 [00094348] (7 bytes => 7 (0x7))
0000 - 16 03 01 00 4a 02
....J.
0007 - <SPACES/NULS>
read from 0008E7D8 [0009434F] (72 bytes => 72 (0x48))
0000 - 00 46 03 01 4b 7c 7b a6-99 60 bb 97 1a a6 63 3c
.F..K|{..`....c<
0010 - 86 b0 11 13 a3 8d 53 72-24 aa 68 62 e5 f5 ae 91
......Sr$.hb....
0020 - 80 aa 06 c3 20 49 36 a9-0e fb cf 7a aa 96 c1 21   ....
I6....z...!
0030 - d1 55 75 3a 22 2e 57 cb-1b 4b 2d 88 88 11 43 de
.Uu:".W..K-...C.
0040 - 31 6c 71 84 5d 00 18
1lq.]..
```

```
0048 - <SPACES/NULS>
SSL_connect:SSLv3 read server hello A
read from 0008E7D8 [00094348] (5 bytes => 5 (0x5))
```

Remarque : Si cette commande génère une erreur, reportez-vous à ***Dépannage de SSL*** (à la page 112).

13 Ouvrez un navigateur sur un client autorisé à se connecter au serveur DNCS et saisissez l'adresse IP du DNCS. Vérifiez le certificat de serveur.

Activer l'authentification des certificats de client

C'est une étape facultative dans la configuration SSL et elle est uniquement requise si une authentification par certificat de client est nécessaire.

1. Connectez-vous au DNCS en tant qu'utilisateur **racine**.
2. Saisissez `cd /etc/opt/certs` puis appuyez sur **Entrée**.
3. Saisissez `cp server.crt  cacert.pem` puis appuyez sur **Entrée** pour copier le fichier server.crt dans cacert.crt.

Configurer le loadDhctService pour l'authentification de base

Suivez ces instructions en tant qu'utilisateur dncs.

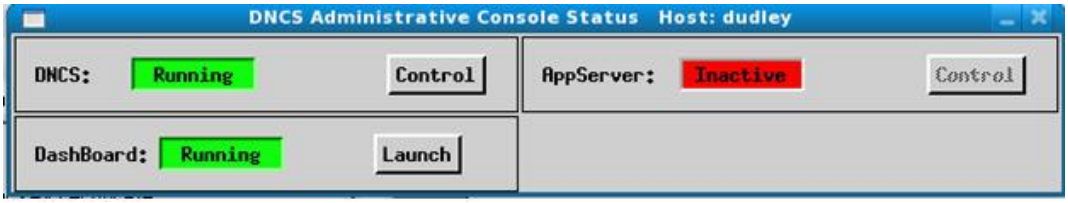
Le fichier de configuration du processus loadDhctService se trouve à l'adresse suivante : /dvs/dncs/etc/LoadDhctServerSOAPCfg.cfg. Voici une partie du fichier en exemple :

