Dispositif NAC (CCA) : Configurer une haute disponibilité pour Clean Access Manager (CAM)

Contenu

Introduction

Ce document décrit comment installer une paire d'ordinateurs de Clean Access Manager (CAM) pour la Haute disponibilité (ha). Quand des gestionnaires de Clean Access sont déployés en mode facilement disponible, vous pouvez s'assurer que l'importante surveillance, l'authentification, et les tâches d'enregistrement continuent en cas d'un arrêt inattendu.

Remarque: Référez-vous à la section (ha) facilement disponible configurante de l'appliance de Cisco NAC - installation et guide d'administration de Clean Access Server (CAS) afin de savoir configurer la caractéristique ha dans CAS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur l'appliance du Cisco Network Admission Control (NAC) - version 4.1 de CAM.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

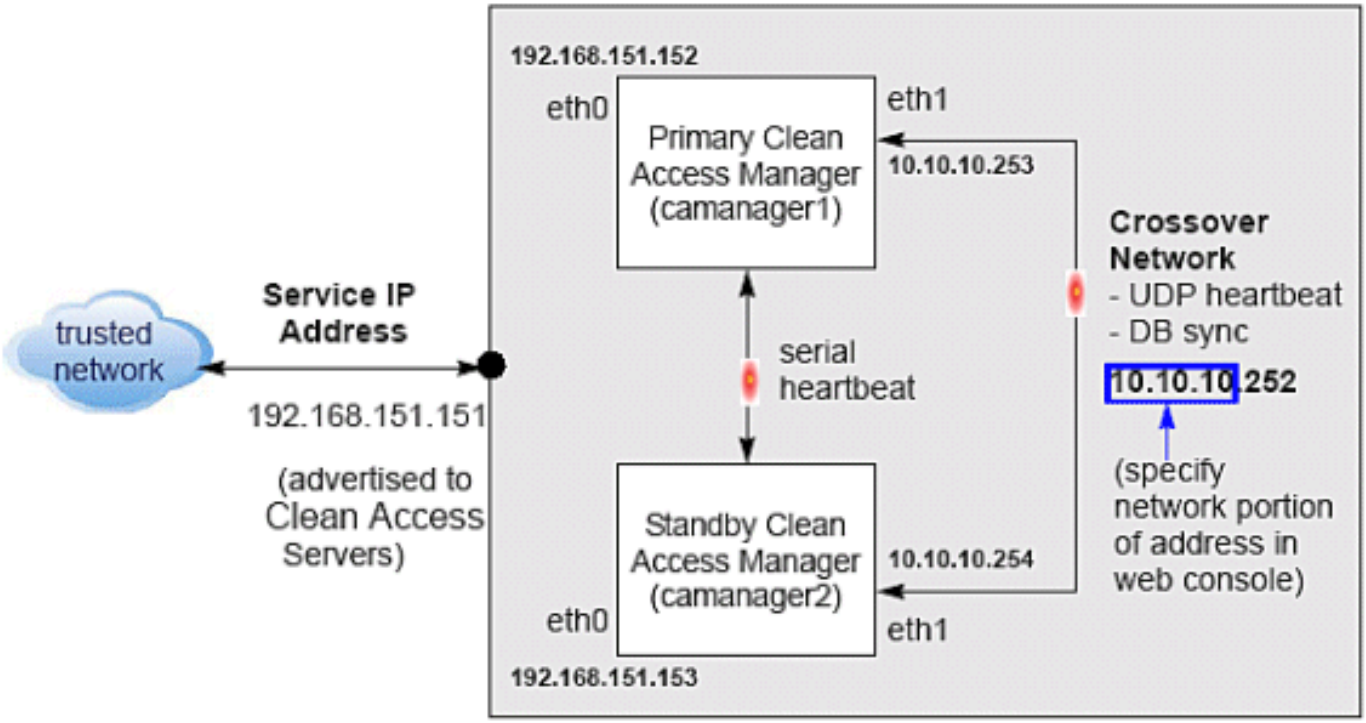
Conventions

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

Aperçu

Ces points clé fournissent un résumé de haut niveau d'exécution HA-CAM :

1. Le mode facilement disponible de Clean Access Manager est configuration active/passive de deux-serveur dans laquelle un ordinateur de réserve de CAM agit en tant que sauvegarde à un ordinateur actif de CAM.
2. Clean Access Manager actif effectue toutes les tâches pour le système. Le CAM de standby surveille le CAM actif et maintient sa base de données synchronisée avec la base de données active de CAM.
3. Les deux CAMs partagent un IP virtuel de service pour l'interface de confiance par eth0. Le nom de domaine doit être utilisé pour le certificat ssl.
4. Les ordinateurs primaires et secondaires de CAM permutent des paquets de pulsation d'UDP toutes les 2 secondes. Si le temporisateur de pulsation expire, le basculement dynamique se produit.
5. L'interface eth1 et/ou l'interface série sur les CAMs peuvent être utilisées pour la synchronisation de paquets et de base de données de pulsation. Si eth1 et interfaces série sont configurés pour la pulsation, les deux interfaces doivent échouer pour que le Basculement se produise.



Le mode facilement disponible de Clean Access Manager est configuration active/passive de deux-serveur dans laquelle un ordinateur de Clean Access Manager de standby agit en tant que sauvegarde à un ordinateur actif de Clean Access Manager. Tandis que le CAM actif porte les la plupart du dans des conditions normales de charge de travail, les moniteurs de secours le CAM actif et garde son magasin de données ont synchronisé avec les données du CAM actif.

Si un événement de Basculement se produit, comme si le CAM actif s'arrêtait ou ne répond pas au signal de « pulsation » du pair, le standby assume le rôle du CAM actif.

Quand vous configurez d'abord les pairs ha, vous devez spécifier un CAM Ha-primaire et le CAM Ha-secondaire. Au commencement, le Ha-primaire est le CAM actif, et le Ha-secondaire est le CAM (passif) de réserve, mais rôles actifs/passifs ne sont pas de manière permanente assignés. Si le CAM primaire descend, le secondaire (standby) devient le CAM actif. Quand les reprises primaires d'origine de CAM, il assume le rôle de sauvegarde.

Quand Clean Access Manager démarre, il vérifie pour voir si son pair est en activité. Sinon, le CAM qui démarre assume le rôle actif. Si le pair est en activité, d'autre part, le CAM qui démarre devient le standby.

