支持智能卡和证书登录

OnCommand Insight

NetApp
April 01, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/oncommand-insight/config-admin/host-configuration-for-smart-card-and-certificate-login.html on April 01, 2024. Always check docs.netapp.com for the latest.

目录

支持智能卡和证书登录

OnCommand Insight 支持使用智能卡(CAC)和证书对登录到Insight服务器的用户进行身份验证。要启用这些功能、必须对系统进行配置。

将系统配置为支持CAC和证书后、导航到新的OnCommand Insight 会话会导致浏览器显示一个本机对话框、为用户提供一个可供选择的个人证书列表。这些证书将根据OnCommand Insight 服务器信任的CA颁发的一组个人证书进行筛选。大多数情况下、只有一个选择。默认情况下、如果只有一个选项、Internet Explorer将跳过此对话框。

对于CAC用户、智能卡包含多个证书、其中只有一个证书可以与受信任的CA匹配。的CAC证书 `identification` 应使用。

有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：

- "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
- "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
- "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
- "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
- "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

为主机配置智能卡和证书登录

您必须修改OnCommand Insight 主机配置、以支持智能卡(CAC)和证书登录。

开始之前

- 必须在系统上启用LDAP。
- LDAP `User principal account name` 属性必须与包含用户ID的LDAP字段匹配。

有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：

- "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
- "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
- "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
- "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
- "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