```
# Port on which server listens for incoming requests
SOAP_PORT = 18284
# Enable/Disable SOAP SSL
SSL_MODE = DISABLE
# Enable or Disable basic authentication (parameters:
DISABLE/ENABLE)
BASIC_AUTH = ENABLE
# Server User Name
SERVER_USER_NAME = dncs
# Server Password
SERVER_PASSWD = dncs123
```

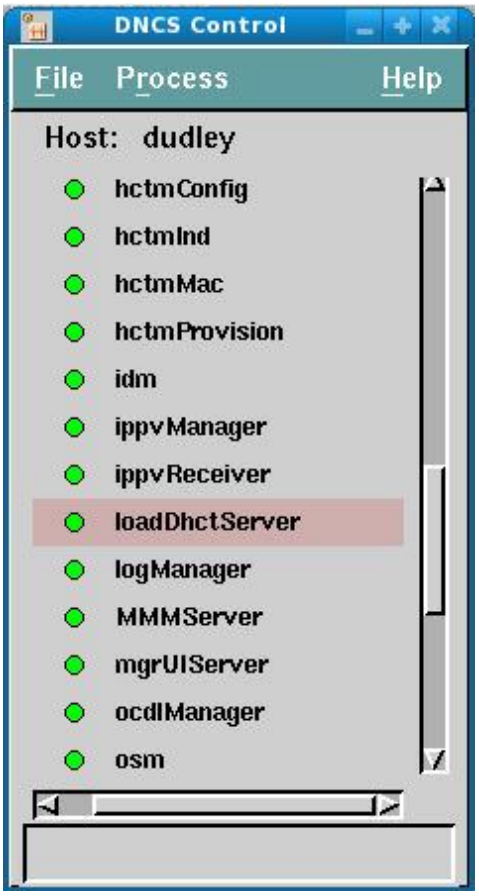
La liste suivante contient une description des paramètres :

- **Server_Port (SOAP_PORT)** - Il s'agit du port sur lequel le loadDhctServer écoute. Il s'agit du port proxy figurant dans le fichier de configuration Apache loadPIMS.https.
- **SSL_MODE** - Ce paramètre doit toujours avoir la valeur **DISABLE**. Le protocole SSL est activé sur la couche du serveur Apache.
- **BASIC_AUTH** - Affectez-lui la valeur **ENABLE**.
- **SERVER_USER_NAME** - Ce paramètre de configuration définit le nom d'utilisateur utilisé par le client de service web loadDhctService pour effectuer l'authentification de base.
- **SERVER_PASSWD** - Ce paramètre de configuration définit le mot de passe à utiliser par le client pour l'authentification de base.

1 Lancez les processus DNCS Control en cliquant sur **Control** dans la fenêtre DNCS Administrative Console Status.



2 Mettez en surbrillance le processus **loadDhctServer** dans la fenêtre DNCS Control.



3 Cliquez sur **Process** puis sélectionnez **Start Process** pour lancer le processus loadDhctServer.

Remarque : Lorsque cette procédure est achevée, configurez le client pour qu'il utilise une authentification de base sur SSL avec l'ID utilisateur et le mot de passe spécifiés dans le fichier /dvs/dncs/etc/LoadDhctServerSOAPCfg.cfg.

Dépannage de SSL

- `svcs -a | grep apache2`

  Si la sortie de cette commande ne répertorie pas le serveur Apache2 comme étant en ligne, le processus httpd doit être supprimé. Suivez les instructions ci-après pour supprimer le processus httpd.

  a Saisissez `ps -ef | grep httpd` puis appuyez sur **Entrée**.

  b Saisissez `kill [PID]` puis appuyez sur **Entrée**, [PID] étant l'ID de processus renvoyé par la commande précédente.

- Erreur `openssl:  not found`

  Si la commande **openssl** n'est pas disponible dans la variable PATH, le chemin d'accès d'openssl doit être explicitement spécifié. L'outil openssl se trouve dans le répertoire suivant : /usr/sfw/bin/openssl

- Si la génération du CSR avec l'option aes256 échoue avec une erreur relative à SUNWcry, générez alors la clé 3DES en saisissant la commande ci-après puis en appuyant sur **Entrée**.

  ```
  openssl genrsa -des3 -out server.key 1024
  ```

- Si la commande s_client **openssl** (étape 12 de ***Modifications nécessaires du fichier /etc/apache2/ssl.conf*** (à la page 104)) génère une erreur, essayez cette commande à la place.

  ```
  openssl s_client -connect localhost:443 -state -debug
  ```

  Si cette commande réussit, c'est probablement dû au fait que SSLCipherSuite n'est pas correctement configuré. Réessayez la commande indiquée à la puce 3 et actualisez le serveur Apache.

Bon à savoir

Création d'un certificat de clé de serveur auto-signé

Effectuez les opérations suivantes pour générer un certificat auto-signé. Une clé SSL et un certificat existants peuvent aussi être utilisés.

Remarque : Exécutez toutes les commandes en tant qu'utilisateur racine dans une fenêtre d'émulation de terminal sur le DNCS.

1. Suivez les instructions ci-après pour ajouter le chemin d'accès de la commande openssl.
   - **a** Saisissez `PATH=$PATH:/usr/sfw/bin` puis appuyez sur **Entrée**.
   - **b** Saisissez `export PATH` puis appuyez sur **Entrée**.
2. Saisissez `cd /etc/apache2` puis appuyez sur **Entrée**.
3. Saisissez la commande suivante puis appuyez sur Entrée pour créer la clé de serveur et le certificat de serveur.

   ```
   openssl genrsa -out /etc/opt/certs/server.key 1024
   ```

   Remarque : Vous pouvez aussi spécifier le format de cryptage de la clé et le nombre de bits de la clé. Les types de cryptage de clé admis sont les suivants :
   - **des** - crypte la clé générée avec le DES en mode cbc
   - **des3** - crypte la clé générée avec le DES en mode ede cbc (clé de 168 bits)
   - **aes128**, **aes192**, **aes256** — crypte la sortie PEM en mode cbc aes

   Les valeurs habituelles du nombre de bits de la clé sont 1024, 2048 et 4096.
4. Saisissez la commande suivante puis appuyez sur **Entrée** pour générer une demande de signature de certificat :

   ```
   openssl req -new -key /etc/opt/certs/server.key -out
   /etc/opt/certs/server.csr
   ```
5. Si vous voulez signer le certificat vous-même, (le certificat généré expirera), saisissez la commande ci-après puis appuyez sur **Entrée**.

   ```
   openssl x509 -req -in /etc/opt/certs/server.csr -signkey
   /etc/opt/certs/server.key -out /etc/opt/certs/server.crt
   ```
6. Saisissez la commande suivante puis appuyez sur **Entrée** pour copier le fichier server.crt dans cacert.crt :

   ```
   cp /etc/opt/certs/server.crt /etc/opt/certs/cacert.crt
   ```
7. Une authentification du client est-elle requise ?
   - Si **c'est le cas**, suivez les étapes présentées dans ***Activer l'authentification du certificat du client*** (à la page 109).
   - Si **ce n'est pas le cas**, vous avez terminé cette procédure.

Exemple d'authentification de base

L'exemple suivant concerne **ResetStagingState** :

