在DigiCert根G2更新後解決AppDynamics SSL/TLS問題

目錄

簡介

本文檔介紹如何解決AppDynamics代理中的SSL（安全套接字層）/TLS(傳輸層安全)證書信任問題。

必要條件

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

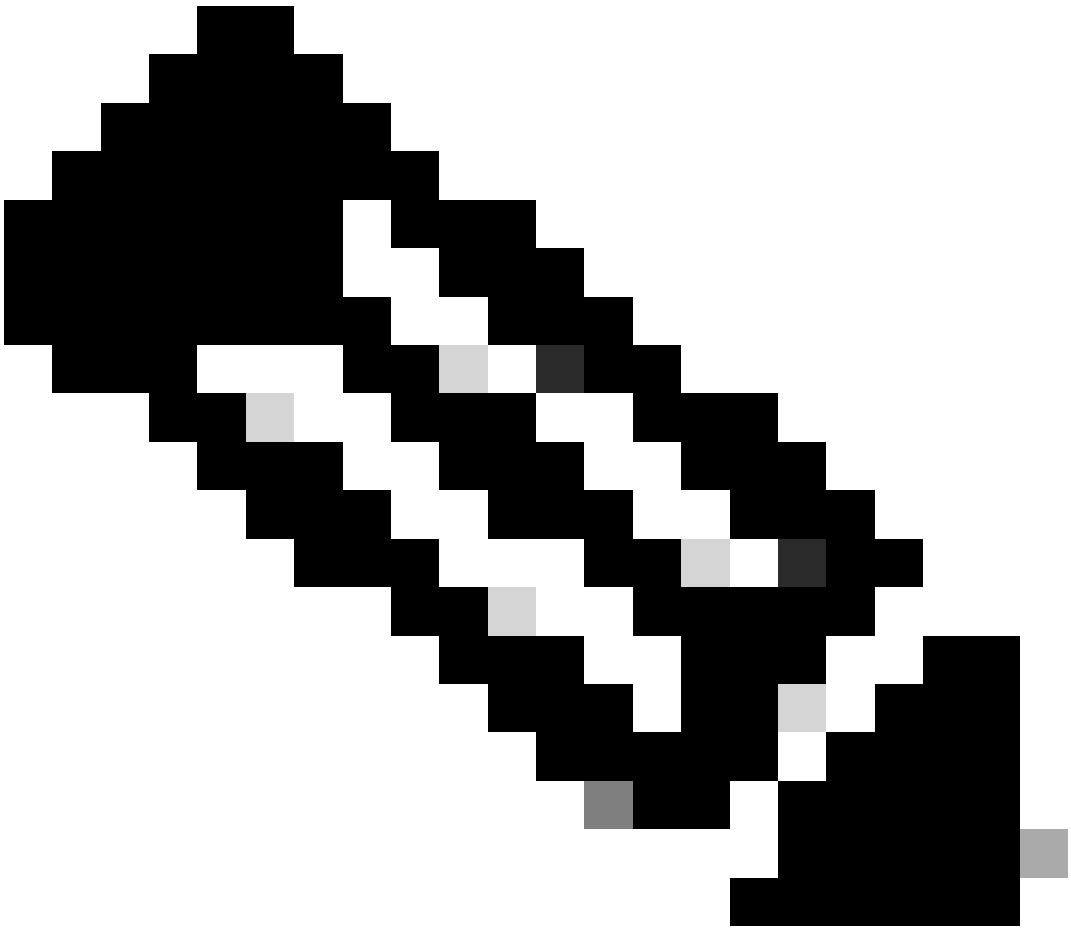
本文檔介紹在最近從DigiCert全域性根CA遷移到DigiCert全域性根G2後，如何解決AppDynamics代理中的SSL（安全套接字層）/TLS（傳輸層安全）證書信任問題。

它提供了詳細的步驟來確保正確配置和恢復無縫連線。

2023年，DigiCert啟動向DigiCert全域性根G2簽名證書的過渡，用於發行公共TLS/SSL證書。這一變化是由Mozilla更新的信任策略引發的，該策略要求根證書每15年更新一次，並且從2025年開始不信任舊證書。

新的簽名證書採用更安全的SHA-256演算法，取代了舊的SHA-1標準。作為此過渡的一部分，AppDynamics更新了域.saas.appdynamics.com的SSL證書，以便在2025-06-10上使用第二代證書。

