apigee

Edge Security

Configuring TLS on an Edge Message Processor

Google Cloud

Agenda

- Prerequisites
- Create obfuscated password
- Create and secure keystore
- Configure Edge Message Processor

apigee

Prerequisites

In order to configure TLS, port 8082 need to be open between the routers and message processors.

From an Edge Router :

```
curl http://<message_processor_ip>:8082/v1/servers/self/uuid
```

Should return the UUID. This needs to be tested between each router and message processor in the region.

Create Obfuscated Password

Some parts of the Edge TLS configuration procedure require you to enter an obfuscated password in a configuration file. An obfuscated password is a more secure alternative to entering your password in plain text.

You can generate an obfuscated password in Java by using the Jetty .jar files installed with Edge.
Example with output : (jar versions will be specific to installed version of Edge)

```
java -cp \
/opt/apigee/edge-gateway/lib/thirdparty/jetty-http-8.0.4.v20111024.jar:/opt/apigee/edge-gateway/
lib/thirdparty/jetty-util-8.0.4.v20111024.jar org.eclipse.jetty.http.security.Password TestMe
```

Output :

```
TestMe
OBF:1ppq1od31yta1ytc1obr1pqo
MD5:2c539f7b23fc3fb3b8ec52d3bfa58834
```

Create and Secure the keystore

Create the keystore as previously described using the private key for the server and an appropriate certificate:

Copy the keystore to a location accessible by the Apigee user, e.g.

```
cp message_processor_keystore.jks /opt/apigee/customer/application/mp_keystore.jks
```

Secure the keystore, e.g.

```
chown apigee:apigee /opt/apigee/customer/application/mp_keystore.jks
chmod 600 !$
```

Configuring the Message Processor

Having created a java keystore and an obfuscated password it’s possible to configure the Message Processor to use TLS.

The following should be appended to: `/opt/apigee/customer/application/message-processor.properties:`

```
conf_message-processor-communication_local.http.ssl=true
conf/message-processor-communication.properties+local.http.port=8443
conf/message-processor-communication.properties+local.http.ssl.keystore.type=jks
conf/message-processor-communication.properties+local.http.ssl.keystore.path=/opt/apigee/customer/application/keyStore.jks
conf/message-processor-communication.properties+local.http.ssl.keyalias=apigee-devtest
# Enter the obfuscated keystore password below.
conf/message-processor-communication.properties+local.http.ssl.keystore.password=OBF:obsPword
```

After completing the change on all message processors, restart all routers and message processors.

apigee

Thank You

Google Cloud