# DigiCertルートG2アップデート後のAppDynamics SSL/TLS問題の解決

## 内容



## はじめに

このドキュメントでは、AppDynamics AgentでのSSL(Secure Socket Layer)/TLS(Transport Layer Security)証明書信頼の問題に対処する方法について説明します。

## 前提条件

### 使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

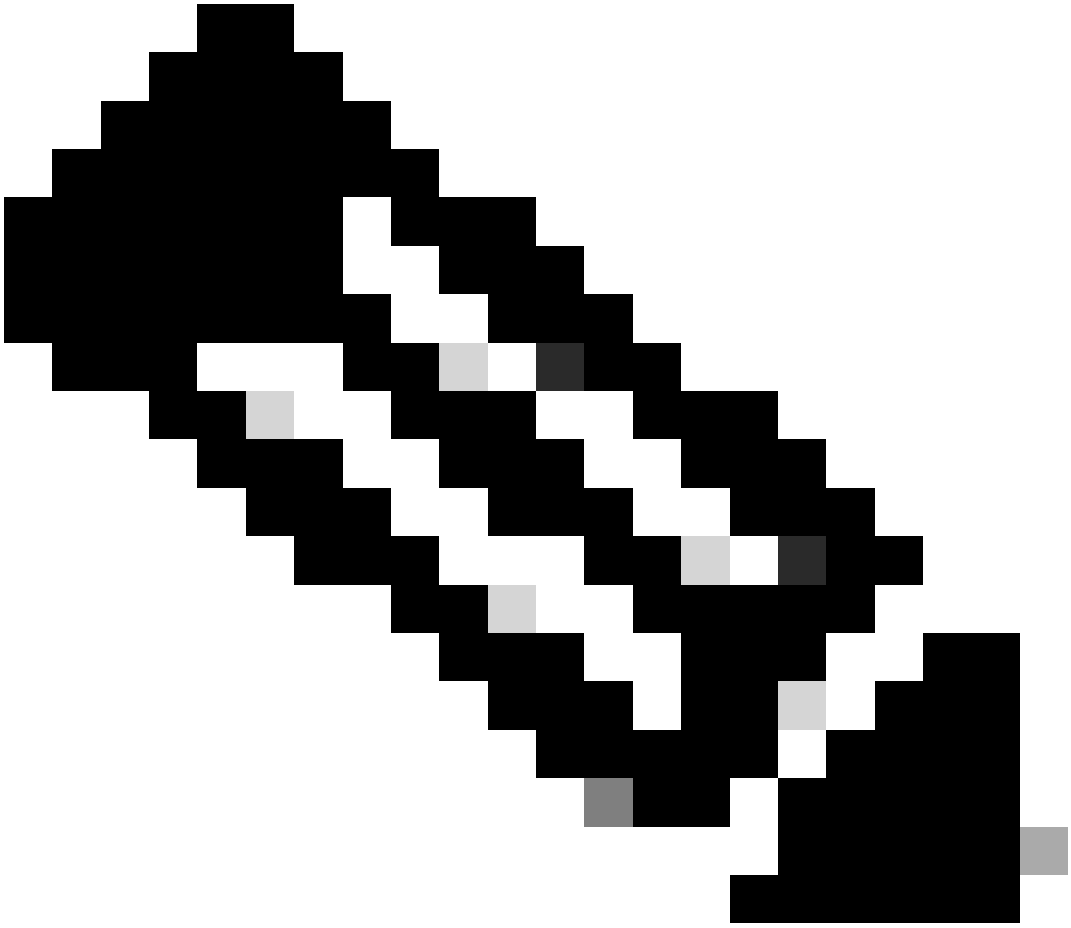
このドキュメントでは、DigiCertグローバルルートCAからDigiCertグローバルルートG2への最近の移行後に、AppDynamicsエージェントでSSL(Secure Socket Layer)/TLS(Transport Layer Security)証明書信頼の問題に対処する方法について説明します。