此更新導致某些應用程式代理由於無法識別新證書而失去與SaaS控制器的連線。為了確保不間斷連線，更新AppDynamics代理信任儲存以包括新的DigiCert全域性根G2和IdenTrust證書至關重要。



附註：此更改主要影響使用自定義truststore或使用非常舊版本的OS/Java(預設的OS/Java信任庫中沒有所需的證書)的代理。

問題

AppDynamics代理和控制器之間存在連線問題，日誌顯示與SSL配置或通訊相關的錯誤。

日誌中的錯誤消息示例："PKIX路徑生成失敗：xxxx:無法找到所請求目標的有效證書路徑嘗試驗證"

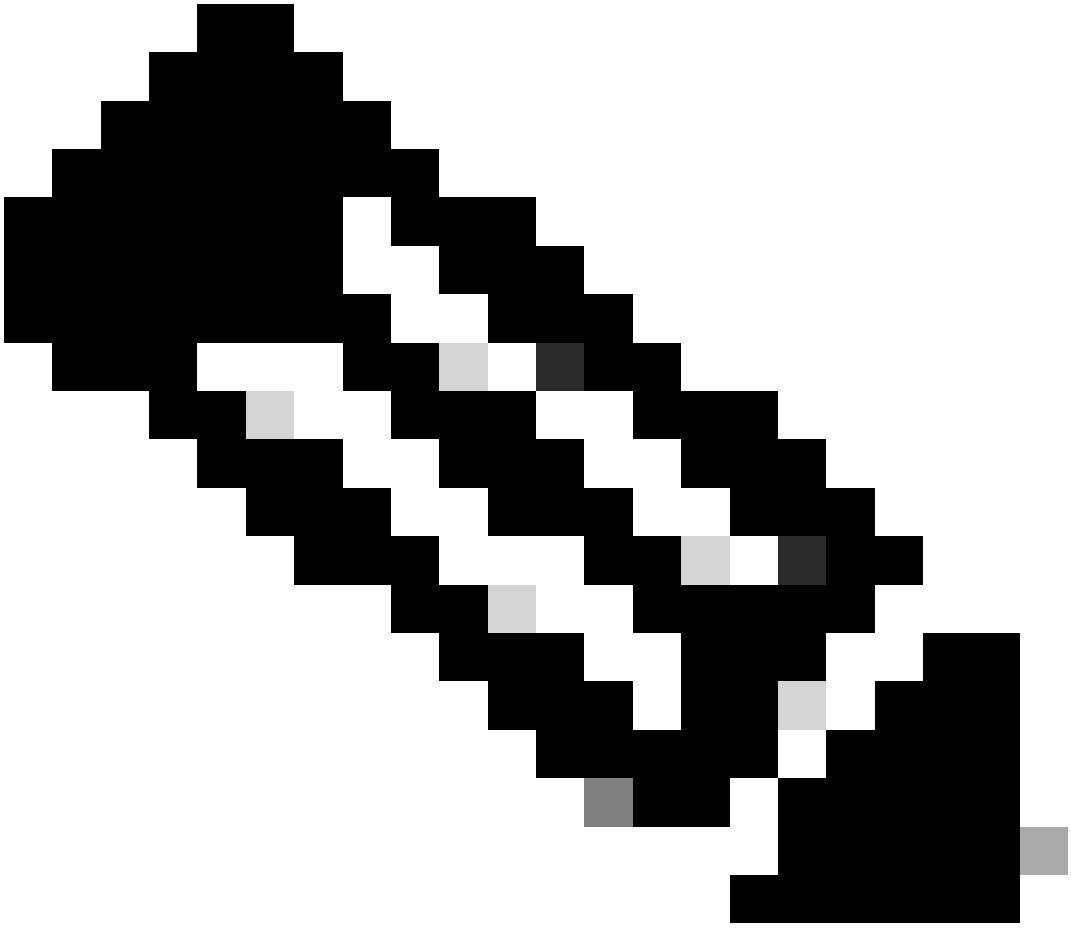
解決方案

步驟1.下載憑證

- DigiCert全域性根G2:
  - 訪問DigiCert受信任的根頒發機構證書
  - 搜尋「DigiCert Global Root G2」並下載證書。

- IdenTrust:
  - 轉到IdenTrust商業根CA 1
  - 複製證書內容並將其另存為檔案（例如Identtrustcommercial.cer或Identtrustcommercial.pem）