Vous pouvez configurer deux gestionnaires de Clean Access pendant qu'une paire ha en même temps, ou vous peut ajouter nouveau Clean Access Manager à un CAM autonome existant pour créer une paire facilement disponible. Pour que les paires apparaissent au réseau et aux serveurs de Clean Access en tant qu'une entité, vous devez spécifier une adresse IP de service à utiliser comme adresse de confiance de l'interface (eth0) pour les paires ha.

Afin de créer le réseau de croisé sur lequel les informations facilement disponibles sont permutées, vous connectez les ports eth1 des deux CAMs et spécifiez une adresse de réseau privé pas actuellement conduite dans votre organisation (le réseau de croisé ha de par défaut est 192.168.0.252). Clean Access Manager crée alors un réseau privé, sécurisé, de deux-noeud pour les ports eth1 de chaque CAM pour permuter le trafic de pulsation d'UDP et pour synchroniser des bases de données. Notez que le CAM utilise toujours eth1 comme interface de pulsation d'UDP.

Pour la Sécurité supplémentaire, vous pouvez également connecter les ports série de chaque

Clean Access Manager pour l'échange de pulsation. Dans ce cas, la pulsation d'UDP et les interfaces séquentielles de pulsation doivent échouer pour que le système de réserve succède.

Remarque: Pour la jonction de câble série pour l'ha (HA-CAM ou HA-CAS), le câble série doit être un câble de « null modem ».

Exigences de base avant que vous poursuiviez

Avertissement : Afin d'empêcher n'importe quelle perte possible de données dans la synchronisation de base de données, assurez-vous toujours que le standby Clean Access Manager (secondaire) est vivant avant de basculer Clean Access Manager (primaire) actif.

Avant que vous configuriez la Haute disponibilité, assurez-vous que vous répondez à ces exigences :

1. Vous avez obtenu un permis facilement disponible (de Basculement).**Remarque:** Quand vous installez un permis du Basculement de CAM (ha), installez le permis de Basculement sur le CAM primaire d'abord, alors chargez tous les autres permis. Des permis autonomes peuvent également être utilisés pour la Haute disponibilité.
2. Les deux CAMs sont installés et configurés.
3. Pour la pulsation, chaque CAM doit avoir une seule adresse Internet (ou le nom du noeud). Pour des paires de CAM ha, ce nom d'hôte est fourni au pair et doit être résolu par des DN ou être ajouté au fichier de /etc/hosts du pair.
4. Vous avez un certificat Ca-signé pour le nom de domaine des paires de CAM ha.
5. Le CAM Ha-primaire est saturé pour l'exécution d'exécution. Ceci signifie que les connexions aux sources d'authentification, des stratégies, des rôles de l'utilisateur, des Points d'accès, et ainsi de suite, sont toutes spécifiées. Cette configuration est automatiquement reproduite dans le CAM (de réserve) Ha-secondaire.
6. Les deux gestionnaires de Clean Access sont accessibles sur le réseau (essai pour les cingler pour tester la connexion).
7. Les ordinateurs sur lesquels le logiciel de CAM est installé ont un port Ethernet libre (eth1) et au moins un port série libre. Employez les manuels de spécification pour le matériel serveur pour identifier le port série (ttyS0 ou ttyS1) sur chaque ordinateur.
8. Dans des déploiements hors bande, la Sécurité de port n'est pas activée sur les interfaces commutateur auxquelles CAS et le CAM sont connectés. Ceci peut gêner la livraison de CAS ha et DHCP.

Ces procédures exigent de vous de redémarrer Clean Access Manager. À ce moment-là, ses services sont brièvement indisponibles. Configurez un CAM en ligne quand le temps d'arrêt a la moins incidence sur vos utilisateurs.

Remarque: Les consoles d'admin de Web d'appareils de Cisco NAC prennent en charge l'Internet Explorer 6.0 ou au-dessus du navigateur.

Connectez les ordinateurs de Clean Access Manager

Il y a deux types de connexions entre les pairs HA-CAM : un pour permuter les données d'exécution qui associent aux activités et à celle de Clean Access Manager pour le signal de pulsation. Dans la Haute disponibilité, Clean Access Manager utilise toujours l'interface eth1 pour l'échange d'échange de données et de pulsation d'UDP. Quand le signal de pulsation d'UDP ne

transmet pas et ne reçoit pas au cours d'un certain délai prévu, le système de réserve succède. Afin de fournir une mesure supplémentaire de Sécurité, il est fortement recommandé pour ajouter une connexion séquentielle de pulsation entre les pairs de Clean Access Manager. La connexion série fournit une méthode dédiée supplémentaire d'échange de pulsation qui doit échouer avant que le système de réserve puisse succéder. Notez que la connexion eth1 entre les pairs de CAM est obligatoire.

Connectez physiquement les gestionnaires de Clean Access de pair comme affichés :

- Utilisez le câble croisé pour connecter les ports Ethernet eth1 des ordinateurs de Clean Access Manager. Cette connexion est utilisée pour l'interface d'UDP de pulsation et d'échange de données (mise en miroir de base de données) entre les pairs de Basculement.
- Utilisez le câble série de null modem pour connecter les ports série (fortement recommandés). Cette connexion est utilisée comme échange séquentiel de pulsation supplémentaire (keep-alive) entre les pairs de Basculement.

Remarque: Pour la jonction de câble série pour l'ha (HA-CAM ou HA-CAS), le câble série doit être un câble de « null modem ».

Connexion série

Si l'ordinateur qui exécute le logiciel de Clean Access Manager a deux ports série, vous pouvez utiliser le port supplémentaire pour la connexion séquentielle de pulsation. Par défaut, le premier port série détecté sur le serveur de CAM 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 (COM1 ou ttyS0), vous pouvez modifier le port pour servir de connexion facilement disponible de pulsation. C'est parce que, après que le logiciel de CAM soit installé, la console de SSH ou KVM peut toujours être utilisée pour accéder à l'interface de ligne de commande du CAM.

