Résoudre les problèmes AppDynamics SSL/TLS après la mise à jour DigiCert Root G2

Table des matières

Introduction

Ce document décrit comment résoudre les problèmes d'approbation de certificat SSL (Secure Socket Layer)/ TLS (Transport Layer Security) dans les agents AppDynamics.

Conditions préalables

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document décrit comment résoudre les problèmes de confiance de certificat SSL (Secure

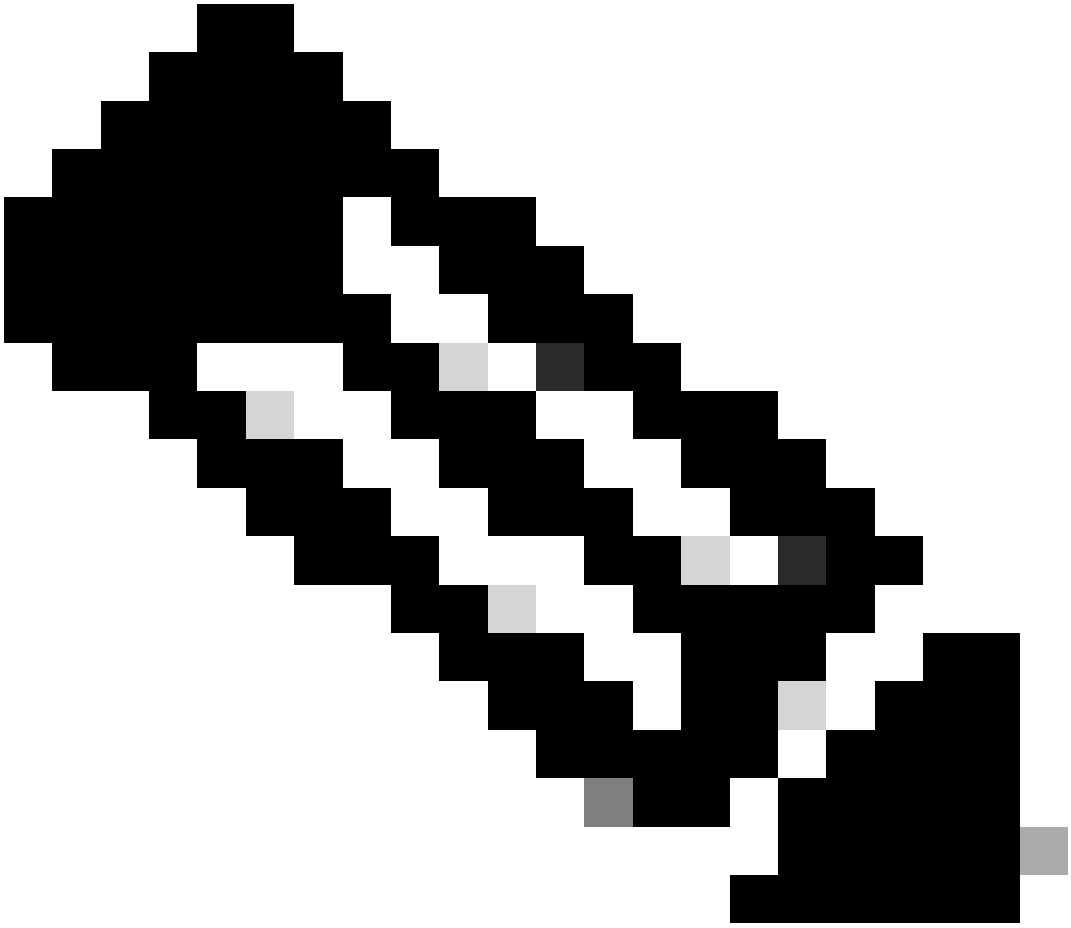
Socket Layer)/ TLS (Transport Layer Security) dans AppDynamics Agents après la migration récente de DigiCert Global Root CA vers DigiCert Global Root G2.

Il fournit des étapes détaillées pour garantir une configuration correcte et restaurer une connectivité transparente.

En 2023, DigiCert a initié la transition vers le certificat de signature DigiCert Global Root G2 pour l'émission de certificats publics TLS/SSL. Cette modification a été provoquée par la mise à jour de la stratégie d'approbation de Mozilla, qui exige que les certificats racine soient mis à jour tous les 15 ans, et par la méfiance envers les certificats plus anciens à partir de 2025.