步驟2.確定Truststore位置

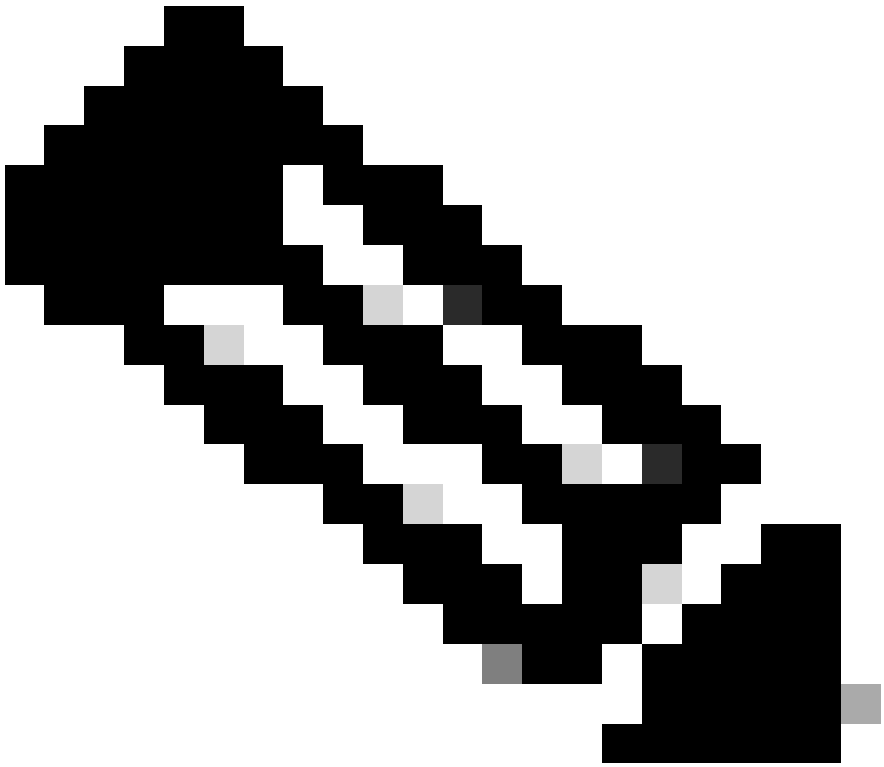


附註：步驟3中需要Truststore位置。將證書匯入Truststore

- Java、資料庫或機器代理
  - JVM引數Truststore屬性
    1. 啟動代理時，檢查是否將-Djavax.net.ssl.trustStore屬性設定為JVM引數。
    2. 如果設定了此屬性，請檢查此屬性指定的金鑰庫檔案，以確認它包含兩個證書（DigiCert全域性根G2和IdenTrust根證書）。
       （如果未設定屬性，請繼續執行下一步。）
  - 控制器資訊XML
    1. 可以將代理配置為使用在agent conf目錄的controller-info.xml檔案中定義的金鑰庫。
    2. 檢查controller-keystore-filename設定。

3. 如果存在，檢查指定的keystore檔案以確認包含兩個證書。
   （如果未找到，請繼續執行下一步。）

- 代理快取.jks檔案
  1. 在代理安裝目錄的容器中檢查名為cacerts.jkssers的檔案。
  2. 檢查此檔案以驗證是否包含兩個證書。
     （如果未找到，請繼續執行下一步。）

