Prise en charge de la connexion par carte à puce et certificat

OnCommand Insight

NetApp
April 01, 2024

Sommaire

Prise en charge de la connexion par carte à puce et certificat

OnCommand Insight prend en charge l'utilisation de cartes à puce (CAC) et de certificats pour authentifier les utilisateurs qui se connectent aux serveurs Insight. Vous devez configurer le système pour activer ces fonctions.

Après avoir configuré le système pour prendre en charge le contrôle d'admission des appels et les certificats, la navigation vers une nouvelle session de OnCommand Insight entraîne l'affichage d'une boîte de dialogue native qui fournit à l'utilisateur une liste de certificats personnels à choisir. Ces certificats sont filtrés en fonction de l'ensemble des certificats personnels émis par les autorités de certification approuvées par le serveur OnCommand Insight. Le plus souvent, il y a un seul choix. Par défaut, Internet Explorer ignore cette boîte de dialogue s'il n'y a qu'une seule option.

Pour les utilisateurs CAC, les cartes à puce contiennent plusieurs certificats, dont un seul peut correspondre à l'autorité de certification approuvée. Le certificat CAC pour `identification` doit être utilisé.

Pour obtenir les instructions les plus récentes sur les cartes CAC et les certificats, consultez les articles suivants de la base de connaissances (connexion au support requise) :

- "Comment configurer l'authentification CAC (Common Access Card) pour OnCommand Insight"
- "Comment configurer l'authentification CAC (Common Access Card) pour l'entrepôt de données OnCommand Insight"
- "Comment créer et importer un certificat signé d'autorité de certification dans OnComand Insight et l'entrepôt de données OnCommand Insight 7.3.x."
- "Comment créer un certificat auto-signé dans OnCommand Insight 7.3.X installé sur un hôte Windows"
- "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"

Configuration des hôtes pour la connexion par carte à puce et certificat

Vous devez apporter des modifications à la configuration de l'hôte OnCommand Insight pour prendre en charge les connexions par carte à puce (CAC) et certificat.

Avant de commencer

- LDAP doit être activé sur le système.
- Le LDAP `User principal account name` L'attribut doit correspondre au champ LDAP qui contient l'ID d'un utilisateur.

Pour obtenir les instructions les plus récentes sur les cartes CAC et les certificats, consultez les articles suivants de la base de connaissances (connexion au support requise) :

- "Comment configurer l'authentification CAC (Common Access Card) pour OnCommand Insight"
- "Comment configurer l'authentification CAC (Common Access Card) pour l'entrepôt de données OnCommand Insight"
- "Comment créer et importer un certificat signé d'autorité de certification dans OnComand Insight et l'entrepôt de données OnCommand Insight 7.3.x."
- "Comment créer un certificat auto-signé dans OnCommand Insight 7.3.X installé sur un hôte Windows"
- "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"

Étapes

1. Utilisez le `regedit` utilitaire permettant de modifier les valeurs de registre dans `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`:
   a. Modifiez JVM_option `DclientAuth=false` à `DclientAuth=true.`
2. Sauvegardez le fichier du magasin de clés : `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Ouvrez une invite de commande en spécifiant `Run as administrator`
4. Supprimez le certificat généré automatiquement : `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. Générer un nouveau certificat : `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. Générer une requête de signature de certificat (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. Une fois la CSR renvoyée à l'étape 6, importez le certificat, puis exportez-le au format base-64 et placez-le dans `"C:\temp" named servername.cer.`
8. Extrayez le certificat du magasin de clés :`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. Extraire une clé privée du fichier p12 : `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`

10. Fusionnez le certificat base-64 que vous avez exporté à l'étape 7 avec la clé privée : `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. Importez le certificat fusionné dans le magasin de clés : `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. Importer le certificat racine : `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. Importez le certificat racine dans le serveur.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. Importer le certificat intermédiaire : `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"`

    Répétez cette étape pour tous les certificats intermédiaires.
15. Spécifiez le domaine dans LDAP pour correspondre à cet exemple.
16. Redémarrez le serveur.

