管理OnCommand Workflow Automation功能SSL憑證

OnCommand Workflow Automation

NetApp
October 09, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/workflow-automation/rhel-install/task-replace-the-default-workflow-automation-ssl-certificate-linux.html on October 09, 2025. Always check docs.netapp.com for the latest.

目錄

管理OnCommand Workflow Automation 功能SSL憑證 1
取代預設的Workflow Automation SSL憑證 1
建立Workflow Automation的憑證簽署要求 2

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」

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。