Risolvi problemi SSL/TLS di AppDynamics dopo l'aggiornamento di DigiCert Root G2

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi di attendibilità dei certificati SSL (Secure Socket Layer)/ TLS (Transport Layer Security) negli agenti AppDynamics.

Prerequisiti

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

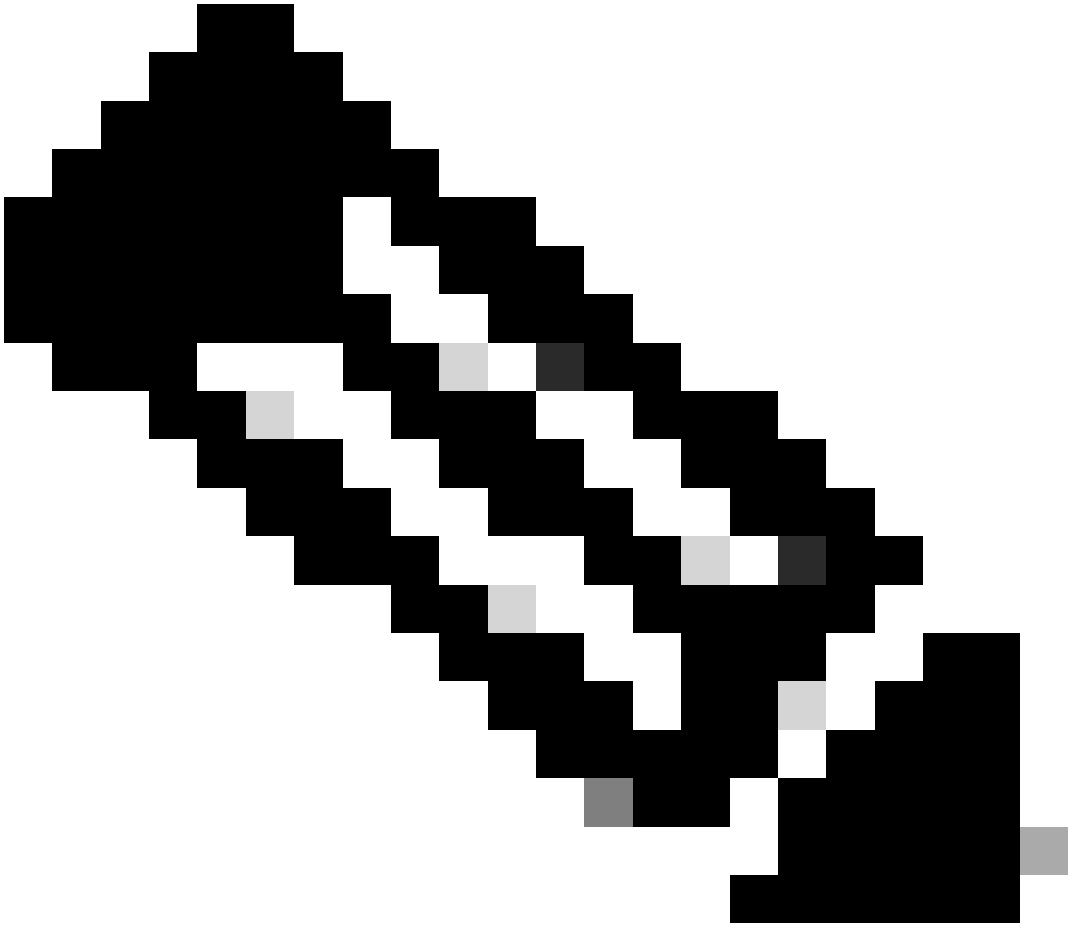
In questo documento viene descritto come risolvere i problemi di attendibilità dei certificati SSL (Secure Socket Layer)/ TLS (Transport Layer Security) negli agenti AppDynamics dopo la recente migrazione dalla CA radice globale DigiCert alla radice globale DigiCert G2.

Fornisce procedure dettagliate per garantire la corretta configurazione e il ripristino della connettività senza problemi.

