Clean Access Server - Forum Aux Questions

Contenu

Introduction

Ce document aborde les questions fréquemment posées (Foires aux questions) liées au serveur de Cisco Clean Access (autrefois serveur de Perfigo SecureSmart).

Les noms de produit ont été modifiés. Ce tableau présente les anciens et les nouveaux noms :

Ancien nom	Nouveau nom
SmartManager	Clean Access Manager
SecureSmart Server	Clean Access Server
SmartEnforcer	Clean Access Agent
CleanMachinesAPIs	Clean Access API

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Installation

Q. Comment est-ce que j'installe les pilotes SCSI LSI pour le Dell 1750 ou d'autres ?

A. Procédez comme suit :

1. Sauvegardez le fichier de rawrite à C:\ et au gestionnaire LSI. Fichiers de mise à jour dans le

même répertoire.
2. Ouvrez une invite de commande et entrez dans **C:\rawrite**.
3. Écrivez le nom complet du fichier source et de la destination en fonction à deux disquettes.
4. Insérez la CD d'installation d'ordinateurs de Clean Access Manager (autrefois CleanMachines) dans le serveur de Cisco Clean Access ou le gestionnaire de Cisco Clean Access.
5. Écrivez la **coutume à la** demande de `boot>`.
6. Suivez les instructions d'entrer dans le disque de mise à jour, et puis le disque de gestionnaire.

Configuration

Q. Comment est-ce que je configure les gestionnaires de Broadcom ?

A. Procédez comme suit :

1. Console dans la case : `cd /lib/modules/kernel-2.4.9-perfigo/drivers/addon/bcm5700`

   `insmod ./bcm5700.o`
2. Si étape 1 a comme conséquence aucune erreurs, sélectionnez la commande de **vi /etc/modules.conf** et ajoutez ces deux lignes : `alias eth0 bcm5700`

   `alias eth1 bcm5700`

Q. Comment est-ce que je configure le serveur de Cisco Clean Access derrière une passerelle NAT ?

A. Terminez-vous ces étapes pour chaque serveur de Cisco Clean Access déployé derrière une passerelle NAT.

1. Le SSH au serveur de SecureSmart ou utilisent une console série pour ouvrir une session comme racine.
2. Éditez le fichier de **/perfigo/access/bin/starttomcat**.
3. Ajoutez **- Djava.rmi.server.hostname=<CAS_hostname> à la** ligne de variable **CATALINA_OPTS**.
4. **Reprise de perfigo de service de** reprise.
5. Le SSH à SmartManager ou utilisent une console série pour ouvrir une session comme racine.
6. Éditez le fichier de **/etc/hosts** et ajoutez cette ligne : `<public_IP_address> <securesmart_hostname> <securesmart_hostname>`

Duplex et configurations de débit

Q. Comment est-ce que je place le duplex et la vitesse sur les cartes d'interface de réseau serveur de Cisco Clean Access ?

A. Employez ceci comme guide pour installer les networks interface cards appropriés dans le fichier de /etc/modules.conf.

Remarque: Ajoutez le paramètre d'options à l'extrémité pour le fichier de /etc/modules.conf avec l'utilisation de l'éditeur vi.

- Placez les cartes du broadcom 5700 au bidirectionnel simultané de 100 Mbits/s : **`options bcm5700 line_speed=100,100 auto_speed=0,0 duplex=1,1`**
- Placez les cartes du broadcom 5700 au bidirectionnel simultané de 1000 Mbits/s : **`options bcm5700 line_speed=1000,1000 auto_speed=0,0 duplex=1,1`**
- Placez les cartes e1000 au bidirectionnel simultané de 100 Mbits/s : **`options e1000 Speed=100,100 Duplex=2,2`**
- Placez les cartes e1000 au bidirectionnel simultané de 1000 Mbits/s : **`options e1000 Speed=1000,1000 Duplex=2,2`**
- Placez les cartes eepro100 au bidirectionnel simultané de 100 Mbits/s : **`options eepro100 option="0x30,0x30"`**

Q. Comment est-ce que je place le duplex/vitesse sur l'interface de Cisco Clean Access "bnx2" ?

A. Sur des périphériques de serveur de Cisco Clean Access (même sur le CAM), il y a des fichiers pour chaque interface réseau qui décrivent les propriétés et expédient/paramètres bidirectionnels.

