DigiCert 루트 G2 업데이트 후 AppDynamics SSL/TLS 문제 해결

목차

소개

사전 요구 사항

- 사용된 구성 요소

배경 정보

문제

솔루션

- 1단계. 인증서 다운로드
- 2단계. Truststore 위치 확인
  - Java, 데이터베이스 또는 머신 에이전트
  - 분석 에이전트
  - DotNet 에이전트
- 3단계. 인증서를 Truststore로 가져오기
  - Java, 데이터베이스, 머신 또는 분석 에이전트
  - DotNet 에이전트
- 4단계. 가져오기 확인
  - Java, 데이터베이스, 머신 또는 분석 에이전트
  - DotNet 에이전트
- 5단계. 에이전트를 다시 시작합니다.

관련 정보

추가 지원이 필요하십니까?

소개

이 문서에서는 AppDynamics 에이전트의 SSL(Secure Socket Layer)/TLS(Transport Layer Security) 인증서 신뢰 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 최근 DigiCert Global Root CA에서 DigiCert Global Root G2로 마이그레이션한 후

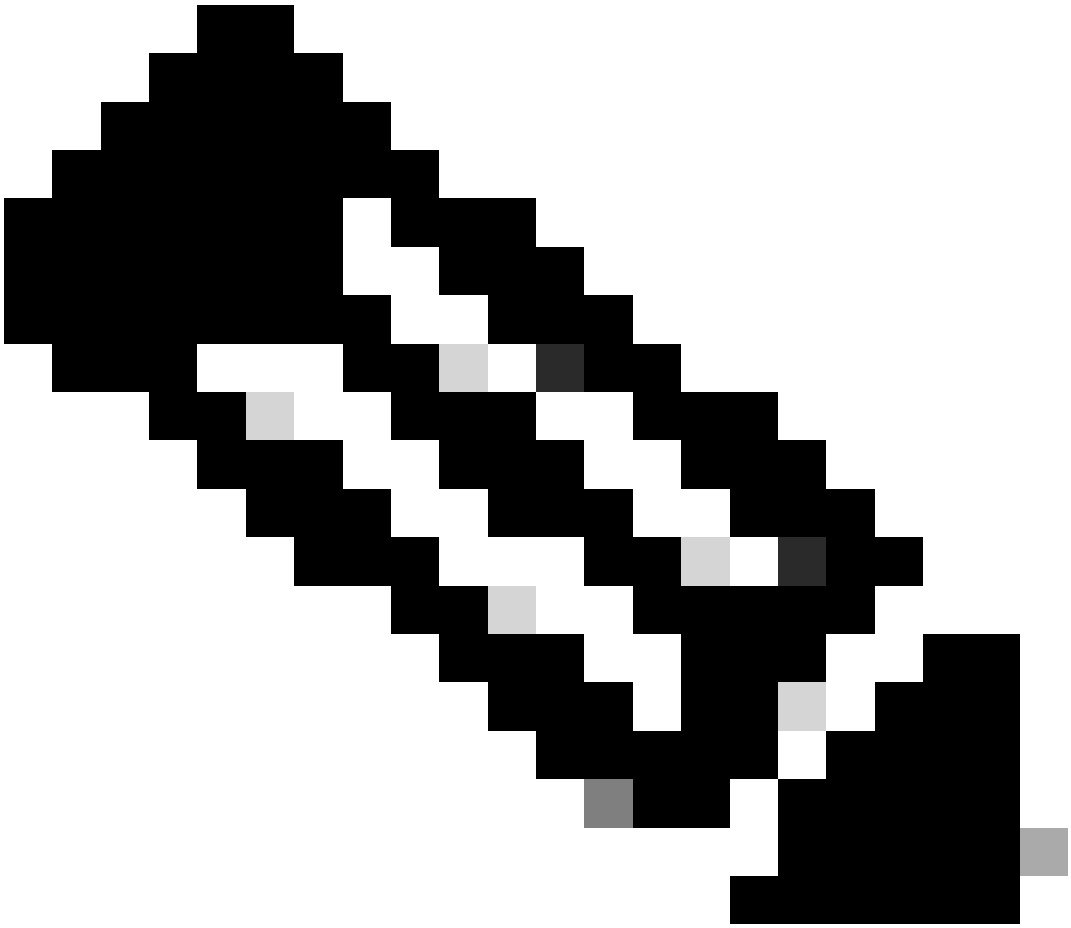
AppDynamics 에이전트에서 SSL(Secure Socket Layer)/TLS(Transport Layer Security) 인증서 신뢰 문제를 해결하는 방법에 대해 설명합니다.

