스마트 카드 및 인증서 로그인 지원

OnCommand Insight

NetApp
April 01, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/oncommand-insight/config-admin/host-configuration-for-smart-card-and-certificate-login.html on April 01, 2024. Always check docs.netapp.com for the latest.

목차

스마트 카드 및 인증서 로그인 지원

OnCommand Insight는 CAC(스마트 카드) 및 인증서를 사용하여 Insight 서버에 로그인하는 사용자를 인증할 수 있습니다. 이러한 기능을 사용하려면 시스템을 구성해야 합니다.

CAC 및 인증서를 지원하도록 시스템을 구성한 후 OnCommand Insight의 새 세션을 탐색하면 브라우저에 기본 대화 상자가 표시되어 사용자가 선택할 수 있는 개인 인증서 목록을 제공합니다. 이러한 인증서는 OnCommand Insight 서버에서 신뢰할 수 있는 CA에서 발급한 개인 인증서 집합을 기반으로 필터링됩니다. 대부분의 경우 단일 선택 옵션이 있습니다. 기본적으로 Internet Explorer는 하나만 선택할 경우 이 대화 상자를 건너뜁니다.

CAC 사용자의 경우 스마트 카드에는 신뢰할 수 있는 CA와 일치할 수 있는 인증서가 여러 개 있습니다. 에 대한 CAC 인증서입니다 `identification` 사용해야 합니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

스마트 카드 및 인증서 로그인을 위한 호스트 구성

스마트 카드(CAC) 및 인증서 로그인을 지원하려면 OnCommand Insight 호스트 구성을 수정해야 합니다.

시작하기 전에

- 시스템에서 LDAP를 활성화해야 합니다.
- LDAP입니다 `User principal account name` 속성은 사용자 ID가 포함된 LDAP 필드와 일치해야 합니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. 를 사용합니다 `regedit` 에서 레지스트리 값을 수정하는 유틸리티입니다 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`:
   a. jvm_option을 변경합니다 `DclientAuth=false` 를 선택합니다 `DclientAuth=true`.
2. 키 저장소 파일을 백업합니다. `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. 를 지정하는 명령 프롬프트를 엽니다 `Run as administrator`
4. 자체 생성된 인증서 삭제: `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. 새 인증서 생성: `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. 인증서 서명 요청(CSR) 생성: `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. 6단계에서 CSR이 반환된 후 인증서를 가져온 다음 Base-64 형식으로 인증서를 내보내고 에 넣습니다 `"C:\temp" named servername.cer`.
8. 키 저장소에서 인증서를 추출합니다.`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. P12 파일에서 개인 키를 추출합니다. `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. 7단계에서 내보낸 Base-64 인증서를 개인 키와 병합합니다. `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. 병합된 인증서를 키 저장소로 가져옵니다. `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. 루트 인증서 가져오기: `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. 루트 인증서를 서버로 가져옵니다. 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. 중간 인증서 가져오기: `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"`

    모든 중간 인증서에 대해 이 단계를 반복합니다.

15. 이 예제와 일치하도록 LDAP에 도메인을 지정합니다.
16. 서버를 다시 시작합니다.

스마트 카드 및 인증서 로그인을 지원하도록 클라이언트 구성

클라이언트 시스템은 스마트 카드 사용 및 인증서 로그인을 지원하기 위해 미들웨어와 브라우저 수정이 필요합니다. 이미 스마트 카드를 사용하고 있는 고객은 클라이언트 시스템을 추가로 수정할 필요가 없습니다.

시작하기 전에

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

다음은 일반적인 클라이언트 구성 요구 사항입니다.

- ActivClient와 같은 스마트 카드 미들웨어 설치(참조
- IE 브라우저 수정(참조
- Firefox 브라우저 수정(참조

Linux 서버에 대한 CAC 활성화

Linux OnCommand Insight 서버에서 CAC를 활성화하려면 몇 가지 수정이 필요합니다.