Nel 2023 DigiCert ha iniziato la transizione al certificato di firma DigiCert Global Root G2 per il rilascio di certificati TLS/SSL pubblici. Questa modifica è stata richiesta da Mozilla ha aggiornato il criterio di attendibilità, che impone l'aggiornamento dei certificati radice ogni 15 anni, e diffidando i vecchi certificati a partire dal 2025.

Il nuovo certificato di firma utilizza l'algoritmo SHA-256 più sicuro, sostituendo lo standard SHA-1 precedente. Nell'ambito di questa transizione, AppDynamics ha aggiornato i certificati SSL per il dominio .saas.appdynamics.com per utilizzare i certificati di seconda generazione in 2025-06-10.

A causa di questo aggiornamento, alcuni agenti dell'applicazione hanno perso la connettività con i controller SaaS a causa della loro incapacità di riconoscere il nuovo certificato. Per garantire una connettività ininterrotta, è fondamentale aggiornare l'archivio di attendibilità dell'agente AppDynamics in modo da includere i nuovi certificati DigiCert Global Root G2 e IdenTrust.



Nota: Questa modifica riguarda principalmente gli agenti che utilizzano il truststore personalizzato o una versione molto vecchia di OS/java in cui il certificato richiesto non è incluso nel truststore predefinito OS/Java.

Problema

Si è verificato un problema di connettività tra gli agenti AppDynamics e il controller e nei log vengono visualizzati errori relativi alla configurazione o alla comunicazione SSL.

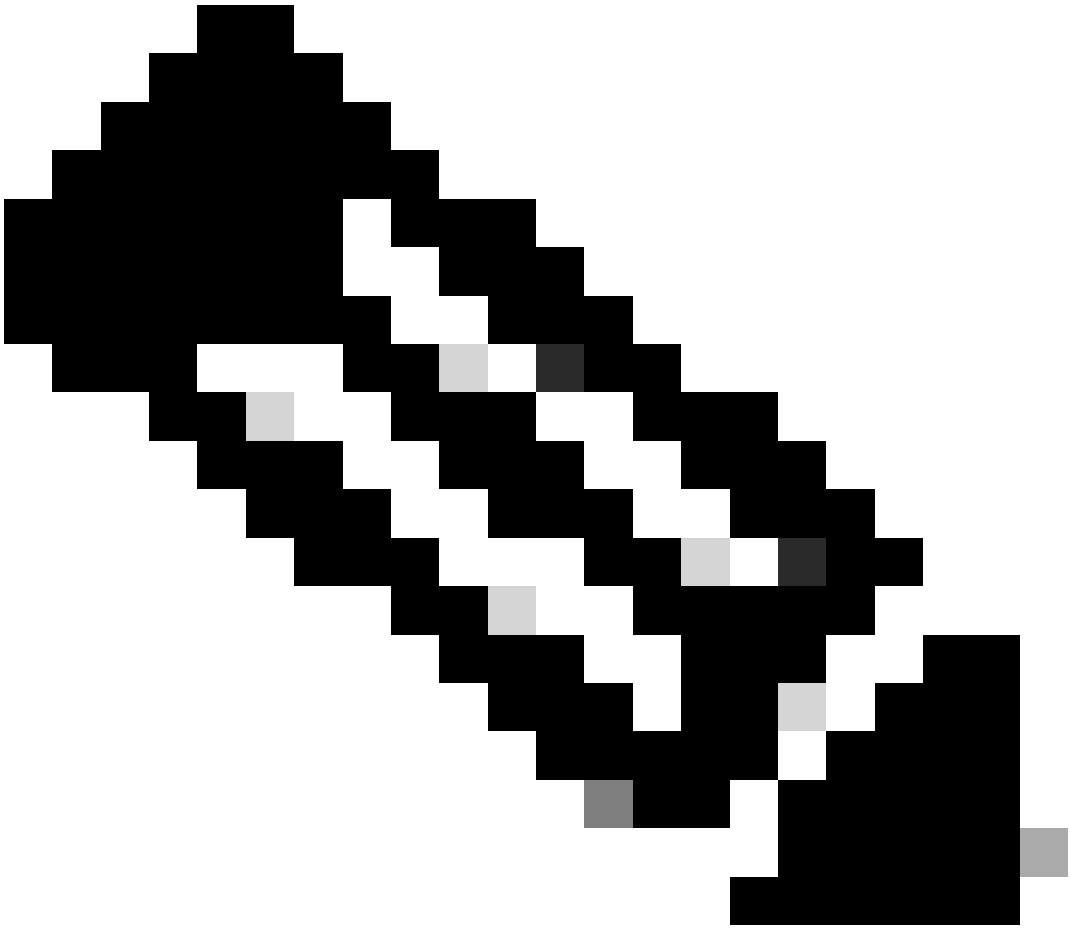
Messaggio di errore di esempio nei registri: "Compilazione del percorso PKIX non riuscita: xxxx impossibile trovare un percorso di certificazione valido per la destinazione richiesta durante il tentativo di convalida"

