智慧卡與憑證登入支援

OnCommand Insight

NetApp
April 01, 2024

目錄

智慧卡與憑證登入支援

支援使用智慧卡（CAC）和憑證來驗證登入Insight伺服器的使用者OnCommand Insight 。您必須設定系統才能啟用這些功能。

設定系統以支援CAC和憑證之後、瀏覽OnCommand Insight 至新的階段作業時、瀏覽器會顯示原生對話方塊、提供使用者可選擇的個人憑證清單。這些憑證會根據OnCommand Insight 由受到該伺服器信任的CA所發行的一組個人憑證進行篩選。通常只有單一選擇。根據預設、如果只有一個選項、Internet Explorer就會跳過此對話方塊。

對於CAC使用者、智慧卡包含多個憑證、其中只有一個可與信任的CA相符。的CAC憑證 `identification` 應使用。

如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：

- "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
- "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
- "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
- "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
- "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

設定主機以進行智慧卡和憑證登入

您必須修改OnCommand Insight 支援Smart Card（CAC）和憑證登入的整套主機組態。

開始之前

- 必須在系統上啟用LDAP。
- LDAP `User principal account name` 屬性必須符合包含使用者ID的LDAP欄位。

如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：

- "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
- "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
- "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
- "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
- "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

步驟

1. 使用 `regedit` 用於修改中登錄值的公用程式 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`：
   a. 變更JVM_Option `DclientAuth=false` 至 `DclientAuth=true.`
2. 備份Keystore檔案： `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. 開啟命令提示字元以指定 `Run as administrator`
4. 刪除自行產生的憑證： `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. 產生新的憑證： `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"`
6. 產生憑證簽署要求（CSR）：`C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"`
7. 在步驟6中傳回CSR之後、匯入憑證、然後以Base -64格式匯出憑證、並將其放入其中 `"C:\temp" named servername.cer`。
8. 從Keystore擷取憑證：`C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12`
9. 從p12檔案擷取私密金鑰： `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. 將您在步驟7中匯出的Base 64憑證與私密金鑰合併： `openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"`
11. 將合併的憑證匯入Keystore： `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"`
12. 匯入根憑證： `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"`
13. 將根憑證匯入server.trustore： `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"`

14. 匯入中繼憑證： `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"`

    對所有中繼憑證重複此步驟。

15. 在LDAP中指定與此範例相符的網域。
16. 重新啟動伺服器。

設定用戶端以支援智慧卡和憑證登入

用戶端機器需要中介軟體和瀏覽器修改、才能使用智慧卡和登入憑證。已使用智慧卡的客戶不應要求對其用戶端機器進行額外的修改。

開始之前

> 如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：
>
> - "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
> - "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
> - "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
> - "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
> - "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

關於這項工作

以下是一般用戶端組態需求：

- 安裝Smart Card中介軟體、例如ActivClient（請參閱
- 修改IE瀏覽器（請參閱
- 修改Firefox瀏覽器（請參閱

在Linux伺服器上啟用CAC

在Linux OnCommand Insight 支援伺服器上啟用CAC需要進行一些修改。

步驟

1. 瀏覽至 `/opt/netapp/oci/conf/`
2. 編輯 `wildfly.properties` 並變更的值 `CLIENT_AUTH_ENABLED` 至「真」

3. 匯入下的「root憑證」 `/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
4. 重新啟動伺服器

設定資料倉儲以進行智慧卡和憑證登入

您必須修改OnCommand Insight 「支援智慧卡（CAC）」和「憑證登入」的「支援資料倉儲」組態。

開始之前

- 必須在系統上啟用LDAP。
- LDAP `User principal account name` 屬性必須符合包含使用者政府ID號碼的LDAP欄位。

  儲存在政府核發之CAC上的一般名稱（CN）通常採用下列格式： `first.last.ID`。對於某些LDAP欄位、例如 `sAMAccountName`、格式太長。對於這些欄位OnCommand Insight 、只會從CNS擷取ID號碼。

> 如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：
>
> - "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
> - "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
> - "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
> - "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
> - "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

步驟

1. 使用RegEdit修改中的登錄值 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. 變更JVM_Option `-DclientAuth=false` 至 `-DclientAuth=true`。

