Compatibilidad con el inicio de sesión de la tarjeta inteligente y el certificado

OnCommand Insight

NetApp
April 01, 2024

Tabla de contenidos

Compatibilidad con el inicio de sesión de la tarjeta inteligente y el certificado 1
Configuración de hosts para el inicio de sesión de tarjeta inteligente y certificado 1
Configuración de un cliente para que admita el inicio de sesión de tarjeta inteligente y certificado 3
Activación de CAC en un servidor Linux 4
Configuración del almacén de datos para el inicio de sesión de la tarjeta inteligente y el certificado 4
Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.5 a 7.3.9) 6
Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.10 y posterior) 7
Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.5 a 7.3.9) 9
Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.10 y posterior) 11

Compatibilidad con el inicio de sesión de la tarjeta inteligente y el certificado

OnCommand Insight admite el uso de tarjetas inteligentes (CAC) y certificados para autenticar a los usuarios que inician sesión en los servidores de Insight. Debe configurar el sistema para habilitar estas funciones.

Después de configurar el sistema para que admita CAC y certificados, desplazarse a una nueva sesión de OnCommand Insight da como resultado que el explorador muestre un cuadro de diálogo nativo, proporcionando al usuario una lista de certificados personales entre los que elegir. Estos certificados se filtran en función del conjunto de certificados personales emitidos por entidades emisoras de certificados de confianza del servidor OnCommand Insight. La mayoría de las veces, existe una única opción. De forma predeterminada, Internet Explorer omite este cuadro de diálogo si sólo hay una opción.

Para los usuarios de CAC, las tarjetas inteligentes contienen varios certificados, sólo uno de los cuales puede coincidir con la CA de confianza. El certificado CAC para `identification` debe utilizarse.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Configuración de hosts para el inicio de sesión de tarjeta inteligente y certificado

Debe realizar modificaciones en la configuración del host de OnCommand Insight para admitir la tarjeta inteligente (CAC) y los inicios de sesión de certificados.

Antes de empezar

- LDAP debe estar habilitado en el sistema.
- El LDAP `User principal account name` El atributo debe coincidir con el campo LDAP que contiene el ID de un usuario.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Pasos

1. Utilice la `regedit` utilidad para modificar los valores del registro en `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`:
   a. Cambie la JVM_OPTION `DclientAuth=false` para `DclientAuth=true.`
2. Realice una copia de seguridad del archivo keystore: `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Abra un símbolo del sistema especificando `Run as administrator`
4. Elimine el certificado autofirmado: `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. Genere un nuevo certificado: `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. Genere una solicitud de firma de certificación (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. Una vez que se devuelva la CSR en el paso 6, importe el certificado y exporte el certificado en formato base-64 y colóquelo `"C:\temp" named servername.cer.`
8. Extraiga el certificado del almacén de claves:`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. Extraiga una clave privada del archivo p12: `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`

10. Fusionar el certificado base-64 exportado en el paso 7 con la clave privada: `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. Importe el certificado combinado al almacén de claves: `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. Importe el certificado raíz: `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. Importe el certificado raíz al servidor.truestore: `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. Importe el certificado intermedio: `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"`

    Repita este paso con todos los certificados intermedios.
15. Especifique el dominio en LDAP para que coincida con este ejemplo.
16. Reinicie el servidor.

Configuración de un cliente para que admita el inicio de sesión de tarjeta inteligente y certificado

Las máquinas cliente requieren middleware y modificaciones a los exploradores para permitir el uso de tarjetas inteligentes y para el inicio de sesión de certificados. Los clientes que ya utilizan tarjetas inteligentes no deben requerir modificaciones adicionales en sus equipos cliente.

Antes de empezar

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Acerca de esta tarea

A continuación se enumeran los requisitos comunes de configuración del cliente:

- Instalación de Smart Card middleware, como ActivClient (consulte
- Modificación del explorador de IE (consulte
- Modificación del navegador Firefox (consulte

Activación de CAC en un servidor Linux

Se necesitan algunas modificaciones para habilitar CAC en un servidor OnCommand Insight de Linux.

Pasos

1. Vaya a. `/opt/netapp/oci/conf/`
2. Editar `wildfly.properties` y cambie el valor de `CLIENT_AUTH_ENABLED` A "Verdadero"
3. Importe el «'certificado raíz» que existe en `/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
4. Reinicie el servidor

Configuración del almacén de datos para el inicio de sesión de la tarjeta inteligente y el certificado

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con las conexiones de tarjeta inteligente (CAC) y de certificados.

