

Resolver Problemas de SSL/TLS do AppDynamics após a Atualização da Raiz G2 do DigiCert

Contents

[Introdução](#)

[Pré-requisitos](#)

[Componentes Usados](#)

[Informações de Apoio](#)

[Problema](#)

[Solução](#)

[Etapa 1. Fazer Download dos Certificados](#)

[Etapa 2. Identificar o local do armazenamento confiável](#)

[Java, agente de banco de dados ou máquina](#)

[Agente de análise](#)

[Agente DotNet](#)

[Etapa 3. Importar Certificados para o Repositório Confiável](#)

[Java, banco de dados, máquina ou agente analítico](#)

[Agente DotNet](#)

[Etapa 4. Verificar a Importação](#)

[Java, banco de dados, máquina ou agente analítico](#)

[Agente DotNet](#)

[Etapa 5. Reiniciar o Agente](#)

[Informações Relacionadas](#)

[Precisa de mais assistência?](#)

Introdução

Este documento descreve como resolver problemas de confiança de certificado SSL (Secure Socket Layer)/ TLS (Transport Layer Security) em Agentes do AppDynamics.

Pré-requisitos

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

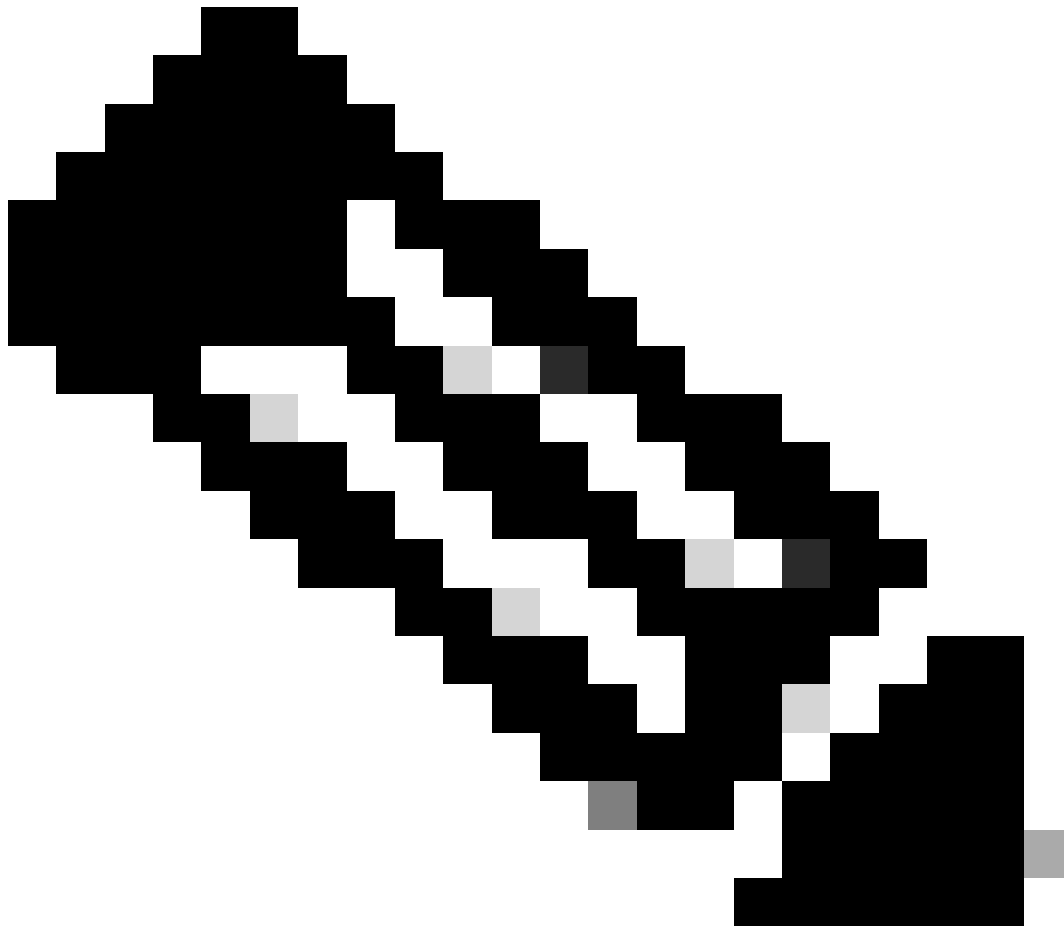
Este documento descreve como resolver problemas de confiança de certificado SSL (Secure Socket Layer)/TLS (Transport Layer Security) em Agentes do AppDynamics após a migração recente da CA raiz global DigiCert para a raiz global DigiCert G2.

