Beheben von AppDynamics SSL/TLS-Problemen nach dem DigiCert-Root G2-Update

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Probleme mit der SSL- (Secure Socket Layer)/TLS-Zertifikatssicherheit in AppDynamics Agents behoben werden.

Voraussetzungen

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

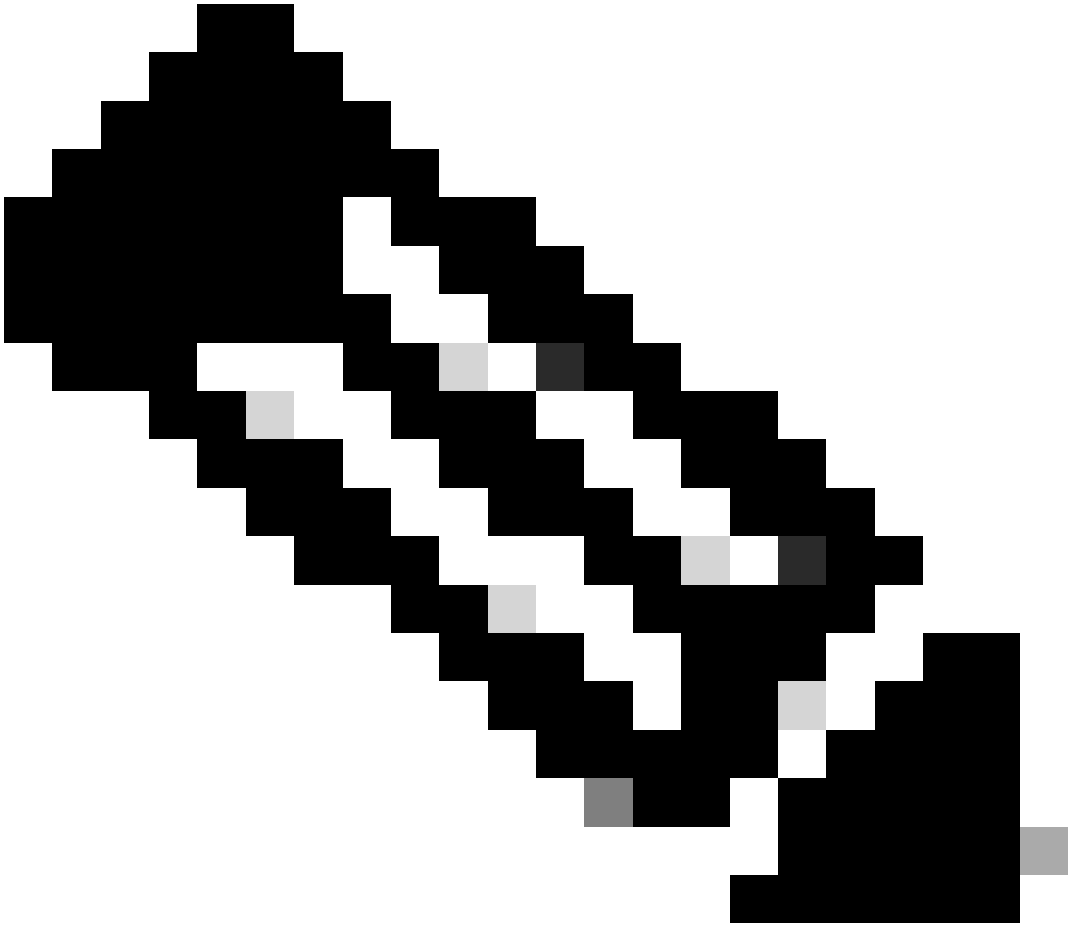
In diesem Dokument wird beschrieben, wie Sie nach der letzten Migration von der globalen DigiCert-Stammzertifizierungsstelle zu der globalen DigiCert-Stammzertifizierungsstelle G2 Probleme mit der SSL- (Secure Socket Layer)/TLS-Zertifikatssicherheit (Transport Layer Security) in AppDynamics Agents beheben.

