



Gerenciando certificado SSL OnCommand Workflow Automation

OnCommand Workflow Automation

NetApp
October 09, 2025

Índice

Gerenciando certificado SSL OnCommand Workflow Automation	1
Substitua o certificado SSL padrão do Workflow Automation	1
Criar uma solicitação de assinatura de certificado para o Workflow Automation.....	2

Gerenciando certificado SSL OnCommand Workflow Automation

Você pode substituir o certificado SSL padrão OnCommand Workflow Automation (WFA) por um certificado autoassinado ou um certificado assinado por uma Autoridade de Certificação (CA).

O certificado SSL WFA auto-assinado padrão é gerado durante a instalação do WFA. Ao atualizar, o certificado da instalação anterior é substituído pelo novo certificado. Se você estiver usando um certificado auto-assinado não padrão ou um certificado assinado por uma CA, você deverá substituir o certificado SSL WFA padrão pelo certificado.

Substitua o certificado SSL padrão do Workflow Automation

Você pode substituir o certificado SSL padrão do Workflow Automation (WFA) se o certificado tiver expirado ou se quiser aumentar o período de validade do certificado.

Você deve ter o root Privileges para o sistema Linux no qual você instalou O WFA.

O caminho de instalação padrão DO WFA é usado neste procedimento. Se você alterou o local padrão durante a instalação, você deve usar o caminho de instalação personalizado DO WFA.

Passos

1. Faça login como usuário root na máquina host WFA.
2. No prompt do shell, navegue para o seguinte diretório no servidor WFA: WFA_install_location/wfa/bin
3. Pare o banco de dados e os serviços de servidor DO WFA:

```
./wfa --stop=WFA
```

```
./wfa --stop=DB
```

4. Exclua o arquivo wfa.keystore do seguinte local:
WFA_install_location/wfa/jboss/standalone/Configuration/keystore.
5. Abra um prompt de shell no servidor WFA e, em seguida, altere os diretórios para o seguinte local:
<OpenJDK_install_location>/bin
6. Obter a chave da base de dados:

```
keytool -keysize 2048 -genkey -alias "ssl keystore" -keyalg RSA -keystore  
"WFA_install_location/wfa/jboss/standalone/configuration/keystore/wfa.keystore  
" -validity xxxx
```

xxxx é o número de dias para a validade do novo certificado.

7. Quando solicitado, forneça a senha (padrão ou nova).

A senha padrão é uma senha criptografada gerada aleatoriamente.

Para obter e descriptografar a senha padrão, siga as etapas no artigo da base de dados de Conhecimento

"Como renovar o certificado auto-assinado no WFA 5.1.1.0.4"

Para usar uma nova senha, siga as etapas no artigo da base de dados de Conhecimento "[Como atualizar uma nova senha para o keystore no WFA.](#)"

8. Introduza os detalhes necessários para o certificado.
9. Reveja as informações apresentadas e, em seguida, introduza Yes.
10. Pressione **Enter** quando solicitado pela seguinte mensagem: Digite a senha da chave para <SSL keystore>.
11. Reinicie os serviços WFA:

```
./wfa --start=DB
```

```
./wfa --start=WFA
```

Criar uma solicitação de assinatura de certificado para o Workflow Automation

Você pode criar uma solicitação de assinatura de certificado (CSR) no Linux para que você possa usar o certificado SSL assinado por uma Autoridade de Certificação (CA) em vez do certificado SSL padrão para automação do fluxo de trabalho (WFA).

- Você deve ter o root Privileges para o sistema Linux no qual você instalou O WFA.
- Você deve ter substituído o certificado SSL padrão fornecido pelo WFA.

O caminho de instalação padrão DO WFA é usado neste procedimento. Se você alterou o caminho padrão durante a instalação, então você deve usar o caminho de instalação personalizado DO WFA.

Passos

1. Faça login como usuário root na máquina host WFA.
2. Abra um prompt de shell no servidor WFA e, em seguida, altere os diretórios para o seguinte local: <OpenJDK_install_location>/bin
3. Criar um ficheiro CSR:

```
keytool -certreq -keystore
WFA_install_location/wfa/jboss/standalone/configuration/keystore/wfa.keystore
-alias "ssl keystore" -file /root/file_name.csr
```

File_name é o nome do arquivo CSR.

4. Quando solicitado, forneça a senha (padrão ou nova).

A senha padrão é uma senha criptografada gerada aleatoriamente.

Para obter e descriptografar a senha padrão, siga as etapas no artigo da base de dados de Conhecimento "[Como renovar o certificado auto-assinado no WFA 5.1.1.0.4](#)"

Para usar uma nova senha, siga as etapas no artigo da base de dados de Conhecimento "[Como atualizar uma nova senha para o keystore no WFA.](#)"

5. Envie o arquivo FILE_NAME.csr para a CA para obter um certificado assinado.

Consulte o site da CA para obter detalhes.

6. Faça o download de um certificado de cadeia da CA e, em seguida, importe o certificado de cadeia para o seu keystore:

```
keytool -import -alias "ssl keystore CA certificate" -keystore  
WFA_install_location/wfa/jboss/standalone/configuration/keystore/wfa.keystore"  
-trustcacerts -file chain_cert.cer
```

chain_cert.cer É o arquivo de certificado em cadeia que é recebido da CA. O arquivo deve estar no formato X,509.

7. Importe o certificado assinado que você recebeu da CA:

```
keytool -import -alias "ssl keystore" -keystore  
WFA_install_location/wfa/jboss/standalone/configuration/keystore/wfa.keystore"  
-trustcacerts -file certificate.cer
```

certificate.cer É o arquivo de certificado em cadeia que é recebido da CA.

8. Inicie os serviços WFA:

```
./wfa --start=DB
```

```
./wfa --start=WFA
```

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSAENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.