올바른 컨피그레이션 및 원활한 연결을 복원하기 위한 자세한 단계를 제공합니다.

2023년에 DigiCert는 공용 TLS/SSL 인증서 발급을 위해 DigiCert Global Root G2 서명 인증서로의 전환을 시작했습니다. 이러한 변경은 Mozilla가 루트 인증서를 15년마다 업데이트하도록 의무화하고 2025년부터 이전 인증서를 불신하는 트러스트 정책을 업데이트한 데 따른 것입니다.

새 서명 인증서는 더 안전한 SHA-256 알고리즘을 사용하여 이전 SHA-1 표준을 대체합니다. 이 전환의 일환으로 AppDynamics는 도메인 .saas.appdynamics.com에 대한 SSL 인증서를 업데이트하여 2025-06-10에 2세대 인증서를 활용했습니다.

이 업데이트로 인해 일부 애플리케이션 에이전트에서 새 인증서를 인식할 수 없어 SaaS 컨트롤러와의 연결이 끊어졌습니다. 중단 없는 연결을 보장하려면 새 DigiCert 전역 루트 G2 및 IdenTrust 인증서를 포함하도록 AppDynamics 에이전트 트러스트 저장소를 업데이트해야 합니다.



참고: 이 변경은 기본적으로 사용자 지정 신뢰 저장소를 사용 중이거나 필수 인증서가 기본

OS/Java 신뢰 저장소에 포함되지 않은 매우 오래된 버전의 OS/Java를 사용 중인 에이전트에 영향을 줍니다.

문제

AppDynamics 에이전트와 컨트롤러 간에 연결 문제가 있으며, 로그에 SSL 구성 또는 통신과 관련된 오류가 표시됩니다.

