在DigiCert根G2更新后解决AppDynamics SSL/TLS问题

目录

简介

本文档介绍如何解决AppDynamics代理中的SSL（安全套接字层）/TLS(传输层安全)证书信任问题。

先决条件

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

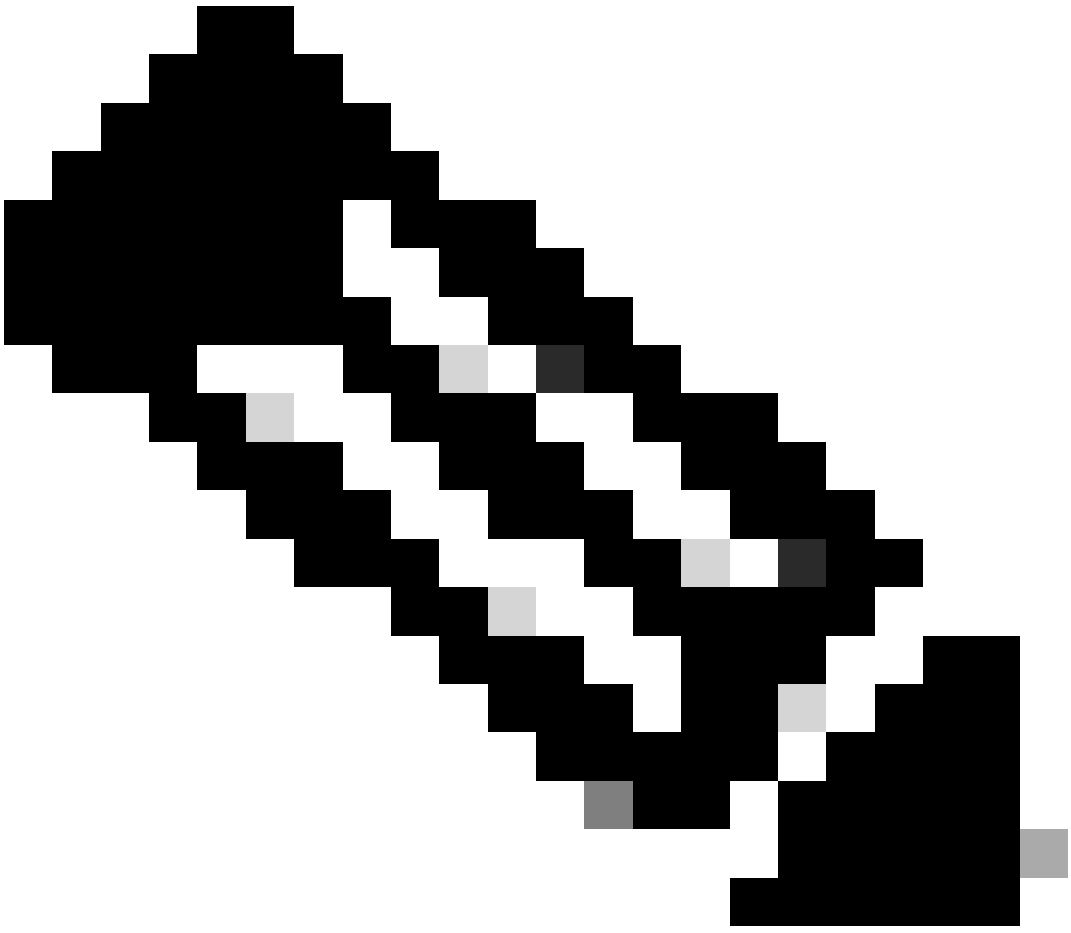
本文档介绍如何解决最近从DigiCert全局根CA迁移到DigiCert全局根G2后AppDynamics代理中的SSL（安全套接字层）/TLS（传输层安全）证书信任问题。

它提供了详细的步骤，以确保正确配置和恢复无缝连接。

2023年，DigiCert发起向DigiCert全局根G2签名证书的过渡，用于颁发公共TLS/SSL证书。此更改是由Mozilla更新的信任策略引发的，该策略要求根证书每15年更新一次，并且从2025年开始不信任旧证书。

新的签名证书采用更安全的SHA-256算法，取代了旧的SHA-1标准。作为此过渡的一部分，AppDynamics更新了其.saas.appdynamics.com域的SSL证书，以便在2025-06-10上使用第二代证书。