Configuration d'un client pour prendre en charge la connexion par carte à puce et certificat

Les ordinateurs clients nécessitent un middleware et des modifications aux navigateurs pour permettre l'utilisation des cartes à puce et la connexion au certificat. Les clients qui utilisent déjà des cartes à puce ne doivent pas nécessiter de modifications supplémentaires sur leurs ordinateurs clients.

Avant de commencer

Pour obtenir les instructions les plus récentes sur les cartes CAC et les certificats, consultez les articles suivants de la base de connaissances (connexion au support requise) :

- "Comment configurer l'authentification CAC (Common Access Card) pour OnCommand Insight"
- "Comment configurer l'authentification CAC (Common Access Card) pour l'entrepôt de données OnCommand Insight"
- "Comment créer et importer un certificat signé d'autorité de certification dans OnComand Insight et l'entrepôt de données OnCommand Insight 7.3.x."
- "Comment créer un certificat auto-signé dans OnCommand Insight 7.3.X installé sur un hôte Windows"
- "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"

Description de la tâche

Les exigences de configuration client courantes sont les suivantes :

- Installation d'un middleware de carte à puce, tel qu'ActivClient (voir
- Modification du navigateur IE (voir
- Modification du navigateur Firefox (voir

Activation de CAC sur un serveur Linux

Certaines modifications sont nécessaires pour activer le contrôle d'accès aux appels sur un serveur OnCommand Insight Linux.

Étapes

1. Accédez à `/opt/netapp/oci/conf/`
2. Modifier `wildfly.properties` et modifiez la valeur de `CLIENT_AUTH_ENABLED` Sur « vrai »
3. Importez le « certificat racine » qui existe sous `/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
4. Redémarrez le serveur

Configuration de Data Warehouse pour la connexion par carte à puce et certificat

Vous devez modifier la configuration de l'entrepôt de données OnCommand Insight pour prendre en charge les connexions par carte à puce (CAC) et certificat.

Avant de commencer

- LDAP doit être activé sur le système.
- Le LDAP `User principal account name` L'attribut doit correspondre au champ LDAP qui contient le

numéro d'identification du gouvernement d'un utilisateur.

Le nom commun (CN) stocké dans les PCA émises par le gouvernement est normalement dans le format suivant : `first.last.ID`. Pour certains champs LDAP, tels que `sAMAccountName`, ce format est trop long. Pour ces champs, OnCommand Insight extrait uniquement le numéro d'ID du CNS.

> Pour obtenir les instructions les plus récentes sur les cartes CAC et les certificats, consultez les articles suivants de la base de connaissances (connexion au support requise) :
>
> - "Comment configurer l'authentification CAC (Common Access Card) pour OnCommand Insight"
> - "Comment configurer l'authentification CAC (Common Access Card) pour l'entrepôt de données OnCommand Insight"
> - "Comment créer et importer un certificat signé d'autorité de certification dans OnComand Insight et l'entrepôt de données OnCommand Insight 7.3.x."
> - "Comment créer un certificat auto-signé dans OnCommand Insight 7.3.X installé sur un hôte Windows"
> - "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"

Étapes

1. Utilisez regedit pour modifier les valeurs de registre dans `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. Modifiez JVM_option `-DclientAuth=false` à `-DclientAuth=true`.

   Pour Linux, modifiez le `clientAuth` paramètre dans `/opt/netapp/oci/scripts/wildfly.server`

2. Ajoutez des autorités de certification (CA) au magasin de données :

   a. Dans une fenêtre de commande, accédez à `..\SANscreen\wildfly\standalone\configuration`.

   b. Utilisez le `keytool` Utilitaire permettant de répertorier les autorités de certification approuvées : `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      Le premier mot de chaque ligne indique l'alias de l'autorité de certification.

   c. Si nécessaire, fournissez un fichier de certificat d'autorité de certification, généralement un `.pem` fichier. Pour inclure les autorités de certification du client avec les autorités de certification de l'entrepôt de données approuvées, rendez-vous sur `..\SANscreen\wildfly\standalone\configuration` et utiliser le `keytool` commande d'importation : `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      My_alias est généralement un alias qui identifie facilement l'autorité de certification dans le`keytool -list` fonctionnement.