Soluzione

Passaggio 1. Scarica certificati

- DigiCert Global Root G2:
  - Visitare il sito Certificati autorità radice attendibili DigiCert
  - Cercare "DigiCert Global Root G2" e scaricare il certificato.
- IdenTrust:
  - Vai alla radice commerciale IdenTrust CA 1
  - Copiare il contenuto del certificato e salvarlo come file, ad esempio Identrustcommercial.cer o Identrustcommercial.pem

Passaggio 2. Identificare la posizione dell'archivio trust



Nota: Percorso Truststore necessario nel passaggio 3. Importare i certificati nel Truststore

- Agente Java, database o computer
  - Proprietà Truststore argomento JVM

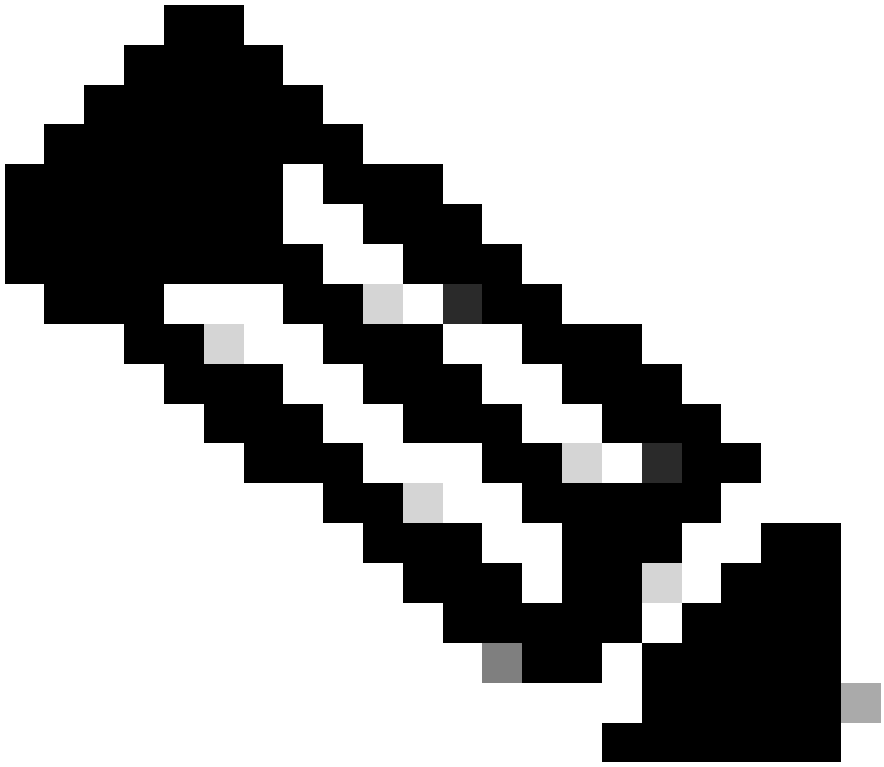
1. Verificare se la proprietà -Djavax.net.ssl.trustStore è impostata come argomenti JVM all'avvio dell'agente.
2. Se questa proprietà è impostata, controllare il file keystore specificato da questa proprietà per verificare che includa entrambi i certificati (certificati radice globale DigiCert G2 e certificati radice IdenTrust).
   Se la proprietà non è impostata, procedere al passaggio successivo.