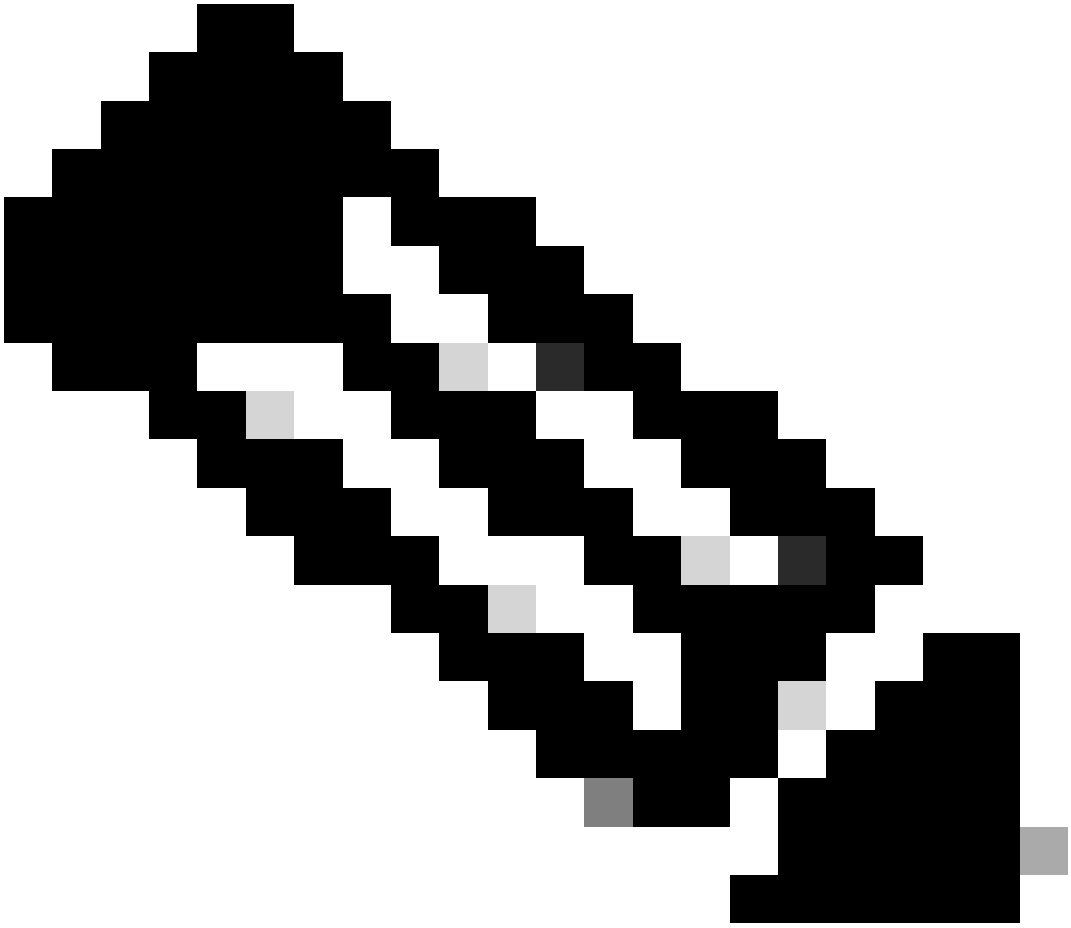
로그의 오류 메시지 예: "PKIX 경로 구축 실패: xxxx: 유효성 검사를 시도하는 요청된 대상에 대한 유효한 인증 경로를 찾을 수 없습니다."

솔루션

1단계. 인증서 다운로드

- DigiCert 전역 루트 G2:
  - DigiCert신뢰할 수 있는 루트 인증 기관 인증서 방문
  - "DigiCert Global Root G2"를 검색하고 인증서를 다운로드합니다.
- IdenTrust:
  - IdenTrust Commercial Root CA 1로 이동
  - 인증서 내용을 복사하여 파일로 저장합니다(예: Identtrustcommercial.cer 또는 Identtrustcommercial.pem).