此更新导致某些应用代理无法识别新证书，从而失去与SaaS控制器的连接。为了确保不间断连接，更新AppDynamics代理信任库以包含新的DigiCert全局根G2和IdenTrust证书至关重要。



> 注意：此更改主要影响使用自定义信任库或使用非常旧版本的OS/Java的代理，其中默认的OS/Java信任库中不包含所需的证书。

问题

AppDynamics代理和控制器之间存在连接问题，日志显示与SSL配置或通信相关的错误。

日志中的错误消息示例："PKIX路径生成失败：xxxx:无法找到尝试验证所请求目标的有效证书路径”

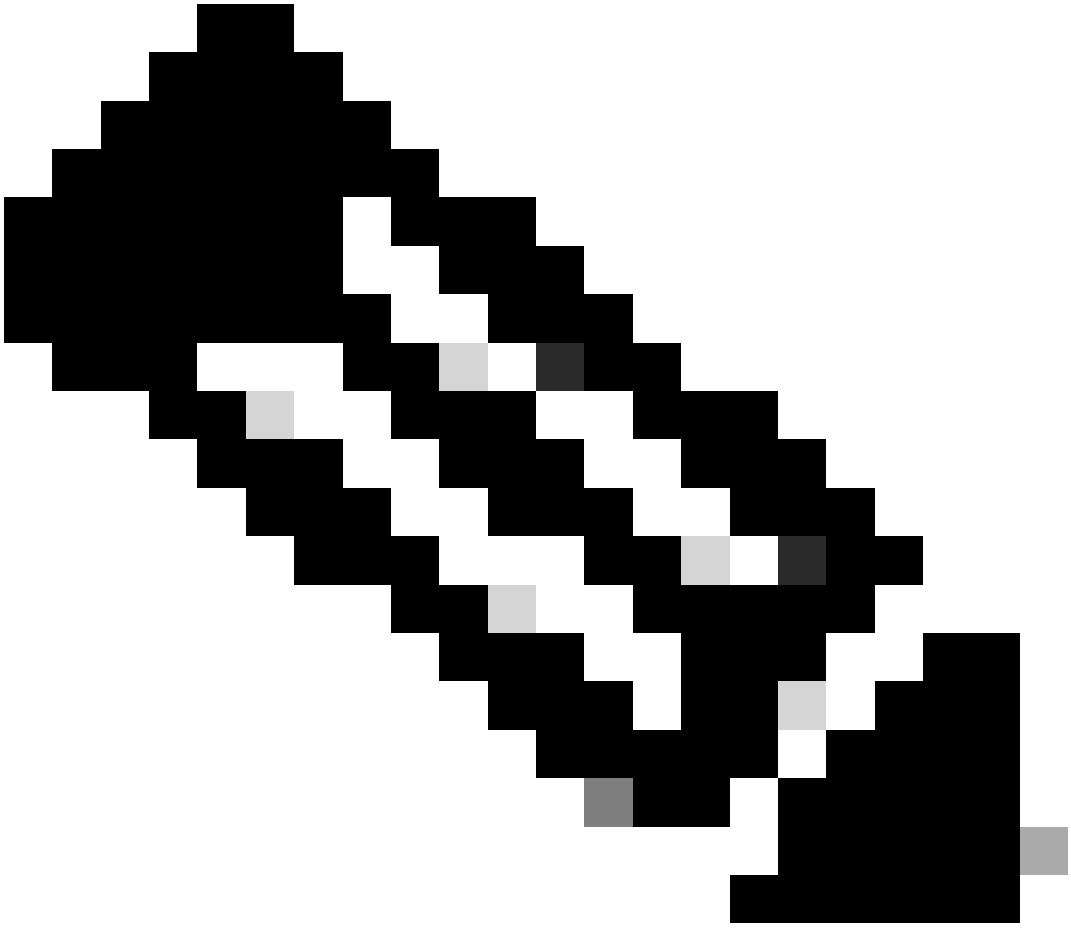
解决方案

步骤1.下载证书

- DigiCert全局根G2:
  - 访问DigiCert Trusted Root Authority证书
  - 搜索“DigiCert Global Root G2”并下载证书。

- IdenTrust:
  - 转至IdenTrust Commercial Root CA 1
  - 复制证书内容并将其另存为文件（例如，Identtrustcommercial.cer或Identtrustcommercial.pem）

