

AppDynamics SSL/TLS problemen oplossen na DigiCert Root G2 update

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Gebruikte onderdelen](#)

[Achtergrondinformatie](#)

[Probleem](#)

[Oplossing](#)

[Stap 1. Certificaten downloaden](#)

[Stap 2. Locatie van Truststore identificeren](#)

[Java Database of Machine Agent](#)

[Analytics-agent](#)

[DotNet Agent](#)

[Stap 3. Certificaten importeren in de Truststore](#)

[Java-, database-, machine- of analyseagent](#)

[DotNet Agent](#)

[Stap 4. Controleer de import](#)

[Java-, database-, machine- of analyseagent](#)

[DotNet Agent](#)

[Stap 5. De Agent opnieuw starten](#)

[Gerelateerde informatie](#)

[Meer hulp nodig?](#)

Inleiding

In dit document wordt beschreven hoe u vertrouwenskwesaties met SSL-certificaten (Secure Socket Layer)/ TLS-certificaten (Transport Layer Security) in AppDynamics Agents kunt oplossen.

Voorwaarden

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

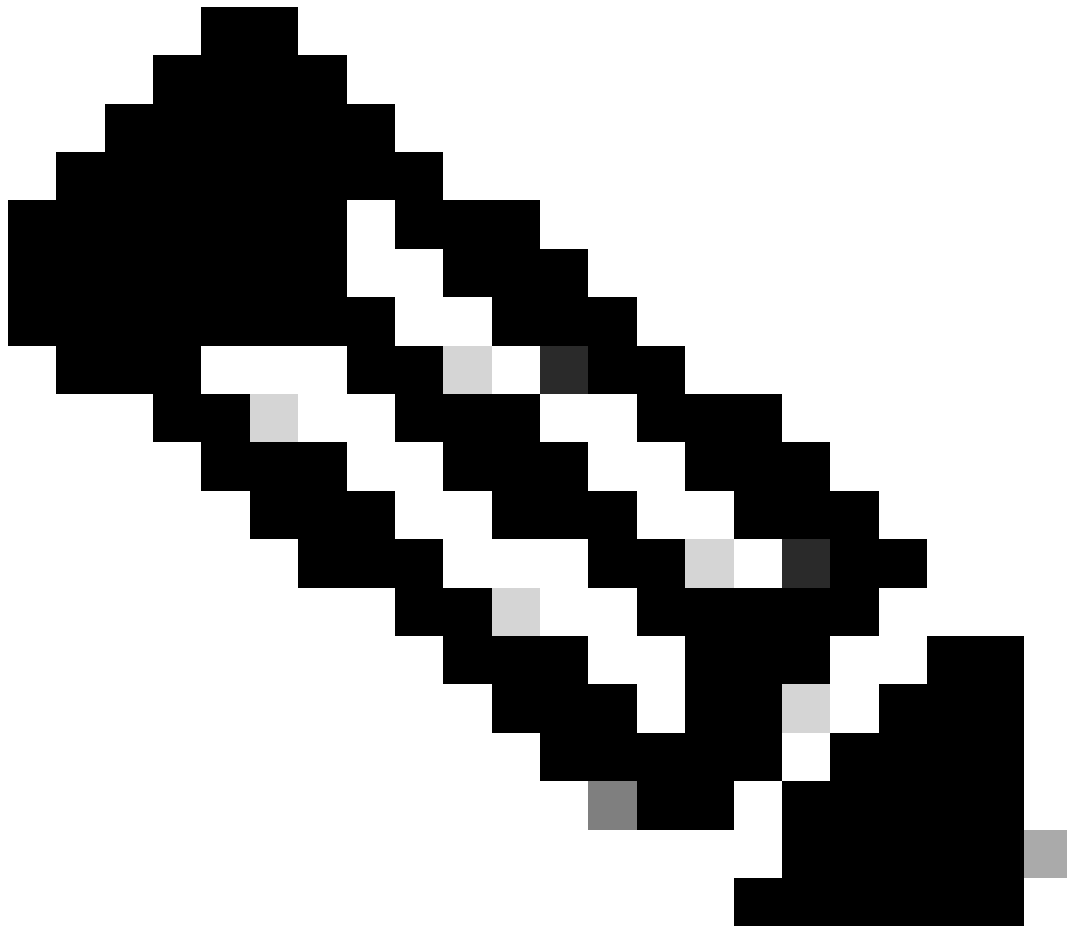
In dit document wordt beschreven hoe problemen met het SSL-certificaat (Secure Socket Layer)/ TLS-certificaat (Transport Layer Security) in AppDynamics Agents kunnen worden opgelost na de recente migratie van DigiCert Global Root CA naar DigiCert Global Root G2.