단계

1. 로 이동합니다 `/opt/netapp/oci/conf/`
2. 편집 `wildfly.properties` 의 값을 변경합니다 `CLIENT_AUTH_ENABLED` "참"으로
3. 아래에 있는 "루트 인증서"를 가져옵니다 `/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
4. 서버를 다시 시작합니다

스마트 카드 및 인증서 로그인을 위한 데이터 웨어하우스 구성

스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

- 시스템에서 LDAP를 활성화해야 합니다.
- LDAP입니다 `User principal account name` 속성은 사용자의 정부 ID 번호가 포함된 LDAP 필드와 일치해야 합니다.

  정부에서 발급한 CAC에 저장된 일반 이름(CN)은 일반적으로 다음과 같은 형식입니다. `first.last.ID`. 와 같은 일부 LDAP 필드의 경우 `sAMAccountName`, 이 형식은 너무 깁니다. 이러한 필드의 경우 OnCommand Insight는 cns에서 ID 번호만 추출합니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. regedit를 사용하여 의 레지스트리 값을 수정합니다 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. jvm_option을 변경합니다 `-DclientAuth=false` 를 선택합니다 `-DclientAuth=true`.

   Linux의 경우 를 수정합니다 `clientAuth` 매개 변수 in `/opt/netapp/oci/scripts/wildfly.server`

2. CA(인증 기관)를 데이터 웨어하우스 trustore에 추가합니다.

   a. 명령 창에서 로 이동합니다 `..\SANscreen\wildfly\standalone\configuration`.

   b. 를 사용합니다 `keytool` 신뢰할 수 있는 CA를 나열하는 유틸리티: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

   c. 필요한 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 `.pem` 파일. 데이터 웨어하우스 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 을 참조하십시오 `..\SANscreen\wildfly\standalone\configuration` 를 사용합니다 `keytool` 가져오기 명령: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      my_alias는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다`keytool -list` 작동.

3. OnCommand Insight 서버에서 를 클릭합니다 `wildfly/standalone/configuration/standalone-full.xml` 에서 verify-client를 "requested"로 업데이트하여 파일을 수정해야 합니다 `/subsystem=undertow/server=default-server/https-listener=default-https`CAC 활성화 Insight 서버에 로그인하고 적절한 명령을 실행합니다.

OS	스크립트
Windows	<install dir>\SANscreen\Wildlfly\bin\enableCACforRemoteEJB.bat 을 참조하십시오

리눅스	/opt/netapp/OCI/Wildlfly/bin/enableCACforRemoteEJB.sh 을 참조하십시오

스크립트를 실행한 후 다음 단계로 진행하기 전에 Wildlfly 서버의 재로드가 완료될 때까지 기다립니다.

4. OnCommand Insight 서버를 다시 시작합니다.

스마트 카드 및 인증서 로그인을 위한 **Cognos** 구성(**OnCommand Insight 7.3.5 ~ 7.3.9**)

Cognos 서버에 대한 스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.5 ~ 7.3.9를 실행하는 시스템에 적용됩니다.

> 최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).
>
> - "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
> - "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
> - "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. Cognos Trustore에 CA(인증 기관)를 추가합니다.
   a. 명령 창에서 로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`
   b. 를 사용합니다 `keytool` 신뢰할 수 있는 CA를 나열하는 유틸리티: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

   c. 적합한 파일이 없는 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 `.pem` 파일.
   d. OnCommand Insight의 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 으로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. 를 사용합니다 `keytool` 을(를) 가져오는 유틸리티입니다 `.pem` 파일: `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` 는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다`keytool -list` 작동.

f. 암호를 묻는 메시지가 나타나면 를 입력합니다 `NoPassWordSet`.

g. 답변 `yes` 인증서를 신뢰할 수 있는 것인지 묻는 메시지가 표시됩니다.