2단계. Truststore 위치 확인

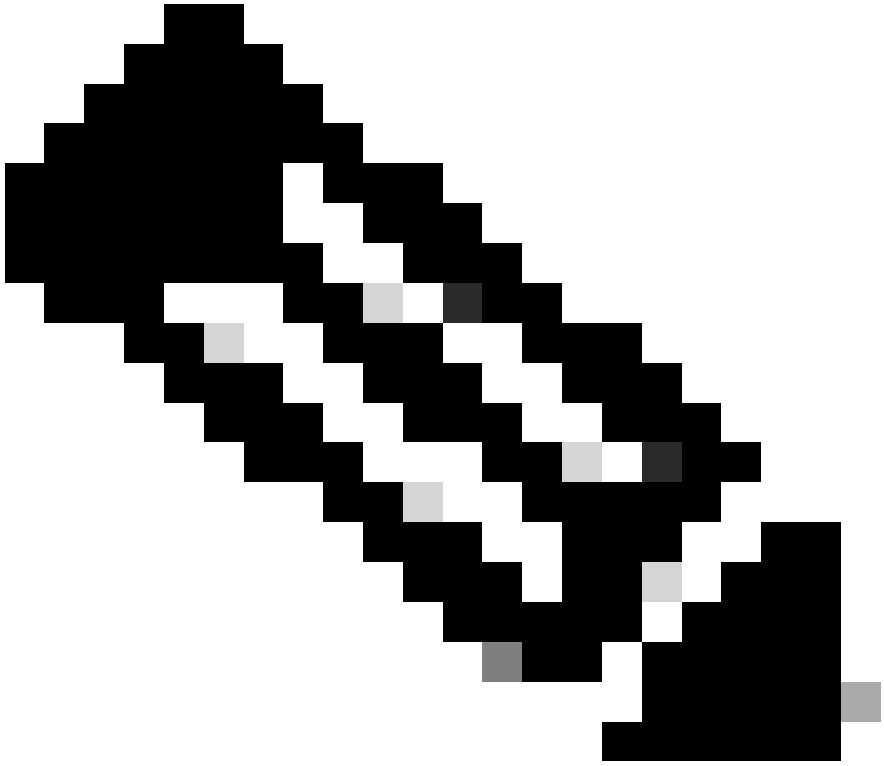


참고: 3단계에서 Truststore 위치가 필요합니다. Truststore로 인증서 가져오기

- Java, 데이터베이스 또는 머신 에이전트
  - JVM 인수 Truststore 속성
    1. 에이전트를 시작할 때 -Djavax.net.ssl.trustStore 속성이 JVM 인수로 설정되어 있는지 확인합니다.
    2. 이 속성이 설정된 경우 이 속성에서 지정한 키 저장소 파일을 검사하여 두 인증서(DigiCert 전역 루트 G2 및 IdenTrust 루트 인증서)를 모두 포함하는지 확인합니다. (등록 정보가 설정되지 않은 경우 다음 단계로 진행합니다.)
  - 컨트롤러 정보 XML
    1. 상담원은 상담원 conf 디렉터리의 controller-info.xml 파일에 정의된 키 저장소를 사용하도록 구성할 수 있습니다.

2. controller-keystore-filename 설정을 확인합니다.
3. 있는 경우 지정된 키 저장소 파일을 검사하여 두 인증서가 모두 포함되어 있는지 확인합니다.
   (찾을 수 없는 경우 다음 단계로 진행합니다.)

◦ 에이전트 cacerts.jks 파일
1. 에이전트 설치 디렉토리의 conffler에서 cacerts.jkssof라는 파일을 확인합니다.
2. 이 파일을 검사하여 두 인증서가 모두 포함되어 있는지 확인합니다.
   (찾을 수 없는 경우 다음 단계로 진행합니다.)