Het biedt gedetailleerde stappen voor een goede configuratie en herstel van naadloze connectiviteit.

In 2023 startte DigiCert de overgang naar het DigiCert Global Root G2-ondertekeningscertificaat voor het uitgeven van publieke TLS/SSL-certificaten. Deze verandering werd ingegeven door het bijgewerkte vertrouwensbeleid van Mozilla, dat vereist dat rootcertificaten elke 15 jaar worden bijgewerkt en oudere certificaten vanaf 2025 wantrouwt.

Het nieuwe ondertekeningscertificaat maakt gebruik van het veiligere SHA-256-algoritme en vervangt de oudere SHA-1-standaard. Als onderdeel van deze overgang heeft AppDynamics zijn SSL-certificaten voor domein `.saas.appdynamics.com` bijgewerkt om de tweede generatie certificaten te gebruiken op 2025-06-10.

Deze update zorgde ervoor dat sommige applicatieagents de connectiviteit met SaaS-controllers verloren vanwege hun onvermogen om het nieuwe certificaat te herkennen. Om ononderbroken connectiviteit te garanderen, is het van cruciaal belang om de AppDynamics agent trust store bij te werken met de nieuwe DigiCert Global Root G2- en IdenTrust-certificaten.



Opmerking: Deze wijziging is voornamelijk van invloed op agenten die de aangepaste truststore gebruiken of een zeer oude versie van OS / java gebruiken waarbij het vereiste certificaat niet is opgenomen in de standaard OS / Java truststore.

Probleem

Er is een connectiviteitsprobleem tussen de AppDynamics Agents en de Controller en de logs tonen fouten met betrekking tot SSL-configuratie of communicatie.

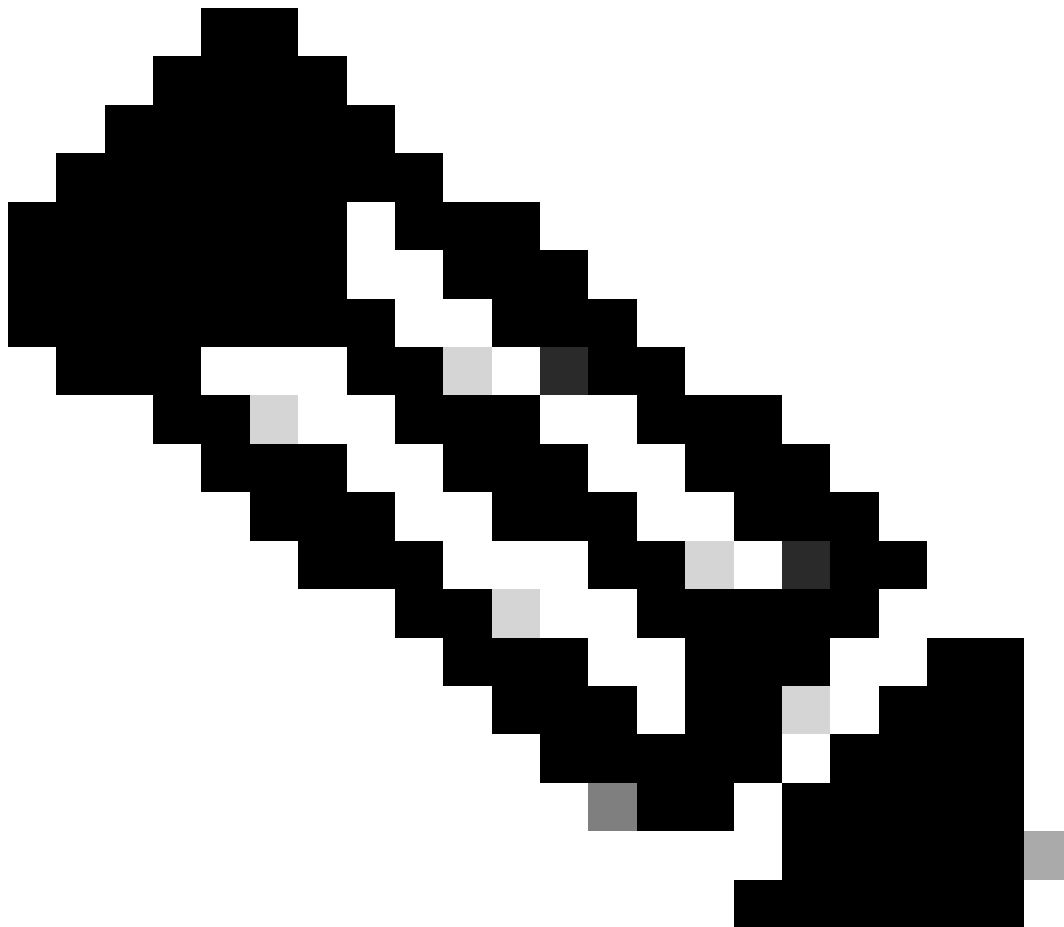
Voorbeeld foutbericht in de logs: "PKIX path building failed: xxxx: cannot to find valid certification path to requested target trying validation" (PKIX-pad bouwen mislukt: xxxx: geldig certificeringspad naar aangevraagd doel niet gevonden)