Voici les étapes comment l'exécuter manuellement :

1. Changez le répertoire à **/etc/sysconfig/network-scripts**. Pour chaque interface il y a un fichier dans ce répertoire nommé ifcfg-ethX, où X peut être 0, 1, 2, etc.
2. Ajoutez cette ligne pour pour n'importe quelle interface vous voulez coder en dur les configurations : `ETHTOOL_OPTS="speed 100 duplex full autoneg off"`
3. Après qu'enregistrant le fichier, exécutez « une reprise de réseau de service ».
4. Assurez-vous que les positions de commutateur sont placées manuellement. Vérifiez vos configurations en émettant la commande d'**ethX d'eth-outil** sur le shell, où X peut être 0 ou 1 pour confirmer les paramètres bidirectionnels sont codés en dur. **Remarque:** Ceci interrompt le service momentanément. Maintenez ceci dans la considération si vous devez programmer un temps d'arrêt.

Q. Comment est-ce que je vérifie pour voir le duplex et la vitesse sur les cartes d'interface de réseau serveur de Cisco Clean Access (NIC) ?

A. Exécutez l'utilitaire de mii-**outil de la** ligne de commande. Cela fonctionne pour le NIC intégré, mais ne prend en charge pas des NIC de fibre.

Pour des NIC de fibre, utilisez la commande du **grep 'eth0** sur /var/log/messages.

Vous pouvez également émettre une **queue -** commande **f** sur /var/log/messages. Ceci affiche des messages toutes les fois qu'un NIC devient actif ou inactif.

Caractéristiques prises en charge

Q. Quel est le nombre de connexions VPN prises en charge par serveur de Cisco Clean Access ?

A. Aucune limite n'est placée pour IPsec.

PPTP et L2TP sont actuellement placés à 32 percent un tunnel chacun.

Q. Comment est-ce que je change l'adresse IP du serveur de Cisco Clean Access ? Est-ce que je dois supprimer et re-ajouter le serveur de Cisco Clean Access ?

A. Cisco recommande que vous changiez l'adresse IP du serveur de Cisco Clean Access par l'intermédiaire du gestionnaire UI. Quand l'adresse IP du serveur de Cisco Clean Access est changée du gestionnaire UI, redémarrez le serveur de Cisco Clean Access. Il essaye automatiquement de se connecter au gestionnaire de Cisco Clean Access sur la réinitialisation. Le gestionnaire de Cisco Clean Access change l'adresse IP du serveur de Cisco Clean Access dans la base de données et le SSKEY reste le même.

Remarque: Si vous supprimez et re-ajoutez le serveur de Cisco Clean Access, vous perdez tous les paramètres de configuration du serveur de Cisco Clean Access.

Q. Comment est-ce que je limite l'accès de SSH au serveur Cisco Clean Access ?

A. Ajoutez une ligne semblable à cet exemple afin de changer le fichier de **/etc/ssh/sshd_config** :

```
ListenAddress IP_address_of_where_you_want_ssh_to_allow_connections
```

Exemple :

```
ListenAddress 192.168.151.60
```

Émettez la commande de **reprise de sshd de service** afin de redémarrer le processus SSHD.

Q. Comment la configuration de rafale de bande passante fonctionne-t-elle ?

A. Sous CleanMachines, décochez **Windows tout** et sélectionnez chaque SYSTÈME D'EXPLOITATION indépendamment pour l'usage Require de SmartEnforcer ou pas.

Q. Je lis récemment dedans la version 3.3BETA d'installation et de guide d'administration de Clean Access Server à la page 68 que le nombre maximal recommandé de sous-réseaux par Clean Access Server est 1000. Je dois créer plus de 1000. Quelle est la limite ?