Es enthält detaillierte Schritte, um eine ordnungsgemäße Konfiguration sicherzustellen und die nahtlose Konnektivität wiederherzustellen.

Im Jahr 2023 leitete DigiCert den Übergang zum DigiCert Global Root G2-Signaturzertifikat für die Ausgabe öffentlicher TLS/SSL-Zertifikate ein. Diese Änderung wurde durch Mozilla aktualisierte Vertrauensrichtlinie, die verlangt, dass Root-Zertifikate alle 15 Jahre aktualisiert werden, und misstrauisch älteren Zertifikaten ab 2025.

Das neue Signaturzertifikat verwendet den sichereren SHA-256-Algorithmus, der den älteren SHA-1-Standard ersetzt. Im Rahmen dieser Umstellung aktualisierte AppDynamics seine SSL-Zertifikate für die Domäne .saas.appdynamics.com, um die Zertifikate der zweiten Generation am 10.06.2025 zu verwenden.

Durch diese Aktualisierung verloren einige Anwendungs-Agents die Verbindung zu den SaaS-Controllern, da sie das neue Zertifikat nicht erkennen konnten. Um eine unterbrechungsfreie Verbindung sicherzustellen, ist es wichtig, den AppDynamics-Agent-Vertrauensspeicher zu aktualisieren, damit er die neuen DigiCert Global Root G2- und IdenTrust-Zertifikate enthält.



Anmerkung: Diese Änderung betrifft in erster Linie Agenten, die den benutzerdefinierten TrustStore verwenden oder eine sehr alte Version von OS/Java verwenden, bei der das erforderliche Zertifikat nicht im standardmäßigen OS/Java TrustStore enthalten ist.

Problem

Es liegt ein Verbindungsproblem zwischen den AppDynamics Agents und dem Controller vor, und in den Protokollen werden Fehler im Zusammenhang mit der SSL-Konfiguration oder -Kommunikation angezeigt.

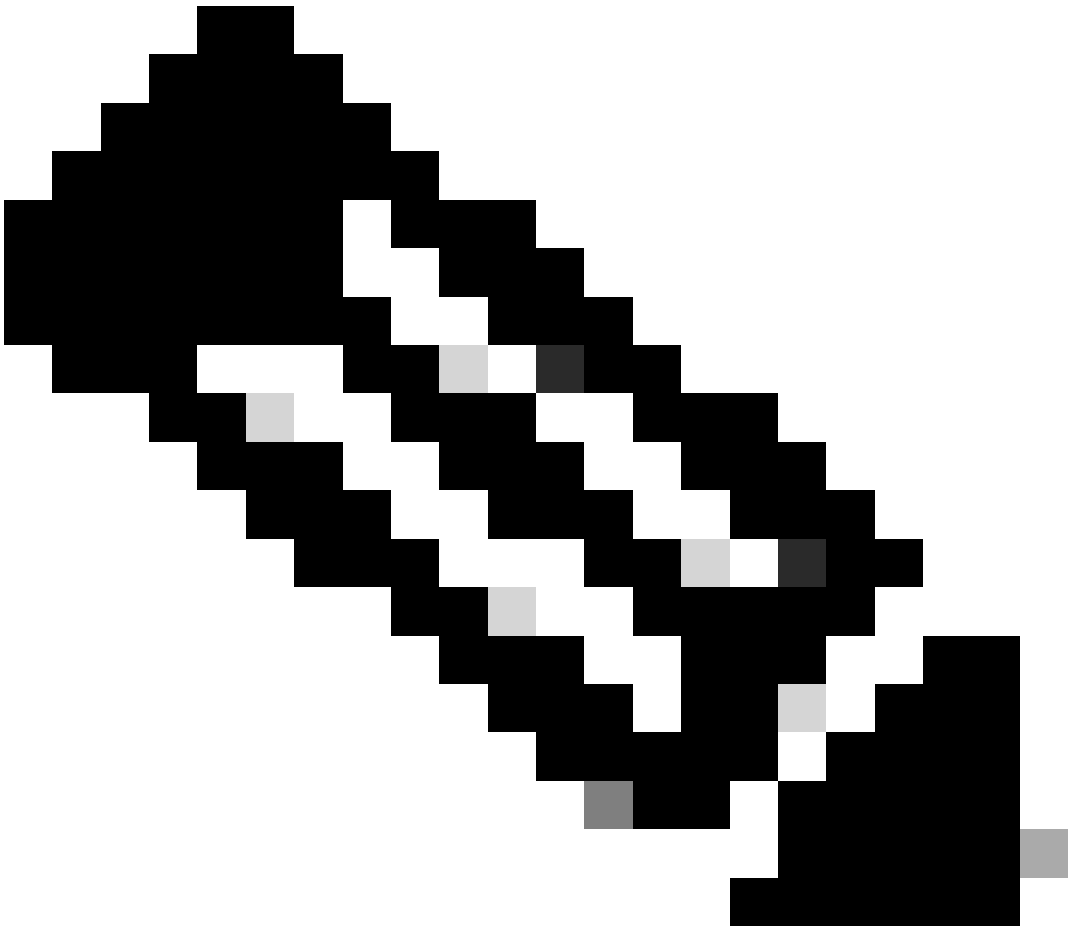
Beispiel für eine Fehlermeldung in den Protokollen: "Fehler beim Erstellen des PKIX-Pfads: xxxx: Es wurde kein gültiger Zertifizierungspfad für das angeforderte Ziel beim Validierungsversuch gefunden."