```
GET /dncs/loadPIMS HTTPS/1.0
Host: localhost
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
 xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:loadPIMS="urn:loadPIMS.xsd">
 <SOAP-ENV:Body>
  <loadPIMS:ResetStagingState>
   <loadPIMS:resetStagingStateRequest>
    <loadPIMS:dhctMacAddress></loadPIMS:dhctMacAddress>
   </loadPIMS:resetStagingStateRequest>
  </loadPIMS:ResetStagingState>
 </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Dans cet exemple, l'ID utilisateur et le mot de passe (Aladdin:open sesame) est codé sous forme de chaîne à base64. Reportez-vous à **Order Management ICD** pour plus d'informations sur les mécanismes d'authentification.

Gestion des droits d'accès sur le client

Pour désactiver la validation de certificats en vue des tests, vous devez remplacer le gestionnaire de droits d'accès par défaut par un gestionnaire de droits d'accès qui fait confiance à tous les certificats. Utilisez le code suivant comme exemple :

```
// Create a trust manager that does not validate certificate
chains
TrustManager[] trustAllCerts = new TrustManager[]{
```

```
    new X509TrustManager() {
        public java.security.cert.X509Certificate[]
getAcceptedIssuers() {
            return null;
        }
        public void checkClientTrusted(
            java.security.cert.X509Certificate[] certs, String
authType) {
        }
        public void checkServerTrusted(
            java.security.cert.X509Certificate[] certs, String
authType) {
        }
    }
};

// Install the all-trusting trust manager
try {
    SSLContext sc = SSLContext.getInstance("SSL");
    sc.init(null, trustAllCerts, new
java.security.SecureRandom());

HttpsURLConnection.setDefaultSSLSocketFactory(sc.getSocketFactory
());
} catch (Exception e) {
}

// Now you can access an https URL without having the certificate
in the truststore
try {
    URL url = new URL("https://hostname/index.html");
} catch (MalformedURLException e) {
}
```

Générer le CSR

1. Saisissez la commande suivante puis appuyez sur **Entrée** pour créer la demande avec un certificat aes256. (Vous serez invité à créer une phrase de passe.)

   ```
   openssl genrsa -aes256 -out server.key 1024
   ```

   Remarque : Sur le DNCS version 4.3.1, vous pouvez recevoir une erreur relative à SUNWcry. Dans ce cas, vous pouvez aussi créer une demande avec une clé 3DES (vous serez invité à créer une phrase de passe). Reportez-vous à ***Dépannage de SSL*** (à la page 112) (troisième puce) pour plus d'informations.

2. Saisissez la commande suivante puis appuyez sur **Entrée** pour générer le CSR à l'aide du server.key.

   ```
   openssl req -new -key server.key -out server.csr
   ```

   Remarque : Vous êtes invité à fournir les champs du CSR, notamment les éléments suivants :

   - **Nom du pays :** US
   - **État :** Pennsylvanie
   - **Nom de la localité :** Philadelphie
   - **Nom de l'entreprise :** Comcast Cable Communications Management LLC
   - **Unité organisationnelle :** CET
   - **Nom commun :** [Nom de domaine qualifié complet, par exemple : service.comcast.net]
   - **Adresse e-mail :** admin@cable.comcast.net
   - **Un mot de passe de stimulation :** .[tapez un point "." pour laisser la zone vide et ne pas utiliser de valeur par défaut]
   - **Un nom de société facultatif :** .[tapez un point "." pour laisser la zone vide et ne pas utiliser de valeur par défaut]

3. Saisissez les commandes suivantes puis appuyez sur **Entrée** pour examiner le fichier server.key et la demande de certificat. (Vous serez invité à entrer la phrase de passe pour le fichier server.key)

   ```
   openssl rsa  -text -in server.key
   openssl req  -text -in server.csr
   ```

4 Envoyez le fichier server.csr par mail à l'autorité de certification. Certaines autorités de certification fournissent un site Web pour y coller le contenu du CSR. Ensuite, envoyez vous-même par e-mail le certificat signé.

5 Saisissez les commandes suivantes puis appuyez sur **Entrée** pour créer une clé de serveur pour laquelle Apache ne demande pas de mot de passe.

```
openssl rsa -in server.key -out server.key.insecure
mv server.key server.key.secure
mv server.key.insecure server.key
```

Important : Bien qu'il ne soit pas nécessaire d'entrer un mot de passe lors du redémarrage du serveur Apache, toute personne obtenant cette clé non sécurisée pourra décrypter vos communications. Conservez-la très soigneusement pour vos autorisations.

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678.277.1000
www.cisco.com

Octobre 2011 Imprimé aux États-Unis Référence 4040725 Rév. A