A. La limite de 1000 est un avertissement seulement. Si l'ordinateur a assez de mémoire (davantage que 1G), vous pouvez configurer jusqu'à 2500 sous-réseaux.

Q. Comment je gère une série de Points d'accès que j'ai sur une particularité VLAN qui est gérée par Clean Access Server. Je les ai ajoutés en Gestion de périphériques de Point d'accès ?

A. Ajoutez les adresses MAC des Points d'accès à la zone de **>Devices de filtres** par opposition à la section de Gestion de périphériques de Point d'accès.

Q. J'ai des sous-réseaux secondaires (secondaire parfois plusieurs) sur chaque VLAN. Le sous-réseau 150 est pour des clients, et le sous-réseau 172 est pour la

Gestion de notre équipement de réseau dans le bâtiment. Clean Access Server peut-il traiter de plusieurs sous-réseaux sur un VLAN simple ?

A. Un exemple de ce problème est :

```
!
  interface Vlan 106
   ip address 150.135.47.1 255.255.255.0
   ip address 172.16.10.1 255.255.255.192 secondary
  !
```

Clean Access Server est en mode virtuel de passerelle :

- Dans ce cas, Clean Access Server ne s'inquiète pas du nombre de sous-réseaux ou de leurs balises associées VLAN. Toutes les informations VLAN traversent sans des exceptions.

Clean Access Server est en mode de passerelle (vrai-IP ou NAT) :

- Dans ce cas, Clean Access Server fonctionne également comme l'un ou l'autre un relais DHCP ou un serveur DHCP. Dans la situation, la plage des adresses IP allouées dépend de la balise VLAN ou de l'adresse de passerelle qui dépend également de la balise VLAN.Par conséquent, Clean Access Server ne peut pas différencier (d'un point de vue DHCP) entre deux sous-réseaux sur le même VLAN. L'une limite est qu'un des deux sous-réseaux sur le même VLAN ne devrait pas utiliser le DHCP pour l'affectation d'adresses. Au lieu de cela, les adresses IP doivent être statiquement assignées. C'est le plus susceptible le point de droit pour le sous-réseau 172 dans le réseau puisqu'il se compose de l'équipement de réseau.

Q. Pourquoi est-ce que je ne peux pas ajouter Clean Access Server à Clean Access Manager (CAM) ?

A. Si vous ne pouvez pas ajouter Clean Access Server au CAM, alors c'est un problème de licence. Assurez-vous que le serveur que des permis sont générés a basé sur les Ethernets du CAM primaire 0 adresses MAC. Les adresses MAC sur le permis de serveur devraient apparier l'adresse MAC (primaire) du CAM.

1. Allez au **CAM GUI > gestion > Clean Access Manager > en autorisant**.
2. Exécutez « retirent tous les permis ».
3. Réinstallez les fichiers de licence de serveur de nouveau.

Q. Est-ce que je devrais générer un nouveau CSR pour renouveler le certificat sur Clean Access Server ?

A. Non. Pour le renouvellement du certificat sur Clean Access Server, ne générez pas un nouveau CSR. Cependant, si vous générez un nouveau CSR, puis vous devez télécharger la clé privée dans Clean Access Server. Après avoir téléchargé la clé privée, redémarrez Clean Access Server. Ceci complète le processus de renouvellement.

Q. Est-il possible de traverser le trafic de multidiffusion par le CCA ?

A. Non, Multidiffusion n'est pas pris en charge sous la vraie passerelle intrabande. Cependant, cela fonctionnera pour la passerelle hors bande ou virtuelle.

Q. Le NAC prend en charge-il le serveur 64-bit de Windows 2008 ?

A. Non, mais lui prend en charge le serveur de 32 bits de Windows 2008.

Q. Le NAC inclut-il une caractéristique pour reproduire les rôles de l'utilisateur et les stratégies/propriétés associées avec lui à un nouveau rôle de l'utilisateur ?

