Suporte para Smart Card e certificado de login

OnCommand Insight

NetApp
October 24, 2024

Índice

Suporte para Smart Card e certificado de login

O OnCommand Insight suporta o uso de cartões inteligentes (CAC) e certificados para autenticar usuários fazendo login nos servidores do Insight. Tem de configurar o sistema para ativar estas funcionalidades.

Depois de configurar o sistema para suportar CAC e certificados, navegar para uma nova sessão do OnCommand Insight resulta no navegador exibindo uma caixa de diálogo nativa fornecendo ao usuário uma lista de certificados pessoais para escolher. Esses certificados são filtrados com base no conjunto de certificados pessoais que foram emitidos por CAs confiáveis pelo servidor OnCommand Insight. Na maioria das vezes, há uma única escolha. Por padrão, o Internet Explorer ignora essa caixa de diálogo se houver apenas uma opção.

Para usuários do CAC, os cartões inteligentes contêm vários certificados, apenas um dos quais pode corresponder à CA confiável. O certificado CAC para `identification` deve ser utilizado.

Para obter as instruções de CAC e certificado mais atualizadas, consulte os seguintes artigos da base de conhecimento (login de suporte necessário):

- "Como configurar a autenticação de cartão de acesso comum (CAC) para o OnCommand Insight"
- "Como configurar a autenticação de cartão de acesso comum (CAC) para o armazém de dados OnCommand Insight"
- "Como criar e importar um certificado assinado pela autoridade de certificação (CA) para o OnComand Insight e o Data Warehouse 7,3.x do OnCommand Insight"
- "Como criar um certificado autoassinado no OnCommand Insight 7,3.X instalado em um host Windows"
- "Como importar um certificado assinado pela autoridade de certificação (CA) do Cognos para o datawarehouse 7.3.3 e posterior do OnCommand"

Configurando hosts para Smart Card e login de certificado

Você deve fazer modificações na configuração do host do OnCommand Insight para oferecer suporte a logins de cartão inteligente (CAC) e certificado.

Antes de começar

- O LDAP tem de estar ativado no sistema.
- O atributo LDAP `User principal account name` deve corresponder ao campo LDAP que contém a ID de um usuário.

Se você alterou as senhas *Server.keystore* e/ou *Server.trustore* usando "administrador de segurança"o , reinicie o serviço *SANscreen* antes de importar o certificado LDAP.

Para obter as instruções de CAC e certificado mais atualizadas, consulte os seguintes artigos da base de conhecimento (login de suporte necessário):

- "Como configurar a autenticação de cartão de acesso comum (CAC) para o OnCommand Insight"
- "Como configurar a autenticação de cartão de acesso comum (CAC) para o armazém de dados OnCommand Insight"
- "Como criar e importar um certificado assinado pela autoridade de certificação (CA) para o OnComand Insight e o Data Warehouse 7,3.x do OnCommand Insight"
- "Como criar um certificado autoassinado no OnCommand Insight 7,3.X instalado em um host Windows"
- "Como importar um certificado assinado pela autoridade de certificação (CA) do Cognos para o datawarehouse 7.3.3 e posterior do OnCommand"

Passos

1. Use o `regedit` utilitário para modificar os valores do Registro no `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`:
   a. Altere a opção JVM_Option `DclientAuth=false` para `DclientAuth=true.`
2. Faça backup do arquivo keystore: `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Abra um prompt de comando especificando `Run as administrator`
4. Excluir o certificado gerado automaticamente: `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. Gerar um novo 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. Gerar uma solicitação de assinatura de certificado (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. Depois que o CSR for devolvido na etapa 6, importe o certificado e, em seguida, exporte o certificado no formato base-64 e coloque-o em `"C:\temp" named servername.cer.`
8. Extraia o certificado do 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. Extraia uma chave privada do arquivo p12: `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`

10. Mesclar o certificado base-64 que você exportou na etapa 7 com a chave 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 o certificado mesclado para o 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. Importar o certificado raiz: `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 o certificado raiz para o 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. Importar o certificado intermédio: `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 esta etapa para todos os certificados intermediários.
15. Especifique o domínio no LDAP para corresponder a este exemplo.
16. Reinicie o servidor.

Configurar um cliente para suportar Smart Card e login de certificado

As máquinas cliente requerem middleware e modificações nos navegadores para permitir o uso de Smart Cards e para login no certificado. Os clientes que já estão a utilizar cartões inteligentes não devem necessitar de modificações adicionais nas suas máquinas cliente.