- XML informazioni controller

1. L'agente può essere configurato per utilizzare il keystore definito nel file controller-info.xml nella directory di configurazione dell'agente.
2. Verificare l'impostazione controller-keystore-filename.
3. Se presente, esaminare il file keystore specificato per verificare che entrambi i certificati siano inclusi.
   (Se non viene trovato, procedere con il passaggio successivo).

- File cacerts.jks dell'agente

1. Cercare un file denominato cacerts.jksnella cartella della directory di installazione dell'agente.
2. Esaminare il file per verificare che entrambi i certificati siano inclusi.
   (Se non viene trovato, procedere con il passaggio successivo).

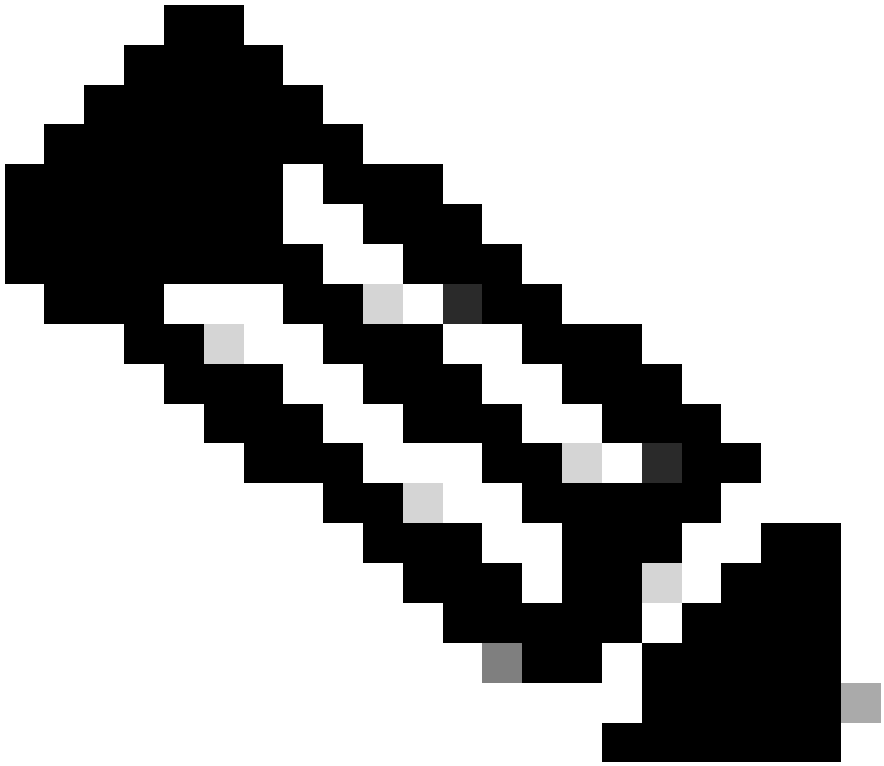


Nota: Directory di installazione dell'agente

Per Java Agent: AGENT_HOME/verxxx/conf o AGENT_HOME/conf

Per il computer o l'agente DB: AGENT_HOME/conf

- Truststore predefinito JRE
  1. Se non viene trovata alcuna delle configurazioni precedenti, come fallback, l'agente utilizza il truststore predefinito di JRE, in genere disponibile in JRE_HOME/lib/security/cacerts.
  2. Esaminare il file per verificare che i certificati siano inclusi.



Nota: Se si utilizza IBM Websphere o IBM Websphere Liberty Profile, JRE_HOME si trova rispettivamente all'interno di AppServer o Liberty Directory nella directory di installazione di Websphere, ovvero IBM_WEBSPHERE_HOME/AppServer/java/ o IBM_WEBSPHERE_HOME/Liberty/java/

- Agente di analisi
  - Verificare se il percorso (incluso il nome) dell'agente truststore è specificato