Lösung

Schritt 1: Zertifikate herunterladen

- DigiCert Global Root G2:
  - Besuchen Sie die vertrauenswürdigen Zertifikate der DigiCert-Stammzertifizierungsstelle.
  - Suchen Sie nach "DigiCert Global Root G2", und laden Sie das Zertifikat herunter.
- IdenTrust:
  - Zu IdenTrust Commercial Root CA 1 wechseln
  - Den Zertifikatsinhalt kopieren und als Datei speichern (z. B. Identrustcommercial.cer oder Identrustcommercial.pem)

Schritt 2: Identifizieren des Standorts des Truststore



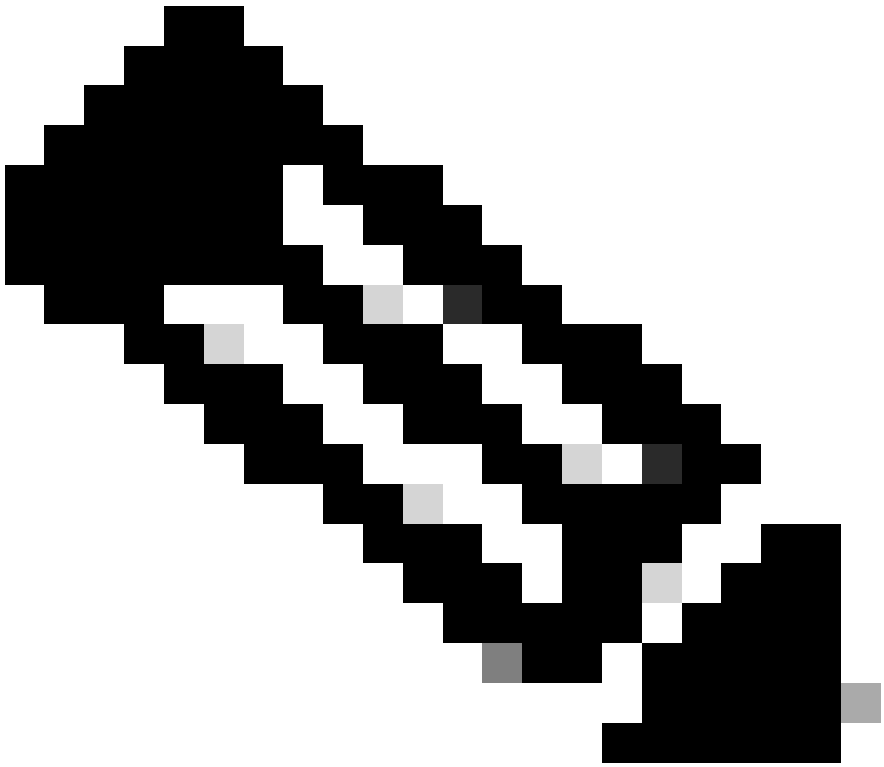
Anmerkung: Vertrauenswürdiger Speicherort ist in Schritt 3 erforderlich. Importieren Sie Zertifikate in den Vertrauenswürdigen Speicher