3. Sur le serveur OnCommand Insight, le `wildfly/standalone/configuration/standalone-full.xml` Le fichier doit être modifié en mettant à jour VERIFY-client sur « REQUEST » dans `/subsystem=undertow/server=default-server/https-listener=default-https`Pour activer CAC. Connectez-vous au serveur Insight et exécutez la commande appropriée :

OS	Script
Répertoires de base	<install dir>\SANscreen\Wildfly\bin\enableCACforRemoteEJB.bat
Linux	/Opt/netapp/oci/Wildfly/bin/enableCACforRemoteEJB.sh

   Après avoir exécuté le script, attendez la fin du rechargement du serveur WildFly avant de passer à l'étape suivante.

4. Redémarrez le serveur OnCommand Insight.

Configuration de Cognos pour la connexion par carte à puce et certificat (OnCommand Insight 7.3.5 à 7.3.9)

Vous devez modifier la configuration de l'entrepôt de données OnCommand Insight pour prendre en charge les connexions de carte à puce (CAC) et de certificat pour le serveur Cognos.

Avant de commencer

Cette procédure concerne les systèmes exécutant OnCommand Insight 7.3.5 à 7.3.9.

> Pour obtenir les instructions les plus récentes sur les cartes CAC et les certificats, consultez les articles suivants de la base de connaissances (connexion au support requise) :
>
> - "Comment configurer l'authentification CAC (Common Access Card) pour OnCommand Insight"
> - "Comment configurer l'authentification CAC (Common Access Card) pour l'entrepôt de données OnCommand Insight"
> - "Comment créer et importer un certificat signé d'autorité de certification dans OnComand Insight et l'entrepôt de données OnCommand Insight 7.3.x."
> - "Comment créer un certificat auto-signé dans OnCommand Insight 7.3.X installé sur un hôte Windows"
> - "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"

Étapes

1. Ajoutez des autorités de certification (AC) au magasin de certificats Cognos.
   a. Dans une fenêtre de commande, accédez à

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

b. Utilisez le `keytool` Utilitaire permettant de répertorier les autorités de certification approuvées : `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

   Le premier mot de chaque ligne indique l'alias de l'autorité de certification.

c. S'il n'existe aucun fichier approprié, fournissez un fichier de certificat d'autorité de certification, généralement un `.pem` fichier.

d. Pour inclure les autorités de certification du client avec des autorités de certification OnCommand Insight approuvées, rendez-vous sur `..\SANscreen\cognos\analytics\configuration\certs\`.

e. Utilisez le `keytool` utilitaire d'importation de `.pem` fichier : `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   `my_alias` Est généralement un alias qui identifie facilement l'autorité de certification dans le`keytool -list` fonctionnement.

f. Lorsque vous êtes invité à saisir un mot de passe, entrez `NoPassWordSet`.

g. Réponse `yes` lorsque vous êtes invité à approuver le certificat.

2. Pour activer le mode CAC, exécutez `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

3. Pour désactiver le mode CAC, exécutez `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

Configuration de Cognos pour la connexion par carte à puce et certificat (OnCommand Insight 7.3.10 et versions ultérieures)

Vous devez modifier la configuration de l'entrepôt de données OnCommand Insight pour prendre en charge les connexions de carte à puce (CAC) et de certificat pour le serveur Cognos.

Avant de commencer

Cette procédure concerne les systèmes exécutant OnCommand Insight 7.3.10 et versions ultérieures.

