Supporto di accesso con smart card e certificato

OnCommand Insight

NetApp
April 01, 2024

Sommario

Supporto di accesso con smart card e certificato . . . 1
Configurazione degli host per l'accesso a smart card e certificati . . . 1
Configurazione di un client per il supporto dell'accesso con smart card e certificato . . . 3
Abilitazione del CAC su un server Linux . . . 4
Configurazione di Data Warehouse per l'accesso a smart card e certificati . . . 4
Configurazione dei Cognos per l'accesso con smart card e certificato (da OnCommand Insight 7.3.5 a 7.3.9) . . . 6
Configurazione dei Cognos per l'accesso con smart card e certificato (OnCommand Insight 7.3.10 e versioni successive) . . . 7
Importazione di certificati SSL con firma CA per Cognos e DWH (Insight da 7.3.5 a 7.3.9) . . . 8
Importazione di certificati SSL con firma CA per Cognos e DWH (Insight 7.3.10 e versioni successive) . . . 10

Supporto di accesso con smart card e certificato

OnCommand Insight supporta l'utilizzo di smart card (CAC) e certificati per autenticare gli utenti che accedono ai server Insight. È necessario configurare il sistema per abilitare queste funzioni.

Dopo aver configurato il sistema per il supporto di CAC e certificati, la navigazione verso una nuova sessione di OnCommand Insight comporta la visualizzazione di una finestra di dialogo nativa che fornisce all'utente un elenco di certificati personali tra cui scegliere. Questi certificati vengono filtrati in base al set di certificati personali emessi dalle CA attendibili dal server OnCommand Insight. La maggior parte delle volte, esiste una singola scelta. Per impostazione predefinita, Internet Explorer salta questa finestra di dialogo se esiste una sola scelta.

Per gli utenti CAC, le smart card contengono più certificati, uno solo dei quali può corrispondere alla CA attendibile. Il certificato CAC per `identification` deve essere utilizzato.

Per le istruzioni più aggiornate sul CAC e sul certificato, consulta i seguenti articoli della Knowledge base (è richiesto l'accesso al supporto):

- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per OnCommand Insight"
- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per il data warehouse OnCommand Insight"
- "Come creare e importare un certificato firmato dall'autorità di certificazione (CA) in OnComand Insight e OnCommand Insight Data Warehouse 7.3.x"
- "Come creare un certificato autofirmato in OnCommand Insight 7.3.X installato su un host Windows"
- "Come importare un certificato firmato dall'autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"

Configurazione degli host per l'accesso a smart card e certificati

È necessario apportare modifiche alla configurazione dell'host OnCommand Insight per supportare gli accessi con smart card (CAC) e certificati.

Prima di iniziare

- LDAP deve essere attivato nel sistema.
- LDAP `User principal account name` L'attributo deve corrispondere al campo LDAP che contiene l'ID dell'utente.

Per le istruzioni più aggiornate sul CAC e sul certificato, consulta i seguenti articoli della Knowledge base (è richiesto l'accesso al supporto):

- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per OnCommand Insight"
- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per il data warehouse OnCommand Insight"
- "Come creare e importare un certificato firmato dall'autorità di certificazione (CA) in OnComand Insight e OnCommand Insight Data Warehouse 7.3.x"
- "Come creare un certificato autofirmato in OnCommand Insight 7.3.X installato su un host Windows"
- "Come importare un certificato firmato dall'autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"

Fasi

1. Utilizzare `regedit` utility per modificare i valori del registro di sistema in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`:
   a. Modificare l'opzione JVM_Option `DclientAuth=false` a. `DclientAuth=true.`
2. Eseguire il backup del file keystore: `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Aprire un prompt dei comandi specificando `Run as administrator`
4. Eliminare il certificato autogenerato: `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. Generare un nuovo certificato: `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. Generare una richiesta di firma del certificato (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 volta restituito il CSR nel passaggio 6, importare il certificato, quindi esportarlo in formato base-64 e collocarlo in `"C:\temp" named servername.cer.`
8. Estrarre il certificato dal keystore:`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. Estrarre una chiave privata dal file p12: `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. Unire il certificato base-64 esportato al punto 7 con la chiave privata: `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. Importare il certificato Unito nel keystore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"`
12. Importare il certificato root: `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. Importare il certificato root nel 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. Importare il certificato 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"`

    Ripetere questo passaggio per tutti i certificati intermedi.

