管理OnCommand Workflow Automation功能SSL憑證

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

目錄

管理OnCommand Workflow Automation 功能SSL憑證

您可以使用OnCommand Workflow Automation 自我簽署的憑證或由憑證授權單位（CA）簽署的憑證來取代預設的WFA（WFA）SSL憑證。

預設的自我簽署WFA SSL憑證會在安裝WFA期間產生。升級時、先前安裝的憑證會被新的憑證取代。如果您使用非預設的自我簽署憑證或由CA簽署的憑證、則必須以憑證取代預設的WFA SSL憑證。

取代預設的Workflow Automation SSL憑證

如果憑證已過期、或您想要延長憑證的有效期間、您可以取代預設的Workflow Automation（WFA）SSL憑證。

您必須擁有已安裝WFA的Linux系統的root權限。

此程序使用預設的WFA安裝路徑。如果您在安裝期間變更了預設位置、則必須使用自訂的WFA安裝路徑。

步驟

1. 以root使用者身分登入WFA主機機器。
2. 在Shell提示下、瀏覽至WFA伺服器上的下列目錄：WFA_install_LOWS/WFA/bin
3. 停止WFA資料庫和伺服器服務：

   「/WFA --停止= WFA」

   「/WFA --stop =資料庫」

4. 請從下列位置刪除WFA .keystore檔案：WFA安裝位置/ WFA / Jboss /獨立式/組態/ Keystore。
5. 在WFA伺服器上開啟Shell提示字元、然後將目錄變更為下列位置：<OpenJDK_install_location>/bin
6. 取得資料庫金鑰：

   「keytool-keysize 2048-genkey -alias "SSL Keystore」-keyalg ra -keystore「wfa_install_location / wfa/jboss/standaled/configuration / keystore/wfa.keystore」-validity xxxx'

   XXXX是新憑證有效的天數。

7. 出現提示時、請提供密碼（預設或新的）。

   預設密碼是隨機產生的加密密碼。

   若要取得並解密預設密碼、請依照知識庫文章中的步驟進行 "如何在WFA 5.1.1.0.4上續約自我簽署的憑證"

   若要使用新密碼、請遵循知識庫文章中的步驟 "如何在WFA中更新Keystore的新密碼。"

8. 輸入憑證的必要詳細資料。
9. 檢閱顯示的資訊、然後輸入「Yes（是）」。

10. 出現下列訊息時、請按* Enter *鍵：輸入<SSL Keystore（<SSL Keystore）>的金鑰密碼（如果與Keystore密碼相同則返回）>。
11. 重新啟動WFA服務：

    「/WFA --start=DB」

    「/wFA --start=wfa」

建立Workflow Automation的憑證簽署要求

您可以在Linux中建立憑證簽署要求（CSR）、以便使用由憑證授權單位（CA）簽署的SSL憑證、而非Workflow Automation（WFA）的預設SSL憑證。

- 您必須擁有已安裝WFA的Linux系統的root權限。
- 您必須更換WFA提供的預設SSL憑證。

此程序使用預設的WFA安裝路徑。如果您在安裝期間變更了預設路徑、則必須使用自訂的WFA安裝路徑。

步驟

1. 以root使用者身分登入WFA主機機器。
2. 在WFA伺服器上開啟Shell提示字元、然後將目錄變更為下列位置：<OpenJDK_install_location>/bin
3. 建立CSR檔案：

    「keytool-certreq -keystore wfa_install_kite/wfa/jboss/standale/configuration / keystore / wfa.keystore -alias "SSL keystore」-file /root/file_name.csr」

    file_name是CSR檔案的名稱。

4. 出現提示時、請提供密碼（預設或新的）。

    預設密碼是隨機產生的加密密碼。

    若要取得並解密預設密碼、請依照知識庫文章中的步驟進行 "如何在WFA 5.1.1.0.4上續約自我簽署的憑證"

    若要使用新密碼、請遵循知識庫文章中的步驟 "如何在WFA中更新Keystore的新密碼。"

5. 將file_name.csr檔案傳送至CA以取得簽署的憑證。

    如需詳細資料、請參閱CA網站。

6. 從CA下載鏈結憑證、然後將鏈結憑證匯入至您的Keystore：

    「keytool-import -alias "SSL keystore CA certe"-keystore wfa_install_stite/wfa/jboss/sinales/configuration / keystore /wfa.keystore」-caclacerts -file chain _cert.cer

    「chain _cert.cer」是從CA收到的鏈結憑證檔案。檔案必須為X・509格式。

7. 匯入您從CA收到的已簽署憑證：

「keytool-import -alias "SSL Keystore」-keystore wfa_install_portion/wfa/jboss/standale/configuration / keystore / wfa.keystore」-cappacerts -file Certificate .cer

「Certificate .cer」是從CA收到的鏈結憑證檔案。

8. 啟動WFA服務：

   「/WFA --start=DB」

   「/wFA --start=wfa」