Le nouveau certificat de signature utilise l'algorithme SHA-256 plus sécurisé, remplaçant l'ancienne norme SHA-1. Dans le cadre de cette transition, AppDynamics a mis à jour ses certificats SSL pour le domaine .saas.appdynamics.com afin d'utiliser les certificats de deuxième génération le 2025-06-10.

Cette mise à jour a entraîné la perte de connectivité de certains agents d'application avec les contrôleurs SaaS en raison de leur incapacité à reconnaître le nouveau certificat. Pour garantir une connectivité ininterrompue, il est essentiel de mettre à jour le magasin de confiance de l'agent AppDynamics afin d'inclure les nouveaux certificats DigiCert Global Root G2 et IdenTrust.



Remarque : Cette modification concerne principalement les agents qui utilisent le truststore personnalisé ou une très ancienne version de OS/java où les certificats requis ne sont pas inclus dans le truststore OS/java par défaut.

Problème

Il y a un problème de connectivité entre les agents AppDynamics et le contrôleur, et les journaux affichent des erreurs liées à la configuration ou à la communication SSL.

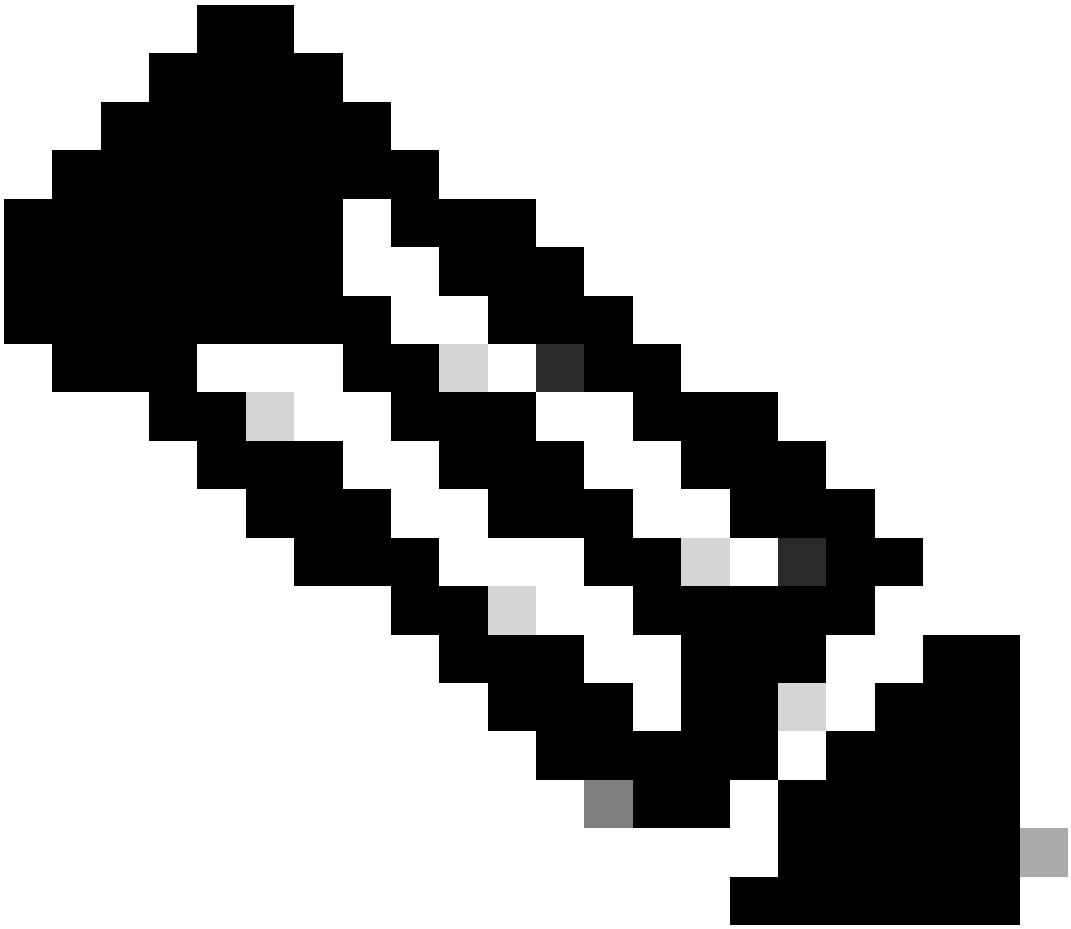
Exemple de message d'erreur dans les journaux : "Échec de la création du chemin PKIX : xxxx : impossible de trouver un chemin de certification valide vers la cible demandée lors de la tentative de validation"