適切な設定を行い、シームレスな接続を復元するための詳細な手順を示します。

2023年、DigiCertは、パブリックTLS/SSL証明書を発行するためのDigiCertグローバルルートG2署名証明書への移行を開始しました。この変更を促したのは、Mozillaが信頼ポリシーを更新し、ルート証明書を15年ごとに更新することを義務付け、2025年以降は古い証明書を信頼しないという方針を打ち出したことです。

新しい署名証明書では、古いSHA-1標準に代わって、より安全なSHA-256アルゴリズムが採用されています。この移行の一環として、AppDynamicsはドメイン.saas.appdynamics.comのSSL証明書を更新し、2025-06-10の第2世代証明書を利用できるようにしました。

この更新により、一部のアプリケーションエージェントは、新しい証明書を認識できないため、SaaSコントローラとの接続を失いました。中断のない接続を確保するには、AppDynamicsエージェント信頼ストアを更新して、新しいDigiCertグローバルルートG2証明書とIdentrust証明書を含めることが重要です。



注：この変更は、主に、カスタムトラストストアを使用しているエージェント、または必要な証明書がデフォルトのOS/Javaトラストストアに含まれていない非常に古いバージョンのOS/Javaを使用しているエージェントに影響を与えます。

## 問題

AppDynamicsエージェントとコントローラーの間に接続の問題があり、ログにSSL構成または通信に関連するエラーが表示されています。

ログのエラーメッセージの例：「PKIX path building failed: xxxx: unable to find valid certification path to requested target attempting validation」

