Resolver problemas de AppDynamics SSL/TLS después de la actualización de DigiCert Root G2

Contenido

Introducción

Este documento describe cómo abordar los problemas de confianza de certificados SSL (Secure Socket Layer)/ TLS (Transport Layer Security) en AppDynamics Agents.

Prerequisites

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

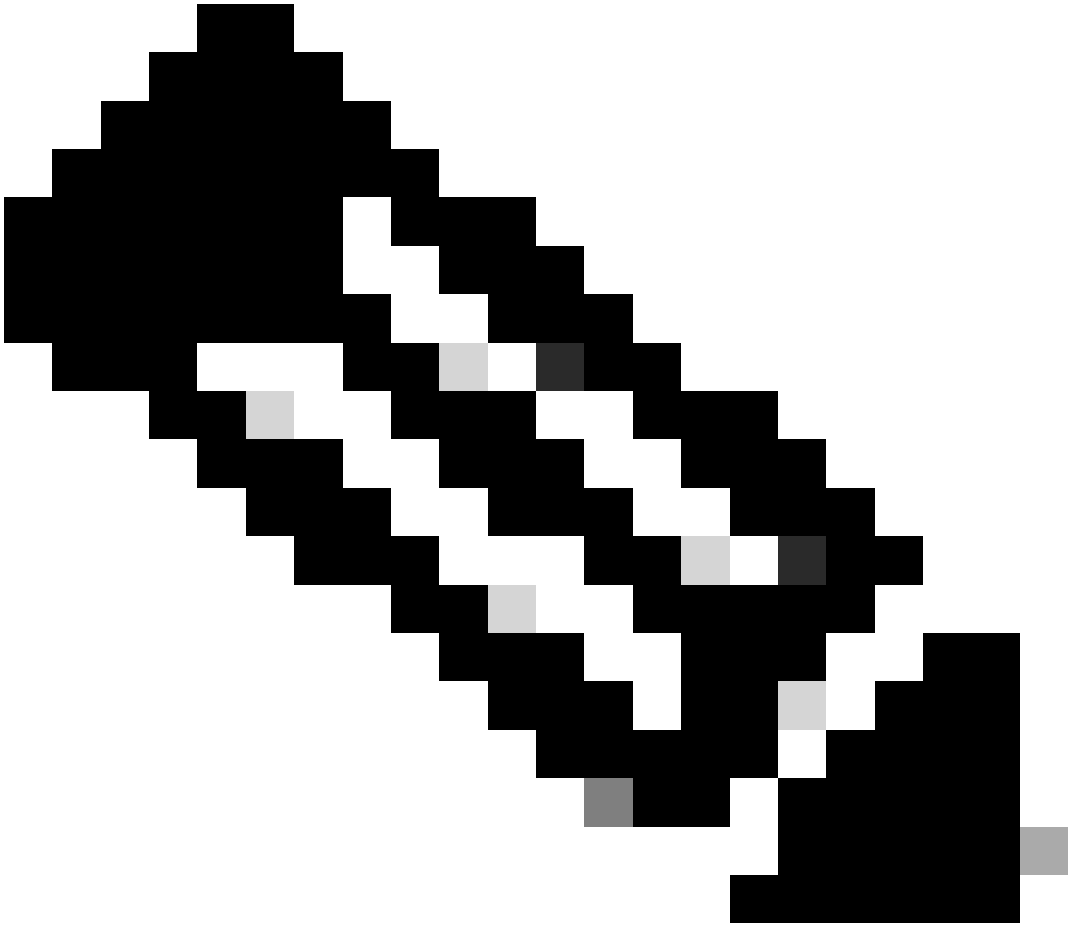
Este documento describe cómo abordar los problemas de confianza de certificados SSL (Secure Socket Layer)/ TLS (Transport Layer Security) en AppDynamics Agents después de la reciente migración de DigiCert Global Root CA a DigiCert Global Root G2.

Proporciona los pasos detallados para garantizar una configuración adecuada y restaurar la conectividad sin problemas.