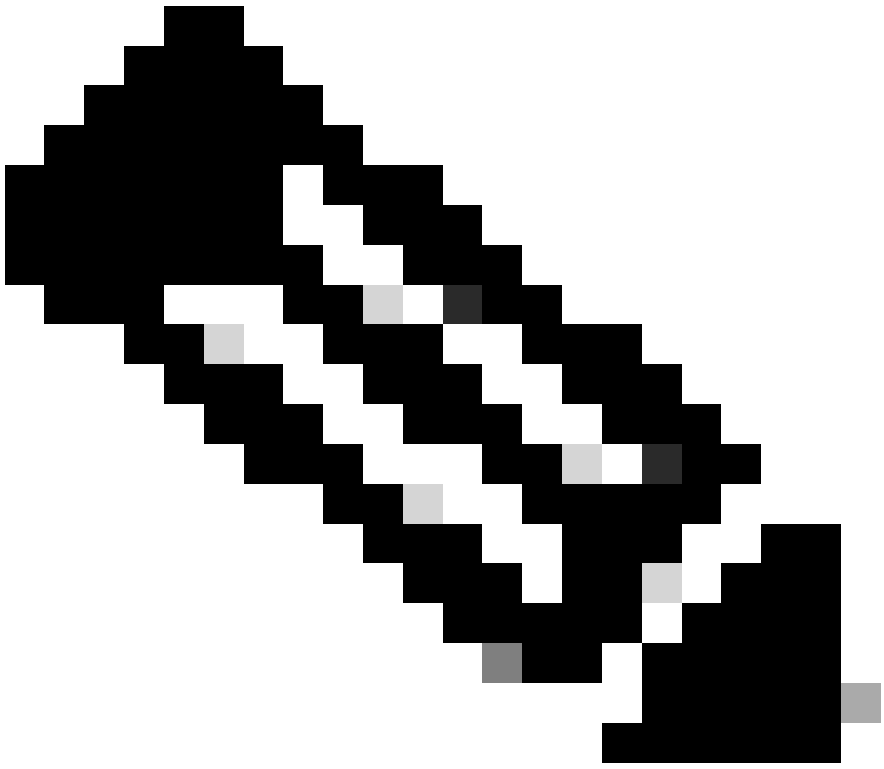


참고: 에이전트 설치 디렉토리

Java 에이전트의 경우: AGENT_HOME/verxxx/conf 또는 AGENT_HOME/conf

시스템 또는 DB 에이전트의 경우: 상담원_홈/컨퍼런스

◦ JRE 기본 트러스트 저장소
1. 이전 컨피그레이션 중 어느 것도 발견되지 않으면 에이전트는 대체로서 JRE_HOME/lib/security/cacerts에 있는 JRE 기본 신뢰 저장소를 사용합니다.
2. 이 파일을 검사하여 인증서가 포함되어 있는지 확인합니다.



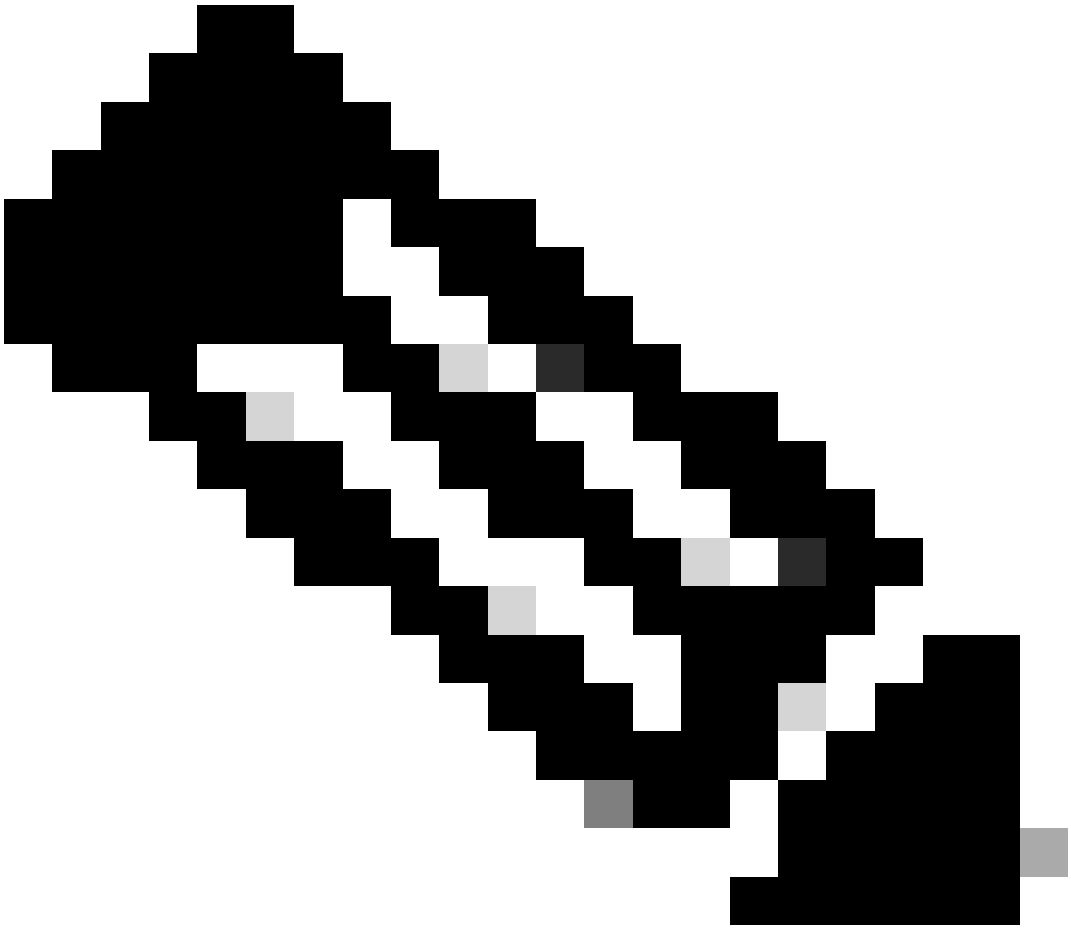
참고: IBM Websphere 또는 IBM Websphere Liberty Profile을 사용하는 경우 JRE_HOME은 각각 AppServer 또는 Websphere 설치 디렉토리 아래의 Liberty Directory(IBM_WEBSPHERE_HOME/AppServer/java/또는 IBM_WEBSPHERE_HOME/Liberty/java/)에 있습니다.