Vous pouvez activer/le port série avec la case **séquentielle de procédure de connexion de débronchement** sur les configurations de CAM ha (sous la **gestion > le Clean Access Manager > le réseau et le Basculement | Configurations de Basculement | Procédure de connexion séquentielle de débronchement**). Quand il y a seulement un port série sur l'ordinateur de CAM, cette case permet à des administrateurs pour désactiver la procédure de connexion séquentielle sur COM1 de sorte qu'elle puisse être utilisée comme interface série de pulsation pour une paire d'Access Manager Ha-propres.

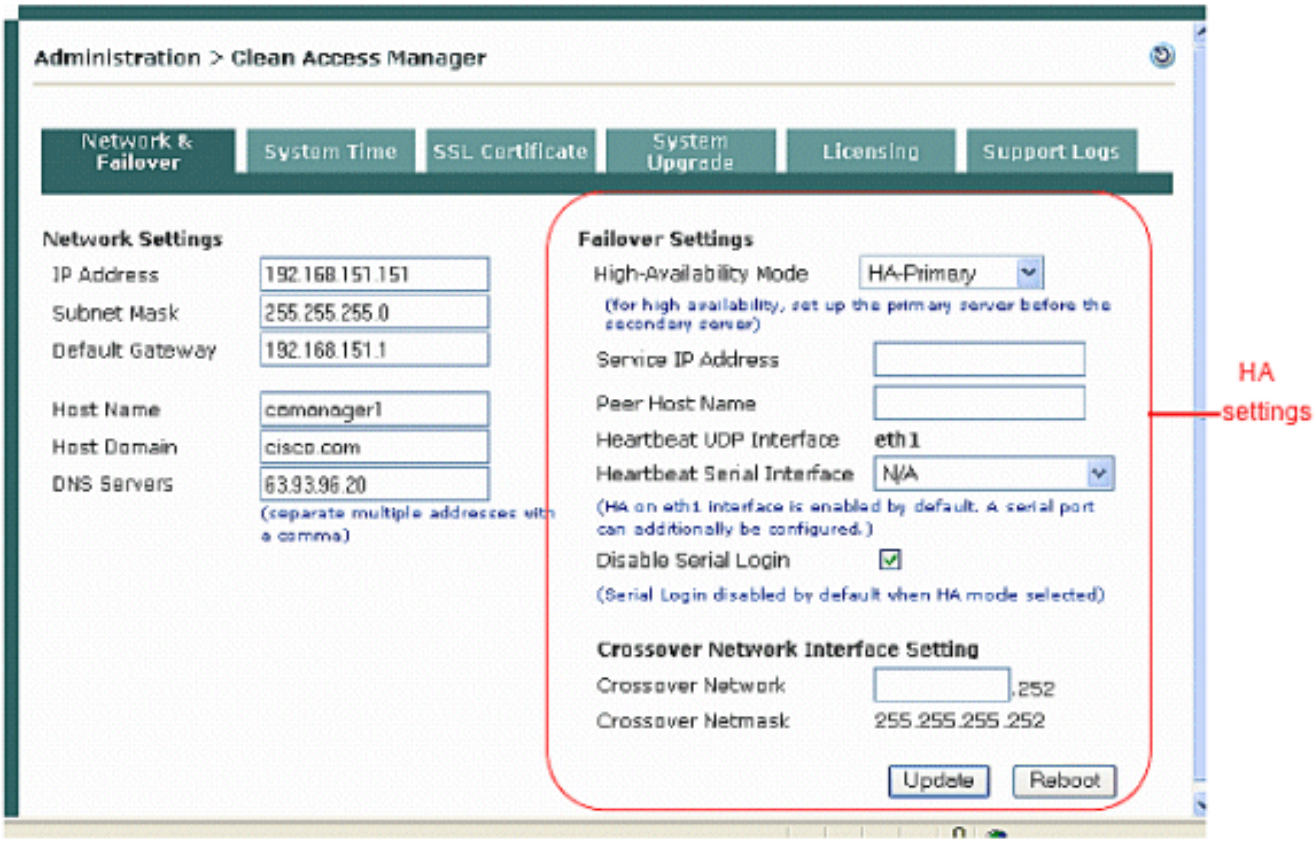
Remarque: La procédure de connexion séquentielle **est activée** par défaut sur le CAM. Si vous utilisez COM1 pour l'interface série de pulsation du CAM, vous devez cliquer sur la case **séquentielle de procédure de connexion de débronchement** pour désactiver la procédure de connexion séquentielle sur COM1.

Configurez le CAM Ha-primaire

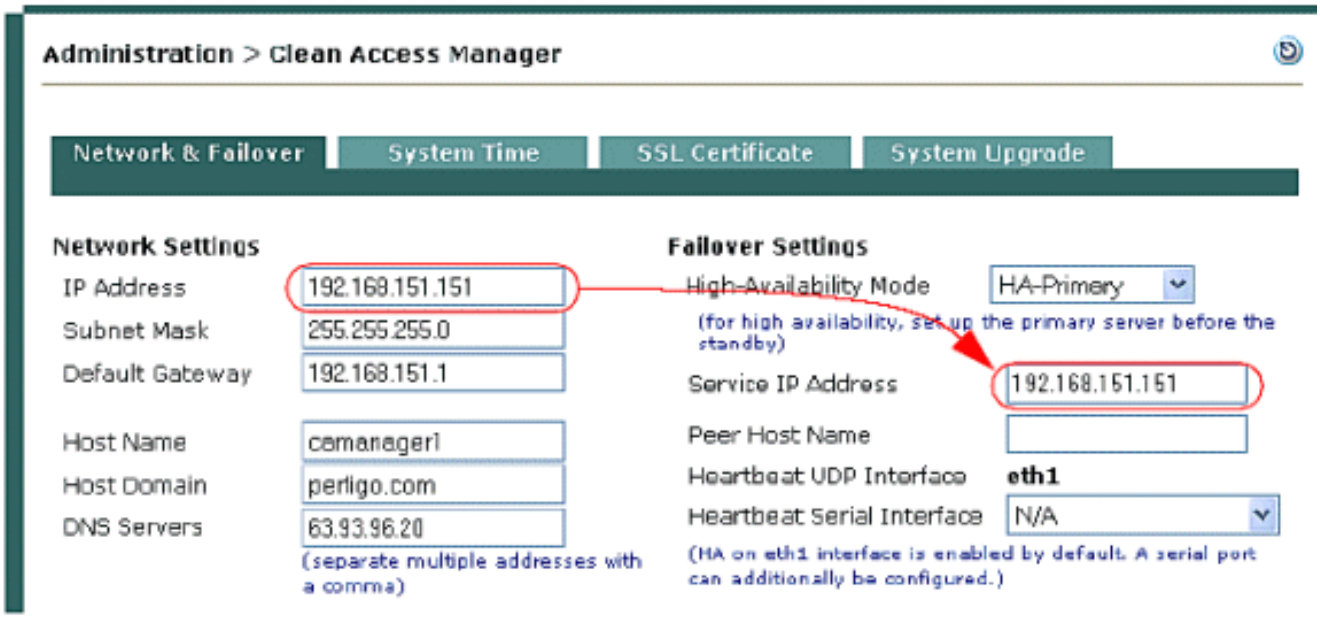
Une fois que vous avez vérifié les conditions préalables, exécutez ces étapes pour configurer Clean Access Manager en tant que Ha-primaire pour les paires facilement disponibles. Voyez la figure pour un exemple de configuration d'échantillon.