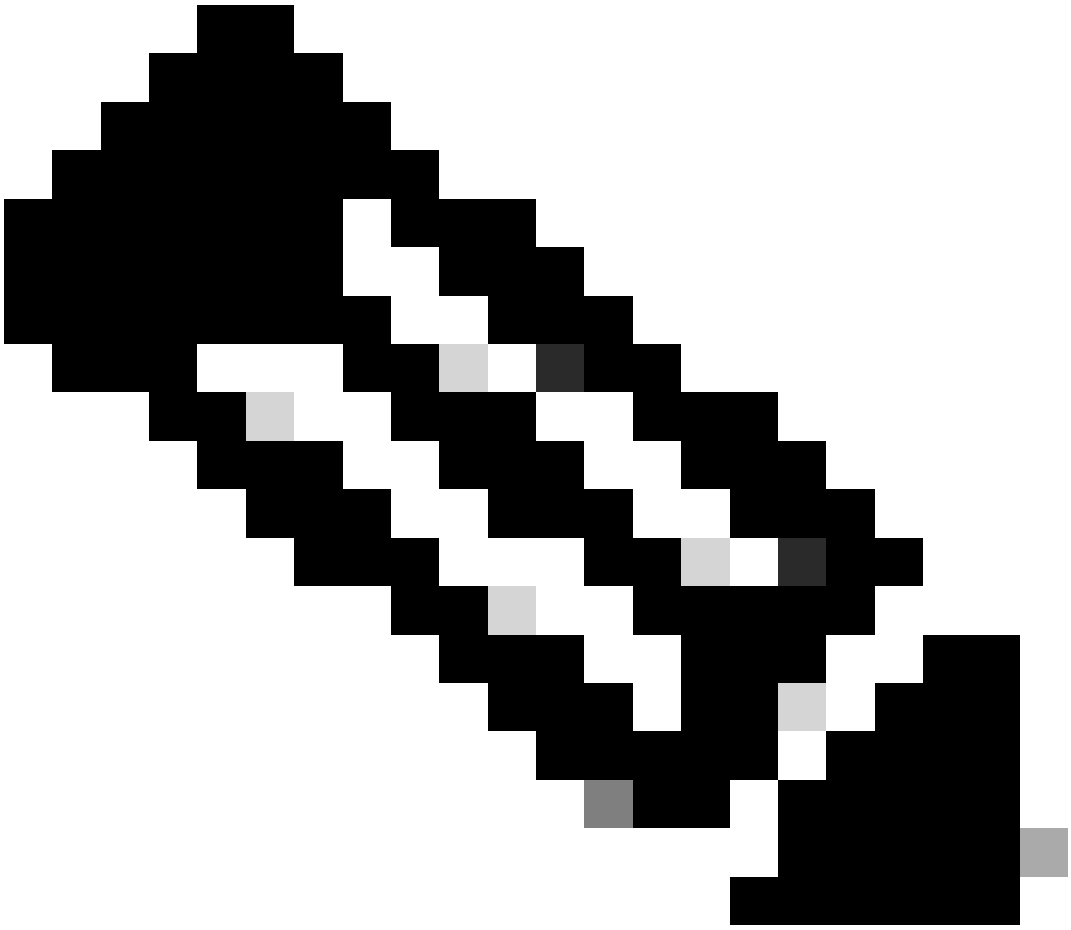
## 解決方法

### ステップ 1：証明書のダウンロード

- DigiCertグローバルルートG2:
  - DigiCert Trusted Root Authority Certificatesにアクセスします。
  - 「DigiCert Global Root G2」を検索し、証明書をダウンロードします。
- Identrust:
  - Identrust Commercial Root CA 1に移動します。
  - 証明書の内容をコピーし、ファイルとして保存します（Identtrustcommercial.cer、Identtrustcommercial.pemなど）。

## ステップ 2：トラストストアの場所の特定

---



注：手順3ではトラストストアの場所が必要です。トラストストアへの証明書のインポート

---

- Java、データベース、またはマシンエージェント
  - JVM引数Truststoreプロパティ

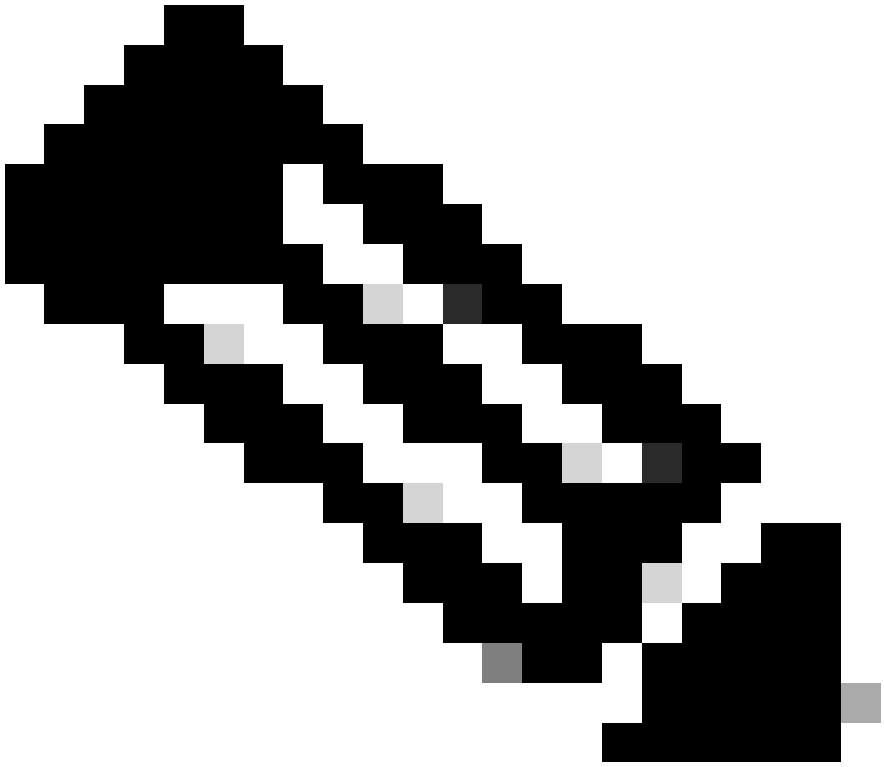
1. エージェントの起動時に、-Djavax.net.ssl.trustStoreプロパティがJVM引数として設定されているかどうかを確認します。
2. このプロパティーが設定されている場合は、このプロパティーで指定されているキーストアファイルを調べて、証明書(DigiCertグローバルルートG2およびIdentrustルート証明書)の両方が含まれていることを確認します。
（プロパティが設定されていない場合は、次の手順に進みます）。