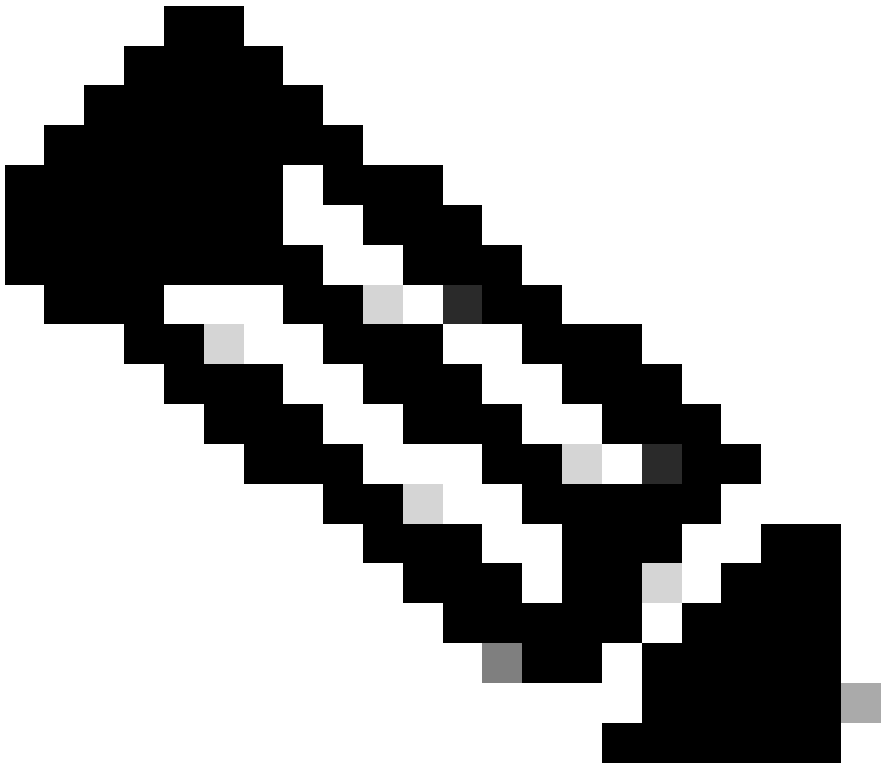


附註：代理安裝目錄

對於Java代理：AGENT_HOME/verxxx/conf或AGENT_HOME/conf

對於電腦或DB代理：AGENT_HOME/conf

- JRE預設信任庫
  1. 如果找不到任何以前的配置，則代理會使用JRE預設信任庫(通常位於JRE_HOME/lib/security/cacerts)作為回退。
  2. 檢查此檔案以確保包含證書。



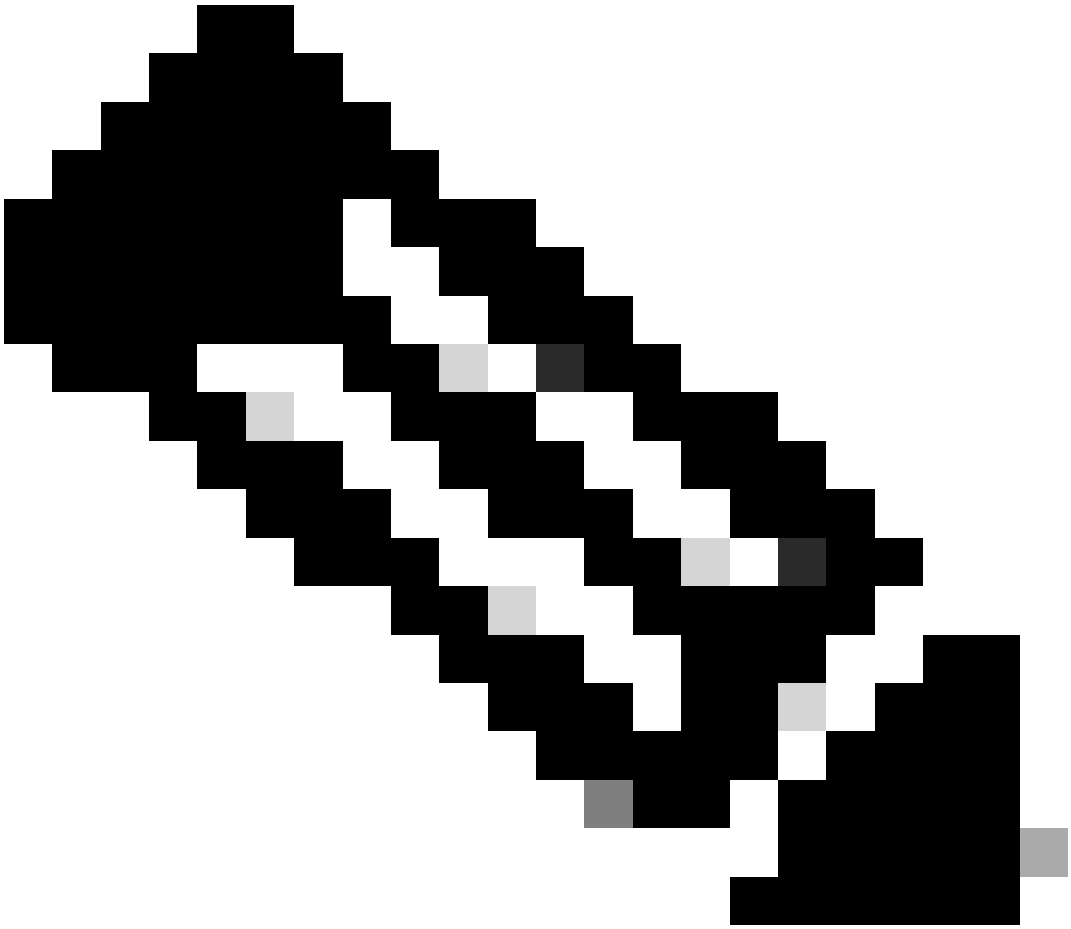
附註：如果您使用的是IBM Websphere或IBM Websphere Liberty Profile，則JRE_HOME分別位於AppServer或Liberty Directory中的Websphere安裝目錄下，即 IBM_WEBSPHERE_HOME/AppServer/java/或 IBM_WEBSPHERE_HOME/Liberty/java/