1. Ouvrez la console d'admin de Web pour que Clean Access Manager soit indiqué en tant que

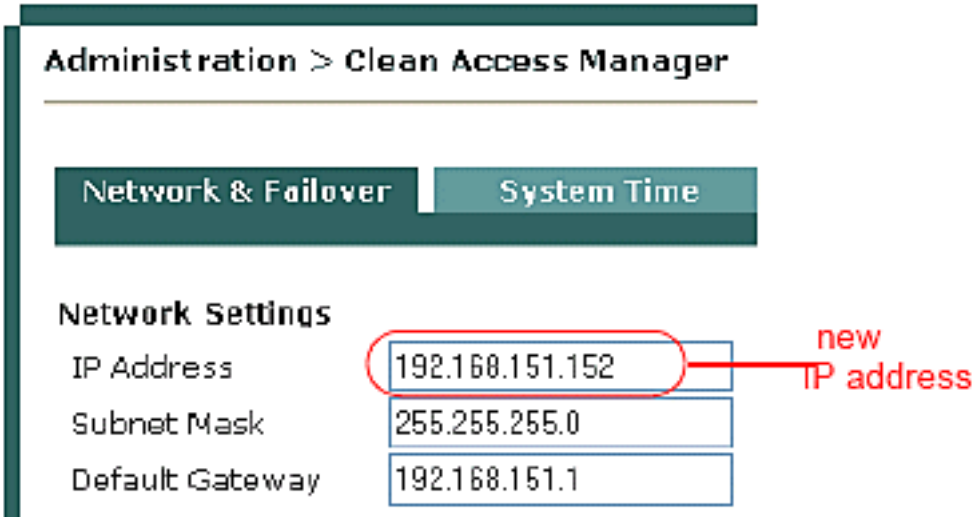
Ha-primaire, et allez à la **gestion > au gestionnaire > au certificat ssl de CCA** pour configurer le certificat ssl pour le CAM primaire. Le formulaire **provisoire de certificat de générer** apparaît.**Remarque:** Les étapes de configuration ha dans ce document supposent qu'un certificat provisoire est exporté du CAM Ha-primaire au CAM Ha-secondaire.*Si vous utilisez un certificat provisoire pour les paires ha, exécutez ces étapes :*Remplissez le formulaire **provisoire de certificat de générer** et le clic **se produisent**. Le certificat doit être généré pour le nom de domaine des paires ha.Après que vous génériez le certificat provisoire, choisissez la **clé/certificat de l'exportation CSR/Private du choisir un** menu d'**action**.Cliquez sur le bouton d'**exportation** pour la **clé privée actuellement installée** pour exporter la clé privée SSL. Sauvegardez le fichier principal au disque. Vous devez importer cette clé dans le CAM Ha-secondaire plus tard.Cliquez sur le bouton d'**exportation** pour le **certificat actuellement installé** pour exporter le certificat ssl en cours. Sauvegardez le fichier du certificat au disque. Vous devez importer ce fichier du certificat dans le CAM Ha-secondaire plus tard.*Si vous utilisez un certificat Ca-signé pour les paires ha, exécutez ces étapes :***Remarque:** Le certificat Ca-signé doit être basé sur le nom de domaine résoluble à l'IP de service par des DN. Référez-vous gèrent des Certificats SSL de CAM sous la section Administration dans l'appliance de Cisco NAC - pour en savoir plus d'installation et de guide d'administration de CAM.Choisissez le **certificat d'importation du choisir un** menu d'**action**.Utilisez le **bouton Parcourir** à côté du gisement de **fichier du certificat** et naviguez vers le certificat Ca-signé.Choose Ca-**a signé le CERT X.509 PEM-encodé du type de fichier** menu déroulant.Cliquez sur Upload pour importer le certificat. Notez que vous devez importer ce même certificat dans le CAM Ha-secondaire plus tard.Cliquez sur **vérifient et installent les Certificats téléchargés**.Choisissez la **clé/certificat de l'exportation CSR/Private du choisir une** liste déroulante d'**action**.Cliquez sur le bouton d'**exportation** pour la **clé privée actuellement installée** pour exporter la clé privée SSL associée avec le certificat Ca-signé. Sauvegardez le fichier principal au disque. Vous devez importer ce fichier dans le CAM Ha-secondaire plus tard.
2. Allez à la **gestion > au gestionnaire de CCA** et cliquez sur le **réseau et le Basculement** tableau choisissent l'option Ha-**primaire du** menu déroulant **facilement disponible de mode**. Les configurations facilement disponibles
apparaissent.



3. Copiez la valeur du **champ IP Address** sous des **paramètres réseau** et écrivez-la dans le **champ IP Address de service**. L'adresse IP de paramètres réseau est l'adresse IP existante de Clean Access Manager en cours. L'idée ici est de transformer cette adresse IP, que les serveurs de Clean Access identifient déjà, en adresse IP virtuelle de service pour les paires de Clean Access
Manager.