Pour obtenir les instructions les plus récentes sur les cartes CAC et les certificats, consultez les articles suivants de la base de connaissances (connexion au support requise) :

- "Comment configurer l'authentification CAC (Common Access Card) pour OnCommand Insight"
- "Comment configurer l'authentification CAC (Common Access Card) pour l'entrepôt de données OnCommand Insight"
- "Comment créer et importer un certificat signé d'autorité de certification dans OnComand Insight et l'entrepôt de données OnCommand Insight 7.3.x."
- "Comment créer un certificat auto-signé dans OnCommand Insight 7.3.X installé sur un hôte Windows"
- "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"

Étapes

1. Ajoutez des autorités de certification (AC) au magasin de certificats Cognos.
   a. Dans une fenêtre de commande, accédez à `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Utilisez le `keytool` Utilitaire permettant de répertorier les autorités de certification approuvées : `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      Le premier mot de chaque ligne indique l'alias de l'autorité de certification.
   c. S'il n'existe aucun fichier approprié, fournissez un fichier de certificat d'autorité de certification, généralement un `.pem` fichier.
   d. Pour inclure les autorités de certification du client avec des autorités de certification OnCommand Insight approuvées, rendez-vous sur `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. Utilisez le `keytool` utilitaire d'importation de `.pem` fichier : `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` Est généralement un alias qui identifie facilement l'autorité de certification dans le`keytool -list` fonctionnement.
   f. Lorsque vous êtes invité à saisir un mot de passe, entrez `NoPassWordSet`.
   g. Réponse `yes` lorsque vous êtes invité à approuver le certificat.
2. Pour activer le mode CAC, procédez comme suit :
   a. Configurez la page de déconnexion CAC en procédant comme suit :
      - Se connecter au portail Cognos (l'utilisateur doit faire partie du groupe administrateurs système, c'est-à-dire cognos_admin)
      - (Uniquement pour 7.3.10 et 7.3.11) cliquez sur gérer -> Configuration -> système -> sécurité
      - (Uniquement pour 7.3.10 et 7.3.11) Entrez cacLogout.html en regard de l'URL de redirection de déconnexion -> appliquer

    - Fermez le navigateur.

  b. L'exécution `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

  c. Démarrez le service IBM Cognos. Attendez que le service Cognos démarre.

3. Pour désactiver le mode CAC, procédez comme suit :

  a. L'exécution `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

  b. Démarrez le service IBM Cognos. Attendez que le service Cognos démarre.

  c. (Uniquement pour 7.3.10 et 7.3.11) Déconfigurer la page de déconnexion CAC, en procédant comme suit :

    - Se connecter au portail Cognos (l'utilisateur doit faire partie du groupe administrateurs système, c'est-à-dire cognos_admin)
    - Cliquez sur gérer -> Configuration -> système -> sécurité
    - Saisissez cacLogout.html par rapport à l'URL de redirection de déconnexion -> appliquer
    - Fermez le navigateur.

Importation de certificats SSL signés par une autorité de certification pour Cognos et DWH (Insight 7.3.5 à 7.3.9)

Vous pouvez ajouter des certificats SSL pour activer l'authentification et le chiffrement améliorés pour votre environnement Data Warehouse et Cognos.

Avant de commencer

Cette procédure concerne les systèmes exécutant OnCommnand Insight 7.3.5 à 7.3.9.

> Pour obtenir les instructions les plus récentes sur les cartes CAC et les certificats, consultez les articles suivants de la base de connaissances (connexion au support requise) :
>
> - "Comment configurer l'authentification CAC (Common Access Card) pour OnCommand Insight"
> - "Comment configurer l'authentification CAC (Common Access Card) pour l'entrepôt de données OnCommand Insight"
> - "Comment créer et importer un certificat signé d'autorité de certification dans OnComand Insight et l'entrepôt de données OnCommand Insight 7.3.x."
> - "Comment créer un certificat auto-signé dans OnCommand Insight 7.3.X installé sur un hôte Windows"
> - "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"

Description de la tâche

Vous devez disposer de privilèges d'administrateur pour effectuer cette procédure.

Étapes

1. Créer une sauvegarde de `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. Créez une sauvegarde des dossiers « certs » et « csk » sous `..\SANScreen\cognos\analytics\configuration`.
3. Générez une demande de cryptage de certificat à partir de Cognos. Dans une fenêtre Admin CMD, exécutez :
   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. Ouvrez le `c:\temp\encryptRequest.csr` classez et copiez le contenu généré.
5. Envoyez encryptRequest.csr à l'autorité de certification (CA) pour obtenir un certificat SSL.

