Unterstützung für Smart Card- und Zertifikatanmeldung

OnCommand Insight

NetApp
April 01, 2024

Inhalt

Unterstützung für Smart Card- und Zertifikatanmeldung

OnCommand Insight unterstützt die Verwendung von Smart Cards (CAC) und Zertifikaten zur Authentifizierung von Benutzern, die sich bei den Insight-Servern anmelden. Sie müssen das System konfigurieren, um diese Funktionen zu aktivieren.

Nach der Konfiguration des Systems zur Unterstützung von CAC und Zertifikaten führt das Navigieren zu einer neuen Sitzung von OnCommand Insight im Browser zu einem systemeigenen Dialogfeld, in dem dem der Benutzer eine Liste mit persönlichen Zertifikaten zur Auswahl hat. Diese Zertifikate werden basierend auf den persönlichen Zertifikaten gefiltert, die von CAS ausgestellt wurden, denen der OnCommand Insight-Server vertraut ist. Meistens gibt es eine einzige Wahl. Standardmäßig überspringt Internet Explorer dieses Dialogfeld, wenn nur eine Option vorhanden ist.

Für CAC-Benutzer enthalten Smartcards mehrere Zertifikate, von denen nur eines mit der vertrauenswürdigen Zertifizierungsstelle übereinstimmen kann. Das CAC-Zertifikat für `identification` Sollte verwendet werden.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

Konfigurieren von Hosts für die Smart Card- und Zertifikatanmeldung

Sie müssen Änderungen an der OnCommand Insight-Hostkonfiguration vornehmen, um Smart Card- (CAC) und Zertifikatanmeldungen zu unterstützen.

Bevor Sie beginnen

- LDAP muss auf dem System aktiviert sein.
- Das LDAP `User principal account name` Das Attribut muss mit dem LDAP-Feld übereinstimmen, das die ID eines Benutzers enthält.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

Schritte

1. Verwenden Sie die `regedit` Dienstprogramm zum Ändern von Registrierungswerten in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`:
   a. Ändern Sie die Option JVM_ `DclientAuth=false` Bis `DclientAuth=true.`
2. Backup der Keystore-Datei: `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Öffnen Sie eine Eingabeaufforderung mit der Angabe `Run as administrator`
4. Löschen Sie das selbstgenerierte Zertifikat: `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. Neues Zertifikat generieren: `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. Zertifikatsignierungsanforderung (CSR) generieren: `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. Nachdem die CSR in Schritt 6 zurückgegeben wurde, importieren Sie das Zertifikat, exportieren Sie das Zertifikat im Base-64-Format und legen Sie es in ein `"C:\temp" named servername.cer.`
8. Extrahieren Sie das Zertifikat aus dem Schlüsselspeicher:`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. Extrahieren Sie einen privaten Schlüssel aus der p12-Datei: `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`

10. Führen Sie das in Schritt 7 exportierte Base-64-Zertifikat mit dem privaten Schlüssel zusammen: `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. Importieren Sie das zusammengeführte Zertifikat in den Schlüsselspeicher: `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. Importieren Sie das Stammzertifikat: `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. Importieren Sie das Stammzertifikat in den 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. Zwischenzertifikat importieren: `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"`

    Wiederholen Sie diesen Schritt für alle Zwischenzertifikate.
15. Geben Sie die Domäne in LDAP an, die diesem Beispiel entspricht.
16. Starten Sie den Server neu.

Konfigurieren eines Clients zur Unterstützung der Smart Card- und Zertifikatanmeldung

Client-Rechner erfordern Middleware und Änderungen an Browsern, um die Verwendung von Smart Cards und die Zertifikatanmeldung zu ermöglichen. Kunden, die bereits Smart Cards verwenden, sollten keine zusätzlichen Änderungen an ihren Client-Computern benötigen.