Antes de começar

Para obter as instruções de CAC e certificado mais atualizadas, consulte os seguintes artigos da base de conhecimento (login de suporte necessário):

- "Como configurar a autenticação de cartão de acesso comum (CAC) para o OnCommand Insight"
- "Como configurar a autenticação de cartão de acesso comum (CAC) para o armazém de dados OnCommand Insight"
- "Como criar e importar um certificado assinado pela autoridade de certificação (CA) para o OnComand Insight e o Data Warehouse 7,3.x do OnCommand Insight"
- "Como criar um certificado autoassinado no OnCommand Insight 7,3.X instalado em um host Windows"
- "Como importar um certificado assinado pela autoridade de certificação (CA) do Cognos para o datawarehouse 7.3.3 e posterior do OnCommand"

Sobre esta tarefa

Os seguintes são os requisitos comuns de configuração do cliente:

- Instalando o middleware Smart Card, como o ActivClient (http://militarycac.com/activclient.htmconsulte)
- Modificação do navegador IE (http://militarycac.com/files/Making_AKO_work_with_Internet_Explorer_color.pdfconsulte)
- Modificação do navegador Firefox (https://militarycac.com/firefox2.htmconsulte)

Habilitando CAC em um servidor Linux

Algumas modificações são necessárias para habilitar o CAC em um servidor Linux OnCommand Insight.

A CA raiz deve ser importada para o repositório de confiança.

Passos

1. Navegue para `/opt/netapp/oci/conf/`
2. Editar `wildfly.properties` e alterar o valor de `CLIENT_AUTH_ENABLED` para "verdadeiro"
3. Importe o "'certificado raiz'" que existe em `/opt/netapp/oci/wildfly/standalone/configuration/server.truststore`
4. Reinicie o servidor

Configurando o Data Warehouse para Smart Card e login de certificado

Você deve modificar a configuração do Armazém de dados do OnCommand Insight para oferecer suporte a logins de cartão inteligente (CAC) e certificado.

Antes de começar

- O LDAP tem de estar ativado no sistema.
- O atributo LDAP `User principal account name` deve corresponder ao campo LDAP que contém o número de ID de governo de um usuário.

  A denominação comum (CN) armazenada em CAC emitidas pelo Governo é normalmente do seguinte formato: `first.last.ID`. Para alguns campos LDAP, como `sAMAccountName`, este formato é demasiado longo. Para esses campos, o OnCommand Insight extrai apenas o número de ID do CNS.

Se você alterou as senhas *Server.keystore* e/ou *Server.trustore* usando "administrador de segurança"o , reinicie o serviço *SANscreen* antes de importar o certificado LDAP.

Para obter as instruções de CAC e certificado mais atualizadas, consulte os seguintes artigos da base de conhecimento (login de suporte necessário):

- "Como configurar a autenticação de cartão de acesso comum (CAC) para o OnCommand Insight"
- "Como configurar a autenticação de cartão de acesso comum (CAC) para o armazém de dados OnCommand Insight"
- "Como criar e importar um certificado assinado pela autoridade de certificação (CA) para o OnComand Insight e o Data Warehouse 7,3.x do OnCommand Insight"
- "Como criar um certificado autoassinado no OnCommand Insight 7,3.X instalado em um host Windows"
- "Como importar um certificado assinado pela autoridade de certificação (CA) do Cognos para o datawarehouse 7.3.3 e posterior do OnCommand"

Passos

1. Use regedit para modificar os valores do Registro em `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. Altere a opção JVM_Option `-DclientAuth=false` para `-DclientAuth=true`.

   Para Linux, modifique o `clientAuth` parâmetro em `/opt/netapp/oci/scripts/wildfly.server`

2. Adicione autoridades de certificação (CAs) ao armazenamento de dados:

   a. Em uma janela de comando, vá para `..\SANscreen\wildfly\standalone\configuration`.

   b. Use o `keytool` utilitário para listar as CAs confiáveis: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>` Consulte "SecurityAdmin"a documentação para obter mais informações sobre como definir ou alterar a senha para Server_trustore.

   A primeira palavra em cada linha indica o alias da CA.

   c. Se necessário, forneça um arquivo de certificado da CA, geralmente um `.pem` arquivo. Para incluir as CAs do cliente com as CAs confiáveis do Data Warehouse, vá para `..\SANscreen\wildfly\standalone\configuration` e use o `keytool` comando de

importação: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

My_alias é geralmente um alias que identificaria facilmente a CA na`keytool -list` operação.

3. No servidor OnCommand Insight, o `wildfly/standalone/configuration/standalone-full.xml` arquivo precisa ser modificado atualizando Verify-client para "REQUESTED" em `/subsystem=undertow/server=default-server/https-listener=default-https`para ativar CAC. Faça login no servidor Insight e execute o comando apropriado:

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

Depois de executar o script, aguarde até que a recarga do servidor Wildfly esteja concluída antes de prosseguir para a próxima etapa.