En 2023, DigiCert inició la transición al certificado de firma G2 raíz global de DigiCert para emitir certificados públicos TLS/SSL. Este cambio fue provocado por la política de confianza actualizada de Mozilla, que exige que los certificados raíz se actualicen cada 15 años, y desconfiar de los certificados antiguos a partir de 2025.

El nuevo certificado de firma emplea el algoritmo SHA-256 más seguro, que sustituye al estándar SHA-1 más antiguo. Como parte de esta transición, AppDynamics actualizó sus certificados SSL para el dominio .saas.appdynamics.com para utilizar los certificados de segunda generación en 2025-06-10.

Esta actualización provocó que algunos agentes de aplicaciones perdieran la conectividad con los controladores SaaS debido a su incapacidad para reconocer el nuevo certificado. Para garantizar una conectividad ininterrumpida, es crucial actualizar el almacén de confianza del agente AppDynamics para incluir los nuevos certificados DigiCert Global Root G2 e IdenTrust.



Nota: Este cambio afecta principalmente a los agentes que utilizan el almacén de confianza personalizado o una versión muy antigua de OS/Java en la que el certificado necesario no se incluye en el almacén de confianza predeterminado de OS/Java.

Problema

Hay un problema de conectividad entre AppDynamics Agents y Controller, y los registros muestran errores relacionados con la configuración o la comunicación SSL.

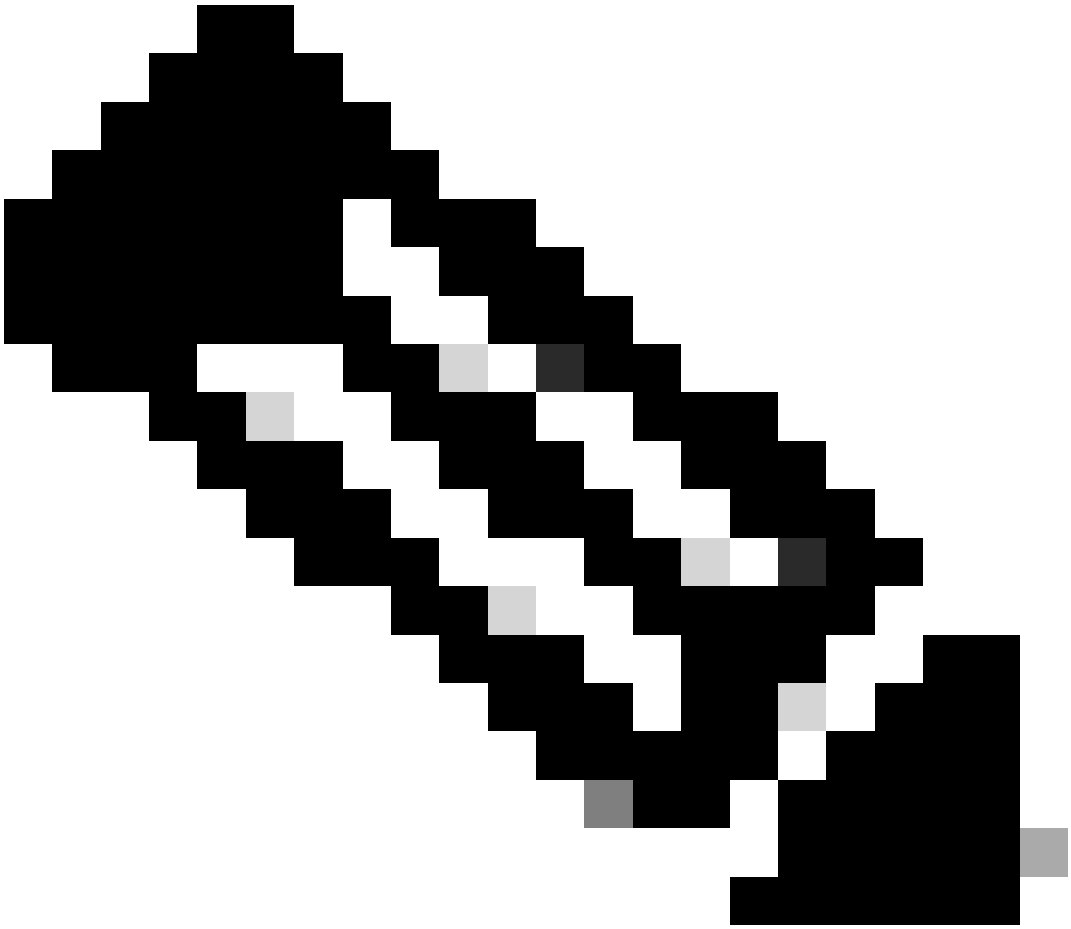
Ejemplo de mensaje de error en los registros: "Error al crear la ruta PKIX: xxxx: no se puede encontrar una ruta de certificación válida para la validación del intento de destino solicitado"