---

- Java-, Datenbank- oder Computer-Agent
    - JVM-Argument Truststore-Eigenschaft
        1. Überprüfen Sie beim Starten des Agenten, ob die -Djavax.net.ssl.trustStore-Eigenschaft als JVM-Argument festgelegt ist.
        2. Wenn diese Eigenschaft festgelegt ist, überprüfen Sie die von dieser Eigenschaft angegebene Schlüsselspeicherdatei, um sicherzustellen, dass sie beide Zertifikate (DigiCert Global Root G2 und IdenTrust Root-Zertifikate) enthält.
           (Wenn die Eigenschaft nicht festgelegt ist, fahren Sie mit dem nächsten Schritt fort.)

    - Controller-Info-XML
        1. Der Agent kann so konfiguriert werden, dass er den in der Datei controller-info.xml in Ihrem Agentenkonf-Verzeichnis definierten Keystore verwendet.
        2. Überprüfen Sie, ob der Controller-Keystore-Dateiname eingestellt ist.
        3. Überprüfen Sie ggf. die angegebene Schlüsselspeicherdatei, um sicherzustellen, dass beide Zertifikate enthalten sind.
           (Wird kein Eintrag gefunden, fahren Sie mit dem nächsten Schritt fort.)

    - Agent cacerts.jks-Datei
        1. Suchen Sie im Ordner des Agent-Installationsverzeichnisses nach einer Datei mit dem Namen cacerts.jksin.
        2. Überprüfen Sie diese Datei, um sicherzustellen, dass beide Zertifikate enthalten sind.
           (Wird kein Eintrag gefunden, fahren Sie mit dem nächsten Schritt fort.)

