Gestión de certificados SSL de OnCommand Workflow Automation

OnCommand Workflow Automation 5.0

NetApp
April 19, 2024

This PDF was generated from https://docs.netapp.com/es-es/workflow-automation-50/rhel-install/task-replace-the-default-workflow-automation-ssl-certificate-linux.html on April 19, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestión de certificados SSL de OnCommand Workflow Automation

Puede sustituir el certificado SSL predeterminado OnCommand Workflow Automation (WFA) por un certificado autofirmado o un certificado firmado por una entidad de certificación (CA).

El certificado WFA SSL autofirmado predeterminado se genera durante la instalación de WFA. Al actualizar, el certificado de la instalación anterior se reemplaza por el nuevo certificado. Si utiliza un certificado autofirmado no predeterminado o un certificado firmado por una CA, debe reemplazar el certificado SSL de WFA por su certificado.

Reemplace el certificado SSL predeterminado de Workflow Automation

Puede reemplazar el certificado SSL predeterminado de Workflow Automation (WFA) si el certificado ha caducado o si desea aumentar el período de validez del certificado.

Lo que necesitará

Debe tener privilegios raíz para el sistema Linux en el que haya instalado WFA.

Acerca de esta tarea

La ruta de instalación predeterminada de WFA se utiliza en este procedimiento. Si ha cambiado la ubicación predeterminada durante la instalación, debe utilizar la ruta de instalación personalizada de WFA.

Pasos

1. Inicie sesión como usuario raíz en el equipo host de WFA.
2. En el símbolo del sistema del shell, desplácese hasta el siguiente directorio en el servidor de WFA:

   ```
   WFA_install_location/wfa/bin
   ```

3. Detenga la base de datos y los servicios del servidor de WFA:

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

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

4. Elimine el `wfa.keystore` archivo desde la siguiente ubicación: `WFA_install_location/wfa/jboss/standalone/configuration/keystore.`
5. Abra un símbolo del sistema del shell en el servidor de WFA y cambie los directorios a la siguiente ubicación:

   ```
   WFA_install_location/wfa/jre/bin
   ```

6. Obtenga la clave de la base de datos:

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

`xxxx` es el número de días para la validez del nuevo certificado.

7. Cuando se le solicite, introduzca la contraseña (predeterminada o nueva).

   `changeit` es la contraseña predeterminada. Si no desea utilizar la contraseña predeterminada, debe cambiar el atributo de contraseña del elemento SSL del `standalone-full.xml` archivo desde la siguiente ubicación: `WFA_install_location/wfa/jboss/standalone/configuration`

   ejemplo

   ```
   <ssl name="ssl" password="new_password" certificate-key-
   file="${jboss.server.config.dir}/keystore/wfa.keystore"
   ```

8. Introduzca los detalles obligatorios para el certificado.
9. Revise la información que se muestra y después introduzca `Yes`.
10. Pulse **Intro** cuando se le solicite el siguiente mensaje: `Enter key password for <SSL keystore> <RETURN if same as keystore password>.`
11. Reinicie los servicios de WFA:

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

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

Cree una solicitud de firma de certificación para Workflow Automation

Puede crear una solicitud de firma de certificación (CSR) en Linux para poder utilizar el certificado SSL firmado por una entidad de certificación (CA) en lugar del certificado SSL predeterminado para Workflow Automation (WFA).

Lo que necesitará

- Debe tener privilegios raíz para el sistema Linux en el que haya instalado WFA.
- Debe haber sustituido el certificado SSL predeterminado que proporciona WFA.

Acerca de esta tarea

La ruta de instalación predeterminada de WFA se utiliza en este procedimiento. Si ha cambiado la ruta predeterminada durante la instalación, debe utilizar la ruta de instalación personalizada de WFA.

Pasos

1. Inicie sesión como usuario raíz en el equipo host de WFA.
2. Abra un símbolo del sistema del shell en el servidor de WFA y cambie los directorios a la siguiente ubicación:

   ```
   WFA_install_location/wfa/jre/bin
   ```

3. Cree un archivo CSR:

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

File_name es el nombre del archivo CSR.

4. Cuando se le solicite, introduzca la contraseña (predeterminada o nueva).

   cambiit es la contraseña predeterminada. Si no desea utilizar la contraseña predeterminada, debe cambiar el atributo de contraseña del elemento SSL del `standalone-full.xml` de la `WFA_install_location/wfa/jboss/standalone/configuration` ubicación.

   ejemplo

   ```
   <ssl name="ssl" password="new_password" certificate-key-
   file="${jboss.server.config.dir}/keystore/wfa.keystore"
   ```

5. Envíe el archivo *file_name.csr* a la CA para obtener un certificado firmado.

   Consulte el sitio web de CA para obtener más información.

6. Descargue un certificado de cadena de la CA y, a continuación, importe el certificado de cadena al almacén de claves:

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

   `C:\chain_cert.cer` Es el archivo de certificado de cadena que se recibe de la CA. El archivo debe tener el formato X.509.

7. Importe el certificado firmado que ha recibido de la CA: `keytool -import -alias "ssl keystore" -keystore WFA_install_location/wfa/jboss/standalone/configuration/keystore/wfa.keystore" -trustcacerts -file C:\certificate.cer`

   `C:\certificate.cer` Es el archivo de certificado de cadena que se recibe de la CA.

8. Inicie los servicios de WFA:

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

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

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.