- コントローラ情報XML

1. エージェントは、エージェントのconfディレクトリにあるcontroller-info.xmlファイルで定義されているキーストアを使用するように設定できます。
2. controller-keystore-filename設定を確認します。
3. 存在する場合は、指定したキーストアファイルを調べて、両方の証明書が含まれていることを確認します。
（見つからない場合は、次の手順に進みます）。

- Agent cacerts.jksファイル
1. エージェントのインストールディレクトリのフォルダ内にあるcacerts.jkssoverという名前のファイルを確認します。
2. このファイルを調べて、両方の証明書が含まれていることを確認します。
（見つからない場合は、次の手順に進みます）。

---



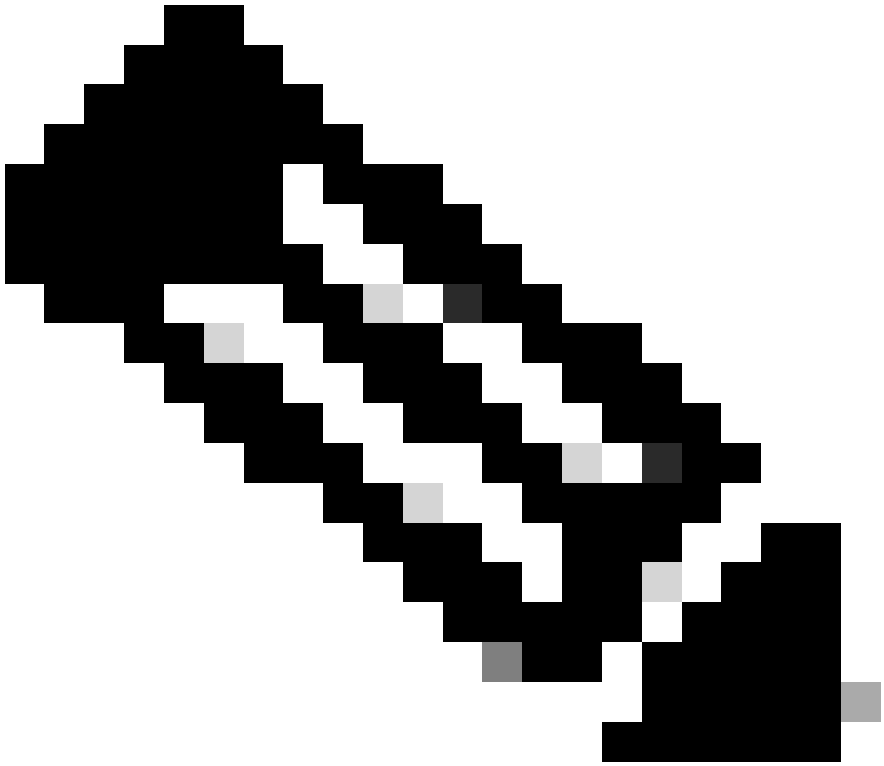
---

注：エージェントのインストールディレクトリ

Java Agentの場合：AGENT_HOME/verxxx/confまたは AGENT_HOME/conf

マシンまたはDBエージェント：AGENT_HOME/conf

- JREのデフォルトのトラストストア
  1. 上記の設定のいずれも見つからない場合、フォールバックとして、エージェントはJREのデフォルトのトラストストア(通常はJRE_HOME/lib/security/cacertsにあります)を使用します。
  2. このファイルを調べて、証明書が含まれていることを確認します。



注: IBM WebsphereまたはIBM Websphere Libertyプロファイルを使用している場合、JRE_HOMEは、それぞれWebsphereインストールディレクトリの下のAppServerまたはLibertyディレクトリ内、つまり IBM_WEBSPHERE_HOME/AppServer/java/または IBM_WEBSPHERE_HOME/Liberty/java/にあります