Bevor Sie beginnen

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

Über diese Aufgabe

Die folgenden allgemeinen Anforderungen an die Client-Konfiguration:

- Installieren von Smart Card Middleware, z. B. ActivClient (siehe
- Ändern des IE-Browsers (siehe
- Ändern des Firefox-Browsers (siehe

Aktivieren von CAC auf einem Linux-Server

Einige Änderungen sind erforderlich, um CAC auf einem Linux OnCommand Insight-Server zu aktivieren.

Schritte

1. Navigieren Sie zu `/opt/netapp/oci/conf/`
2. Bearbeiten `wildfly.properties` Und ändern Sie den Wert von `CLIENT_AUTH_ENABLED` Zu „wahr“
3. Importieren Sie das „`root Certificate`“, das unter vorhanden ist `/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
4. Starten Sie den Server neu

Konfigurieren des Data Warehouse für die Smart Card- und Zertifikatanmeldung

Sie müssen die OnCommand Insight-Data-Warehouse-Konfiguration ändern, um Smart Card- (CAC) und Zertifikatanmeldungen zu unterstützen.

Bevor Sie beginnen

- LDAP muss auf dem System aktiviert sein.
- Das LDAP `User principal account name` Das Attribut muss mit dem LDAP-Feld übereinstimmen,

das die Regierungs-ID-Nummer eines Benutzers enthält.

Der auf staatlich ausgestellten CACs gespeicherte allgemeine Name (CN) wird normalerweise im folgenden Format gespeichert: `first.last.ID`. Für einige LDAP-Felder, z. B. `sAMAccountName`Dieses Format ist zu lang. Für diese Felder extrahiert OnCommand Insight nur die ID-Nummer aus dem CNS.

> Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):
>
> - "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
> - "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
> - "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
> - "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
> - "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

Schritte

1. Verwenden Sie regedit, um Registrierungswerte in zu ändern `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. Ändern Sie die Option JVM_ `-DclientAuth=false` Bis `-DclientAuth=true`.

   Ändern Sie für Linux die `clientAuth` Parameter in `/opt/netapp/oci/scripts/wildfly.server`

2. Zertifizierungsstellen (CAS) zum Data Warehouse trustore hinzufügen:

   a. Wechseln Sie in einem Befehlsfenster zu `..\SANscreen\wildfly\standalone\configuration`.

   b. Verwenden Sie die `keytool` Dienstprogramm zum Auflisten der vertrauenswürdigen CAS: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      Das erste Wort in jeder Zeile gibt den CA-Alias an.

   c. Geben Sie bei Bedarf eine Zertifizierungsstellenzertifikatsdatei an, in der Regel eine `.pem` Datei: Um die CAS des Kunden mit vertrauenswürdigen Data Warehouse-CAS aufzunehmen, gehen Sie zu `..\SANscreen\wildfly\standalone\configuration` Und verwenden Sie die `keytool` Importbefehl: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      My_alias ist normalerweise ein Alias, der die CA in der leicht identifizieren würde`keytool -list` Betrieb.

3. Auf dem OnCommand Insight-Server wird die angezeigt `wildfly/standalone/configuration/standalone-full.xml` Die Datei muss durch Aktualisierung von verify-Client auf „ANGEFORDERT“ in geändert werden `/subsystem=undertow/server=default-server/https-listener=default-https`Um CAC zu aktivieren. Melden Sie sich beim Insight-Server an, und führen Sie den entsprechenden Befehl aus:

BETRIEBSSYSTEM	Skript
Windows	<install dir>\SANscreen\wildfly\bin\enableCACforRemoteEJB.bat
Linux	/Opt/netapp/oci/wildfly/bin/enableCACforRemoteEJB.sh

   Warten Sie nach der Ausführung des Skripts, bis der Neustart des wildfly-Servers abgeschlossen ist, bevor Sie mit dem nächsten Schritt fortfahren.