Solution

Étape 1. Télécharger les certificats

- Racine globale DigiCert G2 :
  - Visiter les certificats d'autorité racine de confiance DigiCert
  - Recherchez « DigiCert Global Root G2 » et téléchargez le certificat.
- IdenTrust :
  - Accédez à IdenTrust Commercial Root CA 1
  - Copiez le contenu du certificat et enregistrez-le dans un fichier (par exemple, Idmandstcommercial.cer ou Idmandstcommercial.pem)

Étape 2 : identification de l’emplacement du Truststore



Remarque : L'emplacement du magasin de confiance est requis à l'étape 3. Importez des certificats dans le magasin de confiance

---

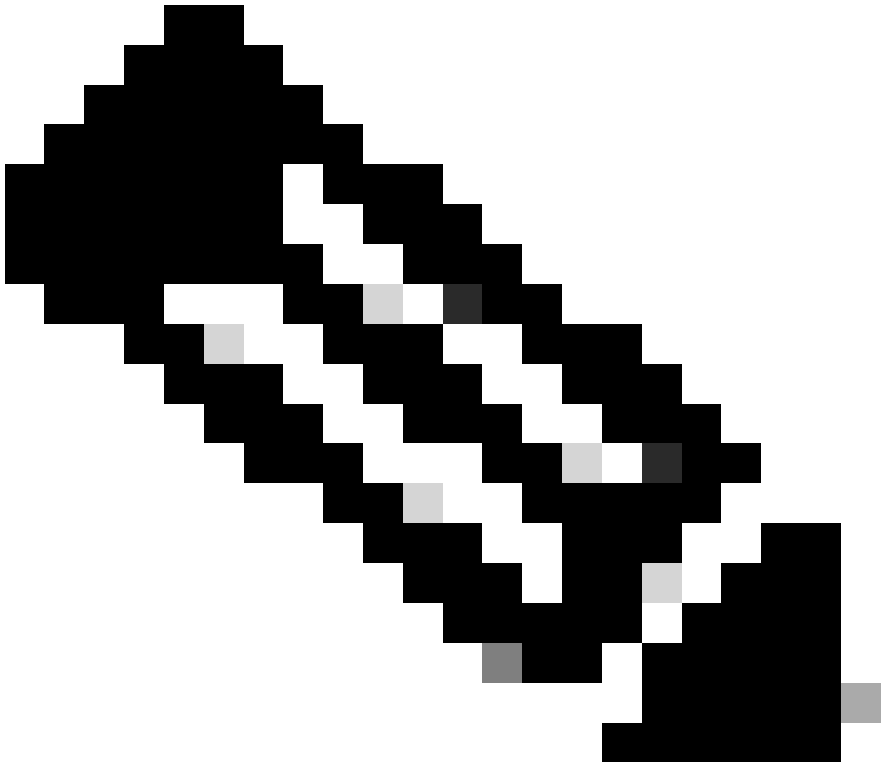
- Java, agent de base de données ou agent machine
  - JVM, argument propriété Truststore

1. Vérifiez si la propriété -Djavax.net.ssl.trustStore est définie en tant qu'arguments JVM lors du lancement de l'agent.
2. Si cette propriété est définie, inspectez le fichier keystore spécifié par cette propriété pour vérifier qu'il inclut les deux certificats (certificats racines DigiCert Global Root G2 et IdenTrust).
   (Si la propriété n'est pas définie, passez à l'étape suivante.)

- XML des informations du contrôleur

1. L'agent peut être configuré pour utiliser le keystore défini dans le fichier controller-info.xml de votre répertoire de conf de l'agent.
2. Vérifiez le paramètre controller-keystore-filename.
3. Le cas échéant, inspectez le fichier keystore spécifié pour vérifier que les deux certificats sont inclus.
   (Si elle est introuvable, passez à l'étape suivante.)

- Fichier cacerts.jks de l'agent
  1. Recherchez un fichier nommé cacerts.jksdans le répertoire d'installation du programme de configuration de l'agent.
  2. Inspectez ce fichier pour vérifier que les deux certificats sont inclus.
     (Si elle est introuvable, passez à l'étape suivante.)