步骤

1. 使用 `regedit` 用于修改注册表值的实用程序

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java：

   a. 更改JVM_Option `DclientAuth=false` to `DclientAuth=true.`

2. 备份密钥库文件： `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. 打开指定的命令提示符 `Run as administrator`
4. 删除自生成的证书： `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. 生成新证书： `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. 生成证书签名请求(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. 在步骤6中返回CSR后、导入证书、然后以Base-64格式导出证书并将其放入 `"C:\temp" named servername.cer`。
8. 从密钥库提取证书：`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. 从p12文件提取私钥： `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. 将步骤7中导出的Base-64证书与私钥合并： `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. 将合并的证书导入到密钥库中： `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. 导入根证书： `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. 将根证书导入到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. 导入中间证书： `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"
```

对所有中间证书重复此步骤。

15. 在LDAP中指定与此示例匹配的域。
16. 重新启动服务器。

配置客户端以支持智能卡和证书登录

客户端计算机需要使用中间件并修改浏览器、才能使用智能卡并登录证书。已在使用智能卡的客户不需要对其客户端计算机进行其他修改。

开始之前

> 有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：
>
> - "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
> - "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
> - "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
> - "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
> - "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

关于此任务

以下是常见的客户端配置要求：

- 安装智能卡中间件、例如ActivClient (请参见
- 修改IE浏览器(请参见
- 修改Firefox浏览器(请参见

在Linux服务器上启用CAC

要在Linux OnCommand Insight 服务器上启用CAC、需要进行一些修改。

步骤

1. 导航到 `/opt/netapp/oci/conf/`
2. 编辑 `wildfly.properties` 并更改的值 `CLIENT_AUTH_ENABLED` 设置为"True"
3. 导入下存在的"`根证书`" `/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
4. 重新启动服务器

为智能卡和证书登录配置数据仓库

您必须修改OnCommand Insight 数据仓库配置以支持智能卡(CAC)和证书登录。

开始之前

- 必须在系统上启用LDAP。
- LDAP `User principal account name` 属性必须与包含用户的政府ID编号的LDAP字段匹配。

  政府颁发的CAC上存储的公用名(Common Name、CN)通常采用以下格式： `first.last.ID`。对于某些LDAP字段、例如 `sAMAccountName`、此格式太长。对于这些字段、OnCommand Insight 仅从CN中提取ID编号。

> 有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：
>
> - "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
> - "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
> - "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
> - "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
> - "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

步骤

1. 使用regedit修改中的注册表值 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. 更改JVM_Option `-DclientAuth=false` to `-DclientAuth=true`。

   对于Linux、修改 `clientAuth` 参数 `/opt/netapp/oci/scripts/wildfly.server`

2. 将证书颁发机构(CA)添加到数据仓库存储库：

   a. 在命令窗口中、转至 `..\SANscreen\wildfly\standalone\configuration`。

   b. 使用 `keytool` 用于列出受信任CA的实用程序： `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      每行中的第一个词表示CA别名。

   c. 如有必要、请提供CA证书文件、通常为 `.pem` 文件要将客户的CA加入到数据仓库受信任的CA中、请转至 `..\SANscreen\wildfly\standalone\configuration` 并使用 `keytool` 导入命令： `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      my_alias通常是一个可轻松在中标识CA的别名`keytool -list` 操作。

3. 在OnCommand Insight 服务器上、 `wildfly/standalone/configuration/standalone-full.xml` 需要通过在中将verify-client更新为"已请求"来修改文件 `/subsystem=undertow/server=default-server/https-listener=default-https`以启用CAC。登录到Insight服务器并运行相应的命令：

os	脚本
Windows	<install dir> \SANscreen\wildfly\bin\enableCACforRemoteEJB.bat
Linux	/opt/netapp/oci/wildfly/bin/enableCACforRemoteEJB.sh

   执行此脚本后、请等待此wildfly服务器的重新加载完成、然后再继续执行下一步。

4. 重新启动OnCommand Insight 服务器。

为智能卡和证书登录配置Cognos (OnCommand Insight 7.3.5至7.3.9)

您必须修改OnCommand Insight 数据仓库配置、以支持Cognos服务器的智能卡(CAC)和证书登录。

开始之前

此操作步骤 适用于运行OnCommand Insight 7.3.5至7.3.3的系统。