Ele fornece etapas detalhadas para garantir a configuração apropriada e restaurar a conectividade contínua.

Em 2023, a DigiCert iniciou a transição para o certificado de assinatura G2 da raiz global da DigiCert para emissão de certificados TLS/SSL públicos. Essa mudança foi motivada pela política de confiança atualizada da Mozilla, que determina que os certificados raiz sejam atualizados a cada 15 anos e desconfie de certificados mais antigos a partir de 2025.

O novo certificado de assinatura emprega o algoritmo SHA-256 mais seguro, substituindo o padrão SHA-1 mais antigo. Como parte dessa transição, a AppDynamics atualizou seus certificados SSL para o domínio `.saas.appdynamics.com` para utilizar os certificados de segunda geração em 10 de junho de 2025.

Essa atualização fez com que alguns agentes de aplicativos perdessem a conectividade com controladores SaaS devido à sua incapacidade de reconhecer o novo certificado. Para garantir conectividade ininterrupta, é crucial atualizar o repositório de confiança do agente AppDynamics para incluir os novos certificados DigiCert Global Root G2 e IdenTrust.



Note: Essa alteração afeta principalmente os agentes que estão usando o armazenamento confiável personalizado ou usando uma versão muito antiga do OS/java, em que o certificado necessário não está incluído no armazenamento confiável padrão do OS/Java.

Problema

Há um problema de conectividade entre os Agentes do AppDynamics e o Controlador, e os logs estão mostrando erros relacionados à configuração ou comunicação SSL.

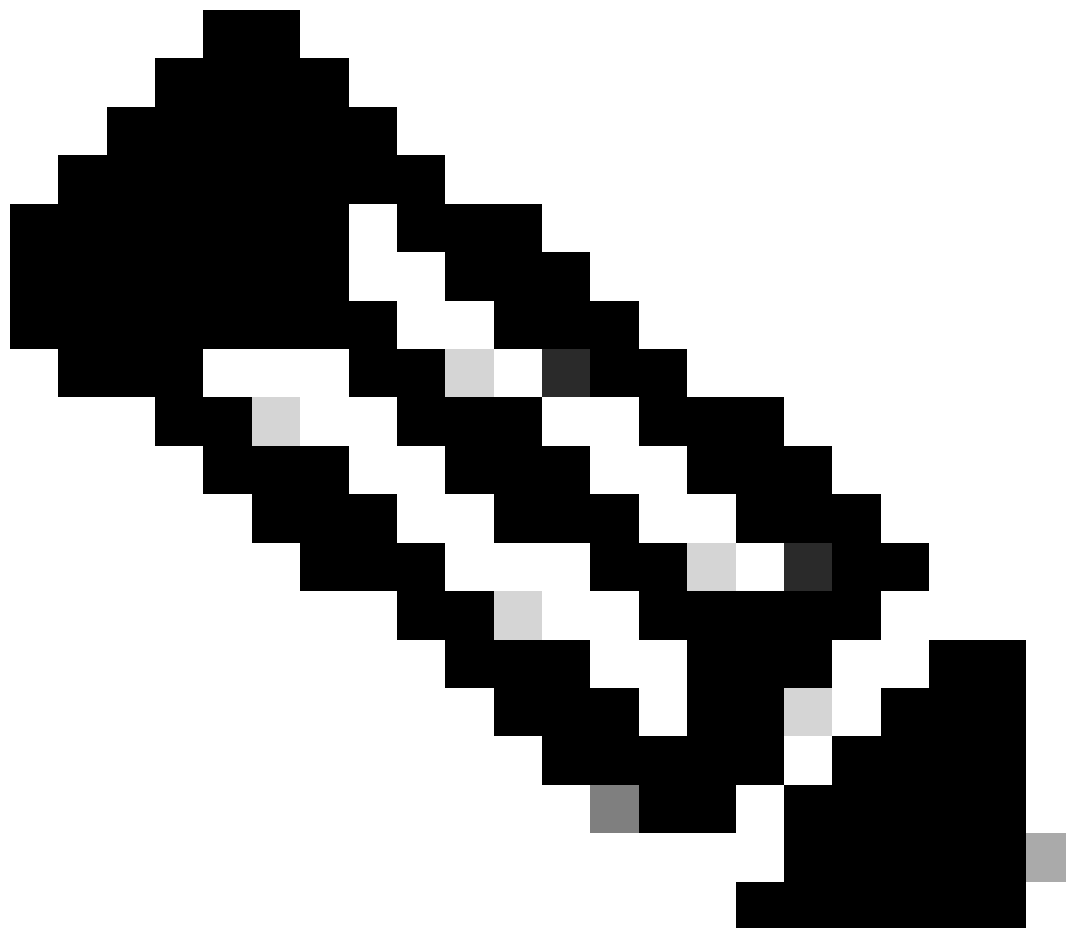
Exemplo de mensagem de erro nos logs: "Falha na criação do caminho PKIX: xxxx: não é possível encontrar um caminho de certificação válido para o destino solicitado tentando a validação"