4. Reinicie o servidor OnCommand Insight.

Configurando o Cognos para login de cartão inteligente e certificado (OnCommand Insight 7.3.10 e posterior)

Você deve modificar a configuração do Armazém de dados do OnCommand Insight para oferecer suporte a logins de cartão inteligente (CAC) e certificado para o servidor Cognos.

Antes de começar

Este procedimento destina-se a sistemas que executam o OnCommand Insight 7.3.10 e posterior.

Para obter as instruções de CAC e certificado mais atualizadas, consulte os seguintes artigos da base de conhecimento (login de suporte necessário):

- "Como configurar a autenticação de cartão de acesso comum (CAC) para o OnCommand Insight"
- "Como configurar a autenticação de cartão de acesso comum (CAC) para o armazém de dados OnCommand Insight"
- "Como criar e importar um certificado assinado pela autoridade de certificação (CA) para o OnComand Insight e o Data Warehouse 7,3.x do OnCommand Insight"
- "Como criar um certificado autoassinado no OnCommand Insight 7,3.X instalado em um host Windows"
- "Como importar um certificado assinado pela autoridade de certificação (CA) do Cognos para o datawarehouse 7.3.3 e posterior do OnCommand"

Passos

1. Adicione autoridades de certificação (CAs) à loja Cognos trustore.
   a. Em uma janela de comando, vá para `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Use o `keytool` utilitário para listar as CAs confiáveis: "…". keytool.exe -list -keystore CAMKeystore.jks -storepass <password>

      A primeira palavra em cada linha indica o alias da CA.

   c. Se não existirem ficheiros adequados, forneça um ficheiro de certificado de CA, normalmente um `.pem` ficheiro.
   d. Para incluir as CAs do cliente com as CAs confiáveis do OnCommand Insight, vá para `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. Use o `keytool` utilitário para importar o `.pem` arquivo: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` Geralmente é um alias que identificaria facilmente a CA na `keytool -list`operação.

   f. Quando for solicitada uma senha, insira a senha do arquivo */SANscreen/bin/cognos_info.dat*.
   g. Responda `yes` quando solicitado a confiar no certificado.
2. Para ativar o modo CAC, faça o seguinte:
   a. Configure a página de logout do CAC, seguindo as seguintes etapas:
      - Logon no portal Cognos (o usuário deve fazer parte do grupo Administradores do sistema, ou seja, cognos_admin)
      - (Apenas para 7.3.10 e 7,3.11) clique em Gerenciar → Configuração → sistema → Segurança
      - (Apenas para 7.3.10 e 7,3.11) Introduza cacLogout.html contra a URL Redirect Logout
      - Feche o navegador.
   b. Executar `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
   c. Inicie o serviço IBM Cognos. Aguarde que o serviço Cognos seja iniciado.
3. Para desativar o modo CAC, faça o seguinte:
   a. Executar `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
   b. Inicie o serviço IBM Cognos. Aguarde que o serviço Cognos seja iniciado.
   c. (Apenas para 7.3.10 e 7,3.11) Desconfigure a página de logout do CAC, seguindo os seguintes passos:
      - Logon no portal Cognos (o usuário deve fazer parte do grupo Administradores do sistema, ou seja, cognos_admin)
      - Clique em Gerenciar "→ Configuração "→ sistema "→ Segurança
      - Digite cacLogout.html contra o URL de redirecionamento de logout '→ aplicar
      - Feche o navegador.

Importação de certificados SSL assinados pela CA para Cognos e DWH (Insight 7.3.10 e posterior)

Você pode adicionar certificados SSL para habilitar autenticação e criptografia aprimoradas para seu ambiente Data Warehouse e Cognos.

Antes de começar

Este procedimento destina-se a sistemas que executam o OnCommand Insight 7.3.10 e posterior.

Para obter as instruções de CAC e certificado mais atualizadas, consulte os seguintes artigos da base de conhecimento (login de suporte necessário):

- "Como configurar a autenticação de cartão de acesso comum (CAC) para o OnCommand Insight"
- "Como configurar a autenticação de cartão de acesso comum (CAC) para o armazém de dados OnCommand Insight"
- "Como criar e importar um certificado assinado pela autoridade de certificação (CA) para o OnComand Insight e o Data Warehouse 7,3.x do OnCommand Insight"
- "Como criar um certificado autoassinado no OnCommand Insight 7,3.X instalado em um host Windows"
- "Como importar um certificado assinado pela autoridade de certificação (CA) do Cognos para o datawarehouse 7.3.3 e posterior do OnCommand"

Sobre esta tarefa

Tem de ter admin Privileges para executar este procedimento.