> 有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：
>
> - "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
> - "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
> - "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
> - "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
> - "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

步骤

1. 将证书颁发机构(CA)添加到Cognos truestore。
   a. 在命令窗口中、转至 `..\SANscreen\cognos\analytics\configuration\certs\`
   b. 使用 `keytool` 用于列出受信任CA的实用程序： `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      每行中的第一个词表示CA别名。

c. 如果不存在合适的文件、请提供CA证书文件、通常为 `.pem` 文件

d. 要将客户的CA与OnCommand Insight 可信CA结合使用、请转至 `..\SANscreen\cognos\analytics\configuration\certs\`。

e. 使用 `keytool` 用于导入的实用程序 `.pem` 文件： `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   `my_alias` 通常是一个可在中轻松标识CA的别名`keytool -list` 操作。

f. 当系统提示您输入密码时、输入 `NoPassWordSet`。

g. 问题解答 `yes` 当系统提示您信任此证书时。

2. 要启用CAC模式、请执行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

3. 要禁用CAC模式、请执行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

为智能卡和证书登录配置Cognos (OnCommand Insight 7.3.10及更高版本)

您必须修改OnCommand Insight 数据仓库配置、以支持Cognos服务器的智能卡(CAC)和证书登录。

开始之前

此操作步骤 适用于运行OnCommand Insight 7.3.10及更高版本的系统。

> 有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：
>
> - "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
> - "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
> - "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
> - "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
> - "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

步骤

1. 将证书颁发机构(CA)添加到Cognos truestore。

   a. 在命令窗口中、转至 `..\SANscreen\cognos\analytics\configuration\certs\`

   b. 使用 `keytool` 用于列出受信任CA的实用程序： `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      每行中的第一个词表示CA别名。

   c. 如果不存在合适的文件、请提供CA证书文件、通常为 `.pem` 文件

d. 要将客户的CA与OnCommand Insight 可信CA结合使用、请转至 `..\SANscreen\cognos\analytics\configuration\certs\`。

e. 使用 `keytool` 用于导入的实用程序 `.pem` 文件： `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   `my_alias` 通常是一个可在中轻松标识CA的别名`keytool -list` 操作。

f. 当系统提示您输入密码时、输入 `NoPassWordSet`。

g. 问题解答 `yes` 当系统提示您信任此证书时。

2. 要启用CAC模式、请执行以下操作：
   a. 使用以下步骤配置CAC注销页面：
      - 登录到Cognos门户(用户必须属于系统管理员组、例如Cognos_admin)
      - (仅适用于7.3.10和7.3.11)单击"管理"→"配置"→"系统"→"安全性"
      - (仅适用于7.3.10和7.3.11)针对注销重定向URL <→应用输入cacLogout.html
      - 关闭浏览器。
   b. 执行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
   c. 启动IBM Cognos服务。等待Cognos服务启动。
3. 要禁用CAC模式、请执行以下操作：
   a. 执行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
   b. 启动IBM Cognos服务。等待Cognos服务启动。
   c. (仅适用于7.3.10和7.3.11)使用以下步骤取消配置CAC注销页面：
      - 登录到Cognos门户(用户必须属于系统管理员组、例如Cognos_admin)
      - 单击"管理"→"配置"→"系统"→"安全性"
      - 在注销重定向URL <→应用中输入cacLogout.html
      - 关闭浏览器。

导入Cognos和DWH的CA签名SSL证书(Insight 7.3.5至7.3.9)

您可以添加SSL证书、以便为数据仓库和Cognos环境启用增强型身份验证和加密。

开始之前

此操作步骤 适用于运行OnCommnand Insight 7.3.5至7.3.9的系统。

有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：

- "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
- "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
- "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
- "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
- "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

关于此任务

要执行此操作步骤 、您必须具有管理员权限。

步骤

1. 创建的备份 `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`。
2. 在下创建"`certs`"和"`csk`"文件夹的备份 `..\ SANScreen\cognos\analytics\configuration`。
3. 从Cognos生成证书加密请求。在管理CMD窗口中、运行：
   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. 打开 `c:\temp\encryptRequest.csr` 归档并复制生成的内容。
5. 将encryptRequest.csr发送到证书颁发机构(CA)以获取SSL证书。

   请务必添加其他属性、例如"`San：dns=fqdn "(例如、hostname.netapp.com)`")以添加SubjectAltName。如果证书中缺少SubjectAltName、则Google Chrome 58及更高版本会进行投诉。