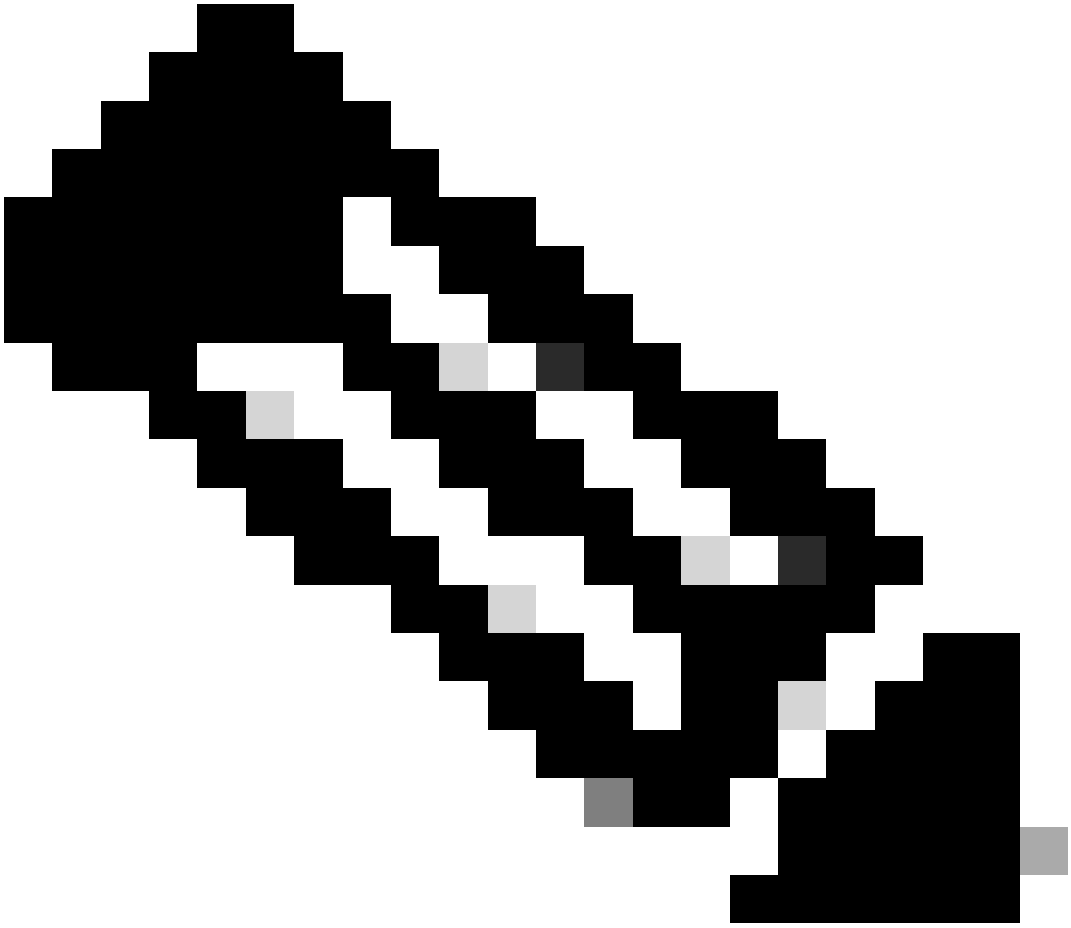
utilizzando l'elemento <ad.controller.https.trustStorePath> nel file di configurazione dell'agente analytics-agent.properties, quindi l'agente carica tale trustore.
    - Se non specificato in thead.controller.https.trustStorePath, carica il truststore Java predefinito della JVM instrumentata, <JRE_HOME>/lib/security/cacerts (modifica password predefinita)
    - Se non specificato in ad.controller.https.trustStorePath e l'agente di analisi viene utilizzato come estensione dell'agente computer, carica l'archivio trust utilizzato dall'agente computer.

- Agente DotNet

    - Per Windows:
        - Passare alla visualizzazione dell'installazione del certificato passando a Esegui> MMC.exe> selezionare File dalla barra degli strumenti e selezionare Aggiungi/Rimuovi snap-in.
        - Viene visualizzata la finestra Aggiungi o rimuovi snap-in. Selezionare Certificati> Fare clic su Aggiungi. Verrà visualizzata la finestra snap-in Certificato. Selezionare Account computer> Scegliere il computer locale o un altro computer di conseguenza >Fare clic su Fine>OK.
        - Espandere Certificati (computer locale) > Selezionare la cartella Autorità di certificazione radice attendibile ed espandere per visualizzare la cartella Certificati.
        - Fare doppio clic sulla cartella Certificati e osservare l'elenco dei certificati attendibili esistenti. Identificare se sono presenti i certificati radice globale DigiCert G2 e IdenTrust altrimenti importare i certificati mancanti.