- 분석 에이전트
    - 에이전트 구성 파일 analytics-agent.properties의 <ad.controller.https.trustStorePath> 요소를 사용하여 에이전트 신뢰 저장소의 경로(이름 포함)를 지정한 다음 에이전트가 해당 신뢰 저장소를 로드하는지 확인합니다.
    - thead.controller.https.trustStorePath에 지정되지 않은 경우 계측되는 JVM의 기본 Java 신뢰 저장소인 <JRE_HOME>/lib/security/cacerts(기본 비밀번호 변경)가 로드됩니다
    - ad.controller.https.trustStorePath와 분석 에이전트가 머신 에이전트 확장으로 사용되고 있지 않으면 머신 에이전트에서 사용하는 신뢰 저장소를 로드합니다.
- DotNet 에이전트
    - Windows의 경우:
        - 도구 모음에서 실행> MMC.exe> 선택File로 이동하여 인증서 설치 보기로 이동한

다음 선택Add/Remove Snap-in(스냅인 추가/제거)을 선택합니다.

- 스냅인 추가 또는 제거 창이 열리고 Certificates(인증서) > ClickAdd(추가)를 클릭합니다. 인증서 스냅인 창이 열립니다. 컴퓨터 계정>로컬 또는 다른 컴퓨터를 선택합니다.>마침>확인을 클릭합니다.
- Certificates (Local Computer)(인증서(로컬 컴퓨터))> Trusted Root Certification Authority(신뢰할 수 있는 루트 인증 기관) 폴더를 선택하고 Certificates(인증서) 폴더를 표시하도록 확장합니다.
- Certificates 폴더를 더블 클릭하고 기존의 신뢰할 수 있는 인증서 목록을 확인합니다. DigiCert 전역 루트 G2 및 IdenTrust 루트 인증서가 둘 다 있는지 확인하고 그렇지 않으면 누락된 인증서를 가져옵니다.

- Linux의 경우:
  - 신뢰 저장소의 위치는 Linux 배포판에 따라 다릅니다. 일반적인 위치: /etc/ssl/certs(CentOS/RHEL/Debian과 같은 OS)



참고: DigiCert 전역 루트 G2 또는 IdenTrust 인증서가 선택된 모든 위치에서 누락된 경우

해당 인증서를 추가해야 합니다. 인증서를 신뢰 저장소로 가져오려면 "3단계. Import Certificates to the Truststore(인증서를 신뢰 저장소로 가져오기)"에서 설명한 단계를 참조하십시오.