Solución

Paso 1. Descargar certificados

- Raíz global DigiCert G2:
  - Visite DigiCert Trusted Root Authority Certificates
  - Busque "DigiCert Global Root G2" y descargue el certificado.
- IdenTrust:
  - Vaya a IdenTrust Commercial Root CA 1
  - Copie el contenido del certificado y guárdelo como un archivo (por ejemplo, Identrustcommercial.cer o Identrustcommercial.pem)

Paso 2. Identificar la ubicación del almacén de confianza



Nota: La ubicación del almacén de confianza es necesaria en el paso 3. Importar certificados al almacén de confianza

- Java, agente de base de datos o de equipo
  - Propiedad Truststore del argumento JVM

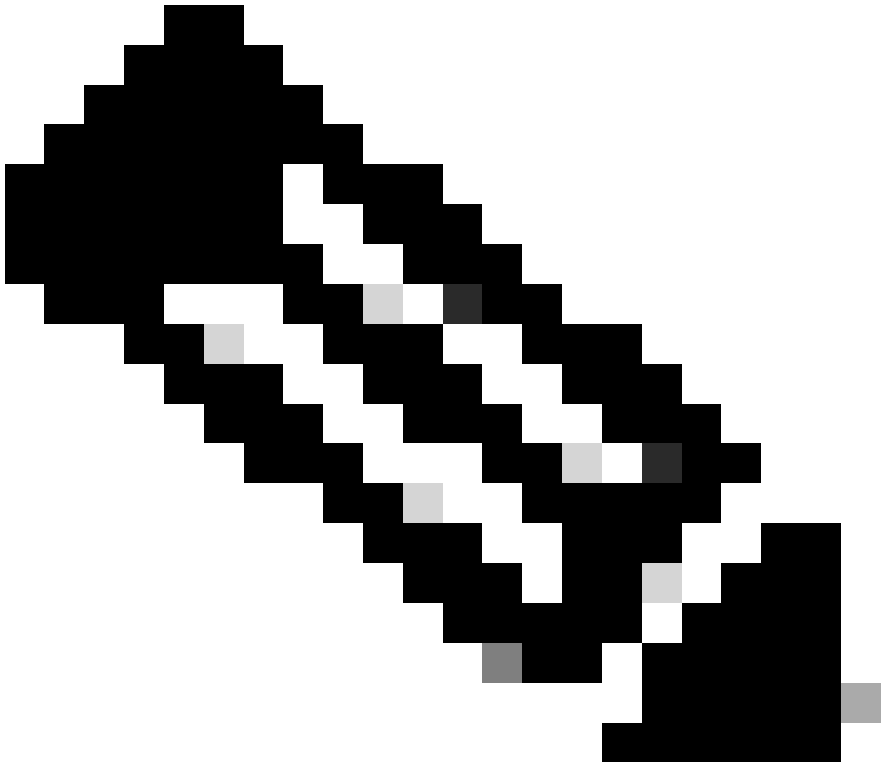
1. Compruebe si la propiedad -Djavax.net.ssl.trustStore está establecida como argumentos de JVM al iniciar el agente.
2. Si se establece esta propiedad, inspeccione el archivo de almacén de claves especificado por esta propiedad para confirmar que incluye ambos certificados (certificados raíz global G2 de DigiCert y certificados raíz de IdenTrust).
   (Si no se establece la propiedad, vaya al paso siguiente.)