2. CAC 모드를 활성화하려면 를 실행합니다 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. CAC 모드를 해제하려면 를 실행한다 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

스마트 카드 및 인증서 로그인에 대한 **Cognos** 구성(**OnCommand Insight 7.3.10** 이상)

Cognos 서버에 대한 스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.10 이상을 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. Cognos Trustore에 CA(인증 기관)를 추가합니다.

   a. 명령 창에서 로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`

   b. 를 사용합니다 `keytool` 신뢰할 수 있는 CA를 나열하는 유틸리티: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

   c. 적합한 파일이 없는 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 `.pem` 파일.

   d. OnCommand Insight의 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 으로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`.

   e. 를 사용합니다 `keytool` 을(를) 가져오는 유틸리티입니다 `.pem` 파일: `..\..\ibm-`

```
jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias
my_alias -file 'path/to/my.pem' -v -trustcacerts
```

`my_alias` 는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다`keytool -list` 작동.

f. 암호를 묻는 메시지가 나타나면 를 입력합니다 `NoPassWordSet`.

g. 답변 `yes` 인증서를 신뢰할 수 있는 것인지 묻는 메시지가 표시됩니다.

2. CAC 모드를 활성화하려면 다음을 수행합니다.

   a. 다음 단계에 따라 CAC 로그아웃 페이지를 구성합니다.

      - Cognos 포털 로그온(사용자는 시스템 관리자 그룹(예: cognos_admin)에 속해야 함)
      - (7.3.10 및 7.3.11에만 해당) 관리->구성->시스템->보안을 클릭합니다
      - (7.3.10 및 7.3.11에만 해당) 로그아웃 리디렉션 URL에 대해 cacLogout.html 을 입력합니다.\ → 적용
      - 브라우저를 닫습니다.

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

   c. IBM Cognos 서비스를 시작합니다. Cognos 서비스가 시작될 때까지 기다립니다.

3. CAC 모드를 해제하려면 다음을 수행합니다.

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

   b. IBM Cognos 서비스를 시작합니다. Cognos 서비스가 시작될 때까지 기다립니다.

   c. (7.3.10 및 7.3.11에만 해당) 다음 단계에 따라 CAC 로그아웃 페이지를 구성 해제합니다.

      - Cognos 포털 로그온(사용자는 시스템 관리자 그룹(예: cognos_admin)에 속해야 함)
      - 관리\ → 구성\ → 시스템\ → 보안을 클릭합니다
      - 로그아웃 리디렉션 URL \ → 적용에 대해 cacLogout.html 를 입력합니다
      - 브라우저를 닫습니다.

Cognos 및 DWH에 대해 CA 서명 SSL 인증서 가져오기(Insight 7.3.5 ~ 7.3.9)

SSL 인증서를 추가하여 데이터 웨어하우스 및 Cognos 환경에 대한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.5 ~ 7.3.9를 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

이 절차를 수행하려면 관리자 권한이 있어야 합니다.

단계

1. 의 백업을 생성합니다 `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. 아래의 ""certs"" 및 ""csk"" 폴더의 백업을 만듭니다 `..\SANScreen\cognos\analytics\configuration`.
3. Cognos에서 인증서 암호화 요청을 생성합니다. 관리자 CMD 창에서 다음을 실행합니다.
   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. 를 엽니다 `c:\temp\encryptRequest.csr` 생성된 콘텐츠를 파일로 만들어 복사합니다.
5. SSL 인증서를 얻으려면 encryptRequest.csr을 CA(인증 기관)에 보냅니다.

   "san:dns=FQDN(예: hostname.netapp.com)`" SubjectAltName을 추가하려면 추가 속성)을 추가해야 합니다. Google Chrome 버전 58 이상에서 SubjectAltName이 인증서에서 누락되면 불만을 표시합니다.