- 分析エージェント

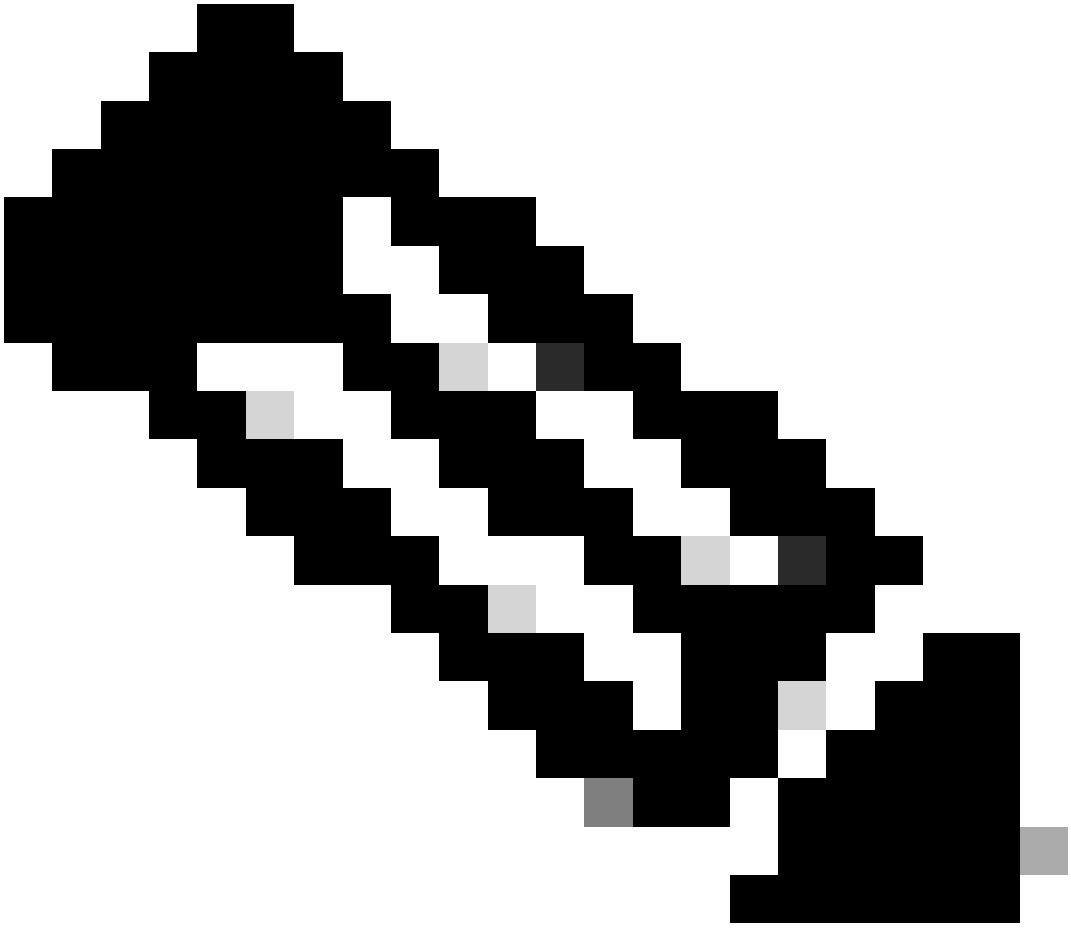
    - 確認エージェントの設定ファイルanalytics-agent.propertiesで<ad.controller.https.trustStorePath>要素を使用して、エージェントのトラストストアのパス（名前を含む）が指定されている場合、エージェントはそのトラストストアをロードします。
    - thead.controller.https.trustStorePathに指定しない場合、インストルメント化されるJVMのデフォルトのJavaトラストストアである<JRE_HOME>/lib/security/cacerts(デフォルトパスワードchangeit)がロードされます
    - ad.controller.https.trustStorePathで指定されておらず、分析エージェントがMachine Agent拡張として使用されている場合、Machine Agentによって使用されるトラストストアがロードされます。