15. Specificare il dominio in LDAP da associare a questo esempio.
16. Riavviare il server.

Configurazione di un client per il supporto dell'accesso con smart card e certificato

I computer client richiedono middleware e modifiche ai browser per consentire l'utilizzo di Smart Card e per l'accesso ai certificati. I clienti che utilizzano già Smart Card non devono richiedere ulteriori modifiche ai computer client.

Prima di iniziare

Per le istruzioni più aggiornate sul CAC e sul certificato, consulta i seguenti articoli della Knowledge base (è richiesto l'accesso al supporto):

- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per OnCommand Insight"
- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per il data warehouse OnCommand Insight"
- "Come creare e importare un certificato firmato dall'autorità di certificazione (CA) in OnComand Insight e OnCommand Insight Data Warehouse 7.3.x"
- "Come creare un certificato autofirmato in OnCommand Insight 7.3.X installato su un host Windows"
- "Come importare un certificato firmato dall'autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"

A proposito di questa attività

Di seguito sono riportati i requisiti di configurazione del client più comuni:

- Installazione del middleware Smart Card, ad esempio ActivClient (vedere http://militarycac.com/activclient.htm)
- Modifica del browser IE (vedere http://militarycac.com/files/Making_AKO_work_with_Internet_Explorer_color.pdf)
- Modifica del browser Firefox (vedere https://militarycac.com/firefox2.htm)

Abilitazione del CAC su un server Linux

Alcune modifiche sono necessarie per abilitare il CAC su un server Linux OnCommand Insight.

Fasi

1. Selezionare `/opt/netapp/oci/conf/`
2. Modifica `wildfly.properties` e modificare il valore di `CLIENT_AUTH_ENABLED` A "vero"
3. Importare il “certificato root” esistente in `/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
4. Riavviare il server

Configurazione di Data Warehouse per l’accesso a smart card e certificati

È necessario modificare la configurazione del data warehouse di OnCommand Insight per supportare gli accessi con smart card (CAC) e certificati.

Prima di iniziare

- LDAP deve essere attivato nel sistema.
- LDAP `User principal account name` L’attributo deve corrispondere al campo LDAP che contiene il numero dell’ID governativo di un utente.

  Il nome comune (CN) memorizzato nei CAC emessi dal governo è normalmente nel seguente formato: `first.last.ID`. Per alcuni campi LDAP, ad esempio `sAMAccountName`, questo formato è troppo lungo. Per questi campi, OnCommand Insight estrae solo il numero ID dal CNS.

Per le istruzioni più aggiornate sul CAC e sul certificato, consulta i seguenti articoli della Knowledge base (è richiesto l'accesso al supporto):

- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per OnCommand Insight"
- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per il data warehouse OnCommand Insight"
- "Come creare e importare un certificato firmato dall'autorità di certificazione (CA) in OnComand Insight e OnCommand Insight Data Warehouse 7.3.x"
- "Come creare un certificato autofirmato in OnCommand Insight 7.3.X installato su un host Windows"
- "Come importare un certificato firmato dall'autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"

Fasi

1. Utilizzare regedit per modificare i valori del Registro di sistema in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. Modificare l'opzione JVM_Option `-DclientAuth=false` a. `-DclientAuth=true`.

   Per Linux, modificare `clientAuth` parametro in `/opt/netapp/oci/scripts/wildfly.server`

2. Aggiungere le autorità di certificazione (CA) al trustore del Data Warehouse:

   a. In una finestra di comando, passare a. `..\SANscreen\wildfly\standalone\configuration`.

   b. Utilizzare `keytool` Utility per elencare le CA attendibili: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      La prima parola in ciascuna riga indica l'alias della CA.

   c. Se necessario, fornire un file di certificato CA, di solito un `.pem` file. Per includere le CA del cliente con le CA attendibili del Data Warehouse, visitare il sito `..\SANscreen\wildfly\standalone\configuration` e utilizzare `keytool` comando di importazione: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      My_alias è in genere un alias che identificherebbe facilmente la CA in`keytool -list` operazione.