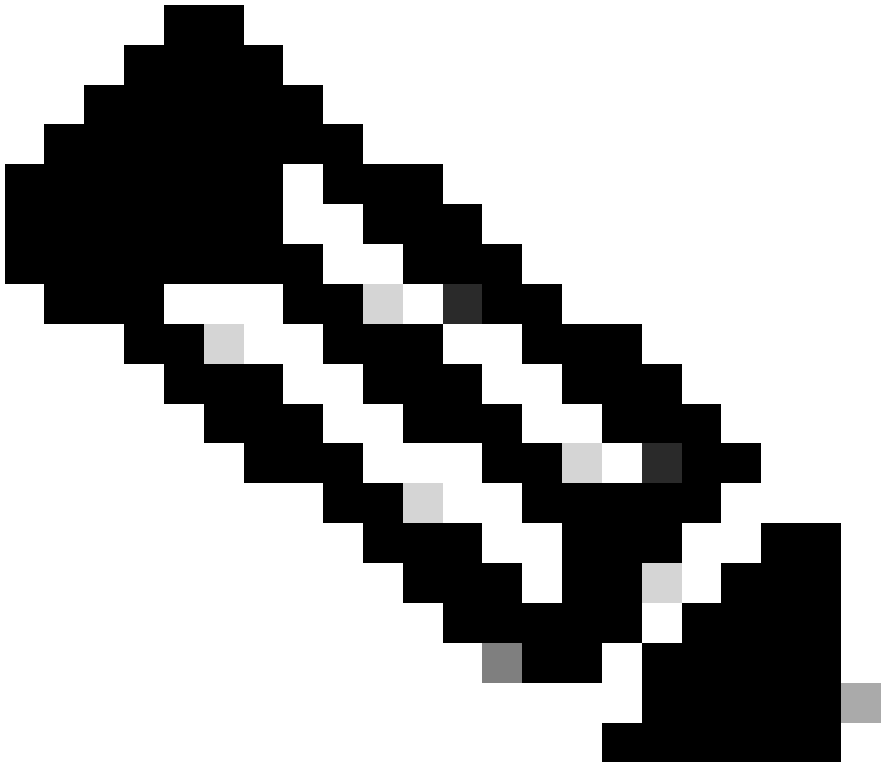


Remarque : Répertoire d'installation des agents

Pour l'agent Java : AGENT_HOME/verxxx/conf ou AGENT_HOME/conf

Pour l'ordinateur ou l'agent DB : AGENT_HOME/conf

- Magasin de confiance par défaut JRE
  1. Si aucune des configurations précédentes n'est trouvée, l'agent utilise le magasin de confiance par défaut de JRE, généralement situé à l'adresse JRE_HOME/lib/security/cacerts.
  2. Inspectez ce fichier pour vous assurer que les certificats sont inclus.



Remarque : Si vous utilisez IBM Websphere ou IBM Websphere Liberty Profile, le répertoire JRE_HOME se trouve dans AppServer ou Liberty Directory sous le répertoire d'installation Websphere respectivement, c'est-à-dire IBM_WEBSPHERE_HOME/AppServer/java/ ou IBM_WEBSPHERE_HOME/Liberty/java/

- Agent analytique
  - Vérifiez si le chemin (y compris le nom) de l'agent truststore est spécifié à l'aide