Antes de empezar

- LDAP debe estar habilitado en el sistema.

- El LDAP `User principal account name` El atributo debe coincidir con el campo LDAP que contiene el número de ID de gobierno de un usuario.

  El nombre común (CN) almacenado en los CAC emitidos por el gobierno suele estar en el siguiente formato: `first.last.ID`. Para algunos campos LDAP, como `sAMAccountName`, este formato es demasiado largo. En estos campos, OnCommand Insight extrae sólo el número de ID del sistema nervioso central.

> Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):
>
> - "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
> - "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
> - "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
> - "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
> - "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Pasos

1. Utilice regedit para modificar los valores del Registro en `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. Cambie la JVM_OPTION `-DclientAuth=false` para `-DclientAuth=true`.

   Para Linux, modifique el `clientAuth` parámetro in `/opt/netapp/oci/scripts/wildfly.server`

2. Agregue las entidades emisoras de certificados (CA) al almacén de datos de trueque:

   a. En una ventana de comandos, vaya a. `..\SANscreen\wildfly\standalone\configuration`.

   b. Utilice la `keytool` Utilidad para enumerar las CA de confianza: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      La primera palabra de cada línea indica el alias de CA.

   c. Si es necesario, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo. Para incluir las CA del cliente con las CA de confianza de Data Warehouse vaya a. `..\SANscreen\wildfly\standalone\configuration` y utilice la `keytool` comando de importación: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      Mi_alias es normalmente un alias que fácilmente identificaría la CA en`keytool -list` funcionamiento.

3. En el servidor OnCommand Insight, el `wildfly/standalone/configuration/standalone-full.xml` El archivo debe modificarse actualizando el cliente de verificación a "SOLICITADO" en `/subsystem=undertow/server=default-server/https-listener=default-https`Para activar CAC. Inicie sesión en el servidor de Insight y ejecute el comando adecuado:

SO	Guión
Windows	<install dir>\SANscreen\wilfly\bin\enableCACforRemoteEJB.bat
Linux	/Opt/netapp/oci/wiland/bin/enableCACforRemoteEJB.sh

   Después de ejecutar la secuencia de comandos, espere hasta que se complete la recarga del servidor de wilfly antes de continuar con el siguiente paso.

4. Reinicie el servidor OnCommand Insight.

Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.5 a 7.3.9)

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con la tarjeta inteligente (CAC) y los inicios de sesión del certificado para el servidor Cognos.

Antes de empezar

Este procedimiento es para sistemas que ejecuten OnCommand Insight 7.3.5 a 7.3.9.

> Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):
>
> - "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
> - "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
> - "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
> - "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
> - "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Pasos

1. Agregue las autoridades de certificación (CA) al almacén de Cognos.
   a. En una ventana de comandos, vaya a. `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Utilice la `keytool` Utilidad para enumerar las CA de confianza: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      La primera palabra de cada línea indica el alias de CA.

   c. Si no existen archivos adecuados, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo.
   d. Para incluir las CA del cliente con CA de confianza OnCommand Insight, vaya a. `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. Utilice la `keytool` utilidad para importar `.pem` archivo: `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` Normalmente es un alias que identificaría fácilmente la CA en`keytool -list` funcionamiento.

   f. Cuando se le pida una contraseña, introduzca `NoPassWordSet`.
   g. Responda `yes` cuando se le solicite que confíe en el certificado.
2. Para activar el modo CAC, ejecute `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. Para desactivar el modo CAC, ejecute `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.10 y posterior)

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con la tarjeta inteligente (CAC) y los inicios de sesión del certificado para el servidor Cognos.

Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Pasos

1. Agregue las autoridades de certificación (CA) al almacén de Cognos.
   a. En una ventana de comandos, vaya a. `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Utilice la `keytool` Utilidad para enumerar las CA de confianza: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      La primera palabra de cada línea indica el alias de CA.
   c. Si no existen archivos adecuados, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo.
   d. Para incluir las CA del cliente con CA de confianza OnCommand Insight, vaya a. `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. Utilice la `keytool` utilidad para importar `.pem` archivo: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` Normalmente es un alias que identificaría fácilmente la CA en`keytool -list` funcionamiento.
   f. Cuando se le pida una contraseña, introduzca `NoPassWordSet`.
   g. Responda `yes` cuando se le solicite que confíe en el certificado.
2. Para activar el modo CAC, realizar lo siguiente:
   a. Configure la página salir de CAC siguiendo los pasos siguientes:
      - Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, cognos_admin)
      - (Sólo para 7.3.10 y 7.3.11) haga clic en Administrar -> Configuración -> sistema -> Seguridad
      - (Sólo para 7.3.10 y 7.3.11) Introduzca cacLogout.html con la URL de redireccionamiento de cierre de sesión -> aplicar