A. Non. Ceci ne peut pas être fait car il n'y a aucune une telle disposition dans le GUI.

Messages de log

Q. Dans /var/log/messages ou les messages de /var/log/ha-log je vois plusieurs messages de pulsation pour le Basculement. Pourquoi est-ce que c'est et comment est-ce que je le répare ?

A. Ce sont les messages de pulsation que vous voyez :

```
heartbeat: 2004/09/15_11:23:27 info: Heartbeat restart on node ss1

heartbeat: 2004/09/15_14:19:17 info: Heartbeat restart on node ss1

heartbeat: 2004/09/15_18:59:53 info: Heartbeat restart on node ss1

heartbeat: 2004/09/15_19:36:18 info: Heartbeat restart on node ss1
```

Vous voyez ces messages quand le serveur de pair est après une réinitialisation. Vous pouvez également le voir dans le login le serveur primaire quand :

- Vous émettez l'**arrêt de perfigo de service** et puis **entretenez le début de perfigo** sur le pair ou l'ordinateur de réserve.ou
- Redémarrez un pair ou un ordinateur de réserve.

Remarque: Quand vous émettez la commande de **reprise de perfigo de service**, elle ne déclenche pas ce log.

Q. Je vois Clean Access Server 2004-08-30 stats de système de 11:30:28 192.168.151.60 : Densité d'occupation 0 (maximum depuis la réinitialisation : 3) Mem : 261160960 237854720 23306240 212992 47259648 99737600 CPU 188552 153 91405324 194183 messages dans mes journaux d'événements. Qu'est-ce que cela signifie ?

A. Des statistiques de système sont générées pour chaque Clean Access Server géré par Clean Access Manager chaque heure par défaut. Les informations signalées incluent la densité d'occupation de chaque serveur, le chargement maximum depuis la réinitialisation, la mémoire, et l'utilisation du CPU.

- **Densité d'occupation** — La densité d'occupation est un nombre qui décrit le nombre de paquets qui attendent d'être traités par le serveur (par exemple, le chargement en cours qui est manipulé par Clean Access Server). Quand la densité d'occupation se développe, c'est une indication que les paquets attendent dans la file d'attente à traiter. Si la densité d'occupation est plus grande que 500 pour n'importe quelle à période cohérente (par

exemple, 5 minutes), alors il est indicatif que Clean Access Server ait une charge élevée régulière du trafic/de paquets qui entrent. Vous devez être concerné si le nombre atteint 500 ou le plus élevé.
- **Maximum depuis la réinitialisation** — Le nombre maximal de paquets dans la file d'attente en même temps (par exemple, le chargement maximum manipulé par Clean Access Server).
- **Mem** — Les statistiques d'utilisation de mémoire. Il y a six nombres (l'unité est des octets). Ces nombres signifient le total, utilisé, libre, partagé, des mémoires tampons, et antémémoire.
- **CPU** — Le chargement de processeur sur le matériel. Il y a quatre nombres qui fournissent des informations au sujet de l'utilisation du CPU (l'unité est des coups d'oeil - sur la plupart des systèmes, un coup d'oeil est une unité de temps du ms 10). Les nombres indiquent le temps passé par le système dans l'utilisateur, gentil, le système, et les processus de veille.

Pour l'exemple a fourni, système % = 91405324*100/(188552+153+91405324+194183) = 99.58%. De même, vous pouvez calculer les autres aussi bien. Cependant, sur Clean Access Server, l'heure système est en général plus grande que 90 pour cent. C'est le signe d'un système sain.

Messages d'erreur

Q. Pourquoi est-ce que je reçois `ne peux pas ajouter le` message d'`erreur du serveur de Clean Access` ?

A. Vérifiez ces éléments :

- Le secret partagé est identique sur le serveur de Cisco Clean Access et le gestionnaire de Cisco Clean Access.
- Les Certificats sont corrects.
- La Connectivité entre le serveur de Cisco Clean Access et le gestionnaire et le celui de Cisco Clean Access là ne sont pas aucun Pare-feu ordonne qui bloquent les ports RMI.