- 分析代理
  - 檢查如果代理信任庫的路徑（包括名稱）是使用代理配置檔案analytics-agent.properties中的<ad.controller.https.trustStorePath>元素指定的，則代理將載入該信任庫。
  - 如果未在thead.controller.https.trustStorePath中指定，則它會載入正在檢測的JVM的預設Java信任儲存，<JRE_HOME>/lib/security/cacerts(預設密碼changeit)
  - 如果未在ad.controller.https.trustStorePath和分析代理中指定，則它將載入電腦代理使用的信任儲存。
- DotNet代理
  - 對於Windows:
    - 導航到證書安裝檢視，方法是從工具欄轉到Run> MMC.exe> 選擇File，然後選擇Add/Remove Snap-in。

- 新增或刪除管理單元窗口開啟，選擇證書>單擊Add。證書管理單元視窗開啟。依次選擇Computer Account> Choose Local or Other Computer（選擇本地電腦或其他電腦）>ClickFinish>OK。
- 展開Certificates(Local Computer)>選擇Trusted Root Certification Authority資料夾，然後展開以顯示Certificates資料夾。
- 按兩下Certificates資料夾，注意現有受信任證書的清單。確定DigiCert全局根G2和IdenTrust根證書是否存在，否則匯入缺少的證書。

- 對於Linux:

  - 信任儲存區的位置在Linux發行版之間有所不同。常見位置包括:/etc/ssl/certs（作業系統如CentOS/RHEL/Debian）



附註：如果所有這些檢查位置都缺少DigiCert全域性根G2或IdenTrust證書，則需要新增它們。請參閱「步驟3.將證書匯入信任庫」中提到的步驟，將證書匯入信任庫。

步驟3.將證書匯入信任庫

- Java、資料庫、電腦或分析代理
  - 開啟終端或命令提示符，然後使用此keytool命令導入DigiCert全域性根G2和IdenTrust根證書。

```
keytool -import -trustcacerts -alias

            -file

             -keystore

              -storepass
```

替換:

- :唯一別名(例如，digicertglobalrootg2, identrustcoomercial)。
- :憑證檔案的路徑(例如/home/username/Downloads/DigiCertGlobalRootG2.crt)。
- :代理信任庫檔案的路徑(例如/opt/appdynamics/agent/ver25.x.x.x/conf/cacerts.jks)。
- :Truststore密碼(預設值：changeit, 除非自定義)。

  - 匯入DigiCert全局根G2證書的示例。

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

  - 匯入IdenTrust商業根證書的示例。

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

- DotNet代理
    - 對於Windows:
        - 導航到證書安裝檢視，方法是從工具欄轉到Run> MMC.exe> 選擇File，然後選擇Add/Remove Snap-in。
        - 新增或刪除管理單元窗口開啟，選擇證書>單擊Add。證書管理單元視窗開啟。依次選擇Computer Account> Choose Local or Other Computer（選擇本地電腦或其他電腦）>ClickFinish>OK。
        - 展開Certificates(Local Computer)>選擇Trusted Root Certification Authority資料夾，然後展開以顯示Certificates資料夾。
        - 按一下右鍵Certificatesfolder並選擇All Tasks > Import.Certificate Import Wizard將開啟，瀏覽說明並新增缺失的DigiCert全域性根G2證書和/或IdenTrust根證書。
    - 對於Linux:
        - 將下載的DigiCert Global Root G2 & IdenTrust Root Certificate檔案複製到標識的信任儲存目錄中。
        - 通過運行該命令更新信任庫。

