# NAC (CCA) : Comment corriger les erreurs de certificat sur CAM/CAS après la mise à niveau vers 4.1.6

## Contenu



## Introduction

Ce document décrit comment corriger des erreurs de certificat sur le serveur d'accès de Clean Access Manager (CAM) /Clean (CAS) avec la version 4.1.6.

## Conditions préalables

### Conditions requises

Cisco recommande que vous ayez la connaissance du processus de mise à niveau pour l'appliance du Cisco Network Admission Control (NAC).

### Composants utilisés

Les informations dans ce document sont basées sur la version 4.1.6 d'appareils de Cisco NAC avec CAM/CAS.

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.

# Procédure

Ces erreurs de certificat sont trouvées dans */perfigo/logs/perfigo-redirect.log0.log.0* ou */perfigo/logs/perfigo-log0.log.0*.

Voici un exemple d'une erreur de certificat :

```
SEVERE: RMISocketFactory:Creating RMI socket failed to host
        10.1.20.10:sun.security.validator.ValidatorException:
        Certificate chaining error
Aug 1, 2008 1:41:22 PM com.perfigo.wlan.web.admin.ConnectorClient connect
SEVERE: Communication Exception : java.rmi.ConnectIOException: Exception
        creating connection to: 10.1.20.10; nested exception is:
 javax.net.ssl.SSLHandshakeException:
        sun.security.validator.ValidatorException: Certificate chaining error
```

Ces erreurs sont un résultat des améliorations de la sécurité faites dans 4.1.6. Dans 4.1.6, CAS et le CAM agissent en tant que client et serveur entre eux et doivent se faire confiance. Chacun exige les Certificats de racine et d'intermédiaire de l'autre. Par exemple, si CAS a un certificat Verisign et le CAM fait avoir besoin un certificat (provisoire) de Perfigo, CAS et CAM de la chaîne de Verisign (racine et intermédiaires) et de la racine de Perfigo.

Terminez-vous ces étapes afin de corriger les erreurs de certificat :

1. Sauvegardez tous les Certificats installés qui ne sont pas les Certificats provisoires.Sur le CAM, ouvrez l'interface web, et allez à la **gestion > au gestionnaire de CCA > au certificat SSL > X509**.Sur CAS, allez directement à l'interface web par l'intermédiaire de https:// <CAS IP>/admin, et puis allez à la **gestion > au certificat SSL > X509**.Choisissez la **clé/certificat de l'exportation CSR/Private du** choisir une liste déroulante d'action.Cliquez sur l'**exportation** située à côté du certificat actuellement installé, et sauvegardez ce fichier.Cliquez sur l'**exportation** située à côté de la clé privée actuellement installée, et sauvegardez ce fichier.
2. Après la sauvegarde, si CAS et le CAM n'utilisent pas déjà les Certificats provisoires, générez-les.Sur le CAM, ouvrez l'interface web, et allez à la **gestion > au gestionnaire de CCA > au certificat SSL > X509**.Sur CAS, allez directement à l'interface web par l'intermédiaire de https:// <CAS IP>/admin, et puis allez à la **gestion > au certificat SSL > X509**.Choisissez **génèrent le certificat provisoire de la** liste déroulante.Complétez les champs répertoriés, et le clic **se produisent**.**Note**: Ceci n'exige plus d'une réinitialisation de prendre effet.
3. Enlevez toutes les autorités de certification de confiance de CAS et du CAM. Cette étape le facilite pour gérer et améliorer la Sécurité.Sur le CAM, allez à la **gestion > au gestionnaire de CCA > au SSL > les autorités de certification de confiance**.Sur CAS, allez à la **gestion > au SSL > les autorités de certification de confiance**.Créez un filtre pour exclure le certificat de Perfigo.Choisissez le **nom unique de la** liste déroulante de filtre d'ajouter.Choisissez **contient pas de la** liste déroulante qui apparaît à côté du nom unique.Tapez Perfigo dans le champ texte, et puis cliquez sur le **filtre**.Choisissez 100 de la liste déroulante située à côté du bouton sélectionné par effacement.Cliquez sur la case au-dessous de la liste déroulante sélectionnée par effacement afin de sélectionner toutes les autorités de certification (CAs) dans la liste.Cliquez sur Delete **sélectionné** afin de supprimer tout le CAs dans la liste.Continuez à cliquer sur la case, et cliquez sur Delete **sélectionné** jusqu'à ce que tous les CAs soient supprimés.

4. Après que vous retiriez tout le CAs, les Certificats de racine et d'intermédiaire doivent être importés.Sur le CAM, allez à la **gestion > au gestionnaire de CCA > au SSL > les autorités de certification de confiance**.Sur CAS, allez à la **gestion > au SSL > les autorités de certification de confiance**.Cliquez sur **parcourent**, et choisissent le certificat racine d'abord.**Note**: Le sujet et l'émetteur devraient être placés à la même valeur.Cliquez sur l'**importation**, et le CA devrait apparaître dans la liste ci-dessous.Exécutez la même procédure pour tous les Certificats intermédiaires.
5. Installez les Certificats de CAS et de CAM que vous avez sauvegardés dans la première étape.Sur le CAM, ouvrez l'interface web, et allez à la **gestion > au gestionnaire de CCA > au certificat SSL > X509**.Sur CAS, allez directement à l'interface web par l'intermédiaire de https:// <CAS IP>/admin, et puis allez à la **gestion > au certificat SSL > X509**.Choisissez le **certificat d'importation de la** liste déroulante.Cliquez sur **parcourent**, et choisissent le certificat enregistré de l'étape 1.Cliquez sur Upload.Cliquez sur **parcourent** de nouveau, et choisissent la clé privée qui a été enregistrée de l'étape 1.Choisissez la **clé privée du** type de fichier liste déroulante, et puis cliquez sur Upload.Cliquez sur **vérifient et installent les Certificats téléchargés**.**Note**: Ce message d'erreur ne doit pas être réparé par ces procédures :

   ```
   SEVERE: SSLFilter:access deniedCN=cas1.domain.com,
           OU=Information Technologies, O=Company, ST=State,
           C=US:Netscape cert type does not permit use for SSL client
   ```

   Si les logs contiennent ce message, vous devez entrer en contact avec le fournisseur de certificat. Le certificat doit être révisé avec le champ de type de CERT de Netscape réglé au serveur SSL et au client SSL.

## Informations connexes

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