IBM Business Analytics Proven Practices: Configure Cube Designer for accessing an SSL enabled BI Gateway

Product(s): IBM Cognos BI - Cube Designer; Area of Interest: Security; Version 1.0

Business Analytics Proven Practices Team
Business Analytics Proven Practices Team
IBM

05 June 2014

An explanation of the steps required to configure IBM Cognos BI Cube Designer for accessing a Secure Sockets Layer (SSL) enabled Cognos BI Gateway.

View more content in this series

Introduction

Purpose of Document

This document explains the steps required to configure IBM Cognos BI Cube Designer for accessing a Secure Sockets Layer (SSL) enabled Cognos BI Gateway.

Applicability

The steps described herein were tested using IBM Cognos BI 10.2.1.1 and to the best knowledge of the author, they also apply to all other versions.

Exclusions and Exceptions

This document will not explain the Network Security Services (NSS)/Netscape Portable Runtime (NSPR) library tools required for managing Netscape keystores other than providing hints on how to obtain them. For details the reader must consult Netscape/Mozilla documentation.

Assumptions

The reader is expected to be familiar with SSL in general as well as Public Key Infrastructure (PKI) concepts such as keystores and certificates.
Architecture and Technical Background

IBM Cognos BI Cube Designer is a think client written in Java using the Eclipse Framework. It reaches out to the IBM Cognos BI Dispatcher URI for external applications and the IBM Cognos BI Gateway URI. Both URIs are specified in the IBM Cognos Configuration tool for the Cube Designer install. Both communication paths can potentially use the Secure Socket Encryption (SSL) protocol if the web server hosting the Cognos BI Gateway and/or the Dispatcher have been configured for it.

When Cube Designer is started, it looks for an already authenticated session to Cognos BI which could have been passed to it from Framework Manager (Cube Designer can be launched from Framework Manager) in the form of some binary information known as a cam_passport. If no such session is found, Cube Designer will reach out to the configured Gateway URI to trigger the authentication process with Cognos BI.

Once an authenticated session is established or the pre-existing session was successfully verified, Cube Designer will communicate with the Relational Metadata Service of IBM Cognos BI. Requests are sent to the URI configured for Dispatcher URI for external applications property in Cognos Configuration.

The communication between Cube Designer and the Dispatcher URI is using the certificates generated by the IBM Cognos BI CAM-CRP component unless the Cognos BI Dispatcher that Cube Designer is reaching out to was deployed to a Java Application Server instead of the Apache Tomcat that is included and pre-deployed with IBM Cognos BI or if a third-party certificate authority (CA) was configured for Cognos BI. Either case, however, does not require any additional configuration steps to be applied to Cube Designer to allow it to support the SSL communication. The reasoning behind this is that both scenarios - SSL for the Dispatcher using CAM-CRP certificates or a third-party CA - require configuration changes to be applied in IBM Cognos Configuration to make the system work. Along with these configuration steps, the proper certificates required to allow SSL communication to the remote Cognos BI Dispatcher will be made available to Cube Designer implicitly.

However, the same does not apply to communication to the configured Cognos BI Gateway URI. As with other clients (such as Framework Manager) that use similar communication paths, Cube Designer employs an embedded browser component to connect to the Cognos BI Gateway as a client. This is important because the Cognos BI Gateway may be protected by a security solution that employs redirects and other HTTP protocol based techniques to implement authentication and this may form part of a single sign-on (SSO) solution to Cognos BI.

To support SSL communication to the Cognos BI Gateway, the embedded browser component needs to establish trust to the server certificate presented by the web server when reaching out to the Cognos BI Gateway.

Where Framework Manager uses an embedded Microsoft Internet Explorer (IE) browser in the form of IECtrl, Cube Designer uses a component provided by the Mozilla organization called XULRunner. This component is essentially an embedded Mozilla browser (such as Firefox) which
is built around the same component. For it to support communication to an SSL enabled server, the server certificate must be trusted, which implies having the adequate CA certificate available in a truststore.

The IEControl shares keystores, and thus the truststore, with the regular IE browser. This means that if the required certificates have been imported using IE on that very same machine, they will be available to the IEControl automatically. Thus SSL communication works for IEControl without any additional configuration required. If IE shows no errors or warnings when reaching out to the Cognos BI Gateway, it’s safe to assume IEControl to be working flawlessly in that regard as well. If IE shows errors or warnings, the same issues will prevent IEControl from functioning. However, the Mozilla XULRunner does not share keystores with other Mozilla-based browsers which might be installed on the same machine. Instead, XULRunner uses its own profile. A profile exists for every user of a Mozilla-based browser on a given computer and is stored on the local machine in a dedicated folder. The name of the folder is composed of a base path dictated by the underlying operating system and two sub-folder names the application can specify. One folder is named after the organization (e.g. “Mozilla”) and the other names the actual application (e.g. “Firefox”).

In this profile folder, there exists a Netscape Security Services (NSS) format keystore (referred to by Netscape as a certificate database) which consists of 3 files,

- cert8.db
- key3.db
- secmod.db

This keystore contains all certificates used for SSL communication. To establish trust to a server certificate, the proper CA certificate needs to be imported into this keystore. Since NSS uses a proprietary format management of the keystore, you must use the certutil tool provided by NSS at https://developer.mozilla.org/en/docs/NSS/tools/NSS_Tools_certutil. Note that Microsoft also has a tool named certutil and it does not work with the NSS keystore.