6. PKCS7 형식을 사용하여 루트 인증서를 포함시켜 체인 인증서를 다운로드합니다

   FQDN.p7b 파일이 다운로드됩니다

7. CA에서 .p7b 형식의 인증서를 가져옵니다. Cognos Webserver의 인증서로 표시하는 이름을 사용합니다.
8. ThirdPartyCertificateTool.bat 에서 전체 체인을 가져오지 못하므로 모든 인증서를 내보내려면 여러 단계가 필요합니다. 다음과 같이 체인을 개별적으로 내보내서 분할합니다.
   a. ""Crypto Shell Extensions""에서 .p7b 인증서를 엽니다.
   b. 왼쪽 창에서 ""인증서""를 찾습니다.
   c. 루트 CA > 모든 작업 > 내보내기를 마우스 오른쪽 버튼으로 클릭합니다.
   d. Base64 출력을 선택합니다.
   e. 루트 인증서로 식별하는 파일 이름을 입력합니다.

f. 모든 인증서를 .cer 파일로 별도로 내보내려면 8a-8C단계를 반복합니다.

g. 파일 이름을 mediateX.cer 및 cognos.cer 로 지정합니다.

9. CA 인증서가 하나만 있는 경우 이 단계를 무시하거나, 그렇지 않으면 root.cer와 mediateX.cer를 모두 하나의 파일로 병합합니다.

   a. 메모장에서 intermediate.cer를 열고 내용을 복사합니다.

   b. 메모장에서 root.cer를 열고 9a의 콘텐츠를 저장합니다.

   c. 파일을 CA.CER로 저장합니다.

10. 관리자 CMD 프롬프트를 사용하여 Cognos 키 저장소로 인증서를 가져옵니다.

    a. cd ""Program Files\SANscreen\cognos\analytics\bin"

    b. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\CA.cer

       그러면 CA.cer가 루트 인증 기관으로 설정됩니다.

    c. ThirdPartyCertificateTool.bat - java:local -i -e -r c:\temp\cognos.cer -t c:\temp\CA.cer

       이렇게 하면 Cognos.cer 가 CA.cer 에 의해 서명된 암호화 인증서로 설정됩니다.

11. IBM Cognos 구성을 엽니다.

    a. 로컬 구성 -→ 보안 -→ 암호화 -→ Cognos 를 선택합니다

    b. "Use third party CA?"를 변경합니다. 를 True로 설정합니다.

    c. 구성을 저장합니다.

    d. Cognos를 다시 시작합니다

12. 관리 CMD 프롬프트를 사용하여 최신 Cognos 인증서를 cognos.crt로 내보냅니다.

    a. "D:\Program Files\SANscreen\Java\bin\keytool.exe" -exportcert -file "" c:\temp\cognos.crt" -keystore "D:\Program Files\SANscreen\cognos\analytics\configuration\certs\CAMKeystore" -storetype PKCS12-storepass NoPassSet-alias 암호화

13. 관리 CMD 프롬프트 창을 사용하여 "'c:\temp\cognos.crt""를 dWh trustore로 가져와서 Cognos와 DWH 간에 SSL 통신을 설정합니다.

    a. "D:\Program Files\SANscreen\Java\bin\keytool.exe" - importcert -file ""c:\temp\cognos.crt" - keystore "D:\Program Files\SANscreen\standalone\configuration\server.trustore" - storepass changeit -alias cognosert

14. SANscreen 서비스를 다시 시작합니다.

15. DWH 백업을 수행하여 DWH가 Cognos와 통신하는지 확인합니다.

Cognos 및 DWH에 대해 CA 서명 SSL 인증서 가져오기(Insight 7.3.10 이상)

SSL 인증서를 추가하여 데이터 웨어하우스 및 Cognos 환경에 대한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.10 이상을 실행하는 시스템에 적용됩니다.

> 최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).
>
> - "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
> - "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
> - "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

이 절차를 수행하려면 관리자 권한이 있어야 합니다.