- XML de información del controlador

1. El agente se puede configurar para utilizar el almacén de claves definido en el archivo controller-info.xml del directorio conf del agente.
2. Verifique la configuración controller-keystore-filename.
3. Si está presente, inspeccione el archivo de almacén de claves especificado para confirmar que se incluyen ambos certificados.
   (Si no se encuentra, vaya al paso siguiente.)

- Archivo cacerts.jks del agente

1. Busque un archivo denominado cacerts.jksen la carpeta conf del directorio de instalación del agente.
2. Inspeccione este archivo para comprobar que se incluyen ambos certificados.
   (Si no se encuentra, vaya al paso siguiente.)

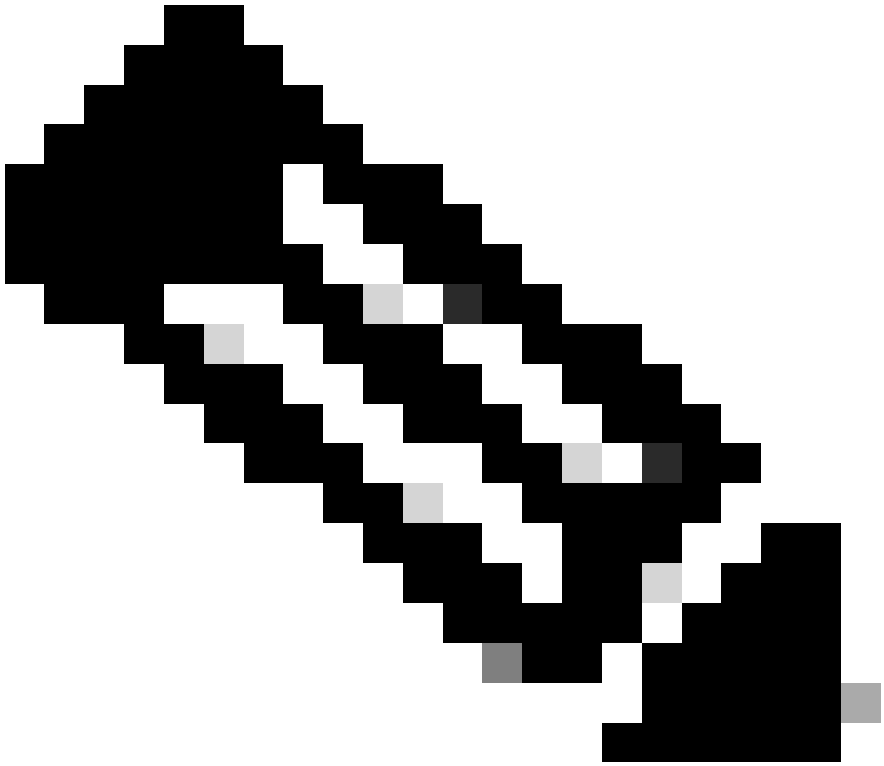


Nota: Directorio de instalación del agente

Para el agente Java: AGENT_HOME/verxxx/conf o AGENT_HOME/conf

Para máquina o agente de base de datos: AGENT_HOME/conf

- Almacén de confianza predeterminado de JRE
  1. Si no se encuentra ninguna de las configuraciones anteriores, como reserva, el agente utiliza el almacén de confianza predeterminado de JRE, que normalmente se encuentra enJRE_HOME/lib/security/cacerts.
  2. Inspeccione este archivo para asegurarse de que se incluyen los certificados.



Nota: Si utiliza IBM Websphere o IBM Websphere Liberty Profile, JRE_HOME se encuentra dentro de AppServer o Liberty Directory en el directorio de instalación de Websphere respectivamente, es decir, IBM_WEBSPHERE_HOME/AppServer/java/ o IBM_WEBSPHERE_HOME/Liberty/java/

- Agente de análisis
  - Verifique Si la ruta (incluido el nombre) del almacén de confianza del agente se