Oplossing

Stap 1. Certificaten downloaden

- DigiCert Global Root G2:
 - Bezoek [DigiCert Trusted Root Authority-certificaten](#)
 - Zoek naar "DigiCert Global Root G2" en download het certificaat.
- IdenTrust:
 - Ga naar [IdenTrust Commercial Root CA 1](#)
 - Kopieer de inhoud van het certificaat en sla deze op als een bestand (bijvoorbeeld Identrustcommercial.cer of Identrustcommercial.pem)

Stap 2. Locatie van Truststore identificeren



Opmerking: de locatie van de Truststore is vereist in stap 3. Certificaten importeren in de Truststore

- Java, Database of Machine Agent
 - JVM-argument Truststore, eigenschap

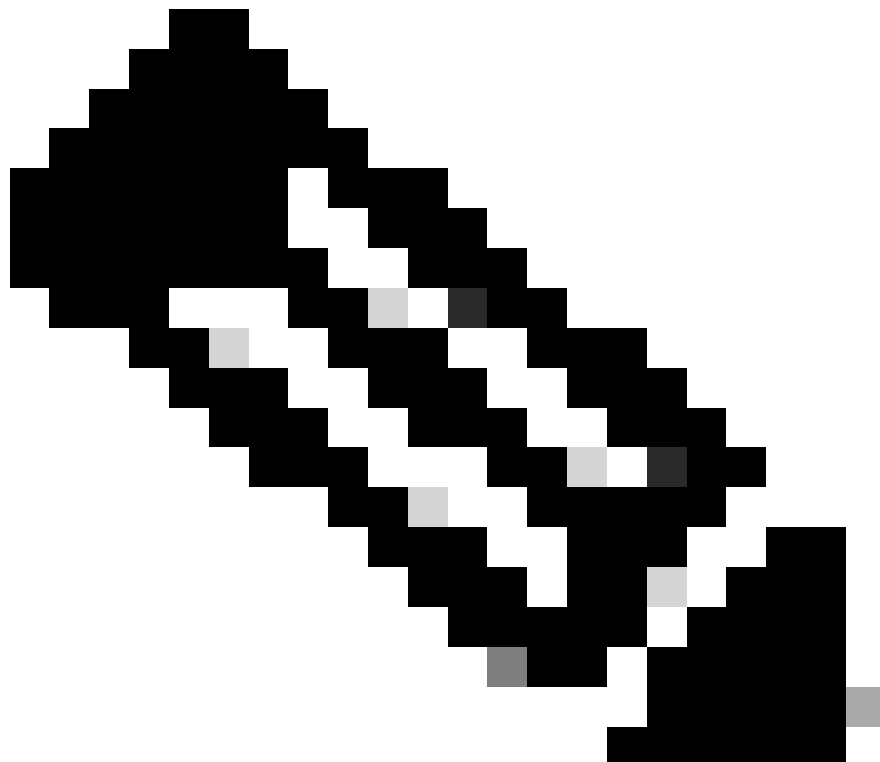
1. Controleer of de eigenschap -Djavax.net.ssl.trustStore is ingesteld als JVM-argumenten wanneer u de agent start.
2. Als deze eigenschap is ingesteld, inspecteert u het keystore-bestand dat door deze eigenschap is opgegeven om te bevestigen dat het beide certificaten bevat (DigiCert Global Root G2- en IdenTrust-rootcertificaten).
(Als de eigenschap niet is ingesteld, gaat u verder met de volgende stap.)