步骤2.确定Truststore位置

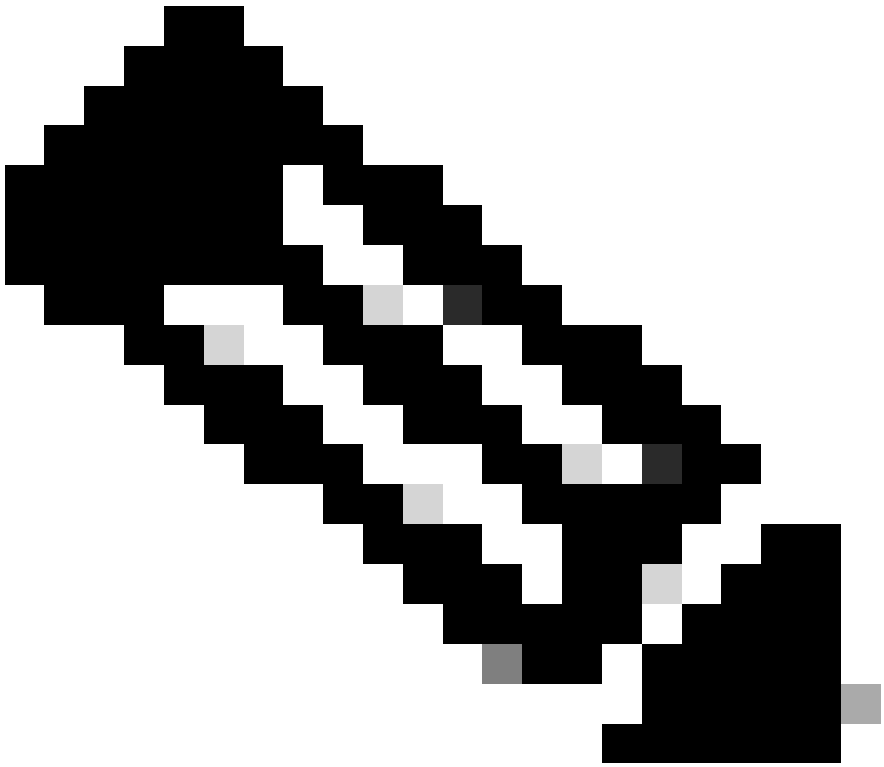


注意：步骤3中需要Truststore位置。将证书导入到Truststore

- Java、数据库或机器代理
  - JVM参数Truststore属性
    1. 启动代理时，检查是否将-Djavax.net.ssl.trustStore属性设置为JVM参数。
    2. 如果设置了此属性，请检查此属性指定的密钥库文件以确认它包含两个证书（DigiCert全局根G2和IdenTrust根证书）。
       （如果未设置属性，请继续执行下一步。）
  - 控制器信息XML
    1. 可以将代理配置为使用在agent conf目录的controller-info.xml文件中定义的密钥库。
    2. 检查控制器密钥库文件名设置。

3. 如果存在，检查指定的密钥库文件以确认包含两个证书。
   （如果未找到，请继续执行下一步。）

- 代理cacerts.jks文件
  1. 在代理安装目录的容器中检查名为cacerts.jkssers的文件。
  2. 检查此文件以验证是否包含两个证书。
     （如果未找到，请继续执行下一步。）