3. Sul server OnCommand Insight, la `wildfly/standalone/configuration/standalone-full.xml` Il file deve essere modificato aggiornando verify-client su "REQUESTED" in `/subsystem=undertow/server=default-server/https-listener=default-https`Per attivare CAC. Accedere al server Insight ed eseguire il comando appropriato:

SISTEMA OPERATIVO	Script

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

Dopo aver eseguito lo script, attendere il completamento del ricaricamento del server wildfly prima di passare al punto successivo.

4. Riavviare il server OnCommand Insight.

Configurazione dei Cognos per l'accesso con smart card e certificato (da OnCommand Insight 7.3.5 a 7.3.9)

È necessario modificare la configurazione del data warehouse di OnCommand Insight per supportare gli accessi con smart card (CAC) e certificati per il server Cognos.

Prima di iniziare

Questa procedura si applica ai sistemi che eseguono OnCommand Insight dalla versione 7.3.5 alla 7.3.9.

> Per le istruzioni più aggiornate sul CAC e sul certificato, consulta i seguenti articoli della Knowledge base (è richiesto l'accesso al supporto):
>
> - "Come configurare l'autenticazione della scheda di accesso comune (CAC) per OnCommand Insight"
> - "Come configurare l'autenticazione della scheda di accesso comune (CAC) per il data warehouse OnCommand Insight"
> - "Come creare e importare un certificato firmato dall'autorità di certificazione (CA) in OnComand Insight e OnCommand Insight Data Warehouse 7.3.x"
> - "Come creare un certificato autofirmato in OnCommand Insight 7.3.X installato su un host Windows"
> - "Come importare un certificato firmato dall'autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"

Fasi

1. Aggiungere le autorità di certificazione (CA) al trustore Cognos.
   a. In una finestra di comando, passare a. `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Utilizzare `keytool` Utility per elencare le CA attendibili: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      La prima parola in ciascuna riga indica l'alias della CA.

   c. Se non esistono file adatti, fornire un file di certificato CA, di solito un `.pem` file.

d. Per includere le CA del cliente con le CA attendibili di OnCommand Insight, visitare il sito Web all'indirizzo `..\SANscreen\cognos\analytics\configuration\certs\`.

e. Utilizzare `keytool` utility per importare `.pem` file: `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   `my_alias` È in genere un alias che identificherebbe facilmente la CA in`keytool -list` operazione.

f. Quando viene richiesta una password, immettere `NoPassWordSet`.

g. Risposta `yes` quando viene richiesto di considerare attendibile il certificato.

2. Per attivare la modalità CAC, eseguire `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. Per disattivare la modalità CAC, eseguire `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

Configurazione dei Cognos per l'accesso con smart card e certificato (OnCommand Insight 7.3.10 e versioni successive)

È necessario modificare la configurazione del data warehouse di OnCommand Insight per supportare gli accessi con smart card (CAC) e certificati per il server Cognos.

Prima di iniziare

Questa procedura riguarda i sistemi che eseguono OnCommand Insight 7.3.10 e versioni successive.

> Per le istruzioni più aggiornate sul CAC e sul certificato, consulta i seguenti articoli della Knowledge base (è richiesto l'accesso al supporto):
>
> - "Come configurare l'autenticazione della scheda di accesso comune (CAC) per OnCommand Insight"
> - "Come configurare l'autenticazione della scheda di accesso comune (CAC) per il data warehouse OnCommand Insight"
> - "Come creare e importare un certificato firmato dall'autorità di certificazione (CA) in OnComand Insight e OnCommand Insight Data Warehouse 7.3.x"
> - "Come creare un certificato autofirmato in OnCommand Insight 7.3.X installato su un host Windows"
> - "Come importare un certificato firmato dall'autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"

Fasi

1. Aggiungere le autorità di certificazione (CA) al trustore Cognos.

   a. In una finestra di comando, passare a. `..\SANscreen\cognos\analytics\configuration\certs\`

   b. Utilizzare `keytool` Utility per elencare le CA attendibili: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

La prima parola in ciascuna riga indica l'alias della CA.

c. Se non esistono file adatti, fornire un file di certificato CA, di solito un `.pem` file.

d. Per includere le CA del cliente con le CA attendibili di OnCommand Insight, visitare il sito Web all'indirizzo `..\SANscreen\cognos\analytics\configuration\certs\`.

e. Utilizzare `keytool` utility per importare `.pem` file: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   `my_alias` È in genere un alias che identificherebbe facilmente la CA in`keytool -list` operazione.

f. Quando viene richiesta una password, immettere `NoPassWordSet`.

g. Risposta `yes` quando viene richiesto di considerare attendibile il certificato.