   若為Linux、請修改 `clientAuth` 參數輸入 `/opt/netapp/oci/scripts/wildfly.server`

2. 將憑證授權單位（CA）新增至資料倉儲信任庫：

   a. 在命令視窗中、前往 `..\SANscreen\wildfly\standalone\configuration`。

   b. 使用 `keytool` 列出信任CA的公用程式： `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      每行的第一個字表示CA別名。

   c. 如有必要、請提供CA憑證檔案、通常是 `.pem` 檔案：若要將客戶的CA納入資料倉儲信任的CA、請前往

`..\SANscreen\wildfly\standalone\configuration` 並使用 `keytool` 匯入命令：

```
C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore
server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts
```

my_alias通常是容易識別中CA的別名`keytool -list` 營運。

3. 在伺服器上OnCommand Insight `wildfly/standalone/configuration/standalone-full.xml` 檔案必須透過將驗證用戶端更新為中的「要求的」來修改 `/subsystem=undertow/server=default-server/https-listener=default-https`以啟用CAC。登入Insight伺服器並執行適當的命令：

作業系統	指令碼
Windows	wildfly \bin\enableCACforRemoteEJB.bat <install dir>
Linux	/opp/NetApp/OCI /萬用里/賓/enableCACforRemoteEJB.sh

執行指令碼之後、請等到重新載入wildfly伺服器完成之後、再繼續下一步。

4. 重新啟動OnCommand Insight 伺服器。

設定Cognos以登入智慧卡和憑證（OnCommand Insight 從版本號到版本號7.3.9）

您必須修改OnCommand Insight 「支援Cognos伺服器的智慧卡（CAC）和憑證登入」的「資料倉儲」組態。

開始之前

此程序適用於執行OnCommand Insight VMware 7.3.5到7.3.9的系統。

> 如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：
>
> - "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
> - "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
> - "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
> - "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
> - "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

步驟

1. 將憑證授權單位（CA）新增至Cognos受託者。
   a. 在命令視窗中、前往 `..\SANscreen\cognos\analytics\configuration\certs\`

b. 使用 `keytool` 列出信任CA的公用程式： `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

   每行的第一個字表示CA別名。

c. 如果不存在適當的檔案、請提供CA憑證檔案、通常是 `.pem` 檔案：

d. 若要將客戶的CA納入OnCommand Insight 可靠的可靠CA、請前往 `..\SANscreen\cognos\analytics\configuration\certs\`。

e. 使用 `keytool` 匯入的公用程式 `.pem` 檔案： `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   `my_alias` 通常是容易識別中CA的別名`keytool -list` 營運。

f. 當系統提示輸入密碼時、請輸入 `NoPassWordSet`。

g. 答 `yes` 當系統提示您信任憑證時。

2. 若要啟用CAC模式、請執行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. 若要停用CAC模式、請執行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

設定Cognos以登入智慧卡和憑證（OnCommand Insight 更新版本：

您必須修改OnCommand Insight 「支援Cognos伺服器的智慧卡（CAC）和憑證登入」的「資料倉儲」組態。

開始之前

此程序適用於執行OnCommand Insight 支援更新版本的系統。

> 如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：
>
> - "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
> - "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
> - "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
> - "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
> - "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

步驟

1. 將憑證授權單位（CA）新增至Cognos受託者。

   a. 在命令視窗中、前往 `..\SANscreen\cognos\analytics\configuration\certs\`

b. 使用 `keytool` 列出信任CA的公用程式： `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

   每行的第一個字表示CA別名。

c. 如果不存在適當的檔案、請提供CA憑證檔案、通常是 `.pem` 檔案：

d. 若要將客戶的CA納入OnCommand Insight 可靠的可靠CA、請前往 `..\SANscreen\cognos\analytics\configuration\certs\`。

e. 使用 `keytool` 匯入的公用程式 `.pem` 檔案： `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   `my_alias` 通常是容易識別中CA的別名`keytool -list` 營運。

f. 當系統提示輸入密碼時、請輸入 `NoPassWordSet`。

g. 答 `yes` 當系統提示您信任憑證時。

2. 若要啟用CAC模式、請執行下列步驟：

   a. 使用下列步驟設定CAC登出頁面：

      - 登入Cognos入口網站（使用者必須是系統管理員群組的一部分、例如Cogns_admin）
      - （僅適用於7.3.10和7.3.11）按一下「管理」（Manage）「組態」（Configuration）「系統」（System）「安全性」（Security）
      - （僅適用於7.3.10和7.3.11）在登出重新導向URL →套用下輸入cacLogout.html
      - 關閉瀏覽器。

   b. 執行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

   c. 啟動IBM Cognos服務。等待Cognos服務啟動。

3. 若要停用CAC模式、請執行下列步驟：

   a. 執行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

   b. 啟動IBM Cognos服務。等待Cognos服務啟動。

   c. （僅適用於7.3.10和7.3.11）使用下列步驟取消設定CAC登出頁面：

      - 登入Cognos入口網站（使用者必須是系統管理員群組的一部分、例如Cogns_admin）
      - 按一下「管理」→「組態」→「系統」→「安全性」
      - 在「登出重新導向URL」→「套用」下輸入cacLogout.html
      - 關閉瀏覽器。