Solução

Etapa 1. Baixar certificados

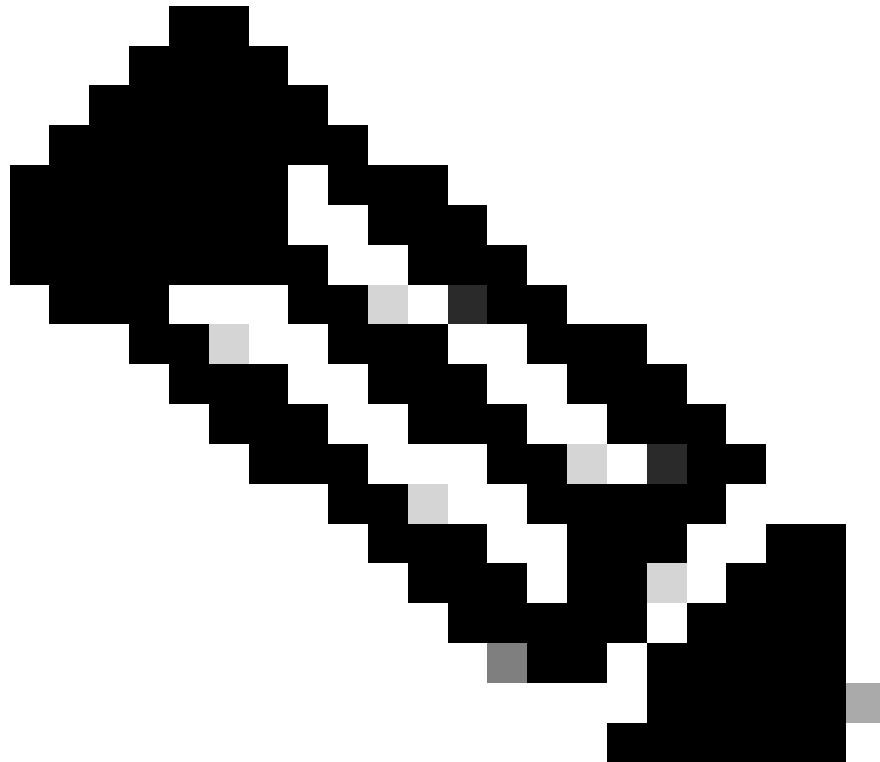
- Raiz Global G2 do DigiCert:
 - Visite [Certificados de Autoridade Raiz Confiável DigiCert](#)
 - Procure "DigiCert Global Root G2" e baixe o certificado.
- IdenTrust:
 - Vá para [IdenTrust Commercial Root CA 1](#)
 - Copie o conteúdo do certificado e salve-o como um arquivo (por exemplo, IdenTrustcommercial.cer ou IdenTrustcommercial.pem)

Etapa 2. Identificar o local do armazenamento confiável



Note: O local do armazenamento confiável é necessário na Etapa 3. Importar certificados para o armazenamento confiável