2. Per attivare la modalità CAC, procedere come segue:

   a. Configurare la pagina di disconnessione CAC, seguendo questa procedura:

      - Accesso al portale Cognos (l'utente deve far parte del gruppo System Administrators, ad esempio cognos_admin)
      - (Solo per 7.3.10 e 7.3.11) fare clic su Manage (Gestisci)→ Configuration (Configurazione)→ System (sistema)→ Security (sicurezza)
      - (Solo per 7.3.10 e 7.3.11) inserire cacLogout.html rispetto all'URL di reindirizzamento disconnessione /→ richiedere
      - Chiudere il browser.

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

   c. Avviare il servizio IBM Cognos. Attendere l'avvio del servizio Cognos.

3. Per disattivare la modalità CAC, procedere come segue:

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

   b. Avviare il servizio IBM Cognos. Attendere l'avvio del servizio Cognos.

   c. (Solo per 7.3.10 e 7.3.11) Disconfigurare la pagina di disconnessione CAC, seguendo la procedura riportata di seguito:

      - Accesso al portale Cognos (l'utente deve far parte del gruppo System Administrators, ad esempio cognos_admin)
      - Fare clic su Manage (Gestisci)→ Configuration (Configurazione)→ System (sistema)→ Security (sicurezza)
      - Inserire cacLogout.html nell'URL di reindirizzamento disconnessione
      - Chiudere il browser.

Importazione di certificati SSL con firma CA per Cognos e DWH (Insight da 7.3.5 a 7.3.9)

È possibile aggiungere certificati SSL per abilitare l'autenticazione e la crittografia avanzate per l'ambiente Data Warehouse e Cognos.

Prima di iniziare

Questa procedura si applica ai sistemi che eseguono OnCommnand Insight dalla versione 7.3.5 alla 7.3.9.

> Per le istruzioni più aggiornate sul CAC e sul certificato, consulta i seguenti articoli della Knowledge base (è richiesto l'accesso al supporto):
>
> - "Come configurare l'autenticazione della scheda di accesso comune (CAC) per OnCommand Insight"
> - "Come configurare l'autenticazione della scheda di accesso comune (CAC) per il data warehouse OnCommand Insight"
> - "Come creare e importare un certificato firmato dall'autorità di certificazione (CA) in OnComand Insight e OnCommand Insight Data Warehouse 7.3.x"
> - "Come creare un certificato autofirmato in OnCommand Insight 7.3.X installato su un host Windows"
> - "Come importare un certificato firmato dall'autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"

A proposito di questa attività

Per eseguire questa procedura, è necessario disporre dei privilegi di amministratore.

Fasi

1. Creare un backup di `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. Creare un backup delle cartelle "certs" e "csk" in `..\SANScreen\cognos\analytics\configuration`.
3. Generare una richiesta di crittografia del certificato da Cognos. In una finestra Admin CMD, eseguire:
   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. Aprire `c:\temp\encryptRequest.csr` archiviare e copiare il contenuto generato.
5. Inviare il file EncryptRequest.csr all'autorità di certificazione (CA) per ottenere un certificato SSL.

   Assicurarsi di aggiungere altri attributi come "SAN:dns=FQDN (ad esempio, hostname.netapp.com)" per aggiungere SubjectAltName). Google Chrome versione 58 e successive si lamenta se SubjectAltName non è presente nel certificato.