4. Starten Sie den OnCommand Insight-Server neu.

Konfigurieren von Cognos für Smart Card- und Zertifikatanmeldung (OnCommand Insight 7.3.5 bis 7.3.9)

Sie müssen die Konfiguration des OnCommand Insight Data Warehouse ändern, um Smart Card- (CAC) und Zertifikatanmeldungen für den Cognos-Server zu unterstützen.

Bevor Sie beginnen

Dieses Verfahren gilt für Systeme mit OnCommand Insight 7.3.5 bis 7.3.9.

> Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):
>
> - "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
> - "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
> - "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
> - "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
> - "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

Schritte

1. Fügen Sie dem Cognos trustore Zertifizierungsstellen (CAS) hinzu.
   a. Wechseln Sie in einem Befehlsfenster zu

`..\SANscreen\cognos\analytics\configuration\certs\`

b. Verwenden Sie die `keytool` Dienstprogramm zum Auflisten der vertrauenswürdigen CAS:
`..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

   Das erste Wort in jeder Zeile gibt den CA-Alias an.

c. Wenn keine geeigneten Dateien vorhanden sind, geben Sie eine Zertifizierungsstellenzertifikatsdatei an, in der Regel eine `.pem` Datei:

d. Wenn Sie Zertifizierungsstellen des Kunden mit vertrauenswürdigen Zertifizierungsstellen von OnCommand Insight einbeziehen möchten, besuchen Sie `..\SANscreen\cognos\analytics\configuration\certs\`.

e. Verwenden Sie die `keytool` Dienstprogramm zum Importieren des `.pem` Datei:
`..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   `my_alias` Ist in der Regel ein Alias, der die CA in der leicht identifizieren würde`keytool -list` Betrieb.

f. Wenn Sie zur Eingabe eines Passworts aufgefordert werden, geben Sie ein `NoPassWordSet`.

g. Antwort `yes` Wenn Sie aufgefordert werden, dem Zertifikat zu vertrauen.

2. Um den CAC-Modus zu aktivieren, führen Sie aus
`..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

3. Um den CAC-Modus zu deaktivieren, führen Sie aus
`..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

Konfigurieren von Cognos für Smart Card- und Zertifikatanmeldung (OnCommand Insight 7.3.10 und höher)

Sie müssen die Konfiguration des OnCommand Insight Data Warehouse ändern, um Smart Card- (CAC) und Zertifikatanmeldungen für den Cognos-Server zu unterstützen.

Bevor Sie beginnen

Dieses Verfahren gilt für Systeme mit OnCommand Insight 7.3.10 und höher.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

Schritte

1. Fügen Sie dem Cognos trustore Zertifizierungsstellen (CAS) hinzu.
   a. Wechseln Sie in einem Befehlsfenster zu `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Verwenden Sie die `keytool` Dienstprogramm zum Auflisten der vertrauenswürdigen CAS: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      Das erste Wort in jeder Zeile gibt den CA-Alias an.
   c. Wenn keine geeigneten Dateien vorhanden sind, geben Sie eine Zertifizierungsstellenzertifikatsdatei an, in der Regel eine `.pem` Datei:
   d. Wenn Sie Zertifizierungsstellen des Kunden mit vertrauenswürdigen Zertifizierungsstellen von OnCommand Insight einbeziehen möchten, besuchen Sie `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. Verwenden Sie die `keytool` Dienstprogramm zum Importieren des `.pem` Datei: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` Ist in der Regel ein Alias, der die CA in der leicht identifizieren würde`keytool -list` Betrieb.
   f. Wenn Sie zur Eingabe eines Passworts aufgefordert werden, geben Sie ein `NoPassWordSet`.
   g. Antwort `yes` Wenn Sie aufgefordert werden, dem Zertifikat zu vertrauen.
2. Gehen Sie wie folgt vor, um den CAC-Modus zu aktivieren:
   a. Konfigurieren Sie die CAC-Abmeldeseite mit den folgenden Schritten:
      - Anmeldung beim Cognos-Portal (Benutzer muss Teil der Gruppe „Systemadministratoren“ sein, d. h. cognos_admin)
      - (Nur für 7.3.10 und 7.3.11) Klicken Sie auf Verwalten -> Konfiguration -> System -> Sicherheit
      - (Nur für 7.3.10 und 7.3.11) Geben Sie cacLogout.html gegen Abmeldung ein Umleiten Sie die URL -> Anwenden