- Controller Info XML

1. De Agent kan worden geconfigureerd voor het gebruik van keystore gedefinieerd in het bestand controller-info.xml in uw agent conf-directory.
2. Controleer of de bestandsnaam controller-keystore-is ingesteld.
3. Indien aanwezig, inspecteert u het opgegeven keystore-bestand om te bevestigen dat beide certificaten zijn opgenomen.
(Als dit niet het geval is, gaat u verder met de volgende stap.)

- Agent cacerts.jks Bestand

1. Controleer of er een bestand met de naam cacerts.jks in de configuratiemap van de installatiemap van de agent aanwezig is.
 2. Inspecteer dit bestand om te controleren of beide certificaten zijn opgenomen.
(Als dit niet het geval is, gaat u verder met de volgende stap.)
-



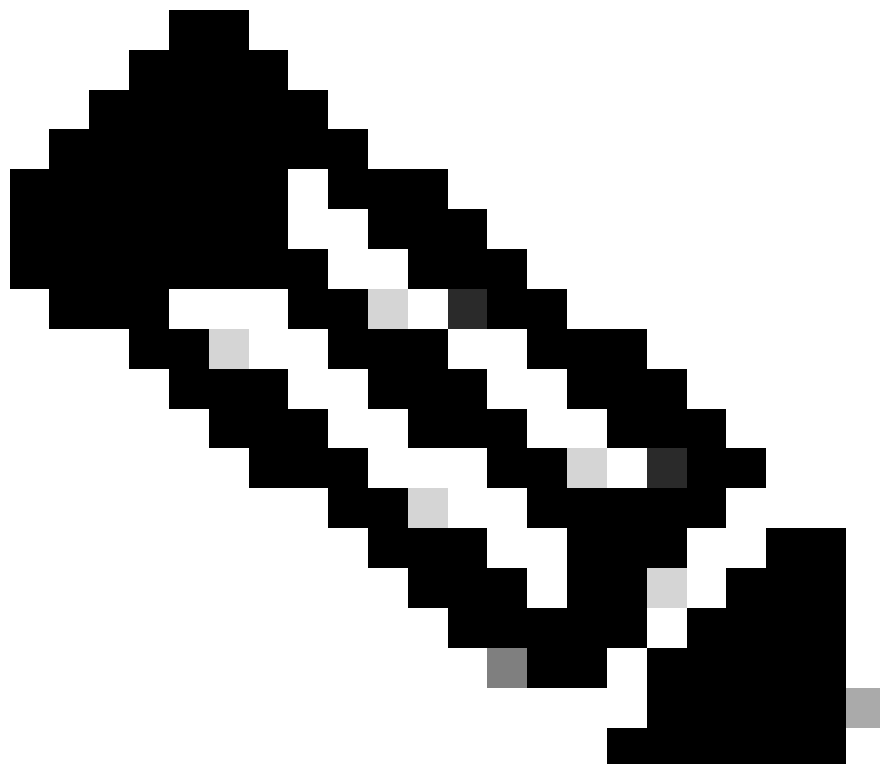
Opmerking: installatiemap van agent

Voor Java Agent: AGENT_HOME/verxxx/conf of AGENT_HOME/conf

Voor Machine of DB Agent: AGENT_HOME/conf

- JRE Default Truststore

1. Als geen van de vorige configuraties wordt gevonden, gebruikt de agent de standaard JRE-truststore, meestal op JRE_HOME/lib/security/cacerts.
 2. Inspecteer dit bestand om er zeker van te zijn dat de certificaten zijn opgenomen.
-



Opmerking: Als u IBM Websphere of IBM Websphere Liberty Profile gebruikt, bevindt de JRE_HOME zich respectievelijk in AppServer of Liberty Directory onder Websphere-installatiedirectory, dat wil zeggen IBM_WEBSPHERE_HOME/AppServer/java/ of IBM_WEBSPHERE_HOME/Liberty/java/