단계

1. IBM Cognos 구성 도구를 사용하여 Cognos를 중지합니다. Cognos를 닫습니다.
2. 의 백업을 생성합니다 `..\SANScreen\cognos\analytics\configuration` 및 `..\SANScreen\cognos\analytics\temp\cam\freshness` 폴더.
3. Cognos에서 인증서 암호화 요청을 생성합니다. 관리자 CMD 창에서 다음을 실행합니다.
   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"`. 참고: 여기서 -H와 -I는 DNS 및 ipaddress와 같은 subjectAltNames를 추가합니다.
4. 를 엽니다 `c:\temp\encryptRequest.csr` 생성된 콘텐츠를 파일로 만들어 복사합니다.
5. encryptRequest.csr 콘텐츠를 입력하고 CA 서명 포털을 사용하여 인증서를 생성합니다.
6. PKCS7 형식을 사용하여 루트 인증서를 포함시켜 체인 인증서를 다운로드합니다

   FQDN.p7b 파일이 다운로드됩니다

7. CA에서 .p7b 형식의 인증서를 가져옵니다. Cognos Webserver의 인증서로 표시하는 이름을 사용합니다.
8. ThirdPartyCertificateTool.bat 에서 전체 체인을 가져오지 못하므로 모든 인증서를 내보내려면 여러 단계가 필요합니다. 다음과 같이 체인을 개별적으로 내보내서 분할합니다.
   a. ""Crypto Shell Extensions""에서 .p7b 인증서를 엽니다.
   b. 왼쪽 창에서 ""인증서""를 찾습니다.
   c. 루트 CA > 모든 작업 > 내보내기를 마우스 오른쪽 버튼으로 클릭합니다.

   d. Base64 출력을 선택합니다.
   e. 루트 인증서로 식별하는 파일 이름을 입력합니다.
   f. 모든 인증서를 .cer 파일로 별도로 내보내려면 8a ~ 8e 단계를 반복합니다.
   g. 파일 이름을 mediateX.cer 및 cognos.cer 로 지정합니다.
9. CA 인증서가 하나만 있는 경우 이 단계를 무시하거나, 그렇지 않으면 root.cer와 mediateX.cer를 모두 하나의 파일로 병합합니다.
   a. 메모장에서 root.cer를 열고 내용을 복사합니다.
   b. 메모장을 사용하여 intermediate.cer를 열고 9a(중간 우선 및 루트 다음)의 콘텐츠를 추가합니다.
   c. 파일을 chain.cer로 저장합니다.
10. 관리자 CMD 프롬프트를 사용하여 Cognos 키 저장소로 인증서를 가져옵니다.
   a. cd ""Program Files\SANscreen\cognos\analytics\bin"
   b. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\root.cer
   c. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\intermediate.cer
   d. ThirdPartyCertificateTool.bat - java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer
11. IBM Cognos 구성을 엽니다.
   a. 로컬 구성 -→ 보안 -→ 암호화 -→ Cognos 를 선택합니다
   b. "Use third party CA?"를 변경합니다. 를 True로 설정합니다.
   c. 구성을 저장합니다.
   d. Cognos를 다시 시작합니다
12. 관리 CMD 프롬프트를 사용하여 최신 Cognos 인증서를 cognos.crt로 내보냅니다.
   a. CD "'C:\Program Files\SANscreen"
   b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore-storetype pkcs12-storepass NoPassWordSet-alias encryption
13. 에서 DWH 서버 트뤼스토어를 백업합니다`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. 관리 CMD 프롬프트 창을 사용하여 "'c:\temp\cognos.crt""를 DWH trustore로 가져와서 Cognos와 DWH 간에 SSL 통신을 설정합니다.
   a. CD "'C:\Program Files\SANscreen"
   b. java\bin\keytool.exe - importcert -file c:\temp\cognos.crt -keystore wandiderfly\standalone\configuration\server.trutstore -storephass changeit -alias coclnos3rdca
15. SANscreen 서비스를 다시 시작합니다.
16. DWH 백업을 수행하여 DWH가 Cognos와 통신하는지 확인합니다.
17. 'sl 인증서'만 변경되고 기본 Cognos 인증서는 변경되지 않은 경우에도 다음 단계를 수행해야 합니다. 그렇지 않으면 Cognos가 새 SANscreen 인증서에 대해 불만을 제기하거나 DWH 백업을 생성할 수 없습니다.
   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"`

일반적으로 이러한 단계는 에 설명된 Cognos 인증서 가져오기 프로세스의 일부로 수행됩니다 "Cognos CA(인증기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.