    - Browser schließen.
  b. Ausführen `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
  c. Starten Sie den IBM Cognos-Dienst. Warten Sie, bis der Cognos-Dienst gestartet wird.
3. Gehen Sie wie folgt vor, um den CAC-Modus zu deaktivieren:
  a. Ausführen `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
  b. Starten Sie den IBM Cognos-Dienst. Warten Sie, bis der Cognos-Dienst gestartet wird.
  c. (Nur für 7.3.10 und 7.3.11) Unconfigure CAC Logout page, mit den folgenden Schritten:
    - Anmeldung beim Cognos-Portal (Benutzer muss Teil der Gruppe „Systemadministratoren“ sein, d. h. cognos_admin)
    - Klicken Sie Auf Verwalten -> Konfiguration -> System -> Sicherheit
    - Geben Sie cacLogout.html für die URL zur Umleitung von Abmeldung ein -> Anwenden
    - Browser schließen.

Importieren von CA-signierten SSL-Zertifikaten für Cognos und DWH (Insight 7.3.5 auf 7.3.9)

Sie können SSL-Zertifikate hinzufügen, um eine erweiterte Authentifizierung und Verschlüsselung für Ihre Data Warehouse- und Cognos-Umgebung zu ermöglichen.

Bevor Sie beginnen

Dieses Verfahren gilt für Systeme mit OnCommnand Insight 7.3.5 bis 7.3.9.

> Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):
>
> - "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
> - "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
> - "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
> - "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
> - "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

Über diese Aufgabe

Sie müssen über Administratorrechte verfügen, um dieses Verfahren durchführen zu können.

Schritte

1. Erstellen Sie ein Backup von `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.

2. Erstellen Sie unter eine Sicherungskopie der Ordner „`certs`“ und „`csk`“ `..\SANScreen\cognos\analytics\configuration`.
3. Erstellen Sie eine Zertifikatsverschlüsselungsanforderung von Cognos. Führen Sie in einem Admin-CMD-Fenster Folgendes aus:
   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. Öffnen Sie das `c:\temp\encryptRequest.csr` Datei und kopieren Sie den generierten Inhalt.
5. Senden Sie die cryptRequest.csr an die Zertifizierungsstelle (CA), um ein SSL-Zertifikat zu erhalten.

   Fügen Sie zusätzliche Attribute wie „`SAN:dns=FQDN“ hinzu (z. B. hostname.netapp.com)`", um den SubjectAltName hinzuzufügen. Google Chrome Version 58 und später beschwert sich, wenn die SubjectAltName fehlt aus dem Zertifikat.