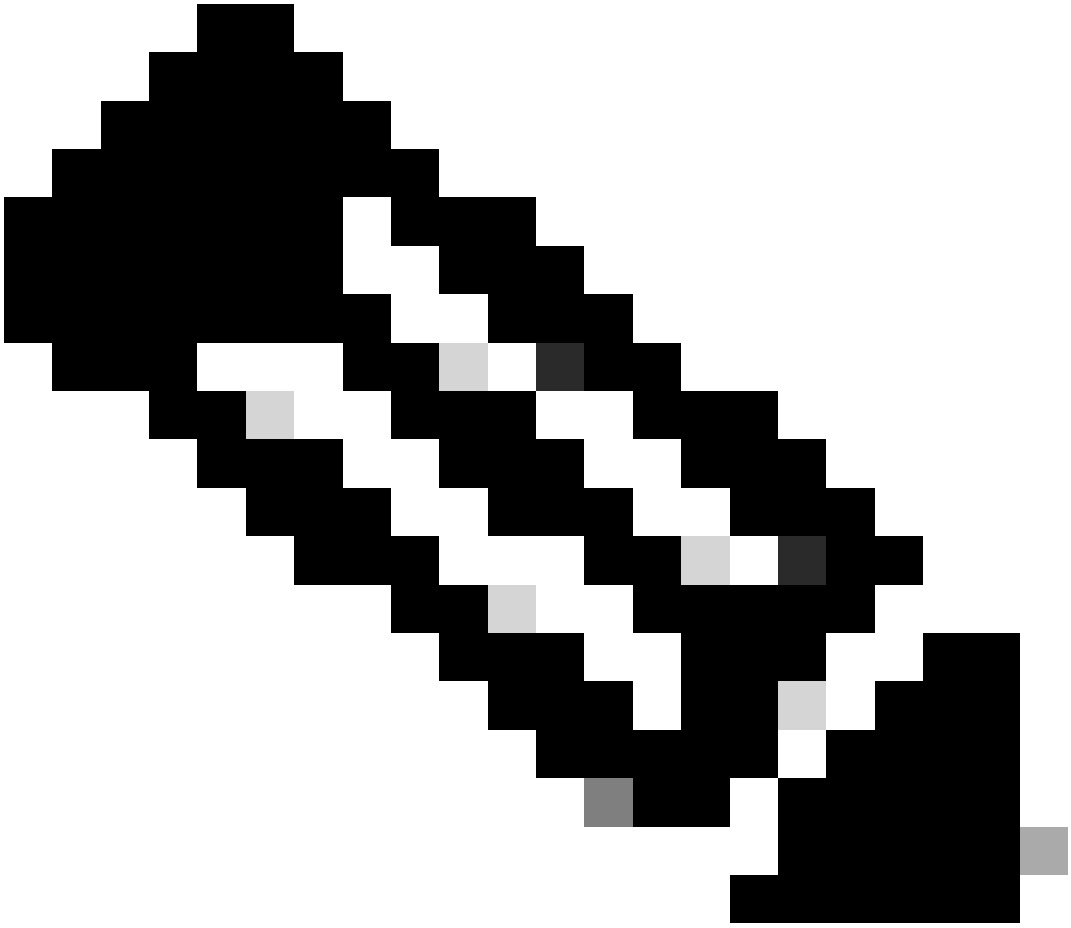
especifica mediante el elemento <ad.controller.https.trustStorePath> en el archivo de configuración del agente analytics-agent.properties, el agente carga ese almacén de confianza.
    - Si no se especifica en thead.controller.https.trustStorePath, se carga el almacén de confianza de Java predeterminado de la JVM que se está instrumentando, <JRE_HOME>/lib/security/cacerts (la contraseña predeterminada changeit)
    - Si no se especifica en ad.controller.https.trustStorePath y el agente de análisis se está utilizando como una extensión de agente de equipo, se cargará el almacén de confianza utilizado por el agente de equipo.

- Agente DotNet

    - Para Windows:
        - Vaya a la vista de instalación del certificado en Ejecutar> MMC.exe> seleccione Archivo en la barra de herramientas y seleccione Agregar o quitar complemento.
        - Se abre la ventana Agregar o quitar complementos, seleccione Certificados> Haga clic en Agregar. Se abre la ventana de complemento de certificados. Seleccione Cuenta de equipo> Elija Local u Otro equipo como corresponda >ClickFinish>OK.
        - Expanda Certificados (Equipo local) > Seleccione la carpeta Entidad emisora de certificados raíz de confianza y expanda para mostrar la carpeta Certificados.
        - Haga doble clic en la carpeta Certificados y observe la lista de certificados de confianza existentes. Identifique si están presentes los certificados raíz global G2 de DigiCert y los certificados raíz de IdenTrust; de lo contrario, importe los certificados que faltan.