- DotNetエージェント

    - Windows の場合：
        - ツールバーでRun> MMC.exe> selectFileの順に選択し、Add/Remove Snap-inを選択して、証明書のインストールビューに移動します。
        - スナップインの追加と削除ウィンドウが開いたら、selectCertificates> ClickAddをクリックします。証明書スナップインウィンドウが開きます。Computer Account> Choose Local or Another Computer assured >ClickFinish>OKを選択します。
        - Certificates (Local Computer)を展開します。> Trusted Root Certification Authorityフォルダを選択し、展開してCertificatesfolderを表示します。
        - Certificatesフォルダをダブルクリックし、既存の信頼できる証明書のリストを確認します。DigiCertグローバルルートG2とIdentrustルート証明書の両方が存在するかどうかを確認します。存在しない場合は、不足している証明書をインポートします。

    - Linuxの場合：

        - 信頼ストアの場所は、Linuxディストリビューションによって異なります。/etc/ssl/certs(CentOS/RHEL/DebianなどのOS)を含む



注：チェックしたすべての場所でDigiCertグローバルルートG2証明書またはIdentrust証明書が欠落している場合、証明書を追加する必要があります。「ステップ3」の手順を参照してください。Import Certificates to the Truststore」を実行して、証明書をトラストストアにインポートします。

## ステップ 3：トラストストアへの証明書のインポート

- Java、データベース、マシン、または分析エージェント
  - ターミナルまたはコマンドプロンプトを開き、このkeytoolコマンドを使用してDigiCertグローバルルートG2およびIdentrustルート証明書をインポートします。

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

```
-file

 -keystore

  -storepass
```

置換:

- ：一意のエイリアス(digicertglobalrootg2, identrustcoomercialなど)。
- ：証明書ファイルのパス(/home/username/Downloads/DigiCertGlobalRootG2.crtなど)。
- ：エージェントのトラストストアファイルのパス (/opt/appdynamics/agent/ver25.x.x.x/conf/cacerts.jksなど)。
- ：トラストストアパスワード(デフォルト：カスタマイズされchangeit, ていない限り)。

◦ DigiCertグローバルルートG2証明書のインポート例。

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

◦ Identrust商用ルート証明書のインポート例。

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

- DotNetエージェント
  - Windows の場合：
    - ツールバーでRun> MMC.exe> selectFileの順に選択し、Add/Remove Snap-inを選択して、証明書のインストールビューに移動します。
    - スナップインの追加と削除ウィンドウが開いたら、selectCertificates> ClickAddをクリックします。証明書スナップインウィンドウが開きます。

Computer Account> Choose Local or Another Computer assured >ClickFinish>OKを選択します。
- Certificates (Local Computer)を展開します。> Trusted Root Certification Authorityフォルダを選択し、展開してCertificatesfolderを表示します。
- Certificatesfolderを右クリックし、All Tasks > Import.Certificate Import Wizardを選択し、指示に従って行き、不足している証明書を追加しますDigiCertグローバルルートG2証明書またはIdentrustルート証明書、あるいはその両方。

- Linuxの場合:
  - ダウンロードしたDigiCertグローバルルートG2およびIdentrustルート証明書ファイルを、指定した信頼ストアディレクトリにコピーします。
  - コマンドを実行して、信頼ストアを更新します。