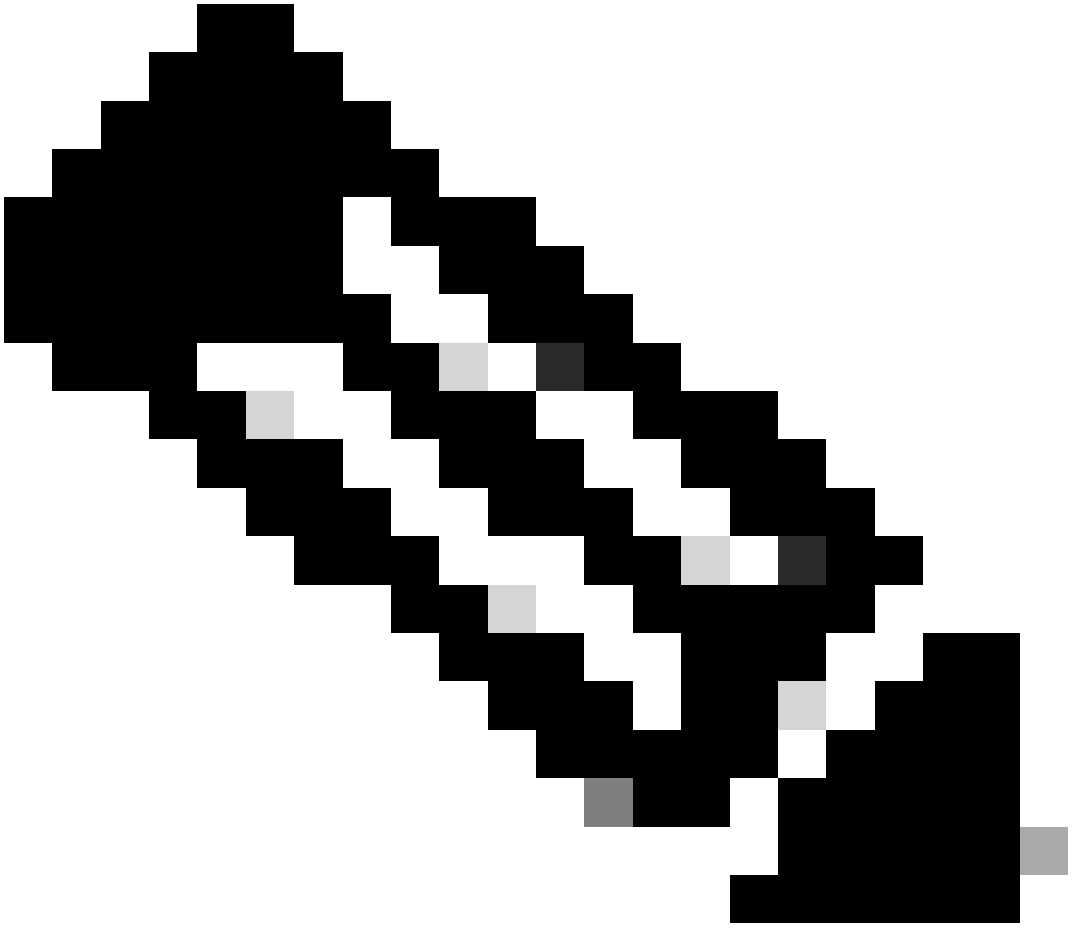
de l'élément <ad.controller.https.trustStorePath> dans le fichier de configuration de l'agent analytics-agent.properties, alors l'agent charge ce trustore.
    - S'il n'est pas spécifié dans thead.controller.https.trustStorePath, il charge le fichier de confiance Java par défaut de la machine virtuelle Java instrumentée, <JRE_HOME>/lib/security/cacerts (default password changeit)
    - Si l'agent ad.controller.https.trustStorePath et l'agent d'analyse ne sont pas spécifiés est utilisé en tant qu'extension d'agent Machine, alors il charge le magasin de confiance utilisé par l'agent Machine.

- Agent DotNet

    - Pour Windows :
        - Accédez à la vue d'installation du certificat en accédant à Exécuter> MMC.exe> selectFile dans la barre d'outils et sélectionnez Ajouter/Supprimer un composant logiciel enfichable.
        - Ajouter ou supprimer des composants logiciels enfichables s'ouvre, sélectionnez Certificats> Cliquez sur Ajouter. La fenêtre du composant logiciel enfichable Certificat s'ouvre. Sélectionnez Compte d'ordinateur> Choisissez Local ou Autre ordinateur en conséquence >Cliquez sur Terminer>OK.
        - Développez Certificates (Local Computer) > Sélectionnez le dossier Trusted Root Certification Authority et développez pour afficher le dossier Certificates.
        - Double-cliquez sur le dossier Certificats et notez la liste des certificats de confiance existants. Déterminez si les certificats racine globaux DigiCert G2 et IdenTrust sont présents ou importez les certificats manquants.

    - Pour Linux :

        - L'emplacement du magasin de confiance varie entre les distributions Linux. Les emplacements courants sont :/etc/ssl/certs (OS comme CentOS/RHEL/Debian)



Remarque : Si les certificats DigiCert Global Root G2 ou IdenTrust sont absents de tous ces emplacements vérifiés, vous devez les ajouter. Reportez-vous aux étapes mentionnées à l'« Étape 3. Importation de certificats dans le magasin de confiance » pour importer les certificats dans le magasin de confiance.