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

步驟4.驗證匯入

- Java、資料庫、電腦或分析代理
    - 要驗證證書是否已成功新增，請運行命令：

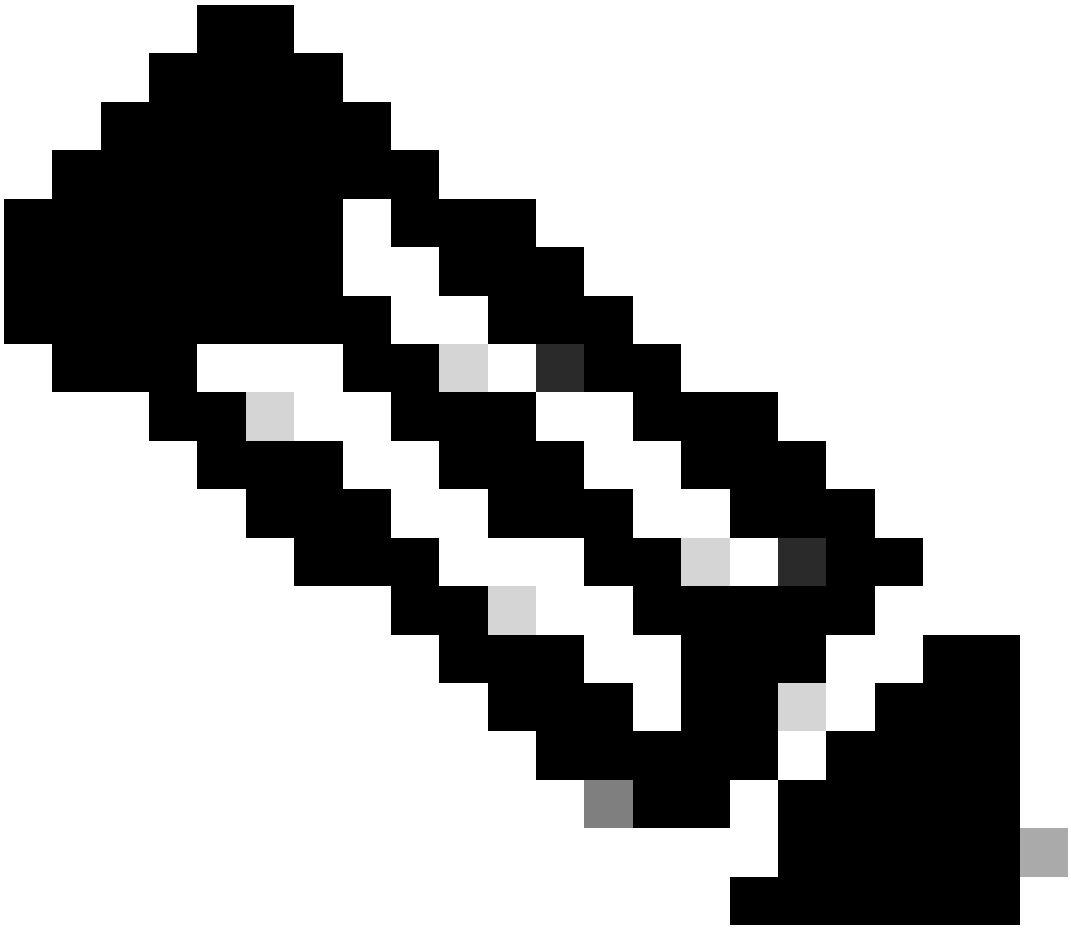
```
keytool -list -v -keystore

        -storepass

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

替換:

- <agent_truststore_path>:代理信任庫檔案的路徑。
- <truststore_password>:信任庫密碼。



附註：確保DigiCert Global Root G2和IdenTrust Commercial Root CA 1都顯示在輸出中。

- DotNet代理
  - 對於Windows:
    - 導航到證書安裝檢視，方法是從工具欄轉到Run> MMC.exe> 選擇File，然後選擇Add/Remove Snap-in。
    - 新增或刪除管理單元窗口開啟，選擇證書>單擊Add。證書管理單元視窗開啟。依次選擇Computer Account> Choose Local or Other Computer（選擇本地電腦或其他電腦）>ClickFinish>OK。
    - 展開Certificates(Local Computer)>選擇Trusted Root Certification Authority資料夾，然後展開以顯示Certificates資料夾。
    - 按兩下Certificates資料夾，您必須看到DigiCert Global Root G2和IdenTrust根證書

。

- 對於Linux:
  - 運行該命令並檢查DigiCert 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
```

步驟5.重新啟動代理

最後，重新啟動AppDynamics代理。這樣更改才會生效。

相關資訊

支援諮詢：將DigiCert和IdenTrust根SSL證書新增到代理信任儲存

需要進一步協助？

如果您遇到問題或遇到問題，請建立包含以下詳細資訊的asupport票證：

- 來自代理的日誌。
- Truststore位置和新增證書的詳細資訊。
- 遇到任何錯誤消息。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。