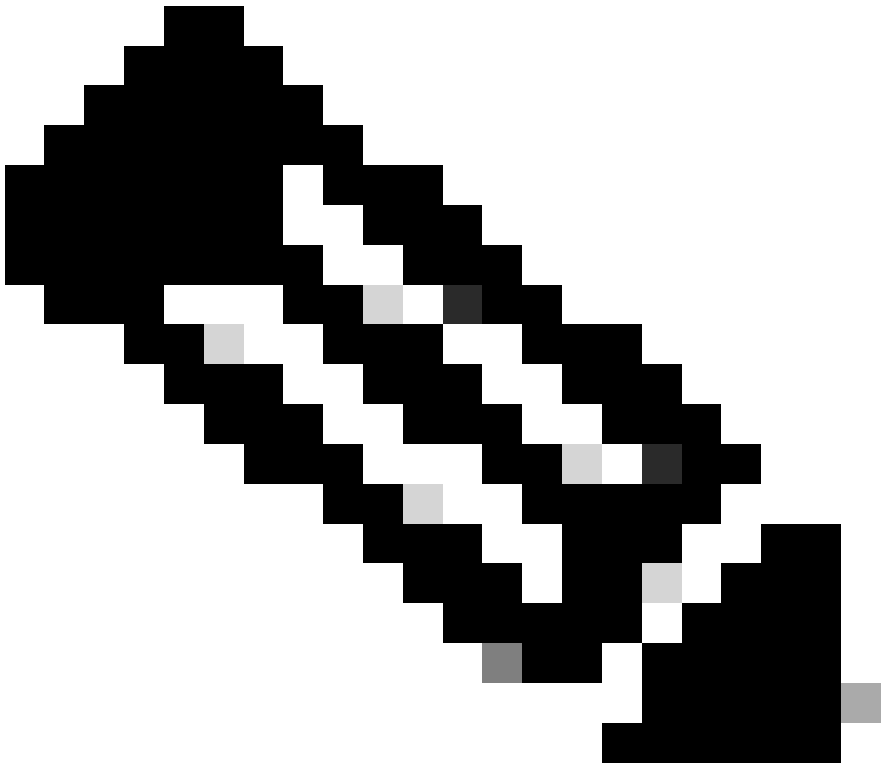


Anmerkung: Installationsverzeichnis des Agenten

Für Java Agent: AGENT_HOME/verxxx/conf oder AGENT_HOME/conf

Für Computer- oder DB-Agent: AGENT_STARTSEITE/KONF

- JRE-Standardvertrauensspeicher
  1. Wenn keine der vorherigen Konfigurationen gefunden wird, verwendet der Agent als Fallback den JRE-Standardvertrauensspeicher, der sich in der Regel unter JRE_HOME/lib/security/cacerts befindet.
  2. Überprüfen Sie diese Datei, um sicherzustellen, dass die Zertifikate enthalten sind.