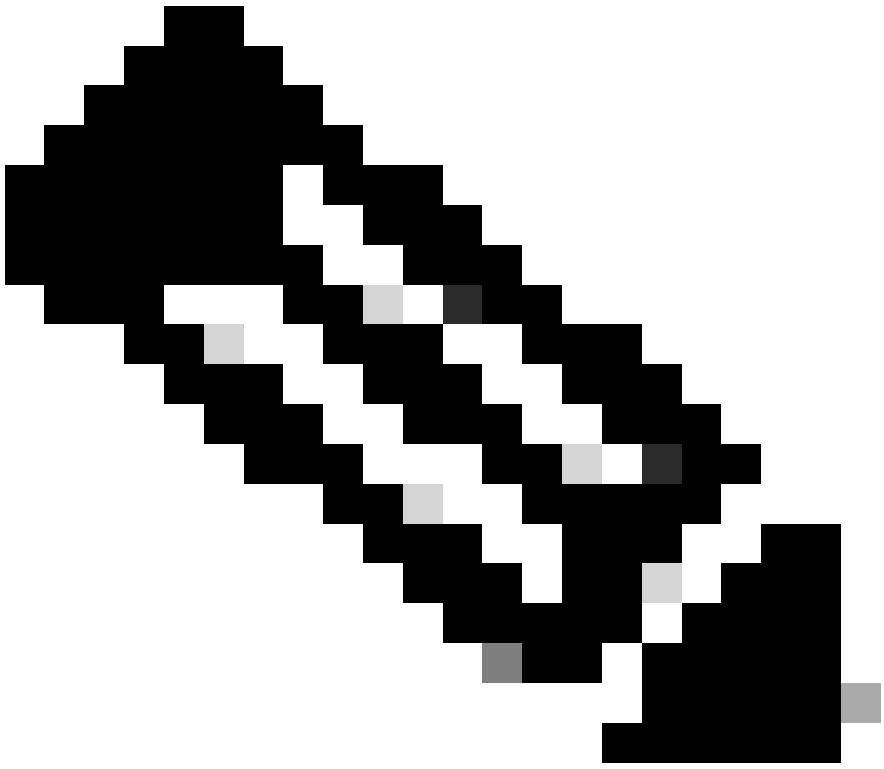


注意：代理安装目录

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

对于计算机或数据库代理：AGENT_HOME/conf

- JRE默认信任库
  1. 如果找不到任何以前的配置，则代理会使用JRE默认信任库(通常位于JRE_HOME/lib/security/cacerts)，作为回退。
  2. 检查此文件以确保包含证书。

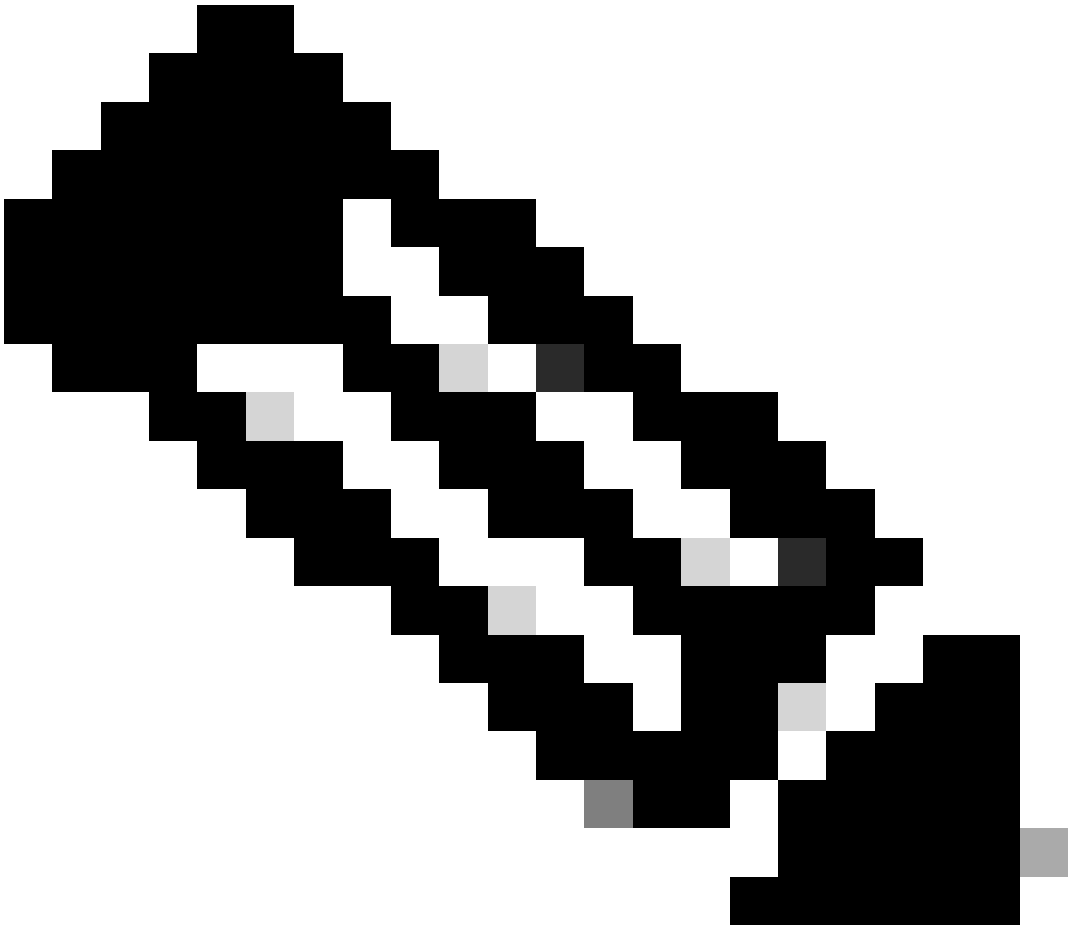


注意：如果使用IBM Websphere或IBM Websphere Liberty Profile，则JRE_HOME分别位于AppServer或Liberty Directory中的Websphere安装目录下，即IBM_WEBSPHERE_HOME/AppServer/java/或IBM_WEBSPHERE_HOME/Liberty/java/