Q. Pourquoi je reçois l'`erreur réseau de CAS : Clean Access Server n'a pas pu établir une connexion sécurisée à Clean Access Manager au null.` message d'erreur ?

A. Vous pourriez recevoir cette erreur si le certificat de Clean Access Manager a expiré, ne pouvez pas êtes de confiance, ou ne pouvez pas être atteint. L'erreur est fondamentalement due des questions de CAS ou de CAM à transmission.

Afin de résoudre ce problème, vérifiez ces éléments :

- Assurez-vous que CAS et le CAM sont la même version.
- Si vous utilisez un nom pour le certificat, assurez-vous que le nom peut être résolu utilisant le nslookup.
- Utilisez l'IP de service pour le certificat de Basculement.
- Assurez-vous qu'ils sont temps synced avant de générer le certificat.
- Make sure a partagé la correspondance de secrets.
- Le Pare-feu ne devrait pas bloc d'ACL aucune transmission SSL.
- Ajoutez le certificat de CAM comme racine non standard à CAS.
- Vérifiez la résolution de noms de DN.
- Assurez-vous que le routage pour l'accessibilité entre le CAM et CAS est correct.

Q. Pourquoi est-ce que je reçois l'**erreur produite alors que la chaîne de certificat X509 de construction… ne peut pas trouver le certificat pour le** message d'erreur **suivant d'autorité de certification** ?

A. Vous devez utiliser le certificat racine correct. Si Microsoft Certificate Authority (CA) est utilisé, sauvegardez le certificat dans Base64 plutôt que le par défaut encodé.

Q. J'obtiens l'erreur de communication de serveur de l'authentification 2004-11-01 15:53:40, l'erreur de communication de baronet de 172.19.168.42 du ## [00:0E:35:5F:F9:91] et de serveur de l'authentification 2004-11-01 15:53:13, les erreurs de baronet de 172.19.168.42 du ## [00:0E:35:5F:F9:91] sur les journaux d'événements. Comment résoudre ce problème ?

A. Si vous exécutez le Basculement Clean Access Server en mode virtuel de passerelle, alors éditez le fichier de vi /etc/hosts et changez l'adresse SS-1 (Clean Access Server) à l'IP de service (adresse virtuelle). Vous devez les changer en les deux serveurs, active et état d'alerte de Clean Access.

- localhost de localhost de 127.0.0.1
- 192.168.1.2 SS-1 SS-1

Q. J'obtiens la signature de pile TCP/IP : Message INCONNU de l'UNKNOWN [65535:64:1:64:M1460,N,W2,N,N,T0,S,E:P] {}. Comment est-ce que je peux répare ceci et est-ce que comment je désactiver installe du client pour des iPhones ?

A. Voici les instructions qui devraient fonctionner pour ne pas exiger l'agent pour des iPhones :

1. Choisissez le rôle sous **Clean Access > la configuration générale > la connexion de l'agent**.
2. Choisissez **MAC_ALL** pour configurer les conditions requises d'agent pour le toucher d'iPhone ou d'iPod. Assurez-vous que l'**utilisation TOUTES LES configurations** pour la famille de MAC OS si aucune configuration de version-particularité n'est spécifiée est décoché, ainsi elle n'utilisera pas la configuration partagée de « TOUS ». En outre, assurez-vous que l'option de téléchargement d'agent d'exigence est décochée, ainsi Clean Access Server ne demandera pas au client (toucher d'iPhone/iPod) de télécharger l'agent.
3. Choisissez **MAC_OSX** pour configurer les conditions requises d'agent pour MAC OS. Vous pouvez vérifier la **TOUTE L'**option de **configurations** ou la décocher pour configurer ce SYSTÈME D'EXPLOITATION spécifique. L'option de téléchargement d'agent d'exigence doit être vérifiée si vous voulez que les utilisateurs réguliers de MAC OS téléchargent l'agent de MAC.