    - Cierre el navegador.
  b. Ejecución `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
  c. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.
3. Para desactivar el modo CAC, realizar lo siguiente:
  a. Ejecución `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
  b. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.
  c. (Sólo para 7.3.10 y 7.3.11) desconfigure la página de cierre de sesión de CAC siguiendo los pasos siguientes:
    - Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, cognos_admin)
    - Haga clic en Administrar -> Configuración -> sistema -> Seguridad
    - Escriba cacLogout.html con la URL de redireccionamiento de cierre de sesión -> aplicar
    - Cierre el navegador.

Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.5 a 7.3.9)

Puede agregar certificados SSL para habilitar la autenticación y el cifrado mejorados para su entorno de Data Warehouse y Cognos.

Antes de empezar

Este procedimiento se aplica a sistemas que ejecutan OnCommny Insight 7.3.5 a 7.3.9.

> Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):
>
> - "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
> - "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
> - "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
> - "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
> - "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Acerca de esta tarea

Debe tener privilegios de administrador para realizar este procedimiento.

Pasos

1. Cree un backup de `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. Crear una copia de seguridad de las carpetas «'certs'» y «'csk'» en `..\SANScreen\cognos\analytics\configuration`.
3. Genere una solicitud de cifrado de certificado desde Cognos. En una ventana Admin CMD, ejecute:
   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. Abra el `c:\temp\encryptRequest.csr` archiva y copia el contenido generado.
5. Envíe el encryptRequest.csr a la entidad de certificación (CA) para obtener un certificado SSL.

   Asegúrese de agregar atributos adicionales como "TAN:dns=FQDN (por ejemplo, hostname.netapp.com)`" para agregar SubjectAltName. Google Chrome versión 58 y posteriores se queja si falta SubjectAltName en el certificado.

6. Descargue los certificados de cadena incluyendo el certificado raíz utilizando el formato PKCS7

   Esto descargará el archivo fqdn.p7b

7. Obtenga un certificado en formato .p7b de la CA. Utilice un nombre que lo marque como el certificado del servidor web Cognos.
8. ThirdPartyCertificateTool.bat no puede importar la cadena completa, de modo que se necesitan varios pasos para exportar todos los certificados. Divida la cadena exportándolos individualmente de la siguiente manera:
   a. Abra el certificado .p7b en "'Extensiones de shell de cifrado'".
   b. Navegue en el panel izquierdo hasta «'certificados'».
   c. Haga clic con el botón derecho del ratón en la CA raíz > todas las tareas > Exportar.
   d. Seleccione salida Base64.
   e. Introduzca un nombre de archivo que lo identifique como certificado raíz.
   f. Repita los pasos del 8 al 8 c para exportar todos los certificados por separado en archivos .cer.
   g. Asigne un nombre a los archivos intermediateX.cer y cognos.cer.
9. Ignore este paso si sólo tiene un certificado de CA, de lo contrario, combine root.cer y intermediateX.cer en un archivo.
   a. Abra Intermediate.cer con el Bloc de notas y copie el contenido.
   b. Abra root.cer con el Bloc de notas y guarde el contenido de 9a.
   c. Guarde el archivo como CA.cer.
10. Importe los certificados al almacén de claves de Cognos mediante el símbolo del sistema Admin CMD:
    a. cd "'Archivos de programa\sanscreen\cognos\analítica\bin'"
    b. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\CA.cer

       Esto establecerá CA.cer como entidad emisora de certificados raíz.

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

Esto establecerá Cognos.cer como certificado de cifrado firmado por CA.cer.

11. Abra la configuración de IBM Cognos.
    a. Seleccione Configuración local-→ Seguridad -→ Criptografía -→ Cognos
    b. Cambiar «¿utilizar CA de terceros?» Para True.
    c. Guarde la configuración.
    d. Reinicie Cognos
12. Exporte el último certificado Cognos a cognos.crt utilizando el indicador de administración CMD:
    a. "D:\Archivos de programa\SANscreen\java\bin\keytool.exe" -exportcert -file "'c:\temp\cognos.crt'" -keystore "D:\Archivos de programa\SANscreen\cognos\analítica\Configuration\certs\CAMKeystore" -storetype PKCS12 -storepass NoWordSet -alias cifrado
13. Importe "'c:\temp\cognos.crt'" en dwh truStore para establecer la comunicación SSL entre Cognos y DWH, mediante la ventana de indicación Admin CMD.
    a. "D:\Archivos de programa\SANscreen\java\bin\keytool.exe" -importcert -file "'c:\temp\cognos.crt'" -keystore "D:\Archivos de programa\SANscreen\wiland\autónoma\Configuration\Server.trustore" -storeprechrit -alias cognoscert
14. Reinicie el servicio SANscreen.
15. Realice una copia de seguridad de DWH para asegurarse de que DWH se comunica con Cognos.

Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.10 y posterior)

Puede agregar certificados SSL para habilitar la autenticación y el cifrado mejorados para su entorno de Data Warehouse y Cognos.

Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Acerca de esta tarea

Debe tener privilegios de administrador para realizar este procedimiento.

Pasos

1. Detenga Cognos utilizando la herramienta de configuración de IBM Cognos. Cierre Cognos.
2. Cree backups de `..\SANScreen\cognos\analytics\configuration` y.. `..\SANScreen\cognos\analytics\temp\cam\freshness` carpetas.
3. Genere una solicitud de cifrado de certificado desde Cognos. En una ventana Admin CMD, ejecute:
   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"`. Nota: Aquí -H y -i van a agregar subyectAltNames como dns e ipaddress.
4. Abra el `c:\temp\encryptRequest.csr` archiva y copia el contenido generado.
5. Introduzca el contenido encryptRequest.csr y genere un certificado mediante el portal de firma de CA.
6. Descargue los certificados de cadena incluyendo el certificado raíz utilizando el formato PKCS7

   Esto descargará el archivo fqdn.p7b

7. Obtenga un certificado en formato .p7b de la CA. Utilice un nombre que lo marque como el certificado del servidor web Cognos.
8. ThirdPartyCertificateTool.bat no puede importar la cadena completa, de modo que se necesitan varios pasos para exportar todos los certificados. Divida la cadena exportándolos individualmente de la siguiente manera:
   a. Abra el certificado .p7b en "'Extensiones de shell de cifrado'".
   b. Navegue en el panel izquierdo hasta «'certificados'».
   c. Haga clic con el botón derecho del ratón en la CA raíz > todas las tareas > Exportar.
   d. Seleccione salida Base64.
   e. Introduzca un nombre de archivo que lo identifique como certificado raíz.
   f. Repita los pasos del 8 a al 8 e para exportar todos los certificados por separado en archivos .cer.
   g. Asigne un nombre a los archivos intermediateX.cer y cognos.cer.
9. Ignore este paso si sólo tiene un certificado de CA, de lo contrario, combine root.cer y intermediateX.cer en un archivo.
   a. Abra root.cer con el Bloc de notas y copie el contenido.
   b. Abra Intermediate.cer con el Bloc de notas y anexe el contenido de 9a (primero intermedio y raíz siguiente).
   c. Guarde el archivo como chain.cer.
10. Importe los certificados al almacén de claves de Cognos mediante el símbolo del sistema Admin CMD:
    a. cd "'Archivos de programa\sanscreen\cognos\analítica\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. Abra la configuración de IBM Cognos.
    a. Seleccione Configuración local-→ Seguridad -→ Criptografía -→ Cognos
    b. Cambiar «¿utilizar CA de terceros?» Para True.
    c. Guarde la configuración.
    d. Reinicie Cognos
12. Exporte el último certificado Cognos a cognos.crt utilizando el indicador de administración CMD:
    a. cd "'C:\Archivos de programa\SANscreen"
    b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analítica\Configuration\certs\CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias cifrado
13. Haga una copia de seguridad del servidor de seguridad DWH en`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. Importe "'c:\temp\cognos.crt'" en DWH truStore para establecer la comunicación SSL entre Cognos y DWH, mediante la ventana de indicación Admin CMD.
    a. cd "'C:\Archivos de programa\SANscreen"
    b. java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore willose\reasone\configuration\server.trustore -storepass chretosca -alias cognos3rdca
15. Reinicie el servicio SANscreen.
16. Realice una copia de seguridad de DWH para asegurarse de que DWH se comunica con Cognos.
17. Los siguientes pasos deben realizarse incluso cuando sólo se cambia el "certificado de l" y los certificados de Cognos predeterminados no se modifican. De lo contrario, Cognos puede quejarse del nuevo certificado SANscreen o no puede crear una copia de seguridad 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”`

    Por lo general, estos pasos se realizan como parte del proceso de importación de certificados Cognos descrito en "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"