   Assurez-vous d'ajouter des attributs supplémentaires tels que `SAN:dns=FQDN (par exemple, hostname.netapp.com)`" pour ajouter le SubjectAltName). Google Chrome version 58 et ultérieure se plaint si le SubjectAltName est absent du certificat.

6. Téléchargez les certificats de chaîne en incluant le certificat racine en utilisant le format PKCS7

   Ceci téléchargera le fichier fqdn.p7b

7. Obtenez un certificat au format .p7b auprès de votre autorité de certification. Utilisez un nom qui le marque comme certificat pour le serveur Web Cognos.
8. ThirdPartyCertificateTool.bat ne parvient pas à importer l'ensemble de la chaîne ; plusieurs étapes sont donc nécessaires pour exporter tous les certificats. Divisez la chaîne en les exportant individuellement comme suit :
   a. Ouvrez le certificat .p7b dans « Crypto Shell Extensions ».
   b. Naviguez dans le volet de gauche jusqu'à "certificats"".
   c. Cliquez avec le bouton droit de la souris sur CA racine > toutes les tâches > Exporter.
   d. Sélectionnez sortie Base64.
   e. Entrez un nom de fichier identifiant celui-ci comme certificat racine.
   f. Répétez les étapes 8a à 8c pour exporter tous les certificats séparément dans des fichiers .cer.
   g. Nommez les fichiers intermediateX.cer et cognos.cer.
9. Ignorez cette étape si vous n'avez qu'un seul certificat CA, sinon fusionnez root.cer et intermediateX.cer en un seul fichier.
   a. Ouvrez intermediate.cer avec le Bloc-notes et copiez le contenu.
   b. Ouvrez root.cer avec le Bloc-notes et enregistrez le contenu à partir de 9a.
   c. Enregistrez le fichier sous CA.cer.
10. Importez les certificats dans le magasin de clés Cognos à l'aide de l'invite Admin CMD :
    a. cd « Program Files\sanscreen\cognos\analytics\bin »
    b. ThirdPartyCertificateTool.bat -Java:local -i -T -r c:\temp\CA.cer

       Cela va définir CA.cer comme autorité de certification racine.

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

   Ceci définit Cognos.cer comme certificat de cryptage signé par CA.cer.

11. Ouvrez la configuration IBM Cognos.
    a. Sélectionnez Configuration locale→ sécurité -→ cryptographie -→ Cognos
    b. Modifier « utiliser une autorité de certification tierce ? » Sur vrai.
    c. Enregistrez la configuration.
    d. Redémarrez Cognos
12. Exportez le dernier certificat Cognos dans cognos.crt à l'aide de l'invite Admin CMD :
    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 WordSet
13. Importez « c:\temp\cognos.crt » dans dwh trustore pour établir une communication SSL entre Cognos et DWH, à l'aide de la fenêtre d'invite Admin CMD.
    a. « D:\Program Files\SANscreen\Java\bin\keytool.exe » -importcert -file « c:\temp\cognos.crt » -keystore « D:\Program Files\SANscreen\Wildfly\standalone\configuration\Server.trustore » -storepass changeit -alias cogoscert
14. Redémarrez le service SANscreen.
15. Effectuez une sauvegarde de DWH pour vous assurer que DWH communique avec Cognos.

Importation de certificats SSL signés par une autorité de certification pour Cognos et DWH (Insight 7.3.10 et versions ultérieures)

Vous pouvez ajouter des certificats SSL pour activer l'authentification et le chiffrement améliorés pour votre environnement Data Warehouse et Cognos.

Avant de commencer

Cette procédure concerne les systèmes exécutant OnCommand Insight 7.3.10 et versions ultérieures.

> Pour obtenir les instructions les plus récentes sur les cartes CAC et les certificats, consultez les articles suivants de la base de connaissances (connexion au support requise) :
>
> - "Comment configurer l'authentification CAC (Common Access Card) pour OnCommand Insight"
> - "Comment configurer l'authentification CAC (Common Access Card) pour l'entrepôt de données OnCommand Insight"
> - "Comment créer et importer un certificat signé d'autorité de certification dans OnComand Insight et l'entrepôt de données OnCommand Insight 7.3.x."
> - "Comment créer un certificat auto-signé dans OnCommand Insight 7.3.X installé sur un hôte Windows"
> - "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"

Description de la tâche

Vous devez disposer de privilèges d'administrateur pour effectuer cette procédure.