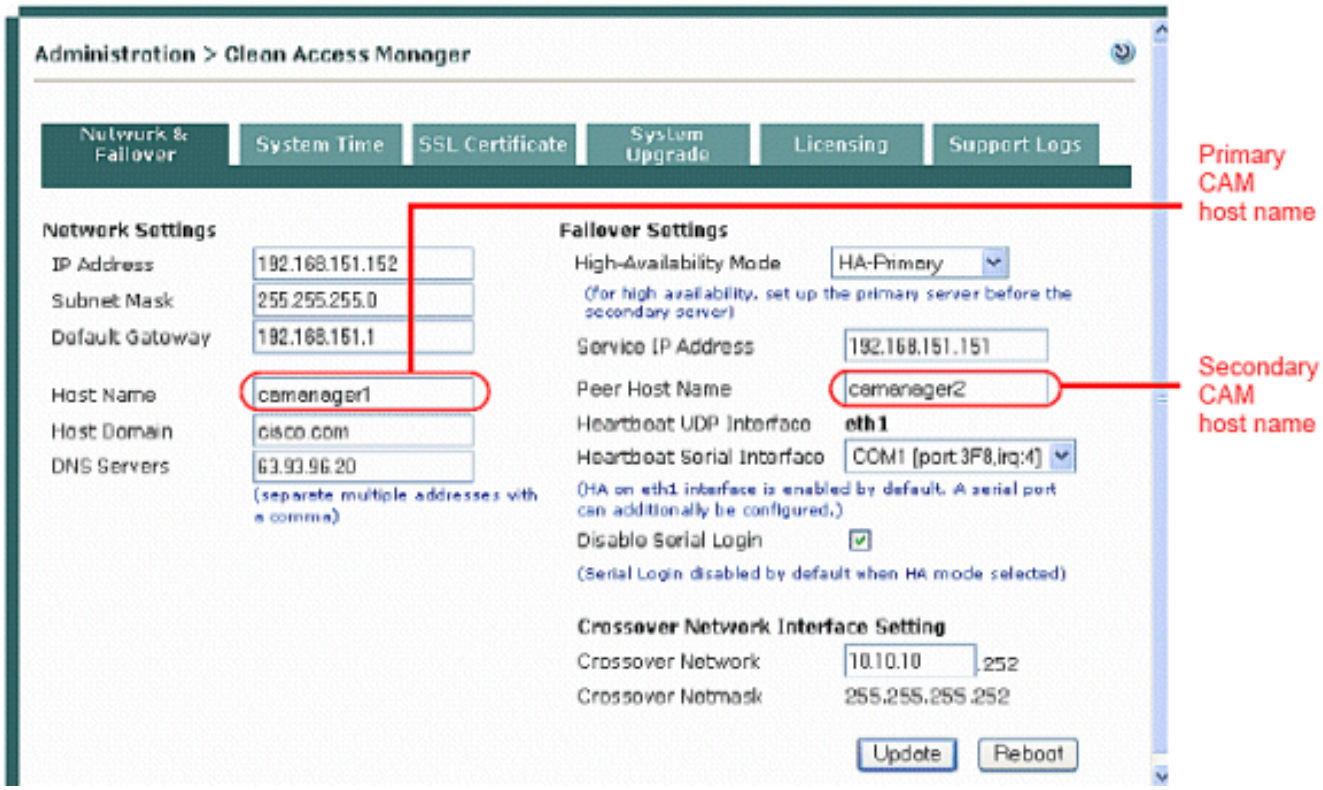


4. Changez l'adresse IP sous des **paramètres réseau à une** adresse disponible, par exemple,



n.152.

5. Chaque Clean Access Manager doit avoir un nom d'hôte unique, tel que camanager1 et camanager2. Introduisez le nom d'hôte du CAM Ha-primaire dans le **champ Host Name** sous des **paramètres réseau**, et introduisez le nom d'hôte du CAM Ha-secondaire dans le **champ Host Name de pair** sous des **configurations de Basculement**.



Une valeur de **nom d'hôte** est obligatoire quand vous installez la Haute disponibilité, alors que le **nom de domaine d'hôte** est facultatif.**Le nom d'hôte** et les **champs Host Name de pair** distinguent les majuscules et minuscules. Veillez à apparier ce qui est tapé ici avec ce qu'est tapé pour le CAM Ha-secondaire plus tard.

6. Du menu déroulant d'**interface série de pulsation**, choisissez le port série auquel vous avez connecté le câble série du CAM Ha-primaire, ou laissez ce non applicable si vous n'utilisez pas une connexion série.
7. Si votre ordinateur a seulement un port série et vous utilisez COM1 comme interface série de pulsation, vous devez cocher la case **séquentielle de procédure de connexion de débronchement** pour s'assurer que la procédure de connexion séquentielle est désactivée sur COM1. Voir la connexion série pour d'autres détails.
8. Afin de mettre à jour la synchronisation, Clean Access Manager scrute des données