匯入Cognos和DWH的CA簽署SSL憑證（Insight 7.3.5至7.3.9）

您可以新增SSL憑證、為Data倉儲和Cognos環境啟用增強的驗證和加密功能。

開始之前

此程序適用於執行OnCommnand Insight 7.3.5到7.3.9的系統。

> 如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：
>
> - "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
> - "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
> - "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
> - "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
> - "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

關於這項工作

您必須擁有管理權限才能執行此程序。

步驟

1. 建立的備份 `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`。
2. 在下建立「certs」和「'csk'」資料夾的備份 `..\ SANScreen\cognos\analytics\configuration`。
3. 從Cognos產生憑證加密要求。在管理CMD視窗中、執行：
   a. CD `"\Program Files\sanscreen\cognos\analytics\bin"`
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr`
4. 開啟 `c:\temp\encryptRequest.csr` 歸檔並複製產生的內容。
5. 將加密Request。CSR傳送至憑證授權單位（CA）以取得SSL憑證。

   請務必新增其他屬性、例如「「：DNS = FQDN」（例如、hostname.netapp.com)`"以新增SubjectAltName。Google Chrome 58版及更新版本會抱怨憑證中是否遺漏SubjectAltName。

6. 使用PKCS7格式加入根憑證、即可下載鏈結憑證

   這會下載FQDN。p7b檔案

7. 從CA取得.p7b格式的憑證。使用名稱將其標示為Cognos Webserver的憑證。
8. ThirdPartyCertificateTool.bat無法匯入整個鏈結、因此匯出所有憑證需要執行多個步驟。請依照下列步驟個別匯出鏈結：
   a. 在「加密Shell Extensions」中開啟.p7b憑證。
   b. 在左窗格中瀏覽至「憑證」。
   c. 在根CA上按一下滑鼠右鍵>「All Tasks（所有工作）」>「Export（匯出
   d. 選取Base64輸出。

   e. 輸入檔案名稱、將其識別為根憑證。
   f. 重複步驟8a到8c、分別將所有憑證匯出至.cer檔案。
   g. 將檔案命名為merginate.cer和Cogns.cer。
9. 如果您只有一個CA憑證、請忽略此步驟、否則請將root.cer和merinateX.cer合併成一個檔案。
   a. 使用「記事本」開啟mintermed.cer並複製內容。
   b. 使用「記事本」開啟root.cer、並儲存9a的內容。
   c. 將檔案另存為CA.cer。
10. 使用管理CMD提示將憑證匯入Cognos Keystore：
   a. CD「Program Files\SANSANSANSANSANSANPC\Cognos /分析\BIN'」
   b. ThirdPartyCertificateTool.bat -Java:local -I -T -r c：\temp\ca.cer

      這會將CA.cer設為根憑證授權單位。

   c. ThirdPartyCertificateTool.bat -Java:local -i -e -r c：\emp\Cogns.cer -t c：\emp\ca.cer

      這會將Cogns.cer設為由CA.cer簽署的加密憑證。

11. 開啟IBM Cognos組態。
   a. 選取「本機組態」→「安全性」→「密碼編譯」→「Cognos」
   b. 變更「Use third party CA？」 為真。
   c. 儲存組態。
   d. 重新啟動Cognos
12. 使用管理CMD提示字元、將最新的Cognos憑證匯出至Cognos。CRT：
   a. 「d:\Program Files\SANSANSANSANSANP\Java\BIN\keytool.exe」-exportcert -file 「'c:\temp\Cogns.crt」-keystore「d:\Program Files\SANSANSANSANSANsce\Cognos \analystation\configuration \certs\CAMKeystore」-storeetype PKCS12 -storeNoPassSet Word-alias加密
13. 使用管理CMD提示視窗、將「'c:\emp\Cognes.crt」匯入DWh信任區、以建立Cognos與DWH之間的SSL通訊。
   a. "d:\Program Files\SANSANSANSANSANSANp\Java\BIN\keytool.exe"-importcert -file ""c:\emp\Cognos.crt"-keystore "D:\Program Files\SANSANscove\wildfly\sonsolation\configuration \server.trustore"-storeepass changit -alias cognoscert
14. 重新啟動SANscreen 此服務。
15. 執行DWH備份、確保DWH與Cognos通訊。

匯入Cognos和DWH的CA簽署SSL憑證（Insight 7.3.10及更新版本）

您可以新增SSL憑證、為Data倉儲和Cognos環境啟用增強的驗證和加密功能。

開始之前

此程序適用於執行OnCommand Insight 支援更新版本的系統。

> 如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：
>
> - "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
> - "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
> - "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnComand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
> - "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
> - "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