Passos

1. Pare o Cognos usando a ferramenta IBM Cognos Configuration. Feche o Cognos.
2. Crie cópias de segurança das `..\SANScreen\cognos\analytics\configuration` pastas e. `..\SANScreen\cognos\analytics\temp\cam\freshness`
3. Gerar uma solicitação de criptografia de certificado do Cognos. Em uma janela Admin CMD, execute:
   a. cd "`\Program Files\sanscreen\cognos\analytics\bin`"
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p <password> -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. Nota: Aqui -H e -I são para adicionar subjetivAltNames como dns e ipaddress.
   c. Para <password>, use a senha do arquivo */SANscreen/bin/cognos_info.dat*.
4. Abra o `c:\temp\encryptRequest.csr` arquivo e copie o conteúdo gerado.
5. Insira o conteúdo cryptRequest.csr e gere o certificado usando o portal de assinatura CA.
6. Faça o download dos certificados em cadeia incluindo o certificado raiz usando o formato PKCS7

   Isso fará o download do arquivo fqdn.p7b

7. Obtenha um cert no formato .p7b da sua CA. Use um nome que o marque como o certificado para o servidor Web do Cognos.
8. O ThirdPartyCertificateTool.bat não importa toda a cadeia, portanto são necessárias várias etapas para exportar todos os certificados. Divida a cadeia exportando-as individualmente da seguinte forma:
    a. Abra o certificado .p7b em "Crypto Shell Extensions".
    b. Navegue no painel esquerdo para ""certificados"".
    c. Clique com o botão direito do rato em CA raiz > todas as tarefas > Exportar.
    d. Selecione Base64 saída.
    e. Insira um nome de arquivo identificando-o como o certificado raiz.
    f. Repita as etapas 8a a 8e para exportar todos os certificados separadamente para arquivos .cer.
    g. Nomeie os arquivos intermediateX.cer e cognos.cer.
9. Ignore esta etapa se você tiver apenas um certificado de CA, caso contrário, mesclar root.cer e intermediateX.cer em um arquivo.
    a. Abra o root.cer com o bloco de notas e copie o conteúdo.
    b. Abra o Intermediate.cer com o bloco de notas e anexe o conteúdo do 9a (intermediário primeiro e raiz seguinte).
    c. Salve o arquivo como chain.cer.
10. Importe os certificados para o keystore do Cognos usando o prompt Admin CMD:
    a. cd "arquivos de programas" SANscreen
    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
11. Abra a configuração do IBM Cognos.
    a. Selecione Configuração local-→ Segurança -→ criptografia -→ Cognos
    b. Altere "usar CA de terceiros?" para verdadeiro.
    c. Salve a configuração.
    d. Reinicie o Cognos
12. Exporte o certificado Cognos mais recente para o cognos.crt usando o prompt Admin CMD:
    a. cd "C: Arquivos de programas" SANscreen
    b. -Storetype PKCS12 -storeppass <password> -alias Encryption keytool.exe
    c. Para <password>, use a senha do arquivo */SANscreen/bin/cognos_info.dat*.
13. Faça uma cópia de segurança da trustore do servidor DWH em`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. Importe o arquivo "'c: cognos.crt" para o repositório DWH para estabelecer uma comunicação SSL entre o Cognos e o DWH, usando a janela de prompt do Admin CMD.
    a. cd "C: Arquivos de programas" SANscreen
    b. keytool.exe -importcert -file c: /temp/cognos.crt -keystore wildfly/standalone/configuration/server.trustore -storeppass <password> -alias cognos3rdca
    c. Para <password>, use a senha do arquivo */SANscreen/bin/cognos_info.dat*.

15. Reinicie o serviço SANscreen.
16. Execute um backup da DWH para garantir que a DWH se comunique com o Cognos.
17. As etapas a seguir devem ser executadas mesmo quando apenas o "certificado ssl" é alterado e os certificados padrão do Cognos são mantidos inalterados. Caso contrário, a Cognos pode reclamar do novo certificado SANscreen ou não conseguir criar um 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 <password> -alias "ssl certificate"`

    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

    Normalmente, essas etapas são executadas como parte do processo de importação de certificados Cognos descrito em "Como importar um certificado assinado pela autoridade de certificação (CA) do Cognos para o datawarehouse 7.3.3 e posterior do OnCommand"

Informações sobre direitos autorais

Informações sobre marcas comerciais