6. Scarica i certificati della catena includendo il certificato root utilizzando il formato PKCS7

   In questo modo si scarica il file fqdn.p7b

7. Ottenere un certificato in formato .p7b dalla CA. Utilizzare un nome che lo contrassegna come certificato per il server Web Cognos.
8. ThirdPartyCertificateTool.bat non riesce ad importare l'intera catena, pertanto sono necessari più passaggi per esportare tutti i certificati. Suddividere la catena esportandole singolarmente come segue:
   a. Aprire il certificato .p7b in "Crypto Shell Extensions".

   b. Selezionare “Certificates” nel riquadro sinistro.
   c. Fare clic con il pulsante destro del mouse su CA principale > tutte le attività > Esporta.
   d. Selezionare l’output Base64.
   e. Immettere un nome di file che lo identifichi come certificato root.
   f. Ripetere i passaggi da 8a a 8c per esportare tutti i certificati separatamente in file .cer.
   g. Assegnare un nome ai file intermediateX.cer e cognos.cer.
9. Ignorare questo passaggio se si dispone di un solo certificato CA, altrimenti unire sia root.cer che intermediateX.cer in un unico file.
   a. Aprire Intermediate.cer con blocco note e copiare il contenuto.
   b. Aprire root.cer con blocco note e salvare il contenuto da 9a.
   c. Salvare il file come CA.cer.
10. Importare i certificati nel keystore Cognos utilizzando il prompt Admin CMD:
   a. cd "`Program Files/sanscreen/cognos/Analytics` bin"
   b. ThirdPartyCertificateTool.bat -java:local -i -T -r c

      In questo modo, CA.cer viene impostato come autorità di certificazione principale.

   c. ThirdPartyCertificateTool.bat -java:local -i -e -r c

      In questo modo, Cognos.cer viene impostato come certificato di crittografia firmato da CA.cer.

11. Aprire IBM Cognos Configuration.
   a. Selezionare Local Configuration (Configurazione locale)-→ Security (protezione) -→ Cryptography (crittografia) -→ Cognos
   b. Modifica “Usa CA di terze parti?” Su vero.
   c. Salvare la configurazione.
   d. Riavviare Cognos
12. Esportare il certificato Cognos più recente in cognos.crt utilizzando il prompt Admin CMD:
   a. "D: File di programma/SANscreen/java/bin/keytool.exe" -exportcert -file “c: Temp/cognos.crt” -keystore "D: File di programma/SANscreen/cognos/analytics/Configuration/CAMKeystore" -storetype PKCS12 -storepass NoPassSet -alias Encryption
13. Importare "`c:` temp cognos.crt" in dwh trustore per stabilire la comunicazione SSL tra Cognos e DWH, utilizzando la finestra del prompt Admin CMD.
   a. "D: File di programma/SANscreen/java/bin/keytool.exe" -importcert -file “c: Temp/cognos.crt” -keystore "D: File di programma/SANscreen/wildfly/standalone/configurazione/server.trustore" -storepass changeit -alias cognoschert
14. Riavviare il servizio SANscreen.
15. Eseguire un backup di DWH per assicurarsi che DWH comunichi con Cognos.

Importazione di certificati SSL con firma CA per Cognos e DWH (Insight 7.3.10 e versioni successive)

È possibile aggiungere certificati SSL per abilitare l’autenticazione e la crittografia

avanzate per l'ambiente Data Warehouse e Cognos.

Prima di iniziare

Questa procedura riguarda i sistemi che eseguono OnCommand Insight 7.3.10 e versioni successive.

> Per le istruzioni più aggiornate sul CAC e sul certificato, consulta i seguenti articoli della Knowledge base (è richiesto l'accesso al supporto):
>
> - "Come configurare l'autenticazione della scheda di accesso comune (CAC) per OnCommand Insight"
> - "Come configurare l'autenticazione della scheda di accesso comune (CAC) per il data warehouse OnCommand Insight"
> - "Come creare e importare un certificato firmato dall'autorità di certificazione (CA) in OnComand Insight e OnCommand Insight Data Warehouse 7.3.x"
> - "Come creare un certificato autofirmato in OnCommand Insight 7.3.X installato su un host Windows"
> - "Come importare un certificato firmato dall'autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"

A proposito di questa attività

Per eseguire questa procedura, è necessario disporre dei privilegi di amministratore.