    - Per Linux:

        - La posizione dell'archivio trust varia tra le distribuzioni Linux. Le posizioni comuni includono:/etc/ssl/certs (sistema operativo come CentOS/RHEL/Debian)



Nota: Se i certificati DigiCert Global Root G2 o IdenTrust non sono presenti in tutti questi percorsi controllati, è necessario aggiungerli. Per importare i certificati nel truststore, fare riferimento alla procedura descritta nel passaggio 3 Importazione dei certificati nel Truststore.

Passaggio 3. Importazione dei certificati nell'archivio protetto

- Agente Java, database, computer o analisi
    - Aprire il terminale o il prompt dei comandi e utilizzare questo comando keytool per importare i certificati radice globali DigiCert G2 e IdenTrust.

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

```
-file

 -keystore

  -storepass
```

Sostituisci:

- : Alias univoco, ad esempio digicertglobalrootg2, identrustcoomercial.
- : Percorso del file del certificato (ad esempio, /home/username/Downloads/DigiCertGlobalRootG2.crt).
- : Percorso del file truststore dell'agente (ad esempio, /opt/appdynamics/agent/ver25.x.x.x/conf/cacerts.jks).
- : Password Truststore (impostazione predefinita: changeit, se non personalizzato).

- Esempio per l'importazione del certificato radice globale DigiCert G2.

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

- Esempio di importazione del certificato radice commerciale IdenTrust.

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

- Agente DotNet
  - Per Windows:
    - Passare alla visualizzazione dell'installazione del certificato passando a Esegui> MMC.exe> selezionare File dalla barra degli strumenti e selezionare Aggiungi/Rimuovi snap-in.
    - Viene visualizzata la finestra Aggiungi o rimuovi snap-in. Selezionare Certificati>

Fare clic su Aggiungi. Verrà visualizzata la finestra snap-in Certificato. Selezionare Account computer> Scegliere il computer locale o un altro computer di conseguenza >Fare clic su Fine>OK.
- Espandere Certificati (computer locale) > Selezionare la cartella Autorità di certificazione radice attendibile ed espandere per visualizzare la cartella Certificati.
- Fare clic con il pulsante destro del mouse sulla cartella Certificati e selezionare All Tasks > Import. Certificate Import Wizard (Tutte le attività > Importazione guidata certificati). Verrà visualizzata l'importazione guidata dei certificati, verranno visualizzate le istruzioni e verranno aggiunti i certificati mancantiCertificato radice globale DigiCert G2 e/o Certificato radice IdenTrust.

- Per Linux:
  - Copiare i file dei certificati radice globali DigiCert G2 e IdenTrust scaricati nella directory identificata dell'archivio attendibile.
  - Aggiornare l'archivio attendibile eseguendo il comando.

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

Passaggio 4. Verifica dell'importazione

- Agente Java, database, computer o analisi
  - Per verificare che i certificati siano stati aggiunti correttamente, eseguire il comando:

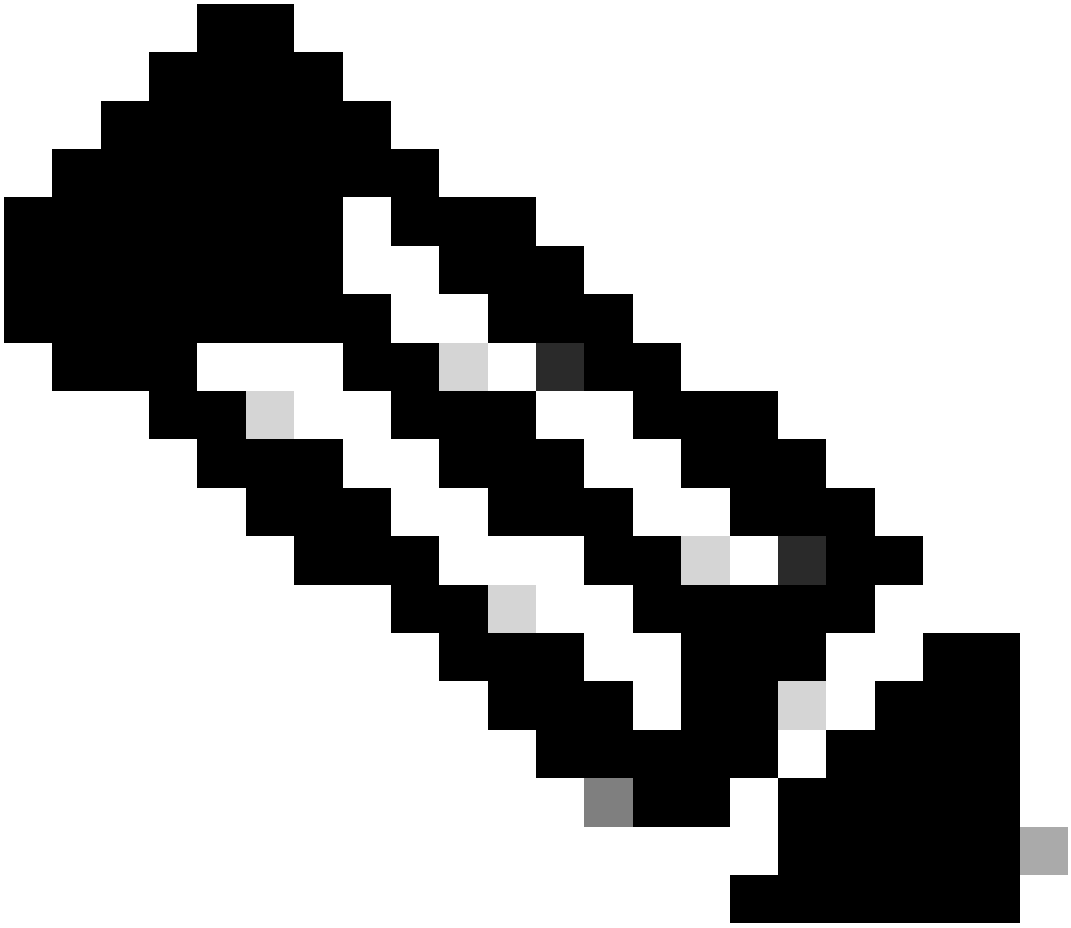
```
keytool -list -v -keystore

            -storepass

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

Sostituisci:

- `<agent_truststore_path>`: Percorso del file truststore dell'agente.
- `<truststore_password>`: La password del truststore.



Nota: Assicurarsi che nell'output vengano visualizzate le directory radice globale DigiCert G2 e radice commerciale IdenTrust CA 1.

- Agente DotNet
    - Per Windows:
        - Passare alla visualizzazione dell'installazione del certificato passando a Esegui> MMC.exe> selezionare File dalla barra degli strumenti e selezionare Aggiungi/Rimuovi snap-in.
        - Viene visualizzata la finestra Aggiungi o rimuovi snap-in. Selezionare Certificati> Fare clic su Aggiungi. Verrà visualizzata la finestra snap-in Certificato. Selezionare Account computer> Scegliere il computer locale o un altro computer di conseguenza >Fare clic su Fine>OK.
        - Espandere Certificati (computer locale) > Selezionare la cartella Autorità di certificazione radice attendibile ed espandere per visualizzare la cartella Certificati.

- Fare doppio clic sulla cartella Certificati per visualizzare i certificati radice globale DigiCert G2 e IdenTrust.

- Per Linux:
  - Eseguire il comando e verificare se esistono certificati radice globale DigiCert G2 e IdenTrust:

```
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
```

Passaggio 5. Riavviare l'agente

Riavviare infine l'agente AppDynamics. In questo modo le modifiche diventano effettive.

Informazioni correlate

Consulenza per il supporto: Aggiunta di certificati SSL radice DigiCert e IdenTrust agli archivi attendibili dell'agente

Ulteriori informazioni

In caso di domande o di problemi, creare un biglietto di assistenza con i seguenti dettagli:

- Registra dall'agente.
- Dettagli del percorso dell'archivio attendibile e dei certificati aggiunti.
- Rilevati messaggi di errore.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).