    - Para Linux:

        - La ubicación del almacén de confianza varía entre las distribuciones de Linux. Las ubicaciones comunes incluyen:/etc/ssl/certs (SO como CentOS/RHEL/Debian)



Nota: Si los certificados DigiCert Global Root G2 o IdenTrust faltan en todas estas ubicaciones comprobadas, debe agregarlos. Consulte los pasos mencionados en "Paso 3. Importar certificados al almacén de confianza" para importar los certificados al almacén de confianza.

Paso 3. Importar certificados al almacén de confianza

- Java, base de datos, equipo o agente de análisis
    - Abra su terminal o símbolo del sistema y utilice este comando keytool para importar DigiCert Global Root G2 & IdenTrust Root Certificates.

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

```
-file

 -keystore

  -storepass
```

Sustituir:

- : Un alias único (por ejemplo, digicertglobalrootg2, identrustcoomercial).
- : Ruta al archivo de certificado (por ejemplo, /home/username/Downloads/DigiCertGlobalRootG2.crt).
- : Ruta al archivo de almacén de confianza del agente (por ejemplo, /opt/appdynamics/agent/ver25.x.x.x/conf/cacerts.jks).
- : Contraseña de TrustStore (predeterminado: changeit, a menos que sea personalizado).

- Ejemplo para importar certificado raíz global G2 de DigiCert.

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

- Ejemplo de importación de certificado raíz comercial de IdenTrust.

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

- Agente DotNet
  - Para Windows:
    - Vaya a la vista de instalación del certificado en Ejecutar> MMC.exe> seleccione Archivo en la barra de herramientas y seleccione Agregar o quitar complemento.
    - Se abre la ventana Agregar o quitar complementos, seleccione Certificados>

Haga clic en Agregar. Se abre la ventana de complemento de certificados. Seleccione Cuenta de equipo> Elija Local u Otro equipo como corresponda >ClickFinish>OK.

- Expanda Certificados (Equipo local) > Seleccione la carpeta Entidad emisora de certificados raíz de confianza y expanda para mostrar la carpeta Certificados.
- Haga clic con el botón derecho del mouse en la carpeta Certificados y seleccione Todas las tareas > Importar.Se abre el Asistente para importación de certificados, siga las instrucciones y agregue el archivo que faltaCertificado Global Root G2 de DigiCert y/o Certificado Root de IdenTrust.

- Para Linux:
  - Copie los archivos descargados del DigiCert Global Root G2 & IdenTrust Root Certificate en el directorio de almacén de confianza identificado.
  - Actualice el almacén de confianza ejecutando el comando.

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

Paso 4. Verificar la importación

- Java, base de datos, equipo o agente de análisis
  - Para comprobar que los certificados se agregaron correctamente, ejecute el comando:

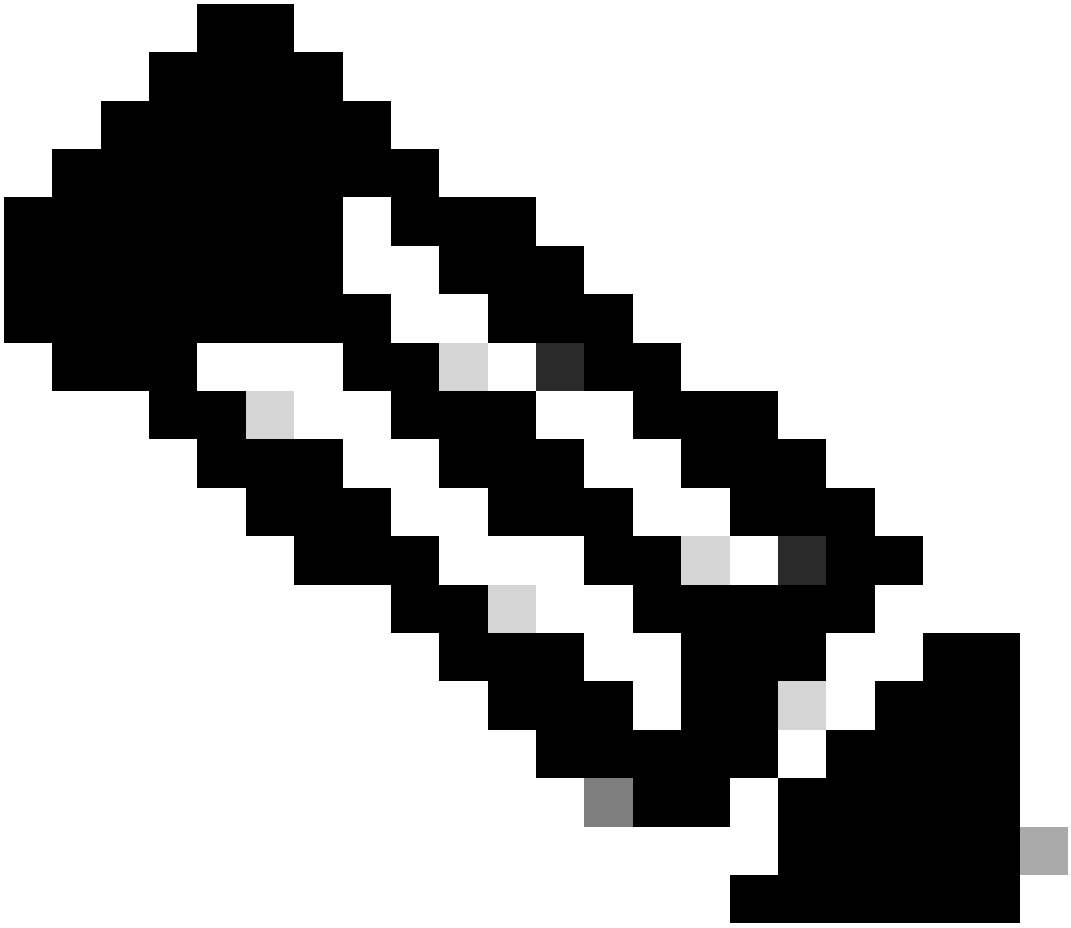
```
keytool -list -v -keystore

            -storepass

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

Sustituir:

- `<agent_truststore_path>`: Ruta al archivo de almacén de confianza del agente.
- `<truststore_password>`: La contraseña del almacén de confianza.



Nota: Asegúrese de que tanto DigiCert Global Root G2 como IdenTrust Commercial Root CA 1 aparezcan en el resultado.

- Agente DotNet
    - Para Windows:
        - Vaya a la vista de instalación del certificado en Ejecutar> MMC.exe> seleccione Archivo en la barra de herramientas y seleccione Agregar o quitar complemento.
        - Se abre la ventana Agregar o quitar complementos, seleccione Certificados> Haga clic en Agregar. Se abre la ventana de complemento de certificados. Seleccione Cuenta de equipo> Elija Local u Otro equipo como corresponda >ClickFinish>OK.
        - Expanda Certificados (Equipo local) > Seleccione la carpeta Entidad emisora de certificados raíz de confianza y expanda para mostrar la carpeta Certificados.
        - Haga doble clic en la carpeta Certificados y debe ver los certificados raíz global G2 de DigiCert y raíz de IdenTrust.

- Para Linux:
  - Ejecute el comando y verifique siDigiCert Global Root G2 & IdenTrust Root Certificate existe:

```
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
```

Paso 5. Reinicie el agente

Por último, reinicie el agente de AppDynamics. Esto permite que los cambios surtan efecto.

Información Relacionada

Asesoramiento de soporte: Adición de certificados SSL raíz de DigiCert e IdenTrust a almacenes de confianza de agentes

¿Necesita más asistencia?

Si tiene alguna pregunta o experimenta algún problema, cree un ticket de soporte con estos datos:

- Registros del agente.
- Detalles de la ubicación del almacén de confianza y certificados agregados.
- Mensajes de error encontrados.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).