3단계. 인증서를 Truststore로 가져오기

- Java, 데이터베이스, 머신 또는 분석 에이전트
  - 터미널 또는 명령 프롬프트를 열고 이 keytool 명령을 사용하여 DigiCert 전역 루트 G2 및 IdenTrust 루트 인증서를 가져옵니다.

```
keytool -import -trustcacerts -alias

            -file

             -keystore

              -storepass
```

교체:

- : 고유한 별칭(예: digicertglobalrootg2, identrustcoomercial).
- : 인증서 파일의 경로(예: /home/username/Downloads/DigiCertGlobalRootG2.crt).
- : 에이전트 신뢰 저장소 파일의 경로(예: /opt/appdynamics/agent/ver25.x.x.x/conf/cacerts.jks)입니다.
- : Truststore 비밀번호(기본값: changeit, 사용자 정의).

  - DigiCert 전역 루트 G2 인증서 가져오기 예.

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

- IdenTrust 상업용 루트 인증서 가져오기의 예.

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

- DotNet 에이전트
  - Windows의 경우:
    - 도구 모음에서 실행> MMC.exe> 선택File로 이동하여 인증서 설치 보기로 이동한 다음 선택Add/Remove Snap-in(스냅인 추가/제거)을 선택합니다.
    - 스냅인 추가 또는 제거 창이 열리고 Certificates(인증서) > ClickAdd(추가)를 클릭합니다. 인증서 스냅인 창이 열립니다. 컴퓨터 계정>로컬 또는 다른 컴퓨터를 선택합니다.>마침>확인을 클릭합니다.
    - Certificates (Local Computer)(인증서(로컬 컴퓨터))> Trusted Root Certification Authority(신뢰할 수 있는 루트 인증 기관) 폴더를 선택하고 Certificates(인증서) 폴더를 표시하도록 확장합니다.
    - Certificates(인증서)폴더를 마우스 오른쪽 버튼으로 클릭하고 All Tasks(모든 작업) > Import(가져오기)를 선택합니다.Certificate Import Wizard(인증서 가져오기 마법사)가 열리면 지침을 검토하고 누락된 항목을 추가합니다DigiCert 전역 루트 G2 인증서 및/또는 IdenTrust 루트 인증서
  - Linux의 경우:
    - 다운로드한 DigiCert 글로벌 루트 G2 및 IdenTrust 루트 인증서 파일을 식별된 트러스트 저장소 디렉터리에 복사합니다.
    - 명령을 실행하여 Trust Store를 업데이트합니다.

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

4단계. 가져오기 확인

- Java, 데이터베이스, 머신 또는 분석 에이전트
  - 인증서가 성공적으로 추가되었는지 확인하려면 다음 명령을 실행합니다.

