Gestione del certificato SSL OnCommand Workflow Automation

OnCommand Workflow Automation 5.0

NetApp
April 19, 2024

Sommario

Gestione del certificato SSL OnCommand Workflow Automation

È possibile sostituire il certificato SSL predefinito di OnCommand Workflow Automation (Wfa) con un certificato autofirmato o firmato da un'autorità di certificazione (CA).

Il certificato SSL WFA autofirmato predefinito viene generato durante l'installazione di WFA. Quando si esegue l'aggiornamento, il certificato per l'installazione precedente viene sostituito con il nuovo certificato. Se si utilizza un certificato autofirmato non predefinito o un certificato firmato da una CA, è necessario sostituire il certificato SSL Wfa predefinito con il certificato.

Sostituire il certificato SSL predefinito di Workflow Automation

È possibile sostituire il certificato SSL predefinito di Workflow Automation (WFA) se il certificato è scaduto o se si desidera aumentare il periodo di validità del certificato.

Di cosa hai bisogno

È necessario disporre dei privilegi di root per il sistema Linux su cui è stato installato WFA.

A proposito di questa attività

In questa procedura viene utilizzato il percorso di installazione predefinito di WFA. Se è stata modificata la posizione predefinita durante l'installazione, è necessario utilizzare il percorso di installazione WFA personalizzato.

Fasi

1. Accedere come utente root sul computer host WFA.
2. Al prompt della shell, accedere alla seguente directory sul server WFA:

   ```
   WFA_install_location/wfa/bin
   ```

3. Arrestare i servizi del server e del database WFA:

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

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

4. Eliminare `wfa.keystore` file dalla seguente posizione: `WFA_install_location/wfa/jboss/standalone/configuration/keystore.`
5. Aprire un prompt della shell sul server WFA, quindi modificare le directory nel seguente percorso:

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

6. Ottenere la chiave del database:

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

`xxxx` indica il numero di giorni di validità del nuovo certificato.

7. Quando richiesto, inserire la password (predefinita o nuova).

   `changeit` è la password predefinita. Se non si desidera utilizzare la password predefinita, è necessario modificare l'attributo password dell'elemento SSL in `standalone-full.xml` file dalla seguente posizione: `WFA_install_location/wfa/jboss/standalone/configuration`

   Esempio

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

8. Inserire i dettagli richiesti per il certificato.
9. Esaminare le informazioni visualizzate, quindi immettere `Yes`.
10. Premere **Invio** quando richiesto dal seguente messaggio: `Enter key password for <SSL keystore> <RETURN if same as keystore password>.`
11. Riavviare i servizi WFA:

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

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

Creare una richiesta di firma del certificato per Workflow Automation

È possibile creare una richiesta di firma del certificato (CSR) in Linux in modo da poter utilizzare il certificato SSL firmato da un'autorità di certificazione (CA) invece del certificato SSL predefinito per Workflow Automation (Wfa).

Di cosa hai bisogno

- È necessario disporre dei privilegi di root per il sistema Linux su cui è stato installato WFA.
- È necessario sostituire il certificato SSL predefinito fornito da WFA.

A proposito di questa attività

In questa procedura viene utilizzato il percorso di installazione predefinito di WFA. Se il percorso predefinito è stato modificato durante l'installazione, è necessario utilizzare il percorso di installazione WFA personalizzato.

Fasi

1. Accedere come utente root sul computer host WFA.
2. Aprire un prompt della shell sul server WFA, quindi modificare le directory nel seguente percorso:

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

3. Creare un file CSR:

   ```
   keytool -certreq -keystore
   ```

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

Nome_file è il nome del file CSR.

4. Quando richiesto, inserire la password (predefinita o nuova).

   changeit è la password predefinita. Se non si desidera utilizzare la password predefinita, è necessario modificare l'attributo password dell'elemento SSL in `standalone-full.xml` dal `WFA_install_location/wfa/jboss/standalone/configuration` posizione.

   Esempio

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

5. Inviare il file *nome_file.csr* alla CA per ottenere un certificato firmato.

   Per ulteriori informazioni, visitare il sito Web della CA.

6. Scarica un certificato di catena dalla CA, quindi importa il certificato di catena nel keystore:

   ```
   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` È il file di certificato di catena ricevuto dalla CA. Il file deve essere in formato X.509.

7. Importare il certificato firmato ricevuto dalla 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` È il file di certificato di catena ricevuto dalla CA.

8. Avviare i servizi WFA:

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

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