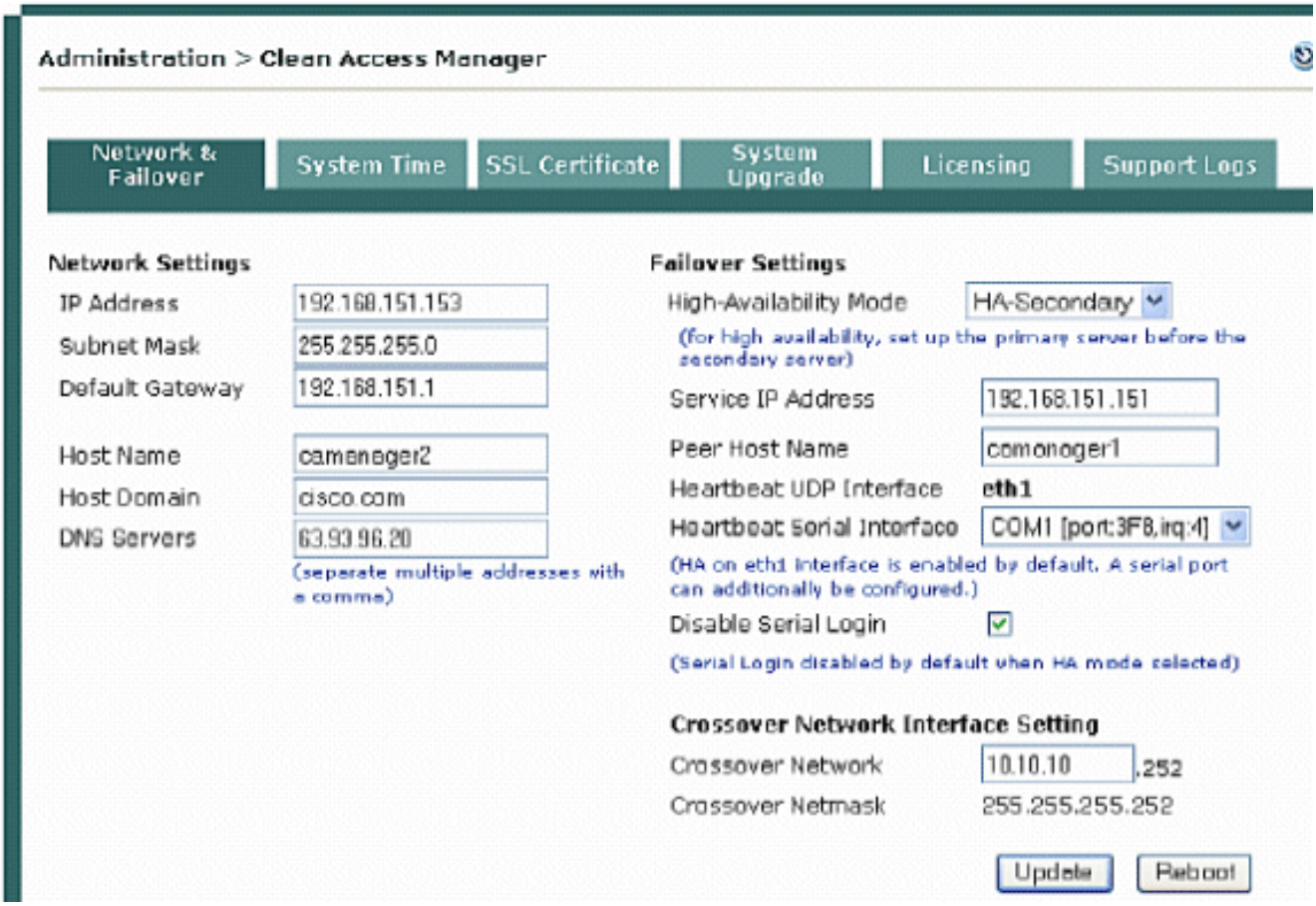
d'échange par un réseau de croisé. Vous devez spécifier une espace adresse d'adresse de réseau privé pas actuellement conduite dans votre organisation dans le domaine de **réseau de croisé**, tel que 10.10.10. Le réseau par défaut de croisé fourni est 192.168.0.252. Si cette adresse est en conflit avec votre réseau, veillez à spécifier un espace d'adressage privé différent. Par exemple, si votre organisation utilise le réseau privé 192.168.151.0, utilisation 10.1.1.x comme réseau de croisé. Le masque de sous-réseau et le dernier octet de l'adresse IP sont réparés, présentent ainsi seulement la partie réseau de l'adresse IP dans le domaine de **réseau de croisé**.

9. Cliquez sur la **mise à jour** et puis **la redémarrez** pour redémarrer Clean Access Manager.Après que Clean Access Manager redémarre, assurez-vous que l'ordinateur de CAM fonctionne correctement. Vérifiez pour voir si les serveurs de Clean Access sont connectés et de nouveaux utilisateurs sont authentifiés.

Configurez le CAM Ha-secondaire

Exécutez ces étapes pour configurer le CAM Ha-secondaire.

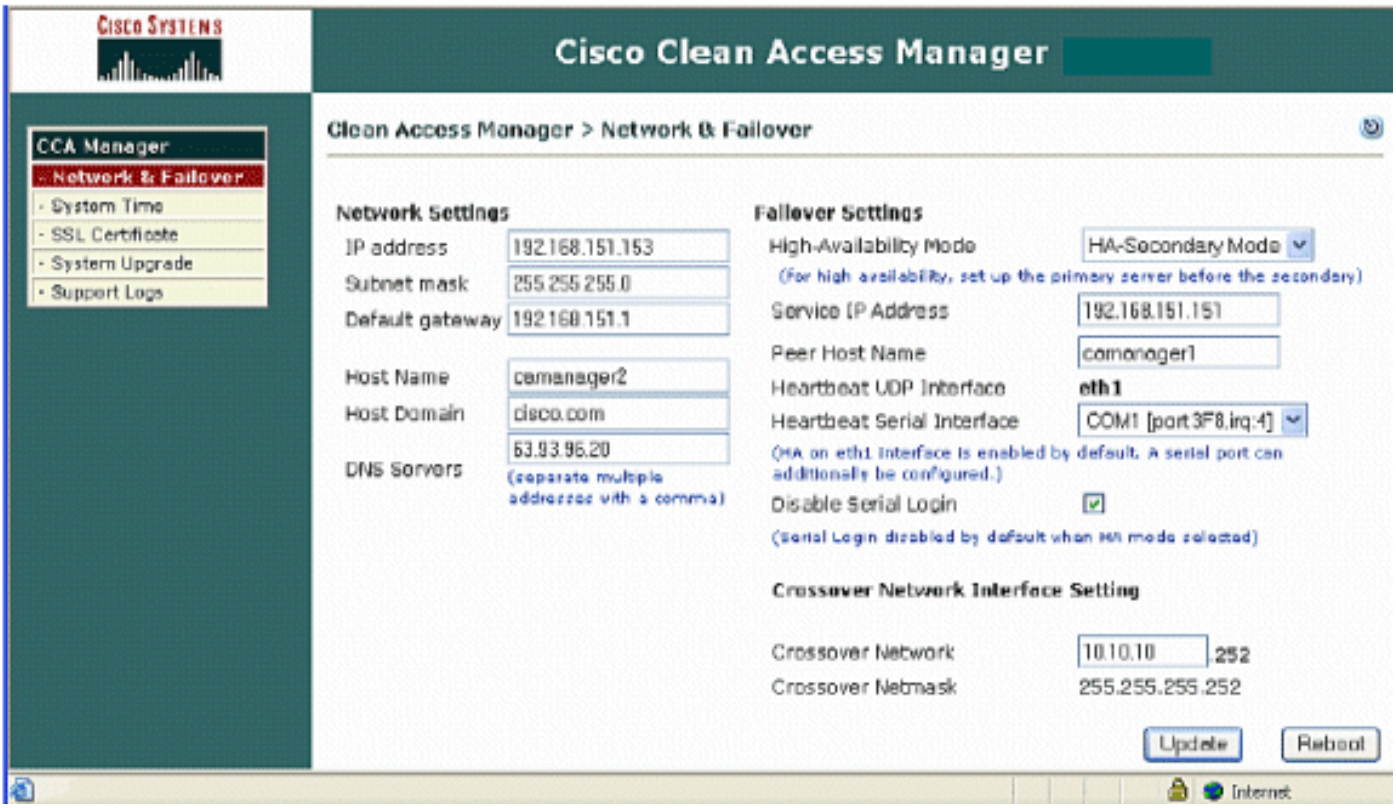
1. Ouvrez la console d'admin de Web pour que Clean Access Manager soit indiqué en tant que Ha-secondaire, et allez à la **gestion > au gestionnaire > au certificat ssl de CCA**.
2. Avant que vous poursuiviez, exécutez ces étapes :Sauvegardez la clé privée du CAM secondaire.Assurez-vous que la clé privée et le certificat ssl classe associé au CAM du service IP/HA-Primary sont disponibles (précédemment exporté comme décrit dedans configurez le CAM Ha-primaire).
3. Importez le fichier principal privé et le certificat du CAM Ha-primaire comme décrit :Dans l'onglet de **certificat ssl**, choisissez le **certificat d'importation du choisir un** menu d'**action**.Cliquez sur **parcourent** à côté du gisement de **fichier du certificat**, et parcourent à votre copie de sauvegarde du fichier principal privé généré avec le certificat qui est utilisé pour les paires ha.Choisissez la **clé privée** comme type de fichier.Cliquez sur Upload pour télécharger la clé privée.**Le certificat d'importation** étant choisi du **choisir un** menu d'**action**, parcourent au certificat (provisoire ou Ca-signé) qui est associé avec la clé privée.Choose Ca-**a signé le CERT X.509 PEM-encodé** comme type de fichier.Cliquez sur Upload pour télécharger le certificat provisoire ou le certificat Ca-signé.Cliquez sur **vérifient et installent les Certificats téléchargés**.Référez-vous gèrent des Certificats SSL de CAM sous la section Administration dans l'appliance de Cisco NAC - pour en savoir plus d'installation et de guide d'administration de CAM.
4. Allez à la **gestion > au gestionnaire > au réseau et au Basculement de CCA | Les paramètres réseau** et changent l'adresse IP du CAM secondaire à une adresse qui est différente de l'adresse IP Ha-primaire de CAM et de l'adresse IP de service.