Q. Vous pourriez recevoir ce message d'erreur : **Erreur : Le téléchargement a manqué. Ce certificat Ca-signé n'apparie pas la clé privée dans la base de données principale.** Comment est-ce que je peux résoudre ce problème ?

A. Pour résoudre ce problème, procédez comme suit :

1. Générez un CSR.
2. Sauvegardez la clé privée.

3. Téléchargez le nouveau certificat avec la clé privée enregistrée.

Q. J'ai reçu ce message d'erreur : `Journal du serveur d'invité NAC : utilisateur _SYSTEM_ (-172.16.98.9) essayant d'authentifier de l'emplacement non valide : XXX@YYY.com 2011 15-Jan-2010 11:41:44`. Comment est-ce que je peux résoudre cette erreur ?

A. Cette question releated pour introduire des erreurs pour tests CSCsq86376 (clients enregistrés seulement) et elle révélerait si vous n'utilisez pas des adresses IP dans leurs paquets RADIUS du WLC.

Q. J'ai reçu ce meaage d'erreur tout en améliorant CAS avec le CD : « `Mettez en mémoire tampon l'erreur E/S sur le périphérique a eu, bloc logique` ». Comment est-ce que je peux résoudre cette erreur ?

A. Cette question habituellement se produit quand le CD est corrompu ou est brûlée à la grande vitesse. Avec une plus grande OIN le CD ne doit pas être brûlé à plus que la vitesse 10X ou 8X.

Q. Vous pourriez recevoir ce message d'erreur quand vous connectez le CAM à CAS : `Erreur : RMISocketFactory : Créant le socket RMI n'a pas hébergé.` Comment résoudre ce problème ?

A. Ce message d'erreur pourrait se produire en raison des versions mal adaptées sur le CAM et CAS ou en raison des Certificats mal adaptés ou du secret partagé utilisé. Pour plus d'informations sur la façon résoudre les problèmes de certificat, référez-vous à NAC (CCA) : Comment corriger des erreurs de certificat sur le CAM/CAS après mise à jour à 4.1.6.

Q. J'ai reçu ce message d'erreur : `L'émetteur de certificat pour ce site est non approuvé ou inconnu. Souhaitez-vous poursuivre ?` Comment est-ce que je peux résoudre cette erreur ?

A. Ce message apparaît parce que le certificat utilisé sur CAS auto-**est émis** et n'est pas enregistré dans le stock de certificat des clients. Cette erreur peut être résolue en chargeant un certificat d'un constructeur externe (tel que Verisign, confiez, etc.) qui est déjà connu aux machines cliente. Ceci exige acheter un certificat d'un de ces constructeurs et l'installer sur CAS, ou vous pouvez utiliser votre propre autorité de certification (cependant, vous devez installer manuellement le certificat de CA de ceci sur chaque client).

Remarque: Réinstaller le certificat sur CAS exige le retirer et re-l'ajouter au CAM. Ceci peut être disruptif à votre réseau. Ceci est fortement recommandé seulement quand il y a une fenêtre possible de panne.

Divers

Q. Le service DHCP de Clean Access Server ne redémarre pas ou de temps en temps des arrêts. Que doit être fait ?

A. Les paramètres DHCP *sont compilés* sur Clean Access Server. Parfois ces configurations compilées peuvent devenir corrompues, particulièrement après une mise à jour au logiciel de

Clean Access Server. La solution est de forcer Clean Access Server pour recompiler les configurations. Afin de faire ceci, apportez une modification, et cliquez sur la **mise à jour**.

Symptômes :

Le serveur DHCP ne démarre pas, ou il échoue de temps en temps sur Clean Access Server.

Instructions :

1. Si le démon DHCP du serveur ne commence pas, allez au gestionnaire, ouvrent ce serveur particulier, et le clic **gèrent**.
2. **Le réseau** choisi **> la liste DHCP > de sous-réseau**, et cliquent sur Edit pour une des listes de sous-réseau.
3. Apportez n'importe quelle modification au sous-réseau (par exemple, augmentez la durée de bail de 1 minute), et cliquez sur la **mise à jour**.
4. Retournez à la page d'état et voyez si le service DHCP a commencé. En ce moment les paramètres DHCP devraient être compilés de nouveau.