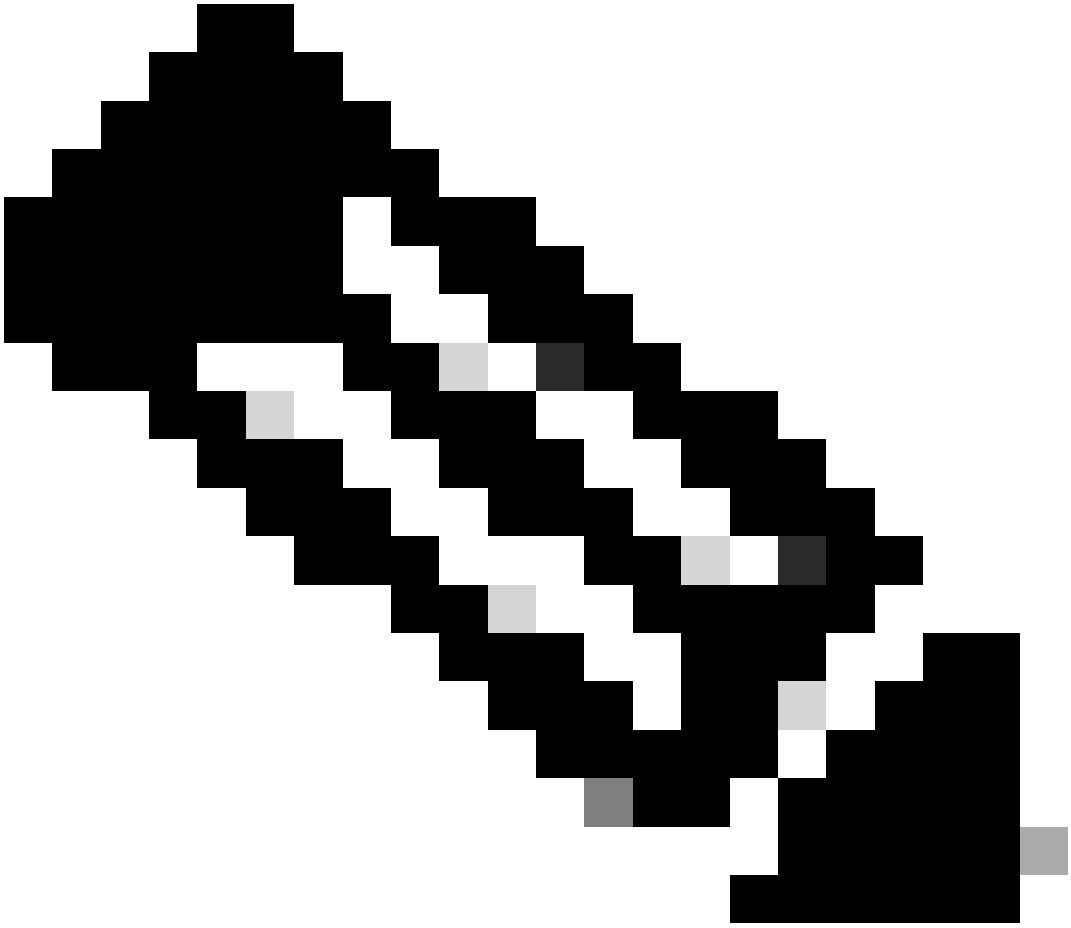


Anmerkung: Wenn Sie IBM Websphere oder IBM Websphere Liberty Profile verwenden, befindet sich JRE_HOME im Installationsverzeichnis von Websphere, d. h. IBM_WEBSPHERE_HOME/AppServer/java/ oder IBM_WEBSPHERE_HOME/Liberty/java/

- Analytiker
    - Aktivieren Sie das Kontrollkästchen Wenn der Pfad (einschließlich des Namens) des Agent-Vertrauensspeichers mit dem Element <ad.controller.https.trustStorePath> in der Agent-Konfigurationsdatei analytics-agent.properties angegeben wird, lädt der Agent diesen Vertrauensspeicher.
    - Wenn nicht in thead.controller.https.trustStorePath angegeben, wird der standardmäßige Java-TrustStore der JVM geladen, die instrumentiert wird, <JRE_HOME>/lib/security/cacerts (Standard-Passwort geändert)
    - Wenn nicht in ad.controller.https.trustStorePath angegeben und der Analytics-Agent als Machine-Agent-Erweiterung verwendet wird, wird der vom Machine-Agent verwendete TrustStore geladen.
- DotNet-Agent
    - Für Windows:

- Navigieren Sie zur Ansicht für die Zertifikatsinstallation, indem Sie zu Run> MMC.exe> select File (Datei) in der Symbolleiste wechseln und Add/Remove Snap-in (Snap-In hinzufügen/entfernen) wählen.
- Snap-In hinzufügen oder entfernen wird geöffnet, wählen Sie Zertifikate> Klicken Sie auf Hinzufügen. Das Snap-In-Fenster für das Zertifikat wird geöffnet. Wählen Sie Computerkonto> Wählen Sie Lokal oder einen anderen Computer aus > Klicken Sie auf Fertig stellen > OK.
- Erweitern Sie Zertifikate (Lokaler Computer) > Wählen Sie den Ordner Vertrauenswürdige Stammzertifizierungsstelle aus, und erweitern Sie den Ordner Zertifikate, um den Ordner Zertifikate anzuzeigen.
- Doppelklicken Sie auf den Ordner Zertifikate, und beachten Sie die Liste der vorhandenen vertrauenswürdigen Zertifikate. Ermitteln Sie, ob sowohl dieDigiCert Global Root G2- als auch die IdenTrust Root-Zertifikate vorhanden sind, andernfalls importieren Sie die fehlenden Zertifikate.

- Für Linux:
  - Der Speicherort des Truststore variiert zwischen den Linux-Distributionen. Gängige Standorte sind: /etc/ssl/certs (OS wie CentOS/RHEL/Debian)



Anmerkung: Wenn die DigiCert Global Root G2- oder IdenTrust-Zertifikate an all diesen überprüften Speicherorten fehlen, müssen Sie sie hinzufügen. Gehen Sie zu den Schritten unter "Schritt 3: Importieren von Zertifikaten in den Truststore", um die Zertifikate in den Truststore zu importieren.

Schritt 3: Importieren von Zertifikaten in den Vertrauensspeicher

- Java-, Datenbank-, Computer- oder Analytics-Agent
    - Öffnen Sie Ihr Terminal bzw. die Eingabeaufforderung, und verwenden Sie diesen Befehl keytool, um DigiCert Global Root G2- und IdenTrust Root-Zertifikate zu importieren.

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

```
-file

 -keystore

  -storepass
```

Ersetzen:

- : Ein eindeutiger Alias (z. B. digicertglobalrootg2, identrustcoomercial).
- : Pfad zur Zertifikatsdatei (z. B. /home/username/Downloads/DigiCertGlobalRootG2.crt).
- : Pfad zur Vertrauensspeicherdatei des Agenten (z. B. /opt/appdynamics/agent/ver25.x.x.x/conf/cacerts.jks).
- : Truststore-Kennwort (Standard): changeit, sofern nicht angepasst).