關於這項工作

您必須擁有管理權限才能執行此程序。

步驟

1. 使用IBM Cognos組態工具來停止Cognos。關閉Cognos。
2. 建立的備份 `..\SANScreen\cognos\analytics\configuration` 和 `..\SANScreen\cognos\analytics\temp\cam\freshness` 資料夾：
3. 從Cognos產生憑證加密要求。在管理CMD視窗中、執行：
   a. CD “`\Program Files\sanscreen\cognos\analytics\bin`”
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d “CN=server.domain.com,O=NETAPP,C=US” -H “server.domain.com” -I “ipaddress”`。附註：此處-H和-I是新增subectAltNames、例如DNS和IP地址。
4. 開啟 `c:\temp\encryptRequest.csr` 歸檔並複製產生的內容。
5. 輸入加密Request。CSR內容、並使用CA簽署入口網站產生憑證。
6. 使用PKCS7格式加入根憑證、即可下載鏈結憑證

   這會下載FQDN。p7b檔案
7. 從CA取得.p7b格式的憑證。使用名稱將其標示為Cognos Webserver的憑證。
8. ThirdPartyCertificateTool.bat無法匯入整個鏈結、因此匯出所有憑證需要執行多個步驟。請依照下列步驟個別匯出鏈結：
   a. 在「加密Shell Extensions」中開啟.p7b憑證。
   b. 在左窗格中瀏覽至「憑證」。
   c. 在根CA上按一下滑鼠右鍵>「All Tasks（所有工作）」>「Export（匯出
   d. 選取Base64輸出。

   e. 輸入檔案名稱、將其識別為根憑證。
   f. 重複步驟8a到8e、分別將所有憑證匯出至.cer檔案。
   g. 將檔案命名為merginate.cer和Cogns.cer。
9. 如果您只有一個CA憑證、請忽略此步驟、否則請將root.cer和merinateX.cer合併成一個檔案。
   a. 使用「記事本」開啟root.cer並複製內容。
   b. 使用「記事本」開啟mender.cer、然後附加9a的內容（中間第一和下一）。
   c. 將檔案另存為chain .cer。
10. 使用管理CMD提示將憑證匯入Cognos Keystore：
   a. CD「Program Files\SANSANSANSANSANSANPC\Cognos /分析\BIN'」
   b. ThirdPartyCertificateTool.bat -Java:local -I -t-r c：\temp\root.cer
   c. ThirdPartyCertificateTool.bat -Java:local -I -T -r c：\temp\minter.cer
   d. ThirdPartyCertificateTool.bat -Java:local -i -e -r c：\emp\Cogns.cer -t c：\emp\chain .cer
11. 開啟IBM Cognos組態。
   a. 選取「本機組態」→「安全性」→「密碼編譯」→「Cognos」
   b. 變更「Use third party CA？」 為真。
   c. 儲存組態。
   d. 重新啟動Cognos
12. 使用管理CMD提示字元、將最新的Cognos憑證匯出至Cognos。CRT：
   a. CD「'C:\Program Files\SANSANSANSANSAND"
   b. Java\BIN\keytool.exe -exportcert -file c：\temp\Cogns.crt -keystore Cognos \分析\組態\certs\CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias加密
13. 備份DWH伺服器信任資源`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. 使用管理CMD提示視窗、將「'c:\emp\Cognes.crt'」匯入DWH信任區、以建立Cognos與DWH之間的SSL通訊。
   a. CD「'C:\Program Files\SANSANSANSANSAND"
   b. Java\BIN\keytool.exe -importcert -file c:\emp\Cognos.crt -keystore wildfly\sisonal\configuration \server.trustore -storepass changit -alias cognos3rca
15. 重新啟動SANscreen 此服務。
16. 執行DWH備份、確保DWH與Cognos通訊。
17. 即使只變更「sSL憑證」、而且預設的Cognos憑證保持不變、仍應執行下列步驟。否則、Cognos可能會抱怨新SANscreen 的不合格證書、或無法建立DWH備份。
   a. `cd “%SANSCREEN_HOME%cognos\analytics\bin\”`
   b. `“%SANSCREEN_HOME%java64\bin\keytool.exe” -exportcert -file “c:\temp\sanscreen.cer” -keystore “%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore” -storepass changeit -alias “ssl certificate”`

c. `ThirdPartyCertificateTool.bat -java:local -i -T -r “c:\temp\sanscreen.cer”`

這些步驟通常是在中所述的Cognos憑證匯入程序中執行 "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"