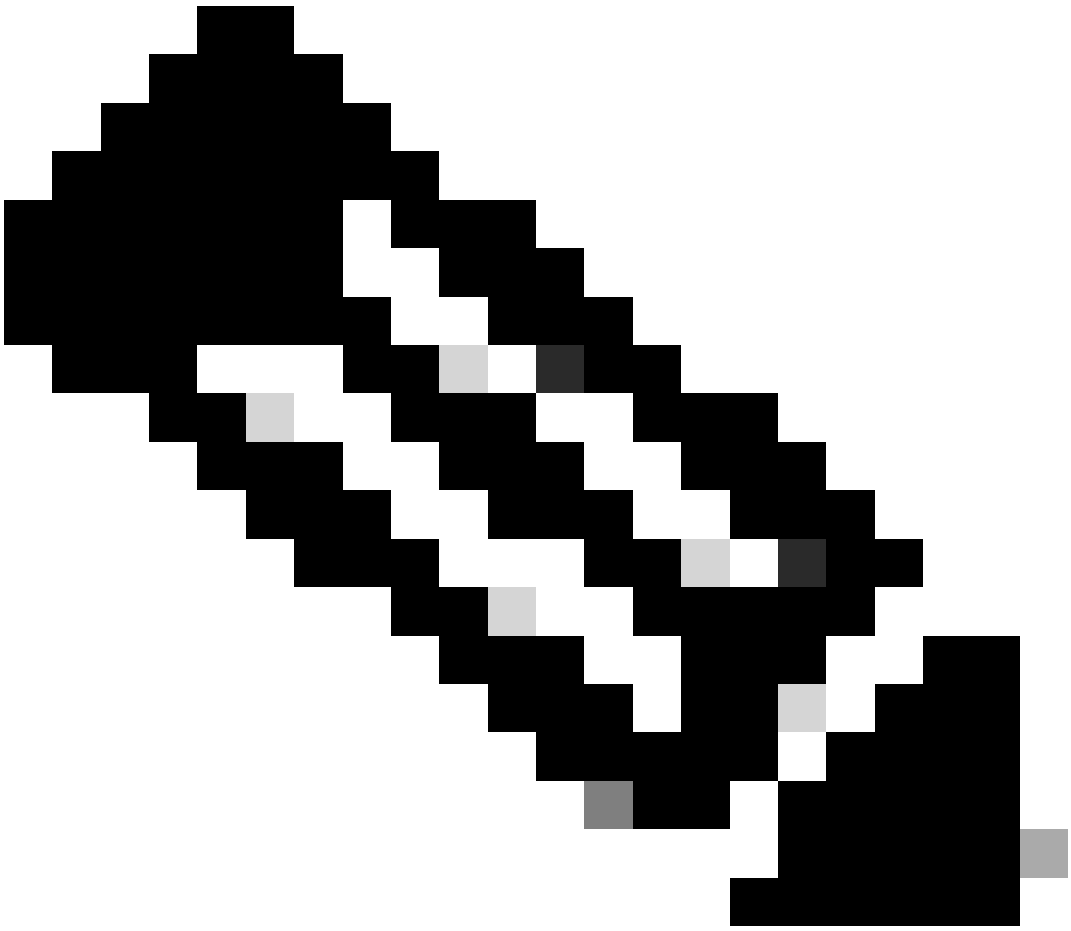
```
keytool -list -v -keystore
```

```
-storepass
```

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

교체:

- <agent_truststore_path>: 에이전트 신뢰 저장소 파일의 경로입니다.
- <truststore_password>: 신뢰 저장소 비밀번호입니다.



참고: DigiCert 글로벌 루트 G2 및 IdenTrust Commercial 루트 CA 1이 모두 출력에 나타나는지 확인합니다.

- DotNet 에이전트

- Windows의 경우:
  - 도구 모음에서 실행> MMC.exe> 선택File로 이동하여 인증서 설치 보기로 이동한 다음 선택Add/Remove Snap-in(스냅인 추가/제거)을 선택합니다.
  - 스냅인 추가 또는 제거 창이 열리고 Certificates(인증서) > ClickAdd(추가)를 클릭합니다. 인증서 스냅인 창이 열립니다. 컴퓨터 계정>로컬 또는 다른 컴퓨터를 선택합니다.>마침>확인을 클릭합니다.
  - Certificates (Local Computer)(인증서(로컬 컴퓨터))> Trusted Root Certification Authority(신뢰할 수 있는 루트 인증 기관) 폴더를 선택하고 Certificates(인증서) 폴더를 표시하도록 확장합니다.
  - Certificates 폴더를 두 번 클릭하면 DigiCert 전역 루트 G2 및 IdenTrust 루트 인증서가 모두 표시됩니다.

- Linux의 경우:
  - 명령을 실행하고 DigiCert 전역 루트 G2 및 IdenTrust 루트 인증서가 있는지 확인합니다.

```
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
```

5단계. 에이전트를 다시 시작합니다.

마지막으로 AppDynamics 에이전트를 다시 시작하십시오. 이렇게 하면 변경 사항이 적용됩니다.

관련 정보

지원 자문: 에이전트 신뢰 저장소에 DigiCert 및 IdenTrust 루트 SSL 인증서 추가

추가 지원이 필요하십니까?

질문이 있거나 문제가 있는 경우 다음 세부 정보가 포함된 지원 티켓을 만드십시오.

- 상담원의 로그
- 추가된 신뢰 저장소 위치 및 인증서의 세부 정보.
- 모든 오류 메시지가 발생했습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.