- 分析代理
    - 选中If the path(including name)of the agent truststore is specified using the <ad.controller.https.trustStorePath>元素(在代理配置文件analytics-agent.properties中)，则代理加载该trustore。
    - 如果未在head.controller.https.trustStorePath中指定，它将加载正在检测的JVM的默认Java信任库，<JRE_HOME>/lib/security/cacerts(默认密码changeit)
    - 如果未在ad.controller.https.trustStorePath和分析代理用作计算机代理扩展，则它会加载计算机代理使用的信任库。
- DotNet代理
    - Windows：
        - 通过从工具栏转到运行> MMC.exe> selectFilefrom并选择添加/删除管理单元，导航到证书安装视图。
        - “添加或删除管理单元”(Add or Remove Snap-inwindow)将打开，选择“证书

”(Certificates)>“单击“添加”(Add)。证书管理单元窗口打开。依次选择Computer Account > Choose Local or Another Computer >ClickFinish>OK。
- 展开Certificates(Local Computer)>选择Trusted Root Certification Authority文件夹，然后展开以显示Certificates文件夹。
- 双击Certificates文件夹，注意现有受信任证书的列表。确定DigiCert全局根G2和IdenTrust根证书是否都存在，否则导入缺失的证书。

- 对于Linux:
  - 信任存储区的位置因Linux发行版而异。常见位置包括:/etc/ssl/certs(操作系统类似于CentOS/RHEL/Debian)



注意：如果所有这些检查位置中缺少DigiCert全局根G2或IdenTrust证书，则需要添加这些证书。请参阅步骤3.将证书导入信任库(Import Certificates to the Truststore)中提到的步骤，将证书导入信任库。

步骤3.将证书导入信任库

- Java、数据库、计算机或分析代理
  - 打开您的终端或命令提示符，并使用此keytool命令导入DigiCert全局根G2和IdenTrust根证书。

```
keytool -import -trustcacerts -alias

            -file

             -keystore

              -storepass
```

替换:

- :唯一别名(例如，digicertglobalrootg2, identrustcoomercial)。
- :证书文件的路径(例如/home/username/Downloads/DigiCertGlobalRootG2.crt)。
- :代理信任库文件的路径(例如/opt/appdynamics/agent/ver25.x.x.x/conf/cacerts.jks)。
- :信任库密码(默认：changeit, 除非自定义)。

  - 导入DigiCert全局根G2证书的示例。

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

  - 导入IdenTrust商业根证书的示例。

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

- DotNet代理
    - Windows：
        - 通过从工具栏转到运行> MMC.exe> selectFilefrom并选择添加/删除管理单元，导航到证书安装视图。
        - “添加或删除管理单元”(Add or Remove Snap-inwindow)将打开，选择“证书”(Certificates)>“单击“添加”(Add)。证书管理单元窗口打开。依次选择Computer Account > Choose Local or Another Computer >ClickFinish>OK。
        - 展开Certificates(Local Computer)>选择Trusted Root Certification Authority文件夹，然后展开以显示Certificates文件夹。
        - 右键单击Certificates文件夹并选择All Tasks > Import.Certificate Import Wizard打开，浏览说明并添加缺失的DigiCert全局根G2证书和/或IdenTrust根证书。
    - 对于Linux:
        - 将下载的DigiCert Global Root G2 & IdenTrust Root Certificate文件复制到标识的信任存储目录中。
        - 通过运行命令更新信任库。