- Analytics-agent

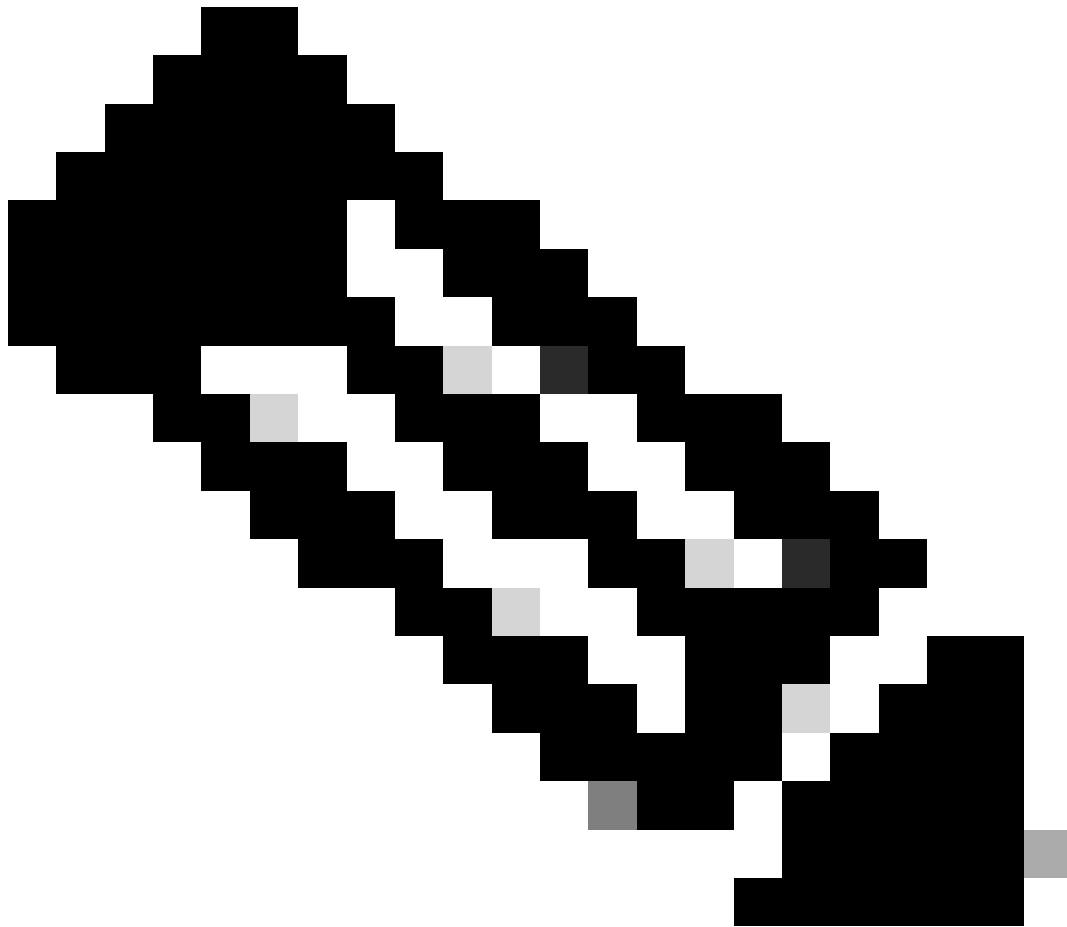
- Controleer of het pad (inclusief de naam) van de agent truststore is opgegeven met behulp van het element `<ad.controller.https.trustStorePath>` in het

configuratiebestand van de agent [analytics-agent.properties](#), en of de agent die truststore vervolgens laadt.

- Indien niet gespecificeerd in `thead.controller.https.trustStorePath`, laadt het de standaard Java truststore van de JVM die wordt geïnstrumenteerd, `<JRE_HOME>/lib/security/cacerts` (standaard wachtwoord wijzigen)
- Als niet gespecificeerd in de `ad.controller.https.trustStorePath` en analytics agent wordt gebruikt als een Machine agent extensie dan laadt de truststore gebruikt door machine agent.