- Java, agente de banco de dados ou máquina
 - Propriedade Truststore do Argumento JVM
 1. Verifique se a propriedade -Djavax.net.ssl.trustStore está definida como um argumento JVM ao iniciar o agente.
 2. Se esta propriedade estiver definida, inspecione o arquivo de armazenamento de chaves especificado por esta propriedade para confirmar se ela inclui ambos os certificados (certificados raiz global G2 DigiCert e raiz IdenTrust).
(Se a propriedade não estiver definida, vá para a próxima etapa.)
 - XML de Informações do Controlador
 1. O Agente pode ser configurado para usar o armazenamento de chaves definido no arquivo controller-info.xml no diretório de configuração do agente.
 2. Verifique a configuração controller-keystore-filename.
 3. Se presente, inspecione o arquivo de armazenamento de chaves especificado para confirmar se ambos os certificados estão incluídos.
(Se não for encontrado, vá para a próxima etapa.)
 - Arquivo cacerts.jks do agente
 1. Procure um arquivo chamado cacerts.jks dentro da pasta conf do diretório de instalação do agente.
 2. Inspecione este arquivo para verificar se ambos os certificados estão incluídos.
(Se não for encontrado, vá para a próxima etapa.)

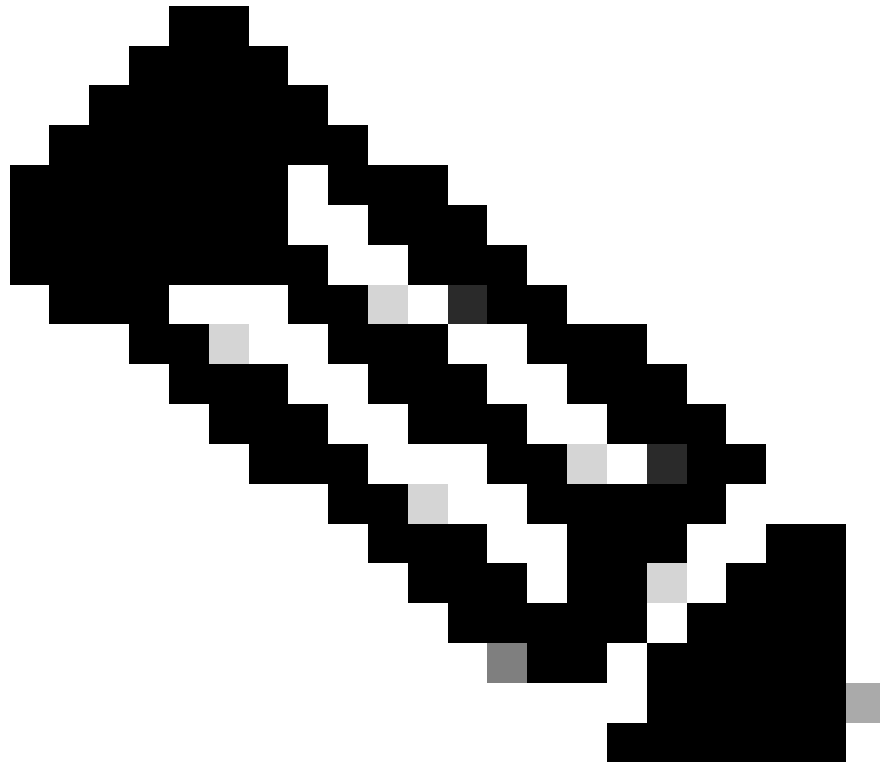


Note: Diretório de instalação do agente

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

Para Máquina ou Agente de BD: AGENT_HOME/conf