5. Placez la valeur de **nom d'hôte** sous des **paramètres réseau à la** même valeur réglée pour le **nom d'hôte de pair** dans la configuration Ha-primaire de CAM. Voyez la figure dans la section primaire ha.**Remarque: Le nom d'hôte** et les **champs Host Name de pair** distinguent les majuscules et minuscules. Veillez à apparier ce qui est tapé ici avec ce qu'a été tapé pour le CAM Ha-primaire.
6. Choisissez Ha-**secondaire** dans le menu déroulant **facilement disponible de mode**. Les configurations facilement disponibles apparaissent.
7. Placez la valeur d'**adresse IP de service** sous des **configurations de Basculement à la** même valeur réglée pour l'**adresse IP de service** dans la configuration Ha-primaire de CAM.
8. Placez la valeur de **nom d'hôte de pair** sous des **configurations de Basculement au** nom d'hôte du CAM Ha-primaire.
9. Du menu déroulant d'**interface série de pulsation**, choisissez le port série auquel vous avez connecté le câble série du CAM Ha-primaire, ou laissez ce non applicable si vous n'utilisez pas une connexion série.
10. Si votre ordinateur a seulement un port série et vous utilisez COM1 comme interface série de pulsation, vous devez cocher la case **séquentielle de procédure de connexion de débronchement** pour s'assurer que la procédure de connexion séquentielle est désactivée sur COM1. Voir la connexion série pour d'autres détails.
11. Tapez les mêmes configurations d'**interface réseau de croisé** que vous aviez écrites pour le CAM Ha-primaire.
12. **La mise à jour de** clic et **redémarrent** alors.

Quand le CAM de réserve démarre, il synchronise automatiquement sa base de données avec le CAM actif.

En conclusion, ouvrez la console d'admin pour le standby de nouveau et terminez-vous la configuration. Notez que la console d'admin pour le standby a maintenant seulement un module de gestion.



Terminez-vous la configuration

Vérifiez les configurations dans la page de **réseau et de Basculement** pour le CAM de réserve.

La configuration facilement disponible est maintenant complète.

Basculer une paire HA-CAM

Avertissement : Afin d'empêcher n'importe quelle perte possible de données dans la synchronisation de base de données, assurez-vous toujours que le CAM de réserve est vivant avant de basculer le CAM actif.

Le Basculement par paires HA-CAM, SSH à l'ordinateur actif dans les paires et exécutent une de ces commandes :

- **arrêt** ou
- **réinitialisation** ou
- **entretenez l'arrêt de perfigo**Ceci arrête tous les services sur l'ordinateur actif. Quand la pulsation échoue, l'ordinateur de réserve assume le rôle actif. Exécutez le **début de perfigo de service** pour redémarrer des services sur l'ordinateur arrêté. Ceci fait assumer l'ordinateur arrêté le rôle de réserve.**Remarque: la reprise de perfigo de service** ne doit pas être utilisée pour tester la Haute disponibilité (Basculement). Au lieu de cela, Cisco recommande l'**arrêt** ou la **réinitialisation** sur l'ordinateur pour tester le Basculement ou les commandes CLI, l'**arrêt de perfigo de service** et le **début de perfigo de service**.