Remarque: Une autre situation qui peut faire ne pas démarrer le serveur DHCP superpose des configurations de sous-réseau. Vérifiez ceci aussi bien.

Q. J'ai configuré le temporisateur de pulsation de sorte qu'un périphérique soit fermé une session le système après une certaine heure inactive. Connectez-vous en cas, il déclare qu'il ne peut pas cingler le périphérique mais le périphérique continue à passer le trafic dans les deux sens. Comment résoudre ce problème ?

A. C'est un exemple de l'erreur :

```
Authentication  2004-08-26 12:13:48
Unable to ping 149.151.206.251, going to logout user user1
```

Vérifiez pour voir si le périphérique a des pare-feux intégrés qui bloquent des paquets d'ARP du serveur de Cisco Clean Access. Le serveur de Cisco Clean Access exécute le ping d'ARP. C'est un message d'ARP et ne devrait pas être bloqué.

Q. J'ai configuré le temporisateur de pulsation de sorte qu'un périphérique ferme une session le système après une certaine période d'inactivité. Connectez-vous en cas, il déclare qu'il ne peut pas cingler le périphérique mais les passages de périphérique trafiquent toujours dans les deux sens. Comment résoudre ce problème ?

A. Assurez-vous que vous configurez un port série pour la connexion de Basculement.

Si l'ordinateur qui exécute le logiciel de serveur de Cisco Clean Access a deux ports série, vous pouvez utiliser le port supplémentaire pour la jonction de câble série. Par défaut, le premier connecteur séquentiel détecté sur le serveur est configuré pour l'entrée/sortie de console (pour faciliter l'installation et d'autres types d'accès administratif). Si l'ordinateur a seulement un port série (ttyS0) et vous n'avez pas l'intention de l'utiliser pour l'accès administratif, vous pouvez modifier le port pour servir de connexion de Basculement.

Terminez-vous ces étapes afin de modifier ttyS0 comme connexion de pulsation :

1. D'un client SSH, accédez au serveur de Cisco Clean Access comme utilisateur de base.
2. Éditez **/etc/lilo.conf** et retirez ou commentez la dernière ligne : `append="console=ttyS0....."` Cette ligne cause la sortie de console d'être réorientée au port série. **Remarque:** Ajoutez a **#** caractère au début de la ligne afin de commenter une ligne. Des lignes qui commencent par ce caractère sont ignorées.
3. Éditez **/etc/inittab** et retirez ou commentez la dernière ligne : `co:2345:respawn ...vt100`Cette ligne fait démarrer un terminal de procédure de connexion sur le port série.
4. **Le lilo de** type et appuient sur **entrent à l'**invite de commande. Ceci commence Lilo, le programme de démarrage de Linux.
5. Sélectionnez la commande de **réinitialisation** de redémarrer l'ordinateur.
6. Répétez les étapes sur le serveur de Cisco Clean Access de pair de Basculement.

Q. Combien de temps le fait pour prendre le gestionnaire de Cisco Clean Access (autrefois SmartManager) pour chronométrer le serveur de Cisco Clean Access et pour le `SecureSmart 2004-08-26 12:26:42 192.168.1.1 est inaccessible !` message à afficher ?

A. Le gestionnaire de Cisco Clean Access porte à trois minutes au délai d'attente chaque serveur de Cisco Clean Access avant qu'il affiche l'état non connecté.

Q. Quelle est l'incidence de changer le network interface card (NIC) sur le serveur de Cisco Clean Access ?

A. Si vous avez un permis de non-site, vous n'avez pas besoin d'informer le support technique de Cisco de la modification sur l'adresse MAC. Vous devez seulement informer le support technique de Cisco quand votre nombre de serveurs de Clean Access change. Si vous avez une licence de site, vous n'avez pas besoin d'informer le support technique de Cisco.