Étapes

1. Arrêtez Cognos à l'aide de l'outil de configuration IBM Cognos. Fermer Cognos.
2. Créer des sauvegardes du `..\SANScreen\cognos\analytics\configuration` et `..\SANScreen\cognos\analytics\temp\cam\freshness` dossiers.
3. Générez une demande de cryptage de certificat à partir de Cognos. Dans une fenêtre Admin CMD, exécutez :
   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"`. Note: Ici -H et -i sont d'ajouter subjectAltNames comme dns et ipaddress.
4. Ouvrez le `c:\temp\encryptRequest.csr` classez et copiez le contenu généré.
5. Entrez le contenu encryptRequest.csr et générez un certificat à l'aide du portail de signature CA.
6. Téléchargez les certificats de chaîne en incluant le certificat racine en utilisant le format PKCS7

   Ceci téléchargera le fichier fqdn.p7b

7. Obtenez un certificat au format .p7b auprès de votre autorité de certification. Utilisez un nom qui le marque comme certificat pour le serveur Web Cognos.
8. ThirdPartyCertificateTool.bat ne parvient pas à importer l'ensemble de la chaîne ; plusieurs étapes sont donc nécessaires pour exporter tous les certificats. Divisez la chaîne en les exportant individuellement comme suit :
   a. Ouvrez le certificat .p7b dans « Crypto Shell Extensions ».
   b. Naviguez dans le volet de gauche jusqu'à "certificats"".
   c. Cliquez avec le bouton droit de la souris sur CA racine > toutes les tâches > Exporter.
   d. Sélectionnez sortie Base64.
   e. Entrez un nom de fichier identifiant celui-ci comme certificat racine.
   f. Répétez les étapes 8a à 8e pour exporter tous les certificats séparément dans des fichiers .cer.
   g. Nommez les fichiers intermediateX.cer et cognos.cer.
9. Ignorez cette étape si vous n'avez qu'un seul certificat CA, sinon fusionnez root.cer et intermediateX.cer en un seul fichier.
   a. Ouvrez root.cer avec le Bloc-notes et copiez le contenu.
   b. Ouvrez intermediate.cer avec le Bloc-notes et ajoutez le contenu à partir de 9a (intermédiaire en premier et racine en suivant).
   c. Enregistrez le fichier sous chain.cer.
10. Importez les certificats dans le magasin de clés Cognos à l'aide de l'invite Admin CMD :
    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. Ouvrez la configuration IBM Cognos.

    a. Sélectionnez Configuration locale→ sécurité -→ cryptographie -→ Cognos

    b. Modifier « utiliser une autorité de certification tierce ? » Sur vrai.

    c. Enregistrez la configuration.

    d. Redémarrez Cognos

12. Exportez le dernier certificat Cognos dans cognos.crt à l'aide de l'invite Admin CMD :

    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. Sauvegardez le serveur DWH trustore sur`..\SANscreen\wildfly\standalone\configuration\server.trustore`

14. Importez « c:\temp\cognos.crt » dans DWH trustore pour établir une communication SSL entre Cognos et DWH, à l'aide de la fenêtre d'invite Admin CMD.

    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 cogoss3rdca

15. Redémarrez le service SANscreen.

16. Effectuez une sauvegarde de DWH pour vous assurer que DWH communique avec Cognos.

17. Les étapes suivantes doivent être effectuées même lorsque seul le "sl certificate" est modifié et que les certificats Cognos par défaut restent inchangés. Dans le cas contraire, Cognos peut se plaindre du nouveau certificat SANscreen ou être incapable de créer une sauvegarde DWH.

    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"`

    Généralement, ces étapes sont effectuées dans le cadre du processus d'importation de certificat Cognos décrit dans "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"