Fasi

1. Arrestare Cognos utilizzando lo strumento di configurazione IBM Cognos. Chiudere Cognos.
2. Creare backup di `..\SANScreen\cognos\analytics\configuration` e. `..\SANScreen\cognos\analytics\temp\cam\freshness` cartelle.
3. Generare una richiesta di crittografia del certificato da Cognos. In una finestra Admin CMD, eseguire:
   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: In questo caso -H e -i devono aggiungere subjectAltNames come dns e ipaddress.
4. Aprire `c:\temp\encryptRequest.csr` archiviare e copiare il contenuto generato.
5. Inserire il contenuto EncryptRequest.csr e generare il certificato utilizzando il portale per la firma CA.
6. Scarica i certificati della catena includendo il certificato root utilizzando il formato PKCS7

   In questo modo si scarica il file fqdn.p7b

7. Ottenere un certificato in formato .p7b dalla CA. Utilizzare un nome che lo contrassegna come certificato per il server Web Cognos.
8. ThirdPartyCertificateTool.bat non riesce ad importare l'intera catena, pertanto sono necessari più passaggi per esportare tutti i certificati. Suddividere la catena esportandole singolarmente come segue:
   a. Aprire il certificato .p7b in "Crypto Shell Extensions".

   b. Selezionare “Certificates” nel riquadro sinistro.
   c. Fare clic con il pulsante destro del mouse su CA principale > tutte le attività > Esporta.
   d. Selezionare l’output Base64.
   e. Immettere un nome di file che lo identifichi come certificato root.
   f. Ripetere i passaggi da 8a a 8e per esportare tutti i certificati separatamente in file .cer.
   g. Assegnare un nome ai file intermediateX.cer e cognos.cer.
9. Ignorare questo passaggio se si dispone di un solo certificato CA, altrimenti unire sia root.cer che intermediateX.cer in un unico file.
   a. Aprire root.cer con blocco note e copiare il contenuto.
   b. Aprire intermediate.cer con blocco note e aggiungere il contenuto da 9a (intermedio prima e root avanti).
   c. Salvare il file come chain.cer.
10. Importare i certificati nel keystore Cognos utilizzando il prompt Admin CMD:
   a. cd "`Program Files/sanscreen/cognos/Analytics` bin"
   b. ThirdPartyCertificateTool.bat -java:local -i -T -r c
   c. ThirdPartyCertificateTool.bat -java:local -i -T -r c
   d. ThirdPartyCertificateTool.bat -java:local -i -e -r c
11. Aprire IBM Cognos Configuration.
   a. Selezionare Local Configuration (Configurazione locale)-→ Security (protezione) -→ Cryptography (crittografia) -→ Cognos
   b. Modifica “Usa CA di terze parti?” Su vero.
   c. Salvare la configurazione.
   d. Riavviare Cognos
12. Esportare il certificato Cognos più recente in cognos.crt utilizzando il prompt Admin CMD:
   a. cd "`C: Programmi/SANscreen"
   b. java keytool.exe -exportcert -file c: Temp cognos.crt -keystore cognos/analytics/Configuration/certs/CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias Encryption
13. Eseguire il backup del trustore del server DWH all’indirizzo`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. Importare "`c:` temp cognos.crt" in DWH trustore per stabilire la comunicazione SSL tra Cognos e DWH, utilizzando la finestra del prompt Admin CMD.
   a. cd "`C: Programmi/SANscreen"
   b. java/bin/keytool.exe -importcert -file c:/temp/cognos.crt -keystore wildfly/standalone/configurazione/server.trustore -storepass changeit -alias codnos3rdca
15. Riavviare il servizio SANscreen.
16. Eseguire un backup di DWH per assicurarsi che DWH comunichi con Cognos.
17. I seguenti passaggi devono essere eseguiti anche quando viene modificato solo il “sSL certificate” e i certificati Cognos predefiniti rimangono invariati. In caso contrario, Cognos potrebbe lamentarsi del nuovo certificato SANscreen o non essere in grado di creare un backup 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”`

In genere, questi passaggi vengono eseguiti nell’ambito del processo di importazione dei certificati Cognos descritto in "Come importare un certificato firmato dall’autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"