Unfortunately there is no recent binary version of that tool provided by Mozilla, so one has to either build the binary from the source code, use some older version which might have a binary or search the Internet for someone to provide a binary. The IBM Cognos BI authentication provider for LDAP also leverages the NSS toolkit to handle SSL encryption. The same requirement of managing an NSS key database applies here. Refer to the IBM Technote at http://www.ibm.com/support/docview.wss?uid=swg21344083 for some hints and tips on how to obtain the NSS toolkit.

It should be pointed out that many Linux distributions already contain a version of the binary. Since the certificate database is platform agnostic, it does not matter on which platform the certificate database is built/managed. Therefore, if there is access to a Linux workstation or server, one can use this Linux environment to build and manage the database and then simply copy the three files specified above that make up the database over to the working environment.

**Adding a CA Certificate to Cube Designer's Truststore**

This section will describe how to import a CA certificate to the Cube Designer's truststore.
1. Obtain the certificate which either directly or indirectly signed the server certificate used by the endpoint referred to by the **Gateway URI property** in IBM Cognos Configuration. This is usually the CA certificate which signed the server certificate of the web server hosting the IBM Cognos BI Gateway but it could also be a certificate chain containing intermediate CA certificates. If the Gateway-URI property refers to a load balancer or a reverse proxy, the appropriate signing certificate is required for those. The certificate should be in PEM or DER format.

   For the remainder of this document we assume a single CA certificate by the name of `ca.cer`.

2. Obtain the NSS **certutil** tool.

3. Locate the XULRunner profile directory. Cube Designer uses **Mozilla** and **eclipse** for the application specific sub-folder names in the profile path. For details on how to locate the Mozilla profile folder, refer to [https://support.mozilla.org/en-US/kb/profiles-where-firefox-stores-user-data](https://support.mozilla.org/en-US/kb/profiles-where-firefox-stores-user-data). For example, on Windows 7 or Windows 2008 the folder is usually, `C:\Users\<LoggedIn_Windows_User>\AppData\Roaming\Mozilla\eclipse`

   Note that the Cube Designer XULRunner profile path might clash with other installs of the Eclipse framework on the same computer which are using Mozilla libraries. Check to see if the profile directory already exists before creating a new key database. If it exists and it's possible to re-configure Eclipse, backup the original files first and re-configure Eclipse to avoid sharing a key database.

4. Use the `certutil` tool to add the CA certificate to the certificate database with the following command,

   ```shell
   certutil -A -n <alias> -d <profile_directory> -i <ca.cer> -t C,C,C
   ```

   where `<profile_directory>` is the profile directory and `<alias>` is a simple arbitrary label to identify the certificate in the certificate database.

   This will add the CA certificate contained in the file specified by `<ca.cer>` to the database and allow it to be used to verify trust for server certificates.

5. Restart Cube Designer and verify that access to the Cognos BI Gateway is working.

### Appendix A – Use Firefox instead of certutil (alternate approach)

In the case where there is no certutil available but there is a local install of Mozilla Firefox, there is a somewhat crude but simple way of adding the certificate to the Cube Designer XULRunner certificate database.

This approach is about copying the certificate database used by the browser to XULRunner. The security implication is that all certificates ever imported by the browser and all personal certificates used by it will be available to XULRunner – something which may or may not be acceptable. This approach is meant as a work-around and quick way to determine if the general solution is working. The best practice clearly is to create a certificate database specifically for XULRunner, which contains the minimal set of certificates required to allow communication to the Cognos BI Gateway.

This technique has been tested using Mozilla Firefox ESR 24 on Windows and to the authors best knowledge, it should work using earlier versions of Mozilla.
1. Use the local copy of Firefox to access the Cognos BI Gateway. In case of any certificate warnings, consider fixing them before adding an exception or importing the proper CA certificate.

2. Obtain the proper CA certificate which signed the certificate presented when accessing the Cognos BI Gateway.

3. Open an instance of a file explorer and locate the Cube Designer profile directory. Select the three files comprising the certificate database - cert8.db, key3.db and secmod.db - and back them up to a safe location.

4. With Firefox opened, find the Options or Preferences menu, click on the Advanced button and click on the Certificates tab.

5. Click on View Certificates and then click on Authorities tab.

6. Click Import..., locate the CA certificate obtained in step 2, and then click OK. A message will confirm the import of the certificate.

7. Click OK to close the Certificate Manager, and then click OK to close the Options.

8. Click Help > Troubleshooting Information.

9. Locate the Profile Directory property in the very first table on that page being shown. Click on the button next to it to open the profile folder in a file explorer.

10. When the file explorer opens, select the three files comprising the certificate database and copy them to the clipboard.

11. Go back to the file explorer opened in step 3, navigate back to the Cube Designer profile directory and paste the three files to this location, making sure to overwrite existing files.

By following these steps, one will have copied the Firefox certificate database for use by XULRunner. After restarting Cube Designer, the SSL access should work.
Resources

- Netscape Security Services Library Documentation
- Configuring LDAPS communication for IBM Cognos BI authentication
- How to locate the Mozilla profile directory
About the author

Business Analytics Proven Practices Team

© Copyright IBM Corporation 2014
Trademarks
(www.ibm.com/developerworks/ibm/trademarks/)