6. 使用PKCS7格式包含根证书以下载链证书

   此操作将下载FQDN.p7b文件

7. 从CA获取.p7b格式的证书。请使用一个名称将其标记为Cognos Web服务器的证书。
8. ThirdPartyCertificateTool.bat无法导入整个链、因此导出所有证书需要执行多个步骤。按如下所示单独导出链、从而拆分链：
   a. 在"`Crypto Shell扩展名`"中打开.p7b证书。
   b. 在左窗格中浏览到"`Certificates`"。
   c. 右键单击根CA >所有任务>导出。
   d. 选择Base64输出。
   e. 输入一个文件名、将其标识为根证书。
   f. 重复步骤8a到8c、将所有证书单独导出到.cer文件中。
   g. 将文件命名为intermediateX.cer和Cognos.cer。

9. 如果只有一个CA证书、请忽略此步骤、否则、请将root.cer和intermediateX.cer合并到一个文件中。
   a. 使用Notepad打开intermediate.cer并复制内容。
   b. 使用Notepad打开root.cer并保存9a中的内容。
   c. 将文件保存为CA.cer。
10. 使用管理CMD提示符将证书导入到Cognos密钥库中：
   a. cd “Program Files\SANscreen\cognos\Analytics \bin”
   b. ThirdPartyCertificateTool.bat -java：local -i -T -r c：\temp\cA.cer

      此操作会将CA.cer设置为根证书颁发机构。

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

      此操作会将Cognos.cer设置为由CA.cer签名的加密证书。

11. 打开IBM Cognos配置。
   a. 选择本地配置→安全性→加密→ Cognos
   b. 更改"`使用第三方CA？`" 设置为True。
   c. 保存配置。
   d. 重新启动Cognos
12. 使用管理CMD提示符将最新的Cognos证书导出到Cognos.crt：
   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 NoPassWordalias -encryption
13. 使用管理CMD提示符窗口将"`c：\temp\cognos.crt`"导入到dwh trustore中、以在Cognos和DWH之间建立SSL通信。
   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"-storepchangeit -alias cognoscert
14. 重新启动SANscreen 服务。
15. 执行DWH备份以确保DWH与Cognos通信。

导入Cognos和DWH的CA签名SSL证书(Insight 7.3.10及更高版本)

您可以添加SSL证书、以便为数据仓库和Cognos环境启用增强型身份验证和加密。

开始之前

此操作步骤 适用于运行OnCommand Insight 7.3.10及更高版本的系统。

有关最新的CAC和证书说明、请参见以下知识库文章(需要支持登录)：

- "如何为OnCommand Insight 配置通用访问卡(CAC)身份验证"
- "如何为OnCommand Insight 数据仓库配置通用访问卡(CAC)身份验证"
- "如何创建证书颁发机构(CA)签名证书并将其导入到OnComand Insight和OnCommand Insight 数据仓库7.3.x中"
- "如何在Windows主机上安装的OnCommand Insight 7.3.X中创建自签名证书"
- "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

关于此任务

要执行此操作步骤 、您必须具有管理员权限。

步骤

1. 使用IBM Cognos配置工具停止Cognos。关闭Cognos。
2. 创建的备份 `..\SANScreen\cognos\analytics\configuration` 和 `..\SANScreen\cognos\analytics\temp\cam\freshness` 文件夹。
3. 从Cognos生成证书加密请求。在管理CMD窗口中、运行：
   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"`。注意：此处的-H和-i将添加subjectAltNames、例如DNS和ipaddress。
4. 打开 `c:\temp\encryptRequest.csr` 归档并复制生成的内容。
5. 输入encryptRequest.csr内容并使用CA签名门户生成证书。
6. 使用PKCS7格式包含根证书以下载链证书

   此操作将下载FQDN.p7b文件

7. 从CA获取.p7b格式的证书。请使用一个名称将其标记为Cognos Web服务器的证书。
8. ThirdPartyCertificateTool.bat无法导入整个链、因此导出所有证书需要执行多个步骤。按如下所示单独导出链、从而拆分链：
   a. 在"`Crypto Shell扩展名`"中打开.p7b证书。
   b. 在左窗格中浏览到"`Certificates`"。
   c. 右键单击根CA >所有任务>导出。
   d. 选择Base64输出。
   e. 输入一个文件名、将其标识为根证书。
   f. 重复步骤8a到8e、将所有证书单独导出到.cer文件中。
   g. 将文件命名为intermediateX.cer和Cognos.cer。

9. 如果只有一个CA证书、请忽略此步骤、否则、请将root.cer和intermediateX.cer合并到一个文件中。
   a. 使用Notepad打开root.cer并复制内容。
   b. 使用Notepad打开intermediate.cer、然后附加9a中的内容(中间优先、根下一个)。
   c. 将文件另存为chain.cer。
10. 使用管理CMD提示符将证书导入到Cognos密钥库中：
   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. 打开IBM Cognos配置。
   a. 选择本地配置→安全性→加密→ Cognos
   b. 更改"`使用第三方CA？`" 设置为True。
   c. 保存配置。
   d. 重新启动Cognos
12. 使用管理CMD提示符将最新的Cognos证书导出到Cognos.crt：
   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. 备份DWH服务器数据存储库`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. 使用管理CMD提示符窗口将"`c：\temp\cognos.crt`"导入到DWH存储中、以便在Cognos和DWH之间建立SSL通信。
   a. CD "`C：\Program Files\SANscreen"
   b. java.bin\keytool.exe -importcert -file c：\temp\cognos.crt -keystore wildfly\standalone\configuration\server.trusstore -storepass changeit -alias cognos3rdca
15. 重新启动SANscreen 服务。
16. 执行DWH备份以确保DWH与Cognos通信。
17. 即使仅更改了`sSL证书`且默认Cognos证书保持不变、也应执行以下步骤。否则、Cognos可能会抱怨新的SANscreen 证书或无法创建DWH备份。
   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”`

   通常、这些步骤会在中所述的Cognos证书导入过程中执行 "如何将Cognos证书颁发机构(CA)签名证书导入到OnCommand 数据中心7.3.3及更高版本中"

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。