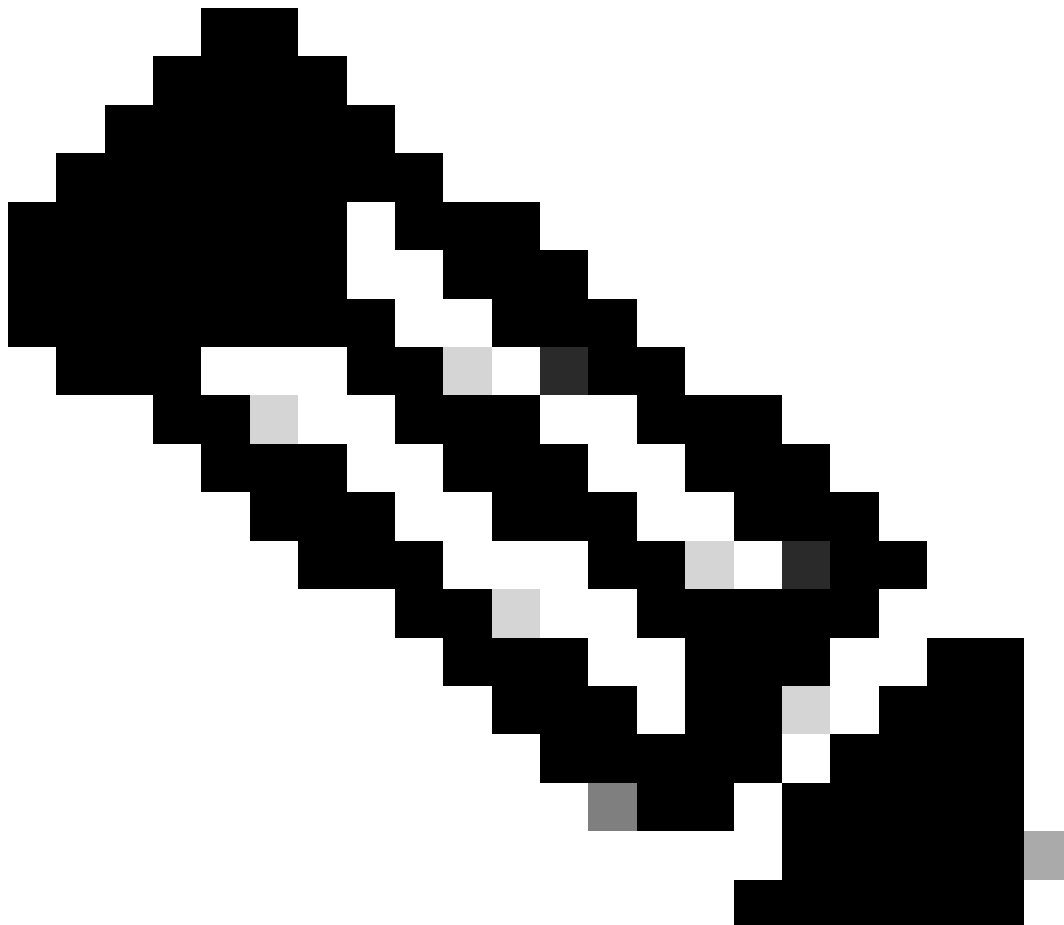
-
- Repositório confiável padrão do JRE
 1. Se nenhuma das configurações anteriores for encontrada, como fallback, o agente usará o armazenamento confiável padrão do JRE, normalmente localizado em JRE_HOME/lib/security/cacerts.
 2. Inspeccione este arquivo para garantir que os certificados sejam incluídos.



Note: Se você estiver usando o IBM Websphere ou o IBM Websphere Liberty Profile, o JRE_HOME estará dentro do AppServer ou do Liberty Directory no diretório de instalação do Websphere, respectivamente, ou seja, IBM_WEBSPHERE_HOME/AppServer/java/ ou IBM_WEBSPHERE_HOME/Liberty/java/

- Agente de análise
 - Verifique se o caminho (incluindo o nome) do armazenamento confiável do agente é especificado usando o elemento `<ad.controller.https.trustStorePath>` no arquivo de configuração do agente [analytics-agent.properties](#) e o agente carrega esse armazenamento confiável.
 - Se não for especificado em `thead.controller.https.trustStorePath`, ele carregará o Java truststore padrão da JVM que está sendo instrumentada, `<JRE_HOME>/lib/security/cacerts` (senha padrão changeit)
 - Se não for especificado no `ad.controller.https.trustStorePath` e o agente de análise estiver sendo usado como uma extensão de agente de Máquina, ele carregará o armazenamento confiável usado pelo agente de máquina.
- Agente DotNet