6. Laden Sie die Kettenzertifikate unter Einbeziehung des Stammzertifikats im PKCS7-Format herunter

   Dadurch wird die Datei fqdn.p7b heruntergeladen

7. Holen Sie sich ein Zertifikat im .p7b-Format von Ihrer CA. Verwenden Sie einen Namen, der ihn als Zertifikat für den Cognos-Webserver kennzeichnet.
8. ThirdPartyCertificateTool.bat kann die gesamte Kette nicht importieren, so dass mehrere Schritte erforderlich sind, um alle Zertifikate zu exportieren. Teilen Sie die Kette auf, indem Sie sie einzeln wie folgt exportieren:
   a. Öffnen Sie das .p7b-Zertifikat unter „`Crypto Shell Extensions`“.
   b. Navigieren Sie im linken Fensterbereich zu „`Zertifikate`“.
   c. Klicken Sie mit der rechten Maustaste auf Stammzertifizierungsstelle > Alle Aufgaben > Exportieren.
   d. Wählen Sie Base64-Ausgabe.
   e. Geben Sie einen Dateinamen ein, der ihn als Stammzertifikat identifiziert.
   f. Wiederholen Sie die Schritte 8a bis 8c, um alle Zertifikate separat in .cer-Dateien zu exportieren.
   g. Benennen Sie die Dateien intermediateX.cer und cognos.cer.
9. Ignorieren Sie diesen Schritt, wenn Sie nur ein CA-Zertifikat haben, andernfalls fügen Sie root.cer und intermediateX.cer in eine Datei zusammen.
   a. Intermediate.cer mit Notepad öffnen und Inhalt kopieren.
   b. Öffnen Sie root.cer mit Notepad und speichern Sie den Inhalt aus 9a.
   c. Speichern Sie die Datei unter CA.cer.
10. Importieren Sie die Zertifikate in den Cognos-Keystore mithilfe der Admin-CMD-Eingabeaufforderung:
    a. cd „`Program Files\sanscreen\cognos\Analytics\bin`“
    b. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\CA.cer

       Dadurch wird CA.cer als Stammzertifizierungsstelle festgelegt.

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

       Dadurch wird Cognos.cer als von CA.cer signiertes Verschlüsselungszertifikat festgelegt.

11. Öffnen Sie die IBM Cognos-Konfiguration.
    a. Wählen Sie Lokale Konfiguration-→ Sicherheit -→ Kryptographie -→ Cognos
    b. „`Drittanbieter-CA verwenden?`“ ändern Nach wahr.
    c. Speichern Sie die Konfiguration.
    d. Cognos Neu Starten
12. Exportieren Sie das neueste Cognos-Zertifikat in cognos.crt mithilfe der Admin CMD-Eingabeaufforderung:
    a. „D:\Programme\SANscreen\java\bin\keytool.exe“ -exportcert -file „`c:\temp\cognos.crt`“ -keystore „D:\Programme\SANscreen\cognos\Analytics\Configuration\certs\CAMKeystore“ -storetype PKCS12 -storepass NoPassWordSet -alias-Verschlüsselung
13. Importieren Sie „`c:\temp\cognos.crt`“ in dwh trustore, um mithilfe des Admin CMD-Eingabefensters die SSL-Kommunikation zwischen Cognos und DWH herzustellen.
    a. „D:\Programme\SANscreen\java\bin\keytool.exe“ -importcert -file „`c:\temp\cognos.crt`“ -keystore „D:\Programme\SANscreen\wildfly\Standalone\Configuration\Server.trustore“ -storepass changeit -alias cognoscert
14. Starten Sie den SANscreen-Dienst neu.
15. Führen Sie eine Sicherungskopie des DWH durch, um sicherzustellen, dass DWH mit Cognos kommuniziert.

Importieren von CA-signierten SSL-Zertifikaten für Cognos und DWH (Insight 7.3.10 und höher)

Sie können SSL-Zertifikate hinzufügen, um eine erweiterte Authentifizierung und Verschlüsselung für Ihre Data Warehouse- und Cognos-Umgebung zu ermöglichen.

Bevor Sie beginnen

Dieses Verfahren gilt für Systeme mit OnCommand Insight 7.3.10 und höher.

> Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):
>
> - "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
> - "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
> - "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
> - "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
> - "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

Über diese Aufgabe

Sie müssen über Administratorrechte verfügen, um dieses Verfahren durchführen zu können.

Schritte

1. Beenden Sie Cognos mit dem IBM Cognos Configuration Tool. Schließen Sie Cognos.
2. Erstellen Sie Backups des `..\SANScreen\cognos\analytics\configuration` Und `..\SANScreen\cognos\analytics\temp\cam\freshness` Ordner.
3. Erstellen Sie eine Zertifikatsverschlüsselungsanforderung von Cognos. Führen Sie in einem Admin-CMD-Fenster Folgendes aus:
   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"`. Anmerkung: Hier sollen -H und -i subjectAltNames wie dns und ipaddress hinzufügen.
4. Öffnen Sie das `c:\temp\encryptRequest.csr` Datei und kopieren Sie den generierten Inhalt.
5. Geben Sie den Inhalt von encryptRequest.csr ein, und erstellen Sie das Zertifikat mithilfe des CA-Signing-Portals.
6. Laden Sie die Kettenzertifikate unter Einbeziehung des Stammzertifikats im PKCS7-Format herunter