- DotNet Agent

- Voor Windows:
 - Navigeer naar de installatieweergave van het certificaat door naar Run> MMC.exe> File op de werkbalk te selecteren en Snap-in toevoegen/verwijderen te selecteren.
 - Snap-in toevoegen of verwijderen wordt geopend. Selecteer Certificaten> ClickAdd. Het venster Certificaat wordt geopend. Selecteer Computeraccount> Kies Lokaal of een andere computer >Klik op Voltooien>OK.
 - Certificaten uitvouwen (Lokale computer) > Selecteer de map Trusted Root Certification Authority en vouw uit om de map Certificaten weer te geven.
 - Dubbelklik op de map Certificaten en zie de lijst met bestaande vertrouwde certificaten. Identificeer of zowel de DigiCert Global Root G2- als de IdenTrust-basiscertificaten aanwezig zijn, anders importeert u de ontbrekende certificaten.
- Voor Linux:
 - De locatie van de vertrouwenswinkel varieert tussen Linux-distributies. Veelgebruikte locaties zijn:/etc/ssl/certs (OS zoals CentOS/RHEL/Debian)



Opmerking: Als de DigiCert Global Root G2- of IdenTrust-certificaten ontbreken op al deze gecontroleerde locaties, moet u ze toevoegen. Raadpleeg de stappen die worden vermeld in "Stap 3. Certificaten importeren in de Truststore" om de certificaten te importeren in de Truststore.

Stap 3. Certificaten importeren in de Truststore

- Java-, database-, machine- of analyseagent
 - Open uw terminal- of opdrachtprompt en gebruik deze opdracht met het sleutelgereedschap om DigiCert Global Root G2 & IdenTrust Root Certificates te importeren.

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


-file

-keystore

-storepass

Vervangen:

- : Een unieke alias (bijvoorbeeld `digicertglobalrootg2`, `identrustcoomercial`).
- : Pad naar het certificaatbestand (bijvoorbeeld `/home/username/Downloads/DigiCertGlobalRootG2.crt`).
- : Pad naar het bestand agent truststore (bijvoorbeeld `/opt/appdynamics/agent/ver25.x.x.x/conf/cacerts.jks`).
- : Truststore-wachtwoord (standaard: `changeit`, tenzij aangepast).
- Voorbeeld voor het importeren van DigiCert Global Root G2 Certificate.

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

- Voorbeeld voor het importeren van IdenTrust Commercial Root Certificate.

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

- DotNet Agent

- Voor Windows:
 - Navigeer naar de installatieweergave van het certificaat door naar `Run> MMC.exe` te selecteren en Snap-in toevoegen/verwijderen te selecteren.

- Snap-in toevoegen of verwijderen wordt geopend. Selecteer Certificaten> ClickAdd. Het venster Certificaat wordt geopend. Selecteer Computeraccount> Kies Lokaal of een andere computer >Klik op Voltooien>OK.
- Certificaten uitvouwen (Lokale computer) > Selecteer de map Trusted Root Certification Authority en vouw uit om de map Certificaten weer te geven.
- Klik met de rechtermuisknop op de map Certificaten en selecteerAlle taken > Importeren.Wizard Certificaat importeren wordt geopend, ga door de instructies en voeg de ontbrekendeDigiCert Global Root G2 certificaat en/of IdenTrust Root certificaat.
- Voor Linux:
 - Kopieer de gedownloadde DigiCert Global Root G2 & IdenTrust Root Certificate-bestanden naar de geïdentificeerde map voor de vertrouwenswinkel.
 - Werk de Trust Store bij door de opdracht uit te voeren.

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

Stap 4. Controleer de import

- Java-, database-, machine- of analyseagent
 - Voer de volgende opdracht uit om te controleren of de certificaten zijn toegevoegd:

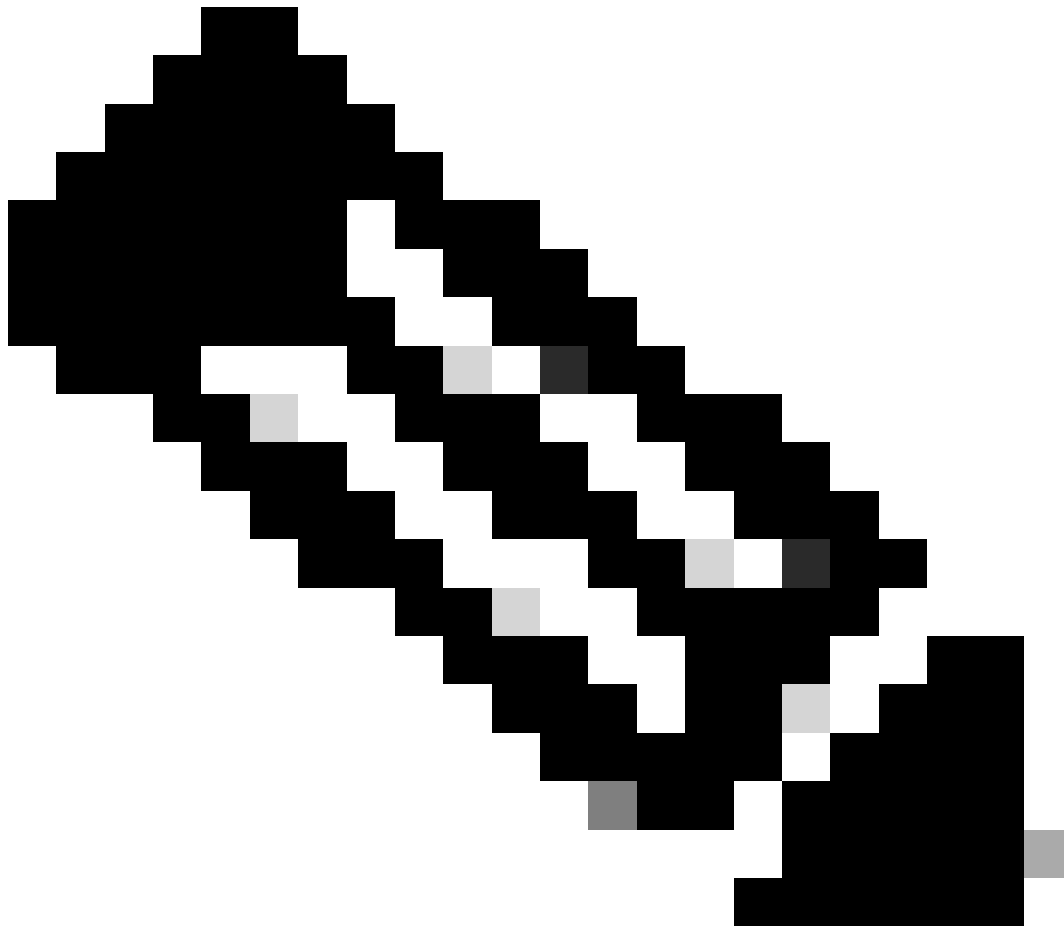
```
keytool -list -v -keystore
```

```
-storepass
```

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

Vervangen:

- <agent_truststore_path>: Pad naar het bestand agent truststore.
- <truststore_password>: Het truststore-wachtwoord.



Opmerking: Zorg ervoor dat zowel DigiCert Global Root G2 als IdenTrust Commercial Root CA 1 in de uitvoer worden weergegeven.

-
- DotNet Agent
 - Voor Windows:
 - Navigeer naar de installatieweergave van het certificaat door naar Run> MMC.exe> File op de werkbalk te selecteren en Snap-in toevoegen/verwijderen te selecteren.
 - Snap-in toevoegen of verwijderen wordt geopend. Selecteer Certificaten> ClickAdd. Het venster Certificaat wordt geopend. Selecteer Computeraccount> Kies Lokaal of een andere computer >Klik op Voltooien>OK.
 - Certificaten uitvouwen (Lokale computer) > Selecteer de map Trusted Root Certification Authority en vouw uit om de map Certificaten weer te geven.
 - Dubbelklik op de map Certificaten en u moet zowel de DigiCert Global Root G2- als IdenTrust-rootcertificaten zien.

- Voor Linux:
 - Voer de opdracht uit en controleer of DigiCert Global Root G2 & IdenTrust Root Certificate bestaat:

```
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
```

Stap 5. De Agent opnieuw starten

Start de AppDynamics-agent opnieuw op. Hierdoor kunnen de wijzigingen van kracht worden.

Gerelateerde informatie

[Ondersteuningsadvies: DigiCert- en IdenTrust Root SSL-certificaten toevoegen aan Agent Trust Stores](#)

Meer hulp nodig?

Als u een vraag hebt of problemen ondervindt, kunt u [een](#) supportticket maken met de volgende gegevens:

- Logboeken van de agent.
- Details van de truststore locatie en certificaten toegevoegd.
- Eventuele foutmeldingen aangetroffen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.