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

步骤4.检验导入

- Java、数据库、计算机或分析代理
    - 要验证证书是否已成功添加，请运行命令：

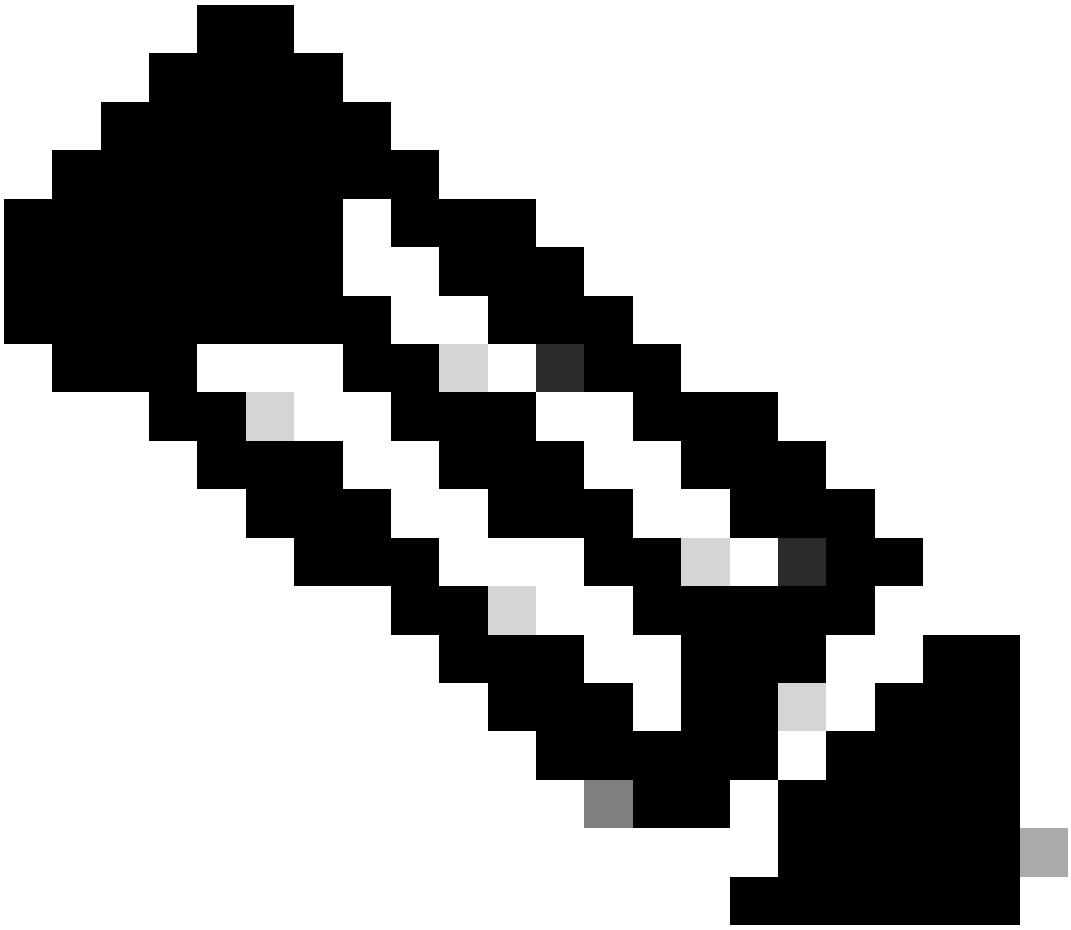
```
keytool -list -v -keystore

        -storepass

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

替换:

- <agent_truststore_path>:代理信任库文件的路径。
- <truststore_password>:信任库密码。



注意：确保DigiCert Global Root G2和IdenTrust Commercial Root CA 1都出现在输出中。

- DotNet代理
  - Windows：
    - 通过从工具栏转到运行> MMC.exe> selectFilefrom并选择添加/删除管理单元，导航到证书安装视图。
    - “添加或删除管理单元”(Add or Remove Snap-inwindow)将打开，选择“证书”(Certificates)>“单击“添加”(Add)。证书管理单元窗口打开。依次选择Computer Account > Choose Local or Another Computer >ClickFinish>OK。
    - 展开Certificates(Local Computer)>选择Trusted Root Certification Authority文件夹，然后展开以显示Certificates文件夹。
    - 双击Certificates文件夹，您必须看到DigiCert Global Root G2和IdenTrust根证书。

- 对于Linux:
  - 运行命令并检查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
```

步骤5.重新启动代理

最后，重新启动AppDynamics代理。这样更改才会生效。

相关信息

支持建议：将DigiCert和IdenTrust根SSL证书添加到代理信任库

需要进一步的帮助？

如果您遇到问题或遇到问题，请使用以下详细信息创建asupport票证：

- 来自代理的日志。
- 信任库位置和所添加证书的详细信息。
- 遇到任何错误消息。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。