Étape 3. Importation de certificats dans le Truststore

- Agent Java, Base de données, Machine ou Analytique
    - Ouvrez votre terminal ou votre invite de commandes et utilisez cette commande keytool pour importer des certificats racine DigiCert Global Root G2 et IdenTrust.

```
keytool -import -trustcacerts -alias
```

```
-file

 -keystore

  -storepass
```

Remplacer :

- : Un alias unique (par exemple, digicertglobalrootg2, identrustcoomercial).
- : Chemin d'accès au fichier de certificat (par exemple, /home/username/Downloads/DigiCertGlobalRootG2.crt).
- : Chemin d'accès au fichier truststore de l'agent (par exemple, /opt/appdynamics/agent/ver25.x.x.x/conf/cacerts.jks).
- : Mot de passe Truststore (par défaut : changeit, sauf sur mesure).

- Exemple d'importation du certificat global racine G2 DigiCert.

```
keytool -import -trustcacerts -alias digicertglobalrootg2 -file /home/username/Downloads/Dig
```

- Exemple d'importation d'un certificat racine commercial IdenTrust.

```
keytool -import -trustcacerts -alias identrustcommercial -file /home/username/Downloads/iden
```

- Agent DotNet
  - Pour Windows :
    - Accédez à la vue d'installation du certificat en accédant à Exécuter> MMC.exe> selectFile dans la barre d'outils et sélectionnez Ajouter/Supprimer un composant logiciel enfichable.
    - Ajouter ou supprimer des composants logiciels enfichables s'ouvre, sélectionnez

Certificats> Cliquez sur Ajouter. La fenêtre du composant logiciel enfichable Certificat s'ouvre. Sélectionnez Compte d'ordinateur> Choisissez Local ou Autre ordinateur en conséquence >Cliquez sur Terminer>OK.
    - Développez Certificates (Local Computer) > Sélectionnez le dossier Trusted Root Certification Authority et développez pour afficher le dossier Certificates.
    - Cliquez avec le bouton droit sur le dossier Certificateset sélectionnezToutes les tâches > Importer.L'Assistant Importation de certificat s'ouvre, suivez les instructions et ajoutez lesCertificat DigiCert Global Root G2 et/ou certificat racine IdenTrust.

- Pour Linux :
    - Copiez les fichiers DigiCert Global Root G2 et IdenTrust Root Certificate téléchargés dans le répertoire du magasin de confiance identifié.
    - Mettez à jour le magasin d'approbations en exécutant la commande.

```
sudo update-ca-certificates
```

Étape 4. Vérification de l'importation

- Agent Java, Base de données, Machine ou Analytique
    - Pour vérifier que les certificats ont bien été ajoutés, exécutez la commande suivante :