Q. Je peux obtenir une adresse IP du serveur DHCP de Clean Access, mais après ce, je continue à voir une « page ne pas fonder » le message quand j'essaye d'ouvrir un navigateur à une adresse d'extérieur. Je n'ai été jamais réorienté à la page de connexion de Web. Pourquoi cela ?

A. Vous pouvez éprouver une de ces questions :

- Les DN du serveur de Cisco Clean Access n'est pas placés dans le serveur DNS.Vous êtes réorienté au nom DNS pour la page de connexion de Web. Vous avez pu ne pas avoir associé securesmart.company.com avec 192.168.0.1 dans votre entrée DNS.
- Le certificat utilise le nom DNS.Les utilisations securesmart.company.com de certificat mais le serveur DNS n'a pas été associées avec le nom. La validation de certification échoue.
- Le certificat est incorrectement créé ou est non valide. Vérifiez pour voir **/perfigo/access/apache/logs/error_log**. Si vous voyez ces erreurs, recréez votre certificat ssl.`[root@securesmart logs]# cat error_log`

  ```
  [Thu Sep 16 18:00:04 2004] [error] Unable to configure RSA
  server private key

  [Thu Sep 16 18:00:04 2004] [error] SSL Library Error:
  185073780 error:0B080074:x509 certificate routines:
  X509_check_private_key:key values mismatch
  ```
  Remarque: Référez-vous à où sont les fichiers

journal dans Clean Access Manager ? pour tous les fichiers journal.

- Le httpd n'est pas commencé. Vérifiez pour voir si le HTTP est commencé par le **netstat - Al |** commande de **HTTP de grep**. Vous devriez voir cette liste. Sinon, émettez la commande de **reprise de perfigo de service**.`tcp 0 0 *:http *:* LISTEN`

  `tcp 0 0 *:https *:* LISTEN`

Q. Est-ce que je dois mettre à jour quelque chose après que je remplace un serveur défectueux de Cisco Clean Access ?

A. Parfois, le ss_key n'est plus identique. Procédez comme suit :

1. Le SSH au gestionnaire de Cisco Clean Access et obtiennent le **ss_key**.
2. Émettez le **psql - h 127.0.0.1 -** commande de **controlsmartdb de postgres U**.
3. Sélectionnez *** du** securesmart_info. `ss_key | ss_group | ss_type | ss_ip | ss_loc`

   `00_40_33_60_43_D2_04_54_48_55_66_D5 | | standard_gateway | 10.0.0.1 |`
4. Le SSH au serveur de Cisco Clean Access et obtiennent/mises à jour le ss_key.
5. Émettez **[root@securesmart etc.] #** commande de **/etc/.GUSSK de cat**. `[root@securesmart etc]# cat /etc/.GUSSK`

   `00_30_48_80_43_D6_00_30_48_80_43_D5`
6. Éditez **/etc/.GUSSK** et mettez- à jourle avec le ss_key de Clean Access Manager.
7. Exécutez une réinitialisation.

Q. La Connectivité de SSH est perdue tandis que l'arrêt du service de perfigo sur CAS utilisant le perfigo de service fermait la commande. Je ne peux pas rebrancher à moins que quelqu'un soit physiquement à la case et peux la redémarrer. Comment puis-je résoudre ce problème ?

A. Cette question peut être résolue à l'aide de la commande de **maintenance de perfigo de service** dans des versions 4.1 et ultérieures NAC.

Q. Je ne peux pas démarrer l'appliance NAC avec le nouveau CD CAS/CAM que j'ai. Que dois-je faire ?

A. Vérifiez le suivant afin de résoudre ceci :

- Assurez-vous que vous avez validé la somme de contrôle pour l'image ISO téléchargée pour CAS/CAM.
- Gravez l'image ISO à la vitesse brûlante la plus lente possible.

Informations connexes

- Foire aux questions de Cisco Clean Access Agent
- FAQ de Cisco Clean Access Manager
- FAQ de Cisco Clean Access Manager 2
- Support technique - Cisco Systems