Commandes utiles CLI pour l'ha

Ce sont les répertoires utiles à savoir pour l'ha sur le CAM :

- /etc/ha.d/perfigo/conf
- /etc/ha.d/ha.cf

Cet exemple affiche que l'emplacement de l'ha mettent au point/fichiers journal, aussi bien que le nom de chaque CAM (noeud) dans les paires ha :

```
[root@cam1  ha.d]#more ha.cf # Generated by make-hacf.pl udpport 694 bcast eth1 auto_failback
off apiauth default uid=root log_badpack false debug 0 debugfile /var/log/ha-debug logfile
/var/log/ha-log #logfacility local0 watchdog /dev/watchdog keepalive 2 warntime 10 deadtime 15
node cam1 node cam2
```

Comment vérifier l'état d'exécution d'Active/Standby sur le CAM ha

Cet exemple affiche comment employer le CLI pour déterminer l'état d'exécution (actif ou de réserve) de chaque CAM dans les paires ha. Vous pouvez généralement trouver la commande de **fostate.sh** à partir du répertoire de /store de votre dernière mise à jour, par exemple, `/store/cca_upgrade-4.x.x.`

1. Exécutez le script de **fostate.sh** sur le premier CAM :`[root@cam1  cca_upgrade-4.x.x]# ./fostate.sh`
   My node is active, peer node is standby [root@cam1 cca_upgrade-4.x.x]# *!--- This CAM is the active CAM in the HA-pair*
2. Exécutez le script de **fostate.sh** sur le deuxième CAM :`root@cam2  cca_upgrade-4.x.x]# ./fostate.sh`
   My node is standby, peer node is active [root@cam2 cca_upgrade-4.x.x]# *!--- This CAM is the standby CAM in the HA-pair*

Comment vérifier état primaire/secondaire de configuration sur le CAM ha

Cet exemple affiche comment employer le CLI pour déterminer le mode ha (primaire/secondaire) pour ce que chaque CAM a été au commencement configuré dans les paires ha.

1. Trouvez le nom des CAMs (Noeuds) avec `/etc/ha.d/ha.cf.`
2. Vérifiez alors l'état sur chaque CAM, par exemple :`[root@cam1  ~]# /perfigo/control/bin/check-ha  cam1`
   `active`
   `[root@cam1  ~]#  /perfigo/control/bin/check-ha  cam2`
   `active`
3. Allez à `/perfigo/control/tomcat et exécutez le LS - La`.Si les webapps indique **normal-webapps**, c'est le CAM primaire.Si les webapps indique l'**admin-webapps**, c'est le CAM secondaire.Par exemple, ce CAM est le CAM primaire :`[root@cam1  tomcat]#  cd /perfigo/control/tomcat`
   `[root@cam1  tomcat]#  ls  -la`
   `total  216`
   `drwxr-xr-x12  root  root4096  Sep  14  23:28  .`
   `drwxr-xr-x8  root  root4096  Aug  28  22:12  ..`
   `drwxr-xr-x4  root  root4096  Aug  28  22:12  admin-webapps`
   `<output  cut…..>`
   `drwxr-xr-x2  root  root4096  Aug  28  22:12  temp`
   `lrwxrwxrwx1  root  root38  Sep  14  23:28` **`webapps -> /perfigo/control/tomcat/normal-webapps`** `drwxr-xr-x 3 root root 4096 Aug 28 15:15 work` Ce CAM est le CAM secondaire :`[root@cam2  tomcat]#  ls  -la`
   `total  216`
   `drwxr-xr-x12  root  root4096  Sep  14  23:33  .`
   `drwxr-xr-x8  root  root4096  Sep  152006  ..`
   `drwxr-xr-x4  root  root4096  Sep  152006  admin-webapps`
   `<output  cut  …>`
   `drwxr-xr-x2  root  root4096  Sep  152006  temp`

```
lrwxrwxrwx1  root  root37  Sep  14  23:33  webapps -> /perfigo/control/tomcat/admin-webapps
drwxr-xr-x 3 root root 4096 Sep 14 23:25 work
```

Dépannez

Problème 1

Une erreur se produit sur le CAM **« SSKEY sur le serveur n'apparie pas la valeur dans la base de données »** quand CAS secondaire dans des paires ha devient actif.

Solution

Résolvez ce problème quand vous poussez manuellement CAS primaire SSKEY au secondaire (bouton de remise SSKEY, ou dépassement manuel sur le fichier de /etc/.GUSSK sur CAS). Habituellement, ce problème se pose quand vous remplacez une appliance et ne faites pas delete/re-add il de/au CAM. Dans ce cas, CAS a son propre SSKEY basé sur son adresse MAC et probablement n'apparie pas celui précédemment réglé sur le CAM. Cela vaut particulièrement pour CAS secondaire parce qu'il a un SSKEY basé sur sa propre adresse MAC. Sur la configuration ha, même la secondaire doit utiliser CAS primaire SSKEY basé sur le MAC de CAS primaire.

Problème 2

Dans les paires de CAM de Basculement, le CAM primaire affiche l'`AVERTISSEMENT ! Connexions fermées à scruter [x.x.x.x] (adresse IP de réserve) base de données ! Veuillez redémarrer le noeud de pair pour apporter des bases de données dans le sync ! !.`

Solution

Quand le lien eth1 primaire a été déconnecté et seulement la liaison série demeure, le CAM renvoie une erreur de base données qui indique qu'elle ne peut pas sync avec son homologue ha, et l'administrateur voit cette erreur dans la console Web de CAM : .

```
WARNING! Closed connections to peer [standby
 IP] database! Please restart peer node to bring databases in
 sync!!
```

Les Certificats auto-signés ou tiers d'utilisation sur le CAM appareillent afin de résoudre ce problème.

Problème 3

Comment changer l'adresse IP pour la Haute disponibilité sur le CAM

Solution

Essayez de réduire le CAM secondaire avec l'**arrêt de perfigo de service**. De cette façon, il ne dirige pas les services de perfigo, mais il est encore accessible par SSH. Sur le CAM primaire, changez l'IP dans la **gestion > le gestionnaire > le réseau de CCA**. Ne le permettez pas de redémarrer encore. Allez alors à l'onglet de Basculement, et changez l'adresse IP de service. Après que cette étape, le redémarrent alors.

Une fois qu'il est entièrement, assurez-vous qu'il est accessible. Exécutez alors le **début de perfigo de service** sur le CAM secondaire, et apportez les mêmes modifications que vous avez faites au primaire. Puis, redémarrez-le, et il devrait monter en tant que secondaire. Pour le CERT SSL, s'il est fourni à un nom, puis changez l'entrée DNS de sorte que le nom le résolve au nouvel IP de service. S'il est fourni à l'IP, régénérez un nouveau certificat provisoire. En ce moment, vous voulez probablement avoir une ouverture de session utilisateur de test. Si cela réussit, le Basculement au secondaire, et s'assurent que vous pouvez également ouvrir une session.

Informations connexes

- Page de support d'appareils de Cisco NAC
- Support et documentation techniques - Cisco Systems