◦ Beispiel zum Importieren des globalen Stamm-G2-Zertifikats von DigiCert.

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

◦ Beispiel zum Importieren des kommerziellen IdenTrust-Stammzertifikats.

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

- DotNet-Agent
  - Für Windows:
    - Navigieren Sie zur Ansicht für die Zertifikatsinstallation, indem Sie zu Run> MMC.exe> select File (Datei) in der Symbolleiste wechseln und Add/Remove Snap-in (Snap-In hinzufügen/entfernen) wählen.
    - Snap-In hinzufügen oder entfernen wird geöffnet, wählen Sie Zertifikate> Klicken

Sie auf Hinzufügen. Das Snap-In-Fenster für das Zertifikat wird geöffnet. Wählen Sie Computerkonto> Wählen Sie Lokal oder einen anderen Computer aus > Klicken Sie auf Fertig stellen > OK.
- Erweitern Sie Zertifikate (Lokaler Computer) > Wählen Sie den Ordner Vertrauenswürdige Stammzertifizierungsstelle aus, und erweitern Sie den Ordner Zertifikate, um den Ordner Zertifikate anzuzeigen.
- Klicken Sie mit der rechten Maustaste auf Zertifikatordner, und wählen SieAlle Aufgaben > Importieren aus.Der Zertifikatimport-Assistent wird geöffnet, durchlaufen die Anweisungen, und fügen Sie das fehlende Element hinzu.DigiCert Global Root G2-Zertifikat und/oder IdenTrust Root-Zertifikat.

- Für Linux:
  - Kopieren Sie die heruntergeladenen DigiCert Global Root G2- und IdenTrust Root-Zertifikatsdateien in das identifizierte Verzeichnis für Vertrauensspeicher.
  - Aktualisieren Sie den Trust Store, indem Sie den Befehl ausführen.

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

Schritt 4: Überprüfen Sie den Import

- Java-, Datenbank-, Computer- oder Analytics-Agent
  - Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Zertifikate erfolgreich hinzugefügt wurden:

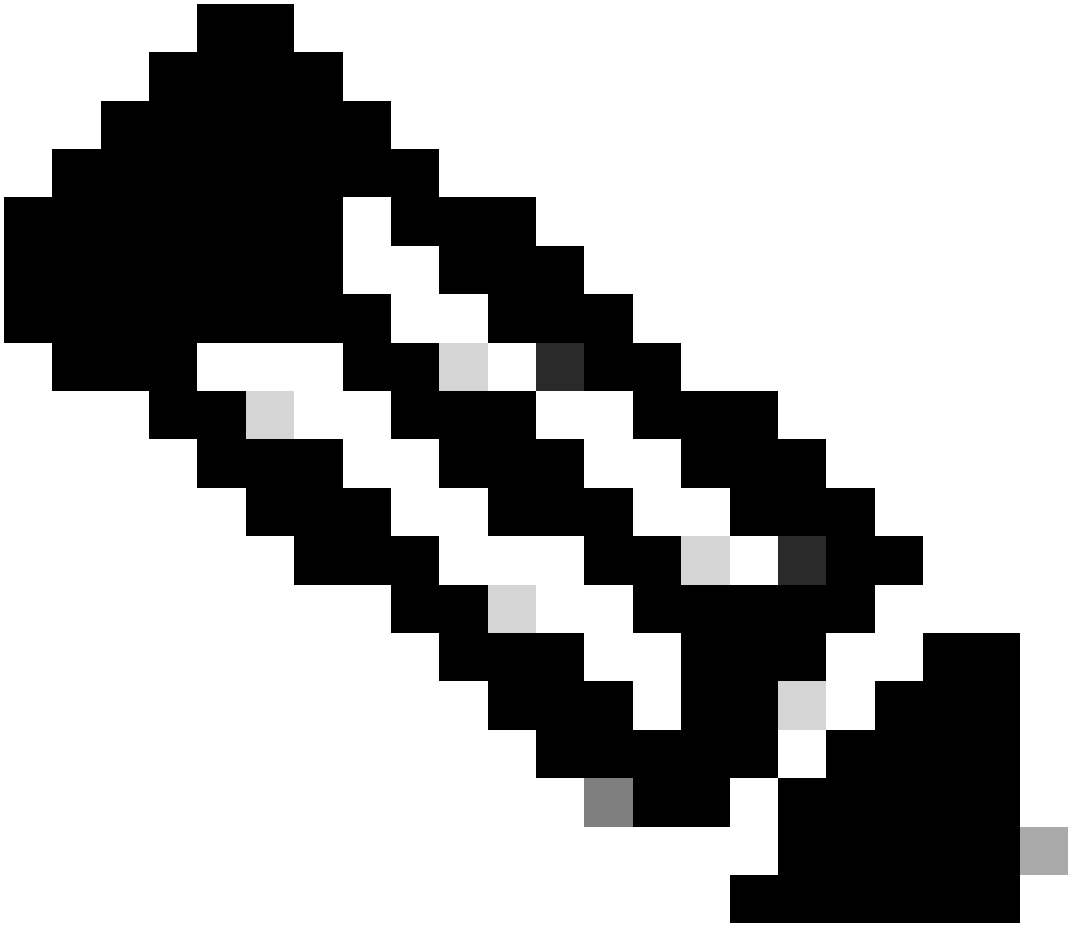
```
keytool -list -v -keystore

            -storepass

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

Ersetzen:

- `<agent_truststore_path>`: Pfad zur Vertrauensspeicherdatei des Agenten.
- `<truststore_password>`: Das TrustStore-Kennwort.



Anmerkung: Stellen Sie sicher, dass DigiCert Global Root G2 und IdenTrust Commercial Root CA 1 in der Ausgabe angezeigt werden.

- DotNet-Agent
    - Für Windows:
        - Navigieren Sie zur Ansicht für die Zertifikatsinstallation, indem Sie zu Run> MMC.exe> select File (Datei) in der Symbolleiste wechseln und Add/Remove Snap-in (Snap-In hinzufügen/entfernen) wählen.
        - Snap-In hinzufügen oder entfernen wird geöffnet, wählen Sie Zertifikate> Klicken Sie auf Hinzufügen. Das Snap-In-Fenster für das Zertifikat wird geöffnet. Wählen Sie Computerkonto> Wählen Sie Lokal oder einen anderen Computer aus > Klicken Sie auf Fertig stellen > OK.
        - Erweitern Sie Zertifikate (Lokaler Computer) > Wählen Sie den Ordner Vertrauenswürdige Stammzertifizierungsstelle aus, und erweitern Sie den Ordner Zertifikate, um den Ordner Zertifikate anzuzeigen.

- Doppelklicken Sie auf den Ordner Certificates (Zertifikate), und Sie müssen dort sowohl die DigiCert Global Root G2- als auch die IdenTrust Root-Zertifikate sehen.

- Für Linux:
  - Führen Sie den Befehl aus, und überprüfen Sie, ob das globale DigiCert-Root G2- und das IdenTrust-Root-Zertifikat vorhanden ist:

```
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
```

Schritt 5: Den Agenten neu starten

Starten Sie abschließend den AppDynamics-Agent neu. Dadurch können die Änderungen wirksam werden.

Zugehörige Informationen

Support-Tipp: Hinzufügen von DigiCert- und IdenTrust-SSL-Stammzertifikaten zu Agent Trust Stores

Benötigen Sie weitere Unterstützung?

Wenn Sie Fragen haben oder Probleme auftreten, erstellen Sie ein Support-Ticket mit folgenden Informationen:

- Protokolle vom Agenten.
- Details zum Speicherort des Vertrauensspeichers und hinzugefügten Zertifikate.
- Es wurden Fehlermeldungen gefunden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.