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

## ステップ 4：インポートの確認

- Java、データベース、マシン、または分析エージェント
  - 証明書が正常に追加されたことを確認するには、次のコマンドを実行します。

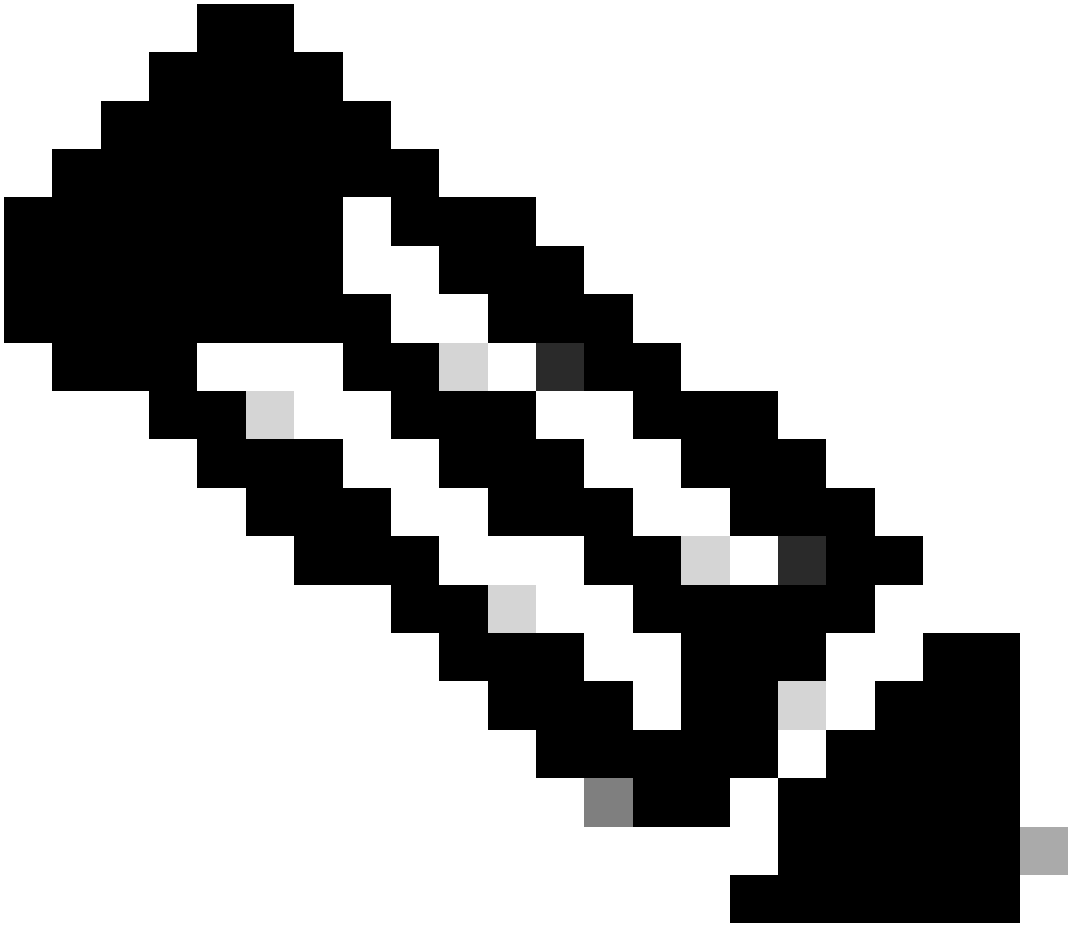
```
keytool -list -v -keystore

        -storepass

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

置換:

- <agent_truststore_path>:エージェントのtruststoreファイルのパス。
- <truststore_password>:トラストストアのパスワード。



注：出力にDigiCert Global Root G2とIdentrust Commercial Root CA 1の両方が表示されることを確認します。

---

- DotNetエージェント
    - Windows の場合：
        - ツールバーでRun> MMC.exe> selectFileの順に選択し、Add/Remove Snap-inを選択して、証明書のインストールビューに移動します。
        - スナップインの追加と削除ウィンドウが開いたら、selectCertificates> ClickAddをクリックします。証明書スナップインウィンドウが開きます。Computer Account> Choose Local or Another Computer assured >ClickFinish>OKを選択します。
        - Certificates (Local Computer)を展開します。> Trusted Root Certification Authorityフォルダを選択し、展開してCertificatesfolderを表示します。
        - Certificatesフォルダをダブルクリックすると、DigiCert Global Root G2とIdentrust root証明書の両方が表示されます。

- Linuxの場合:
  - コマンドを実行し、ifDigiCert Global Root G2 & Identrust Root Certificateexists:

```
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
```

### ステップ 5：エージェントの再起動

最後に、AppDynamicsエージェントを再起動します。これにより、変更が有効になります。

---

## 関連情報

サポートアドバイザリ：DigiCertおよびIdentrustルートSSL証明書のAgent Trust Storeへの追加

## サポートが必要な場合

質問がある場合、または問題が発生した場合は、次の詳細情報を含むasupport チケットを作成してください。

- エージェントからのログ。
- 追加されたトラストストアの場所と証明書の詳細。
- エラーメッセージが表示された。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。