   Dadurch wird die Datei fqdn.p7b heruntergeladen
7. Holen Sie sich ein Zertifikat im .p7b-Format von Ihrer CA. Verwenden Sie einen Namen, der ihn als Zertifikat für den Cognos-Webserver kennzeichnet.
8. ThirdPartyCertificateTool.bat kann die gesamte Kette nicht importieren, so dass mehrere Schritte erforderlich sind, um alle Zertifikate zu exportieren. Teilen Sie die Kette auf, indem Sie sie einzeln wie folgt exportieren:
   a. Öffnen Sie das .p7b-Zertifikat unter „`Crypto Shell Extensions`".
   b. Navigieren Sie im linken Fensterbereich zu „`Zertifikate`".
   c. Klicken Sie mit der rechten Maustaste auf Stammzertifizierungsstelle > Alle Aufgaben > Exportieren.
   d. Wählen Sie Base64-Ausgabe.
   e. Geben Sie einen Dateinamen ein, der ihn als Stammzertifikat identifiziert.
   f. Wiederholen Sie die Schritte 8a bis 8e, um alle Zertifikate separat in .cer-Dateien zu exportieren.
   g. Benennen Sie die Dateien intermediateX.cer und cognos.cer.
9. Ignorieren Sie diesen Schritt, wenn Sie nur ein CA-Zertifikat haben, andernfalls fügen Sie root.cer und intermediateX.cer in eine Datei zusammen.
   a. Öffnen Sie root.cer mit Notepad und kopieren Sie den Inhalt.
   b. Öffnen Sie intermediate.cer mit Notepad und fügen Sie den Inhalt von 9a an (intermediate first und root next).
   c. Speichern Sie die Datei unter Chain.cer.
10. Importieren Sie die Zertifikate in den Cognos-Keystore mithilfe der Admin-CMD-Eingabeaufforderung:
    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. Öffnen Sie die IBM Cognos-Konfiguration.

    a. Wählen Sie Lokale Konfiguration-→ Sicherheit -→ Kryptographie -→ Cognos

    b. „`Drittanbieter-CA verwenden?`“ ändern Nach wahr.

    c. Speichern Sie die Konfiguration.

    d. Cognos Neu Starten

12. Exportieren Sie das neueste Cognos-Zertifikat in cognos.crt mithilfe der Admin CMD-Eingabeaufforderung:

    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-Verschlüsselung

13. Sichern Sie den DWH-Server trustore unter`..\SANscreen\wildfly\standalone\configuration\server.trustore`

14. Importieren Sie „`c:\temp\cognos.crt`“ in DWH trustore, um mithilfe des Admin CMD-Eingabefensters die SSL-Kommunikation zwischen Cognos und DWH herzustellen.

    a. cd „`C:\Program Files\SANscreen“

    b. java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore wildfly\Standalone\Configuration\Server.trustore -storepass changeit -alias cognos3rdca

15. Starten Sie den SANscreen-Dienst neu.

16. Führen Sie eine Sicherungskopie des DWH durch, um sicherzustellen, dass DWH mit Cognos kommuniziert.

17. Die folgenden Schritte sollten auch dann durchgeführt werden, wenn nur das “ssl-Zertifikat” geändert wird und die Standard-Cognos-Zertifikate unverändert bleiben. Andernfalls kann Cognos sich über das neue SANscreen-Zertifikat beschweren oder keine DWH-Sicherung erstellen.

    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”`

    Diese Schritte werden normalerweise im Rahmen des in beschriebenen Cognos-Zertifikatimportprozesses ausgeführt "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"