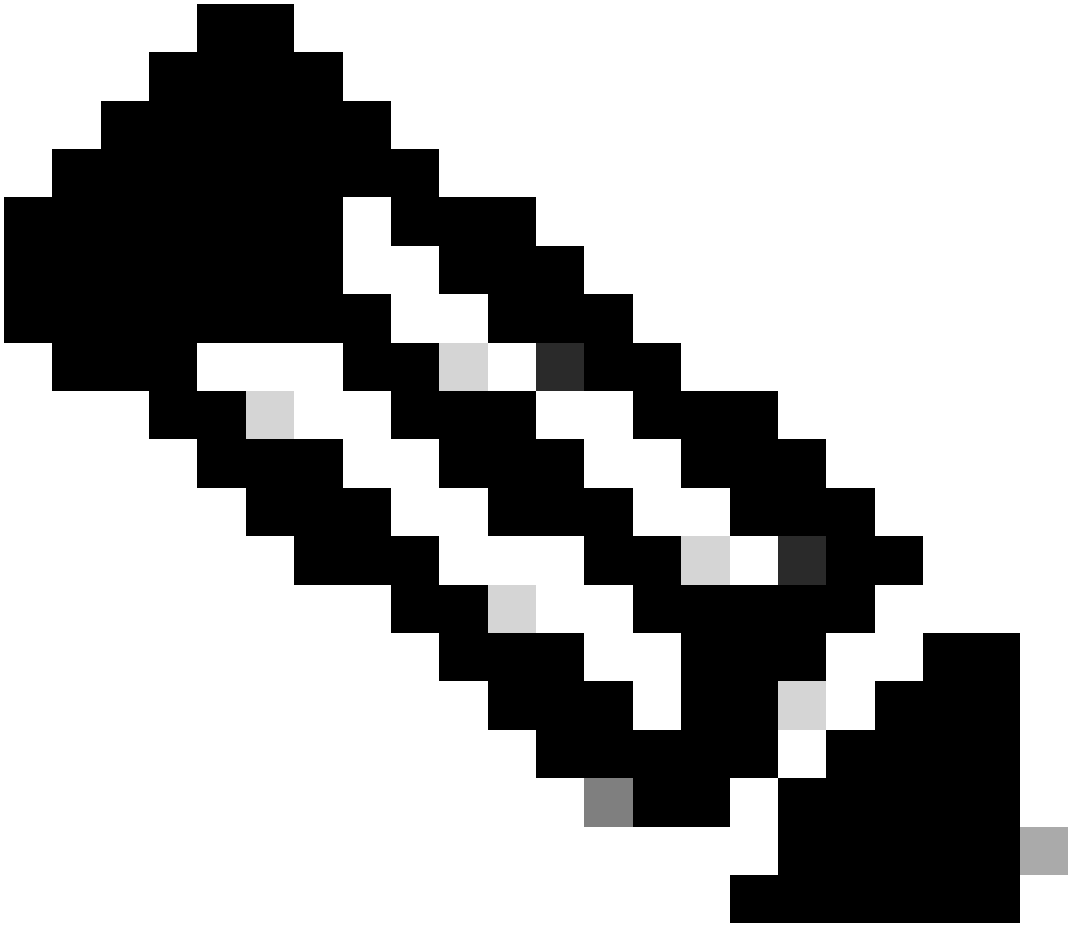
```
keytool -list -v -keystore

            -storepass

             | grep -e "DigiCert Global Root G2" -e "IdenTrust Commercial Root CA 1" -A 10
```

Remplacer :

- `<chemin_magasin_confiance_agent>` : Chemin d'accès au fichier truststore de l'agent.
- `<truststore_password>` : Mot de passe truststore.



Remarque : Assurez-vous que DigiCert Global Root G2 et IdenTrust Commercial Root CA 1 apparaissent dans le résultat.

- Agent DotNet
  - Pour Windows :
    - Accédez à la vue d'installation du certificat en accédant à Exécuter> MMC.exe> selectFile dans la barre d'outils et sélectionnez Ajouter/Supprimer un composant logiciel enfichable.
    - Ajouter ou supprimer des composants logiciels enfichables s'ouvre, sélectionnez Certificats> Cliquez sur Ajouter. La fenêtre du composant logiciel enfichable Certificat s'ouvre. Sélectionnez Compte d'ordinateur> Choisissez Local ou Autre ordinateur en conséquence >Cliquez sur Terminer>OK.
    - Développez Certificates (Local Computer) > Sélectionnez le dossier Trusted Root Certification Authority et développez pour afficher le dossier Certificates.
    - Double-cliquez sur le dossier Certificates et vous devez voir les certificats racine

globaux DigiCert G2 et IdenTrust ici.

- Pour Linux :
  - Exécutez la commande et vérifiez si DigiCert Global Root G2 et IdenTrust Root Certificate existent :

```
awk '/-----BEGIN CERTIFICATE-----/,/-----END CERTIFICATE-----/ {
    print > "/tmp/current_cert.pem"
    if (/-----END CERTIFICATE-----/) {
        system("openssl x509 -noout -subject -in /tmp/current_cert.pem | grep -E \"Digi
        close("/tmp/current_cert.pem")
    }
}' /etc/ssl/certs/ca-certificates.crt
```

Étape 5. Redémarrez l'agent

Enfin, redémarrez votre agent AppDynamics. Cela permet aux modifications de prendre effet.

Informations connexes

Avis d'assistance : Ajout de certificats SSL racine DigiCert et IdenTrust aux magasins d'approbations d'agents

Besoin d'aide supplémentaire ?

Si vous avez une question ou rencontrez des problèmes, veuillez créer un ticket d'assistance avec ces détails :

- Journaux de l'agent.
- Détails de l'emplacement du magasin de confiance et des certificats ajoutés.
- Tous les messages d'erreur rencontrés.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.