- Para Windows:
 - Navegue para a visualização de instalação do certificado indo para Run> MMC.exe> selectFile na barra de ferramentas e selectAdd/Remove Snap-in.
 - A janela Adicionar ou remover snap-ins é aberta, selecione Certificados> Clique em Adicionar. A janela do snap-in de certificado é aberta. Selecione Conta do Computador> Escolha Local ou Outro Computador de acordo >ClickFinish>OK.
 - Expanda Certificates (Local Computer) > Selecione a pasta Trusted Root Certification Authority e expanda para mostrar a pasta Certificates.
 - Clique duas vezes na pasta Certificados e observe a lista de certificados confiáveis existentes. Identifique se os certificados raiz global DigiCert G2 e raiz IdenTrust estão presentes; caso contrário, importe os certificados ausentes.
 - Para Linux:
 - O local do armazenamento confiável varia entre as distribuições Linux. Locais comuns incluem:/etc/ssl/certs (SO como CentOS/RHEL/Debian)
-



Note: Se os certificados Global Root G2 ou IdenTrust do DigiCert estiverem ausentes em todos esses locais marcados, será necessário adicioná-los. Consulte as etapas mencionadas na "Etapa 3. Importar certificados para o armazenamento confiável" para importar os certificados para o armazenamento confiável.

Etapa 3. Importar Certificados para o Repositório Confiável

- Java, banco de dados, máquina ou agente analítico
 - Abra o terminal ou o prompt de comando e use este comando keytool para importar Certificados Raiz Global DigiCert G2 & IdenTrust Raiz.

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

```
-file
```

```
-keystore
```

```
-storepass
```

Substituir:

- : Um alias exclusivo (por exemplo, digicertglobalrootg2, identrustcoomercial).
- : Caminho para o arquivo de certificado (por exemplo, /home/username/Downloads/DigiCertGlobalRootG2.crt).
- : Caminho para o arquivo de armazenamento confiável do agente (por exemplo, /opt/appdynamics/agent/ver25.x.x.x/conf/cacerts.jks).
- : Senha do armazenamento confiável (padrão: changeit, a menos que personalizado).

- Exemplo para importar o certificado G2 raiz global do DigiCert.

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

- Exemplo para importar o certificado IdenTrust Commercial Root.

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

- Agente DotNet

- Para Windows:
 - Navegue para a visualização de instalação do certificado indo para Run> MMC.exe> selectFile na barra de ferramentas e selectAdd/Remove Snap-in.
 - A janela Adicionar ou remover snap-ins é aberta, selecione Certificados> Clique em Adicionar. A janela do snap-in de certificado é aberta. Selecione Conta do Computador> Escolha Local ou Outro Computador de acordo >ClickFinish>OK.
 - Expanda Certificates (Local Computer) > Selecione a pasta Trusted Root Certification Authority e expanda para mostrar a pasta Certificates.
 - Clique com o botão direito do mouse na pasta Certificados e selecione Todas as Tarefas > Importar. O Assistente de Importação de Certificados será aberto, siga as instruções e adicione os Certificado G2 raiz global DigiCert e/ou certificado raiz IdenTrust.
- Para Linux:
 - Copie os arquivos baixados do DigiCert Global Root G2 & IdenTrust Root Certificate para o diretório de armazenamento de confiança identificado.
 - Atualize o Repositório Confiável executando o comando.

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

Etapa 4. Verificar a Importação

- Java, banco de dados, máquina ou agente analítico
 - Para verificar se os certificados foram adicionados com êxito, execute o comando:

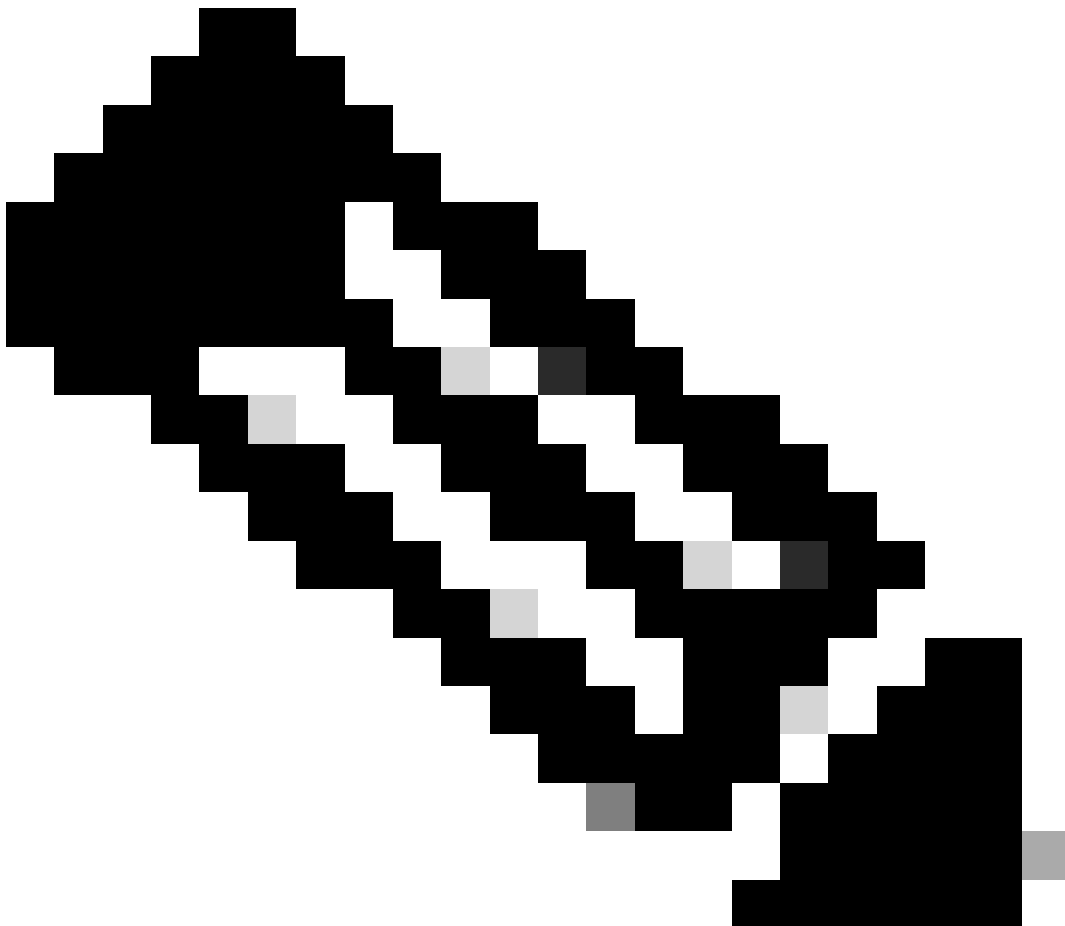
```
keytool -list -v -keystore
```

-storepass

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

Substituir:

- <agent_truststore_path>: Caminho para o arquivo de armazenamento confiável do agente.
 - <truststore_password>: A senha do armazenamento confiável.
-



Note: Certifique-se de que DigiCert Global Root G2 e IdenTrust Commercial Root CA 1 apareçam na saída.

- Agente DotNet
 - Para Windows:
 - Navegue para a visualização de instalação do certificado indo para Run> MMC.exe> selectFile na barra de ferramentas e selectAdd/Remove Snap-in.
 - A janela Adicionar ou remover snap-ins é aberta, selecione Certificados> Clique em Adicionar. A janela do snap-in de certificado é aberta. Selecione Conta do Computador> Escolha Local ou Outro Computador de acordo >ClickFinish>OK.
 - Expanda Certificates (Local Computer) > Selecione a pasta Trusted Root Certification Authority e expanda para mostrar a pasta Certificates.
 - Clique duas vezes na pasta Certificates e você deve ver os certificados raiz global DigiCert G2 e raiz IdenTrust lá.
 - Para Linux:
 - Execute o comando e verifique se o Certificado raiz global G2 e IdenTrust do DigiCert 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
```

Etapa 5. Reiniciar o Agente

Por fim, reinicie o agente do AppDynamics. Isso permite que as alterações entrem em vigor.

Informações Relacionadas

[Consultoria de suporte: Adicionando certificados SSL de raiz DigiCert e IdenTrust a repositórios confiáveis do agente](#)

Precisa de mais assistência?

Se você tiver alguma dúvida ou estiver tendo problemas, crie um tíquete [de suporte](#) com estes detalhes:

- Logs do agente.
- Detalhes do local de armazenamento confiável e certificados adicionados.
- Todas as mensagens de erro encontradas.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.